CRYPTREC 暗号技術ガイドライン (SHA-1)
改定版

2018 年 4 月

国立研究開発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. 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、「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) [C13a]の「運用監視暗号リスト」[1]に記載されているハッシュ関数 SHA-1 を継続して利用する際に参考となる指針を示すものである。そのために、運用監視暗号リストに記載されている SHA-1 を補助関数として用いる暗号技術が、互換性維持の目的であれば継続利用が容認されるかどうかを示す。

2 章において、SHA-1 を用いる補助関数のタイプ別に各々の暗号技術の継続利用の指針について示し、3 章において SHA-1 を用いる補助関数のタイプと継続利用に関する詳細について示す。4 章において SHA-1 の危殆化に関する背景及びそれらに関連する参考情報について示す。

1.2. 本書の適用範囲

本書で取り扱う暗号技術は、1.2.1 節及び 1.2.2 節の範囲とする。

1.2.1. CRYPTREC 暗号リスト

本書で取り扱う暗号技術は、「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) [C13a]の「電子政府推奨暗号」[2]に記載されている暗号技術のうち、SHA-1 を利用する場合のあるものを対象とする(表 1)。

1.2.2. CRYPTREC 暗号の仕様書

本書で取り扱う暗号技術は、「CRYPTREC 暗号の仕様書」[C17b](2018 年 1 月現在)で指定されている仕様書を対象とする(表 1)。

---

[1] 実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

[2] CRYPTREC により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるが今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

表 1: 本書で対象となる暗号技術の範囲と仕様書

技術分類		暗号名称	仕様書
公開鍵暗号	署名	DSA	NIST FIPS PUB 186-4
		ECDSA	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) または ANS X9.62-2005
		RSASSA-PKCS1-v1_5	Public-Key Cryptography Standards (PKCS)#1 v2.2
		RSA-PSS	Public-Key Cryptography Standards (PKCS)#1 v2.2
	守秘	RSA-OAEP	Public-Key Cryptography Standards (PKCS)#1 v2.2
	鍵共有	DH	ANS X9.42-2003 または NIST SP 800-56A Revision2 (May 2013)において FFC DH プリミティブとして規定されたもの
		ECDH	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) または NIST SP 800-56A Revision2 (May 2013)において C(2e,0s,ECC CDH) として規定されたもの
メッセージ認証コード		HMAC	NIST FIPS PUB 198-1
エンティティ認証		ISO/IEC 9798-3	ISO/IEC 9798-3:1998, ISO/IEC 9798-3:1998/Amd 1:2010, ISO/IEC 9798-3:1998/Cor 1:2009, ISO/IEC 9798-3:1998/Cor 2:2012

1.3. 注意事項

本書の内容は、2018 年 1 月時点の情報に基づき記載されている。今後、CRYPTREC 暗号リストの改定や攻撃方法の進展状況等によって、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。

CRYPTREC では、SHA-1 の安全性に関する見解などを公表してきたが、内閣サイバーセキュリティセンター (National center of Incident readiness and Strategy for Cybersecurity、以下 NISC という。) や米国の国立標準技術研究所 (National Institute of Standards and Technology、以下 NIST という。) が示してきたような SHA-1 に関する利用期限については公表していない。

1.4. 謝辞

本書を作成するにあたり、セコム株式会社 IS 研究所の松本 泰 様、佐藤 雅史 様、島岡 政基 様、及び、NPO 日本ネットワークセキュリティ協会(JNSA) 電子署名 WG のメンバーの方々から有益なご意見・コメントいただいた。ここに謝意を表する。

2. CRYPTREC 暗号リストにおいて SHA-1 を補助関数として用いる電子政府推奨暗号の継続利用の指針

ハッシュ関数 SHA-1 は NIST が 1995 年に策定した、ハッシュ長が 160 ビットの暗号学的ハッシュ関数である［NT15b］。一般に、暗号学的ハッシュ関数には、衝突発見困難性[3]、第二原像計算困難性[4]及び原像計算困難性[5]の 3 つの安全性要件を満たすことが求められる。ところが、2017 年に SHA-1 は衝突発見困難性を満たしていないことが発表された［S17a, S17b］。

