Infographics

2025.11

AI 시대의 데이터 보안, 과연 안전한가?
내부자 위협, 제로 트러스트와 통합 보안 솔루션으로 대응

45억 3,600만 원

데이터 유출 사고로 기업이 부담하는 평균비용

국내 기밀/기술 유출의

80%

전·현직 직원에 의해 발생

About UNION biometrics

UNION Biometrics는 생체인식 보안 분야의 글로벌 선도 기업으로서,독자적인 기술과 특허받은 안티 스푸핑(Anti-Spoofing) 기법을 기반으로 한 프리미엄 멀티모달 인식 장치와 고성능 통합 출입통제 솔루션을 제공합니다.

회사는 전 세계의 주요 기반 시설, 기업, 그리고 정부 기관을 대상으로 신뢰할 수 있는 글로벌 파트너 네트워크를 통해 보안을 제공하고 있습니다.

1. 서론

AI와 내부자에 의한 데이터 보안 붕괴

AI를 활용한 데이터 유출 사고가 현실화되면서, AI는 더 이상 가능성의 영역이 아닌 현실적인 보안 위협으로 대두되고 있다. 2024년 홍콩에서 발생한 딥페이크 화상회의 사기(약 340억 원 피해)가 이 위험을 증명하는 대표적 사례이다. 이처럼 정교하게 변조된 AI 음성, 딥페이크 영상 통화는 기존 보안 시스템의 가장 약한 고리인 **'인가된 내부자(Trusted Insider)'를 기만하여 기업의 핵심 데이터에 접근하는 새로운 핵심 공격 벡터(Attack Vector)**로 부상했다.

많은 기업이 데이터 보호를 위해 '망분리(Network Segmentation)'를 구축했지만, 이는 '네트워크를 통해 침입하는 외부의 위협'을 차단한다는 전제에 최적화되어 있다. 산업기밀보호센터에 따르면, **국내 기술/기밀 유출의 약 80%가 전·현직 직원에 의해 발생**하며, Ponemon Institute는 이러한 내부자 위협의 56%가 악의적인 의도보다는 '부주의'나 '실수'로 인해 발생한다고 보고한다. 이는 망분리 환경이 근본적으로 '신뢰받는 내부자'의 행위(악의적이든, 비의도적이든)를 검증하는 강력한 신원 인증 메커니즘이 부재하여 AI 기반 사회공학적 공격에 대한 본질적인 취약성을 내포함을 의미한다.

IBM의 2023년 보고서에 따르면, **데이터 유출 사고로 인해 한국 기업이 부담하는 평균 비용은 45억 3,600만 원에 달한다.** 이는 단순한 기술적 오류가 아닌, 망분리를 포함한 기존 정보보안 솔루션에만 의존하는 전략이 야기할 수 있는 심각한 '구조적 보안 부채(Structural Security Debt)'를 의미하는 정책적 경고로 해석해야 한다.

2. 배경

'견고한 시스템'의 환상과 위협의 범위

데이터 중심 인프라가 보편화됨에 따라, 전통적인 '경계 기반 보안' 모델은 한계를 드러내고 있다. 위협은 외부와 내부를 가리지 않는다. Trend Micro에 따르면, **의료 기관의 57%가 지난 3년 내 랜섬웨어 공격을 경험했으며, 이 중 25%는 운영을 중단할 정도의 심각한 피해를 입었다.** 이처럼 정부, 병원 등 사회 기반 시설을 노리는 외부 공격이 증가하는 동시에, "내부망은 안전하다"는 낡은 믿음은 실제 발생한 내부자 사고 사례들을 통해 무너지고 있다.

특히 최근 **5년간 공공기관 개인정보 유출 건수가 525% 급증**(2019년 8건 → 2023년 41건)한 현실은, 망분리 환경이 내부자 위협에 의해 무력화되는 경로를 분석할 필요성을 시사한다.

- **[유형 1] 악의적 내부자 및 권한 남용 (2013년 스노든 NSA 사건 / 2023년 테슬라 사건)**

시스템 관리자 등 높은 권한을 가진 내부자가 의도적으로 데이터를 유출하는 경우. 스노든은 동료의 ID와 패스워드를 도용했으며, 2023년 테슬라 사건 역시 전 직원이 내부 정책을 위반해 100GB의 기밀 데이터를 반출했다.

