AI 일상화 시대를 준비하는

# SW 공급망 보안 강화 로드맵

SW Supply Chain Security Enhancement Roadmap

**2026. 6.**

**관계부처 합동**

SW 공급망 보안 강화 로드맵

# Contents



Ⅰ 추진 배경 1

Ⅱ SW 공급망의 현황 및 위협 분석 2

Ⅲ 시사점 및 추진방향 5

Ⅳ 비전 및 추진전략 8

Ⅴ 세부 추진과제 9

가. 공급망 위협 예방 역량 강화 9

나. 공급망 위협 신속 탐지·대응 체계 마련 18

다. 정책·제도적 기반조성 25

Ⅵ 향후 추진 일정 31

Chapter 1

# 추진 배경

## 산업·사회 전반에 걸친 소프트웨어 활용 확대

- **AI·클라우드·IoT 등 디지털 기술의 일상화로 온·오프라인 경계가 허물어짐에 따라 SW가 산업·사회 혁신을 주도**
  - SW는 컴퓨터에서만이 아닌, 제조·교통·의료 등 다양한 산업과 일상 속 모든 곳에 융합되며 디지털 전환의 핵심 요소로 역할

## 복잡해지는 소프트웨어의 공급망과 고도화되는 사이버 위협

- **광범위한 취약점 탐지와 빠른 공격 속도가 특징인 AI 기반 공격이 SW 공급망 공격에 활용될 경우 기존 보안 체계로는 대응에 한계**
- **공개SW·타사SW 활용, 제3자 협력 개발 등 SW 개발·공급 역할의 분업화로 SW 공급망*은 지속적으로 확대·복잡화되는 추세**

  * SW 공급망 : 최종 SW 제품을 생산하는 사람, 장치, 시스템의 집합으로 개발자가 코드를 작성하는 때부터 해당 코드가 제품으로 생산된 후, 실행되는 때까지 일어나는 모든 일

- **해커들은 이를 악용하여 SW 개발·공급단계의 약한 고리를 노려 악성코드를 삽입하는 등의 'SW 공급망 공격'이 신종 위협으로 대두**
  - 개별 시스템·네트워크를 노린 기존의 위협과는 달리, SW 공급망 공격은 한 번의 공격으로 수많은 기업·개인에게 영향을 미치는 높은 파급력을 가짐

## 사이버 복원력 중심의 글로벌 정보보호 정책 패러다임 변화

- **美·EU 등 주요국은 SW 공급망 보안을 위해 개발·공급자의 책임 강화 및 지속적 사후관리 요구 등 '사이버 복원력' 확보를 위한 정책 추진**
  - 특히, 강도 높은 공급망 보안 항목들이 인증 요건에 추가되거나 검증된 제품만 납품되는 등 기업의 무역장벽으로 작용할 우려

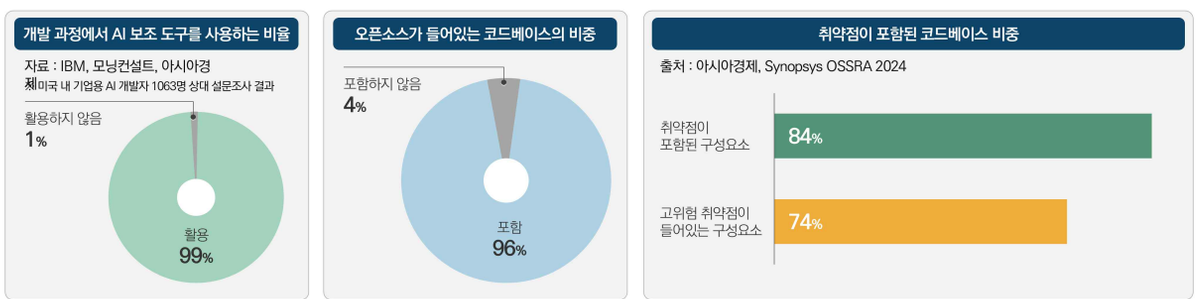
    ※ 글로벌 주요 보안기업 및 IT매체들도 SW 공급망 위협을 주요 보안 이슈로 선정하는 등 SW 공급망 보안의 중요성은 지속적으로 커질 전망

# Ⅱ SW 공급망의 현황 및 위협 분석

## 1 소프트웨어 개발·공급 환경의 변화와 복잡해진 공급망

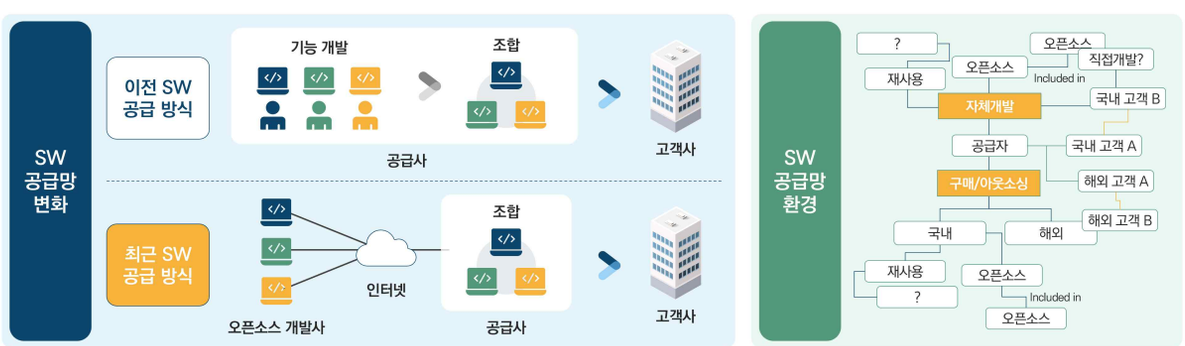
- **디지털 전환 가속화로 SW 개발은 자체 개발보다 외부 개발 SW(공개 SW, 제3자 개발 SW 등)를 적극적으로 활용하는 추세로 변화**
  - 외부 개발 SW의 활용은 생산성과 효율성을 높이고, 최신 기술에 대한 활용성 제고를 통해 혁신적 서비스 개발·확산에 기여

    ※ '25년 전 세계 생성형 AI 서비스 지출이 전년 대비 76.4% 증가한 총 6,440억 달러로 전망('25.4 가트너)




▲ 그림1. AI 도구 및 오픈소스 활용 통계 (출처 : 아시아경제, synopsys OSSRA 2024)

- **이러한 개발·공급 환경의 변화는 기존 단순하고 수직적이었던 SW 공급망을 복잡하고 상호 의존성이 높은 구조로 변화**



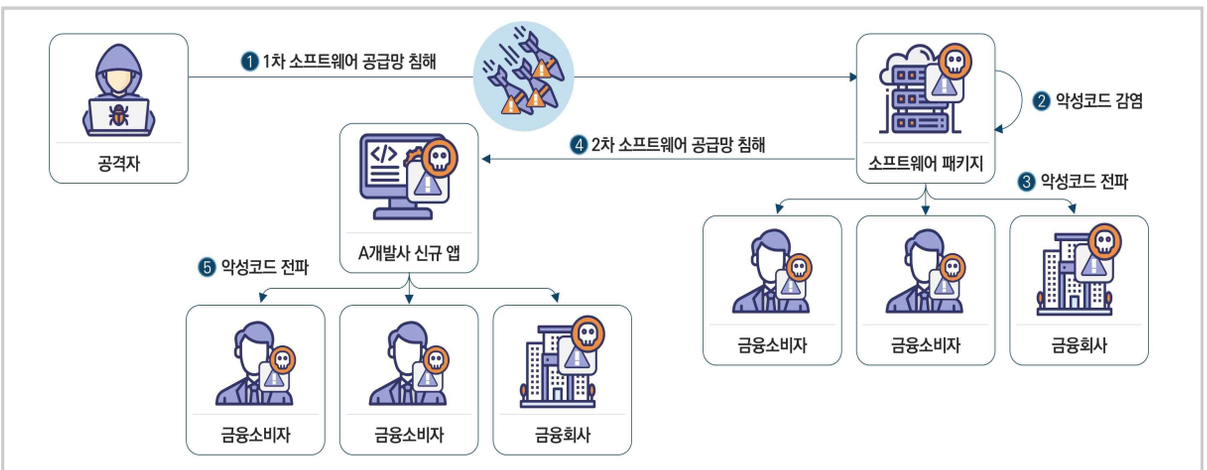

▲ 그림2. 소프트웨어 공급망 개념도

  - 적절한 검증·관리 없는 무분별한 외부 개발 SW의 활용은 SW의 개발주체가 불명확해지고 관리 책임 문제 및 공급망 위협으로 연결

    ※ 공개 SW 및 AI 모델이 생성한 코드 등은 누구나 자유롭게 코드에 접근할 수 있어, 악의적인 공격자가 취약점을 발견하고 악용할 위험성이 높음

