# 2025 사이버 위협 전망

Cyber Security Forecast 2025

AhnLab Genians IGLOO NSHC S2W PLAINBIT

SK 쉴더스 CISCO TALOS Google Microsoft TREND MICRO splunk> zscaler

과학기술정보통신부

KISA 한국인터넷진흥원

Contents

# 2025 사이버 위협 전망

Cyber Security Forecast 2025

## 1. 2024년 사이버 위협 사례 분석

1, 사이버 사기로 인한 국민 불편 및 금융피해 지속

2, SW 공급망 공격은 기본, 복합적인 공격 전술 사용

3, 랜섬 공격기법 고도화, 고객 정보 빌미로 삼중 갈취 공격 지속

## 2. 2025년 사이버 위협 전망

1, 공격자의 생성형 AI 활용 본격화

2, 디지털 융복합 시스템에 대한 사이버 위협 증가 예상

3, 글로벌 환경 변화에 따른 사이버 위협 증가 가능성

4, 무차별 디도스 공격 증가 예상

과학기술정보통신부

KISA 한국인터넷진흥원

# 2025년 사이버 위협 전망

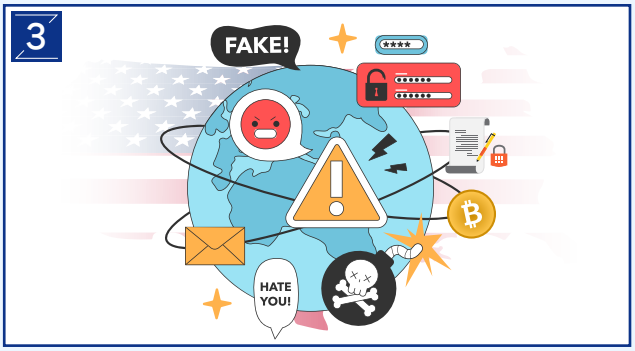
1


공격자의 생성형 AI 활용 본격화

2


디지털 융복합 시스템에 대한 사이버 위협 증가 예상

3




글로벌 환경 변화에 따른 사이버 위협 증가 가능성

4


무차별 디도스 공격 증가 예상

# 2024년 사이버 위협 사례 분석

1

사이버 사기로 인한
국민 불편 및 금융피해 지속

2

SW 공급망 공격은 기본,
복합적인 공격 전술 사용

3


랜섬 공격기법 고도화, 고객
정보 빌미로 삼중 갈취 공격 지속

AhnLab Genians IGLOO NSHC S2W PLAINBIT
SK 쉴더스 CISCO TALOS Google Microsoft TREND MICRO splunk> zscaler

# 2025 사이버 보안 위협 분석과 전망

국가의 지원을 받는 해킹그룹의 활동 증가, 생성형 인공지능의 악용 가능성 증가 등 최근 사이버 위협은 더욱 지능화, 고도화되고 있다. 이러한 사이버 위협에 체계적으로 대응하기 위해서는 올 한 해 동안 발생한 사이버 침해사고를 면밀하게 분석하고, 향후 발생할 수 있는 위협을 전망하여 기업 내부의 대비 태세를 정비할 필요가 있다.

이에 과학기술정보통신부(이하 과기정통부)와 한국인터넷진흥원(이하 KISA)은 국내·외 사이버 위협 인텔리전스 네트워크*와 함께 올 한 해 발생 했던 사이버 침해사고를 중심으로 3가지 사례를(피싱, SW공급망, 랜섬웨어)을 선정·분석하였고, 2025년도에 예상되는 주요 사이버 위협으로 국민의 일상생활과 다양한 산업분야에 가장 큰 영향을 미치고 있는 ① 인공지능(AI), ② 디지털 융합 확산, 우크라이나-러시아 전쟁 등 ③ 글로벌 환경 변화와 관련된 사이버 위협 및 꾸준히 지속되고 있는 ④ 분산 서비스 거부(DDoS) 공격을 선정하였다.

