POLICY BRIEF

왜 한국에서만 은행 업무를 하려면 이상한 프로그램을 깔아야 할까?

한국 금융 보안 시스템의 구조적 문제와 글로벌 표준 전환 로드맵

(주) 옥소폴리틱스

대표 유호현

2026년 3월

핵심 요약 (Executive Summary)

문제: 한국의 금융 보안 시스템은 은행 업무를 할 때마다 사용자 PC에 5~9개의 보안 프로그램을 강제로 설치하게 한다. 이 프로그램들은 커널(운영체제 최상위) 권한으로 키보드 입력, 네트워크 트래픽, 시스템 정보를 전부 감시한다.

아이러니: 보이스피싱을 막겠다고 만든 이 시스템은 실제 보이스피싱에는 무력하다. 피해자가 속아서 '직접' 돈을 보내는 공격을 키보드 보안 프로그램으로 막을 수 없다. 반면 이 프로그램들 자체가 북한 해커(라자루스 그룹)의 공격 통로로 악용됐다.

해결책: 미국·유럽처럼 보안 책임을 사용자 PC가 아닌 은행 서버에 두면 된다. 토큰화, 3D Secure, FIDO2 등 글로벌 표준은 사용자 PC에 아무것도 설치하지 않고도 더 안전하다.

목차

1 처음엔 이유가 있었다

한국의 금융 보안 시스템이 이렇게 된 데는 이유가 있다. 보이스피싱 피해가 진짜 심각했다.

> **보이스피싱 피해 규모**
>
> - 2023년 피해액 약 **1조 965억 원** (경찰청 통계)
> - 하루 평균 **30억 원**이 사기로 빠져나감
> - 피해자 상당수가 노년층, 전 재산을 잃는 경우 빈번

정부 입장에서 "뭐라도 해야 한다"는 압박이 엄청났다. 그래서 나온 것들이:

위협	대책	결과물
해커가 키보드 입력을 훔쳐볼까봐	키보드 암호화	TouchEn nxKey
악성 프로그램이 은행 화면을 조작할까봐	방화벽	AhnLab Safe Transaction
사용자가 진짜 본인인지 확인	인증서	공인인증서, 보안카드, OTP
사기범 IP를 추적하기 위해	IP 수집	IPinside

출발점 자체는 이해할 수 있다. **문제는 이 대책들이 실제 사기 수법과 전혀 맞지 않는다는 것이다.**

2 왜 엉뚱한 방향으로 갔을까?

보이스피싱이 실제로 작동하는 방식

```
1단계: 전화가 온다
    "검찰입니다. 당신 계좌가 범죄에 연루됐습니다."
    "은행입니다. 대출 금리를 낮춰드릴 수 있습니다."

2단계: 피해자가 속는다
    공포·욕심·신뢰 — 사회공학적 조작

3단계: 피해자가 직접 행동한다
    (a) 직접 돈을 이체하거나
    (b) 원격제어 앱을 직접 설치하거나
    (c) 악성 앱을 직접 설치한다

4단계: 돈이 빠져나간다
```

핵심: 피해자가 속아서 자기 손으로 직접 하는 것이다.

한국의 보안 프로그램은 뭘 막을 수 있나?

보이스피싱 공격 방식	키보드 보안이 막나?	방화벽이 막나?	인증서가 막나?
피해자가 **직접** 이체 버튼을 누름	✗ 못 막음	✗ 못 막음	✗ 못 막음 (본인이니까)
피해자가 **직접** 원격제어 앱 설치	✗ 못 막음	✗ 못 막음	✗ 못 막음
피해자가 **직접** 악성 앱 설치	✗ 못 막음	✗ 못 막음	✗ 못 막음
해커가 몰래 키보드 입력을 훔침	✓ **이것만 막음**	—	—

