SSL/TLS 暗号設定ガイドライン改訂及び鍵管理ガイドライン作成のための調査・検討

― 調査報告書 ―

2018 年 6 月

IPA 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

目次

1　件名

「SSL/TLS 暗号設定ガイドライン改訂及び鍵管理ガイドライン作成のための調査・検討」

2　背景・目的

独立行政法人情報処理推進機構（以下「IPA」という。）では、近年の情報セキュリティの基盤技術として広く利用されている暗号について、暗号技術評価プロジェクト CRYPTREC の活動を通じ、SSL (Secure Sockets Layer) /TLS (Transport Layer Security) の適切な利用促進を目的として、SSL/TLS サーバの構築者や運営者が適切なセキュリティを考慮した暗号設定ができるようにするための「SSL/TLS 暗号設定ガイドライン」([IPA2015])を 2015 年 5 月に公開した。その公開から 2 年以上が経過し、SSL/TLS を取り巻く状況の変化や SSL/TLS をサポートするアプリケーションのバージョンアップ等を反映した内容とするための改訂が必要になっている。

また、2016 年の CRYPTREC 活動において、暗号を正しく使うためには暗号鍵が適切に管理されていることが重要であるとの意見が出されたことから、暗号鍵を適切に管理するためのガイドラインとして「鍵管理ガイドライン」の作成を予定している。

本件では「SSL/TLS 暗号設定ガイドライン」の改訂および「鍵管理ガイドライン」の作成を目的とした事前調査を実施する。

3　調査概要

- SSL/TLS 暗号設定ガイドライン改訂に係る調査
  SSL/TLS 暗号設定ガイドライン改訂に係る最新状況の調査を実施する。
- SSL/TLS 暗号設定ガイドライン改訂に係る検討
  SSL/TLS 暗号設定ガイドライン改訂に係る具体的な改訂案の検討を実施する。
- 鍵管理ガイドライン作成に係る事前調査
  鍵管理ガイドライン作成に係る最新状況の事前調査を実施する。
- 調査実施報告書等の作成
  調査実施報告書等を作成する。

4　調査内容

4.1 SSL/TLS 暗号設定ガイドライン改訂に係る調査

①　SSL/TLS に関する国内外の標準化に係る調査

(1) TLS1.3 に関する調査

2018 年 1 月現在で標準化作業中の TLS1.3 について調査した。

TLS1.3 と TLS1.2 の主な差異を以下に示す。

- 暗号スイート、アルゴリズムに関する差異

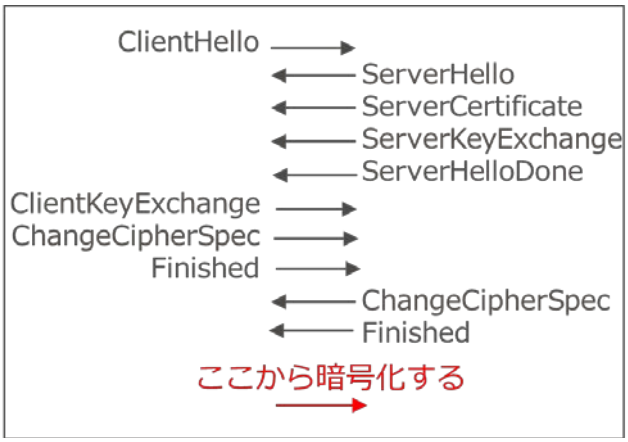
- 脆弱性のある次のアルゴリズムが削除された。
  - ✓ TripleDES、DSA、RC4、MD5、SHA-1、SHA-224、non-AEAD（CBCmode）
  - ✓ static RSA＋DH、anonymousDH
- 認証付き暗号（AEAD: Authenticated Encryption with Associated Data）のみ採用された。この結果、AES（GCM/CCM）と ChaCha20-Poly1305 のみが残った。
- ハッシュは SHA-256 以上になった。
- 鍵交換は DHE、ECDHE のみで、楕円曲線が指定された。secp256r1（必須）
- 署名は RSA、ECDSA、EdDSA に簡素化された。
  - ✓ RSA のパディングは PSS と PKCS#1 V1.5 が必須
  - ✓ ECDSA 用の楕円曲線は 3 種類：secp256r1（必須）、secp384r1、secp521r1
  - ✓ EdDSA 用の楕円曲線は 2 種類：ed25519、ed448

- ハンドシェイクの差異
  - ServerHello 以降のハンドシェイクパラメータを暗号化して保護するようにした。
  - HMAC ベースの導出関数（HKDF: The HMAC-based Extract-and-Expand Key Derivation Function）による鍵導出に変更された。
  - 性能向上のため、1-RTT（Round-Trip-Time）でハンドシェイクが完了するようにメッセージとシーケンスが改良された。
  - QUICK 等のアプリへの適用のため、0-RTT が追加された。事前に鍵共有している場合、ハンドシェイクと同時にアプリデータを送信できる。
  - ドラフト 21 まで ServerHello は TLS1.2 互換がなく、ChangeCipherSpec も不要だったが、TLS1.2 のみをサポートする中間ノードを介した接続性を向上するため、ServerHello は互換を保ち、ChangeCipherSpec を使うように変更された。

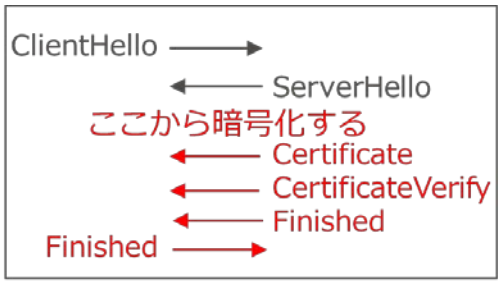
- 暗号化の契機についての差異

  下図のように、TLS1.2 ではハンドシェイクが完了してから暗号化されるのに対し、TLS1.3 ではハンドシェイクの途中で暗号化する。

  - TLS1.2



  - TLS1.3



- TLS1.3　鍵の導出（RFC5869 の活用）

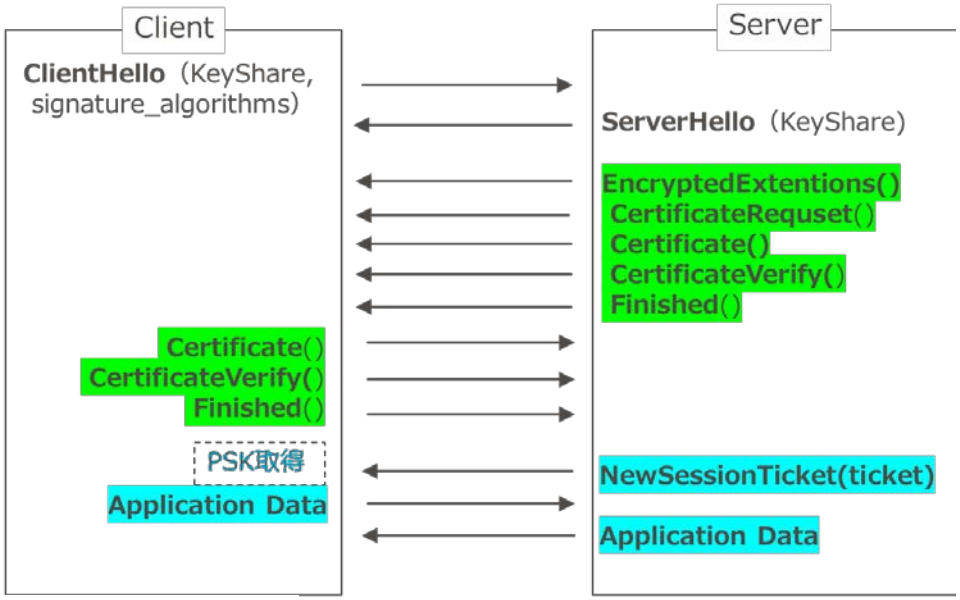
  HMAC ベースの導出関数（Extract と Expand）を使って鍵を生成する。

  TLS1.2 では、1 つのマスターキーから全ての鍵が導出されたが、TLS1.3 では、事前に共有した鍵および受信したメッセージのハッシュを使い、3 段階の導出を行う。

- TLS1.3　初期シーケンス

  クライアントは KeyShare 拡張で、交換する鍵のタイプを指定し、signature_algorithms 拡張で証明書認証の意思を伝える。サーバは CertificateRequest により、クライアント認証の意思を伝える。

  ハンドシェイク完了後、サーバは NewSessionTicket で事前共有鍵（PSK）の情報を伝える。

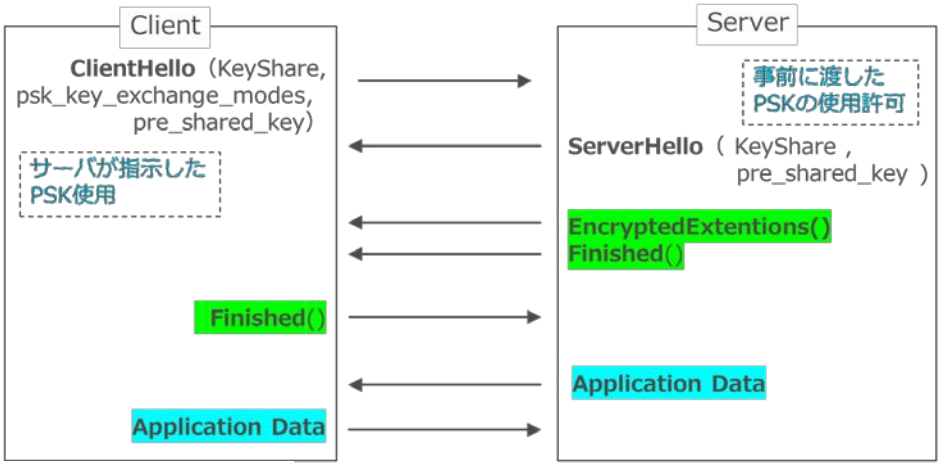


※前図の鍵の色と対応する

- TLS1.3　PSK による認証省略

  事前共有鍵（PSK）を使う場合、公開鍵証明書による認証は省略できる。

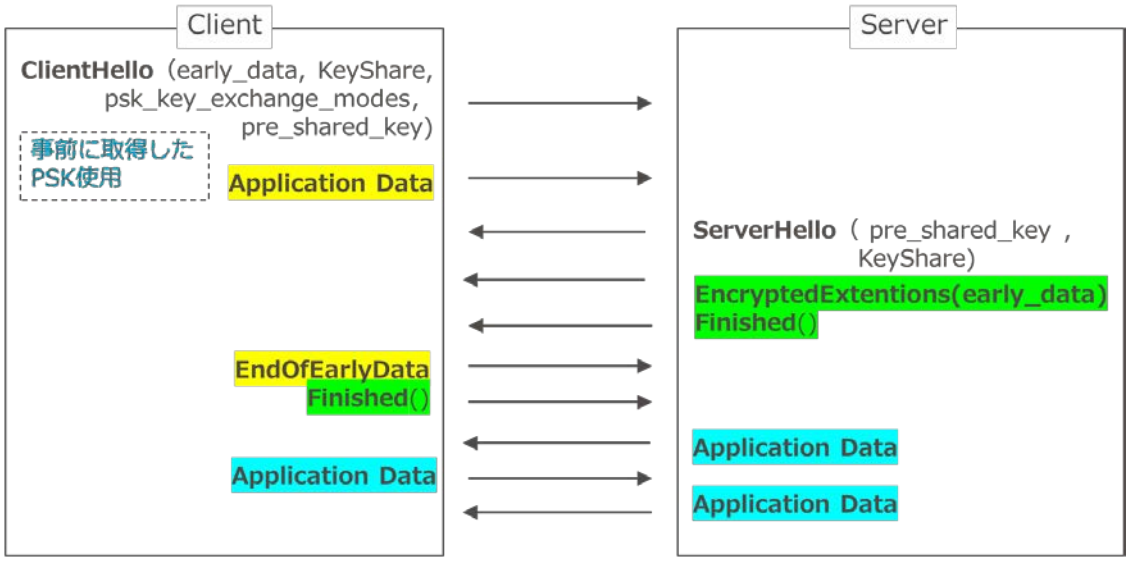
クライアントは psk_key_exchange_modes により PSK を使う意思を伝える。
サーバは pre_shared_key により使用する鍵を指定する。



※前図の鍵の色と対応する

- TLS1.3　0-RTT シーケンス

事前共有鍵（PSK）を使う場合、early_data により 0-RTT モードでの通信を要求する。サーバが認めた場合、クライアントが EndofEarlyData を送るまでの間、EarlySecret から導出された鍵（黄色の部分）を使ってアプリデータを暗号化する。



※前図の鍵の色と対応する

- 標準化の状況

下表に各ドラフトでの主な規定内容を示す。2018 年 1 月現在ドラフト 23 が最新である。

draft	主な変更
2-3	脆弱性の除去（static RSA＋DH、non-AEAD、compression）

draft	主な変更
	1-RTT mode の導入 ECC 導入（RFC4492）
4	脆弱性の除去（renegotiation） ChangeCipherSpec の廃止
6-8	脆弱性の除去（RC4、resumption、MD5、SHA-224）,弱い楕円曲線の削除 HKDF 導入 0-RTT 導入
9	鍵導出の改良 署名を RSA-PSS に変更、DSA 削除
13-14	0-RTT PSK 改良 NewSessionTicket 導入
15-18	PSK 鍵交換の見直し
19-21	RFC7250 対応、繰り返し攻撃への対処
22-	審議中（TLS1.2 互換性）

(2) SSL/TLS に関する RFC の調査

2015 年 1 月以降の“TLS“を含む RFC を検索して 32 件の調査対象を選択した。
プロトコルバージョン、サーバ証明書、暗号スイート（暗号アルゴリズム）の 3 つの観点について、利用可否や利用期限などの記述含まれるものは下表のとおりである。

RFC	Title	プロトコル	サーバ証明書	暗号スイート	内容
7465	Prohibiting RC4 Cipher Suites	×	×	○	RC4 禁止
7507	TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks	×	×	○	新暗号スイートの定義
7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)	○	×	×	SSL2、3 ネゴ禁止 TLS1.0、1.1 ネゴ否推奨
7568	Deprecating Secure Sockets Layer Version 3.0	○	×	×	SSL3 禁止
7905	ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)	×	×	○	ChaCha20-Poly1305 の暗号スイート追加

(3) 国内外の SSL/TLS 暗号設定ガイドラインの調査

暗号通信設定に関して SSL/TLS 暗号設定ガイドラインと同様の目的を持つ以下の国内外の他機関が発行する SSL/TLS に関する文献を調査した。

- エストニア（ESTONIA）　…4 文書
- ドイツ（GERMANY）　…1 文書
- 韓国（大韓民国）　…6 文書
- イギリス（英）　…6 文書　※推奨の暗号スイートの指定あり
- フランス（仏）　…5 文書　※推奨の暗号スイートの指定あり
- カナダ（加）　…5 文書　※推奨の暗号スイートの指定あり
- オーストラリア（豪）　…3 文書
- アメリカ（米）　…2 文書　※推奨の暗号スイートの指定あり

同様に、以下の業界団体が発行する SSL/TLS に関する文献について調査した。

- ETSI　…1 文書　※必須の暗号スイートの指定あり
- CABF　…1 文書
- PCIDSS　…1 文書
- OWASP　…2 文書
- OASIS　…1 文書
- HIPPA　…4 文書
- Mozilla　…1 文書　※必須の暗号スイートの指定あり

文書ごとのプロトコルバージョン、サーバ証明書、暗号スイート（暗号アルゴリズム）についての記載は下表のとおりである。

なお、個々の暗号スイートを含む詳細は、「添付資料 1 SSL/TLS 暗号設定ガイドラインの調査」を参照。

文書名	規定分類	規定内容	
エストニア共和国 **ISKE カタログ Ver 8.03** 発行者 Riigi infosüsteemi Amet（国家情報システム局） 発効日：2017 年 6 月 対象者：電子政府に関連する政府組織	SSL/TLS	TLS / SSL 使用のパラメータ化	
	暗号装置の追加要件	MD2、MD4、MD5 の禁止 RIPEMD-160、SHA-1 の禁止 SHA-2 ファミリ、RIPEMD より長いハッシュを推奨 10 年以上使用　　RSA：1536 ビット以上 15 年以上使用　　RSA：4096 ビット以上	
ドイツ連邦共和国 **IT Baseline Protection Manual** 発行者：BSI（英語名：Federal Office for Information Security） 発効日：2013 年 9 月 対象者：電子政府に関連する政府組織、企業に対しても適用が推奨	SSL	－	TLS 1.0 以上または SSL 3.0 以上を使用する必要があり SSL 2.x は、中間者攻撃に対する保護機能を提供していないため、使用しない
	鍵長	すべき それ以外	少なくとも 100 ビット長 ECB モードで暗号化すべきではない。CBC または CFB モードを使用する必要あり
	ブラウザ	－	HTTPS プロトコルを使用して暗号化された接続が使用されていることを確認する必要がある。
	暗号アルゴリズム	－	AES-128、AES-192、AES-256、SERPENT が含まれ、キー長は少なくとも 128 ビット RSA または楕円曲線に基づく暗号化手順
大韓民国 **ICT Practices in korea** 発行者：Ministry of Science and ICT（科学技術情報通信部） 発効日：2014/12/4 対象者：不明（国民向けと想定）	公共部門に適用される開発枠組みの基準として電子政府標準フレームワークがあるが、暗号関連の技術情報は非公開		

