CRYPTREC 暗号技術ガイドライン (SHA-1)

2014 年 3 月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

目次

1. 本書の位置付け 1
1.1. 本書の目的 1
1.2. 本書の構成 1
1.3. 注意事項 1
2. ハッシュ関数 SHA-1 の利用について 2
2.1. 推奨されない利用範囲 2
2.2. 許容される利用範囲 2
3. 参考情報 4
4. 参考文献 6

1. 本書の位置付け

1.1. 本書の目的

本書は、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報を示すものである。

1.2. 本書の構成

本書では、2 章で SHA-1 に関する非推奨及び許容事項を、3 章で参考情報を示す。

1.3. 注意事項

本書の内容は2014年3月31日時点の情報に基づき構成されている。従って、今後、CRYPTREC 暗号リストの改定や攻撃方法の研究動向等によって、本書に掲載される内容が現実にそぐわないケースが発生する可能性がある。

2. ハッシュ関数 SHA-1 の利用について

2.1. 推奨されない利用範囲

(1)電子署名における署名生成

2012 年度に策定した CRYPTREC 暗号リスト(2013 年 3 月 1 日付) [1]の運用監視暗号リストに記載されている。なお、2008 年 4 月に NISC から「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」 [5]が策定されているため、CRYPTREC 暗号リスト [1]では、RSA-PSS 及び RSASSA-PKCS1-v1_5 には下記の(注 1)が付記されている。

(注 1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年 4 月 情報セキュリティ政策会議決定、平成 24 年 10 月 情報セキュリティ対策推進会議改定)を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf (平成 25 年 3 月 1 日現在)

2.2. 許容される利用範囲

(1) 電子署名における署名検証

2012 年度に策定した CRYPTREC 暗号リスト(2013 年 3 月 1 日付) [1]の運用監視暗号リストに記載されている。なお、一定の検証要件を満たすことにより、電子署名やタイムスタンプの有効期間を超えた後でも、それらの有効性を確認可能な長期署名フォーマット(CMS 及び XML に対応)が標準化(JIS 及び ISO)されている。

(2) The Keyed-Hash Message Authentication Code (HMAC)

NIST FIPS PUB 198-1[7]の仕様に基づく HMAC が CRYPTREC 暗号リスト [1]に記載されている。安全性について特段の問題点は指摘されていない [8]。

(3) Key Derivation Functions (KDFs)

NIST SP 800-56A、ANS X9.42、SEC 1 v1.0 で使用される KDF の安全性について、特段の問題点は指摘されていない [9,10]。

(4) 擬似乱数生成系

・ PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1、
・ PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1、
・ PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

の3つの方式が2002年度に策定した改定前の電子政府推奨暗号リスト [2]に記載されている。
また、NIST Special Publication 800-90A [13]にある

・ Hash_DRBG、
・ HMAC_DRBG、
・ CTR_DRBG

の3つの方式が2009年度版リストガイド [14]に記載されている。

(5) パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)

3. 参考情報

(1)電子署名における署名生成

2002 年度に策定した改定前の電子政府推奨暗号リスト(2003 年 2 月 20 日付) [2]では、ハッシュ関数の SHA-1 は注釈において、『(注 6)新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。』と規定していた。また、暗号技術監視委員会(当時)は「SHA-1 の安全性に関する見解」(2006 年 6 月 28 日付け) [3,4]において、『電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規(更新を含む)に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、256 ビット以上のハッシュ関数の使用を薦める。』と報告していた。

NIST Special Publication 800-131A [6]では、

Digital Signature Process	Use	
Digital Signature Generation	80 bits of security strength: DSA: (($\|p\| \geq 1024$) and ($\|q\| \geq 160$)) and (($\|p\| < 2048$) OR ($\|q\| < 224$)) RSA: $1024 \leq \|n\| < 2048$ EC: $160 \leq \|n\| < 224$	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	≥ 112 bits of security strength: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$ RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	Acceptable