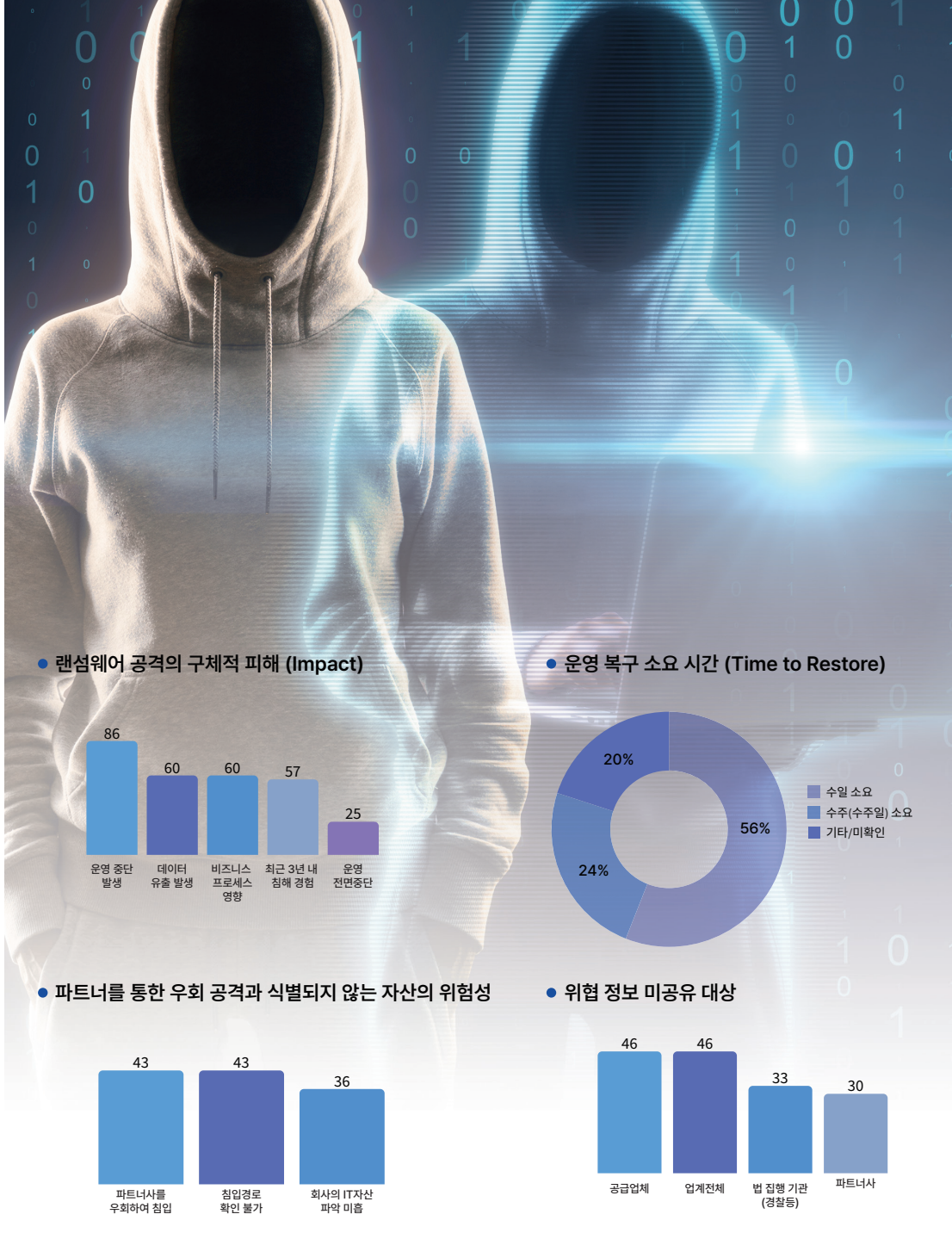
- **[유형 2] 부주의 및 협력업체 리스크 (2014년 카드 3사 개인정보 유출)**

내부자의 '부주의'나 '실수'는(서론에서 언급한 56%) 악의적 의도만큼이나 치명적이다. 2014년 카드 3사 유출 사건은 망분리 환경이었으나, 파견된 협력업체 직원이 USB라는 물리적 매체를 통해 1억 건 이상의 고객 정보를 유출한 대표적 사례이다. 이는 물리적 접근통제와 매체 제어의 실패가 망분리를 무력화시킬 수 있음을 보여주었다.

