Special Report

제로트러스트 보안전략 : 식별자·신원(Identity)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

■ 식별자·신원(Identity) 필러 개요

식별자·신원(Identity) 필러는 제로트러스트 아키텍처의 핵심 요소 중 하나로 사용자, 서비스, IoT 기기 등 모든 엔터티를 고유하게 식별하고 보호하는 역할을 담당한다. 제로트러스트 원칙에 따라 모든 사용자는 신뢰할 수 없는 대상으로 간주되며, 네트워크와 시스템 등에 접근하기 전에 반드시 검증을 거쳐야 한다. 이는 단순히 초기 인증 단계에서의 검증에 그치지 않고, 지속적인 모니터링과 동적 정책 적용을 통해 사용자의 신뢰도를 평가하고 권한을 부여하거나 제한하는 방식으로 운영된다.

식별자·신원 필러는 조직 내 모든 엔터티를 명확히 식별하고, 이를 기반으로 보안 정책을 일관되게 적용할 수 있도록 한다. 사용자와 기기의 신원을 확인하는 과정은 단순한 인증 절차를 넘어, 지속적인 검증과 위험 평가를 포함한다. 이를 통해 조직은 내부 및 외부 위협으로부터 민감한 자산을 보호하고, 보안 사고를 사전에 예방할 수 있다.

제로트러스트 환경에서 식별자·신원 필러는 보안의 출발점이자 중심축으로 작용하며, 신원 관리와 접근 통제를 통해 보안 태세를 강화한다. 특히 사용자의 역할(Role), 부서, 직급 등의 속성을 기반으로 권한을 부여하거나 제한하는 정책은 최소 권한 원칙을 실현하는 데 중요한 역할을 한다. 이러한 정책은 조직 내 모든 시스템과 데이터에 대해 일관된 접근 제어를 가능하게 하며, 보안의 효율성과 신뢰성을 높인다.

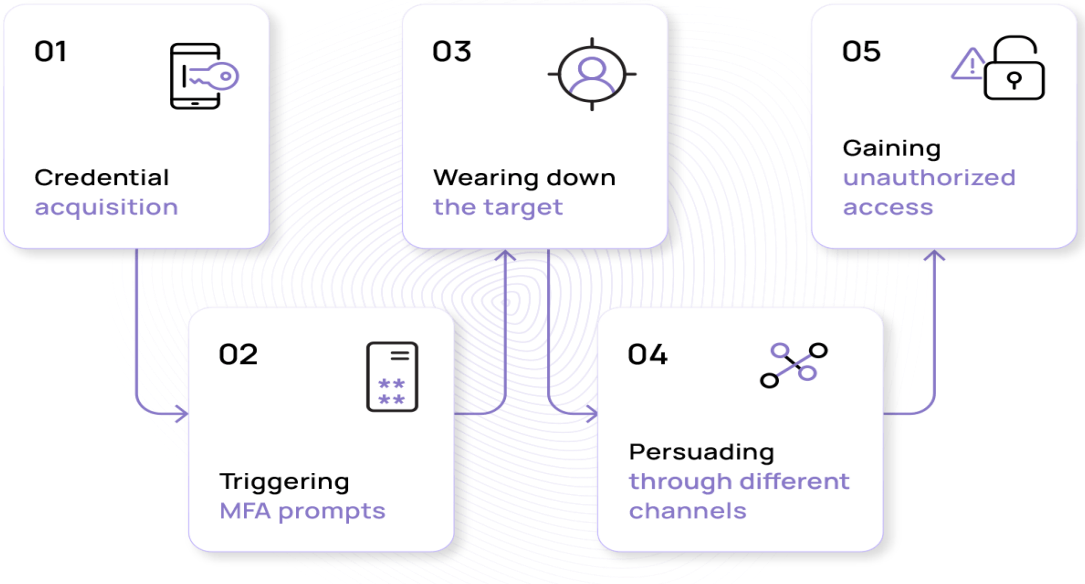
출처 : SK 쉴더스 EQST, "2025 보안 위협 전망 보고서"

그림 1. 2024 보안 이슈 Review

최근 글로벌 위협 보고서에 따르면, 아이덴티티(Identity)를 이용한 공격이 급격히 증가하는 등 공격자들의 주요 표적이 되고 있다. 특히, 크리덴셜 스터핑(Credential Stuffing)은 가장 널리 사용되는 공격 방식 중 하나로, 공격 트래픽의 상당 부분을 차지하고 있다. 크리덴셜 스터핑은 이전 데이터 유출에서 얻은 계정 정보를 자동화된 도구를 통해 여러 플랫폼에서 테스트하여 불법적으로 접근하는 방식으로 이루어진다. 다크웹에서는 이러한 계정 정보가 거래되고 있으며, 이는 공격자들이 초기 침투를 시도하는 데 주요 수단으로 활용된다.

SpyCloud 의 "2025 Identity Exposure Report"에 따르면, 2024 년 한 해 동안 533 억 개의 신원 데이터가 유출된 것으로 나타났다. 이는 전년 대비 22% 증가한 수치다. 이러한 데이터는 크리덴셜 스터핑과 같은 공격에 사용되어 기업과 개인 모두에게 심각한 위협을 초래하고 있다.

