정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

안전한 패스워드 생성 및 이용 지침

박 해 룡*, 이 영 주**, 최 은 영***, 김 종 표****

요 약

본 논문에서는 사용자가 인터넷 사이트에 로그인 할 때, 허가된 사용자임을 확인하는데 이용되는 패스워드를 생성 및 이용에 대한 안전성 측면에 대해서 살펴보고자 한다. 사용자의 패스워드가 노출되면, 사용자의 개인 이메일 정보, 금융정보 등이 타인에게 유출될 수 있다. 이에 사용자는 안전한 패스워드를 생성하고 이용하여야 하며, 또한, 안전하게 관리해야 한다. 이를 준수하기 위해서 안전한 패스워드 정의, 안전한 패스워드 생성팁, 사용자 측면에서의 패스워드 보안 지침, 시스템 관리자 측면에서의 패스워드 보안 지침에 대해서 살펴보고자 한다.

Ⅰ. 서 론

우리는 일상생활에서 PC 혹은 스마트폰을 통해서 다양한 인터넷 서비스를 이용하고 있다. 인터넷 서비스를 안전하게 이용하기 위한 첫 번째 단계로 서비스 사용자 인증을 실행한다. 사용자 인증을 위해서 가장 많이 활용되고 있는 방법이 사용자만 알고 있는 패스워드를 이용하는 방법이다.

사용자가 인터넷 사이트에 로그인 할 때, 허가된 사용자임을 확인하는데 사용되는 패스워드는 문자열로 구성이 된다. 사용자의 패스워드가 노출되면, 사용자의 개인 이메일 정보, 금융정보 등이 타인에게 유출될 수 있다. 이에, 사용자는 안전한 패스워드를 설정하고 이용해야 함과 동시에 안전하게 관리해야 한다.

안전한 패스워드는 제3자가 쉽게 추측할 수 없으며, 시스템에 저장되어 있는 사용자 정보 또는 인터넷을 통해 전송되는 정보를 해킹하여 사용자의 패스워드를 알아낼 수 없거나 알아낸다 하더라도 많은 시간이 요구되는 패스워드를 의미한다. 따라서 안전한 패스워드를 생성하고 이용하기 위한 보안 지침을 설정하고 준수하는 것이 무엇 보다 중요하다.

이에, 본고에서는 안전한 패스워드에 대해서 정의하고 안전한 패스워드를 생성 및 이용을 위한 보안 지침을 제시하고 사용자들이 이를 준수할 것을 권고하고자 한다. 본고의 2장에서는 국내 패스워드 관련 설문조사 결과, 국외 패스워드 관련 현황 등 국내외 패스워드 사용 현황을 분석하고, 3장에서는 패스워드의 안전성 분석하고, 4장에서는 안전한 패스워드를 정의하고, 5장에서는 사용하지 말아야 하는 패스워드를 제시하고, 6장에서는 안전한 패스워드 생성팁을 제시하고, 7장에서는 사용자 측면에서 패스워드 보안 지침을 제시하고, 8장에서는 시스템 관리자 측면에서 패스워드 보안 지침을 제시하고, 9장에서는 결론을 맺고자 한다.

Ⅱ. 패스워드 사용 현황 분석

2.1. 국내 패스워드 관련 설문조사 결과

일반 국민의 패스워드에 대한 인식을 파악하고자 일반인 1837명을 대상으로 패스워드와 관련하여 4가지 항목에 대해 설문조사를 실시하였으며, 그 결과는 다음과 같다.

첫 번째 설문은 권장하는 패스워드 조합에 대한 설문으로 2가지 종류 이상의 문자구성으로 8자리 이상 길이의 작성규칙을 가장 선호하는 것으로 나타났다.