> 💡 **비유**
>
> 집에 도둑이 현관문을 두드려서 "택배입니다"라고 속이면, 집주인이 직접 문을 열어준다. 이때 창문에 아무리 강화유리를 달아봤자 소용없다.
>
> **한국 정부의 대책은 "창문에 강화유리를 의무적으로 달아라"인 것이다.**

실제로 효과 있는 건 따로 있다

보이스피싱에 진짜 효과 있는 대책은 전부 **서버(은행) 쪽**에서 작동한다:

대책	작동 방식	어디서 작동?
이상거래탐지(FDS)	"이 사람이 평소에 안 하던 패턴으로 큰 돈을 보낸다" → 자동 차단	은행 서버
지연이체	큰 금액 이체 시 30분~1시간 후 실행 → 냉각기간	은행 서버
대포통장 탐지	짧은 시간에 여러 계좌에서 돈이 들어오는 패턴 감지	은행 서버
AI 통화 분석	통화 중 "검찰", "계좌 동결" 등 키워드 감지	통신사 서버

이 중 어느 것도 사용자 PC에 프로그램을 설치할 필요가 없다.

진짜 문제: 책임 떠넘기기

🇰🇷 한국의 실제 논리

사고 발생 → 은행: "우리는 보안 프로그램 설치하라고 했잖아요" → 금감원: "은행이 조치했으니 면책" → **사용자 책임**

보안 프로그램의 진짜 역할:
✗ 해킹을 막는 것 (실제로 못 막음)
✓ 은행의 면책 근거를 만드는 것

🇪🇺 EU PSD2의 논리

사고 발생 → 금융기관이 충분한 서버측 보안 조치를 했는가? → 아니라면 → **금융기관 책임**

은행이 "프로그램 깔라고 했으니 우리 잘못 아냐"가 통하지 않음

"사용자 PC가 위험하니까 통제하겠다" vs "사용자 PC는 통제 불가능하니까 서버에서 막겠다"
같은 문제, 정반대의 접근.

---

3 한국에서만 볼 수 있는 것들

공인인증서 → 공동인증서 (이름만 바뀜)

1999년: 정부가 공인인증서를 만들었다. Internet Explorer의 ActiveX로 구현.

2014년: 박근혜 대통령 "천송이 코트" 발언 — 국민적 불만에 불을 붙임.

2020년 12월: 법을 바꿔서 "공인" → "공동"으로 이름이 바뀜.

2026년 현재: 이름만 바뀌었다. USB에 파일 저장하고, 플러그인 깔고 — 기술 구조는 **27년 전 그대로**다.

한국에만 있는 것	뭔가	왜 이상한가
카드 비밀번호 앞 2자리	온라인 결제 시 4자리 중 앞 2자리만 입력	세계 어디에도 없는 방식. 2자리면 100가지 조합뿐
가상 키패드 숫자 섞기	비밀번호 입력 시 숫자 배열이 매번 바뀜	이걸 구현하는 프로그램 자체에 키로깅 취약점 발견
보안카드	30개의 코드가 인쇄된 플라스틱 카드	잃어버리면 끝, 사진 찍어두면 보안 무력화
SMS 인증 만능주의	모든 거래에 문자 인증번호	미국 NIST는 2016년부터 SMS 인증 비권장 (SIM 스와핑 취약)
30만원 한도	30만원 이상 결제 시 공인인증서 의무 (2014 폐지)	법은 바뀌었지만 은행들이 수년간 계속 강요

4 은행이 깔라는 그 프로그램들

한국 은행 웹사이트에 접속하면 **5개 이상**의 프로그램을 깔라고 한다. KAIST 연구에 따르면 한국인 PC에는 평균 **9개**의 이런 프로그램이 설치되어 있다.

TouchEn nxKey (라온시큐어) — "키보드 보안"

은행이 말하는 용도: 해커가 키보드 입력을 훔쳐보지 못하게 막는 프로그램

실제로 하는 일: 키로거를 막기 위해 **자기 자신이 키로거가 된다**. 운영체제 가장 깊은 곳(커널)에서 모든 키보드 입력을 먼저 가로챈다.

