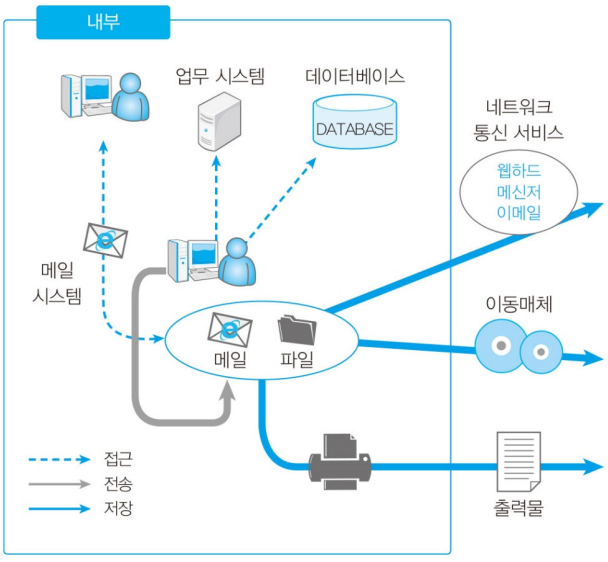
개인정보보호론

[6주차. 안전성확보조치]

한 눈에 보는 정보 유출 단계



상명대학교 SANGMYUNG UNIVERSITY

Adobe hacked, 3 million accounts compromised

The massive attack exposes customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders.

by Rachel King | October 3, 2013 2:31 PM PDT

Follow

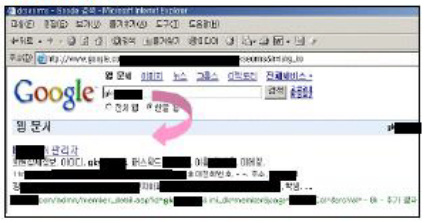
1K 1.1K 60 +1 263 More + Comments 55

Adobe announced on Thursday that it has been the target of a major security breach in which sensitive and personal data about millions of its customers have been put at risk.

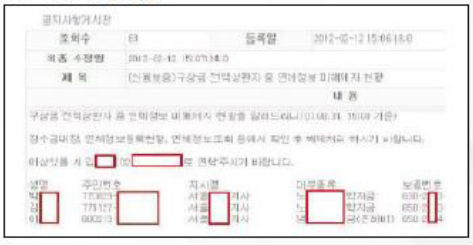
Brad Arkin, senior director of security for Adobe products and services, explained in a blog post that the attack concerns both customer information and illegal access to source codes for "numerous Adobe products."

A few examples include Adobe Acrobat, ColdFusion, and the ColdFusion Builder. However, as far as the source code is concerned, Adobe assured that there is no "increased risk to customers as a result of this incident."

● 검색엔진



● 게시판 게시내용



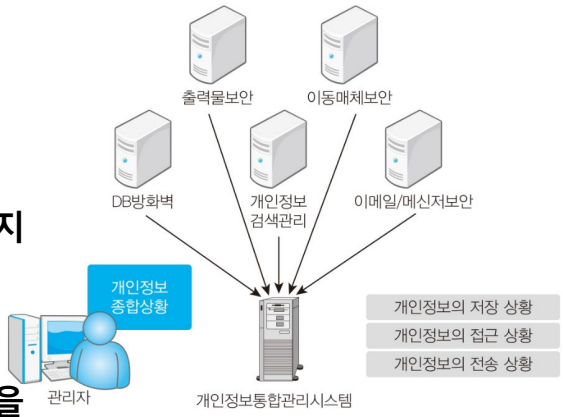
● 게시판 첨부파일

● URL 주소

● 홈페이지 소스코드

개인정보 생명주기 전체에 걸친 개인정보 종합 관리기술

- 개인정보 보호 관련 기술들은 각기 자신만의 보호 기술과 영역을 갖고 있음
  - 해당 조항들을 만족시키기 위해서는 개인정보를 누가 보유하고 있고, 누가 접근했으며, 누가 외부로 전송하였는지 종합적으로 파악할 수 있어야 하며, 유출사고 발생 시 추적할 수 있는 인프라를 구축해야 함
  - 개인정보 종합관리 기술은 이 필요성을 만족시킬 수 있음



