『 선제적인 정보보호를 위한 전략과 거버넌스 』

2013. 12

KB국민은행 정보보호본부

KB 국민은행

KB 금융그룹

목 차

정보보호 관리상 이슈 – 보안관리 발전 동향

KB정보보호본부

기존 외부 침입 대응 중심에서 내/외부 통합 관점의 보안관리 필요성 증가

외부 침입	내부 보안 통제	컴플라이언스
외부로부터의 위협 증대 ✓ DDOS ✓ Zero Day Attack ✓ Watering hole ✓ Spear Phishing	**부주의 또는 악의적인 내부자의 정보유출** ✓ 관리자의 관리소홀 ✓ 부주의한 내부자 행동 ✓ 정보 오남용 ✓ 악의적인 정보유출	**규제의 지속적 강화 또는 중복** ✓ ISO27001 ✓ 신용정보보호법 (1995.1, 2009.4) ✓ 개인정보보호법 (2011.9) ✓ 정보통신망법 개정안 (2012.8) ✓ 금융전산 보안강화대책(2013.7) ✓ 내부 규정/지침

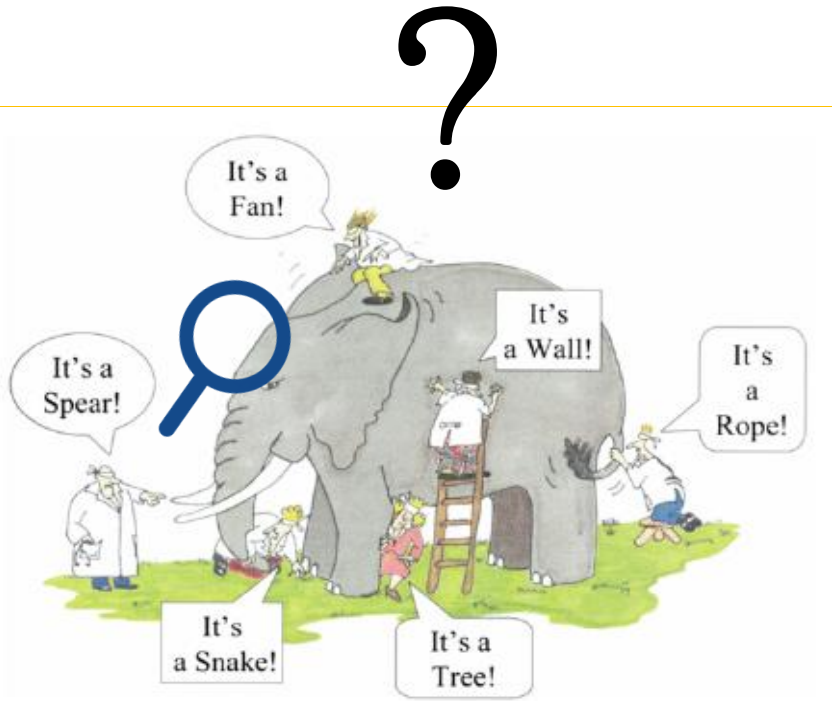
외부 위협과 내부 위협의 혼재, 구분 모호 : APT

규제에 따른 통제 범위 중복 : 개인정보

정보보호 관리상 이슈 – 보안관리의 한계점

KB정보보호본부

최근의 보안위협은 기존 대응체계로 탐지/대응 한계 !!



편리성 위주의 통제

- ✓ 시스템 운영위주의 통제
- ✓ 중요권한을 보유한 계정 탈취
- ✓ 상대적으로 취약한 내부 망 영역

단편 이벤트 위주 탐지

- ✓ 단순 기능위주의 보안솔루션
- ✓ 기술기반의 이벤트 위주 탐지
- ✓ 단편적인 정보 수집

분석 데이터 부족

- ✓ F/W, IDS등의 네트워 이벤트 위주
- ✓ Endpoint수집 데이터 미흡/부재
- ✓ OS/어플리케이션 감사데이터 부재

임계치 기반 관제

- ✓ 임계치 설정의 적정성
- ✓ 통계기반 무시/누락되는 유효한 공격
- ✓ Rule 분석전문가의 부족

지능화된 공격

- ✓ 알려지지 않은 공격(제로데이공격)
- ✓ 보안장비 탐지 한계(암호화통신)
- ✓ 탐지이하(소량)의 이벤트(APT공격)

