보안, 그 이상의 믿음

보안SI를 통한

IT정보보호 구축 가이드

Ver3.0

보안SI사업팀

Global Leading Digital Security Company

보안SI를 통한

IT정보보호 구축 가이드

Ver3.0

보안SI사업팀

SK infosec
Global Leading Digital Security Company

이 문서에 작성된 내용은 SK인포섹 지식자산을 기준으로 작성하였으며, 제품소개는 솔루션 벤더사의 솔루션 소개서와 브로셔, 벤더사 홈페이지의 공유된 공개자료를 활용하여 기능과 특징을 작성하였습니다.

『보안SI를 통한 IT정보보호 구축 가이드』 배포 목적 및 구성

본 문서는 SK인포섹의 '보안SI사업팀'에서 금융권, 제조사, 일반기업, 공공기관, 의료기관 등을 대상으로 정보보안 관련 시스템 구축을 위해 제작하였습니다. 구축 가이드는 우선적으로 고려해야 할 Compliance, 보안 시스템 전체 구성에 대한 미비점 확인 방안, 시스템 구축 시 미리 알아야 할 점 등을 담았으며, 새로운 시스템 구축이나 고도화 계획에 도움을 드리고자 합니다.

제1편 '총괄'은 Compliance, 정보보안 패러다임, 총괄적인 정보보안 시스템 아키텍처로 구성하였습니다. IT정보보호의 근거인 Compliance와 기본을 정립하고 정보보안을 위한 시스템 아키텍처 설명으로 시작합니다.

제2편 '영역별 보안'에서는 실제 시스템을 구축하는 포인트로 통합보안관제 시스템 (SIEM, SOAR 개념 및 구축방안), 계정권한 관리시스템 (통합 권한관리 및 모니터링 시스템), 정보보안 포털 시스템, 이상징후 탐지시스템으로 구성하였습니다. 제2편에서는 영역별 시스템 개념, 구성도, 사전 준비사항 및 주요 구축 내용에 대해 설명하였습니다.

제3편 '솔루션별 보안'에서는 사용자 보안, 시스템 보안, 네트워크 보안의 일반적인 솔루션 설명으로 실제 구축 시 참고 자료로 활용할 수 있도록 하였습니다.

제4편 '기업유형별 보안'에서는 제조업의 스마트 팩토리 보안, 의료정보 보안, 금융 핀테크 보안에 대해서 기업의 유형별 보안의 특성과 보안SI구축에 대한 가이드를 참고할 수 있도록 하였습니다.

문서 내용 중에서, 특정 제품의 일부 기능에 대한 소개는 있을 수 있으나, 제품 홍보나 구매를 유도하는 의사가 없음을 명확히 밝히며, 보안영역의 학습과 참고를 목적으로 기능 위주로 설명하였습니다.

SK인포섹 보안SI사업팀은 다년간 정보보호 시스템 구축 경험을 통해 영역별 구축 방법론과 전문역량 인력을 다수 보유하고 있습니다. 고객의 정보보안을 위해 사업계획수립부터 시스템 구축과 유지보수까지 동행하겠습니다.

세계 일류의 Security Service를 목표로

대한민국 보안산업을 선도하는 SK인포섹

하나, 고객에게 믿음을 주는 회사가 되려 합니다.

둘, 고객의 행복을 실현하려 합니다.

셋, 믿음과 행복을 주는 SK인포섹입니다.

SK인포섹은 지난 2000년에 설립한 이래로 '고객의 행복 추구'라는 SK의 경영철학을 이어받아 ICT산업 분야에서 고객의 안전과 행복을 위해 뛰고 있습니다.

SK인포섹은 날로 고도화되고 있는 ICT기술의 성장과 변화무쌍한 시장환경 속에도 지속적인 경영혁신과 기술개발, 인재양성을 통해 거듭 성장하고 있습니다.

이제 정보보안 서비스를 비롯해 솔루션, 융합보안, 고객 IT서비스 분야에서도 국내를 넘어 세계 일류의 기업이 되도록 최선을 다하겠습니다.

The Trust beyond Security

고객 여러분과 믿음의 관계를 만들어 가겠습니다.

SK 인포섹 사업영역

보안컨설팅

- Compliance
- 정보보호관리체계
- 개인정보보호
- 종합정보보안
- 취약점점검/모의해킹
- ICT/Biz. 컨설팅

보안관제

- 원격 관제 (Big Data플랫폼)
- 파견 관제 (SIEM/ESM)
- 클라우드 관제
- Intelligence 관제
- Top-CERT(침해대응)
- Forensics

보안SI / 보안솔루션

시스템 통합 구축					Server/Application				Endpoint			
보안 관제 (SIEM)	계정관리 / 접근통제	정보보안 포털	이상징후 시스템	기타 SI	E-mail APT 대응	웹쉘 탐지	악성 코드 탐지	개인 정보 보호 (서버)	개인 정보 보호 (단말)	모바일 보안	IoT 보안	PC 가상화

융합보안

- 물리융합보안컨설팅
- 물리보안시스템 구축
- 통합 상황실 구축
- 메인컨트롤러/SW 보유

IT통합상담&PC/OA공급 서비스

- IT Service Desk & IT/보안 Call Center
- 차세대 One Stop Total OA 서비스
- 시스템 기반 자산관리
- PC/OA 공급서비스

Connect everything, Secure everything

보안, 그 이상의 믿음

보안SI를 통한 IT정보보호 구축 가이드

CONTENT

Connect everything, Secure everything

보안, 그 이상의 믿음

보안SI를 통한 IT정보보호 구축 가이드

CONTENT

총괄

CONTENT

총괄

2. 정보보호 위협 패러다임 변화

1) 언택트 패러다임 변화
   가. 언택트 정의
   나. 언택트 보안 위협
   다. 언택트 보안 위협 분석
   라. 언택트 보안 위협 사례
   마. 언택트 보안 위협 대응방안
2) 금융보안원 2021년 디지털금융 및 사이버보안 이슈 전망
3) KISA 2021년 사이버 위협 전망
   가. KISA `21년 사이버 위협 전망 보도
   나. 글로벌 사이버 위협 전망
   다. 국내 사이버 위협 인텔리전스 전망
4) SK인포섹 EQST 2021년 5대 사이버 위협 전망

3. 정보보호 시스템 아키텍처

1) 정보보호 시스템 개념도
2) 정보보호기술 프레임워크
   가. 정보보호기술 아키텍처
   나. 정보보호기술 아키텍처 구성요소
   다. 정보보호기술 요구항목
   라. 정보보호 영역별 구성도
3) 영역별 보안 아키텍처

Part 1

Compliance

1) 정보보호 기본 법령

Compliance란 법규준수/준법감시/내부통제 등 조직이 사회적, 기업적 업무를 수행하면서 반드시 준수해야 할 의무를 말합니다. 정보보호를 위한 위험통제 기술과, 활동은 기업의 손실을 최소화하고 예방할 수 있습니다.

국가가 제·개정한 정보보호 관련 법령은 보안 부분에 있어 반드시 지켜야 하는 필수 요건입니다. 개인정보 및 중요 산업정보를 관리하는 기업은 정보보호 관련 법령을 잘 준수해야 하고, 이를 회사의 규정/지침에 반영하였는지 반드시 검토해야 합니다.

아래 표는 산업별로 정보보호 관련 법령의 주요사항에 대한 주요 법령 내역에 대한 소개입니다.

산업 구분	금융	통신	정보통신 서비스 사업	제조업	보건·의료
보호해야 할 주요대상	개인정보 금융거래정보 계좌정보	통신기반시설 IDC 고객정보	고객(개인)정보	지적재산권, 핵심인력/기술 산업기반시설	개인정보 바이오 정보(의료)
컴플라이언스 (개인)정보 보호	전자금융거래법 전자금융감독규정 신용정보 보호법	정보통신망법	정보통신망법	산업기술의 유출방지 및 보호에 관한 법률, 부정경쟁방지법, 정보통신망법	의료법 국민건강보험법 산업안전보건법
	정보통신기반 보호법, 개인정보보호법				
보안대응	개인(신용)정보 유출, 외부해킹 대응, 망분리	새로운 서비스, 선제적 보안대응	개인정보 유출, 외부해킹 대응	제어정보 시스템보호, 망분리	개인정보(진료정보, 바이오 정보) 유출, 외부해킹 대응
대상	은행, 증권, 보험, 카드사 등	유무선 통신 사업자 (SKT, KT, LG U+ 등) IDC사업자	포털, 게임사, 쇼핑몰, 여행, 의료, 교육 등	에너지, 화학, 반도체, 건설	의료기관[1]

[표 Ⅰ-1. 산업별 정보보호 기본 법령]

1) 의료기관 : 「의료법」 제3조 제2항에 따른 의원급 의료기관, 조산원, 병원급 의료기관

2) 2020년 개정된 데이터 3법[1)]

가. 데이터 3법 정의

데이터 3법이란 개인정보보호법, 정보통신망법, 신용정보법에서 정의한 개인정보 규정에 대해 2020년 8월 5일부터 시행된 개정법입니다.

개인정보 보호법

정보통신망법
(정보통신망 이용촉진 및 정보보호 등에 관한 법률)

신용정보법
(신용 정보의 이용 및 보호에 관한 법률)

나. 주요내용

구분	주요 개정 사항
개인정보 보호법	• 가명정보 개념 도입 – 개인정보와 관련된 개념체계를 개인정보·가명정보·익명정보로 분류 – 가명정보를 정보주체 동의 없이 통계작성, 과학적 연구, 공익적 기록보존 등 목적으로 처리 가능 – 서로 다른 기업이 보유하는 가명정보는 보안시설을 갖춘 전문기관을 통해 결합할 수 있도록 함 – 가명정보를 처리하거나 정보 집합물을 결합하는 경우 안전성 확보조치를 하도록 하고, 특정 개인을 알아보는 행위 금지, 위반 시 형사벌, 과징금 등의 벌칙 부과 • 정보주체의 동의 없이 이용할 수 있는 개인정보 범위 구체화 – 수집 목적과 합리적으로 관련된 범위 내에서 대통령령이 정하는 바에 따라 정보주체 동의 없이 개인정보의 이용·제공 허용 • 개인정보의 범위 명확화 – 익명정보의 법 적용 배제 명확화
정보통신망법	• 개인정보보호 관련사항 「개인정보보호법」으로 이관 • 개인정보 보호관련 구제와 감독 주체를 '개인정보보호위원회'로 변경
신용정보법	• 금융분야 빅데이터 분석·이용 법적 근거 명확화 – 가명정보는 통계작성(상업적 목적 포함), 연구(상업적 목적 포함), 공익적 기록보존 목적으로 동의 없이 활용 가능 – 데이터 결합의 법적 근거 마련하되 국가지정 전문기관 통한 데이터 결합만 허용 • 금융분야 개인정보보호 강화 – 본인 정보를 다른 금융회사 등으로 제공토록 요구 가능한 '개인신용정보 이동권' 도입 – 금융회사 등 개인 신용정보 유출에 대한 징벌적 손해 배상금 강화 (손해액 3배~5배)

[표 I -2. 데이터 3법 개정안 주요내용]

1) 데이터 3법 : 개인정보보호에 관한 법이 소관 부처별로 나뉘어 있기 때문에 생긴 불필요한 중복 규제를 없애 4차 산업혁명의 도래에 맞춰 개인과 기업이 정보를 활용할 수 있는 폭을 넓히기 위해 마련됐다. 이 3법은 2018년 11월 국회에 발의되었고 2020년 1월 9일 열린 본회의에서 통과됐으며, 그해 8월 5일부터 시행에 들어갔다.

법령 개정을 통해 개인정보의 개념을 개인정보·가명정보·익명정보로 분류하고 가명정보를 통계작성, 연구, 공익적 기록보존 목적으로 활용하게 하였습니다.

	개인정보	가명정보	익명정보
개념	개인을 판별할 수 있는 개인 정보	추가정보 없이는 특정개인 판별 불가	개인정보 판별 불가
예시	성명 주민등록번호 휴대폰 번호 주소지 소득 연 6,000만원 비만	홍길동 80년생, 남자 경기도 성남 소득 연 5,000 ~ 6,000만원대 비만	40대, 남자 소득 연 5,000 ~ 6,000만원대 비만
활용가능 범위	사전적, 구체적 개인정보 활용동의를 받은 범위 내 활용 가능	다음 목적에 동의 없이 활용가능 (EU GDPR[1] 반영) ① 통계작성(상업적 목적 포함) ② 연구(상업적 목적 포함) ③ 공익적 기록보존 목적 등	동의 없이 활용 가능

[표 Ⅰ-3. 개인정보 개념 분류]

다. 개인정보 비식별화[2] 정의

개인 식별요소로는 이름, 주소, 주민등록번호, 생년월일, 전화번호, 이메일 주소, 의료기록번호 등과 같이 그 자체로 특정 개인을 직접 식별할 수 있는 식별자(identifier)와 연령, 성별, 거주 지역, 국적, 홈페이지URL 등과 같이 다른 정보와 결합하여 식별할 수 있는 준식별자(quasi-identifier)가 있습니다.

비식별화 방법으로 식별 요소 중 다른 값으로 대체하는 가명처리, 데이터의 종합 값만 보여주고 개별 데이터는 보여주지 않는 총계처리, 일부 식별 요소를 지우는 데이터 삭제, 데이터의 정확한 값은 감추고 범주 값으로 변환하는 범주화, 중요 식별자가 보이지 않게 하는 데이터 마스킹 방법 등이 있으며, 비식별화된 개인정보는 웹, SNS, 의료 기록 등 빅데이터 수집·분석 과정에서 재식별화(re-identification) 될 수 있어 엄격한 관리가 필요합니다.

비식별화와 유사한 용어로 익명화(Anonymization)가 사용되는데, 익명화는 개인정보를 더 이상 식별할 수 없도록 하는 것을 의미합니다.

국제 표준화 기구 ISO/IEC 20889 표준은 '비식별화 과정'을 '정보주체와 식별속성의 집합 간에 연계를 제거하는 과정', 그리고 '비식별화 기술'은 '정보가 개인정보 주체와 연계되는 정도를 감소할 목적으로 데이터 집합을 변환하는 방법' 이라 정의하였습니다.

1) GDPR (General Data Protection Regulation) : 유럽 의회에서 유럽 시민들의 개인정보 보호를 강화하기 위해 만든 통합 규정. 2016년 유럽 의회에서 공표되었으며(Regulation(EU) 2016/679), 약 2년 간의 유예 기간을 가진 후 2018년 5월 25일부터 EU 각 회원국에서 시행. 유럽 연합(EU)의 시민의 데이터를 활용하는 경우 GDPR을 준수해야 함.
2) 비식별화 (de-Identification) : 특정 개인을 식별할 수 없도록 개인정보의 일부 또는 전부를 변환하는 일련의 과정 또는 방법
※ 참고자료: 한국정보화진흥원 '빅데이터 활용을 위한 개인정보 비식별화 기술 활용 안내서'(2015)

라. 개인정보 비식별화 기법

데이터 3법 개정 후 개인정보의 빅데이터 분석·이용에 가명정보의 활용이 가능해짐에 따라 비식별화 기법이 중요하게 되었습니다.

처리기법	예시
가명처리	• 개인 식별이 가능한 데이터에 대하여 직접적으로 식별 할 수 없는 다른 값으로 대체하는 방법 (예시) 홍길동, 35세, 서울거주, 한국대 재학 ➔ 임꺽정, 30대, 서울 거주, 국제대 재학
총계처리	• 개인정보에 대하여 통계값(전체 혹은 부분)을 적용하여 특정 개인을 판단할 수 없도록 함 (예시) 임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm ➔ 물리학과 학생 키 합 : 510cm, 평균키 170cm
데이터값 삭제	• 개인정보 식별이 가능한 특정 데이터 값 삭제 처리 (예시) 주민등록번호 901206-1234567 ➔ 90년대 생, 남자 (예시) 개인과 관련된 날짜정보(합격일 등)는 연단위로 처리
데이터 범주화	• 단일 식별 정보를 해당 그룹의 대표값으로 변환(범주화)하거나 구간값으로 변환(범위화)하여 고유 정보 추적 및 식별 방지 (예시) 홍길동, 35세 ➔ 홍씨, 30~40세
데이터 마스킹	• 개인 식별 정보에 대하여 전체 또는 부분적으로 대체값(공백, '*', 노이즈등)으로 변환 (예시) 홍길동, 35세, 서울 거주, 한국대 재학 ➔ 홍○○, 35세, 서울 거주, ○○대학 재학

[표 Ⅰ-4. 비식별화 기법]

관련 법령	법령 내 안전조치
개인정보 보호법 ('20. 8. 5 시행)	• 제28조의4(가명정보에 대한 안전조치의무 등) ① 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치
신용정보법 ('20. 8. 5 시행)	• 제40조의2(가명처리·익명처리에 관한 행위규칙) ① 가명처리에 사용한 추가정보를 분리하여 보관하거나 삭제 ② 내부관리계획을 수립하고 접속기록을 보관하는 등 기술적·물리적·관리적 보안대책을 수립·시행

[표 Ⅰ-5. 가명정보 관련 법령]

3) 금융 IT보안 Compliance

최근 금융권 보안 사고가 잦아지면서 관련 규제준수(Compliance)에 대한 요구가 높아지고 있습니다. 그러나, 금융회사들이 운영할 수 있는 인력과 예산의 한계로 대응이 쉽지 않은 상황입니다.

금융권의 Compliance를 적용할 때는 회사규모와 서비스 종류, 실제 활용 가능성 등을 고려해야 합니다. 전사적 차원에서 IT 거버넌스와의 연계도 필요하며, 보안 Compliance는 영역 세분화를 통해 보안성을 높여나가는 것이 중요합니다.

금융권에서는 '내부통제'가 가장 중요합니다. 내부통제를 통해 운영의 효과성과 효율성을 높이는 것은 물론이고, 재무보고 신뢰성 유지, 모든 활동에 대한 관련 법규나 내부 정책 및 절차 등을 준수할 수 있기 때문입니다.

금융보안연구원 보고서에 따르면, 금융권 보안 Compliance 강화를 위해 ▲프로세스 지향 ▲통제 기반 ▲측정 중심과 같은 세 가지 요인도 충족이 필요합니다. 아울러 정보보호관리체계의 국제 표준인 ISO 27001과 한국인터넷진흥원(KISA)의 정보보호관리체계(ISMS) 등을 운영하는 기업이나 보안 컨설팅 전문업체 전문가와의 협력을 통한 보안 체계 구축도 이뤄져야 합니다.

[그림 I -1. 금융 Compliance 도메인 및 통제항목]

4) 정보통신 IT보안 Compliance

정보통신 제공자는 이용자의 개인정보를 보호해야 하고, 안전한 정보통신 서비스를 제공해야 하며, 개인정보 자료를 운영하는 기업 및 기관은 반드시 정보통신망법 준수를 위해 제도적 기술적 조치를 수행해야 합니다.

국내주요법령	목적
정보통신기반 보호법	전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립 · 시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장
정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함
개인정보보호법	개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함

[표 Ⅰ-6. 정보통신 주요법령]

법률 및 관련조항	대상시스템	자료 구분
정보통신망법 - 제22조의2(접근권한에 대한 동의) - 제45조(정보통신망의 안정성 확보 등) - 제48조(정보통신망 침해행위 등의 금지) 정보통신망법 시행령 - 제9조의2(접근권한의 범위 등) - 제37조(집적정보통신시설사업자의 보호조치) - 제58조(침해사고 관련정보의 제공방법) 개인정보의 기술적 관리적 보호조치 기준 - 제 4조 (접근통제) - 제 5조 (접속기록의 위.변조방지) - 제 6조 (개인정보의 암호화) - 제 7조 (악성프로그램 방지) - 제 8조 (물리적 접근 방지) - 제 9 조 (출력.복사시 보호조치) - 제10조 (개인정보 표시 제한 보호조치)	1. 운영체제	1-1. 시스템 접근로그 1-2. 시스템 접근 기록의 보관 1-3. 접근권한의 변경과 부여에 대한 기록 1-4. 비밀번호 주기적 변경에 대한 기록 1-5. 실행 명령어 로그
	2. 이중인증 (Two Factor Authentication)	2-1. 개인정보처리 시스템 이중인증 접근에 대한 기록
	3. 침입차단 시스템, 웹방화벽, UTM, IPS	3-1. 개인정보 유출 시도 탐지에 대한 기록
	4. 안티바이러스	4-1. 안티 바이러스 소프트웨어 설치 및 정기적인 업데이트에 대한 기록
	5. 데이터 베이스	5-1. DB접속 기록 5-2. 요청쿼리에 대한 기록 5-3. 쿼리/접근 차단 내역 5-4. 개인정보 암호화 기록
	6. 출력물 보안	6-1. 개인정보 출력과 복사에 대한 기록
	7. 개인정보 처리 시스템	7-1. 개인정보처리 시스템 접근권한 부여, 변경, 말소에 대한 기록 7-2. 개인정보처리 시스템의 접근기록 보관 및 백업

[표 Ⅰ-7. 법률 조항 대비 시스템로그]

5) 제조업 IT산업보안 Compliance

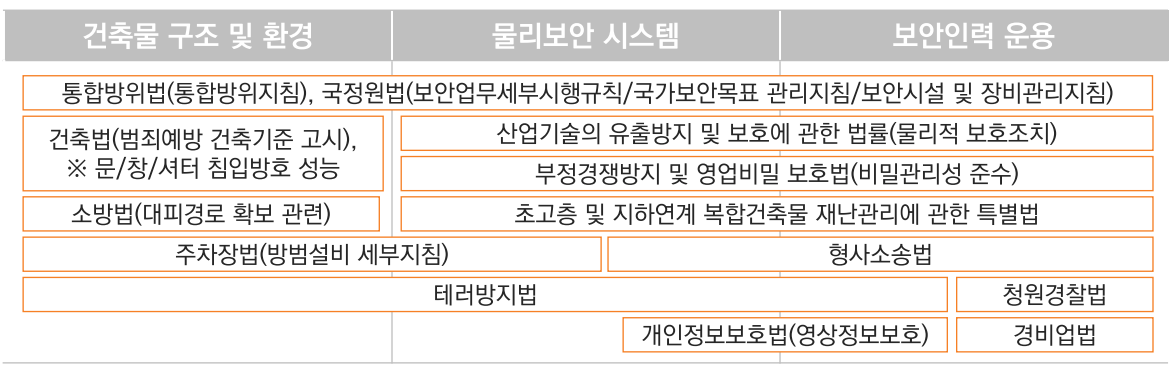
국내·외 시장에서 기술적·경제적으로 가치가 높은 국가의 핵심기술이 해외로 유출될 경우에는 국가의 안전보장과 국민경제의 발전에 중대한 악영향을 줄 우려가 있습니다. 최근 6년간 해외로 유출된 기술 유출 사건은 121건이며, 그 중 정부지정 국가 핵심기술도 29건에 해당됩니다. (산업통상자원부 2020.09 자료기준)

국가의 산업기술은 산업보안 관련법으로 법제화 되어 있고, 정부에서 지정한 국가핵심기술은 반도체, 디스플레이, 자동차/철도, 정보통신 등 각 산업영역에서 지정되어 있습니다.

국내주요법령	목적
산업기술의 유출방지 및 보호에 관한 법률	산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함
중소기업기술 보호 지원에 관한 법률	중소기업기술 보호를 지원하기 위한 기반을 확충하고 관련 시책을 수립·추진함으로써 중소기업의 기술보호 역량과 기술경쟁력을 강화하고 국가경제의 발전에 이바지함을 목적
산업발전법	지식기반경제의 도래에 대응하여 산업의 경쟁력을 강화하고 지속 가능한 산업발전을 도모함으로써 국민경제의 발전에 이바지함을 목적
산업기술혁신 촉진법	산업기술혁신을 촉진하고 산업기술혁신을 위한 기반을 조성하여 산업경쟁력을 강화하고 국가 혁신역량을 높임으로써 국민경제의 지속적인 발전과 국민의 삶의 질 향상에 이바지함을 목적
대·중소기업 상생협력 촉진에 관한 법률	대기업과 중소기업 간 상생협력(相生協力) 관계를 공고히 하여 대기업과 중소기업의 경쟁력을 높이고 대기업과 중소기업의 양극화를 해소하여 동반성장을 달성함으로써 국민경제의 지속성장 기반을 마련함을 목적

[표 I -8. 산업보안 주요법령]

IT정보보안 외에 물리보안 영역에서도 정보보안의 Compliance가 규정화 되어 있습니다. 물리보안 관련법은 자체적인 IT통합관제센터나 보안관제센터를 구축할 때에도 적용해야 합니다.



[그림 I -2. 물리보안 관련 법]

6) 의료정보보호에 관한 법령 강화

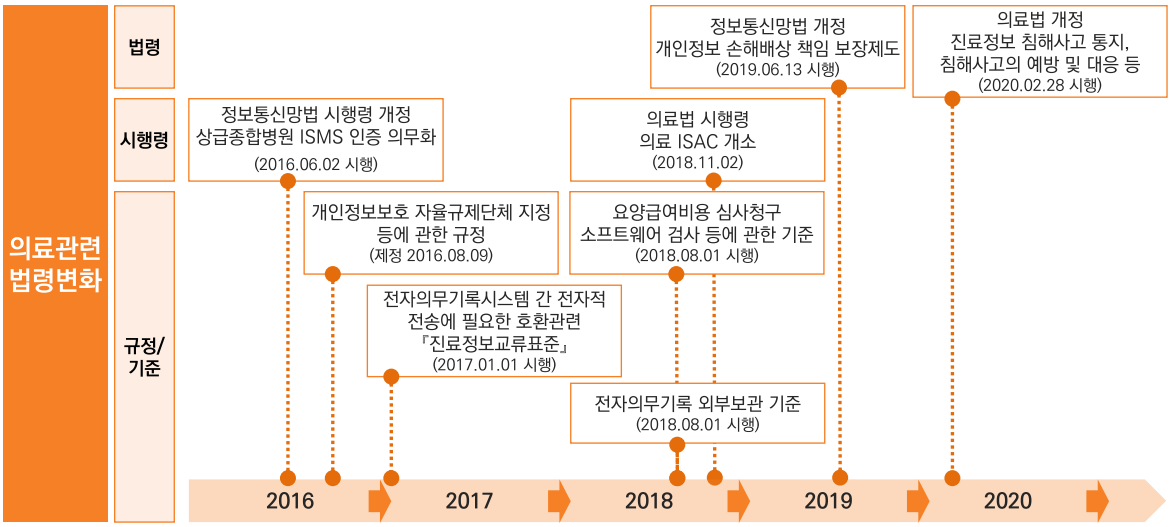
가. 의료정보보호 현황

최근 신종 코로나바이러스 감염증 검사와 확진자의 증가로 병원 등 의료기관에 해당 의료 데이터가 중요 관심 포인트가 되었습니다. 현실적으로도 확진자의 개인정보가 외부로 유출, SNS를 통해 급격히 확산되어 개인정보 유출이 사회적 이슈가 되고 있으며, 이제는 의료정보의 개인정보 보호에 대한 중요성이 다시 한번 강조되고 있습니다.

의료기관에서는 환자의 주민등록번호, 진료정보, 병력, 투약 정보, 의료 영상정보 등 민감한 의료정보를 보유하고 있습니다. 2015년 기준으로, 의료기관의 92.1%, 병원급 이상 95.4%가 전자의무기록 EMR[1]을 사용하고 있으며, OCS[2], PACS[3] 등과 같은 의료정보시스템도 증가하고 있습니다. 하지만, 『2018년 개인정보보호 실태조사(행정안전부, 개인정보보호 위원회)』 결과, 의료기관이 포함된 보건/복지 분야에서 ① 개인정보 처리 절차 복잡(57.3 %), ② 전문인력 부족(81.7 %), ③ 기술적 전문성 부족(64.2%) 등의 문제로 개인정보 보호 관리 문제점을 도출하였습니다.

나. 법령 변화

의료기관의 IT환경변화와 개인정보 침해사고(해킹이나 내부자에 의한 대량 유출) 위험 증가로 인해 관련 법령이 지속적으로 제·개정 되고 있으며, 이를 통해 개인정보 점검/관리, 의료정보시스템의 보안기준 수립 등 개인정보 보호요건이 강화되고 있습니다.



[그림 I -3. 의료관련 법령 변화]

1) EMR (Electronic Medical Record) : 의료기관에서 생성되는 모든 진료정보, 진단결과, 처방결과, 약제 처방자료 등을 저장 관리하는 시스템
2) OCS (Order Communication System) : 환자를 중심으로 발생하는 질병의 제반 내용을 전산화하여 단계별로 저장하는 시스템
3) PACS (Picture Archiving Communication System) : 영상진단장비를 사용하여 촬영한 영상정보를 네트워크를 통해 전달하는 시스템

7) Compliance 준수 대응현황

Compliance 준수

관련 법/제도 기준

- 개인정보보호법, 개인정보의 안전성 확보 조치 기준
- 전자금융거래법, 금융감독규정/시행세칙, 보험업감독규정, 신용정보법, 신용정보업감독규정, 전자서명법
- 정보통신망법
- ISMS-P/ISMS, ISO 27001

IT요소 별 보안기준

- 금융분야 취약점 분석·평가
- 전자금융서비스 유형에 따른 관련 기술 표준 및 보안 가이드라인, 금융회사 자체 보안성심의 가이드, 개인정보 비식별 조치 가이드라인

[그림 I -4. Compliance 대응 정보시스템 계층]

8) 정보보호 영역별 Compliance 근거

정보시스템 계층	Client	Network	Server	Application	Data(DB)
정보보호 기술 영역 / 인증	전자금융거래법 제21조 전자금융감독규정 제12조 (단말기 보호대책) 전자금융감독규정 제16조 (악성코드 감염 방지대책)	전자금융거래법 제21조 전자금융감독규정 제14조 (정보처리시스템보호대책)	전자금융거래법 제21조 전자금융감독규정 제14조 (정보처리시스템보호대책)	전자금융거래법 제21조 전자금융감독규정 제29조 (프로그램 통제)	전자금융거래법 제21조 전자금융감독규정 제13조 (전산자료 보호대책)
	정보통신망법 제45조 (정보통신망의 안정성 확보 등)				
	정보통신기반 보호법 제10조 (보호지침)				정보통신기반 보호법 제10조 (보호지침)
			개인정보보호법 제29조 개인정보보호법 시행령 제30조 (개인정보의 안정성 확보 조치)		신용정보법 제19조 신용정보법 시행령 제16조 (기술적 · 물리적 · 관리적 보안대책의 수립)
접근/권한 통제	전자금융거래법 제21조 전자금융감독규정 제12조 (단말기 보호대책) 전자금융감독규정 제16조 (악성코드 감염 방지대책)	전자금융거래법 제21조 전자금융감독규정 제18조 (IP주소 관리대책) 전자금융감독규정 제14조 (정보처리시스템보호대책)	전자금융거래법 제21조 전자금융감독규정 제13조 (전산자료 보호대책) 전자금융감독규정 제14조 (정보처리시스템보호대책)	전자금융거래법 제21조 전자금융감독규정 제13조 (전산자료 보호대책)	전자금융거래법 제21조 전자금융감독규정 제13조 (전산자료 보호대책)
	개인정보보호법 제29조 개인정보보호법 시행령 제21조 (고유식별정보의 안정성 확보 조치) 개인정보보호법 시행령 제30조 (개인정보의 안정성 확보 조치)				
	정보통신망법 제45조 (정보통신망의 안정성 확보 등)				
	신용정보법 제19조 신용정보법 시행령 제16조(기술적 · 물리적 · 관리적 보안대책의 수립)				
		정보통신기반 보호법 제10조 (보호지침)			
	산업기술보호법 제10조 산업기술보호법 시행령 제14조 (국가핵심기술의 보호조치)				
암호화	전자금융거래법 제21조 전자금융감독규정 제34조 (전자금융거래 준수사항)		전자금융거래법 제21조 전자금융감독규정 제17조 (공개용 웹서버 관리대책)		전자금융거래법 제21조 전자금융감독규정 제17조 (공개용 웹서버 관리대책)
	개인정보보호법 제29조 개인정보보호법 시행령 제30조 (개인정보의 안정성 확보 조치)				
	개인정보보호법 제24조 시행령 제21조 (고유식별정보의 안정성 확보 조치) 시행령 제21조의2 (주민등록번호 암호화 적용 대상 등)		개인정보보호법 제24조 시행령 제21조 (고유식별정보의 안정성 확보 조치) 시행령 제21조의2 (주민등록번호 암호화 적용 대상 등)		개인정보보호법 제24조 시행령 제21조 (고유식별정보의 안정성 확보 조치) 시행령 제21조의2 (주민등록번호 암호화 적용 대상 등)
	정보통신망법 제28조 (개인정보의 보호조치) 정보통신망법 시행령 제15조 (개인정보의 보호조치)		정보통신망법 제28조 (개인정보의 보호조치) 정보통신망법 시행령 제15조 (개인정보의 보호조치)		
부인 방지	전자금융거래법 제21조 전자금융감독규정 제12조 (단말기 보호대책)	전자금융거래법 제21조 전자금융감독규정 제14조 (정보처리시스템보호대책)		전자금융거래법 제21조 전자금융감독규정 제13조 (전산자료 보호대책)	
	개인정보보호법 제29조 개인정보보호법 시행령 제21조 (고유식별정보의 안정성 확보 조치) 개인정보보호법 시행령 제30조 (개인정보의 안정성 확보 조치)				
	정보통신망법 제48조의4 (침해사고의 원인 분석 등)				정보통신망법 제48조의4 (침해사고의 원인 분석 등)
		신용정보법 제20조 (신용정보 관리책임의 명확화 및 업무처리기록의 보존)			
	정보통신기반 보호법 제10조 (보호지침)				
개인 정보 보호		전자금융거래법 제21조 전자금융감독규정 제17조 (홈페이지 등 공개용 웹서버 관리대책)			전자금융거래법 제21조 전자금융감독규정 제17조
	개인정보보호법 제29조 개인정보보호법 시행령 제30조 (개인정보의 안정성 확보 조치) 개인정보보호법 제24조 개인정보보호법 시행령 제21조 (고유식별정보의 안정성 확보 조치)				
	정보통신망법 제28조 (개인정보의 보호조치) 정보통신망법 시행령 제15조 (개인정보의 보호조치)				정보통신망법 제28조 정보통신망법 시행령 제15조
가용성 확보	전자금융거래법 제21조 전자금융감독규정 제23조 (비상대책 등의 수립·운용) 전자금융감독규정 제25조 (정보처리시스템의 성능관리)				
	정보통신망법 제45조 (정보통신망의 안정성 확보 등)				
		신용정보법 제19조 신용정보법 시행령 제16조 (기술적 · 물리적 · 관리적 보안대책의 수립) 신용정보감독규정 제6조 (정보처리 · 정보통신설비)			
		정보통신기반 보호법 제10조 (보호지침)			정보통신기반 보호법 제10조

[그림 I -5. 정보보호 영역별 Compliance 근거]

Part 2

정보보호 위협 패러다임 변화

1) 언택트 패러다임 변화

가. 언택트 정의

전 세계적으로 코로나19(COVID-19) 바이러스 유행이 이어지면서 다양한 분야에서 비대면 서비스 이용이 증가하고 있습니다. 이러한 사회 변화에 따라 접촉을 뜻하는 'Contact'와 부정을 뜻하는 'un'을 조합하여 '접촉하지 않는다'는 의미의 '언택트(Untact)'라는 용어가 변화의 축이 되었습니다. 패스트푸드 프랜차이즈에서 볼 수 있는 '키오스크(Kiosk)', 재택근무, 화상회의, 온라인 강의 등이 언택트의 대표적인 사례입니다.

특히, '20년 상반기 주요 환경변화와 사회·경제 영역 전망'을 통해 비대면·원격 서비스의 보안성 향상이 이슈로 등장했습니다. 다양한 분야에서 비대면·원격 서비스의 제공에 따라 보안성 향상이 이슈로 대두되면서 비대면·원격사회로의 전환이 이루어질 것으로 예상됩니다.

영역	변화동인 및 변화 시나리오
헬스케어	▪ 병원에 가지 않고도 의사의 진단·처방이 가능한 원격의료 요구 증대 ▪ 예방·관리 중요성 증가, AI가 진단·모니터링하는 디지털 전환 가속화
교육	▪ 온라인 개학으로 인해 원격교육 인프라 확충 ▪ 초실감 체험형·몰입형 학습, 양방향 맞춤형 교육 등 에듀테크 발전
교통	▪ 초소형 이동수단(Micro Mobility) 및 자율주행차에 대한 수요 증가 ▪ 공유교통 회피 → 개인교통 증가할 것으로, 원활한 교통수요 관리 필요
물류	▪ 원격경제 활성화로 폭증할 물류의 신속하고 정확한 처리·관리 중요 ▪ 자동화·최적화된 유통망을 통한 비대면·비접촉 배송서비스 수요 증가
제조	▪ 글로벌 공급망 위험회피를 위한 지역 공급망 구축 및 리쇼어링 정책 부상 ▪ 제조공장·장비의 스마트화 및 원격자동·관리 수요 증가
환경	▪ 신종 감염병·질병 출현 및 환경오염 심화 등 인간-동물-환경 상호작용 ▪ 의료폐기물 발생량 증가 및 비대면 사회 도래로 일회용품 사용 증가
문화	▪ 홈엔터테인먼트 소비 증가로 게임, OTT 서비스 등 콘텐츠산업 발전 ▪ 실감·소통형 콘텐츠 기술 및 저작권 보호, 위변조 대응 기술수요 증가
정보보안	▪ 비대면 서비스와 데이터 경제 활성화에 따른 정보보안 이슈 부각 ▪ 비대면 금융거래 증가에 따른 생체인증 수요 확대

* 출처 : 과학기술정보통신부와 한국과학기술기획평가원 보도자료 (2020.04)

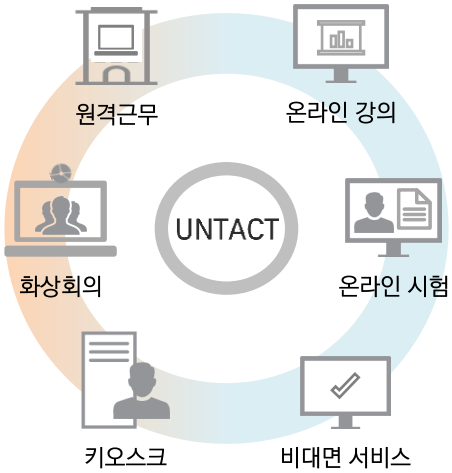
[표 I -9. 주요 환경변화로 예상되는 사회·경제영역 전망]

나. 언택트 보안 위협

언택트 기술 중심의 디지털 전환이 가속화됨에 따라 기존 및 신규 비대면 서비스들의 사용량이 급증하였습니다. 이와 관련하여 다양한 언택트 서비스의 보안위협이 증가하고 있습니다.

기업

- ✓ 원격근무 시 보안정책의 한계
- ✓ 망분리 완화에 따른 위협 증가
- ✓ 화상회의 공격 사례
  - – 대화방 무단접속을 통한 업무 방해, 악성링크 실행유도 공격
- ✓ 기업 내부 정보보호 위협으로 회의 내용과 공유자료의 유출
- ✓ 솔루션 취약점을 통해 원격코드, 인가 취약점을 통한 공격
- ✓ 키오스크 장비 해킹을 통한 정보 추출 및 코드실행 공격



개인

- ✓ 다양한 형식의 피싱 공격 증가
  - 1) 특정 사이트(블로그)의 페이크 앱을 통한 피싱 공격
  - 2) 비대면 업무 관련 사이트로 위장 또는 보건 전문가를 사칭한 피싱 공격
  - 3) 실시간 온라인 강의의 증가로 원격 수업 진행 중 신원을 알 수 없는 사용자가 입장하여 방해
- ✓ 온라인 시험 부정행위
  - – 문제 유출, 컨닝 등의 부정행위로 수험생의 상대적 불이익 발생

[그림 I -6. PC감염 내부침투 및 랜섬웨어 공격 사례]

다. 언택트 보안 위협 분석

다양한 보안 위협 중 화상회의, 원격근무와 같은 업무용 언택트 솔루션 서비스 대상으로 공격 가능성을 확인하고, 기업과 개인에게 발생할 수 있는 피해를 분석하였습니다. 발견된 취약점을 악용할 경우, 기업과 개인 모두 권한 탈취, 랜섬웨어 감염, 악성코드 유포, 정보유출 등의 피해가 발생할 수 있습니다.

취약점	취약점 상세	취약점 악용 예시
불충분한 사용자 인증/인가	▪ 비공개 그룹에 권한 없는 사용자 참가 ▪ 권한 없는 사용자가 그룹 관리자 기능 강제 사용	▪ 그룹 내 주요정보 모니터링 ▪ 그룹 업무 방해 및 유해 사이트 홍보
원격 명령 실행	▪ 사용자 PC에 임의의 파일 배포/실행	▪ 타겟 PC의 제어권 획득
크로스 사이트 스크립트 (XSS)	▪ 그룹 참여자를 대상으로 스크립트 구문 실행	▪ 악성 사이트 유입 유도
정보 노출	▪ 비공개 그룹 참가 비밀번호 노출 ▪ 서버 중요 정보 노출	▪ 권한 없는 사용자가 비공개 그룹에 참가하여 주요정보 모니터링 ▪ 노출된 정보를 활용하여 추가 공격 용이

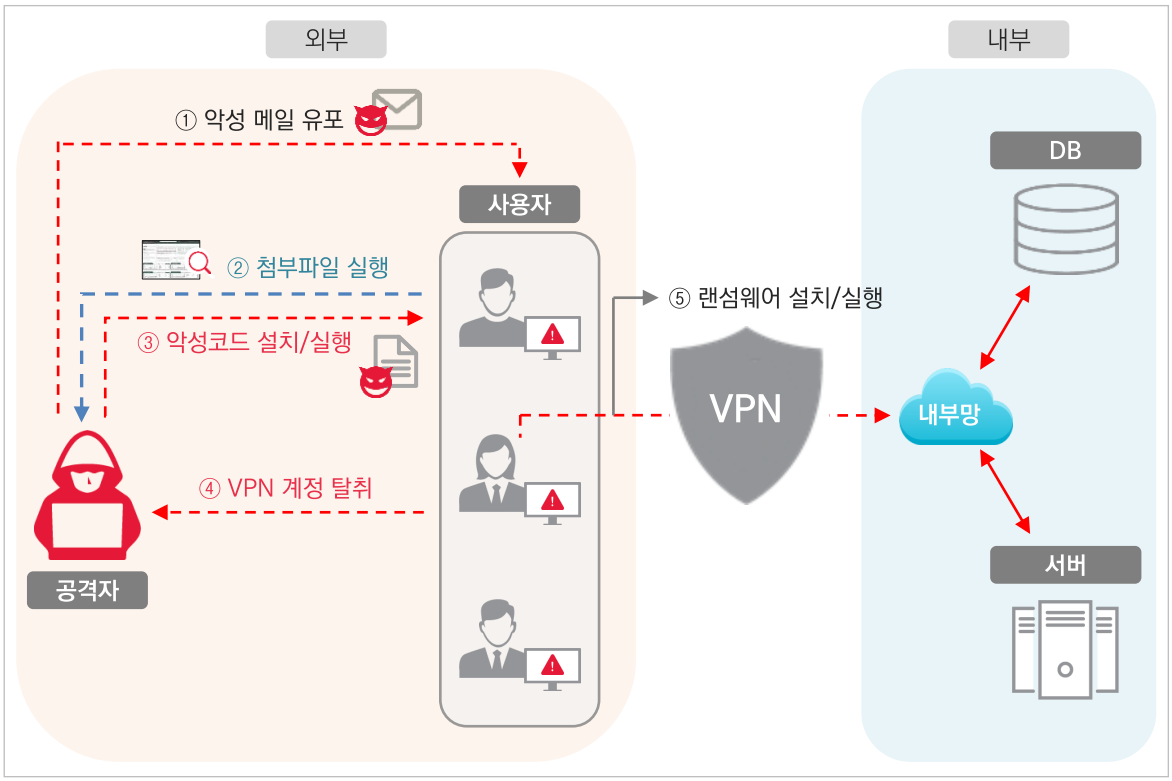
* 출처 : SK인포섹 EQST그룹 취약점 분석 자료

[표 I -10. 언택트 보안취약점]

라. 언택트 보안 위협 사례

✓ 사례 1 기술적 사례

앞서 분석한 보안 위협을 이용해 언택트 업무 환경에서 발생 가능한 가상의 공격 시나리오는 다음과 같습니다. 공격자는 기업 사용자의 PC를 감염시킨 후, 내부망에 침투하여 내부 시스템에 랜섬웨어를 설치하고 실행합니다.



[그림 I -7. PC감염 내부침투 및 랜섬웨어 공격 사례]

공격자는 악성 URL이 담긴 메일을 사용자들에게 전달하고, 사용자들은 메일을 열람하여 악성 URL에 접근합니다. 악성 URL에 접근한 사용자 PC는 원격 코드 실행 취약점에 의해 공격자가 생성한 악성 프로그램이 설치되고 실행됩니다. 공격자는 감염된 사용자의 PC를 장악해 VPN 계정 정보를 탈취합니다. 공격자는 탈취한 VPN 계정 정보를 이용하여 내부망에 침투한 후 랜섬웨어를 설치하고 실행합니다.

랜섬웨어 공격은 위와 같은 피싱 메일을 통한 악성 프로그램 유포와 취약한 경로를 통해 실행되며, 최근 공격 기법은 다양하게 진화하고 있습니다. 랜섬웨어 공격이 주로 사회공학적 기법을 통한 시스템으로의 비인가 접근 방식으로 이루어지는 만큼 메일 발신자, 첨부파일 확인 등의 정보보호 습관이 중요합니다.

✓ 사례 2 Compliance 사례

최근 콜센터 직원들의 재택근무 필요성이 대두되고 있습니다. 업무 환경의 재택 구성에 기술적 문제는 없지만, 업무 특성상 개인정보 조회를 해야 하므로 개인정보 유출, 파일 복제 또는 다운로드 등의 Compliance 이슈가 나타나고 있습니다. 주요 Compliance 내용과 보안 위협 사례는 다음과 같습니다.

개인정보보호법

- 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) ④, ⑥항

정보유출

- 상담 화면 캡처 차단
- 개인정보 무단 저장 및 유출 차단

정보통신망법

- 개인정보의 기술적 관리적 보호조치 기준
  - 제4조(접근통제) ④, ⑤, ⑥항
  - 제9조(출력·복사 시 보호조치) ①항

재택근무

침해사고

- 내부 시스템 접근에 대한 보안 대책
- 단말 보안 대책 (악성코드, 랜섬웨어 등)

전자금융거래법

- 전자금융감독규정 제15조 (해킹 등 방지대책) ①항 3호, 5호

인증/부인방지

- 상담원 본인 확인 수단 강화 필요
- 제3자 접근, 무단 촬영 등 업무 모니터링 대책

[그림 I -8. 언택트로 인한 Compliance 위협]

위와 같은 이슈와 보안 위협으로 언택트 기술에 Compliance 예방을 위한 보안 조치가 필요합니다. 또한, 안전한 재택근무 구성환경을 위해서 내부근무와 유사한 수준의 보안 체계를 유지하는 것이 중요합니다. 개인정보의 기술적/관리적 보호조치 실행과 함께 침해사고가 발생하지 않도록 대응방안을 마련하여 언택트 시대에 맞는 서비스를 제공해야 합니다. 안전한 서비스를 위해 Compliance에 맞는 보안 기술/정책을 적용하여 보안사고가 발생하지 않도록 예방도 필요합니다.

마. 언택트 보안 위협 대응방안

대상	대응방안
재택근무 시행 시 고려사항 (기업)	✓ 가급적 업무 전용 PC 사용 및 최신 버전의 OS 및 소프트웨어 사용 ✓ VPN 또는 VDI 등 원격근무시스템 사용 권장 ✓ 재택근무용 사용자 계정은 2차 인증 적용 ✓ 원격 우회 접속 모니터링 강화 ✓ 회사 보안 정책이 설정된 회사 메일을 우선 사용 ✓ 업무상 불필요한 웹사이트 접속 지양
사용자 실천 수칙 (개인)	✓ 공공 PC / Wi-Fi 사용 주의 ✓ 확인되지 않은 파일 다운로드 주의 ✓ 미 사용 프로그램 삭제 ✓ 안전한 비밀번호 관리 ✓ 소셜 미디어 프로파일 관리 ✓ 보안 취약점을 제거한 최신 S/W 사용 ✓ 의심스러운 메일, SMS, 메신저 주의
개발 시 고려사항 (S/W)	✓ 설치형 솔루션의 경우, 자동 업데이트 기능 구현 시 업데이트 서버의 신뢰 여부 및 업데이트 파일의 디지털 서명 검증 구현 ✓ 암호화 기능 구현 시 자체 알고리즘 개발을 지양하며 공개된 표준 알고리즘 사용 ✓ 비공개 채널 기능 구현 시 안전한 인증 설계 ✓ 그룹 관리 기능 구현 시 안전한 권한 검증 설계 ✓ 사용자 입력이 예상되는 곳에 악성 스크립트 실행 차단 구현

[표 Ⅰ-11. 언택트 보안 위협 대응방안]

2) 금융보안원 2021년 디지털금융 및 사이버보안 이슈 전망

[그림 I -9. 2021 디지털금융 및 사이버보안 이슈 전망]

금융보안원은 '21년에 금융의 디지털·데이터 혁신에 따라 발생되는 각종 리스크 및 사이버보안 위협의 대응과 금융산업의 개방과 경쟁 심화, 비대면·언택트에 따른 서비스 및 업무환경의 변화, 사이버 공격의 고도화·지능화 등으로, 그 어느 해보다 금융권의 디지털·데이터 혁신이 빠르게 진행될 것이고 그에 따라 금융보안의 중요성도 더욱 강조될 것으로 예상하고 있습니다.

3) KISA 2021년 사이버 위협 전망

가. KISA '21년 사이버 위협 전망 보도

[그림 I -10. KISA 2021년 사이버 위협전망]

올해 전 세계적으로 코로나-19가 확산하면서 재택근무, 원격교육, 온라인 쇼핑 등 급격한 비대면 활동 증가와 함께 이를 악용한 사이버 공격 또한 늘어나는 상황입니다. 이에 KISA는 각 국가·기관과 함께 지능화·고도화되는 사이버 위협에 선제적으로 대비하고 사이버 보안 활동을 선도하고자 2021년에 주목해야 할 사이버 위협을 전망했습니다.

이번 발표에서는 글로벌 사이버 위협 전망과 국내 사이버 위협 전망을 나누어 발표했습니다. 특히, 국내·외 공통적으로 가장 주목해야 할 사이버 위협은 랜섬웨어 공격으로 유통업 영업을 종료하거나 공장 시스템이 마비되어 출하가 일시 중단되는 일이 발생하기도 했습니다. 이외에도 해외에서는 랜섬웨어로 병원 시스템이 마비되어 긴급 이송하던 환자가 사망사건까지 발생했습니다.

나. 글로벌 사이버 위협 전망

글로벌 전망
1. 표적형 공격 랜섬웨어의 확산과 피해규모 증가(공통)
▶ 정부 및 기업 등 특정 대상을 표적한 공격 ▶ 서비스 및 제조, 의료 등 다양한 산업 분야로 랜섬웨어 공격 확대 ▶ 내부 정보 유출부터 파일 암호화까지, 협박수단 강화
2. 고도화된 표적형 악성 이메일(호주, Australia, AusCERT)
▶ 맞춤형 악성 이메일과 대량 피싱이 결합한 매스피어링 등장 ▶ Emotet 악성코드를 활용하여 스팸 메일 생성 및 배포 증가 ▶ 유출된 기업 데이터에서 특정 대상의 전자 메일, 계약정보 등을 활용한 맞춤형 공격
3. 코로나-19 사이버 공격 팬데믹(인도, India, CERT-In)
▶ 악성 웹사이트, 악성 첨부파일을 포함한 이메일 등으로 재택근무자 공격 증가 ▶ 재택근무 증가로 엔드포인트 장치에서의 기업 정보 유출 우려 ▶ 취약한 VPN(가상사설망) 등 원격 네트워크 환경을 통한 기업 네트워크 침투 시도
4. 다크웹 유출 정보를 활용한 2차 공격 기승(한국, Korea, KrCERT/CC)
▶ 다크웹 시장 확대로 민감 정보 거래 증가 ▶ 최근 재택근무 상황을 반영하여 VPN, RDP(원격 데스크톱) 등 네트워크 권한 판매 활성 ▶ 공격자들의 협력을 통하여 공격 문턱을 낮추고 공격 규모를 확대
5. 기업을 낚는 사이버 스나이퍼(스리랑카, Sri Lanka, Sri Lanka CERT|CC)
▶ 수출 및 수입 기업을 표적하여 공격 ▶ 피싱, 스피어 피싱 등을 활용하여 기업 전자 메일 계정 공격 ▶ 기업의 협력사 계정으로 견적서를 위·변조하여 발송하는 등 공격의 정교화

[표 I -12. 글로벌 사이버 위협 전망]

다. 국내 사이버 위협 인텔리전스 전망

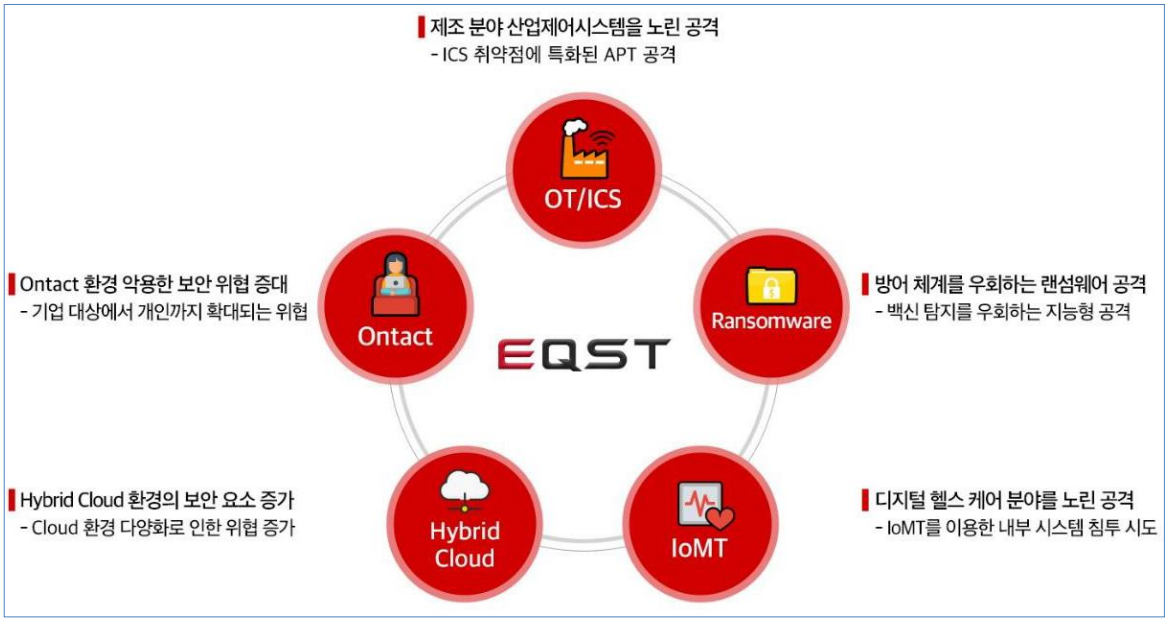
국내 사이버 위협 인텔리전스 전망(회사명 abc, 가나다 순)
1. 표적 공격과 결합된 랜섬웨어의 위협 확대(공통)
▶ 메이즈 랜섬웨어의 은퇴, 하지만 신규 랜섬웨어의 등장으로 피해 발생 ▶ 기업용 소프트웨어 취약점을 악용한 랜섬웨어 유포 ▶ 다양한 산업 분야로 공격의 확대, 피해 증가
2. 거세진 DDoS, 금전까지 요구하는 공격 증가(KISA)
▶ 금융 및 교육, 기업 등을 대상한 DDoS 공격 증가 ▶ 금전을 요구하고 미지불시 공격을 감행하는 랜섬 디도스 기승 ▶ DDoS 신기록 등장, 공격의 고도화
3. 사회기반시설 및 중요 인프라를 겨냥한 사이버 위협범위 확대(NSHC)
▶ 국가 및 사회 기반 시스템에 대한 공격 증가 ▶ 주요 에너지 및 생산 시스템에 대한 사이버 해킹 발생 증가 ▶ 기반 시설 및 인프라 시스템에 대한 생산성 파괴 목적으로 발생
4. 포스트 코로나시대 비대면(언택트) 전환 후 보안 사각지대를 노린 사이버 위협 증가 (빛스캔)
▶ 원격 수업 파일 다운로드를 통한 랜섬웨어 공격 증가 ▶ 재택근무자 공격을 통한 기업 내부 침입 시도 발생 ▶ 코로나-19 관련 메시지와 첨부파일로 악성코드 감염 유도
5. 클라우드 서비스 목표한 공격 증가(안랩)
▶ 클라우드 크리덴셜 및 설정 파일 훔치는 악성코드 등장 ▶ 취약한 관리 시스템과 관리 도구를 이용한 클라우드 내 접근 ▶ 클라우드 서비스를 이용해 악성코드 배포 및 C&C 서버로 활용
6. 국가 지원 해킹 그룹의 공격 증가와 위협 대상 확대 및 다양화(이스트시큐리티)
▶ 정부차원의 국가지원 해킹그룹 지능형지속위협(APT) 공격 증대 ▶ 외교·안보·통일·국방 등 연구 분야 종사자, 언론사 기자들 주요 공격 표적 ▶ 스피어 피싱(Spear Phishing)공격과 시차를 둔 고도화된 신뢰 기반 위협 결합
7. 5G를 이용한 사물인터넷(IoT)제품의 활성화로 새로운 보안 위협의 대두(잉카인터넷)
▶ 다수 기기 보안 기능 제한으로 지속적인 피해 확대 ▶ 신규 취약점 및 미패치된 취약점 공격으로 대규모 IoT 봇넷 감염 및 DDoS 공격의 재개 ▶ 좀비화된 IoT 기기를 통한 개인정보 탈취 및 악성코드 유포의 숙주로의 악용
8. 보안 솔루션을 우회하기 위한 기법 고도화(하우리)
▶ 공격자들의 보안 솔루션을 우회하기 위한 기법 지속적인 개선 ▶ 비실행 파일(LNK, PowerShell, VBS) 중심으로 공격 기법 고도화 ▶ 피싱과 결합하여 공격 시너지를 극대화

[표 I -13. 국내 사이버 위협 전망]

4) SK인포섹 EQST[1] 2021년 5대 사이버 위협 전망

2020년은 코로나19로 인해 사회적으로 많은 변화가 있었으며, 비대면이라는 언텍트(Untact)와 재택근무, 원격근무가 활성화되면서 온택트(Ontact)가 유행어처럼 되었습니다. 작년에 EQST에서 발표했던 2020년 위협전망 중 "N/W 연계 취약점을 악용한 사고의 확산 사례"와 "랜섬웨어의 고도화", "다크웹 거래의 활성화"가 현실화되어 2020년 위협으로 다가왔습니다.

2021년은 계속적인 코로나19로 기업의 업무환경 변화에 따라 새로운 보안위협에 직면하게 되었습니다.



[그림 I -11. SK인포섹 EQST 2021년 5대 사이버 위협 전망]

■ 제조 분야 산업제어시스템을 노린 공격

△ HMI, PLC, DCS 등 제조사 취약점 특화 APT 공격

2021년에는 산업제어시스템을 대상으로 공격이 늘어날 전망입니다. 제조 설비에서 사용하는 운영체제(OS) 및 산업 전용 프로토콜에서 보안 취약점이 지속적으로 발견되고 있으며, 특히 NVD[2]에 공개된 산업제어시스템 취약점 중 70% 이상이 원격 공격으로 악용될 수 있다고 밝혀졌습니다. 또한, OT/ICS를 노린 공격은 국내에서 16.8%, 해외에서 24.4%로 높은 공격 비율을 차지하고 있습니다. 보안 취약점이 증가하는 만큼 대상이 표적화되고, 보다 정교해진 공격이 증가할 것이기에 OT/ICS 영역에 사용되는 운영체제나 소프트웨어의 보안 관리가 꼭 필요한 시점입니다.

1) EQST(Experts, Qualified Security Team) : 사이버 위협 분석 및 연구 분야의 SK인포섹 보안 전문가 그룹
"EQST Annual Report 2021 보안 위협 전망 보고서" 발췌
2) NVD(National Vulnerability Database) : 보고된 소프트웨어 취약점에 대한 표준화된 정보를 관리하는 미국의 국가 취약성 데이터베이스

4) SK인포섹 EQST[1] 2021년 5대 사이버 위협 전망

■ 방어 체계를 우회하는 랜섬웨어 공격

△ 데이터 탈취 수법도 추가

△ 가상화, 윈도우 캐시 매니저 등 탐지 우회 기술의 지능화

랜섬웨어가 처음 등장한 이후 매년 공격이 크게 증가하고 있고, 2021년에도 공격 수법이 더욱 고도화될 것으로 보입니다. 기존의 랜섬웨어 공격은 내부 시스템에 침투해 데이터를 암호화하거나 시스템을 사용하지 못하게 한 후 대가를 요구했습니다. Maze 랜섬웨어[2]는 여기서 더 나아가, 데이터를 탈취한 후 이를 외부에 공개하겠다고 협박하며 금전을 요구했습니다. 이런 수법을 여러 공격자들이 모방하면서 금전을 이중으로 갈취하는 방식으로 랜섬웨어 공격 양상이 변화하고 있습니다. 그리고 호스트의 드라이브를 원격 공유로 마운트 후 가상머신에서 랜섬웨어를 실행하거나, 윈도우 캐시 매니저를 이용해 파일 내용을 암호화하는 등 백신을 우회하는 지능형 랜섬웨어 공격도 생겨났습니다. 랜섬웨어 공격의 대가 비용은 건당 수십억 원까지 늘어나고 있고, 앞으로도 공격자는 더 많은 피해를 입히기 위해 랜섬웨어 공격 기법을 서로 모방하고, 지능화하고 조직화될 것입니다.

■ 디지털 헬스케어 분야를 노린 공격

△ IoMT를 이용한 내부 시스템 침투 시도

코로나 바이러스로 인해 비대면 서비스가 활성화됨에 따라 의료산업에서도 IoMT[3]을 활용하려는 시도가 지속 증가하고 있습니다. 그러나 의료산업에서 IoMT가 활용된 것은 얼마 되지 않았으며, 아직은 초기 단계로 볼 수 있고, 다양한 의료기기 플랫폼에서 허술한 보안 구성을 발견할 수 있으며, 보안에 취약한 소프트웨어를 사용하는 등 위험 요소가 발견되고 있습니다. 이는 공격자에게 내부에 침투할 수 있는 공격의 빌미를 제공하는 것과 마찬가지입니다. 이를 통해 탈취된 개인의 건강정보, 생체정보와 같은 민감 데이터는 다크웹에서 최대 $1,000에 거래되고 있습니다. 해커 입장에서는 기존 $20 정도에 거래되는 신용정보보다 많은 금전적 이득을 취할 수 있는 셈입니다. 이와 같은 이유로 향후 IoMT를 통한 내부 시스템 침투 및 데이터 탈취 등의 공격이 증가할 것으로 보입니다.

■ 하이브리드 클라우드 환경의 보안 요소 증가

△ Hybrid Cloud 사용에 따른 위협 증가

많은 기업들이 Cloud 활용을 최우선으로 생각하는 단계를 넘어서 기업 경영의 모든 서비스를 Cloud에서 개발·운영하려는 "Cloud-Only" 방향으로 가고 있습니다. Flexera 2020 Cloud 보고서에 따르면 기업들의 35.5%가 Cloud 도입을 완료했으며, 그 중 Public과 Private Cloud는 각각 6%, 1%, 나머지 93%는 Hybrid Cloud를 도입한 것으로 조사되었습니다. 기존 Private 환경의 폐쇄성, 낮은 접근성의 문제를 해결하기 위해 Public과 Private의 장점을 모두 살리는 Hybrid Cloud를 선택하는 추세인 것입니다. 하지만 Hybrid Cloud는 여러 Cloud Platform을 조합하여 사용하므로 보안 관리 요소가 늘어납니다. 이처럼 Cloud 종류가 세분화되고 환경이 다양해지면서 보안에 신경 써야 할 부분이 많아질 전망입니다.

2) Maze 랜섬웨어 : 2019년 말에 등장한 랜섬웨어로 처음으로 데이터 갈취가 발견된 랜섬웨어. (2020년 중반기까지 꾸준히 발생)
3) IoMT(Internet of Medical Things) : 의료기기와 소프트웨어로 이루어진 디바이스와 통신으로 제공되는 서비스가 상호 연결된 시스템

4) SK인포섹 EQST[1] 2021년 5대 사이버 위협 전망

■ Ontact 환경 악용한 보안 위협 증대

△ 기업 대상에서 개인까지 확대되는 위협

Ontact는 비대면을 일컫는 Untact에 온라인을 뜻하는 “On”을 합한 말로, 온라인을 통한 각종 비대면 활동을 의미합니다. 코로나19로 인한 재택근무가 증가하면서 원격 의존도가 점차 높아지는 만큼 해킹 위협이 증가하고 있습니다. 실제 재택근무를 하는 직장인들을 노리고, 코로나19 관련 가짜 정보나 업무 파일로 위장한 피싱 공격이 증가했습니다. 또한, 재택근무에 사용하는 개인 PC는 기업내부 보안체계가 제대로 작동되지 않아 각종 보안 위협에 노출될 가능성이 크고, 기업뿐만 아니라, Ontact 환경에서 많은 일상 생활을 하고 있는 개인을 노린 공격도 더욱 거세질 전망입니다.

앞서 언급한 내년도 5대 사이버 위협 이슈에 대응하기 위해 SK인포섹은 IoT 진단 가이드 고도화, Cloud 모의해킹 진단 가이드 개발 등 최신 기법을 반영한 모의해킹 및 취약점 진단 기술을 내재화하여 보안 진단을 수행해 위협을 분석하고, 대책을 제시하고자 합니다.

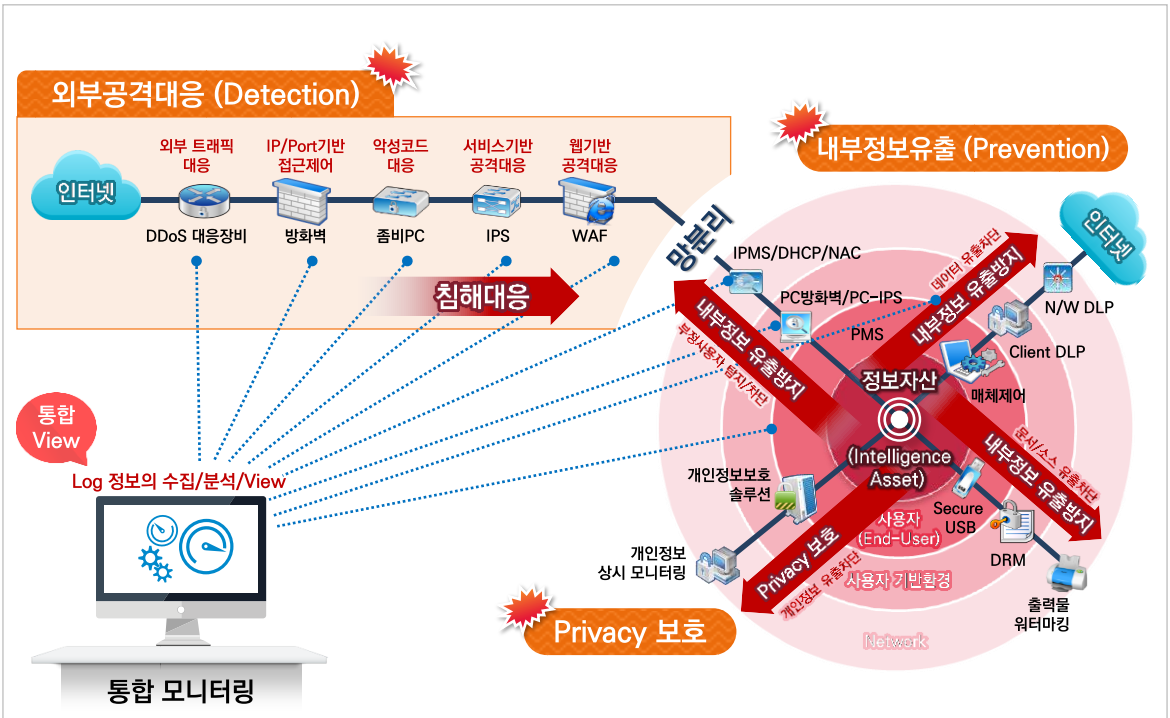
[그림 I -12. EQST그룹 사이버 위협 대응 전략 및 서비스]

2) Secudium Intelligence (SK infosec Service) : 글로벌 위협 정보를 수집하고, 보안 솔루션 또는 SIEM의 이벤트에 대한 신속한 위협 분석을 제공하는 위협 인텔리전스 서비스(Threat Intelligence Service)

Part 3

정보보호 시스템 아키텍처

1) 정보보호 시스템 개념도



[그림 I -13. 정보보호 시스템 개념도]

가. 외부공격대응(Detection)

- 급변하는 해킹 기술의 진화에 따른 실시간 대응 체계
- 해킹 등의 결과에 따른 즉각적인 처리
- 외부 Threat Intelligence 정보체계 강화

나. 내부정보유출(Prevention)

- 매체제어, 내부통제 및 관리 시스템 강화
- 핵심 자료의 관리 방안 체계 마련
- 인적, 물적, 시설물 관리 시스템의 강화
- 스마트 디바이스 등 신규 채널에 대한 통제 강화

다. Privacy 보호

- 개인정보보호법 등 관련 이슈 대응
- 관련 솔루션 및 상시 모니터링 체계 구축

2) 정보보호기술 프레임워크

가. 정보보호기술 아키텍처

[그림 I -14. 정보보호기술 아키텍처]

정보보호 기술 아키텍처는 각 시스템(Client, Network, Server, App, Data)별로 국제표준 아키텍처 기반의 ITU-T X.805[1] 기준으로 정보보호 기술영역과 적용대상에 해당하는 정보시스템 계층으로 정의합니다.

① 인증(Authentication)
② 접근/권한통제(Access Control)
③ 암호화(Encryption)
④ 부인방지(Non-repudiation)
⑤ 개인정보보호(Privacy)
⑥ 가용성/기타(Availability/etc)

1) ITU-T : International Telecommunication Union (국제전기통신연합)
X.805 : Security architecture for systems providing end-to-end communications

나. 정보보호기술 아키텍처 구성요소

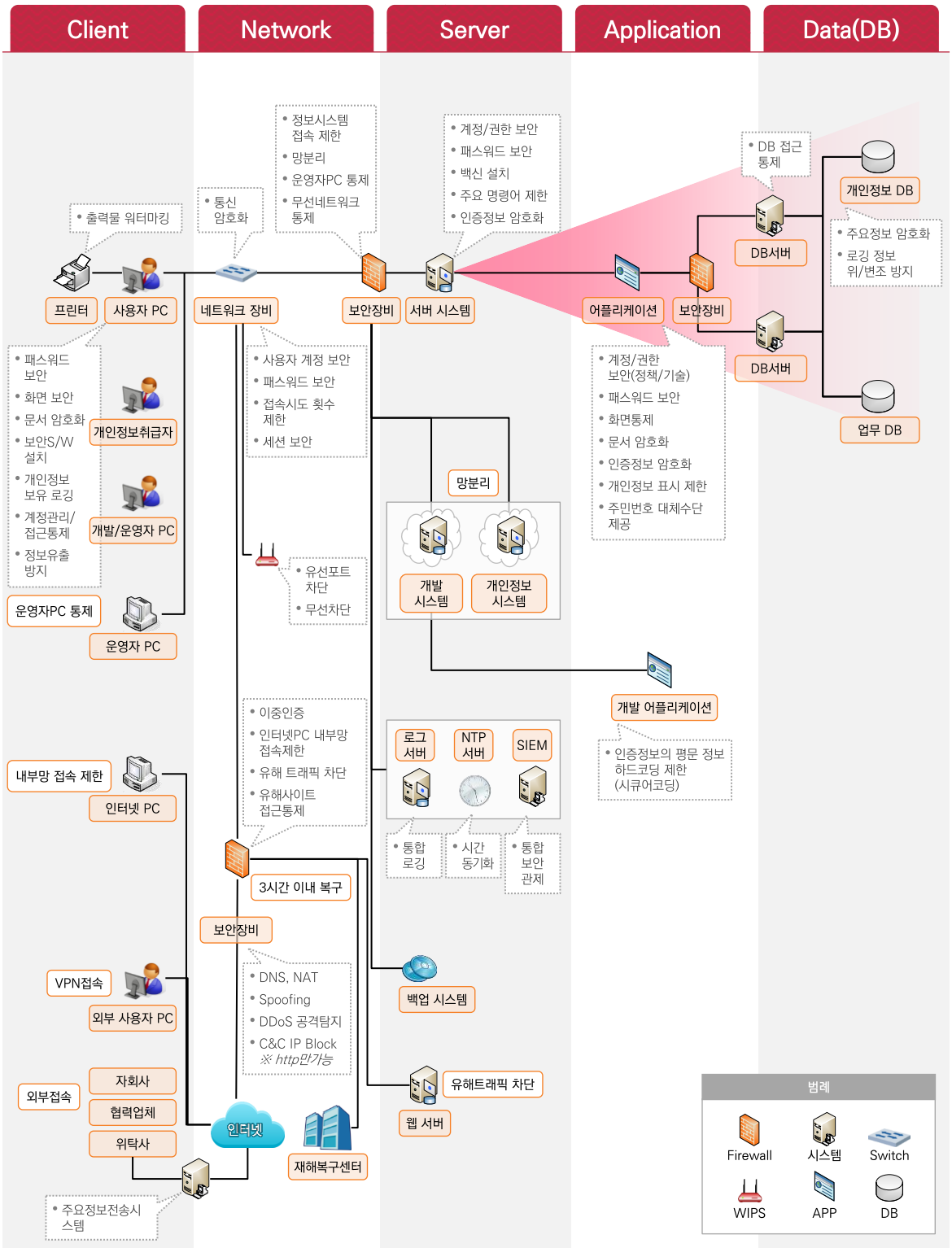
[그림 I -15. 정보보호기술 통제 모델]

다. 정보보호기술 요구항목

정보시스템 계층	Client	Network	Server	Application	Data(DB)
정보보호기술영역 / 인증			사용자 현행화		
			사용자 계정 생성		
	단순 패스워드 제한 / 패스워드 변경주기				
		최초 패스워드 변경/Default 계정 사용 제한/사용자계정 공동 사용 제한/안전한 관리자 패스워드 설정			
	업무용 단말기 인증	외부 접속 시 이중 인증	인증정보의 평문정보 하드코딩 제한		
접근/권한통제		주요 정보시스템 접속제한	바이러스 백신 설치	로그인 실패사유 알림 금지	
		인터넷PC 내부망접속 제한	관리자 역할 분리	최종 접속시간 표시	
		개발/테스트망과 운영망 분리		접속시도 횟수 제한	
		유해트래픽 차단	주요 시스템 명령어 제한	다중 연결세션 차단	
		시스템 관리자/운영자PC 통제		정보시스템 화면통제	
		무선네트워크 통제	불필요한 서비스 금지		DB 접근 통제
		로그오프 또는 세션종료			
암호화	문서 암호화	전송구간 암호화		문서 암호화	주요정보 암호화
	표준 암호화 준수	사용자 인증정보 암호화			
				표준 암호화 준수	
부인방지				조회 로깅	
				주요정보(DB) 변경 로깅	
		관리자/운영자 로깅			
			DB접근 로깅		
	개인정보 출력 로깅	시간 동기화		개인정보 출력 로깅	로깅 정보 위/변조 방지
		통합보안관리		자동 로그인 방지	
			개인정보처리자 계정/권한관리 내역 로깅		
개인정보보호	화면보호기 패스워드 설정				
	파일공유 보안성 강화				
	표준 보안관리 프로그램 설치			개인정보 표시 제한	
	이동저장매체 통제	유해사이트 접근 통제			
	출력물 워터마킹				
가용성/기타		재해복구센터 구축			
		보안설정 가이드 준수(네트워크)	보안설정 가이드 준수(서버)	시큐어 코딩 가이드 준수	보안설정 가이드 준수(DBMS)
			백업		

[그림 I -16. 정보보호 기술영역별 상세 요구항목]

라. 정보보호 영역별 구성도



[그림 I -17. 정보보호 영역별 구성도]

3) 영역별 보안 아키텍처

[그림 I -18. 통합보안 시스템 아키텍처]

보안SI를 통한 IT정보보호 구축 가이드

CONTENT

II

영역별 보안

II
영역별 보안

3. 계정권한관리 시스템

II
영역별 보안

4. 정보보안 포털 시스템

1) 시스템 개요
   - 가. 시스템 개요
   - 나. 시스템 구축 필요성 및 추진방향
   - 다. 주요 구축 내용
   - 라. 보안성심의 정의
   - 마. 기대효과

2) 시스템 구축
   - 가. 시스템 개념도
   - 나. 사전준비 필요사항
   - 다. 구축 유형

5. 이상징후 탐지 시스템

1) 시스템 개요
   - 가. 시스템 개요
   - 나. 시스템 구축 필요성 및 추진방향
   - 다. 주요 구축 내용
   - 라. 기대효과

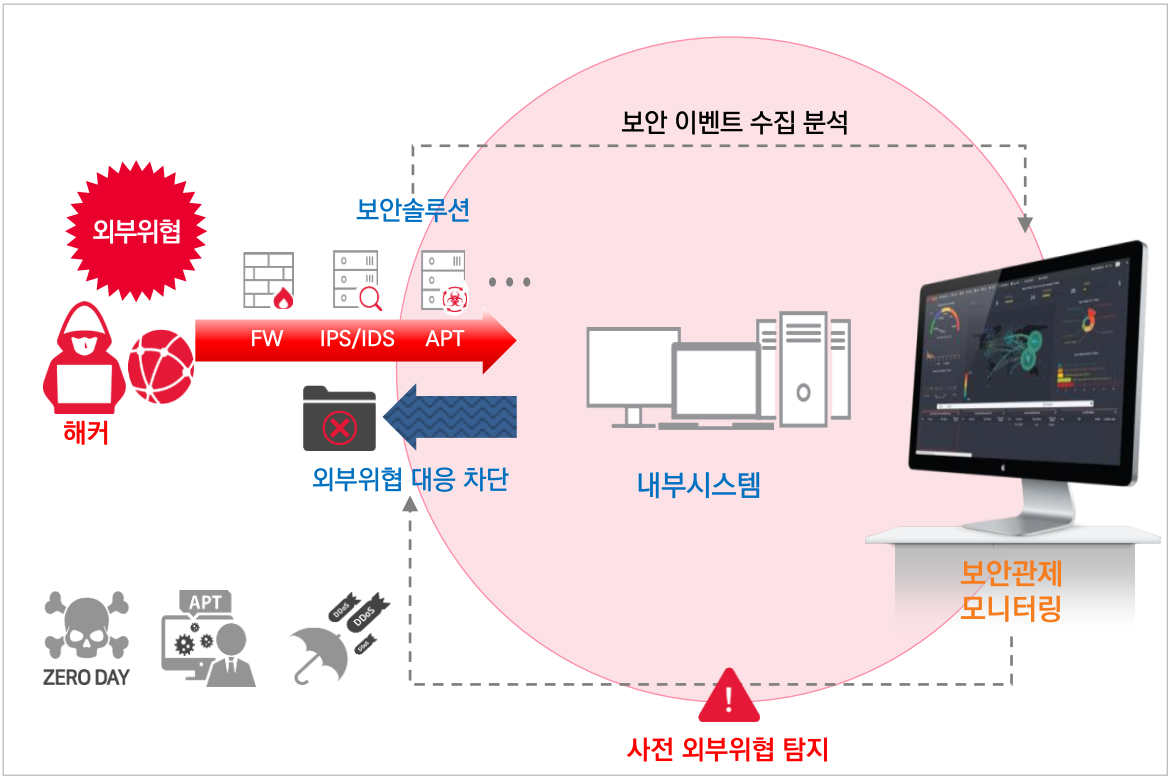
2) 시스템 구축
   - 가. 시스템 개념도
   - 나. 사전준비 필요사항
   - 다. 구축 유형

Part 1

통합 보안관제 시스템

1) 시스템 개요

가. 시스템 개요



[그림 II-1. 통합 보안관제 시스템 개요]

고객의 중요 정보와 인프라에 대한 보안침해 가능성은 늘 상존해 있고 외부위협은 날로 지능화, 고도화되고 있으며 침해를 통한 정보유출 및 시스템 장애는 고객에 큰 손실을 불러 일으키고 있습니다. 이에 많은 기업들이 보안 솔루션을 도입하여 고도화된 외부 위협에 대응하고 있지만, 분산된 보안솔루션 환경과 수동적 관리대응으로 인해 선제적 위협대응 및 정보보호 가시성 확보에는 한계점을 드러내고 있습니다.

통합 보안관제 시스템은 이러한 이기종의 분산된 보안 솔루션들의 위협 이벤트를 통합 상관 분석하여 확장된 보안가시성을 제공하고, 정의된 시나리오를 통해 외부 위협을 선제적으로 대응함으로써 고객의 중요 자산과 정보를 보호하게 합니다.

최근 통합보안 관제 시스템으로 ESM[1]과 SIEM[2] 시스템으로 구축이 활발히 이루어지고 있습니다.

1) ESM (Enterprise Security Management) : 기업 보안관리 시스템
(방화벽, 침입탐지시스템, 가상 사설망 등의 보안솔루션 통합 보안관리)
2) SIEM (Security Information & Event Management) : 정보보안 정보 및 이벤트 보안관제 시스템
(빅데이터 기반 보안솔루션 수집로그 상관분석 이벤트 관리 통합 보안관제 시스템)

나. 시스템 구축 필요성 및 추진방향

대부분 기업에서의 고민은 지능화되고 있는 침해사고 발생에 대한 대응력과 보안의 전문인력 부족으로 실시간, 자동화 방어체계를 필요로 하고 있습니다. 또한, 최근 보안관제를 위한 빅데이터 기반의 솔루션과 새로운 탐지기술이 고도화 되고 있는 상황입니다.

침해 위협에 대응할 수 있는 방어체계를 구축하기 위해서는 능동적인 대응을 위한 중·장기적인 추진 계획 수립이 필요합니다.

