CRYPTREC-MT-1011-2018

資料１

2018 年度 暗号技術検討会

平成３１年３月２９日
１０：００～
経済産業省別館１１階
１１１１各省庁共用会議室

議事次第

１．開会

２．議事

（１） 2018 年度 暗号技術評価委員会 活動報告について【報告】
（２） 2018 年度 暗号技術活用委員会 活動報告について【報告】
（３） 次期 CRYPTREC 暗号リストの改定に向けた検討について【審議】
（４） 「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」の設置について【承認】
（５） 暗号技術検討会　2018 年度　報告書（案）について【承認】

３．閉会

配付資料一覧

資料１	議事次第・配付資料一覧
資料２	暗号技術検討会　構成員・オブザーバ名簿
資料３	2018 年度 暗号技術評価委員会 活動報告
資料３別添１	2018 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料３別添２	耐量子計算機暗号の研究動向調査報告書（案）
資料４	2018 年度 暗号技術活用委員会 活動報告
資料４別添	鍵管理システム設計指針（基本編）　ドラフト素案
資料５	次期 CRYPTREC 暗号リストの改定に向けた検討について
資料５別添	「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」の設置について（案）
資料６	暗号技術検討会　2018 年度　報告書（案）
参考資料	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）

以上

資料２

暗号技術検討会　構成員・オブザーバ名簿

2019.3.29 現在

（構成員）

	今井　正道	一般社団法人情報通信ネットワーク産業協会　常務理事
	上原　哲太郎	立命館大学　情報理工学部　教授
	宇根　正志	日本銀行　金融研究所　情報技術研究センター　情報技術研究グループ長
	太田　和夫	国立大学法人電気通信大学大学院　情報理工学研究科　教授
	岡本　龍明	日本電信電話株式会社　セキュアプラットフォーム研究所 暗号理論研究室　フェロー
	高木　　剛	国立大学法人東京大学大学院　情報理工学研究科　教授
	近澤　　武	独立行政法人情報処理推進機構　セキュリティセンター セキュリティ技術評価部暗号グループ　主任研究員
	手塚　　悟	慶應義塾大学大学院　政策・メディア研究科　特任教授
	本間　尚文	国立大学法人東北大学　電気通信研究所　教授
	松井　　充	三菱電機株式会社　開発本部　役員技監
	松浦　幹太	国立大学法人東京大学 生産技術研究所　教授
座長	松本　　勉	国立大学法人横浜国立大学大学院　環境情報研究院　教授
	松本　　泰	セコム株式会社　IS 研究所 コミュニケーションプラットフォームディビジョン　マネージャー
	向山　友也	一般社団法人テレコムサービス協会　技術・サービス委員会　委員長
	渡邊　　創	国立研究開発法人産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 副研究センター長

（五十音順、敬称略）

（オブザーバ）

一ノ瀬　宏昭	内閣官房内閣サイバーセキュリティセンター 内閣参事官（政府機関総合対策担当）
三原　祥二	個人情報保護委員会事務局　参事官
吉田　和彦	警察庁　情報通信局　情報管理課　情報セキュリティ対策官
小高　久義	総務省　行政管理局　行政情報システム企画課　情報システム管理室長
阿部　知明	総務省　自治行政局　住民制度課長
宮崎　拓也	法務省　民事局　商事課長
髙橋　良明	外務省　大臣官房　情報通信課長
下井　善博	財務省　大臣官房　文書課　業務企画室長
竹田　和彦	文部科学省　大臣官房　政策課　情報システム企画室長
原口　剛	厚生労働省　大臣官房参事官（サイバーセキュリティ・情報システム管理担当）
中野　宏和	経済産業省　産業技術環境局　国際電気標準課長
二宮　　勉	防衛省　整備計画局　情報通信課　サイバーセキュリティ政策室長
宮崎　哲弥	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長
寶木　和夫	国立研究開発法人産業技術総合研究所　情報技術研究部門　副研究部門長
瓜生　和久	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長
大澤　昭彦	一般財団法人日本情報経済社会推進協会　電子署名・認証センター長
和田　雅昭	公益財団法人金融情報システムセンター　監査安全部長

（敬称略）

資料３

2018 年度暗号技術評価委員会活動報告

1. 活動目的

CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記の通り、暗号技術の安全性に係る監視・評価 及び 実装に係る技術の監視・評価を実施した。

① CRYPTREC 暗号等の監視

国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）に関する監視を行い、会議や ML を通して報告する。

- 「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の更新を行う。
  - ○ T.Kleinjung 氏および A.K.Lenstra 氏に計算量見積もりの主要部分の評価を依頼し、素因数分解の困難性に関する計算量の再評価を実施した。評価レポートは、CRYPTREC ホームページに公開予定。
    (資料 3 別添 1)

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

○ 今年度対象となる方式はなかった。

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

○ 監視活動を実施していたが、特に注意喚起レポートを発行する事象は、発生しなかった。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討する。

○ 暗号利用モード(秘匿モード) として、XTS の安全性評価を行うため、外部評価を実施し、XTS モードは、利用条件を満たす範囲においては、十分な安全性を有すると判断した。次年度以降に実装評価を予定している。

⑤ 新技術等に関する調査及び評価

将来的に有用になると考えられる技術やリストに関わる技術について、安全性・性能評価を行う。必要に応じて、暗号技術調査ワーキンググループによる調査・評価、または、外部評価による安全性・性能評価などを行う。

- 暗号技術調査ワーキンググループ（暗号解析評価）を継続し、主に、Post-Quantum Cryptography（耐量子計算機暗号）の技術動向を調査・執筆し、技術報告書として公開する。また、一般数体篩法における篩処理の計算量の評価について、再評価を実施する。

○ 暗号技術調査ワーキンググループ(暗号解析評価)を実施

Post-Quantum Cryptography(耐量子計算機暗号)の技術報告書を完成させた。4 月上旬に CRYPTREC ホームページに公開予定。

「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の更新を検討した。近年の計算機の性能向上が鈍化傾向にあることを踏まえ、この傾向を予測図にどのように反映するかについては慎重に検討する必要があるという意見があり、予測図の更新については、次年度継続検討を行うこととした。

(資料 3 別添 1、別添 2)

○ CRYPTREC における耐量子計算機暗号への対応や次期 CRYPTREC 暗号リストに向けた方針について議論を行った。

(2) 暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）

暗号技術を利用する際の技術面での注意点に関する調査、新技術の安全性・性能に関する調査・評価を行った。

○ Post-Quantum Cryptography(耐量子計算機暗号)の技術報告書を完成させた。4 月上旬に CRYPTREC ホームページに公開予定。

3. 開催状況

暗号技術評価委員会は、下記のとおり 2 回開催した。

表 1 暗号技術評価委員会開催状況

回	開催日	議案
第 1 回	2018 年 7 月 19 日	● 暗号技術評価委員会活動計画の具体的な進め方の検討 ● 暗号技術調査ワーキンググループ(暗号解析評価)の活動計画案の検討 ● XTS モードの安全性評価について外部評価実施の検討 ● CRYPTREC における耐量子計算機暗号への対応について検討 ● 監視活動状況報告
第 2 回	2019 月 3 月 11 日	● 暗号技術調査ワーキンググループ(暗号解析評価)の活動報告 ● XTS モードの安全性評価に関する外部評価レポート報告、および安全性評価検討 ● 次期 CRYPTREC 暗号リストに向けた方針の検討 ● 監視活動状況報告 ● CRYPTREC Report 2018(暗号技術評価委員会報告)の目次案提示 ● CRYPTREC シンポジウム概要案提示

4. 今後の予定

- Post-Quantum Cryptography(耐量子計算機暗号)の技術報告書は 4 月上旬に CRYPTREC ホームページに公開。
- 素因数分解問題の困難性に関する計算量の予測図の更新については、次年度継続検討。

以上

（参考資料）

委員構成

［暗号技術評価委員会］

委員長	太田　和夫	電気通信大学　　教授
委員	岩田　哲	名古屋大学　准教授
委員	上原　哲太郎	立命館大学　教授
委員	金子　敏信	東京理科大学　教授
委員	高木　剛	東京大学　教授
委員	手塚　悟	慶應義塾大学　特任教授
委員	本間　尚文	東北大学　教授
委員	松本　勉	横浜国立大学　教授
委員	松本　泰	セコム株式会社　ディビジョンマネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構　研究室長
委員	山村　明弘	秋田大学　教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所　副研究センター長

［暗号技術調査ワーキンググループ(暗号解析評価)］

主査	高木　剛	東京大学　教授
委員	青木 和麻呂	日本電信電話株式会社　グループリーダ
委員	草川　恵太	日本電信電話株式会社　研究主任
委員	國廣　昇	東京大学　准教授
委員	下山　武司	株式会社富士通研究所　主管研究員
委員	高島　克幸	三菱電機　主管技師長
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	九州大学　准教授

資料３別添１

2018 年度暗号技術調査 WG（暗号解析評価）活動報告

1. 活動目的・方針（2017 年度～2018 年度）

1.1. 耐量子計算機暗号の研究動向調査

近年、量子計算機が実用化されても安全性を保てると期待される暗号(耐量子計算機暗号:PQC)の調査・検討が各国で進められている。特に米国では NIST が PQC の公募を開始しており、欧州では ETSI が PQC の調査活動を行い、ISO/IEC でも標準化に向けた議論が始まっている。このように国内でも PQC の研究動向を把握する必要性がさらに高まっている。

2017 年度暗号技術評価委員会活動計画における「新技術等に関する調査及び評価」の活動として、PQC の技術動向を調査することが暗号技術検討会において承認された。暗号技術評価委員会では、暗号技術調査ワーキンググループ(暗号解析評価)を設置し、本調査を実施する。

- 耐量子計算機暗号（PQC）に関する近年の研究動向を調査し、報告書を作成する。（完成予定は 2018 年度末。）
- PQC の代表的な候補である、四つの分類（格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術）を調査対象とする。
- 上記の各分類において、該当する方式及び文献について三つの機能（暗号化、鍵交換、署名）の観点による整理等を実施する。

1.2. 予測図の更新

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関して CRYPTREC が例年公表している予測図の更新を行う。

2. 委員構成

主査：高木 剛(東京大学)
委員：青木 和麻呂(NTT)
委員：草川 恵太 (NTT)
委員：國廣 昇(東京大学)
委員：下山 武司(富士通研究所)
委員：高島 克幸(三菱電機)
委員：安田 貴徳(岡山理科大学)
委員：安田 雅哉(九州大学)

3. 活動概要（2017 年度～2018 年度）

3.1. 耐量子計算機暗号の研究動向調査

3.1.1. 主要なイベント等

- NIST PQC 標準化の公募では、締め切り(2017 年 11 月 30 日)までに、82 件の方式が提案され、そのうち 69 件が書類基準を満たし、その後、5 件の暗号方式が取り下げられた。
- NIST PQC 標準化プロジェクトにおいて提案された暗号方式の絞り込みが実施された（Second Round Candidates)。暗号方式は 26 件に絞り込まれ、2019 年 1 月 30 日にその候補リストが公開された。提案された暗号方式の安全性を 2018 年から約 5 年をかけて検証することが予定されている。

**This is a tentative timeline, provided for information, and subject to change.*

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
January 30, 2019	Second Round Candidates announced
August 22-24, 2019 *(tentative)*	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

（2019 年 3 月 1 日：
https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline）

3.1.2. 2017 年度第 1 回 WG での実施内容及び決定事項

- 調査対象とする四つの分類項目について担当者を決定した：

	とりまとめ委員	執筆者
導入	高木主査・事務局	高木主査、事務局
① 格子に基づく暗号技術	下山委員	下山委員、安田(雅)委員、青野（事務局）
② 符号に基づく暗号技術	草川委員	草川委員
③ 多変数多項式に基づく暗号技術	安田(貴)委員	安田(貴)委員
④ 同種写像に基づく暗号技術	高島委員	高島委員

- 四つの分類において、調査対象を具体的に何にするかは、担当のとりまとめ委員を中心に決

定する。

- 格子に基づく暗号技術及び符号に基づく暗号技術については 2014 年度の報告書との差分を整理する。

3.1.3. 2017 年度第 2 回 WG での実施内容及び決定事項

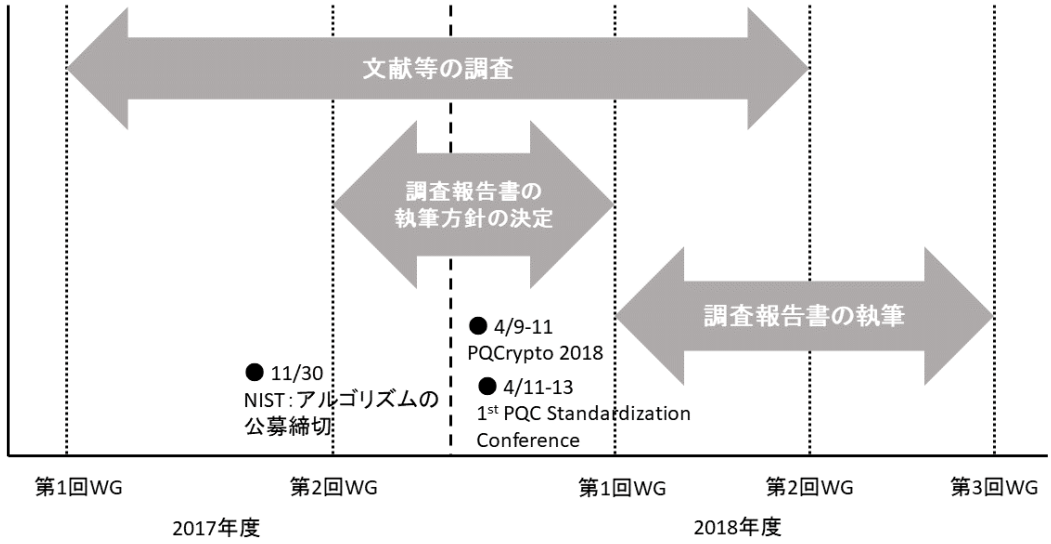
- スケジュールの修正について

  2018 年度は WG を 3 回実施する。

  2018 年度第 1 回 WG（6 月 27 日）：執筆方針を決定する。

  2018 年度第 2 回 WG（10 月）：報告書の中間報告。

  2018 年度第 3 回 WG（ 2 月）：報告書完成。



3.1.4. 2018 年度第 1 回 WG 及びその事前調整会議での実施内容及び決定事項

- 下記の日程で報告書の執筆方針（案）に関する事前調整会議を実施した。

  2018 年 5 月 23 日：主査打ち合わせ（導入の章）

  2018 年 6 月 11 日：執筆担当者打ち合わせ（符号に基づく暗号技術）

  2018 年 6 月 12 日：執筆担当者打ち合わせ（格子に基づく暗号技術）

  2018 年 6 月 14 日：執筆担当者打ち合わせ（多変数多項式に基づく暗号技術）

  2018 年 6 月 14 日：執筆担当者打ち合わせ（同種写像に基づく暗号技術）

- 事前調整会議での議論を基に、耐量子計算機暗号の研究動向調査報告書の執筆方針を決定した。

3.1.5. 2018 年度第 2 回 WG での実施内容及び決定事項

- 報告書（仮原稿）の各章について執筆担当者が説明し、WG にて加筆・修正について議論された。

3.1.6. 2018 年度第 3 回 WG での実施内容及び決定事項

- 報告書（最終版）の各章について執筆担当者が説明し、それらのおおよその内容が WG で了承された。報告書の微修正等の締め切りを 2019 年 3 月 15 日とし、発行日は同年 3 月、Web での公開日は同年 4 月 5 日とすることを決定した。

3.2. 予測図の更新

3.2.1. 2017 年度

- 素因数分解問題および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2017 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った。

