GITSN (주)지슨

# 무선백도어 해킹 대응 솔루션

AI시대, 내부망 보호를 위한 제로트러스트 기반
24시간 상시 탐지 시스템


**지슨의 무선백도어 해킹 보안 제품**은 무선 주파수 통신으로 타겟 시스템에 원격 접속하여 데이터를 탈취하거나 시스템을 붕괴시키는 **신종 해킹 방식에 대응하는 솔루션**입니다.

# 무선 스파이칩 관련 보안 위협 급증에 따른 강화된 법적·정책적 보안 조치

## 법적 근거 및 기준

**「정보통신망 이용촉진 및 정보보호 등에 관한 법률」2024. 1. 23. 개정**

제48조(정보통신망 침해행위 등의 금지) ④ 누구든지 정당한 사유 없이 정보통신망의 **정상적인 보호·인증 절차를 우회하여 정보통신망에 접근**할 수 있도록 하는 프로그램이나 **기술적 장치** 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하거나 이를 전달·유포하여서는 아니 된다. <신설 2024. 1. 23.>

**하드웨어 백도어**

## 보안 관리 및 운영 지침

**「전자금융감독규정」2025. 2. 5.**

제15조(해킹 등 방지대책) ①금융회사 또는 전자금융 업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해 행위로부터 방지하기 위하여 다음 각 호의 대책을 수립, 운용하여야 한다. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영

**「'금융분야 망분리 개선 로드맵'에 따른 보완 대책」2024. 8. 13. 발표**

물리적 망분리 규제 완화에 따른 보완책으로 '단말기 보완' 및 '외부 통신 통제'를 대폭 강화해야 함

**[입법 동향] 디지털 금융안전법(가칭) 제정 추진 2026. 예정**

중대한 해킹 사고 발생 시 징벌적 과징금 부과 및 경영진 책임 명문화, 외부 업체 납품 장비(공급망)에 숨겨진 백도어 등 취약점 점검 의무화(제3자 리스크 관리 강화) 등

## 국가 점검 및 대응 동향

**금융권 무선백도어 해킹 공격 관련 질의 및 대비책 마련 촉구**

국정감사 정무위원회, 금융감독원 감사中 (2024.10.17)

**무선백도어 해킹 관련 질의 및 ISMS 등 인증 항목 검토 및 대비책 마련 촉구**

국정감사 과학기술정보방송통신위원회 과학기술정보통신부 감사中 (2025.10.13)

**금융감독원에서 모든 금융기관 대상으로 "무선백도어 방어수단" 현황에 대해 CPC를 통해 자료 제출 요구**

금융감독원 자료제출요구서 (2024년, 2025년)

# 내부망을 노리는 최신 위협, 무선백도어 해킹

- **무선백도어 해킹 :** 통신 모듈과 초소형 CPU 칩으로 구성된 **무선 스파이칩** 을 활용한 신종 해킹
  - 공급망 해킹 또는 하드웨어 백도어 해킹으로도 불리우며, 반입된 **무선 스파이칩의 무선주파수 통신을 통해 데이터 탈취 또는 시스템 셧다운**
  - 망분리 보안 무력화, WIPS(무선 침입방지 시스템)·방화벽 등 기존 보안체계 우회