<table>
<tr><th>文書名</th><th>規定分類</th><th>規定内容</th></tr>
<tr><td rowspan="6">グレートブリテン及び北アイルランド連合王国
Using TLS to protect data
発行者：NCSC
発効日：2016/10/7
対象者：英国政府、地方自治体、国家インフラ（クラウドサービスベンダを指していると思われる）、サプライヤー</td><td>鍵長</td><td>2048 ビット</td></tr>
<tr><td>署名アルゴリズム</td><td>SHA256</td></tr>
<tr><td>SSL</td><td>SSLv3 の禁止</td></tr>
<tr><td>TLS</td><td>TLS 1.0 の非推奨
TLS 1.1、1.2 の推奨（1.1 は必要最低限に限る）</td></tr>
<tr><td>暗号スイート</td><td>以下の暗号スイートは非推奨<table><tr><td>AEAD の推奨</td></tr><tr><td>ADH は認証を未提供</td></tr><tr><td>NULL 暗号は暗号化を未提供</td></tr><tr><td>Export 暗号スイートは安全ではない</td></tr><tr><td>40、56 ビットの暗号スイートは簡単に破られる</td></tr><tr><td>RC4 は安全ではない</td></tr><tr><td>TripleDES は弱い</td></tr></table></td></tr>
<tr><td>18 個の暗号スイートを推奨</td></tr>
<tr><td colspan="2">TLS 暗号化プロファイル（推奨値）
TLS のスイート B プロファイルの要約<table><tr><td>Protocol</td><td>TLS v1.2</td></tr><tr><td>Encryption</td><td>AES with 128-bit key in GCM mode</td></tr><tr><td>Pseudo-random function</td><td>TLS PRF (with SHA-256)</td></tr><tr><td>Authentication</td><td>ECDSA-256 with SHA-256 on P-256 curve</td></tr><tr><td>Key exchange</td><td>ECDH using P-256 curve</td></tr></table></td></tr>
</table>

文書名	規定分類	規定内容	
		Algorithm type	Description
		TLS の基礎プロファイル	
		Protocol	TLS v1.2
		Encryption	AES with 128-bit key in CBC mode
		Pseudo-random function	TLS PRF (with SHA-256)
		Authentication	X.509 certificates with RSA signatures (2048 bits) and SHA-256
		Key exchange	DH Group 14 (2048-bit MODP Group)
		Integrity	SHA-256
		Algorithm type	Description
フランス共和国 **Security Recommendations for TLS** 発行者：ANSSI （国家情報通信システムセキュリティ庁） 発効日：FR Version 1.1: 2016/8/19 EN Version 1.1: 2017/1/24 対象者：あらゆる規模の組織の管理者、ソリューションの開発者、関連するすべてのユーザ 【注意】 Rx, Rx-, Rx-- 標記：「Rx：推奨事項（x は番号）」、「Rx-：推奨事項が不可能な場合」、「Rx--：最低の信頼レベル」	SSL/TLS	R3	TLS 1.2 のみを使用してください
		R4	SSL v2 の使用禁止
		R3-	TLS 1.2 を優先し、TLS 1.1 と TLS 1.0 は容認
		R4	SSL v2 の使用禁止
		R3--	TLS 1.2 を優先し、TLS 1.1、TLS 1.0、および SSLv3 は容認
		R4	SSL v2 の使用禁止
	鍵交換	R5	鍵交換中にサーバを認証
		R6	常に PFS 対応の鍵交換
		R6-	PFS 対応鍵交換を優先
		R7	ECDHE 鍵交換を実行
		R7-	DHE 鍵交換を実行

文書名	規定分類	規定内容	
	アルゴリズム	R8	AES 暗号化を使用
		R8-	Camellia または ARIA 暗号化を使用
		R8--	AES が望ましく、リフレッシュメントで TripleDES を許容する
	認証コード	R9	SHA-2 で HMAC を構築
		R9-	SHA-2 で HMAC を優先し、SHA-1 で HMAC を容認
	暗号化モード	R10	強力な暗号化モードを使用
		R10-	encrypt_then_mac なしで CBC モードを使用
		推奨	推奨暗号スイートは以下の 28 個
			ECDSA key を含む 6 個
			RSA key を含む 4 個
			Camellia を含む 8 個
			ARIA を含む 8 個
			PSK を含む 2 個
		緩和	緩和暗号スイートは以下の 26 個
			ECC がサポートされていない場合に許容される 6 個
			DH がサポートされていない場合に許容される 6 個
			パスワード認証が許容されている場合の 2 個
			TLS 1.0 で許容されている 4 個
			TLS 1.0 でかろうじて許容されている 8 個
	基本設定	R21	SHA-2 で署名
		R22	3 年の期間有効な証明書を所持

<table>
<tr><th>文書名</th><th>規定分類</th><th colspan="2">規定内容</th></tr>
<tr><td rowspan="8"></td><td></td><td>R23</td><td>十分な大きさのキーを使用</td></tr>
<tr><td rowspan="7">拡張設定</td><td>R24</td><td>適切な KeyUsage</td></tr>
<tr><td>R25</td><td>適切な ExtendedKeyUsage</td></tr>
<tr><td>R26</td><td>適切な（サーバ側の）SubjectAlternativeName を指定</td></tr>
<tr><td>R27</td><td>各証明書を 1 つの TLS 終端ポイントだけ保持</td></tr>
<tr><td>R28</td><td>CA によって定義された SKI に対応する AKI を負担</td></tr>
<tr><td>R29</td><td>失効情報を提供</td></tr>
<tr><td rowspan="4">カナダ
Guidance on Securely Configuring Network Protocols
発行者：CSE（カナダ政府の通信セキュリティ機関）
発効日：2016/8/2
対象者：不明 (政府およびベンダ)</td><td>Public Key Infrastructure</td><td colspan="2">SHA-1 を公開鍵証明書の電子署名の生成または検証に使用すべきではない
NIST SP 800-57 パート 3 Rev1 Section 2 にしたがうことを推奨</td></tr>
<tr><td>SSL/TLS</td><td colspan="2">TLS 1.2 の使用を推奨
（他のバージョンの TLS と全ての SSL の使用は非推奨）
NIST SP 800-52 Rev1 の section 3.9 および 4.9 にしたがうことを推奨</td></tr>
<tr><td>TLS Cipher Suites</td><td colspan="2">ITSP.40.111 で提供される暗号ガイダンスを満たす TLS 暗号スイート 41 個</td></tr>
<tr><td>SSH</td><td colspan="2">CBC モードは SSH で使用しない
以下の暗号アルゴリズムを推奨
aes128-ctr (RFC 4344 [34])
aes192-ctr (RFC 4344 [34])
aes256-ctr (RFC 4344 [34])
3des-ctr (RFC 4344 [34])
cast128-ctr (RFC 4344 [34])</td></tr>
</table>

文書名	規定分類	規定内容	
			AEAD_AES_128_GCM (RFC 5647 [35])
			AEAD_AES_256_GCM (RFC 5647 [35])
オーストラリア連邦 **2017 Australian Government Information Security Manual (Controls)** 発行者：ASD (オーストラリア信号局) 発効日：2017/11/23 更新 対象者：不明 (政府およびベンダ)	暗号アルゴリズム		承認された非対称/公開鍵アルゴリズムは
		高優先度	ECDH ECDSA
		低優先度	DH DSA
			RSA
			承認されたハッシュアルゴリズム SHA-224 SHA-256 SHA-384 SHA-512
			承認された対称暗号化アルゴリズム AES 128 AES 192 AES 256 TripleDES
	デジタル署名	すべき	DSA 2048 ビット以上
		必須	DSA 1024 ビット以上
	スイート B	機密	AES 256 SHA-384

文書名	規定分類	規定内容	
			NIST P‑384 NIST P‑384
		機密 (やや下)	AES 128 SHA-256 NIST P‑256 NIST P‑256
		高機密	CNSSAM recommendation AES 256 bit key CNSSAM recommendation SHA-384 CNSSAM recommendation NIST P‑384 or RSA 3072-bit or larger CNSSAM recommendation DH 3072-bit or larger or NIST P-384 or RSA 3072-bit or larger.

文書名	規定分類	規定内容
アメリカ合衆国 **SP 800-52 Rev.1** 発行者：NIST 発効日：2014 年 4 月 対象者：不明 (政府および ベンダ)	プロトコルバージョン	TLS 1.1 をサポートするよう構成し、TLS 1.2 をサポートするよう構成すべき 政府機関は、2015 年 1 月 1 日までに TLS 1.2 をサポートする移行計画を策定する予定です。
	TLS Cipher Suite	以下の暗号スイート 62 個 Pre-shared Key を含む暗号スイート 20 個 RSA を含む暗号スイート 6 個 ECDSA を含む暗号スイート 3 個 DSA を含む暗号スイート 3 個 DH を含む暗号スイート 3 個 ECDH を含む暗号スイート 3 個

<table>
<tr><th>文書名</th><th>規定分類</th><th colspan="4">規定内容</th></tr>
<tr><td rowspan="5"></td><td rowspan="5"></td><td rowspan="5"></td><td colspan="3">TLS 1.2 向け追加　RSA を含む暗号スイート 8 個</td></tr>
<tr><td colspan="3">TLS 1.2 向け追加　ECDSA を含む暗号スイート 4 個</td></tr>
<tr><td colspan="3">TLS 1.2 向け追加　DSA を含む暗号スイート 4 個</td></tr>
<tr><td colspan="3">TLS 1.2 向け追加　DH を含む暗号スイート 4 個</td></tr>
<tr><td colspan="3">TLS 1.2 向け追加　ECDH を含む暗号スイート 4 個</td></tr>
<tr><td>アメリカ合衆国
SP 800-131A Rev. 1
発行者：NIST
発効日：2015 年 11 月
対象者：不明 (政府および ベンダ)</td><td>デジタル署名</td><td colspan="4">Table 2: Approval Status of Algorithms Used for Digital Signature Generation and Verification
<table><tr><th>Digital Signature Process</th><th colspan="2">Use</th></tr><tr><td rowspan="2">Digital Signature Generation</td><td>< 112 bits of security strength:
DSA: len(p) < 2048 OR
len(q) < 224
RSA: len(n) < 2048
ECDSA: len(n) < 224</td><td>Disallowed</td></tr><tr><td>≥ 112 bits of security strength:
DSA: len(p) ≥ 2048 AND
len(q) ≥ 224
RSA: len(n) ≥ 2048
ECDSA: len(n) ≥ 224</td><td>Acceptable</td></tr><tr><td>Digital Signature Verification</td><td>< 112 bits of security strength:
DSA [*3]: ((512 ≤ len(p) < 2048) OR
(160 ≤ len(q) < 224))
RSA: 1024 ≤ len(n) < 2048
ECDSA: 160 ≤ len(n) < 224</td><td>Legacy-use</td></tr></table></td></tr>
</table>

<table>
<tr><th>文書名</th><th>規定分類</th><th>規定内容</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>≥ 112 bits of security strength:
DSA: len(p) ≥ 2048 AND
len(q) ≥ 224
RSA: len(n) ≥ 2048
ECDSA: len(n) ≥ 224</td><td>Acceptable</td></tr>
</table>
[*3]：The lower bounds for len(p) and len(q) are those that were specified in [FIPS 186-2].
len（p）と len（q）の下限は、[FIPS 186-2]で指定されたものです。
</td></tr>
<tr><td></td><td>ハッシュ関数</td><td>
Table 9: Approval Status of Hash Functions
<table>
<tr><td>Hash Function</td><td colspan="2">Use</td></tr>
<tr><td rowspan="3">SHA-1</td><td>Digital signature generation</td><td>Disallowed
except where specifically allowed by NIST protocol-specific guidance.</td></tr>
<tr><td>Digital signature verification</td><td>Legacy-use</td></tr>
<tr><td>Non-digital signature applications</td><td>Acceptable</td></tr>
<tr><td>SHA-2 family
(SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)</td><td colspan="2">Acceptable for all hash function applications</td></tr>
<tr><td>SHA-3 family</td><td colspan="2">Acceptable for all hash function applications</td></tr>
</table>
</td></tr>
</table>

文書名	規定分類	規定内容
		(SHA3-224, SHA3-256, SHA3-384, and SHA3-512)

文書名	規定分類	規定内容
ETSI 欧州電気通信標準化協会 **ETSI TS 118 103 V2.4.1 (2016-09)** **oneM2M; Security solutions (oneM2M TS-0003 version 2.4.1 Release 2)** 発行者：ETSI 発効日：2016 年 9 月 対象者：不明 (運用者、開発者)	TLS	TLS v1.2 を使用しなければならない
	暗号スイート	TLS-PSK-Based Security Frameworks TLS 実装：TLS_PSK_WITH_AES_128_CBC_SHA256 DTLS 実装：TLS_PSK_WITH_AES_128_CCM_8
		Certificate-Based Security Frameworks TLS 実装：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 DTLS 実装：TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
		【参考】：赤字は、全ての国に記載なし 青字は、米（P451）、英（P87）、仏（R157）、加（Q273）に記載あり
ETSI 欧州電気通信標準化協会 **ETSI TS 133 320 V9.7.0 (2013-02)** **Universal Mobile Telecommunications System (UMTS); LTE; Security of Home Node B(HNB)/Home evolved Node B(HeNB)** 発行者：ETSI 発効日：2013 年 2 月 対象者：不明 (運用者、開発者)	TLS	SSL 3.0 は使用しないでください TLS 1.1 はサポートされなければならない TLS 1.2 はサポートする必要あり
	暗号スイート	RSA_WITH_AES_128_CBC_SHA のサポートは必須 TLS 1.2 に列挙された TLS 暗号スイートのみが使用される RC4 の暗号スイートは使用してはならない RSA_WITH_RC4_128_SHA のサポートは必須ではない

文書名	規定分類	規定内容
CABF CA/Browser Forum	証明書の管理、各種手続き、監査等について規定しており、SSL/TLS についての規定は見つからない。	
PCI DSS （PCI Security Standards Council）	SSL/TLS	SSL および初期の TLS はセキュリティ制御としてこれらの要件を満たすために使用すべきではありません。
OWASP （Open Web Application Security Project） **SECURE WEB APPLICATION FRAMEWORK MANIFESTO** 発行日：2010 年 1 月 10 日 対象者：アプリケーションのセキュリティを向上させることに関心を持つ人	TLS/SSL	実装に関する項があるが「TLS / SSL の要件の網羅的なセットを提供することは、このマニフェストの対象外です」 「TLS / SSL の実装のための TLS 保護のチートシートに従ってください」 などの記載があり、チートシートの参照となる
OWASP （Open Web Application Security Project） **Transport Layer Protection Cheatsheet** 発行日 2017 年 11 月 3 日 対象者 アプリケーションのセキュリティを向上させることに関心を持つ人	TLS/SSL	推奨するバージョン等を明確に規定していない
	暗号スイート	最新の推奨事項を使用 レガシーブラウザを無効にしないための最善の妥協策としての例 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA DES-CBC3-SHA 暗号化されない暗号スイートの無効化 IDEA 暗号スイートの無効化
	鍵長	十分に大きいサイズを使用 128 ビット未満の鍵長の無効化 DHE 暗号は 2048 ビット以上 ECDHE 暗号の 256 ビット以下は非推奨

文書名	規定分類	規定内容
	暗号アルゴリズム	推奨暗号のホワイトリストを取得してポリシー設定する Diffie-Hellman 鍵交換のサポート ECDHE よりも DHE を好む（CPU 使用率の問題） RFC 7027 の TLS、または Edwards Curves で定義されている Brainpool Curves の使用 RSA キーを使用 暗号サイズに関係なく、CBC より GCM を優先 AEAD の使用 ダイジェストには SHA1 以上 TripleDES の無効化 MD5 の無効化 RC4 の無効化
OASIS	SSL/TLS に関するドキュメントは見つからない	
HIPPA （Health Insurance Portability and Accountability Act） **Security Rule Guidance Material** 発行日：不明 対象者：不明	暗号	暗号化することは規定されているが、技術的要件は未記載 ここで、NIST SP 800-53 とのマッピングが示されている
HIPPA （Health Insurance Portability and Accountability Act） **SP 800-66 Rev. 1** 健康保険の携帯性と説明責任に関する法律（HIPAA）のセキュリティルールを実装するための入門資料	暗号	TLS 暗号は NIST SP 800-52 をリンクしている

文書名	規定分類	規定内容	
発行日：2008 年 10 月 対象者：不明			
Mozilla **Security/Server Side TLS** 発行日：2018 年 1 月 17（最終更新日） 対象者：サーバで TLS を構築する運用者	暗号スイート	推奨	10 個の暗号スイート
		互換性維持（既定）	30 個の暗号スイート
		下位互換性	56 個の暗号スイート
	プロトコルバージョン	推奨	TLSv1.2
		互換性維持（既定）	TLSv1.2, TLSv1.1, TLSv1
		下位互換性	TLSv1.2, TLSv1.1, TLSv1, SSLv3
	楕円曲線	推奨	prime256v1, secp384r1, secp521r1
		互換性維持（既定）	prime256v1, secp384r1, secp521r1
		下位互換性	prime256v1, secp384r1, secp521r1
	証明書の種類	推奨	ECDSA
		互換性維持（既定）	RSA
		下位互換性	RSA
	証明書の楕円曲線	推奨	prime256v1, secp384r1, secp521r1
		互換性維持（既定）	'None
		下位互換性	'None
	証明書の署名	推奨	sha256WithRSAEncryption, ecdsa-with-SHA256, ecdsa-with-SHA384, ecdsa-with-SHA512
		互換性維持（既定）	sha256WithRSAEncryption
		下位互換性	sha256WithRSAEncryption
	RSA の鍵長	推奨	2048 (if not ecdsa)

