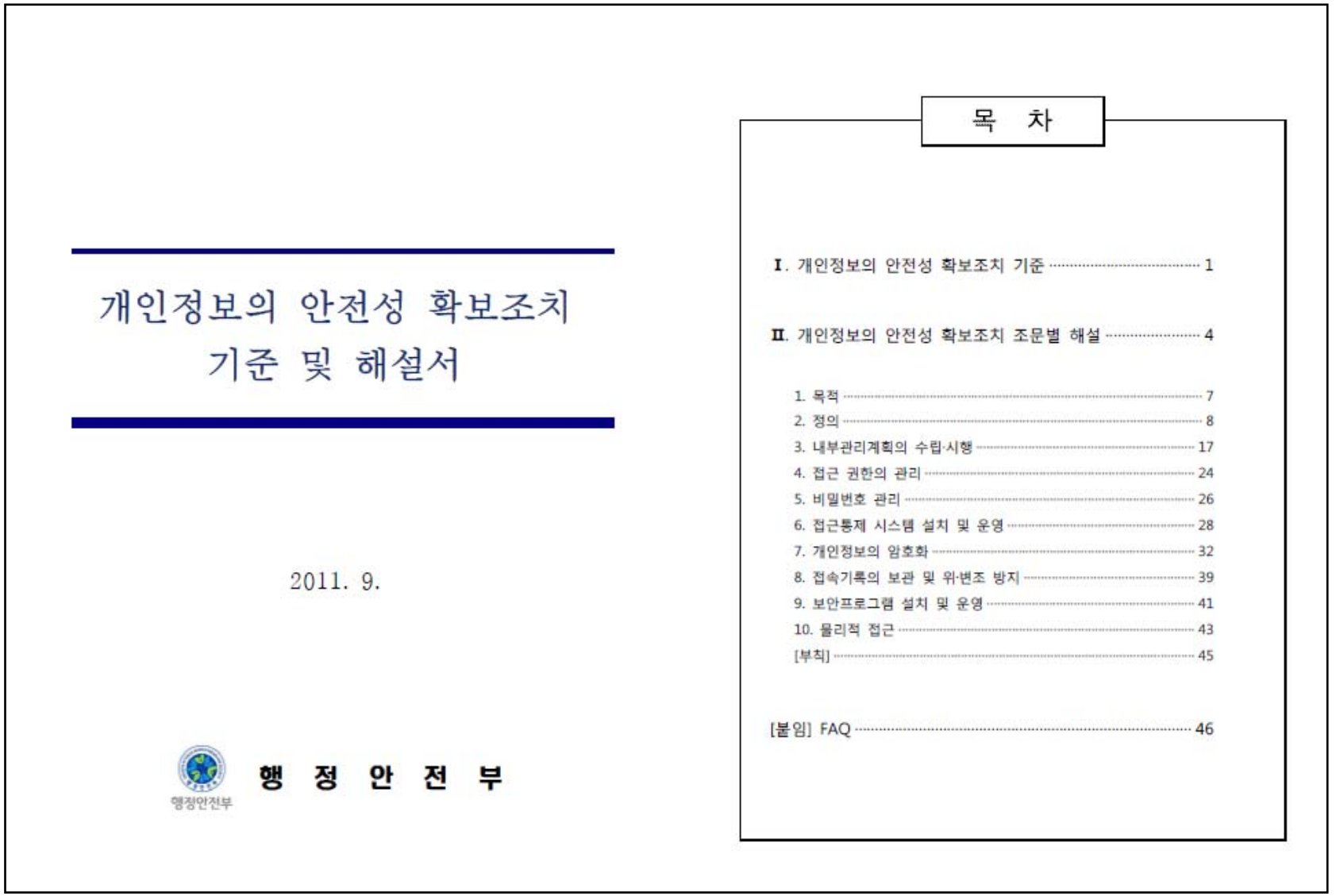
IBM 보안 프레임워크 기반의 개인정보 안전조치 대응

개인정보의 안전성 확보조치 기준 **(2011.9)**



개인정보의 안전성 확보조치
기준 및 해설서

2011. 9.

행정안전부

행 정 안 전 부

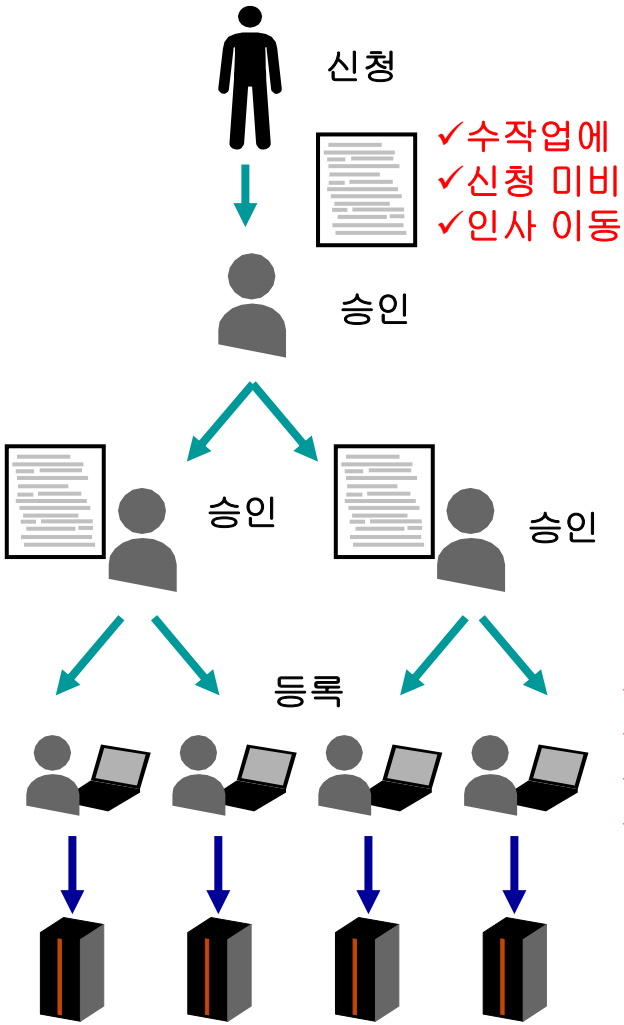
목 차

접근 권한 및 비밀번호의 관리

제4조(접근 권한의 관리)
-개인정보처리시스템에 대한 접근권한을 업무에 맞도록 최소한으로 부여
-인사이동에 대한 접근권한의 변경/말소
-권한 부여/변경/말소 기록의 3년 보관
-1인 1계정 사용을 통한 책임추적성 확보