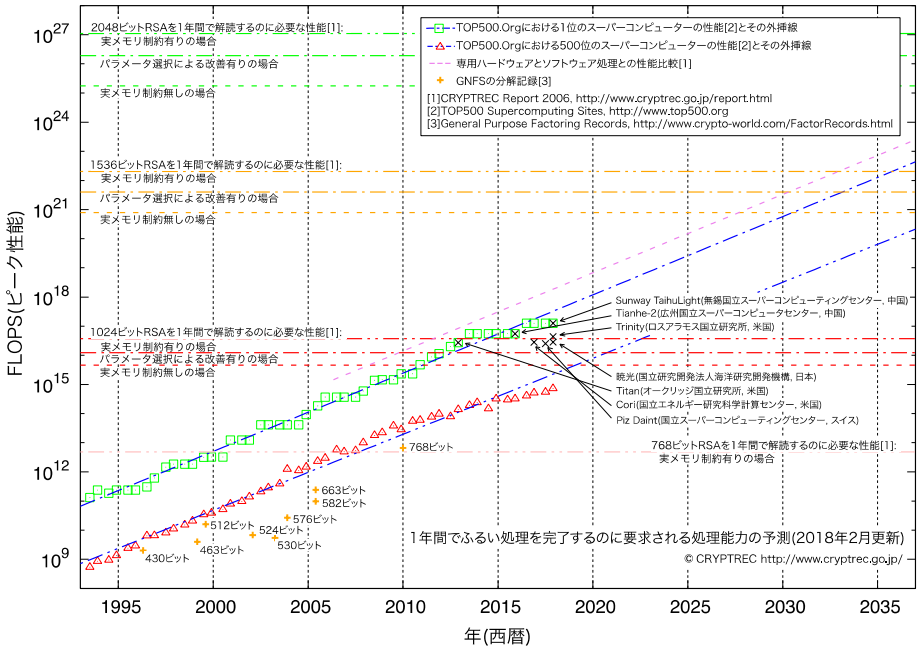


図 1: 素因数分解の困難性に関する計算量評価

(1 年間でふるい処理を完了するのに要求される処理能力の予測、2018 年 2 月更新)

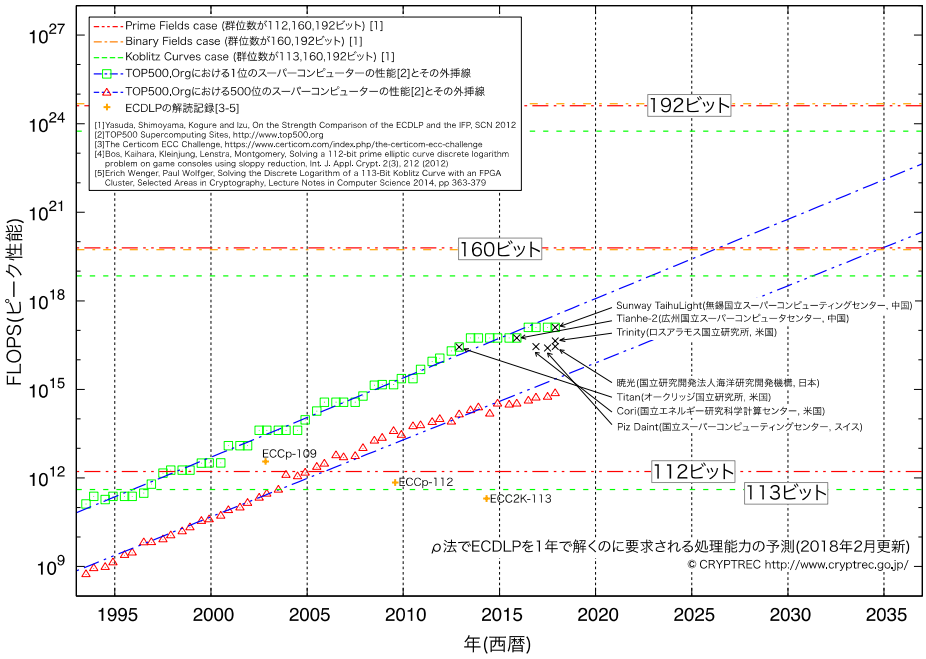


図 2: 楕円曲線上の離散対数計算の困難性に関する計算量評価

(ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2018 年 2 月更新)

3.2.2. 2018 年度

予測図の更新に関して、下記の（１）及び（２）について対応を行った。

（１） 素因数分解問題および楕円曲線上の離散対数問題の困難性に関する計算量の評価に大幅な変更がないかどうかの確認

- 素因数分解問題の困難性に関する計算量評価については、2006 年度に実施した評価結果[1]の更新を行う。

T. Kleinjung 氏及び A. K. Lenstra 氏に評価を依頼し、素因数分解を効率良く解くアルゴリズムとして知られている一般数体ふるい法において、計算時間の主要な部分を占める篩処理部分のソフトウェア評価の再評価を行った。評価結果は下記の表 1 の通りである。

以前の評価結果と比べて大幅な変更はないことが確認された。なお、評価レポート[1]は、技術報告書として Web 公開する予定である[2]。

表 1: 篩処理時間の推測結果（単位は、Intel Xeon E5-2680 v3 2.5 GHz コア・年）

法サイズ（ビット）	768	1024	1536	2048
見積もり	561.99	1.52×10^{6}	0.92×10^{12}	128×10^{15}

[1] Evaluation of complexity of the sieving step of the general number field sieve, T. Kleinjung and A. K. Lenstra, December 5, 2018

（２）素因数分解問題および楕円曲線上の離散対数問題の困難性に関する計算量及び計算機の処理性能の表示等についての検討

計算機の処理性能の表示等に対して、第一回暗号技術評価委員会において、下記の枠内のようなコメントがあった。

- 縦軸についても FLOPS でよいのかという点も含めて検討してもらいたい。
- 可能な範囲で計算機の専門家に協力してもらうなどの努力を重ねてもらいたい。
- 計算機能力の向上の線がなだらかになっている点については、HPC 分野でも認識されている。そうした計算機能力の進展について、専門家にヒアリングするのがよいと思われる。

これらのコメントに対して、計算機の専門家からヒアリングを行った結果、「半導体の微細化は限界が近づいている」、「将来、プロセッサの性能は頭打ちになる」、「計算の目的が多様化してきている」等が指摘された。

[1] https://www.cryptrec.go.jp/exreport/cryptrec-ex-0601-2006.pdf（T. Kleinjung 氏による）

[2] https://www.cryptrec.go.jp/exreport/cryptrec-ex-2802-2018.pdf（予定）

第 3 回 WG において、素因数分解問題および楕円曲線上の離散対数問題の困難性に関する計算量及び計算機の処理性能の表示等についての検討を開始した。

・（１）で述べた 2018 年度に実施された評価結果を予測図に表示する方法について

- 従来通り 1 クロックにつき 2 FLOPS で換算して横線を引く。
- 2018 年度に実施した評価結果に関する横線を新たに引くと、2006 年度に実施された同じビット長の評価結果に関する横線と近くを通り、表示が複雑になるため、新たに引く横線より上方を通る「実メモリ制約有り」の横線を省く。

という提案が事務局からあったが、他に適切な表示があるのではないかという意見が出されたため、新たに得られた評価結果を含め、これら評価結果の解釈については継続審議とすることとなった。

・計算機の処理性能の表示について

以前から外挿線の傾きが徐々に下ってきていることが WG で指摘されていたが、今後どのように外挿するべきかについて検討された。

予測図では、TOP500.Org から公表されているスーパーコンピュータのうち、ピーク性能が 1 位（または 500 位）であるものをプロットして、1993 年から現在までのすべてのデータに最小自乗法を適用して外挿線を引いている。予測図は 2006 年度にはじめて作成され、RSA1024 ビットの危殆化のおおよその時期を予測するために利用された。外挿線の傾きが一定している範囲では解読に必要な計算量に相当する横線と交わる年が危殆化時期の目安となるからである。

外挿線の傾きの変化の様子を下記の図 3 に示す。これによると、2014 年頃から現在まで外挿線の傾きが鈍化し続けていることがわかる。

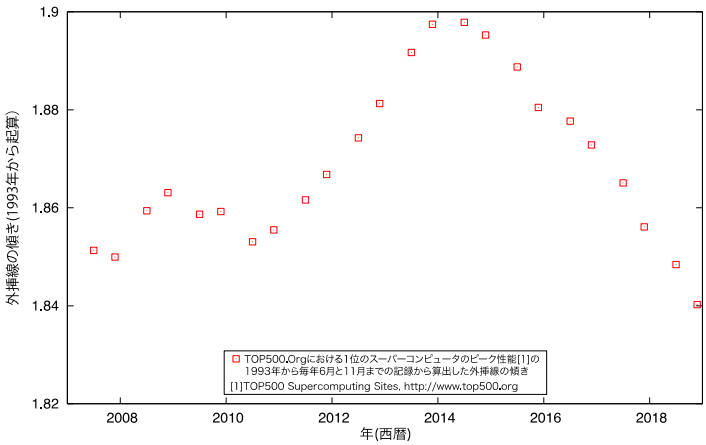


図 3:TOP500.Org における 1 位のスーパーコンピュータのピーク性能の
1993 年から毎年 6 月と 11 月までの記録から算出した外挿線の傾き

- スーパーコンピュータのピーク性能 1 位のプロットは、上述のヒアリングの中の指摘にもあるように凸凹している。
- 1 位から 500 位のピーク性能の合計値(SUM)のプロットはなだらかで、外挿線の傾きの変化が分かり易いため、予測図にピーク性能の合計値のプロットを追加し、それらの外挿線を引く。

という提案が事務局からあったが、短い期間のデータから外挿した直線がどの範囲まで妥当であるかが不明である等、近年のこのような鈍化傾向を予測図にどのように反映するかについては慎重に検討する必要があるという意見があったため、予測図の更新については継続審議とすることとなった。

2018 年度の予測図の更新については継続審議となったが、第二回暗号技術評価委員会において予測図の参照先が明確でないのは不都合であるという指摘があったので、2018 年 6 月・11 月のベンチマーク結果を追加して従来通りの方法で予測図を更新することになった（下記の図 4 及び図 5）。

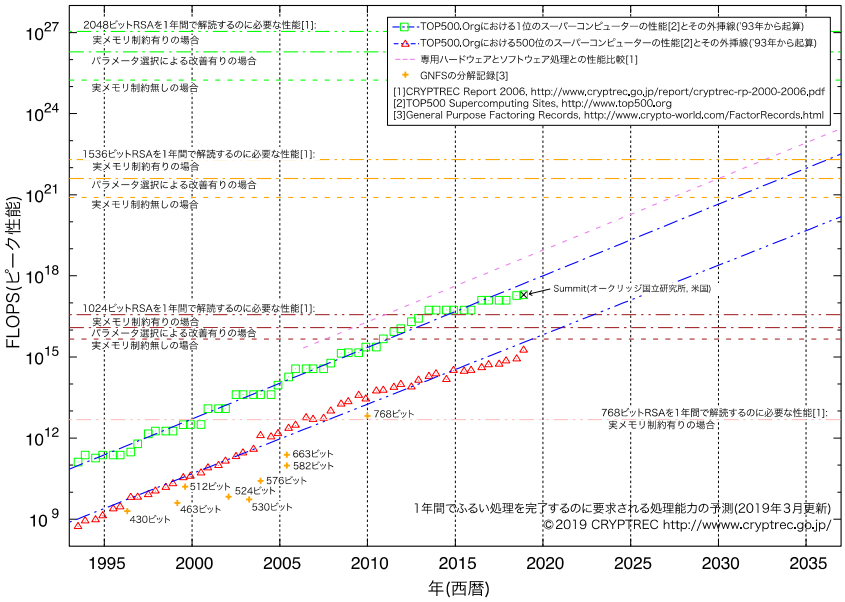


図 4：素因数分解の困難性に関する計算量評価

（1 年間でふるい処理を完了するのに要求される処理能力の予測、2019 年 3 月更新）

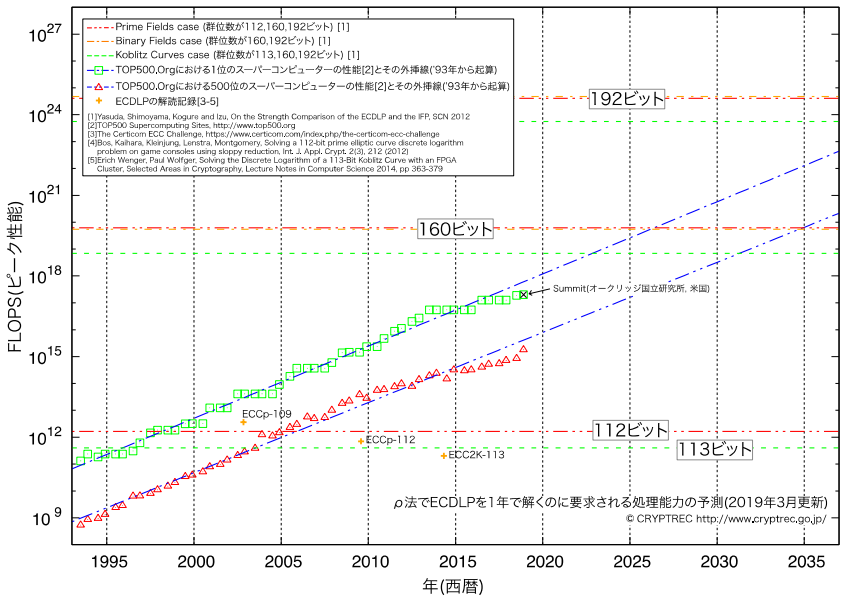


図 5：楕円曲線上の離散対数計算の困難性に関する計算量評価

（ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2019 年 3 月更新）

3.3. 量子計算機による素因数分解について

米国学術機関の統合団体である全米アカデミーズが公表したレポート[2]によれば、十分な性能を有する量子計算機の登場の時期を現時点で予測することは困難であるので、大きな合成数が量子計算機によって解かれる時期について言及することは難しい。従って、現状について、[3]の表 1 をもとにまとめることになった。

表 2: 量子計算機による素因数分解の状況（[3]の表 1 を一部改変）

■量子ゲート計算（#QB は使用した量子ビット数）

分解法	計算手段	合成数	ビット長	発表年	ジャーナル名	備考
Shor※1	NMR	15	4	2001 年	Nature	#QB=7
	光子	21	5	2012 年	Nature Photonics	#QB=1+log3※2
	光集積回路	15	4	2009 年	Science	#QB=5
	ジョセフソン素子	15	4	2012 年	Nature Physics	#QB=3
	イオントラップ	15	4	2016 年	Science	#QB=5

※1: 分解対象の素因数分解結果を用い、Shor のアルゴリズムの演算の一部を省略している

※2: 2 進と 3 進で表現されている

■量子アニーリング計算（#QB は使用した量子ビット数）

分解法	計算手段	合成数	ビット長	発表年	ジャーナル名	備考
素朴法	NMR	21	5	2008 年	Physical Review Letters	#QB=3
筆算法	NMR	143	8	2012 年	Physical Review Letters	#QB=4
	D-Wave	200099	18	2016 年	Scientific Reports	#QB=897

[2] Quantum Computing: Progress and Prospects, The National Academies of Science, Engineering, and Medicine, 2018, http://nap.edu/25196

[3] 素因数分解の現状, 伊豆, 國廣, 2B2-3, 暗号と情報セキュリティシンポジウム 2018 (SCIS2018)

資料3別添２

耐量子計算機暗号の研究動向調査報告書（案）

2019 年 3 月（3/21 版）

目次

資料4

2018年度　暗号技術活用委員会活動報告

1.　2018年度の活動内容と成果概要

1.1　活動内容

2017 年度に実施した「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえ、今後 2 年間かけて鍵管理に関する運用ガイドライン（鍵管理ガイドライン）の整備を開始した。

2018 年度は、「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえて、(1)鍵管理に関するフレームワークの検討、ならびに(2)(1)の検討結果に基づく鍵管理ガイドライン「暗号鍵管理システム設計指針（基本編）」のドラフト版の作成、を実施した。

1.2　暗号技術活用委員会の委員構成及び開催状況

暗号技術活用委員会の委員構成は表 1-1 のとおりである。また、2018 年度に 2 回開催された暗号技術活用委員会での審議概要は表 1-2 のとおりである。この他、鍵管理ガイドラインについての技術検討会合を別途開催した。