文書名	規定分類	規定内容	
		互換性維持（既定）	2048
		下位互換性	2048
	DH の鍵長	推奨	2048 (if not ecdsa)
		互換性維持（既定）	2048
		下位互換性	1024
	ECDH の鍵長	推奨	256
		互換性維持（既定）	256
		下位互換性	256

（4）CABF および主要携帯電話会社での動向調査

・ CABF の調査

CABF での 2015 年 1 月以降の動向について以下の条件で調査をした。

・ 調査対象（文書）

Baseline Requirements（BR）

・ 調査対象バージョン（期間）

BR1.2.4（2015/2/18）～BR1.5.5（2017/12/21）

調査結果は、以下のとおりである。

i. SHA-1 を利用したサーバ証明書の取り扱いについて

調査対象期間で、SHA-1 を利用したサーバ証明書の取り扱い、利用期間等についての変更は無かった。

・ （参考）バージョン 1.5.5　2017/12./21

Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017. This Section 7.1.3 does not apply to Root CA or CA cross certificates. CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate. Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.

ii. 証明書の有効期間について

調査対象期間で、証明書の有効期間について、次の変更があった。

・ バージョン 1.4.4　2017/3/17

- 2017-04-22（Compliance date）
  Reuse of validation information limited to 825 days
- 2018-03-01（Compliance date）
  Certificates issued MUST have a Validity Period no greater than 825 days

・ （参考）バージョン 1　2011/11/22

- Certificates issued after the Effective Date MUST have a Validity Period no greater than 60 months.
- Certificates issued after 1 April 2015 MUST have a Validity Period no greater than 39 months.

iii. 使用できる鍵長について

調査対象期間で、使用できる鍵長についての変更はなかった。

- （参考）バージョン 1.5.5　2017/12./21
  - ルート CA 証明書

ダイジェスト アルゴリズム	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048
ECC	NIST P-256, P-384, or P-521
DSA	L= 2048, N= 224 or L= 2048, N= 256,

  - 下位 CA 証明書

    ルート CA 証明書と同じ
  - 加入者証明書

    ルート CA 証明書と同じ

- 主要携帯電話会社の 2015 年 1 月以降の動向

  主要携帯会社での SHA-1 を利用したサーバ証明書等の扱い、利用期間等について調査した。調査結果は、以下のとおりである。

会社	発表日	タイトル	記載内容
NTT ドコモ	2015/7/15	サーバ証明書の切り替えによるドコモ ケータイへの影響について	暗号化通信で利用されているサーバ証明書の切り替えにより、今後、ドコモ ケータイの一部機種でインターネット接続する際、暗号化通信を利用している一部サイトの利用ができなくなる可能性があります。 https://www.nttdocomo.co.jp/info/notice/pages/150715_00.html
NTT ドコモ	2017/7/3	ドコモ提供 Android アプリの一部サービス提供条件の変更について	「SHA-2」方式に対応していない Android™ 4.2 以下機種、もしくは一部の Android™ 4.3～G 型番以前機種をご利用のお客さまに対しては、一部ドコモアプリでサポート対象の変更を実施いたします。 https://www.nttdocomo.co.jp/info/notice/pages/170703_00.html
KDDI	2015/7/15	<重要なお知らせ> au ケータイをご利用のお客さまへ、サーバ証明書切り替えによる影響について	暗号化通信で使用されるサーバ証明書について、新しいサーバ証明書へと順次切り替わります。これを受けて、KDDI では対象となる au ケータイで順次ケータイアップデートを実施してきましたが、2008 年 12 月以前に発売された一部の au ケータイで、今後、新しいサーバ証明書を使用しているサイトの表示ができなくなる可能性があります 。 http://www.kddi.com/important-news/20150715/
KDDI	－	よくある質問 「<重要なお知らせ> ご利用の au 携帯電話の、新しいサーバ証明書（SHA-2）への対応について」が届きました。どうすればよいですか。	2017 年 1 月 1 日より、サーバ証明書（SHA-1）がご利用いただけなくなります。 SHA-2 を利用するために自動ケータイアップデートを実施いたしますので、2016 年 12 月 2 日～12 月 7 日は au ケータイの電源を「ON」の状態にしてください。 http://bizcs.kddi.com/app/answers/detail/a_id/9075/~/%E3%80%8C%26lt%3B%E9%87%8D%E8%A6%81%E3%81%AA%E3%81%8A%E7%9F%A5%E3%82%89%E3%81%9B%26gt%3B
SoftBank	2015/7/15	SoftBank 3G（携帯電話）をご利用のお客さまへ サーバ証明書切り替えによる影響のご案内	インターネット上の暗号化通信で利用されているサーバ証明書の切り替えにより、今後、SoftBank 3G（携帯電話）の一部機種でインターネット接続する際、暗号化通信を利用している一部ウェブページの利用ができなくなる可能性があります https://www.softbank.jp/mobile/info/personal/news/support/20150715a/

(5) 主要ブラウザでの SSL/TLS に関するサポート状況の調査

以下の方法により、主要ブラウザでの SSL/TLS に関するサポート状況を調査した。

- 調査方法

  調査方法は、以下のとおりである。

  ✓ 原則として公式ベンダサイト記載の内容で調査する

  ✓ 公式サイトに記載がなければ他サイトから情報を収集する

- 公式ベンダサイト

  公式ベンダサイトは以下とする。

ブラウザ	概要	公式サイト
Chrome	chromium から確認可能	http://www.chromium.org/
		https://developer.chrome.com/home
		https://developers.google.com/web/
		https://blog.chromium.org/
		https://bugs.chromium.org/
		https://groups.google.com/a/chromium.org
		https://security.googleblog.com
		https://support.google.com/
Firefox	Mozilla のセキュリティブログ等で確認可能	https://blog.mozilla.org/security/
		https://www.mozilla.org/
		https://www.mozilla.jp
		https://developer.mozilla.org
		https://wiki.mozilla.org/
		https://kb.mozillazine.org
		https://support.mozilla.org
		https://groups.google.com/forum/#!msg/mozilla.dev.security.policy
Safari	iOS での設定を調査する	https://www.apple.com/
		https://developer.apple.com/
		https://support.apple.com/
IE	公式サイトで確認可能	https://docs.microsoft.com/
		https://blogs.windows.com
		https://technet.microsoft.com
		https://blogs.msdn.microsoft.com
		https://support.microsoft.com/

ブラウザ	概要	公式サイト
		https://developer.microsoft.com
		http://download.microsoft.com
		https://msdn.microsoft.com
		https://blogs.technet.microsoft.com/
		https://social.technet.microsoft.com
		https://www.microsoft.com
Edge	公式サイトで確認可能	(IE と同じ)

- 調査項目

  調査項目は、以下のとおりである。

  ✓ サポートするプロトコルバージョン

  ✓ サーバ証明書

  ✓ 暗号スイート

  ✓ 利用期間（例：SHA-1 サーバ証明書の有効期限）

  ✓ 表示方法の変更（例：アドレスバーの鍵アイコンの表示）

  ✓ EV-SSL 証明書の取り扱い方法

  ✓ EV-SSL 証明書でグリーンバー表示にならない場合

- 信頼度の定義

  調査結果として取得した情報に信頼度をつける。信頼度の定義は、以下のとおりである。

  ✓ 信頼度：高＝公式サイトに明示的に記述がある

  ✓ 信頼度：中＝複数の公式サイトの記述から導き出される

  ✓ 信頼度：低＝公式以外のサイトの記述

- 調査結果（例）

  調査結果の例として、Google Chrome の例を以下に示す。

  なお、詳細な調査結果は、「添付資料 2 ブラウザ調査」を参照。

・ Google Chrome

項目	調査結果	記載内容	信頼度	URL
プロトコルバージョン	TLS1.0, TLS1.1, TLS1.2 設定方法： UI は用意されていない。 コマンドラインオプションから、バージョンの指定(Max, Min)はできるようだが推奨していない。	SSLv3 はサポートされない [引用：SSLv3 is no longer supported in Chrome.]	高	http://www.chromium.org/Home/chromium-security/education/tls
		Chrome 39 からデフォルトで SSLv3 は使用不可 [引用：In Chrome 39 (the next version), fallback to SSLv3 will be disabled by default.]	中	https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/Vnhy9aKM_l4
		Chrome 40 から SSLv3 を完全に使用できないようにする [引用：In Chrome 40, we plan on disabling SSLv3 completely, although we are keeping an eye on compatibility issues that may arise.]	中	
		Chrome 44 から SSLv3 のサポート停止 [引用：SSLv3 support will be entirely removed from Chrome in version 44 (around July 2015) after which the setting "ssl3" will be ignored in favor of the then-current default.)	中	https://bugs.chromium.org/p/chromium/issues/detail?id=436391
		SSLVersionMax ポリシーに「tls1.2」が指定できる [引用：(SSLVersionMax ポリシーの項目) it may be set to one of the following values: "tls1.2" or "tls1.3". When set, Google Chrome will not use SSL/TLS versions greater than the specified version. An unrecognized value will be ignored.]	高	http://www.chromium.org/administrators/policy-list-3

項目	調査結果	記載内容	信頼度	URL
		指定しない場合は SSL の最大のバージョンを使用 [引用：If this policy is not configured then Google Chrome uses the default maximum version.]	高	
		Chrome は SSL/TLS オプションを設定する UI を意図的に提供していない。コマンドラインオプションからできるが、その使用は推奨しない。（※） [引用：Chrom[e/ium] intentionally does not provide UI to configure SSL/TLS options (we previously did). There are a set of command-line options for testing, but those are not 'supported', in that we don't recommend users use these (invariably, when people use these, it's to weaken security, unfortunately).]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=391955
		コマンドラインオプション一覧に--ssl-version-max/min がある。 [引用：List of Chromium Command Line Switches] [引用：--ssl-version-max … Specifies the maximum SSL/TLS version ("tls1", "tls1.1", "tls1.2", or "tls1.3"). --ssl-version-min … Specifies the minimum SSL/TLS version ("tls1", "tls1.1", "tls1.2", or "tls1.3").]	低	https://peter.sh/experiments/chromium-command-line-switches/
暗号スイート	追加・削除：不可 優先度変更：不可	SSL/TLS の暗号スイートの優先度を変更するインターフェースがない [引用：there is no interface today to prioritize individual SSL/TLS cipher suites.]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=58833

項目	調査結果	記載内容	信頼度	URL
	設定方法： 追加削除、優先度変更のインターフェースはない。 起動時オプションで禁止できるが、上記（※）よりコマンドラインオプションは推奨されていない	SSL/TLS の暗号スイートの使用・不使用を変更するインターフェースがない [引用：Currently, Chrome does not offer any interface for enabling or disabling individual SSL/TLS cipher suites, either through the UI or through the administrative policies.]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=58831
		特定のアルゴリズムを禁止 アプリケーション起動時のオプションで、ブラックリストを Hex 表記で記述する。 "C:¥Program Files¥Google¥Chrome¥Application¥chrome.exe" --cipher-suite-blacklist=0xc007,0xc011,0x0005,0x0004	低	http://d.hatena.ne.jp/tosi29/20140720/1405854774
		Chrome 6 から Windows で設定した暗号スイート設定が反映されなくなった [引用：In Chrome 5 and earlier, this could be managed on Windows by configuring the Schannel cipher suites (http://msdn.microsoft.com/en-us/library/bb870930(VS.85).aspx). Since Chrome 6, which saw the switch to NSS as the default SSL library, this is no longer possible, unless either "--use-system-ssl" is specified on the command-line (an unsupported option), or the server requests client certificate authentication (which will cause Chrome to fall back to Schannel).]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=58831

項目	調査結果	記載内容	信頼度	URL
		Chrome 5 までは CryptoAPI/CNG (Windows の API) を使用していて、6 で NSS に移行した [引用：Windows 版の Google Chrome の暗号モジュールが CryptoAPI/CNG から Mozilla の NSS に変更になったそうで、そのおかげで Camellia を使った Cipher Suites にも対応するようになったそうです。]	低	http://blog.livedoor.jp/kurushima/archives/1489528.html

（6）RC4、TripleDES、CBC、SHA-1 に関するガイドラインの調査

以下の暗号アルゴリズムの利用可否や利用期限などについて、2015 年 1 月以降に国内外の他機関（例：NIST）が発行・更新したガイドライン等があるかを調査した。

調査結果は、下表のとおりである。

- 暗号アルゴリズム（暗号化） RC4
- 暗号アルゴリズム（暗号化）TripleDES
- 暗号アルゴリズム（暗号利用モード） CBC
- 暗号アルゴリズム（ハッシュ関数） SHA-1

・ RC4

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
RFC7465	Prohibiting RC4 Cipher Suites	February 2015	－	Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections. This pplies to all TLS versions.	
IMPAVA Hacker Intelligence Initiative	Attacking SSL when using RC4	March 2015	－	We show how this vulnerability can be used to mount several partial plaintext recovery attacks on SSL-protected data when RC4 is the cipher of choice, recovering part of secrets such as session cookies, passwords, and credit card numbers.	https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
SSL Labs	SSL and TLS Deployment Best Practices	31 March 2017（最終更新日）	－	·Remove the recommendation to use RC4 to mitigate the BEAST attack server-side. ·Recommend that RC4 is disabled.	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
OWASP	Transport Layer Protection Cheatsheet	2017/11/3	－	・Disable RC4 cipher suites (see [8], [9]) [8]：RFC7465 [9]：On the Security of RC4 in TLS and WPA http://www.isg.rhul.ac.uk/tls/	https://www.owasp.org/?title=Transport_Layer_Protection_Cheat_Sheet

・ TripleDES

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
NIST Special Publication 800-131A Revision 1	Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	November 2015	2 Encryption and Decryption Using Block Cipher Algorithms	Three-key TDEA Encryption and Decryption Acceptable AES and three-key TDEA encryption and decryption: The use of AES-128, AES-192, AES-256 and three-key TDEA is acceptable.	
NIST Computer Security Resource Center News	Update to Current Use and Deprecation of TDEA	July 11, 2017	―	NIST urges all users of TDEA to migrate to AES as soon as possible. NIST is developing a draft deprecation timeline for the 3-key variant of TDEA including a sunset date.	https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA
NIST Computer Security Resource Center Projects	Block Cipher Techniques	November 29, 2017		Revision 2 lowers the 3TDEA limit to 2^{20} 64-bit data blocks per key bundle and disallows the use of TDEA for applying cryptographic protection to new information. These modifications were made in accordance with the announcement by NIST to update its guidance on the current use of TDEA.	
ITL	ITL BULLETIN FOR NOVEMBER 2017 GUIDANCE ON TDEA	NOVEMBER 2017	―	NIST is developing a draft deprecation timeline for the 3-key variant of TDEA, including a sunset date, so while this Recommendation allows the	https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
	BLOCK CIPHERS			continued use of TDEA under certain conditions, NIST urges all users of TDEA to migrate to the more secure and cost-efficient AES as soon as possible.	bulletin/itlbul2017-11.pdf
NIST Special Publication 800-67 Revision 2	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	November 2017	3.4 Usage Guidance	The security of TDEA is affected by the number of blocks processed with one key bundle. One key bundle shall not be used to apply cryptographic protection (e.g., encrypt) more than 2^{20} 64-bit data blocks.	Revision 1 では、 The security of TDEA is affected by the number of blocks processed with one key bundle. One key bundle shall not be used to process more than 2^{32} 64-bit data blocks when the keys conform to Keying Option 1 (see Section 3.2).

・ CBC

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
RFC 7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)	May 2015	4.2. Recommended Cipher Suites	Given the foregoing considerations, implementation and deployment of the following cipher suites is RECOMMENDED: ・TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ・TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ・TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ・TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 These cipher suites are supported only in TLS 1.2 because they are authenticated encryption (AEAD) algorithms [RFC5116].	4.2.では、推奨の暗号スイートが規定されている
			4.2.1. Implementation Details	To maximize interoperability, RFC 5246 implementation of the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite, which issignificantly weaker than the cipher suites recommended here. (The GCM mode does not suffer from the same weakness, caused by the order of MAC-then-Encrypt in TLS[Krawczyk2001], since it uses an AEAD mode of operation.) Implementers should consider the interoperability gain	4.2.1 では、相互運用性を重視する場合は、CBC を含む暗号スイートを含まなければならないとある

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
				against the loss in security when deploying the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite. Other application protocols specify other cipher suites as mandatory to implement (MTI).	
The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-22	The Transport Layer Security (TLS) Protocol Version 1.3	November 29, 2017	9.1. Mandatory-to-Implement Cipher Suites	In the absence of an application profile standard specifying otherwise, a TLS-compliant application MUST implement the TLS_AES_128_GCM_SHA256 [GCM] cipher suite and SHOULD implement the TLS_AES_256_GCM_SHA384 [GCM] and TLS_CHACHA20_POLY1305_SHA256 [RFC7539] cipher suites. (see Appendix B.4)	実装必須暗号スイートにCBCが含まれていない

・ SHA-1

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
NIST Special Publication 800-131A Revision 1	Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	November 2015	9 Hash Functions	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]).	
CA/Browser Forum	Baseline Requirements for the Issuance and Management of	20-Sep-17	7.1.3. Algorithm Object Identifiers	Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA‐1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1	https://cabforum.org/wp-content/uploads/CA-Browser-

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
	Publicly-Trusted Certificates Version 1.5.1			until 1 January 2017. This Section 7.1.3 does not apply to Root CA or CA cross certificates. CAs MAY continue to use their existing SHA‐1 Root Certificates. SHA‐2 Subscriber certificates SHOULD NOT chain up to a SHA‐1 Subordinate CA Certificate. Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA‐1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA‐1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.	Forum-BR-1.5.1.pdf

・ 鍵長に関するガイドライン

ドキュメント（発行元）	タイトル	発行日	記載場所	記載内容	備考
NIST Special Publication 800-57 Part 1 Revision 4	Recommendation for Key Management Part 1: General	January 2016	5.6.2 Defining Appropriate Algorithm Suites Table 4: Security-strength time frames	※別表 1	表 3 NIST SP800-57 でのビット安全性の取り扱い方針（WG で加工）は変更なし
ENISA	Algorithms, key size and parameters report 2014	November 21, 2014	Chapter 2 How to Read this Document 3.6 Key Size Analysis	※別表 2	

※別表 1

Table 4: Security-strength time frames

Security Strength		Through 2030	2031 and Beyond
< 112	Applying	Disallowed	
	Processing	Legacy-use	
112	Applying	Acceptable	Disallowed
	Processing		Legacy use
128	Applying/Processing	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

出展 URL：http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

※別表 2

Classification	Meaning
Legacy ✗	Attack exists or security considered not sufficient. Mechanism should be replaced in fielded products as a matter of urgency.
Legacy ✓	No known weaknesses at present. Better alternatives exist. Lack of security proof or limited key size.
Future ✓	Mechanism is well studied (often with security proof). Expected to remain secure in 10-50 year lifetime.