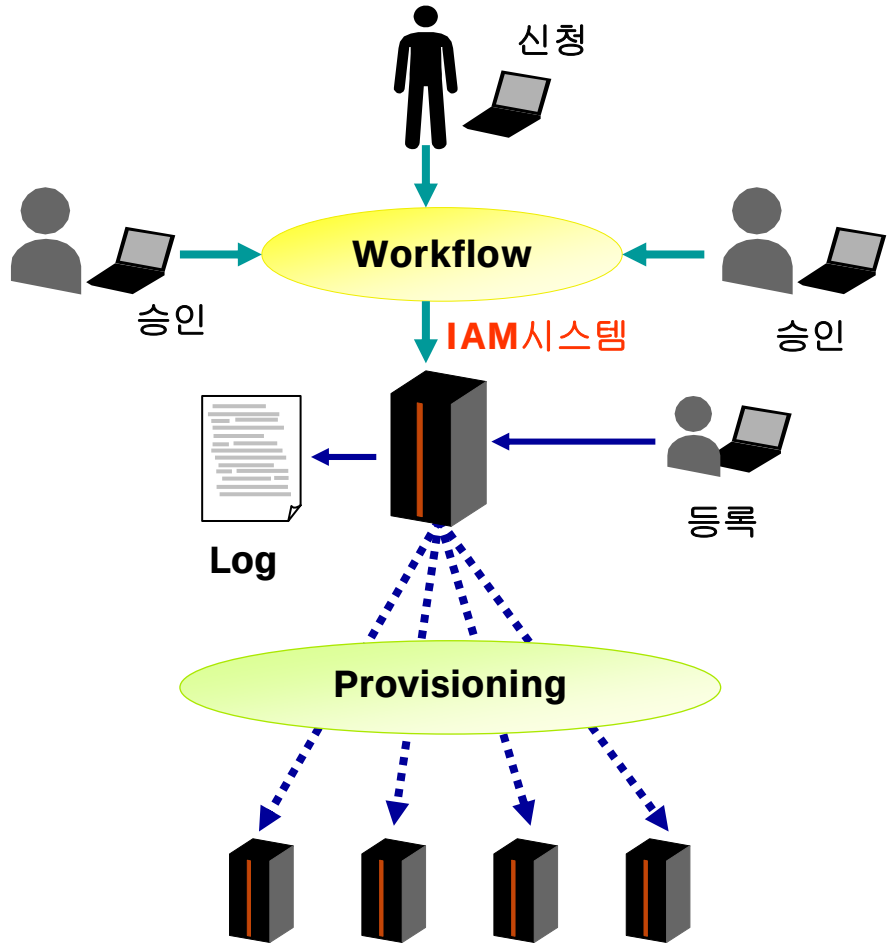
제5조(비밀번호 관리)
- 비밀번호 작성규칙의 수립, 적용을 통한 안전한 비밀번호 설정

접근 권한 및 비밀번호의 관리



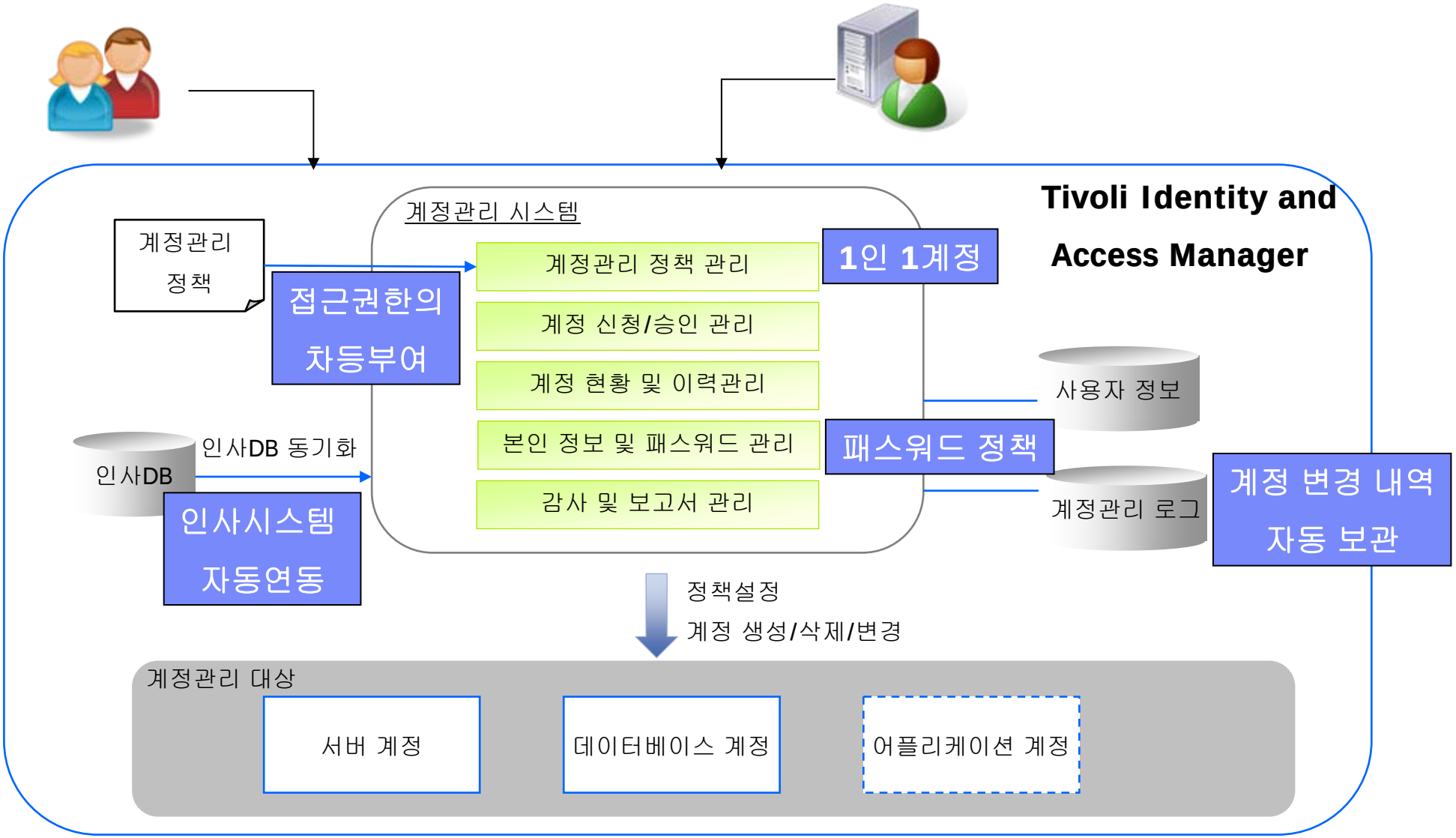
✓수작업에 의한 **Miss,** 지연
✓신청 미비, 부정 가능성
✓인사 이동 현황 파악 어려움