## 2 고도화되는 소프트웨어 공급망 공격

- **특정 기업·서비스의 부실한 보안 관리를 악용하는 사이버 위협에서 SW 공급망의 보안 허점을 노린 공격으로 무게추가 이동 중**
  - 복잡해진 SW 공급망을 악용하여 은밀하고 교묘하게 침투하므로 '망 중심'의 기존 경계 기반 보안체계로는 초기 탐지·예방에 한계
  - 특히, 상대적으로 관리가 취약한 공개 SW 및 중소 개발 협력사 등의 보안 취약점을 노린 공급망 공격이 기승

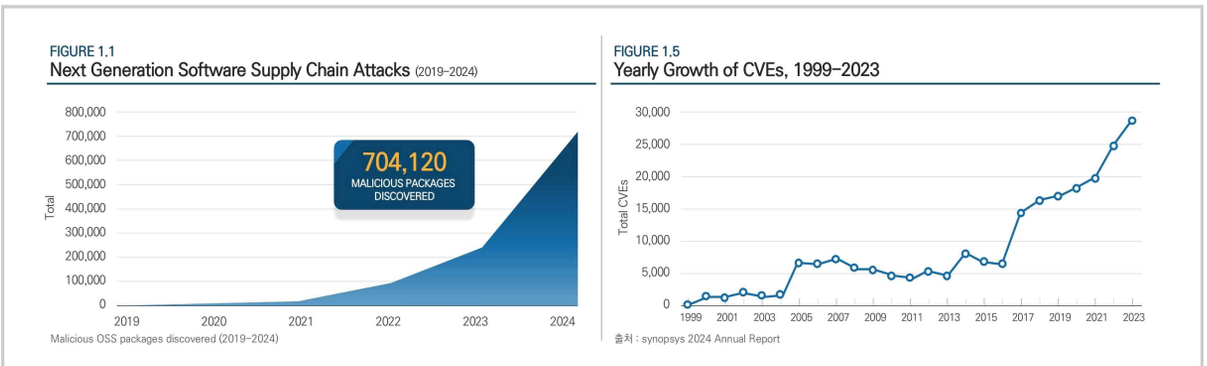



▲ 그림3. 공급망 공격 사례

- **SW 공급망 공격은 특정 기업·개인의 피해에 머무르지 않고, 해당 SW 이용자 전체의 연쇄적인 피해 확산으로 이어지는 파급력이 특징**

  * '24년 카스퍼스키 보안사고·대응·분석 보고서에 따르면, 사이버공격 지속 기간이 평균 253일로 최초 침투 후 8개월 이상 공격을 진행 → 초기 탐지가 어려운 공급망 위협

  ※ 소프트웨어 공급망 공격으로 인한 글로벌 피해액이 2023년 460억 달러(약 64조 원)에서 2031년 1,380억 달러(약 190조 원)로 증가할 것으로 추정(가트너, '24.6월)




▲ 그림4. 공급망 공격 통계 (출처 : synopsys 2024 Annual Report)

## 3 소프트웨어 공급망 보안을 위한 주요국 정책·제도

- **美·유럽 등 주요국들은 SW 공급망 보안 강화 정책 및 제도화를 추진하며, '사이버 복원력*' 확보를 위해 사이버보안의 변화 추진**

* 공급망 공격에 의한 시스템이나 서비스의 피해를 최소화하고 장애 또는 사고가 발생하기 이전 상태로 혹은 그에 준하는 상태로 신속하게 돌아가려는 역량

**참고 : 주요국 공급망 보안 정책**

| 국가 | 분야 | 주요 내용 |
|---|---|---|
| 미국 | 정부 납품 SW | • (안전한 개발 증명) 개발기업이 계약체결 시 안전하게 개발하였다는 것을 증명 (Secure SW Development Attestation Form)('23.6월~)<br>• (위험관리) 연방기관에 공급망 위험관리 관행(SP 800-161r1) 준수 요구('25.1월~) |
| | 의료 FDA | • (FDA 인허가) FDA 인허가 시 안전하게 개발하여 납품 목적으로, 안전한 제품 개발 보안 체계(SPDF) 또는 QS 규정 준수 요구('23.11월 시행) |
| EU | 디지털 요소가 포함된 제품 | • (사이버복원력법) 제조·수입·판매업체별 강도 높은 공급망 보안을 규정하고 모두에게 책임성을 부과하여 지속적인 관리·감독을 추진('27.12월 시행 예정) |

- 특히, SW 개발·공급기업의 책임을 강화하고, SBOM을 활용한 추적·관리* 의무화로 신속한 회복·대응 체계 마련을 추진

* 제품 출시 후 침해사고 혹은 보안 취약점 발생 시 이를 보완·수정하는 SW 업데이트 배포 등 즉각적인 조치와 같은 위험관리 요구

- **주요국의 SW 공급망 보안 정책·제도화는 향후 국내 디지털 기업의 잠재적인 해외 진출 장벽으로 작용할 우려**

◆ "미국 진출 준비를 위한 FDA 인·허가 단계에서 사이버보안 요건으로 SBOM을 요구받아 대응에 어려움이 있었음" (디지털 의료기기 제조기업)

◆ "기존 美 연방정부에 SW를 납품 중이었으나, SBOM 관리요건을 충족하지 못할 경우 차년도부터 계약이 불가함을 통보받음" (美 진출 정보보호기업)

◆ "글로벌 금융기업에 납품을 준비했으나, 사이버보안 요건을 충족시키지 못해 최종 계약까지 이어지지 못한 적이 있음" (인공지능 솔루션 개발기업)

# Ⅲ 시사점 및 추진 방향

**운영 단계에서 개발·공급 단계로 확장되는 사이버 위협**

⇨ 기획부터 유지보수까지 SW 공급망 全단계에 대한 보안 필요

**초기 탐지가 어렵고 연쇄적 피해로 이어지는 SW 공급망 위협**

⇨ SW 공급망의 투명성을 확보하고, 사고 복원력 강화 필요

**주요국의 SW 공급망 보안 제도화 움직임**

⇨ 국내 환경에 맞는 민·관 협력체계 및 제도 개선 등 필요

| 현황 및 문제점 | | 대응 방향 |
|---|---|---|
| 개발·공급 단계 위협 증가 | 개발 단계를 노린 공격에 취약 | 개발·공급기업의 **보안 내재화** 지원 |
| | 복잡해진 SW 공급망 | SBOM을 활용한 **공급망 투명성** 확보 |
| | 보안을 고려하지 않는 기능·성능 중심 개발 관행 | **보안 중심 개발문화** 정착 |
| 피해 확산 방지 미흡 | 초기 탐지의 어려움 | 위협정보 **발굴 체계 다각화** |
| | 2차 피해로 연쇄 확산 | 공급망 참여자 간 **보안정보 공유·협력체계** 마련 |
| 공급망 보안 기반 부족 | 공급망 보안 관련 기준 부재 | 공급망 보안 **원칙 수립** 및 **가이드라인** 등 개발 |
| | 전문인력 부족 | 정보보호 전문인력의 **공급망 보안 역량** 강화 |
| | 시험·점검 환경 부재 | 공급망 보안 **테스트베드** 조성 |

☞ **(예방)** 안전하게 개발하고 책임 있게 공급할 수 있는 보안 내재화 촉진

☞ **(복원)** 공급망 가시화를 통한 신속한 복구·대응 체계 마련

☞ **(기반)** 사이버 복원력 확보를 위한 정책적·제도적 기반 조성

## 참고1 주요 SW 공급망 공격 및 위협 사례

<table>
<tr><th>유형</th><th colspan="2">주요 내용</th></tr>
<tr><td rowspan="4">1. 공개 SW 보안취약점<br>(Vulnerabilities in OSS)</td><td colspan="2">[정의] 널리 사용되는 공개 SW에서 취약점이 발견되어 해당 공개 SW를 사용하여 개발한 모든 SW도 취약하여 해커에 의해 악용</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>Log4Shell<br>(2021년)</td><td>Log4j의 제로데이 보안취약점과 공개된 개념 증명 코드를 악용하여 악성코드를 심고, 전 세계 취약 서버를 대상으로 대량의 해킹 공격 발생</td></tr>
<tr><td>Heartbleed<br>(2014년)</td><td>OpenSSL에서 심각한 취약점이 발견되어 비밀번호, 세션 키, 인증서의 개인키가 유출될 수 있었고, 전 세계 수십만 대의 HTTPS 서버, VPN 서버 등이 영향받음</td></tr>
<tr><td rowspan="4">2. 타사 의존성<br>(3rd Party Dependencies)</td><td colspan="2">[정의] SW 개발에 사용한 타사 SW(상용 SDK, 라이브러리 또는 컴포넌트)에 악성코드 또는 취약점이 발견되어 이를 악용</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>보안인증 SW<br>(2023년)</td><td>금융 보안인증 모듈의 보안취약점을 악용해 PC 해킹 및 악성코드 유포로 국내 61개 기관, 총 207대의 기관, 기업, 개인 PC 해킹 피해</td></tr>
<tr><td>보안 SW<br>(2023년)</td><td>北 정찰총국이 전자서명, 암호화 등에 사용되는 보안 모듈의 보안취약점을 악용하여, 공공기관·언론사·방산·IT 등 50여개 기관을 해킹</td></tr>
<tr><td rowspan="4">3. 공용 리포지토리<br>(Public Repositories)</td><td colspan="2">[정의] GitHub 등 알려진 공개 SW 리포지토리에 합법적인 공개 SW와 유사한 이름을 가진 악성코드를 업로드하거나 공개 SW 관리자의 권한을 탈취하여 합법적인 공개 SW에 악성코드를 삽입</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>set-utils<br>(2025년)</td><td>PyPI의 정상 패키지인 python-utils, utils과 유사한 set-utils를 업로드하고 내부에는 암호화폐 지갑의 개인 키를 탈취하는 코드를 삽입</td></tr>
<tr><td>XZ Utilz<br>(2024년)</td><td>압축 해제 도구로 널리 사용되는 공개 SW인 XZ Utils 개발에 2년간 기여하여 공개 SW 관리자가 된 후, 업데이트 시 백도어를 삽입</td></tr>
</table>