Table 2.1: Summary of distinction between legacy and future use

	Parameter	Legacy	Future System Use	
			Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size	m	80	128	256*
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(p^{k \cdot n}) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512

Table 3.6: Key Size Analysis. A * notes the value could be smaller due to specific protocol or system reasons, the value given is for general purposes.

出展 URL：https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

② SSL/TLS 暗号設定ガイドラインにおける引用文献等の改訂版の内容に係る調査

「SSL/TLS 暗号設定ガイドライン」の本文・コラム・付録・脚注で引用されている文献等について、2015 年 1 月以降の改訂版の有無を調査した。改訂版がある場合は更にその改訂内容を調査し、ガイドライン中の該当する本文・コラム・付録・脚注の記述の変更が必要かどうか分析した。

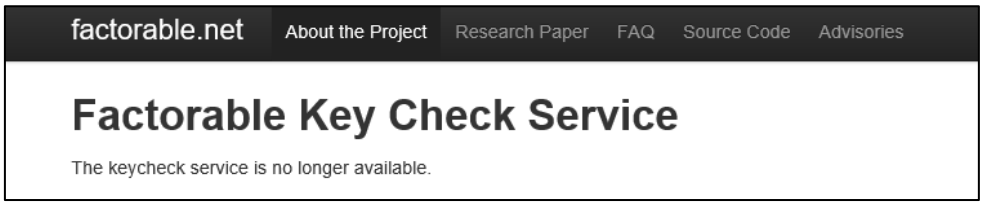
大きく改訂が必要な個所は、以下の 3 点と考えられる。

なお、詳細な調査結果については、「添付資料 3 引用文献調査」を参照。

- 鍵ペアの脆弱性チェックサービスが停止
  - 記載場所　P.45 の脚注 29
  - 記載内容

    例えば https://factorable.net/keycheck.htmlがある。ただし、安全性を100%証明するものではないことに注意されたい。
  - 変更点

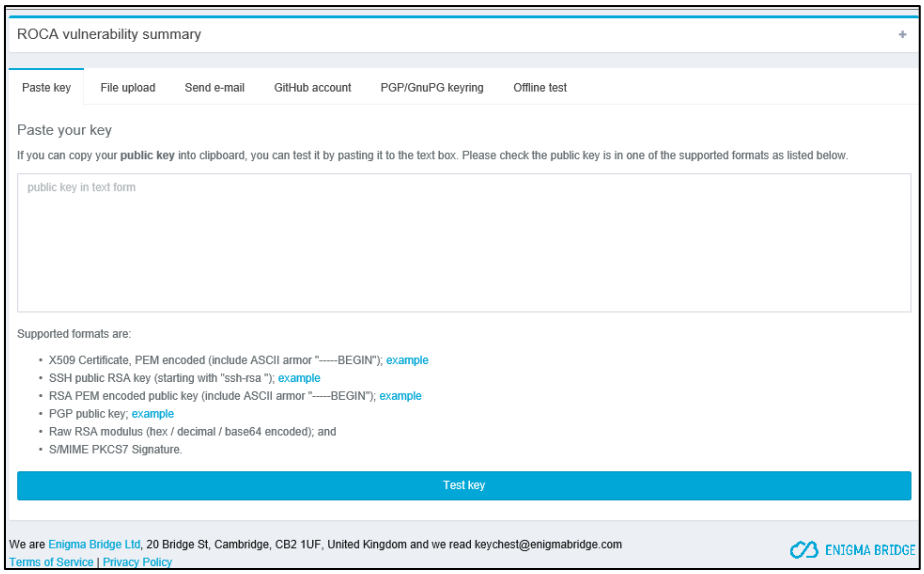
    サービスが停止



  - 代替案

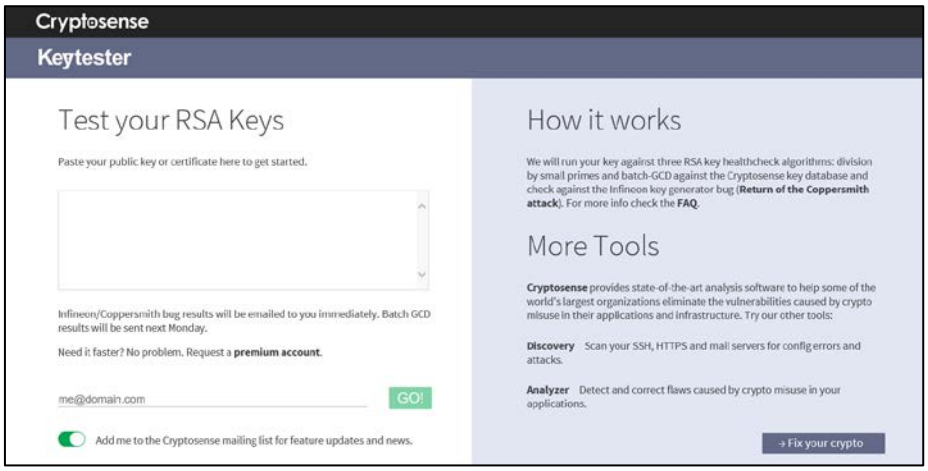
    代替サイトに変更する。あるいは、参考URLを削除する。
  - 代替サイト例
    - ✓ KEYCHEST

      https://keychest.net/roca

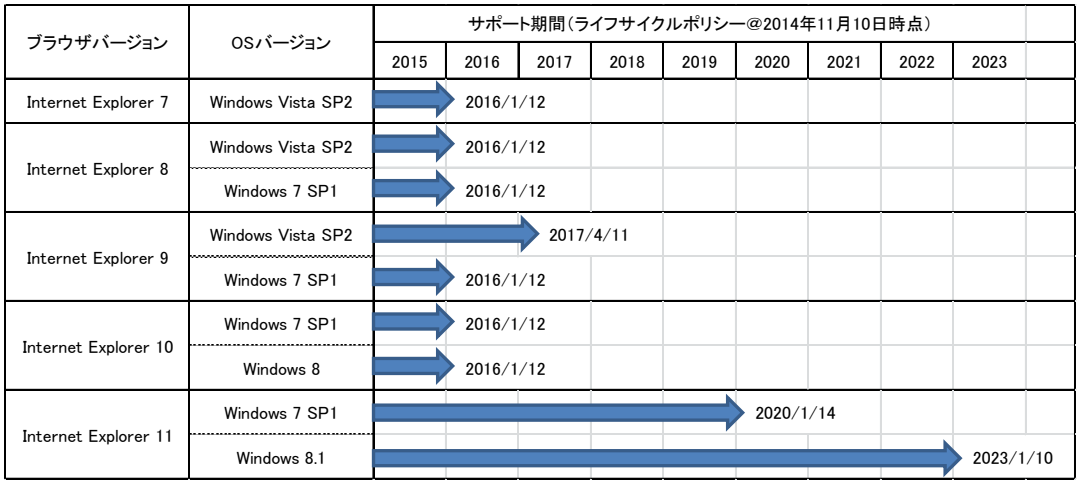


✓ Cryptosence

https://keytester.cryptosense.com/



- WinodwsOSとIEとサポート終了
- 記載場所　P.55 8.1.2 対象とするブラウザのバージョン
- 記載内容



- 変更点

  サポートブラウザはIE11とEdgeのみになった

- 代替案

  IEのサポート切れバージョンは削除し、IE11とEdgeのみの記載にする

  ✓ Microsoft Internet Explorer 11

  ✓ Microsoft Edge

- 関連情報

  ✓ WindowsOS

  P76 B.2.4 Microsoft IISの場合

  URLに記載のOSはサポート切れ

- SHA-1サーバ証明書のサポート終了

- 記載場所

  P.59 8.3.1 鍵長1024ビット、SHA-1を利用するサーバ証明書の警告表示

  ✓ Microsoft Internet Explorer

  ✓ Google Chrome

  ✓ Firefox

- 変更点

  その後の動向を含めた最新情報にする

- 代替案

  ✓ Microsoft Internet Explorer

  2017 年 5 月 10 日、マイクロソフトは SHA-1 証明書で保護されているサイトの読み込みをブロックし、無効な証明書の警告を表示します

  https://technet.microsoft.com/ja-jp/library/security/4010323

※ただし、デフォルトの無効化であり、強行して表示は可能である（付録参照）

- ✓ Google Chrome

  Chrome 56 で、SHA-1 証明書のサポートが廃止される予定です

  https://developers-jp.googleblog.com/2016/11/sha-1-certificates-in-chrome.html

  ※ただし、デフォルトでの廃止であり、強行して表示は可能である（付録参照）

- ✓ Firefox

  2017 年 3 月 7 日の Firefox 52 最終リリースを待つことなく、2 月 24 日にリモートですべての Firefox ユーザの SHA-1 対応を無効化しました

  https://www.fxsitecompat.com/ja/docs/2016/sha-1-certificates-issued-by-public-ca-will-no-longer-be-accepted/

  ※ただし、デフォルトの無効化であり、強行して表示は可能である（付録参照）

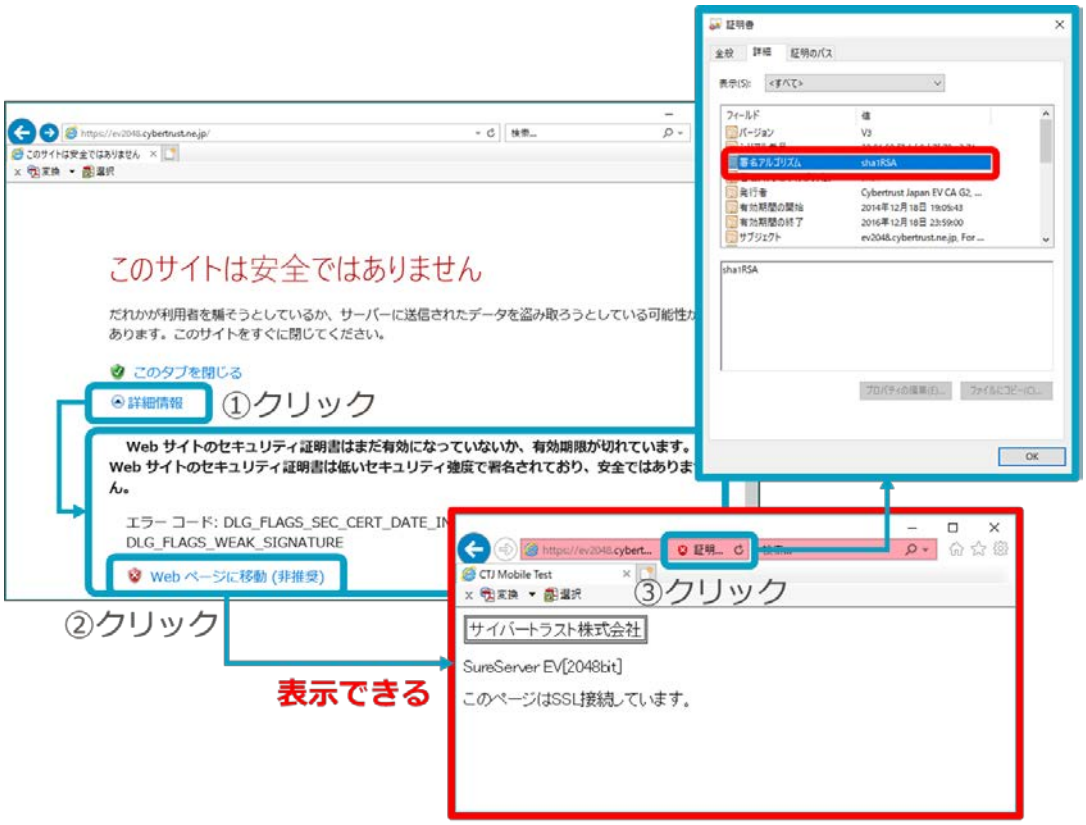
- 備考

SHA-1サポート停止は、商用CAのSHA-1証明書発行を停止（symantec：2015年12月末）から始まった。また、ブラウザベンダがSHA-1証明書への接続停止、警告表示（Chrome：2016年1月1日）を始めている。これらの動きの背景には、CABFのガイドライン※1が影響していると考えられる。

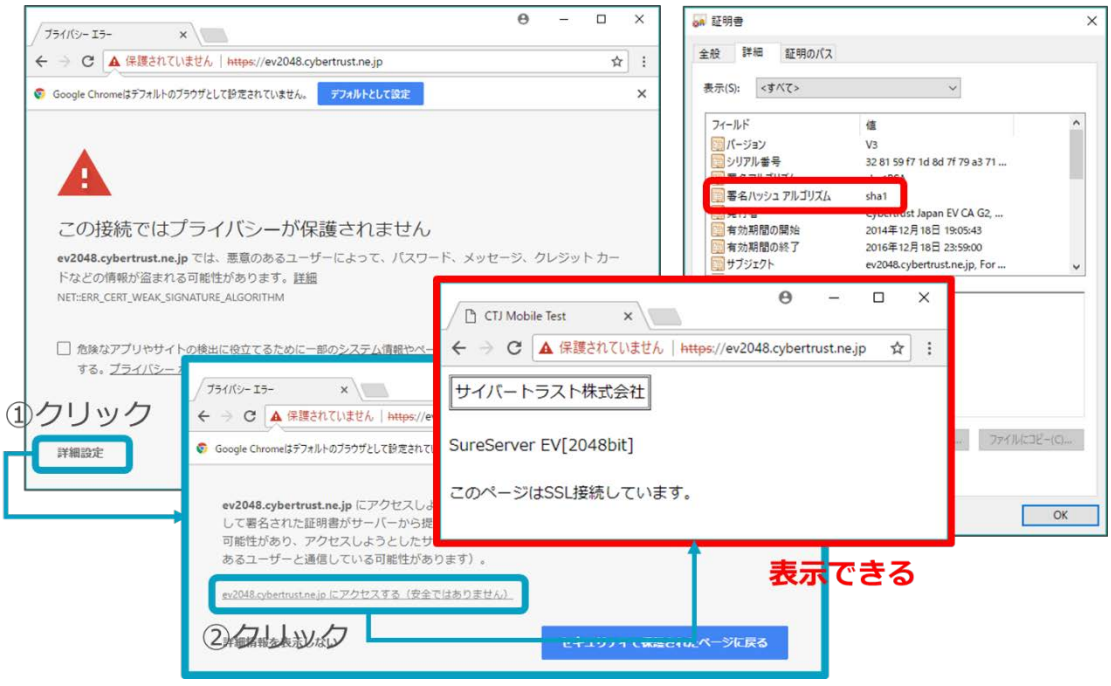
※ Baseline Requirements, v. 1.5.5 December 21, 2017

- ✓ Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA‐1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017.
- ✓ Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA‐1 algorithm with an Expiry Date greater than 1 January 2017