KB국민은행

정보보호 관리상 이슈 – 통합관리의 필요성

KB정보보호본부

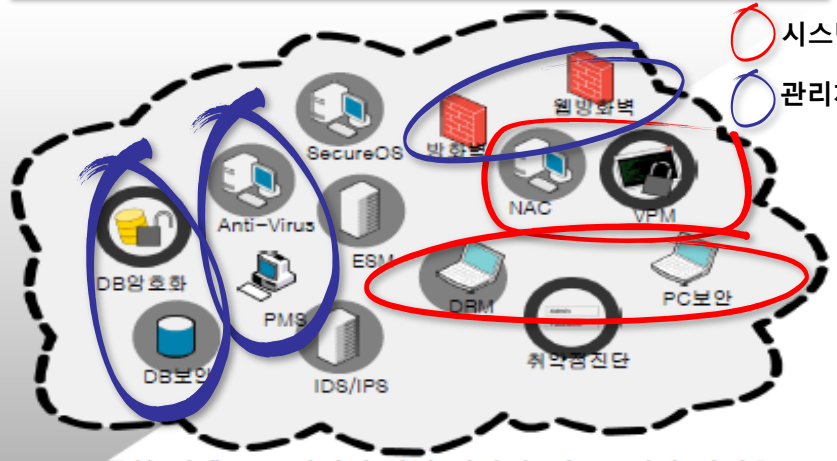
장기적 관점에서 보안시스템과 관리체계 통합 전략 필요

Case by Case로 도입된 방대한 프로세스와 솔루션

상호 연계성 및 일관성이 부족한 프로세스

- 중복된 내용의 서로 다른 업무를 담당자별로 개별 처리
- 감독기관 등의 요구에 대응하는 방식의 업무로 지속성 부족

개별 사상(思想)을 가진 정보보호 솔루션



시스템 통합 필요

관리체계 통합 필요

- 통합 설계로 도입되지 않아 일관된 rule 부여가 어려움
- 방대한 보안 이벤트에서 의미있는 정보는? (Big Data 이슈)