개선사항 및 필요성

외부 보안위협 증가

- 해킹에 의한 고객 중요자료 파괴 및 유출
- 랜섬웨어/제로데이 등 목적에 따른 맞춤형/지능형 공격 증가
- 네트워크를 통한 침해사고 증가
- 다양한 외부위협 및 증가에 따른 감독기관 정보보호 체계강화 요구

보안 전문성 부재

- 한정된 인력자원과 침해대응 건수 증가에 따른 보안관제 시스템 고도화와 업무 프로세스 개선 필요
- 노후화된 기존 ESM 시스템을 통한 로그 수집으로 시스템 모니터링 한계
- 침해사고 시 침해대응 역량 부족

보안 효율성 저하

- 대규모 로그정보의 실시간 통합처리 및 상관분석 필요
- 실시간 침해대응 의사 결정을 위한 C-Level 분석결과, 통계, 리포팅 체계 부재
- 감독규정 Compliance 준수 상시 점검 및 모니터링 시스템 부재
- 보안운영 미흡에 따른 관리 비용의 증가

추진 방향

로그 통합 집중화

분산 이기종 보안 이벤트 중앙 집중화

- 보안장비 로그 및 N/W 트래픽 정보 이벤트 통합 수집/정규화/저장
- 보안 위협 이벤트의 실시간 탐지/분석

보안관제 전문성 확보

침해사고 전문 대응체계 마련

- 보안침해 탐지를 위한 복합 이벤트 상관분석 시나리오 체계 구축
- Threat Intelligence의 실시간 수집 대응으로 위협정보의 선제적 대응
- Unknown 위협 이벤트 고수준 위협 분석을 위한 머신러닝(M/L) 알고리즘 데이터 과학 기법 활용

안정된 보안운영

의사결정 및 보안수준 관리 도구 확보

- 침해대응 의사결정을 위한 전사 통합 View 확보
- 사용자별/영역별/그룹별 관리영역의 권한분리 통합 대시보드
- 보안관제 운영현황 실시간 모니터링 및 주기적 보고체계

다. 보안관제 세대별 동향

과거의 보안관제는 알려진 공격에 대해서만 대응이 가능 하였으나, 점차적으로 위협정보의 공유와 인공지능을 기반으로 한 기술의 발전으로 기계학습을 통해서 알려지지 않은 공격에도 대응할 수 있는 체계로 변화하고 있습니다.

또한, 외부로부터 위협대응을 위주로 운영된 보안관제는 내부정보 유출 모니터링을 통해서 내부위협 분석과 임직원 및 내부 협력사의 이상행위 탐지까지, 내부와 외부를 통합하여 상관분석 할 수 있는 시스템으로 발전하고 있습니다.

보안관제는 SIEM을 기준으로 인공지능 기반 머신러닝의 발전과 Automation 및 시스템간 Optimize가 진행되는 Orchestration으로 진화하고 있습니다.

[그림 Ⅱ-2. 보안관제 세대별 동향]

라. 기대효과

기대 효과

STEP 1

보안 침해사고 대응 및 예방

- 보안솔루션의 연계 후 상관분석을 통한 침해 사고 사전 모니터링
- 사전 모니터링 된 이벤트를 통해 정책을 업데이트 하여 침해사고 예방
- 실시간 데이터 처리 및 자동화를 통해 침해사고 발생 시 대응 시간 단축

STEP 2

보안시스템의 효율적 분석 및 운영

- 보안환경 변화에 대응 가능한 상관분석 시나리오 기반 분석/탐지 역량강화
- 통합 분석을 통해 단위솔루션의 Hole 최소화
- 단위솔루션 로그를 중앙에서 수집, 관리하여 운영 중 이상 확인
- 이벤트 탐지 대응 및 티켓처리 자동화에 따른 이력관리

STEP 3

확장된 보안 가시성 확보

- 분산된 보안 인프라 통합 모니터링을 통한 보안 사각지대 해소
- 경영층의 보안위협 공유를 통한 의사결정 채널확보
- 전사적 보안수준관리 및 통합 모니터링 View확보

STEP 4

Compliance 대응 향상

- 감독규정과 Compliance 준수여부 상시 점검 및 모니터링 체계 구축
- 침해사고 대응 및 결과의 내부 증적자료 마련
- 침해사고 발생 시 기업의 법규상 대응 요구사항 만족

외부침해 위협 대응을 위한
통합 보안관제 시스템 구축

2) 시스템 구축

가. 시스템 개념도

[그림 Ⅱ-3. 통합 보안관제 시스템 개념도]

통합 보안관제 시스템은 Back-End[1] 보안이벤트 수집/분석 시스템으로부터 도출된 정보들을 Front-End[2] 시스템인 보안관제 대시보드와 관제 업무시스템으로 전달하여 효과적인 관제 업무를 수행하도록 합니다.

또한, 보안위협 대응 및 중요정보에 대한 감시를 수행하고, 악의적 보안 위협을 분류하여 탐지된 정보를 체계적으로 관리함으로써 선제적으로 보안 위협에 대응할 수 있습니다.

관제 모니터링, 빅데이터 분석, 인포그래픽 분석 등 다양한 부분의 정보 분석을 위한 시각화 대시보드를 구축하여, 위협 상황을 실시간으로 인지하게 하고, 각 시스템 별로 수집된 보안 이벤트를 통합 검색, 상관관계 분석 및 보안 시나리오 탐지를 통해 보안위협에 대한 원인을 빠르게 파악하고 조치할 수 있습니다.

최근의 보안관제 시스템은 머신러닝(M/L)[3] 기반의 관제 고도화를 통해 수집된 보안위협 정보를 스스로 학습하고 공격유형, 우회패턴, 이상징후 등을 분석하여 지능형 보안 위협에 대한 탐지대응이 가능하도록 하고 있습니다.

이러한 관제 고도화는 사람이 인지하지 못하는 보안위협을 탐지함으로써 보안관제 가시성을 더욱 향상시키고, 지능형 보안위협에 대한 탐지능력을 높일 수 있습니다.

1) Back-End : 서버와 데이터베이스의 내부 시스템 관련 프로그램
2) Front-End : 사용자가 직접 인터페이스 할 수 있는 프로그램
3) Machine Learning : 사람이 학습하듯이 컴퓨터에도 데이터를 전달하여 학습하게 함으로써 새로운 지식을 얻어내게 하는 분야

나. 주요 구축 내용

구축영역	구축방향	주요내용
데이터 수집	신규 및 기 운영 보안솔루션 보안 로그 통합	**보안 로그 통합** 1 보안 솔루션별 로그 통합 수집(F/W, IPS 등) 2 상관분석과 행위분석을 위해 인사정보 및 자산정보 추가 수집
탐지 및 분석	최적화된 보안 시나리오 적용 구성	**보안 시나리오 적용을 통한 상관분석** 3 보안 이벤트 별 탐지 정책 및 복합 상관분석 정책 구성 4 시나리오 컨설팅을 통한 탐지 Rule정의 5 보안 운영환경에 최적화된 보안 시나리오 6 빅데이터 기반 기계학습(M/L)을 통한 위협 분석 7 외부 Threat Intelligence 연계관리 및 분석 체계 구축
대응 프로세스 구현	관제운영 및 침해대응 관리 절차 마련	**보안관제 운영 대응절차 구축** 8 침해 위협 이벤트에 대한 처리 프로세스 체계 구축 9 침해사고 대응정책 및 프로세스 정규화 활동 10 보안 이벤트 발생현황 티켓 처리 및 이력관리 11 탐지결과 알림 및 경보 체계와 주기적 메일링 및 보고체계 구현
모니터링 이력 및 보고관리	보안 이벤트 모니터링, 주기별 보고 및 증적관리	**모니터링 및 이력관리** 12 실시간 모니터링을 위한 영역별 대시보드 13 주기별 보고서 및 탐지결과 증적관리

다. 사전준비 필요사항

통합 보안관제 시스템을 구축하고자 할 때 사전에 관제 운영담당자와 보안담당자는 운영 시스템 현황 조사와 To-Be 모델에 대한 방향성을 정의하여야 합니다.

실제 연동하여 수집되는 보안장비의 종수와 1일 로그량을 산정하여 H/W시스템 용량을 미리 산정하여 요청할 수 있습니다. 보안관제 S/W솔루션은 1일 로그량에 따라 라이선스가 적용되며, 대상장비에 따라 분석/설계 방향을 정의할 수 있습니다. 보안관제를 위한 시스템 도입과 고도화 사업으로 진행 시 새로운 관제 프로세스 개선방안과 신규 정책정의도 사업에 포함하여야 합니다.

[그림 Ⅱ-4. 통합 보안관제 시스템 구축 사전준비]

① 보안 인프라 구성 확인

- 운영 보안인프라 구성환경 확인 (시스템 종류, Node 수)
- 각 솔루션별 로그량 산정 (로그 수집 저장 용량 산정)
- 기 운영 네트워크 구성환경 확인 필요 (로그수집 가능여부)
- 수집 대상 별 수집방식 분류 (Syslog, DB, FILE, 패킷 수집 등)

② 보안관제 업무요건 정의

- 내부규정 확인을 통해 변경 필요사항 확인
- 시스템 운영 담당자와 협의 후 연동 로그 포맷 정의
- 업무 담당자들을 통해 현재의 보안업무 프로세스 확인
- 기존의 업무 Hole등을 고려하여 필요요건 확인

③ 보안 관제 시스템 모델링

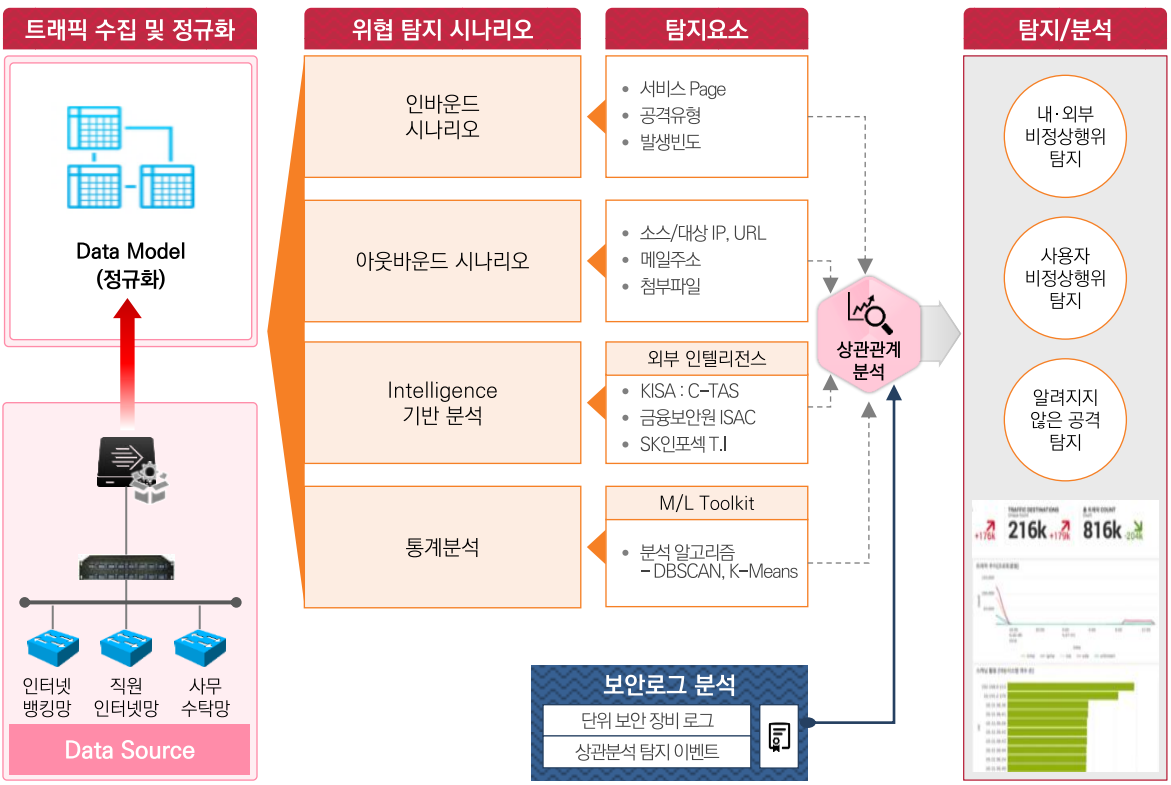
- 수집된 정보를 통해 구축 예상 모델 구성
- 예상 모델에 필요한 사항 체크리스트 작성
- 새로운 보안관제 시스템 구축에 따른 관제운영 절차 재수립

라. 구축 유형

SK인포섹에서 통합 보안관제 시스템을 구축한 사례로 구축 시스템의 특징을 유형별로 나누어 소개합니다.

✓ 유형 1 네트워크 트래픽 수집 및 시나리오 기반 위협탐지분석 구축 사례

기본적인 보안솔루션 로그 수집 외 네트워크 트래픽의 패킷을 수집하여 상관분석을 다양하게 할 수 있도록 추가하였고, 해당 분석 로그자료는 정규화된 시나리오로 이벤트를 탐지하여 처리 할 수 있도록 구축 하였습니다.



[그림 Ⅱ-5. 네트워크 트래픽 데이터 수집분석]

네트워크 트래픽 수집

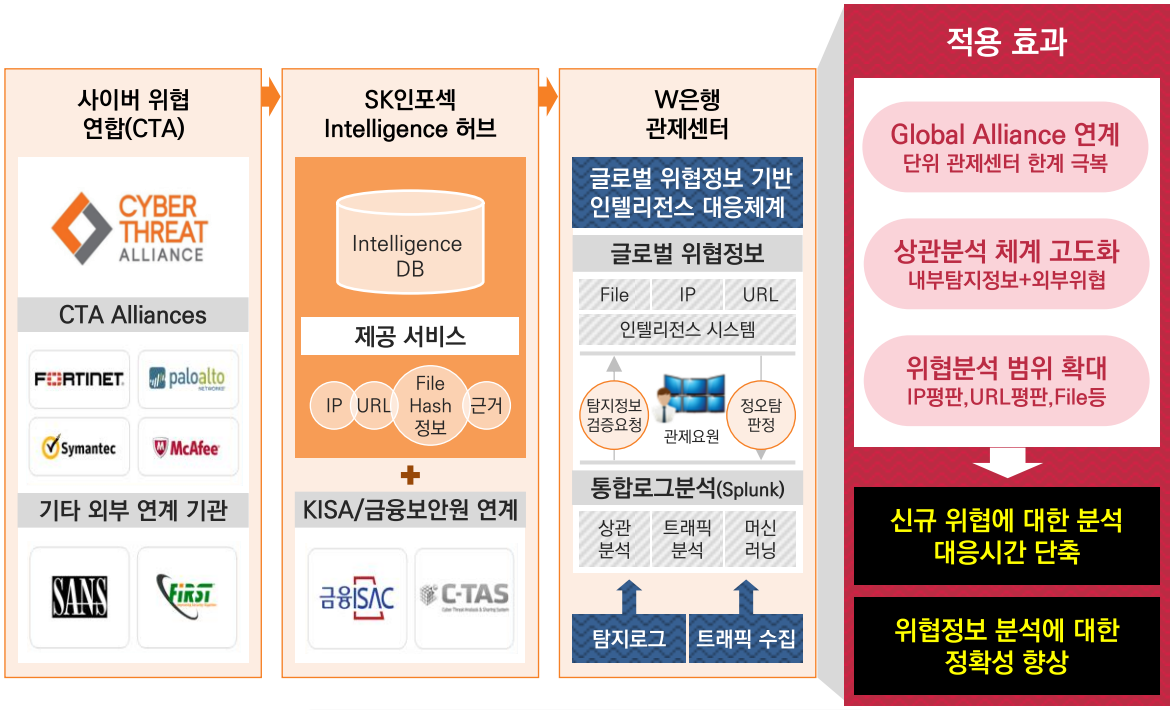
- 보안 솔루션 로그 뿐 아니라 네트워크 트래픽 데이터도 수집하여 상관분석을 통해 침해사고에 대한 대응 능력 향상
- 해당 금융업무 8개 구간 N/W트래픽 상세 정보 수집으로 관제 영역 확대

시나리오 기반 탐지/분석

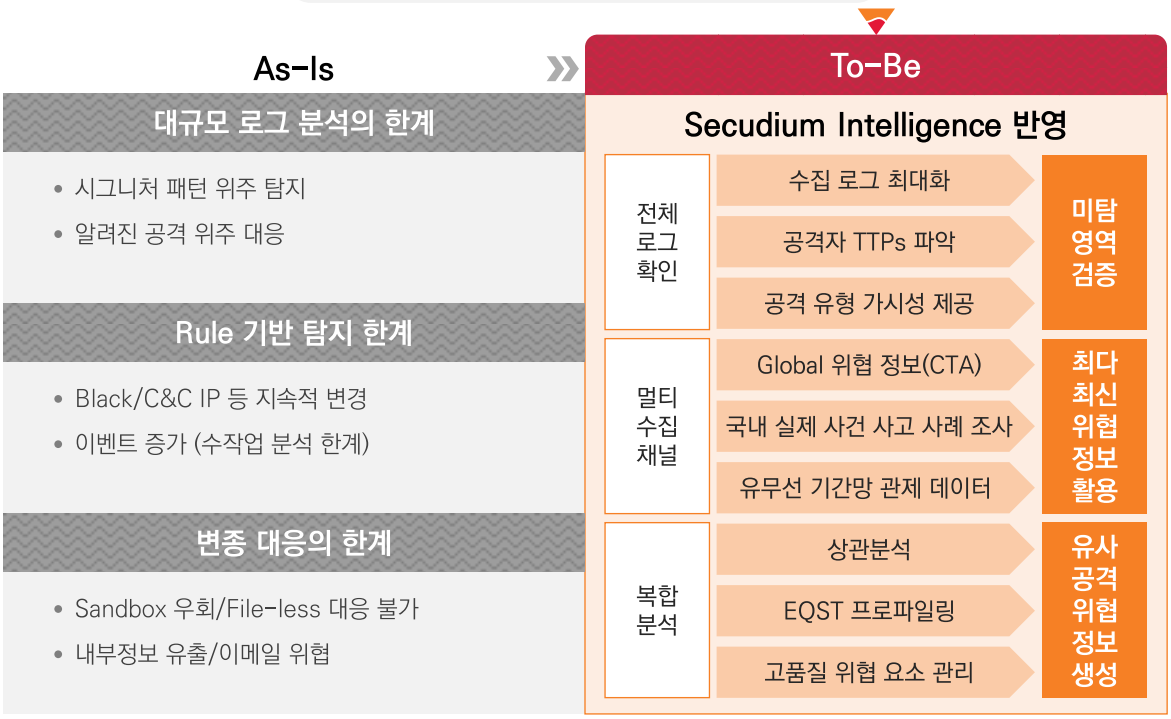
- 인바운드 및 아웃바운드 시나리오 컨설팅에 따른 시나리오 Rule 정의
- 단일/복합 시나리오 Splunk 빅데이터 솔루션 탑재 관리
- 내부 및 외부 시나리오 Rule에 따른 이벤트 발생 및 처리

✓ 유형 2 CTA[1] 기반 글로벌 Threat Intelligence 서비스 구축

SK인포섹은 사이버 위협정보를 공유하는 글로벌 사이버위협 연합(CTA)의 아시아 최초의 정규멤버입니다. Secudium Intelligence[2] 를 통해 고객사로 최신 글로벌 위협정보 서비스를 제공하고 있습니다.



[그림 Ⅱ-6. CTA기반 글로벌 위협정보 서비스]



[그림 Ⅱ-7. CTA 반영모델]

1) CTA(Cyber Threat Alliance) : 사이버 위협과 보안 정보를 실시간으로 공유하여 협력하는 Global 비영리 연합
2) Secudium Intelligence : 지능형 사이버 공격 대응을 위한 최적의 위협 분석 정보를 제공하는 SK인포섹 위협 인텔리전스 서비스

Part 2

SOAR

1) SOAR 개요

가. 보안관제 변화

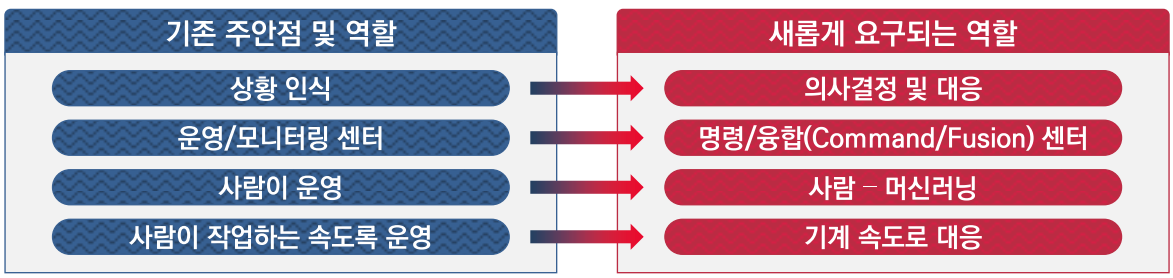
보안관제는 단일 보안시스템 통제로 시작하여 ESM솔루션으로 보안시스템의 로그를 통합 분석하는 시기를 거쳐, 최근에는 대용량 통합 로그분석을 하는 SIEM으로 운영되고 있습니다. 그로 인해 외부 위협이 지능화되고 대용량, 대량의 위협이 발생되고 있습니다. 이에 대한 방어체계로 보안관제의 자동화 대응 처리가 필요하게 되었습니다. 보안 운영 자동화 및 대응을 위한 SOAR[1]는 보안 시스템 운영 시 유입되는 사이버 위협에 대한 대응 레벨을 자동으로 분류하고, 표준화된 업무 프로세스에 따라 사람과 기계가 유기적으로 협력해 대응역량을 높일 수 있도록 지원하는 플랫폼을 의미합니다.

한국인터넷진흥원(KISA)은 '『2019년 보고서』를 통해 최근 보안 제품들간 연계의 중요성이 높아지면서 SOAR가 각광받고 있다'고 밝힌 바 있으며, 해당 보고서에서는 RSA 컨퍼런스를 리뷰하며, '글로벌 트렌드가 통합 보안 관제(SIEM)를 넘어 SOAR로 넘어가고 있다'고 설명했습니다.

보안관제 주요 동향

1. 지능화되고 급변하는 위협환경에 대응하기 위한 효과적 통합 솔루션 필요
2. 보안 전략에 있어서 대용량 데이터 전략 의존도 증가
3. 보안 제품에서 상관 분석 및 머신러닝 활용 증가
4. 보안 인력난 해결방안, 보안 운영에서 자동화 확대가 요구
5. 새로운 형태의 관리형 SOC 보안 모델에 대한 요구
6. 최신 위협정보와 효과적인 위협 탐지/대응 필요에 따른 보안관제 고도화

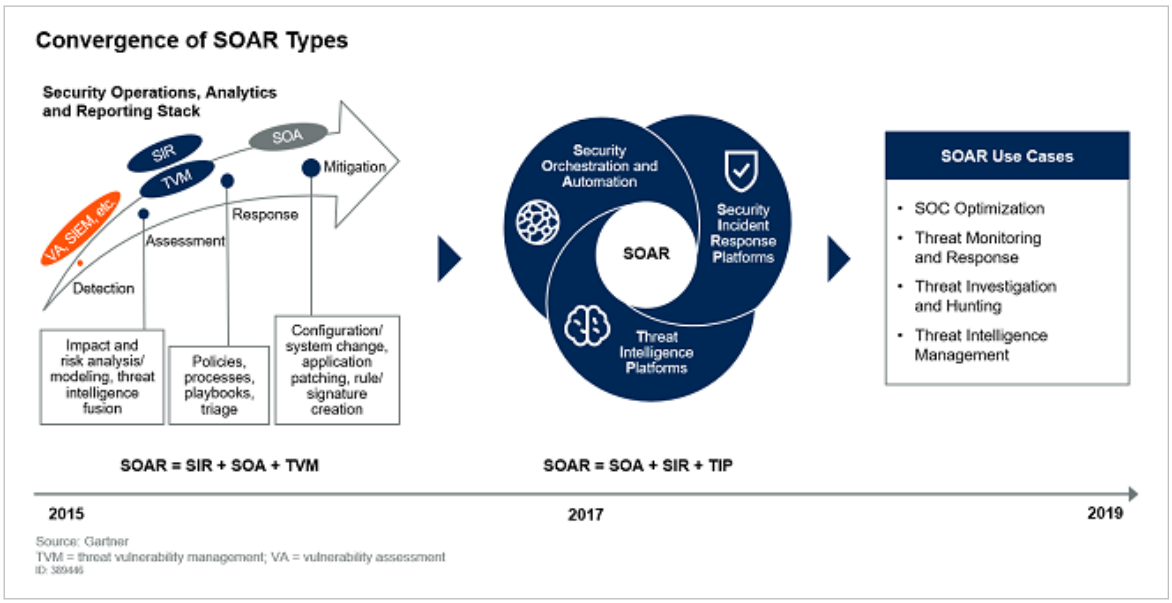
[그림 II -8. 보안관제 주요 동향]



[그림 II -9. 보안관제 주안점 및 역할 변화]

1) SOAR (Security Orchestration, Automation and Response) : 보안 오케스트레이션 및 자동화 대응 플랫폼. 조직내에 있는 모든 보안 도구들을 통합한 다음, 보안 침해 사고대응 Workflow를 자동화 시키는 것

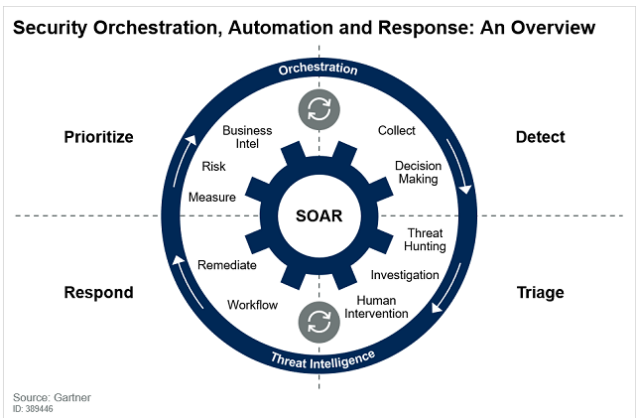
나. SOAR 정의



[그림 II-10. SOAR 유형]

SOAR라는 개념은 2017년 가트너가 처음 제시했습니다. 가트너는 'SOAR'의 주요 기능으로 ▲다양한 보안 솔루션과 연동 ▲보안 업무 자동화 ▲SOC 업무 중 리포트 및 대시보드 통합 등이며, 자세히 살펴보면 SOAR는 작업, 프로세스, 정책 실행 및 리포팅을 자동화하고 보안 솔루션들을 오케스트레이션 할 수 있어야 합니다. 더불어 보안 취약점에 대한 조치 및 작업, 리포팅, 협업도구를 형상화해야 하며, 보안사고에 대해 계획, 관리, 추적하여 대응할 수 있는 기술이 적용되어야 합니다.

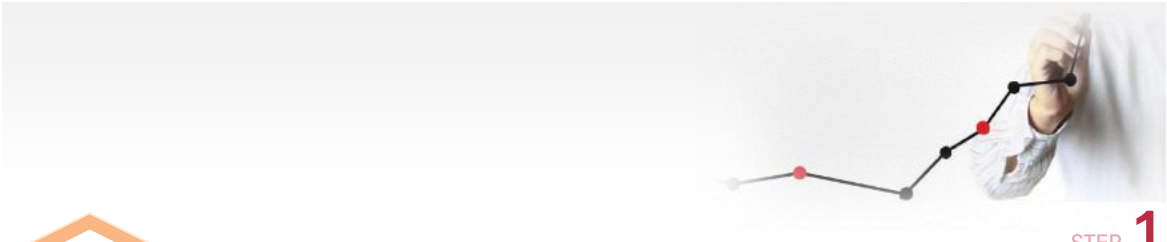
SOAR 솔루션을 구축하면 ▲운영 활동에 대한 우선순위 구분 ▲우선순위 및 위협 대응 형상화 ▲작업 프로세스 자동화 등의 이점을 얻을 수 있으며, 다양한 보안 솔루션에서 발생하는 위협 알람과 IT 시스템 운영 시 발생하는 데이터를 통합할 수 있고, 보안 이벤트의 가시성을 높이고 중요도를 구분해 사이버 위협에 대응할 수 있습니다.



[그림 II-11. SOAR 개요도]

다. SOAR 핵심 기능

SOAR는 다양한 보안 위협에 대한 대응 프로세스를 자동화해 낮은 수준의 보안 이벤트는 사람의 도움 없이 처리하고, 보안 사고 발생시 표준화된 업무 프로세스에 따라 직원이 쉽게 대응할 수 있게 도와주는 보안솔루션입니다. 가트너는 SOAR를 통해 사람(People), 기술(Technology) 그리고 프로세스(Process)를 조율하고 자동화함으로써 조직에서 사고 대응 효율성과 일관성을 개선하고자 합니다. SOAR는 보안 오케스트레이션 및 자동화(Security Orchestration and Automation, SOA), 보안 사고 대응 플랫폼(Security Incident Response Platform, SIRP), 위협 인텔리전스 플랫폼(Threat Intelligence Platform, TIP)의 세 가지 보안 대응 영역을 제공합니다.



STEP 1

SOA(Security Orchestration and Automation : 보안 오케스트레이션 및 자동화)

- 한 조직이 보유한 여러 개의 Workflow를 관리하는 기법
- 툴 간 Workflow를 자동화시키는 영역으로, SOAR의 핵심 기능
- 보안 대응팀의 단조롭고 반복적인 업무를 파악하고 그 업무에 소요되는 시간 절약

STEP 2

SIRP(Security Incident Response Platforms : 보안 사고 대응 플랫폼)

- 툴 간 자동화가 아니라 프로세스의 자동화
- SIEM에서 탐지된 위협 대응 지원 시스템(티켓 처리 시스템)
- 보안 사고가 발생하면 사고 유형별로 내부 보안 사고 대응 정책에 의해 미리 정해진 프로세스에 따라 어떤 업무를 할 것인지, 해당 업무가 누구에게 할당되고 SLA에 의해 언제까지 마무리 해야 하는지 관리

STEP 3

TIP(Threat Intelligence Platforms : 위협 인텔리전스 플랫폼)

- 위협 인텔리전스 중 관련 데이터를 찾아 환경에 맞는 최적의 Action 제시
- 조직에서 발생하는 보안 위협의 분석 업무를 지원하기 위해 여러 소스의 위협 데이터를 실시간으로 수집, 상관 분석 제공
- 분석된 위협 정보 데이터를 기업의 기존 보안시스템이나 대응 솔루션과 연계해 위협 요소를 제공함으로써 보안 인력의 사전 대응력 상승.

라. SOAR 필요성 및 업무효과

보안관제 문제점 및 SOAR 특장점

보안인력 부족 / 보안경고 증가 / 느린 사고대응 / 복잡한 보안 도구 / 프로세스 부족 / 비용

→ 자동화 / 오케스트레이션 / 워크플로우 / 도구 통합

SOAR 핵심 기능

① SOA
- 작업, 프로세스, 정책 실행 및 리포팅 을 자동화 및 오케스트레이션 할 수 있는 기술

② SIRP
- 보안 사고에 대해 어떻게 계 획 하 고 관 리 하 고 , 추적하고, 조화롭게 조정해 대응할 수 있는 기술

③ TIP
- 취약점에 대한 조치 및 작업, 리포팅, 협업 도구를 형상화 하는 기술
- 관제요원의 사전 대응 능력 향상

보안관제의 문제점

① 보안경고 증가
- 보안팀은 수많은 보안대응 경고를 받지만, 이 경고 중 평균 약 7% 미만에 대해서만 응답

② 느린 사고 대응
- 평균 대응 시간(MTTR : Average Mean Time to Respond)은 거의 4.4일 소요

③ 부적절한 보안교육
- 보안 분석가를 효과적으로 교육시키는데 평균 8개월 소요되며, 이 전문가 중 4분의 1은 2년 이내에 조직을 변화

④ 복잡한 보안 도구
- 복잡한 보안 도구로 작업하는 것에 대한 상당한 어려움

⑤ 보안 메트릭 부족
- 인시던트 대응 메트릭 측정 시스템이 없음

SOAR 업무 기대효과

① 운영활동 우선순위 구분
- SOAR는 서로 다른 보안 도구와 3rd Party 위협 피드 및 IT 데이터의 통합
- 보안 이벤트의 가시성을 높여 위협 대응 중요도를 구분하여 대응

② 우선순위 및 위협 대응 형상화
- 최선의 사례를 기반으로 보안 사고를 리뷰하고 평가하며 격리 치료 조치
- 과다한 작업과 부족한 자원의 사이버 보안 작업 환경에서도 빠른 위협 대응 및 문제 해결

③ 작업 프로세스 자동화
- 시간이 많이 걸리고 평범한 행위를 자동화하여, SOC 엔지니어가 위협 헌팅과 같은 더 높은 수준의 위협 분석에 집중

[그림 II -12. SOAR 필요성 및 특장점]

마. 기대효과

기대 효과

STEP 1

오케스트레이션 플랫폼 구축

- 기존 개별적인 보안 인프라를 하나의 플랫폼으로 통합
- 이벤트 발생부터 대응 완료 단계까지 전반적인 워크플로우에 인프라 전체가 방어 전략에 적극 참여하도록 오케스트레이션 수행

STEP 2

관제 업무 효율성 제고

- 관제 대응 절차를 표준화하여 처리 숙련도의 영향을 최소화하여 효율적인 대응이 가능
- 관제 업무에 적용된 정책을 수정, 변경하여 재사용함으로써 효율적인 시나리오 생성 기반 마련
- 담당자별 시나리오 및 정책 공유로 중복 룰을 제거하여 업무 효율성 증대

STEP 3

보안 사고에 대한 대응능력 향상

- 내·외부 감사 및 규제에 대한 선제적 대응
- 자동화를 통하여 신속한 탐지, 조사, 대응함으로써 위험 최소화
- 각종 규제 준수로 인한 대외 서비스 신뢰도 향상
- 보안 프로세스, 자원(인력, 장비 등), 기술, 통제에 대한 효율화, 통합화를 통한 대응 능력 보유

STEP 4

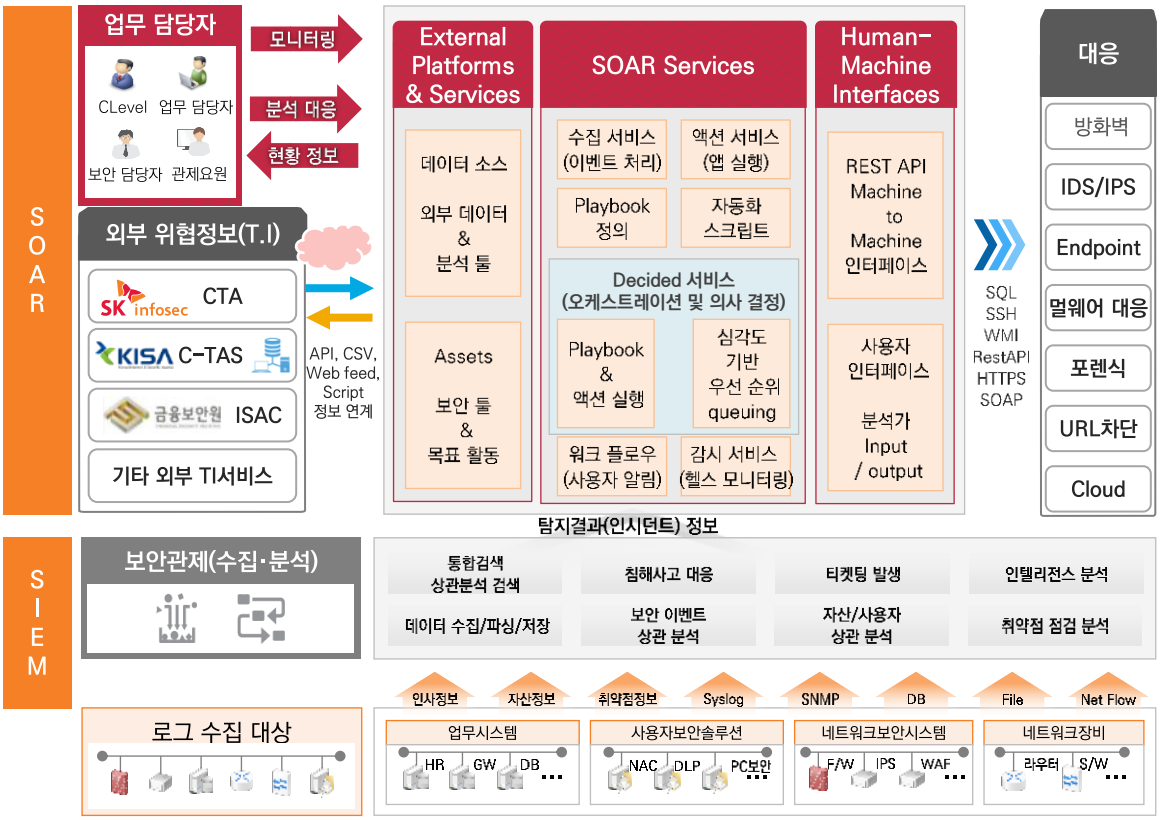
통합 분석기반방식을 통한 대응 체계화

- 보안 조사, 검증, 대응에 이전보다 빠르고 정밀하게 대응하여 여러 문제들에 신속하게 대처
- 기존 보안 인프라를 통합하여 각 부분이 적극적으로 작동하도록 함으로써 방어 강화
- 팀, 프로세스, 도구를 하나로 통합하여 반복 작업의 자동화를 함으로써 스마트한 운영 구현

침해 대응 능력 강화 및 관제 업무 효율화를 위한 보안 운영 자동화 및 대응

2) 시스템 구축

가. 시스템 개념도



[그림 II -13. SOAR 시스템 개념도]

SOAR 시스템은 기본적으로 통합로그분석 시스템(SIEM, ESM)이 구축되어 있어야 하며, SIEM에서 탐지결과 이벤트 발생부터 프로세스가 시작됩니다. SIEM에서 시나리오나 탐지룰을 기반으로 도출된 이벤트(인시던트)는 SOAR로 연동되어 준비된 자동화 프로세스를 실행 시킵니다. 각 업무별 프로세스의 정의는 Playbook이라는 절차에 따라 진행되며 추가분석, 담당자 알림, 외부 T.I(Threat Intelligence)와의 연계 분석, 보안장비 자동 정책적용 등으로 수행됩니다. 이 각각의 업무들은 자동과 수동으로 처리되며, 대응결과는 통계와 보고서로 관리됩니다.

SOAR 시스템 플랫폼 구축 시 중 가장 중요한 부분은 Playbook을 어떻게 만들고 정의하느냐에 따라 운영 효율성의 기준이 됩니다. 기본적으로 기존에 진행했던 보안관제 업무를 정형화, 프로세스화하여 정의 합니다. 단순 반복업무와, 의사결정이 필요한 업무, 공유해야 할 업무나 단계를 우선 정의하고 Playbook으로 구축합니다.

또한, SOAR 구축 시 자동화 대응은 악성 프로세스 동작 점검, 의심파일 수집, T.I연계분석, 감염 Host 네트워크 격리, 불법계정 접근 제한 등으로 처리하는 업무 외에 IP, URL차단과 같은 중요한 업무는 의사결정 후에 처리하는 것이 안전할 수 있습니다.

나. Playbook 작성방법

SOAR 솔루션은 단순히 플러그 앤 플레이(Plug-and-Play) 제품이 아니며, 초기 설치 시 기본적인 라이브러리 Playbook이 제공됩니다. Playbook은 각 기업 환경에 적합하도록 커스터마이징을 해야 합니다. Playbook이란 관제 업무처리에 대한 전체적인 업무처리 프로세스를 시스템화 하는 것으로, 자동화 처리되는 부분과, 담당자가 수동이나 의사결정 후 진행 하는 부분을 모두 포함합니다. 보안관제 업무처리는 외부위협 정보의 Case별로 절차가 구분되어 있으며, 기업 자체적으로 구현은 쉽지 않아서 보안관제 Playbook을 자동화 할 수 있는 전문 기업이나 컨설팅이 필요한 부분입니다.

보안관제 업무처리 정의 단계 이전에 우선 필요한 부분은, 많은 시간이 소요되는 수동업무 선정, 단순반복 작업 선정, 업무처리의 우선순위 설정 등이 필요합니다.

시작 조건

Playbook 프로세스의 첫 번째 이벤트가 나머지 단계를 트리거 하며, 종종 전체 Playbook에서 해결되는 보안 문제입니다.

프로세스 단계

여기에는 시작 조건에 의해 트리거 된 정책 및 절차를 충족하기 위해 조직이 수행해야 하는 모든 주요 활성화가 포함됩니다. 이것은 Playbook의 핵심 구성 요소이며 대응 조치 생성, 응답 승인, 격리 등의 주요 단계를 포함합니다. 이러한 단계는 일반적으로 조직에 현재 이러한 기능이 없더라도 향후 자동화 (Human 통제 포함) 를 장려합니다.

모범 사례 및 지역 정책

이는 조직의 특정 산업에 따라 다릅니다. 여기에는 핵심 프로세스 단계 외에도 수행 할 수 있는 활동이 포함됩니다.

최종 상태

Playbook의 최종 목표입니다. Playbook의 완료를 나타내는 시작 조건에 따라 원하는 결과입니다.

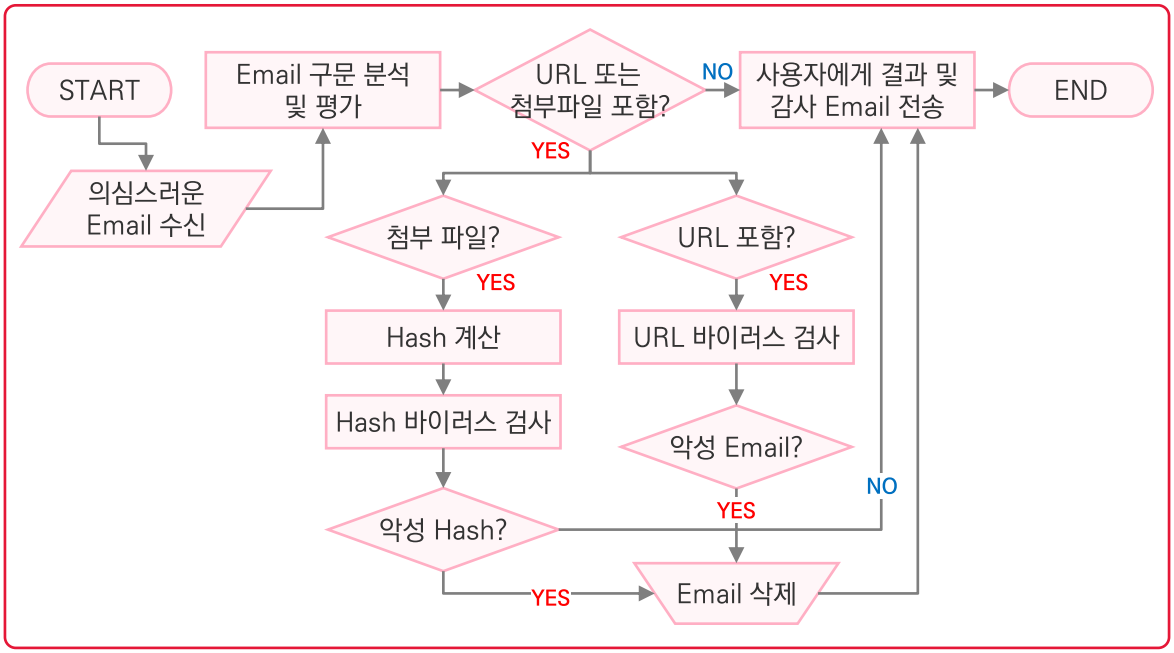
거버넌스 및 규제 요구 사항과의 관계

이 구성 요소는 주요 프로세스 단계를 다양한 준수 및 규제 법률에 필요한 단계와 관련시킵니다.

Playbook 작성 방법

1. 시작 조건 확인
2. 시작 조건에 대한 응답으로 발생할 수 있는 모든 가능한 조치 나열
3. 가능한 모든 조치를 “필수”로 분류하고 위협을 완화하기 위해 수행해야 하거나 “선택 사항” 으로 분류하고 더 많은 모범 사례로 간주
4. 3단계에서 결정된 “필수” 요소만 사용하여 Playbook 프로세스 순서 작성
5. “선택적” 범주의 단계를 활동 또는 기능별로 그룹화 할 수 있는지 확인 (예 : 모니터링, 강화, 응답, 확인 또는 완화)
6. 4단계에서 생성 된 프로세스를 수정하여 선택적 프로세스가 발생할 위치를 나타냄
7. 프로세스 단계의 선택적 작업을 삽입
8. 다른 플레이 북에 대한 종료 상태 또는 다른 시작 조건을 식별
9. Playbook이 충족하는 규제 법률 및 요구 사항을 나열

[그림 II -14. Playbook 작성 방법]



[그림 II -15. 피싱 Playbook 예시]

다. 사전준비 필요사항

① 사고 대응 프로세스 정의

- 기본적인 사고 대응 프로세스 정의
  → 보안 사고 발생시, 어떻게 할 것인지 미리 정의
- 예를 들어, SOC가 랜섬웨어의 감염을 탐지했을 때나 SQL 인젝션 공격을 탐지했을 때, 어떤 조치를 취하고 대응 할 것인지 사전에 업무 프로세스를 수립
- 각 침해위협 유형별로 절차와 담당자 지정 및 공유 대상자 지정

② 자동화 업무 프로세스 선정

- 정의된 업무 프로세스 가운데 자동화시킬 수 있는 부분 선정
- 보안 사고가 발생하면 사전 정의한 업무 프로세스대로 이행하게 되는데, 이 가운데 특정 보안 솔루션과 연계하는 작업이 있으며, 예를 들어,
  ① 샌드박스를 통해 악성코드 유입여부 확인
  ② LDAP에서 감염된 단말의 사용자 확인
  ③ 관계자에게 이메일 송신
  등 여러 가지 업무 중 업무 프로세스 성격에 따라 해당 업무가 사람에게 맡겨지느냐, 툴간 자동화된 프로세스에 맡겨지느냐가 정해짐
- 해당 업무 중 자동화 기술 적용 부분 확인

라. 자동화 적용 절차

자동화 사례 도출
- 고객사 환경의 보안 제품 및 환경 파악
- 수작업으로 진행 중인 보안관제 프로세스 확인 및 문서화
- 수작업 프로세스 기반으로 자동화 사례 도출

설치 및 구성
- 보안솔루션 구축 환경을 기반으로 한 환경 구축
- 도출된 자동화 사례 기반으로 고객사 보안 제품과의 연계를 위한 설정

연계 모듈 개발
- 해당 어플리케이션과의 연계를 위한 연계 모듈 개발
- 기타 공통 처리를 위한 연계 모듈 개발

Playbook 개발
- 선별된 자동화 프로세스에 대한 Playbook 개발
- 상황에 따른 전문인력 커스터마이징 지원

고객 검토
- Playbook 검증
- 추가 요구사항 반영

반복

마. 솔루션별 특징

SOAR 솔루션은 글로벌 시장에서는 공공, 금융, 제조 등 다양한 분야에서 SOAR에 대한 관심과 구축을 시도하고 있습니다. 특히 보안에 대한 투자가 많고, 보안관제센터를 운영하고 있는 기업들로부터 수요가 발생하고 있습니다.

국내시장에서는 금융권을 시작으로 SIEM 구축 이후 SOAR를 거의 2020년부터 구축을 시도하고 있는 상태입니다. 국내제품 장점은 Customizing이 용이한 반면 아직 활성화와 검증이 다소 부족한 부분이 있으며, 글로벌 제품은 고객사 환경에 접합한 Customizing에 한계가 있으나, 다년간 글로벌에서 검증된 제품으로 도입되고 있는 상황입니다.

개발사	제품명	주요기능	솔루션 특징
Paloalto networks	Cortex XSOAR	▪ 폭넓은 보안 사용 사례에 대한 프로세스 표준화 및 자동화 ▪ 350개 이상의 Playbook 제공 ▪ 보안 중심의 사례 관리를 통해 모든 알림에 빠른 대응 ▪ 실시간 협업을 통한 보안운영팀(SecOps) 효율성 향상 ▪ 신뢰성와 성능이 보장된 위협 인텔리전스를 통해 즉각적인 조치 ▪ 챗옵스(ChatOps) 및 가상의 워룸(war room)을 통해 팀 간 조사를 효율화 ▪ 다양한 소스의 취합, 피드 커스터마이징 및 스코어링, 고객 특화 환경에 대한 지표 매칭	▪ 2019년 3월 인수한 데미스토(Demisto) 제품을 고도화한 것 ▪ 전사적인 차원에서 위협에 즉각적으로 대처할 수 있는 기반 제공 ▪ 국내 대형 S제조사 구축 사례
SecuLayer	eyeCloud XOAR	▪ SIEM과 SOAR를 엔드 투 엔드 보안 운영 관리와 결합 ▪ 탐지된 위협 경보를 자동 또는 수동으로 그룹화 및 우선순위 지정으로 지능형 위협 Case 중심 처리 ▪ 국내 최대 보안관제업체 SK인포섹 Secudium Intelligence 글로벌 위협정보 제공 ▪ 보안관제 팀워크의 표준화 ▪ 모든 상호 작용은 중앙에서 쉽게 검색 및 감사 가능한 저장소에 관리 ▪ 반복 가능한 자동 응답 프로세스 생성 ▪ 간단한 드래그 앤 드롭으로 분석부터 대응까지 모든 것을 자동화하는 사용자 정의 가능한 프로세스를 구축 ▪ 보안분석 및 보안관제 전문기업 시큐레이어의 다수의 보안관제시스템 구축 레퍼런스 보유	▪ 컴포넌트 전문 개발자에 의한 커스터마이징 지원 ▪ 국내 보안환경에 따른 침해사고대응 프로세스, 공격별 분석 Playbook 생성 가능 ▪ SIEM + SOAR 단일 플랫폼 및 한글화에 따른 편리한 사용환경
Splunk	phantom	▪ 자동화 기능 : 반복 작업 자동화로 보안팀의 역량을 증대 ▪ 오케스트레이션 기능 : SOC 전반에서 구성되는 복잡한 워크플로우를 손쉽게 조율 ▪ 협업 기능 : 작업 맥락을 잃지 않으면서 의견 교환이 가능하고 관심 아이템을 팀과 공유 ▪ 이벤트 관리 기능 : 가장 관련있는 이벤트부터 우선적으로 분류하고 검증된 이벤트를 공식 케이스로 에스컬레이션 ▪ 케이스 관리 기능 : 기존의 최적의 사례를 더욱 세밀하게 관리하여 정교한 위협의 대응 관리 ▪ 리포팅 및 매트릭 기능 : 운영 상태 및 팀 역량을 신속하게 평가하고 조직의 보안 투자에 대한 효과 입증	▪ 3'd party 제품과 손쉽게 연계하기 위한 APP 및 API 와 약 50여 개의 내장된 Playbook 제공 ▪ GUI 기반의 Playbook 구성 기능 제공 ▪ 사용자가 정의한 Query를 통해 데이터에 대한 조회 수행

개발사	제품명	주요기능	솔루션 특징
Fortinet	FortiSOAR	▪ 인시던트 관리 – SOC 분석 전문가가 효율적으로 알림을 조사하고 인시던트 이해, 검토 및 관리 능력을 향상 ▪ 자동 워크플로우 – 제품 내에서 워크플로우를 생성하고 기존 엔터프라이즈 도구와 통합 – 200여 개의 Playbook 제공 ▪ 손 쉬운 보안 관제 – 고유한 관리형 보안 서비스 제공업체(MSSP) 지원 고객 중심적 대시보드, 워크플로우 및 뷰를 생성하여 고객 세그먼트 전체에서 손쉽게 보안 관제 관리 가능 ▪ SOC 대시보드 및 보고서 – 고급 시각적 대시보드를 내장하여 고객이 보안 관제 내에서 맡은 역할별로 간편하게 대시보드 생성 ▪ 파트너 커넥터 – 기존 엔터프라이즈 보안 솔루션을 통합 – SIEM, 네트워크 보안, 엔드포인트, 클라우드 등에서 기존 공급업체와 연결된 280개 이상의 파트너 커넥터 제공 ▪ 대기열 관리 – 내장된 대기열 관리 기능이 SOC 내의 여러 대기열 및 팀의 자동 작업 할당 처리	▪ 사례 관리 – 인시던트 대응을 위한 OOB 모듈, 취약성 및 위협 관리 – 나만의 모듈 구축(예: GDPR, Legal) – 상황별 가시화 ▪ 간소화된 대응 – 비주얼 Playbook 디자이너 – 자동 작업을 위한 커넥터 제공 – 실제 사용 사례에서 가져온 참조 콘텐츠 ▪ 멀티테넌트 – 분산형/연합형 아키텍처 – 데이터 및 환경설정에 대한 액세스 제어
IBM	Resilient	▪ 동적 Playbook : 사고 상황을 실시간으로 자동 대응하고 분석가가 사고를 접하기 전에 반복적인 초기 단계가 완료 ▪ 시각적 워크플로우 : 복잡 다난한 워크플로우를 시각적으로 보여줌 ▪ 사고 시각화 : 조직 환경에서 발생한 보안 이벤트(사고) 사이의 관계 또는 IoC(Indicators of Compromise) 등을 시각적으로 표시 ▪ 타이머 : 팀이 시기 적절한 대응을 보장하고 병목 현상을 식별하며 SLA를 준수할 수 있도록 워크플로우에서 시간 기반의 규칙 적용 ▪ 아티팩트 워크플로우 : 툴 간 자동화 워크플로우를 구현하는 동시에 사람 중심의 작업 및 승인을 허용 ▪ 작업 및 스크립트 : 워크플로우에서 스크립팅 기능을 추가해 플랫폼 내 자동화	▪ 정보보호 침해사고 대응 시간 단축 ▪ 침해대응 워크플로우 기본 제공 ▪ 자동화 및 국제 표준 프로세스 내장 ▪ 보안팀 대응 역량 업그레이드
Microsoft	Azure Sentinel	▪ 온-프레미스와 여러 클라우드의 모든 사용자, 디바이스, 애플리케이션 및 인프라에서 클라우드 규모로 데이터 수집 ▪ Microsoft의 분석 및 업계 최고의 위협 인텔리전스를 사용하여 이전에 미검사된 위협을 탐지 ▪ Microsoft의 수년 간의 사이버 보안 성과물을 활용하여 인공 지능을 통해 위협을 조사하고 대규모로 의심스러운 활동 헌팅 ▪ 일반 작업의 기본 제공 오케스트레이션 및 자동화로 빠르게 인시던트 대응	▪ SIEM + SOAR제품 ▪ 엔터프라이즈 전반에 지능적인 보안 분석 및 위협 인텔리전스를 제공 ▪ 경고 검색, 위협 가시성, 주도적 헌팅 및 위협 대응을 위한 솔루션

개발사	제품명	주요기능	솔루션 특징
안랩	Sefinity AIR	▪ 오케스트레이션 – 하나의 대응 프로세스에 속해 있는 각 태스크의 조율 – 다양한 솔루션 연동, 양방향 통합, 손쉬운 사용성 ▪ 자동화 – 빌트인 Playbook 제공 및 Playbook 제작 지원 – 스크립트 엔진을 이용한 액션의 자동화 – 조직 내 업무프로세스 자동화 – 표준 대응 절차 제공 ▪ 사고 대응 및 협업 – 대응 내역 및 의사결정에 대한 관리 및 근무자 간의 협업 지원 – 위협 대응, 보안 운영, 업무 요청 및 지원 등 유형별 케이스 생성 및 관리 ▪ 대시보드 및 레포팅 – 대응 활동에 대한 보고 지표, 의사결정 지원 – 공용 대시보드 : 조회 기간 내 선택된 위젯의 정보 – 개인 대시보드 : 계정별 조회 조건 내 수행 내역 정보	▪ 안랩의 보안 운영 및 위협 대응 노하우 ▪ 다양한 솔루션과 효율적 연동 ▪ 머신러닝 기반 분석모듈 ASA
FireEye	Helix	▪ 위협 인텔리전스 – 위협에 대한 최신 인텔리전스 탐지 및 강화 ▪ 보안 오케스트레이션 – 보안 전문가가 사전에 설계한 Playbook을 기반으로 대응 자동화 ▪ 워크플로우 관리 – 자동화된 워크플로우 및 수동 워크플로우를 통해 조사 프로세스 전체의 단계를 체계화, 할당, 협력 및 실행 ▪ 차세대 SIEM – 고급 사용자 동작 분석 기능을 사용하여 위협 및 취약점 탐지 개선 ▪ 조사 워크벤치 – 유연한 보안작업의 전환과 신속한 탐지를 지원하기 위해 인프라 전체에 있는 모든 소스의 경보 및 이벤트 데이터에 걸쳐 인덱싱 , 보관 및 검색을 수행 ▪ 컴플라이언스 보고 – 대시보드 및 위젯을 사용자 지정하고 사용하여 가장 중요한 정보를 시각적으로 취합하고 표시하고 탐색	▪ 여러 툴의 데이터 연관성을 분석하여 보안 사고 탐지 ▪ 상황별 위협 인텔리전스를 이용하여 정보에 근거한 효율적인 결정을 내림 ▪ 보안 데이터 및 인프라 중앙 집중화

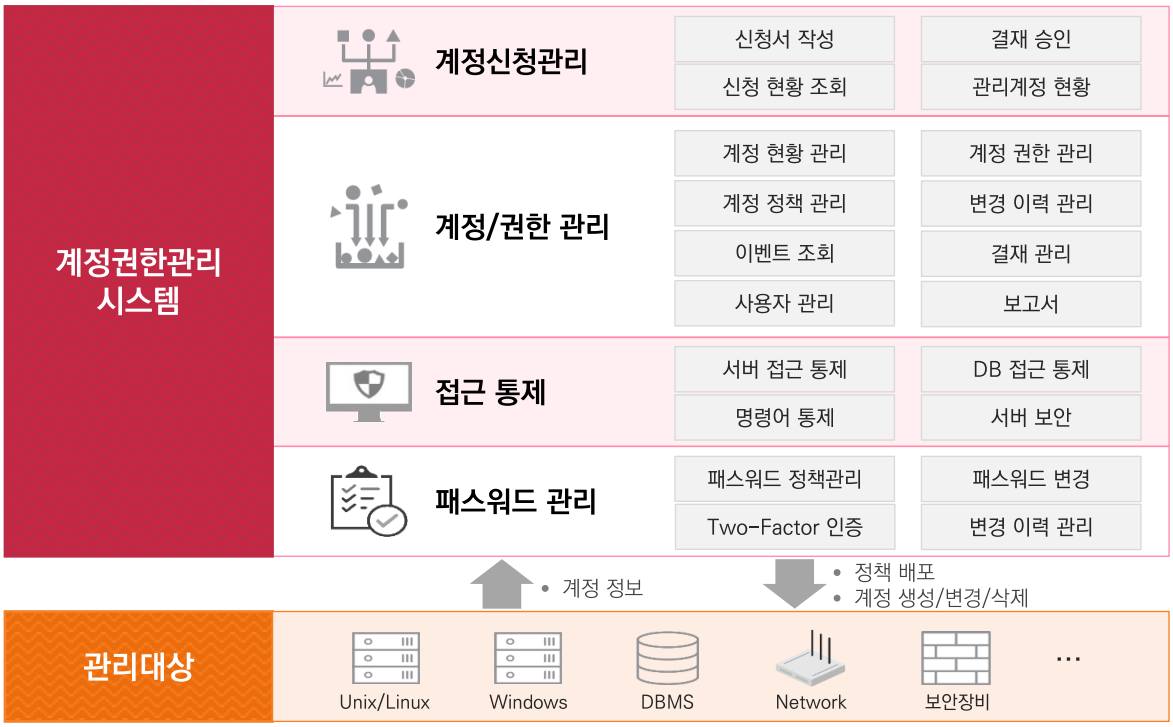
[표 II -1. SOAR 솔루션별 특징]

Part 3

계정권한관리 시스템

1) 시스템 개요

가. 시스템 개요



[그림 Ⅱ-16. 계정권한관리 시스템 개요]

IT인프라에 대한 대다수의 보안 사고는 내부 사용자들의 계정과 권한 관리 소홀로 인한 계정 탈취, 시스템 손상 및 정보 유출 사고가 발생하고 있습니다.

이러한 보안사고를 미연에 방지하기 위해서는 전체 시스템 계정과 권한에 대한 일관적인 Life-Cycle관리가 필요합니다. 분산되어 있는 다수의 계정을 수기관리 및 영역별 관리는 한계가 있으며, 주기적 패스워드 변경 작업과 같은 반복적인 업무는 관리자에게 과다한 업무 부담이 될 수 있습니다.

따라서, 효율적인 계정 및 권한 관리 프로세스 자동화 구성 및 체계적인 계정, 권한 정책수립이 필요합니다.

전체 IT인프라의 계정을 통합하여 계정의 Life-Cycle을 자동화하여 관리할 수 있는 시스템을 계정권한관리 시스템이라고 합니다.

나. 시스템 구축 필요성 및 추진방향

IT인프라의 계정 보안사고의 대부분은 계정과 권한의 관리소홀로 인해 내부자와 외주인력에 의해 발생됩니다.

계정의 생성부터 회수까지 관리될 수 있도록 하고, 불법적인 계정사용과 퇴직자 및 휴면계정을 별도로 관리할 수 있도록 하여, 계정관리의 효율성과 자동화를 추진해야 합니다.

개선사항 및 필요성

이기종 장비에 대한 계정 통합 관리 필요

- 다수의 이기종 장비의 계정현황 확인 및 통합 관리 어려움
- 시스템별로 계정 및 사용자 정보 별도 운영에 따라 계정의 정합성 불일치

계정 관리 수작업 및 계정의 불법접근

- 계정 생성/변경/회수/삭제 작업을 수작업으로 진행하여 업무 부담 증가 및 관리 부실 위험
- 불법계정 및 우회접근에 대한 대비책 미비
- 계정에 따른 접근 권한 관리 미흡

퇴직자나 휴면 계정 관리 필요

- 퇴직자계정과 휴면계정 관리 부재로 해당 계정의 도용이 발생하여 자료 유출 및 보안 사고 위험이 증가
- 퇴직예정자의 계정 회수 및 삭제 정책정의 및 자동반영 필요
- 휴면계정의 사용자 본인 재인증 절차 확인 후 계정 사용 필요

패스워드 복잡도 및 변경 주기 미 준수

- 일괄된 패스워드 정책 관리의 어려움으로 인해 패스워드 노출 위험 증가
- 주기적 정책적 패스워드 관리 필요
- 패스워드 일방향 관리로 패스워드 유출 보안강화 필요

추진 방향

계정 통합 관리

- 분산된 계정의 주기적 자동 수집 및 동기화로 모든 계정에 대한 통합 관리
- 인사정보 연동에 다른 사용자 기준의 계정 관리 정합성 및 모니터링 체계 구축
- 계정 접근 권한 관리를 통해 사용자 접근 통제
- 부서별 역할별 RBAC 기반 접근통제 권한 부여 관리
- Two-Factor 인증을 통한 계정접근 통제 강화

계정 Life-Cycle 관리

- 계정의 생성부터 회수까지 자동으로 관리하여 업무 효율성 향상 및 감사 대응 가능

불법 계정 관리

- 인사 이동, 퇴직, 외주 인력에 대한 잔존 계정 삭제로 계정 도용 방지
- 퇴직자 계정 및 휴면계정 정책 및 프로세스 정의
- SecureOS 관리에 따른 우회접근 차단

패스워드 관리

- 이기종 장비들에 대한 패스워드 통합 정책 구성으로 일괄된 보안 정책 유지 및 패스워드 유출 방지
- 패스워드 관리 자동화 및 일방향 패스워드 관리

다. 주요 구축 내용

계정관리 시스템은 이기종 장비에 산재되어 있는 계정을 통합 수집하여, 정책에 따라 생성부터 삭제까지의 계정 Life-Cycle과 패스워드를 자동 관리 할 수 있는 시스템입니다.

일원화 및 자동화된 계정관리 기능을 통해 시스템의 보안을 강화함과 동시에 불필요한 시간적, 비용적 소모를 줄여, 보다 효율적인 업무환경을 제공 할 수 있습니다.

네트워크와 서버 등 인프라 운영 시스템 사용자의 접근통제는 사용자 접근 및 감사기능으로 시스템 보안을 강화 할 수 있습니다.

구축영역	구축방향	주요내용
계정 관리	계정 관리 자동화	**계정 Life-Cycle 정책관리** 1 시스템 및 장비 별 계정 자동 수집 및 동기화 2 계정 통합 수집 후 시스템 대상으로 프로비져닝 처리 3 계정 사용 신청 및 결재, 이력관리 4 계정 정책 설정 및 자동화 처리 5 불법계정 및 퇴사자 계정, 휴면계정의 자동 잠금, 삭제, 회수, 알림 처리
접근 통제	권한분류 및 접속 권한 관리	**계정 접근권한 관리** 6 사용자 접근 일원화 및 접근권한 통제 7 접속인증 강화 (Two-Factor 인증) 8 금지 명령어 통제 및 위험 명령어 세션 차단
패스워드 관리	패스워드 정책 적용	**패스워드 관리 자동화** 9 패스워드 복잡도, 변경주기의 정책 관리 10 패스워드 관리 자동화 프로세스 수립 11 시스템 패스워드 보안정책 검증
모니터링 및 보고관리	이벤트 모니터링, 주기별 보고 및 증적관리	**모니터링 및 이력관리** 12 실시간 세션 모니터링 및 이벤트 발생 모니터링 13 계정 사용 이력 관리 및 모니터링 14 정책 위반 이력 관리

라. 기대효과

기대 효과

STEP 1

보안규제 강화

- 보안 강화 및 규범 준수를 위한 사용자 계정, 권한 정책 및 감사 추적의 통합관리
- 허가 받은 사용자의 부여된 권한 영역만 시스템 접근 가능
- 계정 패스워드 관리를 시스템화하여 외부 유출 최소화
- 보안사고 발생 시 강력한 증거자료를 제시할 수 있는 보안 감사 및 상세한 통계 제공

STEP 2

시스템 관리 효율 향상

- 전체 운영 시스템 계정 통합 및 권한 관리 일원화
- 패스워드 관리 절차 간소화로 업무 효율성 증대
- 전체 대상 시스템에 대한 계정/권한의 현황 및 사용 이력 점검/모니터링 관리

STEP 3

프로세스 및 체계 정립

- 통합계정관리 프로세스 및 계정관리 Life-Cycle 규정 정립
- 계정/권한 신청, 패스워드 변경, 모니터링 등 자동화에 따른 지연 최소화
- 감사 및 통제 강화를 통한 기업 신뢰도 및 경쟁력 향상

STEP 4

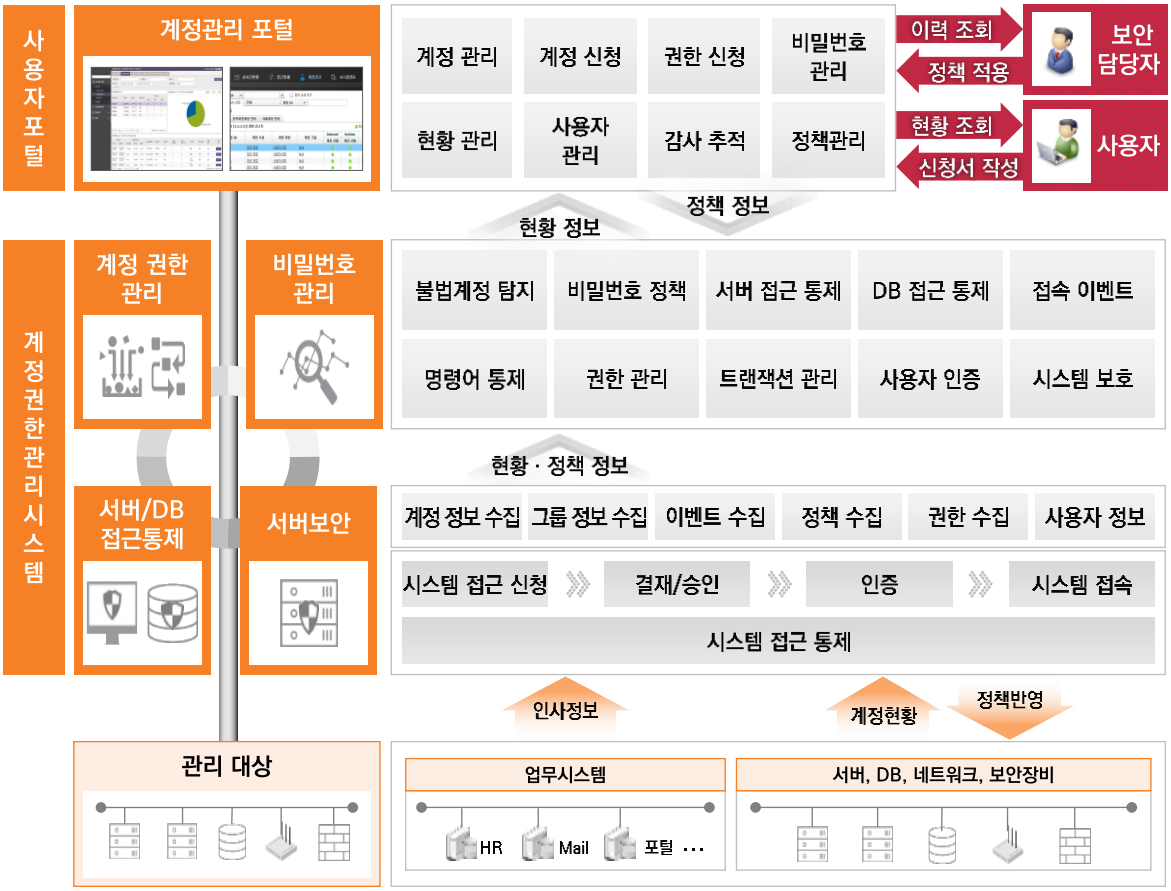
Compliance 대응 향상

- 상위 관리감독기관의 정보기술 부문 보호업무 준수
- 기업내부 보안감사 및 준법감시 요건 만족
- 증빙정보 및 보고서 제공을 통한 정보보안 투명성 확보

인가된 계정과 접근권한 통제를 위한 계정권한관리 시스템 구축

2) 시스템 구축

가. 시스템 개념도



[그림 Ⅱ-17. 계정권한관리 시스템 개념도]

계정권한관리 시스템은 계정관리, 접근통제, 비밀번호관리 시스템을 통합하여 이기종 관리대상 시스템의 계정을 통합수집 관리하고, 허용된 사용자만이 해당 시스템에 접근할 수 있도록 통제합니다.

대상장비는 서버계정, DB계정, 네트워크 계정 및 보안장비로 구분되며, 수집된 계정은 계정분류 작업을 통해 정규화 작업을 시작합니다.

초기 계정분류 컨설팅 작업은 SK인포섹의 계정관리 방법론(Auth-Method)에 의해 크게 특권계정, 공용계정, 개인계정으로 분류되며, 계정정립이 완료된 이후부터는 일관성 있게 계정권한관리 시스템을 통해서만 계정 신청과 권한신청을 할 수 있게 됩니다.

각 시스템은 상호 연동을 통하여 사용자 및 관리자에게 시스템 계정에 대한 사용과 관리 업무의 편의성을 제공하며, 해당 절차에 대한 일원화와 자동화를 통해 보안을 강화할 수 있습니다.

나. 사전준비 필요사항

시스템 구축 이전에 계정을 관리할 대상장비를 선정하고, 연동정보를 정의해야 합니다. 어떤 장비에서 계정을 수집 관리 할 것인지, 해당 장비와 연동할 때 연동방식 (DB, File 등)의 정의가 필요합니다.

시스템 구축이 시작되면 대상장비로부터 수집된 계정은 업무 운영담당자와 보안 담당자와의 협의를 통해 분류작업을 거쳐야 합니다. 불필요한 계정과 퇴사자 계정, 중복계정을 분리하고 정상적인 계정은 특권계정, 공용계정, 개인계정으로 분류 하여 계정 데이터를 Cleansing작업 합니다.

계정 분류 작업은 운영 담당자의 직접 참여가 필요하여 Communication 협업이 중요합니다, 각 시스템의 운영담당자는 계정정리와 권한 분류에 대한 역할과 책임을 가지고 있습니다.

[그림 Ⅱ-18. 계정권한관리 시스템 구축 사전준비]

계정 관리 대상 확인

- 계정 관리 필요 대상 시스템 파악 및 서버, DB, 네트워크, 보안장비 종별 분류
- 계정 유형 분류(특권계정, 공용계정, 개인계정 등)
- 개인계정 사용자 분류(임직원, 외주직원 등)

계정사용 업무 프로세스 및 요건 정리

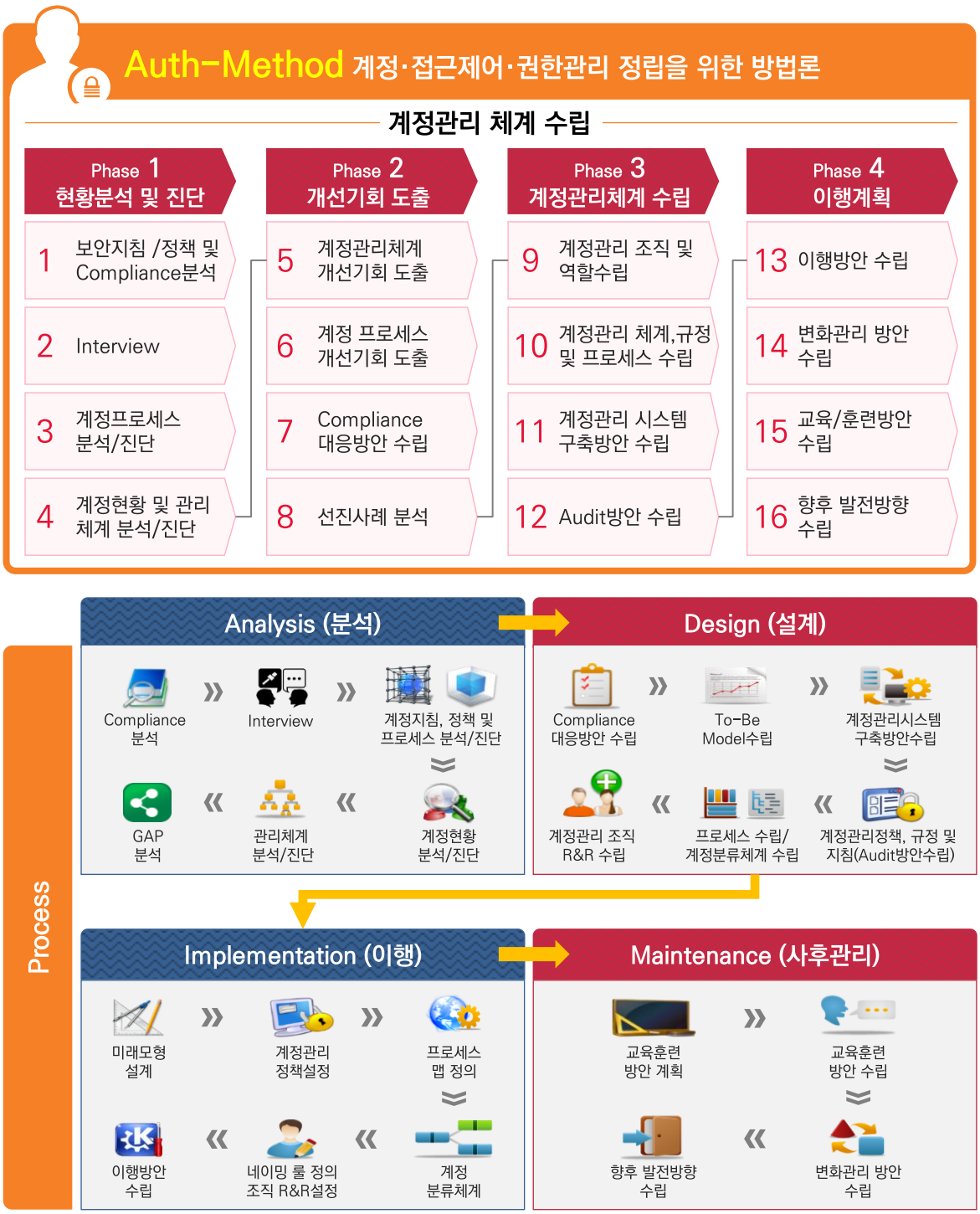
- 업무 담당자들을 통해 현재의 계정 사용 업무 프로세스 파악
- 내부규정 확인을 통해 정책 수립 요건 파악
- 통합 계정권한관리의 새로운 정책 및 프로세스 정의

계정 관리 정책 수립

- 내부 규정 및 지침 취합 확인 후 계정정책 수립
- SK인포섹 계정관리 방법론(Auth-Method)컨설팅 정책 및 프로세스 지원

다. 계정관리 방법론(Auth-Method)

Auth-Method는 SK인포섹의 Know-How를 적용한 계정관리 전용 방법론으로써 성공적인 통합 계정권한관리시스템 구축을 위한 Process 를 수립·적용·관리 개선을 위한 구축모델 입니다.

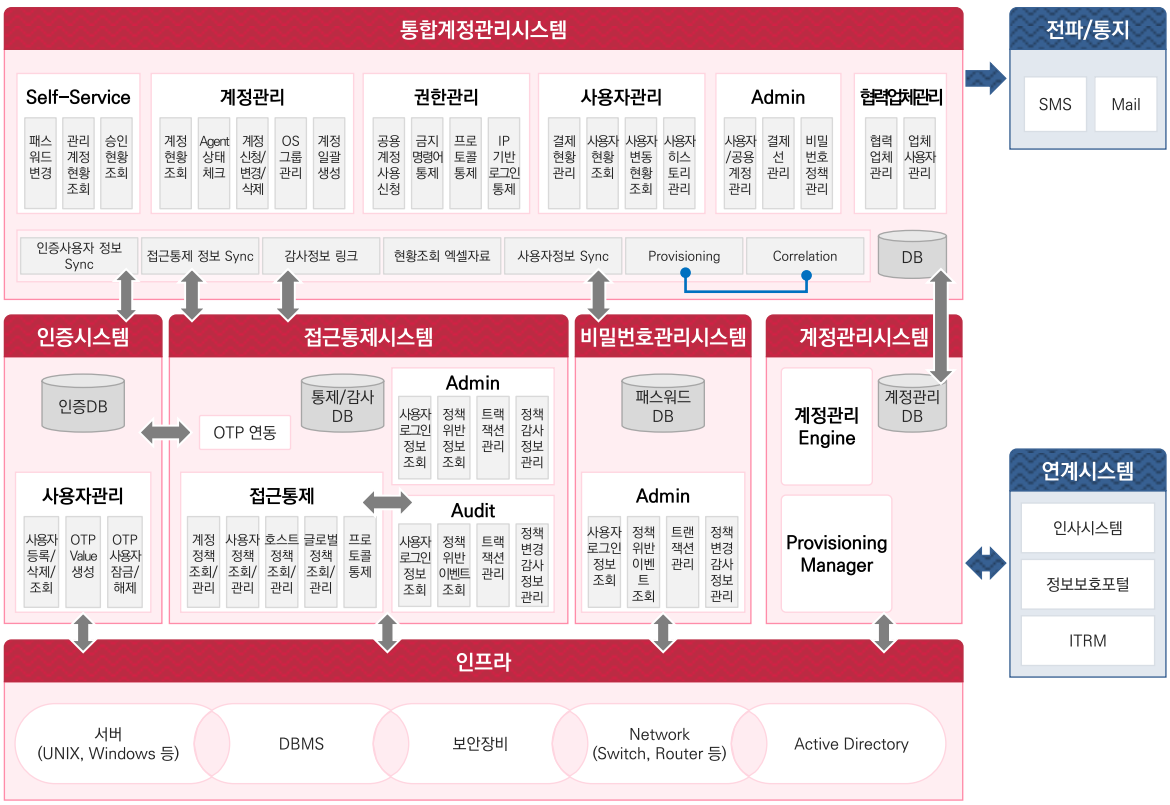


[그림 Ⅱ-19. 계정관리 방법론]

라. 구축 유형

SK인포섹은 다수의 금융사를 대상으로 통합 계정권한관리 시스템을 구축하였습니다. 일부 금융사 구축사례를 아키텍처와 시스템 구성도로 구분하여 다음과 같이 소개 드립니다.

✓ 유형 1 통합계정관리 시스템 아키텍처



[그림 Ⅱ-20. 통합 계정권한관리시스템 구축 유형]

다양한 인프라 지원

- 다양한 인프라(서버, DBMS, 보안장비, Network 등) 및 내부시스템과의 연계를 통하여 통합 계정 관리를 수행함
- 대상장비별 솔루션별 계정정보 Interface정의에 따른 연동정의

사용자 접근 일원화

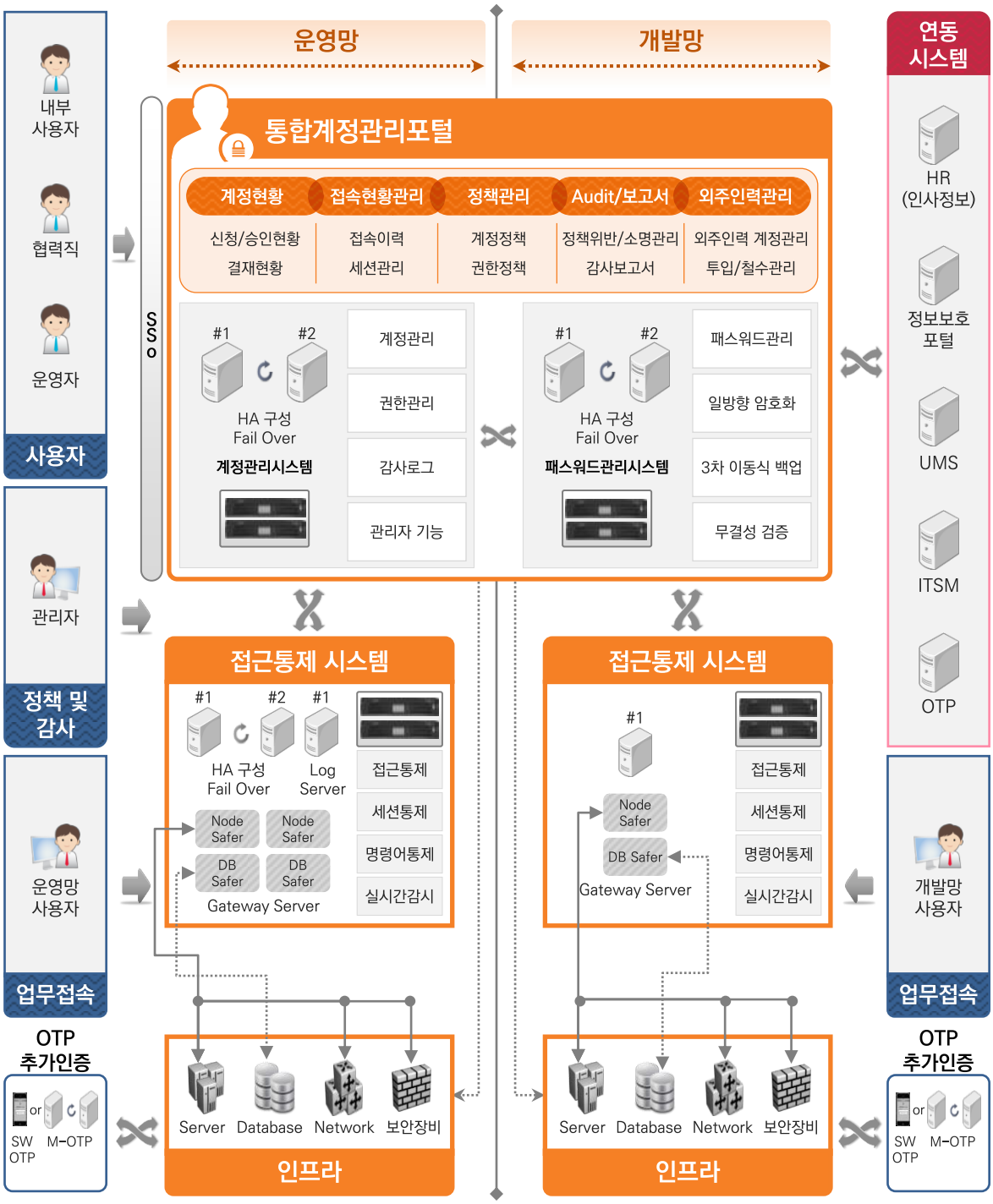
- 다양한 시스템을 통합계정관리시스템으로 통합 관리하여 사용자의 접근 경로를 일원화하여 업무 효율성 증대
- 불법접근 및 우회접근 차단으로 비정상 접근행위 통제 강화

자동화 관리

- 계정 및 비밀번호 자동화 관리로 관리자의 업무 효율성 향상 및 보안성 강화
- 비밀번호 생성정책 및 변경정책에 따른 자동화 관리

✓ 유형 2 통합 계정권한관리 시스템 구축 사례

고객사에서 구축한 시스템은 운영망과 개발망을 구분하여 각각 인프라 계정에 대해 계정수집, 접근통제를 각각 구축하였습니다.