* 한국인터넷진흥원 (연구위원, hrpark@kisa.or.kr), 주저자, 교신저자
** 한국인터넷진흥원 (주임연구원, lyj5607@kisa.or.kr)
*** 한국인터넷진흥원 (책임연구원, bluecey@kisa.or.kr)
**** 한국인터넷진흥원 (수석연구원, skyjp@kisa.or.kr)

〔표 1〕 패스워드 조합 관련 설문조사 결과

선택문항	계(1,837명)
① 2가지 종류 이상의 문자구성으로 8자리 이상의 길이 ※ 문자 구성 : 숫자, 영문 소문자, 영문 대문자, 특수문자	1,119명 (61%)
② 3가지 종류 이상의 문자구성으로 8자리 이상의 길이	533명 (29%)
③ 종류 제한 없이 10자리 이상의 길이 (숫자만 사용하면 안전하지 않을 수 있음)	96명 (5.2%)
④ 종류 제한 없이 12자리 이상의 길이	89명 (4.8%)

두 번째 설문은 패스워드를 주기적으로 변경해야 하는지 여부에 대한 설문으로 일정 주기로 패스워드를 변경하도록 요구하는 것이 필요하다는 답변이 63%를 차지했다.

〔표 2〕 주기적인 패스워드 변경 관련 설문조사 결과

선택문항	계(1,837명)
① 패스워드 변경 요구 필요	1,154명(63%)
② 패스워드 변경 요구 불필요	683명(37%)

세 번째 설문은 인터넷 사이트별로 다른 패스워드를 사용하고 있는지에 대한 설문으로 인터넷 사이트별로 다른 패스워드를 사용한다는 답이 57%를 차지했다.

〔표 3〕 인터넷 사이트 패스워드 관련 설문조사 결과

선택문항	계(1,837명)
① 다른 패스워드 사용	1,050명(57%)
② 동일한 패스워드 사용	787명(43%)

네 번째 설문은 패스워드 변경 요구 시 패스워드 변경 패턴에 대한 설문으로 이전과 비슷한 패스워드로 변경한다는 답변이 65%를 차지했다. 패스워드 변경을 요구 하더라도 새로운 패턴의 패스워드로 변경하지 않는 경향이 있는 것으로 나타났다.

〔표 4〕 패스워드 변경 패턴 관련 설문조사 결과

선택문항	계(1,837명)
① 전혀 다른 패스워드로 변경	637명(35%)
② 이전 패스워드와 비슷한 패스워드로 변경	1,200명(65%)

2.2. 국외 패스워드 사용 현황

2.2.1. 비영어권(중국, 일본 등) 패스워드 작성규칙 현황

중국의 경우 패스워드 작성규칙에 대해서 법령 및 가이드라인 등으로 구체적인 규정 또는 권고사항이 없는 실정이다. 이에 중국은 중국인들이 많이 이용하고 있는 중국의 쇼핑몰, 철도, 차량 예약, SNS, 검색포탈 등을 기반으로 패스워드 사용 현황에 대해서 분석해 보았다.

일본은 중국과 달리 일본 총무성 및 내각사이버보안센터(NISC)에서 일반인에게 패스워드를 안전하게 관리하는 방법을 각각 홈페이지와 가이드북을 통해 안내를 하고 있다. 총무성에서는 '국민을 위한 정보보안 사이트'에서 패스워드는 추측하기 어렵고, 알파벳, 숫자를 혼용하여 적절한 길이의 문자열로 작성할 것을 권고한다. 한편 NISC는 가이드북을 통해 패스워드는 대문자, 소문자, 숫자, 기호를 사용하여 10자리 이상으로

〔표 5〕 중국 주요 인터넷 사이트 패스워드 작성규칙

인터넷 사이트	패스워드 작성규칙
타오바오[8]	대문자, 소문자, 숫자, 특수문자 중 2가지이상 포함하여 6~20자
징등[9]	영어, 숫자, 특수문자 중 2가지이상 포함하여 6~20자
12306[10]	문자, 숫자, 특수문자 6~20자
띠띠추싱[11]	영어, 숫자, 특수문자 중 2가지이상 포함하여 8~16자
웨이보[12]	대문자, 소문자, 숫자, 특수문자 6~16자
QQ[13]	영어, 숫자, 기호 8자~16자
소호[14]	영어·숫자 조합 8~16자(특수문자 포함 가능)
바이두[15]	대문자, 소문자, 숫자, 특수문자 6~14자(허용되는 공백 없음)

복잡하게 사용하도록 권고하고 있다.

중국과 비교해 보고자 일본의 경우도 일본인들이 많이 이용하는 인터넷 사이트에서 사용하는 패스워드 사용 현황에 대해서 분석해 보았다.