* 최신 사이버 위협 정보공유 및 침해사고 공동 대응을 위해 KISA와 국내·외 보안업체가 운영하고 있는 협력 네트워크
  - (국내) 안랩, 지니언스, 이글루코퍼레이션, NSHC, S2W, SK쉴더스, 플레인비트
  - (해외) Cisco Talos, Google, Microsoft, Splunk, Trend Micro, Zscaler

본 보고서를 통해 기업 보안 담당자들은 앞으로도 지속될 사이버 위협에 대해 다시 한 번 내부 보안 상황을 재점검 해보고 다가 올 위협에 체계적인 보안관리와 선제적인 대응 방안을 수립하여 피해 예방에 도움이 될 수 있기를 기대한다.

# 01

# 2024년 사이버 위협 사례 분석

사이버 위협 전망 2025

1, 사이버 사기로 인한 국민 불편 및 금융피해 지속

2, SW 공급망 공격은 기본, 복합적인 공격 전술 사용

3, 랜섬 공격기법 고도화, 고객 정보 빌미로 삼중 갈취 공격 지속

# 1 사이버 사기로 인한 국민 불편 및 금융피해 지속

Cyber Security Forecast 2025

- 주식투자 유도, 티몬·위메프 환불 등 사회적 이슈를 악용한 스미싱 공격 기승
- QR코드 사용 급증으로 신종 사이버 수법 큐싱(정보무늬 사기) 주의

올 한 해 주식투자 유도, 유명스타 콘서트, 티몬·위메프 환불, 수학능력시험 등 사회적 이슈를 악용한 불법스팸, 스미싱(Smishing), 큐싱(Qshing)* 등 사이버 사기 건수가 대폭 증가하여 서민금융 피해가 지속되고 있다.

* 정보무늬(QR코드)와 피싱(Phishing)의 합성어, 악성코드나 유해 웹사이트에 연결되는 정보무늬를 촬영하면 스마트폰에 악성앱이 설치되어 개인 금융 정보를 탈취하거나 소액결제를 유도

**주요 사고 사례 및 동향**

- 기업 문자발송 시스템 및 계정 해킹을 통한 스팸문자 발송 주의(5월)
- '티몬·위메프' 환불 미끼, 스미싱 주의··· 금융·개인정보 털린다(8월)
- 과태료 내려고 QR코드 열었더니... '큐싱' 피해 당부 주의보(10월)
- 정부, 불법 쓰레기 편지(스팸) 방지 종합대책 발표(11월)

올해 상반기는 스팸과 스미싱이 급격하게 증가했었다. 문자재발송사업자의 큰폭 증가, 스팸과 스미싱 신고방법의 편리성 제고 외에 해킹을 통한 스팸 발송 사례도 있었다. 지난 5월, 특정 기업의 문자 발송 시스템이 해킹되어 성인 및 도박 사이트 방문을 유도하는 대량의 스팸 문자가 발송되는 사건이 발생하였다. 공격자가 문자 발송 서버의 웹 취약점(파일 업로드, SQL 인젝션)이나 취약한 전사적 자원 관리(ERP) 시스템의 관리자 계정, 문자 발송 솔루션의 취약점을 악용해 시스템을 장악한 사례이다. 이에 대응할 수 있도록 각 기업은 웹 서버의

취약점을 신속히 제거하고 관리자 계정에 대한 보안 조치를 강화해야 하며, 솔루션 제조사들은 자체 보안 점검을 통해 잠재적인 취약점을 사전에 제거해야 한다.

또한 사회적 이슈를 악용한 스미싱 공격이 여전히 기승을 부리고 있다. 최근에는 국내 이커머스의 미정산 및 환불 지연 사태를 악용한 스미싱이 유포된 적도 있었다. 스미싱 문자에 포함된 URL을 클릭하면 악성 앱 설치를 유도하거나, 피싱 페이지로 연결되어 아이디와 비밀번호 같은 개인정보가 탈취될 위험이 있다. 악성 앱이 설치될 경우, 스마트폰 내 연락처나 공동인증서와 같은 민감한 정보가 유출되어 2차 피해로 이어질 가능성도 있다.

QR코드는 정보를 빠르게 인식할 수 있도록 설계된 2차원 바코드로, 주로 스마트폰에서 복잡한 인터넷 주소 입력을 간소화하거나 앱 설치 및 실행을 돕는 데 활용된다. 최근 공유형 킥보드, 전단지, 상점 홍보물 등에서 QR코드 사용이 급증하고 있다. 국내에서는 공유형 킥보드에 부착된 정상 QR코드 위에 큐싱 스티커를 덧붙이거나, 피싱 메일과 온라인 광고에 큐싱 링크를 삽입해 악성 앱 설치를 유도하는 피해 사례가 발생하고 있다. QR코드는 외관만으로 진위를 판단하기 어렵기 때문에 사용자의 각별한 주의가 요구된다.