SHA-1 は、暗号技術の補助関数としてさまざまな部分で利用されており、CRYPTREC 暗号リストの多くの暗号技術において採用されている。その中には、衝突発見が安全性に直接的に影響を与えるものと与えないものが存在している。現状、実運用環境においては SHA-1 の継続利用を避けることが互換性維持の観点から現実的な選択肢ではない場面も想定されるため、CRYPTREC 暗号リストの電子政府推奨暗号リストにおいて補助関数として SHA-1 を用いる場合(ただし、擬似乱数生成系を除く[6])に、互換性維持の目的であれば継続利用が容認されるかどうかを示す(表 2)。

表 2: CRYPTREC 暗号リストにおいて SHA-1 を補助関数として用いる電子政府推奨暗号の継続利用の指針

技術分類	SHA-1 を補助関数として用いる暗号名称	継続利用の指針
署名	DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS	署名生成については、 電子政府推奨暗号リストに記載されたハッシュ関数への移行を推奨 署名検証については、 互換性維持目的※での継続利用は容認
守秘	RSA-OAEP	互換性維持目的での継続利用は容認
鍵共有	DH, ECDH	
メッセージ認証コード	HMAC	
エンティティ認証	ISO/IEC 9798-3	

※ 電子政府推奨暗号リストに記載されたハッシュ関数への移行が困難な場合や SHA-1 の継続利用を停止すると、より大きなセキュリティ上の懸念が生じうる場合を想定している。また、ここで述べる互換性維持には該当しないが、後述する長期署名における過去の SHA-1 による署名検証も容認される。

[3] ハッシュ関数 Hash が衝突発見困難性を有するとは、$X_1 \neq X_2$ かつ Hash (X_1) = Hash (X_2) となる X_1, X_2 を見つけることが困難であることをいう。

[4] ハッシュ関数 Hash が第二原像計算困難性を有するとは、X_1 に対して、$X_1 \neq X_2$ かつ Hash (X_1) = Hash (X_2) となる X_2 を見つけることが困難であることをいう。

[5] ハッシュ関数 Hash が原像計算困難性を有するとは、Y に対して、Hash (X) = Y となる X を見つけることが困難であることをいう。

[6] 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。

3. SHA-1 を用いる補助関数と継続利用の詳細

3.1. SHA-1 を用いる補助関数のタイプ

表 2 の指針の理由を示すため、本書で対象となる暗号技術の範囲における SHA-1 を用いる補助関数を分類する(表 3)。各補助関数のタイプについては、後述する。

表 3: 本書で対象となる暗号技術と補助関数のタイプ

技術分類	SHA-1 を補助関数 として用いる暗号名称	補助関数のタイプ
署名	DSA, ECDSA, RSASSA-PKCS1-v1_5	・メッセージのハッシュ値
	RSA-PSS	・メッセージのハッシュ値 ・ハッシュ値の連結(MGF)
守秘	RSA-OAEP	・ハッシュ値の連結(MGF)
鍵共有	DH, ECDH	・ハッシュ値の連結(KDF)
メッセージ認証コード	HMAC	・ハッシュ関数のカスケーディング
エンティティ認証	ISO/IEC 9798-3	・上記の署名と同じ

3.1.1. メッセージのハッシュ値

本書で対象となる署名では、ハッシュ関数 Hash に関して、署名生成および署名検証対象のメッセージ M を入力として、その出力値(ハッシュ値) H = Hash(M) の計算を行う。

3.1.2. ハッシュ値の連結

3.1.2.1. マスク生成関数(Mask Generation Function, MGF)

本書で対象となる署名または守秘の中では、ハッシュ関数 Hash に関して、Data を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

h = h || Hash(Data || Counter)　(||は文字列の連結)

のように、ハッシュ値を連結していくことで、指定された長さの出力値 h の計算を行う。

3.1.2.2. 鍵導出関数(Key Derivation Function, KDF)

(a) 本書で対象となる鍵共有の中では、ハッシュ関数 Hash に関して、共有鍵 Z を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

$$h := \mathrm{Hash}(Z \,||\, \mathrm{OtherInfo}) \,||\, h, \text{ または}$$

$$h := \mathrm{Hash}(\mathrm{Counter} \,||\, Z \,||\, \mathrm{OtherInfo}) \,||\, h$$

のように[7]、出力値を次々に連結していくことで、指定された長さの出力値 h の計算を行うことがある。なお、OtherInfo とは、鍵共有が使われる状況に応じて決定される固有のデータを指す。

(b) 本書で対象となる鍵共有の中では、メッセージ認証コード HMAC [NT08]に関して、共有鍵 Z を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

$$h := \mathrm{HMAC}(\mathrm{Counter} \,||\, Z \,||\, \mathrm{OtherInfo}) \,||\, h$$