〔표 6〕 일본 주요 인터넷 사이트 패스워드 작성규칙

인터넷 사이트	패스워드 작성규칙
야후 재팬[16]	영어, 숫자, 특수문자 중 1가지이상 6~32자
NIFTY[17]	영어, 숫자, 일부특수문자 중 1가지 이상 6~24자 ※ 사용가능한 특수문자 : ″# $ % & ‘() * +, -. / :; 〈=〉? @ 〔\〕 ^ _`{|} ~!) ※ 사용자 이름과 동일한 것 사용할 수 없음
infoseek[18]	문자, 숫자 6자 이상
라이브도어[19]	영어, 숫자, 일부특수문자 중 1가지 이상 8자 이상 ※ 사용가능한 특수문자 :「-」「_」「%」「$」「#」
KIRIN홀딩스[20]	영어, 숫자, 특수문자 6~20자
SHARP[21]	영어, 숫자 8~16자

2.2.2. 영어권(미국, 유럽 등) 패스워드 작성규칙 현황

미국, 유럽 등 영어권 국가에서 패스워드 작성규칙을 권고하고 있는 사항에 대해서 살펴보도록 한다. 이를 위해 NIST(미국 국립표준기술연구소) NCSC(영국 사이버보안센터), ACSC(호주 사이버보안센터), ENISA(유럽 네트워크 정보보호원)의 패스워드 관리 주요 내용 분석해 보았다.

NIST는 규칙에 부합하는 패스워드 생성 및 주기적 패스워드 변경 시 사용자는 쉽게 예측 될 수 있는 형태로 단순하게 패스워드를 생성하거나 여러 계정의 패스워드를 파일 및 다른 방식으로 저장・관리하여 추가적인 보안 문제를 초래할 수 있어서 패스워드 생성규칙의 복잡성을 높이거나 주기적 변경 요구를 금지한다. 패스워드 구성 시 최소 8자 이상의 기억하기 쉬운 문장 형태의 패스워드를 권고하고 패스워드 추측공격을 대비하기 위해 연속 인증시도 실패 시 횟수제한 기능을 권고한다.

NCSC는 영국의 각종 기관이 채택한 길이와 혼합규칙은 사용자에게 예측 가능한 패스워드로 생성하도록 유도하고 도난당한 패스워드는 일반적으로 즉시 악용되기 때문에 정기적인 패스워드 변경은 실질적인 이점 없이 사용자의 부담만 가중되기 때문에 권고하지 않는다.

ACSC는 인증수단이 패스워드 한가지인 경우, 영문, 숫자, 특수문자 혼합규칙 방식보다 혼합규칙 없는 장문의 패스워드가 더 기억하기 쉽고, 동등하거나 또는 보다 높은 보안성을 가지고 있어 권고하고 있고 3가지 이상 문자조합으로 패스워드를 설정한다면 최소 10자 이상 패스워드를 설정하도록 권고한다.

ENISA는 5가지 효과적인 패스워드 정책에 대한 기준을 제시했다.

- 패스워드 길이는 무차별대입공격을 기하급수적으로 어렵게 하므로, 복잡성 보다는 패스워드 길이가 길어야 함
- 특수문자가 포함된 문자열 보다 문장이 기억하기 쉽고 보안성이 높아야 함
- 조직의 서로 다른 시스템에는 동일한 암호를 사용 금지 함
- 공격자의 암호 해독시간 제한 및 노출된 패스워드의 도용방지를 위해 정기적인 패스워드 변경이 필요 함
- 사용자가 정기적으로 패스워드를 변경하는 경우, 이전에 사용했던 패스워드를 재상용하는 것을 금지 함

Ⅲ. 패스워드 안전성 분석

제2장에서 국내외 패스워드 관련 현황 분석한 내용을 기반으로 사용자 패스워드 이용의 편의성 측면과 시스템 관리자 패스워드 관리의 안전성 측면을 동시에 고려하여 안전한 패스워드를 살펴보도록 한다.