보안 연구자 평가: 2023년 7개의 심각한 취약점 발견. 악성 웹사이트가 이 프로그램을 이용해 키보드 입력을 전부 훔칠 수 있었다.

Chrome 웹스토어: 1,000만+ 설치, 평점 **1.3/5** — 리뷰는 "제발 없애달라"로 가득.

IPinside (인터리젠) — "IP 확인"

은행이 말하는 용도: 접속자의 IP 주소를 확인해 사기 방지

실제로 하는 일: IP 확인은 핑계. **하드 드라이브 시리얼 번호, 설치된 프로그램 목록, 네트워크 설정, 시스템 정보**를 전부 수집한다.

보안 연구자 평가: "이것은 의무 설치 스파이웨어(mandatory spyware)다" — Wladimir Palant

회사 본업: 인터리젠은 빅데이터 수집·분석 전문 회사. 은행·보험사·정부에 데이터를 판매하는 것이 본업.

Veraport (위즈베라) — "보안 프로그램 관리"

은행이 말하는 용도: 필요한 보안 프로그램을 자동 설치해주는 관리자

핵심 문제: 프로그램을 **암호화 없이(HTTP)** 다운로드 → 중간에서 바꿔치기 가능. 자동 업데이트 기능 없음.

2020년: 북한 라자루스 그룹이 이 프로그램을 이용해 악성코드를 배포했다.

AhnLab Safe Transaction (안랩) — "금융 방화벽"

은행이 말하는 용도: 금융 거래 중 악성 프로그램 차단

실제로 하는 일: 운영체제 최상위 권한(커널 레벨)에서 **PC의 모든 네트워크 트래픽을 감시**한다.

핵심 문제: 이 프로그램 자체가 뚫리면 해커가 PC 전체를 장악할 수 있다.

💡 **비유**

은행이 "보안을 위해 당신 집에 CCTV를 설치하겠습니다. 거실, 침실, 화장실 전부요. 아, 그리고 CCTV 시야 확보를 위해 대문도 열어놔야 합니다. 싫으면 통장을 못 쓰셔요"라고 하는 것과 같다.

	일반 앱 (카톡, 크롬 등)	한국 금융 보안 프로그램
권한	제한됨 (내 파일만)	**운영체제 최상위 권한**
감시 범위	해당 앱 내부만	**키보드, 네트워크, 시스템 정보 전체**
선택	안 깔아도 됨	**안 깔면 은행 업무 불가**

5 왜 오히려 위험한가

문을 많이 만들수록 도둑이 들어올 곳이 늘어난다

보안의 가장 기본 원칙: **공격 지점을 최소화하라.**

한국 방식은 정반대다. PC에 커널 레벨 프로그램을 5~9개 깔면, 각각이 독립적인 "문"이 된다. KAIST가 7개 프로그램을 조사했더니 **19개의 심각한 보안 구멍**을 발견했다.

> 💡 **비유**
>
> 집 보안을 강화한다면서 문을 9개 더 뚫어놓은 셈이다. 하나만 부실해도 도둑이 들어온다.

크롬이 만든 보호막을 부순다

최신 브라우저는 **샌드박스**라는 보호 장치가 있다. 웹사이트가 당신의 PC 파일에 접근하지 못하게 격리하는 기술이다. 한국 보안 프로그램들은 이 보호막을 **일부러 뚫고** 나간다.

암호화된 편지를 중간에서 열어본다

```
[ 정상적인 방식 ]
  당신  →  🔒 암호화된 봉투  →  은행

[ 한국식 "보안" ]
  당신  →  🔓 봉투  →  [ 보안 프로그램이 봉투를 열고 내용 확인 ]  →  🔒 새 봉투  →  은행
```

이걸 하려면 보안 프로그램이 PC에 **가짜 자물쇠 열쇠(Root CA)**를 등록한다. 이 열쇠가 해커 손에 들어가면 **한국 전체 인터넷 사용자의 암호화 통신이 무력화**된다. 프로그램을 삭제해도 이 가짜 열쇠는 PC에 남는다.