제로트러스트 아키텍처의 인증 강화 방안인 다단계 인증(MFA)은 오랫동안 아이덴티티(Identity) 보호를 위한 보안의 표준으로 여겨져 왔지만, 최근에는 이를 우회하려는 다양한 공격 기법들이 등장하면서 다단계 인증만으로는 아이덴티티(Identity)의 보안성을 보장할 수 없게 되었다. 잘못된 MFA 정보를 계속 보내는 MFA 피로공격, 리버스 프록시 아키텍처를 이용한 피싱도구, 중간자 (A.ItM) 피싱, MFA 정보를 보관하는 중간지점 공격 등 다양한 공격이 사용되고 있다.



출처 : Sosafe, "MFA Fatigue Attack"

그림 2. MFA 피로공격 절차

현 시점에서 가장 안전한 인증 방식으로 알려진 생체인증 또한 우회가 불가능한 것은 아니다. 가트너는 딥페이크 공격이 빈번해지면서 2026 년 기업의 30%가 생체 인증을 신뢰할 수 없을 것으로 예상했다. 가트너는 "2024 년 예측: A.I 및 사이버 보안" 보고서에서 신원확인 공급업체의 비공식 탐지 결과를 언급하면서 사기성 신원 인증 시도 중 15%가 딥페이크와 관련 있으며, 탐지되지 않은 것의 비중은 얼마나 될지 알 수 없다고 설명했다.

결론적으로 아이덴티티 기반 공격이 증가하는 상황에서 단순히 기존의 보안 기술에 의존하는 것은 더 이상 충분하지 않다. MFA 와 생체 인증은 여전히 강력한 보호 수단이지만, 이를 우회하려는 공격 기법 또한 정교해지고 있다. 따라서 제로트러스트 원칙을 기반으로 한 지속적인 모니터링과 동적 정책 적용이 필수적이다. 제로트러스트 원칙 중 "지속적인 검증"과 "최소 권한" 원칙을 통해 인증을 일회성으로 끝내는 것이 아닌 사용자의 행동 패턴, 접속 환경, 디바이스 상태 등을 지속적으로 평가하여 추가검증을 해야 한다. 예를 들어, 사용자가 평소와 다른 지역에서 접속하거나 비정상적인 활동을 수행할 경우, 추가 인증 절차를 요구하거나 접근 권한을 제한하는 것이다. 또한 MFA 및 생체 인증을 통한 사용자의 신원 확인 후에도, 업무 수행에 필요한 최소 권한만 부여함으로써 공격 표면을 줄이는 효과를 낼 수 있다. 이를 통해 사용자가 불필요하게 민감한 데이터나 시스템에 접근하지 못하도록 제한하는 것은 물론 내부자 위협이나 권한 남용 위험을 최소화할 수 있다.

궁극적으로 조직은 제로트러스트 기반의 패스워드리스(Passwordless) 인증 도입, 사용자 행동 분석 및 위험 평가 강화, 그리고 생체 인증의 보완과 같은 다층적인 접근 방식을 통해 아이덴티티 보호 체계를 강화해야 한다. 이를 통해 조직은 점점 더 정교해지는 위협 환경에서도 민감한 자산을 안전하게 보호하고, 신뢰할 수 있는 디지털 환경을 구축할 수 있을 것이다.

■ 식별자·신원(Identity) 필러의 주요 요소

제로트러스트 아키텍처에서 식별자·신원(Identity) 필러는 사용자와 관련된 모든 보안 요소를 다루는 핵심 영역으로, 제로트러스트 원칙을 구현하는 데 있어 필수적인 역할을 한다. 사용자는 단순히 사람뿐만 아니라 서비스 계정, IoT 기기 등 다양한 형태로 존재하며, 이들에 대한 신원 확인과 검증은 보안 체계의 출발점이 된다.

특히, 제로트러스트 환경에서는 모든 사용자를 신뢰할 수 없는 대상으로 간주하고, 지속적인 검증과 최소 권한 부여를 통해 접근을 통제해야 한다. 이를 위해 식별자·신원 필러는 사용자 인벤토리 관리, 계정 및 권한 관리, 인증 강화, 위험 평가 등 다양한 요소를 포함하며, 각 요소는 조직의 보안 태세를 강화하는데 중요한 역할을 한다.

아래에서는 식별자·신원 필러의 주요 요소와 이를 구현하기 위한 관리적 및 기술적 방안을 구체적으로 살펴본다.

1. 사용자 인벤토리

사용자 인벤토리는 조직 내 모든 사용자를 식별하고 관리하는 기본적인 출발점이다. 제로트러스트 환경에서는 사용자를 명확하게 식별하고, 이들의 신원을 최신 상태로 유지하는 것이 매우 중요하다. 사용자 인벤토리는 조직 내에서 누가 어떤 자산에 접근할 수 있는지에 대한 정보를 제공하며, 이를 통해 접근 통제 및 권한 부여를 효율적으로 관리할 수 있다.