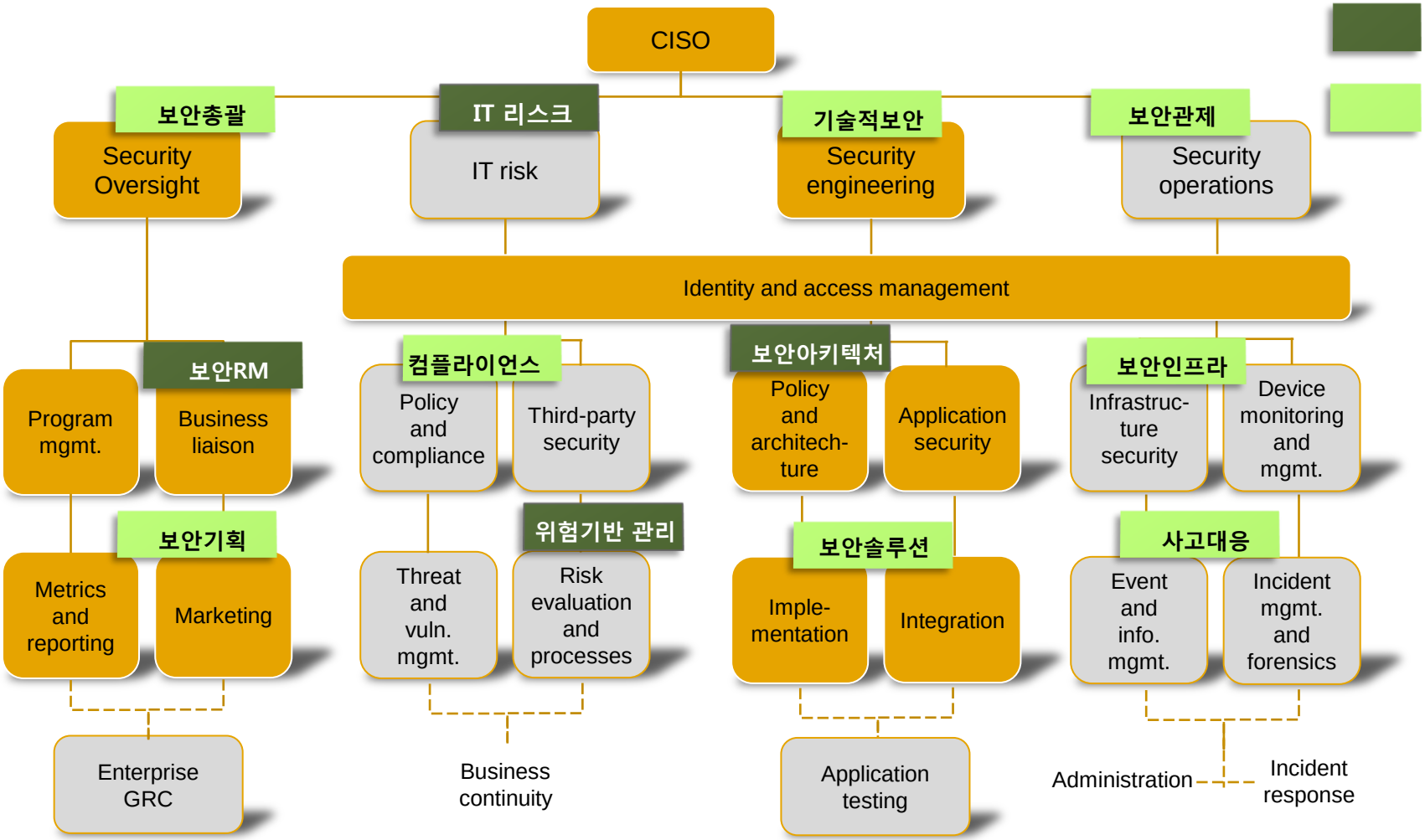
전사 통합 보안 관점에서 중복/누락에 따른 비효율성 존재

출처 : ERNST & YOUNG

KB국민은행

정보보호 거버넌스 체계 – 선진 보안 거버넌스

KB정보보호본부



출처 : Forrester Research, 2010

KB 국민은행

정보보호 거버넌스 체계 – KB국민은행 보안조직의 변화

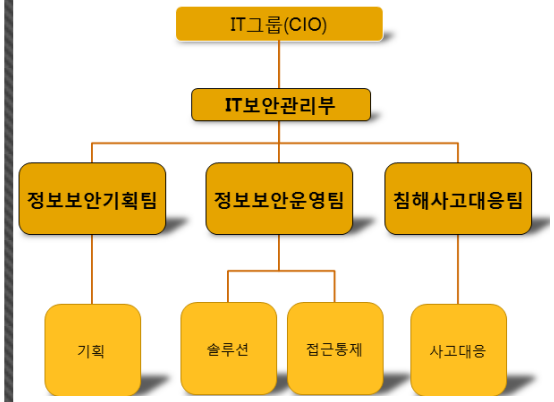
KB정보보호본부

정보보안팀

- 1개팀
- 인원 : 15명
- 연간예산 : 00억
- 인프라기반 투자
- 외부 위협대응
  (7.7 DDoS 대란, 2009년)

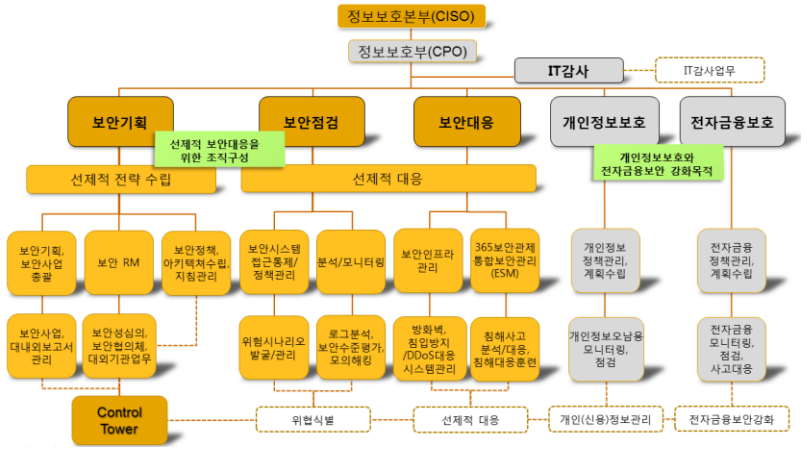
IT보안관리부

- 3개팀
- 인원 : 18명
- 연간예산 : 00억(↑ 100%)
- 솔루션기반 투자
- 내부 위협대응
  (3.20 사이버테러, 2013년)



정보보호본부

- 1본부(CISO) 1부(CPO) 6개팀
- 인원 : 35명
- 연간예산 : 000억(↑ 200%)
- 인적자원기반 투자
- 내/외부 통합 보안관리 + Compliance
- 정보보안 + 정보보호



KB 국민은행

정보보호 거버넌스 체계 – KB국민은행 정보보호 거버넌스

KB정보보호본부

- IT정보보안 기획 총괄
- IT사고예방, 대응 및 내부통제 업무
- IT관련 보안시스템 운영
- 사이버 침해사고 대응
- IT보안성심의 및 정보보안 제규정관리
- IT 및 구매업무 감사

- 전자금융거래의 정보보안업무 총괄
- 전자금융 업무의 대고객 정보보안 정책수립 및 실행

- 신용정보관리·보호 내부관리규정
- 신용정보관리·보호관련 고충의 처리
- 임직원 신용정보관리·보호 관련법령 및 내부관리규정 준수여부 점검
- 신용정보주체의 권리행사 이행여부 점검
- 임직원 신용정보 관리·보호 교육 등

- 개인정보 보호계획 수립 및 시행
- 개인정보 처리실태·관행의 조사 및 개선
- 개인정보 처리 불만 및 피해 구제
- 개인정보유출/오남용 통제시스템 구축
- 개인정보 보호교육 계획수립 및 시행
- 개인정보파일 보호 및 관리감독
- 개인정보 처리방침 수립 및 시행 등

KB국민은행

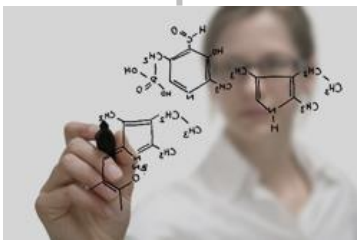
선제적인 정보보호전략

KB정보보호본부

전략

탐지

대응



분석

선제적인 정보보호전략

KB정보보호본부

보안전략

- ✓ 관리적보안 중점 강화
- ✓ 보안 아키텍쳐 수립
- ✓ 중장기적 관점의 사업계획 수립

위험 탐지

- ✓ 계량화를 통한 보안수준 점검
- ✓ 보안 시스템 로그모니터링
- ✓ 24*265 보안관제 운영
- ✓ 위험수준 가시화

선제적 대응

- ✓ 보안위험단계 수립 및 대응절차 마련
- ✓ 보안위험 정도에 따른 대응조치
- ✓ 유사 위협 행위에 대한 선제적 방어
- ✓ 자체 정책에 의한 실시간 방어 체제 구축