[그림 II -21. 통합 계정권한관리시스템 구성도 유형]

3) 통합 권한관리 및 모니터링 시스템

가. 시스템 개요

일반적인 계정관리와 권한관리는 시스템 관점에서의 관리 시스템 구축 영역입니다. 사용자 기준의 실질적인 업무관점 접근 로그를 기반으로 한 『통합 권한관리 및 모니터링 시스템』은 어떤 직원이 접근했던 모든 시스템. 예를 들어, SSO통합 로그인, 업무포털 로그인 후 특정업무 조회 및 등록, 회계시스템 로그인 후 회계 업무처리, 암호화 보안장비 서버 로그인 등 개인이 접근하고 사용했던 모든 시스템 로그를 취합하여 Time Table별로 사용자의 이력을 모니터링 하여 이상징후를 감지하는 시스템을 말합니다.

현재 기업과 금융회사에서는 계정관리와 접근통제 시스템을 구축 운영 중에 있으나, 사용자 기준의 통합 권한관리 및 모니터링은 필요성은 인지하고 있으나, 구축 운영중인 사례는 거의 없다고 판단됩니다. 현황 및 문제점을 공유하고 시스템 구축방향성 과 효과성에 대해서 소개 드립니다.

계정관리 및 권한 현황

1 C-Level 관리자
- 내부 권한 관련 보안정책 수립 및 감사 대응 필요 시 보안 담당자에게 감사 자료 요청
- 평상시 내부 사용자 권한관리 내역 필요 시 보안 담당 제공 자료를 통해 확인

2 보안 담당자
- 신규 사용자에 대한 권한 부여 시 개별 시스템 접속을 통한 접근 권한 부여
- 사용자 업무 변경 시 개별 접속을 통한 권한 변경
- 서비스와 시스템 개별 확인을 통해 감사 대응을 위한 자료 수집
- 평상시 모니터링 업무 수행을 위하여 서비스 별로 콘솔 접속 또는 자료 수집
- 어플리케이션 접근권한에 대한 모니터링 어려움

문제점 및 이슈

1 권한관리에 따른 전사 관리 체계 부재
- 권한 부여 및 변경 작업에 많은 시간 소모 (신규 입사자 발생 이나 조직 개편으로 인한 권한 변경 시)
- 단위 솔루션 별 설정으로 권한설정 시 누락이나 실수발생
- 사용자 단위 권한 부여 현황 확인 어려움 (권한 관련 대시보드)
- 전 임직원에 대한 통제 연계 관리가 현실적으로 불가능

2 감사/통제 업무의 부하 발생
- 전체 권한에 대한 감사 및 통제를 위하여 각 단위 시스템 별 보고서를 출력하여 재가공 하는 작업이 필요
- 정책 수립 및 확인을 위한 사전 준비에 많은 시간이 소모되어 업무효율 저하

- C-Level 관리자의 모니터링 체계 부재
- 단위 솔루션 별 감시 대응을 위한 자료 수집
- 솔루션 개별 콘솔을 통한 모니터링

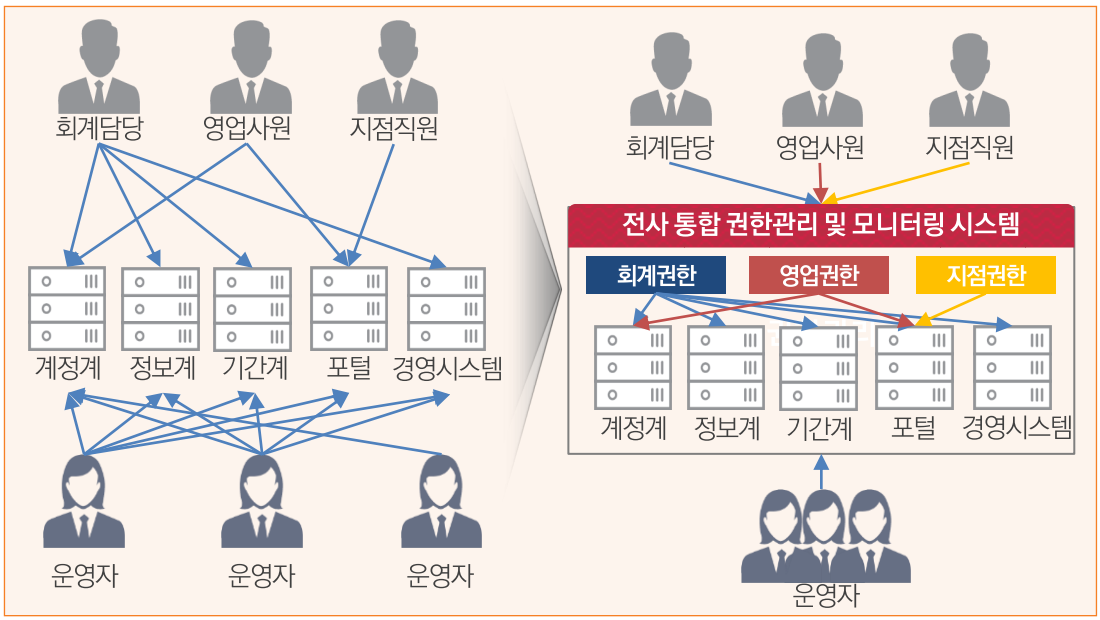
- 권한에 대한 통합관리 불가
- 접근 이력의 통합 모니터링 관리 부재
- 감사 등 관리업무 부하 증가

[그림 II -22. 계정관리 현황 및 문제점]

나. 개선방안 도출

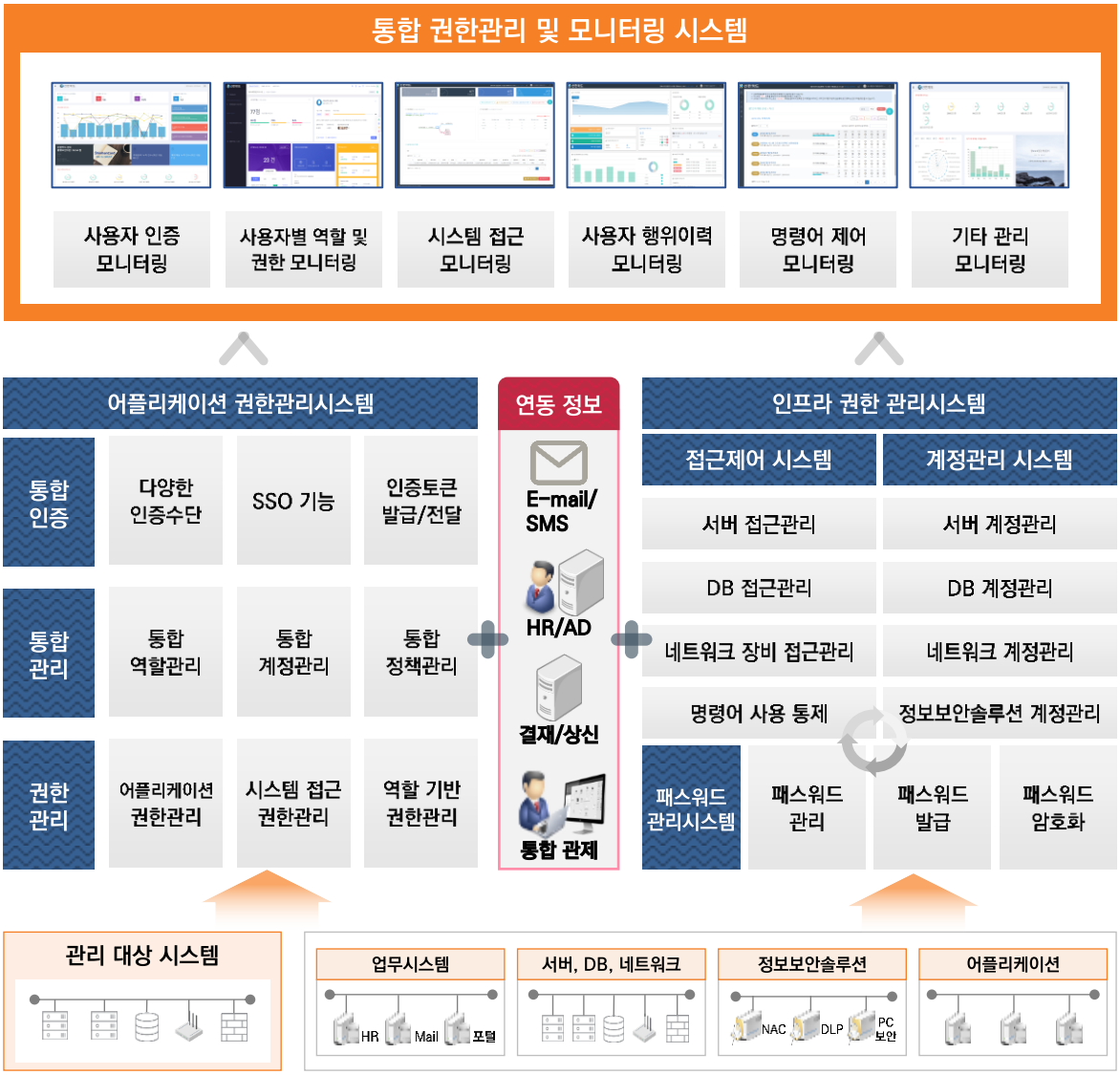
전사적 권한관리 이슈사항		시사점 및 개선방안
기술적 관점	✓ 각기 다른 사용자 인증방식의 통합 필요 ✓ 내부 사용자 뿐만 아니라 개발자, 용역직원 등 외부 사용자에 대한 통제장치 확보 ✓ 다양한 정보시스템에 대한 계정관리 통합 필요 ✓ 사용자 계정의 부여/회수 등을 지원하는 라이프사이클 적용 필요 ✓ 직무&역할별 권한관리를 통한 전사적 보안강화 ✓ 업무화면 별 조회, 저장, 출력, 다운로드 등 속성기능 권한관리 필요 ✓ 보안사고에 대한 감사 모니터링 기능 확보	사용자 통합인증체계 구축/개선 ✓ SSO 기능 개선 및 이용대상 확대 (협력직원) ✓ 인증수단 확대 및 강화 ✓ 접근이력 수집 영역 확대
관리적 관점	✓ 업무 권한을 관리하여 과부여 최소화 ✓ 계정발급/권한부여 이력정보의 통합관리 ✓ 어플리케이션에 대한 계정/권한관리 확대 ✓ 전산자료 위/변조 가능성 있는 내부사용자 관리 ✓ 전자금융거래법 및 개인정보보호법 충족 ✓ 금융감독원 전자금융감독규정, 시행세칙 등 외부규제 준수	어플리케이션 권한관리 시스템 구축 ✓ 어플리케이션 계정 및 권한관리 시스템 구축 전사 통합 권한관리포털 구축 ✓ 직무&역할 정의, 사용자 포탈 통합 ✓ 단위시스템 로그 통합

[그림 Ⅱ-23. 계정/권한관리 이슈 및 개선방안]



[그림 Ⅱ-24. 통합 권한관리 및 모니터링 시스템 구성방안]

다. 시스템 구성도



[그림 Ⅱ-25. 통합 권한관리 및 모니터링 시스템 구성도]

라. 구축 핵심 요소

구분	핵심 요소
적용대상 측면	**쉽고 빠른 적용이 가능한 API 모듈 제공과 단계별 적용 지원** • 어플리케이션 서비스 담당자와 구축 담당자 간 의견 충돌 또는 다양한 문제로 인한 이슈 발생 – 계정관리 대상 제외 요청 또는 추후 진행 요청 – 기존 사용하던 서비스의 설정 변경/추가 등 구축을 위한 필요 내역 요청 시 불허 (시스템 상 서비스 영향 우려, Workflow 증가 거부감)
사업진행 측면	**6개월 이상의 분석/설계 및 능동적 대응이 가능한 플랫폼 기반 구축** • 기본 기능을 넘어선 과도한 요구사항 및 커스터마이징 요청으로 인한 이슈 발생 – 과도한 요구사항 및 커스터마이징으로 인한 기본 일정 준수 어려움 – 시스템의 기능이나 기본 틀을 무시한 무조건적인 수정 요구 – 일반적인 수정이 아닌 경우 기존 완료된 내역의 범위를 침범하여 비용 측면에서 추가 이슈 발생
사용자 측면	**사용자 혼선을 최소화하기 위한 친숙한 UI/UX 제공 및 절차 간소화** • 시스템 도입에 따른 업무변경 내용 적용 등으로 인한 이슈 발생 – 기존 사용 방법의 변경으로 인한 적응기간 중 간편화 요구, 우회 방안 등 제공 요청 – 정책 적용 시 일부 서비스 또는 지정 서비스 예외처리 요청 – 기능 구현내용에 대한 서로 간 이해 불일치

마. 기대효과

기대 효과

STEP 1

역할기반 권한체계 수립

- 수많은 시스템, DB를 이용한 데이터 추적 및 분석 비용 감소
- 일괄된 역할 및 권한관리를 통한 관리의 편의성 제공
- 잘못된 역할 및 권한부여를 즉시 조정하여 보안사고 예방

STEP 2

권한 라이프사이클 관리

- HR 등록과 동시에 권한에 맞는 사용자 계정 시스템별 일괄 부여
- 사용자 업무 변경, 인사 이동 발생 시 적절한 권한 부여/회수 자동화

STEP 3

Compliance 대응 향상

- IT 보안 Compliance 대응
- 엄격한 사용자 정보 및 데이터 접근관리 규제 대응 가능
- 데이터 입력, 처리, 출력, 개인정보 관리, 데이터 백업 등 금융권 Compliance 준수 요건 대응

STEP 4

직무분장 구현

- 적절하지 못한 직무분장 방지
- 사용자 권한의 오/남용 방지
- 내부자 부정행위 예방 가능

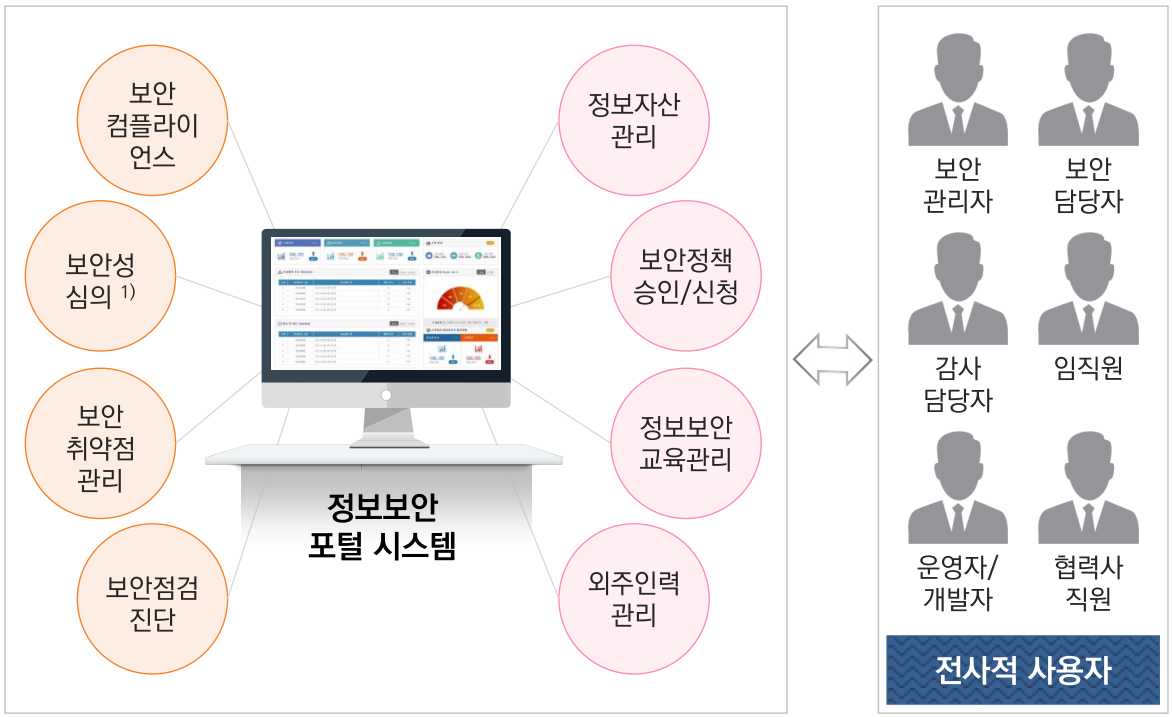
사용자 기준 전사 시스템 접근 이력 모니터링을 위한 통합 권한관리 및 모니터링 시스템 구축

Part 4

정보보안 포털 시스템

1) 시스템 개요

가. 시스템 개요



[그림 Ⅱ-26. 정보보안 포털 시스템 개요]

조직의 정보자산의 안정성과 정보보호 운영을 체계적이고 지속적으로 유지하기 위하여, 관련업무를 통합하고, 전사적으로 운영될 수 있는 시스템을 정보보안 포털 시스템으로 구축할 수 있습니다.

정보보안 포털 시스템은 조직내의 임직원에게 보안과 관련된 업무나 정보를 제공하거나 운영할 수 있도록 합니다. 보안 담당자는 모든 보안업무의 주체와 관리가 될 수 있도록 하며, 관리 포인트를 집중화 하여 업무 효율성과 생산성을 높일 수 있습니다.

또한, 개별 운영되는 보안시스템과 솔루션 등을 한 화면을 통해 관리하고 감시함으로써 보안위협에 대해 빠르게 대응하고, 지속적인 교육 및 관리를 통해 직원들의 보안사고 예방 및 보안의식을 향상시킵니다.

1) 보안성심의 : 보안SI를 통한 IT정보보호 구축 가이드 Ver3.0 추가. “통합 유지보수 관리” 삭제

나. 시스템 구축 필요성 및 추진방향

각 조직에서는 전사적인 보안관리 업무를 해당 부서별로 산재하여 관리하거나, 수작업으로 업무를 운영하는 경우가 많으며, 보안포털의 기능도 고객사별로 필요에 따라 많이 다르게 운영되고 있습니다.

최근에는 보안솔루션 구축 이후 보안업무 통합관리의 경향으로 수요가 바뀌면서, 통합 포털 구축의 요건이 늘어나고 있습니다. 산재되어 있는 보안업무와 수작업 업무를 통합하여 정보보안 포털 업무를 프로세스화 하여 전사적으로 운영할 수 있도록 하는 시스템 구축이 필요합니다.

개선사항 및 필요성

다양한 보안업무의 통합 필요성

- 산재되어 있는 보안업무의 통합으로 업무의 효율성 향상 필요
- 경영층 및 보안관리자의 보안인식 결여 및 인식 부족
- 전사적 보안업무의 통합관리 필요

일원화된 프로세스 통합

- 다양한 보안관련 업무의 각기 다른 결재와 프로세스로 인한 업무 부하 가중
- 다수의 시스템 운영 상황을 일원화하여 모니터링 할 수 있는 통합 관리 필요
- 내부/외부의 체계적인 인력관리 및 장비 상황 파악이 필요

컴플라이언스 대응 및 보안사고 예방

- 내부규정, 감사, 컴플라이언스 대응에 많은 시간이 소요
- 중요정보 유출 사고 예방을 위한 보안 활동 강화 필요

추진 방향

보안관리 프로세스 통합

- 정책 변경요청, 결재 및 승인, 배포 등 관리 프로세스 일원화
- 정보 유출 및 반출 시도에 대한 즉각적인 대응 및 상시 모니터링
- 보안교육관리 및 주기적인 취약점 점검활동을 통한 전사적 보안의식 개선
- 보안성심의 업무 프로세스 정립 및 시스템 화

내부 보안시스템 통합 및 집중화

- 보안 업무의 중앙 집중화 및 일원화
- 전사적인 임직원의 보안업무 관리를 위한 담당자와 관리자의 업무협업체계 구축
- 사용자, 운영자의 역할별 최적화된 통합 대시보드 구축

컴플라이언스 대응체계 확보

- 상위 관리감독기관 대응 및 증적관리
- 내부 감사에 대한 정보보안 규정 및 지침 정책 반영
- 주기적 보고체계 및 감사대응 능력 향상

다. 주요 구축 내용

보안 컴플라이언스
- 보안 통제 항목 기준 및 형상관리
- 보안 컴플라이언스 항목관리 및 현행화
- 보안 통제 항목에 따른 양식관리, 증적 자료 관리

보안성심의
- 보안성심의 규정화에 따른 절차 및 정책 정의
- 신규 장비도입 및 SW구축 이전 사전 보안성심의 프로세스 정립
- 운영 이전 보안성심의(취약점점검 및 인프라 보안점검)활동

보안 취약점 관리
- 취약점 대상, 실행 주기, 유형별 담당자 관리
- 인프라 점검, 소스코드점검, 모의해킹 영역별 취약점 점검 활동
- 취약점 조치 계획 및 처리결과 관리, 결과보고, 이력관리

보안점검
- 보안점검 활동 항목 정의 및 평가
- 주기적 개인별, 부서별 보안점검 활동 및 통제
- 개인별, 부서별 보안수준(모니터링) 결과 지수화

정보보호 자산관리
- 자산정보 등록, 변경, 폐기의 요청/승인 관리
- 정보자산 중요도 평가
- 정보자산 현황/통계/출력 등

보안정책 승인/신청
- 보안정책 및 프로세스 일원화
- 개별 시스템의 솔루션 보안정책 신청, 변경, 삭제, 이력관리
- 개인별, 부서별 보안정책의 신청, 승인 증적 자료

정보보안 교육관리
- 정보보안 교육 계획 및 결과 보고
- 교육현황, 통계, 리포팅
- 교육 후 평가 및 설문조사

외주인력 관리
- 외주인력 관리(출/퇴근, 투입, 연장, 철수)
- 주요 시설 출입이력 관리, 이동 매체 반출입 관리
- 외주인력 전산장비 현황관리

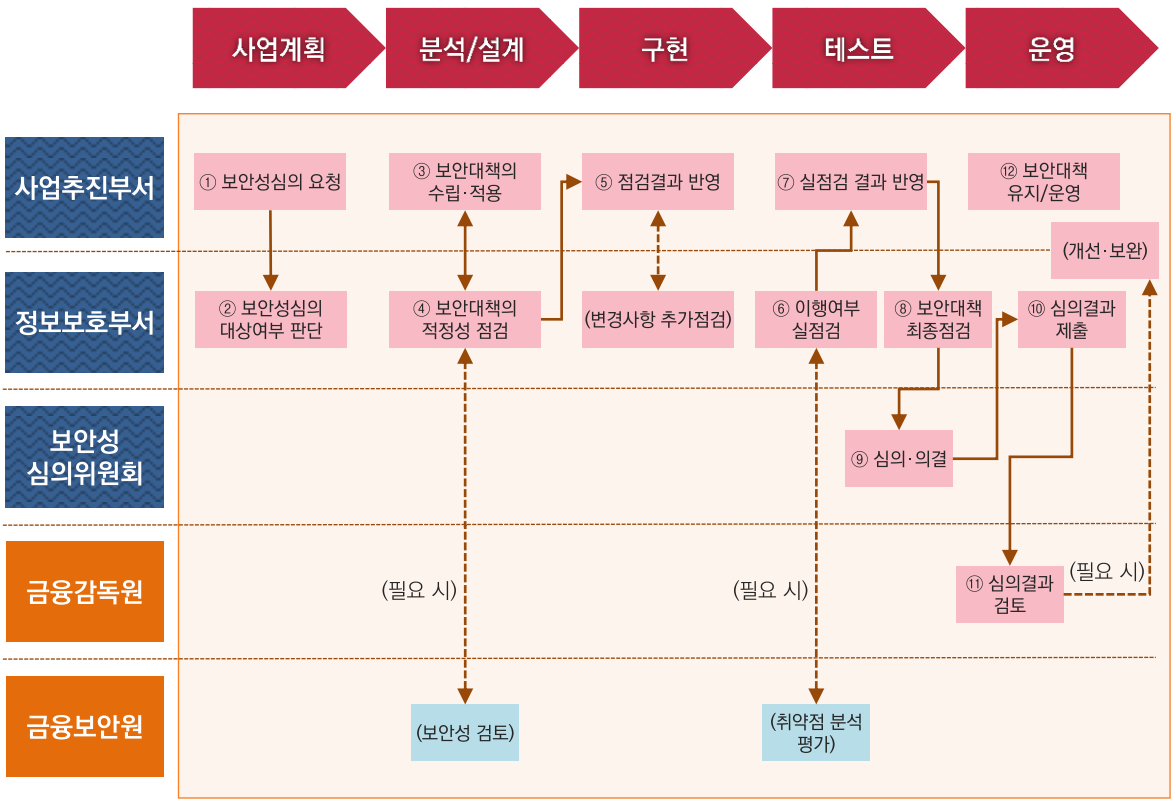
라. 보안성심의 정의

정보보안 포털에서 주요기능으로 보안성점검 항목이 구성될 수 있습니다. 2016년 금융보안원에서는 금융회사에서 자체 보안성심의에 대한 가이드를 발간 공지하였습니다. 금융회사 외에 일반 기업이나 관련 업계에서도 본 기준의 절차나 내용을 따르는 것을 권장합니다.

우선 간략히 설명을 하면, 임의의 업체에서 H/W 장비도입이나 S/W 구축이 필요할 때 사업계획 단계에서 "사전 보안성 검토"를 진행하도록 합니다. "사전 보안성 검토"가 승인 완료되면 사업이나 프로젝트가 수행되고, 그 이후 분석과 설계단계에서는 "보안성 검토"단계를 거칩니다. "보안성 검토"는 금융회사에서 신기술이나 새로운 유형의 시스템 구축 시 『금융보안원』에 검토요청과 승인단계를 거치는 과정이며, 일반기업에서는 자체 『보안성 심의 위원회』에서 수행 할 수 있습니다. 구축 완료 시점에 운영전환이 되기 이전에는 최종 "보안성심의"를 받도록 합니다. "보안성심의"는 인프라 점검, 웹취약점 점검, 모의해킹 등을 수행합니다. "보안성심의"가 완료되고 승인되면 운영으로 전환할 수 있으며, 지속적으로 유지관리 업무를 수행하도록 합니다.

보안성심의 단계의 조직구분은 사업추진부서, 정보보호부서, 보안성심의 위원회로 구성될 수 있습니다. 아래 프로세스의 금융감독원과 금융보안원 절차는 금융기관에 한해서 적용됩니다.

보안성심의의 단계는 "사전 보안성 검토", "보안성 검토", "보안성심의"의 3단계로 절차를 구성하는 것을 권장하며, 개별업체의 정책과 규정에 적합하도록 프로세스화 합니다.



[그림 II -27. 금융보안원 자체 보안성심의 절차 (예시)]

마. 기대효과

기대 효과

STEP 1 업무의 효율성 및 생산성 향상

- 수작업 전산화, 중복업무 방지, 업무자동화에 따른 업무의 효율성 향상
- 보안시스템/솔루션 통합에 따른 업무의 감소 및 처리속도 향상
- 단순 반복업무에서 창의적인 업무로의 전환

STEP 2 보안강화 및 전사적 보안의식 강화

- 보안활동 강화에 따른 내부 정보 유출 사고 방지
- 보안사고 사전예방으로 정보보호 자산 비용절감
- 보안성 검토 및 운영전환 이전 보안성심의 활동으로 보안강화
- 전사적 임직원의 생활보안 의식 강화

STEP 3 Compliance 규제 및 변경에 능동적 대응

- 개인정보 규제 및 내부 규정변경에 대한 선제적 대응
- 개인정보 유출 및 오·남용 사고를 대비한 증적 확보
- 감독기관의 감사 및 규제에 적극적인 대응 및 조치를 위한 기반 확보

STEP 4 대내외 신뢰도 향상 및 업무 투명성 제고

- 내부사용자의 개인정보 취급에 대한 명확한 처리 가이드 제시
- 지속적인 교육을 통한 내부 직원의 정보보안 인식 개선
- 명확한 업무 분담으로 인한 업무의 투명성 제고

정보보안 업무 통합 일원화
정보보안포털 시스템 구축

2) 시스템 구축

가. 시스템 개념도

[그림 Ⅱ-28. 정보보안 포털 시스템 개념도]

정보보안 포털 시스템은 연계대상 시스템으로부터 정보를 연동하는 연계 시스템과 수집된 정보를 활용하여 업무처리를 하는 업무처리 영역 및 현황 관리 부분으로 나눌 수 있습니다.

데이터는 연동 대상 시스템으로부터 정보를 연계 받아서 처리하는 데이터와, 보안포털에서 자체 등록, 수정하여 운영하는 데이터로 구분됩니다.

전사적으로 보안업무의 활동과 모니터링 내역은 사용자와 운영담당자 및 경영층까지 업무처리를 할 수 있습니다.

정보보안 포털 시스템을 구축할 때 회사와 조직의 보안업무 현황을 명확히 파악하여 주요기능을 선별적으로 정의해야 하는 부분이 중요합니다.

나. 사전준비 필요사항

정보보안 포털 시스템을 도입하기 위해서는 회사와 조직의 보안업무 내부 규정 및 지침을 분석하고, 정보보안 포털에 적용할 부분과 프로세스의 재정의가 필요합니다. 그 이후, 필요한 정보를 통합하기 위해서는 연동대상 시스템과 데이터를 정의하고, 내부 정보보호 업무에 적합하게 커스터마이징 부분을 정의하여 요건화 해야 합니다.

기존 업무와 시스템 현황을 사전에 분석하고 구축하고자 할 To-Be모델을 정립하여, 최종적으로 시스템 구축 사업계획을 수립합니다.

내부규정 및 연동 시스템 도출	적정성 평가 및 검토	구축 방안 검토
내부 규정 지침 분석	외산/국산 S/W 커스터마이징 여부	업무 영역 정의에 따른 연동 시스템 검토
연동 대상 업무 도출	연동 대상 일 트래픽 및 일 로그량 확인	현행업무 분석을 통한 사전 컨설팅
각 업무 정책 및 프로세스 개선 요건 파악	내부 시스템 저장용량 확인	기존 보안솔루션 연동에 필요한 개발비 산정
보안업무 수행 내역 확정	개인별/부서별/조직별 객관성 검토	영역별 부서간 요구사항 정립
연동 대상 시스템 도출 (F/W, IPS/IDS, NGF, DLP 등)	보안부서와 감사부서간 보안업무 R&R 재정립	시스템 구축 중장기 로드맵 수립
내부 연계시스템 (그룹웨어, 인사, 자산관리, SMS 등)		

[그림 Ⅱ-29. 정보보안 포털 시스템 구축 사전준비]

다. 구축 유형

✔ 유형 1 보안 포털 시스템 구축 사례

채널보안 포털 대시보드

관리현황 대시보드	보안 대시보드	시스템 성능 대시보드
사용자 계정 및 접근현황	정책요청 및 승인결재 현황	연동시스템 자원관리 및 성능

채널 보안포털 VIEW

통합관리	통합 모니터링	통합 승인
• 사용자/그룹 • PC계정관리 • 계정정책/암호정책관리 • 등록프로그램 정보	• 예외정책승인현황 • 개인정보전송현황 • 망간자료전송현황 • 백신패치현황 • DA설치 패치현황 • DRM설치 및 패치현황 • S/W사용현황 • 백신 최근 검사현황 • 인터넷 접속현황	• PC계정 신청/승인 • 단말보안 신청/승인 • 자료전송 신청/승인

업체관리	자가진단	보안점검	위반 및 소명	서비스 데스크
• 위수탁 업체관리 • 위수탁 업체 담당자	• 자가진단 항목 관리 • 진단일정 및 결과 관리	• 보안점검 항목 관리 • 점검결과 및 보고	• 위반행위탐지 • 소명 및 보고	• 게시판 공지관리 • 자료실 • 교육현황

채널보안 수집모듈

수집방법	수집유형	연동대상
DB, FILE/FTP, AD	정책정보, 성능 로그, 이벤트 로그	인사정보, 자산정보, 보안솔루션

[그림 II -30. 정보보안 포털 시스템 구축 유형]

정보보안업무 일원화
- 시스템, 솔루션 통합관리 및 정보자산관리
- 정보보호 업무를 대시보드를 통해 한 화면에서 처리
- 전체적인 보안 정책의 승인결재 현황관리

프로세스 통합
- 정보보호 업무 및 프로세스 일원화
- 정책, 계정 등의 신청/결재/승인/변경/삭제 등 일괄처리

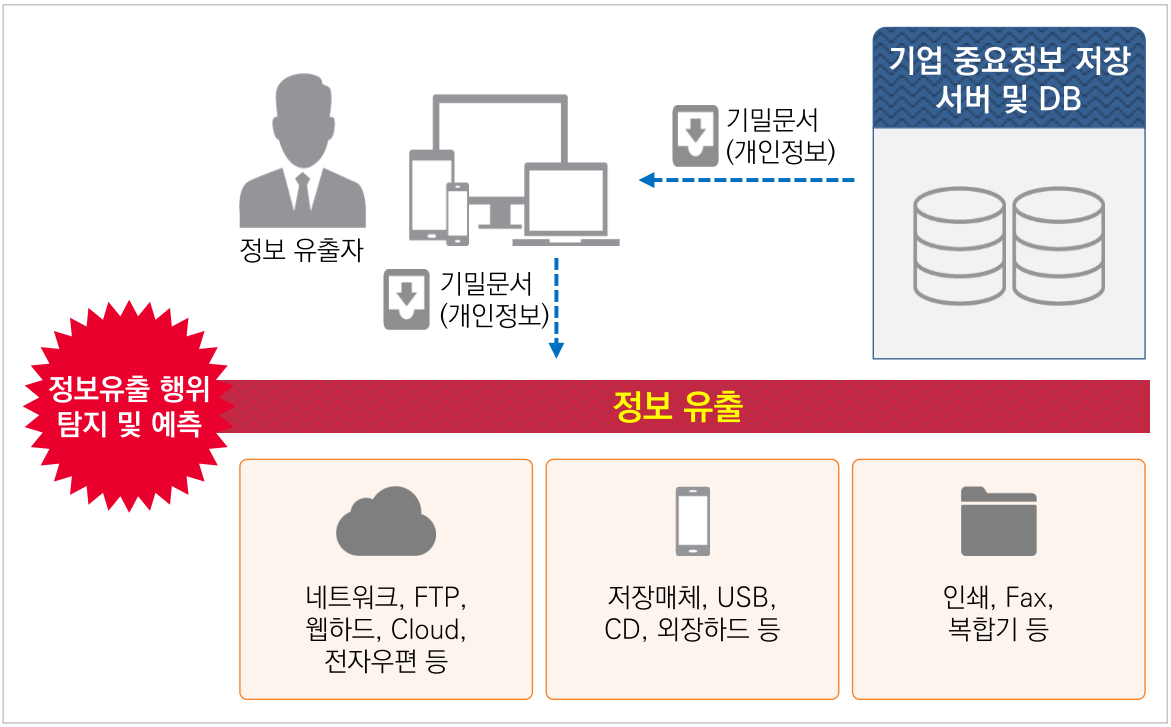
컴플라이언스/교육관리
- 보안관련 법률 정보 제공 및 준수사항검토, 이력관리
- 체계적인 교육 프로세스를 통한 역량 향상

Part 5

이상징후 탐지 시스템

1) 시스템 개요

가. 시스템 개요



[그림 Ⅱ-31. 이상징후 탐지 시스템 개요]

이상징후 탐지란, 전사적 관점의 보안 로그 분석을 통해 정보유출이 가능한 위협의 징후를 감지하고, 이를 보안사고로부터 사전 예방 할 수 있도록 구현하는 방법입니다.

많은 기업들에서는 내부 임직원 및 협력사 직원에 의한 정보유출 사고가 지속적으로 증가하고 있지만, 그에 대한 대비책은 위협으로부터의 방어, 유출 이후 사후조치 정도에 머물고 있습니다.

개인정보 및 기업정보 유출에 대하여 유출사고 발생 후 사후처리를 위한 시스템이 아니라, 정보 유출 이전에 이상행위를 감지하고, 이를 통해 사전에 유출을 차단하는 시스템이 필요하게 되었습니다. 이를 이상징후 탐지 시스템이라고 하며 통합 수집, 저장된 보안 솔루션 로그를 바탕으로 분석하여 탐지된 이벤트를 관리하는 시스템 입니다.

최근에는 사용자 행위분석(UEBA[1]) 기술로 A.I기반 머신러닝 기법을 활용하여 탐지 이벤트를 도출하는 방식으로 발전하고 있습니다.

1) UEBA (User and Entity Behavior Analytics) : 시스템 로그를 기반으로 사용자와 엔티티의 행위를 분석하여 내부자 위협탐지와 이상패턴 감지 및 관리를 위한 보안 프로세스

나. 시스템 구축 필요성 및 추진방향

기업내의 대부분의 유출사고는 인가된 사용자에 의해 발생하는 경우가 대부분이며, 유출사고는 지난 몇 년 간 급속히 증가하고 있습니다.

시스템 구축 시 주요 추진방향은 사용자의 행위를 분석하여 이상행위를 도출 할 수 있는 상관분석 시나리오 도출이 중요합니다.

사용자 사번, IP 기반 행위 뿐만 아니라 행위 중심 분석, 다른 업무처리 간 이상행위의 상관관계를 분석하는 것이 관건하며, 이를 위해서는 업무흐름 관련한 시각화 분석과 비정상적인 행위 탐지, 위험도 점수화 및 우선순위, 이벤트 기반의 행위 모니터링 등이 필요합니다.

개선사항 및 필요성

내부정보 전사적 모니터링 관리 필요

- 개인 및 신용정보 오·남용 모니터링 필요
- 개인정보 및 내부 중요정보 이상과다 조회에 따른 유출 사고 발생 대응력 필요
- 개인정보 및 내부 중요정보 유출에 대한 중·장기적 분석 체계 미비

내부정보 관리체계 미비

- 전사업무와 부서별 업무의 관리 정책 분리 필요 (중요정보 사용부서 R&R분리)
- 시나리오 베이스의 정량적 관리체계 마련 필요
- 이상징후 탐지 이후 분석 대응을 위한 프로세스 정립 필요

개인정보 보호의 사회적 요구 증대

- 개인정보 관련 법제도 강화에 따른 컴플라이언스 준수 및 대응 요구
- 중요정보 유출 사고 예방을 위한 감독기관 점검 대응 체계 필요

추진 방향

관리대상 업무 전사적 확대

- 사용자 PC보안 솔루션의 데이터 통합 수집 및 상관 분석
- 개인정보 오·남용 및 내부 중요정보 유출 모니터링 통합 View 구축

내부정보 관련 이상징후 탐지 체계 최적화

- 이상징후 탐지 시나리오 개발 및 체계화
- 탐지 시나리오 생성, 변경관리 UI 및 기능 구축
- 시나리오 L/C 관리 현행화를 위한 프로세스 정립
- M/L을 통한 통계 분석으로 임계치 자동 반영 (임계치 비고정)

컴플라이언스 대응체계 확보

- 개인정보 법·규제 강화 대응 및 관리 감독기관 대응
- 이상징후 규정 및 지침 정책 반영

다. 주요 구축 내용

이상징후 탐지의 주요구축 내용은 연동, 시나리오, 대응절차의 3가지가 중요합니다. 연동은 수집대상과 연동항목 정의 및 방식을 정의하는데 중점을 두어야 하고, 시나리오는 업무환경 분석을 통해 사용자의 행위기반 분석이 필요하며, 위험지표와 위험 측정 지표를 선정하는 것이 주요 관점입니다. 대응절차는 이상행위가 탐지되었을 때 소명절차와 확인 절차를 프로세스화 하여야 합니다,

구축영역	추진방향	주요내용
데이터 수집	모니터링 영역 전사적 확대	**데이터 연동 처리** 1 이기종의 업무 및 보안 데이터의 연동 기능 2 실시간 데이터 수집 및 무결성 저장 3 연동파일 형식, 주기, 방식, 항목정의
탐지 및 분석	상관분석을 통한 탐지 분석	**데이터 탐지 및 데이터 상관 분석** 4 주요 보안 데이터 분석 및 위험요소 식별 5 과·오탐 최소화를 위한 부서별/업무별/역할별 정책 적용 6 업무별 고위험군 분류 및 퇴직 예정자 식별
시나리오 컨설팅	시나리오 컨설팅을 통한 탐지 Rule정의	**단위 및 복합 시나리오 정의** 7 보안통제 분석 기반 탐지 시나리오 정의 8 통제기반 모델링 및 정규화 작업을 통한 고위험군 관리체계 수립 9 위험측정지표 분석 및 핵심측정지표 정의
대응 프로세스 구현	이상징후 탐지에 대한 대응 처리	**대응 절차 처리** 10 전 임직원 대상 소명, 보고 절차 구축 11 이상징후 대응정책 및 프로세스 정규화 활동
모니터링 이력 및 보고관리	실시간 탐지 모니터링, 주기별 보고 및 증적관리	**모니터링 및 이력관리** 12 실시간 탐지 모니터링 View 13 주기별 보고서 및 탐지결과 증적관리

라. 기대효과

기대 효과

STEP 1

전사 모니터링 관리체계 구축

- 부서별, 개인별 중요정보 사용현황 및 오·남용 사용에 대한 실시간 모니터링
- 전사적 부서별, 영역별 중요정보 사용현황 통계 분석
- 전 임직원 대상 소명 및 보고관리 체계 구축

STEP 2

개인정보 및 기업정보 유출 대응

- 단위솔루션 및 업무시스템 로그 통합수집을 통하여 이상징후 분석 기반 확보
- 단순/복합 상관분석 시나리오 기반 탐지 환경 구축
- 내부사용자에 의한 개인정보 및 기업정보 유출 위험 감소

STEP 3

Compliance 대응 향상

- 개인정보 규제에 대한 선제적 대응
- 개인정보 및 기업 정보 유출 사고를 대비한 증적 확보
- 감독기관의 감사 및 규제에 적극적인 대응 및 조치를 위한 기반 확보

STEP 4

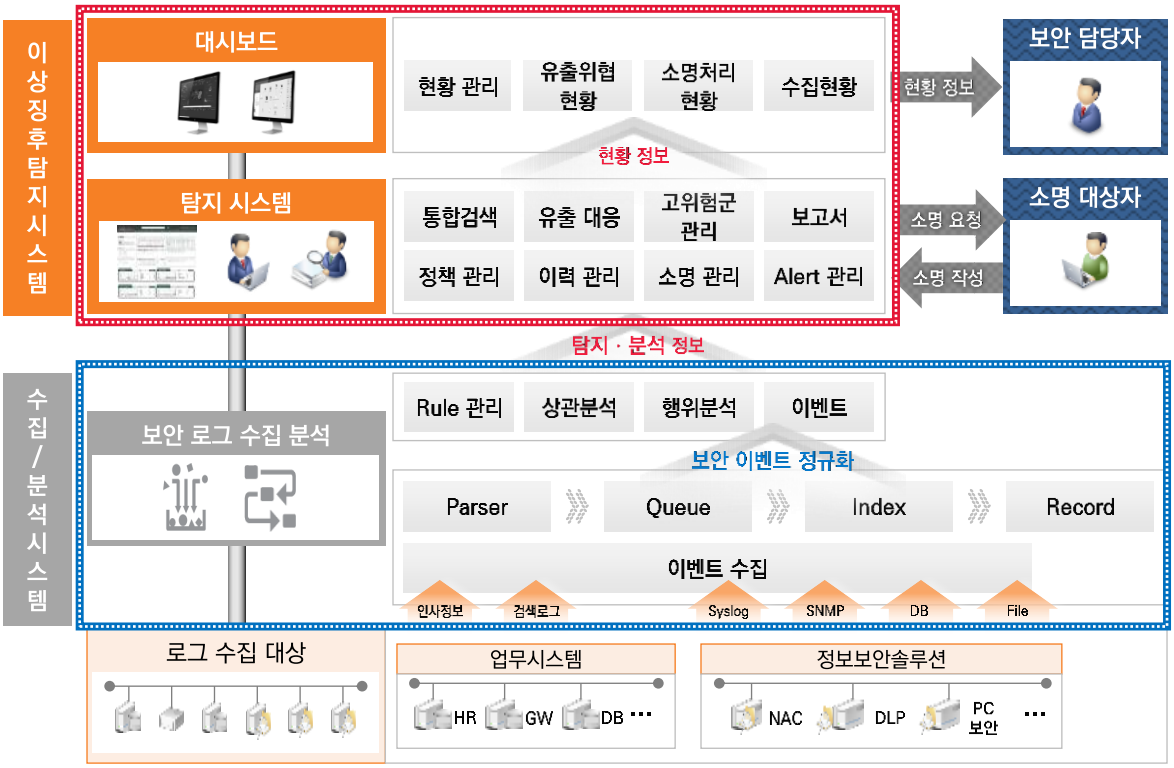
대내외 신뢰도 향상 및 업무 투명성 제고

- 내부사용자의 개인정보 취급에 대한 명확한 처리 가이드 제시
- 소명 활동을 통한 내부사용자의 보안의식 고취
- 감독기관의 감사 및 규제에 대한 적극적인 대응 및 조치 기반 확보

내부정보 유출 탐지 모니터링
이상징후 탐지 시스템

2) 시스템 구축

가. 시스템 개념도



[그림 Ⅱ-32. 이상징후 탐지 시스템 개념도]

이상징후 탐지 시스템은 대상장비로부터 로그수집저장, 분석위협탐지, 대시보드 영역으로 구성됩니다. 해당 보안장비의 로그는 이상징후 탐지 시스템에서 직접 수집하거나 SIEM장비에서 통합된 로그를 수집할 수 있습니다. 시나리오에 의해 탐지된 이벤트는 절차에 따라 소명처리를 진행하며, 결재과정과 기준은 정책적으로 미리 정의 해야 합니다. 즉, 소명자에게 자동이나 수동으로 소명요청의 기준설정, 결재라인 정의, 현장대리인을 통한 외주인력 소명요청 등 프로세스를 정의하여 적용합니다.

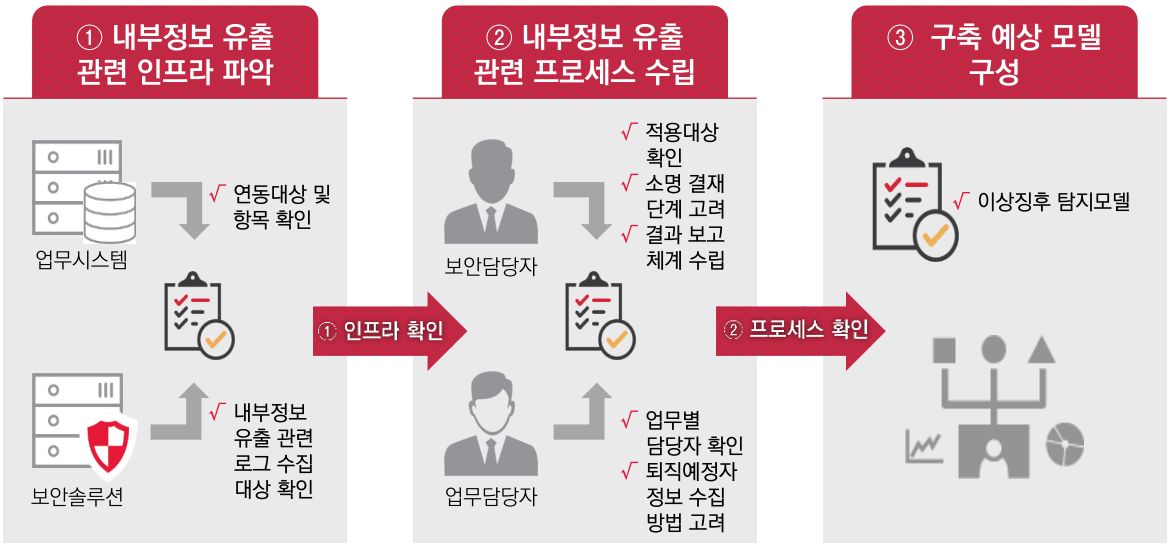
주기적인 1일 수집 로그량과 저장기간을 고려하여 저장공간(H/W구성)을 확보하며, 분석/탐지/통계/소명처리의 업무영역과, 실시간 현황정보 View기능의 대시보드 영역으로 시스템을 구성할 수 있습니다.

수집 장비와 분석/탐지 장비는 안정성을 위해 이중화를 고려해야 하며, 저장공간은 분산저장을 위해 Clustering을 고려 해야 합니다.

나. 사전준비 필요사항

이상징후 탐지 시스템을 구축 하기 이전에 고객사에서 사전 준비할 사항입니다. 로그수집을 위한 대상 시스템 정의, 연동할 항목 정의, 항목의 형태, 수집주기 및 전체 연동 로그의 1일 수집량을 정의해야 합니다.

프로세스 수립은 고객사에서 유출 탐지에 따른 절차를 정의해야 합니다. 소명대상 정의, 결재선, 결재할 역할부서, 결재단계를 정의합니다. 이상징후 탐지의 전체적인 목표 예상 모델을 구성하고, 향후 시나리오를 현행화 운영하는 역할과 대상을 정의하고 시스템 구축 사업을 시작해야 합니다.



[그림 Ⅱ-33. 이상징후 탐지 시스템 구축 사전준비]

내부정보 유출 관련 인프라 파악

- 내부 중요자료 유출 탐지를 위한 로그수집 대상 장비 파악
- 개인정보 오·남용 탐지를 위한 로그수집 대상 장비 파악
- 인사정보, 자산정보, 업무정보 수집 등 시스템 연동항목 정의
- 연동 파일 형식, 주기, 방법, 유형(DB, file/FTP 등)

내부정보 유출 관련 프로세스 수립

- 내부정보 유출 적용 대상 정의 (정직원, 외주 등)
- 소명을 위한 범위, 방법, 결제 단계 고려 (중간결재자 존재 여부 등)
- 업무에 따른 고위험군 분류 및 퇴직예정자 범위 정의

구축 예상 모델 구성

- 수집된 정보를 통한 구축 예상 모델 정립
- 이상징후 탐지 시나리오 현행화 방안 수립

다. 구축 유형

구축 유형으로는 시나리오를 설계하기 위한 방법론으로 『위협분석 및 모니터링 방법론』[1]을 적용한 사례와, 빅데이터 엔진을 기반으로 로그의 상관분석과 비정형 행위 탐지기술을 도출하는 머신러닝(M/L) 적용 구축사례를 소개합니다.

✓ 유형 1 시나리오 전문 컨설팅 적용한 이상징후 탐지 시스템

[그림 II -34. 시나리오 전문 컨설팅 구축 사례]

분석

- 비즈니스 환경 이해, 요구 제약사항 파악 및 위험관리 범위 확인
- 개인정보 통제 현황 파악, 보안솔루션 정책 및 예외 현황 분석
- 업무 처리 절차 분석 및 오·남용에 대한 명확한 이해

평가

- 단일 시나리오 도출
- 4W1H 기반 시나리오 구성요소 분석
- 적용 가능한 시나리오 선별
- 여러 단위 시나리오 연결한 복합 시나리오 도출

구현

- Scoring 모델 수립
- 임계치 설정
- 시나리오 검증을 통한 시나리오 유효성 및 임계치 보정

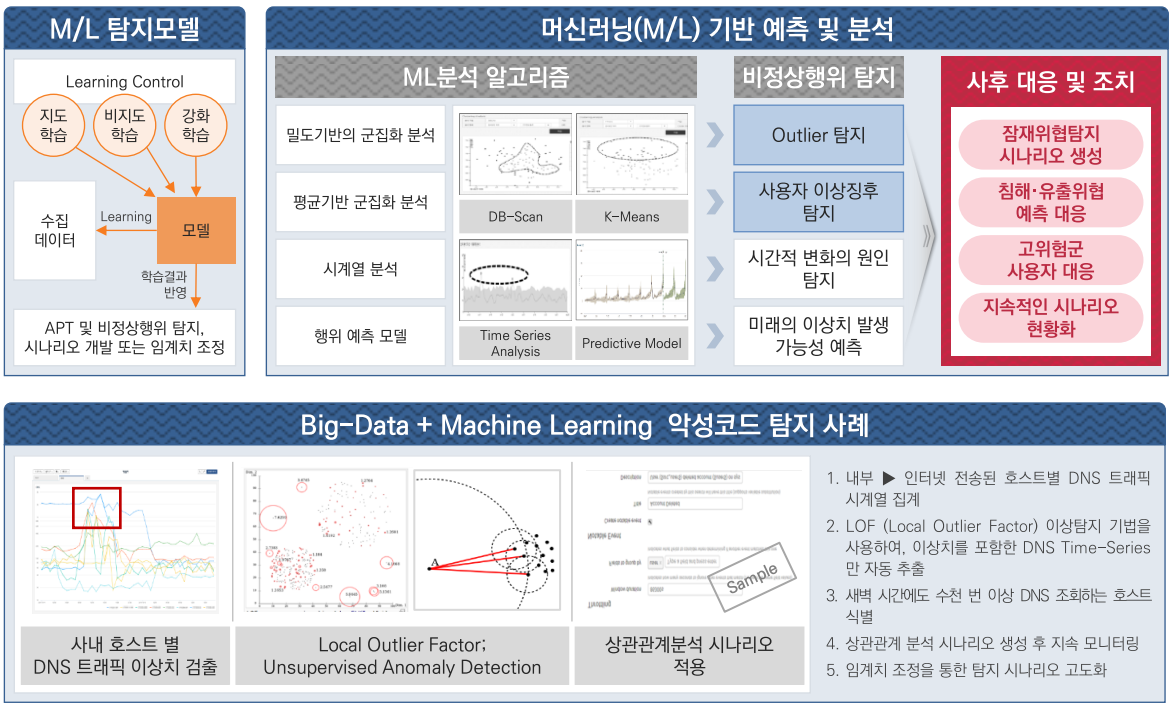
1) 위협분석 및 모니터링 방법론 : 시나리오 구축을 위한 SK인포섹 자체 방법론

✓ 유형 2 머신러닝 기반 이상징후 탐지 시스템

머신러닝은 컴퓨터 과학 중 인공지능의 한 분야로, 패턴인식과 컴퓨터 학습 이론의 연구로부터 진화한 분야입니다. 머신러닝은 경험적 데이터를 기반으로 학습을 하고 예측을 수행하고 스스로의 성능을 향상시키는 시스템과 이를 위한 알고리즘을 연구하고 구축하는 기술이라 할 수 있습니다. 머신 러닝의 알고리즘들은 엄격하게 정해진 정적인 프로그램 명령들을 수행하는 것이라기 보다, 입력 데이터를 기반으로 예측이나 결정을 이끌어내기 위해 특정한 모델을 구축하는 방식을 취한다고 보시면 됩니다.

수집된 다량의 로그정보를 머신러닝 기법을 통해 분석하여 기존 정형화 되어 있지 않은 비정상 행위를 탐지하여 새로운 시나리오를 개발하고, 상황에 따라 변화하는 통계를 기반으로 임계치 조정이 가능합니다.

머신러닝을 통한 분석이 제대로 이루어지기 위해서는 일반적으로 최소 3개월간의 자료가 필요합니다. 최근 솔루션은 머신러닝 모듈을 Toolkit으로 제공하거나 내부 알고리즘 모듈이 탑재되어 서비스 되는 솔루션들이 있습니다.



[그림 II -35. 머신러닝 기반 이상징후 탐지]

분석 및 위협 예측

- 전문 컨설턴트의 시나리오 작성 후 머신러닝 모듈을 이용하여 탐지 결과에 대한 정탐/오탐 학습
- 학습된 데이터를 분석하여 APT 및 이상징후탐지 등 알려지지 않은 위협에 대해 예측하고 대응 가능

시나리오 고도화 및 개선

- 예측된 위협에 대해 신규 시나리오를 추가하여 기존 시나리오를 고도화

보안SI를 통한 IT정보보호 구축 가이드

CONTENT

III

솔루션별 보안

III
솔루션별 보안

3. 네트워크 보안

Part 1

사용자 보안

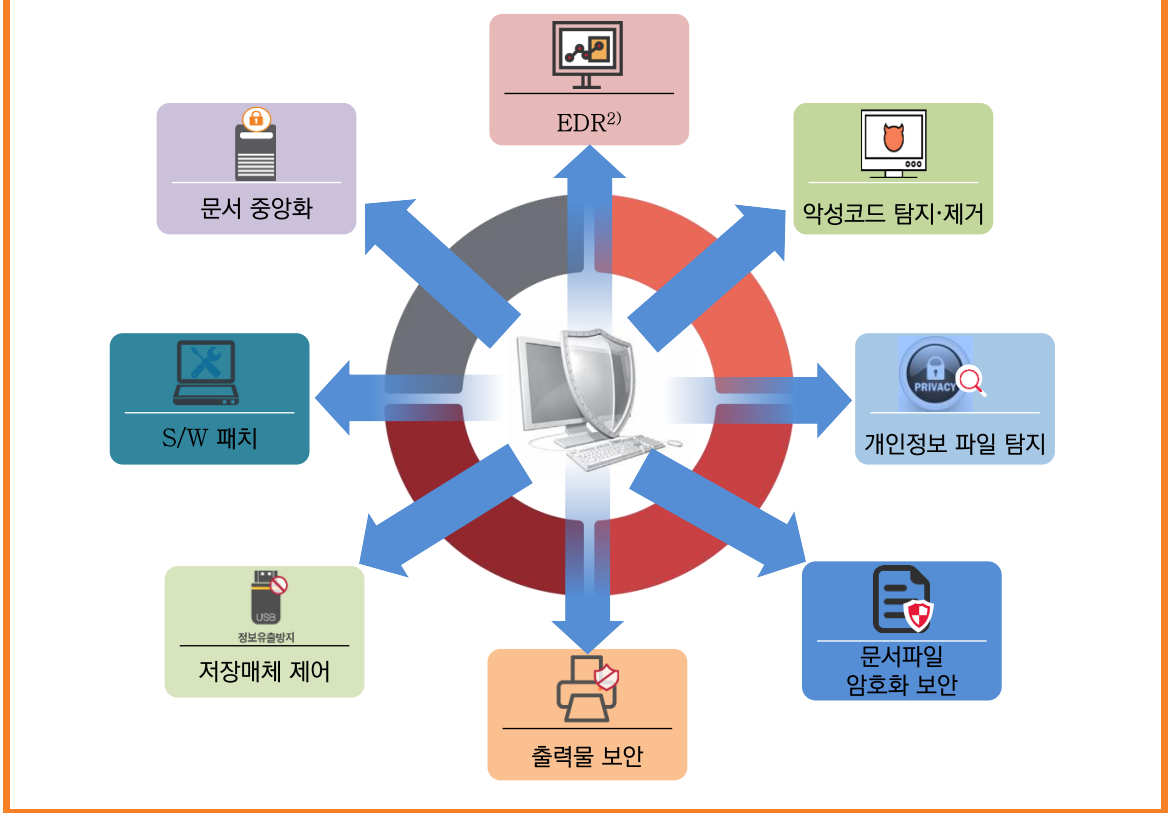
1) 사용자 보안 개념

사용자 보안을 광범위하게 보면 보안의식 제고와 교육 및 관리적 보안이 포함되지만, IT정보보호 관점에서는 사용자 PC를 안전하게 사용하기 위해 악성코드 예방과 치료활동, 정보유출 사전대응, 필수S/W설치유도 및 패치, 네트워크 관리, 물리적 매체에 대한 보호활동 등 주기적인 점검과 제어를 통하여, 사용자 PC의 보안통제를 지원하는 S/W와 H/W의 활동이라고 할 수 있습니다.

최근에는 사용자 PC보안에 관련된 프로그램과 솔루션들이 다양하고 광범위하게 발전하고 있습니다. 또한, EndPoint[1]보안과 IoT(사물인터넷)에 대한 보안영역으로 확장되고 있습니다.

본 장에서는 사용자 보안의 S/W 부분을 중점으로 설명 드리며, 관련된 보안솔루션에 대한 간략한 특징으로 소개하겠습니다.

사용자 보안 주요 솔루션 구성



[그림 Ⅲ-1. 사용자 보안 영역]

1) EndPoint : 어떠한 소프트웨어나 제품의 최종목적지인 사용자를 가리키며, 그 예로는 PC나 노트북, 핸드폰 등 유저가 사용하는 devices등을 말함
2) EDR (EndPoint Detection & Response) : 사용자 단말에서 일반적인 안티 바이러스 시그니처로 차단하지 못하는, 알려지지 않은 위협을 분석하거나 탐지 할 수 있는 차세대 EndPoint 기술

2) 보안 영역별 특징

사용자 단말영역의 보안을 위해 외부로부터 악성코드 침입을 방지하고, 내부 중요정보와 개인(신용)정보의 유출을 방지하려는 노력의 일환으로 다양한 솔루션들이 설치 운영되고 있습니다.

대표적인 8가지 보안 영역에 대해 주요기능과 특징을 소개 드리며, 많은 벤더사에서는 보안영역별로 전문성과 특징을 강조한 솔루션들을 제공하고 있습니다. 최근 사용자 단말보안 솔루션들은 통합이라는 의미로 보안영역별 기능을 하나의 솔루션에 모듈화 탑재하여 판매되고 있습니다.

구분	보안솔루션 영역	목적	일반 주요기능	최신기술 및 특징
1	악성코드 탐지 (백신)	외부의 악성코드 침해위협 대응	▪ 실시간 악성코드 탐지 ▪ 악성코드 진단 및 감염 방지 ▪ 랜섬웨어 진단 및 차단 ▪ 사이버 침해사고 예방	▪ 행위/평판 분석 ▪ 기존 악성코드 데이터를 활용한 머신러닝 분석
2	개인정보 탐지	PC내의 개인정보 탐지에 따른 정보유출방지	▪ 개인정보 기준설정 및 탐지 ▪ 개인정보 정책 정의	▪ OCR(광학적 문자 판독장치)로 이미지의 문자 인식 개인정보 판독 ▪ 성능 이슈와 오탐률 최소화
3	문서 보안 (DRM)	PC내의 파일에 대해 문서 암호화 적용 후 정보유출방지 (DRM)	▪ 파일 암호화 ▪ 파일권한 및 유효기간 관리	▪ 외부인력과 협업으로 인한 문서유출 사고 대응 ▪ 반도체, 자동차, 조선, 철강 등 주요사업 기술에 대한 문서보안 강화
4	출력물 보안	프린트물 내용의 정보 유출 방지	▪ 로고, 이미지, 출력자 정보(ID, IP,시간) 워터마크 ▪ 개인정보 출력 시 신청 프로세스 ▪ 출력이력 출력물 유통 추적	▪ 육안 식별 불가능한 비인지 워터마크 ▪ 특수보안용지 활용으로 출입통제
5	매체제어	각종 매체(CD, USB, Disk 등)에 의한 정보유출방지	▪ 사용자PC에서 로컬 디스크, USB, CD 등 저장매체 차단 ▪ 보안정책 설정에 따라 모니터링 및 운영	▪ 포괄적 정보유출 기술 적용 ▪ 매체제어의 암호화 및 접근통제 기능 강화
6	패치관리 (PMS)	침해위협과 유출방지를 위해 OS 및 특정 보안 솔루션의 최신패치 유지	▪ OS 및 S/W패치 기능 ▪ 패치 종류, 설치 주기/환경 등 정책 설정 ▪ 패치운용현황 모니터링	▪ 패치 일괄 통합관리 ▪ 패치관리의 외부위협으로부터 검증성 확보
7	문서 중앙화	중앙서버에서 모든 문서를 관리하여 보안위협에 대응	▪ 문서 중앙서버 집중화 ▪ 자료 암호화 기술 (서버, 구간 암호화) ▪ 폴더별 접근 권한 ▪ 사용자 PC에서 자료저장 금지 ▪ 원천적으로 서버에 자료저장 ▪ 자료 작업은 서버에서 실행	▪ BYOD 모바일 접근 권한 ▪ 역할기반 권한 제어 ▪ Cloud 연계
8	EDR	EndPoint의 행위기반 악성코드 탐지 대응 솔루션	▪ 알려지지 않은 악성코드 예방 ▪ 분석 및 이상탐지 ▪ 악성코드 제거 및 대응	▪ 행위분석, 머신러닝, IOC (Indicator of Compromise) 탐지기술

[표 Ⅲ-1. 사용자 보안 영역별 특징]

3) 보안 솔루션 소개

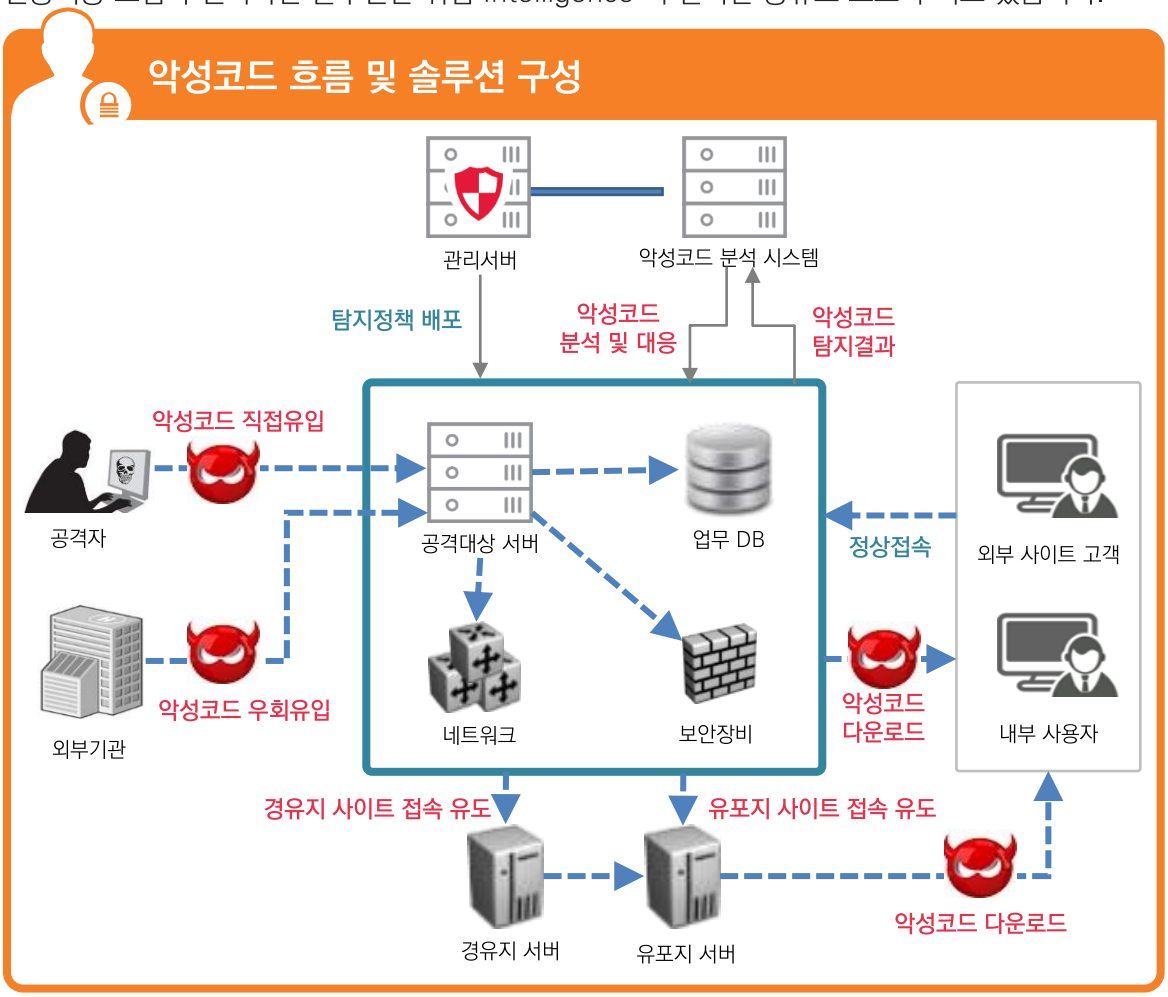
가. 악성코드 탐지 (백신)

A. 솔루션 개념

악성코드란, 악의적이고 의도적으로 사용자에게 피해를 주고자 만든 프로그램, 매크로, 스크립트 등의 컴퓨터 상에서 동작하는 모든 파일 형태를 말합니다.

현재 웜과 바이러스의 악성코드 종류가 지능화되고 다양하게 유포되고 있습니다. 유포 경로 또한 다양하며 컴퓨터의 취약점을 이용하여 스스로 전파되거나 메일과 저장매체로 전파되고 있습니다. 백도어와 트로이 목마, 스파이웨어 등 외부위협의 예방과 대응을 위해 악성코드 탐지 솔루션이 필요하며, 가장 기본적이고 보편화된 보안솔루션으로 백신 솔루션들이 운영되고 있습니다.

최근에는 지능화되고 있는 악성코드의 외부위협에 따라 백신 솔루션들이 최신화되고 머신러닝 기반 인공지능 도입과 벤더사간 솔루션간 위협 Intelligence 의 실시간 공유로 고도화 되고 있습니다.



[그림 Ⅲ-2. 악성코드 탐지 솔루션 구성]

B. 주요기능

악성코드 탐지 솔루션은 기본적으로 정책 설정 부분, 악성코드 탐지 대응, 모니터링 및 결과보고의 3가지로 구성되어 있습니다. 최근 추가적인 기능으로 이동식 저장장치 차단, 행위/평판 진단, 랜섬웨어 대응 등이 추가적인 기능으로 보완되고 있습니다.

탐지 차단에 대한 주요 기능으로는 윈도우 및 응용 프로그램의 취약점을 이용한 익스플로잇(Exploit)공격, 제로데이 공격(Zero-Day Attack) 등 알려지지 않은 보안위협 요소까지 사전 방역 할 수 있는 기능과 악성 스크립트 차단, Rootkit 해킹 공격 차단, 유해 사이트 차단 기능까지 백신 기능은 기능적으로 발전하고 있습니다.

기능영역	주요 기능 내용
정책관리	**사용자 정의 정책 설정** 1 네트워크 환경 및 인터넷 접속 보안정책 2 IP, Domain, String 사용자 정의 패턴 설정 3 실시간 자동 업데이트 환경 구성 및 외부 위협정보 공유
악성코드 처리	**악성코드 진단 및 치료** 1 바이러스, 웜 등 악성코드 실시간 진단 2 악성코드 탐지 결과 정책기준 치료대응 **네트워크 보안** 1 네트워크 침입 차단, 유해 사이트 접속차단
모니터링 및 보고	**모니터링** 1 시스템 상태 정보, 트래픽 탐지 모니터링 2 악성코드 실시간 탐지내역 확인 3 악성코드 탐지 결과 및 통계내역 주기적 보고

C. 솔루션별 특징

악성코드 탐지 처리를 위한 백신 솔루션의 일부 제품을 소개 합니다. 국내외 레퍼런스가 많은 백신용 솔루션으로 각각의 다양한 특징을 참고 바랍니다.

개발사	제품명	주요기능	솔루션 특징
Symantec	Symantec Endpoint Protection 14	▪ 네트워크 방화벽 및 침입 차단 ▪ 애플리케이션 및 매체제어 ▪ 메모리 익스플로잇 공격 차단 ▪ 파일 평판 분석 ▪ 첨단 머신러닝 ▪ 에뮬레이션 ▪ 행동 모니터링	▪ 외산 제품으로 인지도 높음 ▪ 대규모의 글로벌 보안위협 인텔리전스 네트워크를 활용 ▪ 단일 관리 콘솔 및 고성능 경량화 에이전트에서 엔드유저의 PC성능 영향도 낮음
안랩	V3 Internet Security 9.0	▪ 악성코드 진단 ▪ 네트워크 보안 ▪ 행위 / 평판 진단 ▪ Active Defense ▪ PC 최적화	▪ CC인증 ▪ 다차원 분석 플랫폼 적용 ▪ ASD 평판 검사 ▪ ASD 클라우드 기반 탐지 기술 ▪ ASD 시그니처 기반 탐지 ▪ 평판 기반의 프로그램 실행 차단 ▪ 디코이 진단을 통한 랜섬웨어 대응 ▪ 악성 URL/IP 차단 ▪ 네트워크 행위 기반 침입 탐지
하우리	ViRobot 7.0	▪ 악성코드 진단 및 치료 ▪ 사전 방역 기능 ▪ 네트워크 보안 ▪ 랜섬웨어 차단 ▪ PC 관리 ▪ 다양한 부가기능	▪ CC인증 ▪ 행위기반기술이 적용되어 보안취약점을 이용한 보안위협요소의 사전차단 ▪ I/O캐싱엔진이 적용되어 가볍고 빠르게 검사 진행 ▪ APT레이더와 APT실드를 통한 랜섬웨어 실시간 차단
이스트시큐리티	알약 5.0 / 알약 서버 5.0	▪ 악성코드 탐지 및 치료 ▪ 실시간 감시 ▪ 네트워크 보호 ▪ 매체제어 ▪ 랜섬웨어 차단 ▪ PC관리	▪ CC인증 ▪ 국제 인증 자체 엔진인 테라 (Tera),비트디펜더 (Bitdefender), 소포스 (Sophos)의 트리플 엔진 구조 ▪ 국외에서 수집되는 해외 위협요소 DB와 국내 위협요소 DB를 통한 탐지 ▪ AIS (ALYac Intelli gence Scan) 엔진 기반 클라우드 스캔으로 신/변종 위협 실시간 대응 ▪ Smart Scan 기술을 통해 실시간 감시 또는 정밀 검사 시 실제 검사가 필요한 파일 분류
Avast	Avast Business Antivirus	▪ File Shield ▪ CyberCapture ▪ 방화벽 ▪ 행동 감시 ▪ 웹 실드 ▪ 이메일 실드 ▪ Anti-spam ▪ 샌드박스 ▪ 실제 사이트 ▪ 복구 디스크	▪ 안티바이러스 – 4개의 보호 기능을 사용하여 감염된 이메일 송수신 불가 ▪ 방화벽 – Avast의 방화벽이 업무 속도의 저하 없이 사용자를 안전하게 보호 ▪ CyberCapture – CyberCapture는 바이러스 데이터베이스를 항상 최신 상태로 유지하기 위해 전 세계의 의심스러운 파일과 제로데이 위협을 분석 ▪ 스마트 검사 – PC 성능 보장, 시스템의 미취약 부분 스킵

[표 Ⅲ-2. 악성코드 탐지 솔루션별 특징]

나. 개인정보 탐지

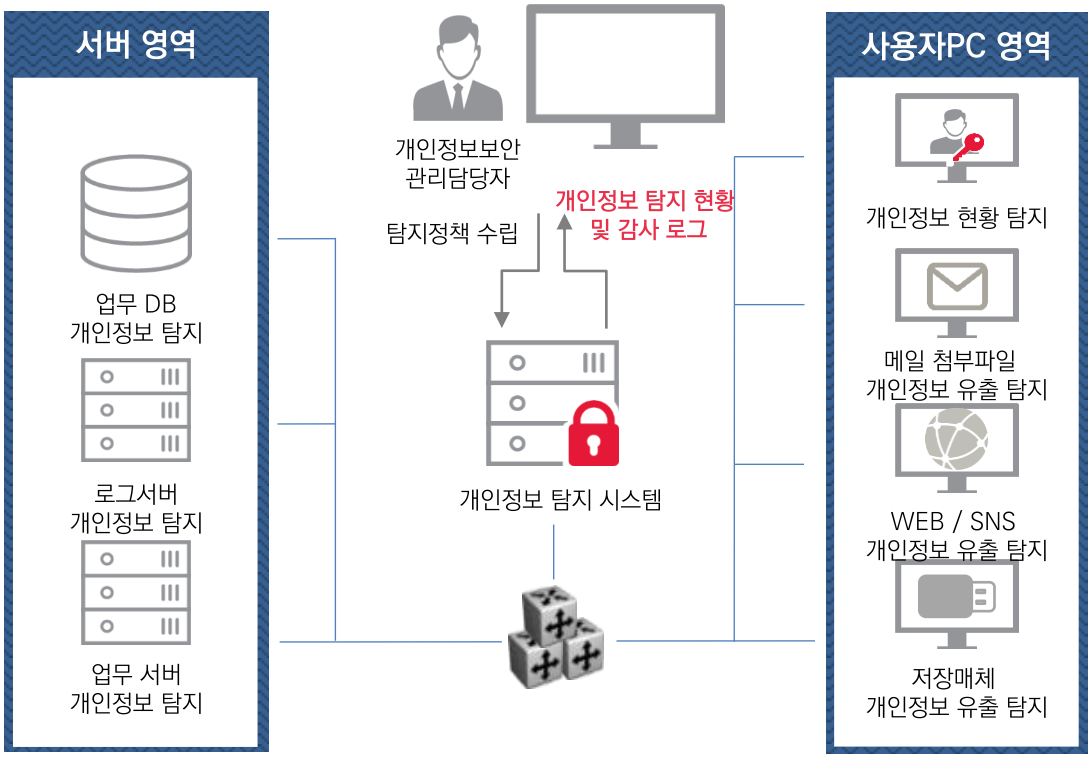
A. 솔루션 개념

개인정보 탐지(데이터 유출 방지 Data Loss Prevention, DLP) 솔루션은 개인정보 유출방지와 기관 Compliance에 대응하며, 기업과 고객의 중요정보를 보호하기 위한 보안 솔루션 중 하나입니다.

개인정보 보안 관리자 및 책임자는 개인정보 탐지 솔루션을 운영하며, 탐지할 개인정보 및 민감정보의 패턴을 설정, 탐지 된 개인정보에 대한 정책을 수립합니다. 개인정보 탐지 솔루션은 사용자 PC 내 개인정보 파일을 탐지하며, 수립된 정책에 따라 개인정보 정책을 수행하게 됩니다. 또한 개인정보 및 민감정보 유출 시도 시 정책에 따른 위반 행위 제어를 통하여 개인정보 보안을 준수 할 수 있습니다.

개인정보 탐지 솔루션 도입의 이점으로, 개인정보 보안 체계 강화, 기업 내 곳곳에 산재되어 있는 개인정보 파일들의 중앙 관리, 개인정보 업무처리의 효율성 증가, 개인정보 유출 사고 방지로 기업의 이미지 제고 등 다방면에서 주요한 이점을 얻을 수 있습니다.

개인정보 탐지 솔루션 구성



[그림 Ⅲ-3. 개인정보 탐지 솔루션 구성]

B. 주요기능

개인정보 탐지 솔루션은 크게 정책 설정, 개인정보 탐지 및 보호, 모니터링 및 결과보고의 3가지로 구성될 수 있습니다. 탐지되어야 할 데이터가 점차 늘어남에 따라 빅데이터 처리 기술을 도입하여 개인정보 탐지 속도 단축, 개인정보 검출 패턴의 다양화 등 개인정보 탐지 솔루션의 기능 보완이 이루어지고 있습니다.

정책설정은 개인정보 검출 패턴과 임계치 설정, 서버 OS별/그룹별 정책설정, 검사 시간 및 예외시간 설정 등이 있으며, 개인정보 탐지 및 보호 기능은 개인정보의 생성/변경/삭제의 탐지와 파일 외부 반출 차단 등의 주요기능이 있고, 결과보고 기능은 주기적 보고서와 개인정보 현황 모니터링이 주요 기능으로 정의 할 수 있습니다.

기능영역	주요 기능 내용
정책 설정	**사용자 정의 정책 설정** 1 키워드/정규식 기반의 검출 패턴 등록 2 파일 포맷에 대한 검출 정책 설정 3 내/외부 저장장치 및 온/오프라인 파일 이동에 대한 정책 설정
개인정보 탐지	**개인정보 탐지** 1 개인정보파일 생성/변경/삭제 실시간 탐지 2 사용자 정의 패턴 탐지
개인정보 보호	**개인정보 파일 보호** 1 검출된 개인정보 파일 암호화 수행(자동정책, 수동) 2 사용자 정의 정책에 따라 파일 외부 반출 차단/허용(감사로그)
모니터링 및 보고	**모니터링 및 주기적 보고** 1 개인정보 현황에 대한 모니터링 2 개인정보 탐지 내역 및 보안정책 위배 행위 이력 관리 3 탐지 결과 및 통계내역 주기적 보고

C. 솔루션별 특징

최근 사용자 PC에서의 개인정보 보호 뿐만 아니라 DB, WAS, WEB 서버 내 개인정보 탐지에 대한 영역이 확대되어 가고 있으며, 빅데이터 및 머신러닝 기술을 도입하여 탐지 시간을 단축하고, 클라우드 환경의 지원 등 점차 다양해진 시장 상황에 따라 각 개인정보 보호 업체의 솔루션 또한 변화하고 있습니다.