のように、出力値を次々に連結していくことで、指定された長さの出力値 h の計算を行う。なお、OtherInfo とは、鍵共有が使われる状況に応じて決定される固有のデータを指す。

3.1.3. ハッシュ関数のカスケーディング

本書で対象となるメッセージ認証コード HMAC [NT08]では、ハッシュ関数 Hash に関して、鍵 K 及びメッセージ M を入力として、

$$\mathrm{HMAC}(K, M) := \mathrm{Hash}(K_2 \,||\, \mathrm{Hash}(K_1 \,||\, M))$$

ただし、$K_1 := K \oplus \mathrm{ipad}$, $K_2 := K \oplus \mathrm{opad}$ である

(ipad と opad はある固定値で、⊕は排他的論理和).

のように、ハッシュ関数 Hash をカスケーディング(関数の合成)してハッシュ値の計算を行う。

[7] 各仕様によって、共有鍵 Z や Counter などの位置が前後する場合がある。

3.2. SHA-1 の継続利用について

3.2.1. 署名

署名には、署名が付与された文書やデータに改ざんが施されていないことを確認する改ざん防止の機能と、文書やデータに付与された署名が署名を付与した本人であることを確認するなりすましを防止する機能がある。ここでは、主に、署名生成から時間が経過した後に署名検証が求められる用途を想定し、指針を示す。このような用途の例としては電子契約等で用いる否認[8]防止目的の署名、コード署名、タイムスタンプ局が発行するタイムスタンプトークンの署名などが考えられる。

(1) 署名生成

署名対象となるハッシュ値が同じである相異なる 2 つの文書やデータの作成が現実的となれば、一方の文書(データ)に署名したあと、他方に差し替えられる(署名者が意図しなかった方の文書やデータに署名したかのように見せかけられる)リスクが高まるため、署名の作成において SHA-1 の継続利用は不適当である。署名を新規作成する場合には、より安全性の高いハッシュ関数(たとえば、ハッシュ関数 SHA-256 など)の利用に切り替えることが推奨される。

(2) 署名検証

電子政府システムやアプリケーションに依存するが、e-文書法など、法律的な要請を考慮して、当面の間、署名検証を必要とする場合もある。過去に SHA-1 を用いて生成された署名であっても、以下に述べる長期署名やその他の手段によって、作成された当時の署名の有効性が維持されていると判断される場合には、署名の検証において SHA-1 の継続利用は容認される。

有効性を維持する方法の一つとして、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、XML 及び PDF に対応)が標準化されているので［I12a, I12b, I17, J08a, J08b］、長期保存が必要な場合は、これらを利用して署名検証を維持・継続できる。

[8] 電子契約等を取り交した後になって、その者がその事実や内容を否定すること。

3.2.2. 守秘

RSA-OAEP [R12]は、3.1.2.1.節で述べたように、マスク生成関数の補助関数としてハッシュ関数を使用している。RSA-OAEP の安全性に関しては、用いられているハッシュ関数に衝突耐性が保証されていなかったとしても安全性が保たれるという理論的な研究がなされている [KA10]。安全性について特段の問題点は指摘されていないため、守秘において SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.3. 鍵共有

過去の評価結果[C00,C01,C02]では、基本的な鍵共有の使用に際しては、受動的攻撃(鍵共有のために通信されるデータに攻撃者が影響を与えることがない場合)に対しては問題点は指摘されていないが、能動的攻撃(鍵共有のために通信されるデータに攻撃者が影響を与える可能性がある場合)に対して、最低限、以下の 3 点に注意を払う必要がある、とされている。

・公開鍵とエンティティとの結び付きを保証する手段を確保する。
・(更新を前提とする)セッション鍵共有方式として使用する場合には、交換する公開鍵は一時的なものとする。
・共有される鍵が乱数と見分けがつかなくするためには鍵導出関数を使用する。

共有される鍵を乱数と見分けがつかなくするために使用される鍵導出関数(Key Derivation Function, KDF)は、3.1.2.2.節で述べたように、補助関数のタイプ別では、ハッシュ値の連結ベースのものと、ハッシュ関数のカスケーディングベースのものの 2 つの構成方法がある。安全性について特段の問題点は指摘されていないため、鍵共有において SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.4. メッセージ認証コード