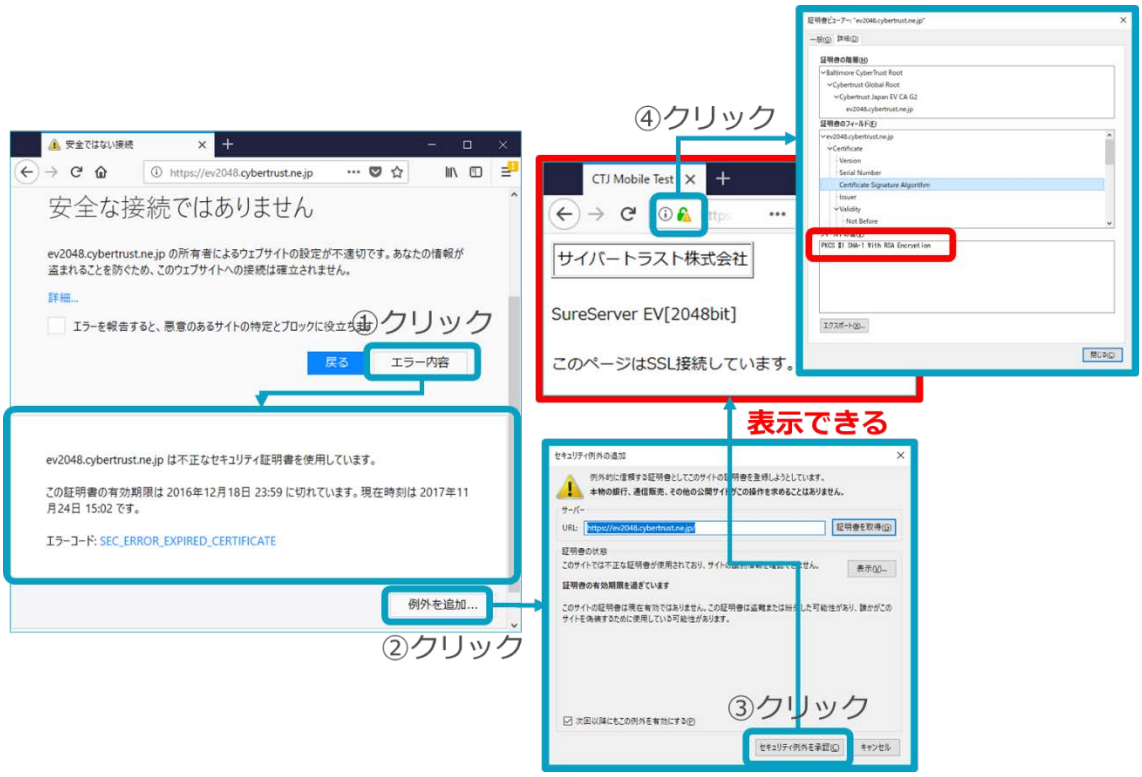
付録：SHA-1証明書の挙動（IE11）



付録：SHA-1 証明書の挙動（Chrome62.0.3202.94）



付録：SHA-1証明書の挙動（Firefox57.0）



③　設定・実装状況に係る調査

以下の調査方法により、主要製品での設定・実装状況を調査した。

- 調査方法

  調査方法は、以下のとおりである。

  - 原則として公式ベンダサイト記載の内容で調査する
  - 公式サイトに記載がなければ他サイトから情報を収集する
  - TLS の実装率は調査サイトを利用する

- 公式ベンダサイト

  公式サイトは、以下とする。

  - サーバ

サーバ	概要	公式ベンダサイト（例）
Apache	公式サイトでサーバの設定の有無を確認可能	http://httpd.apache.org/
		https://wiki.apache.org/general
Lighttpd	redmine のチケットに情報があるが、まとまっていない情報。	https://www.lighttpd.net/
		https://redmine.lighttpd.net/

サーバ	概要	公式ベンダサイト（例）
nginx	公式サイトでサーバの設定の有無を確認可能	http://nginx.org/
		https://trac.nginx.org/
IIS	公式サイトで確認可能	https://support.microsoft.com/
		https://docs.microsoft.com/
		https://technet.microsoft.com/
Google Web Server	確認不可 Google が自前のサービスを動かしているサーバ。 情報は公開されていない。	

- ブラウザ

ブラウザ	概要	公式ベンダサイト（例）
Chrome	chromium から確認可能	http://www.chromium.org/
		https://developer.chrome.com/home
		https://developers.google.com/web/
		https://blog.chromium.org/
		https://bugs.chromium.org/
		https://groups.google.com/a/chromium.org
Firefox	mozilla のセキュリティブログ等で確認可能	https://blog.mozilla.org/security/
		https://www.mozilla.org/
		https://developer.mozilla.org
		https://wiki.mozilla.org/
Opera	Opera blogs で検索できる	http://www.opera.com/
Safari	iOS での設定を調査する	https://www.apple.com/safari/
IE	公式サイトで確認可能	https://docs.microsoft.com/
		https://blogs.windows.com
		https://technet.microsoft.com
		https://blogs.msdn.microsoft.com
		https://support.microsoft.com/
		https://developer.microsoft.com

ブラウザ	概要	公式ベンダサイト（例）
		http://download.microsoft.com
Edge	公式サイトで確認可能	（IE と同じ）

- 信頼度の定義

  調査結果として取得した情報に信頼度をつける。信頼度の定義は、以下のとおりである。

  ✓ 信頼度：高＝公式サイトに明示的に記述がある

  ✓ 信頼度：中＝複数の公式サイトの記述から導き出される

  ✓ 信頼度：低＝公式以外のサイトの記述

- 調査結果

  調査結果は、以下のとおりである。

  - （2.1.1）SSL/TLS の各バージョンでのサーバ及びブラウザでの実装状況

バージョン	実装率	出典・ページタイトル	URL
TLS1.0	87.9%	SSL Pulse Monthly Scan: March 03, 2018	https://www.ssllabs.com/ssl-pulse/
TLS1.1	85.3%		
TLS1.2	91.0%		

  - （6.3.3 節）DHE/ECDHE の鍵長の設定状況

    詳細は、別紙 1 を参照。

  - （7.2.1 節）～（7.2.5 節）

    HTTP Strict Transport Security（HSTS）、OCSP Stapling、Public Key Pinning について、調査をした。

    以下に、OCSP Stapling の調査結果の一部を例として示す。

    他の 2 つについても同様に調査結果をまとめており、詳細は、「添付資料 4 SSL/TLS 実装状況調査」を参照。

    ✓ OCSP Stapling の調査結果（例）

サーバ名	実装状況	記載内容	信頼度	URL
Apache	○	SSLUseStapling が有効ならば、OCSP 応答を格納するキャッシュを設定する [引用：Configures the cache used to store OCSP responses which get	高	http://httpd.apache.org/docs/2.4/ja/mod/mod_ssl.html#sslstaplingcache

サーバ名	実装状況	記載内容	信頼度	URL
		included in the TLS handshake if SSLUseStapling is enabled.]		
		OCSP stapling を有効にするには、httpd の設定を少し変えるだけでよい。 [引用：Once general SSL support has been configured properly, enabling OCSP Stapling generally requires only very minor modifications to the httpd configuration − the addition of these two directives: SSLUseStapling On SSLStaplingCache "shmcb:ssl_stapling(32768)"]	高	http://httpd.apache.org/docs/trunk/ssl/ssl_howto.html

- （8.1.1 節）～（8.1.2 節）

OS およびブラウザのサポート状況について調査をした。

以下に OS の調査結果（例）を示す。

同様にブラウザについても調査結果をまとめており、詳細は、「添付資料 4 SSL/TLS 実装状況調査」を参照。

✓ OS の調査結果（例）

OS 名	サポート状況	サポート終了	記載内容	信頼度	URL
Windows Vista Service Pack 2	×	2017/4/11	（製品のライフサイクルの検索）	高	https://support.microsoft.com/ja-jp/lifecycle/search
Windows 7 Service Pack 1	○	2020/4/11			
Windows 8	×	2016/1/12			
Windows 8.1	○	2023/1/10			
Windows 10	○	2025/10/14			
OS X	-	最終アップデート		高	

OS 名	サポート状況	サポート終了	記載内容	信頼度	URL
Mavericks (10.9)		2016/7/18	（Apple セキュリティアップデート）		https://support.apple.com/ja-jp/HT201222
OS X Yosemite (10.10)	-	最終アップデート 2017/7/19			
OS X El Capitan (10.11)	-	最終アップデート 2017/12/6			
macOS Sierra (10.12)	-	最終アップデート 2017/12/6			
macOS High Sierra (10.13)	-	最終アップデート 2017/12/6			

④ SSL/TLS に関する脆弱性情報・危殆化情報に係る調査

SSL/TLS に関する脆弱性情報・危殆化情報について調査した。

- 調査方法

  インターネットで検索エンジンにキーワード（SSL、TLS、脆弱性等）を入れて調査

- 調査対象期間

  2015 年 5 月～2017 年 12 月

調査結果は、「添付資料 5 SSL/TLS に関する脆弱性情報」を参照。

4.2 SSL/TLS 暗号設定ガイドライン改訂に係る検討

本調査結果を踏まえて、次の①から③の観点で、SSL/TLS 暗号設定ガイドライン改訂に係る具体的な改訂案の検討を実施し、「SSL/TLS 暗号設定ガイドライン改訂案」として取りまとめた。本文とコラム、および、脚注に係る記述の改訂案は、別紙 1 として添付した。また、付録に係る記述の改訂案は、別紙 2 として添付した。

① 本文に係る記述のアップデート

② コラムに係る記述のアップデート

③ 付録・脚注に係る記述のアップデート

4.3 鍵管理ガイドライン作成に係る事前調査

① 鍵管理に関する調査

4.3.1 文献調査

4.3.1.1 調査対象の文献

鍵管理ガイドラインを作成するにあたり、現在国内外にどのような鍵管理ガイドラインが存在するのか、それらの文書体系も含めて把握するため、以下の文献を調査対象とした。

(1) タイトルまたは目次に「Key Management」が含まれている NIST（National Institute of Standards and Technology：アメリカ国立標準技術研究所）の各文献

(2) タイトルまたは目次に「Key Management」が含まれている ENISA（European Network and Information Security Agency：ヨーロッパネットワーク情報セキュリティ庁）の各文献

(3) OASIS Key Management Interoperability Protocol Specification Version 1.3

(4) RFC 3647

(5) 国内の文献

調査対象の文献を鍵管理が主テーマの文献と、個別アプリケーションの文献の中に鍵管理が述べられているものに分けて下表に示す。表の「略称」は本報告書の中で文献を指す際に分かりやすいように付けた名称である。

・　文献一覧　主テーマが鍵管理の文献（国外の文献）

文献番号	文献名	略称	発行日
SP 800-57 Part1 Rev. 4	Recommendation for Key Management, Part 1: General	Part1 General)	2016/1/28
SP 800-57 Part2	Recommendation for Key Management, Part 2: Best Practices for Key Management Organization	Part2(Best Practices)	2005/8/25
SP 800-57 Part3 Rev. 1	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	Part3 (Application)	2015/1/22
SP 800-130	A Framework for Designing Cryptographic Key Management Systems	Framework	2013/8/15
SP 800-152	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Federal	2015/10/28
SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Guideline	2016/8/22
ENISA 2013	Recommended cryptographic measures - Securing personal data	[ENISA] Recommended	2013/11/4
ENISA 2014	Algorithms, key size and parameters report 2014	[ENISA] Algorithms	2014/11/21
ENISA 2011	The Use of Cryptographic Techniques in Europe	[ENISA] Use	2011/12/20
OASIS	Key Management Interoperability Protocol Specification Version 1.3	KMIP	2016/12/27

・　文献一覧　主テーマが鍵管理の文献（国内の文献）

文献番号	文献名	略称	発行日
CR 2010 GK	2010 年度版　リストガイド（鍵管理） CRYPTREC	[CR]リストガイド	2011/6/30
IPA 2008 R	安全な暗号鍵の ライフサイクルマネージメントに関する調査 調査報告書	[IPA]調査報告書	2008/7/25
IPA 2008 G	安全な暗号鍵の ライフサイクルマネージメントに関する調査 鍵管理ガイドライン（案）	[IPA]ガイドライン（案）	2008/7/25
IPA	「暗号鍵の適切な運用・管理に係る課題調査」報告書	[IPA]鍵寄託 (Escrow)	2013/2/25

・　文献一覧　個別アプリケーション

文献番号	文献名	略称	発行日
SP 800-81-2	Secure Domain Name System (DNS) Deployment Guide	DNS	2013/9/18
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	Wireless	2007/2/7
SP 800-111	Guide to Storage Encryption Technologies for End User Devices	Storage	2007/11/15
SP 800-88 Rev. 1	Guidelines for Media Sanitization	Sanitization	2014/12/17
NISTIR 7956	Cryptographic Key Management Issues & Challenges in Cloud Services	Cloud	2013/9/18
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	X.509	2003/11/1
CSI SSH	SSH サーバセキュリティ設定ガイド	SSH	2015/3/15

4.3.1.2 調査方法

以下の方法で調査を行なった。

(1) 調査対象の文献の全体像を把握するため、鍵管理が主テーマ各文献に対して扱っている項目を洗い出し、行に文献の目次の一覧、列に文献を並べたマッピングを作成して別紙 3 にまとめた。

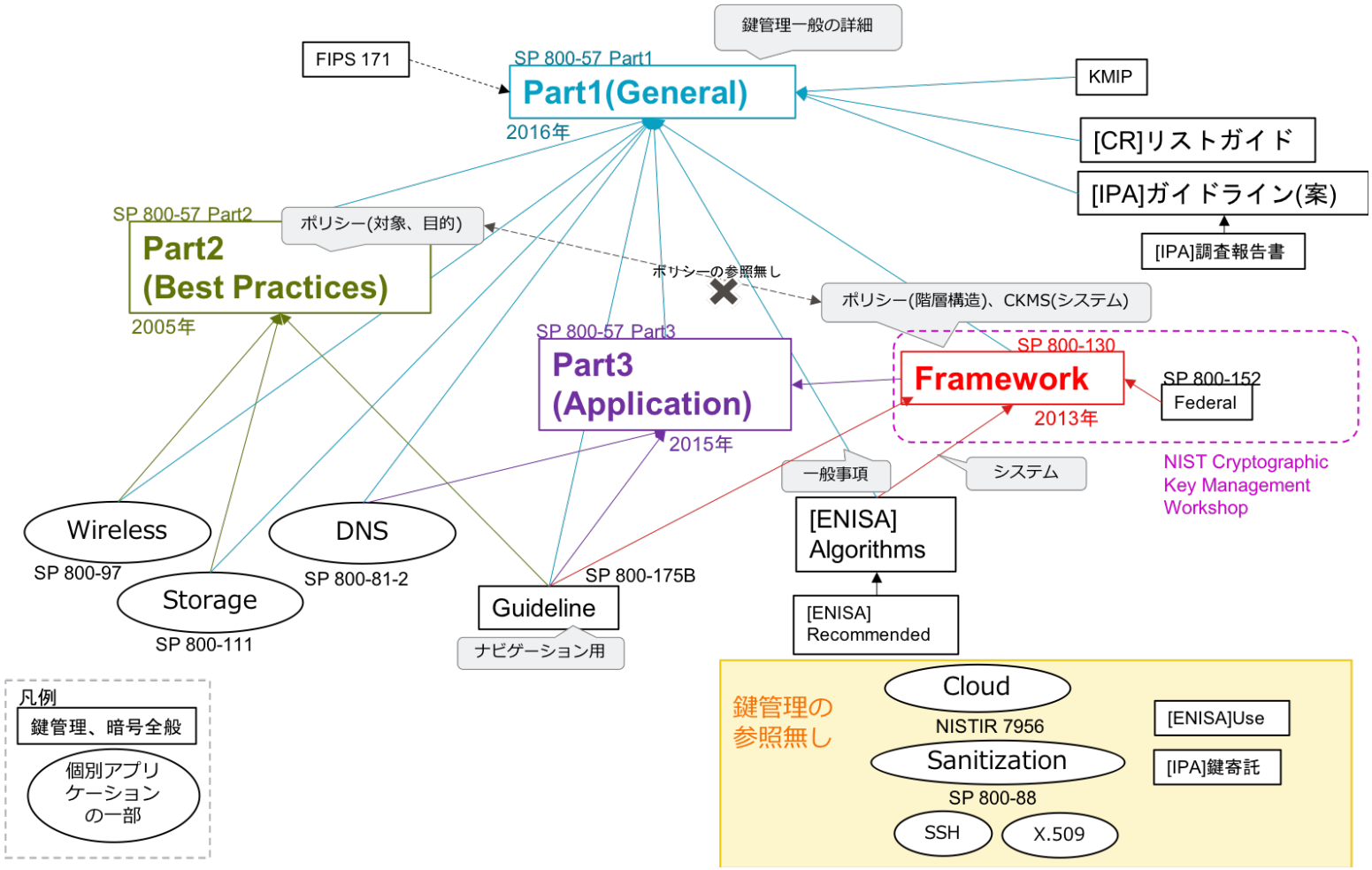
複数の文献で同じ項目や似たような項目を扱っている場合は、述べられている内容が同じなのか違うのかを確認した。

(2) 参照している文献を確認し、図に整理した。

(3) ポイントとなる文献は重点的に内容を確認し、オリジナルな主張を述べている箇所がある文献についてもその内容を確認した。

4.3.1.3 文書体系、他文献との関連

各文献の鍵管理に関する他文献の参照関係を下図に示す。



・　主要な文献の概要

文献番号 (リビジョン)	略称	読者	目的	暗号 アルゴリズム	鍵管理 ガイダンス	保護要件	鍵の状態とフェーズの機能	ポリシー
SP 800-57 Part1 (2005 初版 2006 改訂 2007 改訂 2012 Rev.3 2016 Rev.4)	Part1 (General)	システム管理者、暗号モジュール開発者、プロトコル開発者	・鍵管理の一般的なガイダンスの提供	Hash、共通鍵、MAC、署名、鍵配送・鍵共有、乱数	鍵種別、鍵の有効期間、危殆化、暗号アルゴリズムと鍵サイズの選択・移行	鍵種別ごとの保護要件、送信と保管の可用性・完全性・機密性	状態[活性化前、活性化、一時停止、不活性化、危殆化、破棄] フェーズ[運用前、運用、運用後、破棄後]	なし
SP 800-57 Part2 (2005 初版)	Part2(Best Practices)	システムの所有者と管理者	・鍵管理のポリシー(KMP)とポリシー実施文書(KMPS)作成のガイド ・安全性計画作成のガイド ・鍵管理基盤の構造も示している	なし	鍵の有効期間(SP 800-57 Part1 を参照)	安全性計画の可用性・完全性・機密性	機能[鍵生成、共有、分配・失効、バックアップ・リカバリ] KMPS には、組織の役割・責任・手順と SP 800-57 Part1 の該当セクション番号を記載する	セキュリティの目的、組織の役割と責任
SP 800-57 Part3	Part3	対象のアプリケー	・下記アプリケーショ	推奨アルゴリズ	鍵種別、鍵サ	セキュリ	各アプリケーシ	なし

