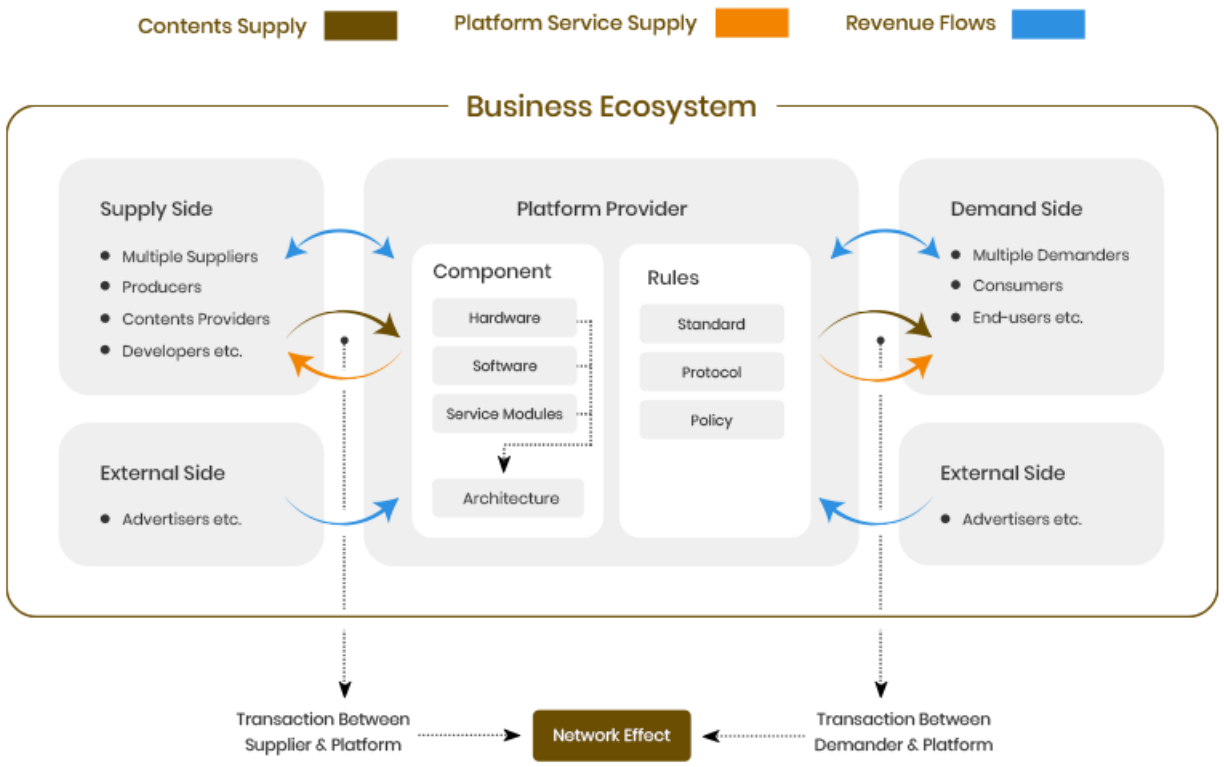
플랫폼 시대의 정보보호 대응체계

플랫폼 특성을 고려한 새로운 대응체계의 필요성

네이버주식회사 이진규 전무 (CISO/CPO)