HMAC [NT08]は、3.1.3.節で述べたように、ハッシュ関数のカスケーディングベースで構成されている。HMAC の安全性に関しては、用いられているハッシュ関数に衝突耐性が保証されていなかったとしても安全性が保たれるという理論的な研究がなされている [B15, G14]。安全性について特段の問題点は指摘されていないため、メッセージ認証コードにおいて SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.5. エンティティ認証

エンティティ認証とは、認証される者が実際にその者であることを確認する機能である。ここでは、エンティティ認証を実現する仕組みとして署名を用いるものを想定している。3.2.1 節の署名とは異なり、チャレンジ-レスポンスのように、署名対象のデータ[9]と署名のデータを短時間で使い捨てるように利用される。衝突を計算する十分な時間が現時点では確保できないと考えられるため、短時間に認証が完了するのであれば、エンティティ認証に用いられる署名において SHA-1 の継続利用は互換性維持目的であれば容認される。

[9] ISO/IEC 9798-3 では、シークエンス番号、タイムスタンプ、ID 番号や乱数等からなるデータの組み合わせが規定されている。

4. SHA-1 の危殆化に関する背景と参考情報

4.1. CRYPTREC 及び NISC における対応

SHA-1 は、2002 年度に策定した「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（電子政府推奨暗号リスト）」(2003 年 2 月 20 日)に、注釈(注 6)[10]を付けて掲載された。暗号技術監視委員会(当時)は、2005 年に SHA-1 に対する衝突探索アルゴリズムに関する論文［W05]が発表された際に、その詳細を検討し［C06]、「SHA-1 の安全性に関する見解」の案［C05]を作成した。その後、この見解案は 2006 年 6 月 28 日に正式に承認され、暗号技術検討会事務局へ提出された［C07]。

その後、電子政府システムにおいて移行についての検討が進められ［ME10,ME11,MI09]、内閣官房情報セキュリティセンター(当時)は、2008 年 4 月に「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」［NC08b]を公表した。なお、この指針は 2012 年 10 月に改定版［NC12b]が公表されている。いままでに、政府認証基盤(GPKI)や地方公共団体組織認証基盤(LGPKI)などにおいて、システムの移行が進んでいる［L14,MI14]。

2012 年度に改定された CRYPTREC 暗号リストにおいては、運用監視暗号リストに、注釈(注 8)[11]を付けて記載された。

2015 年 10 月 8 日に、オランダの国立情報工学・数学研究所(CWI)、フランスの国立情報学自動制御研究所(INRIA)及びシンガポールの南洋理工大学(NTU)の共同研究チームは、SHA-1 のフルラウンド(全 80 ステップ中 80 ステップ)に対して、仕様より緩い条件下ながら衝突発見に成功したと発表した［S15]。暗号技術評価委員会では、CRYPTREC の Web ページにおいてこの件に関する注意喚起を行い［C15a]、暗号技術検討会に報告した［C15b]。

2017 年 2 月 23 日に、CWI 及び Google の共同研究チームは、SHA-1 のフルラウンドに対する衝突発見に成功したと発表した［S17a]。発表された論文［S17b]によれば、衝突発見に要する計算量は、6500 CPU コア・年 + 100 GPU・年であり、768 ビット(10 進 232 桁)の合成数の素因数分解に要した計算量［KL10]や 768 ビットの離散対数の計算［KL17]よりも数倍ほど大きな量であった。暗号技術評価委員会では、CRYPTREC の Web ページにおいてこの件に関する注意喚起を行った［C17a]。

---

[10] 『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。』

[11] 『「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)』

現在までに、SHA-1 の第二原像計算困難性及び原像計算困難性については実運用環境に影響を及ぼすほどの問題は見つかっていない。

CRYPTREC では、表 3 のように、SHA-1 の安全性に関する意見などを公表してきたが、NIST が示してきたような SHA-1 に関する利用期限については公表していない。

表 3: SHA-1 の衝突に係る主な年表

時期	出来事
1995 年 4 月	FIPS PUB 180-1 策定 (NIST)
2003 年 2 月	電子政府推奨暗号リスト策定 (CRYPTREC)
2004 年 8 月	SHA-1 への攻撃に対する短い声明 (NIST) [NT04]
2005 年 8 月	衝突探索アルゴリズムの論文発表 (Wang ら)
2006 年 4 月	SHA-1 への攻撃に対する声明 (NIST) [NT06]
2006 年 6 月	SHA-1 の安全性に関する見解 (CRYPTREC)
2008 年 4 月	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 に係る移行指針の策定 (NISC)
2011 年 1 月	SP 800-131A 策定(2015 年 10 月に Revision 1 に改定) (NIST)
2013 年 3 月	CRYPTREC 暗号リスト策定 (CRYPTREC)
2015 年 10 月	SHA-1 のフリースタート衝突の発見 (Stevens ら)
2017 年 2 月	SHA-1 の衝突発見(Stevens ら)