文献番号 (リビジョン)	略称	読者	目的	暗号 アルゴリズム	鍵管理 ガイダンス	保護要件	鍵の状態とフェーズの機能	ポリシー
(2009 初版 2015 Rev.1)	(Application)	ションのシステム構築者、管理者、ユーザ	ンの鍵管理の推奨事項をガイド。 [PKI 、 IPsec 、 TLS 、 S/MIME、ケルベロス、無線回線経由の鍵更新(OTAR)鍵管理メッセージ(KMM)、DNSSEC、暗号化ファイルシステム(EFS)]	ム、モード	イズ、移行 (SP 800-57 Part1 を参照し、アプリケーション固有の説明を追加。各技術の文献も多く参照)	ティ・適合性の問題	ョン固有の鍵管理の推奨事項を構築者、管理者、利用者ごとに列挙	
SP 800-130 (2013 初版)	Framework	鍵管理システム(CKMS)設計書の作成者	・鍵管理システム設計書のフレームワークを提供。組織はフレームワークをベースに自組織用のプロファイルを作成する。 ・鍵管理ポリシー策定のための分析方法を提供。	なし	鍵種別(SP 800-57 Part1 の種別をまとめた表)、メタデータ(Part1 のメタデータの参照なし)	機密性・完全性・情報源認証 (Part1 との関連なし)	SP 800-57 Part1 のフェーズの各機能を鍵管理システム設計書用の項目に整理している	階層構造で分析、セキュリティドメインの考察 (SP800-57 Part2 の参照なし)
SP 800-175B	Guideline	暗号システム構築	・NIST 暗号標準の概要	Hash、共通鍵、公	セキュリティ	機密性・完	鍵 生 成 (SP800-	X.509 証明書

文献番号 (リビジョン)	略称	読者	目的	暗号 アルゴリズム	鍵管理 ガイダンス	保護要件	鍵の状態とフェーズの機能	ポリシー
(2016 初版) SP800-21 (1999、2005)がベース		の管理者、暗号方式を選択する技術者、暗号サービス利用者	を提供 ・ナビゲーションとして利用	開鍵、MAC、署名、乱数	強度(SP800-152)、鍵サイズ(SP800-57 Part1)、鍵の有効期間(SP800-57 Part1)、移行(SP800-57 Part1 と SP800-131A)	全性・情報源認証 (他文献の参照なし)	133)、鍵導出(SP800-108)、鍵確立・鍵転送(SP800-56A,B)、鍵のラップ(SP800-38F) CKMS・フレームワーク(SP800-130)	ポリシー
ENISA 2014 (2014 発行)	[ENISA] Algorithms	暗号ソリューションの設計者と開発者	・暗号アルゴリズムと鍵サイズをガイド	Hash、共通鍵、公開鍵、MAC、認証、署名、KEM	鍵サイズ(文献と論文の独自の調査・分析)	完全性 (MAC)	SP 800-57 Part1 を参照し、独自の説明を追加	鍵管理システムはポリシーを満たす (SP800-130 を参照)
CR2010 (2011 発行)	[CR] リストガイド	電子政府システムの調達担当者、開発者、運用担当者	・日本政府機関内の暗号鍵管理手順の策定のための資料	なし	鍵の有効期間(SP800-57 Part1 と国内の署名の法制度の鍵の有効期間の	送信と保管の可用性・完全性・機密性 (SP800-57	鍵生成、更新、保存、破棄(SP800-57 Part1 のまとめ)	完全性が失われた場合のポリシー

文献番号 (リビジョン)	略称	読者	目的	暗号 アルゴリズム	鍵管理 ガイダンス	保護要件	鍵の状態とフェーズの機能	ポリシー
					一覧)、移行(国内の SHA-1 と RSA1024 の移行指針)	Part1 のまとめ)	漏洩対策は独自の記述	
IPA2008G (2008 発行)	[IPA] ガイドライン（案）	情報システムの調達/運用担当者	・暗号鍵の生成から破棄までのライフサイクルを考慮した管理手法を策定する	なし	鍵種別、鍵の有効期間(SP800-57 Part1 のまとめ)	なし	生成、配送、利用（変更・導出）、保管・バックアップ、期限切れ・失効・廃棄、回復(SP800-57 Part1 のまとめと追記)	各フェーズで脅威への対策の方針

表中の参照文献

SP 800-21, Guideline for Implementing Cryptography in the Federal Government.

SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.

SP 800-133, Recommendation for Cryptographic Key Generation.

SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions.

SP 800-56A, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.

SP 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography.

SP 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.

多くの文献が鍵管理の一般的事項は SP 800-57 Part 1 (General)を参照するように書いていて、本文献が鍵管理の基礎の位置付けであることが分かる。IPA の鍵管理ガイドライン（案）と CRYPTREC のリストガイドはいずれも本文献を参考にしている。Part 1 と共に Part 2 (Best Practices) と Part 3 (Application)を紹介している文献もある。
SP 800-57 以外では SP800-130 (Framework)が SP 800-175B (Guideline)と ENISA (Algorithms)で参照されていて、そこでは鍵管理(CKM)の文献は SP 800-57 で鍵管理システム(CKMS)の文献は SP 800-130 であるとされている。NIST 「Cryptographic Key Management Workshop」は、鍵管理フレームワーク SP 800-130 (Framework)とこのフレームワークを基に作られた連邦政府向けのプロファイル SP800-152 (Federal)を作成するための会議である。SP800-57 Part2(Best Practices)と SP800-130 (Framework)は”ポリシー”を扱っているため内容を比較したところ、SP800-57 Part2 (Best Practices)では、安全性の検討事項として保護対象の情報、脅威、保護メカニズム、保護要件などが列挙され、組織の役割と責任も説明されている。一方 SP800-130 (Framework)は SP800-57 Part2 の参照はなく、ポリシーを鍵管理システムより上位概念の情報管理ポリシーから階層的に分析していて、ポリシーについてより詳細に述べられている。本調査ではこの SP800-130 (Framework)も重要な文献と位置付け詳しく調査することにした。
NISTIR 7956 (Cloud)や SP 800-88 (Sanitization)などは、鍵管理に関して他の文献を参照せず独自の方法を提案している。

4.3.1.4 各文献の概要

本節では、各文献の概要を説明する。

4.3.1.4.1 SP 800-57 Part 1 (General)

[Recommendation for Key Management, Part 1: General Rev. 4]

本文献は、鍵管理の一般的なガイダンスを提供していて、想定読者はシステム管理者、暗号モジュール開発者、プロトコル開発者と幅が広い。内容も Hash や MAC、乱数生成等の暗号アルゴリズムの説明から鍵管理まで幅広く書かれている。鍵管理のメインは「一般的な鍵管理ガイダンス」の章と「鍵管理のフェーズと機能」の章である。

「一般的な鍵管理ガイダンス」では、鍵の種別を説明し、鍵の種別や非対称鍵/対称鍵ごとに鍵の有効期間を詳しく説明している。鍵サイズや暗号スイートについても述べられている。

「鍵管理のフェーズと機能」では、運用前/運用/運用後/破棄後の 4 つのフェーズでの鍵管理の機能が説明されている。

- 運用前フェーズ : 利用者登録機能、システム初期化機能、鍵材料インストール機能、鍵確立機能、鍵登録機能

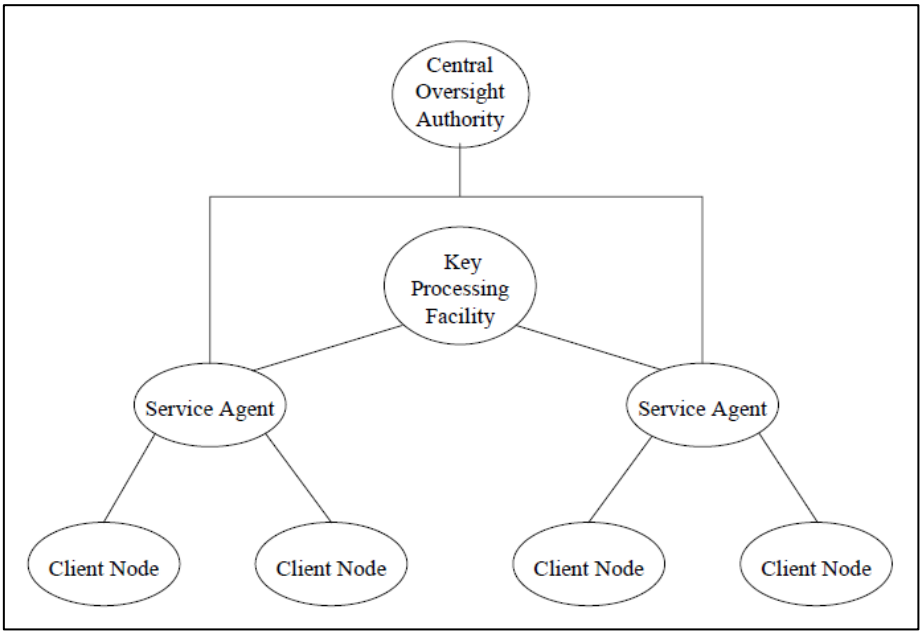
- 運用フェーズ：鍵の保管機能、鍵の変更機能、鍵導出方法
- 運用後フェーズ：アーカイブと鍵回復機能、エンティティ登録抹消機能、鍵登録抹消機能、鍵破棄機能、鍵失効機能
- 破棄後フェーズ：メタデータ記録の保持

この SP800-57 Part 1 は 2005 年に初版が発行され、2006 年と 2007 年に改訂があり、2012 年に Revision 3 となり、現在の最新版は 2016 年の Revision 4 である。初版は FIPS 171「Key Management Using ANSI X9.17」(1992)をベースに作られている。ANSI X9.17 は金融機関の間の鍵転送プロトコルである。

4.3.1.4.2 SP 800-57 Part 2 (Best Practices)

[Recommendation for Key Management, Part 2: Best Practices for Key Management Organization]

本文献は、組織が鍵管理のポリシーを作成する際に検討する内容とポリシーを実現するための文書に書くべき内容をガイドすることを目的にしている。
本文献ではまず、中央監視権限、鍵保持機関、サービス代行者、クライアントノードから成る鍵管理の基盤(KMI)の概念が示されている。その基盤では、中央監視権限は組織の鍵管理システムの安全性監視のためポリシーや実施文書を統括し、鍵保持機関は公開鍵証明書の発行や鍵材料の分配を行う。サービス代行者は組織に該当し、組織内の各クライアントノードと鍵保持機関の通信はサービス代行者を通じて行なわれる。



SP 800-57 Part 2 Figure 1: KMI Components

鍵管理ポリシー作成時には以下を検討しポリシーに含める。
・保護対象のデータ
・脅威
・暗号を用いた保護技術
・暗号のプロセスと鍵材料に対する保護要件
　また、鍵管理の基盤(KMI)での組織の責任と役割も説明されている。
本文献は 2005 年に SP 800-57 Part 1(General) と同時に発行されて以降、改訂されていない。

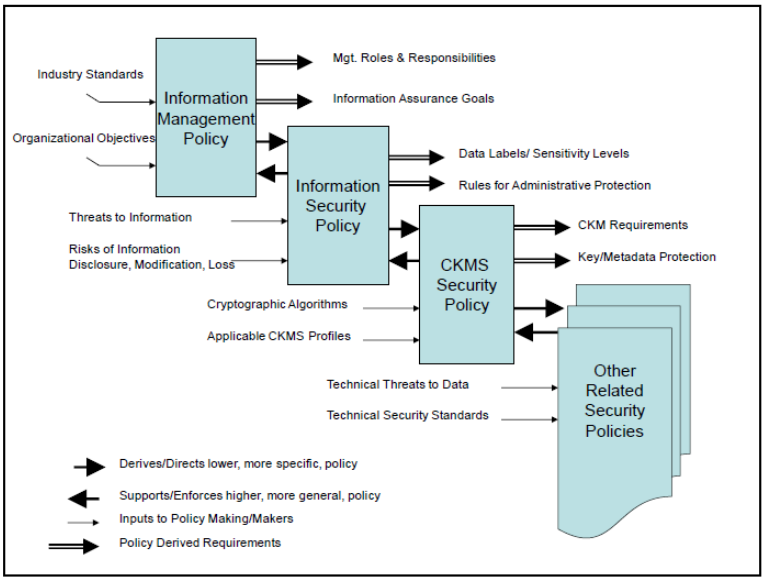
4.3.1.4.3　SP 800-57 Part 3 (Application)
[Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance]
　本文献では、以下のアプリケーションに対して、セキュリティおよび適合性の問題、調達ガイダンス、システムの設置者／管理者／システム利用者ごとの推奨事項が述べられている。
[アプリケーション]
PKI、IPsec、TLS、S/MIME、ケルベロス、無線回線経由の鍵更新(OTAR)鍵管理メッセージ(KMM)、DNSSEC、暗号化ファイルシステム(EFS)

4.3.1.4.4　SP 800-130 (Framework)
[A Framework for Designing Cryptographic Key Management Systems]
　本文献は、鍵管理システム(CKMS)の設計者向けのドキュメントであり、設計書に指定すべきことを記したフレームワークを提案している。フレームワーク本体の前に以下のような鍵管理の考え方が述べられている。

(1) 鍵管理は鍵だけでなく鍵の属性値であるメタデータも管理する必要がある。メタデータは鍵名称、所有者識別子、ライフサイクルのステータス、フォーマット、暗号アルゴリズム、鍵サイズといった属性値を指す。
(2) CKMS 設計者は組織や部門に合わせてフレームワークを変更したオリジナルの CKMS 設計書"プロファイル"を作成する。
(3) プロファイルを満たすには複数のセキュリティメカニズムを組み合わせる。規制品も利用する。標準化された製品の利用も有益である。
(4) 鍵管理システムの設計は鍵管理システムの方針（ポリシー）に沿って作成する。鍵管理システムのポリシーは、最上位概念である情報管理ポリシーから、情報セキュリティポリシー、鍵管理システムポリシーへとブレイクダウンしながら

分析して策定する。情報管理ポリシーでは保護対象の情報や関係する人の役割と責任を分析し、情報セキュリティポリシーでは脅威やリスクを分析し、鍵管理システムポリシーでは用いる暗号アルゴリズムを検討する。

(5) 同じポリシーを適用する範囲をセキュリティドメインと呼ぶ。異なるセキュリティドメインに属するエンティティ同士は、他方のセキュリティポリシーを等価だとお互い認める場合に鍵やメタデータを受け渡すことができる。



SP 800-130 Figure 7: Related Security Policies

フレームワーク本体には、鍵の各ライフサイクルにおいて CKMS に指定すべき内容が SP800-157 Part 1(General)に沿って書かれている。鍵だけでなく鍵のメタデータの管理についても述べられている。

安全性の管理の章には、鍵管理に使用するハードウェアや暗号モジュールのソフトウェアを物理的に保護する方法について言及がある。

4.3.1.4.5 SP 800-152 (Federal)

[A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)]

本文献は、フレームワーク SP800-130(Framework)を基に作られた連邦政府向けの鍵管理プロファイルである。フレームワークの各項目における連邦政府の要件が 3 つのレベルで規定されている。

“PR”: 要件 (shall または shall not)

“PA”: 強く推奨される要件 (should)

“PF”: 可能な機能 (could)

4.3.1.4.6　SP 800-175B (Guideline)

[Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms]

本文献は、NIST の暗号標準の概要を提供することを目的としていて、暗号分野全体の文献を広く紹介しているためナビゲーション用として利用できる文献である。鍵管理については、SP800-57 Part 1(General)、Part 2(Best Practices)、Part 3(Application)および SP800-130 (Framework)を紹介している。

4.3.1.4.7　ENISA (Algorithms)

[Algorithms, key size and parameters report 2014]

本文献は、暗号ソリューションの設計者と開発者に対して暗号アルゴリズムと鍵サイズをガイドすることを目的としている。レガシーシステムが弱いアルゴリズムを使用している場合や鍵サイズが短い場合は、ふさわしい強度のアルゴリズムと鍵サイズに置換するためのアドバイスを行い、将来のシステムに対しては課題を検討している。鍵管理については鍵の生成から破棄までのライフサイクルの一般事項がまとめられていて、鍵管理一般の文献は SP 800-57 で鍵管理システム(CKMS)の文献は SP 800-130(Framework)であるとしている。

4.3.1.4.8　ENISA (Recommended)

[Recommended cryptographic measures - Securing personal data]

本文献は、個人データや機密データを保護するための暗号技術（暗号、認証、Hash、署名）と暗号プリミティブ（共通鍵暗号、公開鍵暗号、暗号の強度、鍵管理）が説明されている。鍵管理部分は、ENISA「Algorithms, key size and parameters Report.2014」と同じである。

4.3.1.4.9　ENISA (Use)

本文献は、ヨーロッパの電子政府で使われている暗号技術の調査の文献である。EU 加盟国に対して電子政府のシステムの仕様やガイドラインに関するアンケートを実施し、13 か国から得た回答の暗号の各技術の使用率などがグラフで示され、推奨事項が述べられている。

鍵管理に関する指摘は以下の通りである。

(1) 鍵管理のための独立した仕様があるべきだが、仕様やガイドラインにあまり書かれていない。
(2) IT 製品では、ベンダのデフォルト鍵や弱い事前共有鍵を使ってしまうことが多く、暗号自体が破られてしまう。

(3) 証明書の署名鍵を OS が管理するファイルシステムに保存するケースが見られるが、耐タンパ性の高いデバイスに保存すべき。

4.3.1.4.10 OASIS (KMIP)

本文献は、鍵管理の鍵管理の相互運用プロトコル(IMIP)のプロトコル仕様書で、暗号クライアントと鍵管理サーバ間の通信および鍵のライフサイクルのプロトコルを定義している。単語の定義と状態遷移で SP 800-57 Part1(General)を参照している。