✓요원의 증가
✓같은 작업의 반복
✓**Miss,** 부정 가능성
✓감사 **Log**의 소실



IAM시스템의 목표 ➔ 정책 적용의 자동화

접근 권한 및 비밀번호의 관리



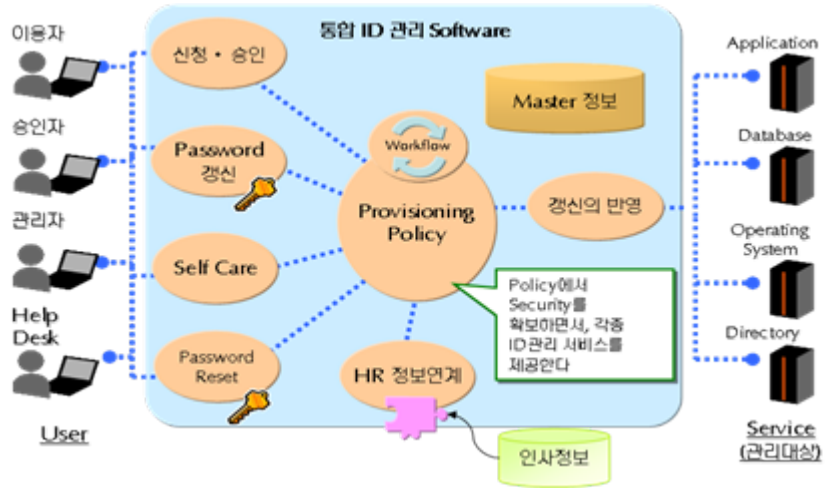
계정권한관리 솔루션

IBM의 계정 및 권한관리 솔루션인 IBM Tivoli Identity & Role Manager는 사용자 계정의 생성, 접근권한 및 자격 부여, 사용 및 종료 등을 구축하여 내부통제를 강화하고 계정을 효율적으로 관리하는 서비스를 제공합니다.

도입 효과

1. 기업 거버넌스 하에서 계정 및 권한 관리 거버넌스의 통일성 확보
2. 비즈니스 요구에 따른 접근성 향상으로 업무 생산성 및 즉시성 증대
3. 계정 및 권한 관리 관련 정보 보안 위험 감소
4. 개인정보보호 관련 제반 법 규정 및 정보보호 표준 준수
5. 내외부 IT/보안 감사에 효과적 대응
6. 업무 및 프로세스 자동화에 따른 관리 업무 감소.
7. 보다 강력한 IT/보안 정책 추진에 따른 사용자 불편 최소화

솔루션 구성



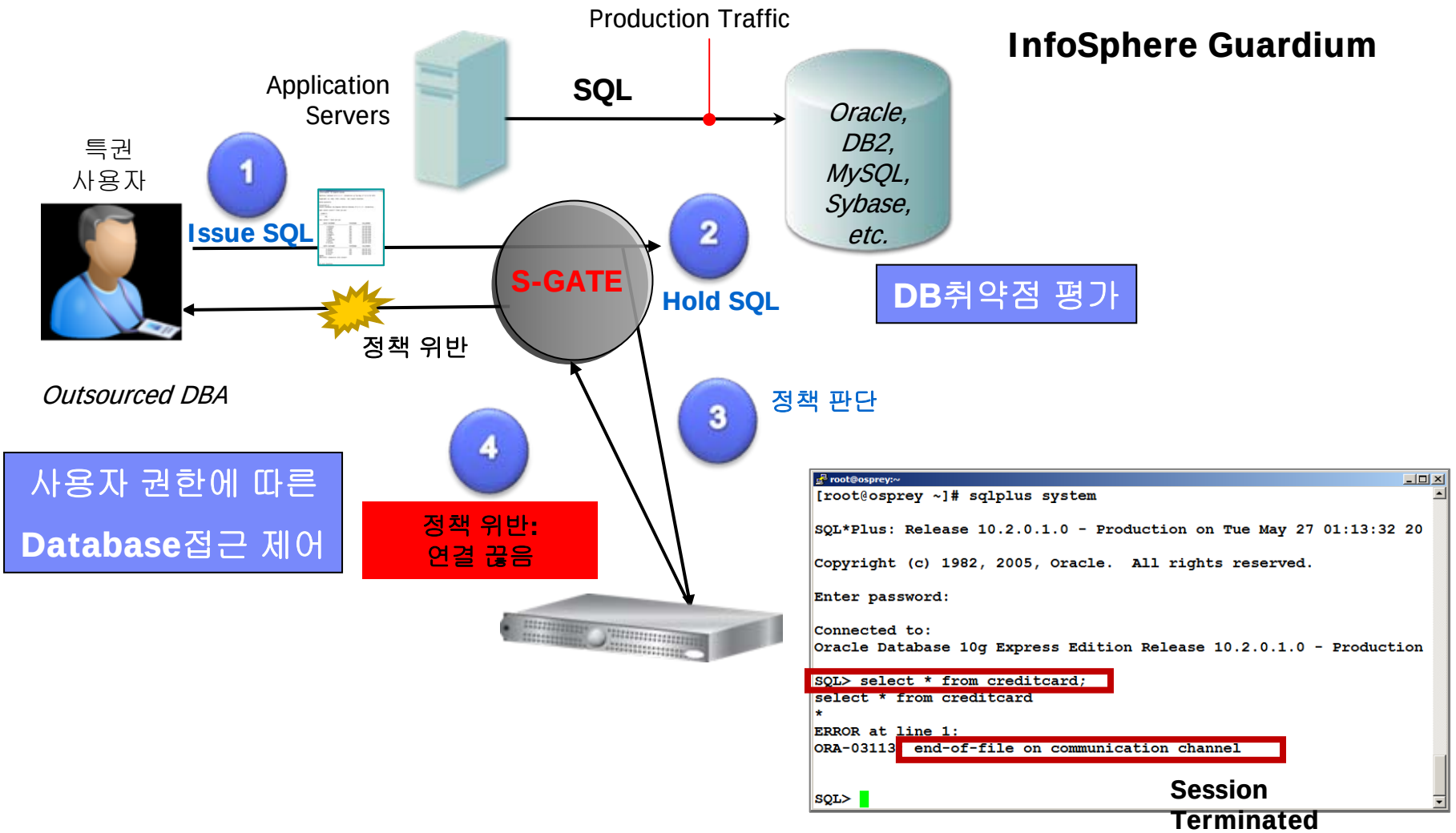
도입 사례

1. 'K' 은행: 전 인프라 시스템을 대상으로 한 계정 및 권한관리 체계 수립 및 구축 (국내 금융권 최대 프로젝트)
2. 'K' 생명: 계정 및 접근통제 관리 체계를 마련하고 인사DB와 연동하여 계정상태 변경 및 인사이동 시에도 강제적으로 보안정책이 유지되도록 관리

솔루션 특징

1. 보안정책 기반의 중앙화된 계정/권한 관리
2. 인사 DB와의 연동으로 자동화된 프로비저닝 정책, 계정관리 자동화
3. 계정생성과 동시에 시스템 사용권한 부여
4. 시스템 서버별, 조직별, 사용자별로 계정 사용 현황관리
5. 메인프레임/서버/DB/애플리케이션의 계정 프로비저닝 지원
6. SOD/재승인 정책등을 통한 계정권한의 통제 실현

접근 권한 및 비밀번호의 관리



데이터베이스 보안 솔루션(접근통제)

IBM InfoSphere Guardium 은 데이터베이스에 대한 접근 및 활동을 실시간으로 모니터링 및 정책 기반으로 통제하여 기업의 중요한 정보를 보호합니다.