경비원이 5년째 졸고 있다

KAIST가 한국인 PC 48대를 조사한 결과:

- 보안 프로그램 평균 **9개** 설치
- 상당수가 **수년간 업데이트 안 된** 구버전
- 한국인 **97.4%**가 설치 (거부하면 은행 업무 불가)

> - **59%**는 이 프로그램이 뭘 하는지 모름

6 실제로 털린 사례들

"이론적으로 위험하다"가 아니다. **실제로 일어난 일**이다.

사례 1: 북한 해커가 Veraport로 악성코드를 퍼뜨렸다 (2020)

공격자: 북한 라자루스 그룹 (국가 지원 해킹 조직)

보고: ESET(글로벌 보안업체), 2020년 11월

① 은행·정부 웹사이트가 쓰는 Veraport를 해킹

② 한국 보안업체 2곳의 **디지털 인감을 훔쳐** 악성코드를 정상 프로그램으로 위장

③ Veraport의 자동 설치 기능으로 사용자 PC에 악성코드 배포

④ 사용자 PC를 원격 조종할 수 있는 백도어 설치 완료

보안 프로그램이 악성코드 배달부 노릇을 했다.

사례 2: 북한 해커가 MagicLine4NX를 뚫고 기업 침입 (2023)

경보: 영국 정보기관(NCSC)과 한국 국가정보원(NIS)이 공동으로 경보 발령

① 뉴스 사이트를 해킹해 악성 코드를 심어둠

② 직원이 뉴스를 읽으면, PC에 설치된 MagicLine4NX의 보안 구멍을 공격

③ 이 프로그램을 통해 기업 내부 네트워크 침입 → 기밀 데이터 탈취

의무적으로 설치한 프로그램이 해킹 통로가 됐다. 직원에게는 이 프로그램을 안 깔 권리가 없었다.

사례 3: TouchEn nxKey로 전 국민 키보드를 엿볼 수 있었다 (2023)

발견자: 보안 연구자 Wladimir Palant

- 악성 웹사이트가 TouchEn nxKey를 통해 **사용자의 모든 키보드 입력을 가로챌 수 있음**
- 이 프로그램은 한국 거의 모든 PC에 설치됨 (Chrome 1,000만+ 설치)
- 하나의 취약점으로 **사실상 전 국민의 키보드를 엿볼 수 있는** 상황이었음

키로거를 막겠다고 설치한 프로그램이 **전 국민 규모의 키로거 취약점**을 만들었다.

7 규제가 만든 이권 구조

누가 돈을 벌고 있나

회사	프로그램	특이사항
라온시큐어	TouchEn nxKey	2024년 매출 533억 원, 전년 대비 **52.6% 급증**
위즈베라	Veraport	보안 프로그램 관리 사실상 독점
안랩	Safe Transaction	한국 1위 보안업체
이니텍	INIpay	전자결제·인증
드림시큐리티	MagicLine4NX	북한 해커에 뚫린 그 프로그램

라온시큐어의 매출이 1년 만에 52.6% 급증한 이유? 취약점이 발견돼서 긴급 패치 계약을 따냈기 때문이다. **보안 구멍이 뚫릴수록 매출이 오른다.**

규제 포획(Regulatory Capture) — 이 시스템이 유지되는 이유

```
① 금감원이 "보안 프로그램 설치하라"고 규정
        ↓
② 은행은 규정 따르려고 특정 업체 프로그램 구매
        ↓
③ 업체는 규제가 보장하는 안정 수입
        ↓
④ 보안 구멍 발견 → 패치 계약 → 매출 증가
        ↓
⑤ 규제를 바꿀 인센티브가 아무에게도 없다
        ↓
① 로 돌아감
```

> **금감원:** 규정 바꾸면 "보안을 약화시켰다"는 비난 위험
>
> **은행:** "규정대로 했으니 면책" — 바꿀 이유 없음
>
> **보안업체:** 규제가 매출을 보장 — 바꿀 이유 없음
>
> **퇴직 공무원:** 금융위·금감원 퇴직 후 금융결제원·인증기관 임원으로 이동

사용자에게 선택권은?