とされている。

(2) 電子署名における署名検証

NIST Special Publication 800-131A [6]では、

Digital Signature Process	Use	
Digital Signature Verification	80 bits of security strength: DSA: (($\|p\| \geq 1024$) and ($\|q\| \geq 160$)) and (($\|p\| < 2048$) OR ($\|q\| < 224$)) RSA: $1024 \leq \|n\| < 2048$ EC: $160 \leq \|n\| < 224$	Acceptable through 2010 Legacy-use after 2010
	≥ 112 bits of security strength: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$	Acceptable

	RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	

Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
Legacy-use means that the algorithm or key length may be used to process already protected information (e.g., to decrypt ciphertext data or to verify a digital signature), but there may be risk in doing so. Methods for mitigating this risk should be considered.

とされている。

(3) Key Derivation Functions (KDFs)

NIST Special Publication 800-135 Revision 1 [11]を含む、一般的なアプリケーションで利用される KDF については、「2012 年度版リストガイド(KDF に関する調査)」に記載されている [12]。

(4) 擬似乱数生成系

現在、NIST Special Publication 800-90A Revision 1 [15]、800-90B [16]及び800-90C [17]はドラフト版になっている。

なお、NIST Special Publication 800-131A [6]では、FIPS 186-2 や ANS X9.62-1998 で指定されている擬似乱数生成系に関する移行指針が下記の通り記載されている。

The use of the RNGs specified in FIPS 186-2, [X9.31] and ANS [X9.62] is **deprecated** from 2011 through December 31, 2015, and disallowed after 2015.

Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).

(5) パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)

NIST Special Publication 800-131A [6]に記載がある。

4. 参考文献

[1] 総務省・経済産業省、電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト)、2013 年 3 月 1 日

[2] 総務省・経済産業省、電子政府における調達のために参照すべき暗号のリスト(電子政府暗号リスト)、2003 年 2 月 20 日

[3] CRYPTREC Report 2005 (第 2 版)[1]、2006 年 5 月 17 日

[4] 暗号技術検討会報告書(2006 年度)[2]、2007 年 3 月

[5] 内閣官房情報セキュリティセンター (NISC)、政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針[3]、2008 年 4 月 22 日

[6] NIST Special Publication 800-131A[4]、2011 年 1 月

[7] NIST FIPS PUB 198-1[5]、2008 年 7 月

[8] Mihir Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance[6], CRYPTO 2006, LNCS 4117, pp. 602-619, 2006.

[9] CRYPTREC Report 2007, 2008 年 3 月

[10] 2007 年度電子政府推奨暗号の利用方法に関するガイドブック[7]、2008 年 3 月

[11] NIST Special Publication 800-135 Revision 1[8], 2011 年 12 月

[12] CRYPTREC Report 2012[9], 2013 年 3 月

[13] NIST, Special Publication 800-90A[10], 2012 年 1 月

[14] 2009 年度版リストガイド[11]、2010 年 3 月 ([1]で例示したもの、及び、[12]の Hash_DRBG、HMAC_DRBG、CTR_DRBG)

[15] NIST, Draft NIST Special Publication 800-90A Revision 1[12]

[16] NIST, Draft NIST Special Publication 800-90B[13]

[17] NIST, Draft NIST Special Publication 800-90C[14]

---

[1] http://www.cryptrec.go.jp/report/c05_wat_final.pdf
[2] http://www.cryptrec.go.jp/report/c06_kentou_final.pdf
[3] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
[4] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
[5] http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
[6] https://eprint.iacr.org/2006/043
[7] http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf
[8] http://csrc.nist.gov/publications/nistpubs/800-135-rev1/sp800-135-rev1.pdf
[9] http://www.cryptrec.go.jp/report/c12_sch_web.pdf
[10] http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
[11] http://www.cryptrec.go.jp/report/c09_guide_final.pdf
[12] http://csrc.nist.gov/publications/drafts/800-90/draft_sp800_90a_rev1.pdf
[13] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

[14] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf

発行日　2014年8月4日　第1版
発行者
・〒184-8795
東京都小金井市貫井北町四丁目2番1号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所 セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人 情報処理推進機構
（セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN