TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.0109 개정일: 2018년 12월 xx일

해시 함수 이용 지침

Guideline on Use of Hash Function

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 **정보보호기반 프로젝트그룹(PG501)**

표준안 심의 위원회 **정보보호 기술위원회(TC5)**

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	김도원	KISA	주임연구원	정보보호기반 프로젝트그룹 위원	TTAKS.KO-12.0109
표준 초안 작성자	김도원	KISA	주임연구원	정보보호기반 프로젝트그룹 위원	TTAKS.KO-12.0109
	김기문	KISA	선임연구원	정보보호기반 프로젝트그룹 위원	TTAKS.KO-12.0109
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12.

서 문

1 표준의 목적

해시 함수는 그 자체로도 다양한 암호 응용에 사용되고 있으며, 주요 정보보호 서비스를 제공하는 암호 알고리즘의 핵심 설계 요소로도 사용된다. 이 표준은 주요 해시 함수의 이용 사례에서 해시 함수가 제공해야 하는 안전성 요구사항을 제시하여, 해시 함수를 사용하는 정보보호 시스템의 안전한 운용을 가능하게 한다.

2 주요 내용 요약

이 표준은 해시 함수의 주요 이용 사례를 분류하고, 각 사례별로 요구되는 해시 함수의 안전성 요구사항을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준은 NIST SP 800-107/R1 기반으로 작성되었다. 그러나 NIST SP 800-107/R1은 해시 함수를 사용하는 응용 사례의 안전성을 위주로 내용을 기술한 반면, 이 표준은 응용 사례에서 기반 해시 함수에 요구되는 안전성을 중점적으로 다루고 있다.

3.2 인용 표준과 본 표준의 비교표

TTAKS.KO-12.0109/R1	NIST SP 800-107/R1	비고
5. 해시 함수	4. Approved Hash Algorithms	내용 수정
6. 해시 함수의 사용	5. Hash Function Usage	
6.1 부분 해시 코드	5.1 Truncated Message Digest	내용 수정
6.2 전자 서명	5.2 Digital Signatures	내용 수정
6.3 메시지 인증 코드	5.3 Keyed-Hash Message Authentication Codes (HMAC)	내용 수정
6.4 키 유도 함수	5.4 Hash-based Key Derivation Functions	내용 수정
6.5 난수발생기	5.5 Random Number (Bit) Generation	내용 수정

Preface

1 Purpose

The hash function itself is used in various cryptographic applications and is also used as a key building block of cryptographic mechanisms that provide several information security services. This standard presents the security requirements of a hash function in such use cases, thereby enabling safe operation of the information protection system using the hash function.

2 Summary

This standard categorizes the major use cases of hash functions and presents the security requirements of a hash function for each case.

3 Comparison with Reference Standards

3.1 Relationship to Reference Standards

This standard is based on NIST SP 800-107/R1. However, while NIST SP 800-107/R1 describes the secure use of applications based on hash functions, this standard focuses on the properties required for the underlying hash functions in such applications.

3.2 Comparison with Reference Standards

TTAKS.KO-12.0109/R1	NIST SP 800-107/R1	Note
5. Hash functions	4. Approved Hash Algorithms	revision
6. Hash Function Usage	5. Hash Function Usage	
6.1 Truncated Hash value	5.1 Truncated Message Digest	revision
6.2 Digital Signatures	5.2 Digital Signatures	revision
6.3 Message Authentication Codes	5.3 Keyed-Hash Message Authentication Codes (HMAC)	revision
6.4 Key Derivation Function	5.4 Hash-based Key Derivation Functions	revision
6.5 Random Number Generation	5.5 Random Number (Bit) Generation	revision

목 차

1 적용 범위 ····· 1

2 인용 표준 ····· 1

3 용어 정의 ····· 1

4 약어 ····· 2

5 해시 함수 ····· 2

6 해시 함수의 사용 ····· 3
6.1 부분 해시 코드 ····· 3
6.2 전자 서명 ····· 4
6.3 메시지 인증 코드 ····· 4
6.4 키 유도 함수 ····· 5
6.5 난수발생기 ····· 5

부록 Ⅰ-1 안전성 수준에 따른 해시 함수 분류 ····· 7
Ⅰ-2 국내·외 기관 / 표준문서 사이트 ····· 9

부록 Ⅱ-1 지식재산권 확약서 정보 ····· 10
Ⅱ-2 시험인증 관련 사항 ····· 11
Ⅱ-3 본 표준의 연계(family) 표준 ····· 12
Ⅱ-4 참고 문헌 ····· 13
Ⅱ-5 영문표준 해설서 ····· 14
Ⅱ-6 표준의 이력 ····· 15