없다.

월급 받으려면 → 은행 인터넷뱅킹 → 보안 프로그램 5개 설치

세금 내려면 → 국세청 홈택스 → 보안 프로그램 3개 설치

정부 민원 → 정부24 → 보안 프로그램 2개 설치

거부하면 서비스 자체를 사용할 수 없다.

8 왜 Stripe가 안 되나

해외에서 온라인 결제를 받으려면 Stripe를 쓰면 된다. 코드 몇 줄이면 카드 결제가 된다. 전 세계 수백만 기업이 쓴다. **한국에서는 안 된다.**

🌍 해외 결제 구조

고객 → Stripe → Visa/Mastercard → 카드 발급 은행

(끝. 이게 전부.)

🇰🇷 한국 결제 구조

고객 → PG사 → VAN사 → 개별 카드사

(각 단계마다 수수료, 별도 계약, 별도 인증)

장벽	내용
법인 등록	한국 사업자등록번호 없으면 PG사 가입 불가. 외국 법인은 자격 없음
허가	외국 기업의 한국 결제 서비스 → 금융위원회 허가 필요 (사실상 불가)
프로토콜	한국 카드사의 통신 방식이 세계 표준과 다름
본인인증	국제 표준(3D Secure) 대신 자체 인증(SMS + 공동인증서)

9 다른 나라는 어떻게 하나

보안은 서버에서, 클라이언트는 깨끗하게.

	🇰🇷 한국	🇺🇸 🇪🇺 미국·유럽
기본 전제	"사용자 PC가 위험하니까 통제하자"	"사용자 PC는 통제 불가, 서버에서 막자"
프로그램 설치	5~9개 필수	**0개**
사고 책임	사용자	**금융기관**
온라인 결제	보안 프로그램 + 인증서 + 가상키패드 + SMS	카드 번호 입력 → 끝
은행 이체	보안 프로그램 + 인증서 + OTP	앱에서 지문 인증 → 끝
키로거 방지	커널 드라이버로 키보드 가로챔	TLS 암호화 (설치 필요 없음)

글로벌 표준 기술들

토큰화 (Tokenization): Apple Pay로 결제하면 실제 카드 번호가 가맹점에 전달되지 않는다. 일회용 가짜 번호(토큰)를 보낸다. 해커가 훔쳐도 쓸모없다.

3D Secure 2.0: 평소와 같은 결제는 자동 통과. 이상한 결제(새벽 3시 해외 고가 구매)만 추가 인증. 프로그램 설치 없이 브라우저에서 동작.

FIDO2/WebAuthn: 비밀번호 대신 지문이나 얼굴인식. 모든 주요 브라우저에 이미 내장. 피싱에 원천 면역(가짜 사이트에서 작동 안 함). Apple, Google, Microsoft 전부 지원.

10 정책 전환 로드맵

Phase 1 — 즉시 실행 (6개월 이내)

① 클라이언트 보안 프로그램 강제 설치 폐지

금감원의 전자금융감독규정 개정. 글로벌 표준(PCI DSS, 3D Secure 2.0)을 충족하면 클라이언트 프로그램 설치 면제.

개정 대상: 전자금융감독규정 제15조(이용자 보호) 내 "이용자 단말기 보호" 조항

② FIDO2/WebAuthn 인증 전면 도입

공동인증서·SMS OTP를 FIDO2로 대체. 이미 아이폰·갤럭시에 내장된 기술. 프로그램 설치 불필요, 피싱에 강함.

참고: 금융결제원이 이미 FIDO 기반 인증 표준을 발표했으나 도입이 미진

③ PCI DSS 의무화

한국 PG사·카드사에 PCI DSS 인증을 의무화. 서버 보안이 올라가면 클라이언트 의존도가 자연스럽게 감소.