상명대학교 SANGMYUNG UNIVERSITY

단계별 보안대책과 보호기술

- 효과적으로 정보 유출을 방지하기 위해서는 접근, 저장, 전송 단계별로 보안대책이 필요함

유출 단계	보안 대책	관련 보호기술/제품
접근	• 중요 정보의 접근 내역을 기록하고 감사 • 권한이 있는 사람만 정보에 접근할 수 있도록 통제 • 해킹을 통한 정보 획득을 차단	• DB보안 기술(DB암호화, DB방화벽) • 네트워크 DLP(이메일/메신저 보안 기술) • IPS/IDS • 방화벽/웹 방화벽 .PC보안/서버보안 기술 • 홈페이지 유출방지 기술
저장	• PC와 서버상에 저장되어 있는 중요 정보를 식별하고 (조직 상황에 따라) 중앙집중적 관리 • 업무상 필요한 정보는 암호화하여 보관 • 업무상 필요 없거나, 필요기간이 지나면 삭제	• 엔드포인트 DLP(개인정보 검색/관리 기술) • 문서 암호화 기술 • 파일 완전삭제 기술
전송	• 외부로 전송되는 정보 내역을 기록하고 감사 • 정당하지 않은 중요 정보의 외부전송 차단	• 이메일/메신저 보안 기술 • 엔드포인트 DLP(이동매체 보안 기술) • 출력물 보안 기술 • 보안서버 • VPN 기능

상명대학교 SANGMYUNG UNIVERSITY

개인정보 생명주기별 기술적 보안 제품

수집	저장	이용	전송	폐기
키보드 보안	PC DRM	PC 보안 / 출력 보안	SSL	데이터완전삭제
온라인 PC 보안	서버 DRM	DB 접근제어 / 서버 보안	보안 메일	디가우저
SSL	DB 암호화	Data Masking	DRM	DRM
공인인증	보안 USB	웹 보안 / 개인정보필터링	외부전송 모니터링	문서파쇄기
I-PIN / G-PIN	로그 백업	EAM / IAM (계정/권한관리)	암호화 Toolkit	현장파쇄서비스
Paperless	테스트 데이터 변환	개인정보 감사 (Forensic)	보안 USB	해지 DB
개인영향평가시스템				
개인정보 오남용 / 정보유출 통합 모니터링(로그분석) 시스템				

법적 근거

고시

개인정보의 안전성 확보조치 기준

(행정안전부 고시 제2016-35호, 2016.9.1. 시행)

개인정보보호법

제29조
(안전조치의무)

개인정보보호법 시행령

제30조
(개인정보의 안전성 확보 조치)

목적과 용어의 정의

▪ [제1조] 안정성 확보조치 기준의 목적

개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보에 필요한 **기술적 · 관리적 · 물리적 안전조치에 관한 최소한의 기준**을 정하는 것