사용자는 지속적으로 업데이트되는 목록화된 정보로 관리한다. 이 목록은 사용자의 기본 정보뿐만 아니라 신원 정보까지 포함해야 한다. 초기 단계에서는 파일이나 수기로 관리될 수 있지만, 성숙도가 높아짐에 따라 자동화된 시스템을 통해 사용자 정보가 실시간으로 업데이트되고, 신뢰도 있는 데이터를 기반으로 권한이 자동으로 변경될 수 있어야 한다.

사용자는 부서, 직급, 역할 등에 따라 그룹핑되어야 하며, 이러한 그룹 정보는 사용자의 상태가 변경될 때마다 자동으로 업데이트되어야 한다. 이를 통해 특정 그룹에 속한 사용자들이 필요로 하는 자산에만 접근되도록 제한한다.

2. 사용자 계정관리

사용자 계정 관리는 각 사용자가 보유한 계정을 통해 리소스에 접근할 수 있도록 하는 체계다. 계정 관리는 단순히 계정을 생성하고 삭제하는 것을 넘어, 계정의 수명주기 전체를 중앙에서 통제하고 관리해야 한다.

각 사용자는 고유한 계정을 부여받아야 하며, 해당 계정은 중앙에서 목록화하여 관리한다. 초기 단계에서는 단순히 파일이나 수기로 계정을 관리할 수 있지만, 점차 ICAM(Identity Credential Access Management)과 같은 통합 시스템을 도입해 모든 계정을 중앙에서 일괄적으로 관리하는 방식으로 발전해야 한다.

사용자 계정의 생성부터 삭제까지의 모든 과정이 자동화될 수 있도록 해야 하며, 이를 통해 불필요한 권한이 남용되지 않게 주의한다. 특히 A.I 및 머신러닝을 활용해 사용자의 신뢰도 데이터를 기반으로 계정의 상태를 지속적으로 검증하고, 필요 시 자동으로 권한을 조정하는 체계를 구축하는 것이 필요하다.

3. 사용자 패스워드 관리

패스워드는 많은 시스템에서 기본적인 인증 수단으로 사용되고 있다. 그렇기 때문에 패스워드 관리는 매우 중요한 요소다. 패스워드 정책은 주기적인 변경 요구와 복잡성 규정을 포함해야 하며, 패스워드 유실이나 도용을 방지하기 위한 추가적인 보안 조치도 필요하다. 사용자는 주기적으로 패스워드를 변경해야 하며, 이러한 변경 요구는 시스템에서 자동으로 알림을 제공해야 한다. 성숙도가 높은 조직에서는 패스워드가 자동으로 변경되고, 사용자는 인증 절차를 통해 새로운 패스워드를 확인하는 방식으로 운영될 수 있다.

패스워드는 정책에 따라 복잡성 요구사항이 설정되어야 한다. 이러한 정책이 준수되도록 모든 사용자를 강제한다. 또한 패스워드 유실 시에는 잠금 정책을 통해 추가적인 보안을 제공해야 하며, 이상 행위가 감지되면 즉시 대응할 수 있는 체계를 마련해야 한다.

제로트러스트 아키텍처에서는 패스워드 관리뿐만 아니라 사용자 행위에 따라 추가 인증이나 다중 인증 요소(MFA)를 적극적으로 활용하는 것을 권장한다. 이는 단순히 비밀번호를 사용하는 것만으로는 부족한 보안성을 강화하기 위해 사용자의 접속 환경과 행동 패턴을 지속적으로 평가하고, 필요 시 추가 인증 절차를 요구하는 방식이다. 예를 들어, 사용자가 평소와 다른 위치에서 접속하거나 비정상적인 활동을 수행할 경우 MFA 를 통해 보안을 강화할 수 있다.

궁극적으로 제로트러스트 아키텍처는 Passwordless 방식으로 전환하는 것을 목표로 한다. 이는 생체 인증(지문, 얼굴 인식), FIDO2 토큰 또는 물리적 키와 같은 강력한 인증 기술을 활용하여 비밀번호의 재사용 문제와 유출 위험을 근본적으로 해결한다. Passwordless 방식은 사용자 경험을 개선하면서도 보안을 강화하는 데 효과적이며, 제로트러스트 환경에서 점점 더 중요해지고 있다.

4. 사용자 권한 관리

제로트러스트 아키텍처에서는 최소 권한 원칙이 매우 중요하다. 사용자 권한 관리는 각 사용자가 업무 수행에 필요한 최소한의 리소스에만 접근할 수 있도록 제한하는 것을 목표로 한다.

각 시스템과 리소스에 대한 접근 권한은 개별적으로 설정되어야 하며, 이러한 권한은 주기적으로 검토되고 업데이트되어야 한다. 또한 각 시스템에서 운영자와 관리자 등 다양한 역할에 따라 접근 권한을 구분한다. 리소스별로 접근 및 수정 권한이 명확하게 정의되어야 가능하다.

사용자가 리소스에 접근하여 수행하는 모든 활동은 실시간으로 모니터링되고, 이상 징후가 발견되면 즉시 차단하거나 경고를 제공하는 체계가 필요하다.

5. 사용자 증명

제로트러스트 환경에서는 단순히 ID 와 비밀번호만으로는 충분하지 않다. 사용자 증명(User Authentication)은 다단계 인증(MFA)을 포함하여 더욱 강력하게 이루어져야 하며, 이를 통해 신뢰성을 강화할 필요가 있다.