과기정통부(KISA)와 관계부처는 신종 사이버 사기 수법인 큐싱을 선제적으로 예방하기 위해 일상생활에서 QR코드를 자주 이용하는 청소년들을 대상으로 정보무늬 사기(큐싱) 예방 수칙과 대응 요령 등 홍보를 강화하였다.

또한, 지난 11월 과기정통부(KISA)와 방송통신위원회는 “불법스팸 방지 종합대책”으로 ▲불법스팸  단계에서 부당 이익 환수, ▲대량문자 유통시장 정상화, ▲불법스팸 발송 차단 강화, ▲불법스팸 수신 차단, ▲스팸 차단 거버넌스 구축 등 총 5개의 추진 전략과 12개의 세부 추진과제 발표를 통해  불법스팸 근절과 방지 전략을 마련하였다.

스미싱, 보이스피싱, 피싱 사이트 등 사이버 사기가 의심될 경우, KISA에서 운영하는 보호나라(www.boho.or.kr) → ‘스미싱 확인서비스’나 ‘전기통신금융사기 통합신고대응센터(☏112)’를 통해 확인하고 신고할 수 있다.

# 2 SW 공급망 공격은 기본, 복합적인 공격 전술 사용

Cyber Security Forecast 2025

- 리눅스 오픈소스 데이터 압축 유틸리티(XZ Utils) 최신버전에서 악성코드 발견
- 다양한 공격 기법(멀버타이징, 제로데이 등)이 결합된 복합적인 사이버 공격 사례 발생

피해 사실조차 알아차리기 어려운 은밀한 소프트웨어(SW) 공급망 공격이 계속되고 있다. SW 공급망 공격은 신뢰받는 소프트웨어와 업데이트 체계를 악용해 SW 개발-유통-이용 등 SW 공급망 전단계에서 광범위하게 악성코드를 유포하고 보안 프로그램의 탐지를 회피할 수 있어, 사이버 공격자들이 선호하는 방식 중 하나다. 특히 공격자들은 공격 대상의 보안 체계를 우회하기 위해 악성코드 삽입과 해킹을 융합하는 등 여러 공격 기법을 결합한 복합적인 전술을 활용하고 있다.

**주요 사고 사례 및 동향**

- 건설 관련 홈페이지의 보안 프로그램 설치 파일 변조(1월)
- 리눅스 오픈소스 압축 프로그램(XZ Utils) 최신버전에서 악성코드 발견(3월)
- 국내 무료 SW의 특정 토스트 팝업 광고 프로그램 악용(5월)

지난 3월, 리눅스 및 GNU 그룹에서 기본적으로 제공되는 데이터 압축 유틸리티(XZ Utils)의 최신 버전(5.60, 5.61)에서 백도어가 발견되었다. 공격자는 2021년부터 오픈소스 프로젝트에 참여하며 운영자와 신뢰를 쌓아 의도적으로 악성 코드를 삽입해 배포한 것으로 드러났다.

국내에서는 다양한 공격 기법이 결합된 복합적인 사이버 공격 사례가 다수 발생하고 있다. 올해 초, 국내 건설기술 분야의 한 홈페이지에서 로그인을 위해 필요한 보안 프로그램 설치 파일이 변조되어 악성코드가 유포된 사건이 발생했다. 공격자는 공격 대상이 자주 방문하는 홈페이지에 잠복해 악성코드를 퍼뜨리는 워터링홀(Watering Hole) 공격 기법과 함께, 악성코드를 이용하여 국내 소프트웨어 개발사의 유효한 디지털 인증서를 탈취해서 믿을 수 있는 서비스로 위장하는 방법으로 백신을 회피하여 보안 프로그램 설치 파일을 변조하는 방식을 결합한 사이버 공격을 감행하였다.

또한, 지난 5월에는 특정 토스트* 광고 프로그램이 광고 콘텐츠를 내려받을 때 지원이 종료된 취약한 인터넷 익스플로러 모듈을 사용한다는 점을 노리고, 국내 특정 기업의 토스트 팝업 광고 프로그램을 악용한 대규모 사이버 공격을 일으켰다. 공격자는 온라인 광고를 통해 악성코드를 유포하는 멀버타이징(Malvertising) 공격 기법과 지원이 종료된 마이크로소프트의 윈도우 익스플로러 브라우저의 제로데이** 취약점을 결합하여 사이버 공격에 악용하였다.

* 사용자의 화면에 일시적으로 표시되는 작고 간단한 메시지 형태의 팝업 광고

** SW의 보안 취약점이 알려지지 않았거나 제조사의 보안패치가 공개되지 않은 상태

지난 5월, 과기정통부(KISA), 국가정보원, 디지털플랫폼정부위원회가 합동으로 발표한 'SW 공급망 보안 가이드라인 1.0'을 통해 SW 공급망 보안관리 체계 확산에 대한 기반을 마련하였고, 2025년부터는 'SBOM* 기반의 SW 공급망 보안관리체계'를 체계적으로 보급해나갈 계획이다.

* SW 구성요소 명세서(SW Bill of Materials)

# 3 랜섬 공격기법 고도화, 고객 정보 빌미로 삼중 갈취 공격 지속

Cyber Security Forecast 2025

- 파일 암호화, 기밀 자료 유출·공개, 디도스 공격 등 랜섬웨어 그룹 3중 갈취 전술 사용
- 피해 시스템 내부의 합법적 자원(SW)을 공격에 악용하는 자급자족(LoTL) 기법 사용

랜섬웨어는 전 세계 모든 국가와 산업에 심각한 영향을 미치는 사이버 범죄이다. 랜섬웨어 그룹의 경제적 동기(높은 수익성, 투자수익률(ROI) 등)는  랜섬웨어가 효과적인 사이버 공격기법으로 여전히 활용될 수 있는 기반이 되고 있으며, 보안 장비 탐지 우회와 ① 데이터 암호화에 그치지 않고, ② 기업의 기밀 자료를 유출하고 공개를 협박하며, ③ 피해 기업에 대해 디도스(DDoS) 공격 등 3중 갈취 전술을 사용하는 고도화된 공격 기법으로 기업과 이용자들을 압박하고 있다.

## 주요 사고 사례 및 동향

- 1분기 랜섬웨어 공격 23% 증가... 보안 시스템 우회·합법적 도구 악용 증가(5월)
- 해커 "법무법인 해킹 후, 탈취한 고객정보 공개 협박" 비트코인 요구(9월)
- 상반기 랜섬웨어 피해 비용 평균 20억···진입장벽 낮아지고 방식 고도화(11월)

또한 최근 랜섬웨어는 피해 시스템 내부의 합법적인 자원(SW)을 공격에 악용하는 LoTL(Living off the Land)* 기법도 사용하고 있다. LoTL 기법은 윈도우나 유닉스 운영체제에서 기본적으로 제공하는 SW를 악용함으로써 정상적으로 발생하는 트래픽과 공격자의 트래픽 구분을 어렵게 만들며, 내부 시스템으로의 전파 및 횡적이동(Lateral Movement)** 시 보안 장비의 탐지 우회 가능성을 높여 공격 지속 시간을 연장시킨다.

* 자급자족 공격으로도 불리며, 피해 컴퓨터나 네트워크에 이미 설치된 여러 자원(표준 시스템 도구와 명령어)을 악용하여 공격하는 기법

** 공격자가 초기 접근 권한을 획득한 후, 민감한 데이터나 고가 자산을 찾기 위해 기업망 내부에서 더 깊이 이동하는 것을 의미

랜섬웨어는 공격자들은 피해 기업의 이해 관계자(협력사, 고객 등)와 직접 접촉하여 랜섬웨어 피해 사실을 알리고, 유출된 정보를 이용해 추가적으로 몸값을 요구한다. 이로 인해 피해 기업의 평판과 신뢰도가 심각하게 훼손되며, 랜섬웨어의 피해 범위는 제3자에게까지 확산될 수 있다.