4.2. NISTにおける対応

(1) ハッシュ関数

NIST SP 800-57 Part 1 Revision 1では、SHA-1については、表4 の通り記載されている。

表4: NISTにおけるハッシュ関数の安全性強度と利用範囲の状況（[NT16]から抜粋）

Security Strength	**Digital Signatures and hash-only applications**	**HMAC, Key Derivation Functions, Random Number Generation**
≤ 80	SHA-1	
112	SHA-224, SHA-512/224, SHA3-224	
128	SHA-256, SHA-512/256, SHA3-256	SHA-1
192	SHA-384, SHA3-384	SHA-224, SHA-512/224
≥ 256	SHA-512, SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-512

また、NIST SP 800-131A Revision 1では、SHA-1については、表5 の通り記載されている。

表5: NISTにおけるSHA-1の承認状況（[NT15c]から抜粋）

Hash Function	**Use**	
SHA-1	Digital signature generation	Disallowed, except where specifically allowed by NIST protocol-specific guidance.
	Digital signature verification	Legacy-use
	Non-digital signature applications	Acceptable

SHA-1 for digital signature generation:
SHA-1 may only be used for digital signature generation where specifically allowed by NIST protocol-specific guidance. For all other applications, SHA-1 **shall not** be used for digital signature generation.

SHA-1 for digital signature verification:
For digital signature verification, SHA-1 is allowed for **legacy-use**.

SHA-1 for non-digital signature applications:
For all other hash function applications, the use of SHA-1 is **acceptable**. The other applications include HMAC, Key Derivation Functions (KDFs), Random Bit Generation, and hash-only applications (e.g., hashing passwords and using SHA-1 to compute a checksum, such as the approved integrity technique specified in Section 4.6.1 of [FIPS 140]).

(2) 擬似乱数生成系

NIST SP 800-131A Revision 1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ついては、表6 の通り記載されている。NISTの基準ではSHA-1 のHASH_DRBG及びHMAC_DRBG での利用が許容されているが、それ以外での利用は現在では承認されていない。

表 6: NIST における乱数生成器の承認状況 ([NT15c]から抜粋)

Description	Use
HASH_DRBG, HMAC_DRBG and CTR_DRBG	Acceptable
DUAL_EC_DRBG	Disallowed
RNGs in FIPS 186-2, ANS X9.31 and ANS X9.62-1998	Deprecated through 2015 Disallowed after 2015

Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
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).

なお、現在、NIST SP 800-90C [NT16b]はドラフト版になっている。NICT SP 800-90B [NY16a]は最終版が 2018 年 1 月に公開されている。

(3) 鍵導出関数

NIST SP 800-131A Revision 1では、鍵導出関数について、表7 の通り記載されている。

表 7: NIST における鍵導出関数の承認状況 ([NT15c]から抜粋)

Algorithm	Use	
HMAC-based KDF	Acceptable	
CMAC-based KDF	Two-key TDEA-based KDF	Deprecated through 2015 Disallowed after 2015
	AES and Three-key TDEA	Acceptable

HMAC-based KDF (HMAC is the Keyed-Hash Message Authentication Code [FIPS 198-1]): The use of HMAC-based KDFs is **acceptable** using an **approved** hash function, including SHA-1. See Section 10 for discussions of the key lengths used with HMAC
CMAC-based KDF:
The use of two-key TDEA as the block cipher algorithm in a CMAC-based KDF is **deprecated** through December 31, 2015.
Two-key TDEA **shall not** be used to derive keying material after December 31, 2015.
The use of AES and three-key TDEA as the block cipher algorithm in a CMAC-based KDF is **acceptable**.