도입 효과

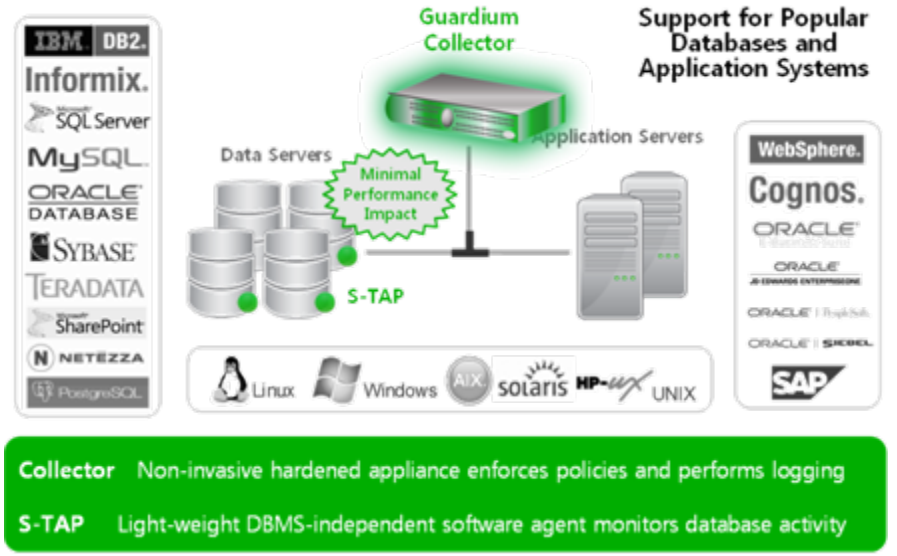
1. 기업 정보 관리 라이프사이클에 따른 데이터베이스 보안 관리 강화
2. 어플리케이션과 연계된 데이터베이스 사용 감시 및 통제를 통해 정보 위험 대응 및 감소
3. 개인정보보호 관련 제반 법 규정 및 정보보호 표준 준수
4. 이기종 데이터베이스와 SAP 등 패키지 어플리케이션 데이버베이스에 통합 모니터링 및 통제로 복잡성 및 관리 업무 감소
5. 내외부 IT/보안 감사의 효과적인 대응
6. 권한 사용자에 대한 내/외부 데이터베이스 사용 내역 감시 및 차단을 통해 중요 정보 유출 위험 감소

도입 사례

여러 주요 고객사에서 법적 규제 준수 및 거버넌스 체계 구축 마련

- FSS: 'C'은행,'J은행', 'I'보험사 등
- IND: 'L' 건설, 'S' 엔지니어링 등 다수
- COM: 'S' 텔레콤, 'K' 사, 'L'사 등
- PUBLIC: 'G' 군, 'S'정부 등 다수

솔루션 구성



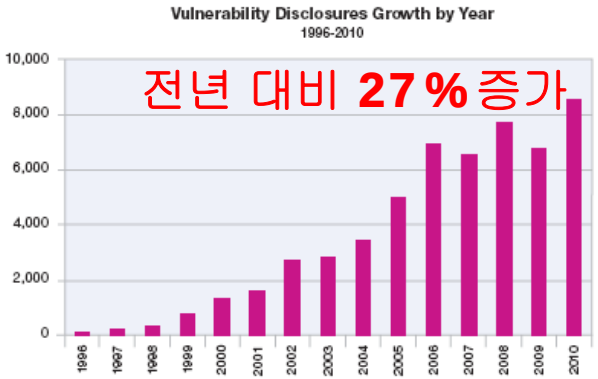
솔루션 특징

1. 다양한 이기종 DB에 대한 실시간 모니터링/로깅/감사
2. S-TAP을 이용한 네트워크 및 로컬 DB 접근 활동에 대한 모니터링
3. 애플리케이션 사용자 ID 인식
4. 정책 기반의 DB 접근제어
5. DB 보안 취약성 평가 및 DB 권한/구성환경의 변경관리
6. 자동화된 컴플라이언스 리포트 제공(PCI-DSS,SOX 등)

접근 통제 시스템 설치 및 운영

제6조(접근통제 시스템 설치 및 운영)
-접근 및 침해사고 방지를 위한 침입차단/침입방지 시스템 설치. 운영
-외부에서의 개인정보처리시스템 접속을 위한 안전한 접속수단 적용
-인터넷 홈페이지등을 통한 개인정보 유출 방지 조치

접근 통제 시스템 설치 및 운영



전년 대비 **27%**증가

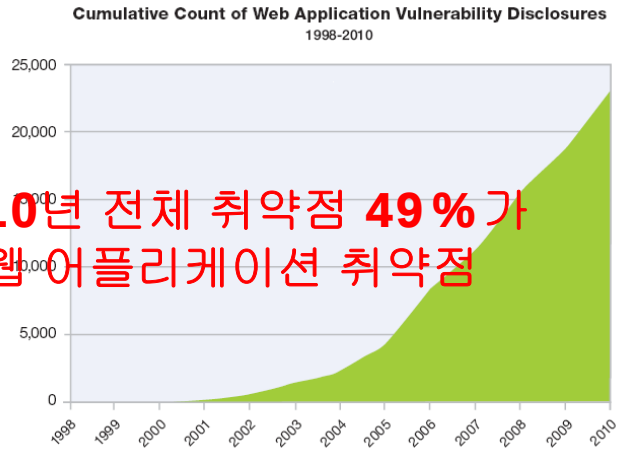
Patch Timeline	All	Top Vendors
Same Day	3400	1814
Week 1	192	34
Week 2	55	11
Week 3	57	12
Week 4	38	7
Week 5	37	7
Week 6	22	4
Week 7	17	3
Week 8	16	8

2010년 전체 취약점 중
44% - No patch!!!