Phase 2 — 중기 과제 (1~2년)

④ 글로벌 PG 시장 개방

전자금융거래법 개정. Stripe, Adyen 등 글로벌 PG사가 한국에서 직접 영업할 수 있게 허용. 경쟁이 생기면 수수료가 낮아지고 기술 혁신이 가속.

개정 대상: 전자금융거래법 제28조(전자금융업의 허가·등록) — 외국 법인 허가 요건 완화

⑤ 독립적 보안 감사 의무화

금융보안원(FSec)의 인증 외에, 독립적 제3자 보안 감사를 의무화. 취약점 공개(responsible disclosure) 절차를 법제화.

⑥ Root CA 등록 금지

금융 보안 프로그램이 브라우저의 HTTPS 암호화를 중간에서 풀어보는 행위를 법으로 금지.

Phase 3 — 구조 개혁

규제 철학 전환: "뭘 깔아라" → "뭘 달성해라"

지금: "키보드 보안 프로그램을 설치해야 한다" (특정 기술을 지정)

바꾸면: "키 입력이 제3자에게 노출되지 않아야 한다" (목표만 지정)

목표만 정해주면 은행이 가장 좋은 기술을 자유롭게 선택할 수 있다. 특정 업체 프로그램을 강제할 이유가 사라진다.

⑧ 사고 책임을 금융기관으로

지금: "프로그램 안 깔았으니 사용자 책임"

바꾸면: "서버 보안이 부족했으니 금융기관 책임" (EU PSD2 모델)

책임이 금융기관에 가면, "프로그램 깔라고 했으니 우리 잘못 아냐"가 통하지 않는다.

참고 법령: EU Payment Services Directive 2 (PSD2) Article 73 — 금융기관의 무과실 책임 원칙

⑨ 회전문 인사 차단

금융위·금감원 퇴직 공무원의 금융결제원·인증기관·보안업체 취업 제한을 강화해야 이권 구조가 깨진다. 이것이 규제 포획(Regulatory Capture) — 규제가 시민이 아니라 피규제 업체의 이익을 위해 작동하는 현상이다.

개정 대상: 공직자윤리법 제17조(취업 제한) — 금융보안 관련 업체를 취업 제한 기관으로 추가 지정

Phase별 기대 효과

Phase	시기	핵심 변화	시민 체감
1	6개월 이내	프로그램 강제 설치 폐지, FIDO2 도입	"은행 사이트에서 프로그램 안 깔아도 된다!"
2	1~2년	글로벌 PG 진입, 보안 감사 강화	"해외 사이트처럼 결제가 간편해졌다"
3	2~3년	규제 철학 전환, 책임 재배치	"사고 나면 은행이 책임진다"

11 정치인을 위한 공약 가이드

아래는 국회의원·시장·도지사·대통령 후보가 **바로 공약으로 내걸 수 있는** 구체적 항목이다. 각 공약에 필요한 법령 개정 사항과 시민이 체감하는 변화를 함께 정리했다.

공약 1: "은행 사이트에서 프로그램 강제 설치를 폐지하겠습니다"

시민 체감: 은행 웹사이트에 접속할 때 프로그램 5개를 깔지 않아도 된다.

필요 조치:

- 전자금융감독규정 제15조 개정 — "이용자 단말기 보호" 조항을 "서버측 보안 조치로 대체 가능"으로 변경
- 금감원 행정지도 변경 — 글로벌 표준(PCI DSS, 3D Secure 2.0) 충족 시 클라이언트 프로그램 면제

해외 사례: 미국·유럽·일본의 어떤 은행도 PC에 보안 프로그램 설치를 강제하지 않는다

공약 2: "금융사고 책임을 은행에 지우겠습니다"

시민 체감: 보이스피싱·해킹 피해 시 "프로그램 안 깔았으니 당신 책임"이 아니라, 은행이 서버 보안을 충분히 했는지를 따진다.