랜섬웨어 공격에 대비하기 위해 각 기업은 공격 표면 관리(ASM, Attack Surface Management), 내부 시스템 보안 점검, 백업 등을 강화해야 한다. 또한, 내부 시스템이나 단말기에 저장된 민감한 고객 정보(예: 환자 정보, 의뢰서, 계약서 등)에 대한 안전 조치를 점검하고 강화하는 것이 필수적이다. 이를 통해 공격에 대한 취약점을 최소화하고, 데이터 유출이나 손상을 방지할 수 있다.

KISA는 랜섬웨어 대응 역량이 부족한 지역 중소 영세기업을 대상으로 무상 보안취약점 점검과 서버 보안점검(내서버돌보미)을 지원 중이며, 한국정보보호산업협회(KISIA)도 랜섬웨어 대응 보안솔루션 패키지 지원사업을 진행 중에 있어, 랜섬웨어 예방 대책이 필요한 기업은 언제든지 도움을 받을 수 있다.

# 02

# 2025년 사이버 위협 전망

사이버 위협 전망 2025

1, 공격자의 생성형 AI 활용 본격화

2, 디지털 융복합 시스템에 대한 사이버 위협 증가 예상

3, 글로벌 환경 변화에 따른 사이버 위협 증가 가능성

4, 무차별 디도스 공격 증가 예상

# 1 공격자의 생성형 AI 활용 본격화

Cyber Security Forecast 2025

- 생성형 AI의 악용이 본격화되며 사이버 범죄 도구로 활용될 가능성 증가
- 기업의 안전한 생성형 AI 사용을 위해 보안 내재화, 보안 모니터링 체계 필요
- 사회적 갈등과 혼란을 부추기는 가짜뉴스 및 게시글을 통한 여론조작 우려

AI 기술의 빠른 발전으로 다양한 생성형 AI 모델과 서비스가 널리 보급되고 있다. 최근에는 저비용과 고효율을 갖춘 소형언어모델(sLLM)이 주목받으면서 AI 활용 범위가 넓어지고 있다. AI는 혁신과 편리함을 제공하지만, 활용 목적에 따라 악의적으로 사용될 수 있는 양면성을 가지고 있어서 주의가 필요하다.

생성형 AI를 악용한 사이버 위협은 더욱 늘어날 전망이다. 다크웹을 중심으로 FruadGPT(사기), WormGPT(악성코드 생성)와 같이 사이버 범죄에 특화된 악성 생성형 AI 모델이 다양하게 활용될 가능성이 있다. 또한, ChatGPT와 같은 검증된 서비스를 활용해 맞춤형 스피어피싱 메일을 작성하거나 공격 도구(취약점 탐색, 침투 등)를 개발하는 등의 악용 사례가 증가할 것으로 보인다.

또한 온라인에 공개된 사진과 동영상을 활용해 딥페이크(Deepfake)* 영상을 제작하고 이를 피해자 협박에 사용하는 사례도 증가할 것으로 예상된다.

* 인공지능 기술로 영상이나 이미지를 조작하여 사실처럼 보이게 만드는 합성 기술

최근 오픈AI에 따르면 러시아와 중국 등 일부 국가에서 인터넷상 여론 조작 및 정치적 선전을 위해 ChatGPT를 사용한 것으로 나타났다. AI를 활용해 정교하게 작성된 콘텐츠(허위정보)는 진위 구별이 어렵다. 허위정보는 가짜뉴스와 SNS(커뮤니티, 페이스북 등), 유튜브 등 인터넷을 통해 빠르게 확산되고 사람들의 판단에 영향을 끼친다. 이로 인해 특정 집단에 의한 여론조작으로 사회적 갈등과 혼란을 증가시킬 가능성이 크다.

생성형 AI는 기업의 효율과 혁신을 높이는 핵심 도구로 빠르게 자리잡고 있지만 보안 위협도 증가하고 있다. API 키 탈취, 데이터 유출, 플러그인 및 확장 프로그램 취약점 등 대표적인 위험 요소이다. 특히, 생성형 AI가 기업 내부 시스템과 연동되어 구축된 경우 민감 데이터의 노출과 오용 가능성이 커진다. 이에 따라 기업들은 안전한 생성형 AI 사용을 위해 도입 단계에서 보안을 내재화하고, 상시 모니터링 체계를 구축하여 지속적으로 관리해야 한다.