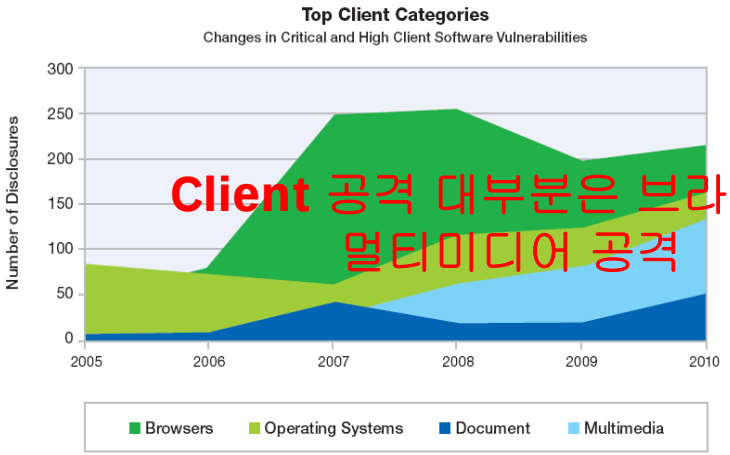
출현한 공격 대부분이
0 day

Figure 54: Public Exploit Disclosure Timing by Weeks – 2010

Exploit Timing	0 Days	1 Week	2 Weeks	3 Weeks	4 Weeks
0 Days	854	270	18	9	9



2010년 전체 취약점 49%가
웹 어플리케이션 취약점



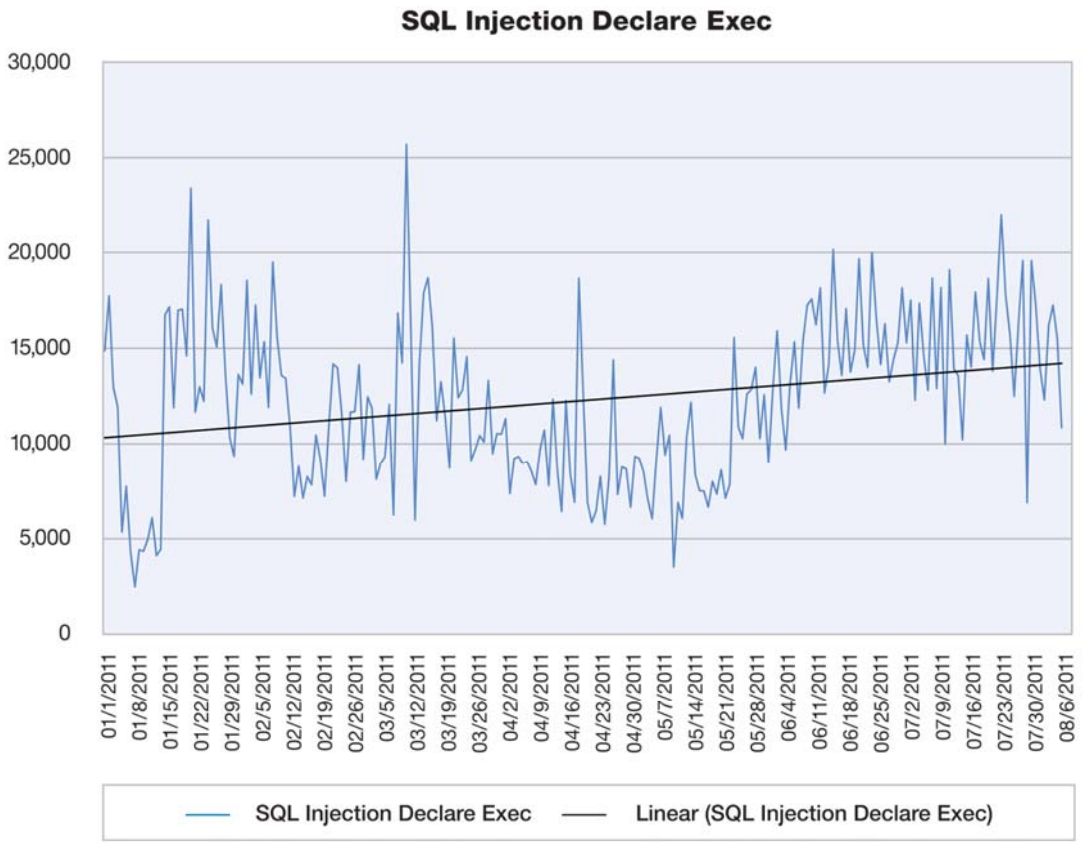
Client 공격 대부분은 브라우저,
멀티미디어 공격

접근 통제 시스템 설치 및 운영

SQL 인젝션은 지속적으로 공격자들이 가장 즐겨 사용하는 기법
- IBM X-Force 2011 상반기 보고서

- 공격자들이 악용할 수 있는 SQL 인젝션 취약점을 찾기 위해 웹 어플리케이션을 분석합니다.

- 취약한 웹 어플리케이션이 발견되는 즉시, 공격자는 대상 사이트의 공격 프로세스를 자동화하기 위해 검색 엔진을 사용합니다.



Source: IBM X-Force® Research and Development

접근 통제 시스템 설치 및 운영

개인정보처리 시스템에 대한 접속권한을 **IP**주소 등으로 제한, 인가 받지 않은 접근제한

개인정보처리 시스템에 접속한 **IP**주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

IBM Security

Network Intrusion Prevention System

- 연구결과 기반의 위험 감소
  - 성능 저하 없는 방어 제공
  - **IBM X-Force R&D**의 선제적 방어 제공

- **GX7800: True 10Gbps IPS/IDS**

네트워크 보안 솔루션

IBM Security Network IPS는 기업의 중요 자산 및 IT 인프라를 보호하는 네트워크 침입방지 솔루션입니다. 네트워크의 가용성과 연속성을 보장하면서, 기업 네트워크로 유입되는 유해 트래픽을 능동적으로 방어하며, 추후 발생 할 수 있는 위험을 선제적으로 방어합니다.

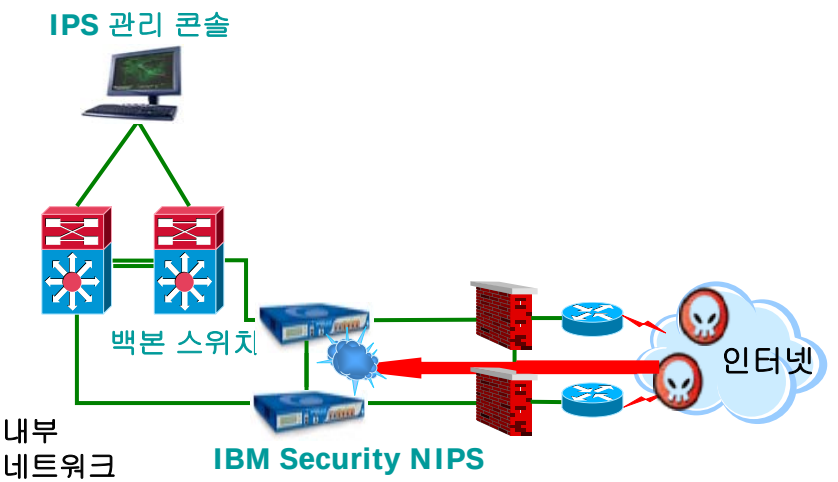
도입 효과

1. 비즈니스의 중요 자산에 대해 IBM 보안 연구소의 취약점 연구에 따른 선제적인 보호로 보다 앞선 보안 위험 관리 및 손실 최소화
2. 개인정보보호법 및 각종 법 규제 준수 및 대응
3. 신규 투자 없이 빠르게 새로운 IT 동향에 따른 보안 위험 대응
4. 가상 패치 기술 통해 패치 적용을 위한 시간 확보로 보안 대응을 위한 관리 부담 감소