- **[유형 3] 물리적/논리적 접점 붕괴 (2016년 국방부 DIDC 해킹 / 2024년 'GoldenJackal' APT)**

망분리 환경이라도 백신 서버, 패치 서버 등 두 망의 '접점'이 존재한다. 2016년 국방부 해킹은 이 접점을 악용해 내부 작전망까지 침투했으며, 2024년 'GoldenJackal' APT 그룹은 악성 USB를 통해 망분리(Air-gapped) 환경을 공략했다.

망분리 구축을 포함한 전통적인 정보보안 전략은 이처럼 고도화된 외부 공격과 복합적인 내부자 위협에 동시 대응할 수 없으며, 이는 금융, 제조, 공공, 방산을 막론하고 심각한 보안 공백을 초래한다.



출처 : Trend Micro ResearchgQuarter of Healthcare Ransomware Victims Forced to Halt Operations (단위 %)

기술적 대응:
'제로 트러스트(Zero Trust)'로의 패러다임 전환

1세대: 물리적 보안
자물쇠, 경비원 등 전통적인 물리적 통제 수단에 의존하는 단계.

2세대: 경계 기반 보안
방화벽, 망분리 등 외부 침입을 막는 '디지털 장벽' 구축 단계.
한계: 한번 뚫려서 내부로 들어오면 무조건 신뢰하므로 내부자 위협에 취약

3세대: 제로 트러스트 아키텍쳐
아무도 믿지 않고(Never Trust), 항상 검증한다(Always Verify)는
원칙의 최신 보안 모델. 내/외부 구분 없이 모든 접근을 지속적으로 확인.

3. 기술적 대응
'제로 트러스트(Zero Trust)'로의 패러다임 전환

위협의 진화에 대응하여 데이터 접근 보안 패러다임 또한 '성곽과 해자(Castle-and-Moat)' 모델에서 **'제로 트러스트(Zero Trust)' 모델**로 전환하고 있다.

- **1세대 (물리적 보안):** 자물쇠, 경비원 등 전통적인 물리적 통제.
- **2세대 (경계 기반 보안):** 방화벽, IPS 등 외부와 내부를 나누는 '디지털 해자' 구축. 망분리가 이에 해당한다. 이 모델의 근본적 한계는, 일단 경계 내부로 진입하면(로그인 성공) 그 사용자를 '신뢰'한다는 점이다. 전 세계 물리 보안 시장은 2032년 1,967억 달러에 이를 것으로 예측되나, 이러한 2세대 방식만으로는 내부자 위협을 막을 수 없다.
- **3세대 (제로 트러스트 아키텍처):** "절대 신뢰하지 않고, 항상 검증한다(Never Trust, Always Verify)"는 원칙이다. 이는 내부/외부를 구분하지 않고, 데이터에 접근하는 모든 순간 사용자의 신원, 단말기의 안전성, 접근 위치, 요청 행위의 적절성 등을 반복적·지속적으로 검증하는 패러다임이다.

AI가 내부자의 ID를 탈취하거나 정교한 딥페이크로 사용자를 기만하려는 현시점에서, 보안의 핵심은 '네트워크 분리'가 아닌 '신뢰할 수 있는 사용자 인증'으로 이동해야 한다.

4. 기술 신뢰성 검증

유니온바이오메트릭스의 통합 접근 제어 (UBio-Connect ezPass)

'제로 트러스트' 아키텍처는 "절대 신뢰하지 말고, 항상 검증하라"는 원칙에 기반한다. 유니온바이오메트릭스는 이러한 제로 트러스트 환경 구축 시 가장 기본이 되는 '신원(Identity)'과 '인증(Authentication)' 요소를 강력하게 지원하여, 망분리 환경의 구조적 취약성을 보완하는 서버 기반의 통합 생체 인증 솔루션 UBio-Connect ezPass를 제공한다.

핵심 기능 1: 얼굴인식 기반 로그인 및 이력 관리 (Always Verify 원칙 지원)
기존의 ID/Password 방식은 도용(스노든 사례)에 극히 취약하다. UBio-Connect ezPass는 제로 트러스트의 핵심 원칙인 '항상 검증'을, 정적인 패스워드가 아닌 안티스푸핑(PAD)이 검증된 동적 생체 정보(얼굴)를 통해 강화한다. 이를 통해 실제 그 사용자(The Right Person)가 접근했는지 검증하고, 모든 로그인 이력을 생체 정보와 함께 저장하여 강력한 감사 추적(Audit Trail)을 보장한다.