위협 분석

- ✓ 보안시스템 로그 상관관계 분석
- ✓ 로그분석을 통한 위협시나리오 도출
- ✓ 위협시나리오를 통한 보안위험 발굴

선제적인 정보보호를 위한 전략과 거버넌스

KB국민은행

선제적인 정보보호전략 - 보안전략

외부공격

DDoS

1차 방어

내부공격

Virus

2차 방어

사회공학적 공격

APT공격

ZeroDay Attack

3차 방어

기술적 보안

관리적 보안

Infra Based Security

네트워크보안시스템

Internet

Solution Based Security

PC보안 솔루션

침해방지

유출방지

시스템접근통제

Risk Based Security

모니터링

계량화

리스크분석

위협 시나리오도출

RULE

위협식별

대응

선제적 대응

선제적인 정보보호전략 - 위험탐지

탐지

"측정할 수 없다면 관리할 수 없다" - 피터 드러커

RAW 데이터의 수집 및 저장 → 데이터 분석을 통한 위협 정보 실시간 제공 → 기존의 공격 모델을 기반으로 침해 사고 탐지 → 위험 경고를 통한 신속한 대응

침해사고의 증가 | 보안장비의 증가 | 공격 피해의 심각성 심화 | 다수의 보안장비 관리의 어려움

KB 국민은행

선제적인 정보보호전략 - 위험탐지

탐지

DashBoard

대상	위협경로	정보유출 위험 통제방안	비인가 접근 통제방안
업무용 PC			
고객 PC			
자동화기기			
서버			
DB서버			
네트워크			
업무용 모바일			
고객용 모바일			
웹 프로그램			

보안 위험관리 현황표(DashBoard)

저
중
고

대상		보안수준 등급
PC	영업점	
	본부	
	콜센터	
	IT개발부서	
	IT운영부서	
	전자금융	
	외주업체	
서버	인터넷뱅킹	
	업무	
	중계	
	DB	
	보안	
네트워크	외부망	
	내부망	
	무선망	
자동화기기	점내	
	점외	
사무용기기	복합기	
모바일기기	스마트폰	
	태블릿	
웹 프로그램	외부망 사용	
	내부망 사용	

선제적인 정보보호전략 - 위협분석

분석

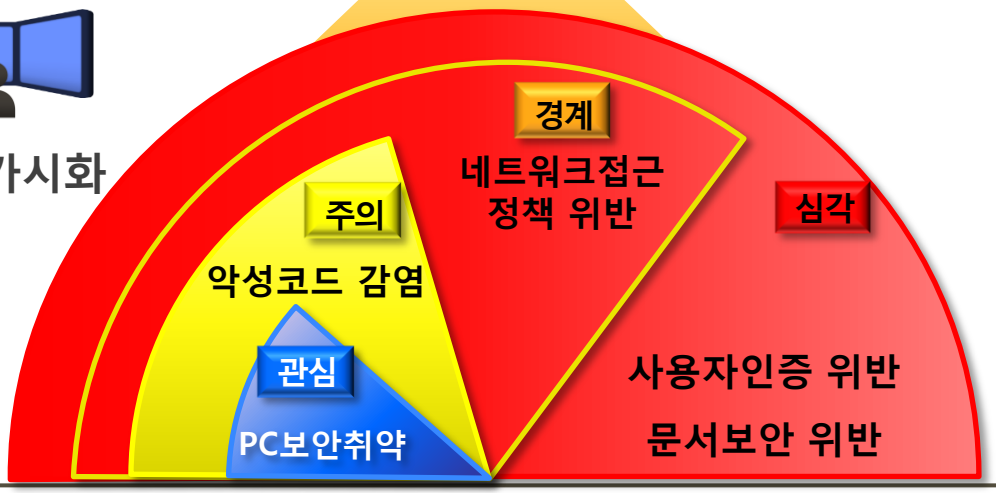
보안시스템 모니터링을 통해 위협을 분석하고, Rule을 만들어 위협을 가시화