ID 페더레이션은 한 번의 로그인으로 여러 서비스에 접근할 수 있도록 하는 체계다(SAML, OAuth 등 표준 활용). 전사적인 ID 페더레이션 체계를 구축하면 모든 시스템과 애플리케이션에서 일관된 인증 절차를 거칠 수 있다.

다중 인증(MFA)을 통해 추가적인 보안 레이어를 제공하며, 신뢰도 판단 데이터를 기반으로 인증 절차를 강화해야 한다. MFA 는 지식 기반(비밀번호), 소유 기반(OTP), 생체 기반(지문) 등을 결합하여 보다 안전하게 사용자 인증을 수행한다.

6. 통합 ICAM 플랫폼

통합 ICAM(Identity Credential Access Management) 플랫폼은 제로트러스트 아키텍처의 핵심 구성 요소 중 하나로, 모든 리소스에 대한 접근 제어와 자격 증명을 중앙에서 통합적으로 관리하는 역할을 수행한다. ICAM 은 기존 IAM(Identity and Access Management)의 확장 개념으로, 단순히 신원(Identity) 관리에 그치지 않고 자격 증명(Credential)까지 포함하여 사용자와 엔터티의 신뢰도를 더욱 정교하게 평가한다.

ICAM 플랫폼은 모든 사용자와 관련된 정보를 중앙에서 일괄적으로 관리하며, 이를 통해 자격 증명과 인증 절차를 자동화한다. 역할 기반 제어(Role-Based Access Control) 기능으로 각 사용자의 역할에 따라 리소스 접근 권한이 자동으로 부여되거나 제한된다. 또한, 속성 기반 접근 제어(Attribute-Based Access Control)를 활용하여 사용자의 위치, 디바이스 상태, 행동 패턴 등 다양한 컨텍스트를 고려한 동적 정책 적용이 가능하다.

ICAM 은 PIP(Policy Information Point)를 활용하여 SIEM(Security Information and Event Management), EDR(Endpoint Detection and Response), UEM(Unified Endpoint Management) 등에서 전달된 정보를 바탕으로 사용자의 신원(Credential)을 판단한다. 이러한 정보는 사용자의 행동 패턴과 디바이스 상태를 실시간으로 분석하여 위험도를 평가하고, 이를 기반으로 지속적인 인증 및 검증을 수행한다. 예를 들어, 사용자가 비정상적인 네트워크 활동을 수행하거나 보안 정책을 위반한 경우, ICAM 플랫폼은 즉시 경고를 생성하거나 추가 인증 절차를 요구할 수 있다.

ICAM 은 또한 PAM(Privileged Access Management)과 연계되어 특권 계정의 접근을 제어하고 모니터링함으로써 Identity 기반의 자격 증명을 더욱 강화한다. PAM 과의 통합은 민감한 시스템과 데이터에 대한 접근을 엄격히 제한하며, 내부자 위협이나 권한 남용을 방지하는 데 중요한 역할을 한다.

7. 사용자 위험평가

제로트러스트 환경에서는 각 사용자의 위험도를 평가하고 이를 바탕으로 보안 정책을 동적으로 조정하는 것이 중요하다. 각 사용자의 위험도는 컴플라이언스 준수 여부나 이상 행위 탐지에 따라 정량화하여 평가된다.

위험도 평가는 인증 강화 및 권한 부여 시 중요한 데이터로 활용되며, 실시간 모니터링을 통해 즉각적인 대응이 가능하도록 해야 한다.

식별자·신원 필러는 이러한 주요 요소들을 통해 조직 내 민감한 자산을 보호하고 내부자 위협과 외부 공격 모두를 효과적으로 차단할 수 있다. 나아가 변화하는 위협 환경에 적응할 수 있는 유연성과 신뢰성을 제공하며, 제로트러스트 환경에서 일관된 보안 정책 적용과 지속 가능한 디지털 보안 체계를 구축하는 데 핵심적인 역할을 한다. 이를 통해 조직은 더욱 강력하고 신뢰할 수 있는 보안 태세를 유지하며, 안전한 디지털 환경을 조성할 수 있을 것이다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행할 수 있는 시스템은 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙을 기반으로 한다. 이를 실현하기 위해 사용자와 엔터티의 신원을 확인하고, 지속적으로 검증하며, 최소 권한 접근을 보장을 수행할 수 있는 시스템이 필수적이다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 식별자(Identity) 관점으로 중요한 역할을 담당하며, 이들 시스템은 상호 연계되어 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.

출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 3. 식별자·신원 주요 시스템

1. SSO(Single Sign-On)

SSO 는 하나의 인증으로 여러 애플리케이션과 시스템에 접근할 수 있도록 하는 통합 인증 시스템으로, 사용자 편의성과 운영 효율성을 동시에 확보할 수 있는 인증 기술이다. 하지만 제로트러스트 환경에서는 단순한 사용자 편의성만으로는 충분하지 않으며, 지속적인 검증과 동적 통제가 가능한 보안 역량이 필수적으로 요구된다.