<table>
<tr><th>유형</th><th colspan="2">주요 내용</th></tr>
<tr><td rowspan="4">4. 변환 시스템<br>(Build Systems)</td><td colspan="2">[정의] 개발 프로세스 자동화를 위한 CI/CD 상의 중요 코드, 리포지토리, 컨테이너 및 변환 서버를 침해하여 악성코드로 교체</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>SolarWinds<br>(2020년)</td><td>러시아 기반 해킹 그룹의 공격으로 IT SW 공급사의 SW 개발환경 및 배포 시스템이 해킹되어 18,000개 이상의 기관이 피해를 입음</td></tr>
<tr><td>3CX<br>(2023년)</td><td>악성코드가 삽입된 X-트레이더 금융 SW를 다운받은 3CX 직원의 PC를 통해, 3CX의 빌드 서버를 침해. 3CX 데스크톱 앱에 악성코드를 주입하여 60만 명 이상의 고객과 1,200만 개 조직으로 전파</td></tr>
<tr><td rowspan="4">5. 업데이트 가로채기<br>(Hijacking Updates)</td><td colspan="2">[정의] 공격자가 SW 업데이트 과정을 침해하거나 업데이트 서버의 관리 권한을 가로채어 악성코드를 삽입</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>ASUS<br>(2018년)</td><td>ASUS 소프트웨어 업데이트 서버를 해킹하여 업데이트에 백도어 삽입하여 ASUS가 생산한 컴퓨터 백만 대 이상을 손상</td></tr>
<tr><td>ERP 솔루션<br>(2024년)</td><td>북한으로 추청되는 해커가 국내 ERP 솔루션 업체의 업데이트 서버에 공격하여 기존 ERP 솔루션의 업데이트 프로그램에 악성 루틴 삽입</td></tr>
<tr><td rowspan="4">6. 내부 리포지토리<br>(Private Repositories)</td><td colspan="2">[정의] 공격자가 기업 내부에서 사용 중인 코드 저장소에 침입하여 악성코드를 삽입</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>닛산소스코드 유출<br>(2021년)</td><td>내부적으로 소스 코드를 관리하는 Git 리포지토리 서버를 기본 ID와 비밀번호를 유지한 채로 운영. 해커가 이 계정을 활용하여 내부 소스코드를 탈취</td></tr>
<tr><td>PHP 악성코드 삽입<br>(2021년)</td><td>PHP 프로그래밍 언어 배포를 위해 PHP가 자체로 운영하는 Git 서버가 공격당하여 악성코드 삽입. PHP 자체 운영 Git 서버 운영을 중단하고 GitHub을 메인 리포지토리로 변경</td></tr>
<tr><td rowspan="3">7. 공급사 및 협력사<br>(Suppliers and Business Partners)</td><td colspan="2">[정의] SW 완제품 개발사, 공급사 등으로부터 외부 서비스를 제공받는 경우 관리되지 않는 타사 위험(Risk)이 내부 시스템으로 전이</td></tr>
<tr><td>공격사례</td><td>시나리오</td></tr>
<tr><td>CCTV 백도어<br>(2018년)</td><td>군의 고성능 감시장비 구축 사업으로 도입된 중국산 CCTV 260여대에서 백도어 발견 확인</td></tr>
</table>

# Ⅳ 비전 및 추진전략

## 비전

**안전하고 책임 있는 공급망 보안 체계의 전환을 통한 사이버 복원력 확보**

### 목표

**역량 강화**

- SW 공급망 보안 및 위험관리 모델 확보
- 전문 기술·인력 양성

**체계 마련**

- 민간·공공의 유기적인 공급망 위협 정보 공유
- 선제적 피해확산 차단

**기반 조성**

- 일관성 있는 SW 공급망 보안 정책·제도 운영
- 국제협력·공조 체계 구축

### 추진전략 및 세부 과제

| 추진전략 | 세부 추진과제 |
|---|---|
| 가 공급망 위협 예방 역량 강화 | 1 공급망 전주기의 보안 내재화 지원 |
| | 2 SW 공급망의 투명성 제고 |
| | 3 보안 중심 개발 문화 정착 |
| 나 신속한 탐지 · 대응 체계 마련 | 4 공급망 위협정보 모니터링·탐지 강화 |
| | 5 공급망 보안 위험관리 체계 구축 |
| | 6 신속한 피해확산 차단 |
| 다 정책·제도적 기반 조성 | 7 정책 추진체계 구축 |
| | 8 법·제도 정비 |
| | 9 글로벌 협력 확대 |

# Ⅴ 세부 추진과제

## 가 공급망 위협 예방 역량 강화

☞ SW 공급망 위협을 완화하기 위해 개발·공급 단계부터 보안을 내재화하고 SW 투명성을 제고하여 사고 예방 역량을 강화

### 1 공급망 전주기의 보안 내재화 지원

◆ 운영 단계 중심의 보안을 개발·공급단계까지 확대하기 위해 공급망 보안 기준 및 가이드라인을 제시하고, 기업 자체의 보안 역량을 강화

#### | 1 | SW 생애 주기별 공급망 보안 기준·가이드 개발

● **(보안 기준) SW의 개발부터 운영까지 생애 주기별 공급망 보안 원칙·기준을 개발·배포하여, 능동적인 공급망 위협 대응을 위한 기반 마련('26~)**

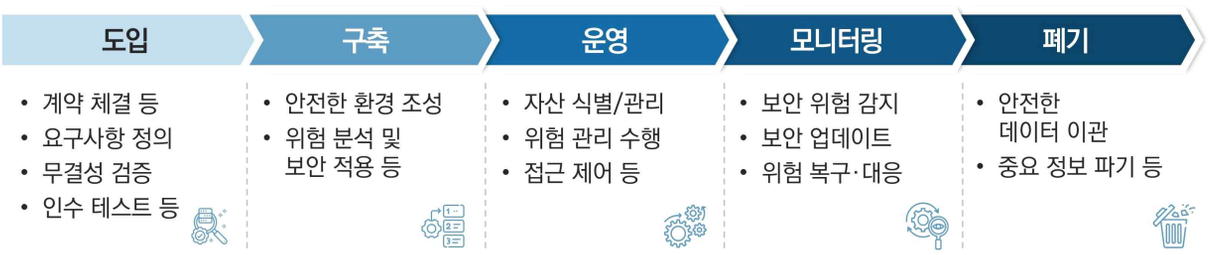
– 기업이 안전하게 SW를 개발·공급할 수 있도록 국내 환경에 적합한 기준·활동 등 '안전한 SW 개발 방법론*' 제시

* 美 NIST의 SSDF(Secure Software Development Framework) 등을 참고하여, 설계단계부터 개발·테스트 및 배포까지 전체 SW 개발 주기에서 단계별로 활용할 수 있는 SW 공급망 보안 지침 개발


▲ 그림5. 개발·공급 기업이 준수해야 할 공급망 보안 활동 예시

- 백신·방화벽과 같은 보안 솔루션으로는 예방하기 힘든 공급망 위협을 사전에 식별하고 완화할 수 있도록 기본 수칙·방안을 마련

  ※ 기업 규모 및 산업별 SW 공급망 특성 등에 따라 차등적으로 적용할 수 있도록 특화된 기준을 함께 마련하여 현장의 활용도를 제고




▲ 그림6. 도입·운영기업이 준수해야 할 공급망 보안 위험관리 활동 예시

- **(가이드라인) 공급망 관리에 어려움을 겪는 기업·기관이 활용할 수 있도록 SW 개발·공급 관련 가이드라인 발간 추진('26~)**

  - 현장 의견 등을 수렴하여 안전한 오픈소스 도입 방법 등이 포함된 사례 중심 실무 가이드라인 개발·보급('26~)

    ※ 인식 제고가 주요 내용이었던 「SW 공급망 보안 가이드라인 1.0」을 개선하여, 실제 SW 개발·운영 현장에서 참고할 수 있도록 가이드라인 2.0을 개발