핵심 기능 2: 복수 사용자 로그인 차단 및 계정 공유 방지 (Least Privilege 원칙 지원)
'최소 권한의 원칙(Least Privilege)'은 제로 트러스트의 또 다른 기둥이다. UBio-Connect ezPass는 하나의 계정으로 여러 단말기에서 동시에 접속하거나(계정 공유), 비인가된 사용자가 접근하는 것을 시스템 레벨에서 차단한다. 이는 내부자의 권한 남용 및 협력업체 직원의 비인가 행위를 원천 통제하는 **제로 트러스트의 최소 권한 원칙을 실현하는 핵심 기능이다**.

핵심 기능 3: 물리-논리 보안 융합 (Context-Aware Access 기반 강화)
UBio-Connect ezPass는 데이터센터나 서버실의 물리적 출입통제(유니온바이오메트릭스 UBio-X 시리즈)와 연동될 수 있다. 제로 트러스트는 '상황 인식(Context-Aware)'을 강조한다. "물리적으로 해당 공간에 출입한 사람"과 "논리적으로 해당 서버에 로그인한 사람"의 신원이 일치하는지 교차 검증하는 것은, 2014년 카드사 유출 사건과 같은 물리적 매체 반입 위협을 이중으로 차단하는 강력한 상황 인식 보안 정책을 구현한다.

이러한 기술의 통합은 고위험 환경에서 요구되는 두 가지 핵심 보안 지표, 즉 **Access Assurance (정확한 접근 보장)와 Data Integrity (데이터 무결성)**를 동시에 극대화하는 강력한 보안 기반을 제공한다.

- **UBio-Connect ezPass**
  UBio-Connect ezPass는 서버 기반 생체인식 솔루션으로, 단일 얼굴 인증 PC 로그인과 기존 출입통제 연동을 통해 비인가 접근 및 데이터 유실을 원천 차단하고, 강력하고 신뢰성 있는 보안 체계를 구축한다.

근태 현황 대시보드
전체 접속자 수, 근무시간, 장소 등으로 구분되어 출퇴근 현황을 한눈에 확인할 수 있는 대시보드를 제공

얼굴 생체 인증
얼굴 기반 생체 인증 솔루션으로, ID나 PW를 입력하지 않아 비밀번호 분실로 인한 회사 자산 및 개인정보 유출의 피해를 차단

생체 개인정보 분산 저장
사용자의 생체 정보를 분산 저장하고 자동 암호화 알고리즘을 통해 데이터를 주기적으로 자동 암호화 변경하여 최고 수준의 데이터 보안을 사용자들에게 제공

비인가자 원천 차단
얼굴인식 생체 인증 기술을 활용하여 사용자의 얼굴을 실시간으로 분석하고 비인가자가 화면에 감지되면 자동으로 PC가 잠기는 보안 기능을 가동하여 민감한 데이터 노출을 방지

5. 기업 유형별 보안 위협 진단표

'만약 귀사가 아래의 A유형과 B유형에 동시에 해당한다면(예: 외부 개발자가 많은 금융 기관, 퇴사자 관리가 미흡한 첨단 기술 기업), 데이터 유출은 단순 사고가 아닌 '예견된 재앙'이다.

구분	A. 공격에 '취약한' 기업 유형
유형1	외부 인력 의존도가 높은 기업 (협력업체, 파견직, 외주 개발자)
특징	낮은 보안 의식 및 소속감 업무 편의상 과도한 접근 권한 부여
유형2	물리 보안 및 출입 통제가 미흡한 기업
특징	USB 등 저장매체 반입/반출 통제 부재 서버실 등 핵심 구역 접근 기록 관리 부실
유형3	이직이 잦고 내부 통제가 복잡한 기업
특징	퇴사자/휴면 계정 관리 실패 복잡한 권한 관리로 인한 추적 어려움
유형4	보안보다 편의를 우선하는 문화의 기업
특징	보안 정책 예외 만연 부실한 보안 교육 및 인식

구분	B. 유출 시 '타격이 큰' 기업 유형
유형1	금융 및 핀테크 기업 (고객 신뢰 붕괴, 막대한 규제 및 소송)
보유 데이터	고객 자산 정보, 결제 정보 등 민감 데이터 전자금융거래법 등 강력한 법적 규제 대상
유형2	첨단 기술 및 제조업 (핵심 경쟁력 상실, 생존 위협)
보유 데이터	반도체 설계도, 소스 코드, 생산 공정 데이터 기술 유출 시 미래 가치와 시장 지위 상실
유형3	의료 및 제약/바이오 기업 (초민감 정보 유출, R&D 가치 상실)
보유 데이터	개인 질병, 유전 정보 등 민감 정보 신약 개발, 임상 데이터 등 천문학적 가치
유형4	국가 기반 시설 및 공공 기관 (사회적 혼란 야기, 정부 신뢰도 하락)
보유 데이터	전력, 통신, 교통 등 국가 안보 데이터 대국민 개인정보 및 행정 데이터