表 1-1 暗号技術活用委員会　委員構成

委員長	松本　勉	国立大学法人横浜国立大学　大学院環境情報研究院　教授
委員	上原　哲太郎	立命館大学　情報理工学部情報システム学科　教授
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティレスポンスチーム セキュリティプログラムマネージャー
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
委員	須賀　祐治	株式会社インターネットイニシアティブ セキュリティ本部セキュリティ情報統括室　シニアエンジニア
委員	杉尾　信行	株式会社 NTT ドコモ　サービスイノベーション部
委員	清藤　武暢	日本銀行金融研究所　情報技術研究センター
委員	手塚　悟	慶應義塾大学　大学院政策・メディア研究科　特任教授
委員	寺村　亮一	NRI セキュアテクノロジーズ株式会社 サイバーセキュリティ事業開発部　主任
委員	松本　泰	セコム株式会社　IS 研究所　コミュニケーションプラットフォームディビジョン　マネージャー
委員	三澤　学	三菱電機株式会社　情報技術総合研究所　情報ネットワーク基盤技術部 トラステッドシステム技術グループ　主席研究員
委員	満塩　尚史	内閣官房　IT 総合戦略室　政府 CIO 補佐官
委員	山岸　篤弘	一般財団法人日本情報経済社会推進協会 電子署名・認証センター　客員研究員
委員	山口　利恵	国立大学法人東京大学　大学院情報理工学系研究科 ソーシャル ICT 研究センター　特任准教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　副研究センター長

表 1-2　暗号技術活用委員会　開催状況

回	開催日	議案
第 1 回	2018 年 9 月 6 日	■ 活用委員会活動計画の確認 ■ 鍵管理に関するフレームワークについての検討
技術検討会合	2018 年 12 月 26 日	■ 鍵管理ガイドラインのドラフト素案作成に向けた技術的検討
第 2 回	2019 年 3 月 14 日	■ 鍵管理ガイドラインのドラフト素案の審議 ■ 次期 CRYPTREC 暗号リスト策定に向けた方針についての検討

1.3　成果概要

1.3.1　鍵管理に関するフレームワーク（暗号鍵管理システム設計指針）についての検討

鍵管理に関連する代表的なガイドラインの事前調査結果（図 1-1）を踏まえ、以下の調査対象のガイドラインについて、想定読者や目的、及び相互の関連性について、より詳細に調査を行った。

＜調査対象とするガイドライン＞

- SP800-57 Part1 revision4: Recommendation for Key Management, Part 1: General
- SP800-57 Part2 revision1(draft): Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
- SP800-130: A Framework for Designing Cryptographic Key Management Systems
- SP800-152: A Profile for U.S. Federal Cryptographic Key Management Systems

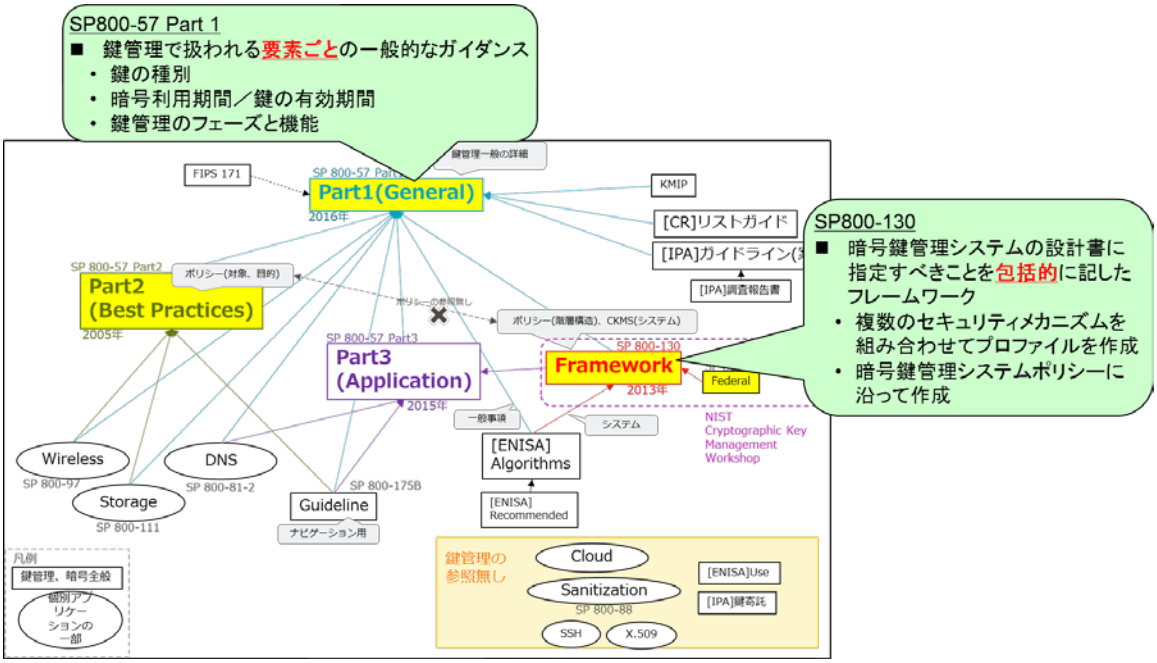


図 1-1　鍵管理に関連する代表的なガイドラインの事前調査結果

表 1-3　各ガイドラインの想定読者や目的

SP800-57 Recommendation for Key Management	暗号メカニズムの不適切な選択による安全性確保は困難であり、プロトコルやアプリケーションの実際の安全性にほとんどまたはまったく寄与しない。暗号メカニズムを選択・利用する際の、バックグランド情報の提供及び適切な選択を支援するためのフレームワークの提供が目的
Part 1: General	• システム開発者／管理者： 役に立つ汎用的な鍵管理ガイダンス • 暗号モジュール開発者： 具体的なアプリケーションでサポートが必要となる鍵管理特性の理解のための汎用的なガイダンス • プロトコル開発者： 具体的なアルゴリズムスイートによる鍵管理特性の確認や理解 • システム管理者： 構成設定の最適な決定のための推奨
Part 2: Best Practices for Key Management Organization	• システム／アプリケーション所有者： 組織の適切な鍵管理基盤の特定、鍵管理方針の確立、及び鍵管理の実践と計画を規定する際の使用に適合するガイダンス • 特に、暗号鍵の確立と管理の役割を担う連邦政府システムの所有者と管理者向け
SP800-130 A Framework for Designing Cryptographic Key Management Systems	暗号鍵管理システムの設計時に考慮すべきトピックや対処すべき仕様要求について記載されたフレームワークを提供が目的 • 暗号鍵管理システム設計者： チェックリストとして活用 （カバーすべき全てのトピックに対する対処方法、暗号鍵管理システムに関する全ての観点での検討、暗号鍵管理システム内でのポリシー／コンポーネント／デバイスの選択、決定事項の明示、詳細仕様や理由を含めた全ての決定方針の文書化、等）
SP800-152 A Profile for U.S. Federal Cryptographic Key Management Systems	連邦政府機関や請負業者が全ての暗号鍵や関連メタデータを管理するために利用する連邦暗号鍵管理システムに対する要求事項を明示 • 暗号鍵管理システムの設計者／実装者： 適切なセキュリティサービスや鍵管理機能の選択／実装を支援 • 連邦暗号鍵管理システムの調達者／管理者／サービス利用機関： 適切な暗号鍵管理システムの選択を支援

各ガイドラインの想定読者や目的は表 1-3 のとおりである。簡単に言えば、SP800-57 Part 1 では「鍵管理で扱われる要素ごとの一般的なガイダンス」について記載されており、特に、鍵の種別、暗号利用期間／鍵の有効期間、鍵管理のフェーズと機能といったトピックが取り上げられている。また、SP800-130 では「暗号鍵管理システムの設計書に指定すべきことを包括的に記したフレームワーク」を提示しており、暗号鍵管理システムポリシーに沿って複数のセキュリティメカニズムを組み合わせてプロファイルを作成するための指針を示している。

これらのガイドラインに記載された内容から、鍵管理を考えるうえでのあるべき構造を図 1-2 のように整理し、鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした。構成要素としては以下の 4 つからなる。

① 「Guidance」：鍵管理についての技術的な理解を助け、推奨設定などを提供する文献。
例えば、SP800-57 part 1、同 part 3、CRYPTREC 暗号リスト、リストガイド（鍵管理）、

SSL/TLS 暗号設定ガイドライン、などが該当する。

② 「Framework Requirements」：あらゆるケースにおける鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項を包括的に一覧として取りまとめたもの。SP800-130 が代表例である。あらゆるケースに適用できるように、採用すべき具体的な技術仕様は規定しておらず、あくまで③Profile Requirements や④System Requirements を具体的に検討・設計する際の考え方や検討項目を示す、設計手引書的な位置づけのものである。

③ 「Profile Requirements」：業界（セクタ）固有の特性や環境を踏まえた共通的な条件や設計ポリシーに基づき、①Guidance の技術的根拠を加味して、②Framework Requirements に沿って、業界（セクタ）内で共通に実現すべき要求事項（設計方針・運用要件等）を規定したもの。例えば、SP800-152 は、米国政府システム共通の暗号鍵管理システムとしての要求事項が規定されたものである。

④ 「System Requirements」：③Profile Requirements に適合するように、システム個別の環境／条件を考慮して作成された、実際の暗号鍵管理システムが実現すべき具体的な設計仕様書や運用マニュアル等のこと。システムが依存する環境や条件と①Guidance の技術的根拠の両方を加味して、具体的な技術仕様として取りまとめられる。

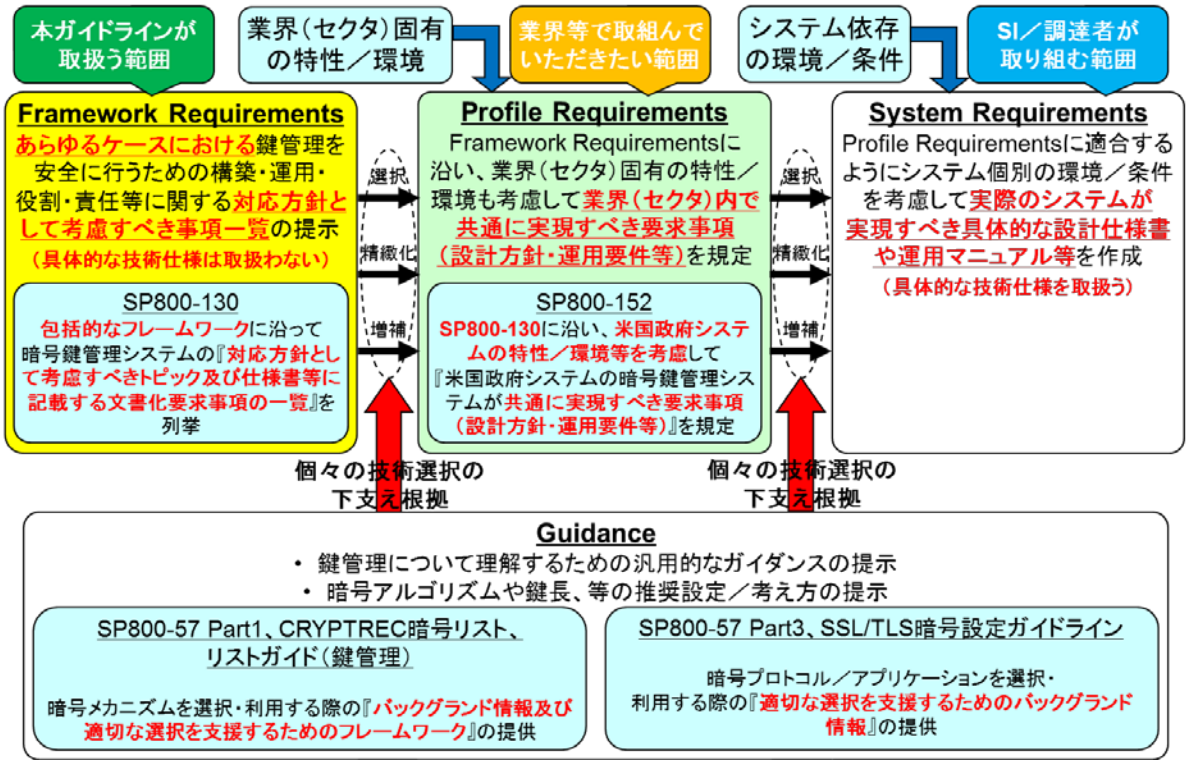


図 1-2　鍵管理を考えるうえでのあるべき構造

暗号技術活用委員会としては、①Guidance に含まれるガイドラインだけでは鍵管理ガイドラインとして不十分であり、②Framework Requirements を扱うガイドラインを作成すべきと判

断し、SP800-130 をベースに作業を行うこととした。なお、③Profile Requirements や④System Requirements については、個別の要件や環境等に依存する側面が強くなると考えられるため、各業界等で取り組んでいただくことを期待している。

1.3.2　暗号鍵管理システム設計指針（基本編）のドラフト素案の取りまとめ

SP800-130 では、暗号鍵管理システムを構築するうえで考えるべき検討項目が網羅的にカバーされており、この範囲をベースに考えれば漏れはほとんどないと思われる。しかし、検討すべき項目（Framework Requirements）が全部で 258 個もあり、かつ記載内容も教科書的な並びになっているため、必要な個所を見つけ出すことが難しい。

一方、日本では、今まで SP800-130 のような暗号鍵管理システムの設計指針の基準となる包括的・統一的な鍵管理ガイドラインが作られていないため、「鍵管理」のあり方や考え方が十分に解説されていなかった。その結果、Guidance に含まれるガイドラインを「鍵管理ガイドライン」としてきた経緯もあり、Guidance に記載がある特定の項目（例えば、暗号アルゴリズムや鍵長など）については細かく規定しているのにも関わらず、鍵管理上は重要なのに Guidance が扱っていない項目（例えば、鍵のライフサイクルや安全な鍵の保管方法、危殆化時の対策など）については規定がなかったり抽象的な記述の規定にとどまったりといったことが懸念される。このことは、鍵管理（システム）という視点で見てみると、規定した内容の粒度にムラを生じさせるということであり、システム全体の安全性確保を困難にする原因になると推察される。

そこで、暗号技術活用委員会では、イントロダクションとして鍵管理のあり方や考え方を解説し、技術的には SP800-130 の理解を深める解説書・利用手引きとして活用するための「暗号鍵管理システム設計指針（基本編）」を「鍵管理ガイドライン」として位置付けることとした。

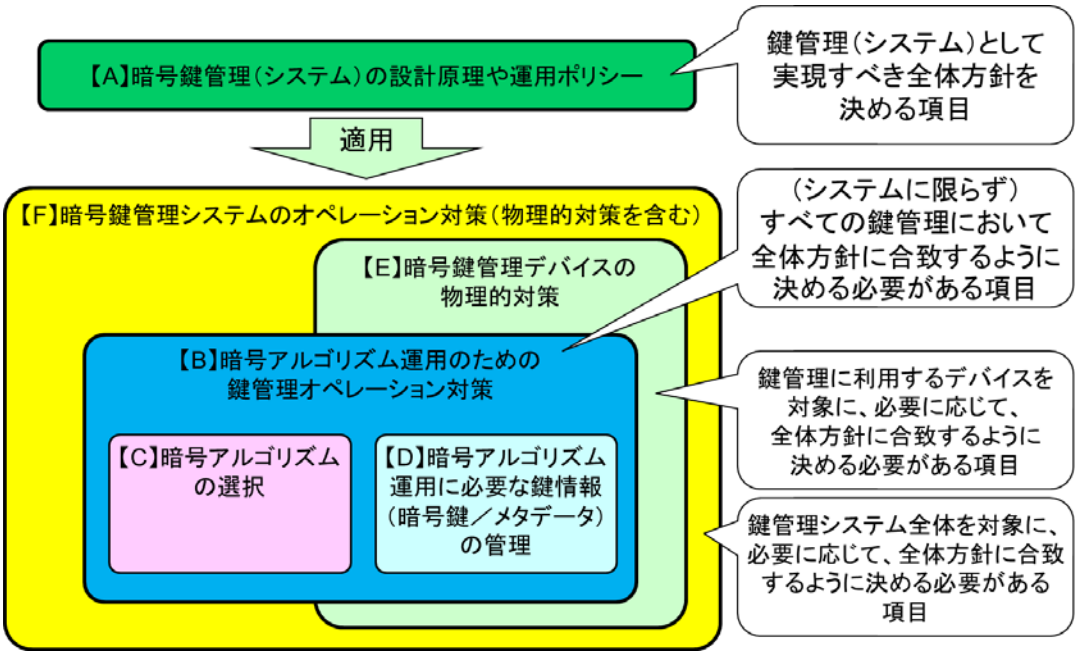


図 1-3　鍵管理における目的

その方針に基づき、(i) SP800-130 全体の日本語訳を作成するとともに、(ii) SP800-130 に記載されているトピックや Framework Requirements を『鍵管理における目的』に応じた対象範囲に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化し、分かりやすく表現することを目指している。具体的には、どのような目的のためにどのような項目を取り扱わなければならないのかを関係性が分かるように、6 つの目的に分類・再構築する方向で、ドラフト素案の取りまとめを行っている（図 1-3、図 1-4 参照）。