보안시스템

네트워크접근	안티바이러스	패치관리	계정관리	사용자인증	문서보안
내부침입방지	내부침입방지	내부침입방지	시스템접근통제	시스템접근통제	정보유출방지

로그 분석 + 위협 시나리오 = 위협식별 RULE

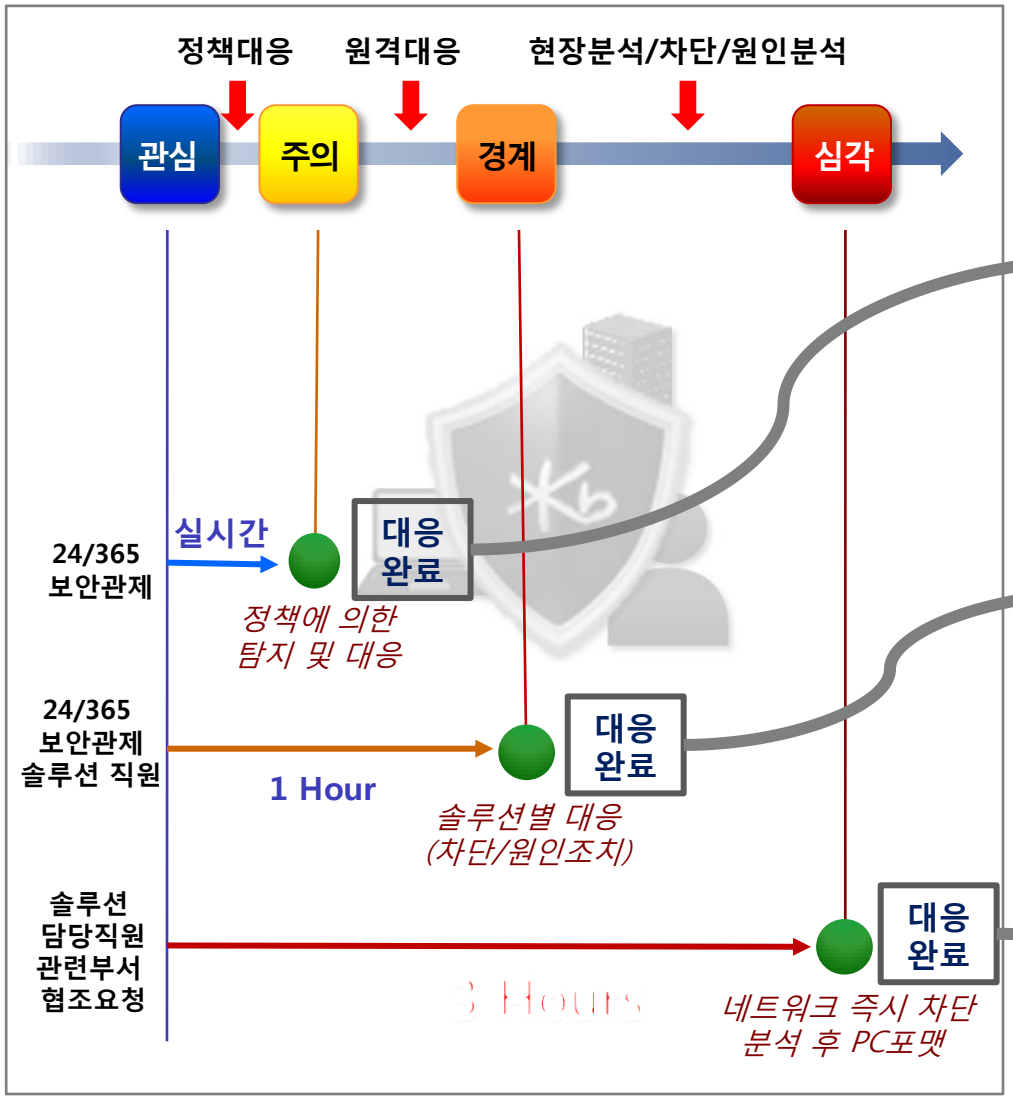
위협의 가시화



KB 국민은행

선제적인 정보보호전략 – 선제적 대응

대응



위협 유형	대 응
주의	
보안위반 S/W 사용	▪ 탐지 PC 1:1 점검 및 프로그램 삭제 ▪ 해당 컨텐츠 보안시스템 차단
기타 보안 위협	▪ 위협별 각종 보안시스템 이용 차단 (IP/URL 차단 및 패턴업데이트 등)
경계	
악성코드 감염	▪ 감염 PC 1:1 수동 점검 및 조치 ▪ 감염 경로 및 악성코드 유포지 차단
피싱/파밍	▪ 금융위원회/KISA에 피싱 신고 ▪ ISP업체 피싱 차단여부 확인
심각	
해킹	▪ 해당 네트워 단절 ▪ 전문 보안업체 포렌식 진행
DDoS 공격	▪ DDoS 차단시스템에 의한 공격 차단 ▪ 센터별 트래픽 분산처리 ▪ 금융ISAC 연계 비상대피소 활용

KB 국민은행

사례 연구

사례연구 – 고객정보 유출방지

전략

암호화 위주의 유출방지와 통제

▣ PC 문서 암호화

✓ 일부 문서만 암호화
- 엑셀, 워드, 파워포인트, PDF

단편적인 요구사항도출

▣ 파일 반출, USB 사용 통제

✓ 파일 반출 및 USB 사용 허용 시 책임자 승인 처리

사용자 편의보다 보안 중심의 통제

▣ 사용 절차

✓ 암호화 문서 반출 신청/승인(15단계)
✓ USB 사용 요청 시 마다 재로그인

법규강화로 추가요건발생

사용자편의성 개선필요

고객정보 유출방지 시스템

▣ PC 문서 암호화 확대

✓ 모든 문서 암호화 확대
- 엑셀, 워드, 파워포인트, PDF, 그림, TXT 등
- 보고서툴에 의해 생성된 DB 데이터 파일 등

▣ 파일 반출, USB 사용 통제 강화

✓ 파일 반출 및 USB 사용시 뿐만 아니라 문서 출력 및 USB 저장 시에도 개인정보 포함여부 자동 검사 및 책임자 승인 절차 적용

비용 발생

▣ 사용 절차 간소화

✓ 암호화 문서 반출 신청/승인(15단계 → 7단계)
✓ USB 사용 요청 시 재로그인 절차없이 즉시 사용 (재로그인 미 진행 시 기존 30분 이상 소요)