(출처) 블룸버그 비즈니스위크

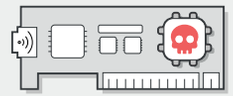
# 무선백도어 해킹 관련 사례

## USB 장치

**2014년 -** 미국 국가안보국(NSA)이 USB 장치(COTTONMOUTH-1)를 통해
악성 소프트웨어 업로드, 장치가 발산하는 무선주파수로 백도어 활성화

→ 전 세계 10만대의 PC에 소프트웨어를 심어 정보를 빼내거나 사이버 공격에 활용

## 외장 연결 보드

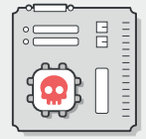


**2022년 -** 현역대위가 무선백도어 장치(포이즌 탭)로 한국군 합동지휘통제체계 서버 해킹 시도

**2025년 -** 해커가 은행 ATM 네트워크에 소형 PC인 라즈베리파이 기기를 연결 후 현금 인출 시도

→ 무선주파수 통신을 통해 기존 네트워크 보안(방화벽 등)을 우회해 내부망에 침투한 사례

## 공급망 보드



**2024년 -** 미국 항구 내 중국산(ZPMC) 크레인에서 요청하지 않은 통신장치 발견

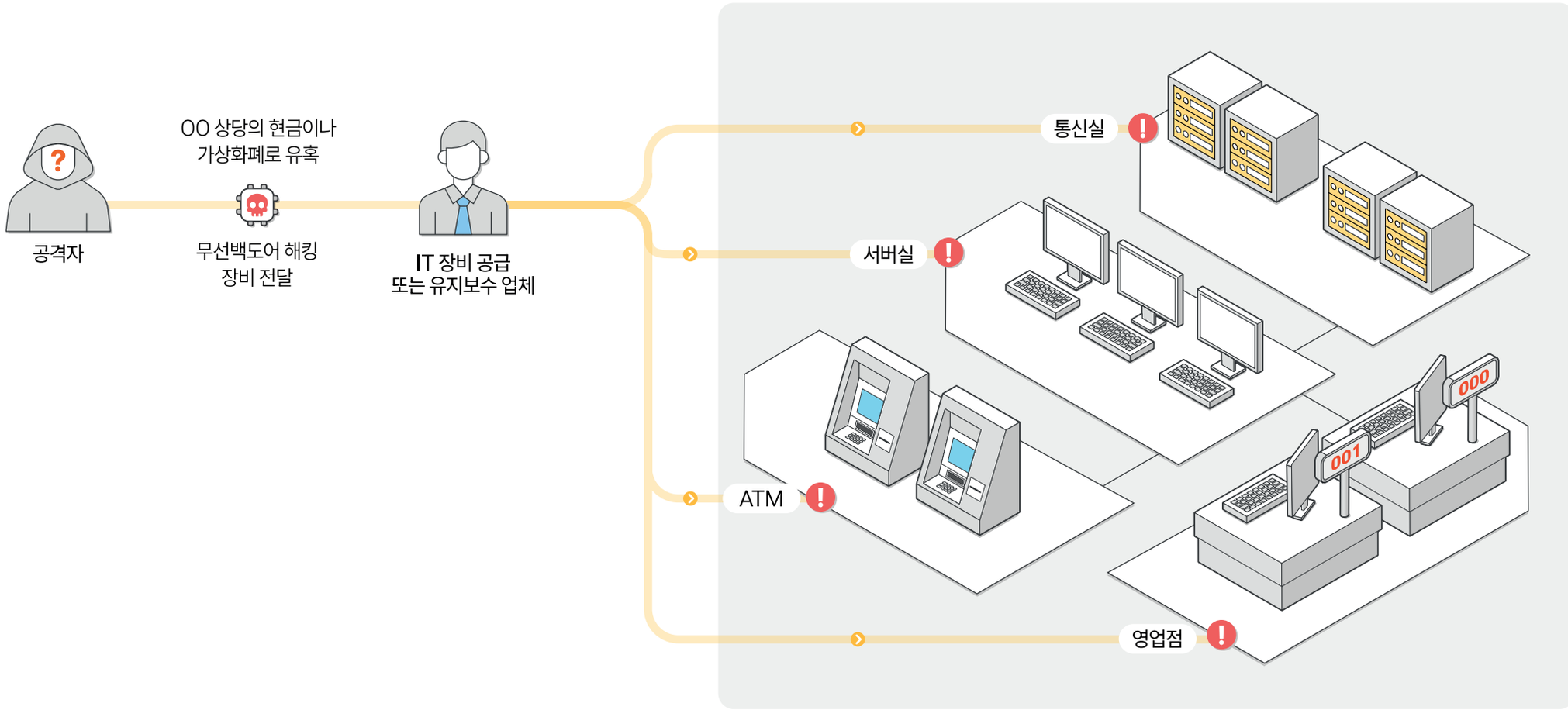
**2025년 -** 美에너지부, 중국산 태양광 인버터에서 제품 설명서에 명시되지 않은 통신장치 발견

- EU, 노르웨이, 영국, 이스라엘 등 중국산 전기차(관용차량, 버스)에서 비인가 통신장치 발견

→ 방화벽을 우회해 중국과 직접 통신 가능한 기능을 포함, 원격 제어·중단·변경 등 교란 가능성 제기

# 무선백도어 해킹에 노출된 주요 장소들

- 고객 및 경영 관련 주요 데이터가 저장된 **데이터센터**
- 장비 도입, 테스트, 유지관리 등으로 외주 인력이 자주 출입하는 **본사 및 지역 IT 관리 구역**(서버실·통신실 등)
- 유지보수나 장비 교체를 위해 외부 인력이 방문하는 **영업점, 해외법인·지점 및 365코너**(ATM 설치 구역)