필요 조치:

- 전자금융거래법 제9조(금융기관의 책임) 개정 — EU PSD2 Article 73 모델 도입
- 현행: 이용자 고의·중과실 시 금융기관 면책 → 개정: 금융기관이 충분한 서버측 보안을 입증하지 못하면 금융기관 책임

효과: 은행이 "프로그램 깔라고 했으니 면책"이 통하지 않으면, 진짜 보안(서버측 이상거래탐지, 토큰화)에 투자할 수밖에 없다

공약 3: "지문·얼굴 인증으로 공인인증서를 대체하겠습니다"

시민 체감: USB에 인증서 복사하고, 비밀번호 치고, 플러그인 깔던 시대가 끝난다. 스마트폰 지문이나 얼굴로 인증.

필요 조치:

- 전자서명법 시행령 개정 — FIDO2/WebAuthn을 전자서명 수단으로 명시 인정
- 금융결제원 인증 표준 개정 — FIDO2 기반 인증을 공동인증서와 동등하게 인정

해외 사례: Apple, Google, Microsoft가 이미 지원. 피싱에 원천 면역(가짜 사이트에서 작동 안 함)

공약 4: "한국 기업이 해외에서도 쉽게 결제를 받을 수 있게 하겠습니다"

시민 체감: 한국 스타트업·소상공인이 해외 고객에게 결제를 받기가 쉬워진다. 국내 결제 수수료도 낮아진다.

필요 조치:

- 전자금융거래법 제28조 개정 — PG 허가 요건을 국제 표준 기반으로 현대화
- VAN 의무 경유 폐지 — 카드사 직접 연결(Direct Connection) 허용으로 수수료 인하
- 3D Secure 국제 표준 채택 — 한국 결제 시스템이 세계와 호환되게 전환

효과: 한국 기업이 해외 판로를 열 때 결제 인프라가 걸림돌이 되지 않는다. 소비자도 결제 과정이 간편해진다

공약 5: "금융 보안 프로그램이 내 PC를 감시하지 못하게 하겠습니다"

시민 체감: 은행 프로그램이 내 하드디스크 시리얼 번호, 설치 프로그램 목록, 네트워크 트래픽을 들여다보지 못한다.

필요 조치:

- 정보통신망법 또는 전자금융거래법에 "금융 보안 프로그램의 수집 범위 제한" 조항 신설
- 금융 보안 프로그램의 Root CA 등록(HTTPS 중간 복호화) 금지
- 수집 데이터 범위·보관기간·제3자 제공 여부를 이용자에게 명시 고지 의무화

근거: 보안 연구자 Palant — IPinside를 "의무 설치 스파이웨어"로 규정

공약 6: "금융 보안 소프트웨어를 독립 기관이 감사하게 하겠습니다"

시민 체감: 내 PC에 깔리는 프로그램이 최소한 안전한지 누군가가 제대로 검증한다.

필요 조치:

- 금융보안원(FSec) 인증 외에, 국제 인증(Common Criteria 등) 또는 독립 제3자 보안 감사 의무화
- 취약점 공개(Responsible Disclosure) 절차 법제화 — 발견자 보호, 90일 내 패치 의무
- 보안 프로그램 자동 업데이트 의무화 — "수년간 방치된 구버전" 방지

근거: KAIST 연구 — 한국인 PC에 평균 9개 보안 프로그램, 다수가 수년간 업데이트 안 된 구버전

공약 7: "금융위·금감원 퇴직자의 보안업체 취업을 제한하겠습니다"

시민 체감: "규제하는 사람이 규제받는 회사로 가는" 회전문이 막히면, 규제가 업체 이익이 아니라 시민 보호를 위해 작동한다.