해시 함수 이용 지침
(Guideline on Use of Hash Function)

1 적용 범위

해시 함수는 정보보호 시스템에서 다양한 목적을 위해 광범위하게 사용된다. 이 표준은 해시 함수를 기반으로 동작하는 암호 알고리즘이 제공해야 하거나 제공할 수 있는 안전성 수준을 실제로 보장하기 위해 요구되는 해시 함수의 조건을 제시한다. 이 표준에서 다루는 해시 함수 기반 암호 알고리즘은 전자 서명, 메시지 인증 코드, 키 유도 함수, 그리고 난수발생기를 포함한다.

2 인용 표준

NIST SP 800-107/R1, Recommendation for Applications Using Approved Hash Algorithms, 2012.08.

3 용어 정의

3.1 해시 함수

임의의 길이의 문자열을 고정된 길이의 이진 문자열로 매핑하여 주는 함수

3.2 해시 코드

해시 함수의 출력 비트 문자열

3.3 메시지 인증 코드(MAC, Message Authentication Code)

메시지의 인증을 위해 메시지에 부가되어 전송되는 작은 크기의 정보

3.4 키 유도 함수(KDF, Key Derivation Function)

키 유도 함수로 공유된 비밀값을 이용하여 비밀키를 생성하는 함수

3.5 난수발생기(RNG, Random Number Generator)

특정한 제한 조건에 따라 일련의 난수를 발생시키기 위해 설계된 프로그램이나 하드웨어

[출처] 한국정보통신기술협회 정보통신용어사전

4 약어

DRBG Deterministic Random Bit Generator
FIPS Federal Information Processing Standard
HMAC The Keyed-Hash Message Authentication Code
SHA Secure Hash Algorithm

5 해시 함수

정보보호 시스템에서 사용되는 암호학적 해시 함수(cryptographic hash function)는 다음의 세 가지 성질을 가진다.

- 충돌 저항성(collision resistance): 같은 해시 코드를 가지는 서로 다른 해시 함수 입력 값을 찾는 것이 어려워야 한다.
- 역상 저항성(preimage resistance): 임의로 선택된 해시 코드에 대응하는 해시 함수 입력 값을 찾는 것이 어려워야 한다.
- 제 2 역상 저항성(2nd preimage resistance): 주어진 해시 함수 입력 값과 이에 대응하는 해시 코드에 대해, 같은 해시 코드를 가지는 다른 해시 함수 입력 값을 찾는 것이 어려워야 한다.

해시 함수 출력 값의 비트 길이를 L이라 할 때, 기대하는 충돌 저항성에 대한 안전성 수준은 L/2 비트이고, (제 2) 역상 저항성에 대한 안전성 수준은 L 비트이다. 예를 들어 해시 함수 SHA-256[9]과 LSH-256[6]은 충돌 저항성 측면에서 128 비트 안전성을 제공하고, (제 2) 역상 저항성 측면에서 256 비트 안전성을 제공한다. 참고로 일부 해시 함수의 경우 제 2 역상 저항성 측면의 안전성이 입력되는 메시지 길이에 의존하는 경우가 있다.

해시 함수를 기반으로 동작하는 암호 알고리즘에서 요구하는 해시 함수의 안전성은, 어떤 해시 함수의 안전성에 의존하는지 여부에 따라 달라진다. 만일 한 가지 이상의 해시 함수 특성을 이용하는 경우, 상대적으로 약한 안전성 수준이 해시 함수에 대해 요구되는 안전성이 된다. 예를 들어 전자 서명의 경우 해시 함수의 충돌 저항성과 제 2 역상 저항성이 모두 필요하기 때문에, 요구되는 해시 함수의 안전성은 L/2 비트이다.

해시 함수를 기반으로 동작하는 암호 알고리즘에 따라 요구되는 해시 함수의 특성이 다르기 때문에, 이를 고려하여 적합한 해시 함수를 선택해서 사용해야 한다.

이 표준에서는 112 비트 이상의 안전성을 제공하는 해시 함수 알고리즘을 주로 고려한다. 대표적인 해시 함수 알고리즘으로는 국내 암호모듈 검증제도(KCMVP)의 검증 대상 암호로 지정된 SHA-2[9]와 TTA 표준인 LSH[6]가 있다.

6 해시 함수의 사용

6.1 부분 해시 코드

일부 응용에서는 기반 해시 함수가 생성하는 해시 코드의 길이보다 짧은 값을 요구하는 경우가 있다. 이러한 경우에는 해시 코드를 절삭한 부분 해시 코드를 사용하는 것이 적절할 수 있다.