사용자의 패스워드 이용의 편의성을 제고하고자 안전한 패스워드를 생성하는 규칙의 간소화 및 변경 주기를 권고하지 않는 것과 동시에 시스템 관리자 측(서비스 제공자, 업체)에서 사용자의 패스워드 입력 및 저장 시 사용되는 일방향 해시함수 적용횟수 증가, 일방향 해시함수 입력값으로 패스워드와 함께 솔트(Salt) 사용 및 안전한 저장이 필요하다.

이에, 시스템 관리자 안전성 측면에서 사용자 패스

워드의 안전한 저장을 위한 방법 및 솔트에 대한 보안 강화 사항 반영이 필요하다. 패스워드 생성 규칙을 간소화하는 대신 패스워드 저장 시 일방향 해시함수를 여러번 적용하여 출력된 값을 저장(패스워드 입력 횟수 제한 포함)하거나, 패스워드와 함께 사용되는 솔트를 안전하게 저장한다면 패스워드 안전성이 강화된다. 또한, 패스워드 변경주기에 맞춰 사용자들에게 변경을 유도해도 변경률이 저조하여[6] 실효성이 떨어지며 위의 조치를 취하면 패스워드 변경주기를 없애는 것도 가능하다. Y. Zhang 등이 제안한 논문[6]에서는 상용화 서비스에서 사용자들이 패스워드를 변경했는지 여부를 실제로 확인한 내용을 기술하였기 때문에 좀 더 신뢰도가 높다고 생각해야 할 것이다.

우리는 패스워드를 일방향 해시함수로 100회 적용 시 전수조사 소요시간이 얼마나 걸리는지 실험을 해보았다. 패스워드 뿐만 아니라 솔트를 일방향 해시함수의 입력값으로 사용한다면, 전수조사 소요시간은 훨씬 증가할 것이며 안전성이 증대될 것으로 기대하고 있다. 패스워드 문자열은 대문자, 소문자, 숫자, 특수문자 등을 조합하여 생성하였고 PC의 사양 등은 다음과 같다.

〔표 8〕 패스워드 연산측정 PC 사양

CPU	Inter(R) Core(TM) i5-6500 3.20GHz
RAM	4 GB
OS	Windows 10 Home
LANGUAGE	JAVA
BIT	64-bit
Hash Function	SHA-256

Ⅳ. 안전한 패스워드

안전한 패스워드는 제3자가 쉽게 추측할 수 없으며, 시스템에 저장되어 있는 사용자 정보 또는 인터넷을 통해 전송되는 정보를 해킹하여 이용자의 패스워드를 알아낼 수 없거나 알아낸다 하더라도 많은 시간이 요구되는 패스워드를 의미한다. 앞서 분석한 내용을 기반으로 안전한 패스워드의 문자열을 다음과 같이 둘 중 하나를 만족하는 것을 사용하도록 권고하고자 한다.

- 두 종류 이상의 문자구성으로 8자리 이상의 길이로 구성된 문자열

〔표 7〕 패스워드를 일방향 해시함수로 100회 적용 시 전수조사 소요시간

조합	자릿수						
	6	7	8	9	10	11	12
숫자	40분	6.7시간	2.8일	27.8일	278일	7.6년	76년
대문자	8.5일	222일	15.8년	411년	10,697년	278,118년	7,231,074년
특수문자	18.3일	4.7년	54.6년	1,802년	59,462년	1,962,264년	∞
대문자+숫자	97.2일	9.6년	345년	12,425년	447,284년	16,102,225년	∞
특수문자+숫자	179.4일	21년	909년	39,087년	1,680,765년	72,272,927년	∞
대소문자	1.6년	84.4년	4,388년	228,199년	11,866,378년	∞	∞
대문자+특수문자	3.5년	204년	12,037년	710,231년	41,903,663년	∞	∞
대소문자+숫자	4.7년	291년	18,011년	1,116,696년	69,235,193년	∞	∞
대문자+특수문자+숫자	8.6년	595년	41,064년	2,833,467년	∞	∞	∞
대소문자+특수문자	29년	2,532년	215,267년	18,297,779년	∞	∞	∞
대소문자+특수문자+숫자	56년	5,398년	512,811년	48,717,086년	∞	∞	∞