개발사	제품명	주요기능	솔루션 특징
세이퍼존	Eagleye For Server	▪ 주민번호, 신용카드번호, 외국인 등록번호 등 개인정보 검색 정합성 검증 ▪ 정규식 패턴에 의한 사용자 정의패턴 지원 ▪ 다중 압축파일 검색 지원 ▪ 리소스(CPU/Memory/Network) 사용량 측정 및 제한 ▪ 검사현황 리포트, 대시보드 지원 ▪ 검출파일에 대한 조치지원(암호화, 격리, 삭제) ▪ 개인정보 패턴, 문서등급 설정기능 제공 ▪ 서버별 패턴, 등급, 다양한 검사옵션 설정기능	▪ CC인증 ▪ Java 기반 으로 다양한 OS 지원 ▪ 에이전트 리스 방식 지원 ▪ Plug-In CPU, Network 제한 기능 ▪ Plug-In 강제정지 가능 ▪ 대상서버의 리소스 모니터링 기능 ▪ 대상서버의 검출 진척률 표시 기능
	Eagleye C/S 3.0	▪ 주민번호, 신용카드번호, 외국인 등록번호 등 개인정보 검색 정합성 검증 ▪ 정규식 패턴에 의한 사용자 정의패턴 지원 ▪ 다중 압축파일 검색 지원 ▪ 검사현황 리포트, 대시보드 지원 ▪ 검출파일에 대한 조치지원(암호화, 격리, 삭제) ▪ 개인정보 패턴, 문서등급 설정기능 제공 ▪ 등급, 다양한 검사옵션 설정기능 제공	▪ CC인증(EAL2) ▪ 실시간 검색 구조 ▪ 동종 제품 대비 최상의 검색속도 ▪ 메일 검사 및 이동형 저장장치 검출 ▪ 개인정보 파일에 대한 등급 적용 ▪ 지원 환경 확대, 글로벌 환경 지원
소만사	Privacy-i	▪ 사용자 및 부서 관리 기능 ▪ 로그 조회 기능 ▪ 원격 검사 기능 ▪ 보안 정책 설정 기능 ▪ 기밀데이터(개인정보) 설정 기능 ▪ 통계 및 보고서 생성 기능 ▪ 서버설정 및 화면 잠금 기능 ▪ DB스캔 기능 ▪ 개인정보 검출/파기/암호화 ▪ 매체/출력물을 통한 개인정보유출제어	▪ CC인증(EAL2), GS인증 ▪ Mac/Linux버전 엔드포인트 DLP ▪ 빅데이터 검색을 통한 전사적 Print& Copy 자산관리 ▪ 서버 및 네트워크 DLP 솔루션 보유 (Server-I / Mail-i)

개발사	제품명	주요기능	솔루션 특징
지란지교데이터	PCFILTER 3.0	▪ 검사기능 – 전체검사/선택검사/간편검사 – 개인정보 파일 열기/저장/전송 시 실시간 알림 – 위/변조 확장자 및 숨김 속성 파일/폴더에 대한 검사 ▪ 보호기능 – 개인정보 파일 암/복호화 – 암호화 파일 편집 후 자동 암호화 ▪ 로그센터 – 관리자/선택/전체/간편/예약 검사 로그 – 실시간 알림 및 보호조치 로그 ▪ 설정 및 기타 – PC사용량 조절 기능 – 용량 및 다중압축 단계 설정 기능 ▪ 관리서버 기능 – 대시보드 형태의 개인정보 보유/보호 조치/알림 현황 – 기간/그룹/개인 별 통계현황 – 관리자 PC와 관리 시스템 간 암호화 통신(SSL) 지원	▪ CC인증(EAL2) ▪ OCR기능을 통한 이미지 파일 내 민감·개인정보 검사 제공 ▪ 구축형, SaaS형, USB형, 진단도구 등 라인업 구비
Ground Labs	Enterprise Recon	▪ 개인정보 검출 – 전세계 50여개국의 200개 이상의 개인정보 유형검출 가능 – 정형, 비정형 데이터 및 대용량 압축파일에 있는 개인정보 검출 가능 – 모든 운영체제와 DBMS E-Mail, cloud 지원 ▪ 개인정보 관리 – 시각화된 개인정보 통합 분석 관리 – 중앙통제 환경 제공 – 자동화된 개인정보 관리 – 다양한 형태의 리포팅 제공 ▪ 개인정보 보호 – 검출된 개인정보를 폐기/격리/마스킹/암호화 등 후속조치	▪ 정형 비정형 데이터를 직접 디코딩하여 성능 확보 ▪ C/C++ 기반으로 제작되어 안정적 하드웨어 제어 ▪ 파일분할방식 – 대용량 파일인 경우 작은 단위로 분할 후 메모리로 로딩하여 사이즈가 큰 파일이라도 과도한 메모리를 사용하지 않게 하는 기술

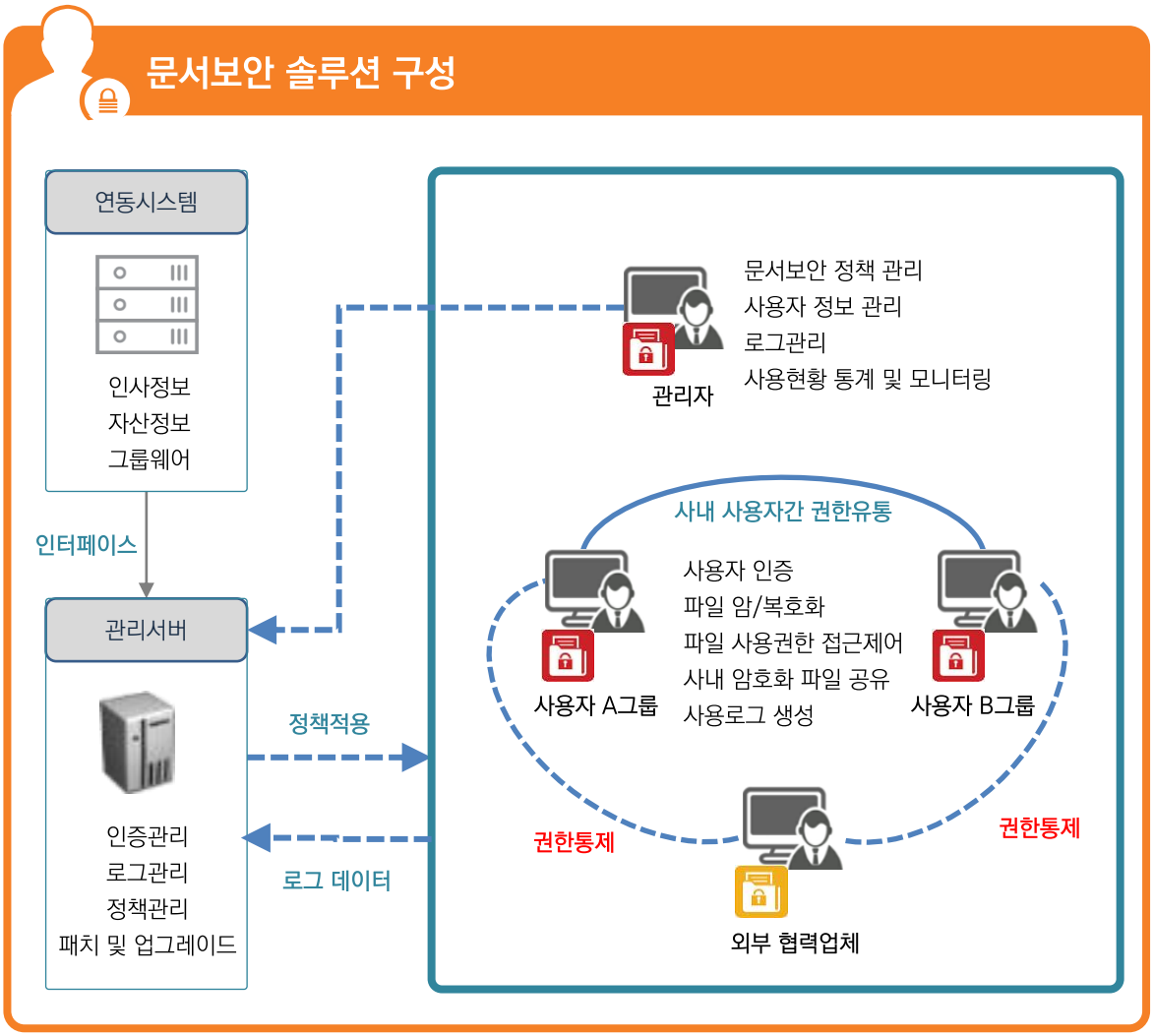
[표 Ⅲ-3. 개인정보 탐지 솔루션별 특징]

다. 문서 보안 (DRM)

A. 솔루션 개념

기업과 조직내의 문서는 대부분 전자파일로 관리되며, 개인정보와 중요정보의 외부유출을 방지하기 위한 보안 솔루션으로 파일을 암호화하고, 문서권한을 부여하는 문서보안 솔루션을 설치 운영하게 되었습니다. 문서보안 솔루션은 구축 이후 업무 관점에서 비효율적이며, 생산성을 저하 시키지만 문서보호를 위해서는 기본적이고 강력한 보안조치로 운영되고 있습니다.

Compliance를 준수해야 하는 기업과 산업기밀, 영업정보 등 중요 데이터를 보호해야 하는 목적, 그리고, 외부협력업체와 협업으로 업무를 수행하는 일이 많아지면서 내부정보 유출방지가 중요하게 되었습니다. 문서보안 솔루션은 파일을 암호화하고 사용권한을 통제하는 주요기능이 있으며, 추가적인 보안기능으로 구성되어 있습니다. 또한 암호화 기술은 최근 다양하고 복잡한 알고리즘을 적용하여 보안이 강화되고 있습니다.



[그림 Ⅲ-4. 문서보안 솔루션 구성]

B. 주요기능

중요정보가 담긴 전자문서는 문서생성부터 편집사용을 거쳐 폐기까지의 Life-Cycle을 관리하게 되는데, 생성과 유통에서의 문서보안 암호화와 복호화를 처리하는 프로세스와 이력과 로그관리까지를 주요기능으로 정의 할 수 있습니다.

문서의 사용권한에 대한 영역은 문서의 열람, 편집, 화면 캡처, 암호화 해제, 권한 변경, 열람 가능 일수 등을 사용자별/그룹별로 정책을 정의 할 수 있으며, 사용자 및 그룹별로 문서보안 등급을 설정할 수 있습니다. 사용이력에 대해서는 로그와 문서 파일의 암호화 해제와 반출에 대한 승인정보 결과로 감사업무에 대응합니다.

기능영역	주요 기능 내용
기준정보	**권한 및 기준정보** 1 사용자별 그룹별 역할별 권한설정 2 문서의 열람/편집/출력/복호화 권한 관리 3 인사정보와 그룹웨어 등 업무 시스템 연계
DRM 암호화/복호화	**파일/폴더 암호화 및 프로세스** 1 파일 암호화 알고리즘 적용 2 보안정책에 따른 파일 및 폴더 암호화 3 복호화 신청 프로세스 및 결재선 관리 4 주기적 통계 보고서 관리
이력 및 로그관리	**이력관리** 1 생성/열람/편집/출력/반출/해제 등에 대한 사용자 이력관리 2 정책변경, 사용자/그룹 변경 등 관리자 행위이력관리 3 암/복호화 통계 및 로그관리

C. 솔루션별 특징

문서보안 솔루션의 국내 많은 제품 중 7가지 솔루션을 선정하여 각각의 특징을 나열하였습니다. 문서보안 솔루션(DRM)의 중요요소인 암호화 기술, 접근제어 기술, 위험관리를 위한 기술로 나누어 소개 드리며, 최근에는 OS 및 시스템별로 문서보안 대상이 PC에서 서버, MAC, WEB, Mobile, Cloud로 확대되고 있습니다.

개발사	제품명	문서보안(DRM) 솔루션 주요기능		
		접근제어 기능	암호화 기능	리스크 관리
마크애니	Document SAFER	▪ 암호화 문서적용 권한에 따라 열람, 편집, 저장, 사용기간 및 인쇄기능 제어, 사용자 인증을 통한 비인가자 문서 사용제어	▪ 전체 문서 암호화 ▪ 암호화 자동처리	▪ 암호화 문서의 생성, 출력, 전달 등 사용이력관리 ▪ 사용목적에 따른 열람, 편집 설정 ▪ 암호화 해제 신청 프로세스
소프트캠프	Document Security	▪ 문서에 대한 열람(열람 횟수) / 편집 / 출력(출력 횟수) / 복호화 권한 제어 ▪ 사용자/그룹별, 문서의 등급별로 서로 다른 문서 사용 권한 설정 가능	▪ 보안정책에 따라 강제(자동) 암호화, 폴더 암호화, 단순 암호화 지원	▪ 사내 환경으로 복귀 시, 오프라인 사용 로그를 관리서버로 일괄 전송함과 동시에 온라인 로그인 상태로 자동 전환 ▪ 보안문서 생성 / 열람 / 편집 / 출력 / 반출 / 해제 등 사용자 행위와 정책변경, 사용자 및 그룹 변경 등 관리자 행위에 대한 각종 로그 기록 및 조회 가능
가비아	가비아DRM	▪ 인가자와 인가된 어플리케이션만 복호화 허용, 암호화된 파일의 비인가 접근차단	▪ Kernel Mode 자동 암/복호화	▪ 문서 콘텐츠 분석에 의한 개인정보 추출 및 문서삭제, 격리, 문서현황파악, 문서중앙 백업 및 다운로드
파수닷컴	Fasoo Enterprise DRM	▪ Rich Context 정보활용 ▪ 사용자의 세부권한을 동적으로 적용	▪ FIPS 140-2 인증 암호화 모듈 ▪ 지정된 등급으로 자동 암호화 처리	▪ 데이터 중심 사용로그분석을 통한 정책적용 ▪ 예외처리 문서의 사후보안관리 지원으로 위협 차단
이스트시큐리티	시큐어디스크	▪ 권한별 접근제어, 매체제어, 기능제한, 로그관리, 문서변조 차단, 캡처 및 출력 차단, 온라인 유출 차잔	▪ 서버 및 전송구간 암호화	▪ 서버에 저장한 문서버전 관리, 복원 ▪ 시큐어디스크 에이전트 중지신호, 보안정책 및 확장자 변경 시도 차단
블루문소프트	DocuRay DRM	▪ 비인가자 문서접근 차단 ▪ 유출된 정보보호	▪ 개인PC 개인정보 파일 암호화 ▪ Kernel Mode 자동 암복호화	▪ 키워드.패턴에 의한 중요정보 도출 ▪ 전체 문서 흐름관리/감시/추적/모니터링/파기
드루안	ShadowCube-EE	▪ Domain, URL 단위로 컨텐츠 제어 ▪ 전자서명(자치인증기관/CA) ▪ PKI (Public Key Infrastructure) 적용	▪ 일괄적 강제 암호화 및 선택적 암호화 ▪ 모든 문서 실시간 암호화 ▪ 개인별/부서별 암호화 방식 별도 적용	▪ 내부유출에 대한 부인행위 방지 ▪ 복호화 결재 시스템 ▪ 보안문서의 출력 시점에 워터마크를 삽입

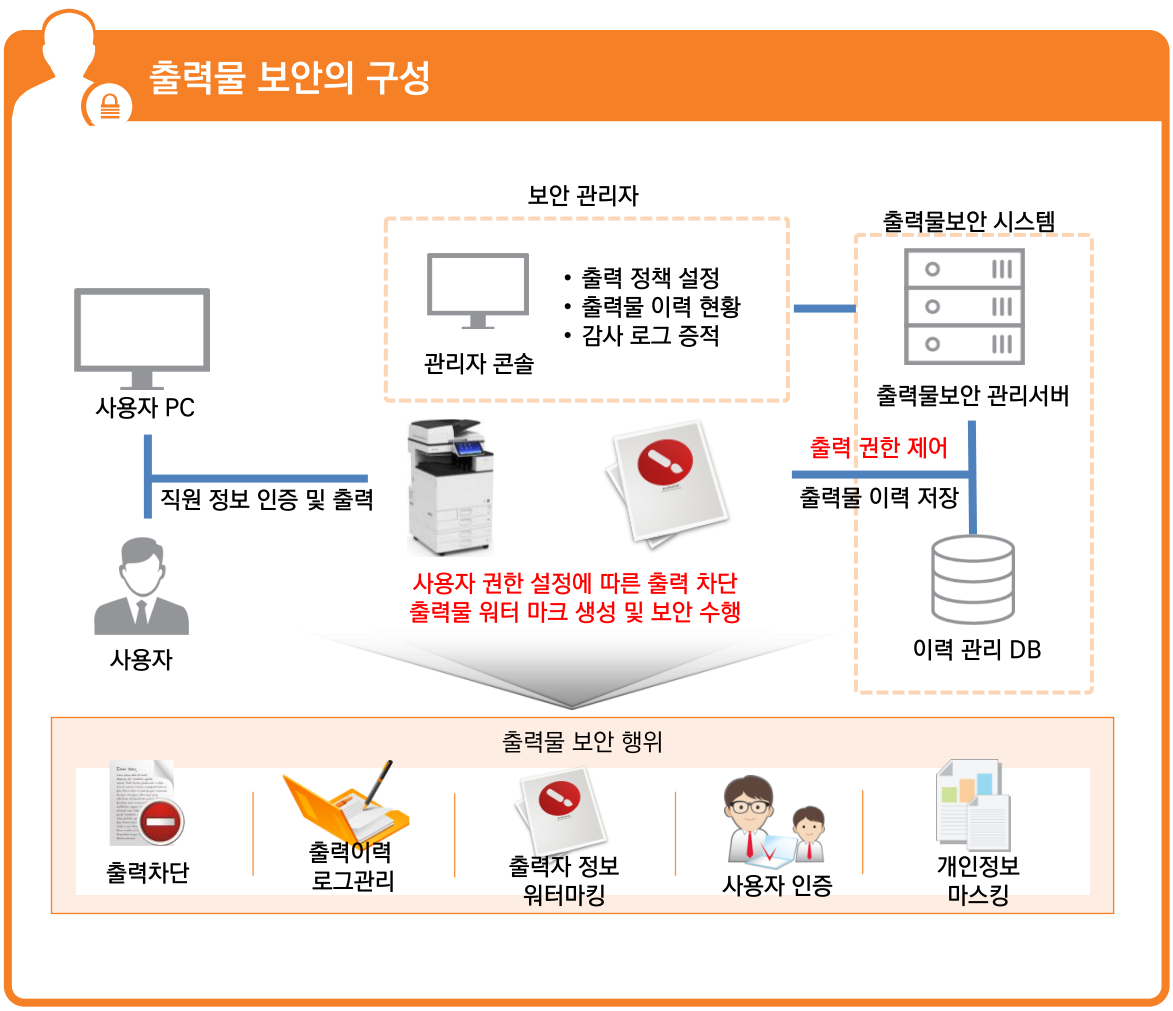
[표 Ⅲ-4. 문서보안 솔루션별 특징]

라. 출력물 보안

A. 솔루션 개념

국내외 정보유출 사례를 보았을 때, 출력물을 통한 기업의 핵심기술자료와 개인정보 유출사고 사례는 과거부터 현재까지 지속적으로 발생하고 있습니다. 출력물 보안 솔루션은 출력물을 통한 정보유출 사고를 예방하고 통제하기 위한 솔루션 입니다. DLP, DRM, 매체제어 등의 보안솔루션을 도입하여 전자매체를 통한 유출방지 체계를 마련 하였다면, 물리적인 프린트물 유출방지를 위해서는 출력 시도에 대한 통제, 출력 이력 및 감사 추적을 통하여 출력물 보안관리를 수행할 수 있습니다. 프린트 보안의 기능은 사용자별로 출력권한을 부여하고 워터마킹이나 마스킹으로 데이터에 대한 제한을 두거나, 출력한 이력을 관리하게 됩니다.

또한, 최근에는 특수 제작된 보안전용지로만 프린트가 되는 프린터(복합기)가 있으며, 위변조가 방지되는 전용용지가 있습니다. 또한 전자감응형 특수용지는 종이의 원재료 내부에 자기형태를 삽입해 외부 유출을 방지하는 솔루션도 상용되고 있습니다.



[그림 Ⅲ-5. 출력물 보안 솔루션 구성]

B. 주요기능

출력물 보안 솔루션은 출력물 보안정책 설정, 출력 통제, 모니터링 및 보고 세가지 기능 영역으로 분류할 수 있습니다. 출력물 통제의 주요영역은 사용자별 출력 권한부여, 워터마크 삽입을 통한 출력물 저작권 보호, 출력 시도에 대한 제어, 출력물 이력 관리와 감사 추적 등의 주요기능이 있습니다.

솔루션별로 주요기능은 큰 차이는 없으나, 최근 솔루션들의 많은 정책이 다양하게 제공되고 있으며, 솔루션을 구축하고자 할 때는 자사의 정책과 매핑될 수 있고, 유연한 정책 설정이 가능한지를 검증해야 합니다. 또한, 개인정보 포함문서 출력 시 프로세스(신청/승인)도 자사정책에 적합한지 확인하고, 관리자가 출력활동에 대한 전체적인 모니터링과 감사 대응이 가능한지도 확인이 필요합니다.

기능영역	주요 기능 내용
보안정책	**출력물 정책 설정** 1 워터마크 삽입 정책 설정 2 사용자 및 파일 별 출력 권한 정책 설정 3 출력물 원본 저장 정책 설정
출력 통제	**출력물 보안 수행** 1 관리자가 설정 한 워터마크(CI, 로고, 인쇄자 정보) 삽입 2 관리자 설정 정책에 근거한 출력물 차단 3 사용자 인증을 통한 출력물 이력 관리 4 개인정보 키워드 탐지를 통한 마스킹 기능
모니터링	**모니터링 및 결과보고** 1 출력물 이력 검색 및 통계 2 출력물 통합 관리 및 감사로그 보고서 제공

C. 솔루션별 특징

출력물 보안 솔루션은 다수의 국내제품이 운영 중에 있으며, 주요기능은 거의 동일하지만, 기존 보안솔루션과의 연동을 통해서 기능확장을 수행하고 있습니다.

개발사	제품명	주요기능	솔루션 특징
파수닷컴	FSP (Fasoo Smart Print)	▪ 출력자 정보, 보안 등급, 경고문구 등 워터마크 종류별 삽입 및 워터마크 디자인 ▪ 윈도우가 지원하는 프린트 드라이버 제공 ▪ Application Hooking 방식으로 전용 작업창 불필요 ▪ 인쇄출력 로그 관리 ▪ 다양한 사용자 관련 설정 ▪ 텍스트 및 이미지 로그관리	▪ 인쇄물 개인정보 검출 ▪ 중요 키워드에 따른 차등적인 보안 적용 가능 ▪ 모바일 인증을 거쳐 원하는 시점 및 특정 장비에서만 인쇄하는 기능
엘아이텍	SECUPRINT (EnterPrise)	▪ 출력물 로그저장 및 검색조회 ▪ 워터마킹 설정 및 보안정책 설정 ▪ 출력물 통계 기능 제공 ▪ 관리자 등급별, 그룹, 사용자 별로 별도의 정책관리 ▪ 출력통제 기능 (출력 매수, 어플리케이션, 특정 프린터, 사용자/부서/전체 출력통제 기능) ▪ 복사방지마크 삽입 기능 ▪ 바코드 생성 기능 ▪ 출력자 정보 삽입	▪ 출력물 원본 이미지/텍스트 저장 및 조회 ▪ 클라이언트 삭제 방지기능 ▪ SSO, DRM 연동기능 제공
와우소프트	Print Chaser v 3.0	▪ 출력물에 대한 출력현황 로그 저장 ▪ 출력물에 회사로고, 출력자 정보, UUID, QR등 워터마크 삽입 (Printer, Application, URL 별 예외가능) ▪ 로그 조회 및 현황 정보 ▪ 관리자 정책 설정 로그 감사 ▪ 실시간 정책적용 및 모듈패치 기능 ▪ 주요 복합기 제조사 운영시스템과 통합 구성으로 운영환경 개선	▪ 출력물 본문 이미지 및 텍스트 저장 ▪ 출력시 실시간 개인정보 탐지 ▪ 개인정보 허용치 초과시 출력 차단 및 승인 결재 워크 플로우 ▪ 빈번한 개인정보 출력시 경고 메시지 알림

개발사	제품명	주요기능	솔루션 특징
컴트루테크놀러지	셜록홈즈 PC정보보안-출력물 보안	▪ 출력제어를 통한 정보 유출 방지 (비인가자/비인가 문서 차단) ▪ 부서, 그룹, 사용자 별 출력 정책 설정 ▪ 실시간 출력 차단 및 감사로그 ▪ 워터마크를 통한 출력물 보호 ▪ 기업에 맞는 워터마크 설정 기능 ▪ 출력자 정보, 패턴 별 개인정보 검출 개수, 차단여부, 출력 일시 등 기록 ▪ 보고서 및 통계 기능	▪ 자사 보안 솔루션 PC스캔 모듈 연동 개인정보 출력 문서 및 파일을 한 에이전트에서 동시 관리 ▪ 출력물 원본 이미지, 텍스트 보장 ▪ 출력물 반출-승인 기능을 통한 원활한 업무 활용
마크애니	Print SAFER	▪ 워터마크(visible invisible), 사용자 정보 삽입 지원 ▪ 출력물의 출력자, 프린터 정보 등 출력물의 유통정보 관리를 통한 추적 및 감사 ▪ 사용자별, 부서별 출력 정책 적용 ▪ 출력 횟수 제한 등 다양한 출력정책 설정 지원 ▪ PCL,PS등 다양한 프린터 드라이버 및 모든 기종 지원 ▪ 관리 웹을 통한 출력 정책, 사용자 관리 및 다양한 이력관리 지원 (문서보안 등과 통합관리 지원)	▪ 출력 이미지 및 텍스트 저장으로 감사로그 제공 ▪ 개인정보 포함 문서의 출력시 출력 신청 및 관리자 승인 절차를 통해 출력물로 인한 개인정보 유출 방지(옵션 제공) ▪ 비인지 워터마크 삽입 및 검출로 중요정보 유출방지

[표 Ⅲ-5. 출력물 보안 솔루션별 특징]

마. 매체제어

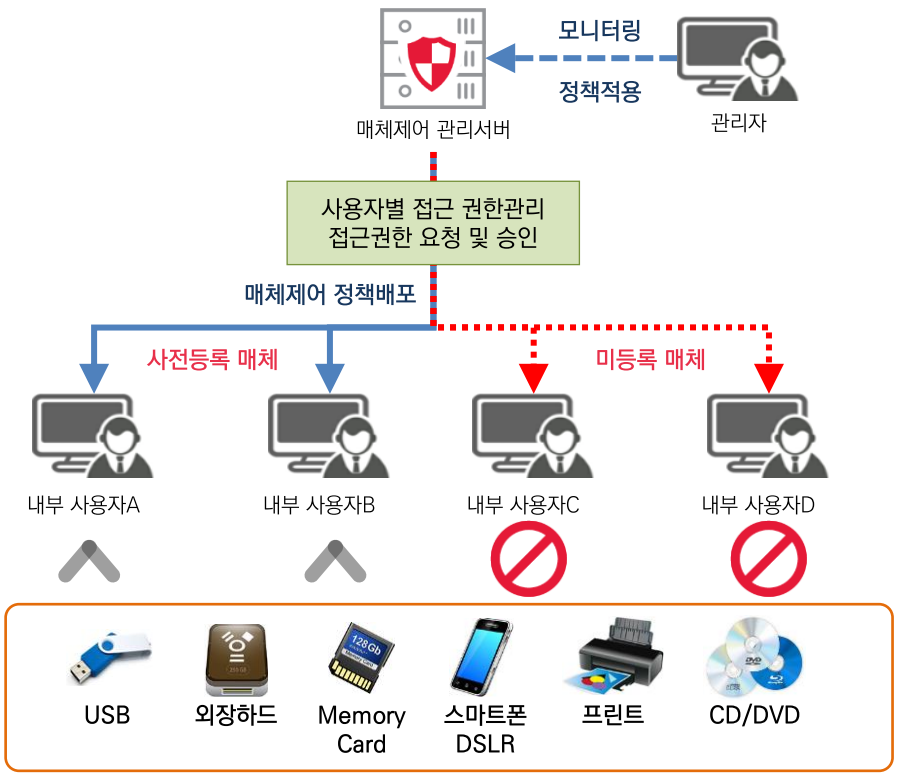
A. 솔루션 개념

매체제어란 USB, CD/DVD, 외장하드, 메모리카드 등의 물리적 매체를 통한 정보유출을 차단하는 솔루션을 말합니다.

최근 기업 내 IT비즈니스 업무의 증가에 따른 다양한 매체 사용량의 증가로 내부정보유출의 빈도도 함께 증가하고 있습니다. 최근 발생하고 있는 보안사고가 외부가 아닌 내부인력으로 인해 발생하고 있으며 그 빈도수와 파급력은 증가되고 있습니다.

이제는 정보보안 솔루션 관점에서 매체제어만의 통제 솔루션보다는 다수의 보안기능이 융합된 End Point 보안솔루션으로 발전하고 있습니다.

매체제어 보안 솔루션의 흐름 및 구성



[그림 Ⅲ-6. 매체제어 솔루션 구성]

B. 주요기능

매체제어 솔루션은 기본적으로 매체제어 정책관리, 매체 차단/실행, 모니터링 및 결과보고 3가지로 구성될 수 있습니다. 그 밖에 제품 별 매체 데이터 암호화, 매체 전용 백신, 도난방지용 설정 등 다양한 기능이 추가적으로 구성되어 있습니다.

매체제어의 상세 주요기능은 주요 포트와 매체의 통제, 주변기기 통제, 데이터 교환 모니터링, 데이터 교환의 기록 및 보고, 승인된 장치의 데이터 전송 시 자동 암호화 처리로 볼 수 있습니다. 매체제어 솔루션 선택 시 대상 OS의 지원환경(windows, mac, RedHet, CentOS, openSUSE, Ubuntu 등)과 관리되는 매체 종류(일반USB, 보안USB, 외장HDD, FDD, CD/DVD, SD Card 등)도 확인이 필요합니다.

기능영역	주요 기능 내용
매체제어 정책관리	**매체사용 정책 관리** 1 인가 및 비인가 매체 설정 2 사용자별 매체제어 여부 설정(시간, 장소) 3 추가기능 적용여부 설정(도난방지, 암호화 등)
매체별 차단/실행	**매체 제어** 1 설정 된 정책에 따른 차단/실행 수행 2 추가기능에 따른 상세 내역 적용 **옵션 기능** 1 도난방지(파일암호화, 패스워드)
모니터링 및 결과보고	**모니터링** 1 비 인가된 매체 사용여부 확인 2 정상적인 사용내역 및 비정상적 사용내역 확인 3 매체제어 통계내역 주기적 보고

C. 솔루션별 특징

매체제어를 위한 솔루션 선택은 회사 내부에서 주로 사용하고 통제가 필요한 매체를 기준으로 선택해야 합니다. 즉, USB, 무선NIC, Mac과 같은 특정 사용여부 등 솔루션 특징을 고려해야 합니다.

개발사	제품명	주요기능	솔루션 특징
Symantec	Symantec Endpoint Protection 14	▪ 네트워크 방화벽 및 침입 차단 ▪ 애플리케이션 및 매체제어 ▪ 메모리 익스플로잇 공격 차단 ▪ 파일 평판 분석 ▪ 첨단 머신러닝 ▪ 에뮬레이션 ▪ 행동 모니터링	▪ 외산 제품으로 인지도 높음 ▪ 대규모의 글로벌 보안위협 인텔리전스 네트워크를 활용 ▪ 단일 관리 콘솔 및 고성능 경량화 에이전트에서 엔드유저의 PC성능 영향도 낮음
컴트루테크놀러지	셜록홈즈 PC정보보안 (매체보안)	▪ 매체이동 차단 – USB메모리, 외장HDD, CD,DVD등 저장매체 차단 – 인증 받은 보안 USB만 사용 허가 ▪ 정책 관리 – 그룹/사용자 별 개별 정책 설정으로 매체에 대한 차단, 허용, 반입 전용 정책을 설정 관리 – 세부 정책을 통한 매체보안 정책 관리 ▪ 로그 기록 – 매체보안 내역 로그 기록	▪ 내용인식/키워드 인식 기반의 개인정보 및 중요정보 매체제어 수행 ▪ USB인증 기능 추가로 사전에 인증 받은 USB에 한하여 사내에서 사용 가능 ▪ 셜록홈즈 PC정보보안 제품을 통하여 다양한 엔드포인트 보안 모듈 연계활용 가능
잉카인터넷	nProtect UMS V3.5	▪ 매체제어 – CD/DVD, FDD, eSATA, FireWire, Bluetooth, USB 등 다양한 매체 제어 ▪ 정책관리 – 중앙관리 서버를 통한 다수의 보안정책 배포 – 조직별, 개인별 매체반출 신청 및 승인자 관리 – 관리자 승인, 사용자 무단 반출 및 예외 사용자 정책 ▪ 중앙관리 – 통합 에이전트 기반 패치, 매체제어, 취약점 분석, 방화벽 관리 및 운영 ▪ 통합 대시보드 제공 및 매체사용 이력 로그 제공	▪ CC 및 GS인증 ▪ 리눅스 환경 지원 ▪ MS Active Directory 연동 ▪ 인사정보 DB 연동

개발사	제품명	주요기능	솔루션 특징
시큐드라이브 (브레인즈스퀘어 2019년 분사)	SecuDrive V3.0	▪ 보안 USB 기능 – 물리적인 유출 방지 및 분실 시 데이터 파괴 – 비밀번호 인증 – AES-256 암호화 – 화이트리스트 접근제어 – 파일 및 클립보드 복사 방지 ▪ 보조기억매체 제어 – USB, 외장 HDD, FDD,CD/DVD등 – 스마트 기기, 스마트 폰, Wireless Lan, Bluetooth 등 ▪ 관리 기능 – 각종 통계 및 Dashborad 기능 – 매체 관리, 에이전트 관리, 정책 관리 – 보고서 작성, 로그 수집, 사용자 관리 기능	▪ CC인증 ▪ 보안USB내 특수 합금 삽입으로 보안게이트 무단 반출 방지
세이퍼존	세이퍼존 보안 USB System (Agent Type)	▪ 보안정책 및 로그 실시간 송수신 ▪ Bad USB 원천 방지 기능 ▪ 보안 USB에 저장된 원본 파일 및 로그를 서버로 전송 시 암호화 통신 지원 ▪ Agent 프로그램 임의 종료 방지 ▪ 매체제어 수행 – USB, 외장 HDD, CD/DVD 등 매체제어 수행 ▪ 분실 도난 시 저장 데이터의 보호를 위한 삭제 ▪ 중앙관리 시스템 – 보안정책 설정 – 로그 및 통계 리포팅	▪ Windows, Mac, Linux , 모바일 OS 등 다양한 운영체제 지원 ▪ 보안 USB 분실 시 데이터의 보호를 위한 삭제 기능 제공 ▪ 사용자 인증 및 식별
안랩	AhnLab V3 Endpoint Security 9.0	▪ USB 제어 – USB 저장 장치 사용, USB 저장 장치 접근 로깅 ▪ 네트워크 제어 – 유선/무선 네트워크, 외장 네트워크 어댑터 ▪ 드라이브 제어 – 디스크 드라이브, 모뎀, 플로피 디스크 드라이브, CD/DVD 드라이브, 스마트 카드 리더 ▪ 기타 장치 제어 – IEEE 1394 (FireWire), PCMCIA 어댑터,적외선 장치, Bluetooth 장치, COM/LPT 포트	▪ CC인증 ▪ 엔드포인트 통합 관리 솔루션으로, 매체제어 뿐만 아닌 악성코드 탐지 차단 및 네트워크 제어 등 다양한 기능 제공

개발사	제품명	주요기능	솔루션 특징
COSOSYS	Endpoint Protector V5.0	▪ 콘텐츠 인식 보호(CAP) – 네트워크상 컴퓨터와 엔드포인트 데이터 제어 – 문서 전송 로그관리 – 정책에 따른 파일전송 및 허용/차단 ▪ eDiscovery – 민감한 보전 데이터(data rest)를 스캔 – 특정파일 유형, 개인정보 또는 사용자 정의, 파일이름, 정규식, HIPPA를 기반으로 스캔설정 – 스캔결과 암호화 및 삭제조치 ▪ 매체제어 – 웹 인터페이스로 사용자의 USB와 포트 제어 – 매체사용정책에 의한 유출 위협 탐지 ▪ 모바일 기기관리(MDM) – Android와 iOS 모바일 외에 MacOS 제어 – 응용프로그램, 네트워크 설정 등을 모니터링과 푸시	▪ CC 인증 ▪ Windows, Mac, Linux 지원 ▪ 30분 이내 설치 및 사용 가능
지란지교소프트	OfficeKeeper V4.0	▪ 이동식 저장매체 – USB, 외장하드, 스마트폰, CD로 복사반출 차단 ▪ 인터넷 파일첨부 차단 – 메일, Cloud, 웹브라우저 등 인터넷 기반 파일첨부 차단 ▪ 소프트웨어 파일반출 차단 – 메신저, 원격제어, 웹하드 등 소프트웨어로 반출 차단 ▪ 무선인터넷 접속 차단 – WiFi, Bluetooth를 활용한 인터넷 우회접속 차단 ▪ 화면캡쳐/공유폴더 차단 – 캡쳐 프로그램, 공유폴더를 활용한 정보공유 차단 ▪ 로그 및 원본 저장 – 모든 파일의 공유/반출 시도에 대한 로그와 해당 원본 파일 조회	▪ CC 인증 ▪ Agent 미설치자 강제 설치 유도 ▪ 업무공유와 편의성을 위한 오피스 메신저 옵션 기능
솔루피아	ESCORT	▪ 정보유출 차단 및 로깅 – 외부저장장치 사용통제 및 쓰기파일 로깅 – 보안USB 저장장치 연계 통제 – 이동통신(Wibro, LTE), 무선통신, 블루투스 통제 ▪ IP 관리 및 사용이력 로깅 ▪ 소프트웨어 라이선스 관리 ▪ 보안 USB(옵션) – 사용자 인증식별, 실시간 암호화 – H/W타입, 분실장치 통제 – 외장하드 주입기능 – 파일 암호화 및 백업	▪ Client PC CPU 영향 최대 5% ▪ 상주 프로세스 메모리 최소화 ▪ 취약점 강화 기능 ▪ S/W라이선스 관리

[표 Ⅲ-6. 매체제어 솔루션별 특징]

바. 패치관리 (PMS)

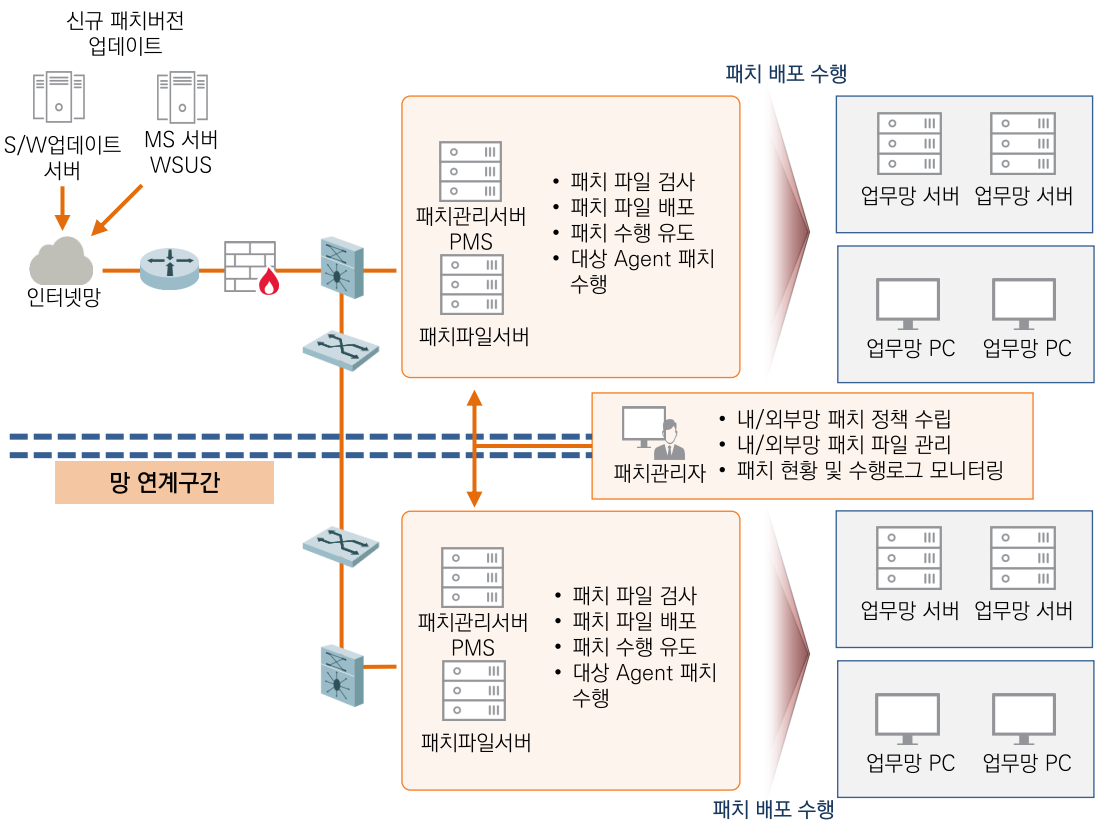
A. 솔루션 개념

패치관리시스템이란, 시스템의 보안취약점을 보완하기 위해 배포되는 Windows 보안 패치 또는 기타 패치파일들에 대하여 원격에서 자동으로 설치 관리해주는 솔루션을 말합니다.

최신의 보안패치를 설치하지 않아서 발생한 보안사고는 모든 산업분야에서 발생하고 있습니다. 이와 같은 취약점을 통해 Malware 및 Ransomware 감염이 증가하고 있으며, 이로 인하여 데이터와 시스템의 파괴, 손실, 금전적 피해, 개인 정보 유출 등의 피해가 지속적으로 발생하고 있습니다.

패치관리시스템은 최신 파일 Update를 위해 패치 설치의 권고/유도를 포함하여 필요 시 강제적으로 설치하도록 관리합니다.

패치관리 시스템 솔루션 구성



[그림 Ⅲ-7. 패치관리 시스템 솔루션 구성]

B. 주요기능

악성코드와 외부 위협으로부터의 방어책으로 패치관리시스템은 기업 내 PC의 윈도우와 주요 소프트웨어의 패치, Update를 일괄적으로 수행합니다. 최근에는 사용자 PC외에 서버에 대한 패치도 함께 대상으로 실행하고 있으며, 해당 패치의 설치현황 결과와 상세보고서를 제공합니다.

패치관리의 주요기능에 대한 필요사항은 대상 PC에 대한 정확한 패치현황을 파악하고, 패치내역의 우선순위가 제공되어야 하며, 패치파일 및 배포파일에 대해 위·변조를 원천적으로 봉쇄해야 합니다. 또한, PMS Agent의 자체 보호, 동작의 안정성, 패치의 무결성도 확보되어야 합니다.

패치작업은 일반적으로 대량의 PC에 일괄 배포하기 때문에 관리자의 설치와 운영 편의성이 중요하며, 그룹관리, 예약작업, 타 솔루션과 연동여부 등이 원활해야 합니다.

기능영역	주요 기능 내용
패치 관리 정책 설정	**패치 정책 설정** 1 사용자별/그룹별 패치정책 2 패치 알림, 유도 및 강제 패치 배포정책 3 패치 스케줄
패치 배포 및 수행	**패치 수행 및 롤백** 1 Windows OS에 대한 패치 기능 2 어플리케이션(Adobe, 한글, MS 오피스 등) 취약점 권고 패치 3 패치 롤백 및 백그라운드 설치 4 Console 을 통한 SW 등록 및 배포 5 패치 미수행 에이전트 확인
모니터링 및 결과	**모니터링** 1 패치 수행 현황 정보 2 기업내 소프트웨어 현황 정보 3 통계 및 감사 보고

C. 솔루션별 특징

최근 패치관리시스템은 단순 패치관리를 수행하는 제품에서, SandBox[1] 분석 등 신규 기술을 통해 패치 파일에 대한 2차 검증을 수행하는 강화된 보안환경으로 발전하고 있습니다. 또한, 백신 및 엔드포인트 보안제품과 연계하여 보편적인 패치관리 기능에서 통합 보안관리 플랫폼으로 진화하고 있습니다.

패치관리시스템의 솔루션 및 제품별 특징을 소개합니다. 시스템 구축이 필요한 회사의 사용자 규모와 패치 영역을 확인 하시고 제품 구축에 참고 바랍니다.

개발사	제품명	주요기능	솔루션 특징
아이티스테이션	TA-PRS	▪ 인터넷 차단에 의한 에이전트 자동 배포 및 패치 관리 ▪ PKI 및 BIO 인증에 의해 검증된 파일의 등록 ▪ 내부정책에 따른 정책 설정 기능(스케쥴, 적용대상) ▪ 패치랩 구축 신규 패치에 대한 신속한 검증 및 롤백 지원 ▪ MS운영체제 및 어플리케이션 자동 패치 ▪ 실시간 리포트 및 Dashborad 지원 ▪ 비업무용 SW 설치 PC 인터넷 차단 ▪ 지원중단 OS 사용자 인터넷 차단	▪ 비인가 변경 데이터 제거 ▪ 장애로 인한 시스템 재기동 시 저장된 원본 시스템으로 복원 ▪ 랜섬웨어 및 악성 행위 보호
안랩	AhnLab Patch Management	▪ 자체 패치랩을 통한 패치 검증 수행 및 별도 관리 지원 ▪ 취약점 권고 패치 자동적용 지원 ▪ OS 및 SW 10여 종 패치 지원 ▪ 백그라운드 자동 설치 ▪ SW / HW 현황 파악 관리 ▪ 다수의 PC 및 서버에 대한 소프트웨어 패치 일괄 적용 ▪ 운용 현황 파악 Dashboard 제공 ▪ 사용자 현황 요약 및 상세 보고서 제공 ▪ 패치 진행 상태 실시간 모니터링	▪ CC인증 ▪ 다수의 보안 솔루션에 대한 연계 정책 및 대응 ▪ 자사 엔드포인트 보안 플랫폼과 연계 통합관리
이스트시큐리티	알약 패치관리 (PMS)	▪ 대시보드를 통한 패치 운용 현황 확인 ▪ 미설치 패치 및 사용자에 대한 순위 제공 ▪ MS OS 및 제품군 외 30여종의 다양한 SW 패치 제공 ▪ PC 환경 및 상태별 맞춤 패치 ▪ 패치 종류, 설치 주기/환경 등 그룹별 맞춤 정책 설정 ▪ 패치 롤백, 패치 적용/금지 시간 등 다양한 설치 옵션 제공 ▪ 패치 및 에이전트 별 통계 보고서 제공	▪ CC인증 ▪ 자체검증 및 테스트 후 패치 적용으로 안정성 확보 ▪ 알약 제품군 구매시 별도의 구축 없이 라이선스 구매만으로도 사용 가능 ▪ 패치 스케쥴 관리 옵션 제공

1) Sandbox : 외부로부터 들어온 위협되는 프로그램이 보호된 영역(아이들이 안전하게 놀 수 있는 모래밭에서 유래)에서 코드를 동작해 시스템이 부정하게 조작되는 것을 미리 확인하여 위협을 방어할 수 있도록 하는 보안 형태

개발사	제품명	주요기능	솔루션 특징
하우리	ViRobot Patch management System 2.0	▪ 대시보드를 통한 패치현황 점검 ▪ 정책 운영 및 서버 운영 현황 파악 ▪ 운영체제 및 주요응용프로그램 보안패치 ▪ 맞춤 배포 정책 설정 가능 ▪ 백그라운드 파일 배포 가능 ▪ 패치 현황 보고서 제공 ▪ 원격명령 및 정책설정 등 보안감사 보고서 제공 ▪ 관리자 공지 메시지 전송 기능	▪ CC인증 ▪ 내부 통신 및 암호화 강화 ▪ 무결성 탐지 기능 ▪ 관리자 지문정보를 이용한 배포 파일 제작 ▪ 파일 위·변조 차단 및 레지스트리·프로세스 보호 같은 자체 보호
엠엘소프트	TCO!hotpatch	▪ 중요패치에 대한 자동배포 설정 ▪ 사용자 PC의 언어를 자동으로 판단 스마트한 패치 배포 ▪ 윈도의 패치의 경우 MS Update와 동일한 매커니즘으로 설계된 자체 패치 클라우드 시스템 이용 ▪ 56kbps의 낮은 속도의 네트워크에서도 안정적인 배포 가능 ▪ 패치 문제 발생시 롤백 가능	▪ 국내 및 국외 중국, 말레이시아 등 PC를 보유한 기업에서 운용 ▪ 보안 패치 및 일괄 강제 설치 ▪ 패치 배포 후 시스템 재시작, Push, PULL 스케줄 등 다양한 패치 적용 지원
에스지에이솔루션즈	PatchChaser 2.1	▪ 기업 환경에 맞는 정책 설정 ▪ 패치관리 소프트웨어 및 운영체계에 대한 최신 보안 업데이트 지원 ▪ 백그라운드 패치 및 롤백 지원 ▪ 전자서명 및 암호화 채널을 통한 패치 배포 ▪ 통합관리 (네트워크제어, 파일시스템, 매체제어 등) ▪ 단순한 UI 및 GUI로 관리 접근성 향상 ▪ 패치 현황 보고 ▪ 자산 현황 보고	▪ CC인증 ▪ SGA 특허기술(등록번호 10-0894813)에 의한 지능형 파일 분배 기법을 통한 신속한 보안 패치 ▪ 듀얼의 별도 사전 검증체계로 패치 검증

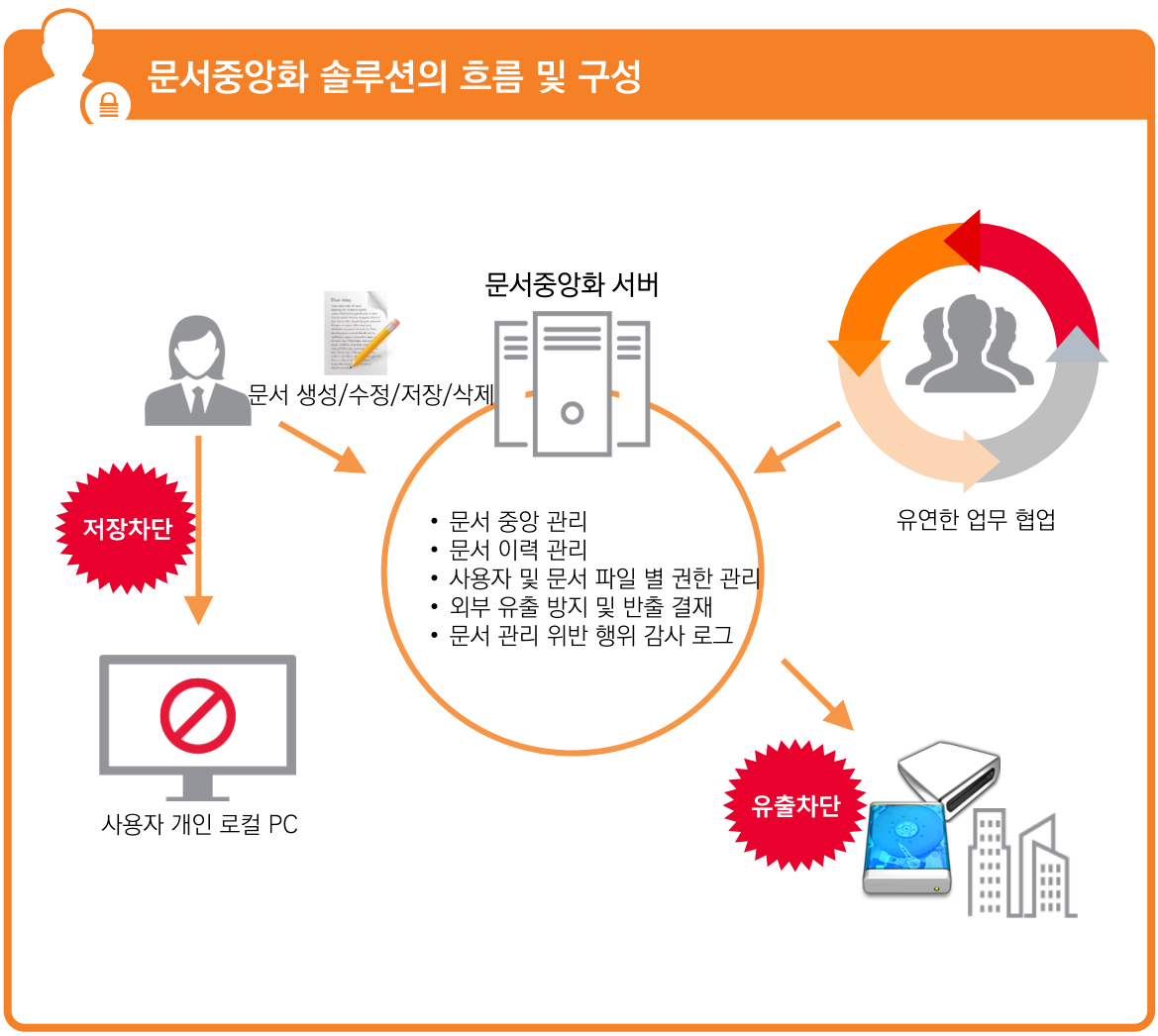
[표 Ⅲ-7. 패치관리 솔루션별 특징]

사. 문서중앙화

A. 솔루션 개념

일반적으로 기업 내부에서 업무를 수행할 때 사용자 각각의 개인 PC에서 업무를 보며 문서를 작성합니다. 이와 같이 개인 각각의 PC에 문서가 산재해 있는 경우는 외부로 문서와 중요정보가 유출될 가능성이 높습니다. 이에 대한 방안으로 문서를 중앙서버에서 관리하고 특정 사용자에게만 권한을 부여하여 정보유출과 파일의 안정성에 대한 보안을 강화할 수 있는 솔루션이 문서 중앙화 솔루션 입니다. 최근 랜섬웨어 사고가 증가함에 따라 많은 기업들이 문서중앙화를 도입하고 있습니다.

문서중앙화 솔루션 도입에 따른 효과는 문서자산 관리체계를 개인이 아닌 중앙에서 관리자에 의해 관리되며, 문서 통합 및 검색관리, 유출방지, 통합적인 문서 암호화 및 개인정보 파일관리, 사내 협업 시 문서 공유 용이, 매체를 통한 유출 차단, 문서를 중앙서버에 저장함으로 악성코드나 랜섬웨어와 같은 위협으로부터 안정성을 보장 받을 수 있는 이점이 있습니다.



[그림 Ⅲ-8. 문서중앙화 솔루션의 흐름 및 구성]

B. 주요기능

문서중앙화 솔루션은 기본적으로 문서 권한 정책 관리, 문서 관리, 보안 위협 관리, 감사 로그 관리 네 가지 영역으로 나누어 볼 수 있습니다. 대부분의 문서중앙화 솔루션은 개인PC에서 문서중앙화 서버에 접근하여 문서 작업을 수행하기에 정보유출방지(DLP) 기능과 문서 중앙화 기능이 통합되어있는 것이 특징입니다. 또한 문서가 한곳에 집중되어 관리되기 때문에 랜섬웨어와 같은 위협으로부터 접근 차단 기능 또한 중요한 기능이라 할 수 있습니다.

문서중앙화는 사용자의 PC자료를 중앙서버로 자동이관 및 저장하고, 내부자료가 로컬PC에 저장되지 않도록 통제하는 기능과, 서버 및 전송구간에 암호화를 적용하여 자료의 유출에 대한 보안을 강화하며, 랜섬웨어 감염과 사용자 실수 또는 임의 변경과 삭제에 대한 복원기능이 있습니다.

기능영역	주요 기능 내용	
문서 권한 정책 관리	문서 보안 정책 설정	1 파일 및 사용자별 문서 접근 권한 설정 2 로컬 저장 및 외부 반출 프로세스 정립
문서 관리	효율적인 문서 관리	1 문서 변경 버전 이력 관리 2 업무 공유 폴더 및 파일 관리 3 문서 백업
보안 위협 관리	문서 보안 관리	1 접근 권한 정책에 맞춘 파일 및 폴더 통제 2 로컬 PC 저장 차단 3 외부 반출 문서 승인 결재
감사 로그 관리	감사 로그	1 문서 변경 이력 로그 기록 2 보안 정책 위배 행위 로그 기록 3 문서 현황 모니터링 및 디스크 용량 관리

C. 솔루션별 특징

최근 효율적인 문서관리의 측면과 DRM과 DLP 솔루션의 대체제로 떠오르며 많은 기업에서 도입을 진행하고 있습니다. 또한 랜섬웨어와 같은 악성코드, 보안 컴플라이언스 충족에 유용한 솔루션으로 인정 받고 있습니다.

개발사	제품명	주요기능	솔루션 특징
액츠솔루션	문서중앙화	▪ PC저장금지 및 DLP 기능 - PC에서 저장금지, 온라인 첨부 차단, 인쇄통제, 프린터 워터마킹, 화면캡쳐방지, 클립보드 복사방지 기능 제공 ▪ 문서중앙화 - 윈도우 탐색기에서 바로 사용 가능한 기능 - 동시 편집 시 문서유실 방지 기능 제공 ▪ 반출 시 결재 기능 ▪ 문서 공유 ▪ 랜섬웨어 차단 기능 - WhiteList 정책을 통해 랜섬웨어를 차단	▪ DLP, DRM, 문서중앙화 통합기능 ▪ 윈도우탐색기 바로가기
사이버다임	Cloudium	▪ 미등록 프로그램 차단 - 사전에 허용된 프로세스만 접근 가능한 화이트 리스트 방식으로 랜섬웨어를 차단 ▪ 자동 백업 - 정해진 시간에 데이터를 자동으로 백업하여 데이터 손상 대비 ▪ 문서 암호화 - 중앙서버 내 모든 문서는 암호화되어 저장 ▪ 중앙 정책 관리 - 각각의 문서 및 폴더 6단계 접근권한 제어 - 외부 반출 문서의 승인 프로세스 적용 ▪ 문서 유출 경로 차단 - 서버에 있는 문서는 외부 저장 매체로 저장 불가 - 중앙화 정책에 따라 우회적인 유출행위 차단	▪ 파일 수정은 가상보안영역인 샌드박스 내로 제한하고 중앙서버 내 직접 수정은 차단 ▪ 스마트워크 환경 구성 ▪ 인쇄 및 웹메일/메신저 유출 차단
파수닷컴	Wrapsody	▪ 문서 보호 - 랜섬웨어 및 문서 유출 차단 ▪ 문서 버전 관리 - 산재된 문서를 하나의 문서로 통합 관리 - 자동 동기화를 통한 최신 버전 문서 관리 - 문서 백업 및 복구 지원 ▪ 현황 관리 - 문서의 사용횟수 및 참여자 활동 내역 파악 - 문서 실시간 점검	▪ 모든 문서의 자동버전 관리 및 동기화 ▪ 디지털 문서 최신 상태 유지 ▪ 문서별 의견 남기기 기능 지원

개발사	제품명	주요기능	솔루션 특징
이스트시큐리티	SecureDisk	▪ 저장 매체 차단 및 프로그램 접근 제한 – 로컬디스크, USB 등 저장 매체로의 저장 원천 차단 – 서버 내 문서는 관리자가 지정한 프로그램만 접근 가능 ▪ 캡쳐, 출력 차단 및 온라인 유출 차단 – 화면 캡쳐, 복사 및 붙여넣기, 문서 출력 등 제어 – 웹메일, 아웃룩, 메신저, 웹하드 등 온라인을 통한 파일 첨부 및 유출 차단 ▪ 업무 효율성 극대화 – 모든 문서에 대한 버전 관리 및 복원 가능 – 조직별, 프로젝트 별 원활한 파일 공유 ▪ 다양한 로그 관리 – 사용자의 모든 작업 내역과 파일 유통 경로 조회 – 인가되지 않은 작업 또는 유출 시도에 대한 로그 제공 ▪ 자료 반출 프로세스 – 자체 탑재된 반출 시스템 제공, 상급자 승인 후 메일 또는 USB를 통해 파일의 외부 전달 가능	▪ 서버 내 알약 for Linux가 포함되어 악성코드로 인한 시스템 장애 사전방지 ▪ 자가보호기능 적용 ▪ 윈도우 탐색기 인터페이스를 통해 사용자에게 기존과 동일한 업무 환경 제공 ▪ 모바일 뷰어 지원
넷아이디	ClouDoc	▪ 기본모듈 – 문서 버전 관리 및 사용 중 파일 자동 잠금 – 폴더 관리자에 의한 권한, 용량 관리 게스트 ID 기능 – 폴더 공유 / 문서링크 ▪ DiskLock – 랜섬웨어, 로컬저장 차단, 반출 절차 및 디바이스 통제 ▪ Disklock Plus – 화면 캡쳐, 인쇄, 클립보드 복사 차단 – 인쇄 로그 및 프린트 워터마크 제공 ▪ 검색 엔진 – 다양한 파일 포맷, 메타 정보, 스캔 문서 검색 ▪ PC 백업 – 즉시/스케쥴링 백업 – 무결성 확인 및 복원 기능 제공	▪ 네트워크 락 기능제공 – 내부망, 외부망 모드 – 망간 자료 교환 ▪ 악성코드 및 랜섬웨어 차단 ▪ OneAgent 통합 환경
소프트캠프	MAXEON	▪ 윈도우 탐색기를 통한 ECM 접근 – ECM과 연계하여 생성/수정/버전업/삭제/잠금/자금해제 등의 ECM 기능을 동일하게 지원 ▪ 로컬 PC 보안 드라이브 제공 – 임시 파일(cache) 저장소 역할 및 암호화된 보안 드라이브 제공 ▪ 문서 저장 통제 기능 – 사용자의 로컬 PC로의 문서 저장을 차단하고 ECM로 강제로 저장, 라이브 내의 기업 자산 보호를 위해 이동/복사 원천 차단 ▪ 다양한 시스템 환경 지원 – ECM, PLM, EDMS, File Server(NAS) 등 ▪ 웹 기반 업무시스템과의 연동을 통해 ECM 데이터의 안전한 유통 지원	▪ 로컬 PC 보안 드라이브 제공 ▪ 웹 기반 업무 시스템 ▪ 지정파일의 url path 파일 지원

개발사	제품명	주요기능	솔루션 특징
엑스소프트	PC문서 중앙화 – rGate	▪ 사용자 편의 기반의 문서중앙화 ▪ 문서 버전 및 이력관리 ▪ 네트워크 드라이브 기반 문서중앙화 ▪ 타부서와의 편리하고 효율적인 협업/문서공유 지원 ▪ 문서 유출 및 분실 방지를 위한 보안기능	▪ Real Network 드라이브 ▪ 로컬드라이브로 다운로드 불필요 (문서열람 및 작성, 압축풀기, 동영상 재상, mp3 재생 등을 수행)
	서버 문서 중앙화(EiR)	▪ 문서 암호화 ▪ 자료 분산/복제 관리 ▪ 통합 검색 ▪ 표준 인터페이스 API ▪ 멀티파일 Upload Component ▪ 다양한 통계현황 제공	▪ 데이터 통합관리 ▪ 고가용성 클러스터링 환경 구성 지원 ▪ Java 기반 표준 Architecture로 다양한 운영환경 지원

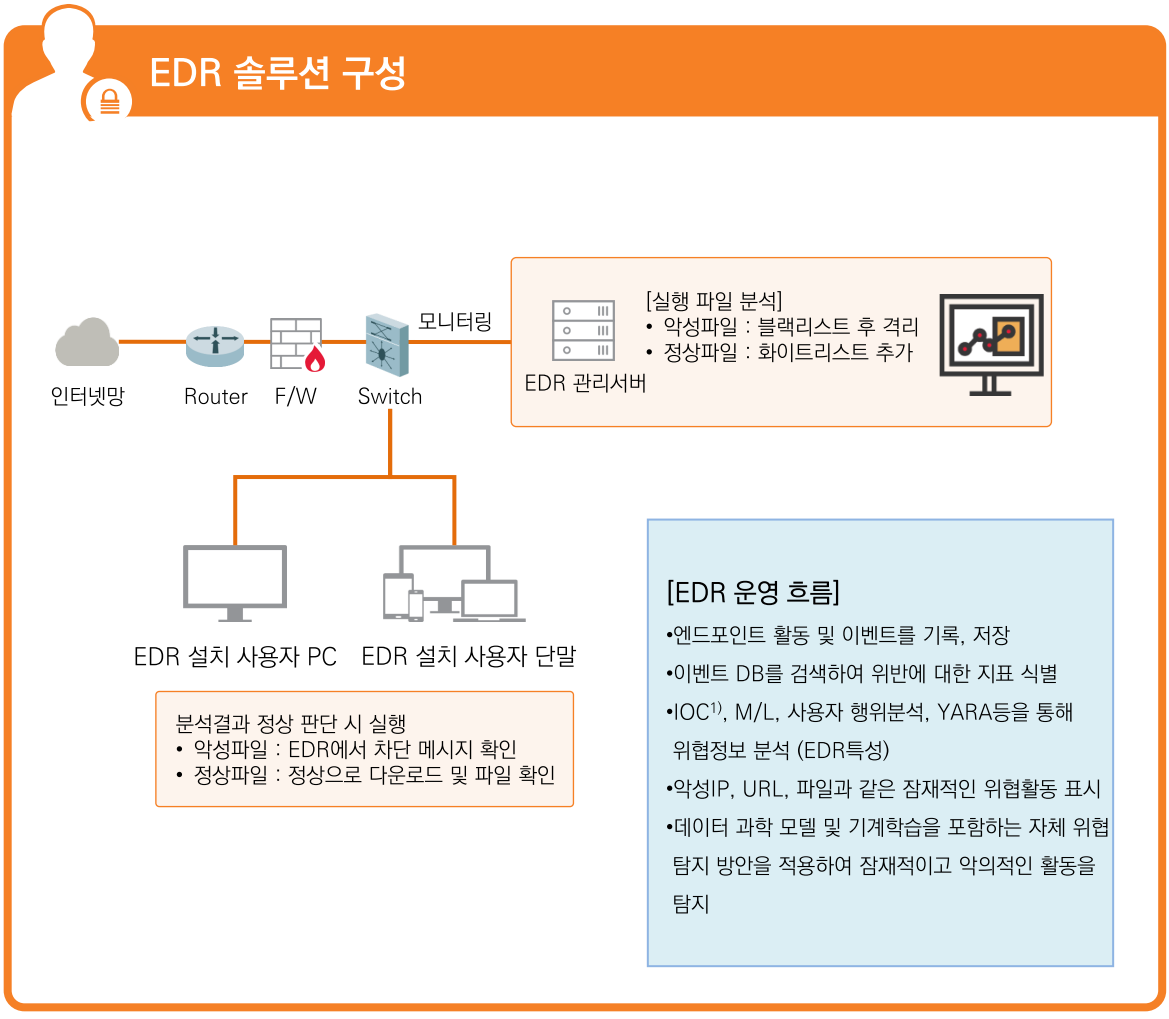
[표 Ⅲ-8. 문서중앙화 솔루션별 특징]

아. EDR

A. 솔루션 개념

EDR(EndPoint Detection & Response)은 엔드포인트에서 행위기반으로 시스템의 위협행위를 탐지하고 대응하는 솔루션입니다. 가트너의 정의에 따르면, 엔드포인트 시스템 레벨의 동작을 기록, 저장하고 의심스러운 시스템 동작을 탐지하여, 상황에 맞는 정보를 제공 및 악성활동을 차단하고 영향을 받는 시스템을 복원하기 위한 개선안을 제공하는 다양한 데이터 분석 기술을 사용하는 솔루션이라고 정의 했습니다.

EDR은 일반적인 안티바이러스 시그니처로 차단하기 어려운 알려지지 않은 위협분석과 탐지를 할 수 있는 보안기술이며, 랜섬웨어와 지능형지속공격(APT)등 고도화된 보안위협에 효과적으로 대응 할 수 있는 강점이 있습니다.



[그림 Ⅲ-9. EDR 솔루션 구성]

1) IOC (Indicator of Compromise) : 사이버 공격의 증거(Source IP, URL등)의 유형을 지표화하여 침해사고 대응에 사용하기 위하여 공통화하여 공유하는 분석 자료

B. 주요기능

EDR은 사용자 단말에서 행위기반 악성코드 탐지로 알려지지 않은 위협정보에 대한 분석으로 신속한 대응이 대표적인 기능입니다. Zero-Day 공격에 효과적, 원천적으로 대응이 가능하도록 구성되어야 하며, 네트워크를 우회하여 유입되는 악성코드에 대한 실시간 탐지 기능과 데이터 및 시스템에서 멀웨어 검색기능이 있어야 합니다.

또한, 관리자의 실시간 대응력 확보와 모니터링을 위한 기능도 포함되어야 합니다. 위협이 발생할 때와 기기손상 및 Resource 과부하가 발생할 때 관리자에게 경고 알림이 있어야 하고, Detect 현황, EndPoint 분석현황 등을 실시간으로 모니터링 할 수 있는 View가 제공되어야 합니다.

기능영역	주요 기능 내용
예측(Predict)	**보안위협 예측** 1 기본 보안태세 (Baseline Security Posture) 2 위협예측 (Anticipate threats) 3 위험평가 (Risk Assessment)
탐지(Detect)	**악성코드 탐지** 1 사고탐지 (Detect Incidents) 2 사고포함 (Contain Incidents) 3 위험확인 및 우선순위 지정 (Confirm and Prioritize Risk)
방어(Prevent)	**탐지결과 방어활동** 1 시스템 강화 (Harden System) 2 시스템 격리 (Isolate System) 3 공격 방지 (Prevent Attacks)
대응(Respond)	**대응절차** 1 치료 (Remediate) 2 Design Policy change 3 사건조사 (Investigate incidents)

C. 솔루션별 특징

최근에는 EDR을 보안업체 벤더에서 사용자 단말 기준으로 시장을 활성화하고 있습니다. EDR은 엔드포인트와 지능형 공격에 대한 특화된 보안 기능을 요구하지만 아직은 EDR로서 부족한 수준으로 판단됩니다. 2019년 02월에 (사)한국침해사고대응팀협의회와 (사)한국CPO포럼에서 발표된 Security Consumer Report〉-EDR(Endpoint Detection & Response)솔루션 내용으로 솔루션 특징을 기술하였습니다.

개발사	제품명	주요기능	솔루션 특징
Cybereason	Cybereason EDR	▪ 상관분석 및 머신러닝을 통한 이상행위 탐지 및 대응 ▪ 엔드포인트 데이터 수집 및 위협 분석 ▪ 시각화 대시보드 ▪ 행위분석 엔진 ▪ 빅데이터 분석 가능 ▪ 파일리스 공격 탐지 및 대응 ▪ 엔드포인트 격리 ▪ 덤프 기능 제공 ▪ Known/Unknown 공격 탐지 및 대응	▪ 공격 라이프 사이클(사이버 킬체인)에서 위협의 구체적 탐지 및 대응
Symantec	Symantec Endpoint Detection and Response	▪ 머신러닝 및 행위기반 분석 가능 ▪ Synapse 기술을 통한 상관관계 분석 ▪ 파일리스 공격 탐지 및 대응 ▪ Known/Unknown 공격 탐지 및 대응 ▪ 리포트 및 대시보드 ▪ 엔드포인트 억제 및 격리 ▪ 덤프 기능 제공	▪ 엔드포인트 활동 중단 없이 기록 및 침해사고 재연 보장
엔피코어	ZombieZERO EDR	▪ 패턴 풀링 기능을 통한 상관분석 ▪ 동적 분석을 통한 신종 위협 탐지 ▪ 파일리스 공격 탐지 ▪ 행위 분석 기능 ▪ 단말 격리 기능 ▪ Known/Unknown 공격 탐지 및 대응 ▪ 의심 파일 실행 보류 ▪ 대시보드 및 리포팅	▪ 교육부 YARA Rule 연동
지니언스	Insight E	▪ IOC 침해사고 지표 탐지 ▪ 머신러닝을 통한 이상행위 탐지 ▪ Known/Unknown 공격 탐지 및 대응 ▪ 행위기반분석(XBA) 엔진 제공 ▪ YARA 위협 탐지 ▪ 시각화 대시보드 및 리포트 ▪ 단말 네트워크 격리 ▪ 파일리스 공격 탐지 ▪ 덤프 기능	▪ RestFul API 제공 ▪ 파일 유입 경로 및 상세 내용 제공 ▪ 자체 인텔리전스 서비스 EcoSystem 제공
Trendmicro	Apex One	▪ 파일리스 위협 및 이상행위 탐지 및 대응 ▪ 자사 샌드박스(Deep Discovery Analyzer)장비 연동을 통한 분석 ▪ Known/Unknown 공격 탐지 및 대응 ▪ 자사 APT 장비 연동을 통한 상관관계 분석 ▪ 대시보드 및 리포트 기능 제공 ▪ 악성코드 탐지	▪ SaaS형태 및 On-Premise 구축 환경 제공 ▪ 자사 다양한 보안 장비 연계를 통한 다양한 분석 기능 제공

개발사	제품명	주요기능	솔루션 특징
Fireeye	FireEye Endpoint Security	▪ 지능형 공격 및 해킹에 대한 위협 탐지 및 대응 ▪ 센서를 통한 정보 수집 ▪ 머신러닝 분석 기능 제공 ▪ 시그니쳐 기반의 AV 엔진 ▪ 행동 기반의 Exploit guard 엔진 ▪ IOC 침해 지표를 통한 탐지 ▪ 대시보드 및 리포트 기능 제공 ▪ Known/Unknown 공격 탐지 및 대응 ▪ 단말 및 악성파일 격리 제공	▪ FireEye Intelligence 정보 Update ▪ APT 공격에 대한 효율적인 탐지 및 대응
Paloalto	XDR	▪ 네트워크 IPS 공격 탐지 기술 제공 ▪ Known/Unknown 공격 탐지 및 대응 ▪ 평판 데이터를 통한 탐지 ▪ 파일리스 공격 탐지 및 대응 ▪ 행위기반 분석 제공 ▪ 시스템 덤프 기능 제공 ▪ 파일 및 엔드포인트 격리 기능 제공 ▪ 대시보드 및 리포트 기능 제공	▪ AI를 통한 엔드포인트 및 네트워크 학습 및 분석 ▪ 자사 AutoFocus 인텔리전스 서비스

출처 : 〈Security Consumer Report〉-EDR(Endpoint Detection & Response)솔루션. 2019.02 (사)한국침해사고대응팀협의회, (사)한국CPO포럼

[표 Ⅲ-9. EDR 솔루션별 특징]

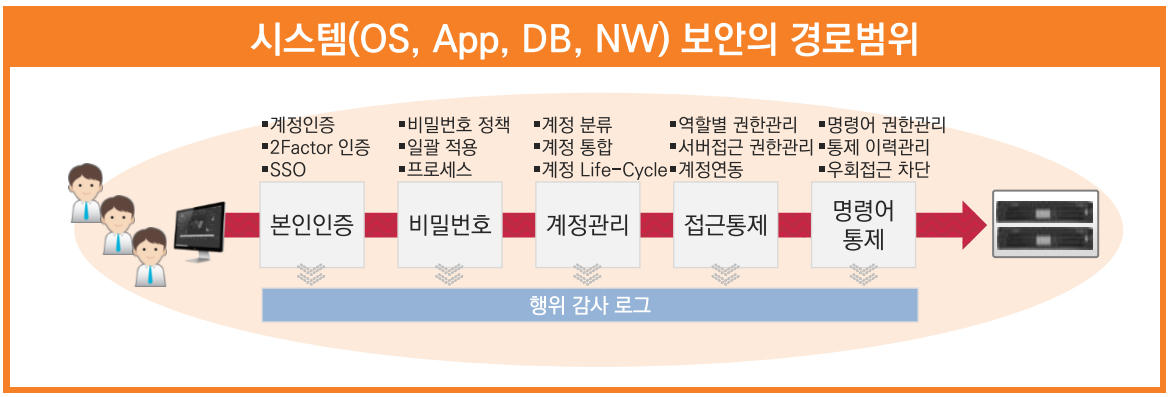
Part 2

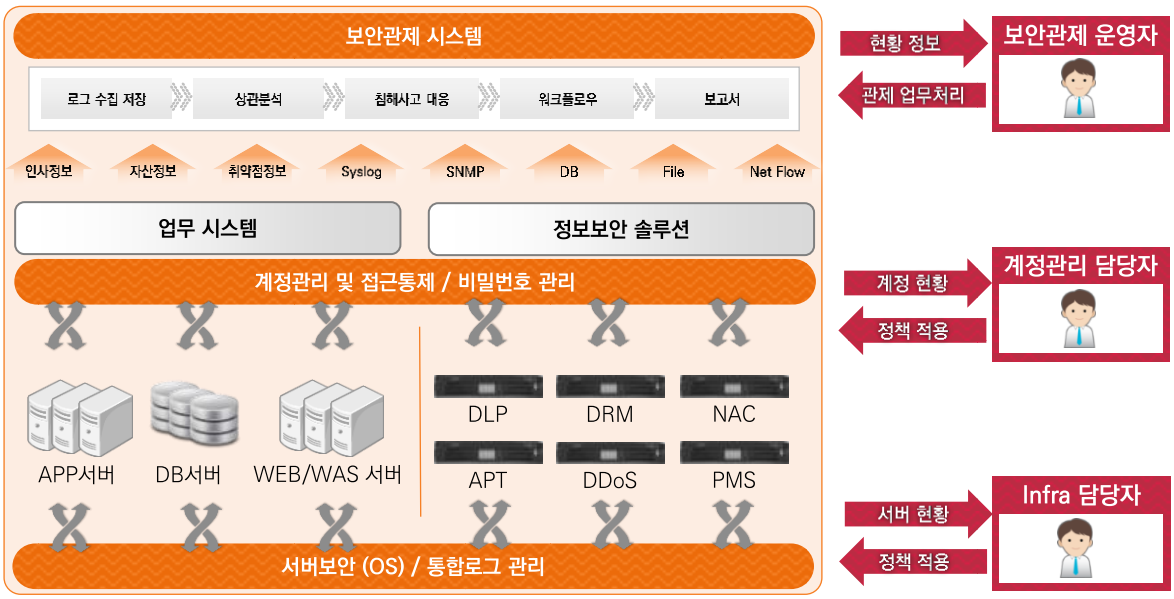
시스템 보안

1) 시스템 보안 개념

시스템 보안은 시스템에 접근 가능한 사용자의 파일, 폴더, 장치의 제어를 통제하는 기능입니다. 시스템 보안의 주요 6가지 주제는, 계정관리와 비밀번호 관리, 일정시간 동안 세션을 유지하는 세션관리, 시스템 네트워크에서 다른 시스템으로부터 접근을 통제하는 접근제어, 사용자별로 부여된 권한으로 정보자산에 접근하는 권한관리, 모든 접속 기록 및 행위를 관리하는 로그관리, 시스템에 대한 결함을 체계적으로 관리하는 취약점 관리로 볼 수 있습니다.

본 가이드에서의 시스템 보안 영역이란 업무서버, DB서버, 보안장비 서버 등 사용자 단말이 아닌 시스템 서버 기준의 정보보호 솔루션을 말합니다. 본 장에서는 시스템 보안의 S/W 부분을 중점으로 설명 드리며, 관련된 보안솔루션에 대한 특징으로 소개하겠습니다.





[그림 Ⅲ-10. 시스템 보안 영역]

2) 보안 영역별 특징

시스템 보안의 주요 6가지 주제를 기반으로 영역별 보안솔루션은 서버와 DB의 계정관리 및 접근통제, DB서버에 등록된 데이터의 암호화, 서버 OS자체의 보안관리 영역, 서버 접근 시 비밀번호를 정책별로 통합관리 하는 비밀번호 관리, 서버에 대한 접근, 행위 결과의 전체 로그 통합관리, 보안솔루션의 로그분석을 통한 보안관제 솔루션으로 구분하도록 합니다.

구분	보안솔루션 영역	목적	일반 주요기능	최신기술 및 특징
1	계정관리 및 접근통제	시스템 계정(ID)의 생성, 변경, 삭제의 Life-Cycle 관리 자동화와 Workflow 기반의 전자결재를 통해 접근권한을 관리하여, 서버접근 권한 통제	▪ 계정관리 Life-Cycle 정책관리 ▪ 사용자 인증 ▪ 시스템 접근 권한 ▪ 시스템 명령어 통제 ▪ 시스템 작업 로그/감사	▪ 초기 분산된 계정관리 중앙 집중식 통합 및 계정유형 정의 ▪ 우회접근 차단을 위한 차별화 모듈 ▪ 비정상적인 계정 파악/제거 보안 수준 향상
2	DB암호화	DB내에 중요 데이터를 암호화하여 정보유출에 대하여 근원적으로 데이터를 보호하기 위함	▪ 알고리즘을 통한 암호화 기술적용 ▪ DBMS 유형별 암호화 적용 ▪ 로깅 및 감사기능 ▪ 접속통계 보고서	▪ 칼럼 암호화 방식 (API방식, Plug-In방식, Proxy방식) ▪ 블록 암호화 빙식 (TDE방식, 파일 암호화) ▪ 암호 알고리즘 (SHA-256/384/512 및 키 길이 128bit 이상의 AES, TDES, SEED, ARIA 등)
3	서버보안	운영체제 보안솔루션을 통해 서버에 존재하는 다양한 형태의 위협을 보안기능을 통해 방지	▪ 관리자 권한 분리 ▪ 계정관리 및 로그인 통제 ▪ 불법 명령어 통제 ▪ 보안정책관리 ▪ 보안감사 및 보고서	▪ Access 정책에 의한 서버 OS 접근통제
4	비밀번호관리	최고 권한 계정(root, 관리자, 공용 계정)과 사용자의 패스워드를 주기적, 일괄적으로 변경하고 프로세스를 통하여 권한이 부여된 사용자에게 패스워드를 생성/발급하여 비밀번호 관리의 보안성과 통합을 위함	▪ 패스워드 정책정의 ▪ 패스워드 주기적/일괄변경 ▪ 패스워드 신청/승인 ▪ 감사로그 및 보고서	▪ 차별화된 암호화 방식적용 ▪ 2차 인증방식으로 접근 통제 강화
5	통합로그관리	이기종 시스템 로그통합을 통한 컴플라이언스 준수 및 로그분석 대응	▪ 로그 수집 및 저장 ▪ 로그 검색 및 분석 ▪ 모니터링 시각화 ▪ 권한관리 및 보고서	▪ 대용량 데이터 처리 기술 ▪ 1일 기준 로그량 저장공간 산정
6	보안관제시스템	이기종의 분산된 보안 솔루션들의 위협 이벤트를 통합 상관 분석하여 외부 위협을 선제적으로 대응함	▪ 이벤트 로그 수집 ▪ 로그 상관분석 ▪ 탐지 이벤트 처리 ▪ 시나리오 룰 정의 ▪ 보안관제 대시보드	▪ AI기반 머신러닝 상관분석 ▪ 내부유출과 외부 침해위협의 통합관제 ▪ 상관분석 시나리오의 Intelligence 분석

[표 Ⅲ-10. 시스템 보안 영역별 특징]

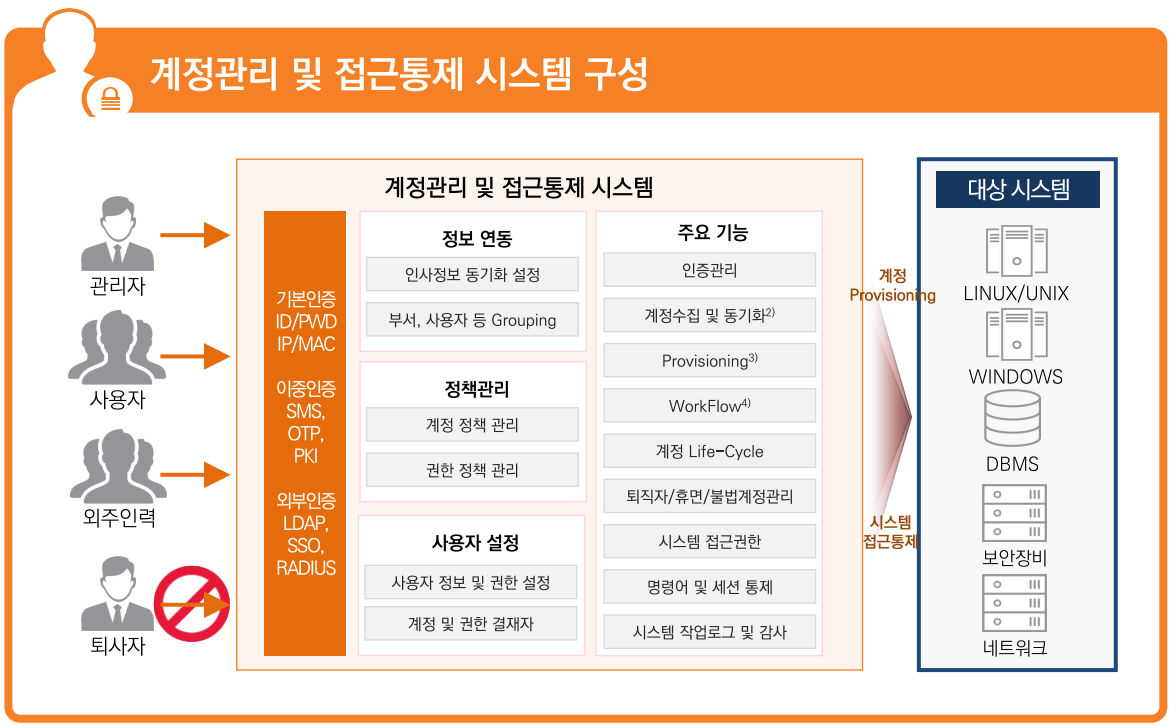
3) 보안 솔루션 소개

가. 계정관리 및 접근통제

A. 솔루션 개념

시스템 보안 관점에서 계정(ID)과 접근권한의 관리는 기본적이고 중요한 보안 관리 중 하나입니다. IT 보안관리자는 최근 시스템 인프라 환경에서 대형화되고 세분화된 각 시스템의 계정과 시스템 접근 권한을 통제관리 해야 합니다. 이에 대한 방안으로 보안관리자는 계정관리 및 접근통제 솔루션을 사용하여 중앙 관리 통제방식으로 각 시스템 관리자 및 사용자에게 계정을 생성 및 관리하며, 각 업무 계정에 적합한 접근 권한을 부여하여 계정/접근 정책을 운영해야 합니다.