필요 조치:

- 공직자윤리법 제17조 개정 — 금융보안 관련 업체(라온시큐어, 위즈베라, 이니텍 등)를 취업 제한 기관으로 추가 지정
- 금융결제원·한국정보인증 등 인증 관련 기관도 취업 제한 대상에 포함
- 제한 기간: 퇴직 후 최소 3년 (현행 2년에서 확대)

공약 8: "규제를 '기술 지정'에서 '목표 지정'으로 바꾸겠습니다"

시민 체감: 특정 업체의 특정 프로그램을 강제로 깔 필요가 없어진다. 은행이 가장 좋은 기술을 자유롭게 선택.

필요 조치:

- 전자금융감독규정 전면 개정 — "키보드 보안 프로그램을 설치해야 한다"(기술 지정) → "키 입력이 제3자에게 노출되지 않아야 한다"(목표 지정)
- 금융보안원 기술 인증 기준을 결과 기반(outcome-based)으로 전환

효과: 은행이 TLS, FIDO2, 서버측 암호화 등 최적의 기술을 자유롭게 채택. 특정 업체 독점 구조 해체

공약 요약표 — 한눈에 보기

공약	시민이 느끼는 변화	핵심 법령	난이도
1. 프로그램 강제 설치 폐지	은행 사이트 접속이 깨끗해진다	전자금융감독규정 제15조	★★☆
2. 금융사고 책임 전환	해킹 피해 시 은행이 책임	전자금융거래법 제9조	★★★
3. 지문·얼굴 인증 도입	인증서·비밀번호에서 해방	전자서명법 시행령	★★☆
4. 결제 인프라 현대화	한국 기업 해외 진출 용이, 수수료 인하	전자금융거래법 제28조	★★★
5. PC 감시 범위 제한	내 PC 정보가 보호된다	정보통신망법 신설 조항	★★☆
6. 독립 보안 감사	프로그램이 최소한 안전	금융보안원 인증 기준 개정	★★☆
7. 회전문 인사 차단	규제가 시민 편에 선다	공직자윤리법 제17조	★★★
8. 목표 기반 규제 전환	특정 프로그램 강제 종료	전자금융감독규정 전면 개정	★★★

이 8개 공약의 핵심은 하나다:
"보안의 책임을 사용자 PC에서 금융기관 서버로 옮긴다."
다른 나라는 이미 다 하고 있는 것이다.

한 줄 요약

한국의 금융 보안 프로그램은 **보이스피싱을 막지 못하고**, **북한 해커에게 문을 열어줬으며**, **은행의 면책 도구로 기능하면서**, **규제가 만든 이권으로 소수 업체에 매년 수백억 원을 보장해주는** 시스템이다.

해결책은 간단하다: 다른 나라처럼 **서버에서 막고, 책임을 금융기관에 두면** 된다.

12 출처

보안 연구 (기술적 분석)

- Wladimir Palant, "South Korea's online security dead end" (2023.01) — palant.info
- Palant, "TouchEn nxKey: The keylogging anti-keylogger solution" (2023.01) — palant.info
- Palant, "IPinside: Korea's mandatory spyware" (2023.01) — palant.info
- Palant, "Weakening TLS protection, South Korean style" (2023.02) — palant.info
- KAIST / USENIX Security 2025, "Too Much of a Good Thing" — usenix.org (PDF)

실제 해킹 사례

- ESET, "Lazarus supply-chain attack in South Korea" (2020.11) — welivesecurity.com
- BleepingComputer, "North Korean hackers exploited MagicLine4NX zero-day" (2023) — bleepingcomputer.com
- AhnLab ASEC, "RaonSecure 제품 보안 권고" (2024) — asec.ahnlab.com

규제 및 시장

- The Register, "South Korea kills ActiveX-based government digital certificate service" (2020.12) — theregister.com
- 바이라인네트워크, "공인인증서가 결국 폐지되기까지" (2020.12) — byline.network

결제 시스템

- Stripe, "How to accept payments in South Korea" — stripe.com
- The Paypers, "South Korea: 2025 analysis of payments and ecommerce trends" — thepaypers.com

---