▣ 사용자 편의성 개선

✓ 반출신청 작성으로 즉시 이동(마우스 원 클릭)
✓ 팝업 알림 메시지 제공(반출승인 요청 및 결재 완료 시)

안정성저하

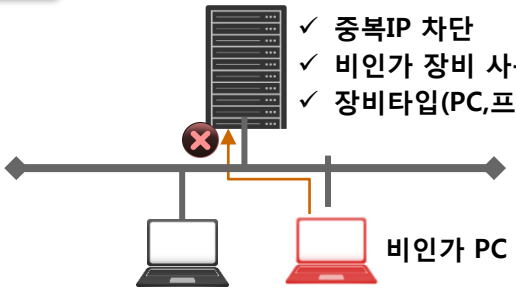
사례연구 – 시스템 통합

IP주소관리 & 네트워크접근제어 시스템

네트워크담당부서
(네트워크장비)

IP주소관리시스템

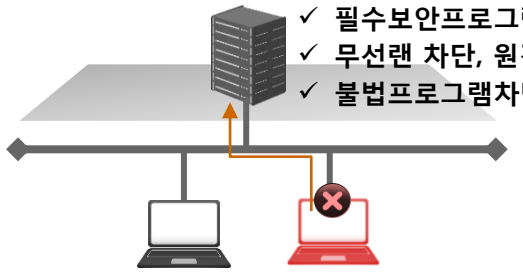
- ✓ 중복IP 차단
- ✓ 비인가 장비 사용 차단
- ✓ 장비타입(PC,프린터등)구분



보안부서
(보안시스템)

네트워크접근제어(NAC)시스템

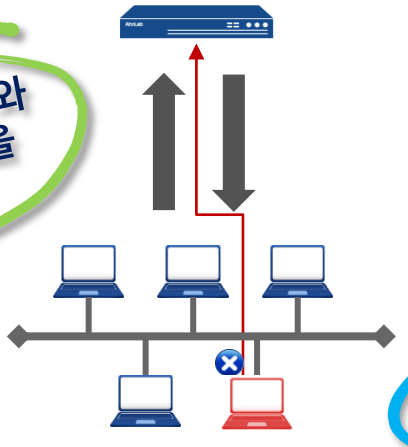
- ✓ 필수보안프로그램설치점검
- ✓ 무선랜 차단, 원격차단
- ✓ 불법프로그램차단



네트워크장비와
보안시스템을
통합구축

통합네트워크접근제어 시스템

단일서버구성



- ✓ 중복IP 차단
- ✓ 비인가 장비 사용 차단
- ✓ 장비타입(PC,프린터등)구분
- ✓ 필수보안프로그램설치점검
- ✓ 무선랜 차단, 원격차단
- ✓ 불법프로그램차단

