

# SECURITY DAILY REPORT

MSS(Managed Security Service)



24x365



Security



AI analytics

## 1. 보안동향

한국제로트러스트위원회 배환국 의장, “제로트러스트는 새로운 보안 패러다임”

### [미리보기]

‘팀 ZeroTrust, KOZETA 에서 제시하는 제로트러스트 구축전략 컨퍼런스’ 개최제로트러스트 가이드라인 2.0 논의, 기업들의 다양한 구축전략 볼 수 있는 자리로 마련배환국 의장, “국내 제로트러스트 활성화에 필요한 의견 제시하는데 힘쓸 것”한국정보보호산업협회 조영철 회장, “다양한 기업이 협업하는 문화 구축하는 중”[보안뉴스 김경애 기자] 제로트러스트

[바로가기](#)

[속보] 금융보안원, 비상계엄 이후 비상상황 대응 긴급 임원 회의

### [미리보기]

비상상황 대응 긴급 임원 회의 개최, 금융시스템 안전성 강화에 총력[보안뉴스 김경애 기자] 금융보안원은 4 일(수) 김철웅 원장이 주재하는 긴급 임원 회의를 개최했다. 이는 비상계엄 이후 사회적 혼란 상황에서 국가 배후 세력 등 외부 공격이 발생할 가능성이 있는 만큼, 금융권에 미치는 영향 등을 분석하고 보안관제 등 대응 상황 점검에 나선 것이다. 금융보안원

[바로가기](#)

## SGA, 한화시스템·한국교원대와 AI 에듀테크 플랫폼 활성화 상호협력 업무협약 체결

### [미리보기]

SGA·한화시스템·한국교원대학교, AI 기반 교육 플랫폼 개발 등 공동사업 추진 예정교육과정·정책·신기술 전문성 기반 교육 관련 사업에서 긍정적 시너지 창출 기대 [보안뉴스 박은주 기자] 교육정보화 전문기업 'SGA(대표 박재한)'가 한화시스템(대표 손재일), 한국교원대학교(총장 차우규)와 AI 에듀테크 선도를 위한 플랫폼 활성화 업무협약을 체결했다고 4 일

[바로가기](#)

## 아울시스템즈 DB 암호화 솔루션 PrivacyDB, 중소기업기술마켓 인증제품으로 지정

### [미리보기]

PrivacyDB 로 중소기업 기술 혁신과 산업 발전에 기여할 발판 마련 [보안뉴스 박은주 기자] 데이터베이스 보안 전문기업 아울시스템즈(대표 강병승)는 자사의 DB 암호화 솔루션 PrivacyDB 가 중소·벤처기업을 위한 통합 기술마켓 플랫폼인 중소기업기술마켓 인증제품으로 지정됐다고 밝혔다. 이번 인증은 PrivacyDB 의 기술력과 제품 우수성을 공식적으로

[바로가기](#)

## 우리나라 사이버보안의 현재와 미래, 'KISA 사이버보안 성과 발표회'에서 듣는다

### [미리보기]

2025 년 사이버보안 10 대 이슈 및 트렌드 전망보안정책, 침해대응, 개인정보, 보안 산업, 디지털 안전 등 5 가지 키워드[보안뉴스 박은주 기자] 한국인터넷진흥원(원장 이상중, 이하 KISA)은 2024 년 KISA 의 사이버보안 주요 정책연구 및 사업성과 등을 이해관계자와 국민에게 공유하기 위한 'KISA 사이버보안 성과 발표회'를 12 월 11 일 전쟁기념관

[바로가기](#)

## 2. 보안권고문

### 美 CISA 발표 주요 Exploit 정보공유(Update. 2024-12-03)

#### [미리보기]

2024-12-24 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. North Grid Proself Enterprise/Standard, Gateway, and Mail Sanitize contain an improper restriction of XML External Entity (XXE) reference vulnerability, which could allow a remote, unauthenticated attacker to conduct an XXE attack. 2024-12-03 North Grid Proself Improper Restriction of XML External Entity (XEE) Reference Vulnerability North Grid CVE-2023-45727 2024-12-24 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. ProjectSend contains an improper authentication vulnerability that allows a remote, unauthenticated attacker to enable unauthorized modification of the application's configuration via crafted HTTP requests to options.php. Successful exploitation allows attackers to create accounts, upload webshells, and embed malicious JavaScript. 2024-12-03 ProjectSend Improper Authentication Vulnerability ProjectSend CVE-2024-11680 2024-12-24 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Multiple Zyxel firewalls contain a path traversal vulnerability in the web management interface that could allow an attacker to download or upload files via a crafted URL. 2024-12-03 Zyxel Multiple Firewalls Path Traversal Vulnerability Zyxel CVE-2024-11667

[바로가기](#)



주소 | 서울특별시 서초구 서초대로 255 고덕빌딩 2 층(06595)

전화 | 02-2105-4400 (영업문의-1 번, 보안관제문의-2 번, 기술문의-3 번)

팩스 | 02-2105-4456

영업문의 | [sales@eosec.co.kr](mailto:sales@eosec.co.kr) 보안관제 및 기술 문의 | [tech@eosec.co.kr](mailto:tech@eosec.co.kr)

©EYEON SECURITY All Right Reserved.