FPRI
Future Policy Research Institute

"PASSWORD"

- 비밀번호 보안 정책에 대한 미신과 진실_II V1.0 -

(The Myth and Truth about Password Security Policy II)

2018.04.10

Jason, Min

FPRI
Future Policy Research Institute

[고찰] 비밀번호의 보호조치의 의미

□ 비밀번호의 실질적 보호는 어느 단계가 중요한가?

☞ 입력 시 : 단말(PC/모바일기기 등) 해킹 시 비밀번호규칙은 의미없음

☞ 전송 시 : 암호화 전송 *개인정보의 안전성 확보조치 기준 제7조

☞ 저장 시 : 정보유출에 대비한 해시충돌에 대비한 충분한 강도필요(인정)

* 이용자/사용자 비밀번호를 길게 하여 해시충돌에 대비할게 아니라, 저장 시 자체적으로 엔트로피를 증가시키는 방법을 적용해야 함, **즉 비밀번호 강도의 기준은 입력 시 기준이 아니라 저장시의 기준이어야 함**

□ 법제도 고찰

☞ 개인정보보호법-시행령-시행규칙-개인정보의 안전성확보조치기준

주요내용 : 비밀번호의 작성규칙 수립/적용, 전송 시 암호화, 저장 시 일방향 암호화
검토결과 : FIDO, 사설인증서, FingerPrint 등 최신 인증기술에 대해 현 방침대로 적용 가능

☞ 전자금융거래법-시행령-시행세칙

주요내용 : 비밀번호의 작성규칙 세부사항이 규제되고 있음
검토결과 : **FIDO, 사설인증서, 바이오 인증 등 최신기술의 적용에 장애요소로 작동하고 있음**

개인정보 보호법

[시행 2017.7.26.] [법률 제14839호, 2017.7.26., 타법개정]

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24>

개인정보 보호법 시행령

[시행 2017.10.19.] [대통령령 제28355호, 2017.10.17., 일부개정]

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 행정안전부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. <개정 2013.3.23, 2014.11.19, 2017.7.26>

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다. <개정 2013.3.23, 2014.11.19, 2017.7.26>

FPRI
Future Policy Research Institute

개인정보의 안전성 확보조치 기준

[시행 2017.7.26.] [행정안전부고시 제2017-1호, 2017.7.26., 타법개정]

고유식별정보 안전성확보조치

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

12. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

해설서 : 개인정보처리시스템에서의 개인정보 유출시 우려

- 비밀번호는 알 수 있는 형태로 관리되어서는 아니된다. 내부직원 또는 비인가자나 공격자 등에 의하여 고의 또는 악의적으로 개인정보처리시스템 등에 접속하여 개인정보를 유출하는 등 불법행위가 가능하기 때문이다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

※ 시스템에 전달되어 확인되는 경우의 비밀번호임, 안전함의 의미는 ①입력 ②전송 ③저장 중 어느부분일까?

⑥개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

- 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 한다.
  ※ 비밀번호 이외의 추가적인 인증에 사용되는 휴대폰 인증, 일회용 비밀번호(OTP) 등은 비밀번호 작성규칙을 적용하지 아니할 수 있다.
- 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다.

※ 전통적인 개념에서의 비밀번호 추측, 크래킹 방지임
즉 시스템에 접속할 수 있는 PC외 다른 기기에서 접근이 가능하다는 것을 전제로 기술하고 있음

- **비밀번호의 복잡성은 입력시의 키로거 보호를 제공하지 않음, 저장시와 임의 추측공격시도(BF공격)에 의미가 있음**
  -> 저장시 SALT 추가등의 기법으로 해결
  -> BF(BruteForce)공격은 특정기기에서만 접근이 가능하도록 하면 해결
  (특정기기의 해킹시에는 키로거 공격에 의해 모든 보호기법이 무의미함)

비밀번호 작성규칙 예시

· 비밀번호는 문자, 숫자의 조합·구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정
※ 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있다.
- 최소 10자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개), 특수문자(#, [, ", 〈 등, 32개) 중 2종류 이상으로 조합·구성한 경우
- 최소 8자리 이상: 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우

· 비밀번호는 추측하거나 유추하기 어렵도록 설정
- 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등을 사용하지 않도록 한다.