※ ∞는 1억년 이상 시간이 소요되는 것을 의미함

※ 단, 문자종류는 알파벳 대문자와 소문자, 특수문자, 숫자 등 4가지임

- 10자리 이상의 길이로 구성된 문자열
  ※ 단, 숫자로만 구성할 경우 취약함

Ⅴ. 권장하지 않는 패스워드

5.1. 안전하지 않은 패스워드

패스워드를 생성하기 위해서 제4장에서 제시한 안전한 패스워드를 준용해야 하며 또한 특정 패턴을 갖는 패스워드, 제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 패스워드, 사용자 ID를 이용한 패스워드, 한글・영어 등을 포함한 사전적 단어로 구성된 패스워드, 특정 인물의 이름이나 널리 알려진 단어를 포함하는 패스워드, 숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 패스워드 등을 사용하면 안 된다.

5.1.1. 특정 패턴을 갖는 패스워드

‘aaaabbbb’, ‘1234512345’ 등과 같이 동일한 문자의 반복되는 패스워드를 사용하면 안 되고, ‘qwertyui’, ‘asdfghjk’ 등 키보드 상에서 연속한 위치에 존재하는 문자들의 집합을 사용하면 안 된다. 또한, ‘security1’, ‘1security’ 등 숫자가 제일 앞이나 제일 뒤에 오는 구성의 패스워드를 사용하면 안 된다.

5.1.2. 제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 패스워드

가족이름, 생일, 주소, 휴대전화번호 등을 포함하는 패스워드를 사용하면 안 된다.

5.1.3. 사용자 ID를 이용한 패스워드

사용자의 ID가 ‘KilDHong’인 경우 패스워드를 ‘KilDHong12’ 또는 ‘HongKilD’으로 설정하면 안 된다.

5.1.4. 한글, 영어 등을 포함한 사전적 단어로 구성된 패스워드

‘바다나라’, ‘천사1004’, ‘love1234’ 등과 같이 한글, 영어 등을 포함한 사전적 단어로 구성된 패스워드를 사용하면 안 된다.

5.1.5. 특정 인물의 이름이나 널리 알려진 단어를 포함하는 패스워드

컴퓨터 용어, 사이트, 기업 등의 특정 명칭을 포함하는 패스워드, 유명인, 연예인 등의 이름을 포함하는 패스워드를 사용하면 안 된다.

5.1.6. 숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 패스워드

영문 대문자 ‘O’를 숫자 ‘0’ 으로, 영문 대문자 ‘I’를 숫자 ‘1’로 치환하는 문자를 포함하는 패스워드를 사용하면 안 된다.

5.1.7. 기타

인터넷 서비스(시스템)에서 초기에 설정되어 있거나 예시로 제시되고 있는 패스워드, 한글의 ‘사랑’을 영어 ‘SaRang’으로 표기하거나 영문자 ‘LOVE’의 발음을 한글 ‘러브’로 표기하는 문자열을 포함하는 패스워드를 사용하면 안 된다.

Ⅵ. 안전한 패스워드 생성팁

6.1. 안전한 패스워드

패스워드를 생성하기 위해서 제4장에서 제시한 안전한 패스워드를 생성하기 위한 팁을 제시하고자 한다. 기억하기 쉬운 패스워드 설정방법, 사이트별 상이한 패스워드 설정을 위한 방법 등을 사용하면 된다.

6.1.1. 기억하기 쉬운 패스워드 설정방법

6.1.1.1. 특정명칭을 선택하여 예측이 어렵도록 가공하여 패스워드 설정

‘한국인터넷진흥원’의 경우 홀수 번째 ‘한인넷흥’이 ‘gksdlssptgmd’로, 짝수 번째 ‘국터진원’이 ‘rnrxjwlsdnjs’로 패스워드를 사용하면 된다. 이와 같이

특정명칭의 홀수/짝수 번째의 문자를 구분하는 등의 가공방법을 통해 패스워드를 설정하거나 국내 이용자는 한글 자판을 기준으로 특정명칭을 선택하고 가공하여 패스워드를 설정하면 된다.