무선백도어 해킹 탐지 시스템

# Alpha-H


조달청 우수제품 지정

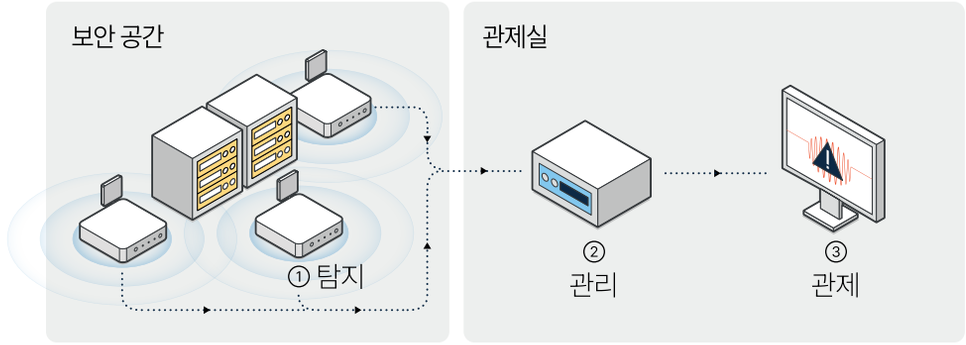
중소벤처기업부 성능인증

## 무선백도어 해킹 대응 솔루션

데이터 센터, 서버실, 집무실 등에 침투되어
망분리 체계를 무력화시키는 무선백도어를 실시간 탐지

- 24/365 상시 탐지
- 신호원 위치 추정
- 다수의 단말기 통합 관제
- 통합 관제 프로그램

운용 프로세스



# 무선백도어 해킹 대응 솔루션 도입 기대효과

보안은 비용이 아닌, 지속 가능한 성장을 위한 가장 확실한 투자입니다.

**50×**
투자 대비 복구 비용 절감 효과

**100%**
국감·감독기관 지적 완벽 대응

**ESG**
거버넌스 부문 핵심 가점

## 압도적 경제성 & 리스크 제로화

- **예산 효율성**: 사후 복구 비용 대비 1/50 수준의 합리적인 사전 예방 투자

- **비즈니스 연속성**: 24시간 무중단 탐지로 핵심 시스템 가동 중단 리스크 완전 제거

- **손실 방지**: 단 1건의 사고 차단만으로도 ROI(투자회수) 200% 달성 가능

## 전략적 경영 보호 & 책임방어

- 경영진 보호 : 최신 위협 대응력 입증으로 경영진의 선관주의 의무 이행 증명

- 규제 준수 : 정보통신망법(2024년 개정), 전자금융감독 규정 등 대응 가능 유일한 솔루션

- 혁신 기반 : AI·클라우드 등 디지털 신사업 추진을 위한 안전한 기반 환경 확보

## 지속 가능 가치 & 신뢰 자본

- **투자자 신뢰**: 국민연금 등 주요 기관 투자자의 리스크 평가에 긍정적 시그널

- ESG 신뢰자본 축적 : 보안 무사고로 금융사의 차별화된 무형 가치 제고

- **시장 리더십**: 업계 내 '가장 안전한 금융사'로서의 독보적 포지셔닝 구축

[금융권 보안 사고 리스크: IBM Security 2024]
- 피해 규모: 평균 72억 원 손실, 복구 기간 219일 소요
- 비용 비교: 사후 복구 비용이 예방 투자비(약 1.5억원(솔루션 도입 비용))보다 약 50배 더 발생

[ROSI(보안 투자 회수율) 시뮬레이션: IBM Security 2024 기준]
- 연간 예상 손실: 7.2억 원 (사고 피해 72억 × 확률 10%)
- 투자 효과: 2.4억 원 투자 시 ROI 200% 달성

## “가장 취약한 보안 수준이 전체 보안 수준을 결정한다.”

기존 시그니처 기반 탐지 방식으로는
새로운 유형의 침해 사고에 대응할 수 없습니다.
이미 위협이 내부에 있다고 전제하고,
모니터링, 행동 기반 방식으로 대응해야 합니다.

무선백도어 해킹은 외부가 아닌 ‘내부’에서 침투 합니다.
Alpha-H는 무선백도어 해킹에 유일하게 대응 가능한 솔루션입니다.


최소의 법칙(Law of Minimum) - 리비히

GITSN (주)지슨

문의 : 전략사업본부, 02.852.3560, sales@gitsn.com