5. 参考文献

[B15] M. Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance, Journal of Cryptology 28(4): 844-878 (2015). https://eprint.iacr.org/2006/043

[C00] CRYPTREC Report 2000, 2001年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C01] CRYPTREC Report 2001, 2002年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C02] CRYPTREC Report 2002, 2003年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C03a] 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 http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_fy2005.pdf

[C05] CRYPTREC Report 2005 (第2版), 2006年5月17日 http://www.cryptrec.go.jp/report/c05_wat_final.pdf

[C06] ハッシュ関数(SHA-1)の安全性評価および攻撃手法整理, CRYPTREC技術報告書501番, 2006年3月, http://www.cryptrec.go.jp/estimation/rep_ID0501.pdf

[C07] 暗号技術検討会報告書(2006年度), 2007年3月 http://www.cryptrec.go.jp/report/c06_kentou_final.pdf

[C08a] CRYPTREC Report 2007, 2008年3月 http://www.cryptrec.go.jp/report/c07_wat_final.pdf

[C08b] 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, 2008年3月 http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

[C10] 2009年度版リストガイド, 2010年3月 http://www.cryptrec.go.jp/report/c09_guide_final.pdf

[C13a] 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 http://cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

[C13b] CRYPTREC Report 2012, 2013年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C15a] SHA-1の安全性について, 平成27年12月18日 http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

[C15b] 暗号技術検討会報告書(2015年度), 2016年3月 http://www.cryptrec.go.jp/report/c15_kentou_final.pdf

[C17a] SHA-1の安全性低下について, 平成29年3月1日 http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

[C17b] CRYPTREC暗号の仕様書, 2017年6月 http://www.cryptrec.go.jp/method.html

[G14] P. Gaži, K. Pietrzak, and M. Rybár: The Exact PRF-Security of NMAC and HMAC, CRYPTO 2014, Lecture Notes in Computer Science vol. 8616, pp.113-130, 2014. https://eprint.iacr.org/2014/578.pdf

[I98] ISO/IEC 9798-3:1998, Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques

[I12a] ISO 14533-1:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

[I12b] ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

[I17] ISO 14533-3:2017, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)

[IK03] Tetsu Iwata and Kaoru Kurosawa: OMAC: One-Key CBC MAC. Fast Software Encryption 2013: 129-153.
https://eprint.iacr.org/2002/180.pdf

[J08a] JIS X 5092:2008, CMS 利用電子署名(CAdES)の長期署名プロファイル
Long term signature profiles for CMS advanced electronic signatures (CAdES)

[J08b] JIS X 5093:2008, XML 署名利用電子署名(XAdES)の長期署名プロファイル
Long term signature profiles for XML advanced electronic signatures (XAdES)

[J14] 独立行政法人情報処理推進機構, 承認されたセキュリティ機能に関する仕様(平成 26 年 4 月 1 日),
https://www.ipa.go.jp/security/jcmvp/documents/asf01.pdf

[K10] Hugo Krawczyk: Cryptographic Extraction and Key Derivation: The HKDF Scheme. CRYPTO 2010, Lecture Notes in Computer Science vol. 6223, pp. 631-648, 2010.
https://eprint.iacr.org/2010/264.pdf

[KA10] Akinori Kawachi, Akira Numayama, Keisuke Tanaka, Keita Xagawa: Security of Encryption Schemes in Weakened Random Oracle Models. Public Key Cryptography 2010: 403-419.
https://www.iacr.org/archive/pkc2010/60560406/60560406.pdf

[KL10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann: Factorization of a 768-bit RSA modulus. CRYPTO 2010, Lecture Notes in Computer Science vol. 6223, pp. 333-350. 2010. https://eprint.iacr.org/2010/006.pdf

[KL17] T. Kleinjung, C. Diem, A. K. Lenstra1, C. Priplata, and C. Stahlke, Computation of a 768-bit prime field discrete logarithm
https://eprint.iacr.org/2017/067.pdf

[L09] G. Leurent, P. Q. Nguyen: How Risky Is the Random-Oracle Model?, CRYPTO 2009, Lecture Notes in Computer Science vol. 5677, pp. 445-464. 2009.
https://iacr.org/archive/crypto2009/56770440/56770440.pdf

[L14] 地方公共団体情報システム機構, LGPKI の移行方針について, 2014 年 12 月 19 日更新, http://www.lgpki.jp/unei/LGPKI_ikouhoushin_20141219.pdf

[ME10] 「電子署名法における暗号アルゴリズム移行研究会」報告書(2010 年 3 月)
http://www.meti.go.jp/policy/netsecurity/docs/esig/h21_esign-crypto-report.pdf