플랫폼 시대의 정보보호 대응체계: 문제 제기

플랫폼 사업자의 특성에 적합한 정보보호 체계의 부재



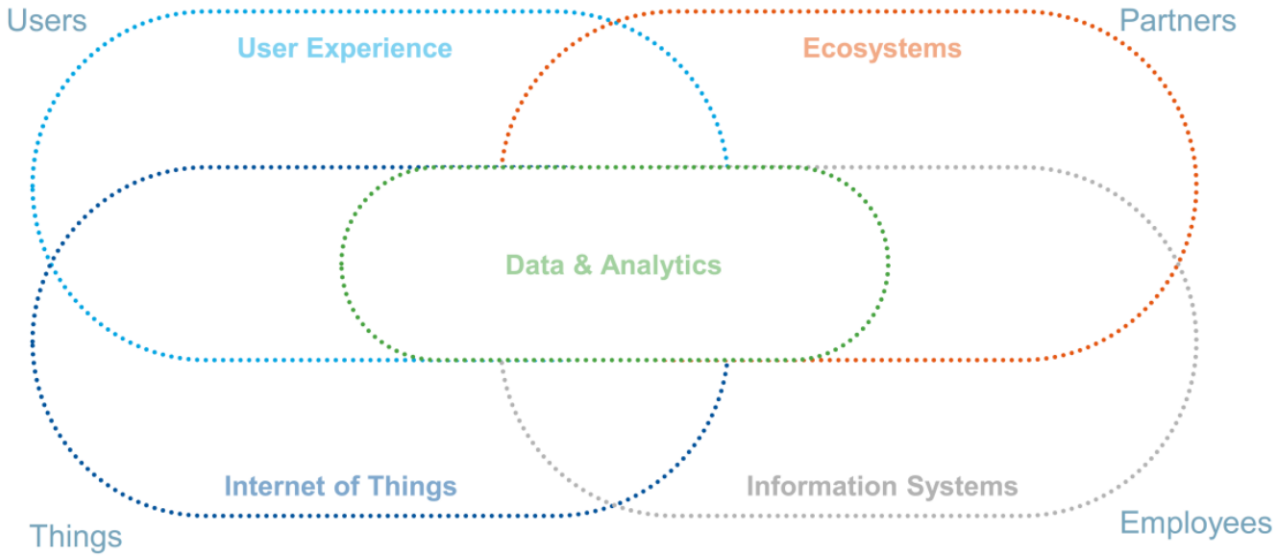
- **다면시장 구조**
  : 복잡한 이해관계 형성
- **다양한 문제 발생**
  : 정보 유통량 증가, 공격 노출도 증대
  : 참여자 보호 요구증가
- **현행 정보보호 체계**
  : 일반 사업자 중심으로 형성
- **플랫폼 특성 고려한 정보보호 체계 필요↑**

플랫폼 사업자의 책임 구조

플랫폼은 에코시스템을 구성하고, 참여자들의 이해관계를 조정하는 조정자

- **현실은 생태계에서의 조정자**
  : 다수 인식은 보통의 '서비스 제공자'
- **다양한 참여자**(이용자, 입점사, 광고주, 제휴사 등)**를 포괄적으로 보호해야 할 책임 존재**
- **플랫폼의 신뢰 기반을 좌우하는 핵심 요소**
  : 공평한 게임의 룰 & 정보보호
- **참여자 보호 실패의 결과**
  : 생태계 전체에 리스크 전파