  - 개발 보안 분야 등 기존 가이드라인* 개정을 통해 공급망 위협 식별 및 대응·관리 등 공급망 보안 요소 보완·고도화 추진

    * 기존 SW개발보안가이드('21.11), 언어별(Python, Javascript) 시큐어코딩 가이드('23.12) 등

| 기존 | 개선 |
|---|---|
| 라이선스 측면의 오픈소스 활용 가이드 | 보안 측면의 안전한 오픈소스 도입 가이드 |
| 시큐어코딩 등 자체 개발 코드 중심의 개발 보안 | 공개/상용 SW 등 공급망 전반에 걸친 개발 보안으로 확대 |
| 제품·서비스 중심의 보안 | 공급망 전반의 보안으로 확대 |
| - | (신규) 보안을 준수한 자동화 도구 활용 |

▲ 표1. 실무가이드 개선 방향(안)

- 특히, 美·EU 등 SW 공급망 보안을 제도화*한 주요국의 기준을 분석·반영하여 수출기업의 해외 규제 극복에도 활용할 수 있도록 개발

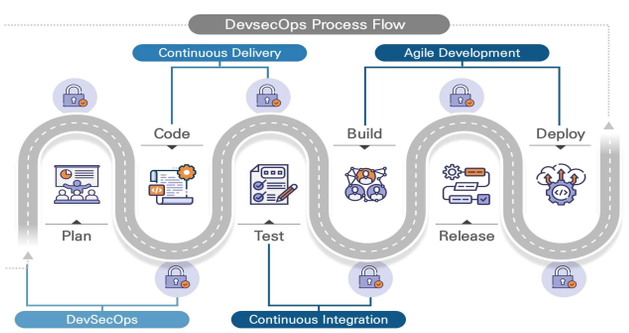
  * (美) EO 14028에 따라 연방기관이 도입하는 SW는 NIST SSDF(Secure Software Development Framework)를 준수해야하며, 주정부 등도 이를 준용하는 추세

    (EU) 사이버복원력법('27.12월 예정)에 따라 EU에서 판매되는 디지털요소가 포함된 제품은 SBOM 관리, 취약점 관리, 보안을 고려한 설계·개발·생산 의무화

## | 2 | SW 보안 수준 시험·점검 제공

- **(테스트베드) 공급망 보안 인력·인프라를 단기에 마련하기 어려운 기업 대상 SW 보안점검 및 기술지원을 제공하는 테스트 환경 구축('26~)**
  - 개발보안허브·NCSC(판교) 등 기존 사이버보안 지원시설을 활용하여 SW 공급망 보안점검 도구 이용환경을 단계적으로 확충

    ※ SW의 정적·동적 분석, 공개SW 사용현황, 시큐어코딩 및 공개된 취약점 점검 등
  - 지역정보보호클러스터를 활용, 테스트베드를 광역권 단위로 점진적 확대하여 지역 SW기업들의 공급망 보안 시험·점검 접근성을 제고

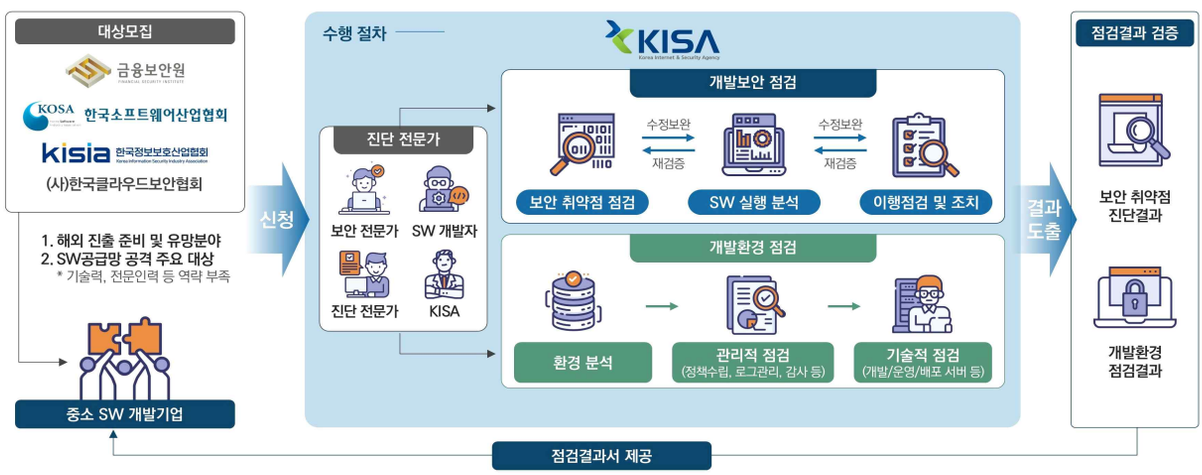
| 주요 내용 | |
|---|---|
|  | **[점검항목]**<br>1. SBOM 생성 및 보안취약점 점검 지원<br>2. 개발공급기업 보안 내재화 점검 지원<br>3. IoT 기기, 융합산업 제품 등 공급망 보안점검 및 컨설팅 지원<br>4. 의료기기 인허가, EU CRA법 등 글로벌 규제 점검 지원 |

▲ 표2. SW 공급망 보안점검 시험환경 - 예시

- **(온라인지원) SW 개발·공급사 대상 사각지대 없는 공급망 보안 지원을 위해 온라인을 활용한 점검·대응 체계 마련('27~)**
  - 지방 소재 기업 등 테스트베드 방문이 어려운 개발·공급사를 대상으로 SW 공급망 보안 비대면 점검 서비스 제공
  - SW 개발 보안 포털(가칭) 등을 통해 SW 구성요소(오픈소스 SW 등)의 안전한 활용을 위한 대응방안, 질의응답, 취약 SW 정보 등 제공
- **(AI 점검 인프라 구축) 고성능 AI 모델을 활용한 중소기업 제품(SW) 대상 취약점 점검 인프라 제공, 전문가 조치 지원('27~)**

## | 3 | 기업의 안전한 개발·공급 환경 전환 지원

- **(컨설팅) 안전한 SW 개발환경 전환을 위해 기업의 개발 인프라 및 관리체계(조직·프로세스) 등 전문 보안컨설팅 추진('26~)**
  - SW 개발·공급기업의 주요 개발 인프라 구성 및 보안 정책의 적절성, 보안 취약점 식별·조치 등에 대한 환경분석 및 진단 지원
  - 컨설팅의 효과성을 높이고 기업의 보안관리 수준을 제고하기 위해 후속진단 및 조치 방안에 대한 기술적 지원까지 함께 제공




▲ 그림7. SW 개발기업 보안점검 및 후속 조치 지원 절차 - 예시

- **(솔루션 도입 지원) 자체적으로 안전한 개발환경 구축이 어려운 소규모 SW기업 대상으로 SW 개발환경 개선지원 추진('27~)**
  - 보안 전담 인력을 두기 어려운 소규모기업에 적합한 클라우드 기반 개발환경 보급 및 보안 솔루션 도입·전환 등을 지원

※ 전체 SW기업 중 81%가 10인 미만 사업장으로 SW 공급망 보안을 위한 전문인력 확보·운영이 어려워 안전한 SW 개발 환경 및 기술지원 등 필요

**참고 : 종사자 규모별 SW기업 수**

| 구분 | 5인 미만 | 5~9인 | 10~19인 | 20~49인 | 50~99인 | 100~299인 | 300~999인 | 1,000인 이상 | 합계 |
|---|---|---|---|---|---|---|---|---|---|
| 기업수 | 28,616 | 7,015 | 4,090 | 2,722 | 840 | 523 | 104 | 22 | 43,932 |

※ 출처 : 2023년 SW산업 실태조사

## 2 SW 공급망의 투명성 제고

◆ SW 공급망의 가시성과 투명성을 제고하여 부적절한 SW 구성요소의 사용을 사전 예방하고, 보안 취약점에 대한 관리를 강화

### | 1 | SBOM 기반의 공급망 보안 관리 모델 적용·확산

- **(SBOM* 관리 모델) 기업이 스스로 SW의 구성요소를 SBOM으로 관리할 수 있도록 공급망 보안 모델 구축을 통한 보안 위협 추적·관리 지원('26~)**

  * SBOM(SW Bill of Materials) : SW의 구성요소 정보를 기술하고 있는 명세서

  - 주요국의 공급망 보안 제도화 대상이 되는 수출기업* 및 사이버 위협 발생 시 파급력이 높은 분야** 등을 중심으로 우선 지원

    * (美) FDA의 의료기기 인허가 시 SBOM 확인, 상무부의 커넥티드카·자율주행시스템 SBOM 관리의무
      (유럽) 사이버복원력법(CRA) 시행에 따른 '디지털 요소가 있는 기기'의 SBOM 관리의무

    ** 보안 SW, 금융·교통 등 사회 기반 분야 SW 및 건강·의료 등 민감정보 관리 SW

  - 산업별 특성(主 사용 공개 SW 및 언어, 관련 규제 등)을 고려한 SW 공급망 보안 모델 발굴 및 모범 사례 확산 지원


▲ 그림8. SBOM 기반 공급망 보안 모델 구축(인프라) - 예시

### 참고 : SBOM 개요

**○ SBOM(Software Bill of Materials)이란?**

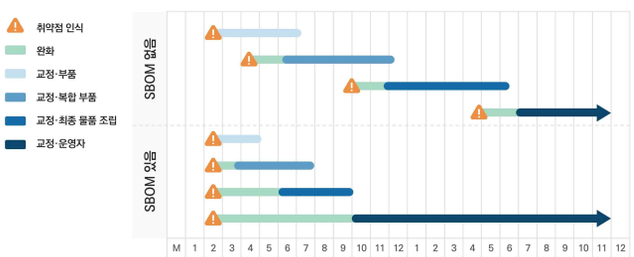
- SW를 구성하는 전체 컴포넌트들의 구성요소와 의존 관계를 기술한 것으로 국내에서는 SW 구성요소 명세서, SW 자재명세서 등으로 불림