4.3.1.4.11 CR (リストガイド)

本文献は、電子政府推奨暗号リストの適切な利用を目的とし、「政府機関の情報セキュリティ対策のための統一基準（第 4 版）」で規定が求められている暗号鍵の管理手順の各フェーズ（生成、有効期限、破棄、更新、鍵が露呈した場合の対処）について、CRYPTREC の活動内容と SP 800-57 等の文献の鍵管理の情報をまとめ、公開鍵暗号の場合と共通鍵暗号の場合に分けて説明している。公開鍵暗号・共通鍵暗号の共通項目として、鍵の転送時の保護とストレージで保管する際の保護についてまとめている。電子署名に関係する日本の法制度や、SHA-1 と RSA1024 の移行指針など日本固有の情報も含まれている。

4.3.1.4.12 IPA (調査報告書)

本文献は、日本の鍵管理ガイドライン制定に向けて行われた鍵管理の研究動向と国外のガイドラインの調査の報告書である。研究動向ではグループ鍵共有や ID ベース暗号、プロキシ暗号の研究が紹介されている。国外のガイドラインは、NIST SP800 の各種文献や ISO の金融における鍵管理、IETF の鍵管理の RFC が紹介されている。
また、文献調査とヒアリングにより国内の鍵管理の実態と課題、ニーズが議論され、次節の鍵管理ガイドライン（案）が作成された。

4.3.1.4.13 IPA (ガイドライン(案))

本文献は、IPA (調査報告書)を元に作成された文書で、SP 800-57 Part 1 (General)を参考にして鍵管理のライフサイクルの各段階ですべきことをガイドラインとしてまとめている。また、PKI を例に各段階で想定される脅威と対策が述べられている。

4.3.1.4.14 IPA (鍵寄託)

本文献は、米国と国際社会の鍵寄託と暗号技術の輸出規制の歴史的動向をまとめた文献である。鍵寄託とは暗号鍵を政府機関に登録することで、米国は 1993 年の世界貿易センター爆破事件以降、テロ組織による暗号の利用を警戒して鍵寄託と暗号技術の輸出制限の政策(Clipper 政策)を行ったが、米国内や国際機関に支持されずこの政策は消滅した。また、本文献には日本での暗号政策の歴史と 1996 年、1997 年、1998 年に試作された鍵寄託・鍵回復システムの仕組みも説明されている。

国の安全保障政策としての鍵寄託・鍵回復システムは否定された一方、民間部門での鍵紛失対策としての鍵回復システムは必要性が認識されていて、本文献では鍵回復の基本的な機能を 3 つ挙げ、鍵回復システムの方式を提案している。

[鍵回復システムの機能]

(1) データを暗号化する者は、復号できる者を明示的に指定できる。
(2) 指定された復号者は、復号に必要な情報（共通鍵）をシステム的に入手し、復号を行う。
(3) 法令の規定、組織ポリシーの規定、事故・災害時等の緊急対応方針等に準じて、1.で指定された者以外の者が復号できる手段を提供する。このとき、対象の暗号化データと復号者を限定できる。

4.3.1.4.15 SP 800-81-2 (DNS)

[Secure Domain Name System (DNS) Deployment Guide]

本文献は、商用の安全な DNS の開発のための文献であり、DNS の仕組みや DNS データ、脅威や安全性や保護について説明されている。DNSSEC の仕組みでは DNS データの認証と完全性を保証するため、ゾーン管理者はゾーン署名鍵（ZSK）で作成した署名を付加した DNS データを返す。また、ゾーン署名鍵に対して鍵署名鍵（KSK）で署名を作成し、鍵署名鍵の検証鍵（公開鍵）は親ゾーンに登録される。本文献ではゾーン署名鍵（ZSK）と鍵署名鍵（KSK）の計画的なロールオーバーと緊急時のロールオーバーについて述べられている。緊急ロールオーバーでは、ゾーン署名鍵（ZSK）が漏洩した場合は速やかに鍵署名鍵（KSK）も更新し、鍵署名鍵（KSK）が漏洩した場合は親ゾーン管理者に速やかに通知する。

4.3.1.4.16 SP 800-97 (Wireless)

[Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i]

本文献は、無線 LAN のセキュリティに関する規格 IEEE 802.11i(Robust Security Network)のガイドで、無線の安全性や通信の暗号化、認証プロトコルなどが説明されている。
鍵管理は SP800-57 Part 1 (General)と Part 2 (Best Practices)が参照され、ユニキャスト通信用の Pairwise 鍵およびブロードキャスト通信用のグループ鍵の階層構造についての説明がある。

4.3.1.4.17 SP 800-111 (Storage)

[Guide to Storage Encryption Technologies for End User Devices]

本文献は、PC やスマートフォン、CD/DVD 等のディスク、USB メモリ等のリムーバブルディスクの中の機密情報を保護するための方法として、アクセス制御、暗号化、鍵管理および認証について述べている。暗号化はフルディスク暗号化、仮想ディスクとボリュームの暗号化、ファイルとフォルダの暗号化ごとに技術が説明されている。
鍵管理に関しては、鍵保有者が組織を離れたり鍵を紛失したりして鍵が失われデータが復元できなくなるケースに着目していて、その場合にもデータを復元できるように、鍵の管理者は鍵のコピーを中央で一括管理したり外部メディアに保存する等の対策をとる必要があると述べている。鍵の保管場所はローカルハードディスクや USB メモリ、TPM チップなどから選択する。鍵を自動的に中央サーバに保管したり、鍵を持たずユーザが入力したパスワードから毎回鍵を生成したりする製品の機能も紹介されている。
また、鍵へのアクセスはパスワードやスマートカード等の認証技術により制限されるべきとしている。

4.3.1.4.18 SP 800-88 (Sanitization)

[Guidelines for Media Sanitization]

本文献は、サニタイズの方法についてデバイス（印刷物、機器、メディア等）ごとに説明している。サニタイズとは、破棄したデータを攻撃者が復元できないようにデータを消去、除去、破壊することである。
鍵管理に関する箇所は、データを復号する鍵をサニタイズすることによりデータを復号不可能にする Cryptographic Erase (CE)技術である。Cryptographic Erase は、以下の条件にあてはまる場合に利用できる。

(1) 鍵が保管されている場所が分かり、その場所をデバイス固有の方法でサニタイズできる場合
(2) 鍵のコピーの所在がわかる場合
(3) 鍵は多重に暗号化（ラップ）されることがある。ラップしている場合はラップ

鍵もサニタイズする必要がある

Cryptographic Erase は 2014 年の改訂（Revision 1）で追加された新しい項目で、他の文献の参照はなく本文献固有の説明である。

4.3.1.4.19 NISTIR 7956 (Cloud)

本文献は、クラウドアーキテクチャの IaaS/PaaS/SaaS ごとに鍵管理に関するセキュリティ要件と課題、課題の解決策が詳細に述べている。他の文献の参照はなくクラウド環境固有の鍵管理を説明していて、クラウド環境では情報と管理が複数のアクターに分離しているため状況が複雑である点を強調している。アクターにはサービス利用者(Cloud Consumer)、サービス提供者(Cloud Provider)、サービス利用者とサービス提供者の交渉をするアクター(Cloud Broker)、監査機関(Cloud Auditor)、サービス提供者からサービス利用者への接続と転送を仲介するアクター(Cloud Carrier)がある。サービス利用者が鍵を自分で管理したくてもストレージは物理的/論理的にサービス提供者の管理下にあるため、サービス利用者が期待できる安全保障には限界があると述べている。

4.3.1.4.20 X.509

本文献は、PKI の X.509 証明書の証明書ポリシー（CP）と認証実施規定（CPS）作成時に検討すべき論点を提供している。証明書ポリシー（CP）とは証明書がどのようなコミュニティまたはアプリケーションに使うことができるかの要件で、証明書の中に指定される。認証実施規定（CPS）は、CA が宣言する証明書の発行・管理・失効・更新・再作成の実施内容である。本文献では証明書の申請・発行・失効等のライフサイクルごとに、証明書発行 CA や利用者が検討すべき項目を挙げている。

4.3.1.4.21 SSH

本文献は、SSH サーバの構築と運用の担当者向けにセキュリティ設定の手順が説明されている。鍵管理に関しては、以下の 2 点を推奨している。

(1) 秘密鍵ファイルにパスフレーズを付けること

(2) 秘密鍵ファイルは SSH サーバ上に置かない

4.3.2 ワークショップの調査

NIST で鍵管理のワークショップ「Cryptographic Key Management Workshop」が 4 回開催され、鍵管理のフレームワーク(SP800-130)とフレームワークを基にした連邦政府向けの鍵管理プロファイル(SP800-152)が作られた。

日付	**SP 800-130 (Framework)**	**SP 800-152 (Federal)**
2009/6/8-9	鍵管理ワークショップ(1 回目) ・NIST や企業の発表者が各自のテーマで発表	―
2010/6/15	SP 800-130 ドラフト第 1 版 作成 ・6 章以降のフレームワーク本体は、この後大きな改訂なし	―
2010/9/20-21	鍵管理ワークショップ(2 回目) ・SP800-130 ドラフト第 1 版の議論	―
2012/4	SP 800-130 ドラフト第 2 版 作成 ・ポリシーの説明を追加	―
2012/8		SP 800-152 ドラフト第 1 版 作成
2012/9/10-11	鍵管理ワークショップ(3 回目) ・SP 800-130 ドラフト第 2 版と SP 800-152 ドラフト第 1 版の議論 ・連邦政府の将来のセキュリティ製品の課題の議論	
2013/8/15	SP 800-130　発行 ・フレームワークとプロファイルの違いを追加	―
2014/1	―	SP 800-152 ドラフト第 2 版 作成
2014/3/4-5	―	鍵管理ワークショップ(4 回目) ・SP800-152 ドラフト第 2 版の各章のレビュー
2014/12	―	SP 800-152 ドラフト第 3 版 作成
2015/10/28	―	SP 800-152 発行

4.3.2.1　2009 年鍵管理ワークショップ(1 回目)

2009 年に以下を目的として鍵管理ワークショップが開催され、NIST や企業の発表者が各自のテーマで発表を行った。

(1) 将来のコンピューター環境や商用アプリケーションがどのようになるか認識し、それらの安全性を満たすために必要な鍵管理の技術が何か知ること
(2) 効率的な暗号技術を用いた将来の環境のための鍵管理の設計フレームワークの作成について議論すること
(3) 開発、標準化、実用時の計画の基礎を築くこと

2010 年に鍵管理のフレームワーク(SP800-130)のドラフト第 1 版が出され、ワークショップの議論の一部（ポリシーの階層構造や CKMS の使いやすさ）が反映された。

ワークショップのまとめの文献には、すべての発表のハイライトが下記 15 個の項目にまとめられている。

(1) ポリシー

・鍵管理のライフサイクルでは、ポリシーとワークフローが継続し、すべてのコンポーネントが適切に統合されなければならない。商用の暗号ポリシーは包括的で、証明書、鍵、アルゴリズム、有効期間、複数の人によるコントロールなど、幅広いコンポーネントをカバーする必要がある。

・鍵管理フレームワークはポリシー、コンポーネント、保証の一般的な情報を定義および提供する。

・組織は、組織のポリシーや要件、制約をフレームワークに入力してその組織用の鍵管理ポリシーを作成する。

(2) 信頼

・信頼はエンティティの質で、エンティティに高いレベルの信頼があれば求められるセキュリティ対策は少ない。

・通信するパーティは、共通のセキュリティポリシーに基づいた信頼レベルを用いる。

・通信の両方のパーティが正確な情報と保証を得られることが平等な情報交換で、トランザクションは再実行されないことが必要。

(3) 障害

・特許や知的財産権を侵害する場合、標準化は難しい。

・信頼された環境の中で利用者と管理者が人間系でやりとりする必要があるため、鍵管理の中では利用者登録がもっとも費用がかかり難しい。

・手動の鍵の分配や鍵の置き換え、失効リストの更新も問題。合理的に少ない手順で行える必要がある。

(4) 可用性

・鍵管理はユーザのニーズを知ることから始める。

・ユーザにとってセキュリティは本業務ではないので、トレーニングなしで利用できるようにする。

・今の鍵管理に代わるアプローチも検討する（ID ベース鍵管理など）

(5) スケーラビリティ

・鍵管理のスケーラビリティは利用者数の拡大やシステムのグローバルな利用のこと。

・ユーザは失効リストをメンテナンスしないことがベンダから見たユーザの問題である。

(6) インターフェース

・鍵管理システムのインターフェースには、鍵管理(KM)-組織、KM-管理者、KM-ユーザ、KM-通信チャネル、KM-ストレージ、KM-アプリケーションがある。

・ID ベース鍵管理(IDKM)の利点は、ユーザ ID の認証が復号時にできることと、鍵の生存期間が短いこと、新規の公開鍵が無料で作成できること、ID と鍵の紐づけの時間が短いことである。

(7) アルゴリズム

・閾値暗号は、暗号化データ保管アクセスに有用。

・鍵管理の問題は、弱い疑似乱数生成、アプリケーションに鍵がハードコーディングされること、証明書の認証、鍵が期間内に更新されないこと、鍵とパスワードがストレージ内や通信で暗号化により保護されていないことである。

(8) 鍵種別

・製造元はデバイスに秘密鍵やデバイス証明書を埋め込んで出荷する。これによりデバイス同士が認証できる。

(9) 鍵のライフサイクル

・2010/12/31 まで 80bit セキュリティが有効で、その後 NIST は最小 112bit セキュリティを推奨している。

・クラウド環境では、鍵管理をインフラ側が行うケースと、アプリケーションが行うケースがある。

(10) 鍵のメタデータ

・証明書の期間がいつ切れるか、切れたときに何をすべきか、誰を CKMS の管理者にすべきか、情報が漏洩した場合に情報が暗号化されていたか、鍵管理は自動化されているか手動か、どの暗号アルゴリズム/プロトコル/インターフェースが使われているかが課題である。

(11) 標準化

・鍵管理の領域の標準化の組織には、NIST、IETF、ANSI、ISO、OASIS がある。
・証明書の登録の標準化の以前の試みは失敗した。
・鍵生成、分配、アカウント管理、破棄、商用実装、鍵のフォーマットは少し標準がある。

(12) 要件・推奨
・既存のシステムに実装できる自動 CKM システムが必要。その要件は、 1）認証された/許可された鍵の配布、2）鍵の長期間の保管、3）必要に応じて鍵を交換/更新するシステム、4）鍵の作成を集中化してはならない、5）操作は少ないこと。このタイプの KM システムの候補は、Kerberos（セッション鍵用）、OASIS（ストレージ鍵用）または GDOI（グループ鍵管理用）。
・個人の認証には複数の識別子による多重認証が必要。属性証明書がサポートされるべき。
・役割ベースの認証が必要。

(13) 新しい技術
・クラウドで使われる仮想マシンはコピーされたり移動したり停止したりするので、簡単に信頼できない。クラウドの鍵管理システムで鍵を安全に通信するためにクラウドの中に信頼できる部分が必要。
・耐量子コンピューターのアルゴリズムやスキームに注目する。
・ID ベース共通鍵暗号は共通鍵の鍵配布の問題を減らすことができる。

(14) フレームワーク
・フレームワークには各コンポーネントの特性を述べる。
・SP800-57 からスタートするのがふさわしい。

(15) アプリケーション
・暗号機能は、完全性と認証のメカニズムで特に重要である。

4.3.2.2　2010 年鍵管理ワークショップ(2 回目)
2010 年のワークショップでは、SP800-130 (Framework)ドラフト第 1 版をもとにフレームワークとプロファイルについて議論が行われた。議論の結果は以下の通り。

(1) フレームワーク
・読者を設計者、オペレーター、セキュリティアーキテクトに狭める。

・プロファイルや CKMS 設計がフレームワークの要件を満たしているか検証できるようにする。
・フレームワークとプロファイルは技術、イノベーション、新しいアプリケーションを制限すべきではない。
[セキュリティポリシーについて]
・ポリシーを決める際は、組織の目的からスタートする。
・要件は、ポリシーから導出される。

(2) プロファイル
・フレームワークとプロファイルの違いを定義する。
・鍵の使われ方によって、プロファイルが定まる。
・鍵が保護しているデータの機密性とリスクに対する CKM 要件の依存性を明確にする。
・仕様と技術のギャップ（例えば、鍵のアーカイブ）を特定する。

ワークショップの結果を受け、2012 年に出されたドラフト第 2 版には 2 章「フレームワークの基本」と 4 章「セキュリティポリシー」に説明が追加された。セキュリティポリシーでは特にセキュリティドメインの概念が導入された。

4.3.2.3　2012 年鍵管理ワークショップ(3 回目)

2012 年のワークショップでは、1 日目に SP800-130(Framework)のドラフト第 2 版と SP800-152(Federal)のドラフト第 1 版のレビューが行われ、2 日目は連邦政府システムの将来のセキュリティ製品とサービスに向けた課題に焦点があてられた。

4.3.2.3.1　SP800-130 ドラフト第 2 版のレビュー

(1) 歴史的観点
- 鍵配布は人手が必要なのでコストがかかる。コストを下げる方法が今の課題。
- 今の公開鍵システムは今後、量子コンピューターの影響を考える必要がある。

(2) SP800-130(Framework)のドラフト第 2 版の概要説明
- 調達担当者は、対象製品の設計書がフレームワークに準拠しているか判断することにより、対象製品や競合製品の機能の有無をチェックすることができる。
- 各トピックのすべての要件は設計書に書かれるべきだが、機能を CKMS の設計に含めるか否かは設計者の判断次第。