Moderation & Protection



Trust & Safety

기존 정보보호 대응체계: 한계

플랫폼 사업자의 특성을 제대로 이해하지 못한 채, 동일한 규율을 적용하려 시도

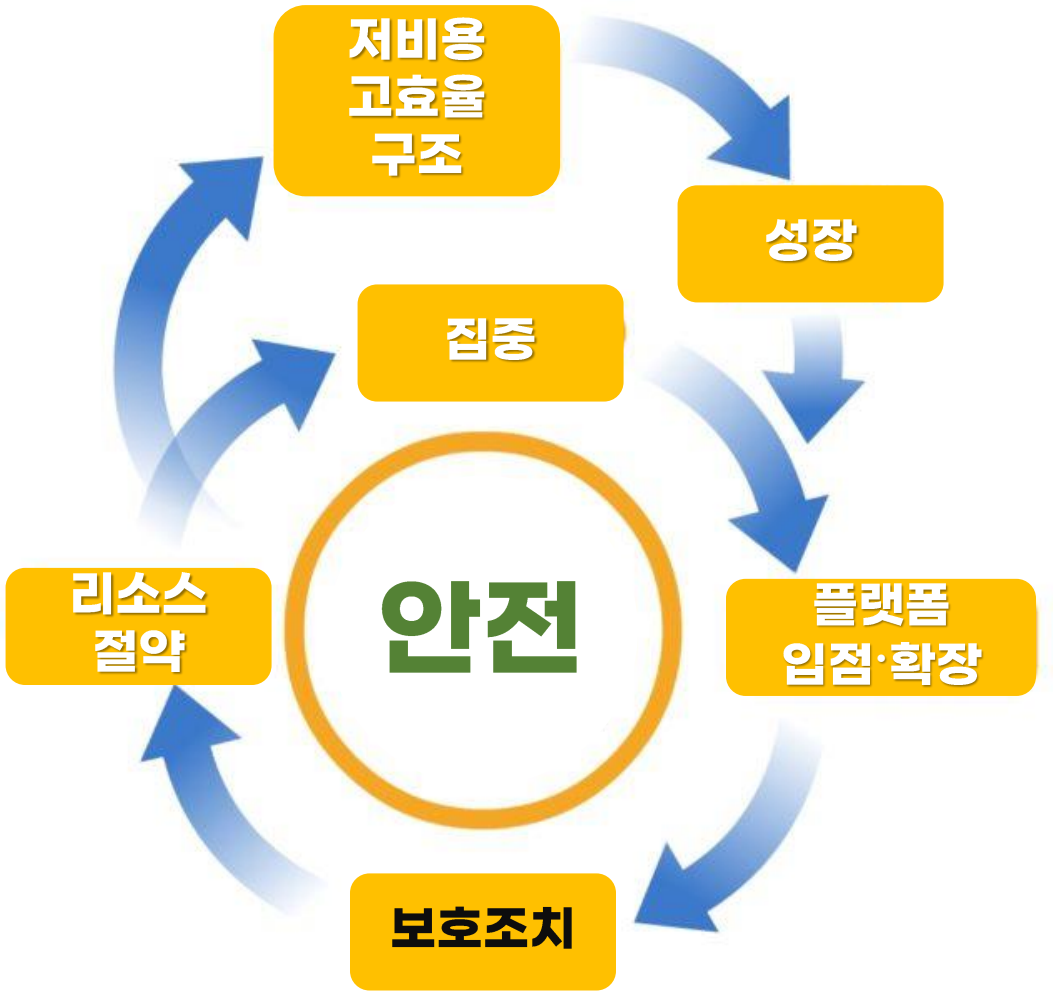
	일반 기업	플랫폼 기업
모델	재고 보유형	중개형
수익구조	직접판매 수입	거래수수료 등
기술 구조	자체 전산중심	개방형 구조
참여자	B2C	Multi-sided
핵심자산	제품, 물류 등	알고리즘 등
성장전략	마케팅, 제품	참여자 증대

- **기존의 법령 체계**
  : 일반적 규율을 플랫폼에 동일하게 적용
- **명확한 한계**
  : 본질적 차이를 전혀 반영하지 못함
- **한계로 인한 결과**
  : 과도하거나 불충분한 보호조치가 병존
- **변화 방향**
  : 플랫폼 특성 고려한 '맞춤형 접근 방식'

인식의 전환: 플랫폼 사업자 보호조치의 '레버리징 효과'

[플랫폼의 고도화된 보호조치 → 전체 참여자 혜택 → 네트워크 효과 강화]의 선순환 구조

- **플랫폼의 고도화된 보호조치 도입 효과**
  : 참여자들이 고루 누리는 혜택
- **입점사 내지 개인사업자**
  : 별도의 보안투자 없이 플랫폼 이용
- **절약한 리소스의 재분배**
  : 시간과 비용을 오롯이 비즈니스에 활용
- **플랫폼의 역할**
  : 정보보호를 '공공재'화 하는 기능을 수행