도입 사례

1. FSS: 'K'은행, 'I'은행, 'H'은행, 'W' 투자증권 등 다수
2. IND: 'H' 자동차, 'L' 화학, 'C' 시스템즈 등 다수
3. COM: 'S' 텔레콤, 'K' 사, 'L'사 등
4. GB: 'N' 포털, 'D' 포털, 'A' 마켓 등
5. PUBLIC: 'K' 대학교, 'M' 대학교, 'K'병원, 'U'병원 등 다수

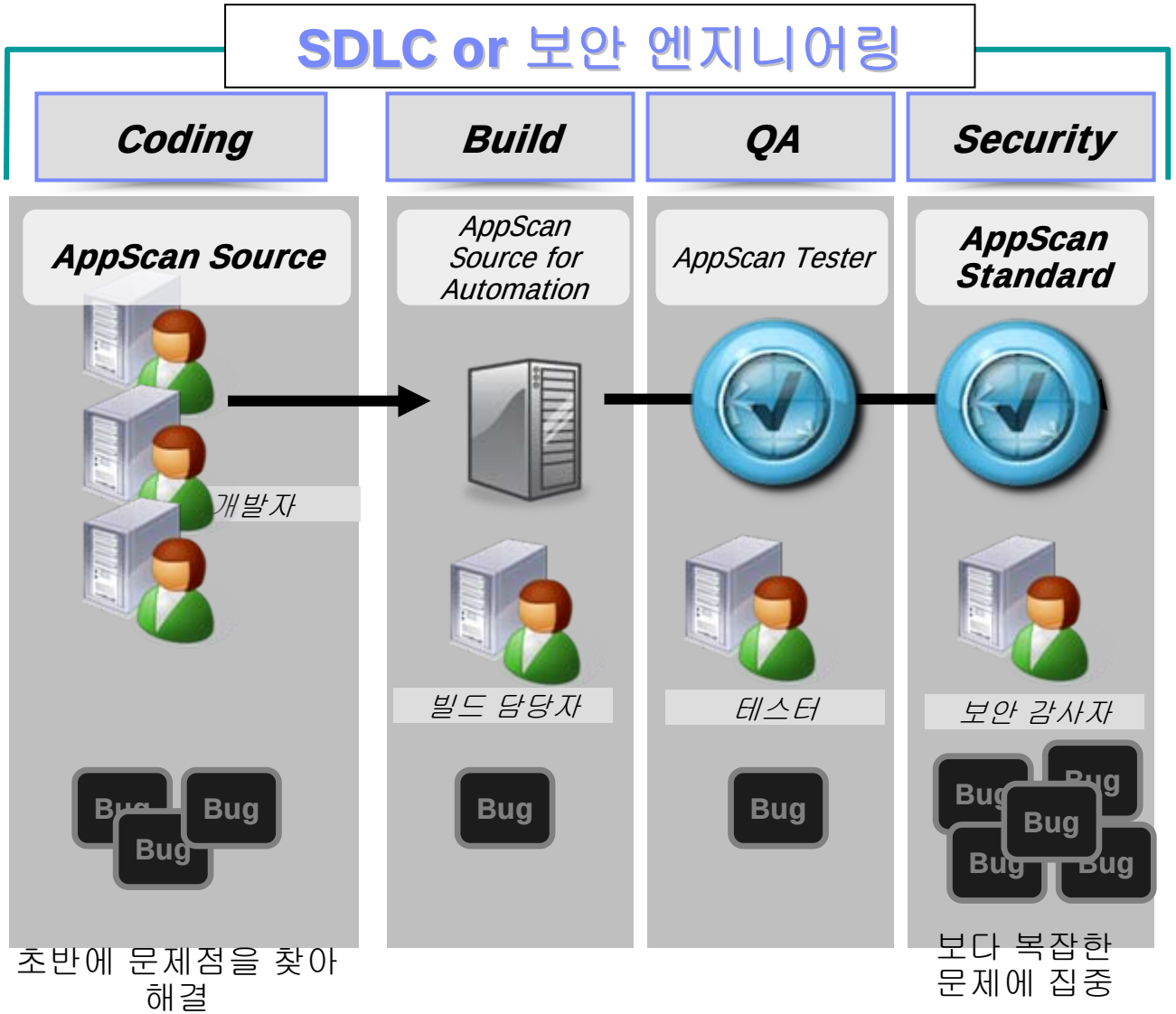
솔루션 구성



솔루션 특징

1. 글로벌 리딩 IPS 솔루션으로써의 안정성 및 신뢰성
2. 클라우드 환경의 고 성능 네트워크 지원 (20Gbps+)
3. 프로토콜 분석 및 다차원 탐지 기법을 통해 알려지지 않은 위협에 대한 선제적 방어 제공(Virtual Patch)
4. X-FORCE 보안 연구소가 개발/검증하는 시그너처 자동 업데이트
5. 웹 어플리케이션 보호 및 데이터 유출 방지 제공