# 2 디지털 융복합 시스템에 대한 사이버 위협 증가 예상

Cyber Security Forecast 2025

- 스마트팜, 스마트축산 등 디지털 융복합 시스템을 겨냥한 사이버 공격 확대
- 5G 특화망(이음5G) 활용 확대에 따른 스마트시티 등 사이버 위협 우려
- 주기적인 공격 표면 관리(ASM)로 위험 요소 제거 및 IoT 기기의 보안 강화 필요

디지털 전환이 가속화되면서 정보통신기술(ICT)이 다양한 산업, 기술과 결합한 디지털 융복합 시스템 및 서비스가 확산되고 있다. 최근 언론에 보도되었던 국제 해킹 그룹의 국내 스마트팜* 농가에서 사용하는 원격제어 설비 시스템 해킹 사례는 디지털 융복합 시스템에 대한 사이버 위협이 현실화되고 있음을 보여준다.

* ICT와 농업이 결합해 농작물이나 가축을 자동으로 관리하고 최적의 환경을 조성하는 시스템

자율주행차, 스마트그리드, 스마트 빌딩, 스마트 교통 시스템 등 디지털 융합 기술을 포함한 스마트 시티가 전 세계적으로 확산되고 있다. 국내에서는 5G 특화망(이음5G)*의 활용이 제조, 의료, 자동차, 조선 분야로 확대되며 산업별 디지털 전환이 가속화되고 있다. 따라서 5G 특화망뿐만 아니라 이동통신망 기반의 융합 제품 및 서비스에 대한 보안 위협이 증가할 것으로 보인다.

* 특정 지역이나 한정된 공간에서 사용하기 위해 맞춤형으로 구축된 소규모 5G 네트워크


국민의 일상생활과 다양한 산업분야에서 사물인터넷(IoT) 기기가 빠르게 확산되고 있어서 IoT 기기에 대한 사이버 위협은 꾸준히 증가하고 있다. 공격자는 보안이 취약한 IoT 기기를 탐색한 후 악성코드를 감염시킨 후 디도스(DDoS) 공격과 같은 사이버 공격*에 봇넷(Botnet)**으로 악용한다. 또한, IP 카메라, 공유기가 해킹된 경우 개인 사생활이 외부에 노출되거나 범죄에 악용되는 등 심각한 피해를 초래할 수 있다.

* 공격자의 원격 명령에 따라 악성 행위를 수행하는 디지털 기기들의 집합

** 중국 해킹그룹 플랙스 타이푼은 전세계 26만대 IoT 장비로 구성된 봇넷 운영 적발(9월)

따라서 스마트시티, 디지털 융복합 시스템 및 서비스, IoT 기기 등에 대한 설계 및 개발 단계에서부터 사이버 위협으로부터 보호할 수 있는 보안을 내재화하여 안전한 운영 환경을 보장할 필요가 있다. 또한, 운영 중인 디지털 제품 및 서비스의 외부 접점을 지속적으로 모니터링하는 공격 표면 관리(ASM, Attack, Surface, Management)가 필수적이다. 사용자는 IoT 기기의 보안 설정을 강화하고, 보안 인증을 받은 기기를 사용하는 노력이 필요하다.

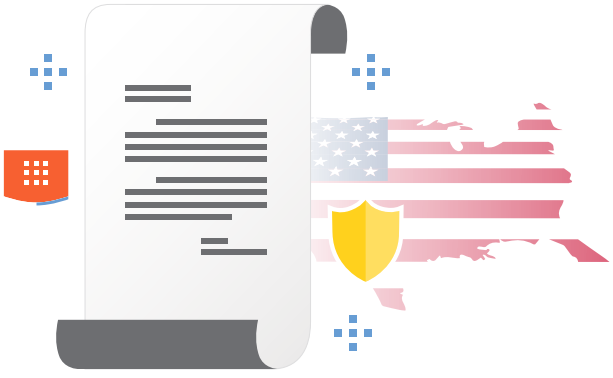
# 3 글로벌 환경 변화에 따른 사이버 위협 증가 가능성

Cyber Security Forecast 2025

- 트럼프 2기 행정부의 자국 우선주의, 가상자산 등 정책 변화에 따른 혼란 예상
- 국가배후 공격그룹과 핵티비스트 그룹의 공격 확대 우려
- 국가 안보실을 중심으로 민·관·군의 사이버 위협 대응 및 협력체계 강화 필요