2章（フレームワークの基本）：フレームワークの基本的な概念をカバーし、フレームワークの概要を記載
3章（目的）：堅牢な暗号鍵管理システム（CKMS）の目的を定義
4章（セキュリティポリシー）：システム構成、及び情報管理、情報セキュリティ、CKMSセキュリティ並びに他の関連するセキュリティポリシーの必要性について記載
5章（役割と責任）：CKMSをサポートする役割と責任を提示
6章（暗号鍵とメタデータ）：CKMSの最も重要な要素（利用可能な鍵とメタデータの定義、及び鍵とメタデータの管理機能、等）を包括的に記載
7章（相互運用性と移行）：相互運用性と将来ニーズに対応するための容易な移行能力の必要性について記載
8章（セキュリティコントロール）：典型的なCKMSに適用されるセキュリティコントロールを記載
9章（テストとシステム保証）：セキュリティテストと保証について記載
10章（災害復旧）：一般及びCKMS特有の災害復旧について記載
11章（セキュリティアセスメント）：CKMSのセキュリティアセスメントについて記載
12章（技術的課題）：暗号アルゴリズム、鍵確立プロトコル、デバイス、量子コンピュータに関する新しい攻撃によってもたらされる技術的課題について記載

	目的	取扱い項目
A	暗号鍵管理（システム）の設計原理や運用ポリシー	セキュリティポリシー
		暗号鍵管理システムの構築環境／利用条件
		将来的な移行対策
B	暗号アルゴリズム運用のための鍵管理オペレーション対策	鍵情報のライフサイクル
		鍵情報のライフサイクル管理機能
		鍵情報の保管方法
		鍵情報の鍵確立方法
		鍵情報の危殆化時の BCP 対策
C	暗号アルゴリズムの選択	暗号アルゴリズムの安全性
D	暗号アルゴリズム運用に必要な鍵情報（暗号鍵／メタデータ）の管理	鍵情報（暗号鍵／メタデータ）の選択
		鍵情報の保護方針
E	暗号鍵管理デバイスの物理的対策	鍵情報へのアクセスコントロール
		セキュリティ評価・試験／システム保証
F	暗号鍵管理システムのオペレーション対策（物理的対策を含む）	暗号鍵管理システム（物理／OS とデバイス／ネットワーク）へのアクセスコントロール
		災害発生時の BCP／復旧対策（バックアップ）

図 1-4　SP800-130 目次と暗号鍵管理システム設計指針（基本編）（ドラフト素案）との対比

1.3.3　次期 CRYPTREC 暗号リスト策定に向けた方針についての検討

2022 年度に予定されている次期 CRYPTREC 暗号リスト策定に向けた方針について、暗号技術活用委員会として議論を行ったところ、「策定方針を前提とするのではなく、リストの位置づけから根本的に見直したほうがよいとの意見が多数あった」とのまとめ意見を暗号技術検討会に報告することとなった。

2.　今後に向けて

鍵管理ガイドラインについては、引き続き作業を行い、CRYPTREC シンポジウム 2019 でドラフト版を公開、2019 年度末に同ガイドラインを完成させる予定である。また、SP800-130 の日本語訳も公開する予定である。

2017 年度に一部改訂した SSL/TLS 暗号設定ガイドラインについては、その後の SSL3.0 利用禁止及び TLS1.3 リリースを踏まえ、2019 年度に内容を大幅に見直す方針とする。

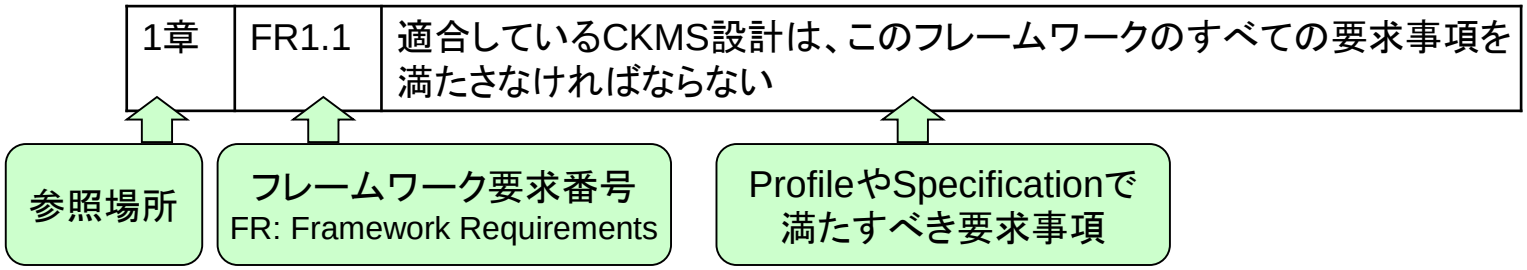
資料4別添

暗号鍵管理システム設計指針（基本編）
～サブタイトル（検討中）～

（ドラフト素案）

本ガイドラインの位置づけ

- 位置づけ
  - イントロダクションとして:「鍵管理」のあり方／考え方の解説
  - 技術的な中身として:SP800-130の理解を深める解説書・利用手引きとして活用
    - オリジナルな「鍵管理ガイドライン」ではない。あくまでSP800-130がベース
    - SP800-130に記載されているトピック／FR(Framework Requirements)を『鍵管理における目的に応じた』対象範囲に分類・整理することによって検討すべき項目の目的や必要性を明確化(分かりやすく表現)



    - 参照すべき文書へのリンク情報を提供

- 主な想定読者
  - セキュリティシステム管理責任者
  - 暗号鍵管理システム(CKMS)設計者
  - システムインテグレータ
  - 調達責任者／担当者

鍵管理全体の俯瞰図

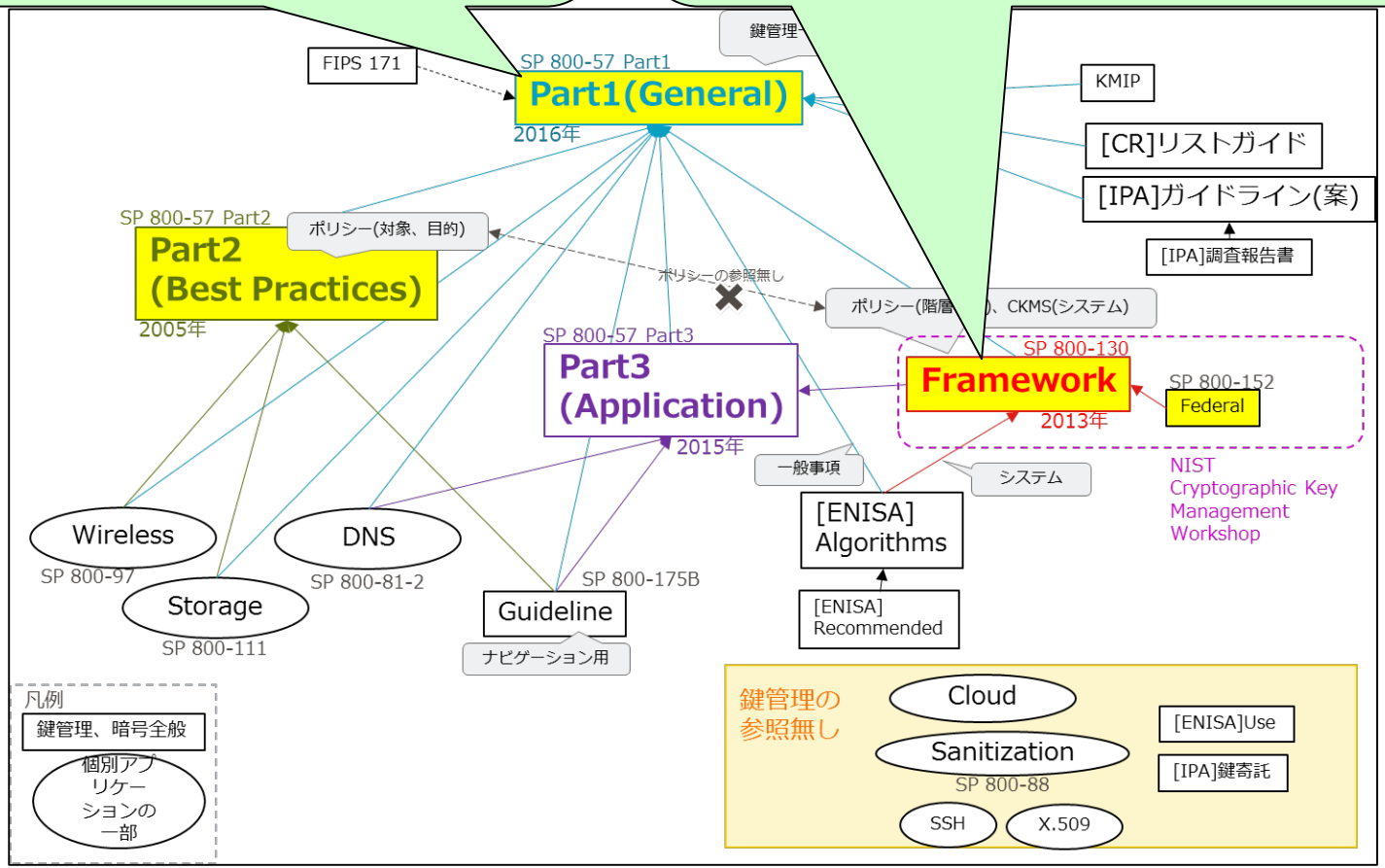
- 鍵管理に関連する代表的なガイドラインの事前調査結果

SP800-57 Part 1

- 鍵管理で扱われる**要素ごと**の一般的なガイダンス
  - 鍵の種別
  - 暗号利用期間／鍵の有効期間
  - 鍵管理のフェーズと機能

SP800-130

- 暗号鍵管理システムの設計書に指定すべきことを**包括的**に記したフレームワーク
  - 複数のセキュリティメカニズムを組み合わせてプロファイルを作成
  - 暗号鍵管理システムポリシーに沿って作成



鍵管理全体の俯瞰図

■ 鍵管理を考える上でのあるべき構造

本ガイドラインが取扱う範囲

業界（セクタ）固有の特性／環境

業界等で取組んでいただきたい範囲

システム依存の環境／条件

SI／調達者が取り組む範囲

Framework Requirements

あらゆるケースにおける鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧の提示

（具体的な技術仕様は取扱わない）

SP800-130

包括的なフレームワークに沿って暗号鍵管理システムの『対応方針として考慮すべきトピック及び仕様書等に記載する文書化要求事項の一覧』を列挙

選択

精緻化

増補

Profile Requirements

Framework Requirementsに沿い、業界（セクタ）固有の特性／環境も考慮して業界（セクタ）内で共通に実現すべき要求事項（設計方針・運用要件等）を規定

SP800-152

SP800-130に沿い、米国政府システムの特性／環境等を考慮して『米国政府システムの暗号鍵管理システムが共通に実現すべき要求事項（設計方針・運用要件等）』を規定

選択

精緻化

増補

System Requirements

Profile Requirementsに適合するようにシステム個別の環境／条件を考慮して実際のシステムが実現すべき具体的な設計仕様書や運用マニュアル等を作成

（具体的な技術仕様を取扱う）

〇〇システム設計仕様書

〇〇システム運用マニュアル

個々の技術選択の下支え根拠

個々の技術選択の下支え根拠

Guidance

- 鍵管理について理解するための汎用的なガイダンスの提示
- 暗号アルゴリズムや鍵長、等の推奨設定／考え方の提示

SP800-57 Part1、CRYPTREC暗号リスト、リストガイド（鍵管理）

暗号メカニズムを選択・利用する際の『バックグランド情報及び適切な選択を支援するためのフレームワーク』の提供

SP800-57 Part3、SSL/TLS暗号設定ガイドライン

暗号プロトコル／アプリケーションを選択・利用する際の『適切な選択を支援するためのバックグランド情報』の提供

SP800-130の紹介概要　－　イントロダクション（1章、2.4節）

- 暗号鍵管理システム（CKMS）設計における**包括的なフレームワーク**に沿って**考慮すべきトピック及び仕様書等に記載する文書化要求事項の一覧**を列挙
  - 望ましいCKMSを構築、調達及び評価するため、統一的な仕様を作成できるように設計時に文書化する必要がある事項を洗い出したもの
    - CKMSにおけるいかなる特定のポリシー、手続き、セキュリティ要求事項、システム設計制約を課さない。特定のセキュリティ機能を義務づけるわけではない
    - 比較できるように、構造的な方法で文書化されることを要求しているだけ
  - どのような要求仕様／設計方法を採用するかは、設計者、又はこのフレームワークに基づいたセキュリティプロファイルのような他のドキュメントに委ねられる
    - 設計者が利用する際は、CKMS設計に選択し得るオプションリストとして使用することで要求仕様を決定する
    - 考慮対象とする要求事項の場合は、要求事項によって課される情報を記載する

      例）要求事項がどのように満たされているのか（どのように実装され、実施され、使用されるのか）、どこに（論理的にはシステム中のどこに）実装メカニズムが存在するのか
    - 考慮対象外とする要求事項の場合は、考慮対象外とする理由を記載する。もしくは、考慮対象の範囲を先に明示しておくことによって、考慮対象外の要求事項の範囲を明確化しておく

1章	FR1.1	適合しているCKMS設計は、このフレームワークのすべての要求事項を満たさなければならない
2.4節	FR2.3	適合しているCKMS設計は、このフレームワークの要求事項で要求されているように設計選択を記載し文書を提供しなければならない

SP800-130の紹介概要　－　各章構成（1.3節）

2章（フレームワークの基本）：フレームワークの基本的な概念をカバーし、フレームワークの概要を記載

3章（目的）：堅牢な暗号鍵管理システム（CKMS）の目的を定義

4章（セキュリティポリシー）：システム構成、及び情報管理、情報セキュリティ、CKMSセキュリティ並びに他の関連するセキュリティポリシーの必要性について記載

5章（役割と責任）：CKMSをサポートする役割と責任を提示

6章（暗号鍵とメタデータ）：CKMSの最も重要な要素（利用可能な鍵とメタデータの定義、及び鍵とメタデータの管理機能、等）を包括的に記載

7章（相互運用性と移行）：相互運用性と将来ニーズに対応するための容易な移行能力の必要性について記載

8章（セキュリティコントロール）：典型的なCKMSに適用されるセキュリティコントロールを記載

9章（テストとシステム保証）：セキュリティテストと保証について記載

10章（災害復旧）：一般及びCKMS特有の災害復旧について記載

11章（セキュリティアセスメント）：CKMSのセキュリティアセスメントについて記載

12章（技術的課題）：暗号アルゴリズム、鍵確立プロトコル、デバイス、量子コンピュータに関する新しい攻撃によってもたらされる技術的課題について記載

本ガイドラインでの鍵管理の考え方

- 鍵管理の考え方の理解促進のため、SP800-130に記載されているトピック／FR（Framework Requirements）を鍵管理における目的（取扱い項目）別にグループ化