국내외 플랫폼 규제환경: 비교

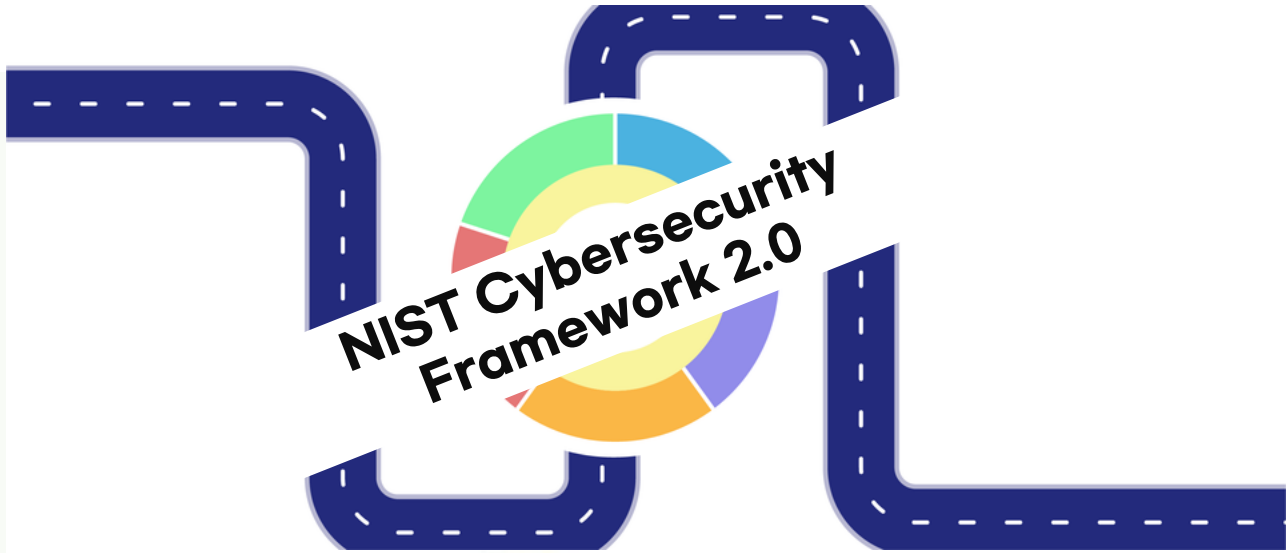
국내외 규제환경의 차이는 플랫폼 경쟁력에 어떤 영향을 미치는가?

- **국내 - 중첩 규제로 인한 사업자 규제부담**
  : 개인정보보호법, 정보통신망법 등
- **해외 - 플랫폼별 차등 적용**
  : 자율규제, 가이드라인 중심 다수 확인
- **글로벌 vs. 국내 플랫폼 경쟁력**
  : 규제 준수 비용에서의 차이
- **형평성과 실효성 고려 필요**
  : 공정한 게임의 룰이 동일하게 적용되도록

해외 사례: (1) 미국

가이드라인 제공과 인증을 통한 민간 자율 대응의 유도

- **민간 자율 대응을 유도**
  : NIST Cybersecurity Framework
- **낮은 강제력**
  : 가이드라인 제공 및 인증 유도
- **자율성 보장**
  : 정부는 표준과 가이드라인에 집중
- **혁신 촉진**
  : Safe Harbor 제공, 신기술 개발 등



해외 사례: (2) 유럽연합

GDPR & DSA를 활용하여 정보보호와 플랫폼 책임을 동시에 대응

The EU Data Strategy
- systematic roadmap

- **원칙 중심의 법제 개발**
  : GDPR, DSA, DMA, AI Act 등

- **플랫폼 규모에 따른 차등 규제 도입**
  : VLOP 별도 규제
  : 투명성 보고와 위험평가 강제
  : SME 보호를 위한 법제 개선 (진행 중)