제로트러스트 환경에서 SSO 는 더 이상 단일 포털 인증 수준에 머물지 않는다. 웹 환경은 물론 클라우드 서비스(AWS, Azure, GCP)와의 연계, 그리고 C/S 기반 내부 시스템까지 포함하여 다양한 접근 경로에 대한 통합 인증을 지원해야 하며, 각 환경에서의 인증 요구사항을 만족할 수 있도록 표준 인증 프로토콜(SAML, OAuth, OIDC 등)에 기반한 상호 운용성과 확장성을 갖추는 것이 기본 전제가 된다.

제로트러스트 원칙에서 SSO 는 단순히 최초 인증을 처리하는 시스템이 아니라, 최초 인증 이후에도 지속적으로 세션의 유효성, 사용자 행동 변화, 접속 단말과 위치, IP 주소, 접속 시간 등의 컨텍스트 정보를 실시간으로 분석하여 인증 값의 변조 가능성을 탐지하고 필요 시 재인증이나 세션 차단 등 후속 조치를 수행할 수 있어야 한다. 이 과정에서 인증 토큰에 대한 암호화는 기본이며, 인증값 위·변조 방지 기술을 통해 세션 하이재킹 등 공격 시도에 선제적으로 대응할 수 있는 구조가 요구된다.

더불어, 사용자 인증 시 단순한 정적 규칙 기반 접근이 아니라, 다중 요소(단말 유형, 접속 위치, 시간대, IP 특성 등)를 기반으로 리스크 스코어링을 수행하여 동적으로 인증 수준을 조정하거나 인증 경로 자체를 변경할 수 있는 유연한 정책 구성이 필요하다. 예컨대 동일한 자격 증명을 보유하더라도 평소와 다른 지역, 의심스러운 시간대, 새로운 디바이스로 접속 시 추가 인증(MFA)이나 접근 제한 조치가 병행되어야 한다.

이러한 모든 인증 활동과 접근 흐름은 시각화된 대시보드를 통해 실시간 모니터링되어야 하며, 인증 성공·실패 이력, 사용자별 접속 이력, 리스크 이벤트 발생 현황 등을 체계적으로 리포트할 수 있어야 한다. 이는 단순한 보안 감시를 넘어서, 사용자 행동 기반의 이상 탐지(UEBA)나 보안 정책 강화에도 활용될 수 있는 주요 기반 데이터로 작용한다.

결국 SSO 는 제로트러스트 환경의 '초기 관문'으로서 단순한 인증 시스템의 범주를 넘어, 사용자와 엔터티에 대한 지속 가능한 검증 체계를 제공하는 실시간 보안 운영 인프라로 자리매김하고 있다. 제대로 된 SSO 구현 없이는 제로트러스트 아키텍처의 출발점조차 성립하기 어려운 만큼, 해당 시스템에 대한 기술적·관리적 완성도는 제로트러스트 환경에서 매우 중요한 요소이다.

2. IAM(Identity and Access Management)

IAM 은 제로트러스트 아키텍처의 핵심 구성요소로, 사용자 계정과 권한을 중앙에서 통합 관리하고 다양한 업무 시스템과의 연동을 지원함으로써 보안 통제력을 강화하는 역할을 한다. IAM 은 단순한 계정 등록과 삭제를 넘어, 사용자의 신원과 권한을 연계한 세분화된 접근 제어를 실현하며, 이를 통해 최소 권한 원칙을 지속적으로 유지할 수 있도록 한다.

제로트러스트 환경에서의 IAM 은 인사 정보나 사용자 속성 같은 다양한 데이터를 연계하기 위해 LDAP, AD, DB File 등과 같은 디렉터리 시스템과의 연동 기능을 갖추고 있어야 하며 웹 기반, C/S 환경, 클라우드 플랫폼 등 이기종 시스템과 유연하게 통합되도록 표준 프로토콜(SAML) 및 API 연동을 지원해야 한다. 이를 통해 조직은 모든 업무 시스템에 대한 사용자 계정과 권한을 중앙에서 통합적으로 관리할 수 있으며, 정책 위반 계정 탐지, 휴면 계정 정리 등의 작업도 자동화하여 지속적인 권한 적정성을 유지할 수 있다.

특히 제로트러스트 원칙에 따라 ABAC(속성 기반 접근 제어), RBAC(역할 기반 접근 제어) 등의 정책 모델을 정교하게 구현해야 하며, 사용자의 직무, 부서, 위치, 접속 환경 등 다양한 속성을 기반으로 한 권한 제어가 가능해야 한다. 이러한 역할 기반·속성 기반 권한 설정은 단순히 관리자에 의해 수동으로 구성되기에는 한계가 있으며, A.I 나 머신러닝을 통한 정책 자동화 기능이 함께 도입되어야 한다.

예측 기반의 접근 권한 추천, 권한 충돌 감지, 이상 행위 기반의 정책 재구성 등은 단순히 이론적 기능이 아닌, 최근 상용 IAM 제품들이 실제로 구현하고 있는 핵심 기능이다. 예를 들어, 일부 글로벌 IAM 솔루션은 사용자의 과거 접근 패턴과 직무 이력을 학습하여 새로운 업무 시스템 연동 시 자동으로 적절한 권한을 추천하거나, 유사 직무자와의 권한 비교를 통해 초과 권한 여부를 탐지한다.