(주)유니온바이오메트릭스
Sales Inquiry: 02.6488.3027 (ext.3202) / www.unionbiometrics.com / salesinquiry@unionbiometrics.com

6. 결론 및 정책제언: '네트워크 신뢰'의 종말 과 '신원 검증'으로의 전환

앞서 배경에서 설명했듯이 AI와 내부자에 의한 복합 위협은 '망분리만 하면 안전하다'는 기존의 믿음이 얼마나 큰 '구조적 보안 부채(Structural Security Debt)'였는지 증명하고 있다.

앞서 살펴본 주요 보안 사고들이 보여준 공통점은 명확하다. 모든 사고는 '신뢰받는 경계' 혹은 '인가된 내부자'라는 이름의 가장 약한 고리가 무너질 때 발생했다. AI가 사용자의 얼굴과 목소리를 흉내 내고(위협), 내부자가 실수하거나 악의를 품는(경로) 현실에서, '네트워크 분리'라는 정적인 방어벽은 더 이상 핵심 해법이 될 수 없다.

보안의 패러다임은 '신뢰할 수 없는 네트워크(Untrusted Network)'를 전제로, 데이터에 접근하는 '신원(Identity)'을 지속적으로 검증하는 제로 트러스트로 반드시 전환해야 한다.

유니온바이오메트릭스의 UBio-Connect ezPass는 이러한 시대적 요구에 맞춰, 안티스푸핑 생체인증과 물리-논리 보안 융합을 통해 제로 트러스트의 핵심 원칙(Always Verify, Context-Aware)을 구현하는 가장 실질적인 기술이다. 이는 '인가된 사용자'라는 명목상의 신뢰가 아닌, '지금 접근하는 바로 그 사람(The Right Person)'을 실시간으로 검증하여 망분리 환경의 근본적인 취약성을 보완한다

- **데이터 리소스:**

- CNN, SCMP 등. (2024). "Hong Kong 'deepfake' scam sees finance worker pay out $25.6 million after video call."
- IBM. (2023). Cost of a Data Breach Report 2023.
- Ponemon Institute. (2023). 2023 Cost of Insider Threats Global Report.
- 산업기밀보호센터(NCISE) 및 경찰청 산업기술유출수사대 통계.
- Trend Micro. (2022). "Quarter of Healthcare Ransomware Victims Forced to Halt Operations."
- 캐치시큐. (2024). "2024년 상반기 공공기관 개인정보 유출 사고 얼마나 발생했을까?"
- Fortune Business Insights. (2024). "Physical Security Market Size, Share | Industry Trends [2032]."
- The Guardian. (2023). "Report: 'massive' Tesla leak reveals data breaches, thousands of safety complaints."
- ESET. (2024). "Mind the (air) gap: GoldenJackal gooses government guardrails."
- 보안뉴스, 연합뉴스 등. (2014-2016).

- **정책 제언: 고위험 환경에서의 표준 의무화**

1 제로 트러스트 기반 통합 신원 인증 도입

AI와 내부자 위협에 대응하기 위해, 망분리 환경의 '내부망' 접속 시 단순 ID/PW가 아닌 안티스푸핑이 적용된 생체인식(얼굴) 기반의 사용자 신원 검증(Always Verify)을 의무화해야 한다.

2 물리-논리 보안 연동(Context-Aware)

데이터센터, 서버실 등 핵심 구역의 물리적 출입자와 시스템 논리적 접속자 정보의 교차 검증 체계를(예: UBio-Connect ezPass + UBio-X Face) 구축하여 '상황 인식' 기반의 보안을 강화해야 한다.

3 제로 트러스트 아키텍처로의 전환

"내부망은 안전하다"는 2세대 경계형 보안의 가정을 폐기하고, 모든 접근에 대해 '최소 권한의 원칙(Least Privilege)'을 적용하며 지속적인 모니터링 및 감사 체계를 수립해야 한다.

(주)유니온바이오메트릭스

Sales Inquiry: 02.6488.3027 (ext.3202) / www.unionbiometrics.com / salesinquiry@unionbiometrics.com