전체 길이가 L 비트인 해시 코드에 대해서, 길이가 λ (< L) 비트인 부분 해시 코드를 사용하기 위해서는 다음의 조건을 충족시켜야 한다.

o 해시 코드의 왼쪽 끝을 기준으로 λ 비트(leftmost λ bits)를 부분 해시 코드로 선택해야 한다.

o 충돌 저항성이 요구되는 경우, λ는 요구되는 충돌 저항성 측면의 안전성 s (비트)의 두 배 이상이어야 한다.(즉, λ ≥ 2s)

해시 함수 SHA-256의 해시 코드 길이는 256 비트(L = 256)이다. <표 5-2>는 요구되는 충돌 저항성(안전성)이 64 비트(s = 64)이고 부분 해시 코드로 상위 128 비트(λ = 128)를 이용하고자 할 경우, 출력된 해시 코드에 대한 부분 해시 코드 예제이다.

<표 5-1> 상위 128 비트 부분 해시 코드 이용의 예

SHA-256	해시 코드	e3b0c442 98fc1c14 9afbf4c8 996fb924 27ae41e4 649b934c a495991b 7852b855
	부분 해시 코드	e3b0c442 98fc1c14 9afbf4c8 996fb924

해시 코드의 절삭은 해시 코드를 이용하는 응용의 안전성에 영향을 줄 수 있다. 예를 들어 충돌 저항성 측면의 기대 안전성은 L/2 (비트)에서 λ/2 (비트)로 낮아진다. <표 5-1>에서 살펴보면, SHA-256은 충돌 저항성 측면에서 128 비트 안전성을 제공하지만 128 비트 부분 해시 코드의 사용으로 제공하는 충돌 저항성 측면의 안전성은 64 비트이다. 또한

역상 저항성 측면의 기대 안전성도 L(비트)에서 λ(비트)로 낮아진다.

해시 코드의 절삭은 해시 함수 기반의 응용에서 해시 코드의 사용과 관련하여 사용자들에게 혼란을 줄 수 있다. 따라서 해당 응용을 사용하는 모든 사용자들에게 사용되는 해시 함수 알고리즘과 절삭 크기에 대해 주지시킴으로써 문제의 소지를 미연에 방지해야 한다.

6.2 전자 서명

RSA나 (EC-)DSA, (EC-)KCDSA[1,2,10,11]와 같은 전자 서명에 사용되는 해시 함수는 충돌 저항성이 요구된다. 예를 들어 같은 해시 코드를 가지는 다른 두 개의 메시지가 있으면, 한 메시지에 대해 생성한 서명 값을 다른 메시지에 대한 서명 값으로도 사용할 수 있다. 이런 경우 서명 검증을 통해 서명된 메시지에 대한 인증을 제공하지 못하게 된다.

전자 서명의 안전성은 기반 해시 함수의 안전성을 넘을 수 없다. 따라서 전자 서명에서 해시 함수를 사용하기 위해서는 다음의 조건을 고려해야 한다.

o 전체 해시 코드
  - 전자 서명의 기대 안전성이 s(비트)일 때, 해시 코드의 길이 L(비트)은 충돌 저항성 측면의 안전성을 고려하여 s의 두 배 이상이어야 한다. (즉, $L \geq 2s$)

o 부분 해시 코드
  - 전자 서명의 파라미터 크기에 따라 부분 해시 코드를 사용해야 하는 경우가 발생할 수 있다. 부분 해시 코드의 사용에 대해서는 6.1절을 참조한다.
  - 6.1절에서 언급한 바와 같이, L비트 크기의 해시 코드를 λ비트로 절삭($\lambda \leq L$)하는 경우, 충돌 저항성 측면의 안전성은 λ/2비트로 낮아진다. 따라서 λ는 전자 서명의 기대 안전성의 두 배 이상으로 설정되어야 한다.

예를 들어, 전자 서명에 요구되는 안전성이 112비트일 경우 224비트 길이 이상의 해시 코드를 사용해야 한다. SHA-2나 LSH는 112비트 이상의 안전성을 제공하므로 이러한 경우에 사용이 가능하며, 특히 SHA-224, LSH-224, LSH-512/224는 절삭 없이 사용할 수 있다. 해시 함수는 절삭되는 길이가 최소화도록 선택하는 것을 권고한다.