・ 政府組織は自分が入るセキュリティドメインを選択する。グループにセキュリティポリシーを定義することによりセキュリティドメインを作ることができる。組織が複数のセキュリティドメインに入っていることもある。
・ オペレーターは、緊急事態を含む多くの状況で何をすべきかを知る必要がある。CKMS 設計者は、CKMS の動作のさまざまな異常を評価し、各状況で何をすべきかに関するガイダンスを提供する必要がある。 CKMS 設計文書には、どのような潜在的な異常が調査されたか、どのような回避メカニズムが CKMS 設計に含まれているかを述べるべきである。

(3) SP800-130(Framework) のドラフト第 2 版へのコメント

・ フレームワークとプロファイルの違いをもっと説明すべき。

SP800-130(Framework)は、ワークショップの結果を受けて 2 章にプロファイル及びフレームワークとプロファイルの違いの説明が追加され、2013 年に初版が発行された。

4.3.2.3.2 SP800-152 ドラフト第 1 版のレビュー

SP800-152(Federal)のドラフト第 1 版には、SP800-130(Framework)の主要な要件(FR:)に対する連邦政府のプロファイルが表形式で示されている。連邦政府のプロファイルは、基本的な要件、高いセキュリティが要求される場合の要件、オプションの要件の 3 段階で書かれている。

SP800-152(Federal)ドラフト第 1 版のレビューでは以下の議論が行われた。

・ 質問 : フレームワークからプロファイルを作成する際は、アルゴリズムや機能が制限されるのか追加されるのかどちらか？
回答：プロファイルは他のアルゴリズムやメカニズムを追加できるが、その使い方は連邦政府用に制限されるだろう。
・ 異なる領域（健康領域や金融領域）では異なるプロファイルと異なるセキュリティドメインが使われる。
・ 各領域の中にはプロファイルの要件のいくつかのレイヤーが存在するので、各領域はポリシーや要件、CKMS 仕様の階層構造を持つ。
・ Accountability(責任追跡性)と匿名を同時に満たすことは困難。

4.3.2.3.3 連邦政府システムの将来のセキュリティ製品とサービスに向けた課題

2012 年のワークショップでは、下記の連邦政府システムの将来の鍵管理の課題についても議論された。

(1) 鍵管理の課題

・ ドメインを超えた相互運用が課題。連邦政府の PKI の経験では、証明書のクロス証明は大変困難だった。
・ 匿名化が課題。鍵管理の目的は正しい鍵を正しい人に渡すことで人の検証が必要。
・ 通常、異なるアプリケーションには異なる CKMS が必要。
・ CKMS のスケーラビリティが難しい問題。

(2) 鍵管理の基盤としてのセキュリティポリシー
・ セキュリティポリシー仕様の言語形式、自動化されたセキュリティポリシー言語プロセッサ、自動化されたセキュリティポリシー実行システムの利用の勧め。
・ 異なるセキュリティドメイン間の情報共有に関するポリシーと、セキュリティドメインの複数のレベルについて議論された。

(3) ユーザ認証におけるプライバシーと鍵管理のバランス
・ 個人のプライバシーと Accountability(責任追跡性)の衝突に関する議論
・ 暗号は Accountability とプライバシーを両方提供できるが、匿名性とプライバシーを解決できないという矛盾がある。
・ 人の識別を知ることなしに人の行動をリンクするアプローチが提案されている。
・ 匿名の認証情報を失効させる方法として、Dynamic accumulator が説明されている。

(4) 無線/モバイルアプリケーションの課題
・ モバイルは移動する際に接続している基地局の切り替えが発生するが、従来のモバイルネットワークでは接続の認証鍵の受け渡しの基盤で切り替えを実現している。切り替え前後のリンクが異なるセキュリティドメインや異なる無線技術を採用している場合があり、さらに異なる認証プロトコルだと鍵の階層構造が異なり、鍵の受け渡しに課題がある。
・ 解決のアプローチ：鍵の分離、異なるネットワークに同一の認証情報を使用する、メディアに依存しない鍵配布のサービスを使う。

(5) クラウド環境の鍵管理
・ クラウド環境の要件：ユーザと管理者の認証、通信保護、共有環境でのデータのパーティションと保護。

・ 暗号はデータの機密性（サービス提供者に対しても)、データの完全性を提供すべき。

(6) ランダムビット生成(RBG)

・ SP800-90 シリーズの概要

(7) 安全な鍵の保管と真の乱数生成

・ 電源オンの時にデバイス固有の値から鍵を生成すれば、鍵を保管する必要がなくなる。
・ PUFs(Physically Unclonable Functions)は、刺激に対してデバイス固有の方法で予測できない動きをするので、乱数生成に使える。

(8) 可用性

・ システムが複雑だとユーザは利用を避けるか正しく使わない。初回の”使いやすい”経験が重要。

(9) ドメイン間の相互運用

・ クロスドメインのセキュリティの課題：信頼の構築、鍵のオーナーシップ、鍵の保管と通信の保護、鍵ポリシーの通知、鍵ポリシーの交渉、鍵へのアクセス管理、鍵のライフサイクルの管理、所有の証明。
・ 量子鍵配布(Quantum Key Distribution ： QKD)：量子チャネルは一方向チャネル、認証されたクラシカルなチャネルは両方向、目標は、最終鍵を作成すること。
・ 量子鍵配布は 5 年以内に開発されるだろう。量子鍵配布は有効な技術で、チャネル内の情報の損失は盗聴者に起因する。

(10) 認証情報の保護

・ モバイルデバイスには耐タンパ性の高いストレージがないため、デバイス内の認証情報の保護が課題。

4.3.2.4 2014 年鍵管理ワークショップ(4 回目)

SP800-152(Federal)は、ドラフト第 1 版の表形式から SP800-130(Framework)と同様の章立ての連邦政府向けプロファイルの文章に書き換えられたドラフト第 2 版が 2014 年に作成された。2014 年のワークショップではそのドラフト第 2 版の各章のレビューが行われた。ワークショップの後、2014 年 12 月にドラフト第 3 版が作成され、2015 年 10 月に SP800-152(Federal)が発行された。

議論の内容やまとめの資料は公表されていないため、発表スライドの項目を以下に記す。

[イントロダクション　1〜3 章]

・プロファイル、スコープ、目的、読者

・フレームワーク要件、プロファイル要件、プロファイル拡張、プロファイル機能

・フレームワークとプロファイルの構造と違い

[基本概念、セキュリティのポリシーと役割　4、5 章]

・FCKMS(Federal CKMS)と CKMS

・FCKMS モジュール

・セキュリティポリシー

・セキュリティドメイン

・役割

[安全なアーキテクチャ　6 章と 10 章]

・鍵とメタデータの保護と管理機能

・アクセスコントロール

・情報漏洩の回復

・災害からの回復

・ネットワーク設定

[アプリケーション]

・Email

・モバイル

・クラウドのセキュリティ

・鍵とメタデータの保管

・鍵確立

[対策とセキュリティ管理　6 章と 8 章]

・セキュリティ長

・FIPS 140-2 暗号モジュールのセキュリティレベル

・データの影響と機密レベル(FIPS 199、FIPS200、FIPS800-53)

・低中高の要件

・セキュリティ管理

[テスト、評価、検証　9 章と 11 章]
・テストの種類
・維持
・FIPS 199、FIPS 200、 SP 800-53
・アセスメント
・検証

[相互運用と移行　7 章]
・相互運用のデフォルトと推奨
・移行

4.3.3　中間報告会での有識者の議論

中間報告会での有識者の鍵管理に関する議論は以下の通り。

(1) 暗号鍵の運用ではハードウェアセキュリティモジュール(HSM)を利用するので、鍵管理ガイドラインには HSM や FIPS140-2（暗号モジュールのセキュリティ要件）の内容を含めた方がよい。
(2) 鍵管理システム構築のガイドラインと鍵管理の運用のガイドラインを分けずに一般的なガイドラインを記述するのは難しいだろう。全体像は必要だが、読者や対象のフェーズは絞り込んだ方がよい。
(3) 鍵を管理する対象のアーキテクチャを明確にすべき。PKI のように明確なアーキテクチャの中の鍵管理はガイドラインの記述ができるが、対象のアーキテクチャが定まっていないとガイドラインの記述は困難だろう。
(4) 公開鍵系は仕様が公開されていてプラクティスも知られているが、共通鍵系は情報が外に出てこない。共通鍵のシステムを開発しているチームの中にはナレッジがあるのだろう。
(5) 暗号の技術者の裾野が広がって専門家以外が鍵管理のシステムを開発すると知識がなく危険。ガイドラインを作る意義がある。
(6) 今回調査した文献の中では SP800-130(Framework)がポリシーの階層構造を分析していて良い文献。
(7) 個人情報保護委員会のガイドライン案の中の「高度な暗号化等の秘匿化がされている場合」の鍵管理も確認した方がよい。EU の個人情報保護の規則 GDPR（General Data Protection Regulation）も注目されている。個人情報漏洩の話は鍵管理に行きつく。
(8) 近年の技術動向を考えると、IoT の鍵管理のガイドラインが必要。

リストガイドは SP800-57 Part 1(General)を参考にしているが、リストガイド発行(2010 年)以降も SP800-57 Part 1 は 2011 年と 2015 年に改訂されているため、リストガイドも変更する必要があるか否かの調査依頼があった。そのため、SP800-57 Part 1 Appendix D (附属書 D)の改訂履歴の 2011 年と 2015 年の改訂のうちリストガイドに影響する項目があるか調査を行った。リストガイドの変更が必要または反映すべきか検討が必要な項目を下表に示す。文言変更や参照の追加など軽微な変更は除外する。

・ 2011 年の改訂

No	**Part1 章・節**	**改訂内容**	**反映**	**リストガイドへの影響**
3	Sec 2.1	鍵導出関数、鍵導出鍵、鍵長、鍵サイズ、乱数ビット生成器および利用者の定義が追加された。アーカイブ、鍵管理アーカイブ、鍵回復、ラベル、所有者、プライベート鍵、保有の証明、公開鍵、データのセキュリティ寿命、シード値、共有秘密、及び“should”等の定義が修正された。暗号モジュールの定義が削除された。	必要	2 章　用語の定義の表を更新する。
11	Sec 5.3.1	要員交替が追加のリスク要因に追加された。	要検討	リストガイドの「個別暗号鍵の有効期間の設計指針」の"個別の暗号鍵の有効期間の設計は、鍵の種類、用途、運用環境、利用している暗号アルゴリズムなど、様々な要因によって左右される。"に要員交替を追加するか否か。
12	Sec 5.3.4	公開鍵の暗号期間と証明書の有効期限の間の違いを明確化するよう記述が挿入された。	要検討	リストガイドの公開鍵の「個別暗号鍵の有効期間の設計指針」に反映するか否か。
15	Sec 5.5	CA の署名用プライベート鍵の危殆化についての記述が追加され、そのような事象の取り扱いについてのアドバイスが提供された。	要検討	リストガイドの「3.6 鍵が漏洩した場合のリスクを低減する方法」の手段のリストに"特に CA 鍵が危殆化した場合における、危殆化回復計画の

No	Part1 章・節	改訂内容	反映	リストガイドへの影響
				作成。"を追加するか否か。
18	Sec 5.6.5	この新しいセクションは、計算能力または暗号解析の進歩によるセキュリティ強度の低下と関連する影響に対処するために追加された。	要検討	リストガイドに、追加されたセキュリティ強度の低下を追加するか否か。
24	Sec 8.2.4	本セクションは SP 800-56A、SP 800-56B、SP 800-56C、SP 800-108 および SP 800-132 と一貫するよう改訂された。	要検討	リストガイド 4.2.2 の訳に反映するか否か。
25	Sec 8.3.1	表 9 は静的鍵共有用鍵をアーカイブすることが許容されることを示すように修正された。	要検討	リストガイド表 4, 5 に影響があるか否か
26	Sec 8.3.1 付属書 B.3	アーカイブが鍵の暗号期間の終了後にのみ実行されるような表現（例．鍵は活性化において直ちにアーカイブされる可能性がある）、およびアーカイブにおける鍵は履歴としての意図でのみのためにあること（例. それらは鍵の暗号期間の後データを復号する必要とされるかもしれない）を削除した。	要検討	リストガイド 4.4.1 の記述に影響するか否か
27	Sec 8.3.3	危殆化した鍵および危殆化していない鍵の登録抹消についての議論が修正された。	要検討	リストガイド表 3, 7 に影響するか否か
28	Sec 8.3.5	PKI および対称鍵システムに関する失効がどのように達成されるかについての議論が追加された。	要検討	リストガイド 3.5.2 に影響するか否か

・ 2015 年の改訂

No	Part1 章・節	改訂内容	反映	リストガイドへの影響
4	Sec 2.1	アルゴリズム作成者の使用期限、	必要	リストガイドの「2 章　用語

No	Part1 章・節	改訂内容	反映	リストガイドへの影響
		アーカイブ、認証、認証コード、認証局、DRBG、デジタル署名、鍵導出、鍵暗号化用鍵、鍵管理方針、鍵配送、鍵更新、鍵ラッピング、鍵ラッピング用鍵、メッセージ認証コード、否認防止、所有者、受領者の使用期限、RBG シード値、セキュア通信プロトコル、セキュリティサービス、署名生成、署名検証、情報源認証、およびトラストアンカーの定義を修正した。データ暗号化用鍵、アイデンティティ認証、完全性認証、完全性保護、鍵導出方法、鍵長、NIST 標準、情報源認証の定義を追加した。鍵属性と作業の定義を削除した。		の定義」を更新する。
7	Sec 3 および文書全体	完全性認証または情報源認証のいずれかについてのより多くの明確にするために認証についての説明。アイデンティティ認証は、情報源認証と見なされる。	要検討	リストガイドの「技術の利用モデル」の"認証"を完全性認証と情報源認証に分けて説明するか否か。
8	Sec 3.3	完全性認証または情報源認証について明確化するための書き換え。	要検討	リストガイドの「技術の利用モデル」の"認証"を完全性認証と情報源認証に分けて説明するか否か。
10	Sec 3.5	否認防止のより現実的な議論、即ち、実際の否認防止の提供よりも、否認防止のサポートについての議論、の提供のための書き換え。否認防止のサポートを説明するために書き換えられた文書における否認防止への参照。	要検討	リストガイドの「技術の利用モデル」の"否認防止"に、追加された説明を加えるか否か。
24	Sec 5.3.1	リスト内の量子コンピューターへの参照を追加。	要検討	リストガイドの「個別暗号鍵の有効期間の設計指針」の"個

No	Part1 章・節	改訂内容	反映	リストガイドへの影響
				別の暗号鍵の有効期間の設計は、鍵の種類、用途、運用環境、利用している暗号アルゴリズムなど、様々な要因によって左右される。"に"新しい破壊的技術からの情報への脅威（例. 量子コンピューター）"を追加するか否か。
25	Sec 5.3.4	非対称鍵ペアの作成者の使用期限と受領者の使用期限について議論するために書き換え。	要検討	リストガイドの公開鍵の「個別暗号鍵の有効期間の設計指針」に反映するか否か。
29	Sec 5.4.4	SP800-89 で議論されたので、プライベート鍵所持の保証の取得についての詳細が削除された。この保証が CA によって取得される可能性があるという注釈が追加された。	要検討	リストガイドの「3.2.2 登録局 RA および認証局 CA への申請」に追加するか否か。
36	Sec 6.2.1.3	追加のガイダンスが鍵構成要素の生成について追加された。	要検討	リストガイドの「5.1.3　守秘性」に、追加された説明を加えるか否か。
37	Sec 6.2.2.1	鍵の可用性が求められないような場合について記述パラグラフが追加された、および暗号学的無害化（サニタイズ）を説明するような刊行物への参照を提供。	要検討	リストガイドにサニタイズを追加するか否か。
43	Sec 8.1.5.1	1 つの文章が、組織のサブエンティティへの鍵材料の配付について、第 2 段落の最後に追加された。	要検討	リストガイドに組織のサブエンティティへの鍵材料の配付について追加するか否か。
44	Sec 8.1.5.1.1.1	トラストアンカー（即ち、認証局、その認証局用の証明書ではなく）とは何かについてより明確に、正確に記述するために、改訂された。	要検討	リストガイドに、追加されたトラストアンカーの説明を加えるか否か。
46	Sec 8.1.5.2	鍵変更のための承認された方法として鍵更新の使用への参照が削除	要検討	No 51 と同様

No	Part1 章・節	改訂内容	反映	リストガイドへの影響
	8.1.5.2.2 8.2.3.2	または修正された。		
50	Sec 8.2.1.1 8.2.1.2	適切な参照は暗号モジュールなので、“デバイス”の記述が削除された。	要検討	リストガイドの「鍵の保存手順」の"デバイス"を削除するか否か。
51	Sec 8.2.3.2	SP 800-152 で述べるように、鍵更新は現在許可されていない。 【補足】 「8.2.3.2 Key Update Function」に "Federal applications shall not use key update (also, see [SP800-152])." が追加された。 “key update”は8.2.3.2で定義された機能で、鍵を変更する時に古い鍵から作られた鍵で置き換える方法である。	要検討	リストガイドの「3.4.2 鍵の変更」「4.4.2 鍵の変更」に反映するか否か。
52	Sec 8.3.1	アーカイブの使用におけるさらなるガイダンスが提供された。	必要	リストガイドのアーカイブの表の「認証用共通鍵」の保有期間に"アイデンティティの認証"を追加する。
53	Sec 8.3.4	破棄された鍵を含むメディアの破壊ではなく鍵の破棄について説明するために文章が修正された。	必要	リストガイドの記述において、消去対象をメディアから鍵に変更する。