- **방향성**
  : 이용자 권리 보호와 정보보호 균형 추구
  : 글로벌 플랫폼 견제, 내부 경쟁력 확보

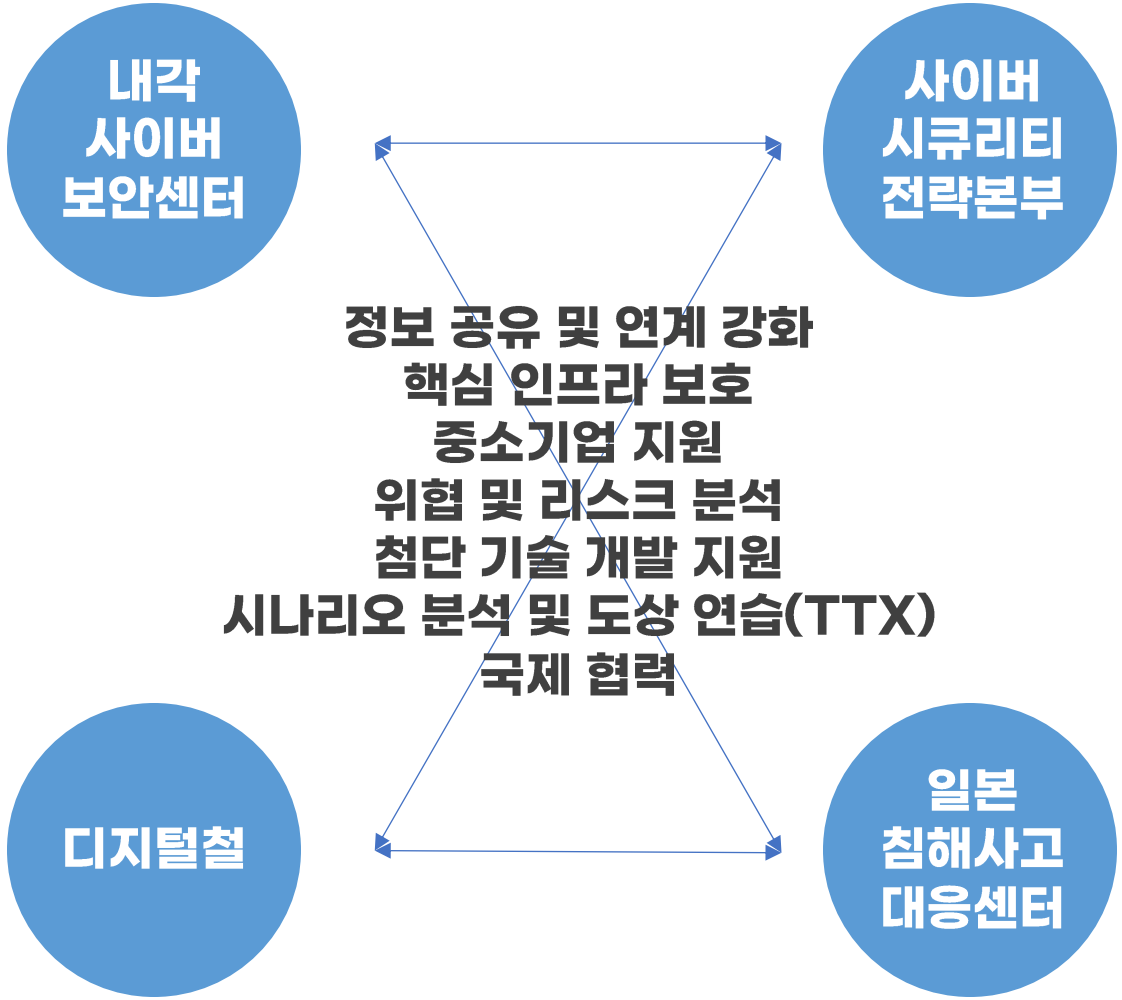
해외 사례: (3) 일본

민관 협력 모델과 자율규범의 조화

- **민간 자율규범과 정부 협업**
  : “유연한 규제”의 실현

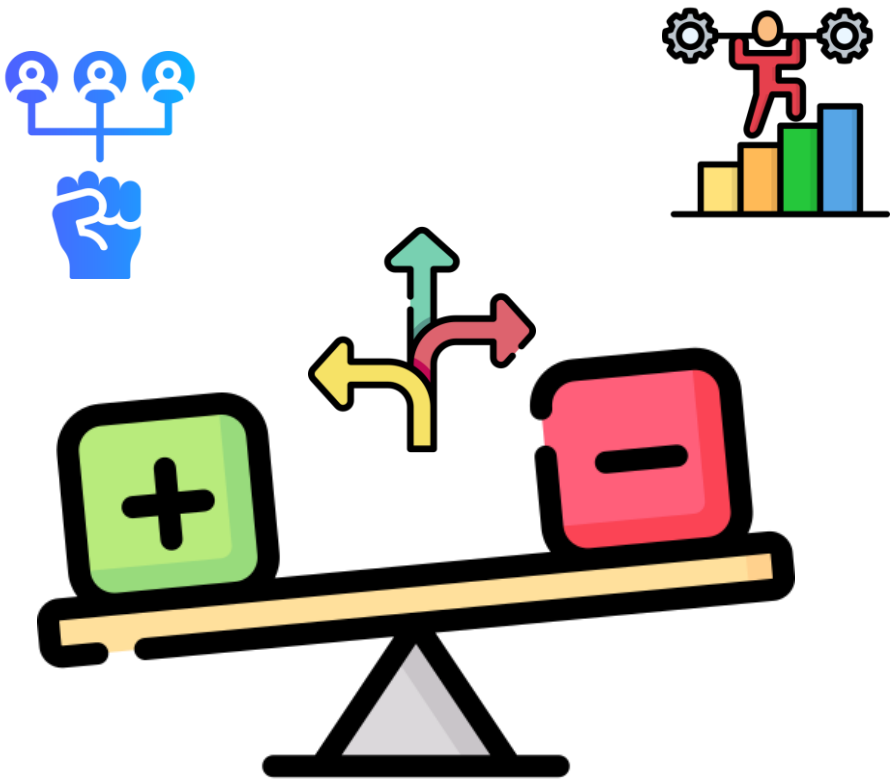
- **중소 플랫폼에 대한 맞춤형 지원**
  : 맞춤형 가이드 제공
  : 공동 모의 훈련
  : 사이버 위협 정보 공유체계 운영