+α

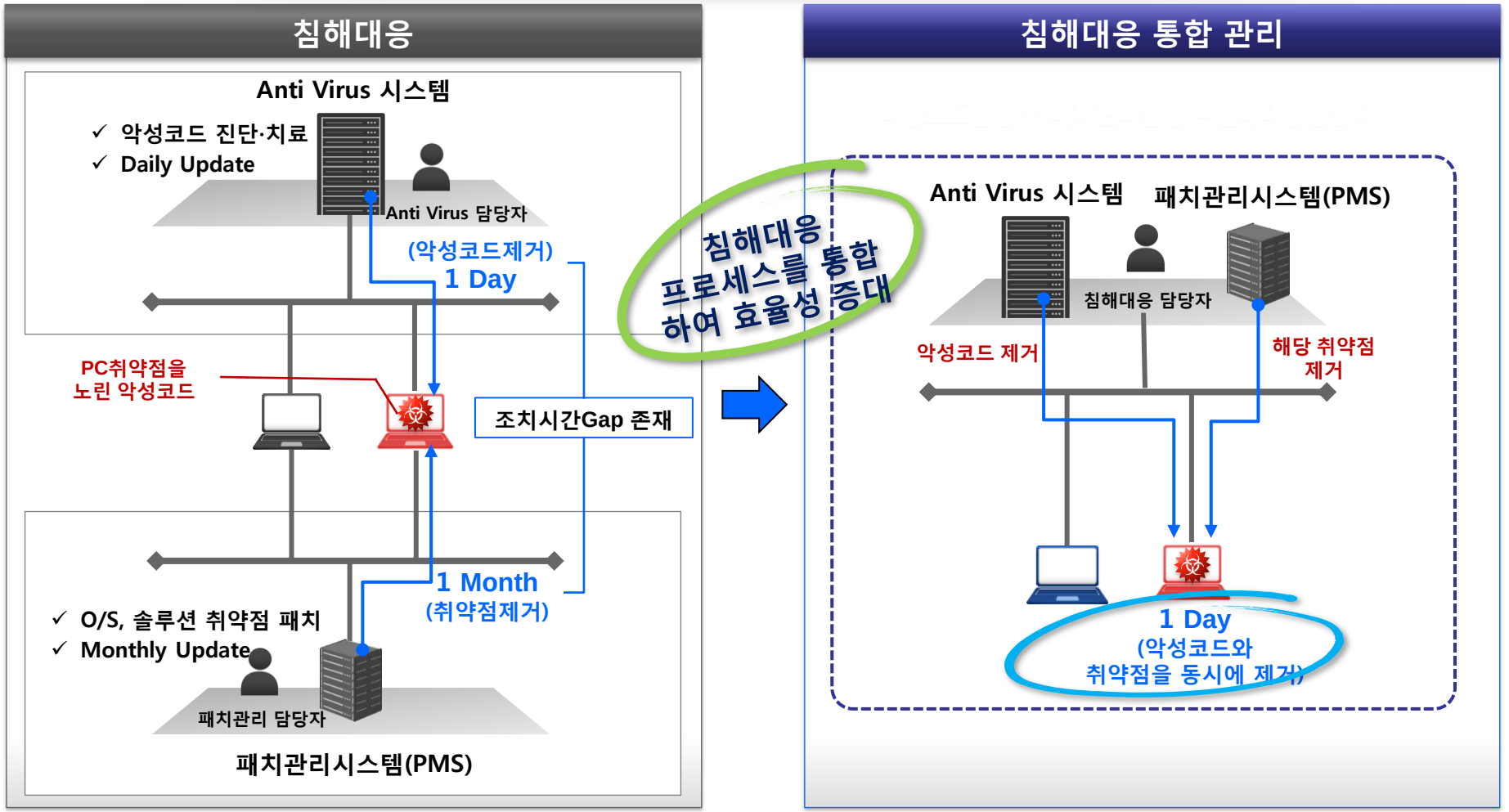
- ✓ 은행전체 IP 실명제
- ✓ NAC Agent 미설치 탐지

편의성

안정성

TCO 절감

사례연구 – 관리체계 통합


침해대응
Anti Virus 시스템
✓ 악성코드 진단·치료
✓ Daily Update
Anti Virus 담당자
(악성코드제거)
1 Day
PC취약점을
노린 악성코드
조치시간Gap 존재
1 Month
(취약점제거)
✓ O/S, 솔루션 취약점 패치
✓ Monthly Update
패치관리 담당자
패치관리시스템(PMS)
침해대응
프로세스를 통합
하여 효율성 증대
침해대응 통합 관리
Anti Virus 시스템
패치관리시스템(PMS)
침해대응 담당자
악성코드 제거
해당 취약점
제거
1 Day
(악성코드와
취약점을 동시에 제거)

사례연구 – 위협분석시스템

분석

보안시스템 위협 식별 요소

네트워크접근	안티바이러스	패치관리	계정관리	사용자인증	문서보안
프린터로 할당 된 IP	키로깅 악성코드발견	보안 취약점 패치 미적용	시스템 접근이력 탐지	보안토큰 미사용 PC	DRM 미설치

프린터 IP로 위장한후 **악성코드**를 유포, **계정탈취** 및 DB서버로부터 **고객정보 유출** 시도

위협식별 Rule

Rule NO	위협 시나리오	위협수준	위협내용
Rule 1	**프린터IP + 악성코드감염 + PC취약점존재 + 시스템 접근이력 + 토큰미사용 + DRM미설치**	**심각**	**정보유출 가능성**
Rule 2	프린터IP + 악성코드감염 + PC취약점존재	경계	내부침입 가능성
Rule 3	프린터IP + 악성코드감염	주의	비인가접근 시도