▪ [제2조] 사용하는 용어

- 정보주체
- 개인정보파일
- 개인정보처리자
- 대기업
- 중견기업
- 중소기업
- 소상공인

- 개인정보보호책임자
- 개인정보취급자
- 개인정보처리시스템
- 위험도분석
- 비밀번호

- 정보통신망
- 공개된 무선망
- 모바일 기기
- 바이오정보
- 보조저장매체
- 내부망
- 접속기록
- 관리용 단말기

※용어의 정의는 고시 참조

유형별 안전조치 적용

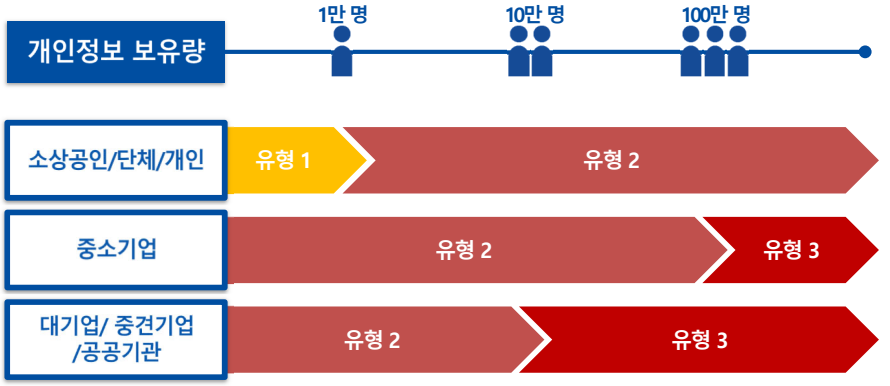
▪ [제3조] 안전조치 기준 차등 적용

[별표] 개인정보처리자 유형에 따른 안전조치 기준 차등 적용

유형1 (완화)	1만 명 미만의 개인정보를 보유한 소상공인, 단체, 개인
유형2 (표준)	1만 명 이상의 개인정보를 보유한 소상공인, 단체, 개인 10만 명 미만의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 미만의 개인정보를 보유한 중소기업
유형3 (강화)	10만 명 이상의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 이상의 개인정보를 보유한 중소기업

유형별 안전조치 적용

▪ [제1조] 안정성 확보조치 기준의 목적



유형1 (완화)

- 제5조: 제2항~제5항
- 제6조: 제1항, 제3항, 제6항, 제7항
- 제7조: 제1항~제5항, 제7항
- 제8조, 제9조, 제10조, 제11조, 제13조

유형2 (표준)

- 제4조: 제1항 제1호~제10호, 제15호, 제3항, 제4항
- 제5조
- 제6조:제1항부터 제7항까지
- 제7조:제1항부터 제5항까지, 제7항
- 제8조, 제9조, 제10조, 제11조, 제13조

유형3 (강화)

- 제4조부터 제13조까지

상명대학교 SANGMYUNG UNIVERSITY

11

주요 보호 조치 기준

상명대학교 SANGMYUNG UNIVERSITY

12

내부 관리계획의 수립과 시행(제4조)

개인정보보호
내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육

관리적

4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지

기술적

9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립 · 시행
12. 위험도 분석 및 대응방안 마련
13. 재해 · 재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

유형1 선택조항

15. 그 밖에 개인정보 보호를 위해 필요한 사항

물리적

내부 관리계획의 수립과 시행(제4조)

개인정보보호
내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육

관리적

4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지

기술적

9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립 · 시행
12. 위험도 분석 및 대응방안 마련
13. 재해 · 재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

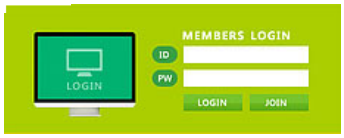
유형1 선택조항

15. 그 밖에 개인정보 보호를 위해 필요한 사항

물리적

상명대학교 SANGMYUNG UNIVERSITY
14

접근권한의 관리(제5조)



① 개인정보처리시스템에 대한 접근 권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여

유형1 선택조항

② 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 접근 권한을 변경 또는 말소

③ 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관

④ 개인정보처리시스템의 사용자계정 발급시 개인정보취급자 별로 발급하며, 다른 개인정보취급자와 공유되지 않도록 함

⑤ 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용

⑥ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한 등 필요한 기술적 조치

유형1 선택조항

접근통제(제6조)

① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 기본 조치

1. 접속 권한을 IP주소 등으로 제한 → 인가 받지 않은 접근 제한
2. 접속한 IP주소 등을 분석 → 불법적인 개인정보 유출 시도 탐지 및 대응