6.3 메시지 인증 코드

메시지 인증 코드는 비밀로 관리되는 암호 키를 이용하여 메시지 인증과 무결성을 제공하는 암호 알고리즘으로, 해시 함수를 기반으로 동작하는 대표적인 방식으로는 HMAC[7]이 있다.

해시 함수 기반 메시지 인증 코드 알고리즘의 안전성은 메시지 인증 코드에 사용되는 비밀키, 기반 해시 함수, 그리고 출력 값인 인증 태그(authentication tag)의 안전성에 의해 결정된다. HMAC에 대한 관련 설명은 [7]을 참조할 수 있다.

해시 함수 기반 메시지 인증 코드에 사용되는 해시 함수는 역상 저항성이 요구된다. 해시 함수 SHA-1의 경우 충돌 저항성 측면의 안전성은 63 비트 수준이나 역상 저항성 측면의 안전성은 160 비트이다. 따라서 HMAC의 기대 안전성 수준이 80 비트일 때 SHA-1[9]의 사용이 허용된다.

6.4 키 유도 함수

키 유도 함수(Key Derivation Function)는 비밀로 관리되는 하나의 마스터 키로부터 다양한 용도의 암호 알고리즘 또는 다수의 개체가 사용할 개별 암호 키를 생성하는 용도로 사용된다. 해시 함수는 직접 또는 HMAC에 적용된 형태로 키 유도 함수의 설계 요소로 사용될 수 있다.

키 유도 함수의 안전성은 키 유도 키(key derivation key)와 같은 입력 비밀 정보의 크기와 기반 해시 함수의 안전성, 그리고 유도된 암호 키의 길이에 의해 결정된다. HMAC 기반 키 유도 함수에 대한 관련 설명은 [5]를 참조할 수 있다.

해시 함수(또는 HMAC) 기반 키 유도 함수에 사용되는 해시 함수는 역상 저항성이 요구된다. 따라서 키 유도 함수로부터 유도된 암호 키가 s 비트의 안전성 수준을 제공해야 할 경우, 기반 해시 함수의 역상 저항성 측면의 안전성은 s 비트 이상이어야 한다.

6.5 난수발생기

결정론적 난수발생기(DRBG, deterministic random bit generator)는 결정론적 난수 발생 메커니즘(이하 DRBG 메커니즘)을 기반으로, DRBG 메커니즘이 생성하는 값에 대한 난수성을 보장할 수 있는 엔트로피 소스(entropy source)의 관리를 포함한다. DRBG 메커니즘은 초기값인 씨드(seed)로부터 비트열을 생성하는 알고리즘을 사용하며, 이때 씨드는 엔트로피 소스로부터 선택된 값에 의해 결정된다. 해시 함수는 직접 또는 HMAC에 적용된 형태로 DRBG 메커니즘의 설계 요소로 사용될 수 있으며, 대표적인 방식으로는 Hash_DRBG[3]와 HMAC_DRBG[4]가 있다.

해시 함수 기반의 DRBG 메커니즘이 보장 가능한 최대 안전성은 기반 해시 함수의 역상 저항성에 의존한다. 따라서 개별 DRBG 메커니즘 인스턴스(instance)의 최대 안전성 수

준이 s 비트일 경우, 기반 해시 함수의 역상 저항성 측면의 안전성은 s 비트 이상이어야 한다. 역으로 기반 해시 함수의 역상 저항성 측면의 안전성은 DRBG 메커니즘의 최대 지원 가능한 안전성 수준을 결정한다. Hash_DRBG와 HMAC_DRBG에 대한 관련 설명은 [3,4]를 참조할 수 있다.

부록 Ⅰ-1

안전성 수준에 따른 해시 함수 분류

한국인터넷진흥원이 발간한 "암호 알고리즘 및 키길이 이용 안내서[8]"에서는 전자 서명과 메시지 인증 코드, 키 유도 함수, 난수발생기로 대상을 구분하여 안전성 수준에 따라 사용 가능한 해시 함수를 <표 Ⅰ-1>과 <표 Ⅰ-2>에 명시하고 있다.

<표 Ⅰ-1> 안전성 수준에 따른 전자 서명에서의 해시 함수 사용

안전성 수준	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	SHA-224/256/384/512	SHA-256/384/512 RIPEMD-160	SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-224/256/384/512
112 비트 이상	SHA-224/256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-224/256/384/512
128 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-256/384/512 Whirlpool	SHA-256/384/512
192 비트 이상	SHA-384/512	SHA-384/512	SHA-384/512 Whirlpool	SHA-384/512
256 비트 이상	SHA-512	SHA-512	SHA-512	SHA-512

현재 SHA-1은 (충돌 저항성 측면에서) 80 비트 안전성을 제공하지 못하는 것이 밝혀졌기 때문에, SHA-1을 사용하지 않는 것을 권고한다.