- **민-관 협력 모델**
  : 정부가 집중해야 할 지점을 옳게 선정
  : 협력 모델을 체계적으로 발전



플랫폼 정보보호 체계의 설계 원칙

변화하는 환경에 유연성을 가지고서 빠르게 회복할 수 있는 체계를 갖출 필요



- **자율성** (autonomy)
  : 플랫폼 스스로 목표를 설정하고 실행
- **유연성** (flexibility)
  : 다양한 기술 환경과 리스크에 대응
- **회복탄력성** (resilience)
  : 빠르게 복구하고 재발 방지하는 구조
- **균형성 및 포용성** (balance & inclusiveness)
  : 참여자와 사업자간 책임 균형성 확보 등

포용성: 배제될 수 있는 취약한 참여자를 각별히 보호함

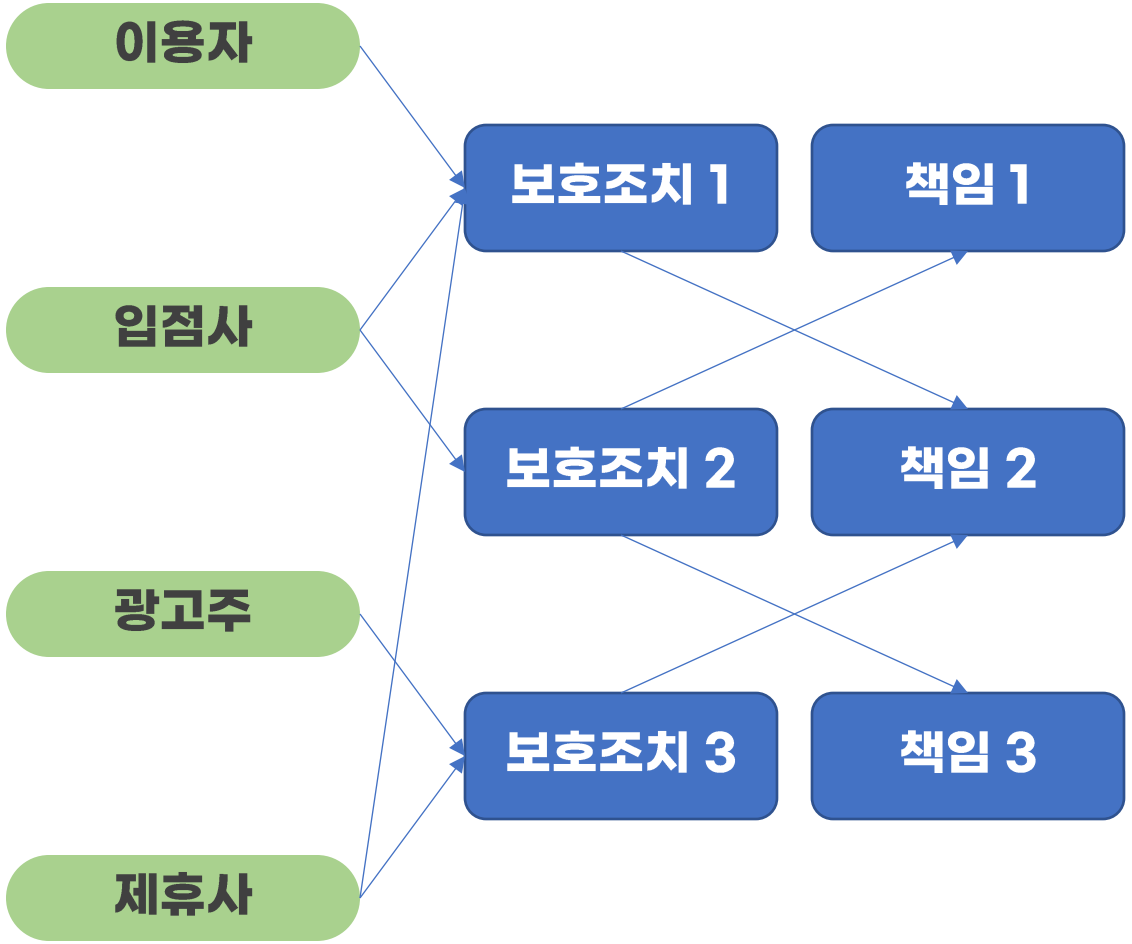
플랫폼 맞춤형 보호 프레임워크: 제안

보호조치와 책임을 이해관계자 별로 매핑하는 구조의 설계

- 3-Layer 구조
  1) 인프라 보안
  2) API·서비스 보안
  3) 참여자 거버넌스

- 원칙 중심적 접근
  : Secure by Design
  : Zero Trust
  : Participants-Driven Security