【A】暗号鍵管理（システム）の設計原理や運用ポリシー

鍵管理（システム）として実現すべき全体方針を決める項目

適用

【F】暗号鍵管理システムのオペレーション対策（物理的対策を含む）

【E】暗号鍵管理デバイスの物理的対策

【B】暗号アルゴリズム運用のための鍵管理オペレーション対策

【C】暗号アルゴリズムの選択

【D】暗号アルゴリズム運用に必要な鍵情報（暗号鍵／メタデータ）の管理

（システムに限らず）すべての鍵管理において全体方針に合致するように決める必要がある項目

鍵管理に利用するデバイスを対象に、必要に応じて、全体方針に合致するように決める必要がある項目

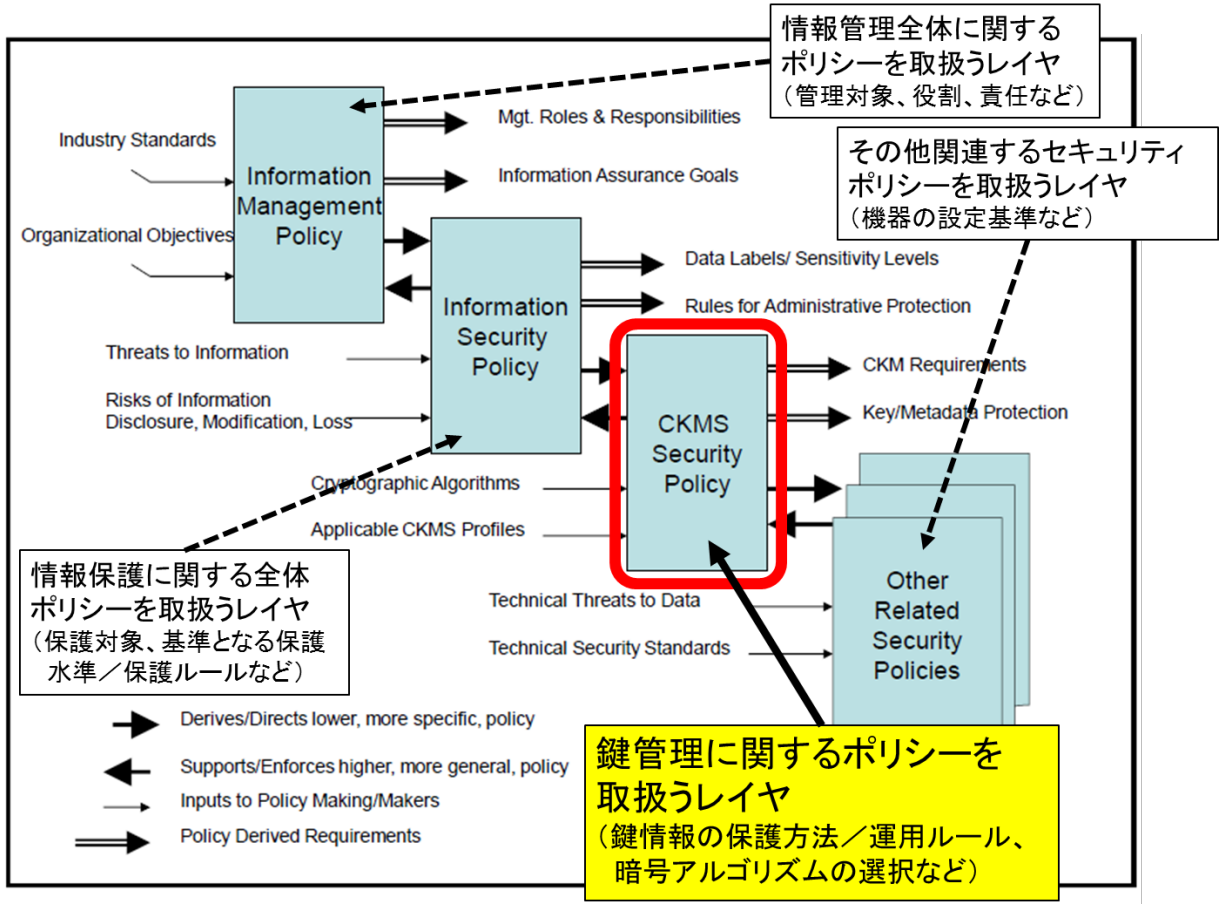
鍵管理システム全体を対象に、必要に応じて、全体方針に合致するように決める必要がある項目

本ガイドラインでの鍵管理の考え方

	目的	取扱い項目	参照箇所
A	暗号鍵管理（システム）の設計原理や運用ポリシー	セキュリティポリシー 暗号鍵管理システムの構築環境／利用条件 将来的な移行対策	2.10節、3章全体、4章（4.3節～4.9節）、5章、6.2節、7章、12章
B	暗号アルゴリズム運用のための鍵管理オペレーション対策	鍵情報のライフサイクル 鍵情報のライフサイクル管理機能 鍵情報の保管方法 鍵情報の鍵確立方法 鍵情報の危殆化時のBCP対策	6.3節、6.4節、6.5節、6.6節、6.8節 SP800-57 part1（6章、7章、8章）
C	暗号アルゴリズムの選択	暗号アルゴリズムの安全性	SP800-57 part1（4章） CRYPTREC暗号リスト 2.1節
D	暗号アルゴリズム運用に必要な鍵情報（暗号鍵／メタデータ）の管理	鍵情報（暗号鍵／メタデータ）の選択 鍵情報の保護方針	2.1節、2.2節、2.5節 6.1節、6.2節 SP800-57 part1（5章）
E	暗号鍵管理デバイスの物理的対策	鍵情報へのアクセスコントロール セキュリティ評価・試験／システム保証	6.7節、6.8節、8.4節、9章全体、11章全体
F	暗号鍵管理システムのオペレーション対策（物理的対策を含む）	暗号鍵管理システム（物理／OSとデバイス／ネットワーク）へのアクセスコントロール 災害発生時のBCP／復旧対策（バックアップ）	6.8節、 8章（8.1節～8.3節）、 10章全体

参考:【A】セキュリティポリシー(4章)

- 使用する各組織の目的をサポートする方法で設計されなければならず、いくつかのポリシーはCKMSの設計と使用に影響を及ぼす
  - 情報管理レベルの課題を取り扱う上位のポリシーと、データ保護に関する特定のルールを取り扱う下位のポリシーから成る階層構造のポリシーに依存することが多い
  - ポリシーの各層(例:情報管理、情報セキュリティ、物理セキュリティ、コンピュータセキュリティ、通信セキュリティ、暗号鍵セキュリティ)は、様々な形態で相互に関係



参考：【A】セキュリティポリシー　－　CKMSセキュリティポリシー（4.3節～4.5節）

- CKMSがサポートしなければならない鍵とメタデータの保護のルールを規定
  - CKMSによって使用されるすべての暗号鍵及びメタデータの機密性、完全性、可用性、及びソース認証（source authentication）を保護するためのルール
  - 鍵の全ライフサイクルにわたってカバー
  - CKMSセキュリティポリシーは組織の高位レベルのポリシー群（情報管理ポリシーや情報セキュリティポリシー）と整合している必要がある
  - ポリシーを保守することに責任を持つ要員がポリシーを容易に理解し役割と責任を正しく実行できるように書かれるべき

4.3節	FR4.1	CKMS設計は、実施するために設計した設定可能なオプションとサブポリシーを含むCKMSセキュリティポリシーを明記しなければならない
4.3節	FR4.2	CKMS設計は、CKMSセキュリティポリシーがCKMSによってどのように実施されるのか（例えば、ポリシーが要求する保護を提供するために使用されるメカニズム）を明記しなければならない

- CKMSセキュリティポリシーは、他のセキュリティポリシーや他組織の様々なポリシーに依存することがあるので、それらを意識しておく必要がある

4.4節	FR4.4	CKMS設計は、CKMSセキュリティポリシーをサポートする他の関連するセキュリティポリシーを明記しなければならない
4.5節	FR4.5	CKMS設計は、CKMS設計によってサポートされるポリシーと、その設計によってどのようにサポートされるのかの要約を明記しなければならない

参考:【B】鍵情報のライフサイクル(6.3節、SP800-57 Part1 7章)

- 鍵情報のライフサイクルは、鍵状態と遷移(Key States and Transitions)に基づく

【鍵状態】

- 活性化前(Pre-Activation)
- 活性化(Active)
- 非活性化(Deactivated)
- 一時停止(Suspended)
- 危殆化(Compromised)
- 破壊(Destroyed)

【遷移】

- 正常な遷移:①→④→⑧→⑭
- それ以外はすべて何らかの異常による遷移

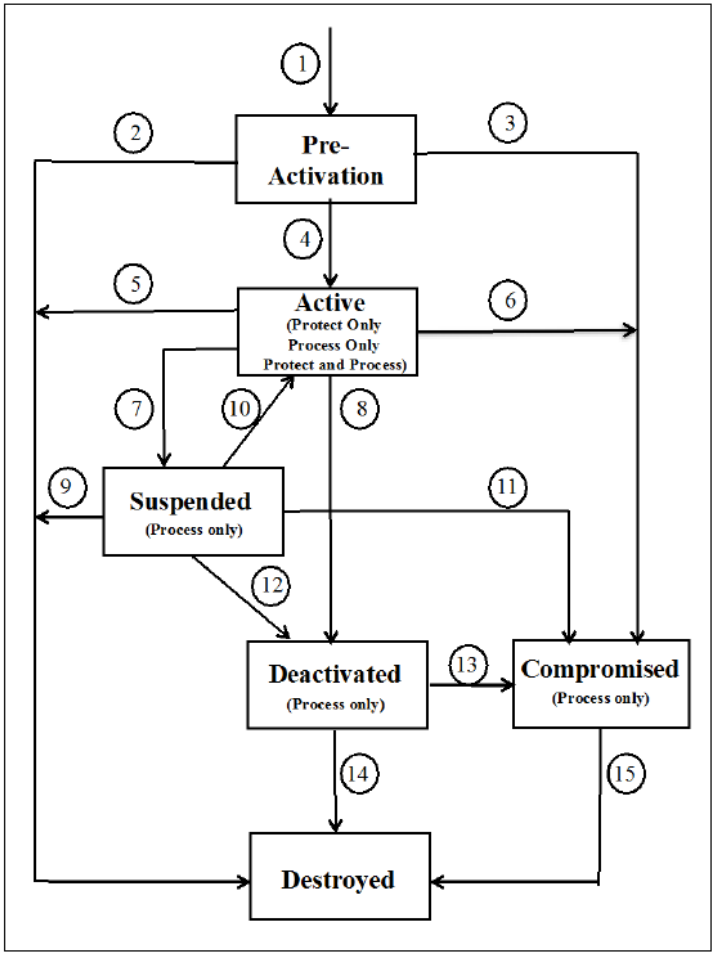


Figure 3: Key state and transition example.
(SP800-57 Part 1 Rev.4より)

6.3節	FR6.15	CKMS設計は、CKMSの鍵が取り得るすべての状態を明記しなければならない
6.3節	FR6.16	CKMS設計は、すべてのCKMS鍵状態間の遷移と遷移を起こすことに関係するデータ(入力と出力)を明記しなければならない

参考:【B】鍵情報のライフサイクル管理機能(6.4節)

- 鍵活性化機能
  - 活性化前(pre-activation)状態から活性化(active)状態への遷移(④)を提供

6.4.3節	FR6.22	CKMS 設計は、それぞれの鍵タイプがどのように活性化されるか、及び鍵の活性化される状況を明記しなければならない
6.4.3節	FR6.23	それぞれの鍵タイプに対して、CKMS設計は鍵活性化の通知の要求事項を明記しなければならない。それにはどの当事者が通知を受けるか、どのように通知されるか、どのセキュリティサービスが通知に適用されるか、及び通知の期間が含まれる

- 暗号機能
  - データへの暗号学的保護を提供
  - 署名生成、署名検証、暗号化、復号、鍵ラッピング、鍵アンラッピング、MAC生成、及びMAC検証を含む

6.4.27節	FR6.69	CKMS設計は、サポートされているすべての暗号機能及びCKMSのどこで実行されるか(例えば、CA、ホスト、又はエンドユーザシステム)を明記しなければならない

参考:【C/D】暗号アルゴリズム／暗号鍵／メタデータの選択(2.1節、2.5節)

- 機微なデータを保護するために、
  - 攻撃者が回避したり覆したりすることが実行不可能であるようなセキュリティ強度を有する暗号技術を使用する
  - CKMSによって、そのライフサイクルにわたって管理及び保護されている暗号鍵を使用する
  - 暗号鍵をエンティティに提供するために、システムをどのように構築するかを明記する

2.1節	FR2.1	CKMS設計は、システムによって使用されるすべてのアルゴリズムとそれぞれのアルゴリズムでサポートするすべての鍵サイズを明記しなければならない
2.1節	FR2.2	CKMS設計は、鍵と鍵に結び付けられたメタデータを保護するために導入されているそれぞれの暗号技術について推定されるセキュリティ強度を規定しなければならない
2.5節	FR2.4	CKMS設計は、以下を含む高レベルの概要を明記しなければならない a) それぞれの鍵タイプの用途 b) 鍵が生成される場所と手段 c) それぞれの鍵タイプとの信頼関係で使用されるメタデータ要素 d) 鍵及び／又はメタデータが、存在している場所のそれぞれのエンティティのストレージにおいてどのように保護されるか e) 鍵及び／又はメタデータが配付時にどのように保護されるか f) 鍵及び／又はメタデータが配送され得る先となるエンティティのタイプ(例えば、ユーザ、ユーザデバイス、ネットワークデバイス)

参考:【D】鍵情報(暗号鍵／メタデータ)の選択(2.2節、6.1節、6.2節)

凡例: ○ 記載あり　－ 記載なし
リストガイド:CRYPTREC 2010年度版リストガイド(鍵管理)

■ 暗号鍵(鍵タイプ)一覧

	SP800-130	SP800-57	リストガイド
1) Private Signature Key	○	○	○
2) Public Signature Key (Public Signature-verification Key)	○	○	○
3) Symmetric Authentication Key	○	○	○
4) Private Authentication Key	○	○	○
5) Public Authentication Key	○	○	○
6) Symmetric Data Encryption/Decryption Key	○	○	○
7) Symmetric Key Wrapping Key	○	○	－
8) Symmetric RNG Key	○	○	－
9) Private RNG Key	○	－	－
10) Public RNG Key	○	－	－
11) Symmetric Master Key	○	○	○(一部)
12) Private Key Transport Key	○	○	－
13) Public Key Transport Key	○	○	－
14) Symmetric Key Agreement Key	○	○	－
15) Private Static Key Agreement Key	○	○	－
16) Public Static Key Agreement Key	○	○	－
17) Private Ephemeral Key Agreement Key	○	○	－
18) Public Ephemeral Key Agreement Key	○	○	－
19) Symmetric Authorization Key	○	○	－
20) Private Authorization Key	○	○	－
21) Public Authorization Key	○	○	－

参考:【E】鍵情報へのアクセスコントロール(6.7節、6.8節、8.4節)

- アクセスコントロールシステム
  - 鍵とメタデータ管理機能が認可されたエンティティ の要求(呼び出し)への応答としてのみ実行され、すべての適用可能な制限が満たされている ことを保証する
  - 暗号モジュールと連動して機微な鍵とメタデータへのアクセスを制御する

6.7.1節	6.88	CKMS設計は、エンティティ、ACS、機能ロジックの配置、及びそれらの間の接続を示すことでCKMSのトポロジーを明記しなければならない
6.7.1節	6.89	CKMS設計は、適切な操作を保証するために実装されている鍵管理機能に対する制限を明記しなければならない
6.7.1節	6.90	CKMS設計は、鍵管理機能がどのように認可されたエンティティに制限しているかを明記しなければならない
6.7.1節	6.91	CKMS設計は、鍵管理機能へのアクセスを制御するためのACSとそのポリシーを明記しなければならない
6.7.1節	6.92	CKMS設計は、少なくとも以下を明記しなければならない a) エンティティの粒度(例: 人、デバイス、組織) b) エンティティが識別されているかどうか、及びその方法 c) エンティティが認証されているかどうか、及びその方法 d) エンティティの認可が検証されているか、及びその方法 e) それぞれの鍵管理機能のアクセスコントロール
6.7.1節	6.93	CKMS設計は、CKMSセキュリティポリシーを適応、実装、施行するためのACSの能力を明記しなければならない