접근 통제 시스템 설치 및 운영



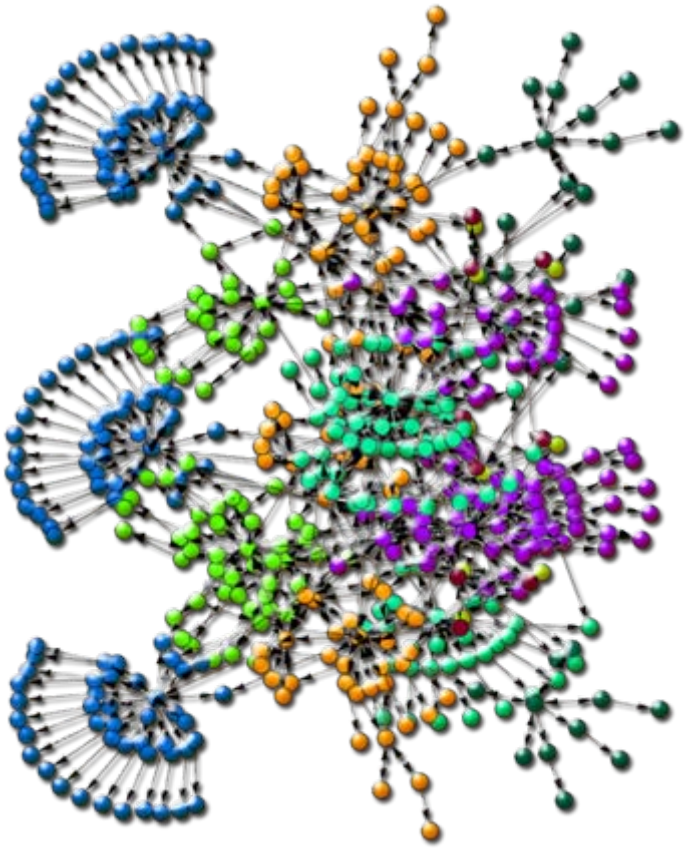
IBM Rational AppScan

인터넷 홈페이지를 통한 개인정보 유출 방지

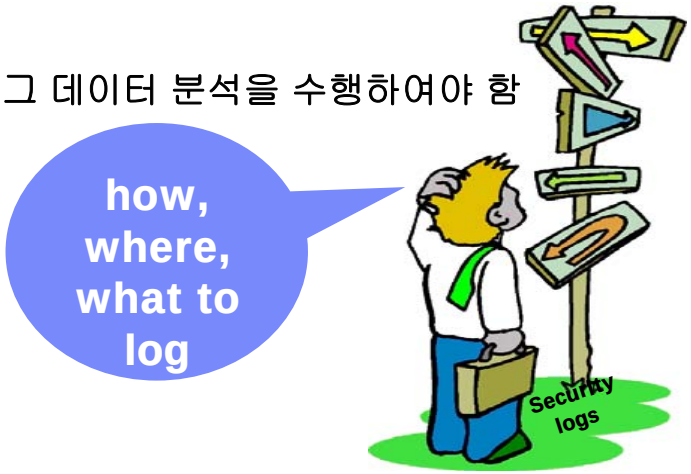
접속기록의 보관 및 위.변조 방지

제8조(접속기록의 보관 및 위.변조 방지)
-개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관.관리
-접속 기록의 위.변조 및 도난, 분실로부터 안전하게 보호

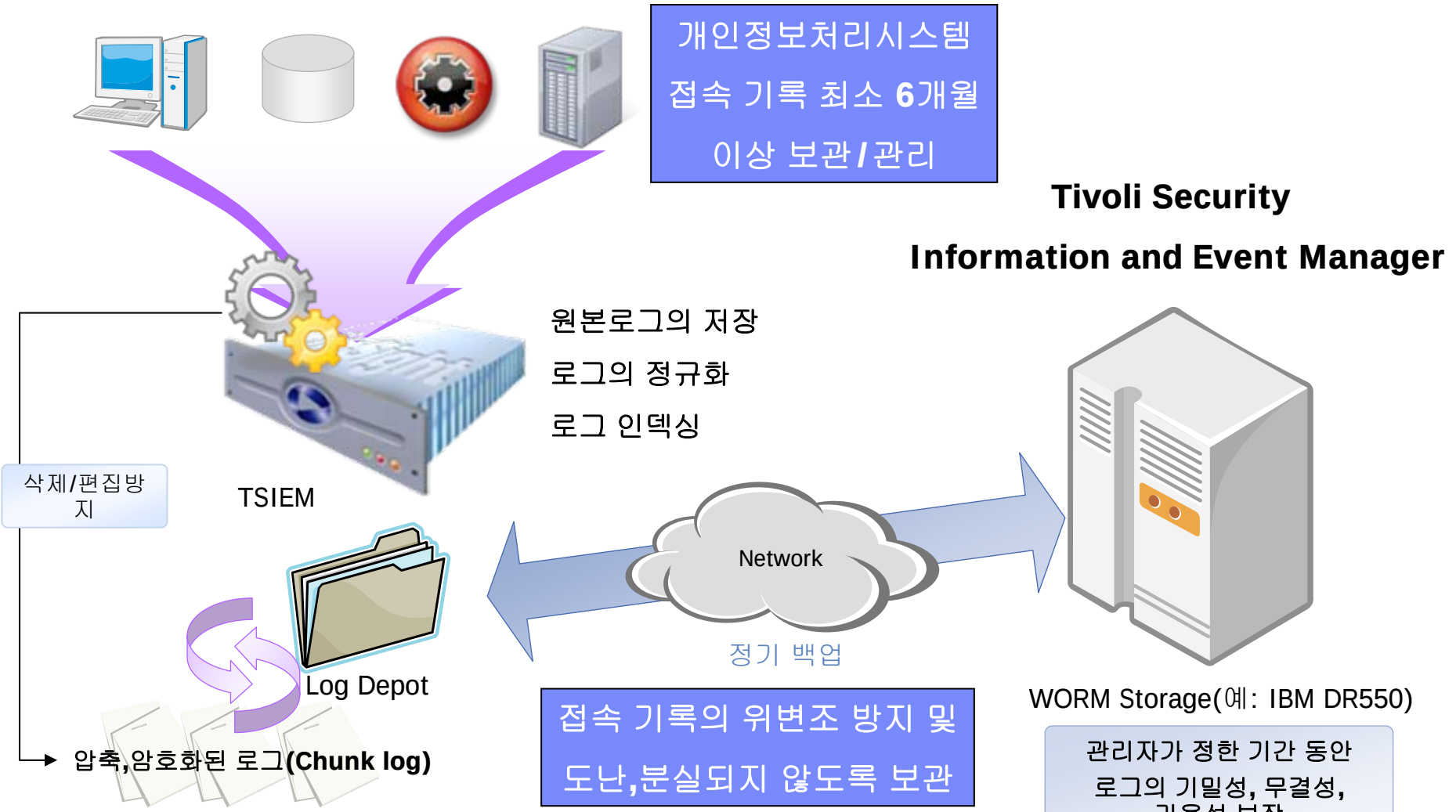
접속기록의 보관 및 위.변조 방지



- 로그데이터는 지속적으로 조직에 공급되지만 이를 관리하는 조직의 리소스는 제한되어 있음
- 로그는 너무 복잡함(많은 로그 소스, 로그 내용의 다양성, 다양한 포맷, 타임 스탬프...)
- 로그는 시간이 지날수록 계속적으로 크기가 증가함
- 로그의 기밀성, 무결성, 가용을 보장하여야 함
- 관리자가 주기적으로 로그 데이터 분석을 수행하여야 함



접속기록의 보관 및 위.변조 방지



통합 로그 관리 솔루션

TSIEM (Tivoli Security Information and Event Manager) 은 기업의 다양한 이벤트 소스(시스템, 네트워크, 정보보호시스템, DB, 애플리케이션 등)로부터 로그 및 감사 기록을 수집하여 분석, 저장하고 정책에 기반한 분석을 통해 기업의 컴플라이언스 수준을 실증합니다.