위협분석시스템

KB 국민은행

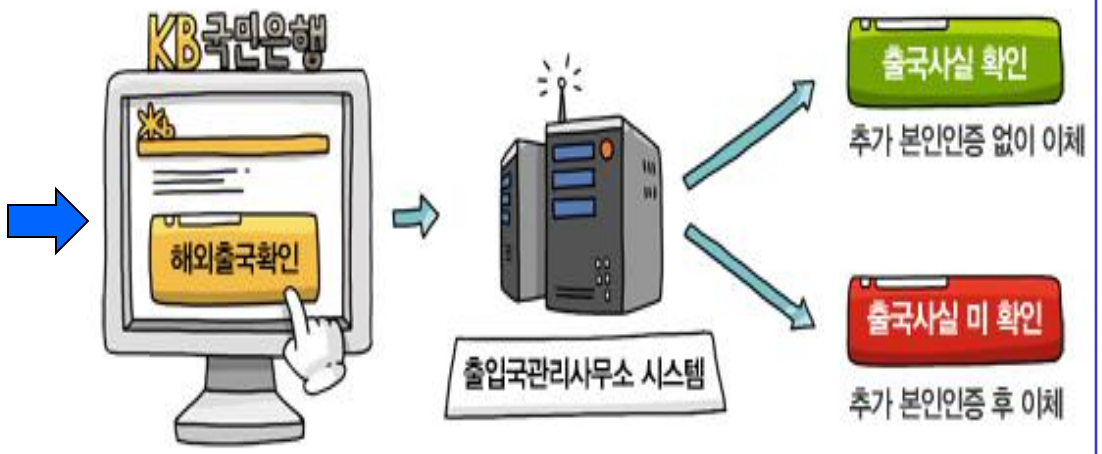
사례연구 – 룰에 의한 전자금융사기 대응

대응

❑ 이체거래 시 이상징후 유형

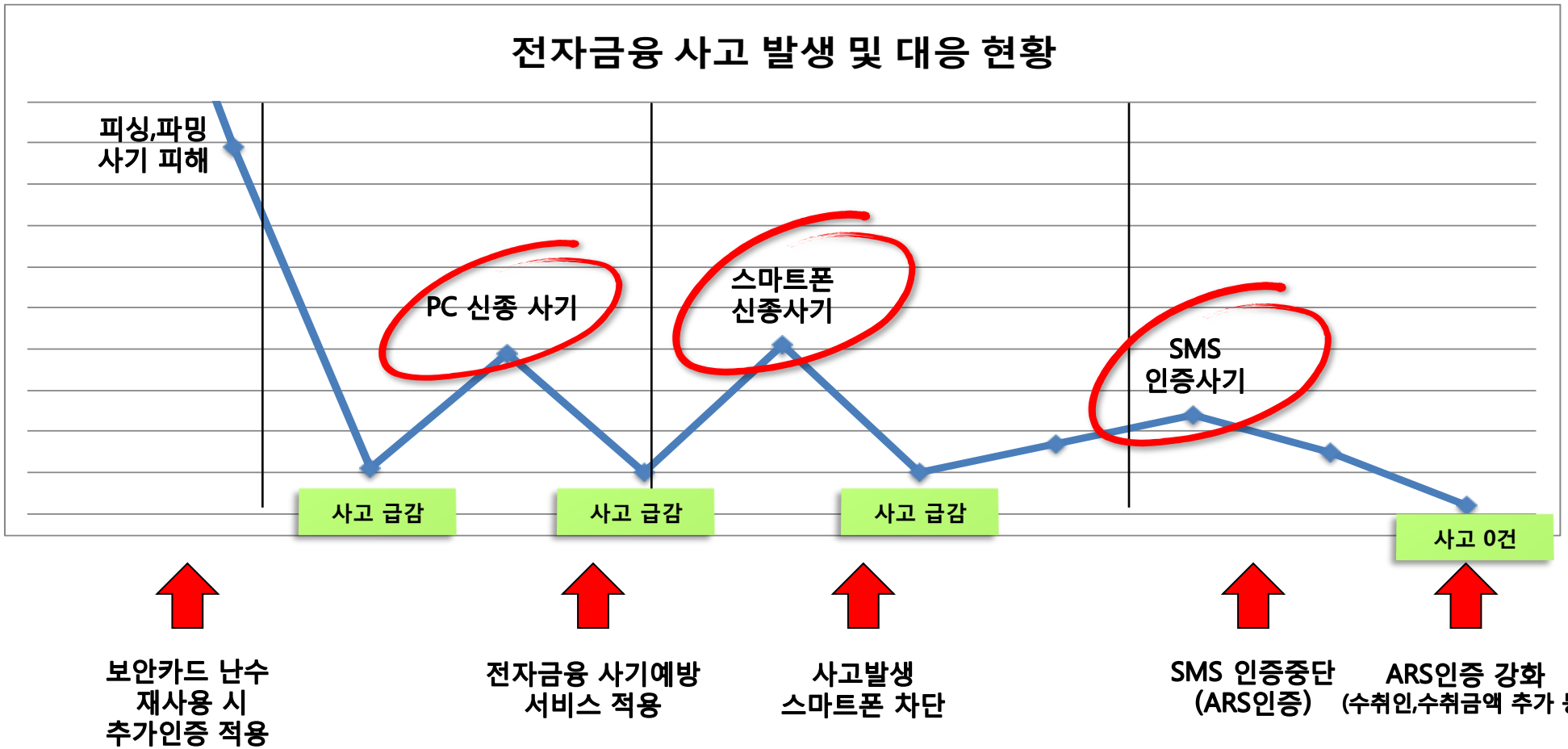
구 분	신규 매체		사고 시간대		이체종류		사고연관 IP 종류		피해자 브라우저
패턴	PC	스마트폰	00~03	17~23	타행	다계좌	중국	VPN	IE 6.0
위험값	50	50	30	10	10	10	10	5	5

사고거래 유형 분류		
신규매체 (PC/스마트폰)	심야시간 (00~03시)	해외(중국)IP/ 국내IP위장 해외IP(VPN)



사례연구 – 전자금융사기 선제대응

대응



KB 국민은행