[ME11] 「電子署名法における暗号アルゴリズム移行研究会」報告書(2011 年 3 月)
http://www.meti.go.jp/policy/netsecurity/docs/esig/h22esig-alg-report.pdf
[MI09] 「公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書」,
平成 21 年 1 月,
http://www.soumu.go.jp/main_sosiki/kenkyu/kouteki_kojin/pdf/090126_houkoku.pdf
[MI14] 総務省 行政管理局 政府認証基盤, 暗号アルゴリズムの移行について,
https://www.gpki.go.jp/documents/angouikou.html
[NC08a] 内閣官房情報セキュリティセンター (NISC), 情報セキュリティ政策会議 第 17 回会合 資料 3-1, 政府機関における安全な暗号利用の促進, 移行指針(案)に基づく暗号方式の移行完了までのスケジュール, 2008 年 2 月 4 日
http://www.nisc.go.jp/conference/seisaku/dai16/pdf/16siryou0301.pdf
[NC08b] 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, 2008 年 4 月 22 日, 情報セキュリティ政策会議決定
http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
[NC12a] 内閣官房情報セキュリティセンター (NISC), 情報セキュリティ政策会議 第 31 回会合 資料 3-1, 政府機関の暗号アルゴリズムに係る移行指針の改定概要, (参考) 政府機関における暗号移行スケジュール, 平成 24 年 11 月 1 日
http://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryou0301.pdf
[NC12b] 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, 2012 年 10 月 26 日改定, 情報セキュリティ対策推進会議決定
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
[NT04] NIST Brief Comments on Recent Cryptanalytic Attacks, 2004 年 8 月,
https://csrc.nist.gov/News/2004/NIST-Brief-Comments-on-Recent-Cryptanalytic-Attack
[NT06] NIST Comments on Cryptanalytic Attacks on SHA-1, 2006 年 4 月,
https://csrc.nist.gov/News/2006/NIST-Comments-on-Cryptanalytic-Attacks-on-SHA-1
[NT08] NIST FIPS PUB 198-1, 2008 年 7 月
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
[NT09] NIST Special Publication 800-108, 2009 年 10 月
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf
[NT11] NIST Special Publication 800-135 Revision 1, 2011 年 12 月
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
[NT13] NIST Special Publication 800-56A Revision 2, 2013 年 5 月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf
[NT15a] NIST, Special Publication 800-90A Revision 1, 2015 年 6 月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
[NT15b] NIST FIPS PUB 180-4, 2015 年 8 月
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[NT15c] NIST Special Publication 800-131A Revision 1, 2015年11月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
[NT16] NIST, NIST Special Publication 800-57 Part 1 Revision 4, 2016年1月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
[NT16a] NIST, NIST Special Publication 800-90B, 2018年1月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
[NT16b] NIST, (Second DRAFT) NIST Special Publication 800-90C
http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf
[NO8] Akira Numayama, Toshiyuki Isshiki, Keisuke Tanaka: Security of Digital Signature Schemes in Weakened Random Oracle Models. Public Key Cryptography 2008: 268-287.
https://www.iacr.org/archive/pkc2008/49390269/49390269.pdf

[R12] RSA Laboratories, PKCS #1 v2.2: RSA Cryptography Standard, 2012年10月
https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
[S15] Press Release “Researchers urge: industry standard SHA-1 should be retracted sooner”, CWI, INRIA, NTU, October 8, 2015.
https://www.cwi.nl/news/2015/researchers-urge-industry-standard-sha-1-should-be-retracted-sooner
[S17a] Announcing the first SHA1 collision
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html, February 23, 2017.
[S17b] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, The first collision for full SHA-1,
CRYPTO 2017, Lecture Notes in Computer Science vol. 10401, pp. 570-596, 2017.
https://shattered.io/static/shattered.pdf, February 23, 2017.
[W05] X. Wang, Y. Lisa Yin, and H. Yu, Finding Collisions in the Full SHA-1, CRYPTO 2005, Lecture Notes in Computer Science vol. 3621, pp. 17-36, 2005.
https://www.iacr.org/archive/crypto2005/36210017/36210017.pdf

以上

CRYPTREC 暗号技術ガイドライン(SHA-1), CRYPTREC GL-2001-2013R1

発行日　2018 年 4 月 12 日　改定版

発行者

・〒184-8795

東京都小金井市貫井北町四丁目 2 番 1 号

国立研究開発法人情報通信研究機構

（サイバー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

（技術本部 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