参考：【E】鍵情報へのアクセスコントロール（6.7節、6.8節、8.4節）

- 暗号モジュール
  - 暗号ベースのセキュリティ機能を実装するハードウェア、ソフトウェア、ファームウェアの集合（暗号境界内（境界自体も）の全てを包含）
  - セキュリティ機能の完全性と、暗号鍵とメタデータの保護を取り扱う
  - 暗号モジュールセキュリティポリシーに従って実行するように作られるべき

8.4節	FR8.19	CKMS設計は、以下を含む、使用する暗号モジュールとそれぞれのセキュリティポリシを特定しなければならない。 a) 各モジュール（ソフトウェア、ファームウェア、ハードウェア、またはハイブリッド）の実装形態 b) 各モジュールの完全性を保護するために使用されるメカニズム c) 各モジュールの暗号鍵を保護するために使用される物理的および論理的メカニズム d) 各モジュール（セキュリティ機能を含む）で実行された第三者試験と検証、及び各モジュールで使用される保護措置

参考：【F】物理セキュリティコントロール（6.8節、8.1節）

- コンポーネント、デバイス、及びCKMS内に保持されている機微なデータが認可されない開示及び改変から保護されるように物理的に保護するためのセキュリティコントロール
  - コンポーネントとデバイスのセキュリティの重要性に応じて、物理的に保護するためのメカニズムが選択されるべき
    - フェンス、門、ドア、カバー
    - 警備員
    - 錠（物理鍵又は組み合わせ数字）
    - タンパ検出及び防御
    - パスワード
    - バッジ
    - カード及びトークンシステム
    - 生体認証デバイス
    - 警報システム
    - 監視カメラ
    - 監査システム
    - 入退室ログ

8.1節	FR8.1	CKMS設計は、CKMSデバイスと意図する目的をそれぞれ明記しなければならない
8.1節	FR8.2	CKMS設計は、CKMSコンポーネントを含むそれぞれのデバイスを保護するための物理セキュリティ制御を明記しなければならない

参考：【F】災害発生時のBCP／復旧対策（10章）

- コンポーネント障害又は鍵及びメタデータの破損発生時における運用継続性を確保するための準備
  - 設備への物理的損害発生時におけるバックアップ及び回復
    - 保護されるデータと運用の価値と機微度にふさわしいレベルで、バックアップ及び回復設備が設計、実装、運用されるべき

10.1節	FR10.1	CKMS設計は、必要な環境的、火災、及び物理的なアクセスコントロール保護のメカニズムと、障害からの基幹及びすべてのバックアップ設備への回復手続きを明記しなければならない

  - 公共サービス（電気、水道、下水道、空調等）の停止時におけるバックアップ
    - 非常時に最低限確保すべき電力量等を明確にする

10.2節	FR10.2	CKMS設計は、基幹及びすべてのバックアップ設備に対する、電気、水道、衛生、暖房、冷房、及び空気清浄に関する要求値の推奨値だけでなく最小値についても明記しなければならない

  - 通信と計算の機能停止時におけるバックアップ及び回復
    - 高可用性を保証するために冗長な設備が設置されることも多い

10.3節	FR10.3	CKMS設計は、ユーザ、エンタープライズ、及びCKMSアプリケーションによる予測されるニーズに見合うサービスの運用継続を保証するために、設計内に存在し、運用中に利用可能であることを要求される通信及び計算の冗長性を明記しなければならない

資料５

次期 CRYPTREC 暗号リストの改定に向けた議論について

現在の CRYPTREC 暗号リストの策定（2013 年 3 月 1 日）から６年が経過することや、量子コンピュータの動向や新たな暗号技術の動向等を踏まえ、次期 CRYPTREC 暗号リストの改定に向けて、CRYPTREC 事務局で作成した改定方針等の素案について、暗号技術評価委員会及び暗号技術活用委員会でいただいたご意見を紹介する。

次期 CRYPTREC 暗号リストについて（CRYPTREC 事務局において作成した素案）

1 改定方針

- 【改定時期】現在の CRYPTREC 暗号リストは 2013 年 3 月 1 日に改定されており、改定より 10 年後の 2023 年 3 月の改定を目指して検討を開始する。
- 【リスト構成】現在の「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」から大幅見直しは行わない。
- 【暗号公募について】一般への暗号公募は行わない。
- 【新たに追加する暗号技術の候補について】主として標準化動向をもとに事務局で選出を行い、暗号技術検討会で審議の上決定する。学会に提案されている新たな暗号技術については、仕様、安全性評価、知的財産権、調達可能性等の観点で問題ないと判断できれば候補になりうる。
- 【暗号技術評価委員会の役割】暗号技術評価委員会では、安全性評価および実装評価を行う。評価対象は新たに追加する暗号技術の候補のみとする。現リストに掲載されている暗号技術については安全性監視を継続しており、改めて評価を行うことはしない。
- 【暗号技術活用委員会の役割】暗号技術活用委員会では、利用実績調査を行う。
- 【選考基準について】選考基準は 2021 年度までに両委員会で議論の上、暗号技術検討会で決定する。

2 耐量子計算機暗号への対応

- 次期 CRYPTREC 暗号リストへの反映
  - 2022 年度開始までに NIST PQC 標準化で選定された方式を、新たに追加する暗号技術の候補の参考とする。
  - Hash-based signature については IETF 標準をベースに新たに追加する暗号技術の候補の参考とする。
- PQC への移行計画策定については、その時期を含めて NISC でご検討頂く。
- RSA-2048 からの移行については既に始まっているところもあり、何をすべきか議論を開始する。

3 軽量認証暗号・軽量ハッシュ関数への対応

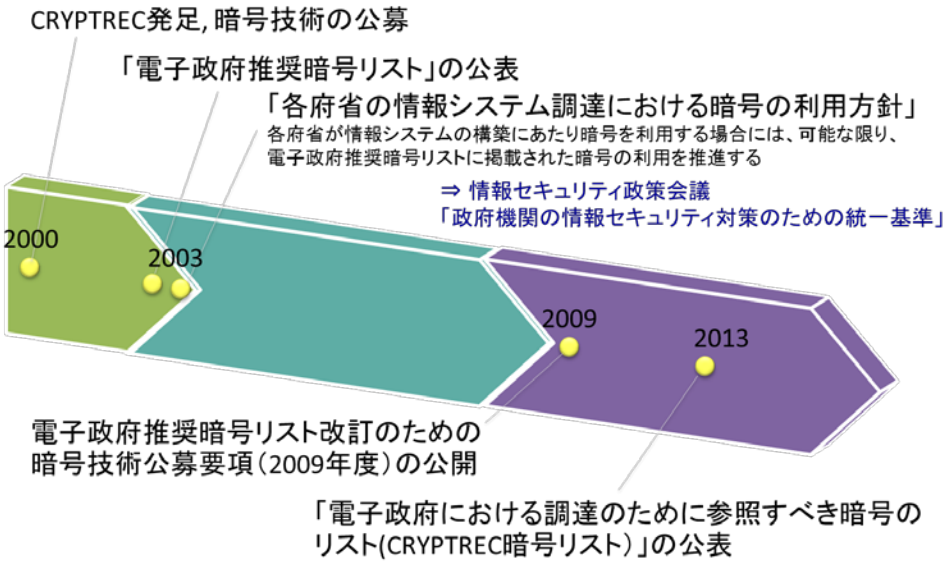
- 次期 CRYPTREC 暗号リストへの反映
  - 2022 年度開始までに NIST 軽量暗号標準化で選定された方式を、新たに追加する暗号技術の候補の参考とする。
    - NIST 軽量暗号標準化
      軽量認証暗号と軽量ハッシュ関数のみ(2019.2.25 応募締切、2-4 年後完了)
      “some algorithms could be selected for standardization after two to four years”

4 その他

次期 CRYPTREC 暗号リストの改定に向けて議論すべき項目は何か、追加・削除を検討すべき技術分類はあるか。

例)

- 64 ビットブロック暗号の利用について
- 64 ビットブロック暗号を安全に利用するための暗号利用モード
- 現リストに掲載されている暗号技術に対する量子計算機の影響
  (鍵長、パラメータ等)
- 秘密分散(ISO/IEC 19592) や準同型暗号(ISO/IEC 18033-6)など



図：これまでの電子政府推奨暗号リストおよび CRYPTREC 暗号リストの改定の流れ

参考：PQC標準化をめぐる国内外の動き

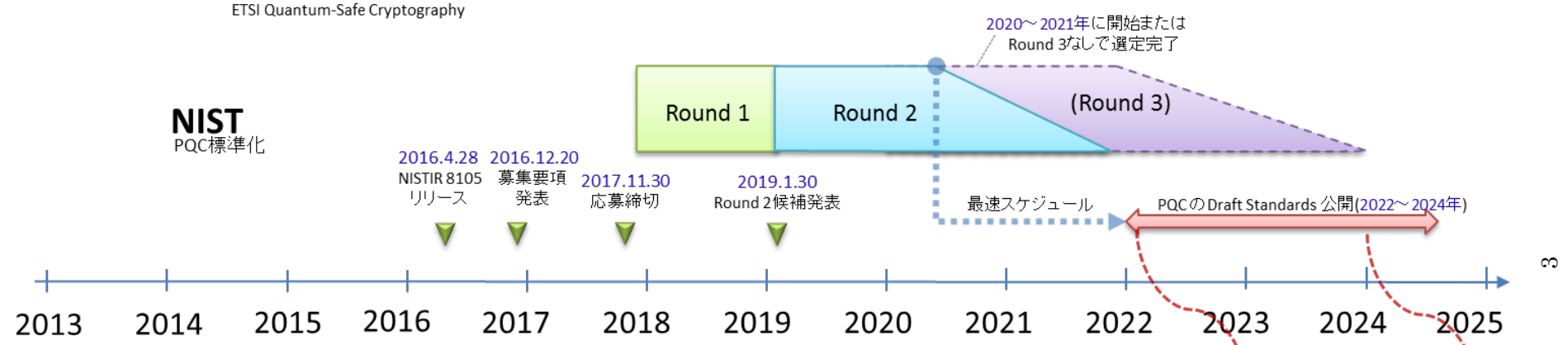
国際

ISO/IEC SC27 WG2 SD8 (Post-Quantum Cryptography)

Asia Asia PQC Forum

EU H2020 ECRYPT
PQCRYPTO
ETSI Quantum-Safe Cryptography

NIST
PQC標準化



CRYPTREC
PQCに関連する活動

2013.3.1
CRYPTREC暗号リスト
発表

2023.3
CRYPTREC暗号リスト
改定？

タイミングを
合わせる？

CRYPTRECにおける
PQC対応
検討開始

暗号技術検討会

暗号技術評価委員会

2015.3
「格子問題等の困難性に
関する調査」発行

2019.3
PQC技術報告書
発行予定

暗号解析評価WG

暗号解析評価WG

国内

暗号技術評価委員会（2018 年 7 月 19 日、2019 年 3 月 11 日開催）で頂いた主な意見

● 「耐量子計算機暗号について」

- 量子計算機の性能については、不確定要素が多いことから、予想通りには進展しないかもしれないが、進展した場合に備えて暗号技術評価委員会で PQC に関する技術的な検討を行う必要がある。
- PQC への移行計画を考えるのは時期尚早であろう。また、簡単ではない。
- PQC への移行について、複数の方式を対応する「暗号 Agility」の考え方で対応が検討されている。

● 「RSA-2048 からの移行について」

- PQC への移行以前に、RSA-2048 からの移行問題が先にあり、20 年という期間の対応が求められている認証局ではすでに移行が始まっている。それは電子政府関係も無縁ではない。例えば電子パスポートについては、国際的な観点から ICAO の動きに対応して移行が検討されている。ICAO 仕様のルート証明書に ECDSA が含まれている。

● 「量子コンピュータの共通鍵暗号への影響について」

- 共通鍵暗号分野においても、量子計算機による影響について適切に監視する必要がある。

● 「軽量暗号について」

- NIST では軽量暗号の認証暗号やハッシュ関数の標準化公募を始めようとしている。2023 年のリスト改定に向けては、PQC だけではなく軽量暗号のことも考えておいた方が良い。
- 軽量暗号技術は、その性質上、セキュリティマージンを厳しく設定していることが多く、一般的な実装とは思想的に違う位置づけになるのかもしれない。64 ビットブロック暗号も多いということから、CRYPTREC 暗号リストの枠組みとの整合性を整理した上でリストの改定にのぞむべきである。
- NIST の公募と CRYPTREC における軽量暗号の範囲との関係を整理する必要がある。

● 「CRYPTREC 暗号リスト（の改定）について」

- 次期 CRYPTREC 暗号リストの改定方針について議論する前に、そもそも次期リストに求める要件を明確にする必要がある。
- リストの構成は、このままでよいのかという点を改めて議論してもよいと思われる。
- 産業界や政府、NISC などにヒアリングして、これまで CRYPTREC がどのように役に立ってきたのかを確認してはどうか。その際に、従来の暗号技術の評価と監視だけではなく、別の役割を求められているのならそれを含めて検討した方が良い。

暗号技術活用委員会（2019 年 3 月 14 日開催）で頂いた主な意見

- **「改定方針を前提とするのではなく、リストの位置づけから根本的に見直したほうがよい」**

- 改定方針には、暗号そのものを考える暗号アルゴリズムに閉じた世界ではなくて、今後どうやって暗号を使ってもらうのかということが盛り込まれていて欲しい。
- 他の政策テーマやアーキテクチャなどの連携との関連性を整理して暗号リストを位置づけてもらいたい。何のための暗号リストなのかの大方針を明確にすべきである。
- 現在リストが 3 個あるが、その形態が妥当であるかについても考える必要がある。

- **「次の暗号アルゴリズムの移行に向けて政策的な議論をする場が必要である」**

- 前回（RSA1024 から RSA2048 への移行）は移行のためのリソースや体制等があり業界全体が一致して動いたが、今はそれだけのリソースも体制もない。資金手当てを含めた政策的な誘導がないと移行が進まないし、時間もかかると思われる。
- PQC への移行は相当困難である。暗号技術活用委員会としては、暗号を移行できる（暗号アジリティ(Crypto-agility)を持った)システムを作らせるという活動をすべきである。PQC への移行を考える前に、暗号を移行できるシステムを作るということを念頭においた活動を行わないと、現実的には PQC への移行は破綻するのではないかと思われる。
- RSA2048 から（PQC ではなく、より強度が高い公開鍵暗号）の移行が、少なくともルート認証局では始まっており、新しく建てるルート認証局では RSA2048 はなくなりつつあると思われるので、実態調査を実施した方がよい。
- スマホでどの程度の強度の暗号がハードウェアでサポートされているのかなど、RSA2048 よりも強度の高いアルゴリズムがどのように使われるか、今現在使えるのか、といった点について、実態調査を実施した方がよい。
- RSA2048 からの移行は直近に移行完了させなければならない課題ではないので、無理なく暗号を移行できるために必要なプロセスの洗い出しから始めたほうがよい。それを専門に検討するチームで議論してもらうべきである。

資料５別添

「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」の設置について（案）

平成 31 年３月 29 日
暗号技術検討会事務局

１．目的

近年、耐量子計算機暗号の研究開発・標準化が各国で進められているところ、我が国においても耐量子計算機暗号について議論を行う必要性が高まっていることから、大規模な量子コンピュータの出現に向けて、次期 CRYPTREC 暗号リストの要件等を整理するため、「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下「タスクフォース」という。）を設置する。

２．検討事項

（１）大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件等の検討

（２）その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

３．検討体制

（１）タスクフォースは、暗号技術検討会の下に設置する。

（２）タスクフォースは、検討事項について機動性を持って検討を行い、随時議論できる場を確保する。

（３）タスクフォースは、暗号技術評価委員会及び暗号技術活用委員会における検討状況を把握するとともに、次期 CRYPTREC 暗号リストの要件等の整理に当たっては、課題を具体的に明確にした上で、必要な調査等を暗号技術評価委員会及び暗号技術活用委員会に求めることができる。

（４）タスクフォースの事務局は、CRYPTREC 事務局（総務省、経済産業省、NICT、IPA）が担当する。オブザーバについては追って調整する。

（５）タスクフォースの構成員は、追って、CRYPTREC 事務局と暗号技術検討会座長が相談の上、調整し定める（暗号技術検討会、暗号技術評価委員会及び暗号技術活用委員会の中からも参画いただくとともに、その他、暗号技術の専門家や量子コンピュータに関して知見を有する者を数名追加することを想定。）。