계정관리(IM)와 접근제어(AM)를 하나의 솔루션으로 통합한 통합계정접근관리(IAM) 솔루션은 레거시 시스템 및 인사정보 시스템과 연동하여, 계정관리 프로세스를 통합화, 자동화 함으로서 비즈니스 업무효율을 극대화하고 있습니다. 대다수의 IAM 솔루션에서는 권한관리를 위하여 RBAC[1]에 기반을 둔 권한 프로세스를 제공하고 있습니다. RBAC은 역할(Role)과 사용자(User)에 업무수행에 필요한 서비스 자원을 할당하는 개념입니다.



[그림 Ⅲ-11. 계정관리 및 접근통제 솔루션 구성]

1) RBAC (Role-Based Access Control) : 계층적으로 구성된 Organization안에 Organization Role을 정의하게 되며 이러한 Role은 대상 시스템 별로 접근할 수 있는 사용자/그룹을 동적으로 부여하는 개념
2) 계정수집 및 동기화 : 솔루션 초기 구축 시 서버와 DB의 모든 계정을 수집하고 계정을 정책에 맞춰 정리 후 시스템 운영 시 지속적으로 계정관리 솔루션과 실제 서버와의 계정을 동기화 하는 기능
3) Provisioning : 사용자에게 계정정보와 계정 접근권한에 필요한 제반 자원을 제공하는 서비스 설정 과정
4) WorkFlow : 계정관리 및 접근통제에서 WorkFlow는 계정의 Life-Cycle에 관련된 내용을 정책에 기반한 결재를 통해 수행하는 절차를 말한다. (계정생성, 권한부여 및 변경, 계정 잠금 및 해제, 계정삭제 등)

B. 주요기능

계정관리 및 접근통제 기능은 계정관리 영역과 접근통제 영역으로 나누어 집니다. 계정관리는 각 시스템 계정(ID)의 Life-Cycle관리, 계정정책 관리, 계정 생성 및 변경을 위한 프로세스 관리, 이력 및 감사보고가 있고, 계정의 패스워드를 IAM솔루션에서 통합 관리하는 솔루션도 있습니다. 접근제어 영역은 사용자별 권한설정, 명령어와 세션의 통제, 감사추적 기능을 주요 기능으로 볼 수 있습니다.

계정관리 주요 기능	기능영역	접근통제 주요 기능
계정정책 관리 1 시스템 계정 수집 정책 2 계정 및 Password 정책 설정 3 시스템 연동 설정 4 계정유형 정의	정책 설정	**접근제어 정책 관리** 1 사용자 인증 방식 설정 2 접근제어 정책 설정 3 세션 통제 정책 설정
계정 Life-Cycle관리 1 계정 생성/변경/통제(잠금)/삭제 2 계정 수집 및 동기화 3 계정 WorkFlow 관리 4 Provisioning 관리 5 퇴사자/휴면/불법계정관리	영역 주요 기능	**접근제어 기능 수행** 1 사용자, IP, 시간 별 접근제어 2 비인가자 시스템 접근 차단 3 위험 명령어 통제 4 연결 세션 관리 및 통제
이력 및 감사보고 1 계정 Life-Cycle 이력관리 2 계정 모니터링 및 보고관리 3 로깅 및 감사, 주기적 리포팅	모니터링 및 보고	**모니터링 및 보고** 1 비인가 접속 모니터링 2 위험 명령어, 작업 로그 관리 3 시스템 접근 감사로그

C. 솔루션별 특징

계정관리의 영역은 서버, 네트워크, 보안장비의 시스템 계정관리와 DBMS의 DB계정관리, 업무 시스템의 Application 계정관리로 구분할 수 있습니다. Application 계정관리는 구축방식과 솔루션이 별도로 구성되어 있어 본 장에서는 시스템 계정관리와 DB계정관리 솔루션으로 특징을 정의합니다.

개발사	제품명	솔루션 기능		
		계정관리 기능	접근통제 기능	특징
넷엔드	HIWARE	▪ 시스템/DBMS/AD 계정관리 ▪ 계정 Life-Cycle 정책관리 ▪ 패스워드 정책 관리 ▪ 통합 계정 정책 관리 ▪ 퇴직자/휴면/불법 계정 탐지 ▪ DBMS 테이블 단위의 권한 설정 ▪ 기간별 권한 설정 ▪ AD계정 도메인 관리 기능 제공 ▪ 서버/DBMS/NW/보안 장비 지원	▪ 시스템 및 DBMS 접근통제 ▪ 사용자 인증 강화 -LDAP, OTP, PKI등 ▪ 사용자 별, IP, 프로토콜 별 접근 권한 통제 ▪ DBMS 쿼리 통제 ▪ 시스템 명령어 통제 – 금지 키워드 적용, 금지 명령어 입력 시 즉시 경고 및 세션 차단, SMS및 E-Mail 통보 ▪ 실시간 세션 통제 ▪ 작업 로그 기록 및 감사	▪ CC인증 ▪ 보안위협 사전 탐지 및 차단 ▪ 조달청 접근통제 5년 연속 판매 1위 ▪ 클라우드 환경에서 기존 레거시 환경과 동일한 수준의 보안관리 지원 ▪ 국내 최초 A.I 선제 대응형 보안 관리
IBM	IBM Security Secret Server	▪ 정책 자동배포 ▪ 계정 Life-Cycle 정책 관리 ▪ 동기화 기능을 통하여 계정관리시스템의 계정정보와 시스템 계정정보 정합성 유지 ▪ 주기적인 패스워드 강제 변경 ▪ 권한 위임 설정 ▪ 서버와 계정관리대상서버간의 암호화 통신 ▪ 워크 플로우 (결재) 기능 ▪ 정책위반/시스템 직접 변경 탐지 및 보고 ▪ 보고서 기능 제공 ▪ DBMS, N/W 장비 지원 ▪ 서버/DBMS/N/W 장비 지원 및 통합관리 시스템	▪ 역할 및 요청기반 접근통제 ▪ 세션 통제 ▪ 사용자 UI 접근에 대한 2 Factor 인증 ▪ DBMS 접근통제 수행 (Chakra-MAX) ▪ 키 인증방식의 SSH 프로토콜 접근 지원 ▪ 외부 원격 접속 프로그램 연동(RDP, Putty 등) ▪ Agent less 방식의 운영 지원 ▪ 작업내용 암호화 기록 ▪ 감사로그 및 스케줄 리포트 지원	▪ Qrader, Splunk, ArcSight 등 SIEM/ESM 기본 연동 ▪ Secret Server에 한번의 인증으로 여러 서버 동시 접근 가능 ▪ 글로벌 기업으로 해외 다수 레퍼런스 보유

개발사	제품명	솔루션 기능		
		계정관리 기능	접근통제 기능	특징
피앤피시큐어	DBSAFER (접근통제 DB/AM/OS) (계정관리 IM)	▪ 시스템/DBMS 계정관리 ▪ 계정 Life-Cycle 관리 ▪ 계정 생성/삭제/잠금 ▪ 비밀번호 관리 정책 ▪ Work-Flow 지원 ▪ 불법계정 및 만료 휴면계정 관리 ▪ 관리자,시스템,사용자 계정 분류 및 비밀번호 관리 ▪ 서버/DBMS 장비 지원 ▪ 감사로그 제공	▪ DBMS 및 시스템 접근제어 수행 ▪ 접속 및 권한 제어 ▪ 사용자 인증 (2 Factor) 기능 제공 ▪ DBMS 데이터 마스킹 ▪ DBMS 결과값 제어 ▪ 감사로그 암호화 기록 ▪ 모니터링 ▪ 결재 시스템 제공 ▪ 명령어, 파일 접근통제, 무결성 체크 ▪ 통신구간 암호화 ▪ 감사로그 제공 및 정책위배 로그	▪ CC인증 ▪ DBSAFER 제품간 완벽한 연동 기능 제공 ▪ 계정의 비밀번호 노출 없이 DBMS에 대한 자동 접속 기능 제공 ▪ 우회접속 사용자 통제 및 사후 감사 기능 수행
시큐브	iGriffin	▪ 시스템/DBMS 계정관리 ▪ 계정 Life-Cycle관리 ▪ 신청서 기반 Work-flow 지원 ▪ 역할기반 계정관리 ▪ 인사정보 변동에 따른 자동화된 계정 발급 및 회수 체계 지원 ▪ 계정 및 패스워드 관리 ▪ 서버/DB/NW장비까지 모든 IT 인프라의 계정을 통합계정 권한 관리 시스템으로 관리 ▪ 서버/DB/NW장비 지원 및 통합관리 시스템	▪ 복합 인증 및 신청 시스템을 통한 시스템 접근제어 기능 제공 ▪ 특정 위험명령어 사용금지를 위한 명령어 통제 ▪ 신청/승인 절차를 통한 위험 명령어 예외 허용 ▪ 시스템 사용자 행위감사 및 모니터링	▪ CC인증 ▪ Hypervisor-Cloud 지원 ▪ 복합인증 (PKI인증서, 지문, 스마트카드, OTP, ARS등)을 시스템 접근에 적용 ▪ 자사 서버보안제품 (Secuve TOS) 연계 가능
엘에스웨어	Omni-IM (Omni-UAC/UPV/UCC)	▪ 시스템/DBMS 계정관리 ▪ 계정 Life-Cycle 관리 ▪ 이기동 OS및 DBMS 계정 관리 수행 ▪ 인사정보 연동 및 관리 ▪ 이기종 서버 동시 계정 생성 및 변경 삭제 ▪ 그룹별 일괄 보안정책 ▪ 계정변경 이력관리 ▪ 패스워드 정책 관리 ▪ 계정 잠금/보안 정책 설정 ▪ 서버/DBMS 장비 지원 ▪ 계정 상태 보고서	▪ 서버 접근제어 ▪ 그룹/서비스/IP별 접근제어 ▪ 포트 접근제어 ▪ 접근 IP 그룹 설정 ▪ 위험명령어 사용 추적 ▪ 세션 replay 기능 ▪ 세션 조회 및 관리 ▪ 감사 로그 기록 ▪ 웹 URL로깅	▪ 전사자원관리(ERP), 내부결재, 업무메일, 인사DB 등 사내 기간계 시스템 연동을 지원

개발사	제품명	솔루션 기능		
		계정관리 기능	접근제어 기능	특징
휴네시온	NGS V7.0	▪ 시스템/DBMS 계정관리 ▪ 접속계정관리 ▪ 시스템 접속 계정 생성, 수정, 삭제 ▪ 계정 Life-Cycle 관리 ▪ 패스워드 관리 ▪ 일회용 root 패스워드 발급 ▪ 사용자 인증 ▪ 휴면 계정, 삭제 사용자 계정 관리 ▪ 일정기간 미접속 시 계정 권한 회수 ▪ 사용자 IP별, MAC별 접근 제한 ▪ 서버/DBMS 장비 지원	▪ Black/Whitelist 기반 실시간 명령어 통제 ▪ NGS를 우회하는 접속 시도 탐지 및 알림 (Syslog 연동) ▪ Dashboard 형태의 관리자 모니터링 화면 ▪ 접속현황, 실행 명령어, 발생 이벤트 등에 대한 실시간 모니터링 ▪ 명령어 입· 출력 내역 저장 (Unix, Linux, DMBS) ▪ 작업내용 동영상 저장 (Windows, http(s))	▪ CC인증 ▪ 관리 시스템에 대한 보안 취약점 점검 기능 제공 ▪ 다양한 상용 접속 클라이언트, DB접속툴, 개발툴 지원 ▪ 서버보안, 계정관리, DB 접근제어 기능까지 통합 제공 ▪ 계정관리 부문에서 계정·패스워드 관리와 생체인증을 통한 사용자 인증 관리 ▪ KT클라우드 마켓플레이스에 입점
브로드컴	CA-IM (계정관리 솔루션)	▪ 시스템/DBMS 계정관리 ▪ Unix/Linux/DBMS등 다양한 이기종 계정관리 지원 ▪ 위임된 사용자 관리 ▪ 사용자 셀프 서비스 ▪ 통합된 워크 플로우 지원 ▪ 패스워드 관리 기능 ▪ 구조화된 관리 모델 및 커스터마이징 지원 ▪ 통합 컴플라이언스 지원 ▪ 개방형 인터페이스로 타사 시스템 상호 운용 지원		▪ 다수 금융권 레퍼런스 보유 ▪ 글로벌 SW 제공 업체 ※ 2018.11 CA테크놀로지 한국지사 철수
에스지앤	SecureGuard	통합계정관리 (IM) ▪ 사용자 계정, 그룹, 조직도(ORG)를 바탕으로 정책을 수립 ▪ 사용자(계정) 수집 (Reconciliation) ▪ 사용자(계정) 배포(Provisioning) ▪ 계정 현황, 감사용 조사, 정기 보고서 및 실시간 모니터링을 통해 위험 요소를 사전에 제거하고 경고	시스템접근통제 (AM) ▪ 2-Factor 인증 ▪ 전용 클라이언트를 통하여 사용자별 계정할당 ▪ 명령어 제어 수행, 세션 접속 차단 및 경고 ▪ 모바일 OTP 제공 ▪ 윈도우 서버 snapshot 감사 기록 ▪ 로그인 조회/명령어 조회/실시간 조회 기능 ▪ 서버와 Network 장비에 접근/통제 기능	▪ CC인증 ▪ 업계 유일의 SOCKS5 표준 프로토콜을 사용 네트워크 환경 변화 없이 시스템 구축 ▪ Agentless 방식 ▪ 공공, 금융, 기업, 국방 등 레퍼런스 보유 ▪ 국가정보자원관리원 2만여 시스템의 접속에 대한 인증 및 접근을 통제

[표Ⅲ-11. 계정관리 및 접근통제 솔루션별 특징]

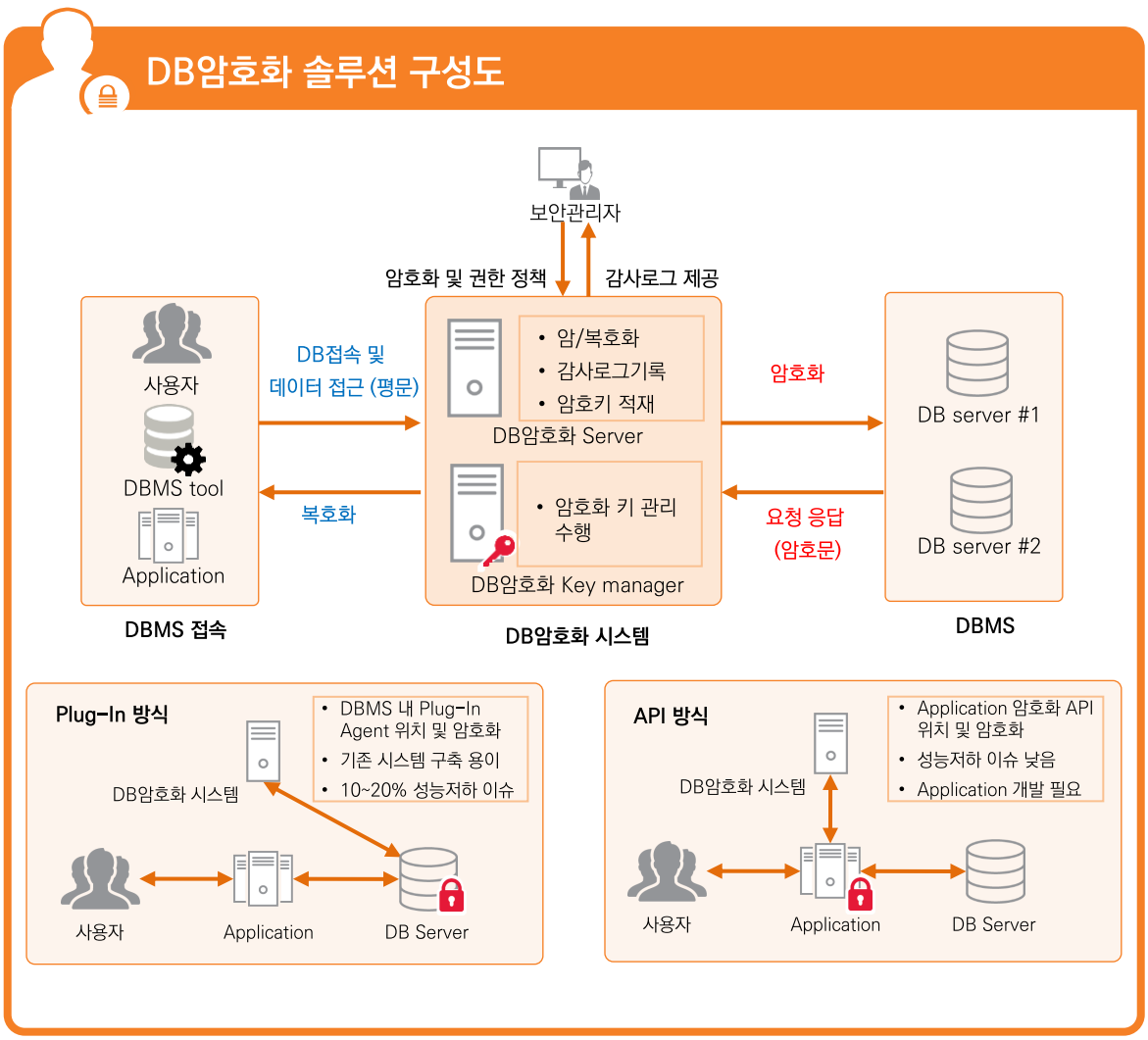
나. DB암호화

A. 솔루션 개념

개인(신용)정보, 주요거래정보, 기업기밀 등을 저장하고 있는 기업의 중요 데이터는 내·외부 위협에 대한 대응조치가 필요하며, 보안 컴플라이언스 준수 요건에도 필수적으로 부합해야 합니다.

DB암호화 솔루션은, 데이터 보안 중 하나로 데이터베이스 내에 저장되어 있는 데이터를 암호화하여 외부로부터의 위협이나 내부자에 의한 유출 시 암호화를 통하여 정보유출을 근본적으로 보호하는 솔루션입니다.

최근 DB암호화 솔루션들은 Plug-in 방식, API 방식, 두 구성 방식을 혼합한 Hybrid 방식, 블록단위 암호화 방식 등 다양한 구성 방식을 지원하고 있으며, 현재 운영중인 IT인프라의 환경과 신규 구축 환경 등을 고려한 안정적이고 효율적인 DB암호화 시스템으로 구성되고 있습니다.



[그림 Ⅲ-12. DB암호화 솔루션 구성도]

B. 주요기능

DB암호화 솔루션은 데이터 베이스에 저장된 데이터에 대한 암호화와 접근권한 설정, 암/복호화 적용, 감사 및 이력관리 등 DB암호화에 대한 전반적인 기능을 제공합니다. 주요기능 외에도 암호화 솔루션 적용 후 서버의 성능 이슈에 대한 방안과 암호화 알고리즘 결정, 키 관리에 대한 이슈를 고려하여야 합니다.

국가정보원 IT보안인증사무국에서는 DB암호화 제품 구축 시 △안정성이 검증된 암호모듈 및 알고리즘 사용 △암호화 키 생성, 접근, 갱신, 폐기 등의 안정성 확보 △암호문, 인덱스 등 중요 데이터의 안정성 확보 △암호키, 암호문 등에 대한 비인가자의 접근 통제 △전송 데이터의 기밀성, 무결성 유지 △제품 사용자의 신원 확인 및 검증 △제품 관련 중요 이벤트에 대한 감사 기록 시스템 구축 등을 권고하고 있습니다.

기능영역	주요 기능 내용
정책 설정	**암호화 및 접근권한 설정** 1 암호화 대상 정의 2 사용자 및 그룹 별 데이터 접근권한 설정 3 암호화 키 관리 정책 설정 (생성/삭제/갱신 등)
데이터 암/복호화	**암/복호화** 1 암호화 알고리즘 정의 및 적용 2 대상 컬럼/필드/데이터의 암호화/ 복호화 처리 3 사용자별 데이터 접근 제어 4 암호화 키 관리 5 로그 위·변조 유출 보안이슈 방지
감사 및 이력관리	**감사/이력/모니터링** 1 정책 설정, 암호화 키 변경 등 감사 2 접근 및 작업 감사 조회 및 보고서 3 DB 성능 현황 모니터링

C. DB암호화 제품의 핵심보안 요구사항

암호화 알고리즘을 적용하는 데이터 암복호화는 매우 간단하지만, 암복호화의 키 관리는 매우 중요하며 신중한 관리절차가 필요합니다. 암복호화의 대상이 일반 파일이나 네트워크 구간이 아닌 DB이기 때문에, 서비스의 연속성을 위해서 DB 암호화 후 기존 DB 제약사항 유지나 서비스의 안정성이 무엇보다 중요합니다. DB에는 중요한 정보들이 여러 테이블의 컬럼에 존재하고 있고, 이러한 정보들은 DB 내부의 인덱스(Index), 내장 애플리케이션(Stored Application), 패키지(Package), 함수(Function) 그리고 DB 외부의 애플리케이션들과 밀접하게 상호 작용을 하므로, DB 암호화 후에도 이러한 시스템적 관계유지가 절대적으로 필요합니다. 또한, DB 암호화를 위해 솔루션 도입 시에는 다음의 국가정보원"DB 암호화 제품의 핵심 보안요구 사항"을 준수해야 합니다.

구분	보안 요구사항	요구 기능	설명
암호지원	안정성이 검증된 암호모듈·알고리즘 등 사용	▪ ARIA 128/192/256, SEED ▪ SHA 256이상, HAS-160	▪ 국정원 암호모듈 검증필
암호키 관리	암호 키 생성·접근·갱신·파기 등의 안정성 확보	▪ 암호키 유도는 검증된 국제표준 알고리즘 ▪ 공유 메모리에 로드된 암호키는 평문 불가	▪ 국정원 "DB암호제품 보안요구 사항" (2010.04)
DB 데이터 암·복호화	암·복호화 암호문·인덱스 등 중요 데이터의 안정성 확보	▪ 안전한 암호모듈을 통하여 암·복호화 ▪ 원본 데이터는 암호화 후 삭제	▪ 암호모듈 검증제도에 검증받은 암호모듈
접근제어	암호키·암호문 등에 대한 비인가자의 접근차단	▪ DB계정, IP, 어플리케이션, 접속기간 등 조건별 제한	▪ 국정원 "DB암호제품 보안요구 사항" (2010.04)
암호통신	전송 데이터의 기밀성·무결성 유지	▪ 제품 구성요소간 안정한 전송	
식별 및 인증	인증제품 사용자의 신원 확인 및 검증	▪ 사용자의 연속된 인증 실패 후 초기화 ▪ 인증 데이터 재사용 공격방지	
보안감사	제품관련 중요 이벤트에 대한 감사 기록	▪ 감사 데이터는 인증된 사용자만 접근 ▪ DB테이블명, DB칼럼명, 쿼리 유형에 따라 검토	
보안관리	보안정책·감사 기록 등의 효율적인 관리	▪ 암호키 및 보안정책 등 중요 데이터에 대한 백업 및 복구 기능 제공	

출처 : DB암호제품 핵심보안 요구사항 – IT보안인증사무국 / 국가보안기술연구소

[표 Ⅲ-12. DB암호화 보안요구사항]

D. 솔루션별 특징

국내 유통되고 있는 DB암호화 솔루션의 암호화 적용기술, 지원 가능한 암호화 구성 방식, 각 솔루션의 특징을 소개해 드립니다. 최근 DB암호화 솔루션은 단순 암호화 영역에서 고도화 되어 통합적인 DB접근제어까지 제품의 기능 영역을 확장하여 제공되고 있습니다. 또한 클라우드 환경의 DB암호화 지원 등 IT 인프라 환경의 변화에 맞추어 솔루션들이 보완되고 있습니다.

[DB암호화 솔루션 구축 이전에 고려사항]

- 암호화 대상 및 범위를 위험도 분석 결과에 따라 철저한 분석
- 국내외 연구기관에서 검증된 암호화 알고리즘의 적용
- 개인정보는 양방향 개인정보 필수 적용
- 암호화 인덱스 지원, 성능을 고려해 부분 암호화 적용
- 암복호화 키, 마스터 키 등 모든 키를 생성에서 폐기까지 안전하게 관리

개발사	제품명	솔루션 기능		
		주요 기능	지원 구성 방식	특징
케이사인	SecureDB	▪ 암/복호화 기능 제공 ▪ SEED,TDES,AES,ARIA 등 암호화 알고리즘 ▪ 접근 권한 관리 기능 ▪ 감사로그 관리 기능 ▪ 암호화 키 관리 및 Admin 기능 ▪ ORACLE, MSSQL, Mysql, MariaDB, Cubrid 지원	▪ API 방식 제공 ▪ Plug-In방식 제공 ▪ SPIN(Token)방식 제공	▪ CC인증 ▪ 국내외 표준 알고리즘 지원 ▪ 암호 키 관리 및 접근제어 기법 기술 특허 제품 ▪ RBAC 기반 사용자 접근통제
한컴시큐어	XecureDB	▪ ARIA, SEED, AES, 3DES, SHA2, FPE, OPE, 압축암호화 등 암호화 알고리즘 제공 ▪ 암/복호화 기능 제공 ▪ 접근제어 기능 제공 ▪ 인덱스 검색제공 ▪ 암호화 키 변경 옵션 기능 ▪ API 암/복호화 서비스 모니터링, ▪ CPU 및 메모리, 프로세스 모니터링 제공 ▪ ORACLE, Sybase, Tibero, MSSQL, Mysql, DB2 지원	▪ API 방식 제공 ▪ Plug-In방식 제공 ▪ Hybrid 방식 제공	▪ 국내외 표준 알고리즘 지원 ▪ 국정원 암호검증제도(CMVP) 인증모듈 사용 ▪ GS인증, SAP Integration Certification 인증 ▪ NIST 표준을 준수한 늘어나지 않는 암호화(FPE) 지원 ▪ 운영, DW 환경 및 임베디드(POS, PDA) 환경을 모두 지원

개발사	제품명	솔루션 기능		
		주요 기능	지원 구성 방식	특징
펜타시큐리티	D'Amo	▪ 암/복호화 기능 제공 ▪ 국내외 표준, FIPS 인증 암호 알고리즘 제공 ▪ 키관리 기능 제공 ▪ 접근제어 기능 제공 ▪ 중앙 집중형 로그 관리 ▪ 접근,정책,상태 로그 ▪ 로그자동 백업 및 조회 ▪ ORACLE, Altivase, MSSQL, DB2 지원	▪ API 방식 제공 ▪ Plug-In 방식 제공 ▪ 커널 레벨 암호화 방식 제공 ▪ DBMS 엔진 암호화 방식 제공	▪ CC인증 EAL3+ 획득 ▪ GS인증, SAP Integration Certification 인증 ▪ 자체 개발한 국가정보원 검증필 암호모듈 사용(CIS-CC) ▪ 미연방정보처리표준(FIPS) 인증 ▪ CYBERSECURITY Excellence Awards 데이터베이스 보안 부문에서 제품의 우수성을 인정 ▪ 다양한 구성 방식 제공
신시웨이	PETRA CIPHER	▪ 고객환경에 최적화된 암호화 기술 ▪ 안전한 키 생성 및 관리 기능 ▪ 키 관리 서버 이중화 및 로컬 관리 ▪ DB 접근제어와 DB 암호화 연동 ▪ 컬럼 단위 암호화 ▪ 관리자 권한 분리 기능 ▪ 암호화 데이터 접근에 대한 감사 로그 조회 ▪ 모니터링 기능 제공 ▪ ORACLE, Altivase, MSSQL, DB2, Mysql, Cubrid, Sybase, Tibero 지원	▪ API 방식 제공 ▪ Plug-In방식 제공 ▪ 쿠폰 방식 제공 ▪ Transformer (SQL 변환) 방식 제공	▪ CC인증, GS인증 ▪ PETRA 접근제어 솔루션과 완벽 연동으로 IP기반 접근제어 수행 ▪ C언어 기반 모듈 사용으로 빠른 속도로 암·복호화를 진행
Vormetric	Vormetric Data Security	▪ 암호화 키관리 ▪ 3DES, AES, ARIA 등 암호화 알고리즘 제공 ▪ 접근통제 수행 ▪ 권한 및 역할 관리 ▪ 감사 및 데이터 보안 ▪ 정형 및 비정형 데이터 암호화 제공 ▪ 하드웨어 암호 가속화 기술 지원 ▪ ORACLE, MSSQL, DB2, Mysql, Sybase, MongoDB 지원	▪ 커널 암호화 방식 – 암복호화 모듈이 운영체제 커널안에 로딩 파일에 대한 암복호화 수행	▪ 자사 및 타사 암호화 제품의 키관리 ▪ FIPS 인증 ▪ 암호화 성능 오버헤드 줄임으로써 어플리케이션 성능 및 SLA 유지

[표 Ⅲ-13. DB암호화 솔루션별 특징]

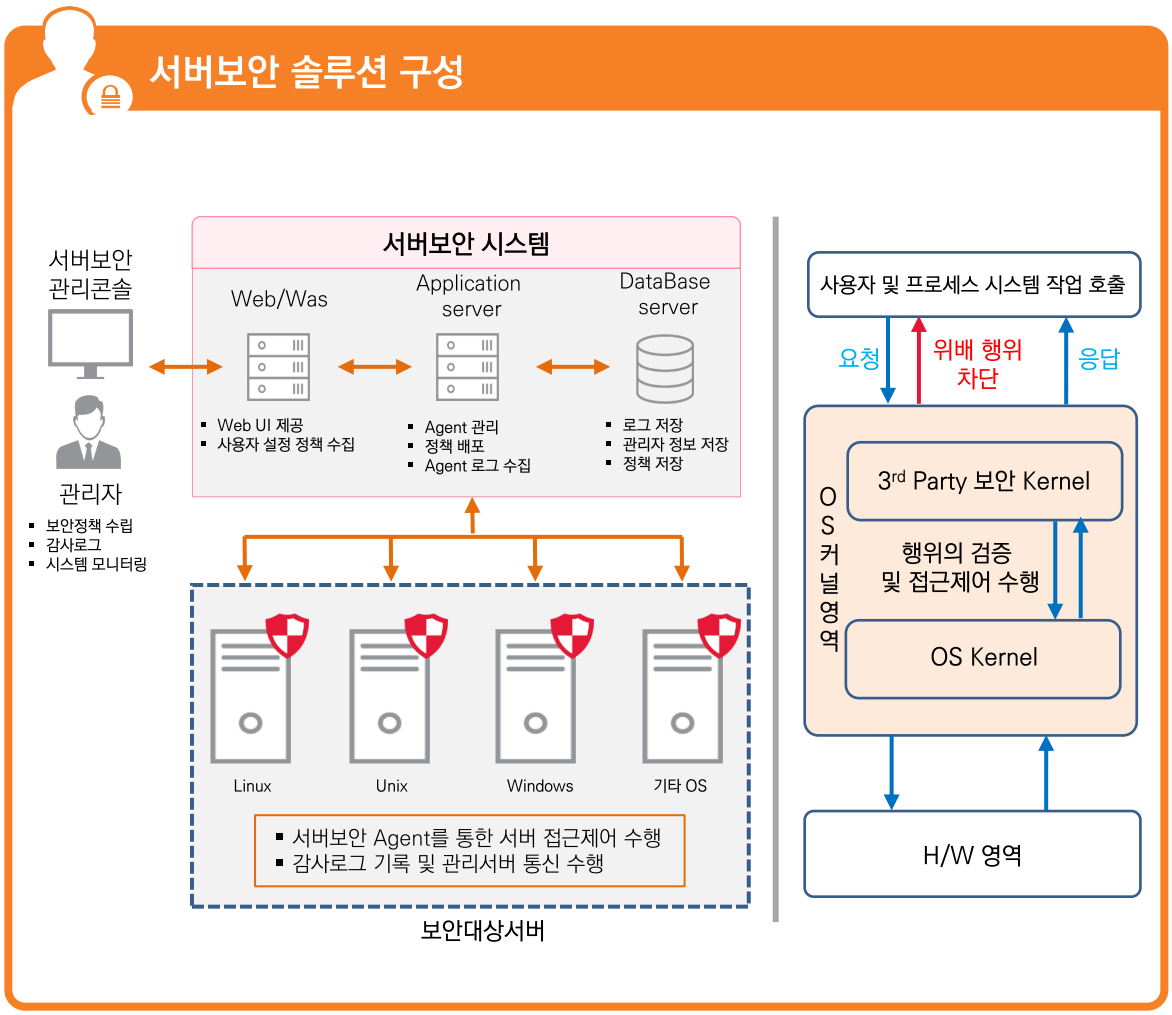
다. 서버보안

A. 솔루션 개념

서버보안 솔루션은 서버 운영체제의 보안 취약점과 외부 위협으로부터 내부 시스템을 보호하기 위한 OS Layer에 대한 보안 솔루션입니다. 기존의 OS Kernel 내 보안 기능을 제공하는 Security Kernel 영역을 이식하여 OS 보안을 수행하게 됩니다.

서버보안은 서버에 접근하는 사용자와 프로세스와 접근 주체의 권한을 식별하고, 파일 접근, 네트워크 접근 등 사용자와 프로세스의 행위를 감시하며, 보안 정책 위배 시에는 행위를 통제하게 됩니다.

최근 공공기관, 기업 및 금융권에서 퍼블릭, 프라이빗 환경의 클라우드 시스템을 구축과 운영을 하고 있습니다. 이러한 시장변화에 맞춰 각 서버보안 솔루션 또한 클라우드 환경의 운영체제와 클라우드 시스템 활용 이점을 유지하도록 솔루션을 개발하여 시장의 변화에 대응하고 있습니다.



[그림 Ⅲ-13. 서버보안 솔루션 구성]

B. 주요기능

서버보안 시스템의 기능은 보안정책 설정 및 배포를 수행하는 정책 설정 영역, 파일 및 네트워크 등의 접근제어 영역, 보안정책 위배 행위 감사 및 모니터링 영역으로 나누어 볼 수 있습니다.

서버보안 관리자는 서비스 운영 및 시스템 영향도를 고려, 서버보안 솔루션을 통하여 OS 주요 파일 시스템과 중요 파일 보호 정책, 서버간 불필요한 네트워크 통신 차단 정책, 서버 로그인 및 계정 접근 통제 정책 등을 체계적으로 설정하여 보안 위협으로부터 서버 시스템을 보안유지 해야 합니다.

기능영역	주요 기능 내용
보안 정책 설정	**보안 정책 설정** 1 계정 로그인 및 패스워드 등 사용자 접근 정책 설정 2 파일, 프로세스 및 네트워크 등 시스템 접근 제어 정책 설정 3 사용자 행위 및 프로세스 행위 감사 로그 설정 4 보안 정책 일괄/부분 배포 수행
접근제어 수행	**접근제어 수행** 1 파일 및 프로세스 접근제어 수행 2 서버의 네트워크 접근제어 수행 3 사용자 계정 로그인 및 패스워드 제어 4 보안 정책 시뮬레이션 기능
감사로그 및 모니터링	**감사로그 및 모니터링** 1 시스템 내 정책 위배행위 로그 기록 2 사용자 행위 감사 로그 기록 3 시스템 모니터링

C. 솔루션별 특징

서버보안 솔루션의 주요 기능 요소인 접근제어 기능, 사용 환경, 특징으로 구분하여 설명합니다.

최근 가상화 및 클라우드 환경에서의 서버보안 솔루션 설치 및 운영 지원 등 서버보안 적용 환경의 변화와 계정관리, 접근제어, 보안관제 시스템 등 이기종 보안시스템과의 연동을 통한 보안 영역 확장이 이루어 지고 있습니다.

개발사	제품명	솔루션 기능		
		접근제어 기능	사용 환경	특점
하우리	RedOwl	▪ MLS/RBAC/ACL/DAC 접근제어 방식 제공 ▪ 파일 및 디렉토리 접근제어 ▪ 레지스트리 변경 제어 ▪ 원격 접근 및 로그인 접근제어 ▪ IP 및 port 네트워크 제어 ▪ 다중등급의 시스템 보안 ▪ 계정 및 패스워드 관리	▪ Solaris ▪ HP ▪ AIX ▪ Linux ▪ Windows ▪ 가상화 및 클라우드 환경	▪ CC인증 ▪ 행위 기반 알고리즘을 통한 해킹탐지 ▪ 오버헤드 최소화 최적의 성능 (3%이내) ▪ 대량 로그 처리 기술 ▪ 암호화 통신 수행 ▪ 중앙관리 GUI 제공
SGA솔루션즈	RedCastle	▪ 파일 및 디렉토리 접근제어 ▪ 레지스트리 변경 제어 ▪ IP 및 port 네트워크 제어 ▪ 프로세스 보호 ▪ 사용자 로그인 통제 ▪ 계정 및 패스워드 관리 ▪ 관리자 권한 분리 및 통제 ▪ 파일, 프로그램 무결성 ▪ 서버 방화벽 기능 수행 ▪ 명령어 제어	▪ Solaris ▪ HP ▪ AIX ▪ Linux ▪ Windows ▪ 가상화 및 클라우드 환경	▪ CC인증 ▪ 2Factor 인증 ▪ 해킹시도 원천 차단 ▪ 보안관리와 시스템 관리 통합 관리환경 제공 ▪ 해킹방지 기능 수행
시큐브	Secuve TOS	▪ MLS/RBAC/ACL 접근제어 방식 제공 ▪ 파일 및 디렉토리 접근제어 ▪ 레지스트리 변경 제어 ▪ 계정 및 패스워드 관리 ▪ 사용자행위감사 및 권한 위임 ▪ 명령어 통제 ▪ 네트워크 접근통제 ▪ 사용자 로그인 제어	▪ Solaris ▪ HP ▪ AIX ▪ Linux ▪ Windows ▪ 가상화 및 클라우드 환경	▪ CC인증 ▪ PKI기반의 사용자 인증 ▪ OS 벤더 별 가상화 환경 및 Cloud 환경 지원

[표 Ⅲ-14. 서버보안 솔루션별 특징]

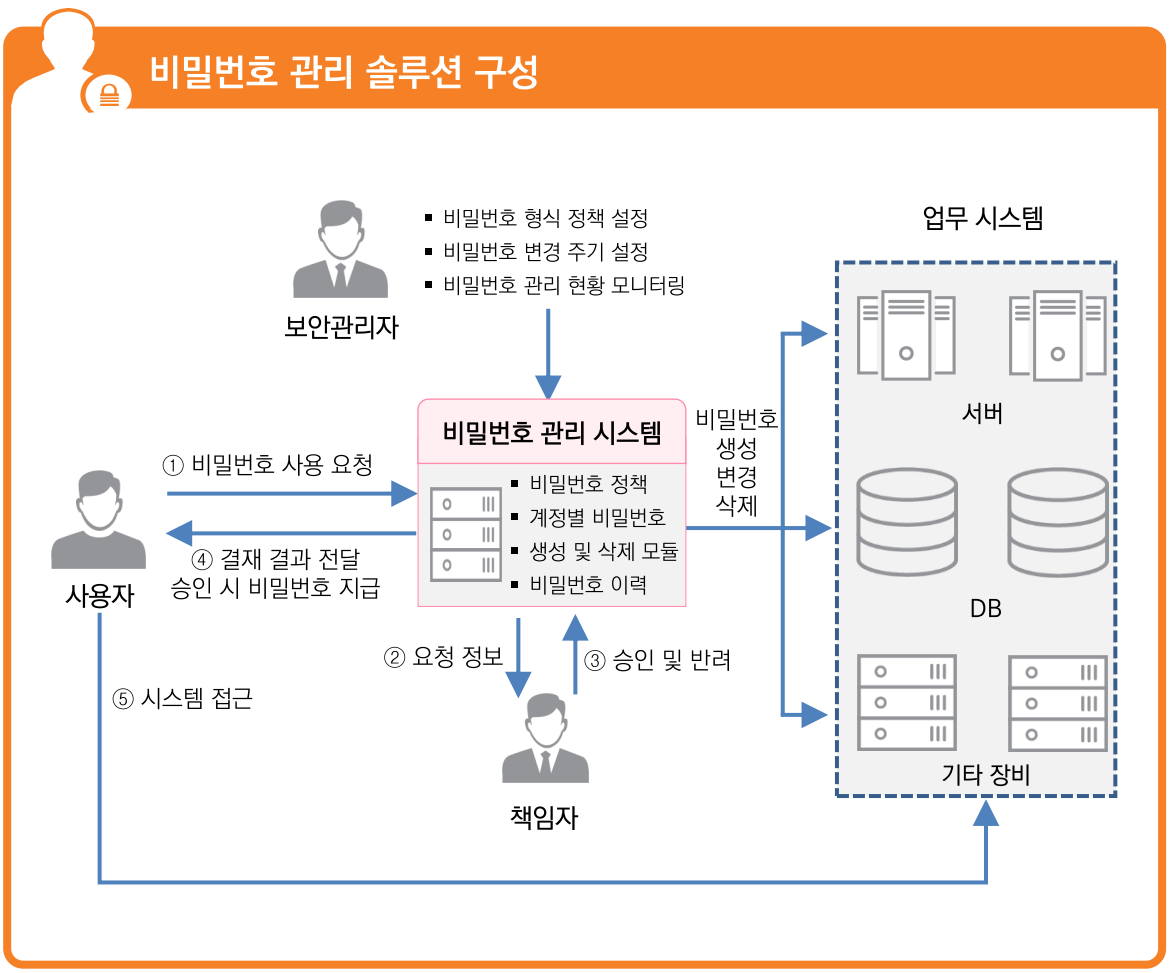
라. 비밀번호관리

A. 솔루션 개념

전체 IT인프라 시스템 상에 산재되어 있는 계정의 비밀번호를 개인별로 수작업을 통하여 생성과 변경하는 것은 업무효율성 하락과 보안취약점이 발생합니다. 다수의 시스템 비밀번호를 공통으로 적용하거나, 업무 관련자 사이에서의 비밀번호 공유하고, 비밀번호를 기억하기 위해 종이나 전자문서에 기록하는 것은 치명적인 보안 사고의 원인이 될 수 있습니다.

비밀번호 관리 솔루션은, 주기적인 계정별 비밀번호 변경, 워크플로우를 통한 일회용 비밀번호 발급 등 보안 기능을 제공합니다. 이러한 제공 기능을 통해 보안취약점을 조치 하며, 보안 컴플라이언스를 준수할 수 있습니다.

최근 비밀번호 관리 솔루션의 관리대상은 서버 OS에서부터 네트워크 장비, 데이터베이스, 업무 어플리케이션 등 여러 인프라 계정의 비밀번호 관리를 통합관리 하도록 대상영역이 점차 확장되고 있습니다.



[그림 Ⅲ-14. 비밀번호 관리 솔루션 구성]

B. 주요기능

비밀번호 관리 솔루션은 일괄적인 비밀번호 변경 및 관리, 결재를 통한 비밀번호 요청 승인 및 일시적인 비밀번호 제공, 감사 및 모니터링 기능이 주요 기능입니다. 솔루션 도입으로 각 시스템 계정의 비밀번호를 안전하게 관리를 할 수 있게 되었으나 모든 시스템 계정의 비밀번호를 저장 및 관리는 내·외부의 위협 대상이 될 수 있습니다. 이러한 위협으로부터 보호하기 위해 비밀번호 관리 솔루션이 제공하는 자체 보유 데이터의 암호화 및 키관리 보안 확보는 중요한 기능 요소 중 하나입니다. 비밀번호 암호화는 일방향 암호화와 SHA256이상의 알고리즘 적용을 권고하고 있습니다.

솔루션 구축 시 주요기능 외에도 업무 환경에 적합한 비밀번호 정책과 워크플로우 정의, 보안강화를 위한 인증관리, 대상 시스템의 비밀번호관리를 위한 프로토콜 제공, 계정관리와 접근통제와의 연동을 통한 효율적 운영방안이 필요합니다.

기능영역	주요 기능 내용
비밀번호 정책설정	**정책 설정 및 비밀번호 변경** 1 계정별 비밀번호 정책설정 (복잡성, 변경주기) 2 자동변경(Job Schedule), 수동변경 3 비밀번호 키관리
비밀번호 프로세스	**비밀번호 Life-Cycle** 1 비밀번호 사용신청 및 승인결재 2 비밀번호 인증키 발급(메일, 문자, OTP) 3 사용자별 접속 가능 계정 및 서버 지정 4 서버별 계정 및 비밀번호 관리
접속 및 감사로그	**로그 및 이력관리** 1 비밀번호 발급 및 변경 이력 2 비밀번호 변경 관리 모니터링 3 감사로그 생성 및 보고 4 비밀번호 암호화 백업

C. 솔루션별 특징

솔루션의 기능은 제품별로 큰 차이는 없으나, 계정관리 및 접근제어 시스템이나 2차 인증(OTP, 생체인증 등) 시스템과 연동하여 접근보안을 강화 할 수 있는 솔루션들이 있습니다. 솔루션 도입 시 당사 현황에 적합한 제품으로 선정될 수 있도록 대상 시스템 사전조사가 필요합니다.

개발사	제품명	솔루션 기능		
		비밀번호 관리	자체보안	지원시스템
에스지앤	SecureGuard PM	▪ Rule 엔진을 통한 패스워드 자동관리 ▪ 자동/수동 패스워드 변경 ▪ 패스워드 변경 스케쥴 설정 ▪ 비밀번호 관리 대장 제공 ▪ 결재 시스템을 통한 패스워드 임시 사용 허용	▪ 어플라이언스 자체 방화벽 ▪ 디스크 암호화 ▪ 국정원 인증 암호화 모듈 사용 암호화 ▪ USB 실시간 백업을 2-Factor 인증	▪ GS인증 ▪ Unix/Linux ▪ Windows ▪ Active Directory ▪ N/W 제품 ▪ 보안 장비 ▪ Telnet/SSH 지원 기타 장비 ▪ VM ESX 가상화 등
시큐어가드 테크놀러지	APPM for Password	▪ 패스워드 재사용 방지 ▪ 패스워드 일괄 변경 기능 ▪ 계정 사용 권한 신청 승인 워크플로우 제공 ▪ 일회성 패스워드 신청/승인 ▪ 사전/사후 승인 기능 제공 ▪ 계정 소유자 패스워드 자동/수동 변경 ▪ 패스워드 변경 Verify 기능 ▪ 관리자 권한 위임 ▪ 요청/승인/사용 이력 보고	▪ 디스크 암호화 ▪ 디스크 Bay 잠금 ▪ 콘솔 로그인 제한 ▪ 2Factor 인증 ▪ 3차 USB 백업 ▪ 패스워드 암호화 ▪ 서비스 프로세서 및 패스워드 변경 모듈 보호	▪ GS인증 ▪ Unix/Linux ▪ Windows ▪ Active Directory ▪ N/W 장비 ▪ 보안 장비 ▪ 데이터베이스 ▪ 어플리케이션 ▪ 웹 기반 솔루션 ▪ 가상화 환경 등
에스엠에스	PASSVAULT	▪ 패스워드 자동/수동 변경 ▪ 사용신청 및 승인 결재 ▪ 1회성 키 제공 및 키를 통한 패스워드 확인 ▪ 패스워드 사용 후 재변경 ▪ 사용이력 보고서 제공 ▪ 요청/승인/사용 이력 보고	▪ 디스크 암호화 ▪ DB암호화 ▪ 2 Factor 인증 ▪ 서버 접근제한	▪ GS인증 ▪ Unix/Linux ▪ Windows ▪ Active Directory ▪ N/W 제품 ▪ 보안 장비 ▪ DBMS ▪ 어플리케이션 등
모두스원	GATEONE-PASS	▪ 패스워드 자동 관리 ▪ 패스워드 주기적 변경 및 수동 변경 기능 ▪ 사용 패스워드 자동 변경 ▪ Workflow 기능을 통한 비밀번호 결재 시스템 제공 ▪ 요청, 승인, 사용로그 및 보고서 제공 ▪ 접근제어와 통합 관리(옵션)	▪ 계정 패스워드 암호화 저장 ▪ 관리 시스템 파일 암호화 ▪ 관리 계정의 패스워드 암호화 ▪ 장애대비 USB 백업	▪ GS인증 ▪ Unix/Linux ▪ Windows ▪ Active Directory ▪ N/W 장비(L4,L2) ▪ SSH 지원 기타장비

[표 Ⅲ-15. 비밀번호 관리 솔루션별 특징]

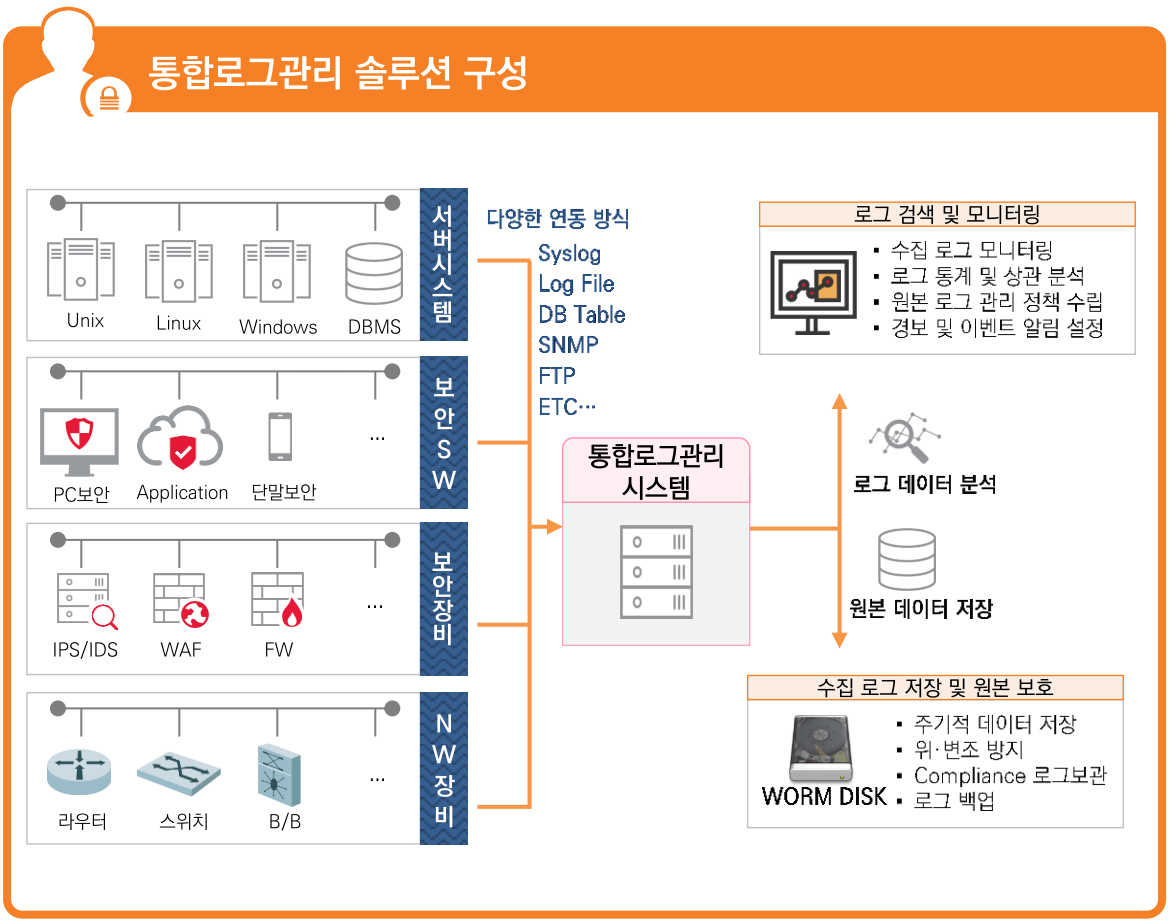
마.통합로그관리

A. 솔루션 개념

통합로그관리는 정보시스템에서 생성되는 다양한 로그를 수집, 저장하여 필요한 정보를 검색하고 분석하여 IT인프라 상태와 현황을 관리하는 솔루션입니다. 로그 데이터를 확인하여 사고의 원인분석 및 대응방안, 방어 대책수립이 가능하기에 로그 데이터의 수집 및 관리는 중요한 Compliance 요건입니다.

각각의 솔루션에서 발생하는 로그를 별도로 분석하고, 그에 대한 대응활동은 시간적으로나 구조적으로 어려움이 있었습니다. 통합로그관리 솔루션은, 이 기종 장비 및 어플리케이션에서 발생하는 로그를 통합 수집하여 로그 관리체계를 구축하며, 로그관리의 효율성과 로그의 상관분석을 통한 위협대응 방안을 마련할 수 있습니다.

통합로그관리는 ESM, SIEM과 구분이 되며, 개념을 정리하면, 통합로그관리 솔루션은 로그 수집, 저장, 분석이 기본이고 ESM은 이벤트 위주의 단시간 위협분석과 DBMS기반이며, SIEM은 빅데이터 수준의 장기간 심층분석과 Indexing기반이라는 것이 차이점입니다.



[그림 Ⅲ-15. 통합로그관리 솔루션 구성]

B. 주요기능

솔루션의 주요기능은 로그 수집 및 저장, 로그 검색 및 분석, 모니터링 및 시각화 세가지 기능 영역으로 나눌 수 있습니다. 상세 기준에 대해서는 △개인정보보호법, 정보통신망법 등 법규 준수를 위한 컴플라이언스 적용 △다양한 이기종 장비에서 발생한 로그통합 △상관관계 분석 △장애원인 추적가능 △사고/침해 예방 및 원인 규명 △감사 증적 자료 △데이터 무결성 보장(원본로그가 훼손되지 않음) △대시보드 등으로 정의할 수 있습니다.

다양한 수집환경(보안, Network, OS, Database, Application 등)에서 제한 없는 로그 수집이 가능해야 하고, 수집된 다양한 로그의 형태들을 표준 포맷으로 통합할 수 있어야 하고, 로그를 기반으로 보안·운영·감사 측면에서 식별 및 사용이 가능한 유용한 정보를 제공하며, 기업의 보안관리 및 감사 프로세스를 수행할 수 있어야 합니다.

기능영역	주요 기능 내용
로그 수집 및 저장	**로그 수집 및 저장** 1 OS System Log(syslog, wtmp, utmp 등) 수집 설정 2 Network, 보안장비 등 Appliance 로그 수집 설정 3 Application 발생 로그 수집 설정 4 수집로그 암호화 저장 및 관리 정책 수립
로그 검색 및 분석	**로그 검색 및 분석** 1 빅데이터 기반 로그 처리 시스템 2 실시간 로그 검색 기능 지원 3 정규화, 필터링, 키워드 검색 등 다양한 검색 기능 제공 4 수집로그의 상관분석 기능
모니터링 및 시각화	**모니터링 및 시각화** 1 실시간 수집 로그 모니터링 2 분석 통계 및 수집 데이터 시각화 UI 제공 3 원본 로그 보존 및 보고서 기능 제공

C. 솔루션별 특징

통합로그관리 솔루션은 이 기종 시스템의 로그를 수집 후 위·변조 방지의 저장기능 중심에서, 로그 분석 및 시각화 기능이 강조되며, ESM, SEIM과 같은 통합보안관제 영역의 기반이 되고 있습니다.

개발사	제품명	솔루션 기능		
		로그 관리	로그 분석	특징
이너버스	LogCenter	▪ 원본로그 위·변조 방지 ▪ Application, 장비, 서버시스템, DB 등 이 기종 로그 수집 ▪ 원본 로그 암호화 ▪ 비정형로그,SNMP,DB,FTP등 다양한 수집방식 지원 ▪ 시스템/DBMS/Application/NW/Security/가상화 이기종 로그수집 지원	▪ 문법활용 다차원 상관분석 ▪ 지능형 고속검색 ▪ 보고서 지원 ▪ 사용자 정의 시각화 보드 ▪ 실시간 탐지	▪ CC인증 ▪ 국내 로그분야 특허 보유 ▪ APT및 DDOS등 외부공격 감지 및 대응 ▪ 이상징후 탐지 및 BigData 처리 등 SIEM 기능 영역 확대 지원
시큐브	LogGriffin	▪ 수집 Agent와 수집 서버간 암호화 통신 ▪ Agent,SNMP,FTP,SCP등 다양한 수집 방식 지원 ▪ CPU부하에 따른 로그 수집 속도 조절 ▪ 원본로그 WORM 스토리지 저장 ▪ 시스템/DBMS/Application/NW/Security/가상화 이기종 로그수집 지원	▪ Big Data 분산검색엔진 적용 ▪ 비정형연관분석 ▪ 사용자정의 Query 기반 검색 ▪ 보고서 지원 ▪ 사용자 Dashboard 지원 ▪ 실시간 상관관계 탐지 및 분석	▪ CC인증 ▪ 분석체인을 이용한 사용자 선택기반의 비정형 연관분석 특허기술 보유 ▪ 원본로그 보관 관련 컴플라이언스 가이드라인 ▪ Soft WORM 스토리지를 통한 데이터 보존
나일소프트	LogCops	▪ 실시간, 배치 및 포워딩 로그 수집 ▪ WORM,DVD/CD, JukeBox 장비 등 원본보호 ▪ 시스템로그, Web, FW, IDS등 다양한 장비 로그 수집 ▪ 서버보안체제 구축으로 로그의 위·변조 차단 ▪ 시스템/DBMS/Application/NW/Security/가상화 이기종 로그수집 지원	▪ 기본검색, 고급검색, 연관검색, 패턴검색, 차트 등 다양한 검색 제공 ▪ 로그 보고서 엔진 제공 ▪ 로그검색 즉시 보고서 제공 ▪ 검색 템플릿 및 보고서 템플릿 마법사 제공 ▪ 실시간 로그 View 모니터링 제공 ▪ 실시간 로그 탐지 및 해킹여부 탐지	▪ CC인증 ▪ 별도의 인덱싱 작업이 필요 없는 로그 수집, 분석 지원 ▪ 무제한 결과 내 검색 기능 및 순차 정렬 ▪ 고성능 트랜잭션 처리기방의 Memory Q System 분석처리 엔진 탑재
디에스앤텍	LogSaver	▪ 이 기종 장비 로그 수집(서버, NW, 보안장비 Application 등) ▪ TIOR(사용자키로그) 수집 ▪ WORM Disk, Blu-Ray 등 다중저장 및 원본로그 장기 보존 ▪ 원본 데이터 암호화 ▪ 시스템/DBMS/Application/NW/Security/가상화 이기종 로그수집 지원	• Web Dashboard 제공 • 중요서버의 작업내역 분석 및 실시간 모니터링 제공 • I/O 전문에 대한 형상관리 지원 • 포렌식 기반의 원본 로그 분석	▪ CC인증 ▪ 원격 접속을 통한 작업내역 로그 저장 기능 (TIOR) ▪ 무결성 저장 기능 강점(로그 생성시 즉시 Blu-Ray, WORM 저장)

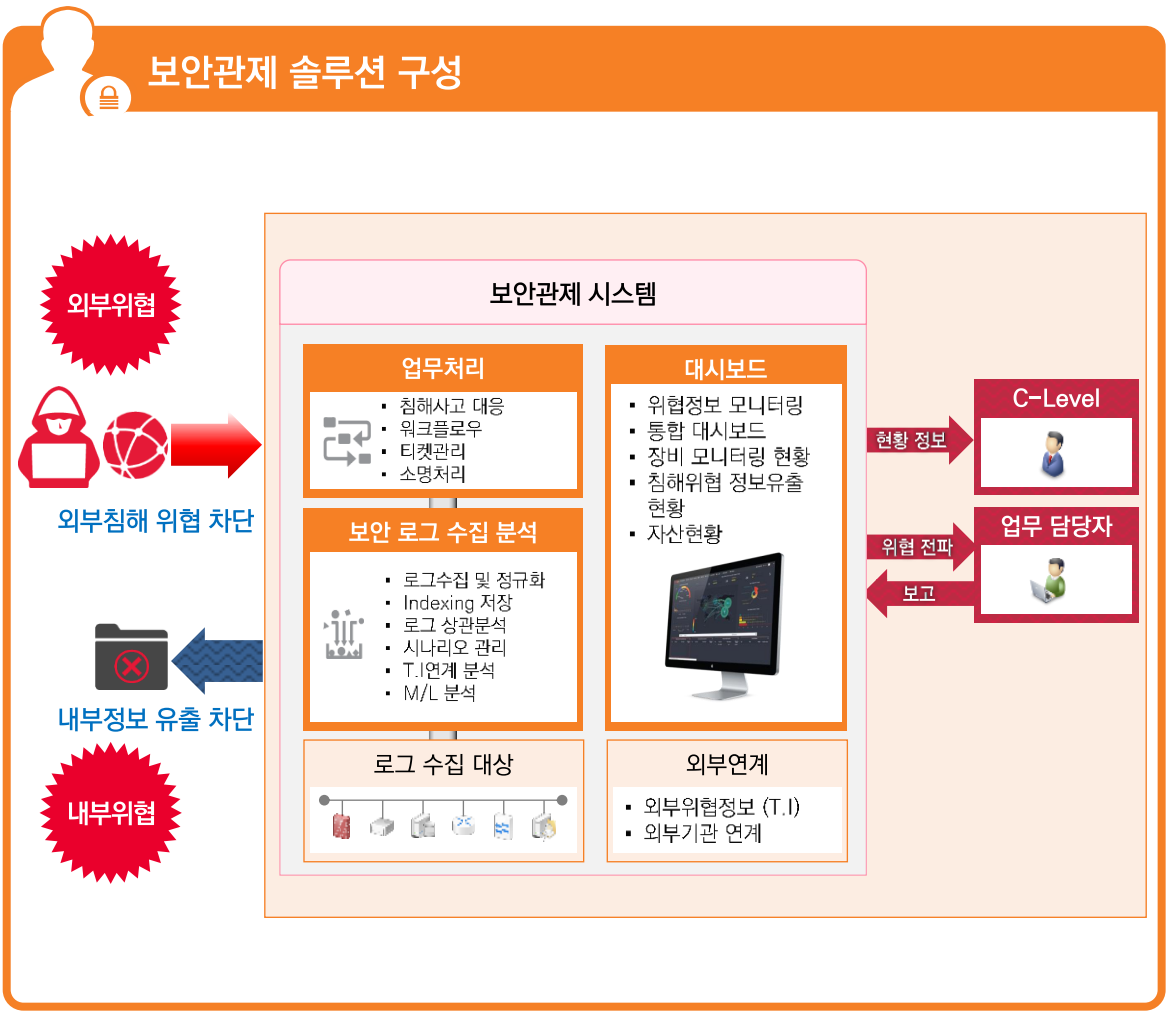
[표 Ⅲ-16. 통합로그관리 솔루션별 특징]

바.보안관제시스템

A. 솔루션 개념

본 장에서의 보안관제시스템은 SIEM(Security Information & Event Management)을 기준으로 설명 드리겠습니다. 최근 보안관제를 위한 솔루션은 빅데이터 분석기술과 통합하고, 지능적 상관분석 플랫폼으로 진화하고 있습니다. 종전 방식의 시그니처 기반 탐지의 한계를 극복하고 기업 IT인프라 전반의 빅데이터를 실시간으로 분석해 잠재적 위협을 식별한다는 방향입니다.

이를 위해서는, 정형/비정형 데이터와 로그 데이터에서 침입정보를 신속히 분석하고 예측해야 합니다. 분석기술에서는 사용자행위분석(UEBA), 데이터 학습을 통한 머신러닝 알고리즘 분석, 외부위협정보(Threat Intelligence)연계분석 등으로 방어적인 탐색 기능에서 예방적인 대응기능과 모델링 툴 분석 적용으로 발전하고 있습니다. 보안관제 영역에서는 외부침해위협과 내부정보 유출방지를 위한 IT인프라의 모든 서버와 어플리케이션 로그를 취합 분석하고 내·외부 통합을 통한 전사적인 통합로그 분석 플랫폼으로 변화하고 있습니다.



[그림 Ⅲ-16. 보안관제 솔루션 구성]

B. 주요기능

보안관제를 위한 시스템은 최근 대용량 데이터 분석이 확대되면서, 수집/저장 시 용량산정을 중요시하게 되고 있어 Scale-Out과 Scale-Up의 확장개념이 적용되고 있습니다. 저장된 데이터는 탐지/분석영역에서 룰, 시그니처, 시나리오 기반의 규칙을 미리 정의하여 탐지 정책을 수립하고, 위협탐지 영역을 자동화하고 확대하기 위해 머신러닝의 알고리즘을 적용하여 탐지영역을 확장하고 있습니다. 다음 단계로 탐지 현황과 운영현황을 모니터링 할 수 있고 이벤트 프로세스를 대시보드 형태로 가시화 하는 영역이 있습니다.

최근 SIEM 시스템에 대한 동향은 빅데이터를 활용한 데이터 학습활동으로 머신러닝 모듈을 적용하고 있지만, 실질적으로 아직 충분한 결과를 보장하지는 않고 있습니다. 외부의 위협정보를 공유하여 분석활동에 적용할 수 있는 위협정보 공유도 글로벌 정보, 공공기관, 벤더사에서 활발히 이루어 지고 있습니다.

기능영역	주요 기능 내용
데이터 수집	**보안로그 수집 및 저장** 1 보안장비 원본 로그 수집 (Agent, Agentless) 2 로그 정규화 및 인덱싱 (용량산정에 따른 공간확보) 3 네트워크 트래픽 로그 수집 (Option)
분석 및 탐지	**로그 검색 및 분석/탐지** 1 로그 검색 및 연관 검색 (대용량 데이터 성능 확인) 2 상관 분석, IP평판 분석, 행위분석, 위험도 분석 3 시나리오 관리 및 도출 4 탐지대응 및 티켓팅 프로세스
모니터링	**모니터링 및 시각화** 1 대시보드 제공 실시간 수집 통계 모니터링 2 실시간 보안관제 모니터링 3 상관분석 결과 및 기타 감사 보고서 기능 지원

C. 솔루션별 특징

최근에는 빅데이터 기반기술은 대용량 데이터 처리를 위해 하둡(Hadoop) 기반의 분산형 데이터 처리기술이 이루어지고 있습니다. 빅데이터를 이용한 머신러닝 기반의 관제 고도화를 통해 수집된 보안위협 정보를 스스로 학습하고 공격유형, 우회패턴, 이상징후 등을 분석하여 지능형 보안 위협에 대한 탐지대응이 가능하도록 구축되고 있습니다.

개발사	제품명	솔루션 기능		
		수집	분석	특징
시큐레이어	eyeCloudSIM	▪ 에이전트 및 다양한 프로토콜 지원 ▪ 데이터 정규화 ▪ 로그 수집, 분산처리, 인덱싱 및 저장 ▪ 병렬확장 아키텍처 구조 성능저하 최소화 ▪ 네트워크 flow 모니터링	▪ 이벤트 상관분석 및 네트워크 가시성 확보 ▪ 위협분석을 위한 데이터 시각화 제공 ▪ 빅데이터 배치 분석 ▪ 인메모리 방식 지원 ▪ 자산별 위협 분석 지원 ▪ NetFlow 및 Sflow 네트워크 모니터링 지원	▪ CC인증 ▪ 빅데이터 기반의 AI플랫폼 ▪ 관제 티켓팅 업무처리
LogPresso	LogPresso	▪ 네트워크 프로토콜, 에이전트 방식의 수집 ▪ 정확한 증분 데이터 수집 ▪ 데이터 정규화 필터링 및 가공 ▪ 데이터 수집 이중화	▪ 스트리밍 분석 ▪ 배치 분석 ▪ 실시간 분석 ▪ 다양한 원천 데이터 통합 분석 ▪ 그루비 및 자바스크립트 확장 ▪ R 연동 분석	▪ CC인증 ▪ 관제 티켓팅 업무처리 (SONAR) ▪ 머신러닝
Splunk	Splunk	▪ 범용 데이터 수집 Agent ▪ 데이터 수집 및 인덱싱 ▪ 형식이나 위치에 관계없이 모든 머신 데이터를 인덱싱 ▪ 표준방식의 API 제공 기존 프로그램에서도 사용 가능 ▪ 다양한 프로토콜을 지원 ▪ 분산 배치 수집 및 확장성	▪ 시간, 위치 또는 사용자 지정 검색 결과를 기반으로 상관 ▪ 머신 러닝 기능 ▪ 트랜잭션 명령어를 사용 실패한 트랜잭션을 조사	▪ 보안패키지(Enterprise Security) ▪ 머신러닝 툴킷
IBM	Qradar	▪ 로그 수집을 위한 다양한 프로토콜을 지원 ▪ Auto-Discovery기능 ▪ 정규화 및 인덱싱 기능 ▪ 네트워크로부터 Flow정보를 수집, 분석	▪ 상관관계 분석 ▪ Well-Known 포트에서의 봇넷 탐지 ▪ 사용자 의심 행위 탐지 ▪ 정보 유출 탐지 ▪ 포괄적 상관관계 분석	▪ 중앙 집중화 Web 기반 대시보드
MICRO FOCUS	ArcSight	▪ 다양한 프로토콜을 지원 ▪ 자동 이벤트 파싱 지원 ▪ 정형화, 카테고리화 ▪ 로그 표준화(CEF)를 통한 관리성 향상	▪ 상관관계 룰 작성 ▪ 평판기반의 인텔리전스 지원 ▪ RepSM 분석을 통한 내부 감염자산 모니터링 ▪ 영상,개인정보 암호화	▪ Event Graph를 통한 공격의 contextual 분석 지원

[표 Ⅲ-17. 보안관제시스템 솔루션별 특징]

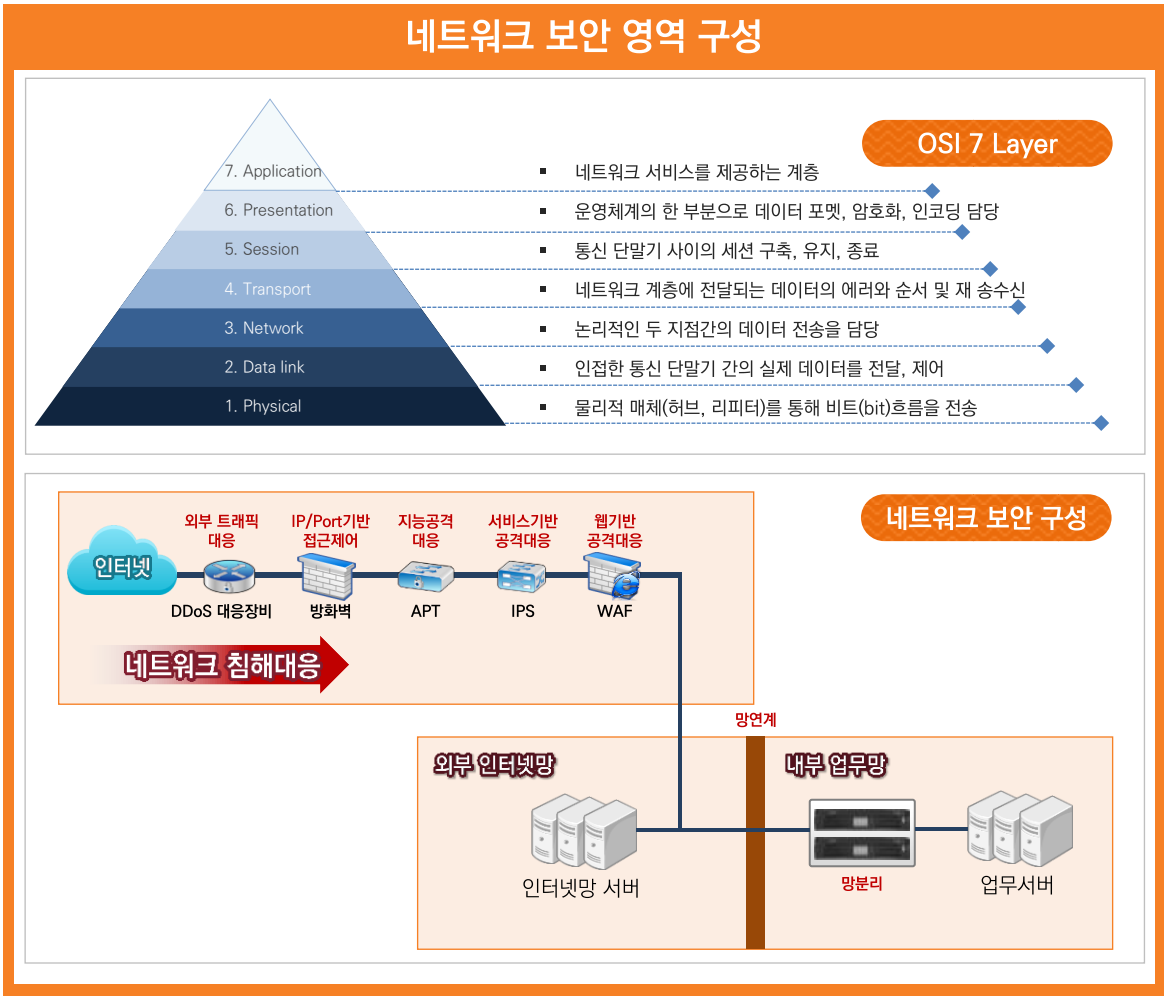
Part 3

네트워크 보안

1) 네트워크 보안 개념

네트워크 보안은 시스템 보안과 다르게, 주로 침해위협에 관련된 데이터의 이동에 대한 보안입니다. 네트워크를 이해하기 위해서는 우선, OSI(Open System Interconnection) 7계층에 대해서 알아야 합니다. 외부로부터의 직·간접적인 위협인 해킹기술에 대해서도 종류와 방법을 알아야 합니다. 그 이후에 해킹을 방어하기 위해 어떤 보안 솔루션이 있고 기능이 무엇이 있는지도 소개해 드리겠습니다.

네트워크와 관련된 해킹기법은 스니핑, 스푸핑, 세션 하이재킹과 같은 오래된 기법과, 최근에는 서비스 거부 공격(DoS)이나 무선 랜 공격의 경우와 같이 새로운 형태로 나타나고 있습니다. 또한, 임의로 파일을 암호화하여 금전을 요구하는 랜섬웨어와 같은 해킹기법이 다양하고 고도화되고 있습니다.



[그림 Ⅲ-17. 네트워크 보안 영역]

2) 보안 영역별 특징

단순히 네트워크 보안영역을 솔루션으로 명확히 구분하여 외부위협을 방지할 수는 없으며, 복합적인 보안솔루션 적용과 기능을 고도화하여 네트워크 상의 침해위협으로부터 보안을 강화해야 합니다. 네트워크 최적화의 필수 구성요소인 네트워크 보안 솔루션은 데이터 보안정책, 긴급사태 및 재난복구계획, 정기적인 취약점점검 및 모의해킹까지 마련해야 합니다.

구분	보안솔루션 영역	목적	일반 주요기능	최신기술 및 특징
1	방화벽	미리 정의된 보안 규칙에 기반한, 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어함.일반적으로 신뢰할 수 있는 내부 네트워크, 신뢰할 수 없는 외부 네트워크 간의 장벽을 구성	▪ 관리자가 방화벽에 통과시킬 접근과 그렇지 않은 접근을 명시하고 수행 ▪ 룰셋 설정과 변경, 관리자의 접근, 네트워크 트래픽의 허용 또는 차단과 관련한 사항을 로깅 ▪ 한 방화벽에서 다른 방화벽으로 데이터를 암호화 전송	▪ IP관점 통제에서 어플리케이션 통제가 가능한 차세대 방화벽으로 진화함 ▪ 기존 방화벽에 다양한 보안 솔루션에 기능이 함께 포함됨
2	웹방화벽	일반적인 네트워크 방화벽 (Firewall)과는 달리 웹 애플리케이션 보안에 특화되어 개발된 솔루션으로 SQL Injection, Cross-Site Scripting(XSS) 등과 같은 웹 공격을 탐지하고 차단하는 것을 목적으로 함	▪ OWASP 및 SANS 등에서 정의한 주요 웹 어플리케이션 취약점 대응 가이드라인을 기반으로 침해 모니터링 및 탐지/차단 기능 제공 ▪ 현재 알려졌거나 알려지지 않은(Zero-Day Attack) 보안 위협으로 부터 방어기능 수행 ▪ 어플리케이션 레벨에서 발생하는 서비스 거부 공격 방어기능 수행 ▪ SSL, PKI 등과 같은 암호화된 전송 데이터 분석 및 차단기능 제공 ▪ 실시간 컨텐츠 모니터링을 통한 컨텐츠 변조 감시 및 복구 기능 제공	▪ 새로운 취약점을 포함한 알려지지 않은 공격(제로데이 공격)에 대응하기 위해 머신러닝 적용 중 ▪ 클라우드 환경을 위한 서비스형 WAF 수요 증가
3	NAC	일련의 프로토콜들을 사용해 엔드포인트 (Endpoint)가 처음 내부망 네트워크에 접근 시도를 할 때 기존 내부망에 피해를 끼치지 않도록 접속하는 모든 기기를 검사, 악성코드에 감염되거나 기업 보안정책에 따르지 않는 기기를 차단함	▪ 내부직원 역할기반 접근제어 ▪ 네트워크의 모든 IP기반 장치 접근제어 ▪ PC 및 네트워크 장치 통제(무결성 체크) ▪ 해킹/Worm/유해트래픽 탐지 및 차단 ▪ 사내 정보보호 관리체계 통제 적용	▪ 적용 대상이 PC 및 모바일 디바이스를 넘어 IoT 디바이스에도 적용되고 있음 ▪ 클라우드 환경에 대응하기 위해 클라우드 버전 NAC도 출시됨 ▪ IPv6 환경 대응을 위한 기능을 탑재한 제품도 출시
4	APT	패턴, 시그니쳐 기반의 알려진 공격에 대한 대응으로 불가한 지능형 지속 위협(Advanced Persistent Threats) 공격에 대응하는 솔루션으로 기존의 보안 솔루션을 우회하는 공격에 대응함	▪ 가상 머신(샌드박스) 기반의 신종 악성 파일 분석 ▪ 파일 유입 및 유출의 양방향 트래픽 모니터링 ▪ 내부 PC의 유해 사이트 접근 및 봇(Bot)트래픽 탐지 및 차단 ▪ 내부 PC의 DDoS 공격 트래픽 탐지	▪ 대응 위치에 따라 네트워크 APT대응, 이메일 APT 대응, 엔드포인트 APT 대응으로 분류 ▪ 정찰, 무기화 및 전달, 익스플로잇/설치, 명령 및 제어, 행동 및 탈출 5단계로 분류되는 공격전 사이버 킬체인 중 하나를 차단하여 방어 성공하는 방식으로 구현

구분	보안솔루션 영역	목적	일반 주요기능	최신기술 및 특징
5	IPS	기존 트랙픽 유통에 직접적으로 관여하여 침입이 일어나기 전에 실시간으로 침입을 막고, 유해 트래픽을 차단하는 능동형 보안 솔루션으로 In-Line 방식으로 구성함	▪ OS나 Application의 취약점 을 능동적으로 사전에 예방 ▪ 외부에서 내부 네트워크로의 침입 방지 ▪ 위험 인지와 시스템 인지를 통해 능동적인 방어 제공 ▪ 비정상적인 트래픽 차단	▪ 위협 인텔리전스 연동을 통해 최소의 오탐과 잠재적인 공격으로 부터 보호 ▪ 머신러닝과 연동을 통해 알려진 또는 알려지지 않은 멀웨어 집단의 특징을 모방하는 네트워크 트래픽을 차단
6	DDoS	끊임없이 진화하고 다양한 기술을 사용하는 DDoS(Distributed Denial of Service) 공격을 하드웨어 또는 소프트웨어 방식으로 차단함	▪ 국가별/IP그룹/URL 평판분석을 통한 자동화 공격차단 ▪ DNS 요청 트래픽에 대한 탐지/방어	▪ 대규모 공격에 대응하기 위한 클라우드형 서비스 출시
7	망분리	법규정에서 정의하고 있는 망분리 요건을 충족하기 위한 물리적 망분리와 논리적 망분리 중 솔루션으로 가능한 논리적 망분리를 지원함	▪ 가상환경을 이용한 망분리 환경 구축 ▪ 가상환경내 환경 통제	▪ 기존 사용자 PC에 구성되는 클라이언트 방식 보다는 안정성과 관리효율이 높은 VDI방식 선호
8	망연계	망분리된 환경에서 인터넷망과 업무망간 실시간 데이터 연계(Streaming) 또는 파일전송(File Transfer) 서비스를 보안정책에 따라 안전하게 전송해 줄 수 있는 환경을 제공	▪ 서버 to 서버 또는 서버 to PC간 실시간 데이터 연계 필요 시 Streaming서비스 제공 ▪ PC to PC 환경에서 인가된 사용자들과의 파일 반입 반출을 위한 File Transfer 서비스 제공	▪ 망연계시 지연속도 최소화를 위한 다양한 방식의 솔루션들 제공

[표 Ⅲ-18. 네트워크 보안 영역별 특징]

3) 보안 솔루션 소개

가. 방화벽

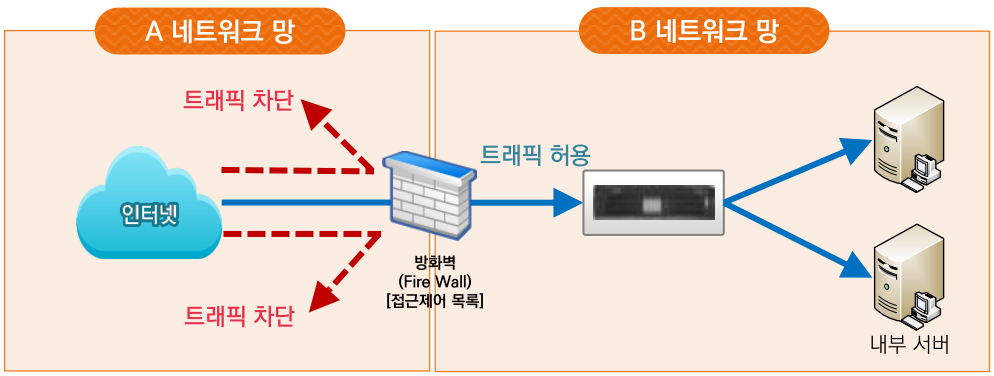
A. 솔루션 개념

인터넷 프로토콜(IP)로 접속되어 있는 네트워크 상의 장비를 인가되지 않은 침입으로부터 보호하기 위하여 게이트웨이(gateway)에 설치되는 접속 제한을 방화벽이라고 합니다. 인터넷에서는 한쪽 방향의 접속이 가능하면 역방향의 접속도 가능하기 때문에 IP로 접속되어 있는 네트워크는 외부에서도 접속할 수 있습니다. 이것은 접속을 제한함으로써 어느 정도 보안을 확보할 수 있는데, 구체적으로는 네트워크 간의 IP 패킷 전송을 차단하는 방법, 특정의 애플리케이션에 의한 패킷만을 전송하도록 하는 방법 등이 있습니다. 기본적으로 방화벽은 라우터(router) 프로그램과 밀접하게 동작함으로써, 모든 네트워크 패킷들을 수신처로 전달할 것인지를 결정하기 위해 검사하고, 여과합니다.