- 보호조치와 책임을 이해관계자별로 매핑



책임기반 보호조치의 매핑

현장에서 살아 숨쉬는 맵을 구성

이해관계자 no. 7 - ‘픽 미’ 입점 판매자

- **위협 시나리오**
  : 마케팅 업체에 의한 판매자 정보 크롤링
  : 도매업체 가장한 접근
  : 재고 관리 등 시스템 운영 위탁을 가장한 접근

- **보호조치**
  : 크롤링 대응을 위한 캡차 등 기술적 조치
  : 소셜 엔지니어링 방지를 위한 교육
  : 시스템 운영 위탁 제한을 위한 접근제한 적용

- **위협탐지 방식**
  : 정기, 비정기 인터뷰 및 이상행위 탐지 등

- **이해관계자별 위협 시나리오 정의**
  : 이해관계자마다 다른 상황을 반영

- **보호조치 카탈로그 설계**
  : 참여자에 따른 보호조치 카탈로그 설계
  : 이를 책임범위와 연계하여 관리

- **다층 구조**
  : 위협탐지, 사고대응, 취약점 관리 등
  : 입체적으로 설계하되, 이해하기 쉽게

보호수준의 최소 기준과 확장성

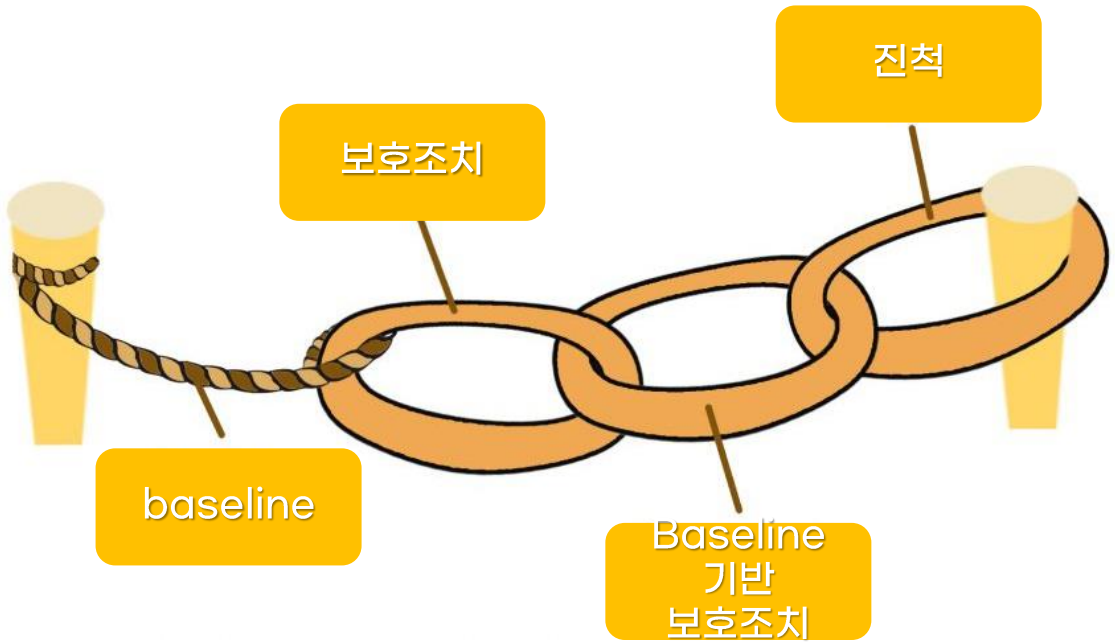
보호조치에 대한 baseline의 설정 및 차등적 보호조치 적용에 대한 인센티브 제시