資料６

暗号技術検討会
２０１８年度　報告書（案）

２０１９年３月

目　　次

１．はじめに

情報通信技術の急速な発展により、自動車、家電、医療、農業、工場など様々な分野で、あらゆるモノがネットワークに繋がる IoT 社会が到来し、サイバー空間と実空間の高度な融合により、多様なニーズにきめ細やかに対応したモノやサービスを提供できる社会への産業構造の変化が進みつつある。一方で、IoT 機器の普及に伴うサイバー攻撃の起点の増加や、サイバー攻撃自体の巧妙化・複雑化が続く中で、サイバー攻撃の影響が実空間にまで到達するリスクも増していくと考えられる。このような産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応したセキュリティ確保が求められる中、暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものであるが、IoT 機器から得られる大量のデータの流通・連携を支える上でも、その重要性は一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC においても、これまで取り組んできた暗号アルゴリズムのセキュリティ確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供等の貢献が求められている。

本年度の各委員会の活動として、暗号技術評価委員会では、学会等での情報収集に基づく CRYPTREC 暗号等の監視、新世代暗号（XTS）に係る安全性評価等を行ったほか、同委員会の下に設置された暗号技術調査 WG において、耐量子計算機暗号の技術動向の調査等を行った。暗号技術活用委員会では、鍵管理に関する運用ガイドライン等の作成に向けた検討を行っているところである。本年度の CRYPTREC は、各委員会での検討結果を踏まえ、「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）」（以下「CRYPTREC 暗号リスト」という。）の改定に向けた検討を行った。これらの 2018 年度の活動の詳細については、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構が取りまとめる「CRYPTREC Report 2018」を参照いただきたい。

今後も暗号技術を用いた情報システム及び情報社会全体のセキュリティ確保のために、成果物の検討や情報発信等を行っていく所存である。

末筆であるが、暗号技術検討会及び関係委員会等に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2019 年 3 月

暗号技術検討会
座長　松本　勉

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001 年度から暗号技術検討会を開催した。

暗号技術検討会において 2002 年度に策定された電子政府推奨暗号リストは、2012 年度に 10 年ぶりの改定が行われ、CRYPTREC 暗号リストとして発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、総務省及び経済産業省は、継続的に暗号技術検討会を開催している。

２．２． CRYPTREC の体制

CRYPTREC とは、Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：松本勉横浜国立大学教授）と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

2018 年度の CRYPTREC においては、暗号技術評価委員会では、学会等での情報収集に基づく CRYPTREC 暗号等の監視等を行い、暗号技術活用委員会では、鍵管理に関する運用ガイドライン（鍵管理ガイドライン）等の作成を行った。

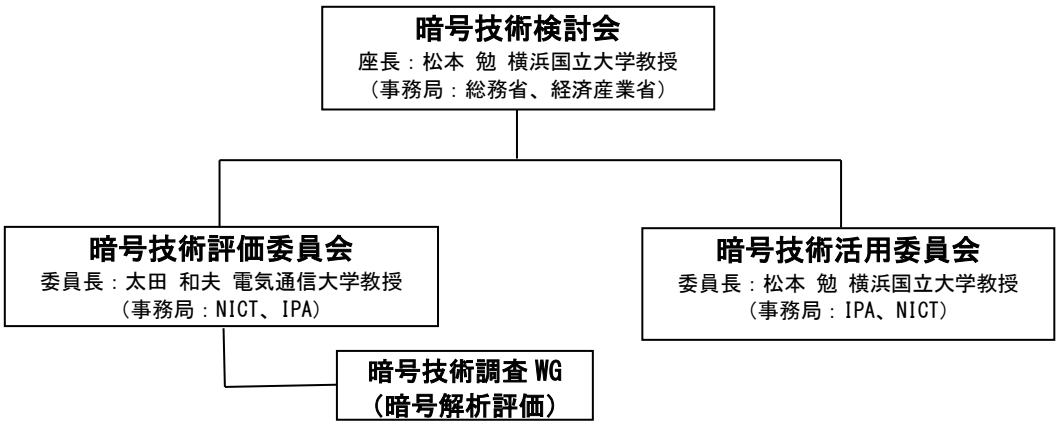


図 2.2.1　2018 年度 CRYPTREC 体制図

２．３．暗号技術検討会の開催実績

2018 年度の暗号技術検討会は、暗号技術評価委員会、暗号技術活用委員会の活動報告、次期 CRYPTREC 暗号リストの改定に向けた検討に係る審議、「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」の設置に係る承認等を行うために１回開催した。

【第 1 回】2019 年 3 月 29 日（金）10:00～**:**（検討会の閉会時刻を記載）
（主な議題）
・ 2018 年度 暗号技術評価委員会 活動報告について
・ 2018 年度 暗号技術活用委員会 活動報告について
・ 次期 CRYPTREC 暗号リストの改定に向けた検討について
・ 「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」の設置について
・ 暗号技術検討会　2018 年度　報告書（案）について
（概要）
・ 検討会での議論を基に作成

３．各委員会の活動報告

３．１．暗号技術評価委員会

３．１．１．活動の概要

暗号技術評価委員会は、CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。主要な検討課題は以下のとおりである。

・暗号技術の安全性及び実装に係る監視及び評価
・推奨候補暗号リストへの新規暗号（事務局選出）の追加
・新技術等に関する調査及び評価

これらの課題について 2018 年度に行った具体的な検討内容を、以下のとおり報告する。

３．１．２．2018 年度の活動内容

暗号技術の安全性及び実装に係る監視及び評価

2018 年度は、①学会等での情報収集に基づく CRYPTREC 暗号リストの安全性及び実装に係る技術に関する監視、②「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の更新の検討を実施した。

①について、研究集会、国際会議、研究論文誌の情報等を収集し、リスト掲載暗号の安全性について監視活動を行った。

②について、「素因数分解の困難性に関する計算量評価」、「楕円曲線上の離散対数計算の困難性に関する計算量評価」の更新を検討し、T.Kleinjung 氏および A.K.Lenstra 氏に計算量見積もりの主要部分の評価を依頼し、素因数分解の困難性に関する計算量の再評価を実施し、計算量見積もりの再評価レポートなどを得た。評価レポートは、CRYPTREC ホームページに公開予定である。一方、近年の計算機の性能向上が鈍化傾向にあることを踏まえ、この傾向を予測図にどのように反映するかについては慎重に検討する必要があるという意見を踏まえ、今年度は前年度までと同じ方法により更新を行うとともに、以降の更新の在り方については、次年度継続検討を行うこととした。

新世代暗号に係る調査

本項目に係る活動に関しては、暗号利用モード XTS の安全性評価を行った。XTS モードは、以下の条件下では、暗号利用モード（秘匿モード）として CRYPTREC 暗号リストへ追加するための安全性要件を満たしていると判断した。

（条件 1）利用用途は IEEE および NIST SP-800-38E の規格に沿ったストレージやディスクの暗号化に限る。

（条件 2）XTS 内のブロック暗号には、 CRYPTREC 暗号リスト掲載の 128 ビットブロック暗号を使う。

（条件 3）鍵を変えずに処理するデータ量は、2^{20} ブロックまでとする。

新技術等に関する調査及び評価

本項目に係る活動に関しては、①耐量子計算機暗号の技術動向調査等、②今後の CRYPTREC 暗号リストにかかわる検討を実施した。

①について、暗号技術評価委員会の下に暗号技術調査 WG（暗号解析評価）を設置し、主に、耐量子計算機暗号（Post-Quantum Cryptography）の技術動向調査・執筆を実施し、技術報告書を完成させた。技術報告書は、CRYPTREC ホームページに公開する。

②について、第一回委員会では、CRYPTREC における耐量子計算機暗号への対応について議論し、第二回委員会では、次期 CRYPTREC 暗号リストに向けた方針の議論を行った。委員会で出た意見をまとめ、暗号技術検討会に報告した。

３．１．３．暗号技術評価委員会の開催状況

2018 年度、暗号技術評価委員会は計２回開催した。各回会合の概要は表 3.1.1 のとおりである。

表 3.1.1　暗号技術評価委員会の開催状況

回	開催日	議題
第１回	2018 年７月 19 日	・ 暗号技術評価委員会活動計画の具体的な進め方の検討 ・ 暗号技術調査ワーキンググループ（暗号解析評価）の活動計画案の検討 ・ XTS モードの安全性評価について外部評価実施の検討 ・ CRYPTREC における耐量子計算機暗号への対応について検討 ・ 監視活動状況報告
第２回	2019 年３月 11 日	・ 暗号技術調査ワーキンググループ（暗号解析評価）の活動報告 ・ XTS モードの安全性評価に関する外部評価レポート報告及び安全性評価検討 ・ 次期 CRYPTREC 暗号リストに向けた方針の検討 ・ 監視状況報告 ・ CRYPTREC Report 2018（暗号技術評価委員会報告）の目次案提示 ・ CRYPTREC シンポジウム概要案提示

2018 年度、暗号技術調査 WG（暗号解析評価）は計３回開催した。

３．２．暗号技術活用委員会

３．２．１．活動の概要

2017 年度に実施した「鍵管理に関する運用ガイドライン作成に向けた事前調査」の結果を踏まえ、2018 年度は鍵管理ガイドラインの作成を開始し、主に以下の活動を行った。

- 鍵管理に関するフレームワークの検討
- 上記の検討結果に基づく鍵管理ガイドライン「暗号鍵管理システム設計指針（基本編）」のドラフト版の作成

３．２．２．2018 年度の活動内容

鍵管理に関連する代表的なガイドラインの事前調査結果（図 3.2.1）を踏まえ、以下の調査対象のガイドラインについて、想定読者や目的、及び相互の関連性について、より詳細に調査を行った。

鍵管理に関するフレームワーク（暗号鍵管理システム設計指針）についての検討

＜調査対象とするガイドライン＞

- SP800-57 Part1 revision4: Recommendation for Key Management, Part 1: General
- SP800-57 Part2 revision1(draft): Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
- SP800-130: A Framework for Designing Cryptographic Key Management Systems
- SP800-152: A Profile for U.S. Federal Cryptographic Key Management Systems

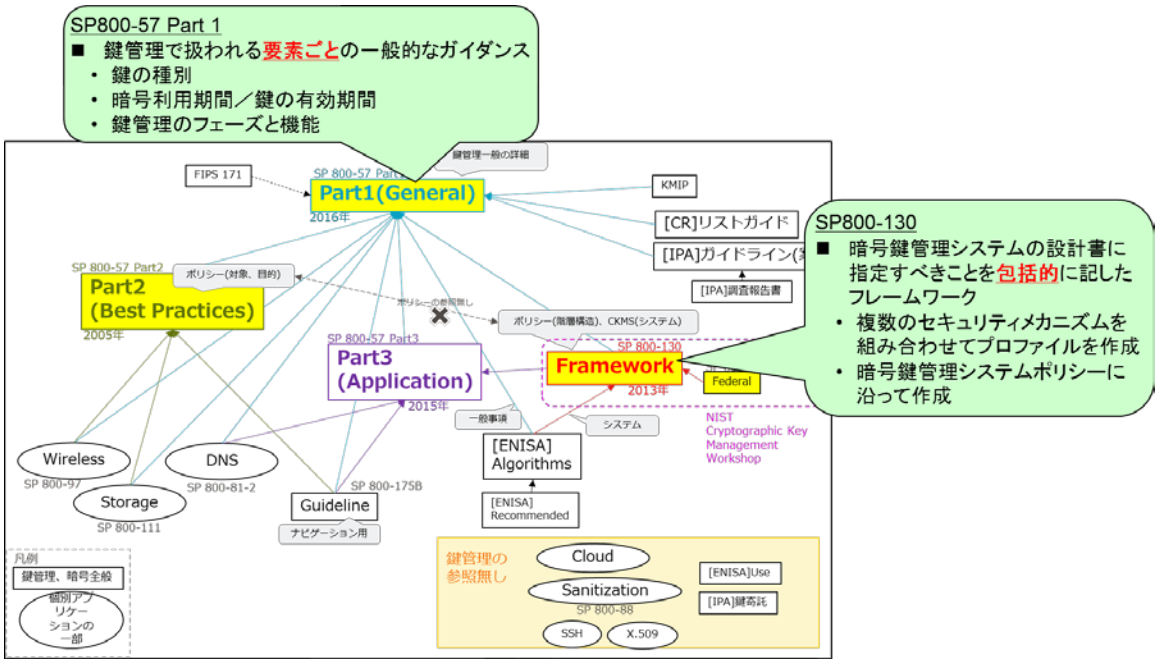


図 3.2.1　鍵管理に関連する代表的なガイドラインの事前調査結果

表 3.2.1　各ガイドラインの想定読者や目的

SP800-57 Recommendation for Key Management	暗号メカニズムの不適切な選択による安全性確保は困難であり、プロトコルやアプリケーションの実際の安全性にほとんどまたはまったく寄与しない。暗号メカニズムを選択・利用する際の、バックグランド情報の提供及び適切な選択を支援するためのフレームワークの提供が目的
Part 1: General	・システム開発者／管理者 役に立つ汎用的な鍵管理ガイダンス ・暗号モジュール開発者 具体的なアプリケーションでサポートが必要となる鍵管理特性の理解のための汎用的なガイダンス ・プロトコル開発者 具体的なアルゴリズムスイートによる鍵管理特性の確認や理解 ・システム管理者： 構成設定の最適な決定のための推奨
Part 2: Best Practices for Key Management Organization	・システム／アプリケーション所有者 組織の適切な鍵管理基盤の特定、鍵管理方針の確立、及び鍵管理の実践と計画を規定する際の使用に適合するガイダンス ・特に、暗号鍵の確立と管理の役割を担う連邦政府システムの所有者と管理者向け
SP800-130 A Framework for Designing Cryptographic Key Management Systems	暗号鍵管理システムの設計時に考慮すべきトピックや対処すべき仕様要求について記載されたフレームワークを提供が目的 ・暗号鍵管理システム設計者： チェックリストとして活用（カバーすべき全てのトピックに対する対処方法、暗号鍵管理システムに関する全ての観点での検討、暗号鍵管理システム内でのポリシー／コンポーネント／デバイスの選択、決定事項の明示、詳細仕様や理由を含めた全ての決定方針の文書化、等）
SP800-152 A Profile for U.S. Federal Cryptographic Key Management Systems	連邦政府機関や請負業者が全ての暗号鍵や関連メタデータを管理するために利用する連邦暗号鍵管理システムに対する要求事項を明示 ・暗号鍵管理システムの設計者／実装者： 適切なセキュリティサービスや鍵管理機能の選択／実装を支援 ・連邦暗号鍵管理システムの調達者／管理者／サービス利用機関：適切な暗号鍵管理システムの選択を支援

各ガイドラインの想定読者や目的は表 1-3 のとおりである。簡単に言えば、SP800-57 Part 1 では「鍵管理で扱われる要素ごとの一般的なガイダンス」について記載されており、特に、鍵の種別、暗号利用期間／鍵の有効期間、鍵管理のフェーズと機能といったトピックが取り上げられている。また、SP800-130 では「暗号鍵管理システムの設計書に指定すべきことを包括的に記したフレームワーク」を提示しており、暗号鍵管理システムポリシーに沿って複数のセキュリティメカニズムを組み合わせてプロファイルを作成するための指針を示している。

これらのガイドラインに記載された内容から、鍵管理を考えるうえでのあるべき構造を図 3.2.2 のように整理し、鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした。構成要素としては以下の四つからなる。

①「Guidance」：鍵管理についての技術的な理解を助け、推奨設定などを提供する文献。例えば、SP800-57 part 1、同 part 3、CRYPTREC 暗号リスト、リストガイド（鍵管理）、SSL/TLS 暗号設定ガイドライン、などが該当する。

②「Framework Requirements」：あらゆるケースにおける鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項を包括的に一覧として取りまとめたもの。SP800-130 が代表例である。あらゆるケースに適用できるように、採用すべき具体的な技術仕様は規定しておらず、あくまで③Profile Requirements や④System Requirements を具体的に検討・設計する際の考え方や検討項目を示す、設計手引書的な位置づけのものである。