**○ 필요성**

- 공급망 위협은 오픈소스, 서드파티, 외주 개발 등 외부 활용 코드에서 주로 발생, SBOM은 구성요소를 식별하여 신속하게 탐지·조치가 가능

**○ 기대효과**

- 기존 보안취약점 발견 및 조치에 수개월~수년 소요되었으나, SBOM 활용 시 보안취약점의 신속한 식별 및 완화·조치 즉시 가능




## | 2 | SW 공급망 보안 기술 고도화

- **(SBOM 기술) SBOM의 신뢰도와 편의성 등을 개선하여 기업의 SBOM 접근성·활용성을 제고할 수 있는 관련 기술의 고도화 추진('26~)**
  - (신뢰도) SBOM 정확도 및 적용 범위 검증, SW 수정 시 SBOM 이력 관리 등 기술 개발 및 실증
  - (자동화) SBOM 생성·검증, 위협 수준 분석, 대응조치 방안 제시까지 SW 공급망 위협 식별 기술 자동화
  - (보관·유통) SBOM에 포함된 민감정보(취약점 등)를 기업 간 안전하게 유통할 수 있는 관리 방안 연구
- **(신기술 대응) AI 등 디지털 신기술 일상화에 대응하여 해당 분야 공급망 보안 모델 개발을 위한 다각적 연구·실증 등 추진('27~)**
- **(보안 운영 재설계) 사람 중심의 SW 취약점 탐지 및 수동 대응(패치) 등 경직된 프로세스를 AI 중심 자율체계로 전환하기 위한 연구 지속 추진**

## 3 보안 중심 개발 문화 정착

◆ SW 개발 과정에서 보안을 후순위로 고려했던 관행에서 보안이 '동반기술'로 인식될 수 있도록 보안 중심의 개발 문화 확산 지원

### | 1 | 이해관계자별 맞춤형 인식제고

- **(인식제고 활동) 공급망 보안의 중요성 인식 제고를 위해 경영진부터 개발자·운영인력 등 全 구성원 대상 맞춤형 인식 제고 활동 확대('26~)**
  - CISO 협의회 등을 통한 경영진을 대상으로 위협사례, 주요국 정책 동향 등 SW 공급망 보안의 중요성 인식을 제고
  - 재직 중인 개발자 대상 SW 공급망 보안 및 개발보안 교육 등을 제공하여 기업의 모든 구성원이 보안을 고려할 수 있도록 지원
- **(SW 교육 반영) SW 인재 양성 교육과정과 연계하여 공급망 보안 기본 소양교육을 반영, 신규 SW 개발자 대상 인식을 제고('26~)**

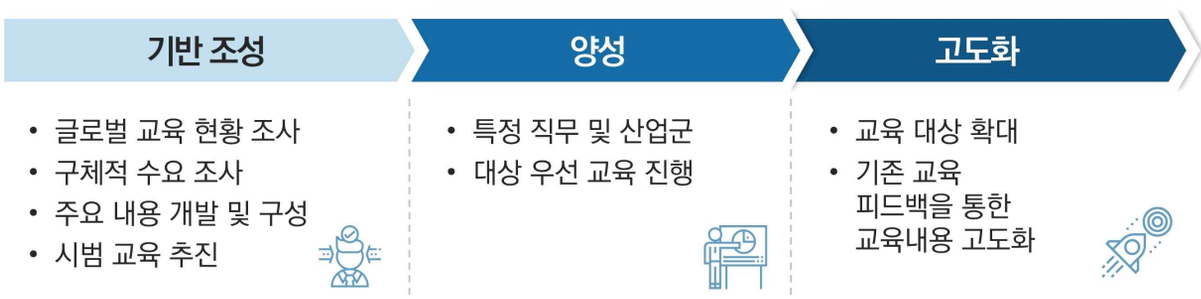
  ※ 교육과정에 SW 공급망 위협 동향 및 대응 방안 등 기초 인식 교육 반영 등 추진
  - 특히, SW 중심대학 등과 연계한 행사를 기획·개최하여 SW개발 입문단계부터 보안 중심에 익숙하도록 문화를 조성
- **(문화확산) 산·학·연·관 협력을 통해 다양한 캠페인, 자율 협약, 컨퍼런스 등 홍보활동 추진('26~)**
  - 기존 정보보호 전문가 중심의 보안 분야 컨퍼런스 뿐만 아니라, SW 개발 관련 컨퍼런스에도 공급망 보안 주제 발표 등 지원
  - 특히, 취약점 존재가 아닌 취약점 방치가 문제점임을 국민·기업이 인식할 수 있도록 SNS 등을 통한 인식 제고 활동 추진

## | 2 | 공급망 보안 전문기업·인력 양성

- **(전문기업 육성) 민간 중심의 공급망 위협 예방·대응 경험 축적을 통해 SW 공급망 보안 전문 서비스 기업 육성('27~)**
  - 정보보호 전문서비스 기업 제도 개편*을 통해 우수한 SW 공급망 보안 서비스 역량·인력을 갖춘 기업을 지정

    * 전문서비스 분야 세분화 등을 통해 SW 공급망 보안 분야 전문 서비스 기업 지정
  - 공급망 보안 서비스에 대한 업무 기준·요건 등을 제시하여 신뢰성·전문성을 가진 전문기업이 육성될 수 있도록 제도적 지원
- **(전문인력 양성) 현장에서 요구하는 보안 기술(Skill)을 발굴하고 체계화하여 전문인력 양성을 단계적으로 추진('26~)**
  - SW 개발자·운영자 등 현장의 실무 담당자 대상으로 SW 공급망 위협 대응 및 보안 강화를 위한 맞춤형 교육과정 개발·제공
  - 기존 정보보호 전문인력의 SW 공급망 보안 분야 전문 역량을 강화할 수 있도록 온·오프라인 전문 교육과정 신설

    ※ 실전형 사이버훈련장, K-Shield 등 재직자 교육과정 내 공급망 보안 분야 신설·강화
  - 자동차·의료기기 등 공급망 보안 규제가 강화되는 특정 산업의 경우 유관 부처·단체와 협력하여 특화 교육·훈련 프로그램 마련




▲ 그림9. 단계적 전문인력 양성 추진 방향

# 나 공급망 위협 신속 탐지·대응 체계 마련

☞ 단일 기업의 피해에 머무르지 않고 연쇄 피해로 이어지는 공급망 위협의 빠른 탐지·대응을 위한 관리체계 마련을 통해 피해 확산 최소화

## 4 공급망 위협정보 모니터링·탐지 강화

◆ 보안취약점 발굴 활성화, 사이버 위협 정보의 신속한 공유를 통해 침해사고 및 피해 방지를 위한 사전 예방 기반 마련

### | 1 | 보안취약점 발굴·조치 활성화

- **(발굴 채널 확대) SW 개발·공급기업, 정보보호기업(백신, 진단 도구 등), 정부가 함께 협력하는 SW 공급망 위협 발굴채널 확대('26~)**
  - 기업의 자발적인 버그바운티 프로그램 운영 및 정부의 보안취약점 신고포상제 등 다양한 위협정보 발굴 채널 확대

    ※ (예시) KISA 보안취약점 신고포상제('12년)의 범위 확대를 통한 활성화 추진
  - 공급망 위협 조기 탐지·분석을 위한 기업 · 기관의 자발적 취약점 발굴·조치인 CVD*·VDP 제도의 단계적 확대 및 활성화 지원 추진

    * Coordinated Vulnerability Disclosure: 기업은 자사 SW 대상 화이트해커의 취약점 발굴을 허용하고 발굴된 취약점을 신고 받아 조치 및 공개하는 취약점 관리제도


▲ 그림10. CVD 제도 도입을 통한 보안 취약점 발굴 체계 - 예시

- **(보안 실태점검) 국민 사생활과 밀접하거나 국가 경제 중요성이 높은 디지털 제품군*에 대한 보안 실태점검 등 추진('26~)**

  * 예시) 로봇청소기, IP카메라 등 IoT 가전 및 태양광 발전 인버터 등 정보통신망연결기기등 대상

  - 실태점검 결과에 대한 대외 공표 및 취약점 개선 권고를 통해 디지털제품 취약점 조치 및 침해사고 위험 완화

    ※ 보안 실태점검 공표 및 취약점 개선권고를 위한「정보통신망법」개정 추진

- **(미흡기업) 침해사고 발생 및 보안취약점 발견 이후 후속 대응 조치가 미비한 기업·제품 대상 공공분야 도입 제재조치 강화('27~)**

- **(발굴 체계 전환) 신속한 제로데이 취약점 발굴을 위해 실시간 모니터링이 가능한 AI 기반 자동화 체계의 개발·전환('28~)**

  - 주요 취약점 평가(위험도 등) 방법론* 개발, 공격 가능성이 있는 기존 취약점의 자동화 식별·평가 기술 연구개발 등 추진

    * CVSS Score 등 기존 평가 방법론을 개선하여 AI를 활용하여 고도화되는 사이버위협 요소를 반영한 새로운 위험도 산정 방식 도입 등

## | 2 | 위협정보 탐지·발굴 다각화

- **(AI 기반 탐지) 개발·공급 업체 대상 위협탐지*와 외부 위협 정보**를 통합 분석하는 AI 기반 탐지체계 운영을 통해 은닉된 위협 발굴('26~)**