2025년 1월에는 트럼프 2기 행정부의 출범이 예정되어 있다. 미국은 정부 개입을 최소화한 기술 완화 및 혁신, 자국 우선주의, 가상자산 규제 개선 등 정책변화가 예상된다. 우크라이나-러시아 전쟁 조기 종전에 대한 기대감으로 핵티비스트(Hacktivist: Hacking+activist)들의 공격 활동이 감소할 수 있으나, 이를 반대하는 측의 불만이 사이버위협으로 나타날 가능성도 있다.

국제정세의 변화는 핵티비스트들 활동에 직접적인 영향을 미칠 가능성이 크다. 글로벌 이슈, 전쟁, 정치적 갈등이 심화될 경우 핵티비스트 그룹은 사이버 공격을 통해 자신의 메시지를 전달하려 할 것이다. 특히, 특정 국가나 단체를 겨냥한 정교한 공격으로 이어질 가능성이 있다. 이러한 공격은 단순한 해킹을 넘어 사회적 혼란을 유발하고 국민들의 불안을 가중시킬 수 있다.



미국의 (친) 가상자산 정책으로 비트코인 가치 변동성이 확대되어 국가배후 공격그룹과 사이버 범죄 조직의 활동이 증가할 것으로 예상된다. 이들은 가상자산 사업자, 블록체인 기업, 가상자산 이용자, 가상자산 거래소 등을 대상으로 한 공격이 집중될 것으로 보인다. 특히, 이와 같은 가상자산 절취로 인한 경제적 피해가 발생할 수 있다.

또한 양자 기술, 인공지능 등 핵심 신흥 기술이 국가 경제 발전과 안보를 좌우하는 핵심 요소로 부상하면서, 원천 기술 보호의 중요성이 강조되고 있다. 보안 관리가 부족하거나 보안이 취약한 협력사를 노린 사이버 공격으로 원천 기술을 절취하려는 시도가 늘어날 것으로 예상된다.

따라서, 미국 정부의 친 가상자산 정책 변화는 국제 사이버 위협 환경에 새로운 변화를 가져올 것으로 보인다. 기업들은 사이버 보안 체계를 상시 점검하고 협력사의 보안 역량을 강화하여 대응 능력을 높여야 한다. 아울러, 국가안보실을 중심으로 민·관·군이 협력하여 공세적 방어 체계와 사이버 억지 전략을 통해 사회적 혼란을 최소화해야 한다.

# 4 무차별 디도스 공격 증가 예상

Cyber Security Forecast 2025

- 핵티비스트 등 다양한 목적의 무차별 디도스 공격 시도 증가 예상
- 보안에 취약한 라우터 장비 대상 디도스 봇넷 구축 우려
- KISA "디도스 사이버대피소"를 활용한 중소기업의 대응체계 강화 필요

디도스(DDoS·분산서비스거부) 공격은 악성코드에 감염된 단말기를 이용해 대규모 트래픽을 발생하여 기업에서 운영 중인 서버의 자원이나 네트워크 대역폭을 고갈시키는 전통적인 사이버 공격 방식이다. 이러한 공격 방식은 단순하지만 공격으로 인해 서비스 중단 시 기업의 서비스 신뢰도 하락이나 금전적인 피해 등이 발생한다.

올해 2월 국내에서 생방송으로 진행된 온라인 게임 대회의 중단이 대표적인 피해 사례이다. 올해 하반기에는 정치적 이념을 내세운 핵티비스트들의 정부기관 디도스 공격 등 다소 무차별적인 공격 성향도 보이고 있다. 특히, 다크웹*에서는 서비스형 디도스(DDoS-as-a-Service)** 도구가 판매되고 있어 기술적 지식이 부족한 사람도 손쉽게 디도스 공격을 시도할 수 있는 환경이 조성되고 있다.