③「Profile Requirements」：業界（セクタ）固有の特性や環境を踏まえた共通的な条件や設計ポリシーに基づき、①Guidance の技術的根拠を加味して、②Framework Requirements に沿って、業界（セクタ）内で共通に実現すべき要求事項（設計方針・運用要件等）を規定したもの。例えば、SP800-152 は、米国政府システム共通の暗号鍵管理システムとしての要求事項が規定されたものである。

④「System Requirements」：③Profile Requirements に適合するように、システム個別の環境／条件を考慮して作成された、実際の暗号鍵管理システムが実現すべき具体的な設計仕様書や運用マニュアル等のこと。システムが依存する環境や条件と①Guidance の技術的根拠の両方を加味して、具体的な技術仕様として取りまとめられる。

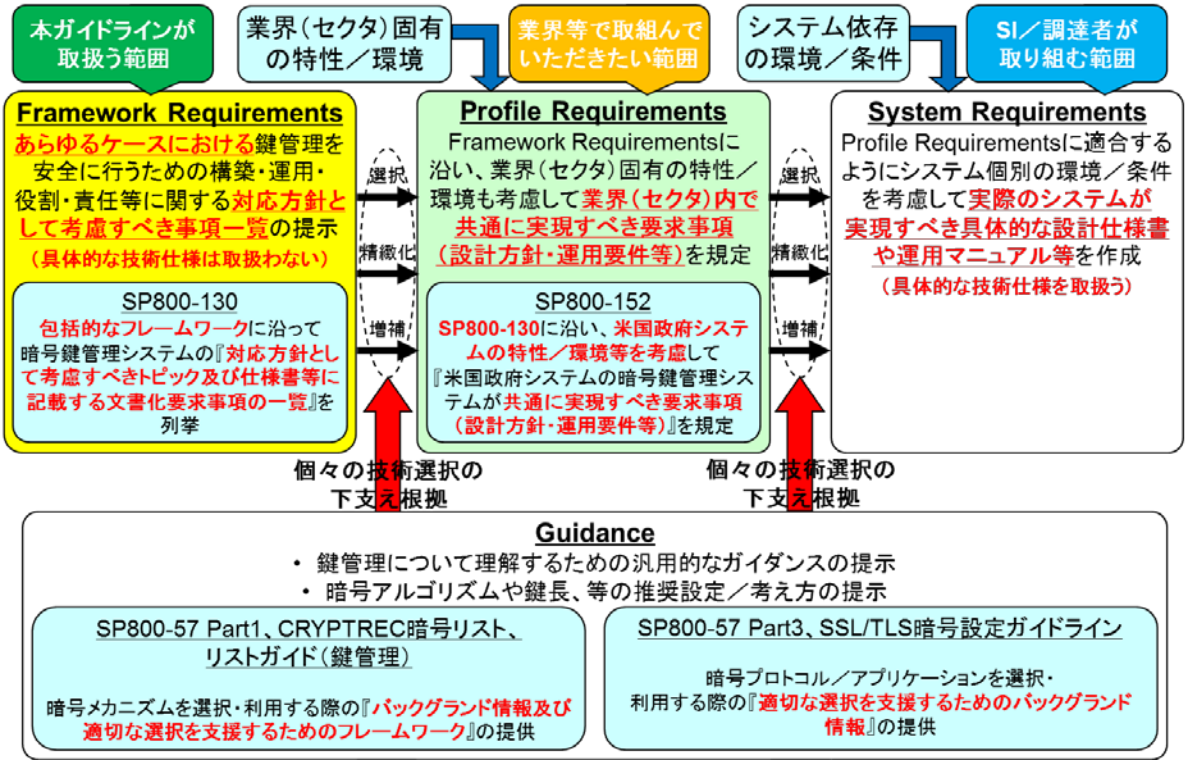


図 3.2.2　鍵管理を考えるうえでのあるべき構造

暗号技術活用委員会としては、①Guidance に含まれるガイドラインだけでは鍵管理ガイドラインとして不十分であり、②Framework Requirements を扱うガイドラインを作成すべきと判断し、SP800-130 をベースに作業を行うこととした。なお、③Profile Requirements や④

System Requirements については、個別の要件や環境等に依存する側面が強くなると考えられるため、各業界等で取り組んでいただくことを期待している。

暗号鍵管理システム設計指針（基本編）のドラフト素案の取りまとめ

SP800-130 では、暗号鍵管理システムを構築するうえで考えるべき検討項目が網羅的にカバーされており、この範囲をベースに考えれば漏れはほとんどないと思われる。しかし、検討すべき項目（Framework Requirements）が全部で 258 個もあり、かつ記載内容も教科書的な並びになっているため、必要な個所を見つけ出すことが難しい。

一方、日本では、今まで SP800-130 のような暗号鍵管理システムの設計指針の基準となる包括的・統一的な鍵管理ガイドラインが作られていないため、「鍵管理」のあり方や考え方が十分に解説されていなかった。その結果、Guidance に含まれるガイドラインを「鍵管理ガイドライン」としてきた経緯もあり、Guidance に記載がある特定の項目（例えば、暗号アルゴリズムや鍵長など）については細かく規定しているのにも関わらず、鍵管理上は重要なのに Guidance が扱っていない項目（例えば、鍵のライフサイクルや安全な鍵の保管方法、危殆化時の対策など）については規定がなかったり抽象的な記述の規定にとどまったりといったことが懸念される。このことは、鍵管理（システム）という視点で見てみると、規定した内容の粒度にムラを生じさせるということであり、システム全体の安全性確保を困難にする原因になると推察される。

そこで、暗号技術活用委員会では、イントロダクションとして鍵管理のあり方や考え方を解説し、技術的には SP800-130 の理解を深める解説書・利用手引きとして活用するための「暗号鍵管理システム設計指針（基本編）」を「鍵管理ガイドライン」として位置付けることとした。

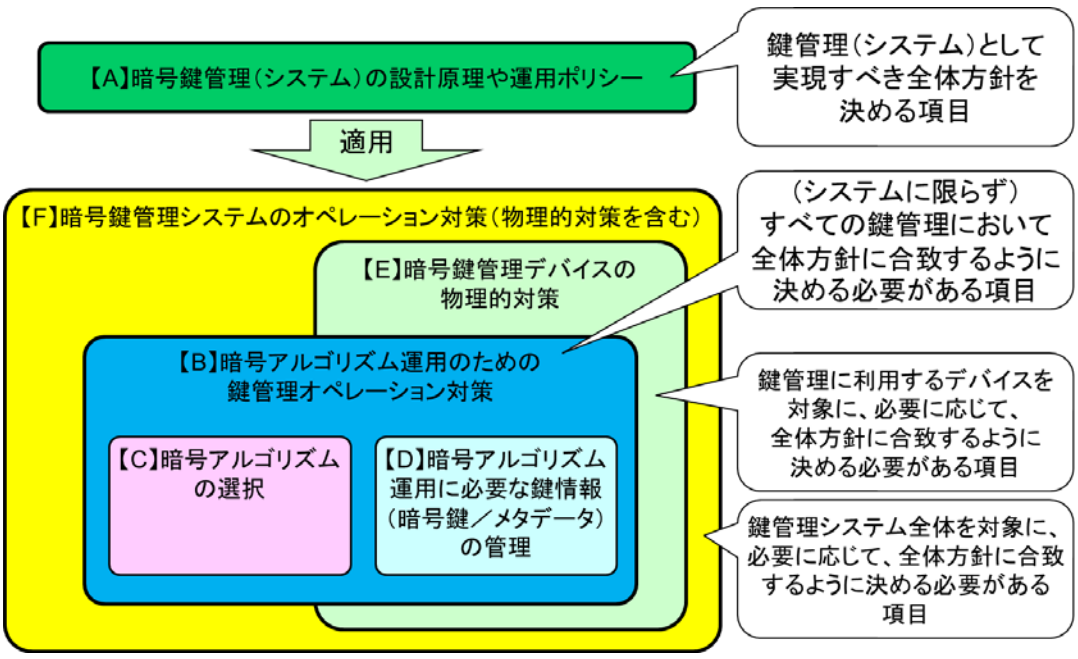


図 3.2.3　鍵管理における目的

その方針に基づき、(i) SP800-130 全体の日本語訳を作成するとともに、(ii) SP800-130 に記載されているトピックやFramework Requirements を『鍵管理における目的』に応じた対象範囲に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化し、分かりやすく表現することを目指している。具体的には、どのような目的のためにどのような項目を取り扱わなければならないのかを関係性が分かるように、六つの目的に分類・再構築する方向で、ドラフト素案の取りまとめを行っている（図 3.2.3、図 3.2.4 参照)。

2章（フレームワークの基本）:フレームワークの基本的な概念をカバーし、フレームワークの概要を記載
3章（目的）:堅牢な暗号鍵管理システム(CKMS)の目的を定義
4章（セキュリティポリシー）:システム構成、及び情報管理、情報セキュリティ、CKMSセキュリティ並びに他の関連するセキュリティポリシーの必要性について記載
5章（役割と責任）:CKMSをサポートする役割と責任を提示
6章（暗号鍵とメタデータ）:CKMSの最も重要な要素(利用可能な鍵とメタデータの定義、及び鍵とメタデータの管理機能、等)を包括的に記載
7章（相互運用性と移行）:相互運用性と将来ニーズに対応するための容易な移行能力の必要性について記載
8章（セキュリティコントロール）:典型的なCKMSに適用されるセキュリティコントロールを記載
9章（テストとシステム保証）:セキュリティテストと保証について記載
10章（災害復旧）:一般及びCKMS特有の災害復旧について記載
11章（セキュリティアセスメント）:CKMSのセキュリティアセスメントについて記載
12章（技術的課題）:暗号アルゴリズム、鍵確立プロトコル、デバイス、量子コンピュータに関する新しい攻撃によってもたらされる技術的課題について記載

	目的	取扱い項目
A	暗号鍵管理（システム）の設計原理や運用ポリシー	セキュリティポリシー
		暗号鍵管理システムの構築環境／利用条件
		将来的な移行対策
B	暗号アルゴリズム運用のための鍵管理オペレーション対策	鍵情報のライフサイクル
		鍵情報のライフサイクル管理機能
		鍵情報の保管方法
		鍵情報の鍵確立方法
		鍵情報の危殆化時の BCP 対策
C	暗号アルゴリズムの選択	暗号アルゴリズムの安全性
D	暗号アルゴリズム運用に必要な鍵情報（暗号鍵／メタデータ）の管理	鍵情報（暗号鍵／メタデータ）の選択
		鍵情報の保護方針
E	暗号鍵管理デバイスの物理的対策	鍵情報へのアクセスコントロール
		セキュリティ評価・試験／システム保証
F	暗号鍵管理システムのオペレーション対策（物理的対策を含む）	暗号鍵管理システム（物理／OS とデバイス／ネットワーク）へのアクセスコントロール
		災害発生時の BCP／復旧対策（バックアップ）

図 3.2.4　SP800-130 目次と暗号鍵管理システム設計指針（基本編）（ドラフト素案）との対比

３．２．３．暗号技術活用委員会の開催状況

2018 年度に２回開催された暗号技術活用委員会での審議概要は表 3.2.1 のとおりである。この他、暗号技術活用委員会とは別に、鍵管理ガイドラインについての技術検討会合を開催した。

表 3.2.1　暗号技術活用委員会の開催状況

回	開催日	議題
第１回	2018 年９月６日	・活用委員会活動計画の確認 ・鍵管理に関するフレームワークについての検討
技術検討会合	2018 年 12 月 26 日	・鍵管理ガイドラインのドラフト素案作成に向けた技術的検討
第２回	2019 年３月 14 日	・鍵管理ガイドラインのドラフト素案の審議 ・次期 CRYPTREC 暗号リスト策定に向けた方針についての検討

４．今後のCRYPTRECの活動について

CRYPTREC では、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、鍵管理の安全な運用に向けた取組など、暗号をとりまく環境変化に応じた新たなニーズへの対応などに取り組むこととしている。

暗号技術検討会の下に、大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件等を検討するための「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」を新たに設置することとした。また、暗号技術評価委員会においては、引き続き、暗号技術の安全性に係る監視・評価及び実装に係る技術の監視・評価を行うとともに、同委員会の下に設置された暗号技術調査 WG において、素因数分解の困難性に関する計算量の予測図の更新、耐量子計算機暗号の共通鍵暗号への影響の調査を行う。暗号技術活用委員会においては、2019 年度末の完成を目途に鍵管理ガイドラインの作成作業等を行う。なお、両委員会の範囲を超えるものについては、必要に応じて、暗号技術検討会で審議・判断する。

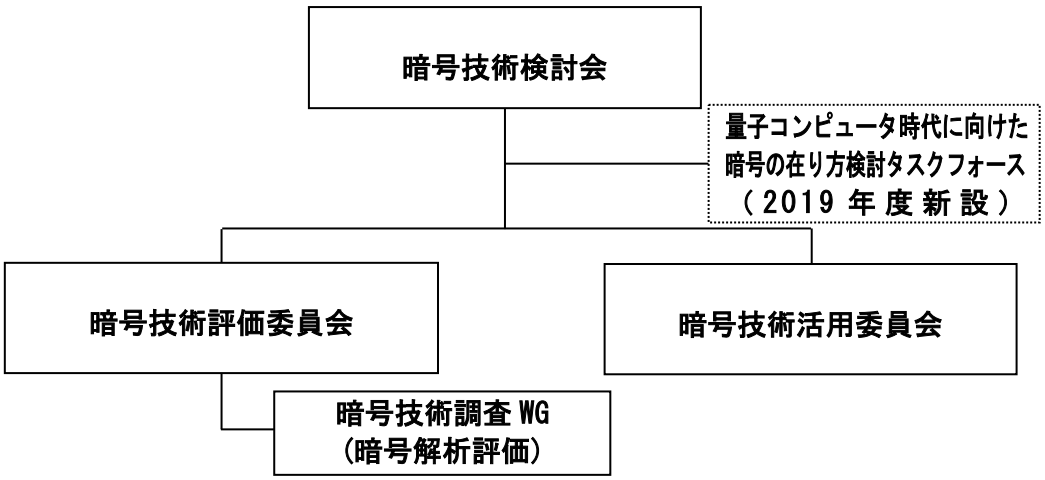


図 4.1.1　2019 年度 CRYPTREC の体制図（予定）

参考資料

CRYPTREC LS-0001-2012R4

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）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか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。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号(注2)	該当なし
	128 ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報セキュリティ担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

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

（注2） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

（注13） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM (Key Encapsulating Mechanism) – DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

（注6） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注7） 平文サイズは 64 ビットの倍数に限る。

（注12） ハッシュ長は 256 ビット以上とすること。

（注14） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

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とCRYPTRECにより確認された暗号技術[4]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。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号(注15)	3-key Triple DES
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注16)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号		該当なし
エンティティ認証		該当なし

（注8） 「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）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注15） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	（注１０）	128-bit RC4 は、 SSL(TLS1.0 以上)に限定して利用すること。	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。
平成28年 3月29日	推奨候補 暗号リスト （技術分類： ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)
	（注１２）	[新規追加]	ハッシュ長は 256 ビット以上とすること。
平成29年 3月30日	推奨候補 暗号リスト （技術分類： ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128(注12) SHAKE256(注12)
平成30年 3月29日	（注２） （注６）	より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。
	（注１５）	[新規追加]	
	電子政府推奨 暗号リスト （技術分類： 共通鍵暗号）	3-key Triple DES(注3)	該当なし
	（注３）	3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。 １）NIST SP 800-67 とし	[削除]

		て規定されていること。 ２）デファクトスタンダードとしての位置を保っていること。	
	運用監視暗号リスト（技術分類：共通鍵暗号）	該当なし	3-Key Triple DES（注１５）
	電子政府推奨暗号リスト	［技術分類の新設］	技術分類：認証暗号 暗号技術：該当なし
	推奨候補暗号リスト		技術分類：認証暗号 暗号技術： ChaCha20-Poly1305
	運用監視暗号リスト		技術分類：認証暗号 暗号技術：該当なし
	（注１３） （注１４） （注１６）	［新規追加］	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		