6.1.1.2. 노래 제목이나 명언, 속담, 가훈 등을 이용/가공하여 패스워드 설정

영문사용의 경우, ‘This May Be One Way To Remember’를 ‘TmB1w2R’이나 ‘Tmb1w>r~’로 패스워드를 활용하면 된다. 한글사용의 경우, ‘백설공주와 일곱 난쟁이’를 ‘백설+7난장’로 구성하고 ‘QorTjf+7SksWkd’ 등으로 패스워드를 활용하면 된다.

6.1.2. 예측이 어려운 문자구성의 패스워드 설정방법

6.1.2.1. 영문 대문자/소문자, 숫자, 특수문자들을 혼합한 구성으로 패스워드 설정

‘10H+20Min’, ‘I!Can&9it’ 등과 같은 패스워드를 활용하면 된다.

6.1.2.2. 영문자 앞뒤가 아닌 위치에 특수문자 및 숫자 등을 삽입하여 설정

패스워드의 길이를 증가시키기 위해서 알파벳 문자 앞뒤가 아닌 위치에 특수문자 및 숫자 등을 삽입하여 패스워드를 설정하면 된다. 예를 들어, ‘Security12’가 아니라 ‘Secu1ri2t&&y’와 같은 형태로 패스워드의 길이를 늘려서 설정하면 된다.

6.1.2.3. 영문 대/소문자를 구별할 수 있을 경우 대/소문자를 혼합하여 설정

특정위치의 문자를 대문자로 변경하거나 모음만을 대문자로 변경하여 패스워드를 설정하면 된다. 예를 들어, ‘gkswjdqhwlsdnjs’ 대신 ‘gKsWjDqHwLsDnJs’ 를 패스워드로 설정하거나 ‘rnrqhghgmd’ 대신 ‘rNrQhGhGmD’를 패스워드로 설정하면 된다.

6.1.3. 사이트별 상이한 패스워드 설정을 위한 방법

6.1.3.1. 기본 패스워드 문자열에 사이트별로 특정 규칙을 부여하는 설정방법

자신이 직접 기본 패스워드 문자열을 설정하고 사이트별로 특정 규칙을 적용하여 패스워드를 설정하면 된다. 예를 들어, 패스워드 문자열을 ‘’86*+’로 설정하고, 사이트 이름의 짝수 번째 문자 추가를 규칙으로 yahoo.com는 ‘486*+ao.o’을 패스워드로 설정하거나 google.co.kr는 ‘486*+ogec.r’를 패스워드로 설정하면 된다.

Ⅶ. 사용자 측면에서 패스워드 보안 지침

앞에서 분석한 내용을 종합하여 사용자 측면에서 안전한 패스워드를 생성하고 이용하기 위한 보안 지침을 설정하고자 한다. 다음은 사용자 측면에서 패스워드 보안 지침을 설명한 내용이다.

① 사용자는 제6장을 참고하여 안전한 패스워드를 설정하여 사용해야 한다.
② 초기 패스워드가 시스템에 의해 할당되는 경우, 이용자는 빠른 시간 내에 해당 패스워드를 새로운 패스워드로 변경해야 한다.
③ 패스워드 변경 시, 이전에 사용하지 않은 새로운 패스워드를 사용하고 변경된 패스워드는 이전 패스워드와 연관성이 없어야 한다.
④ 자신의 패스워드가 제3자에게 노출되지 않도록 해야 한다.
⑤ 자신의 패스워드가 제3자에게 노출되었을 경우, 즉시 새로운 패스워드로 변경해야 한다.
⑥ 여러 계정이나 시스템에서 동일한 패스워드를 사용하지 않도록 해야 한다.

Ⅷ. 시스템 관리자 측면에서 패스워드 보안 지침

앞에서 분석한 내용을 종합하여 시스템 관리자 측면에서 사용자들이 안전한 패스워드를 생성하도록 유도함과 동시에 안전한 패스워드 관리 측면에서 보안 지침을 설정하고자 한다. 다음은 시스템 관리자 측면에서 패스워드 보안 지침을 설명한 내용이다.

시스템 관리자 측면에서 안전한 패스워드를 생성하여 이용하기 위한 보안 지침은 아래와 같다.