기본적으로 방화벽은 모든 접근을 거부 (deny) 한 후 허용할 접근만 단계적으로 허용(allow /permit)하는 방식입니다. 네트워크를 통해 데이터가 이동하는 통로를 '포트(port)'라 하는데, 방화벽은 기본적으로 약 65,000여 개의 통신 포트 모두를 차단한 후 접근을 허용하는 특정 포트만을 열어 두게 됩니다. 홈페이지 운영을 위한 웹 서비스(http)를 제공한다면 80 포트를, FTP 서비스(ftp)를 제공한다면 20/21 포트 등을 접근 허용해야 합니다. 통신 포트뿐 아니라 외부로부터 접근하는 IP 주소나 특정 프로그램에 따라 접근/거부 여부를 결정할 수 있습니다. 이러한 보안 규칙 설정이 모두 접근 제어 목록에 포함되어 일괄 적용됩니다.

이러한 방화벽의 개념에 따른 종류로는 패킷 필터링 방화벽(packet filtering firewall), 상태 기반 방화벽(Stateful Inspection firewall), 네트워크 주소변환(NAT)을 이용한 방화벽 등이 있습니다.

방화벽 기본 구성



[그림 Ⅲ-18. 방화벽 기본 구성도]

B. 방화벽 차단방식

NO	방화벽 차단 방식	방식 설명	기능 장점	기능 단점
1	패킷 필터링	데이터링크 계층에서 네트워크 계층으로 전달되는 패킷 헤더의 주소와 서비스 포트를 검색하여 서비스 허용 여부 파악	▪ 네트워크 계층 (전송계층에서 동작) ▪ 속도 빠름 ▪ 1세대 방화벽	▪ 패킷 내 데이터 파악 어려움 ▪ 패킷 헤더 조작 가능 => 보안상 취약점 ▪ 사용자 인증 및 로깅 약함 ▪ 패킷 필터링 규칙 검증 어려움 => 방화벽 부하
2	어플리케이션 게이트웨이	OSI 7계층 전 구간 동작, 페킷의 헤더안의 Data 영역까지 확인. 해당 서비스별로 프락시라는 통신 중계용 데몬이 구동됨. 이 것을 바탕으로 서비스 요청에 대해 방화벽이 접근 규칙을 적용하고 연결을 대신하는 역할을 수행	▪ 외부 network, 내부 network이 프록시 서버를 통해만 연결이 됨 ▪ 패킷 필터링 방화벽 보다 높은 보안 설정 가능 ▪ 일회용 패스워드를 이용한 강력한 인증기능 제공 ▪ Session에 대한 정보 추적 및 내용 보안 가능	▪ 응용 계층에서 동작, 네트워크에 많은 부하 예상 ▪ 일부 서비스에 투명성 제공 어려움 ▪ 하드웨어에 의존적 ▪ 새로운 서비스 추가 (새로운 데몬 추가) ▪ 시그니쳐 기반으로 미리 정의된 Application만 수용
3	서킷 게이트웨이	OSI 7계층 구조에서 5계층(세션) ~ 7계층(응용) 사이에서 접근제어를 실시하는 방화벽을 지칭. 서비스별로 프락시가 존재하는게 아니고 어느 서비스도 이용할 수 있는 일반적이고 대표적인 프락시가 존재함	▪ 내부 IP 주소를 숨길 수 있음 ▪ 첫 패킷 검사 후, 다음 패킷은 전달만 함 ▪ 모든 서비스가 이용 가능한 일반적인 프록시가 존재 ▪ 수정된 클라이언트 프로그램이 설치된 사용자에게 별도의 인증 절차 없이 투명한 서비스를 제공	▪ 방화벽에 접속하기 위해서 서킷 게이트웨이를 인식할 수 있는 수정클라이언트 프로그램이 필요하므로 사용자에게 배포 혹은 사용 중인 프로그램을 수정해야 함
4	하이브리드	하이브리드 방식은 패킷 필터링과 어플리케이션 방식을 혼합한 것임. 패킷 필터링의 장점과 어플리케이션 방식의 장점을 결합한 방식으로 패킷 레벨 접근 제어뿐만 아니라 응용 프로그램의 사용자 제어의 장점을 가지게 됨	▪ 내부 보안 정책 및 어플리케이션 등에 맞추어 선택적인 보안설정 가능 ▪ 여러 유형의 방화벽 특징을 보유함으로써 모든 서비스에 유동적으로 대처가 가능	▪ 관리가 복잡함 ▪ 설치 시 전문적인 컨설팅이 필요함
5	상태추적 (Stateful Inspection)	앞의 패킷 필터링 방화벽 및 어플리케이션 게이트웨이의 장점만으로 방화벽으로 분류되었음. 방화벽의 보안정책(ACL)을 통해서 허용된 패킷은 일정 시간 동안 상태 테이블에 저장이 되고, 패킷이 올 때마다 OSI 7계층을 거치지 않고 방화벽에서의 상태 테이블의 허용된 내용을 통해 패킷을 통과시켜주는 방식임	▪ 모든 통신채널에 대해 추적 가능 ▪ 높은 필터링 기능 제공 ▪ 어플리케이션 방화벽과 같은 성능 저하가 발생하지 않음 ▪ UDP, RPC 패킷 추적이 가능 ▪ 패킷 내 데이터의 상태가 저장되고 지속적으로 갱신됨	▪ 상태목록에 DOS, DDOS 공격으로 인한 거짓 정보가 차게 되면 장비가 일시적으로 정지하거나 재가동 해야 함 ▪ 예기치 않은 상황에서 방화벽 재가동 시 현재 연결에 대한 모든 정보를 잃어버리게 되고 정당한 패킷에 대해 거부가 발생할 수 있음

[표 Ⅲ-19. 방화벽 차단 방식]

C. 주요기능

대부분의 방화벽은 정책 기반의 방화벽이며 다양한 수준의 정책으로 네트워크 간의 트래픽을 제어합니다. 초창기에는 IP/Port를 기반으로 허용/차단을 구분하였으며, 점차 고도화 되어 현재는 도메인, 트래픽의 바이트 수, 프로토콜 종류 등으로도 허용/차단하는 방식이 제공되고 있습니다.

기능영역	주요 기능 내용
접근 제어 (Access Control)	**룰셋 설정 및 접근제어** 1 방화벽 정책 (룰셋) 설정 및 변경 2 네트워크 트래픽 허용 및 차단
주소변환 (NAT[1])	**네트워크 주소 변환 기능** 1 외부에 드러나는 주소를 실제주소와 다르게 유지 2 IPv4 를 보다 효율적으로 내부에서 사용 3 포트 주소 변환 기능
인증 (Authentication)	**접속 Host 검증** 1 메시지 인증, 사용자 인증, 클라이언트 인증 방식 등 2 정당성 여부 인증 처리
감사/기록 (Auditing/Logging)	**이력관리 및 모니터링** 1 전체 트래픽 기록 유지 2 로깅 및 감사추적 3 실시간 차단/허용 내역 모니터링

1) NAT (Network Address Translation) : 내부 네트워크에서 사용하고 있는 사설 IP를 공인 IP로 변환하여 부족한 공인 IP 주소 부족 문제를 해결하는 동시에 내부 네트워크에 대한 보안도 강화하는 기능

D. 솔루션별 특징

1세대 방화벽인 Packet Filter는 1980년대에 등장했습니다. 일반적으로 라우터(Router)에 포함돼 있는 방화벽으로 IP Header, Port 정보로 접근을 허용하거나 차단하는 방화벽입니다. 2세대 방화벽 Stateful Inspection은 패킷 필터링 방화벽의 단점을 보완해 등장했으며, 트래픽의 흐름 안에서 포트 번호를 기반으로 트래픽을 분류해 필터링 합니다. 3세대 방화벽인 '차세대 방화벽'은 1·2세대 방화벽을 보완한 제품으로, 게이트웨이(Gateway) 경계에서 정책을 제어하고, 모든 트래픽을 검사할 수 있는 기능을 갖춘 방화벽을 의미합니다.

개발사	제품명	주요기능	솔루션 특징
안랩	AhnLab TrusGuard	▪ Stateful Packet Inspection 방식 ▪ Black & white List 기반 필터링 ▪ 정책 및 세션 수에 독립적인 성능 보장 ▪ 다양한 NAT 기능 지원 ▪ 정책 유효성 검증 기능 ▪ 사용자 기반 방화벽 정책 설정/관리 ▪ 정책/객체 자동 생성 지원 ▪ 애플리케이션 제어	▪ CC인증 ▪ C&C 탐지 및 차단 ▪ 글로벌 대응조직 ASEC 과의 대응
윈스	SNIPER NGFW V2.0	▪ 상황인식 위협 추정 – 네트워크 보안위협에 대한 트래픽 식별 분석 제어 – 트래픽 모니터링/추적 대응 관리 – 트래픽 이상징후 분석 ▪ 우회 접속 정보유출 원천 차단 ▪ SSL 검사로 암호 채널 공격 탐지 ▪ 애플리케이션 보안을 통한 응용계층 서비스 제어 ▪ 안티바이러스/안티스팸 ▪ 암호화 통신	▪ CC인증 ▪ 위협 추적 중심 지능형 차세대 방화벽 ▪ 트래픽 추적/분석을 통한 보안정책 수립 ▪ 주요 서버 정보유출 차단
넥스지	nexG FW V1.2	▪ Stateful Inspection 방식 ▪ 사용자 기반 보안정책 ▪ Zone, Domain 기반 보안정책 ▪ 사용자 인증 지원 ▪ 인터페이스/회선 상태에 따른 정책 변경 지원 ▪ NAT, Application, VPN 기능 지원	▪ CC인증 ▪ DNS 서버기능 제공 ▪ VPN 기능 제공 ▪ 자체 부하분산 처리기능으로 고성능 보장
Fortinet	FortiGate NGFW	▪ 애플리케이션 제어 ▪ FortiSandbox 클라우드 기능으로 멀웨어 분석 식별 ▪ 바이러스 백신 ▪ 웹 필터링 ▪ 침입방지 ▪ 콘텐츠 해체 및 재구성	▪ CC인증 ▪ ICSA보안인증 ▪ FotiGuard Labs 보안 서비스를 통한 지속적인 위협 정보 업데이트 ▪ 가트너 인증
CISCO	Cisco Firepower	▪ 정책기반 트래픽 제어 기능 ▪ 동적 위협 차단 ▪ 내부 네트워크 자산 가시성 제공 ▪ IP 기반, 도메인 기반, 파일 기반 평판 및 룰 업데이트 제공 ▪ IPS 기능 일부 제공	▪ 단독형, 중앙 집중형, 클라우드 기반 제공 ▪ 타사 대비 탐지능력 우수 ▪ CISCO 자체 보안 인텔리전스 제공

개발사	제품명	주요기능	솔루션 특징
소포스	XG Firewall	▪ 정책기반 트레픽 제어 기능 ▪ 동적 위협 차단 ▪ 알려지지 않은 위협 방어 ▪ 사고 자동화 대응 ▪ Web F/W 기능 일부 제공 ▪ 강력하고 간결한 룰 제공 기능	▪ 네트워크 영역 및 PC영역을 동시에 보호 ▪ 네트워크 영역 보안의 심플화 모토 ▪ 위험 가시성 및 레포팅 제공
주니퍼 네트웍스	SRX Service Gateway	▪ 정책기반 트레픽 제어 기능 ▪ VPN, Web F/W, IPS 기능 일부 제공 ▪ 알려지지 않은 위협 방어 ▪ JSA 위협 분석 기능	▪ SPC 카드 추가 탑재로 성능 업그레이드 가능 ▪ 클라우드 기반 위협 인텔리전스 제공

[표 Ⅲ-20. 방화벽 솔루션별 특징]

나. 웹방화벽

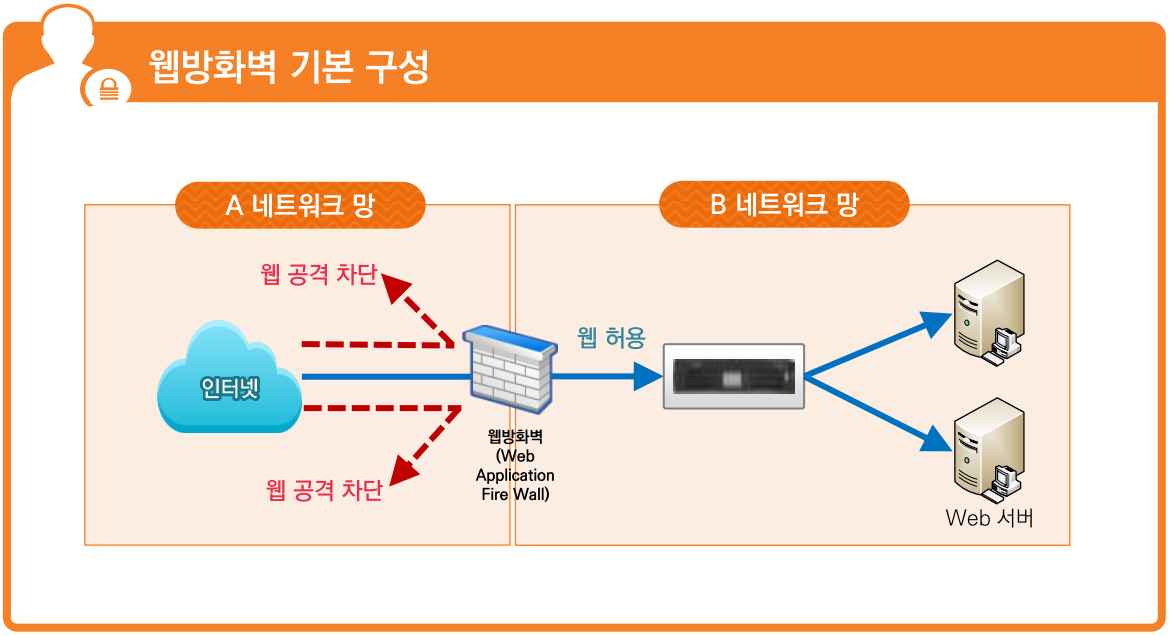
A. 솔루션 개념

웹방화벽((Web Application Firewall, WAF)은 기존 네트워크 레벨의 취약성에 대응하는 네트워크 방화벽의 웹 대응 한계에 따라 개발된 웹 어플리케이션 보안에 특화된 솔루션입니다. 인터넷으로부터 유입되는 트래픽 중에는 내부 웹 서버를 대상으로 하는 공격 패킷이 포함되어 있을 수 있으며, SQL Injection, Cross-Site Scripting(XSS) 등과 같은 웹 공격을 탐지하고 차단합니다. 직접적인 웹 공격 이외에도, 정보유출방지솔루션, 부정로그인방지솔루션, 웹사이트위변조방지솔루션 등으로 추가 활용이 가능합니다.

웹방화벽의 동작원리는 WAF 하단에 위치한 서버나 스위치, 기타기기 등의 웹으로 유입되는 패킷에 대해서 설정에 따라 차단, 탐지 하는 역할을 기본적으로 수행합니다. 예를들어, 물리적으로 WAF가 설치가 된 상태에서 하단에 서버가 위치해 있고 웹사이트를 사용한다면 그 웹사이트나 서버 IP로 injection, webshell, XSS 공격 등 웹으로 공격행위가 있었을 시 설정된 패턴에 의해 자동으로 차단이 되어 공격을 실시한 공격자에게는 에러메시지를 보여지게 합니다.

차단되는 패킷은 서버로 전달이 되지 않으며, 서버에서도 Log 확인이 되지 않습니다. 하지만, WAF에서 사용하는 Manager 에서 탐지되는 모든 Log는 검색이 됩니다. 정상적인 이용자가 http 나 https로 접속하고 사용을 한다면 패턴과 일치되지 않기 때문에 웹방화벽에서는 Log를 남기는 않습니다.

웹방화벽은 일반적으로 외부에서 유입되는 트래픽을 방화벽이 우선적으로 선별한 이후의 http 패킷을 분석하도록 구성합니다. 웹방화벽과 네트워크 레벨의 보안장비를 병행 운영하여 웹 어플리케이션 시스템을 보호하는 것을 권장합니다.



[그림 Ⅲ-19. 웹방화벽 기본 구성도]

B. 웹방화벽 구성방식

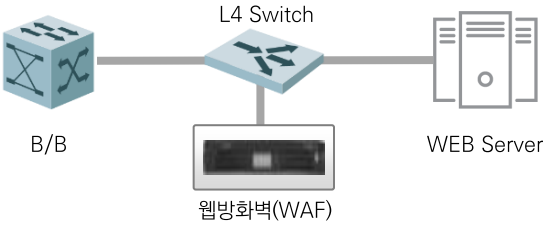
기존 네트워크 방화벽은 네트워크의 구성에 In-Line 방식으로 삽입되어 작동하지만, 웹방화벽은 Proxy[1]역할을 하기 때문에 One-Armed방식과 Mirroring방식이 추가로 설치 가능합니다.

웹방화벽 구성별 특징

[In-Line]

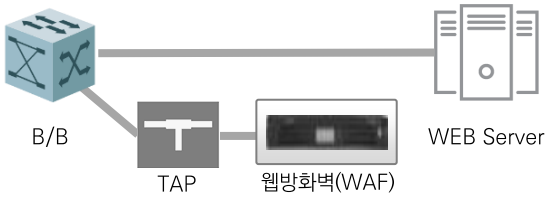
- 네트워크 경로상에 Bridge 형태로 In-Line 구성
- 탐지/차단 가능
- 장비 이상 시 Bypass 기능 필수
- 전체 트래픽이 웹방화벽을 통과하기 때문에 고사양 장비 또는 모니터링 패킷 선정 필요

[One-Armed]



- L4 Switch 에서 Port Redirection을 이용한 구성
- 탐지/차단 가능
- 기존 네트워크 환경 변경사항 없음
- 웹 서버 로그에는 사용자 IP로 웹방화벽의 IP가 남게 됨
- 한 개의 IP를 가진 웹서버를 10대 운용 중이면 웹방화벽에 할당할 VIP 10개가 필요

[Mirroring]



- TAP 또는 L2 switch의 Mirror 기능을 이용한 구성
- 기존 네트워크 환경 변경사항 없음
- 모니터링만 가능

[그림 Ⅲ-20. 웹방화벽 구성방식]

1) Proxy : 컴퓨터 네트워크에서 다른 서버로의 자원 요청을 중계하는 서버로, 분산 시스템의 구조를 단순화하고 캡슐화하여 서비스의 복잡도를 줄이는 역할을 한다. 일반적으로 Proxy는 대부분 Web Proxy를 말한다.

C. 주요기능

대부분의 기업에서는 네트워크와 시스템 보안에 대해서는 이해와 보안 솔루션 구축에 노력을 하지만, 웹 애플리케이션 계층은 고도화되고 있고, 종류도 다양하기 때문에 대부분의 보안 관리자들이 웹 애플리케이션 보안을 적용함에 있어서 어려움을 겪고 있는 상황입니다.

웹방화벽의 기본 역할은 웹 어플리케이션을 대상으로 하는 공격을 탐지하고 차단하는 것이며 주된 탐지방법은 http Packet을 검사하는 것으로 이루어집니다. http 트래픽을 원활히 컨트롤 할 수 있는 기능과, 웹방화벽의 운영업무 효율성과 생산성을 높이는 기능으로 고도화 되고 있습니다.

기능영역	주요 기능 내용
웹 공격 차단	**웹 공격 차단** 1 웹 공격에 대한 탐지 및 차단 수행 2 다양한 공격에 대한 요청/응답 기반 공격 탐지
정보유출방지	**개인정보 유출 방지** 1 개인정보 유출 공격 탐지 및 차단 2 주요 서버 정보 및 개인정보 유출 방지
부정 로그인 방지	**로그인 공격 탐지** 1 SQL 삽입 차단 2 과다 로그인 요청 차단
웹 위변조 탐지	**웹 위변조 탐지** 1 암호화된 HTTPS 통신 웹 보안 2 스크립트 삽입 차단

D. 솔루션별 특징

웹 보안을 위한 주요 솔루션으로 지능적이고 차별화된 기능이 추가되면서 차세대 웹방화벽으로 발전하고 있습니다. 솔루션 선정 기준은 HTTPS 트래픽 컨트롤과 운영 및 관리의 효율성이 중요합니다.

개발사	제품명	주요기능	솔루션 특징
펜타시큐리티시스템	WAPPLES	▪ 웹 공격 대응 ▪ 정보유출방지 ▪ 부정 접근 방지 ▪ 웹 위변조 방지 ▪ APT 등 신종공격 대응 ▪ 지능형 논리 분석 엔진 기반 알려지지 않은 공격 탐지 ▪ 3세대 기반 웹 방화벽으로 높은 보안 레벨 보장	▪ CC인증
파이오링크	WEBFRONT-K	▪ 웹 공격 대응 ▪ 정보유출방지 ▪ 부정 접근 방지 ▪ 웹 위변조 방지 ▪ 웹 트래픽 처리 및 리소스 사용 극대화 ▪ 보안 분석 및 통계 관리 ▪ 요청 검사, 응답검사, 학습, 위장 등 기능 제공	▪ CC인증
수산INT (트리니티소프트 양도 2020년)	WEBS-RAY	▪ 웹 공격 대응(OWASP 10대 취약점) ▪ 정보유출방지 ▪ 특정 URL 차단 ▪ 서비스 거부 공격 방어 ▪ 단계 별 탐지 및 차단 기능 ▪ 암호화 된 데이터 검사 기능	▪ CC인증 ▪ 정부중앙부처 95% 시장 점유율 ▪ Real-Time White-URL 기술 이용 ▪ Multi-Level 3단계 방어체제를 이용한 효율적인 처리시간
모니터랩	AIWAF	▪ 웹 공격 대응 ▪ WEB기반 직관적인 사용자 친화적인 인터페이스 ▪ 정보유출방지	▪ CC인증
Fortinet	FortiWeb	▪ 검증된 웹 애플리케이션 보호 ▪ 동작 기반 탐지로 알려지지 않은 공격 탐지 ▪ 지능형 시각 분석 도구 제공 ▪ 하드웨어 기반 가속화 기능	▪ 자사 방화벽 제품과 연동하여 APT 차단 ▪ 업계 최고의 보호된 WAF 처리량

[표 Ⅲ-21. 웹방화벽 솔루션별 특징]

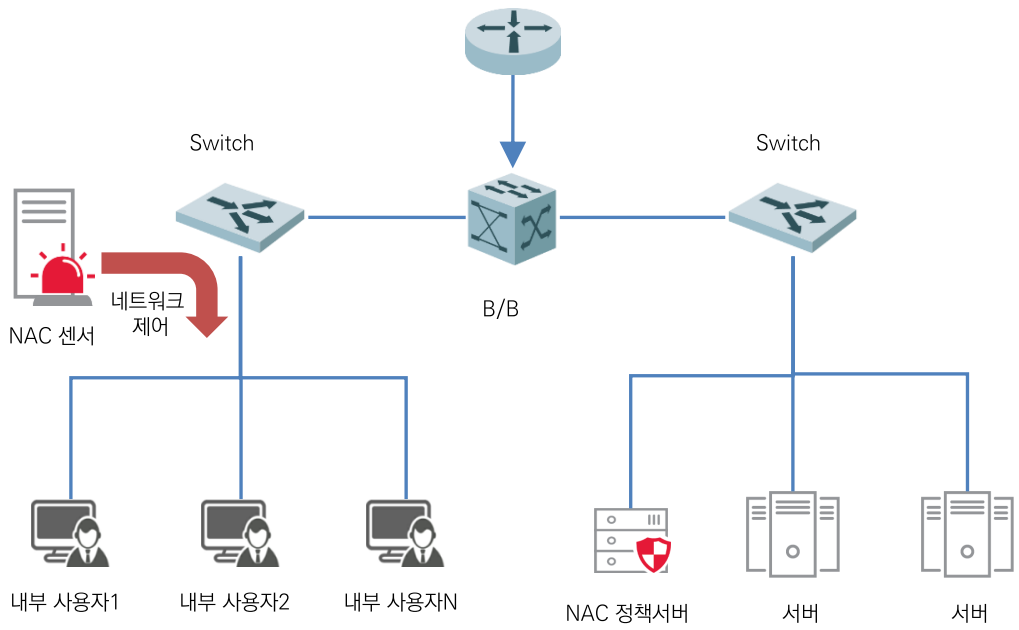
다. NAC

A. 솔루션 개념

NAC(Network Access Control)은 기본적인 IP관리 시스템에 네트워크 접근 제어를 제공하는 네트워크 보안 솔루션입니다. NAC의 접근 제어와 인증 기능은 일반적으로 MAC 주소를 기반으로 수행됩니다. 먼저 네트워크에 접속하려는 사용자는 네트워크 접속에 사용할 시스템의 MAC 주소를 IP 관리 시스템의 관리자에게 알려줘야 합니다. 관리자가 해당 MAC 주소를 NAC에 등록하면 사용자는 비로소 해당 네트워크를 사용할 수 있는 권한을 가집니다. NAC은 등록된 MAC 주소만 네트워크에 접속할 수 있게 허용해주므로 라우터로 구분된 서브 네트워크마다 에이전트 시스템이 설치되어 있어야 합니다.

NAC은 클라이언트가 네트워크에 접근하는 것을 통제할 뿐만 아니라, IP가 무질서하게 사용되는 것을 막아 가용 IP를 쉽게 확인할 수 있게 해주고, IP 충돌로 인한 문제를 막아줍니다. 또한 NAC은 보안 사고가 발생했을 때 공격자를 추적하는 데에도 도움이 됩니다. NAC에는 접속에 성공한 사용자에 대한 MAC 주소와 IP 주소의 매칭 뿐만 아니라 사용자 이름이나 소속 등을 기록하고 있어 공격 대상 시스템의 로그를 통해 공격자를 쉽게 찾아낼 수 있기 때문입니다.

NAC 기본 구성



[그림 Ⅲ-21. NAC 기본 구성도]

B. 주요기능

NAC의 기본기능은 사용자 인증을 통해 네트워크의 접근을 통제하여 허가되지 않은 비인가 장비들이 네트워크에 접근할 수 없도록 차단하는 것입니다.

주요기능으로는 사용자가 정해진 절차에 따라 네트워크에 접속할 수 있는 권한을 할당 받고, 외부에서 내부 네트워크에 접속하기 위해서는 적절한 승인 절차가 필요합니다. 클라이언트의 접속에 대한 인증을 수행하기 위해 클라이언트 시스템에 대한 자동 확인 장치를 고려할 필요가 있습니다.

또한, 네트워크를 사용자 및 업무 목적에 따라 적절히 분리하고, 공용 네트워크를 통과하는 네트워크 접속은 적절히 암호화되거나 보호되어야 합니다.

기능영역	주요 기능 내용
네트워크 접근제어	**네트워크 접근제어** 1 접근통제 정책 정의 2 사용자 및 IP 매핑으로 네트워크 접근 및 통제
사용자 관리	**사용자 관리** 1 ID/PW 등 네트워크 접근 인증 2 사용자 정보, 사용이력, 패치정보, 위치정보 관리
무선 네트워크 관리	**무선 네트워크 관리** 1 비인가 AP 탐지 및 차단 2 테더링 등 외부 네트워크 직접 연결 통제
패치 및 필수SW 관리	**프로그램 및 패치 설치유도** 1 필수 보안프로그램 설치 유도 2 패치 자동설치

C. 솔루션별 주요기능 비교표

개발사	제품명	주요기능		
		단말 인증	접근 통제	모니터링
지니언스	Genian NAC	▪ CWP 인증 제공 ▪ AD 인증 연동(SSO) ▪ 802.1x RADIUS 인증 제공 ▪ LDAP,SMTP,POP3, IMAP 외부인증 연동 ▪ SAML 인증 연동 ▪ 지문인식 및 OTP연동	▪ 비인가 단말의 네트워크 사용 통제 ▪ 방문자 단말 네트워크 사용제한 ▪ 단말 노드 그룹의 보안위협 수준에 따른 30여가지 제어 기법 제공 (경고/차단/격리) ▪ 불법 AP탐지 및 유무선 Agent통한 입체적 차단	▪ 대용량 로그 감지 기록 저장(빅데이터 엔진 적용) ▪ 실시간 로그 데이터 검색 ▪ 감사 기록 Full-Text 검색 및 Google Map 기반 실시간 이벤트 모니터링 지원 ▪ 국내외 40여개 보안제품 연동 통합관리 기능 ▪ 다양한 무선랜 상태 정보 ▪ 사용자 기반 AP위치정보
넷맨	SMART NAC	▪ 인사정보 시스템 연동 사용자 정보 동기화 ▪ 사용자 계정 신청 프로세스 ▪ 단말 및 IP지정 사용자 인증 ▪ 유·무선 통합 사용자 인증 서플리컨트 제공 및 이력통합 ▪ 사용자와 IP고정한 인증 Master지원(API제공)	▪ 비인가 단말 네트워크 접근통제 ▪ 그룹별 네트워크 접근제한 ▪ 불법 우회경로(테더링 등) 탐지 및 차단 ▪ 불법 DHCP서버, 유해 트래픽 탐지 및 차단 ▪ ARP 스푸핑 등의 네트워크 위험요소 탐지 및 차단 ▪ ARP기반 IP통제/SNMP이용한 IP관리/수동 IP입력관리	▪ 네트워크에 접속된 모든 단말 정보 실시간 자동 수집 및 관리 ▪ IP/MAC/호스트명/작업그룹/검출시간/최종감지시간 관리 ▪ 단말의 물리적인 네트워크 위치 추적관리 ▪ IP장애 이벤트 로그관리 ▪ 주요 네트워크 장비에 대한 맵 구성 및 장비 생사 판별 ▪ 주요 네트워크 장비 포트의 bps/pps 현황관리 ▪ 주요 스위치 포트에 연결된 단말의 IP/MAC정보 수집관리
한류AI센터	SAFE NAC	▪ PC 및 모바일 단말에 대한 802.1x 통합인증 제공 ▪ 보안 무결성 점검 및 조치	▪ 인가된 AP(SSID) 통제 ▪ 임계치 이상 트래픽 발생 노드 격리 ▪ 특정 트래픽(P2P) 등 탐지 차단 ▪ 네트워크(IP,포트,프로토콜, 서비스)등 사용권한 통제	▪ 인증, 제한 사용자 현황, 단말에 대한 설치 S/W 현황, 사용자별 IP 사용 현황 및 이력

개발사	제품명	주요기능		
		사용자 인증	네트워크 접근 제어	모니터링 및 가시성
스콥정보통신	IP Scan NAC	▪ IP/PWD 인증, 인사DB, AD인증 ▪ Web계정 신청 ▪ PC소유자 등록/변경/이력관리 (방문자/임시 포함)	▪ 권한별 접근통제 및 그룹간 통신제어 ▪ 과다 트래픽 차단 ▪ 비인가 IP/MAC 차단 ▪ 무선 장비 통제	▪ Agent 접속관리 및 미설치자 현황 파악 ▪ 과다 트래픽 모니터링 ▪ 이벤트 로그저장 ▪ 조회/리포트 기능 ▪ 시스템 현황 ▪ 검역 보고서 등 출력 ▪ 대시보드 제공
CISCO	시스코 ISE	▪ 유·무선 및 VPN 인증 ▪ 권한부여(TrustSec 기능 포함) ▪ 로깅 ▪ 802.1x RADIUS 인증 제공 ▪ LDAP,SMTP,POP3, IMAP 외부인증 연동	▪ 인증 및 권한관리를 통해 보안위협 있는 단말 체크 및 접근 차단 ▪ 단말 프로파일링 ▪ dACL, VLAN 항당, URL 리디렉션 등 광범위한 엑세스 제어	▪ 워크센터 통해 쉽게 설정 및 모니터링
엠엘소프트	Tgate	▪ 장비 및 사용자 인증 (ID/PWD, 공용PC인증, SSO인증, LDAP, AD인증)	▪ 정책기반 그룹간 접근제어 ▪ Guest제어 ▪ 외부 인터넷망 사용권한	▪ 유해트래픽 감지 및 모니터링 ▪ 로그, 리포트, 이력관리
포어스카우트 (ForeScout)	ForeScout CounterACT	▪ 사용자가 허용된 장치를 사용해야만 네트워크 자원에 접근 허가	▪ Wi-Fi 네트워크에 연결된 휴대용 모바일 장치 탐지 제어 ▪ 행위기반으로 악의적인 공격 차단	▪ 실시간, 다방면 네트워크 가시성 및 제어 ▪ 사용자, 어플리케이션, 프로세스, 서비스, 포트, 외부장비 등을 추적 및 제어 ▪ 정책준수 등급 모니터링 ▪ 감사 요구사항 ▪ 통합 레포팅

[표 Ⅲ-22.NAC 솔루션별 주요기능 비교표]

D. 솔루션별 특징

사물인터넷과 스마트시티 확산에 따른 네트워크의 다양화와 보안위협의 지능화로 최근 네트워크 접근제어 솔루션은 각종 스마트 기능으로 무장하고 있습니다.

개발사	제품명	주요기능	솔루션 특징
지니언스	Genian NAC	▪ 네트워크 관리 – 네트워크 접근제어 – 무선 네트워크 인프라 접근 통제 – IP 관리 ▪ 단말 관리 – 네트워크 보안관리 – PC 보안 – 모바일 관리 ▪ 내부 보안 정책 – PC 자산 관리 – 패치 관리 – 어플리케이션 관리 – 보안서약 동의 ▪ 사용자 관리 – 사용자 인증	▪ CC인증 ▪ 유 무선 인프라 통합구축 ▪ 클라우드 기반 플랫폼 분석 ▪ 대용량 로그 분석 가능 ▪ 단말의 취약점(CVE)관리 ▪ Agent less 방식의 구현 가능
넷맨	SMART NAC	▪ 네트워크 접근 통제 ▪ 사용자 인증 ▪ PC보안 관리 ▪ 패치 관리 ▪ IP 사용 현황 및 장애 모니터링 ▪ IP/MAC 통제 ▪ 네트워크 트래픽 현황 관리 ▪ DHCP 기능 제공 ▪ IPv6 제공 ▪ PC 자산관리	▪ CC인증 ▪ 유 무선 통합 네트워크 접근 제어 ▪ 강력한 IP/MAC 통제 ▪ IP6 네트워크 환경 대응 특허권 보유
한류AI센터	SAFE NAC	▪ 비인가 단말, 장비 네트워크 접근 차단 ▪ 단말, 모바일 인증 제공 ▪ 단말 무결성 검사 ▪ 필수 S/W 설치 유도 ▪ IP관리	▪ CC인증
스콥정보통신	IP Scan NAC	▪ 사내 네트워크에 접속되는 모든 단말기 접속 통제 ▪ 사내 자료 외부유출 방지 ▪ S/W 및 패치 설치유도 ▪ 단말 중앙관리 ▪ 외부 사용자 접근통제 ▪ 취약점 사전 점검 ▪ PC, 모바일, 단말, 서버, CCTV 등 IT자산관리	▪ CC인증 ▪ 기존 네트워크 환경에 영향 없는 설치 ▪ IPv6 지원을 통한 IoT 기기 제어 ▪ Agent 방식 및 Agentless 방식 혼합 구성 ▪ 네트워크 보안 위험요소 사전 제거 및 예방

개발사	제품명	주요기능	솔루션 특징
CISCO	시스코 ISE	▪ 유선/무선/VPN에 대한 인증, 권한부여(TrustSec 기능 포함), 로깅 ▪ 단말 프로 파일링, 단말 상태체크(포스쳐 기능) ▪ 게스트 관리 및 포탈 기능 ▪ 단말 OS, 백신 등 패치관리	▪ TACACS+ 프로토콜을 이용 ▪ 네트워크 장비 뿐만 아니라 3rd 파트 스위치 및 컨트롤러와 연동 가능 ▪ PxGrid 확장을 통한 자동화
엠엘소프트	Tgate	▪ 유무선 네트워크 접근통제 ▪ 유무선 인증 및 사용자 인증 기능 ▪ 고유 인증서를 이용한 사용자 인증 ▪ 필수 소프트웨어 설치, 악성 소프트웨어 제거 강제화 ▪ 파일/소프트웨어 존재여부 확인 ▪ 불법 무선 공유기 차단 ▪ 패치관리시스템 연동 시너지	▪ CC인증 ▪ 유무선 기기에 인증기능 수행
포어스카우트 (ForeScout)	ForeScout CounterACT	▪ 미러링 방식 제품 구성 ▪ 네트워크에 접근한 IP 기반의 모든 장비에 대해 정보수집 ▪ 수집된 정보 기반 인프라 보안준수요건에 따른 접근 통제 ▪ 위협 통제 및 자산관리 기능 ▪ IT Compliance 준수	▪ CC EAL4 인증 ▪ 중국 공안부 인증 ▪ 네트워크 위험 통제 및 보안컴플라이언스 기본 탑재 ▪ 전세계 NAC 제품 유일 미국방성 AIAAPL 인증

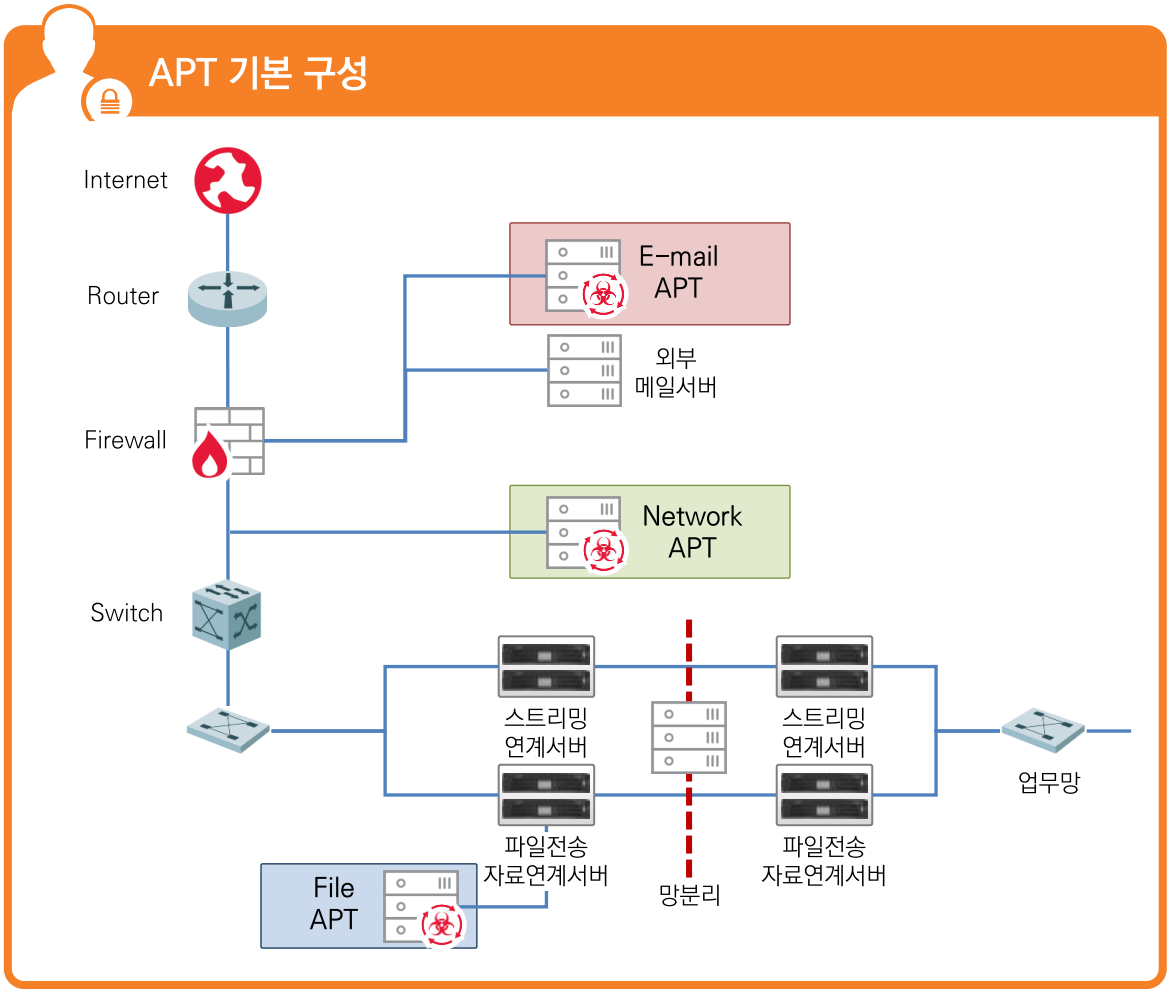
[표 Ⅲ-23. NAC 솔루션별 특징]

라. APT

A. 솔루션 개념

APT(Advanced Persistent Threat)란 지능화된 지속 공격으로, 외부에서 다양한 위협방식을 활용하여, 특정 기업이나 조직내부의 네트워크에 지속적으로 공격을 가하는 행위입니다. 이러한 행위는 짧을 수도 있지만 공격 기법에 따라 매우 길수도 있으며 대상의 정보를 탈취할 때까지 계속 진행됩니다. APT의 공격 기간은 평균 1년으로, 길게는 5년 가까이 공격을 하는 경우도 있어 APT의 공격을 당했는지는 확인하기 어려운 경우도 많습니다. 공격탐지의 효율성 강화를 위해서 심층 대응(Defense in Depth) 전략을 수립하는 한편, 새로운 보안 위협에 대한 신속한 대응을 위해 시큐리티 인텔리전스(Security Intelligence)를 확보해야 합니다.

솔루션으로는 일반적으로 외부로부터 유입되는 탐지 위치에 따라 네트워크 APT대응시스템, 이메일 APT대응시스템, 엔드포인트 APT대응시스템 등이 있으며 분석을 위한 APT 분석서버와 관리를 위한 관리서버가 제공되는 경우가 일반적입니다. 또한 망연계 솔루션이 도입되어 있는 경우 외부망에서 내부망으로 파일이 전달될 때 탐지하는 망연계용 APT대응 시스템도 구성할 수 있습니다.



[그림 Ⅲ-22. APT 기본 구성도]

B. 주요기능

일반적으로 APT는 5단계(정찰, 악성코드전달, 악성코드설치, 명령 및 제어, 행위 및 탈출)를 거쳐 공격을 진행합니다. APT 대응 시스템은 이러한 공격이 각 단계 별로 시작하기 전에 차단한다는 의미인 사이버 킬체인 방식을 기반으로 움직입니다. 예를들어 네트워크 APT 대응시스템과 이메일 APT 대응시스템은 정찰과 악성코드 전달 단계에서 활용되고 엔드포인트 APT 대응시스템은 악성코드 설치 단계부터 주로 활용됩니다.

기능영역	주요 기능 내용
APT 공격 Life-Cycle	**탐지/분석/적용/대응** 1 위협 탐지 및 방어 2 위협정보 분석 3 블랙/화이트 리스트 패턴 적용 4 공격정보 제공 및 제거/치료
탐지방법	**악성코드 탐지방법** 1 알려진 악성코드에 대한 빠른 탐지/차단 기능 2 샌드박스를 통한 알려지지 않은 신, 변종 악성코드 탐지/차단 가능 3 위협 탐지 엔진 4 파일 구조 분석으로 의심 파일을 탐지
모니터링	**대시보드 모니터링** 1 네트워크 플로우 분석 모니터링 2 이벤트 상관 분석 모니터링 3 악성 파일 분석 현황 4 주요 이벤트, 현황 정보 파악 5 주요 보안 이벤트 발생 시 알림(E-mail, SMS 등)

C. 솔루션별 특징

APT 제품은 장비 증가에 대비한 유연한 확장성과 통합관리를 위한 안정성 확보를 고려하여 솔루션을 선별 해야 합니다. 최근에는 사고 대응 결과 정보를 활용한 위협 인텔리전스 영역을 확보하여 서비스 될 수 있는 제품으로 구축되고 있습니다.

개발사	제품명	주요기능	솔루션 특징
Core Security (DAMBALLA)	Failsafe	▪ 탐지 – 알려지지 않은 위협 감지 – 다양한 OS에 대해 위협 탐지 – 네트워크기반 외부 위협 탐지 – 다양한 네트워크 접속 위협 정보 탐지 ▪ 관리 – 실시간 감염 장비의 탐지 정보 제공 – 장비에 대한 완벽한 포렌식 증거 제공 : 다운로드한 파일, 연결된 Site, 실행파일, DNS Query – Risk가 큰 장비부터 우선순의로 나열 – 다양한 인텔리전스 정보 제공	▪ 침투한 악성코드 검출 특화되어 있음 ▪ 머신러닝과 빅데이터 기반 외부위협 탐지 대응
안랩	MDS	▪ 위협 및 이상 트래픽 탐지/분석 – 주요 인터넷 서비스 프로토콜 수집 및 분석 – 파일 유입 및 유출에 대한 양방향 트래픽 모니터링 – 가상머신(VM)기반 분석을 통한 신종 악성 코드 분석 ▪ 이메일 기반 위협 탐지 및 격리 – 악성 또는 첨부파일 및 URL 포함 이메일 탐지 및 자동 격리 – 이메일 첨부파일, 본문 내 URL 동적, 다차원 분석 제공 – 라이선스 적용 방식임 ▪ 위협 대응 및 치료 – 탐지된 악성코드 감염 의심 호스트에 대해서 악성코드 치료 및 네트워크 격리 ▪ 통합 모니터링 및 로그 관리 – 주요 이벤트 정보 제공 – 실시간 악성코드 유입 현황 및 이상 트래픽 발생 확인 – AD연동을 통한 내부 사용자 정보 제공 – MDS 에이전트 미설치 호스트에 자동 배포	▪ CC인증 ▪ 에이전트 없는 방식과 에이전트 방식 제공 ▪ 네트워크 로우 데이터 저장을 동적 행위 및 동적 콘텐츠에 대해 분석 가능 ▪ 글로벌 인증기관 ICSA Labs 인증 획득 (2019.11)
엔피코어	Zombie Zero	▪ 탐지 – 행위기반 악성 코드 탐지 : 샌드박스를 통한 가성코드 탐지/차단 : 가상분석을 통한 오탐 최송화 – 폐쇄 환경 악성 코드 탐지 – 빠른 탐지 분석 환경 제공(Network, E-mail, File APT) – 장비 증가에 대비한 유연한 확장성 – 주요 보안 이벤트 발생시 알림 발송	▪ CC인증
TrendMicro	Deep Discovery	▪ 악성코드 및 APT 공격 탐지 ▪ 샌드박스 분석 ▪ 스피어 피싱 이메일을 통한 악성 컨텐츠 탐지 및 차단 ▪ 네트워크 상의 탐지 정보와 엔드포인트 분석 정보를 연계한 상세분석 제공(포렌직) ▪ 유해 C&C통신 탐지 및 차단 ▪ 멜웨어 네트워크 악성 행위 탐지	▪ 커스텀 샌드박스 ▪ Threat Intelligence Center ▪ 글로벌 인증기관 ICSA Labs 인증 획득

개발사	제품명	주요기능	솔루션 특징
FireEye	FireEye (NX,EX,HX)	▪ EX(이메일 보안) – 샌드박스 기반의 스피어싱 대응 – 동적 URL 분석 기능 – VM 성능 지원(자체 VM지원) – 스피어 피싱 이메일, 혼합 공격 방어 – 아카이브에 숨겨진 공격, 위협 이메일 분석 기능 ▪ NX(웹기반의 네트워크 보안) – 혼합된 스피어 피싱 공격 차단 – 역할 기반 접근 제어와 감사 기록을 제공 – 윈도우, 맥OS X 환경 지원 – 행위기반 분석 기능 – 동시 분석 기능 제공 – 실시간 C&C 접속 차단 및 악성 코드 유포지 차단 – APT빅데이터 기반 정보 제공	▪ 기술, 인텔리전스, 전문성을 통합하여 67개국의 2,700여 고객의 글로벌 방어 커뮤니티 공유
FortiNet	FortiSandbox	▪ 지능형 제로데이 멀웨어 탐지 및 방어 자동화하여 실시간 정보 제공 ▪ 보고 및 조사 도구 제공 ▪ 타사 보완 벤더 제품 연동 가능 ▪ 분석을 위한 파일 전송 및 결과 제공 ▪ 이메일 게이트웨이 및 방화벽을 통한 장치 격리 및 차단 ▪ 악성 코드 식별과 위험 등급 알림 기능 제공 : 지능적인 위협 치료	▪ NSS Labs, ICSA Labs 인증

[표 Ⅲ-24. APT 솔루션별 특징]

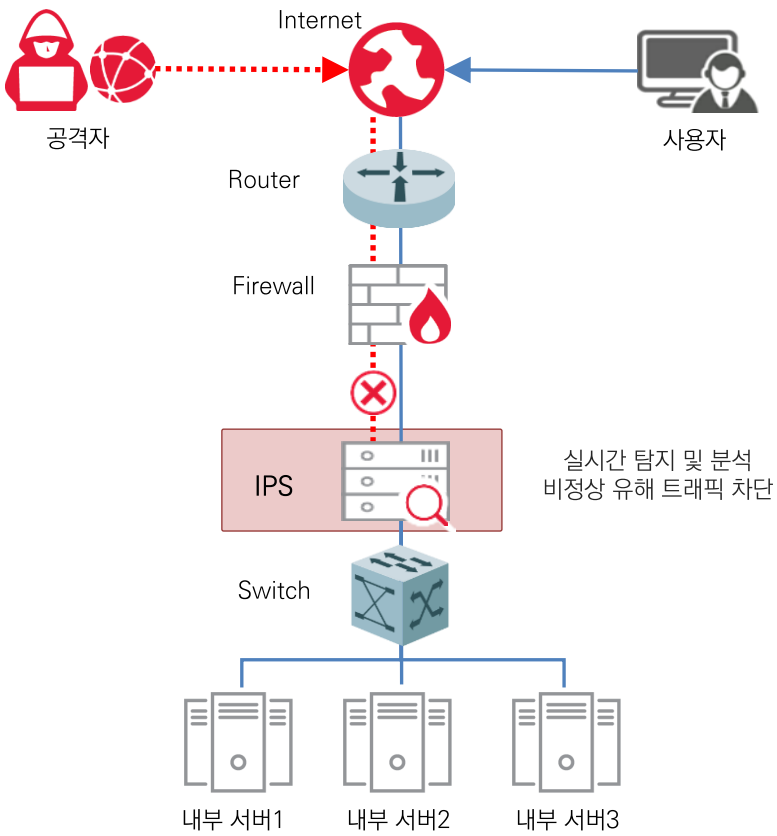
마. IPS

A. 솔루션 개념

IPS(Intrusion Prevention System)는 능동형 보안솔루션으로 인터넷 웜과 같은 악성코드 및 해킹의 유해 트래픽을 차단해주는 솔루션 입니다. 탐지된 공격에 대해 웹 연결을 끊는 등 능동적으로 방어하는 솔루션 입니다. 방화벽처럼 네트워크에 In-Line 모드로 설치되어 공격을 차단하는 네트워크기반 IPS와 서버 어플리케이션을 담당하는 호스트기반 IPS등의 두 종류가 있습니다. 네트워크기반 IPS는 네트워크 라인상에 위치하여 비정상적인 트래픽을 실시간으로 탐지, 차단하고 능동적으로 실시간 방어를 취할 수 있는 시스템이며, 호스트기반 ISP는 호스트에서 감사 기록이나 들어오는 패킷 등을 검사해 침입을 탐지 및 감염 차단을 수행하는 시스템입니다.

IPS는 기업 외부에서 내부 네트워크로의 침입을 방지하며, 공격이 실제 피해를 주기 전 미리 능동적으로 공격을 차단함으로써 공격 피해를 최소화할 수 있는 능동적 보안대책이라는 점이 큰 장점입니다. 또한 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제할 수 있습니다.

IPS 기본 구성



[그림 Ⅲ-23. IPS 기본 구성도]

B. 주요기능

IPS의 기본기능은 네트워크에서 침입이 탐지되면 바로 차단하여 인가자의 비정상적인 행위 등을 통제할 수 있는 시스템 입니다.

침입 탐지 기능을 수행하는 모듈이 패킷 하나하나를 검사하여 그 패턴을 분석한 뒤 정상적인 패킷이 아니면 방화벽 기능을 가진 모듈로 이를 차단합니다. 하지만 웜이나 악성코드의 공격기술이 점차 다양해지면서, 코드나 패킷 분석을 통해 탐지하는 방법의 한계가 발생하였습니다. 최근에는 침입 방지 시스템에 가상머신(Virtual Machine)을 이용한 악성코드 탐지 개념을 도입하여 적용하고 있습니다. 즉 가상머신에서 실행된 코드나 패킷들이 키보드 해킹이나 무차별 네트워크 트래픽 생성과 같은 악성코드와 유사한 동작을 보이게 되면 해당 패킷을 차단하게 됩니다.

기능영역	주요 기능 내용
침입 탐지 및 차단	**침입 탐지 및 차단** 1 웜/바이러스, 스팸메일, P2P 및 메신저 통신 등에 대한 비정상 네트워크 트래픽 탐지 및 차단 2 유해 정보 차단 및 내부정보 유출 차단
실시간 분석	**실시간 분석** 1 실시간 네트워크 및 시스템 부하량 모니터링 2 프로토콜/서비스/IP별 네트워크 트래픽 트렌드 상세 분석
패턴 업데이트	**패턴 업데이트** 1 신규 취약성, 위협에 대한 빠른 업데이트 2 위협 및 취약성 정보를 지속적으로 공급 받아 사전 대응을 위한 침입 패턴 DB 업데이트
네트워크 관리	**네트워크 관리** 1 방화벽에서 탐지 못하는 공격 탐지 기능 지원 2 외부로부터 유입되는 유해한 패킷을 제어

C. 솔루션별 특징

침입방지시스템 IPS는 알려지지 않은 공격도 방어할 수 있는 실시간 침입방지시스템으로 OS레벨에서 실시간 방어와 탐지 기능을 같이 제공하며, 기존 보안장비가 가지는 수동적인 방어 개념의 방화벽이나 침입탐지시스템과 달리 침입 유도 시스템이 지닌 지능적인 기능과 적극적으로 자동 대처하는 능동적인 기능이 합쳐진 개념의 보안솔루션으로 침입방지시스템은 차세대 보안솔루션으로 발전하고 있습니다.

개발사	제품명	주요기능	솔루션 특징
CISCO	NGIPS	▪ 패턴 기반 알려진 유해트래픽 탐지 ▪ Hash 값 인텔리전스 조회로 알려진 악성파일 탐지 ▪ 로컬 샌드박스 연동을 통한 알려지지 않은 악성파일 탐지 ▪ 인텔리전스 기반 공격서버와의 통신 여부 탐지 ▪ 트래픽 기반 자동 자산식별	▪ 차세대 방화벽과 차세대 IPS 기능을 결합, 네트워크와 보안 위협 변화에 대응 ▪ NSS Labs 인증
TrendMicro	TippingPoint	▪ DVLabs 및 Zero Day Initiative를 통하여 최신 보안취약점(Zero-day Vulnerability) 으로부터 네트워크 및 중요자산 보호 ▪ 멀웨어, 랜섬웨어 및 C&C 통신에 대한 방어 ▪ Score 기반으로 악성 IP DNS에 대한 통신 제어 ▪ 인텔리전스 방어 기법인 위치 정보, User ID 기반의 접근제어	▪ NSS Labs 인증 ▪ NIPS, HIPS 제품 지원 ▪ Gartner, NSS, IDC등 글로벌 리서치 조사 클라우드,네트워크,엔드포인트 보안 입증
안랩	TrusGuard IPX	▪ 시그니처 기반 공격 탐지 ▪ 행위(Behavior) 기반 공격 탐지 ▪ 일일(daily) 정기 업데이트 ▪ 6,000여 개의 시그니처 기본 제공 ▪ 악성코드 공격 방어 ▪ 각종 취약점 공격 방어 ▪ 제로데이 공격 방어 ▪ Application Control	▪ CC인증 ▪ 자체 C&C 서버 블랙리스트 DB를 탑재
시큐아이	SECUI MFI	▪ 64비트 SecuiOSTM과 고성능 멀티코어 플랫폼에 최적화된 아키텍처로 Wired-Speed 제공 ▪ Full Stack Inspection으로 Exploit 공격, 웹 취약점 공격뿐만 아니라 애플리케이션까지 제어 ▪ 검증된 Anti-DDoS 전용 장비 엔진 탑재 ▪ 취약점 진단 툴 및 시큐아이 보안포털서비스 제공 ▪ C&C 서버와 내부망 좀비PC까지 탐지 차단	▪ CC인증 ▪ 고객과 벤더간의 연계를 통해 개방적인 문제 해결 접근을 추구 ▪ 사용자 인증 방화벽 SECUI MF2 시리즈와 연계
FortiNet	FortiGate IPS	▪ 네트워크에서 지능형 위협, 봇넷, 제로데이를 심층 검사 ▪ 독립적 타사 검증을 통해 우수한 탐지 및 최고의 가격 성능 입증 ▪ 샌드박스와 어플라이언스 또는 클라우드 서비스를 매끄럽게 통합해 지능형 위협으로부터 보호 ▪ 보안 패브릭 통합 ▪ 고성능 네트워크 처리량 및 심층적 보안 검사를 위한 혁신적 보안 프로세서(SPU) 기술	▪ 자사 하드웨어 칩 spu 제공 ▪ NGIPS 기능을 제공하는 것뿐만 아니라 보안 패브릭의 중심으로 동작 ▪ NSS Labs 인증

[표 Ⅲ-25. IPS 솔루션별 특징]

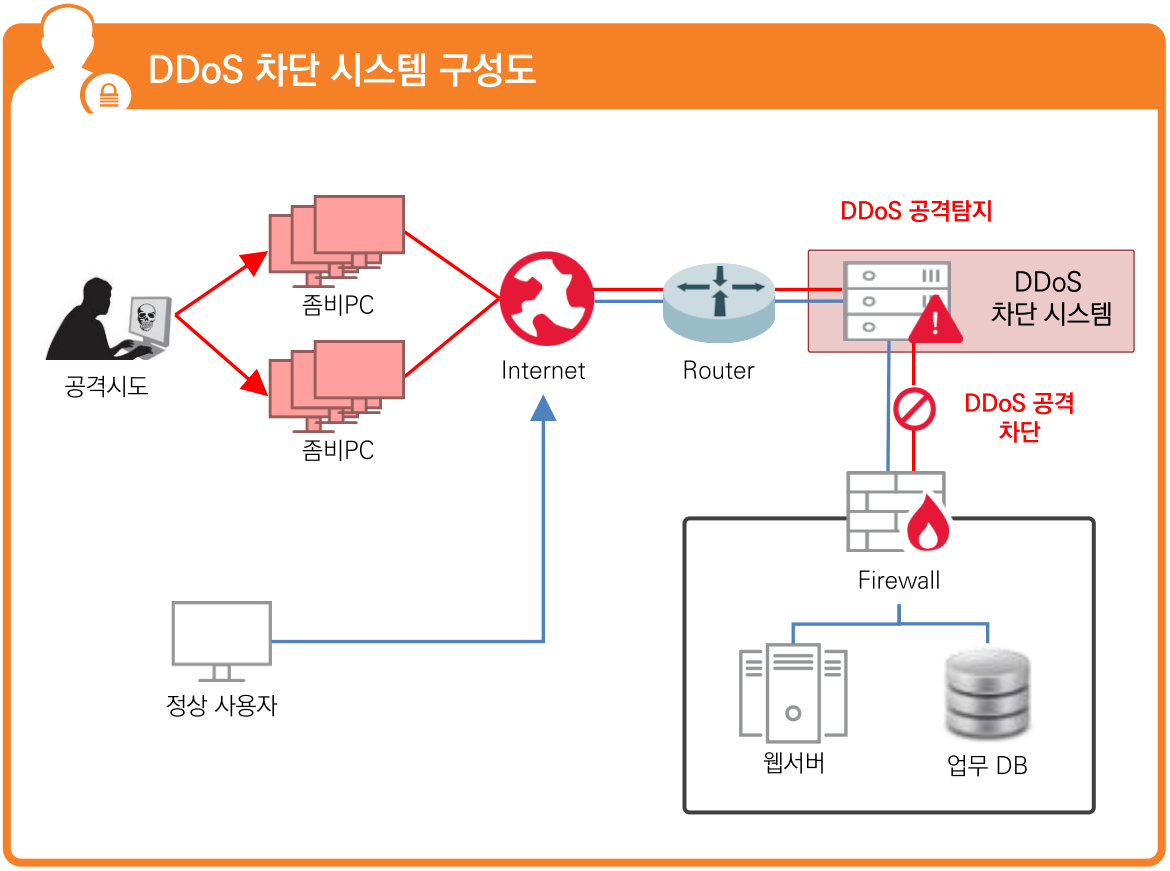
바. DDoS

A. 솔루션 개념

DDoS (Distributed Denial of Service, 분산서비스거부) 차단 시스템은 외부의 공격자가 규모의 공격 단말을 이용하여 공격대상에 과도한 트래픽을 발생시켜 정상서비스 제공에 장애를 발생하게 하는 악성코드나 트래픽을 차단하는 시스템을 말합니다. 특정 인터넷 사이트가 소화할 수 없는 규모의 접속 통신량(트래픽)을 한꺼번에 발생시켜 서비스 체계를 마비 시킵니다. 불특정 다수의 컴퓨터에 악성 컴퓨팅 코드인 '좀비(Zombie)'를 퍼뜨린 뒤 DDoS 공격에 이용하는게 특징입니다. 좀비에 감염된 수많은 컴퓨터가 일시에 특정 사이트를 공격(접속)하는 트래픽에 동원되는 구조입니다. 공격 대상 컴퓨터 안에 담긴 자료를 몰래 빼내거나 삭제하지는 않습니다.

DDoS의 대비책으로 보안관리자는 DDoS 차단 장비를 기업 내부 네트워크 구성에 In-Line 또는 Out-of-Path 구성 방식 등으로 기업의 환경에 적합한 DDoS 방어 체계를 구축 할 수 있습니다.

최근에는 DDoS공격에 사용되는 단말이 일반 Zombie PC뿐만 아니라 IoT 단말을 사용하여 기존 공격규모에서 더 큰 규모의 트래픽을 발생 시키는 DDoS 공격 사례도 늘어나고 있습니다. 보안관리자는 DDoS 공격에 대한 방어 시스템을 구축하여 공격 트래픽에 대한 즉각적인 차단 및 상위기관 보고 등 DDoS 공격에 대한 대응 방안을 마련하여야 합니다.



[그림 Ⅲ-24. DDoS 차단 시스템 구성도]

B. 주요기능

DDoS 공격 기반은 네트워크 기반과 어플리케이션 기반 두 가지로 나누어 볼 수 있습니다. 네트워크 기반은 UDP, ICMP, TCP, IP Flooding과 같은 공격, 애플리케이션 기반은 HTTP, SIP, VoIP Flooding 공격 등이 있습니다. DDoS 차단 솔루션은 이러한 다양한 공격 패턴을 탐지 및 차단을 수행하며 DDoS 공격 패턴과 동일한 요청의 정상/비정상을 지능적으로 판단 하는 기술이 보완되고 있습니다. 네트워크 환경변화와 기존의 보안 시스템을 우회하는 최신 DDoS공격에 대해서 능동적인 방어가 필요합니다.

DDoS 차단 솔루션의 주요 기능은 DDoS보안 정책 수립, 탐지/공격 차단, 실시간 모니터링으로 정의할 수 있습니다.

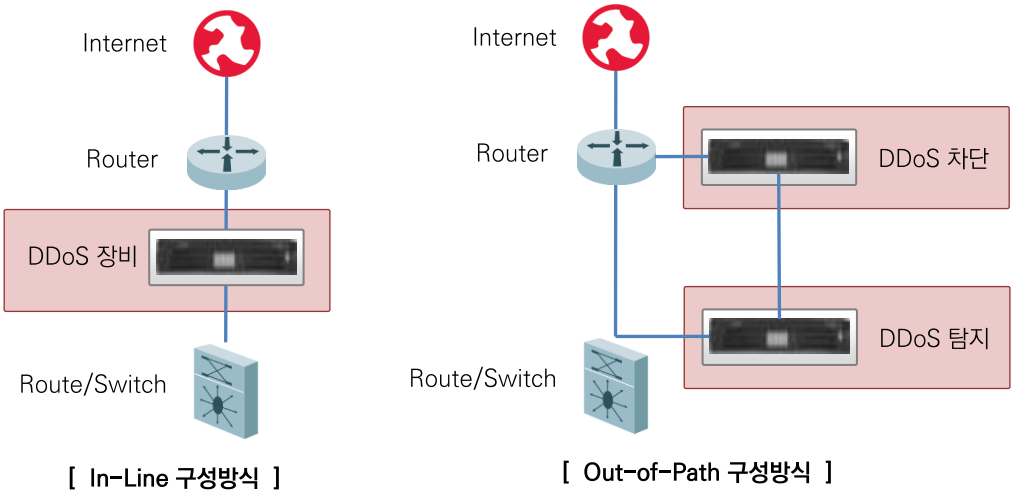
기능영역	주요 기능 내용
정책 수립	**탐지 및 차단 정책** 1 국가,IP,URL별 차단 정책 수립 2 자동패턴 추출 및 IP Pool 객체 정책 3 관제 체계와 연동 및 위협 알림 정책 설정
공격 차단	**다양한 DDoS 공격 차단** 1 TCP 기반 공격 방어 (SYN, ACK, RST 등) 2 UDP, ICMP 기반 공격 방어 (Flooding 공격, UDP Land Attack, ICMP Echo Flooding, 등) 3 HTTP 및 SIP 어플리케이션 기반 공격 방어 (Flooding, HTTP post Attack, Request Flooding 등) 4 기타 공격 유형 및 비정상 패킷 탐지 및 방어
모니터링	**탐지 및 모니터링** 1 탐지/차단 정보 및 임계치 정보 2 분석 통계 및 수집 데이터 시각화 UI 제공 3 감사로그 및 보고서 기능 제공

C. DDoS 솔루션 네트워크 구성방식

DDoS장비의 구성방식은 네트워크 라인에 설치 구성하는 In-Line 방식과, 네트워크 Line에서 별도로 외부에 위치하게 하는 Out-of-Path방식 있습니다. 네트워크 트래픽 대상으로는 유입되는 In-Bound와 유출되는 Out-Bound가 있으며, 양방향관리와 단방향 관리로 구분할 수 있습니다.

DDoS 구성상에서 중요하게 고민해야 할 사항은 기존 시스템 네트워크 트래픽 환경과 특성에 따라 DDoS 공격을 어떻게 방어 할 수 있는지, 공격방어 기능에 대해서 설계해야 합니다.

DDoS 네트워크 구성방식



[그림 Ⅲ-25. DDoS 네트워크 구성방식]

구분	In-Line 방식	Out-of-Path 방식
방식 설명	▪ 방화벽이나 IPS와 같은 보안장비와 같이 트래픽 구간에 설치되는 방식	▪ 트래픽 소통 구간에서 외부로 별도 설치되는 방식
구성 위치	▪ 네트워크 Line 구간 내 위치	▪ 네트워크 메인 Line 과 별도 Line으로 외부에 위치
네트워크 트래픽 대상	▪ 양방향 트래픽 기준 (In-Bound, Out-Bound 트래픽 대상)	▪ 단방향 트래픽 기준 (In-Bound 트래픽 대상) (일부 양방향 트래픽 대상 있음)
방식의 장점	▪ 신속한 위협 대응	▪ 기존 네트워크 안정성 확보 (영향도 없음) ▪ 대용량 트래픽에 적합
방식의 단점	▪ 기존 네트워크 트래픽에 영향이 있음	▪ In-Line에 비해 대응이 느림 ▪ 구축 시 설치적용이 복잡함

[표 Ⅲ-26. DDoS 네트워크 구성방식 비교]

D. 솔루션별 특징

DDoS 차단 솔루션은 TCP/IP계층 부터 어플리케이션 계층까지 다양하게 진화하고 있는 DDoS 공격으로 부터 안전한 보안을 사수하기 위해 기능 보완이 지속적으로 이루어지고 있습니다. 또한 솔루션 자체에서 다양한 공격 패턴을 탐지 및 자동 학습하여 공격에 대한 차단을 수행함으로 보안 관리자의 개입을 최소화 업무 효율 및 생산성 증대 효과를 지원하도록 보완되고 있습니다.

개발사	제품명	솔루션 기능		
		공격 방어	부가 기능	특징
윈스	Sniper ONE-d	▪ 통계기반 Legacy DDoS 기능 ▪ HTTP/WEB 공격 차단 ▪ 국가별, IP-Pool, 그룹별 정책 관리 ▪ DNS, VoIP 기반 flooding 차단 ▪ 시그니쳐 기반 다양한 패킷 차단 ▪ 평판 분석으로 자동화 공격 차단 ▪ DNS 전용정책으로 공격 차단	▪ Smart QoS 기능 제공 ▪ 세션 인증관리로 업무 연속성 보장 ▪ 자산정보 연계를 통한 봇넷 사전 대응 ▪ IN-Line, Out-of-Path 구성 지원 ▪ 자동 학습을 통한 정상 사용자 인지와 내부 자산 시스템과의 연동 ▪ 모니터링 및 리포팅 기능	▪ CC인증 ▪ DNS 전용 정책 적용으로 유해 DNS 요청 트래픽에 대한 탐지/방어/QoS 기능 제공
안랩	TrusGuard DPX	▪ 대용량 Flooding 공격 방어 ▪ TCP 상태 고갈 공격 방어 ▪ 애플리케이션 레이어 공격 방어 ▪ Fragmentation 공격 방어 ▪ Scanning 공격 방어 ▪ 비정상 패킷 차단 ▪ 시그니처 기반 차단	▪ IN-Line, Out-of-Path 구성 지원 ▪ 자동학습기반의 트래픽 유형별 상세 정책 설정 ▪ DDoS 관련 관제 및 프로세스 컨설팅 서비스 ▪ 통합 모니터링 및 관제 연동 및 지원 ▪ 리포팅 기능 지원 ▪ 자동 학습 시스템	▪ CC인증 ▪ 클러스터 구성을 통한 대규모 DDoS Traffic 처리 가능
시큐아이	SECUI MFD	▪ 비정상 프로토콜 방어 ▪ Multi-Stage, Multi-Layer DDoS Protection ▪ 응용 계층 방어 ▪ 지역 기반 방어 ▪ 시그니처 기반 방어 ▪ 프로토콜 취약점 방어 ▪ Flooding 및 다양한 공격 방어	▪ 자동 학습 방어 ▪ Anti-Botnet 솔루션 연동 ▪ IN-Line, Out-of-Path 구성 지원 ▪ 통합 모니터링 및 실시간 대시보드 ▪ 리포트 기능 지원	▪ CC인증 ▪ Virtual Domain 기능으로 유연한 DDoS 방어 체계 구현 ▪ 위협관리시스템 및 정보보안센터와 연계 효과적인 방어체계 구축 ▪ Snort, PCRE 지원 ▪ 트래픽 분산 처리 및 멀티코어 최적화 기술 (SC FDE)

[표 Ⅲ-27. DDoS 차단 시스템 솔루션별 특징]

사. 망분리

A. 망분리 개념

망분리란 내부 업무망과 외부 인터넷망의 네트워크를 분리하여, 서로간 격리된 환경에서 업무를 진행하도록 구성된 네트워크 체계를 말합니다. 망분리 체계는 악성코드 또는 외부에서의 해킹 공격을 막기 위한 것과, 중요한 내부자료 및 인프라를 보호하기 위한 근본적인 대책으로 정부 정책으로 시작되어 공공기관과, 금융기관은 망분리 체계를 의무적으로 구축한 상태입니다.

현재, 다양한 법령 및 가이드라인 등을 통해 공공기관은 물론 금융, 제조, 일반기업에 이르기까지 망분리를 권고 또는 의무화 하고 있으며 특히 금융회사의 경우 2016년 말까지 모든 망분리를 추진하도록 가이드라인을 배포한 바 있습니다.

망분리는 크게 물리적 망분리와 논리적 망분리로 나뉩니다. 물리적 망분리는 개인 당 두 개의 PC를 사용하거나 전환 스위치로 망을 분리하는 방식과 네트워크 카드를 두개 탑재한 PC를 사용하는 방식 등이 있습니다. 초기에는 대부분의 공공기관들은 보안 등의 이유로 두 개의 PC를 사용하는 물리적 망분리를 실시해 왔습니다. 완벽한 망분리가 보장되어 내부망의 안전성이 높다고 평가되기 때문입니다. 논리적 망분리는 일종의 가상화 영역의 망분리로, 개인 당 한 개의 PC에서 내부망과 외부망을 분리하는 방식입니다. 때문에 기반환경 구축에 대한 관리 및 운영비용이 물리적 망분리보다 저렴합니다. 하지만 웜이나 바이러스 유입이 가능하고 내부망에서 인터넷망으로 바로 연결될 수 있다는 보안 취약점이 있습니다.

논리적 망분리는 다시 가상화 기술을 이용한 VDI[1] 방식과 PC 운영체제를 분리하는 OS 커널 분리 방식으로 나뉩니다. VDI는 데스크톱을 가상화시켜 서버에서 전산자원을 끌어다 사용하는 방식으로 업무용 VDI 전환을 통한 망분리와 개인용 VDI 전환을 통한 망분리로 분류됩니다.

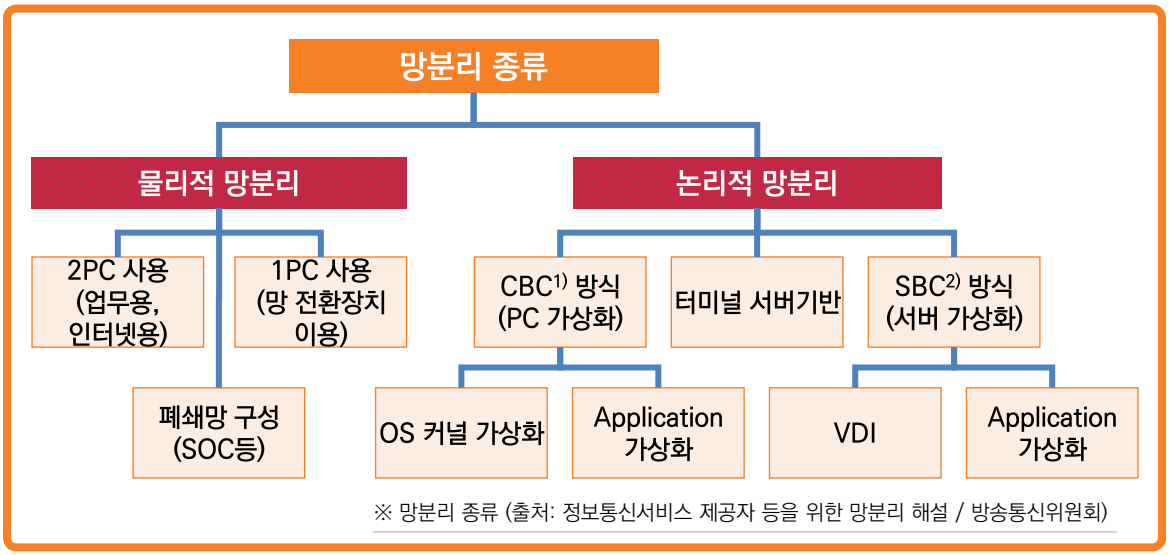
업무용 VDI 구축의 경우 업무 전체의 전산 자원을 서버에서 가져오는 방식으로 정보자원의 중앙통제를 통한 보안 유지와 언제 어디서나 개인 단말기로 업무를 볼 수 있는 스마트워크, 효율적인 PC관리가 강점입니다. 다만 업무용 VDI 전환을 통한 망분리는 전체 업무에 대한 가상화로 비용이 높다는 단점이 있습니다.

이로 인해 나온 개념이 개인용 VDI 전환을 통한 망분리 입니다. 개인용으로 활용하는 부분만을 가상화하는 것이라 상대적으로 비용이 저렴합니다. 이 같은 VDI 컨셉트는 우리나라에만 존재하는 것으로 VDI 구축 벤더들이 만들어 낸 정책입니다.

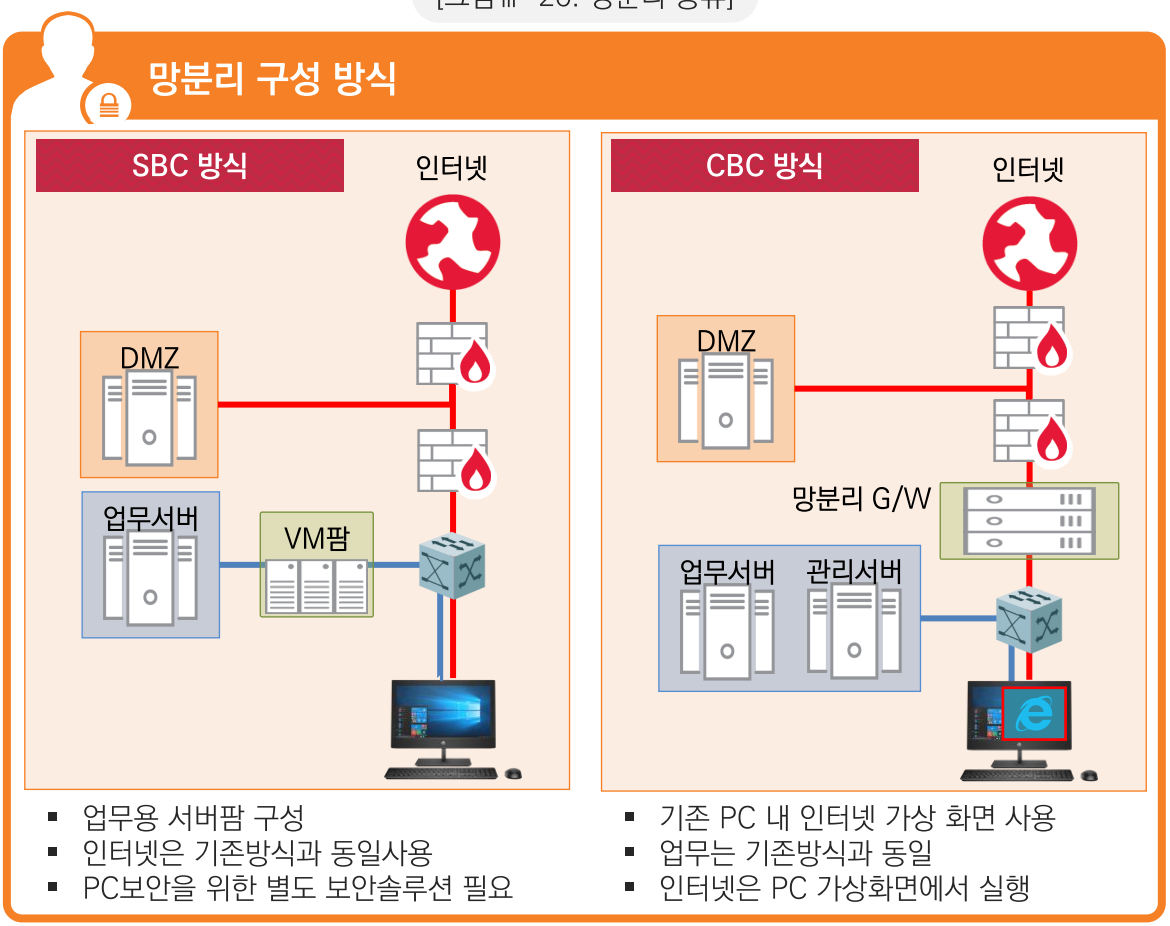
이렇듯 망분리는 각각 장단점을 가지고 있습니다. 어떤 방식을 택하느냐에 따라 사이버 테러에 대한 위험도가 달라질 수 있기 때문에 신중한 결정이 필요합니다.

1) VDI (Virtual Desktop Infrastructure) : 데스크톱 가상화란 물리적으로 존재하지 않지만, 컴퓨터(PC, Mobile, Tablet 등) 안에서 또 하나의 가상 컴퓨터를 만드는 기술. 가상 데스크톱을 로컬 시스템이 아닌 중앙 서버에서 작동하는 가상머신 계층, 가상머신 데이터를 저장하는 스토리지 계층, 각 가상머신을 클라이언트에게 연결하는 세션 관리 계층, 서비스를 받는 클라이언트 계층으로 이루어짐. 즉, VDI 기술은 다수 가상 데스크톱을 자신의 로컬 시스템에서 운영하고 있는 것처럼 보여주는 기술을 의미

B. 망분리 구성 종류



[그림 Ⅲ-26. 망분리 종류]



[그림 Ⅲ-27. 망분리 구성 방식]

1) CBC (Client based Computing) : PC가상화 기반의 망분리 방식으로 개인 PC에 업무용 로컬망과 인터넷을 이용하는 방식
2) SBC (Server based Computing) : 서버 기반의 가상화 방식으로 서버에 사용자별 가상공간을 할당하여 이용하는 방식

C. 망분리 구성 비교

구분		물리적 망분리	논리적 망분리	
			서버기반 가상화	PC기반 가상화
구성방법		▪ 2대의 PC를 이용해 업무용과 인터넷용으로 PC와 네트워크를 물리적으로 분리	▪ 업무용 PC를 서버의 가상화 PC로 중앙 집중화 ▪ 사용자는 가상PC에 접속하여 업무를 실행	▪ PC에 가상화 S/W를 설치하여 외부와 격리된 가상공간을 구축하여 인터넷 영역으로 사용
추가 장비		▪ 추가 PC 네트워크 망 구축	▪ 서버 가상화 S/W ▪ 전용서버 ▪ 외장 스토리지	▪ PC가상화 S/W ▪ 네트워크 분리장비(VPN)
장점		▪ 구축 위험도 낮고 용이함 ▪ 타 방식에 비해 비교적 높은 보안 수준 ▪ 외부 위협정보의 원천적인 차단 ▪ 해커의 직접적인 접근 차단	▪ 자료의 중앙 집중관리로 관리의 효율성 및 보안성 제고 ▪ 스마트 오피스 최적화	▪ 기존 장비 재활용으로 도입비용 효율적 ▪ 구축 용이로 현재 업무환경 변화 낮음
단점		▪ PC,네트워크 이중화로 고비용 (관리부담) ▪ 전력, 발열, 공간 비효율적 ▪ 스마트 오피스 불가	▪ 최초 도입 서버 팜 구성으로 고비용 ▪ WAN 구간 작업이나 다수접속 시 성능 저하 ▪ 시스템 오류 발생 시 복구 복잡	▪ 다양한 PC환경의 호환성 어려움 ▪ 안정성 관리 효율성 낮음
사용자 환경	PC장애 시 (데이터)	▪ 복구 어려움 (PC저장)	▪ 문제 없음 (서버에서 관리)	▪ 복구 어려움 (PC저장)
	N/W장애 시	▪ 모든 작업 중지	▪ 모든 작업 중지 (세션은 유지)	▪ 모든 작업 중지 (세션은 유지)
	N/W 부하	▪ 높음	▪ 낮음	▪ 높음
관리자 환경	사용자 관리	▪ 없음	▪ 중앙집중식	▪ 없음
	계정인증 관리	▪ 없음	▪ 조직도, 그룹, 계정통합관리	▪ 기본 계정관리
	데이터 관리	▪ 별도 물리적 추출 승인이 필요	▪ 사용자PC와 서버간 이동/복사 제어	▪ 제어 어려움
	정책 관리	▪ 없음	▪ 보안레벨, 사이트 차단제어	▪ 없음
	로그인, 사용시간 제한	▪ 없음	▪ 있음	▪ 없음
보안성	장치를 통한 유출	▪ 없음	▪ 있음 (IP, MAC, ID)	▪ 없음
	데이터 유출	▪ 없음 (별도 솔루션 필요)	▪ 있음	▪ 없음 (별도 솔루션 필요)
	보안 및 대응책	▪ 기 사용정책에 따름	▪ 인증, 환경, 네트워크, 사용성, 관리운영성, 유지보수, 대응처리, 로그/추적 프로세스	▪ 없음 (향후 초기검토 및 검증단계 필요)
활용도		▪ 개인정보 관리, 개발	▪ 주요자산관리, 문서 중앙화, BYOD	▪ 일반 OA사용자

[표 Ⅲ-28. 망분리 구성 비교]

D. 주요기능

앞서 소개한 바와 같이 망분리의 주요 기능은 외부의 공격 및 악성코드 등으로 인한 피해를 원천적으로 차단하기 위해 인터넷망과 업무망을 분리하는 것이며 솔루션별로 추가적인 제어기능을 제공합니다. 최근에는 물리적인 망분리 외에 업무 효율성과 편의성을 위해 VDI 형식의 망분리 구축이 활성화 되고 있습니다. 해당 기업의 업무환경과 성격에 적합하도록 망분리 방식을 선택하고 솔루션을 선택해야 합니다.