또한 머신러닝 기반의 이상행위 탐지 엔진은 사용자 행위가 통상적인 업무 흐름과 벗어날 경우 경고를 생성하거나 권한을 자동 축소하는 정책을 실시간 적용한다. 이러한 기능들은 IAM 을 단순한 계정 관리 시스템이 아닌 ‘지능형 접근 제어 허브’로 진화시키며, 제로트러스트 보안 체계의 실행력을 강화하는 데 실질적으로 기여하고 있다.

IAM 은 확장될 경우 기존 IAM 시스템에서 신원(Credential)을 포함한 ICAM(Identity, Credential and Access Management)으로 확장 구성될 수 있으며, 이는 제로트러스트 기반의 핵심 통합 시스템으로 작동한다. ICAM 은 EDR, UEM, Micro-Segmentation, SIEM/SOAR, DLP, DSPM 등의 다양한 PIP(Policy Information Point)와 연동되어 사용자와 기기의 신뢰 수준을 실시간으로 평가하고 이를 기반으로 동적 접근 정책을 적용하는 역할까지 수행하게 된다. 따라서 IAM 은 단순한 인증 및 계정 관리 체계를 넘어, 제로트러스트 환경의 기반이 되는 '핵심 시스템'으로 기능해야 한다.

* 근거 문서

1. "NIST SP 800-207" (NIST)
2. "Automating Access Governance for Zero Trust" (KuppingerCole) 3."The Importance of Least Privilege in a Zero Trust World" (SANS Institute)
4. "User and Entity Behavior Analytics (UEBA) for Zero Trust" (Gartner) 5."The Role of SIEM in a Zero Trust Architecture" (Forrester)

그림 4. 제로트러스트 기반 SSO/IAM 의 주요기능

3. MFA (Multi-Factor Authentication)

다중 인증(MFA)은 제로트러스트 환경에서 '지속적인 검증' 원칙을 실현하는 핵심 수단으로, 사용자 인증에 있어 단일 수단에 의존하지 않고 다양한 인증 방식을 조합해 보안성을 강화하는 역할을 수행한다. 특히 해외에서는 MFA 가 SSO 기능과 통합되어 하나의 인증 플랫폼으로 운영되는 경우가 많지만, 국내 보안 환경에서는 MFA 를 별도의 독립된 인증 시스템으로 구축하고 관리하는 경우가 일반적이다. 이러한 구조는 시스템 구성의 유연성과 보안정책의 분리 운용 측면에서 각각의 장단점을 가지고 있으며, 제로트러스트 환경에서는 양쪽 모두에 대한 고려가 필요하다.

MFA 시스템은 기본적으로 SSO, IAM 에서 사용자 이상행위가 탐지되었을 때 추가 인증 수단을 수행하는 역할을 하며, OTP(일회용 비밀번호), 하드웨어/소프트웨어 토큰, 휴대폰 기반 생체 인증(FIDO2 기반 지문·얼굴 인식) 등의 다양한 방식이 사용된다. 이때 인증 수단은 정보보안 인증의 기본 개념인 Type1(지식), Type2(소유), Type 3(존재)을 조합하여 구성되며, 다중 요소 인증의 본질은 바로 이 복합 인증 요소들의 상호 보완성을 통해 인증 위협을 차단하는 데 있다.

최근 MFA 기술은 단순한 인증 수단 제공을 넘어 진화하고 있다. 예를 들어, FIDO2 이후에는 브라우저·디바이스 간 인증 연계성, 생체 인증의 보안성 강화, 인증 절차 단순화 등을 중심으로 한 차세대 기술 개발 논의가 지속되고 있으며, 특히 생체 인증 과정에서의 라이브니스 감지(Liveness Detection) 기술은 딥페이크나 녹화 영상 등의 위조 시도를 탐지하는 데 활용되고 있다. 또한 인증 토큰 발급 및 전달 과정에서 PQC(Post-Quantum Cryptography, 양자 내성 암호) 등 차세대 암호 알고리즘을 적용하려는

움직임도 나타나고 있다. 이처럼 MFA 는 고도화된 인증 위협에 대응하기 위한 핵심 기술로 자리매김하고 있으며, 단순한 인증 절차를 넘어 제로트러스트 아키텍처의 정밀한 인증 관문으로서의 역할을 강화하고 있다.

결과적으로 MFA 는 사용자의 인증을 일회성으로 처리하지 않고, 위험 기반 인증(RBA: Risk-Based Authentication), 행위 기반 재인증, 컨텍스트 기반 정책 적용 등을 통해 지속적이고 동적인 인증 체계를 제공한다. 이는 단순한 로그인 절차를 넘어서 지속적으로 신뢰를 평가하고 강화하는 제로트러스트 모델의 핵심 구성 요소로 기능하며, SSO, IAM 과의 긴밀한 연동을 통해 사용자 신원을 정교하게 검증하는 보안 인프라로 자리매김하고 있다.