<표 Ⅰ-2> 보안강도에 따른 HMAC/HKDF/RNG용 해시 함수 분류안전성 수준에 따른 메시지 인증 코드, 키 유도 함수, 난수발생기에서의 해시 함수 사용

안전성 수준	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
80 비트 이상	SHA-1 SHA-224/256/384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256/384/512
112 비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SAH-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-224/256/384/512
128 비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	HAS-160 SHA-1 SHA-256/384/512
192 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-256/384/512
256 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-256/384/512 Whirlpool	SHA-256/384/512

<표 Ⅰ-3>은 한국인터넷진흥원이 발간한 "암호 알고리즘 및 키길이 이용 안내서"에서 명시하고 있는 이용연도별 안전성 수준, 전자 서명의 최소 키 길이와 권고하는 해시 함수를 정리한 것이다.

<표 Ⅰ-3> 이용연도별 안전성 수준, 전자서명의 키 길이와 해시 함수

이용연도 (년도)	안전성	전자서명				해시 함수 (보안강도)
		인수분해 (비트)	이산대수		타원곡선 암호 (비트)	
			공개키 (비트)	개인키 (비트)		
2010년까지	80 비트	1024	1024	160	160	80
2011년에서 2030년까지 (최대20년)	112 비트	2048	2048	224	224	112
2030년 이후 (최대30년)	128 비트	3072	3072	256	256	128
	192 비트	7680	7680	384	384	192
	256 비트	15360	15360	512	512	256

부록 Ⅰ-2

국내·외 기관 / 표준문서 사이트

부록 Ⅱ-4에서 명시한 국내·외 기관들의 홈페이지와 문서들은 다음의 사이트에서 찾을 수 있다.

기관 및 문서	사이트 주소
CRYPTREC	http://www.cryptrec.go.jp/english/
IETF	http://www.ietf.org/
TTA	http://www.tta.or.kr/
NIST SP 800	http://csrc.nist.gov/publications/PubsSPs.html
NIST FIPS PUB	http://csrc.nist.gov/publications/PubsFIPS.html
RFC	http://www.ietf.org/rfc.html

부 록 II-1

지식재산권 확약서 정보

II-1.1 지식재산권 확약서 : 해당 사항 없음

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

부 록 II-2

시험인증 관련 사항

II-2.1 시험인증 대상 여부 : 해당 사항 없음

II-2.2 시험표준 제정 현황 : 해당 사항 없음

부 록 II-3

본 표준의 연계(family) 표준

해당 사항 없음

부 록 II-4

참고 문헌

[1] TTA, TTAK.KO-12.0001/R4, “부가형 전자 서명 방식 표준 - 제2부: 한국형 인증서 기반 전자 서명 알고리즘(KCDSA)”, 2016. 12.
[2] TTA, TTAK.KO-12.0015/R3, “부가형 전자 서명 방식 표준 - 제3부: 타원 곡선을 이용한 한국형 인증서 기반 전자 서명 알고리즘(EC-KCDSA)”, 2016. 12.
[3] TTA, TTAK.KO-12.0190-Part1, “해시 함수 기반 결정론적 난수발생기 - 제1부: 일반”, 2018. 12.
[4] TTA, TTAK.KO-12.0191-Part1, “HMAC 기반 결정론적 난수발생기 - 제1부: 일반”, 2018. 12.
[5] TTA, TTAK.KO-12.0273-Part1, “HMAC 기반 키 유도 함수 - 제1부: 일반”, 2018. 12.
[6] TTA, TTAK.KO-12.0276, “해시 함수 LSH”, 2015. 12.
[7] TTA, TTAK.KO-12.0xxx, “해시 함수 기반 메시지 인증 코드 (HMAC) - 제1부: 일반”, 2018. 12.
[8] 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2013. 1.
[9] ISO, ISO/IEC 10118-3, “Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions“
[10] ISO, ISO/IEC 14888-2, “Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms“
[11] ISO, ISO/IEC 14888-3, “Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms“

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 II-5

영문표준 해설서

해당 사항 없음

부 록 II-6

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2009.12.22	제정 TTAK.KO-12.0109	해쉬함수 이용 지침	정보보호기반 (PG501)
제2판	2018.12.xx	개정 TTAK.KO-12.0109/R1	해시 함수 안전성 권고 기준의 변동에 따른 권고기준/예시 수정	정보보호기반 (PG501)