망분리 방식 중 가상화 기준(SBC, CBC)으로 주요기능을 설명 드리겠습니다.

기능영역	주요 기능 내용
망분리	**인터넷망 및 업무망 분리** 1 인터넷망 <-> 업무망 접근 차단 2 해킹 및 악성코드로 인한 피해를 전파되지 않도록 방지 3 내부자료 유출 방지(매체 권한관리)
가상화	**서버가상화 주요기능** 1 사전 구축된 VDI로 접근할 수 있도록 제공 2 패치 및 솔루션 설치 등 일괄적으로 배포 가능 **데스크탑 가상화 주요기능** 1 G/W 서버를 이용해 논리적 망분리 진행 2 기존 PC 내 VDI 생성
기타기능	**기타** 1 브라우저 정책, VDI 별 제공용량 등 선별 2 VDI 백업 및 복구 기능

E. 솔루션별 특징

망분리 솔루션을 선택하기 이전에 기업 내 사용자수와 비용 등을 고려하여 상황에 맞게 적용 방안을 계획해야 합니다. 논리적 망분리는 각각의 제조사에서 가상화 솔루션을 개발 및 판매를 하고 있습니다. 시장에는 다수의 제품이 출시되어 현재 영업도 활성화 되고 각각 제품의 장단점이 어필이 되고 있습니다.

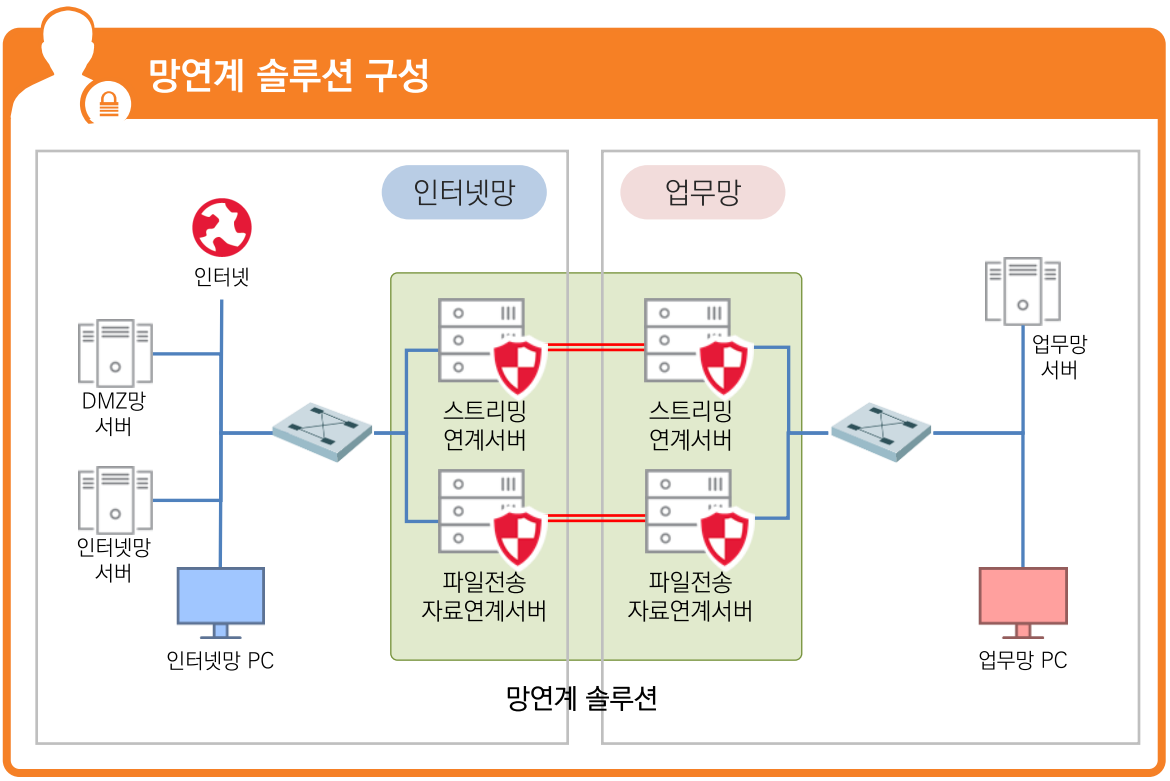
개발사	제품명	주요기능	솔루션 특징
VMware	Vmware horizon (View)	▪ Windows, Linux 등 다양한 OS 가상 desktop 환경 제공 ▪ 물리 데스크톱 이미지 관리 ▪ 실시간 어플리케이션 배포 ▪ 인스턴스 클론 ▪ VDI 인프라 모니터링 및 성능분석, 최정화 ▪ 스토리지 가상화	▪ 자동화를 위한 REST API제공
Citrix	XenDesktop	▪ Windows, Linux 등 다양한 OS 가상 desktop 환경 제공 ▪ 기기, 시간, 장소에 관계없이 PC, MAC, 태블릿 또는 스마트폰에서 사용 가능 ▪ Flash 멀티미디어, USB 주변 장치 및 3D 그래픽 지원 ▪ Windows, Web, SaaS 지원	
Microsoft	Hyper-V	▪ Windows 전문 가상OS 환경 제공 (타OS 제공) ▪ 하드웨어 가상화 제공 ▪ 가상화 별 완전 별개의 OS 사용 ▪ VM 운영체제 별 유효한 라이선스 필요	
SK Broadband	CLOUD PC	▪ 클라우드 서버에서 가상화 VDI 제공 ▪ Windows, Linux 등 다양한 OS 가상 desktop 환경 제공 (TmaxOS 등) ▪ 기기, 시간, 장소에 관계없이 PC, MAC, 태블릿 또는 스마트폰에서 사용 가능 ▪ 모든 PC 자원 가상화 지원 ▪ 구축 시 필요한 보안솔루션 추가 구축 제공	▪ 클라우드 기반 VDI ▪ 구축형 외 서비스형 제공
Tilon	Dstation	▪ 개인 데스크톱 OS, 가상디스크, S/W 등을 제공 ▪ VM Provisioning 자동화 ▪ 모바일 단말 지원에 따른 확장성 보유 ▪ 스마트 세션 관리 및 장애 대응 ▪ 공인인증서 가상화 기능 제공 ▪ 온라인 디스크 기능 제공	▪ 리눅스 환경의 가상 데스크톱 Lstation 가상 어플리케이션 Astation 등 제공

[표 Ⅲ-29. 망분리 솔루션별 특징]

아. 망연계

A. 망연계 개념

망분리로 인하여 외부 인터넷망과 내부 업무망 사이가 모두 차단되어 많은 업무적 문제점이 발생하게 되었고, 이에 따라 망연계의 NEES가 발생하게 되었습니다. 망연계 솔루션은 서로 다른 망 사이를 파일전송 방식과 스트리밍 방식을 통해 연계하여 꼭 필요한 경우에 한하여 연결할 수 있는 솔루션입니다.



[그림 Ⅲ-28. 망연계 솔루션 구성]

스트리밍(Streaming) 서버는 망간에 꼭 필요한 연결이 있을 경우 실시간으로 암호화 통신하여 서로 다른 망에 있는 서버 → 서버, 또는 사용자 → 서버가 연결될 수 있도록 합니다. 메일서버 간 연동, 또는 WEB서버와 DB서버의 통신 등에 사용되는 것이 일반적입니다. 또한 업무망PC에서 특수목적을 가진 사용자(금융, 재무, 증권 등)가 인터넷을 이용해 필요한 사이트에 접근할 수 있도록 지원 합니다.

파일전송(File Transfer) 서버는 인증된 사용자가 업무망 → 인터넷망, 또는 인터넷망 → 업무망으로 필요에 따라 파일 반입 및 반출이 가능하도록 지원합니다. 반출/반입되는 파일은 보안을 위해 사전 정책화(파일크기, 확장자)된 파일만 전달이 가능하며 필요에 따라 결재절차가 함께 진행됩니다. 또한 백신 또는 APT모듈과 연계하여 망간 이동 시 위협요소를 사전 검증할 수 있도록 합니다.

B. 주요기능

망연계 솔루션은 파일전송(File Transfer)과 스트리밍[1](Streaming)을 통해 분리된 망을 연결하여, 필요한 파일 및 데이터 통신을 송/수신할 수 있도록 지원하는 것이 주요기능입니다.

파일전송은 분리된 망의 사용자 PC간 저장 자료(파일 등) 전송을 위해 사용됩니다. 파일전송의 주요기능은 내부망에서 외부망으로 전송시 외부 반출 자료에 대한 승인 절차와 추적관리가 있고, 외부망에서 내부망으로 전송시는 악성코드 검사와 유입자료 추적이 주요 기능입니다. 스트리밍 통신은 내부망에서 외부망으로는 내부망에서 발생하는 외부 서버로의 요청을 수집하여 외부 서버와의 실시간 통신 중계가 있고, 외부망에서 내부망으로는 외부망에서 발생하는 내부망 서버로의 요청을 수집하여 외부 서버와의 실시간 통신 중계가 주요 기능입니다.

기능영역	주요 기능 내용
파일전송	**망간 자료전송** 1 분리된 망 간 인증 후 파일전송 가능 2 인가된 파일정책에 따라서만 파일전송 가능 3 파일전송 승인/반려 및 이력관리
스트리밍	**서버 → 서버 간 스트리밍** 1 망 간 다른 서버 간 스트리밍 연계 2 서버 간 암호화 통신기능
	업무망 사용자 인터넷 접속 1 특수목적용으로 업무망PC에서 인터넷 접속 가능 (망분리 예외정책적 승인 필요)
모니터링/연동	**모니터링 및 연동** 1 파일전송 상세로그 확인 2 파일전송 및 실시간 스트리밍 관련 설정진행 3 파일전송을 검증하기 위한 백신, APT 모듈 등 연동

1) Streaming
- 서버 <-> 서버 실시간 서비스 연계 : 단방향 Outbound Session을 암호화 통신
- 서버 <-> PC 실시간 서비스 연계 : White List 기반으로 유효한 인터넷 사이트 연계

C. 시스템 연계 주요요건

망연계 솔루션은 국정원 보안 요구사항으로 중요자료, 소통·저장을 위한 암호 사용 시 검증된 암호 모듈의 탑재가 필요하다고 되어 있습니다. 네트워크 전체의 폐쇄성을 유지한 상태로 보안성을 준수하며 신속한 서비스 연계가 요구됩니다. 아래 표는 망연계 솔루션의 구축 연계 시 통신관련 필수적인 주요 포인트입니다.

연계 구분	내용
1. 단방향 통신	▪ 단방향 통신으로 외부 침해 또는 내부 유출에도 침입 및 유출방지
2. 전용 프로토콜 통신	▪ 알려지지 않은 전용 프로토콜 통신을 통해 네트워크 단절 효과
3. 검증된 암호화 모듈	▪ 국정원 검증필 암호화 모듈 탑재로 신뢰된 암호화 통신
4. 실시간 데이터 통신	▪ 대외 서비스를 위한 메모리를 통한 전송 방식으로 연계 데이터의 실시간성을 보장

[표 Ⅲ-30. 시스템 연계 주요요건]

D. 솔루션별 특징

개발사	제품명	주요기능	솔루션 특징
휴네시온	i-oneNet	▪ 파일전송/스트리밍을 이용한 망연계 ▪ TCP, UDP, http(s), MySQL, MS-SQL, Oracle, FTP, SSH 등 모든 응용프로토콜 연계 가능 ▪ WEB GUI 환경 파일 전송 ▪ 전용 프로토콜을 이용한 전송	▪ CC인증 ▪ 국정원 검증필 암호화 모듈을 이용한 채널암호화 ▪ 백신 엔진 기본 제공
한싹시스템	SecureGate	▪ 파일전송/스트리밍을 이용한 망연계 ▪ 인사정보, DRM, DLP, NAC, AD, LDAP, SSO, APT 등 연동 가능 ▪ 고속 데이터 처리 기술 탑재	▪ CC인증 ▪ 메일 송/수신 전용 방식 사용 ▪ 백신 엔진 기본 제공
에스큐브아이	Net-Protect	▪ 파일전송/스트리밍을 이용한 망연계 ▪ Web, Agent 방식 모두 지원 ▪ 다양한 OS 및 웹 브라우저 지원 ▪ Non-ActiveX 적용	▪ CC인증 ▪ 10G 급 망연계 제품
소프트위드솔루션	CrossNet	▪ 파일전송/스트리밍을 이용한 망연계 ▪ 메일보안필터 제공 ▪ AES-256 암호화 통신 ▪ SHA-512 해쉬함수를 이용한 무결성 검사	▪ CC인증 ▪ 국정원 검증필 암호화 모듈을 이용한 채널암호화
시큐에버	reverseWall-MDS	▪ 망간 데이터 스트리밍 연계 중심 ▪ 보안감사 기능 ▪ 사용자 데이터 보호 기능	▪ CC인증

[표 Ⅲ-31. 망연계 솔루션별 특징]

Ⅳ
기업유형별 보안

1. 제조 스마트 팩토리 보안

Ⅳ
기업유형별 보안

2. 의료정보 보안

Ⅳ
기업유형별 보안

3. 금융 핀테크 보안

Part 1

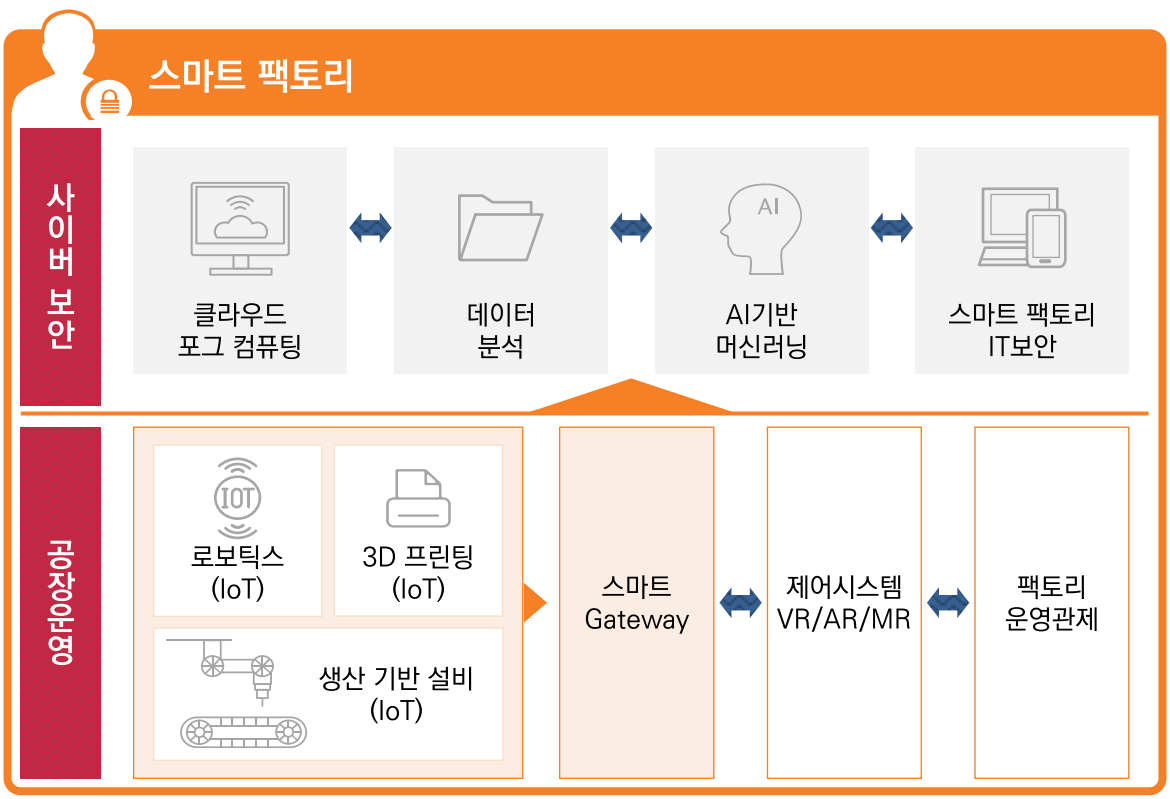
제조 스마트 팩토리 보안

1) 스마트 팩토리 정의

스마트 팩토리란 생산공장의 혁신적인 변화로 설계·개발, 제조 및 유통·물류 등 생산과정에 디지털 자동화 솔루션이 결합된 정보통신기술(ICT)을 적용하여 생산성, 품질, 고객만족도를 향상시키는 지능형 생산공장을 의미합니다. 또한, 공장 내 설비와 기계에 사물인터넷(IoT)를 설치하여 공정 데이터를 실시간으로 수집하고, 이를 분석해 목적된 바에 따라 스스로 제어할 수 있는 공장을 말합니다. 최근에는 가볍고 유연한 생산체계가 요구됨에 따라, 제조업 혁신 방안으로서 대두되고 있습니다.

스마트 팩토리의 전환은 제조업의 생산성과 효율성을 향상 시키고, 가상의 공간에서 제조현장을 모니터링 할 수 있을 뿐더러 제어까지 가능하여 공장 관리가 용이하며 품질 및 원가 경쟁력 강화로도 이어질 것으로 전망됩니다.

그에 따라 ICT와 데이터, 하드웨어가 결합되는 스마트 팩토리의 도입에 사이버 보안의 필요성이 강화되고 있습니다.



[그림Ⅳ-1. 스마트 팩토리 및 사이버 보안 영역]

2) 제조분야 사이버 보안

제조현장에서 급격히 늘어나는 연결기기와 사물인터넷을 통해서 설계단계부터 생산, 유통 및 서비스 과정에 이르기까지 각 프로세스의 정보가 가상공간에서 통합됨에 따라 정보 및 기술 유출의 위험성이 더욱 커지고 있습니다.

최근 공장에 생산설비, 무선센서, 휴대기기를 사물 인터넷으로 통신하고 있는데, 사물인터넷과 관련된 사이버 위협이 보안에 취약점으로 대두되고 있습니다.

모든 사물들이 연결된 스마트 팩토리는 상호 유기적으로 결합되어 플랫폼에서 연결된 속성으로 인해 플랫폼 위에 축적된 전반적인 연계정보까지 유출될 위험이 커집니다. 4차 산업혁명 시대에는 사물인터넷 및 플랫폼의 보안기술이 센서나 네트워크 기술만큼이나 강조되고 있으며, 기업들은 산업현장의 보안을 위협하는 요소들을 파악하여 체계적이고 효율적인 사이버 보안 전략수립이 중요 이슈가 되었습니다.

[그림Ⅳ-2. 제조분야의 사이버 보안]

1) 멀웨어 (Malware) : 컴퓨터 사용자 시스템에 침투하기 위해 설계되어진 소프트웨어를 뜻하며 컴퓨터바이러스, 웜바이러스, 트로이목마, 애드웨어 등이 포함된다

3) 산업용 IEC 보안모델

산업용 사이버 보안의 기준으로 IEC 62443[1]은 사람, 환경 및 운영기술 (OT)을 보호하려는 궁극적인 목표에 따라 사람, 프로세스 및 기술이 융합되는 통합적인 프레임워크입니다. 요구사항을 해결하고 각 이해관계자(제품, 시스템 공급자, 자산소유자)의 역할에 따라 서로 다른 이해관계자에 대한 요구사항을 정의합니다. IEC 62443은 전 세계적으로 채택되고 있으며 산업 부문에 걸쳐 폭넓게 수용되고 있습니다.

스마트 팩토리의 계층별 보안 요구 사항을 반영한 스마트 팩토리 보안 모델(안)은 IEC 62443 계층별로 네트워크 보안, 침입/악성코드 탐지, 중요정보 보호, 생산 설비 보안을 위해 요구되는 보안 기술을 제시합니다.

IEC 62443 계층			보안요구사항				
			네트워크 보안	침입/악성코드 탐지	중요정보보호	생산설비 보안	
IT 영역	Level 4 (Enterprise Biz System)	EPR, PLM, SCM	네트워크 분리/접근통제 DDoS방지 원격접근통제 무선보안	침입 차단/방지/탐지 Anti-Virus 패치관리	암호화/DB보안 인증 및 권한관리 문서보안/매체제어 이메일 보안	-	통합 보안 관제
OT 영역	Level 3 (Operation Management)	MES, WMS	PlantDMZ 구축 네트워크 분리/접근통제 원격접근통제 무선보안	침입 차단/방지/탐지 Anti-Virus 패치관리	암호화/DB보안 인증 및 권한관리 이메일 보안	-	
	Level 2 (Supervisory Control)	HMI, EWS, Historian					
	Level 1 (Basic Control)	DCS, SCADA, PLC, RTU	네트워크 분리/ 접근통제 원격접근통제 무선보안	침입 방지 Anti-Virus(Whitelist) 패치관리 제어장비 무결성 보증	인증 및 권한관리 매체제어	-	
	Level 0 (Field Device)	엑츄에이터, 센서, 로봇, 생산설비	네트워크 분리/접근통제 무선보안	침입 방지	통신 암호화 무결성 보장	기기/상호 인증 시큐어부트	

[그림Ⅳ-3. 스마트 팩토리 보안 모델(안)]

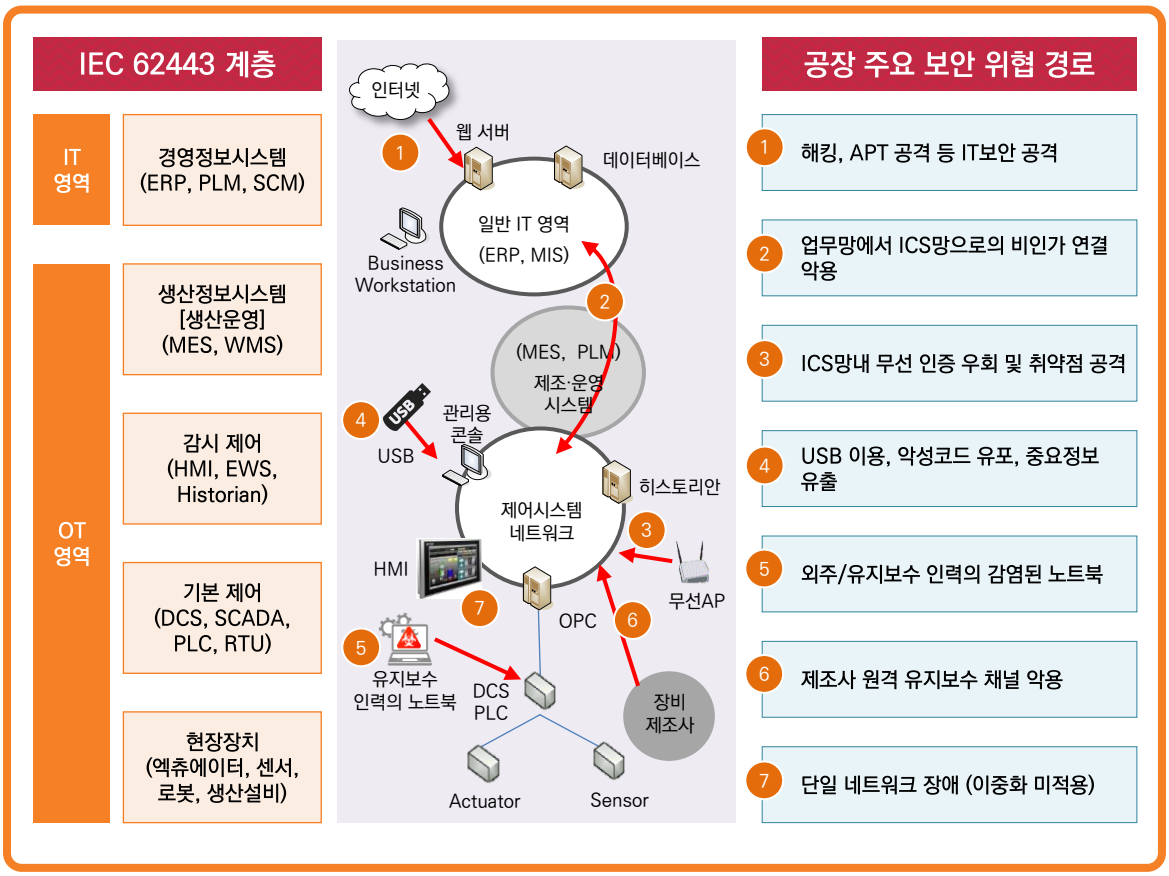
1) IEC 62443 (International Electrotechnical Commission) : 모든 전기, 전자 및 관련 기술에 대한 국제 표준을 준비하고 게시하는 국제 표준기구. IEC 표준은 발전, 송전 및 배전에서 가전 제품 및 사무 기기, 반도체, 광섬유, 배터리, 태양 에너지, 나노 기술 및 해양 에너지 및 기타 많은 기술에 이르기까지 광범위한 기술을 다룸. IEC는 또한 장비, 시스템 또는 구성 요소가 국제 표준을 준수하는지 여부를 인증하는 4 개의 글로벌 적합성 평가 시스템을 관리

4) 스마트 공장 주요 위협 경로

네트워크 망 구간 영역으로 구분하면, 스마트 팩토리는 임직원들이 업무를 수행하는 업무 영역(Level 4, Enterprise Biz System)과 제품 생산을 위한 제어시스템 운영 관리 영역(Level 3, Operations Management), 그리고 제조 공정을 제어하고 제품을 생산하는 ICS 영역(Level 0~2)으로 구성됩니다.

업무 영역에 대한 보안위협은 다양한 IT보안위협(해킹, 악성코드 감염, APT공격 등)이 있으며, 산업제어시스템에 대한 보안위협은 악의적 공격자가 업무 영역에 우선 침투하여 내부 정보를 수집한 후 ICS 영역을 공격하는 형태로 진행이 됩니다.

스마트 팩토리에 대한 보안위협은 매우 다양하게 존재하나 아래의 그림에서는 주요한 보안위협 사례를 예시로 설명합니다.



[그림Ⅳ-4. 스마트공장 주요 위협 경로]

5) 제조업 특성 및 보안이슈

최근 세계 유수의 생산시설을 대상으로 한 사이버공격이 연이어 발생하면서, 국내에서도 대기업을 중심으로 보안을 강화하려는 관심이 높아지고 있습니다. 하지만 현실적으로 생산시설 보안을 위한 전문가는 부족한 상태입니다. IT나 ICT에서 말하는 보안은 OT(Operation Technology, 제조 운영 기술)나 ICS(산업제어 시스템, Industrial Control System)에서의 보안과 의미가 다릅니다.

OT는 기본적으로 폐쇄망이며, PLC, RTU, HMI 등 공장에서 운용하는 생산망과 설비망, 공정망은 내부적으로만 통신하며 제품을 생산하기 때문에, 공장운영자는 외부 침해에 대한 사이버보안에 대해서는 취약한 편입니다. 이러한 측면에서 제조 공장에서의 보안 위협에 대한 근본적인 원인을 먼저 확인 해보겠습니다.

스마트공장 보안 위협에 대한 근본 원인

스마트공장 보안 조직 미흡

- ✓ 공장 보안 Ownership 부재 => 공장 보안 사각지대
  - 보안담당자의 생산설비 장비 및 네트워크 현황에 대한 이해 부족
  - 생산 담당자는 보안에 대한 이해 부족

스마트공장 보안 기준 부족

- ✓ 공장 보안 적용을 위한 보안가이드 부족
  - 공장 보안을 적용하기 위해 필요한 보안 기준 부족 (보안절차, 보안솔루션 등)
- ✓ 보안을 고려하지 않고 시스템을 도입하거나 네트워크 구축
  - 신규 공정/라인기획/설계 단계부터 보안을 적용하기 위한 기준 미흡

시스템 도입 후 보안 설정 변경 無

- ✓ 산업제어시스템 수명주기 15~20년 => 장비 초기 설정 이후 변경 無, 보안패치 미흡
- ✓ 네트워크 구축과 운영의 편의성을 위해 신규 장비 초기 설정 시 보안 해제

스마트공장 보안 인식 부족

- ✓ 공장은 폐쇄망으로 구성하여 안전하다는 인식, 유지보수업체에 대한 의존도 높음
- ✓ 공장 보안에 대한 법적 준거성 부재 => 공장 보안 필요성 자각 미흡, 보안투자 저조

제조업의 특성 및 이슈

- 가용성/안전성이 최우선
- 장비 도입 후 변경 없음
- 제조사, 유지보수업체 의존도 높음

[그림Ⅳ-5. 스마트공장 특성 및 이슈]

6) 제조 시스템 표준별 보안대책

산업제어시스템 보안 표준 NIST[1] 800-82에서는 업무망과 공장망 간 직접 접속을 통제하기 위해 Plant DMZ를 구성하고, 단방향 게이트웨이를 통해 중요 네트워크 영역에 대한 보안 접속을 통제하도록 권고하고 있으며, OT 영역에서 가장 중요한 요소인 가용성을 보장하기 위해서 장비 이중화에 대한 부분도 강조하고 있습니다.

다음은 산업제어시스템 보안 표준 및 보안가이드에서 제안하고 있는 스마트팩토리 보안 요구사항 입니다.

구분	보안 기능	산업제어시스템 보안 표준		정보보호 표준	스마트공장 보안가이드	
		NIST800-82	ISA/IEC 62443	NIST800-53	유출방지 가이드	최소보안 체크리스트
인증 및 권한 관리	인증 및 권한 관리	○	○	○	○	○
	기기인증	-	○	○	-	-
네트워크 보호/원격제어	네트워크 분리	○	○	○	○	-
	Plant DMZ 구성	○	○	-	○	-
	FA망/사무망간 프록시 서버	○	○	-	-	-
	단방향 게이트웨이	○	-	-	-	-
	침입 차단	○	○	○	-	○
	원격 제어	○	○	○	○	○
	무선 보안	○	○	○	-	○
	DDoS방지	-	-	○	-	-
모니터링, 감사, 탐지	보안 모니터링, 로그관리, 사고 탐지/대응/복구	○	○	○	○	○
침입/악성코드 탐지	침입탐지	○	○	○	-	-
	악성코드/바이러스 탐지	○	○	○	○	○
시스템/데이터/어플리케이션보안	화이트리스트 적용	○	-	-	-	-
	매체제어	○	○	○	○	-
	장비 이중화(Redundancy)	○	○	-	-	-
	패치 적용	○	○	○	○	-
	데이터 암호화	○	○	○	○	○
물리보안	물리적 접근통제	○	○	○	○	-
	영상정보기기 보안	-	-	-	-	○

[표Ⅳ-1. 보안표준 및 가이드]

1) NIST (National Institute of Standards and Technology) : 미 상무부(United States Department of Commerce) 기술관리국이 운영하는 국립 연구소
- 산업의 기술적 발전을 보조하고 상품 생산과정을 현대화하며 상품에 대한 신뢰성을 증대시키기 위한 목적으로 미국 의회에 의해 설립
- NIST는 과학기술 분야의 각종 표준과 관련된 기술연구를 담당
- 각종 측정기구 및 국가표준도량형을 마련해 산업현장에서 필요로 하는 각종 기술과 측정 기술에 대한 국가표준을 선정하고 개발 및 적용

7) ICS 보안 고려사항

제조공장의 보안위협 대응을 이행하기 이전에 고려해야 할 사항은 공장별로 자산파악과 분석을 통한 정책의 효율성 검토와 담당자의 보안사고에 대한 영역과 대응방안에 대한 숙지를 해야 합니다.

OT/ICS 보안을 위해 자산의 식별부터 정책까지 고민하다 보면, 다시 기본인 IT 보안 요구 사항의 검토가 필요하게 됩니다. 해당 사항에서 ICS 환경만의 차이점과 운영 사항의 이해는 필수입니다.

자산파악

- 각 공장별로 ICS 장비가 다르고, 네트워크 및 시스템 구성도를 이해하며, 공장의 공정과 해당 운영 장비 및 구성에 대한 분석을 통해 보호 대상 및 방안에 대한 고려가 필요
- ICS 자산장비가 노후화, 관습화 된 경우가 다수 있어서 분석의 어려움 발생함
- ICS의 전체적인 자산의 관리 명확화와 가시성을 확보를 목표로 함

자산분석

- 장비 별 설명서를 통해 해당 장비의 역할과 사고 발생 시 영향력(생산 및 인명사고 등)을 판단하여 보호단계 및 대응방안을 수립해야 함
- 해당 보안 및 복구 기능 등을 사전에 확인 후 대응 절차 수립
- 장애발생 대응 매뉴얼은 OT운영인력 주관으로 관리

보안 정책 효율성 검토

- ICS 표준 보안 정책이 실제 운영에 효율적인지 검토
- 사용자의 아이디/패스워드 이용 인증 방식이 ICS 시스템에 제공될 수 있는가를 검토
- PLC 장비군에 해당 항목 자체가 적용되기 어려운 점을 확인해야 함
- 자산파악과 분석을 통해 실제 보안정책이 장비 별 보안 특성을 포함하는지 검토하고, 수행 가능하며 효율성 있는 보안 점검계획을 수립
- IT보안의 경우 보안정책 준수를 강요할 수 있으나, 각 ICS 시스템의 유기적 관계를 고려한다면, 특정 장비 운영만을 위한 보안 정책을 강요한다고 모든 것이 해결될 수 없음

IT / ICS 통합 보안 사고 대응 관리

- ICS 보안에서 사고 발생시 해당 사고에 대한 대응 방안 및 사후 관리를 진행
- ICS 사고는 상위 IT 보안까지 연결되어 발생할 확률이 높음
- 사례를 검토해 보면 외부 저장 매체 반입, 유지 보수 디바이스의 악성코드 감염, 네트워크 취약점을 통한 HMI 서버 공격 등 IT 연결 요소가 원인으로 지목되고 있음
- ICS 보안 전문가는 IT보안에 대해서도 숙지가 필요

8) 보안강화 방안

가. OT/ICS 보안전략

OT/ICS의 심층적인 보안 전략을 수립하기 위해서는 다각적인 RISK도출 및 분석 컨설팅과 출입 및 전산기기 반·출입 관리를 위한 물리보안, 네트워크 및 보안정책, 침해사고를 기반으로 한 기술적 보안 영역을 분석하여 실질적인 다각도의 심층 보안전략을 수립하여야 합니다.

[그림Ⅳ-6. OT/ICS 심층 보안전략]

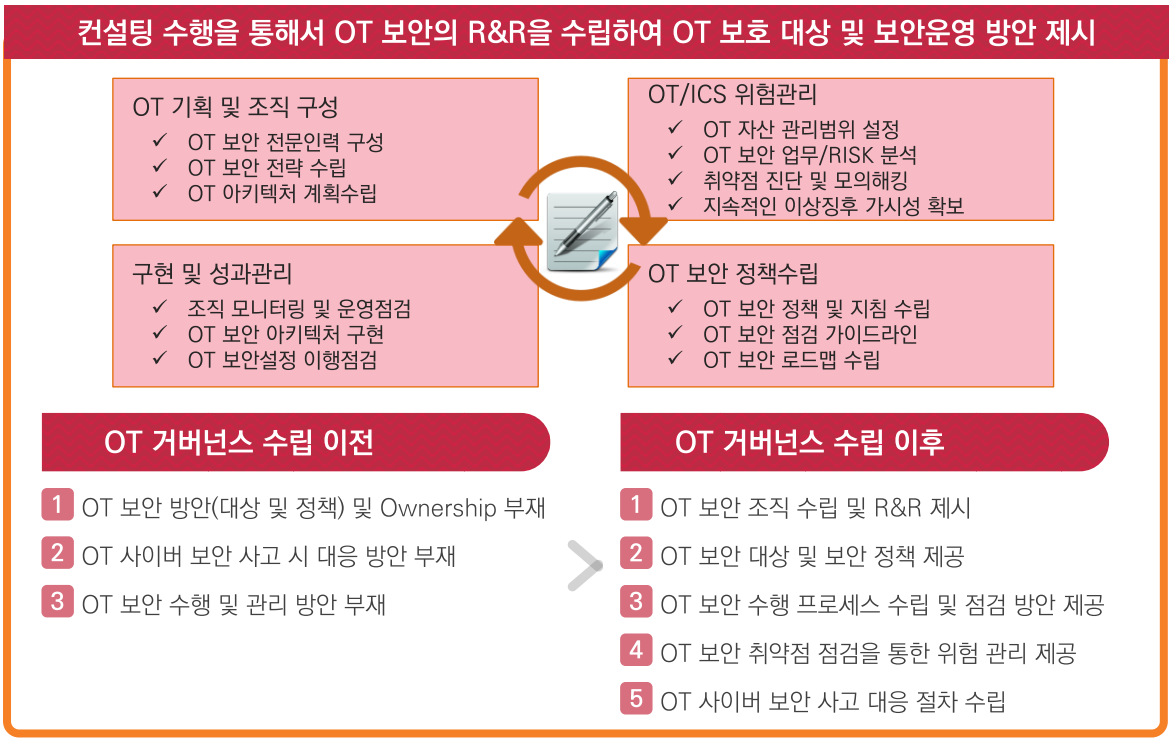
나. OT 보안 거버넌스 수립

OT 보안의 거버넌스 개선을 위해서는 인력에 대한 역할정의와, 조직과 업무 분석을 통한 정책과 지침이 정해지고, 보안전략에 대한 계획이 수립되어야 합니다. OT에 대한 네트워크와 아키텍처를 구축하고 거버넌스를 개선할 때에는 OT/ICS 관련 국제 표준 활용이 우선되어야 합니다. 국제 표준은 ISA/IEC 62443, NIST 800-82 등이 있으며, 해외에서는 정부 주도로 OT 보안 관련 표준을 제정해 OT보안 구현을 강제하거나 인증을 권고하고 있습니다.

OT/ICS 위험관리 분석을 위해서는, 보호해야 할 대상 자산을 선별해 RISK를 분석하고 그에 따른 보호 방안을 수립해야 합니다. 예를 들어, 공장제어·공정데이터 업무망, 제어공정시스템 관리망과 장비망, 장비별로 분류하고 보호기술 적용을 수행합니다. 이를 대상으로 지속적인 가시성을 확보해 비정상·이상징후를 탐지해야 합니다. 사고가 발생하더라도 원인 파악이 가능한 환경을 구축하고, 대응과 복구 방안도 수립해야 합니다. 결과적으로 식별-보호-탐지-대응-복구로 이어지는 보안 프레임워크를 구축하게 됩니다.

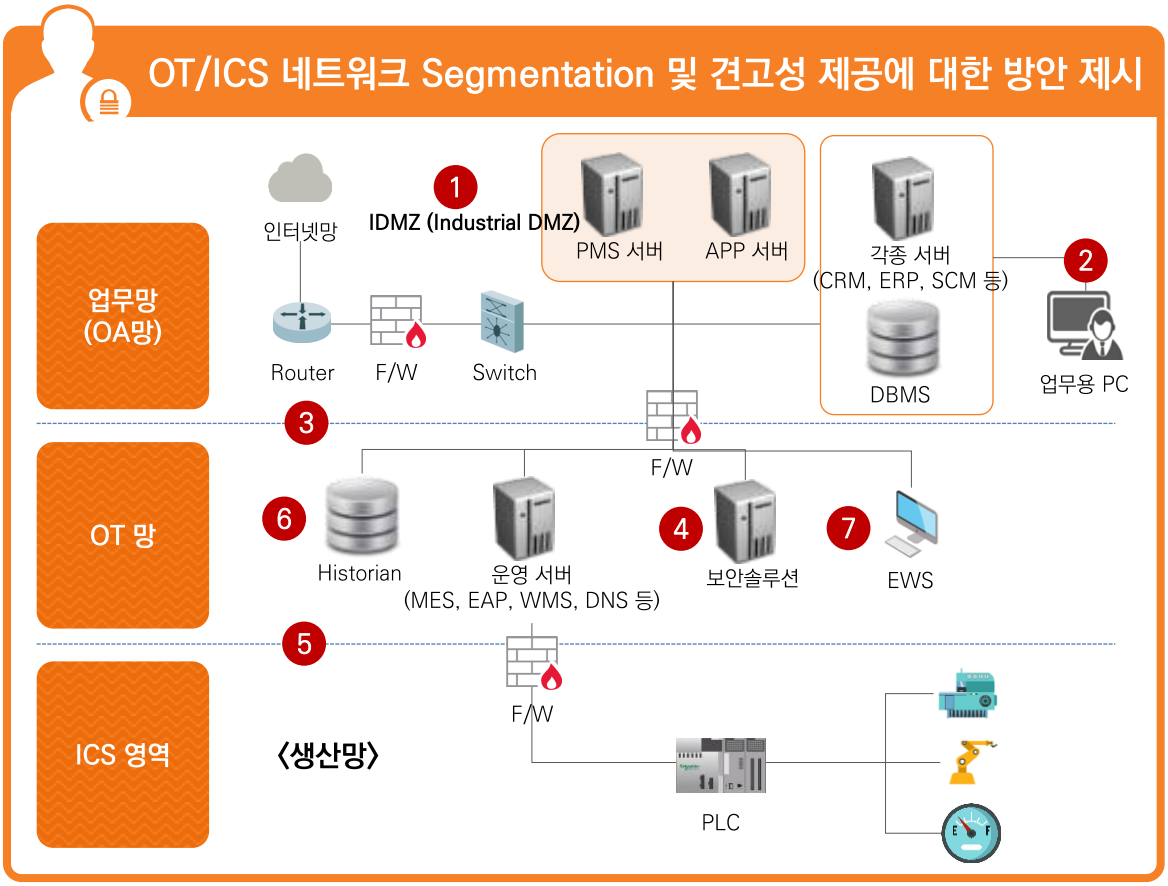
정책적으로는 OT 보안에 대해 정책, 지침, 가이드라인 등이 제시되어야 합니다. 업무망, 관리망, 장비망 별로 각각 특징적이고 제약적인 정책과 프로세스가 정의 되어야 하며, 내·외부 환경변화와 내부 시스템 구성 변화에 따라 정책 변경에 대한 대응방안을 마련해야 합니다.

To-Be 아키텍처 모델을 만들고 책임과 역할(R&R)에 대한 거버넌스를 정의한 뒤에 필요한 OT 제조사가 제공하는 보안 기술이나 OT 전문 보안, IT 보안 기술과 솔루션을 구축합니다.



[그림Ⅳ-7. OT 보안 거버넌스 계획수립]

A. OT 네트워크 영역



[그림Ⅳ-8. 악성코드 탐지 솔루션 구성]

영역	보안 포인트	보안구성	상세방안
업무망 ↔ OT망	1	IDMZ 구성	▪ 방화벽으로 분리된 산업전용 DMZ 구성
	2	원격접속 제어	▪ 네트워크 구성 및 방화벽 정책 확인 ▪ 비정상접근/불필요 서비스 포트 차단 ▪ 모의해킹을 통한 보안 Hole 확인
	3	네트워크 Segmentation	▪ OT망 ↔ IT 업무망 분리 (IDMZ 구축)
OT망 ↔ ICS영역	4	OT 보안 솔루션 구축	▪ ICS 이상징후 탐지 솔루션 ▪ 단방향 게이트웨이 등 맞춤 솔루션 도입
	5	네트워크 Segmentation	▪ 주요 생산/설비 네트워크 이중화
전체영역	6	네트워크 통합 모니터링	▪ 산업용 프로토콜 분석 및 모니터링
	7	ICS 이상징후 탐지	▪ 비정상 접근 및 비 인가자 접근탐지 및 차단 ▪ 최신 제조산업 취약점 반영

[표Ⅳ-2. OT 네트워크 영역 구성방안]

B. OT 장비 보안 영역

OT/ICS 자산 가시성확보부터 장비별 보안점검 관리까지 심층 보안전략 수립

기존공장대응

비식별자산

생산·설비자산

OT 보안 자산 확인

화이트리스트 백신설치

보안패치 및 업데이트 여부

매체제어

자산 보안 현황 파악

OT자산 가시화

신규공장대응

Security By Design
- ✓ 산업설비 도입 전 보안성 검토 진행
- ✓ 신규 구축 제조공장 보안시스템 설계 지원

장비 보안 취약점 분석
- ✓ 제조사별 장비 체크리스트 기반 취약점 점검
- ✓ OT 장비 필수 보안설정 확인 및 적용

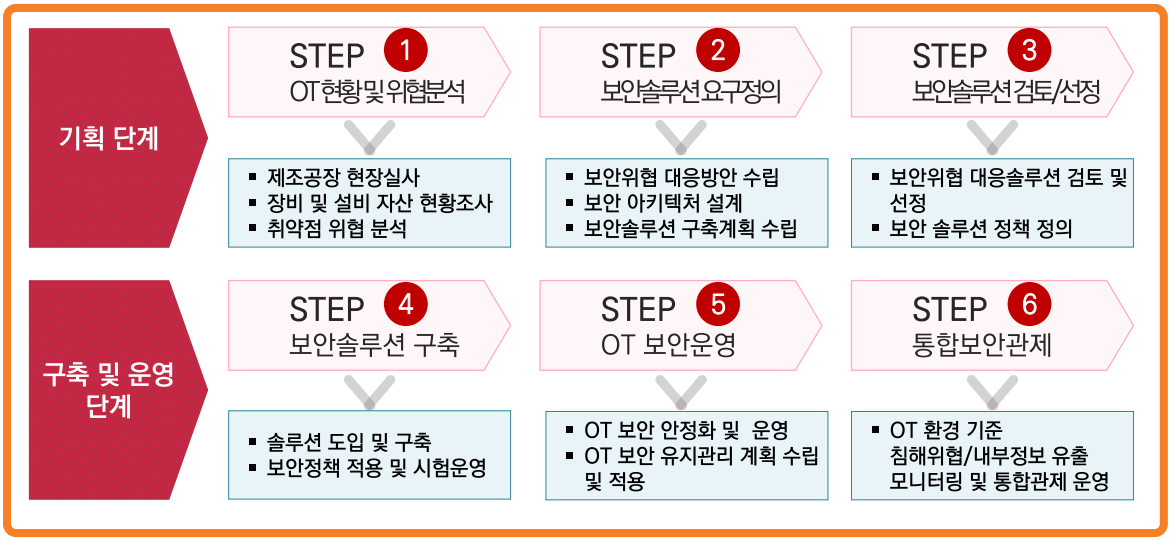
패치 및 취약점 관리
- ✓ 유지보수PC 관리
- ✓ 설비 단말 최신 보안 패치
- ✓ EOS 장비 관리

OT 장비보안 수립 이전
1. OT 자산 식별 및 보안 대상 구분 필요
2. OT 자산에 대한 보안 점검 방안 부재
3. OT 자산에 대한 보안 관리 방안 필요

OT 장비보안 수립 이후
1. OT 장비 식별 및 대상 조사 진행 (가시성 보안 솔루션 구축)
2. OT 장비 보안 점검 항목 제공 (국내외 표준 기반의 OT장비 보안 요구사항)
3. OT 장비 별 보안 점검 가이드라인 제공 (제조사별 보안요건 분석)
4. OT 장비 취약점 보고서 및 이행 관리 제공

[그림Ⅳ-9. OT 장비 보안 영역]

9) OT 보안 솔루션 구축 시 고려사항



[그림Ⅳ-10. OT 보안 솔루션 구축 시 고려사항]

현장실사

- OT 보안 위협에 대한 현장 점검
- OT/ICS 운영 환경에 대한 분석

보안솔루션 요구사항

- 현장 실사에 따른 산업용 프로토콜 지원 및 구축 제반 사항
- 소스코드 취약점 점검 및 보안 디자인 적용 여부 검토
- 도입 보안 솔루션의 OT/ICS 네트워크 및 장비 가용성 영향도 검토

보안 아키텍처 설계

- 보안 솔루션 도입으로 인한 OT/ICS 네트워크 및 보안 설계
- 표준 OT/ICS 보안 요구 사항에 따른 보안 솔루션 구성 제시

통합보안관제

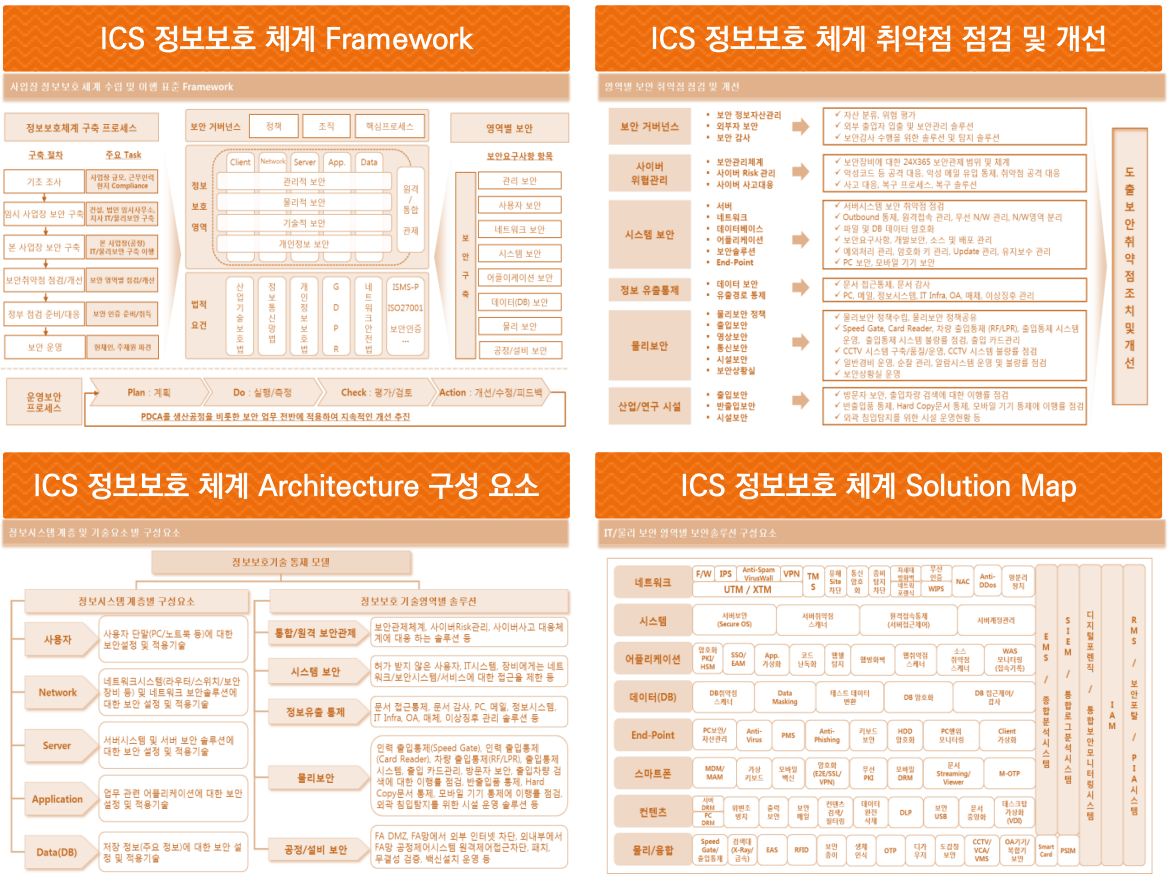
- OT/ICS 보안 솔루션 이벤트 로그 수집 및 통합 모니터링
- OT/ICS 네트워크 패킷 분석을 통한 이상행위 모니터링
- IT/OT 통합 모니터링을 통한 융합 보안 제공

✓ ICS 정보보호 체계 표준 SK인포섹 ICS 정보보호 체계[1] Overview

SK인포섹은 정보보호 기준 참조모델을 토대로 국내·외 보안 요구사항을 충족하는 ICS 정보보호 체계 Framework, Architecture 구성요소 및 Solution Map, 취약점 점검 및 개선을 포함한 정보보호 체계를 보유하고 있습니다.

ICS 정보보호체계는 각기 다른 산업 제조시설에도 적용 가능한 표준 보안 모델입니다. △네트워크, 서버, 어플리케이션(앱), 데이터 등 영역별로 필요한 기술적·물리적·관리적 보안 요구사항 △보안 정책, 수행 조직 등 보안 기준과 프로세스 △관련 보안 인증과 법적 요건 등을 반영했습니다.

이를 활용하면 기업 핵심 기술과 영업 기밀 등급에 맞춰 보안 체계를 갖출 수 있으며, 정부 보안성 평가 지표에 따른 정보·물리·제조 시스템 보안 요구사항을 충족하고 이를 위한 구축·운영 방법론을 적용할 수 있습니다.



[그림Ⅳ-11. ICS 정보보호 체계]

1) ICS 정보보호 체계 : SK인포섹이 산업제어시스템(ICS) 정보보호체계 국내 최초 특허 출원(2020.10)
스마트 공장 보안 설계와 구축, 운영을 위한 기술적 토대를 마련

✓ ICS 정보보호 체계 표준 ICS 정보보호 체계 중점과제 및 추진방향

중점 과제	추진 방향
관리적 보안 측면 ▪ 보안정책 수립 및 정보보호 등급 분류 ▪ 보안 구축 및 운영 조직 R&R 확립 ▪ 보안점검 및 교육 상시화	**글로벌 수준의 정보보호 정책 적용** ✓ SK 그룹사 정보보호 정책 반영 – 중요정보 식별, 분류, 통제 정책 마련 – 유출 방지를 위한 중요정보 Life-Cycle 관리 – 취약점 점검 및 정기적인 보안점검 시행
물리적 보안 측면 ▪ 다양한 경로의 물리보안 대책 마련 ▪ 출입통제 통합관제 체계 구축 (Gate, 차량, CCTV, MDM, 보안검색)	**정보유출 차단을 위한 융합관제 체계 구축** ✓ 외부 저장매체 통제 강화 ✓ 중요정보 유출방지 솔루션 적용(DRM, DLP, 매체제어, PC보안 등) ✓ 복합인증과 통합관제를 통한 출입자 추적관리
기술적 보안 측면 ▪ 보안 취약점에 대한 대응 체계 구축 – 네트워크 망분리, 방화벽 룰 관리 – 매체 제어 및 정보유출 차단, 암호화 (DRM, 비인가SW·유해 콘텐트 차단)	**최적의 보안시스템 적용을 통한 보안 강화** ✓ 인터넷 망, 업무망, FA 보안 Zone 구성 ✓ APT 공격 대응을 위한 관제 체계 구축 ✓ 백신 및 패치 강화(윈도우 기반 생산설비)

산업제어시스템 보안 이슈

- ✓ 산업제어시스템 보안사고의 95%는 인적 보안
- ✓ 접근경로의 통제 미흡 (인터넷, 이더넷, 모바일 등)
- ✓ 네트워크 세그멘테이션 및 보안 모니터링 미흡 (오피스와 폐쇄망의 양방향 연동, 근거리 무선 연결)
- ✓ 생산/설비망 접근통제 미흡 (원격 액세스 모뎀, 시리얼 연결, 모바일, USB 디바이스)
- ✓ 지능화, 고도화되고 있는 APT 공격 대응 미흡 (이메일, USB 실행, 변조된 파일 공격, 모바일 공격)

[그림Ⅳ-12. ICS 추진방향]

Part 2

의료정보 보안

1) 개념 및 관련법령

가. 의료정보 보안의 정의

의료정보란 의료행위를 통하여 수집된 자료 및 이 자료들을 기초로 하여 연구 및 분석된 정보들을 포괄하는 것으로 진단과 치료행위, 치료 후의 관찰 등을 포함하여 의료행위의 전 과정에서 수집된 환자의 건강상태 등에 한 정보입니다. 따라서 의료정보는 매우 민감한 사생활 정보입니다. 철저하게 정보 비밀이 보장되어야 하며 의료기관 특유의 신속한 처리 요구에도 대응해야 합니다.

정보 구분	의료정보 내용	정보 구분	의료정보 내용
환자의 기본 정보	성명, 연령, 생년월일, 주소, 연락처, 근무지, 가족관계 등	진료기록 정보	진단, 진료계획, 현 병력 등
건강보험과 복지 정보	건강보험정보, 장애자 기록	지시실시 기록 정보	처방기록, 수술기록, 처치기록 등
진료 관리용 정보	진료정보, 적용보험정보, 내왕일자, 입•퇴원 등	진료정보 교환 정보	진단서 등
생활배경 정보	흡연여부, 음주여부, 정신상태 여부	진료설명과 동의정보	각종설명정보, 각종동의정보
의학적 배경 정보	출생 시 체중, 임신분만에 대한 진료기록, 예방접종에 대한 기록	사망기록정보	사망진단서, 부검기록 등

* 출처 :“헌법상 환자의 의료정보에 대한 권리에 관한 연구”, 『헌법학연구』 제11권 제3호, 2005

[표Ⅳ-3. 주요 의료정보 구분]

의료정보 보안	구분	금융정보 보안
의료행위를 통하여 수집된 개인정보, 진단자료, 치료행위 등을 포함하여 의료행위의 전 과정에서 수집된 환자의 정보	기본 정의	금융거래를 위한 개인정보, 금융 매체 정보, 거래정보 등 금융거래 행위에 따른 전체적인 정보
의료법, 의료기기법, 정보통신망법, 개인정보보호법	Compliance	전자금융거래법, 신용정보보호법, 정보통신망법, 개인정보보호법, 전자금융감독규정
의료기관 인증평가 정보보호관리체계(ISMS-P) 인증	관리 인증	정보보호관리체계(ISMS-P) 인증
▪ 진료정보 변조 ▪ 개인(의료) 정보유출 ▪ 의료기기 소프트웨어 위변조 ▪ 내부 전산망 랜섬웨어 ▪ 신종 사이버 위협 (APT 등)	위협정보	▪ 거래정보 변조 ▪ 개인(금융) 정보유출 ▪ 비대면 거래기기 소프트웨어 위변조 ▪ 온라인 서비스 거부 공격 ▪ 신종 사이버 위협 (APT 등)
건강보험정보, 장애인정보, 진료정보, 흡연/음주/정신상태 , 임신분만정보, 처방기록, 진단서 등	주요 보호 대상 정보	통장번호, 카드번호, 주민등록번호, 핸드폰번호, 금융거래정보 등

[표Ⅳ-4. 의료보안 및 금융보안 비교]

나. 개인정보 파일 관리의 근거법령

개인정보 파일명	근거법령
진료 신청서	의료법 제22조
선택진료 신청서	의료법 제46조, 선택진료에 관한 규칙 제2조
진료기록부	의료법 제22조, 같은 법 시행규칙 제14조
조산기록부	의료법 제22조, 같은 법 시행규칙 제14조
간호기록부	의료법 제22조, 같은 법 시행규칙 제14조
환자명부	의료법 제22조, 같은 법 시행규칙 제15조
처방전	의료법 제18조, 같은 법 시행규칙 제12조
수술기록	의료법 제22조, 같은 법 시행규칙 제15조
검사소견서	의료법 제22조, 같은 법 시행규칙 제15조
방사선사진.소견서	의료법 제22조, 같은 법 시행규칙 제15조
진단서	의료법 제17조, 같은 법 시행규칙 제9조
사망진단서(사체검안서)	의료법 제17조, 같은 법 시행규칙 제10조
출생증명서	의료법 제17조, 같은 법 시행규칙 제11조
사산.사태증명서	의료법 제17조, 같은 법 시행규칙 제11조
감염병환자, 감염병의사환자, 병원체보유자 신고	감염병의 예방 및 관리에 관한 법률 제11조, 같은 법 시행규칙 제6조, 성매개감염병 및 후천성면역결핍증 건강진단규칙 제7조
응급환자이송	응급의료에 관한 법률 제11조, 같은 법 시행규칙 제4조
감염인 진단.검안사실 신고	후천성면역결핍증예방법 제5조
특정수혈부작용신고	혈액관리법 제10조, 같은 법 시행규칙 제13조
뇌사추정자신고	장기 등 이식에 관한 법률 제17조, 같은 법 시행규칙 제11조
질병자 또는 질병의심 대상자 발견 보고, 신고, 통지 등	보건의료기본법 제5조
환자진료기록의 열람 및 사본 교부	의료법 제21조, 같은 법 시행규칙 제13조의2
요양급여 의뢰서	국민건강보험법 제41조, 국민건강보험 요양급여의 기준에 관한 규칙 제2조
외국인환자유치사업실적보고	의료법 제27조의2, 같은 법 시행규칙 제19조의9

[표Ⅳ-5. 개인정보 관리 근거법령]

다. 의료정보 용어 정의

의료정보 보안 관련 용어는 국내외 표준 문서와 TTA 정보통신 용어사전, 식약처 가이드라인에서 부분적으로 준용하여 설명 합니다.

구분	내용
개인정보	생존하는 개인에 관한 정보로서 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 개인을 식별할 수 있는 정보
의료정보	국가적 차원의 보건정책을 위한 자료제공의 역할에서부터 각종 보건 의료종사자들에 대한 정보제공과 각 분야의 실무종사자가 필요로 하는 정보제공의 역할까지를 포함하는 광범위한 개념 협의로는 서면 혹은 전자문서의 형태로 기록 저장된 환자의 의무기록에 관련된 정보로 진료기록 혹은 진료내용과 동일한 의미
진료기록	환자의 건강력, 진단명, 현 질병 상태나 과거 질병에 대한 사항과 그 치료내용 및 경과, 각종검사결과, 그 외 환자진료에 필요한 지극히 개인적인 정보들을 포함하여 환자나 그 가족, 측근들로부터 얻어져 문서 혹은 컴퓨터에 기록, 저장되어있는 모든 정보
진료기록의 유출	의료기록에 대한 접근권리를 지닌 개인당사자가 아닌 제3자에게 진료기록의 내용이 제공되는 것
사적 비밀보장	정보에 있어서 프라이버시로 많은 직업적인 관계를 포함한 특별한 관계 속에서 오고 가는 정보들을 당사자의 허가 없이 유출하지 않는 것 환자·의료인이라는 특정관계에서 의료인은 의료행위 도중 알게 된 환자와 관련된 사항이나 그가 관찰한 환자의 허가 없이 누구에게도 누설해서는 안됨
전자의무기록 (EMR: Electronic Medical Record)	의료기관에서 생성되는 모든 진료정보, 진단결과, 처방결과, 약제 처방자료, 인사과 기록, 비용 등의 원무 자료, 외래 자료, 사용되는 의료 전문용어, 진단 및 처방 결정을 위한 보조 시스템 등 총체적 자료. 이러한 자료들의 전산 매체 저장은 단순히 환자의 병력을 조회하고 의료적인 판단을 돕는 것을 넘어 법적, 행정적, 재정적 자료와 연동되는 기록을 포함
전자건강기록 (EHR: Electronic Health Records)	한 기관이 아닌 여러 기관에서 나오는 모든 의료 정보를 다루는 것을 의미, 즉, 기관 대 기관으로 정보를 통합하고 전달하여 공유하는 내용 포함
처방 전달 시스템 (OCS: Order Communication System)	환자를 중심으로 발생하는 질병의 제반 내용을 전산화하여 단계별로 기록하는 시스템으로서, 진료기록을 전산화하여 쉽게 공유하고 의료진이 진료, 약과 주사, 수술, 처치, 검사, 촬영 등을 신속하게 전달토록 하는 시스템
의료영상 저장전송시스템 (PACS, Picture Archiving Communication System)	X-ray, 자기공명영상촬영장치(MRI: Magnetic Resonance Imaging), 컴퓨터단층촬영장치(CT:Computed Tomography), 양전자 방출 단층 촬영 (PET: Positron Emission Tomography), 투시촬영장치, 혈관조영장치, 유방암검진기 등 영상진단장비를 사용하여 촬영한 영상정보를 네트워크를 통해 전달하는 시스템
방사선정보시스템 (RIS: Radiology Information System)	방사선과 검사 접수부터, 촬영, 결과 보고서 생성까지 전반적인 방사선과 업무를 전산화하는 시스템

[표Ⅳ-6. 의료정보 용어 정의]

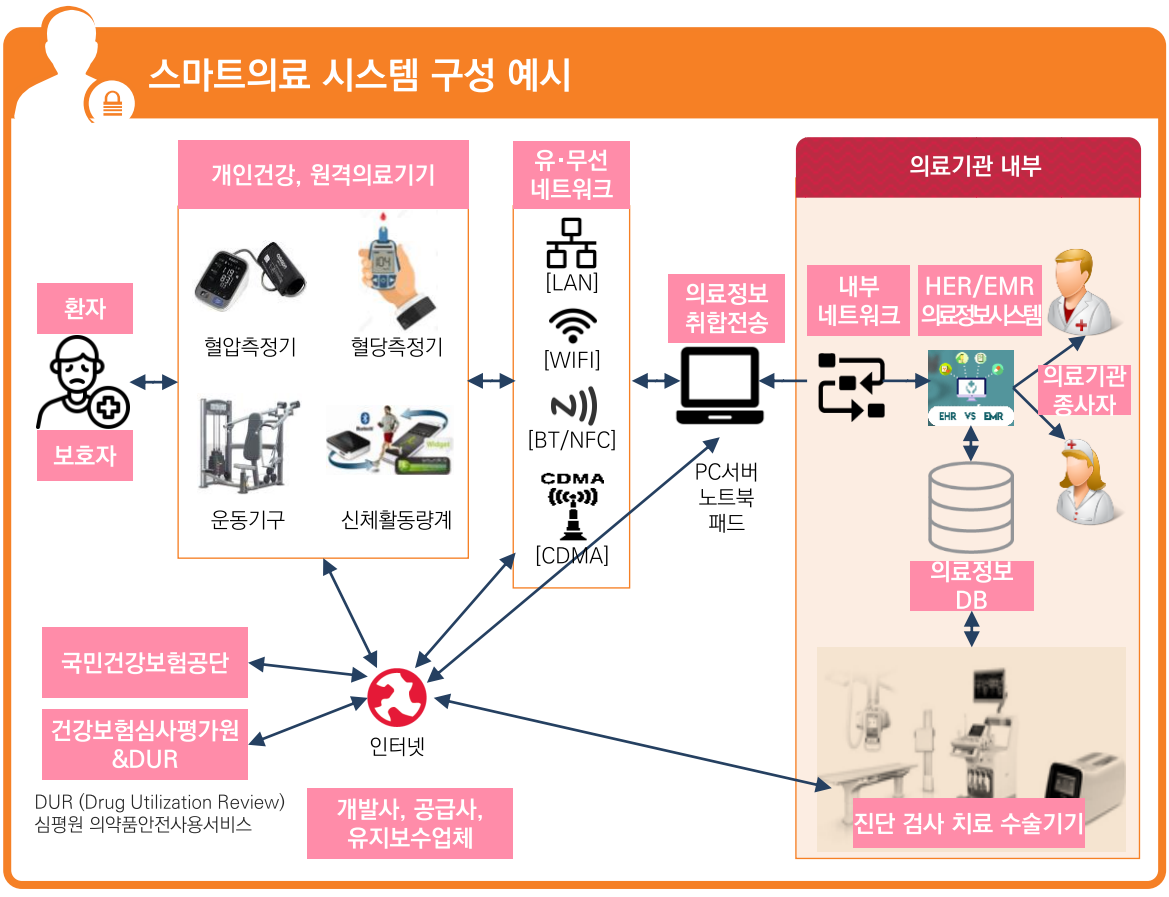
2) 스마트 의료 시스템 위협 현황

가. 스마트 의료 시스템 현황

최근 네트워크 기반의 의료기기 및 의료정보시스템이 인공지능, 빅데이터 등 최첨단 기술이 발전하고 있으며, 통신 기술을 이용한 의료기기가 증가함에 따라 의료기기 해킹, 정보 유출 등 사이버 보안 위협의 사례도 증가하고 있습니다. 이러한 사이버 보안 위협은 의료기기의 오류와 결함을 발생시키고, 환자 건강에 해를 가할 수 있어 보안 위협에 대한 의료기기의 안전성이 확보되어야 합니다. 유·무선 통신이 가능한 의료기기에 대해 사용자의 건강에 직접적인 영향을 미칠 수 있는 사이버 보안 위협에 대하여 방어할 수 있는 체계가 필요한 시점입니다.

하지만, 국내 의료기기 업체에서는 의료기기 사이버 보안에 대한 인식과 대처가 미흡하고, 의료기기 허가 신청 시 사이버 보안과 관련된 첨부자료의 작성에 어려움이 있는 것이 현실입니다.

의료기관 내에서 활용되는 의료기기부터 의료진에 의해 모니터링 되고 처리되는 영역까지 발생 가능한 보안위협을 제시하고 대응방안에 대한 방향을 전달 드립니다.



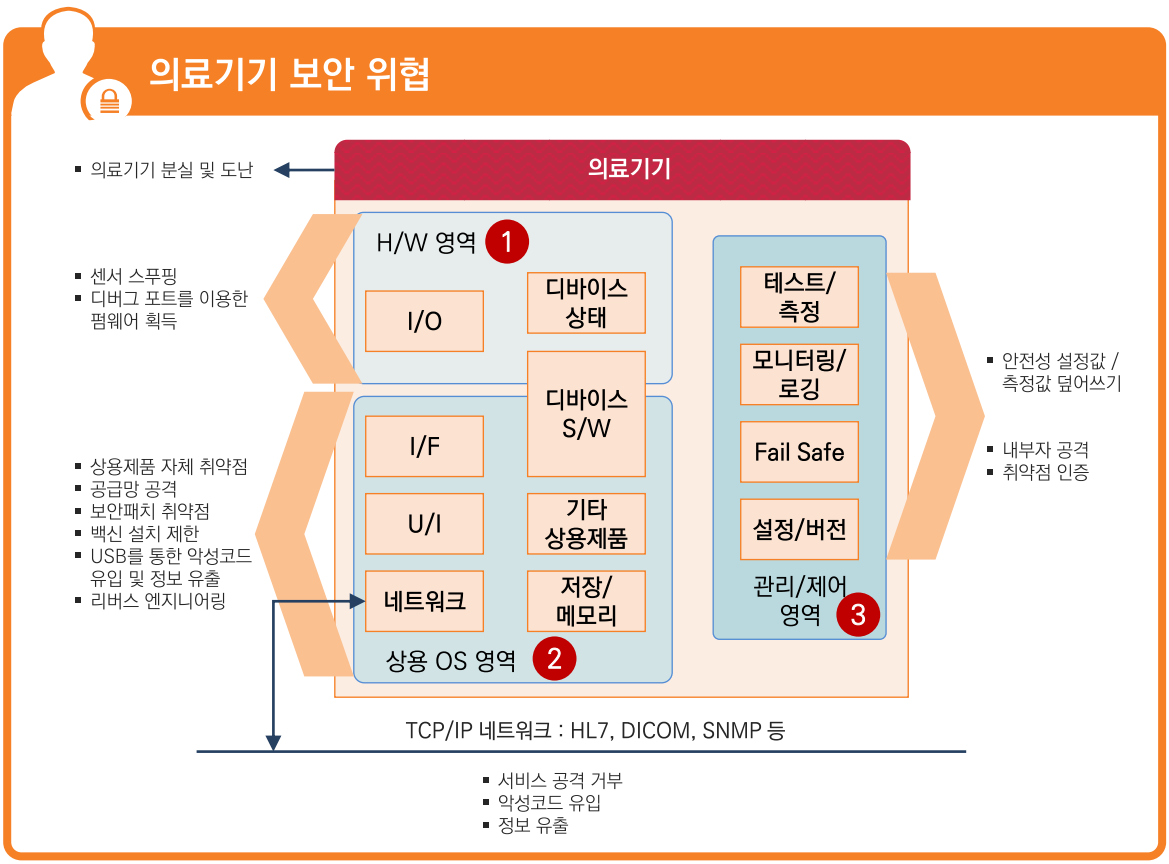
* 출처 :『스마트의료 사이버보안 가이드』, 한국인터넷진흥원 2018. 5.

[그림Ⅳ-13. 스마트의료 시스템 구성]

나. 스마트 의료기기 보안위협

A. 의료기기 위협

스마트 의료기기는 의료 목적과 용도의 특수성으로 인해 다양하고 복잡한 기기들이 많이 사용되고 있습니다. 특히, 의료기기의 고유기능과 사용 목적, 네트워크 연결방식 및 연결목적, 저장·전송되는 데이터 타입 등에 따라 매우 다양하며, 헬스케어 시스템 간의 상호연동을 위해 개발된 의료정보 분야의 대표적인 표준이라 할 수 있는 HL7[1], 의료영상에서의 표준인 DICOM[2] 등 의료기기 관련 표준들도 매우 다양합니다. 미국 의료분야 비영리기관인 IHE[3]는 사이버 보안의 위협과 대응방법을 정립하기 위하여, 다양한 종류의 의료기기의 특성을 통합하고 상위 수준의 중요 구성요소를 도출함으로써 일반적으로 적용될 수 있는 의료기기 아키텍처를 제시하였습니다. 의료기기의 H/W영역, 상용 OS 영역, 관리/제어 영역으로 나누어 보안위협의 주요 요소를 아래와 같이 정의하였습니다.



출처 : IHE, Medical Equipment Management
Medical Device Cyber-Security-Best Practice Guide 재구성

[그림Ⅳ-14. 의료기기 보안 위협]

1) HL7 (Health Level 7) : 의료에서 사용되는 네트워크 통신 프로토콜
2) DICOM (Digital Imaging and Communications in Medicine) : 의료용 디지털 영상 및 통신 표준은 의료용 기기에서 디지털 영상표현과 통신에 사용되는 여러 가지 표준을 총칭
3) IHE (Integrating the Healthcare Enterprise) : 병원, 의료기기 간 국제표준 기반 의료정보 공유를 통해 상호운용을 추진하는 단체

B. 의료기기 위협 상세

의료기기 영역별 위협 구분	특성 및 이슈
1 의료기기 하드웨어 ✓ **의료기기 분실 및 도난** : 물리적 의료기기를 분실, 도난으로 의료기기 내 저장되어 있는 데이터 유출의 위험 존재 ✓ **디버그 포트를 이용한 펌웨어 획득** : 의료기기 개발 시 사용된 디버그에 포트를 제거하지 않은 의료기기에서 디버그 포트를 활용하여 펌웨어 등을 획득하는 공격으로 공격자가 내부 소스코드 및 구조를 파악 할 수 있으며, 이를 기반으로 알려지지 않은 취약점을 확인하거나 특정 부분을 변조하여 의료기기에 다시 주입공격 등을 할 수 있음 ✓ **부채널 공격** : 의료기기에서 전송되는 정보를 암호 알고리즘이 작동할 때 전기 소모량, 전자기 신호량 등을 분석해 암호키 등을 유추하는 공격 ✓ **USB를 통한 악성코드 감염** : USB 포트를 통한 악성코드 유포 또는 정보 유출 ✓ **센서 스푸핑** : 인증체계를 적용하지 않은 센서에 스푸핑 공격 등으로 데이터 감지를 방해함으로써 의료기기 오작동 유발	물리적 장비 보안위협
2 스마트의료기기 상용 OS 영역 ✓ **3rd party 소프트웨어 취약점** : 의료기기에 펌웨어, 운영체제, 어플리케이션 소프트웨어 (운영체제, 라이브러리, 데이터베이스, 모듈 등 공개용 및 상용 소프트웨어) 자체에 포함된 취약점으로 인한 기기 오동작 및 정보 노출 ✓ **부적절한 소프트웨어 패치** : 최신 버전의 소프트웨어 보안 패치가 이루어지지 않거나 안전한 경로를 통하지 않은 패치로 인한 악성코드 감염, 패치 전 적절한 안전성 테스트를 수행하지 않아서 발생하는 의료기기 오작동 등 ✓ **악성코드 감염(랜섬웨어)** : Anti-virus 시스템이나 백신 설치 어려움과 같은 의료기기 구조적 문제로 발생하는 위협으로 실행파일 검증 부족 등을 통한 악성코드 감염	OS 및 S/W 영역의 위협
3 스마트의료기기 관리 및 제어 영역 ✓ **설정 및 측정값(Calibration Values) 조작** : 악의적 공격자가 안전성 제어 또는 측정 기능의 값을 '덮어쓰기' 공격으로 변경하여 해당 기능을 상실하거나 안전성 한도 값을 초과하여 환자의 생명과 건강에 치명적인 위협을 가함 ✓ **내부자 공격** : 악의적 의도를 가진 관리자 기기 설정 변경 또는 비정상적인 활동 ✓ **취약한 인증** : 안전한 인증체계 미적용으로 권한 없는 사람이나 기기가 의료기기에 접근하여 권한을 탈취	권한 및 인증 보안위협

다. 의료정보시스템 보안위협

의료정보시스템이란 원무관리, 일반관리, 처방 전달, 검사 및 진료 지원 관리, 경영정보 관리, 영상의 저장과 전달, 전자의무기록 등 병원관리 관련하여 전산으로 정보가 저장, 관리되는 시스템이라고 할 수 있습니다. 의료정보시스템에 대한 보안은 매우 중요한 사항이나, 시스템의 세부적인 구조는 대부분은 일반적인 서버와 같은 형태로 구현되어 있어서 의료정보시스템에 대한 보안위협도 일반적인 인터넷 환경에서 서버가 갖는 보안위협과 유사합니다. 다만, 의료정보시스템에 저장·관리되는 정보는 매우 민감하고 중요한 정보들로 정보의 안전한 관리 측면에서 보안위협을 정의합니다.