  * 웹, 네트워크, 단말 영역의 위협탐지 시스템으로부터 수집되는 정보

  ** 국내·외 정보보호 기업의 위협 데이터베이스 등 다양한 사이버 위협정보

  - Data Lake에 축적된 다양한 위협 정보 간 연관분석*하고 AI 기반 실시간 분석 기능을 접목하여 사이버공격 사전 탐지 역량 강화

    * 디지털 환경 구간별(네트워크, 웹, 단말 등) 탐지 정보에 대한 관계성, 상관관계 등을 연결 및 분석하여 단편적인 사건에서 전체적인 사이버공격 흐름 파악 및 관련 인프라 식별

- **(AI 기반 방어) AI를 활용한 사이버공격에 대해 자동 패치, 조치 완화, 피해 억제 등 신속한 복원력 확보를 위한 AI 기반 방어체계 구현('27~)**

- **(위협정보 수집 확대) 美 CVE 프로그램* 종료 가능성**에 대비하여 대체 프로그램 발굴 등 위협정보 수집 채널 확대 추진('26~)**

  * CVE(Common Vulnerabilities and Exposures)는 공개적으로 알려진 SW의 취약점 목록으로 다수의 개발자가 SW 개발, 유지보수, 취약점 탐지에 활용하는 보안 위협 목록

  ** 美 연방정부의 지원으로 운영되고 있었으나 최근 구조조정으로 인해 '26년 이후 지원 불투명

## | 3 | 안보위해 제품 대응 체계 마련

- **(검증체계 구축) 공공분야에 도입·운용 중인 정보통신제품 대상으로 안보위해* 여부를 식별·분석·관리하는 검증체계 마련 및 운영('26~)**

  * 안보위해 제품 : 국제 사회에서 위해성이 제기되는 제품, 국제 및 국가배후 해킹조직이 개발·유통에 관여하는 제품, 해킹사고 발생 또는 개연성이 존재하는 제품 등

  - △안보위해 요소 정의 △제품 선정 △결과 대응조치 방안 등 검토를 위한 분야별 민·관·군 전문가로 구성된 '안보위해 평가 협의체' 운영

    ※ 안보위해 제품 실시간 도입·운용·조치 현황 관리를 위한 모니터링 시스템 구축

  - 국제사회 제재를 받는 IT제품·ODM 제품에 대한 검증을 강화하고, 공공분야 보안취약 제품 도입 여부 주기적 실태점검 정례화

- **(체크리스트 개발) 개발·공급업체 대상 안보위해성 자가 점검 체크리스트를 마련('27~), 공공분야 납품시 안전성 확인 강화('28~)**

  - 취약점 존재 품목 사용 여부 등 안보위해성 확인을 위해 필수 점검항목·해설·사례 등을 포함한 체크리스트 개발

    ※ 외교·안보·국방 등 주요 기관에 IT제품 납품 시 체크리스트 제출을 우선 적용('28~)하고 향후 단계적 확대

## 5 공급망 보안 위험관리 체계 구축

◆ 체계적인 SW 공급망 위험관리를 위해 SBOM 표준화 및 취약점 데이터베이스 구축, 공급망 위협 추적·관리 환경 마련

### | 1 | 공공분야 공급망 위험관리 체계 구축

- **(체계 표준화) 공공분야에 조달되는 SW의 투명성 및 안전성 강화를 위한 공공분야 SBOM 관리체계 개발('26~)**
  - 국내 정보 통신 환경 및 보안 정책, 해외 SW 공급망 보안 추진 동향 등을 반영한 SBOM 항목 도출* 및 표준화
    * SBOM 항목은 기업의 해외 수출 등에 이중 규제로 작용하지 않도록, 해외 SBOM 요구사항 및 표준화 동향을 고려하여 최소한의 항목으로 도출
  - △SBOM 생성·공유·교환 방식 △SBOM 공개·활용 범위에 따른 접근통제 △SBOM 통합관리 절차 등 마련
- **(신뢰성 보장) SW 공급망 위험관리 프로세스의 신뢰성 보장방안 마련('27~)**
  - SBOM 및 취약점 영향도 분석 정보(VEX*) 등 공급망 위험관리 체계 전반에 대한 기밀성·무결성·가용성 확보 기술 개발
    * VEX(Vulnerability Exploitability eXchange) : 소프트웨어 구성요소에 존재하는 알려진 취약점의 악용 가능성 여부를 전달하기 위한 프레임워크
  - 공급망 위험관리 체계 신뢰성 보장 기술의 안전성 및 효율성 검증을 위한 실증을 실시하고 관련 기술 정립 등 체계화

- **(관리 시스템) 공공분야 도입 SW 제품 및 구성요소 정보를 관리할 수 있는 공공분야 SBOM 통합 관리 시스템 구축('26~)**
  - 국가·공공기관이 도입하는 SW 제품에 대한 SBOM을 등록·관리하고 SW 공급망 위험을 실시간으로 모니터링·공지
  - 보안기능 시험 및 보안적합성 검증필 제품 대상 SBOM 관리

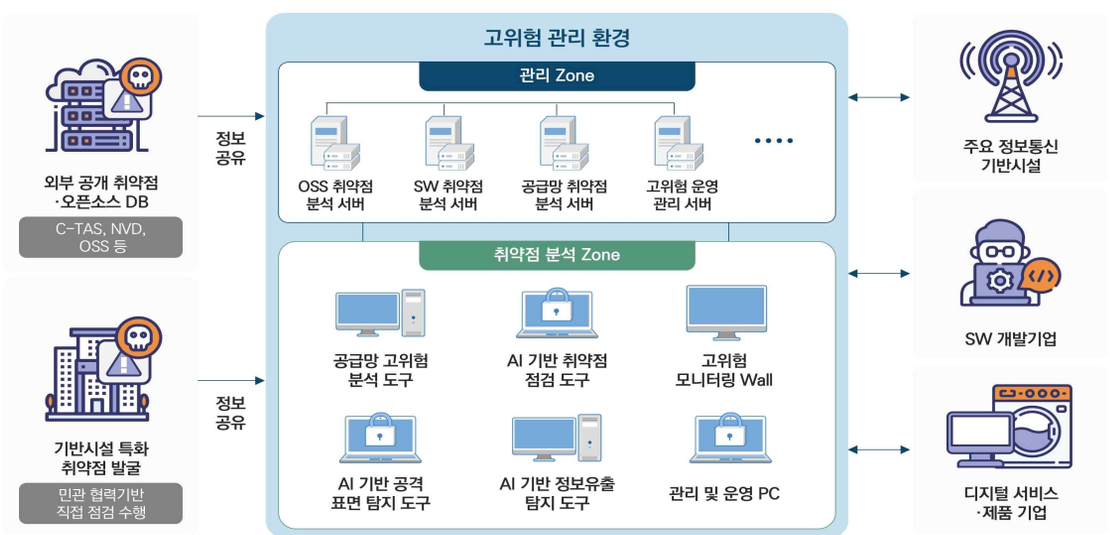
    ※ 보안기능 시험을 신청한 SW 제품 대상으로 SBOM 생성 및 검증체계 실증('27년~), HW 제품 펌웨어 및 클라우드 서비스 등 다양한 제품군으로 실증 확대
- **(취약점 DB 구축) 국내·외 유통되는 상용 및 공개 SW에 대한 취약점 정보를 실시간 수집, 취약점 정보 DB 구축('28~)**

  ※ △공개정보 △국내·외 취약점 분석 전문업체 등을 활용하여 취약점 정보를 수집
  - 공급망 위협에 신속하고 유기적으로 대응할 수 있도록 취약점·조치 정보의 등록·공유 및 이력 관리가 가능한 시스템 구축

## | 2 | 민간 분야 공급망 위험 관리 체계 구축

- **(취약점 관리) 민간기업·시설에서 주로 사용되는 SW 및 보안제품의 고위험 취약점* 포함 여부에 대한 상시 관리체계 도입·운영('26~)**