· 비밀번호를 최소 6개월마다 변경하도록 변경기간을 적용하는 등 장기간 사용하지 않는다.
- 변경시 동일한(예시: Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 한다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

FPRI
Future Policy Research Institute

전자금융거래법

[시행 2017.10.19.] [법률 제14828호, 2017.4.18., 일부개정] 최종공포내용

제1조(목적) 이 법은 전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전성과 신뢰성을 확보함과 아울러 전자금융업의 건전한 발전을 위한 기반조성을 함으로써 국민의 금융편의를 꾀하고 국민경제의 발전에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.4.27., 2008.2.29., 2012.3.21., 2012.6.1., 2013.5.22.>

10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
    가. 전자식 카드 및 이에 준하는 전자적 정보
    나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조제7호의 인증서
    다. 금융회사 또는 전자금융업자에 등록된 이용자번호
    라. 이용자의 생체정보
    마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

※ 가목 : 통장, 체크카드, 신용카드 + 비밀번호

나목 : 인증서 + 비밀번호

※ 다목의 이용자번호(이용자ID)에 따른 비밀번호는 지정되지 않음

전자서명법
[시행 2017.7.26.] [법률 제14839호, 2017.7.26., 타법개정]

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
4. "전자서명생성정보"라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

전자금융감독규정

[시행 2016.10.5.] [금융위원회고시 제2016-37호, 2016.10.5., 일부개정]

제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경
   나. 비밀번호 보관 시 암호화
   다. 시스템마다 관리자 비밀번호를 다르게 부여
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

제33조(이용자 비밀번호 관리) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.

② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

※ 제2항 제2호의 경우는 통신용비밀번호가 유출된 경우, 계좌원장비밀번호에 영향을 미치지 않도록 하는 조항임.
예를 들어 계좌원장 비밀번호는 숫자 4자리,
" 통신용비밀번호는 사설인증서 이용시, 사설인증서 개인키 접근용 비밀번호를 계좌원장의 비밀번호와 비교하여야 하는가?"
하는 의문이 생길 수 있다. 이 경우 계좌원장 비밀번호와 비교하는 로직의 추가가 보안강화에 도움이 되느냐의 질문으로
치환이 가능하다.

=> 인증서 비밀번호의 설정단계에서는 사전에 본인인증 수행 후 진행되므로 설정 시 카드비밀번호를 알아내는 공격의 위협증대
*** 본인인증이 통과되었다고 가정하였으므로, 이후 전자금융거래서비스 이용이 가능한 상태임**
이용하는 비밀번호의 키로깅 or 화면캡처 공격의 경우, 접근매체 전체를 확보하지 못한 경우이나, 접근매체의 비밀번호
추측습득은 가능하므로 증대되는 위협은 있다고 할 수 있음
*** 이 경우에는 이미 이용단말기가 장악된 경우이므로, 전자금융거래서비스 악용이 가능한 상태임**
또한
키로깅 or 화면캡처 공격이 가능한 기술수준인 경우 파밍에 의해 필요한 정보(카드비밀번호 등)는 습득이 가능함

소결 : 사설인증서 비밀번호(숫자4자리의 경우) 설정과 관련하여 카드비밀번호 비교로직의 구현은 득 보다는 실이 더 크다 할 수 있다.
(최근 자동로그인 기능까지 적용되고 있음을 감안할 필요도 있음)

"만약 당신이 미래를 꿈꾸지 않거나 지금 기술개선을 위해 노력하지 않는다면 그건 곧 낙오되고 있는 것이나 마찬가지 입니다."

그윈 쇼트웰(Gwynne Shtwell, SpaceX CEO, COO)

감사합니다

(facebook.com/sangshik, mikado22001@yahoo.co.kr)