→ 위 기능을 포함하여 조치해야 함

IP(Internet Protocol)

② 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 접속수단 또는 안전한 인증수단 적용

유형1 선택조항

※ 가상사설망 (VPN : Virtual Private Network) 또는 전용선 등

③ 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 개인정보가 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등 조치 수행

접근통제 (제6조)

④ 인터넷 홈페이지를 통해 고유식별정보가 유출.변조.훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치 수행 ☑ 유형1 선택조항

⑤ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 해야 함 ☑ 유형1 선택조항

⑥ 별도의 개인정보처리시스템이 아닌 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우

- 제1항 적용 안 함
- 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능 이용 가능

⑦ 업무용 모바일 기기의 분실.도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치

개인정보의 암호화(제7조)

암호화 필요 대상 고유식별정보, 비밀번호, 바이오정보

암호화 기준

구 분				암호화 기준
정보통신망, 보조저장매체를 통한 송, 수신 시	비밀번호, 바이오정보, 고유식별정보			암호화 송, 수신 ※제7조 ①항 TIP 참조
정보처리 시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별정보	주민등록번호		암호화 저장
		여권번호, 외국인등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점 (DMZ)	암호화 저장
			내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부.적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장 시	비밀번호, 바이오정보, 고유식별정보			암호화 저장(비밀번호는 일방향 암호화 저장)

- 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행 ☑ 유형1,2 선택조항
- 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장

접속기록의 보관 및 점검(제8조)

① 접속한 기록을 **6개월 이상 보관.관리**

② **반기별로 1회 이상** 점검 → 개인정보의 **분실.도난.유출.위조.변조 또는 훼손** 등에 대응하기 위하여

③ 개인정보취급자의 접속기록이 위.변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관

접속ID, 날짜와 시간, IP주소, 수행업무

정기적으로 백업 수행

정기 점검 / 후속 조치

악성프로그램 등 방지(제9조)

악성프로그램 등을 방지.치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치.운영해야 함

1. 보안 프로그램은 항상 최신의 상태로 유지

- 자동 업데이트 기능 사용
- 일 1회 이상 업데이트 실시

2. 악성프로그램 관련 경보 발령 또는 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트 실시

3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

관리용 단말기의 안전조치(제10조)

개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로
개인정보처리시스템에 직접 접속하는 단말기

1 인가 받지 않은 사람이 임의로 조작하지 못하도록 조치

2 본래 목적 외로 사용되지 않도록 조치

3 악성프로그램 감염 방지 등을 위한 보안조치 적용

상명대학교 SANGMYUNG UNIVERSITY

물리적 안전조치(제11조)

① 개인정보 보관을 위한 물리적 보관 장소(전산실, 자료보관실 등)는
출입통제 절차를 수립.운영

② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는
안전한 장소에 보관

③ 개인정보가 포함된 보조저장매체의 반출.입 통제를 위한 보안대책을 마련

다만, 별도의 개인정보처리시스템 없이 업무용 컴퓨터 또는 모바일 기기를 이용하여
개인정보를 처리하는 경우는 예외

상명대학교 SANGMYUNG UNIVERSITY

재해·재난 대비 안전조치(제12조) ☑ 유형1,2 선택조항

화재, 홍수, 단전 등의 재해.재난 발생 시

① 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검

② 개인정보처리시스템 백업 및 복구를 위한 계획 마련

상명대학교 SANGMYUNG UNIVERSITY

개인정보의 파기(제13조)

① 개인정보 파기 조치

1. 완전파괴(소각.파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 1항의 방법이 어려울 경우 일부 파기 조치

전자적 파일	개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
기록물, 인쇄물, 서면, 그 밖의 기록매체	해당 부분을 마스킹, 천공 등으로 삭제

상명대학교 SANGMYUNG UNIVERSITY

기술적 안전성 확보 조치 종합