  * 중대(Critical)한 알려진 취약점, 신규/은닉형 악성코드 등을 고위험 취약점으로 분류·관리




▲ 그림11. 고위험 취약점 점검 및 경보 시스템 - 예시

- **(경보 제공) 신규 보안취약점 발견 시, SBOM 생성·관리 기업을 대상으로 공급망 위험 경보 시스템 구축·운영('27~)**

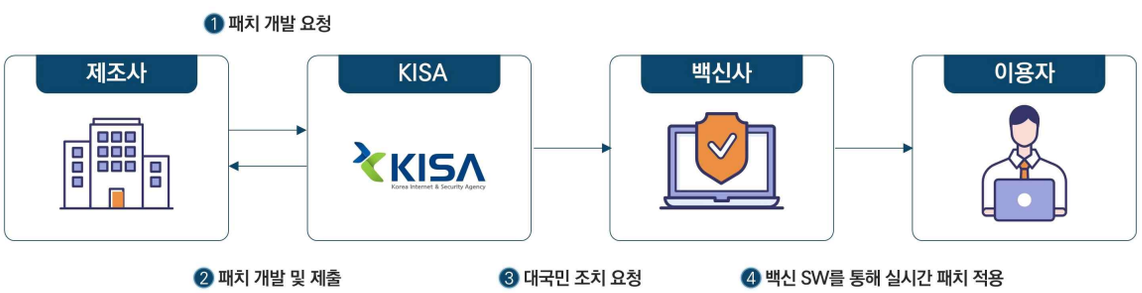
- **(수준 진단) 기업의 SW 자산식별 및 위험 요소 분석을 통해 SW 공급망 위험 수준을 진단하고 완화 조치 지원 사업 추진('28~)**

  ※ 불법적으로 사용하는 소프트웨어·장비, 불필요하거나 위험한 권한 보유자 식별 및 취약점 상태를 확인하여 우선순위 지정 등을 통한 정책적/기술적 조치 방향 제공

- **(대응) 공급망 침해사고가 발생하거나 악용 가능성이 높은 취약점 발견 시 신속한 대응·조치 지원('28~)**

  - (클리닝 서비스) 기업·이용자 PC 대상 보안 취약점 실시간 탐지 · 제거

  ※ 취약점 발견 시 해당 SW 제조사에 보안 패치 개발을 요청하고, 백신 SW를 통해 취약한 SW를 일괄 삭제 후 개발된 패치 안내(평균 4개월 이상→3일 내)




▲ 그림12. C-Clean 서비스 운영체계

## 6 신속한 피해확산 차단

◆ SW 공급망 위협에 대한 상시적인 관리와 함께 신속한 피해 복구 체계를 수립하여 연쇄적 피해로 이어지지 않도록 차단

- **(위협정보 전파) 공급망 침해사고 및 위협정보가 발견되는 즉시 공공·민간에 신속하게 전파하는 절차 마련('26~)**
  - 모니터링·신고 등 다양한 경로로 확인된 위협정보를 민간과 공공이 공유하기 위한 정보공유 표준화 절차 마련
  - 각 분야별 공급망 위협 경보 시스템 구축·운영, 상호간 실시간 위협정보 연동 기능 개발·적용

| |
|---|
| • (인프라 조성) NCTI·KCTI·CTAS 등 사이버 위협 정보공유 시스템을 활용한 정보공유 자동·일원화를 통해 공급망 위협 정보 신속 즉시 전파<br>* (공공) 국가 사이버 위협정보 공유 시스템 NCTI(중앙, 산하, 지자체)·KCTI(민간) 연동 운영 중,<br>(민간) 사이버 위협정보 분석공유 체계 C-TAS 운영 중 |
| • (위협 정보) 공공·민간·국방·금융 등 분야를 넘나드는 공급망 위협에 대한 유관기관 間 정보공유 및 원인분석·조치 등 협력 강화 |
| • (최신기술) 공급망 인텔리전스 구축을 통해 최신 보안 정보 교류 및 고위험 사고의 공동 분석 체계 구축 등 협력 강화 |

▲ 표3. 신속한 공유·협력체계 예시

- **(확산방지 체계 운영) 각 분야별 공급망 위협 경보 시스템을 활용, 영향도·피해범위 확인 및 조치 방안 마련 등 확산방지체계 구축('28~)**
  - (공공분야) △도입·운영 현황 확인 △대응 방안 마련 및 기관 통보 △업체 대상 제품 개선 조치 요청 △패치 적용 등 조치 완료 확인
  - (민간분야) △위협정보가 확인된 제품 개발업체 대상으로 대응·복구 조치 지원 △SBOM 생성·관리 기업에 맞춤형 공급망 위협정보 알림

# 다 정책·제도적 기반 조성

☞ 개발·공급 단계부터 사후관리까지 SW 공급망 위협 관리를 위해 정책 추진체계를 구축하고 제도를 정비하는 등 보안 강화 기반 조성

## 7 정책 추진체계 구축

◆ 일원화된 정책을 마련하고 현장의 목소리를 반영하기 위한 소통·협력 채널 구축하여 한국에 적합한 공급망 보안 정책 추진

### | 1 | 범정부 정책협력체계 구성

- **(정책협의체) 심화되는 SW 공급망 위협 및 글로벌 규제 강화에 전략적 대응을 위한 (가칭) 범정부 SW 공급망 보안협의체 마련('26~)**
  - 사이버보안 유관부처 및 전문기관* 참여를 통해 SW 공급망 보안 위협 사례·이슈 공유 및 보안 정책·제도 논의

    * 한국인터넷진흥원(KISA), 금융보안원 등 보안 관련 기관
  - 분야별로 산재되어 있는 사이버보안 관련 제도 및 부처·유관기관 간 협업 강화를 위한 추진 방안 마련


▲ 그림13. SW 공급망 보안 범정부 협의체(가칭) 구성(안)

## | 2 | 민간 자율 활동 지원

- **(민·관 합동 포럼) 정부와 전문가가 함께 참여하는 (가칭)민·관 합동 SW 공급망 보안 포럼 운영을 통해 현장의견 수렴('26~)**
  - 실제 SW 개발·운영 현장에서의 공급망 보안 이슈, 국내·외 위협정보 공유 등 공급망 보안 분야 정책·제도 논의
- **(자율협의체) SW 공급망 보안의 중요성이 높은 산업 분야 등을 대상으로 자율협의체 구성을 통한 SW 공급망 보안 활동 활성화('26~)**
  - 가이드라인의 공통 보안 원칙을 기반으로 산업 특성에 맞는 자율적인 보안 수칙 개발·확산 및 점검 등 자발적 공급망 보안 강화 유도
  - 자율협의체를 통한 주기적 실태조사를 추진하여 산업 분야별 정확한 SW 공급망 현황 파악 및 구조적 개선 방안 발굴 등 추진

# 8 법·제도 정비

◆ 개발·공급단계부터 사후관리까지 공급망 위협에 적시 대응할 수 있도록 도와줄 수 있는 제도의 개선

## | 1 | 민간분야 공급망 보안 제도 정비

- **(시범인증) 안전한 개발 등 공급망 보안을 확인하는 자율 신청 기반 SW 공급망 보안관리 검증 및 우수기업 확인서* 발급 시범 운영('27~)**

* (가칭) SSS Verified, Software Supply-Chain Security Verified

  - 향후 美·EU 등 SW 공급망 보안이 제도화된 국가와의 상호인정을 추진하여 국내기업의 무역장벽 극복 및 불확실성 해소를 지원
  - 시범 운영 후 기존 정보보호 인증제도(ISMS, CSAP, IoT 등) 內 공급망 보안 시험평가 요소를 반영하여 정규 제도화 추진

- **(사후관리 유도) SW 개발·공급 이후에도 생명주기 전체에 대한 지속적인 보안 지원*이 이루어질 수 있도록 제도 개선 방안 마련('27~)**

  * 보안업데이트 제공, 보안지원 종료(EoS, End of Service) 사전공지, 취약점 제보·공개 및 SW 대가산정 가이드 등에 공급망 보안 관련 요소 반영 등

  - 국외 사례 등을 참고, SW기업이 사후관리를 제공하도록 인센티브 근거 마련 및 취약점 미조치 시 시정권고 등 기업의 책임성 강화 검토·추진

**참고 : 해외 사례**

- (EU, CRA*) 제조업체는 제품 출시 후 생명주기동안 보안업데이트 제공, 교정된 취약점 공개 방침(CVD) 수립 등 취약점이 효과적으로 처리되도록 보장할 의무를 부과

  * Cyber Resilience Act(사이버복원력법) : 24년 12월 공포, 27년 12월 시행 예정

- (美) Cyber Trust Mark 인증 기준에 소비자로부터 사이버보안 관련 질의응답 제공 및 관련 정보·업데이트를 소비자에게 제공할 것을 규정(시행 예정)

- (英, PSTI) 제조업체는 소비자에게 사이버보안 문제 보고를 위한 제조업체 연락처 정보 게시, 보안업데이트 지원 기간 공개 등을 의무화

  * Product Security and Telecommunication Infrastructure Act(제품보안및통신인프라법) : 24년 4월 시행

## | 2 | 공공분야 공급망 보안관리 절차·지침 마련

- **(정보시스템 보안) 공공분야 정보시스템의 개발 · 운영 · 유지보수 등 全과정에서 SW 공급망 보안 강화를 위한 보안 활동 절차 마련('27~)**