- Tier-1: baseline
  : 모든 플랫폼에 요구되는 최소 보호조치

- Tier 2~3: differential security
  : 플랫폼 규모
  : 기술 성숙도
  : 특성, 성격, 활동(자율적 보호조치 등)

- **실효성 제고**
  : 자율평가 툴 제공
  : 정부 지원 프로그램과의 연계

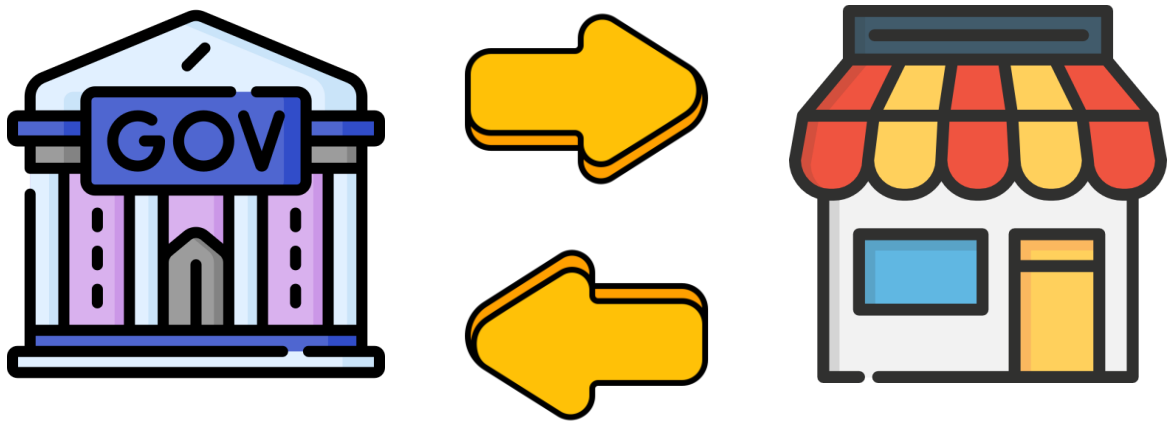
Baseline의 중요성



민관 협력 기반체계 구축

플랫폼을 레버리징할 수 있는 또 하나의 방식

연계, 공유, 협력



레버리징, 경험 전이

- **정보공유센터(ISAC)과 연계**
  : 위협정보 공유체계 확대
  : 플랫폼의 네트워크를 활용

- **정기적 정보 공유**
  : 정부-산업계 간 정기 협의체 구성
  : 현장감 있는 논의에 집중

- **협력 모델 다양화**
  : 보안 교육, 공동 R&D
  : 사고 대응 훈련 등

예상효과 및 기대성과

신뢰의 제고, 비용의 절감, 역량 강화, 그리고 지속 가능한 성장의 지원

보호 수준 강화	→	생태계 신뢰 제고
사고 예방, 대응력 강화	→	사회적 비용 절감
정보보호 역량 확보	→	글로벌 수준 도약
지속 가능한 성장 지원	→	선순환 구조 완성

요약 및 제언

새로운 방향의 필요성 인식 & 함께하는 발전을 지향

기존 체계는 **플랫폼 특성**을 **반영**하지 못하며,
새로운 방향이 필요합니다.

플랫폼 특성에 맞는 정보보호체계를 통해
실효성, 신뢰성, 공공성 모두 확보해야 합니다.

정부-민간-이해관계자가
함께 설계하고 발전시켜야 할 시점입니다.

감사합니다.