① 사용자가 안전한 패스워드를 선택할 수 있도록 제7장을 참고하여 패스워드 선택 기준을 안내해야 한다.
② 초기 패스워드, 패스워드 분실 등의 이유로 사용자에게 제공하기 위해 생성된 패스워드는 최소 6자 이상이어야 하며 안전하게 생성된 난수여야 한다.
③ 패스워드를 최소 8자 이상으로 요구해야 하며, 영문, 숫자, 특수 기호를 조합하여 사용할 수 있도록 허용해야 한다.
④ 반복적으로 잘못된 패스워드를 입력할 경우, 입력 횟수를 제한하는 시스템을 구현해야 한다.
⑤ 패스워드는 여러 번의 일방향 해시함수를 사용하고 패스워드와 함께 사용하는 솔트는 안전하게 저장하여야 한다.

Ⅸ. 결 론

패스워드는 인터넷 사이트에 로그인 할 때 사용자 인증을 위해서 흔히 사용되는 방법으로 사용자 패스워드가 노출되면, 보안상 심각한 문제가 발생할 수 있기 때문에 인터넷 서비스에서 사용자가 안전한 패스워드를 생성하고 이용하는 방법은 가장 중요하다고 할 수 있다. 본고에서는 최종적으로 사용자 측면 또는 시스템 관리자 측면에서 안전한 패스워드를 생성하여 이용하기 위한 보안 지침을 제시하고 향후 인터넷 서비스 사용자 및 시스템 관리자가 이를 준수한다면 인터넷 서비스가 보다 안전하게 이용될 수 있는 기반이 마련될 것으로 기대해 본다.

참 고 문 헌

[1] “패스워드 선택 및 이용 안내서” 한국인터넷진흥원, 2019. 6.
[2] “NIST SP 800-63B Digital Identity Guidelines - Authentication and Lifecycle Management,” NIST 2021. 1.
[3] “Password Guidance.” NCSC, 2019. 4.
[4] “Passphrase Requirements,” ACSC, 2017. 11.
[5] “Hacking Team Series - Password Policy”, ENISA, 2015. 8.
[6] Y. Zhang, F. Monrose, and M.K. Reiter, “The Security of Modern Password Expiration : An Algorithmic Framework and Empirical Analysis,” ACM Conference on Computer and Communications Security 2010.
[7] https://www.taobao.com/
[8] https://www.taobao.com/
[9] https://www.jd.com/
[10] https://www.12306.cn/
[11] https://www.didiglobal.com/
[12] https://www.weibo.com/
[13] https://www.qq.com/
[14] https://www.sohu.com/
[15] https://www.baidu.com/
[16] https://www.yahoo.co.jp/
[17] https://www.nifty.com/
[18] https://www.infoseek.co.kr/
[19] https://www.livedoor.com/
[20] https://www.kirin.co.jp/
[21] https://www.sharp.co.jp/

〈저 자 소 개〉

박 해 룡 (Haeryong Park)
종신회원
1999년 2월 : 전남대학교 수학과 졸업
2001년 2월 : 서울대학원 수리과학부 석사
2006년 8월 : 전남대학원 정보보호학과 박사
2000년12월~현재 : 한국인터넷진흥원 팀장
<관심분야> 암호 설계 및 분석, 사용자 인증, 정보보호 R&D, 스팸 정책 및 조사

이 영 주 (Yeong Ju Lee)

정회원

2017년 2월 : 전남대학교 지리학과 졸업

2018년 6월~현재 : 한국인터넷진흥원 차세대암호융합팀 주임연구원

<관심분야> 암호 구현, 랜섬웨어

최 은 영 (Eun Young Choi)

정회원

2001년 8월 : 고려대학교 수학과 졸업

2003년 8월 : 고려대학교 정보보호학과(공학석사)

2009년 8월 : 고려대학교 정보보호학과(공학박사)

2007년 10월~현재 : 한국인터넷진흥원 수석연구원

<관심분야> 암호 프로토콜, IoT, 양자내성암호, 침해사고 분석 등

김 종 표 (Jongpyo Kim)

정회원

2001년 8월 : 경희대 정보통신전문대학원 정보통신망관리공학과 석사

2018년 8월~현재 : 전남대 대학원 정보보안협동과정 박사과정

2005년3월~현재 : 한국인터넷진흥원 팀장

<관심분야> 개인정보보호, 보이스피싱, 불법스팸