  - 공공분야 정보시스템 구축 · 운영 등 정보화사업 추진 시, 보안 관련 요구사항 등에 SBOM 제출 및 취약점 대응 절차 도입

  - 공공분야에 도입되는 SW 보안취약점 관리를 위해 SBOM 제출 및 SW 보안취약점 관리 담당관 지정 등 사이버보안 관련 지침 개정

- **(위험관리) 정보통신제품을 도입 · 운영하는 기관이 준수해야할 '공급망 사이버보안 위험관리 절차서'를 마련 · 적용('27~)**

  - 사이버보안 위험을 효과적으로 식별 · 평가 · 대응할 수 있도록 제품 도입 · 운영 절차 세분화 및 단계별 위험관리 활동을 명시

## | 3 | 보안적합성 검증 제도 개선

- **(환경변화 대응) 공공분야에 도입되는 제품의 안전성을 확인하는 보안적합성 검증 제도의 보안 요구사항 개선 및 검증 대상 제품 점증 확대('27~)**
  - 신종 · 융복합 정보통신제품의 기능에 맞춰 보안요구사항을 조합 · 활용할 수 있도록 '국가용 보안요구사항'을 기능단위로 세분화
  - 검증제도 대상을 해킹사고 빈발 또는 중대한 취약점 발견 시 국가기관 전산망에 심각한 피해를 유발할 수 있는 IT 제품으로 확대

    ※ 검증제도 자문위원회를 구성, △국가망보안체계(N2SF) 등 환경변화 △제품에 대한 보안위협 발생 시 파급력 등을 고려하여 검증대상 제품 선정 및 검증항목 마련
- **(기준 강화) 실무안내서 · 점검환경 지원 · 컨설팅 등 기업지원 및 실증 사례를 참고, 보안적합성 검증에 SW 공급망 보안 평가 기준 마련 · 반영('26~)**
  - 보안적합성 검증 또는 도입단계에서 기업이 공급망 위험을 자체적으로 확인하고 증명할 수 있도록 세부 기준항목 개발 · 적용('26~)
  - 보안취약점 추적 · 관리를 위한 SBOM 제출 및 SW 공급망 보안 검증 요건으로 '안전한 SW 개발 방법론' 준수 여부 등 확인('27~)

## 9 글로벌 협력 확대

◆ 국경 없는 SW·사이버보안 특성을 고려, SW 공급망 보안을 주도하는 주요국 등과 글로벌 협력 및 공조 체계 구축

### | 1 | 사이버보안 관련 협력 확대

- **(국제협력) 美·EU 등 사이버보안을 선도하는 국가와 공급망 위협 관련 정보공유 및 규제 동향 파악 등을 위한 협력체계 강화('26~)**
  - 국경이 없는 공급망 위협에 대해 국제사회와 취약점 등 위협 정보를 지속 공유하고 공동 대응체계 마련
  - 美 CISA(사이버보안청) 등 주요국 사이버보안 전문기관 및 GGEF* 협력을 통한 공동 가이드라인 발간 등 협력 지속

    * GGEF(Global Government Expert Forum) : 미국, 독일, 영국 등 31개국 참여

### | 2 | 해외 진출 지원 체계 마련

- **(수출 지원) 미국, 유럽, 일본 등 해외 주요국의 공급망 보안 제도 동향 공유 및 무역장벽 극복 방안을 위한 지원 체계 마련('26~)**
  - 주요국*과 지속적인 소통을 통해 정책을 파악하고, 관련 표준 제·개정 과정에 국내 산업계 의견 반영 요청 등 협력 확대

    * EU집행위원회 정보통신총국(DG CONNECT), 英 과학혁신기술부(DSIT) 등 협력
  - 국가별 요구하는 공급망 보안 관련 인증제도*의 특성을 분석하고 이를 기반으로 분야별 무역장벽 극복 컨설팅 제공

    * (유럽) CRA, (美)FDA, U.S. Cyber Trust Mark 등

- **(상호인정) EU·英 등 사이버보안 관련 제도 강화에 대응하여 국내 인증제도(IoT 보안인증 등)와 상호인정(MRA) 확대 추진('26~)**

※ (사례) EU CRA(Cyber Resilience Act, 사이버복원력법) : 역내 유통되는 디지털기기 대상 제조·유통·수입업체에 강도 높은 공급망 보안을 요구하는 신규 법안 통과('24년)·시행('27.12월)

- 상호인정 확대를 통해 국내 기업의 해외 수출을 지원하고, 인증 수요 확대 및 제품의 보안성 제고를 유도
- 최근 IoT 분야 해외 인증제도가 신설*에 따른 기업의 중복 투자 방지를 위해 단일 표준 제정과 같은 국제 공동 논의** 참여

* (美) FCC에서 소비자용 IoT 기기 대상 자율 인증인 U.S. Cyber Trust Mark 제도 근거 마련('24) 및 시행 준비 중

(EU) 무선기기에 사이버보안을 의무화한 CE RED('25.8~) 및 SBOM 관리 의무화한 CRA 등

** GCLI(Global Cybersecurity Labelling Initiative) : 우리나라를 포함 EU·日·獨·英·싱가포르 등 주요국이 IoT 분야 보안인증(라벨)의 상호인정 및 단일표준 제정 등에 대해 논의 중

Chapter VI

# 향후 추진 일정

| 추진과제 | 소관 부처 | 추진일정 | | |
|---|---|---|---|---|
| | | '26 | '27 | '28 |
| **가. 공급망 위협 예방 역량 강화** | | | | |
| **[1] 공급망 전주기의 보안 내재화 지원** | | | | |
| ❶ SW 생애 주기별 공급망 보안 기준·가이드 개발 | 과기정통부·국정원·행안부 | | ■ | ■ |
| ❷ SW 보안 수준 시험·점검 제공 | 과기정통부·국정원 | ■ | ■ | ■ |
| ❸ 기업의 안전한 개발·공급 환경 전환 지원 | 과기정통부 | ■ | ■ | ■ |
| **[2] 공급망 투명성 제고** | | | | |
| ❶ SBOM 기반의 공급망 보안 관리 모델 적용·확산 | 과기정통부 | ■ | ■ | ■ |
| ❷ SW 공급망 보안 기술 고도화 | 과기정통부·국정원 | | ■ | ■ |
| **[3] 보안 중심 개발문화 정착** | | | | |
| ❶ 이해관계자별 맞춤형 인식제고 | 과기정통부·국정원·행안부 | ■ | ■ | ■ |
| ❷ 공급망 보안 전문기업·인력 양성 | 과기정통부 | | ■ | ■ |
| **나. 공급망 위협 신속 탐지·대응 체계 마련** | | | | |
| **[4] 공급망 위협정보 모니터링·예방 강화** | | | | |
| ❶ 보안취약점 발굴·조치 활성화 | 과기정통부·국정원 | ■ | ■ | ■ |
| ❷ 위협정보 탐지·발굴 다각화 | 과기정통부·국정원 | | ■ | ■ |
| ❸ 안보위해 제품 대응 체계 마련 | 국정원 | ■ | ■ | ■ |
| **[5] 공급망 보안 위험관리 체계 구축** | | | | |
| ❶ 공공분야 공급망 위험관리 체계 구축 | 국정원·행안부 | ■ | ■ | ■ |
| ❷ 민간분야 공급망 위험관리 체계 구축 | 과기정통부 | ■ | ■ | ■ |
| **[6] 신속한 피해확산 차단** | | | | |
| ❶ 위협정보 전파 및 확산방지 체계 운영 | 과기정통부·국정원 | ■ | ■ | ■ |
| **다. 정책 · 제도적 기반 조성** | | | | |
| **[7] 정책 추진체계 구축** | | | | |
| ❶ 범정부 협력체계 구성 | 과기정통부·국정원 | ■ | ■ | ■ |
| ❷ 민간 자율 활동 지원 | 과기정통부·국정원 | ■ | ■ | ■ |
| **[8] 법·제도 정비** | | | | |
| ❶ 민간분야 공급망 보안 제도 정비 | 과기정통부 | | ■ | ■ |
| ❷ 공공분야 공급망 보안관리 절차·지침 마련 | 국정원·행안부 | | ■ | ■ |
| ❸ 보안적합성 검증 제도 개선 | 국정원 | ■ | ■ | ■ |
| **[9] 글로벌 협력 확대** | | | | |
| ❶ 사이버 보안 관련 협력 확대 | 과기정통부·국정원 | ■ | ■ | ■ |
| ❷ 해외 진출 지원 체계 마련 | 과기정통부 | ■ | ■ | ■ |

과학기술정보통신부
Ministry of Science and ICT

국가정보원
NATIONAL INTELLIGENCE SERVICE

KISA 한국인터넷진흥원

# AI 일상화 시대를 준비하는
# SW 공급망 보안 강화 로드맵

2026년 6월 24일 1판 1쇄

**발행처** 한국인터넷진흥원
나주시 진흥길 9 한국인터넷진흥원

**제 작** 과학기술정보통신부, 국가정보원, 한국인터넷진흥원

AI 일상화 시대를 준비하는

# SW 공급망 보안 강화 로드맵


과학기술정보통신부
Ministry of Science and ICT

국가정보원
NATIONAL INTELLIGENCE SERVICE

KISA 한국인터넷진흥원