4. AD(Active Directory)

Active Directory(AD)는 마이크로소프트가 제공하는 디렉터리 서비스로, 가장 많이 사용되는 Windows 기반 인프라 환경에서 사용자 계정, 그룹, 장치, 정책 등을 중앙에서 관리하는 핵심 시스템이다. 오랜 역사를 가진 레거시 시스템이지만, 현재도 대다수의 기업 환경에서는 여전히 중심적인 사용자 인증 및 접근 제어 인프라로 활용되고 있으며, 특히 온프레미스 AD 와 Microsoft 의 클라우드 기반 디렉터리 서비스인 Entra ID(구 Azure AD)의 연동을 통해 하이브리드 환경을 구성하는 사례가 빠르게 확산되고 있다.

AD 는 단순한 사용자 저장소를 넘어, 조직 내 다양한 시스템(SaaS 애플리케이션, 파일 서버, ERP 등)과 연계되어 사용자 신원 정보와 그룹 속성, 권한 정책을 실시간으로 제공하는 정보 허브 역할을 수행한다. 특히 SSO, IAM, EDR, UEM 등 다수의 보안 시스템들은 AD 를 기반으로 사용자 권한을 해석하고 동적으로 접근 제어 정책을 적용하기 때문에, AD 정보의 정확성과 최신성은 전체 보안 체계의 신뢰성을 좌우하는 요소로 작용한다.

제로트러스트 환경에서 AD 는 그 자체로 보안 대상이며 동시에 공격 표적이 된다. 공격자는 초기 침입 이후 권한 상승을 위해 AD 를 우선적으로 노리고, 관리자 계정 탈취, 권한 확장, 서비스 접근 경로 확보 등의 행위를 AD 내부에서 수행하려 한다. 실제로 다수의 침해 사고 사례에서 AD 가 권한 탈취의 통로로 활용된 바 있으며, 이로 인해 AD 는 제로트러스트 보안 전략 내에서 최우선 보호 대상 자산으로 간주된다.

따라서 AD 는 단순한 운영 관리 대상이 아니라 보안 인프라로서 기능해야 하며, 이를 위해 다양한 보안 솔루션이 함께 적용되어야 한다. 예를 들어, AD 내부의 이상 행위를 실시간으로 탐지하는 보안 로그 분석 시스템, 관리자 권한의 위임 및 승인 체계를 적용하는 PAM 연계, 불필요한 그룹 정책이나 계정 설정을 탐지하고 정리하는 정책 감사 도구 등이 대표적인 보안 기술이다. 이외에도 AD 자체에 대한 정기적인 위협 분석 및 강화 설정 점검이 필수적으로 수행되어야 한다.

AD 는 제로트러스트 환경에서 사용자의 실시간 상태, 디바이스 연결 여부, 로그인 시도 기록 등을 기반으로 리스크 기반 인증 정책이나 세분화된 접근 통제를 수행하는 데 기초 데이터를 제공한다. 따라서 AD 와 연계되는 보안 시스템은 AD 로부터 제공되는 정보를 토대로 지속적인 사용자 신뢰 평가와 권한 검증을 수행해야 하며, 이를 위해 AD 는 항상 최신의 정확한 데이터를 유지해야 한다.

결과적으로 AD 는 더 이상 단순한 사용자 관리 시스템이 아니라, 제로트러스트 환경을 구현하기 위한 보안 기반 플랫폼 중 하나로서 기능하며, 그 운용 수준에 따라 전체 보안 아키텍처의 완성도 또한 달라질 수 있다.

5. HR 시스템 (Human Resources System)

HR 시스템은 조직 내 모든 사용자에 대한 신원, 직무, 소속 부서, 고용 상태 등의 인사 정보를 관리하는 핵심 시스템으로, 제로트러스트 환경에서는 사용자 신뢰 수준 판단과 권한 정책 적용의 기초 데이터 소스로서 기능한다. 기존 보안 아키텍처에서는 HR 시스템이 단순한 행정 시스템으로 여겨졌으나, 제로트러스트 체계에서는 사용자 검증과 접근 통제를 위한 핵심 연동 대상 시스템으로 그 중요성이 재조명되고 있다.

이처럼 HR 시스템은 사용자 라이프사이클 전반에 걸쳐 보안 정책을 연계·적용하기 위한 '권한 정책의 출발점'으로 작동하며, 특히 부서 이동, 직무 변경, 장기 휴직 등 사용자 속성의 변화가 발생할 경우 이를 신속하게 연동 시스템에 반영할 수 있어야 한다. 이를 통해 불필요한 권한 유지, 휴면 계정 방치 등으로 발생할 수 있는 보안 리스크를 사전에 차단할 수 있다.

또한, HR 시스템은 사용자 데이터를 기반으로 한 RBAC(역할 기반 접근제어) 및 ABAC(속성 기반 접근제어) 정책 설계의 핵심 기반이 되며, 이는 제로트러스트의 '최소 권한 원칙'을 실현하는 데 필수적인 요소다. 특히 최근에는 HR 시스템에 저장된 데이터를 기반으로 머신러닝을 활용한 권한 적정성 평가, 초과 권한 자동 탐지 등 지능형 접근 제어 기능의 정확도를 높이는 데 사용하고 있다.