* 일반적인 검색 엔진으로 접근할 수 없고, 특정 SW와 경로를 통해서만 접근 가능한 네트워크

** 누구나 비용을 지불하면 구축된 인프라를 통해 디도스 공격을 실행할 수 있는 서비스

2024년 한국인터넷진흥원에 신고 접수된 디도스 공격 침해사고 건수도 작년 대비 증가하는 추세(23% ↑, 24.11월 기준)를 보이고 있어 내년에는 디도스 공격에 대한 주의가 필요할 것으로 보인다. 특히 최근에는 취약한 라우터* 등 네트워크 장비를 악용하여 대규모의 네트워크 트래픽을 유발하거나 데이터 유출 등 공격 사례가 있으므로 기업들의 주의가 필요하며, 라우터와 같은 기업의 중요 네트워크 장비가 악성코드 감염 시 업무 장애나 중요 기밀 정보의 유출 등 심각한 피해가 발생할 수 있으므로 외부에 노출된 중요 네트워크 자산의 경우, 주기적인 보안패치와 비정상 네트워크 활동에 대해 모니터링 등을 강화해야 한다.

* 네트워크 간 데이터를 효율적으로 전달하고 인터넷 연결을 관리하는 장치

2024년도 디도스 증가 추세를 고려할 때, 2025년도에는 정부 공공 및 민간 기업을 가리지 않고 지속적인 증가 추세를 보일 것으로 보인다. 기업들은 디도스 공격이 발생하기 전에 인터넷서비스제공자와의 대응 협력 체계를 마련할 필요가 있으며, 정보보호 전문 인력 및 보안 설비 구축을 위한 투자 여력이 부족한 중소기업의 경우 피해 발생 시 아래 KISA의 "디도스 사이버대피소"이용방법을 참고하여 적극적으로 활용해 피해를 최소화할 수 있도록 준비해야 한다.

**※ 중소기업「디도스 사이버대피소」이용방법**

① 네이버 등 포탈 사이트에서 **'보호나라'** 를 검색

② 검색결과 화면에서 **'KISA 보호나라 (www.boho.or.kr)' 접속**

③ 메뉴 → 정보보호 서비스 → **온라인 신청 서비스 → DDoS 사이버 대피소 선택**

④ **'서비스 신청하기'를 통해 신청서 작성 및 제출강화 필요**

# 맺음말

Cyber Security Forecast 2025

국민의 일상생활과 다양한 산업분야에서 디지털 대전환의 가속화와 AI 기술을 기반으로 한 혁신은 우리의 삶을 보다 편리하게 변화시키고 있다. 그러나 이와 같은 디지털화는 사이버 공격 대상을 기업에서 가정, 기기까지 그 범위를 크게 확대하였다. 이에 따라 공격자들은 다양한 디지털 제품 또는 서비스의 보안 취약점을 악용하여 악성코드 감염, 계정 탈취를 시도하거나 생성형 AI 도구를 악용하여 더욱 은밀하고 예측하기 어려운 공격 수법을 지속적으로 개발 활용하면서 대응을 어렵게 만들 것으로 예상된다.

따라서 민간과 공공은 영역의 구분 없이 지금보다 더욱 유기적으로 사이버 위협을 탐지·공유·대응하는 협력체계를 강화하여 대규모 사이버 공격이나 변화하는 위협 환경에 효과적으로 대응할 수 있어야 한다. 또한 기업들은 랜섬웨어나 공급망 위협 사고 등에 대비하여 협력사와 함께하는 상시 모의침투 훈련이나 보안 교육 등 보다 적극적인 협력체계로 공급망 회복력을 강화하는 것이 더욱 필요할 것으로 분석된다.

마지막으로 기업들은 침해사고가 발생한 경우, 지체없이 과기정통부-KISA에 신고하여 신속하게 사고원인을 분석·제거하여 사업을 정상화하고 KISA의 실전형 모의침투 훈련, 보안 취약점 점검 등 다양한 예방 서비스를 통해 보안 방어력을 더욱 높이는 것이 중요할 것으로 생각된다.

# 2025 사이버 위협 전망

Cyber Security Forecast 2025

KISA 한국인터넷진흥원

**[나주본원]** 전라남도 나주시 진흥길 9 한국인터넷진흥원

**[서울청사]** 서울시 송파구 중대로 135 (가락동) IT벤처타워 TEL. 1544-5118 / 02-405-5118