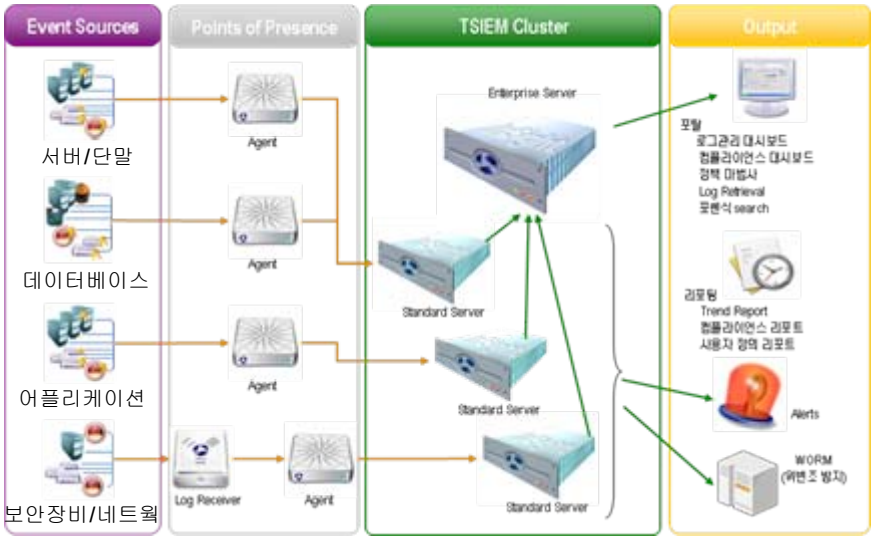
도입 효과

1. 단일/통합 대쉬보드를 통해 기업 내 컴플라이언스 수준에 대한 가시성 확보
2. 법적으로 요구되는 로그 관리 체계 지원으로 개인정보보호 관련 제반 법 규정 및 정보보호 표준 준수
3. 정책 위반 사항의 적시 탐지 및 대응을 통해 정보 위험 감소
4. 중앙 집중적이고 자동화된 로그 수집을 통해 로그 관리를 위한 비용, 시간, 관리 업무 감소.
5. 특권 사용자들의 불법 행동을 모니터링하고 탐지하여 정보 위험 대응.

도입 사례

1. 'S' 사 보안관제 시스템 구축: TSIEM을 이용한 클라우드 컴퓨팅 서비스 환경의 보안관제시스템 구축
2. '신용보증기금 통합 로그 관리 시스템 구축
3. 'S'사 통합로그 시스템 구축: CCTV시스템을 위한 로그통합관리시스템 구축(CCTV/Network/시스템 로그 통합)

솔루션 구성



솔루션 특징

1. 통합된 시스템 로그 관리 및 리포팅(한글로그 완벽지원)
2. 전사 컴플라이언스 대시보드
3. 컴플라이언스 관리 모듈 및 규정에 특화된 리포트
4. 다양한 로그들을 비즈니스 측면에서 이해할 수 있도록 해주는 W7 로그 정규화
5. 규정과 회사 정책에 기초한 사용자 행위 감시

보안프로그램 설치 및 운영

제9조(보안프로그램 설치 및 운영)
-보안 프로그램 설치.운영
-보안 프로그램의 자동 업데이트 기능을 사용 또는 일 1회 이상 업데이트 실시
-응용프로그램 또는 운영체제 S/W 벤더의 보안 업데이트 공지 시, 즉시 업데이트 실시

보안프로그램 설치 및 운영

▪ 보안 관리를 위해 필수 패치가 정해진 시간 내에 적용되었다는 것을 확신할 수 있습니까**?**

▪ 업데이트 및 패치 필요시 언제**,** 어디서나**,** 네트워크 환경에 구애 받지 않고 적용이 가능합니까**?**

▪ 다양한 엔드포인트 **O/S** 및 플랫폼에 대한 한 개의 **Tool** 사용으로 효율성을 높일 수 있습니까**?**

보안프로그램 설치 및 운영

보안 업데이트 공지 시
즉시 업데이트 실시

Tivoli Endpoint Manager

Content Sites

보안 프로그램 자동 업데이트/
일 **1**회 이상 업데이트

보안 프로그램 설치/운영

시스템 및 엔드포인트 보안 솔루션

IBM의 시스템 및 엔드포인트 통합보안 솔루션인 IBM Tivoli Endpoint manager는 하나의 통합 Agent를 이용하여 다양한 시스템 및 엔드포인트에 대한 자산 관리, 보안 구성 관리, 취약점 관리, 패치 관리, 전력 관리, Anti-Virus 등 통합 보안 기능을 제공합니다.

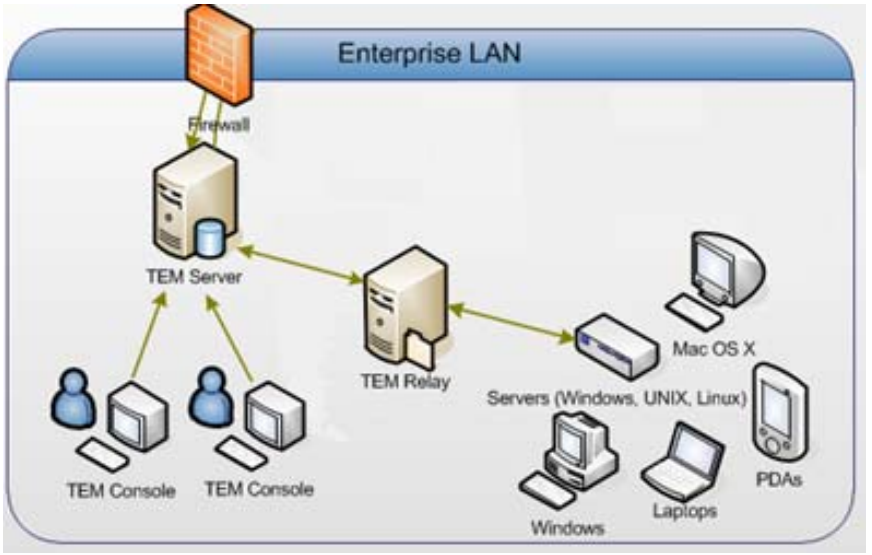
도입 효과

1. 서버 및 엔드포인트 등 기업 내 모든 IT 자산에 대한 자산 탐지 및 관리로 종합적인 가시성 및 현황 제공
2. 단일 플랫폼 상에서 패치, 취약점, 보안 구성 및 전력 관리 등 전체 기능 제공으로 관리 및 운영 부담 감소
3. 이슈 발생 시 해당되는 IT 자산의 대한 식별로 효과적인 대응 및 피해 최소화

도입 사례

1. 'S' 유통: 다수의 POS시스템에 대한 종합 엔드포인트 보안
2. '해외 사례
   - Tech: Intel, LSI Logic, KRONOS 등
   - Manufacture: TRW Automotive, PILKINGTON등
   - Retail: Marriott, STAPLES 등

솔루션 구성



솔루션 특징

1. 멀티벤더 엔드포인트에 대한 종합 보안 기능 제공
2. 자동화된 자산 발견 및 패치 관리 기능
3. 네트워크 연결 여부와 상관 없는 보안 정책 적용
4. 99.9%의 정확성을 가지는 Host-base 취약점 진단
5. 고객의 정책에 의거한 보안 구성 진단