결과적으로 HR 시스템은 보안 시스템과 별도로 존재하는 관리 시스템이 아니라, 제로트러스트 보안 체계 전반에 데이터를 공급하고 사용자 행위를 통제하는 핵심 정보 연계 시스템으로 기능해야 한다. HR 정보의 정확성과 시의성은 사용자 권한 설정의 정확도뿐 아니라 전체 보안 정책의 실효성을 결정짓는 요인으로 작용하며, 이를 위한 체계적인 연동 구조와 지속적 데이터 정합성 확보가 무엇보다 중요하다.

식별자·신원 필러의 각 시스템은 단순한 기능 단위를 넘어, 제로트러스트 아키텍처를 기술적으로 구현하는 실질적인 수단으로 작동한다. SSO, IAM, MFA, AD, HR 시스템은 서로 독립된 기능을 수행하면서도 상호 유기적으로 연계하여, 사용자 식별부터 인증, 권한 부여, 활동 모니터링에 이르기까지 전 과정에 걸친 통합 보안 통제를 가능하게 한다.

이로써 조직은 물리·가상·클라우드 등 다양한 환경에서도 일관되고 정밀한 신원 기반 접근 제어를 구현할 수 있으며, 다양한 보안 위협 환경 속에서도 신뢰 중심의 보안 전략을 지속 가능하게 유지할 수 있다.

결국 제로트러스트의 핵심 원칙인 '지속적인 검증'과 '최소 권한 부여'는 이러한 시스템들을 통해 구체적으로 구현되며, 이는 조직의 보안 전략을 이론적 구상에 머물게 하지 않고, 실제 환경에서 적용 가능하고 운영 가능한 수준으로 끌어올리는 기반이 된다.

■ 맺음말

제로트러스트 아키텍처에서 식별자(Identity)는 모든 보안 전략의 시작점이자, 사용자와 엔터티에 대한 신뢰를 평가하고 검증하는 중심 축이다. 사용자, 기기, 서비스 계정 등 다양한 주체에 대한 정확한 식별과 지속적인 신뢰 평가가 수반되지 않는다면, 제로트러스트의 핵심 원칙인 '지속적인 검증'과 '최소 권한'은 형식적인 구호에 그칠 수밖에 없다.

식별자 필러의 주요 시스템인 SSO, IAM, MFA, AD, HR 시스템은 단순히 개별 기능을 수행하는 시스템이 아니라, 식별자 기반 통제 체계를 구성하는 유기적이고 상호 보완적인 보안 인프라다. 이들 시스템은 사용자 정보를 생성하고 검증하며, 이를 바탕으로 접근 권한을 부여하고, 이상 행위를 탐지해 실시간으로 정책을 조정하는 등, 제로트러스트 환경에서 요구되는 핵심 보안 통제 기능을 분산 수행한다.

특히 식별자 필러는 사용자 신원과 권한에 대한 데이터 흐름을 제어하고 연결하는 '허브' 역할을 수행하며, 다른 모든 필러의 기반을 제공한다. 식별자 필러가 정교하게 설계되고 운영될 경우, 조직은 사용자 단위의 통제는 물론, 디바이스, 네트워크, 애플리케이션, 데이터 등 제로트러스트 아키텍처 전 영역에 걸쳐 일관된 보안 정책을 적용할 수 있는 구조적 기반을 확보하게 된다. 반대로 식별자 필러가 허술하게 구축되면, 권한 오남용, 비인가 접근, 내부자 위협에 대한 감시가 어려워지고, 전체 보안 체계의 연속성 역시 약화될 수 있다.

또한 식별자·신원 기반 통제가 견고하게 작동할수록, 조직은 보안 사고에 대해 보다 안전한 상태를 유지할 수 있다. 이는 단순히 사고를 예방하는 수준을 넘어, 사고 발생 시 원인 분석과 사용자 이력 추적, 포렌식까지 신속하게 수행할 수 있는 기반이 된다는 점에서 중요하다. 이러한 정보는 사고 대응과 재발 방지, 정책 보완 등 보안 운영 전반에 실질적인 효과를 제공한다.

식별자 필러는 단순한 인증 기능이 아니라, 제로트러스트 아키텍처 전반을 실질적으로 작동시키는 '기반 필러'이자 '보안 전략의 관문'이다. 조직은 이 영역을 전략적으로 우선 구축하고, 이를 토대로 다른 필러로 확장하는 단계적 접근을 통해 리스크를 통제 가능한 수준으로 줄이고, 신뢰 기반의 디지털 보안 환경을 실현할 수 있을 것이다.

■ 참고 문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] DoD, “Zero Trust Overlays”, 2024.06

[3] 과학기술정보통신부/KISA, “제로트러스트 가이드라인 V1.0”, 2023.06

[4] 과학기술정보통신부/KISA, “제로트러스트 가이드라인 V2.0”, 2024.12

[5] SK쉴더스, “2025 보안 위협 전망 보고서”

[6] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” - 브로슈어

[7] SpyCloud, “2025 Identity Exposure Report”

[8] Gatner, "Predicts 2024: AI & Cybersecurity - Turning Disruption Into an Opportunity"

[9] SC Media, "How attackers outsmart MFA in 2025"

[10] Sosafe, "MFA Fatigue Attack"