의료시스템 영역별 위협 구분	특성 및 이슈
1 계정 및 패스워드 보안 위협 ✓ 사용자나 관리자의 계정, 패스워드를 획득하여 개인의 의료정보 등을 유출 특히, 교대근무가 빈번하고 다양한 직종들이 서로 상이한 근무조건에서 업무를 수행하기 때문에 의료기관의 경우 다른 분야보다 계정관리가 어려움 – 관리자 그룹에 일반 사용자 계정이 존재 – 불필요한 계정 존재 및 Guest 계정 활성화 – 취약한 패스워드 사용 및 패스워드 주기적으로 변경하지 않음 – 계정 잠금 임계값 설정하지 않음 – 패스워드 최대 사용기간 설정하지 않음 – 계정, 패스워드를 문서상에서 일괄적으로 관리 (노출, 공유)	계정관리 보안위협
2 접근 통제 보안 위협 ✓ 계정관리와 마찬가지로 다양한 직군이 상이한 업무시간에 직무를 수행하는 보건 의료 환경에서 권한에 맞는 적절한 접근 통제 정책을 적용하는 것은 매우 어려움 – 관리용 기본 공유 및 불필요한 공유 제거하지 않음 – 널 세션 접근 차단하지 않음 – 원격에서 레지스트리 접근 제한하지 않음 – 적절하지 않은 윈도우 시스템 디렉토리 접근 권한 – 원격 사용자의 시스템 셧다운 방지 설정을 하지 않음 – 세션 타임 아웃 설정하지 않음 – 관리자 계정 자동 로그온	접근통제 보안위협
3 비인가 프로그램 및 취약 S/W사용 ✓ 원격접근 차단, 불필요한 공유 제거 등 보안을 위한 기본적인 설정 오류 및 비인가 프로그램 사용으로 인해 의료정보시스템 내 중요정보 유출 가능 ✓ 의료정보시스템과 연계된 데이터베이스 보안설정 문제 및 DB자체의 보안취약점, 어플리케이션 취약점 등으로 인한 중요 데이터 유출 가능	S/W 취약점

3) 스마트 의료 보안 대응 방안[1)]

가. 접근통제 및 인증

대응방안	상세대응 정책 및 설정
역할기반 사용자 접근 통제 적용	✓ 접근통제 정책 수립 – 정보자산의 정의와 사용자 역할별 그룹 대상을 식별 – 시스템 및 네트워크 접근 권한과 정보 등급 – 환자정보 관련 시스템 접근 권한과 환자 정보 무관 정보 및 응용프로그램 접근 권한 분리 – 의료정보의 모든 접근은 로그를 기록하여 감사 추적성 확보 ✓ 접근권한 부여 절차 수립 – 담당 업무별 최소권한 및 최소인원 부여 원칙과 직무 분리 원칙 준수 – 동일 직종 내에서도 부서가 다른 경우에는 환자의 정보에 접근하는 권한을 다르게 부여 ✓ 인증 정책 및 절차 수립 – 특수 권한자에 대한 인증 정책 수립 – 일정 시간 미사용 시 세션 자동 종료 (시간 설정 값 지정) – 가능한 경우 기기 인증서 및 기기 인증 관리 – 로그인, 로그아웃 등 접속로그 기록 – 패스워드는 네트워크를 통해 평문 전송하지 않음 ✓ 주기적 로그 감사 및 교육 – 주기적 로그 감사를 통하여 권한 없는 데이터 및 시스템에 접근한 사람 식별 – 접근통제정책 위반자에 대한 정책에 따라 교육, 훈련 및 징계 ✓ 접근통제 정책 주기적 검토 – 최소한 연 1회 이상 접근통제 정책 검토 – 위반율이 높은 정책에 대한 재검토를 통하여 현실적으로 적용 가능한 접근통제 정책 수립
관리자 및 특수 권한 관리	✓ 관리자 및 특수 권한 할당 및 사용 시에는 책임자의 승인을 포함한 인가 절차 수립 ✓ 관리자 권한 및 특수 권한을 식별하여 별도 목록으로 관리 – 각 시스템 및 프로세스(OS, DB, 어플리케이션 등) 관련 특수 접근권한과 이 권한 부여가 필요한 사람을 식별 – 관리자 권한을 식별하여 사용자를 최소한으로 제한하고 관리자 권한의 계정은 별도의 목록으로 관리하는 등 통제절차를 수립 ✓ 특수권한 계정 설정 시 Default 계정 사용 제한 (administrator, admin, root 등) ✓ 특수권한 계정의 변경은 주기적인 검토를 위해 로그를 기록 ✓ 시스템 관리자, 개인정보 및 의료정보처리시스템 등 중요 정보 취급 사용자 인증은 Two-Factor 인증 추가
의료기기 로그인 인증 강화	✓ 의료기기를 실행시켰을 때 로그인 과정 없이 바로 의료기기 어플리케이션이 실행되지 않도록 부팅 패스워드 또는 로그인 절차 설정 ✓ 의료기기 어플리케이션 접속을 위한 로그인 절차 설정 ✓ 의료기기 어플리케이션 셧다운 시 OS에 접근할 수 없도록 차단 기능 설정
응급모드 관리	✓ 환자의 생명과 건강을 보호해야 할 위급한 필요성을 입증할 수 있을 경우에만 엄격하게 인증우회를 허용하며 사전에 응급사항에 대한 정의와 절차 등을 수립 ✓ 의료기관은 응급상황에 대한 오남용과 보안위협을 대응하기 위해 인증우회에 대한 사후보고와 주기적인 로그 감사를 수행

[표Ⅳ-7. 접근통제 및 인증 대응방안]

1) 스마트 의료 보안 대응 방안 : 『스마트의료 사이버보안 가이드』 인터넷진흥원 2018.05 발행 내용 참조

나. 패스워드 및 암호화 키 관리 방안

대응방안	상세대응 정책 및 설정
안전한 패스워드 설정	✓ 패스워드 보호 및 길이 : 숫자, 영문자, 특수문자를 혼합하여 8자리 이상 ✓ 패스워드 변경주기 : 최대 3개월 이내 ✓ 메모장, 엑셀 등을 통한 일괄적인 계정/패스워드 관리 금지 ✓ 잘못된 패스워드 설정 예 : 생일, 주민등록번호, 전화번호, 연속된 번호 등 추측 가능한 비밀번호
패스워드 보호	✓ 패스워드 저장 시 암호화 - SHA224/256/384/512 등 SHA2 이상의 해쉬 함수(단방향 암호) 적용 - DB 접속 인증정보는 AES-128 이상 암호화 알고리즘으로 암호화하여 저장 ✓ 패스워드 입력 시 마스킹 처리 ✓ 패스워드 검증 실패 시 공격자에게 힌트가 될 수 있는 정보를 제공하지 않음 ✓ 일정 횟수 이상 패스워드를 잘못 입력 시 의료기기 및 의료정보시스템 접근 제한
초기 설정 비밀번호 변경	✓ 의료기기 및 의료정보시스템의 초기 설정 비밀번호는 단순한 패스워드로 설정되어 있는 경우가 많으므로 실제 운영하기 전에 반드시 보안성이 높은 패스워드로 변경 필요 ✓ 내장된 패스워드(혹은 암호키)를 사용하는 경우가 있는데, 기기 내부에 하드코딩된 패스워드(암호키)의 경우 중요정보가 유출될 수 있으므로 기기 내에 내장된 패스워드를 사용하지 않고, 별도의 패스워드를 생성하여 이용할 수 있도록 조치
하드코딩된 암호화 키 사용 금지	✓ 코드 내부에 하드코딩된 암호화 키를 사용하여 암호화를 수행하면 정보 유출 가능성 높음 ✓ 일부 해쉬 함수들은 역계산이 가능하고 무차별 대입(Brute-Force) 공격에 취약 ✓ 하드코딩된 암호화 키가 한번 해독되면 변경이 어렵고 공격자가 같은 컴포넌트를 사용하는 모든 제품에 대해 사이버침해가 가능 ✓ 암호화 수행 시 상수가 아닌 암호화키를 사용하도록 설계하고 소스코드 내부에 저장하지 않도록 처리
안전한 암호화키 관리 방안	✓ 고강도의 암호 알고리즘으로 암호화한 데이터라 하더라도 암호화키를 안전하게 관리하지 못한다면 환자의 의료정보 및 개인정보는 쉽게 유출
암호화를 위한 하드웨어 보안 모듈	✓ HSM(Hardware Security Module) : HSM은 시스템의 외부(모듈이나 카드형태)에 추가하여 암호화키를 관리, 생성 및 저장할 수 있는 보안 장치 ✓ HSM은 착탈식 또는 외부 장치이기 때문에 좀더 넓게 사용되고 있으며 TPM이 제공되지 않은 시스템에서도 쉽게 추가 가능 ✓ TPM(Trusted Platform Module) : 암호화 키를 시스템에서 하드웨어 칩으로 제공되며, 많은 노트북 컴퓨터가 TPM이 포함되어 있으며 시스템에 TPM이 포함되어 있지 않으면 추가 불가 ✓ TPM을 통해 전체 디스크 암호화 기능을 제공하여 인증 프로세스 완료 전까지 저장장치를 봉인 된 상태로 유지할 수 있음

[표Ⅳ-8. 패스워드 및 암호화 키 관리 대응방안]

다. 데이터 보호

대응방안	상세대응 정책 및 설정
저장 데이터 암호화	✓ 개인정보보호법상 데이터 중 환자를 식별 할 수 있는 고유식별번호(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오 정보 등의 암호화 대상 정보를 전송, 저장 시 개인정보 암호화 적용 기준에 따라 암호화 처리
영상의료 데이터 등 전송 데이터 암호화	✓ 의료 영상 데이터의 경우 의료기기 표준 통신프로토콜인 DICOM을 많이 사용하고 있으며, TLS기반으로 통신구간 암호화를 지원하는 DICOM-TLS 프로토콜 적용이 가능한 의료기기의 경우, 의료기기와 게이트웨이, PACS 서버 등의 DICOM 암호화 설정에서 DICOM-TLS 기능을 활성화하여 영상의료 데이터를 포함한 데이터 전송 시 암호화 적용이 가능

[표Ⅳ-9. 데이터 보호 대응방안]

라. 악성코드 감염 방지

대응방안	상세대응 정책 및 설정
악성코드 감염경로 차단	✓ 인터넷 : 의료기관 내부 망(의료정보망)에서의 인터넷 사용을 원칙적으로 금지 ✓ USB 연결장치 : 승인된 USB 외의 사용 금지, USB 포트 차단 ✓ 공유폴더 : 공유폴더 사용 금지해야 하며, 특히 의료기기 및 게이트웨이에서 사용하는 공유폴더에 대한 대안 마련 ✓ 이메일 : 이메일을 통해 악성프로그램 유입이 증가함에 따라 이메일 첨부파일, 본문내 링크 등을 검사하여 병원내 악성프로그램 감염을 차단
권장 백신 사용	✓ 안티바이러스 백신의 실시간 감시 및 차단 기능 활성화 ✓ 안티바이러스 백신의 주기적 업데이트를 통한 최신상태 유지 ※ 의료기기의 경우 자동 업데이트를 하지 말고 제조사 및 개발사에서 충분히 검증된 버전 사용
악성프로그램 실행 방지	✓ 의료기기 구동 응용프로그램, 게이트웨이 응용프로그램 등 의료용 응용프로그램을 제외한 악성프로그램이 실행되지 않도록 프로그램 실행 통제 정책을 마련하여 적용

[표Ⅳ-10. 악성코드 감염 방지 대응방안]

마. 이동식 저장매체(USB 등) 보안

대응방안	상세대응 정책 및 설정
USB 포트 접속 통제	✓ 의료기기, PC, 서버 등의 USB 포트는 사용을 차단하고 정해진 절차에 따라 승인된 보안 USB 장치만 사용할 수 있도록 보안설정을 강화 ※ EMR 등을 사용하는 의료기관 내부망과 연결된 컴퓨터에서는 승인된 USB 외의 사용을 원칙적으로 금지(USB 포트 잠금 장치 등 활용가능) ✓ USB는 자동실행 되지 않도록 실행권한을 차단하여 악성코드의 감염을 방지 ✓ USB 전용 PC는 의료기기 및 네트워크가 연결되지 않은 상태에서 운영
유지보수 시 USB 사용 관리·감독	✓ 제조 및 판매업체, 유지보수업체에서 USB를 통해 주요 시스템의 보안패치 또는 유지보수 시, 사전에 등록한 보안 USB만을 사용하도록 하며, 사용하기 전 바이러스 검사 실시 ✓ 의료기기의 주요 시스템 접속하거나 환경설정에 접근하기 위한 인증키가 저장된 USB를 제조 및 판매업체, 유지보수업체에서 이용하는 경우, 해당 의료기관의 보안 담당자는 인증키 사용자를 확인하고 외부업체의 작업 후 변경된 내용에 대해 검토해야 함

[표Ⅳ-11. 이동식 저장매체(USB 등) 보안 대응방안]

바. 소프트웨어 보안패치

대응방안	상세대응 정책 및 설정
최신 패치 관리계획 수립	✓ 의료기관은 효과적인 최신 패치관리 절차를 수립하고 개발사와 밀접한 관계를 유지하여 변경 가능성, 중요도, 진료에 미치는 영향도에 따라 우선순위를 결정 ✓ 의료기기의 버전 업데이트 주기를 고려하여 패치 계획 수립 ※ 일반적으로 의료기기 개발사는 18~24개월 마다 새로운 버전을 출시하고, 소규모 업데이트나 장애처리를 빈번하게 수행하므로 의료기기 버전 업데이트 시 보안 패치도 함께 수행 가능
보안 패치 파일의 안전성 및 보안성 확인	✓ 해당 의료기기 개발업체에서 안정성과 보안성을 충분히 검증한 보안 패치인지 사전에 검토 ※ 빈번한 보안 패치와 신규 버전 제공 주기 등으로 인해 개발사가 충분한 검토 및 확인 없이 출시하는 경우가 있기 때문에 반드시 제품의 안전성을 검증해야 함 ✓ Code Signing, MD5 등을 통해 의료기기에 설치된 소프트웨어 보안 패치가 승인된 버전인지 여부 및 무결성 등을 검증한 이후 설치 ✓ 기기 종류(의료기기 vs. IT기기)와 패치로 인해 진료 등의 이용과정에서의 발생할 수 있는 영향 등을 고려하여 패치 적용
안전한 경로를 통한 보안 패치	✓ 패치 서버 : 의료기기, 의료정보시스템 등이 운영되는 망의 경우 보안 패치 서버는 의료기관 내부망에 설치하여 운영 – 패치관리시스템은 침해사고 발생 시 의료기관 내 모든 컴퓨터에 영향을 주므로 보안성 강화를 위해 인터넷 연결을 차단하고 운영 – 패치파일은 관리자가 수동으로 다운로드하고 무결성 검증 및 악성코드 감염여부 등을 확인 후 패치관리시스템에 적용 – 패치관리시스템은 인가된 관리자 PC에서만 접속할 수 있도록 네트워크 접근 통제 ✓ 패치 수행 이력관리에 대한 로그 기록은 1년 이상 보존하도록 조치 ✓ 온라인을 통한 패치 : White List 방식으로 허용된 사이트에서만 패치 허용 (Windows 업데이트, 제조사 홈페이지, 안티 바이러스 백신 사이트 등) ※ 의료기기의 경우,Windows 자동 업데이트 설정하지 않고 해당 패치의 보안성을 충분히 확인 후 업데이트 실시 ✓ USB 저장장치 : 등록된 보안 USB 저장장치를 이용하여 허가된 직원이 업데이트
보안 패치 후 시스템 안전성 및 보안성 확인	✓ 의료기기 보안패치 작업 후 의료기관 현장에서 기존 의료정보시스템 및 의료기기에 영향을 미치지 않고 안전하게 작동하는지 충분한 테스트를 수행 ✓ 작업을 통하여 기존에 설정되어 있는 보안 설정에 변경사항이 없는지 확인하고, 패치 후 관리자 및 사용자 대상 교육을 실시

[표Ⅳ-12. 소프트웨어 보안패치 대응방안]

사. 시큐어 코딩

대응방안	상세대응 정책 및 설정
안전한 의료기기 및 서비스를 위해 SW 개발 생명주기별 주요 보안활동	✓ 요구사항분석 : 요구사항 중 어떤 의료정보 및 개인정보들이 시스템을 통해 관리되어야 하고, 이때 이 정보들은 얼마만큼의 보안등급(기밀성, 무결성, 가용성)을 가져야 하는지 정의 ✓ 설계 : 시스템을 분석해 위협들을 도출해내는 위협 모델링, 보안통제 기준 설정과 같이 개발보안가이드가 제시하는 작업을 기존 개발 프로세스에 추가 ✓ 구현 : 소프트웨어 개발보안가이드를 모든 개발자들이 준수하여 개발하는 것이 중요하며, 구현단계에서 단위테스트를 통해 소프트웨어가 가질 수 있는 보안 취약점을 충분히 제거할 수 있도록 해야 하며, 코드 리뷰 또는 구현 시 주기적인 소스 코드 진단 작업을 통해 소스 코드 수준의 안전성 보장 ✓ 테스트 : 설계 단계에서 도출된 위협들이 구현 단계에서 해당 취약점들이 없는 어플리케이션으로 개발되었는지를 동적 분석 도구를 이용하거나 모의 침투테스트를 통해 검증 ✓ 유지보수 : 각 개발 단계에서 안전한 소프트웨어를 만들기 위해 노력하였음에도 불구하고 발생될 수 있는 보안사고에 대한 관리 및 사고대응, 패치관리를 병행
개발 단계에서 시큐어 코딩을 적용하여 보안취약점을 사전에 제거	✓ 보안취약점 들은 분석·설계 단계에서부터 고려되어야 대응이 가능하며, 일부 항목은 개발 단계에 시큐어코딩 규칙을 준수하는 것만으로도 보안 취약점 제거가 가능

[표Ⅳ-13. 시큐어 코딩 대응방안]

아. 네트워크 보안

대응방안	상세대응 정책 및 설정
네트워크 보안 솔루션 도입	✓ 네트워크 기반 보안 대응체계는 응용 프로그램 수준에서 데이터 스트림을 통제하는 Application Proxy 형태의 구조와 Packet 단위 데이터를 통제하는 Inline 형태의 구조로 구현 ✓ 일반적인 IP 네트워크 데이터 단위가 Packet임을 감안할 때 네트워크 보안 솔루션 운영은 3계층 에서 Packet의 흐름을 통제하는 방식을 주로 사용
네트워크 보안 솔루션 도입- 네트워크 패킷 통제 장비	✓ 네트워크 Packet 단위에서 통제하는 대표적인 보안솔루션으로는 스크리닝 라우터, 방화벽, IPS 등 이 있음 ✓ 보통 OSI 3~4계층 수준(IP주소 대역 및 포트번호)에서 네트워크 트래픽을 통제
네트워크 보안 솔루션 도입- Application Proxy 구조 장비	✓ 응용 프로그램 수준 Proxy 구조의 주요 보안 솔루션으로는 WAF(웹 방화벽)가 있으며, 패킷의 헤더를 떼어낸 Payload의 연속된 흐름을 관찰하기에 용이한 구조 ✓ 패킷 단위로 정보를 살펴볼 수는 없지만 흐름 전체를 파악하기에는 Proxy 구조가 유리 ✓ 특히, 압축파일처럼 전체 파일을 확보해야만 하는 경우 Packet 단위로는 처리하기가 난해함 ✓ Inline 구조의 패킷 필터링 방화벽이나 IPS는 네트워크 수준에서 패킷의 흐름을 통제 ✓ 방화벽 안쪽에 존재하는 응용 프로그램 Proxy 구조의 WAF(Web Application Firewall)는 대외에 마치 웹 서버처럼 알려짐 ✓ 클라이언트들은 WAF를 웹 서버로 인식해 접속 ✓ WAF는 클라이언트가 송신한 데이터를 소켓 스트림 수준에서 검사하고 허용된 데이터에 대해 실제 웹서버로 WAF가 전달 ✓ 의료기관 운영하는 웹서버 앞에 WAF등을 설치한다면 보다 안전하게 운영할 수 있음
네트워크 보안 솔루션 도입- NAC 장비를 활용한 네트워크 접근통제 구현	✓ NAC(Network Access Control) 시스템을 운영하면 효율적인 네트워크 접근통제가 가능 ✓ 일반적으로 NAC 장비는 시스템에 등록된 MAC주소를 가진 게이트웨이나 의료기기만 네트워크에 접근할 수 있도록 L2 Access 수준에서 통제 ✓ 비인가 기기가 네트워크에 임의 접근하는 취약점과 MITM(Man In The Middle) 공격에 대응할 수 있음 ✓ 최근에는 인증된 MAC주소를 가진 기기라고 하더라도 일정수준의 보안 수준을 추가로 통과한 기기(예. 최신 보안패치 설치 유무와 백신 검사 통과 유무 등)만 내부 네트워크에 접속을 허용하는 정책을 추가로 구현하여 보안을 강화 하는 경우도 늘어나는 추세
의료기관 서브네트워크 분할 방안	✓ 스마트 의료 환경에서 의료기관은 네트워크를 자산의 가치 및 목적, 필요한 환경에 따라 적절한 네트워크 분할을 통한 구역 기반 보안 접근방식을 사용해야 함 ✓ 네트워크를 하위 구역으로 나누고 네트워크 구역 사이를 네트워크 보안솔루션으로 통제하면 PHI 등 중요정보가 저장된 구역(예. EMR 서버 영역)으로 신뢰도가 낮은 영역에서의 접속(게스트 네트워크 영역)을 제한하여 사이버보안을 강화 시킬 수 있고, 의료기관 내 스마트 의료기기가 외부와 정보를 교환할 때 복수 단계의 보호기능을 제공 할 수 있음
사전에 인가된 네트워크 정책만 허용	✓ 보안적으로 적절한 네트워크 구성은 업무나 역할에 따라 네트워크를 따로 분할한 후 서로간의 통신을 차단하는 것에서 시작 ✓ 특정 네트워크 혹은 단말간의 통신을 모두 차단하는 것을 전제로 필요한 것만 골라 허용해주는 보안 정책을 화이트 리스트 기반 정책이라 함

[표Ⅳ-14. 네트워크 보안 대응방안]

자. 무선 네트워크 보안

대응방안	상세대응 정책 및 설정
무선 WIFI 관리 방안	✓ 무선 의료기기의 경우 NIST의 「SP 1800-8, Securing Wireless Infusion Pumps('17.5)」 가이드에서는 의료기기 구역의 네트워크를 완전히 폐쇄된 네트워크로 구성하고 의료기관 내 코어네트워크에 무선의료기기가 직접 연결되는 방식이 아닌, 무선접속기(AP)와 무선 LAN컨트롤러(WLC)를 통해 통신하고 무선 WIFI를 관리 방식을 권장
WIFI 인가 방법	✓ 와이파이 네트워크에 연결을 시도하는 무선 의료기기는 상호 협의된 공유키나 인증서로 인가 받아야 함 ✓ NIST 1800-8에서 권장하는 인가 방식은 사전 공유키 인가 방식의 WPA-PSK와 인증서 인가 방식의 EAP-TLS 2가지 방식을 권장
무선 WIFI 암호 설정	✓ KRACK 취약점은 WPA2 프로토콜을 그대로 사용하고 공유기나 클라이언트 기기에서 보안 패치를 진행하는 것으로 대응이 가능하기 때문에 공유기나 무선 의료기기를 최신 보안패치를 수행하여야 함 ✓ KRACK 취약점 패치가 배포 전까지 통신사 와이파이 포함, 공공 와이파이는 사용 자제하고 암호화된 HTTPS 프로토콜을 연결하는 서비스, 신뢰 있는 VPN 서비스나 유선 네트워크를 권장
블루투스 보안 방안	✓ 초기 비밀번호 변경 : 0000, 1111로 설정되어 있는 초기 비밀번호 변경 ✓ 페어링 시 핀코드로 기기 인증 가능하도록 설계 ✓ 보안패치 업데이트를 통한 최신화 ✓ 사용하지 않을 경우 블루투스 기능을 항상 꺼둘 것

[표Ⅳ-15. 무선 네트워크 보안 대응방안]

차. 망분리

대응방안	상세대응 정책 및 설정
망분리 유형	✓ 망분리는 해킹 등 주요 사이버 공격으로부터 개인건강정보, 의료정보 등 중요 자료의 유출을 근본적으로 차단하기 위해 외부 인터넷 영역과 내부 업무 영역을 물리적 또는 논리적(가상화) 기술을 이용하여 네트워크, 서버 및 PC를 분리해서 사용하는 것
의료기관의 망분리 방안	✓ 의료 네트워크에서 의료 센서와 보안 게이트웨이는 사실상 인터넷에 접근할 이유가 많지 않으므로 물리적으로 인터넷망과 분리하는 것이 적절 ✓ 비용적인 문제 등으로 물리적 망분리를 바로 도입하기 어려운 의료기관의 경우 최소한 악성코드 감염의 많은 부분을 차지하는 것으로 파악되는 의료인 PC나 노트북을 통한 악성코드 감염을 최소화하기 위해 PC 기반(CBC) 논리적 망분리 라도 실시 ✓ 의료인의 PC등에 감염된 악성코드가 내부 의료 네트워크로 유입되는 것을 차단
망분리에 따른 영역별 보안솔루션 구축	✓ 외부 인터넷 영역과 내부 업무 영역을 네트워크로 분리하여 각 영역별 해당 보안 솔루션을 구축해야 함 ✓ 외부 인터넷 영역은 주로 외부 사이버 침해위협에 대한 방어 솔루션(DDoS, APT, IPS, IDS 등)으로 구축하고, 내부 업무 영역은 내부 의료정보 및 개인정보가 유출 되지 않도록 보안 솔루션(DRM, DLP, 매체제어, PC보안 등)으로 구축을 해야 함 ✓ 업무의 필요성과 필수적인 내·외부 통신을 위해 망연계 솔루션을 구축 ✓ 망연계 솔루션은 최소한의 파일과 스트림을 연계하고, 외부에서 내부로 연계는 악성코드 검사와 메일 내용 이미지 처리(외부 URL 링크 불가) 등으로 침해 방지를 하고, 내부에서 외부로의 연계는 정책적으로 관리자의 승인을 거쳐 처리 할 수 있도록 함

[표Ⅳ-16. 망분리 대응방안]

카. 감사로그 기록 및 관리

대응방안	상세대응 정책 및 설정
감사로그 식별 및 목록화	✓ 의료기기 : 로그인 아이디 및 시각, 환자 식별정보, 생성·열람한 환자정보, 의료기기의 환경설정 정보의 열람·생성·변경·삭제 이력, 외부 저장매체 등 입출력 기기의 연결 및 제거에 관한 로그 등 ✓ 게이트웨이 : 게이트웨이 로그인 아이디 및 시각, 의료기기와 의료정보 시스템간 송·수신되는 환자의 의료정보 및 개인정보, 게이트웨이 환경설정 정보의 열람·생성·변경·삭제 이력 등 ✓ 네트워크 : 네트워크 접속 IP, 시간, 네트워크 장비 환경설정 정보의 생성·변경·삭제 이력, 보안장비의 침입탐지 로그 등 ✓ 의료정보시스템 : 의료정보 시스템 접속 정보(ID, 접속시각, IP 등), 환자의 개인정보(이름, 주민등록번호, 환자 식별번호, 주소, 전화번호 등) 및 의료정보(진료기록, 병명, 진료영상 등)의 열람·등록·변경·삭제 이력, 외부 저장매체 등 입출력 기기의 연결 및 제거에 관한 로그 등
감사로그 기록 및 관리	✓ 감사로그에는 사용자를 특정할 수 있도록 ID, IP 등 고유 식별정보를 포함해야 함 ✓ 감사로그 중 개인정보, 비밀번호 등이 포함된 경우 암호화하여 저장해야 함 ✓ 감사사고 발생 시 사고의 내용을 확인하고 추적할 수 있도록 IP, ID, 시각, 접근한 정보 목록 등,작업내용 전부를 기록해야 함 ✓ 의료기기 및 의료정보 시스템의 접근 성공 및 실패 이벤트를 포함해야 함 ✓ 의료기기 및 의료정보 시스템의 입출력장치의 연결 및 제거에 관한 로그를 저장하고 검토해야 함 ✓ 관리자 및 특수권한을 가진 사용자의 모든 작업 활동을 기록하고 검토해야 함 ✓ 의료기기의 작동 및 오류, 경고 메시지 등 이벤트를 기록하고 점검해야 함 ✓ 의료정보시스템 이용자가 비정상적으로 많은 환자의 개인정보 및 의료정보를 열람할 경우 관련로그를 기록하고 검토해야 함 ✓ 감사로그 모니터링, 사고의 조사 등을 위해 자동화된 도구 또는 시스템을 구축·운영해야 함 ✓ 감사로그의 정확성을 보장하고 법적인 자료로써 효력을 지니기 위해 의료기기, 네트워크 정비, 의료정보시스템의 서버 등은 시각은 표준시간으로 정확하게 동기화(NTP 서버)해야 함
로그의 위변조 방지	✓ 감사로그는 위변조 되지 않도록 기술적 조치를 취해야 함 ✓ 감사로그의 편집, 삭제 권한과 감사기록 생성 중지 권한은 지정된 관리자만 수행 가능 ✓ 감사로그의 삭제, 변경, 천재지변에 의한 소실 등을 대비하여 별도의 저장매체에 백업해야 함 ✓ 감사로그 저장 공간 고갈에 따른 로그파일 덮어쓰기 또는 로그생성 중단 등 로그 손실을 방지해야 함
관리자 및 특수권한 접속기록 관리	✓ 관리자, 특수권한을 가진 자의 감사로그에는 접근한 파일, 작업내용 일체, 시작 및 종료시각, 접근정보(ID, IP 등)를 포함하여 기록해야 함 ✓ 계정 및 권한 관리자, 운영 관리자, 작업 관리자 등 모든 관리자 활동을 감사기록으로 생성해야 함 ✓ 관리자 및 특수권한을 가진 자의 로그기록에는 관리자 작업 활동에서 실행된 프로세스 정보를 포함해야 함 ✓ 관리자 및 특수권한을 가진 자의 로그기록은 관련 규정에서 정한 주기에 따라 검토해야 함

[표Ⅳ-17. 감사로그 기록 및 관리 대응방안]

✓ 의료 표준 스마트 의료 서비스의 주요 국제표준

● HL7 (Health Level 7)

미국 전자공업협회(EIA: Electronic Industries Alliance)가 의료정보의 전자 문서의 표준 교환 형식에 대한 표준 제정을 위한 표준화 기구 또는 이 표준화 기구에서 제정한 사실 표준. 'Level 7'는 OSI 7계층의 7번째 계층인 어플리케이션 계층을 의미하며 어플리케이션 계층은 어플리케이션 프로세스를 위한 공통 어플리케이션 서비스에 직접 접속하거나 실행함

정보보안을 담당하는 Security Working Group에서는 HL7에서 요구되는 인증, 무결성, 암호화, 감사 등의 보안서비스와 이를 구현하기 위한 메카니즘을 제시함. HL7에서 권장하고 있는 의료정보 전송 시 데이터 보호기법으로는 ① DES에 의한 데이터 암호화 후 전송, ② HTTPS 등 SSL 프로토콜 적용, ③ 보안메일 전송에 의한Secure EDI 사용 등이 있음

● DICOM (Digital Imaging and Communications in Medicine)

DICOM 표준은 의료용 기기에서 디지털 영상 표현과 통신에 사용되는 여러 가지 표준을 총칭하는 말로 미국방사선의학회(ACR)와 미국전기공업회(NEMA)에서 의료영상장비 표준화를 위해 구성한 1983년 발족한ACR-NEMA 디지털 영상전송 표준위원회에서 발표함

DICOM은 20개의 하위 표준(PS, Part Standard)으로 구성되어 있으며 이중 PS3.15이 Security and System Management Profiles임. PS3.15는 DHCP, LDAP, ISCL[1] 등 외부에서 개발된 표준을 참조하여 규정되었으며, Security protocol은 공인키와 '스마트카드'와 같은 보안기술을 사용할 수 있음. 데이터 암호화는 다양한 표준 데이터 암호화 스키마를 사용할 수 있음

PS3.15는 보안 정책 이슈를 다루는 것이 아니라 단지 DICOM 오브젝트 교환에 관한 보안정책을 구현할 때 사용할 수 있는 메커니즘을 제공함. 적절한 보안 정책을 수립하는 것은 로컬 관리자의 책임으로 DICOM은 암호화와 같은 보안메커니즘을 DICOM 환경에서 어떻게 적용할 수 있는지에 대한 방법만을 제시함

PS3.15는 다음의 8가지 프로파일을 제공함

- Secure Use Profiles
- Secure Transport Connection Profiles
- Digital Signature Profiles
- Media Storage Security Profiles
- Network Storage Security Profiles
- Time Synchronization Profiles
- Application Configuration Management Profiles
- Audit Trail Profiles

1) ISCL(Integrated Secure Communication Layer) : Presentation 계층과 TCP/IP 계층 간의 보안 기능을 관리하는 보안 계층
- ISCL 메커니즘은 스마트 IC 카드의 기본 기능과 대칭 비밀키 메커니즘에 의존
- 각 세션에 대한 대칭 키는 임의의 숫자를 가진 스마트 IC 카드의 내부 인증 기능에 의해 제공
- ISCL에는 인증, 확신 및 무결성을 보장하는 세 가지 기능이 있음
- 엔티티 인증 과정은 스마트IC 카드의 내부 인증 및 외부 인증 기능을 사용하여 3 경로 4 방향 방식으로 이루어짐
- 기밀 알고리즘과 무결성을 위한 MAC 알고리즘을 선택할 수 있음
- ISCL 프로토콜은 메시지 헤더와 메시지 데이터로 구성된 메시지 블록을 통해 통신

Part 3

금융 핀테크 보안

1) 금융 핀테크 정의

핀테크는 Finance(금융)와 Technology(기술)의 합성어로써 금융서비스와 정보기술의 융합을 통한 새로운 금융서비스를 말합니다. 금융 창구에서 행해지던 업무가 인터넷 뱅킹, 모바일 뱅킹, ATM 등 비대면 전자금융 서비스로 대체되는 것이 대표적입니다.

실제로 금융과 IT가 융합된 서비스이며, IT에 관련된 보안 이슈에 그대로 노출되고 있습니다. 특히 결제, 송금, 자산관리, 클라우드 펀딩 등의 다양한 서비스에 관련되어 있기에 보안이 취약하다면 예상치 못할 규모의 경제 손실이 발생할 수 있어서 보안 대응이 중요시 되고 있습니다. 핀테크 산업이 점차 확대되어 인터넷과 모바일 결제가 급증하고 있는 가운데 신용카드의 비대면거래(NCP)에 대한 부정사용 손실액도 꾸준히 증가하고 있습니다. 또한 고객의 편의성을 강조하면서 보안성에 대한 중요도가 더더욱 커지고 있습니다.

수년 전부터 금융분야의 정보보안 패러다임은 상급기관의 규제 중심에서 금융회사의 자율과 책임 중심으로 변화하고 있습니다. 보안의 자율성 강화는 보안수준의 다양화를 추구하는 것이며, 자율보안이라는 변화된 흐름에 맞추어 금융회사와 핀테크 기업은 그간의 타율 보안체계하에서 관련 법규정 준수라는 소극적 차원에서 벗어나, 필요한 보안 요소를 사업모델에 맞게 유연하게 적용함으로써 서비스의 보안성과 편리성을 함께 확보할 수 있어야 할 것입니다.

핀테크에서 IT기술을 적용하여 혁신적인 금융서비스를 제공하는 중요 요소로 핀테크 활성화 인증, 고객정보 보호, 이상거래탐지 등 보안적 요소를 비즈니스 모델 안에 재구성하여 안전함과 편리함을 동시에 구현해 나가야 할 것입니다.

규제에서 자율과 책임으로 금융 보안의 패러다임 변화

	규제 중심	자율과 책임중심
정책방향	사전 규제	사후관리 및 점검강화
보안영역	Prevention => Detection, Recovery	Prevention = Detection = Recovery
관리체계	Danger 관리 : 비용	Risk 관리 : 투자
보호대상	IT : 정보 & 시스템	전사적 : 비즈니스 전체
담당자	IT부서, 보안전문가	전부서
신뢰시스템	정부정책 (공인인증서 등)	시장 (소비자의 선택)

[그림Ⅳ-15. 금융보안 패러다임 변화]

2) 핀테크 서비스 분류

핀테크 서비스 분야 중 가장 기본적인 △'간편지급/지급결재' 서비스는 기존의 인증 과정을 최소화·간편화(단순 PIN번호 입력 등)하여 편리하고 빠른 결제·송금을 가능하게 합니다. 이를 위해서 인증 수단을 제공하는 핀테크 기업마다 중요 정보(개인정보 및 금융정보)를 직접 보유해야 하므로 개별 기업들은 금융소비자의 중요정보를 안전하게 저장·관리를 해야 합니다. △'인터넷 전문은행'은 모든 은행 업무(예금, 대출, 송금업 등)가 오프라인 점포 없이 온라인(웹, 모바일 등) 만을 이용하여 제공되는 은행을 말합니다. △'크라우드 펀딩' 분야의 핀테크 서비스는 온라인 매체(SNS, 웹 등)를 활용하여 불특정 다수로부터 빠르게 펀딩 자금(대출, 투자, 후원 등)을 조달하게 해주는 서비스입니다. △'로보 어드바이저'는 4차 산업혁명의 인공지능에 의한 자산관리 서비스를 제공하는 투자 플랫폼입니다. △'자산관리'는 소비자의 자산을 디지털화 하여 금융사와의 데이터 연계를 통한 서비스입니다. △'보안/인증'은 사용자단에서 비대면 핀테크에 대한 인증이 강화되고 있습니다.

분류	내용
간편송금/지급결제	▪ 웹이나 모바일 기기를 이용한 간편결제의 방식으로 QR코드나 애플리케이션으로 송금 및 결제서비스가 가능 ▪ 공인인증서를 이용하는 복잡한 인증 절차 없이 이체 비밀번호 또는 지문인식, 홍채인식, 얼굴인식과 같은 바이오 인증을 활용
인터넷 전문은행	▪ 모든 금융서비스를 인터넷 상에서 서비스 ▪ 지점을 운영하는데 소요되는 막대한 비용을 낮은 대출 금리나 저렴한 수수료 등으로 서비스 제공 (365일 24시간 운용)
크라우드 펀딩	▪ 창업기업이나 영화, 문화 등 콘텐츠 사업을 온라인상에서 중개업체를 통해 불특정 다수의 투자자로부터 사업자금을 투자 받는 방식 ▪ P2P(개인간 직거래) 금융 대출형, 신생기업이나 개발프로젝트에 투자하고 지분 획득을 하는 투자형, 금전적 보상과 상관없는 후원형, 기부형 등이 있음
로보 어드바이저	▪ 로봇에 의한 자산관리서비스를 제공하는 것으로 로봇 기반의 인공지능 투자 플랫폼 ▪ 4차 산업혁명에서 금융권 인공지능에 대한 재조명과 핀테크 발전에 따라 빅데이터 기술을 활용한 알고리즘 운영 전략의 성장을 통해 30~40대, IT 선호층을 대상으로 시장이 확대 되고 있음 ▪ 국내의 경우, 펀드 운용 허용, 펀드·일임 재산 운용 위탁 허용 등이 가능해져 산업의 활성화를 기대
자산관리	▪ 소비자 등의 자산관리를 디지털화하여 제공하는 핀테크 업체 활성화 ▪ 국내 자산관리 핀테크 서비스는 금융사와의 데이터 연동을 통해 금융상품 통합관리, 신용점수 관리, 데이터 기반 금융상품 추천, 금융 개인비서 등 폭넓은 자산관리 기능을 제공 ▪ 기존 오프라인에서 자산관리사나 재무설계사가 고소득자에게만 제공했던 개인자산관리 서비스를 대체
보안/인증	▪ 최근 핀테크 서비스와 비대면 거래가 증가하면서 핀테크 보안/인증 기술이 발전 ▪ 국내 핀테크 보안/인증 기술은 사용자 인증이 중심에 있으나 해외에서는 핀테크 사업자의 서버 보안에 더 신경을 쓰는 추세

[표Ⅳ-18. 핀테크 주요분야]

3) 핀테크의 특징

인터넷을 기반으로 한 스마트폰, 태블릿과 같은 모바일 사용이 확산되면서 금융 디지털 환경은 핀테크를 발전시키고 있습니다. 변화되고 있는 금융 핀테크의 특징을 살펴보면,

△결제단계, 입력정보, 인증방식의 간소화를 통해 사용자의 편의성을 추구합니다. 과거에는 이용과정의 불편보다는 안전성을 중시해 공인인증서, 일회용비밀번호, 각종 보안프로그램을 사용하고 거래 시 마다 결제정보 및 인증정보를 입력하도록 하여 사고를 예방해 왔습니다. 핀테크 서비스의 하나인 간편결제 방식은 카드정보 유출사고 발생 시 부정사용에 대한 보안위협 발생이 야기될 수 있습니다.

△금융·기술·서비스의 다양하고 복합적인 변화가 발생합니다. 핀테크를 통해 비금융회사가 금융업에 진출하여 소비자의 편익을 증가시킬 것으로 예상되지만, 금융IT와 비 금융IT, 온라인과 오프라인, 모바일기술 간의 복합이 일어나기 때문에, 접점을 증가시키고 새로운 취약점을 발생시키게 됩니다. 이는 기술적으로 대응수단을 복잡하게 할 뿐 아니라 현실에서 금융 서비스와 온라인 서비스(SNS, 포털 등)간에 결합이 발생될 때 전체적 보안수준이 높은 쪽에서 낮은 쪽으로 내려가는 현상 발생에 대한 우려가 발생하고 있습니다.

△거래과정에서 데이터 공유가 광범위하게 이루어지게 됩니다. 다양한 핀테크 서비스를 제공하기 위해서는 고객정보의 수집이 확대되고, 사업자간의 정보 공유도 증가할 것이므로, 고객 정보유출이나 프라이버시 침해 사고 가능성도 역시 증가할 것입니다. 오래 전부터 정보유출이 있었으나 최근 들어서 꾸준히 대량 정보유출 사태가 발생하고 있고 유출된 정보의 내용으로는 단순 개인정보에 대한 것과 신용카드 정보까지 다양합니다.

△정보보안 관련 규제가 완화됩니다. 핀테크 산업 성장 부진의 원인으로 법과 규정에 의한 사전규제가 지목되는 현 상황에서 산업의 활성화를 추진하는 정부 당국과 IT기업들의 요구에 따라 보안성 심의제도 등 정보보안 규제가 완화 또는 폐지되고 있습니다.

해당 연도	규제 완화 내용	비고
2014.5	▪ 공인인증서 사용 의무화 폐지	▪ 금융위원회
2014.7	▪ PG사 카드정보 저장 허용 등 전자상거래 결재 간편화 방안	▪ 관계부처 합동
2015.1	▪ 보안성심의 제도 폐지 등 IT·금융융합 지원방안	▪ 금융위원회
2015.4	▪ 실물카드 없는 모바일카드 단독 발급 허용	▪ 금융위원회
2015.5	▪ 계좌개설 시 비대면 실명확인 방식 허용	▪ 금융위원회
2015.6	▪ 인터넷 전문은행 도입방안	▪ 금융위원회
2016.6	▪ OTP, 보안카드의 사용의무 폐지	▪ 전자금융거래법 시행령
2018.3	▪ 공인인증서의 우월적 지위를 없애기 위한 법령 개정	▪ 전자서명법, 전자상거래법
2018.4	▪ 금융혁신지원특별법 시행	▪ 금융혁신지원특별법

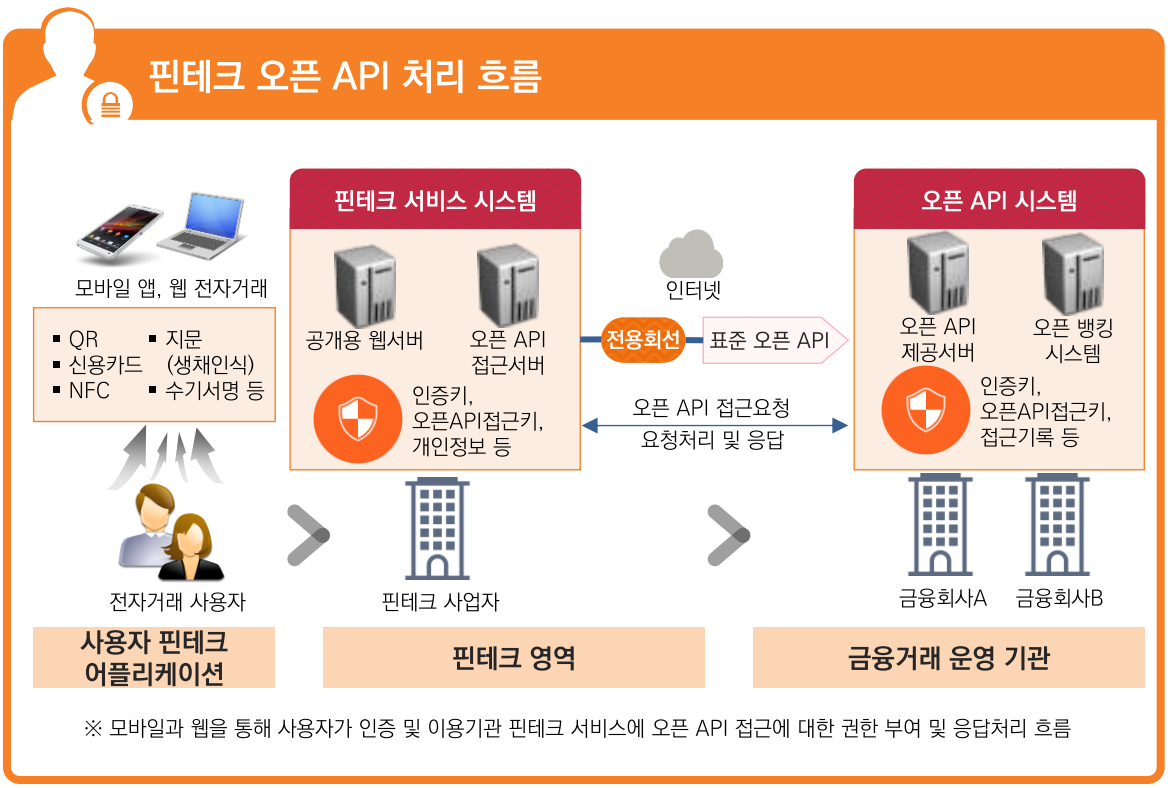
[표Ⅳ-19. 금융보안 규제 완화 사례]

4) 핀테크 서비스 흐름

금융보안원에서 공개한 『금융권 오픈API 이용기관 자체 보안점검 가이드』에서는 핀테크 기업이 금융회사의 오픈API를 이용하는 경우 참고할 수 있는 가이드를 제시하고 있습니다. 오픈API는 데이터나 서비스를 외부에서 쉽게 접근하여 활용할 수 있도록 제공하는 공개 응용 프로그램을 말합니다.

금융권 오픈API의 특성을 반영하여 오픈API 기술 도입 시 발생 가능한 위험을 사전에 이해하고, 이를 완화 또는 제거할 수 있도록 하는데 초점을 맞추고 있습니다. 오픈API 이용 구조에서 각 영역별(사용자, 이용기관, 운영기관) 발생 가능한 위험과 해당 위험에 대응하기 위한 보안대책 예시를 서술하고, 오픈API 운영기관과 이용기관이 각각 자체 보안점검 시 참고할 수 있는 점검항목 예시도 포함하고 있습니다.

금융사 대상 가이드라인은 '거래 당사자 인증', '거래정보의 기밀성 및 무결성' 등 8개 점검 분야와 '이용자 인증 방법의 적정성', '접근키 등 유출 위험 완화 대책', '이용기관 정보유출 방지대책' 등 36개 점검항목을 담고 있습니다. 핀테크 기업 대상 가이드라인은 '정보보호 정책·조직', '외부자 관리', '접근통제' 등 15개 점검분야와 '정보보호 정책 수립 및 공표', '설계 시 보안 요구사항 도출 및 반영', '중요 정보 암호화 정책 수립 및 이행' 등 38개 점검항목을 명시하고 있으며, 이를 통해 가져온 데이터를 어떻게 안전하고 다루고 보관해야 하는지에 대해 전달하고 있습니다.



[그림Ⅳ-16. 핀테크 오픈 API 처리 흐름]

5) 핀테크의 보안 이슈

가. 보안이슈 및 발생위협

핀테크 서비스의 보안이슈는 현재 금융 서비스에서 나타나는 보안위협과 또 다른 보안위협을 함께 가지고 있습니다. 핀테크 서비스에서 원클릭으로 계정이 탈취되는 크로스사이트 요청위조(Cross Site Request Forgery)[1] 취약점이 발견되었듯이, 서비스의 안전성 보다는 사용자의 편의성이 중시되는 핀테크 서비스는 해킹 등 위험성이 증가하고 있으며, 다양한 보안이슈가 발생되고 있습니다.

핀테크 보안 이슈	발생 위협
1 네트워크 ✓ 핀테크는 금융회사, PG사[2], IT회사, 창업기업 간의 제휴 또는 협력 필요 ✓ 다양한 매체와 메쉬(Mesh) 구조[3]의 복잡한 네트워크로 연결 ✓ 일부 영역에 보안위협에 노출되면 금융시스템 전체로 확산될 위험성 높음	✓ 서비스 거부공격(DOS) ✓ 세션 하이재킹 (Session hijacking)[4]
2 인증 ✓ 인증측면에서 기존 방식은 로컬의(Local) 카드정보, 단말 플랫폼 보안, 추가 인증수단을 사용하였으나 결제 편의를 위해 초기 인증이 단순화, 비설치화 하는 형태로 변화 ✓ 지문, 정맥을 이용하는 생체인증, IC카드 등을 이용하는 소지매체를 활용한 신규 인증기법이 활성화	✓ 개방형 모바일 플랫폼과 신규 인증기법의 취약점을 이용한 ID 도용 ✓ 추가인증 우회, 피싱 및 파밍 공격
3 서비스 ✓ 간편 결제를 위해 카드정보 저장 주체가 카드사에서 PG사, 쇼핑몰 확대 ✓ 메신저 기반 송금 서비스처럼 금융서비스와 기존 IT서비스와 결합 ✓ 기존 금융서비스가 온라인 대출 플랫폼과 같은 신규 IT 플랫폼화로 변화 ✓ 서비스 체인(Chain)상 보안이 가장 취약한 계약업체를 먼저 공격한 후 기업 간 신뢰관계를 악용하여 보안이 양호한 기업(예: 금융회사)을 공격하는 경우가 발생	✓ 외부채널을 시발점으로 내부채널로 연계하는 사회공학적 공격 ✓ IT업자 등 관리가 취약한 영역을 노리는 공격 ✓ 금융·IT 연계 취약성을 노린 공격
4 사물인터넷 확산 ✓ 금융서비스와 IT기술간 융합으로 시스템(Back-end) 중심에서 네트워크(Middle-end)를 거쳐 사용자(User-end)로 접속기기의 활용범위가 점차 확대 ✓ 핀테크를 통해 사물과 금융서비스의 접목이 더욱 확산 ✓ 사물인터넷(IoT)의 취약점을 악용한 보안위협 및 금융사고 확산	✓ 악성코드 공격 위협 ✓ 모바일 기기와 서비스 제공자의 PC보안 위협 확대 ✓ 원격제어 공격위협으로부터 접근통제 및 인증 강화 필요 ✓ 사용자 정보수집 정보주체의 사전 동의 확보 필요

1) Cross Site Request Forgery : 사이트가 신뢰하는 사용자를 통해 공격자가 원하는 명령을 사이트로 전송하는 공격 기법
2) PG사 (Payment Gateway) : 인터넷 상에서 금융 기관과 거래를 대행해 주는 서비스
신용 카드, 계좌 이체, 핸드폰 이용 결제, ARS 결제 등 다양한 소액 결제 서비스를 대신 제공해 주는 회사
3) 메쉬(Mesh) 구조 : 망(Network)구성 방식의 하나로 각 노드가 복잡하게 그물망 모형으로 연결된 구조
4) 세션 하이재킹 (Session hijacking) : 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화 상태를 가로채는 공격 기법

나. 핀테크 보안취약점

스마트폰과 함께 핀테크 산업이 발전함에 따라 디지털 금융서비스도 다양해지고 있습니다. 하지만 핀테크 산업 활성화를 위한 지속적인 규제 완화와 이용자 편의성을 위한 각종 절차의 간소화 등은 새로운 보안위협으로 대두되고 있으며 결과적으로는 서비스 안정성에 문제가 발생할 수 있습니다.

분류	보안취약점 발생 내역
이용자 편의성 중시	▪ 금융거래의 보안성 보다 이용자의 편의성 차원에서 서비스 간소화 추구 – 결제단계, 정보입력 및 인증방식 등 결제절차 간소화 – 오프라인 결제수단(종이통장, 신용카드, 쿠폰 등)을 스마트폰으로 일원화하는 휴대 편의성 추구 – 온·오프라인에서 동일한 결제수단의 사용 추구
채널, 서비스, 기술의 융·복합 발생	▪ 온라인과 오프라인 인프라가 상호 동작하는 신규 서비스 환경, 금융IT와 비 금융IT간의 결합 등에 따른 보안 취약점 발생 및 인증수준 악화 가능성 ※ 관련기술 : 비콘, NFC, 바코드, GPS 등 ▪ 융·복합 현상은 취약한 접점을 증가시켜 알려지지 않은 위협에 노출되고 사고 대응 수단을 복잡하게 함
개인정보의 수집, 이용 니즈 증대	▪ 핀테크 서비스를 제공하기 위해 고객의 개인정보 및 금융정보 수집·저장·이용에 대한 니즈 증가 – 모바일 기기 등에 저장된 정보 유출 가능성 – 빅데이터 분석을 통한 프라이버시 침해 가능성 증가 – 비금융회사의 금융정보 저장은 정보 유출 가능성 – 단말과 디바이스로부터 정보수집 시 사용자 등의 획득방법 제공 어려움
정보보안 규제 완화	▪ 핀테크 활성화, 소비자 편의 제고 및 금융비용 절감의 정책목표는 정보보안 강화 정책과 상충 가능성 ▪ IT기업은 금융업무 진입을 위해 정보보안 관련 규제 완화 요구 ▪ 금융 업무를 IT기업과 함께 수행할 경우 해킹, 사기, 정보 유출 등의 사고 발생시 금융회사와 IT기업간 책임 소개 및 소비자 보호 등과 관련 리스크 발생가능성

* 출처 : [한국인터넷정보학회 컬럼] 핀테크 보안의 걸림돌 4가지와 추진과제

[표Ⅳ-20. 핀테크 보안취약점]

6) 핀테크 보안기술

핀테크가 활성화됨에 따라 보안기술 또한 변화해 가고 있습니다. 핀테크의 보안취약점을 보완하기 위해 다양한 솔루션 및 시스템, 기술이 개발되고 있으며 핀테크의 주요 보안기술에 대해 소개합니다.

기술명	특징	적용예시	적용현황
TrustZone	▪ 핀테크를 이용한 전자금융거래 시 안전한 실행환경 보장을 위해 프로세서를 일반영역과 보안영역으로 분리/운영	▪ 스마트기기 전자금융서비스 이용 시 일반영역에 전자금융서비스 앱을 설치 후 보안 영역에 거래 시 사용되는 암호화 키 및 인증 값을 저장하여 중요정보를 보호할 수 있는 핀테크 서비스 제공	▪ 삼성, LG 스마트 폰 내 삼성페이 등에서 사용 중
FDS (이상금융 거래 탐지 시스템)	▪ 전자금융서비스 고객의 거래 내역을 실시간 분석하여 부정거래 여부를 판별하고 부정거래 탐지 시 대응하는 시스템	▪ FDS는 금융회사의 규모별, 데이터 처리 규모 별, 기존 시스템의 구성에 따라 관련 부서간 상호협의를 통해 자사에 적합한 형태로 구축 필요 ▪ 거래 내역의 부정거래 유무를 정확히 판별하기 위해 수집기능, 분석평가기능, 대응기능 등의 기능구현 필요	▪ 2017년 기준 국내 46개 은행/증권사 구축 및 운영 중
결제토큰	▪ POS 등을 이용한 카드정보유출로 인한 부정거래를 막기 위한 기술로 원본 신용카드정보 대신 임의 값으로 변환 처리된 가상 토큰 또는 카드를 결제에 사용하는 기술	▪ 일회성 방식과 고정형 방식으로 구분하여 서비스 함 ▪ 일회성의 경우 결제 유효시간 내 진행하는 방식으로 짧은 시간 설정 내 암호화, 해쉬 적용, 고정형의 경우 동일 토큰 카드번호로 지속 사용 가능하므로 토큰카드번호를 주기적으로 변경 필요	▪ 카드 사 앱 등 다양한 페이먼트에서 사용 중
바이오 인증 (FIDO)	▪ 지문, 홍채, 사인 등 본인을 증명할 수 있는 생체정보를 이용하여 인증하는 방법	▪ 바이오 인증 관련 솔루션 ▪ 전자금융거래 시 대부분 본인인증용도로 공인인증서 대신 활용	▪ 스마트뱅킹 ▪ 홍채ATM ▪ 디지털 키오스크
블록체인	▪ 블록에 거래데이터를 담아 중앙서버가 아닌 거래에 참여한 모든 사용자에게 해당 데이터를 복사하여 분산저장 ▪ 데이터의 위변조 방지 및 조작통제가 불가능하도록 서로간 데이터 교환을 감시	▪ 가상화폐거래소에서 블록체인 기반의 가상화폐를 거래 ▪ 금융권 내에서는 블록체인 간 상호호환성을 확대하는 방식으로 자산교환이 가능하도록 기술구현 중	▪ 가상화폐거래 ▪ 블록체인 기반 인증

* 출처 : [금융보안원]전자금융과 금융보안 정기간행물

[표Ⅳ-21. 핀테크 보안기술]

7) 핀테크 정보보안 대응방안

가. 사용자 인증 (FIDO[1])

핀테크와 IoT 서비스 환경은 보안상 취약한 접점이 증가하여 고객이 실수로 악성코드를 받게 될 가능성과 원격접속을 통해 공격을 받을 위험성도 더욱 커지고 있습니다. 이러한 상황에서 본인 확인을 위한 인증 강화가 해킹사고 예방 측면에서 중요합니다. 서비스 관점에서 사용자와의 첫 번째 접점인 사용자 인증 기술은 서비스의 성공 여부에 커다란 영향을 미치는 요소가 됩니다.

최근 보안에 취약한 문자 패스워드를 대체하기 위해 핀테크 서비스의 핵심 보안기술인 FIDO가 만들어 지면서 최근 금융·결제분야에서 중요한 기술로 활용되고 있습니다. FIDO 표준의 원격 인증은 안전이 입증된 공개키 암호에 기반합니다. 이 기술은 개인의 고유특성을 사용자가 소지한 기기에서만 확인하고 이용해 프라이버시 위험 없이 안전하고 편리하게 인증할 수 있는 표준화된 플랫폼을 제공하기 때문에 단기적으로는 스마트폰에 탑재된 생체인식 기술을 중심으로 확대 적용될 것으로 예상됩니다.

인증강화를 위한 신 인증기술은 보안성을 높이면서도 편의성이 우수한 방식(생체인증, H/W방식 등)을 선택해야 합니다. 또한, 사고가 발생하더라도 해당 기관으로만 피해가 한정되어야 하며, 금융회사의 인증수단이 아닌, 이용자가 원하는 인증수단을 선택할 수 있는 구조를 갖추어야 합니다. 추가적으로 다양한 전자금융환경에 적용할 수 있도록 특정기술을 이용하지 않아야 하며, 피싱, 파밍을 이용한 지능형 사기, 메모리 공격 방어 기술(스마트OTP, NFC인증 등), 사용자 고유정보(생체, 행위, 환경 등)를 이용한 상황인지 기반 인증, 부인방지 전자서명 기술들이 제공되어야 합니다. 마지막으로 웨어러블 기기를 포함한 사물인터넷이 확산되는 상황에서, 개인정보 보호를 위한 각종 동의 및 고지 절차를 효율적으로 처리할 수 있는 기술이어야 합니다.

[그림Ⅳ-17. FIDO 인증]

1) FIDO (Fast IDentity Online) : 온라인 환경에서 ID,비밀번호 없이 생체인식 기술을 활용하여 보다 편리하고 안전하게 개인 인증을 수행하는 기술

나. 단말 보안

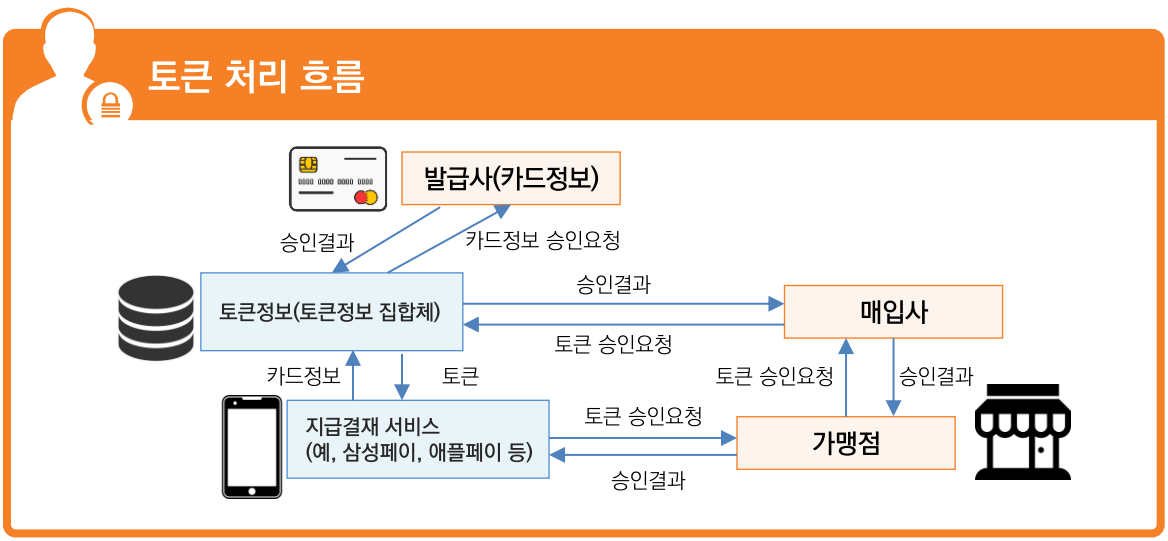
핀테크를 위한 보안 중 모바일 단말 보안은 주로 악성코드 등에 의한 앱의 위·변조방지와 악성 앱 설치 차단이 중요한 대응책이었으나, 소프트웨어 방식으로 한계가 발생하였습니다. 스마트폰에 대한 공격이 소프트웨어 취약점을 악용하기 때문에 하드웨어 중심의 해킹 차단 원리인 신뢰된 실행환경(TEE: Trusted Execution Environments) 기술의 적용을 고려해 볼 필요가 있습니다.

이 방식은 스마트폰의 AP(Application Processor)를 일반영역과 보안영역으로 논리적으로 분리하는 기술이며, 보안영역이 활성화 되면 모든 일반영역의 활동은 홀딩되어 보안영역으로 접근이 불가능하게 됩니다. 또한 각 영역은 별도의 OS가 구동되고 보안영역이 항상 먼저 부팅되어 일반영역으로부터 격리되는 특징을 가집니다. 스마트폰에서 입출력되는 화면과 좌표값을 보호할 수 있기 때문에 안전한 모바일 금융거래 환경 구현이라는 목표에 부합되는 기술입니다.

다. 결재정보 보안

핀테크 서비스의 발전으로 금융사, 통신사, PG사, 플랫폼사, 스마트폰 제조사 등 여러 사업자들이 융·복합되면서 보안의 안전성과 개방성이 가능한 기술로 토큰화(Tokenization) 기술이 활성화 되고 있습니다. 토큰이란 실제 카드 하나에 등록되는 온라인 결제 서비스와 오프라인 모바일 지갑별로 서로 다른 가상의 카드가 생성되는 것입니다. 사용자가 카드를 등록할 때 마다 카드사에서 생성된 이 토큰(가상카드 번호)이 온라인 결제서비스 또는 오프라인 모바일 지갑 사업자에게 전달되어 사용자의 아이디 등 식별정보에 매핑되어 저장이 됩니다. 이후 결제 시 토큰이 카드사에 전달되어 연결되어 있는 실제 카드로 승인이 처리되게 되는 방식입니다

상위 금융 감독기관의 강화되는 컴플라이언스와 빅데이터 환경에서의 보안대응을 위해 결제 데이터를 토큰(Token)으로 치환하여 원본데이터 대신 토큰을 사용하는 기술인 토큰화 기술이 하나의 중요한 보안 대응 방안 입니다.



[그림Ⅳ-18. 토큰 처리 흐름]

라. API 보안

IT시스템의 연결을 위해 최근 API(Application Program Interface)를 통한 서비스가 다양하게 활성화되고 있으며, 외부 서비스와 내부 시스템을 연동시키면서 API가 차세대 해킹 공격의 통로가 될 수 있다는 경고가 나오고 있습니다.

API는 소프트웨어 간에 상호작용 및 데이터 교환이 가능하게 하는 인터페이스이며, 비즈니스 관점에서 내부 자산을 외부에 공개해 새로운 서비스를 개발하고, 사업 기회를 찾을 수 있도록 하는 방법으로 널리 활용되고 있습니다. 특히, 핀테크 시대를 맞아 금융인프라 개방을 통한 상생의 핀테크 생태계 조성의 일환으로 핀테크 기업 등이 제공하고자 하는 서비스와 연관된 금융회사 시스템 또는 정보에 접근할 수 있도록 하는 통로의 개념으로 부상하고 있습니다.

스냅챗(Snapchat)의 해킹사례에서 보듯이 방대한 양의 트래픽을 집중시켜 웹서비스를 중단시키는 디도스(DDoS) 공격은 API를 통해 서비스되는 애플리케이션 환경에서도 똑같이 발생할 수 있는 보안상 위험성을 가지고 있습니다.

많은 핀테크 기업과 다양한 핀테크 서비스가 오픈 API를 활용할 경우 각종 보안사고가 발생할 수 있으므로, 검증된 소프트웨어의 사용을 통해 보안성을 확보하고 권한 있는 사용자가 편리하게 사용할 수 있도록 해야 할 것입니다.

마. 이상거래 탐지

핀테크, IoT 등이 확산되면 기존 보안시스템은 더욱 한계를 갖게 될 것이므로 지금까지 금융서비스를 보호하기 위한 대부분의 보안 S/W와 인증 기술들이 사용자 구간에 집중된 사실상 단일 계층 보안체계를 다계층 방어로 전환해야 합니다. 사용자단의 보안 절차가 간소화되고 사용자의 PC나 모바일 단말기에 설치되어야 할 모듈들이 줄어들거나 없게 되는 핀테크 서비스에서 유출된 개인정보 등을 이용한 인증 후에 발생하는 위협과 악성코드 등에 의한 인증절차를 우회한 부정 거래 시도를 차단하는 것이 중요합니다.

FDS의 실효성을 높이기 위해서는 무엇보다도 구축도 중요하지만, 운영의 문제로 접근해야 합니다. 사용자 정보, 거래정보 등을 모니터링, 분석하여 서버단에서 이상거래를 탐지·차단하는 시스템(FDS) 구축 및 고도화가 필요합니다. 또한, FDS를 우회하거나 복제 단말 사용, 사용자 단말기 권한 탈취 등 FDS가 탐지하기 어려운 새로운 위협에 어떻게 대응할 것인가도 고민해야 합니다.

이상거래를 탐지하는 FDS는 고객 거래에 직접적 영향을 미칩니다. 탐지 제품은 오탐을 하기 마련이고, 침입탐지시스템(Intrusion Detection System)의 경우 오탐이 나더라도 IT와 보안전문가의 영역에 머물고 있으나 FDS 오탐으로 인해 고객의 정상적인 송금 요청이 거절된다면 고객은 매우 불편해 할 것입니다. 그런 점에서 현장과의 커뮤니케이션이 중요하고 이상거래를 탐지·분석하고 차단하는 과정에서 수반될 수 있는 거래지연 현상에 대해 업무 약관 등 제도적 측면에서 보완도 필요합니다.

바. 사고대응

보안 사고를 100% 막을 수 있는 보안기술은 없으며, 특히 핀테크 시대에는 어떤 기술 및 공격이 등장할지 정확히 알 수 없으나 침해는 어떤 형태로든 발생할 수 있습니다. 침해사고로부터 위협을 탐지하고 대응하는 스피드가 보안 수준을 결정하게 되며, 기업은 사고가 발생했을 때 피해를 최소화하고, 원인을 명확히 파악해서 기업의 운영업무의 정상상태를 유지하는데 목적이 있습니다. 침해를 적절하게 제어하기 위한 관련 시스템 간 상호 연관성에 대한 충분한 이해와 정립된 정책 및 프로세스를 포함하는 비즈니스 연속성 대책(BCP: Business Continuity Plan)을 갖추어야 하고, 사고 발생 시 긴급 조치와 사고원인을 분석하여 재발방지 대책 등을 수립하는 상시적 조직이 필요합니다.

공격수법의 고도화, 지능화로 인하여 전자금융사기를 원천적으로 차단하는 것은 더욱 어려워 질 전망입니다. 특히 사용자 편의성을 중시하는 간편 결제 및 송금 서비스에서는 전자금융사기 발생 가능성이 더욱 높아질 것이며, 금융 소비자 보호와 기업의 위험 분산을 위해 전자금융사고에 대한 보험 관련 대책을 강화하고 보상체계 등을 포함한 분쟁조정 방안 마련 역시 중요할 것입니다.

✓ 핀테크 보안점검 항목정의 핀테크 서비스 보안취약점 점검항목(핀테크 기업)

금융보안원은 핀테크 서비스를 제공하는 회사가 중요정보 보호를 위한 보안관리체계를 마련하고 있는지 보안점검을 수행하고 있습니다.해당항목은 전체 3개 영역, 14개 분야, 30개 점검항목으로 구성되어 있습니다.

보안영역	점검분야	점검항목
관리	▪ 정보보호 정책·조직	▪ (정보보호최고책임자 지정 및 실무조직 구성) 정보보호최고책임자를 지정하고 실무조직을 구성하고 있는지와, 동조직이 정보보안 점검항목을 마련하여 정기적으로 점검을 수행하고 있는지 점검
		▪ (정보보호정책 수립 및 공표) 정보보호정책 및 정책시행 문서를 수립하여 문서화하고, 이를 임직원에게 공표하고 있는지 점검
	▪ 외부자 관리	▪ (위탁업체 선정 및 관리) 위탁업체 선정 시 보안 요구사항을 정의하여 계약서에 반영하고 있는지 점검
	▪ 정보자산 관리	▪ (정보자산 식별) 오픈API 관련 정보자산을 식별하여 목록을 관리하고 있는지 점검
	▪ 정보보호 교육	▪ (실무자 정보보호 교육 이수) IT직무자(개발, 운영) 및 정보보호 직무자는 직무 수행에 필요한 정보보호 교육을 이수하고 있는지 점검
	▪ 인적 보안	▪ (비밀유지서약서) 내외부 직원 대상으로 비밀유지서약서를 받고 있는지 점검
		▪ (퇴직 및 직무변경 관리) 내외부 직원의 퇴직 및 직무 변경 시 권한 관리를 적절히 수행하고 있는지 점검
	▪ 위험 관리	▪ (취약점 점검 정책 수립 및 점검 수행) 중요 정보자산에 대해 취약점 점검 정책을 수립하고, 취약점 점검을 수행하고 있는지 점검
	▪ 침해사고 대응	▪ (침해사고 대응절차 마련 및 임직원 대상 공표) 침해사고 대응절차를 마련하고 임직원 대상으로 공표하고 있는지 점검
		▪ (침해사고 대응 관련 로그 보존 및 모니터링) 침해사고 대응에 필요한 로그를 일정기간 보전하고 주기적으로 검토하고 있는지 점검
	▪ 이용자 보호	▪ (개인정보 처리 관련 이용자 보호) 개인정보 처리방침을 이용자가 확인하기 쉽게 공개하고 이용자로부터 개인정보 처리 동의를 받고 있는지 점검
		▪ (개인·신용정보 접근 및 거래지시 권한 관련 안내) 오픈API를 통한 개인·신용정보 접근 및 전자금융거래지시 가능 사실에 대해 이용자에게 안내하고 있는지 점검
		▪ (이용자 고충 처리방침 마련 및 공개) 이용자 문의에 대응하는 처리방침을 마련하고 이용자가 확인하기 쉽게 공개하고 있는지 점검
물리	▪ 물리적 보안	▪ (보호구역 지정 및 출입 통제) 중요 시스템이 운영되는 장소에 대해 보호구역을 별도로 지정하고 출입을 통제하고 있는지 점검
		▪ (보호구역 반출입 관리) 휴대장치의 통제구역 반출입을 통제하고, 중요 단말기 및 휴대장치 등의 사무실 반출입을 통제하고 있는지 점검

보안영역	점검분야	점검항목
기술	▪ 개발 보안	▪ (설계 시 보안 요구사항 도출 및 반영) 신규개발 및 변경 시 보안 요구사항을 도출하고 이에 대한 대책을 설계에 반영하고 있는지 점검
		▪ (테스트 시 이용자 개인·신용정보 사용 제한) 개발 및 테스트 시 서비스 이용자의 개인·신용정보를 사용하지 않고 있는지 점검
	▪ 암호 통제	▪ (중요 정보 암호화 정책 수립 및 이행) 오픈 API 관련 중요정보 보호를 위해 암호화 정책을 수립 및 이행하고 있는지 점검
	▪ 접근 통제	▪ (중요 정보자산 계정 및 접근 권한 관리) 오픈 API 관련 정보처리시스템 및 관리자 권한 프로그램에 대해 접근 권한을 안전하게 통제하고 있는지 점검
		▪ (중요 단말기 지정 및 접근 통제) 오픈API 이용서비스 관련 중요 단말기를 지정하고, 접근을 통제하고 있는지 점검
	▪ 시스템 보안	▪ (주요 시스템 등의 악성코드 감염 및 정보유출 방지) 오픈API 관련 정보처리시스템의 악성코드 감염 및 정보유출 방지 대책을 마련하고 있는지 점검
		▪ 인터넷망을 통한 원격관리 통제) 오픈API관련 정보처리시스템에 대해 인터넷망을 통한 원격관리를 통제하고 있는지 점검
		▪ (주요 시스템 목적 외 기능·프로그램·포트 등을 제거하고 있는지 점검
		▪ (중요서버 독립 운영 및 정보보호시스템 적용) 오픈API 관련 서버는 독립서버로 운영하고, 정보보호시스템을 적용하여 보호하고 있는지 점검
		▪ (공개용 웹서버 보호대책 마련) 공개용 웹서버에 대한 보호대책을 마련하여 적용하고 있는지 점검
		▪ (중요 보안패치 적용 지침 수립 및 이행) 회사에 적합한 보안패치 적용 지침을 수립하고, 주기적으로 검토 및 적용하고 있는지 점검
	▪ 네트워크 보안	▪ (DMZ 구간 구성) DMZ 구간을 구성하여 내부 네트워크를 보호하고 있는지 점검
		▪ (내부망 사설IP 활용 및 주요 시스템 배치) 내부망은 사설IP 주소를 활용하고 업무영역에 따라 핵심 시스템은 내부망에 배치하고 있는지 점검
		▪ (무선 네트워크 이용 최소화 및 보안대책 수립·적용) 무선 네트워크는 통제 하에 이용을 최소화하며, 책임자 승인 하여 이용 시 보호 대책을 적용하고 있는지 점검
		▪ (대외기관과 통신 시 보안통신 적용) 대외기관과 통신 시 보안통신이 적용되어 있는지 점검

* 출처 : [금융보안원] 핀테크 기업 보안점검 안내 (2020.3)

[표Ⅳ-22. 핀테크 서비스 보안취약점 점검항목(핀테크 기업)]

✓ 핀테크 보안점검 항목정의 핀테크 서비스 보안취약점 점검항목(웹·앱)

금융보안원에서 개발한 핀테크 서비스에서 발생할 수 있는 보안취약점 점검항목을 소개합니다. 웹과 앱에 해당하는 점검항목은 평가 전문기관이나 이용기관 자체 전담반을 통해서 서비스 하고 있습니다.

플랫폼	점검분야	점검항목
웹	▪ 중요정보 보호	▪ (DOM 영역 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 DOM 영역 내 평문 노출 여부를 점검
앱	▪ 중요정보 보호	▪ (디버그 로그 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 디버그 로그 내 평문 노출 여부를 점검
	▪ 클라이언트 보안	▪ (앱 위·변조 탐지 적용 수준) 점검대상 앱의 중요파일에 대한 위·변조 수행 후 서비스 정상 실행 가능여부를 점검
		▪ (해킹OS 탐지 적용 수준) 루팅/탈옥된 단말에서 점검대상 앱 실행 시 정상 실행 가능 여부를 점검
		▪ (안티디버깅 적용 수준) 디버거를 이용한 동적 디버깅 시도 시 정상 실행 가능 여부를 점검
		▪ (코드 난독화 적용 수준) 점검대상 앱의 디컴파일 가능 여부 및 복구된 소스코드의 난독화 적용 여부를 점검
		▪ (안티바이러스 적용 수준) 점검대상 앱 실행 시 악성코드 방지 대책을 점검
공통	▪ 중요정보 보호	▪ (메모리 내 노출 방지 수준) 기밀성이 요구되는 이용자 중요정보의 메모리 내 평문 노출 여부를 점검
		▪ (네트워크 구간 내 노출 방지 수준) 기밀성이 요구되는 중요정보의 네트워크 구간 내 평문 노출 여부 및 네트워크 보안 설정 등을 점검
		▪ (중요정보 파일 저장 수준) 기밀성이 요구되는 중요정보의 이용자구간 내 파일 저장 여부를 점검
		▪ (중요정보 화면 표시 및 보호 수준) 기밀성이 요구되는 중요정보의 화면 표시 및 화면 캡처를 통한 탈취 가능 여부를 점검
		▪ (입력정보 보호 적용 수준) 이용자 입력 중요정보의 노출 방지를 위해 구현된 보호기능 적용 여부를 점검
	▪ 거래정보 위·변조	▪ (계좌번호 변조 방지 수준) 전자금융거래 이용 중 무결성이 요구되는 계좌정보를 메모리 및 네트워크 구간에서 위·변조 시 부정이체 가능 여부를 점검
		▪ (금액변조 방지 수준) 전자금융거래 이용 중 무결성이 요구되는 금액정보를 메모리 및 네트워크 구간에서 구간에서 위·변조 시 부정이체 가능 여부를 점검
		▪ (거래정보 재사용 방지 수준) 전자금융거래에 이용되는 거래정보의 재사용 가능 여부를 점검
	▪ 서버 보안	▪ (서버 보안 적용 수준) 잘 알려진 웹서비스 취약점에 대한 보안대책 적용 등 서버 보안대책 적용 여부를 점검
	▪ 인증	▪ (멀티 로그인 탐지 적용 수준) 서로 다른 단말에서 동일 계정으로 로그인 시 탐지 및 대응 여부를 점검
		▪ (인증 우회 방지 수준) 이용자 인증 및 세션 관리와 관련된 기능 구현의 적정성을 점검

* 출처 : [금융보안원] 오픈뱅킹 관련 보안점검 주요내용 (2019.6)

[표Ⅳ-23. 핀테크 서비스 보안취약점 점검항목(웹·앱)]

부록

이상징후 탐지모델

외부 침해위협과 내부정보 유출위협의 대응은 이벤트 탐지기술을 기반으로 대응 조치를 수행합니다. 위협 이벤트를 탐지하는 로그분석 방법으로 탐지 모델이 있습니다. 이 모델은 특정한 기준 데이터를 기반으로 탐지하는 방식에서 시나리오 기준 탐지 방식과, 사용자의 행동기반 분석을 통한 탐지, 그리고, 머신러닝 기반의 데이터 군집분석, 시계열 분석, 행위예측 분석을 통한 탐지 방법으로 발전하고 있습니다.

향후 탐지방식 (내부유출 외부침해 통합관제)

A.I.기반 머신러닝

군집분석, 시계열 분석, 행동분석 탐지 기술적용

예시) 특정기간 평균 대비 매체 사용량 임의 배수 증가
특정기간과 임의 배수는 기존 로그분석 학습을 통해 자동정의

통계 및 행위기반

영역별, 시간별 각종 통계를 기반으로 이상징후 발생 탐지 기술

예시) 사용자 계정에서 DRM 암호화 해제, 매체제어 위반이 과다 발생에 따른 퇴직 징후자 도출

위협 인텔리전스

외부 위협정보 서비스를 통해 IP, 도메인, URL, 해시정보 탐지

예시) SK인포섹T.I서비스, 금융ISAC, KISA C-TAS 정보 연계

기존 탐지방식 (외부침해 위주)

이벤트 연관

다단계 공격 등 이기종 이벤트 상관 관계를 실시간으로 탐지

예시) 취약 서버 익스플로잇 탐지 후 아웃바운드 C&C 서버 접속 시도

패턴 매칭

IP및 문자열 패턴매치 방식 으로 단순 조건 탐지 수행

예시) 특정 IP와 URL을 외부 유입되는 Web서버에서 탐지 시 경보
DMZ 서버에 OpenSSH Heartbleed[1] 공격 탐지 시 경보 등

1) OpenSSH Heartbleed : 인터넷에서 각종 정보를 암호화하는 데 쓰이는 오픈소스 암호화 라이브러리인 오픈SSL(OpenSSL)에서 발견된 심각한 보안 결함

부록 "위협분석 및 모니터링 방법론" 내부위협 분류 체계

SK인포섹에서는 내부 및 외부위협 모니터링 방법론으로 고객사의 시스템 구축 시 시나리오 컨설팅 업무를 수행합니다. 그 중 내부정보 위협에 관련된 분류를 다음과 같이 체계화하여 정의 하였습니다.

분류 / 영역	대분류	중분류
보안통제 위반	계정/권한 통제 위반	비인가 계정사용
		허가되지 않은 사용자 계정 생성
		불필요한 계정 존재
		추측 가능한 관리자/특수권한 사용
		로그인 연속 실패
		영업/업무시간 외 접속
		비인가 접속
		계정 공유
	단말보안 통제 위반	PC 시스템 정보 임의 변경
		비인가 소프트웨어 사용
		비인가 저장매체 사용
		보안프로그램 강제 종료/삭제
		보안패치 미적용
		단말기 전원 미 OFF
		Mobile OS 위변조
		부적절한 예외정책
	서버보안 통제 위반	불필요한 서비스 사용
		비인가 파일 접근
		파일 위변조 시도
		금지 명령어 사용
	DB보안 통제 보안	DMZ 구간 내 DB설치
		금지 명령어 사용
	네트워크 보안 통제 위반	비인가 사이트 접속
		인터넷 차단 우회
		비인가 AP 설치

부록 "위협분석 및 모니터링 방법론" 내부위협 분류 체계(계속)

영역 \ 분류	대분류	중분류
오·남용	과다 조회	임직원별 과다조회
		영업점별 과다조회
		퇴직(예정/징후자) 과다조회
		타관리점 고객정보 과다조회
		DB과다 조회
		특정 고객정보 집중 조회
		영업/업무시간 외 조회
		정상화면 이용패턴 이탈
	목적 외 조회	동료직원 정보 조회
		본인 or 가족정보 조회
		업무처리 미수반 고객정보 조회
		분리보관 고객정보 조회
	과다 보유	개인정보파일 과다 보유
		PC문서 과다 보유
		비인가자 개인정보 파일 보유
	암호화 해제	암호화 과다 해제
		암호화 해제 자가 승인
정보유출	과다 반출	외부 반출 과다 신청
		보안 USB 과다 사용
		보안 USB 자가 승인
		비인가자 반출
	과다 출력	문서 과다 출력
		문서 출력 자가승인
		비인가 출력
	과다 전송	외부메일 과다 전송
		외부메일 자가승인
		비인가 외부메일 전송
		비인가 망연계 외부망 전송
	이상징후/시도	정보유출 이상징후
물리적 통제 위반	출입통제 위반	비인가자 출입

[표 부록-1. 내부위협 분류체계]

보안SI를 통한 IT정보보호 구축 가이드

TABLE & PICTURE

표

Connect everything, Secure everything

보안, 그 이상의 믿음

보안SI를 통한 IT정보보호 구축 가이드

TABLE & PICTURE

SK infosec

표

Connect everything, Secure everything

보안, 그 이상의 믿음

보안SI를 통한 IT정보보호 구축 가이드

TABLE & PICTURE

그림

보안SI를 통한 IT정보보호 구축 가이드

TABLE & PICTURE

그림

Connect everything, Secure everything

보안, 그 이상의 믿음

보안SI를 통한 IT정보보호 구축 가이드

TABLE & PICTURE

그림

마무리 하며…

2020년은 무엇보다도 코로나 팬더믹이 사회적으로 많은 이슈가 발생한 해였으며, 회사 내부의 보안사업도 많은 영향을 미친 것도 사실입니다. 그로 인해, 이번 버전에서는 특히 의료정보 보안, 제조업 보안 등에서 보안역할과 필요성에 대해 Compliance와 구축 부분으로 작성하였습니다. 해당 분야 업체에서 조금이나마 정보보안 역할에 도움이 되길 기대합니다.

2000년 정보보안을 위해 설립된 SK인포섹은 정보보안 국내 1위를 넘어 Global Leading Digital Security Company로 성장하고 있습니다. SK인포섹은 정보보안, 물리보안 영역을 융합하는 서비스를 지원하며, 컨설팅, SI, 관제 등 보안의 시작부터 구축, 운영까지 고객과 함께하고 있습니다.

『보안SI사업팀』의 보안 아키텍처 기반 설계와, 구축 수행을 통해 얻어진 역량과 기술력, 노하우를 고객과 함께 공유하고자 가이드를 발간하였습니다. IT정보보호 구축 가이드는 업체나 솔루션의 홍보나 사업을 위한 자료가 아니라, 대외 모든 구독자의 정보보안의 이해를 도모하고자 제작 발간하고 있습니다. 고객사에서는 보안 시스템 통합 구축을 계획하는데 조금이나마 도움이 되길 바랍니다.

2019년 3월에 초판으로 '제1,2편'을 발간하였고, '제1,2편' 보완과 '제3편'의 솔루션 편을 추가하여 통합본을 발간 했으며, 2021년 1월에는 이전버전의 현행화와 내용정비 및 부분적인 보안영역을 추가하고, '제4편' 기업유형별 보안편으로 금융 핀테크, 제조업의 스마트팩토리 보안, 의료정보보안 부분을 추가적으로 발간하였습니다. 본 문서의 버전은 V3.0이며, 주기적으로 추가보완 관리하여 SK인포섹 홈페이지를 통해 공유할 예정입니다.

마지막으로, SK인포섹 사내 관련 부서(EQST담당, OT/ICS사업팀)의 협조에 감사 드립니다.

감사합니다.

Global Leading Digital Security Company

■ 제 작 사 : SK인포섹(주) (www.skinfosec.com)
13486 경기도 성남시 분당구 판교로 227번길 23, 4&5층
Tel) 02-6361-9114 Fax) 02-6361-9999

■ 담 당 팀 : Enterprise사업그룹 〉〉 보안SI사업팀

■ 제 작 일 : 2021년 01월 04일

■ 버　　전 : V3.0