暗号技術活用委員会活動報告

2019年7月12日

暗号技術活用委員会 委員長
（横浜国立大学 教授）
松本　勉

目次

1．暗号技術活用委員会　概要

2017／2018年度 CRYPTREC体制

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会

事務局：総務省，経済産業省

（1）CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
（2）CRYPTREC暗号リストの改定に関する調査・検討
（3）関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

暗号技術評価委員会

事務局：NICT, IPA

（1）暗号技術の安全性及び実装に係る監視及び評価
（2）新世代暗号に係る調査
（3）暗号技術の安全な利用方法に関する調査

暗号技術調査WG
（暗号解析評価）

暗号技術活用委員会

事務局：IPA, NICT

（1）暗号の普及促進・セキュリティ産業の競争力強化に係る検討
（2）暗号技術の利用状況に係る調査及び必要な対策の検討
（3）暗号政策の中長期的視点からの取組の検討

2017／2018年度 暗号技術活用委員会委員

CRYPTREC Cryptography Research and Evaluation Committees

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　主査
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	株式会社NDIAS　自動車セキュリティ事業部　マネージャー
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　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	国立研究会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

（注）2019年3月末時点

暗号技術活用委員会活動目的＆計画

CRYPTREC
Cryptography Research and Evaluation Committees

【活動目的】

暗号技術活用委員会では、**情報システム全般のセキュリティ確保に寄与**することを目的として、**暗号の取り扱いに関する観点から必要な活動**を行うものとする。
具体的には、実運用とセキュリティ確保の両面の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント

【活動計画】

2．2017年度暗号技術活用委員会　活動概要

SSL/TLS暗号設定ガイドライン改定の紹介

2017年度 暗号技術活用委員会審議状況

CRYPTREC
Cryptography Research and Evaluation Committees

回	開催日時	主な議題
第1回	2017.09.07	● SSL/TLS暗号設定ガイドラインのアップデート作業について ● 鍵管理に関する運用ガイドラインの事前検討について
報告会	2017.12.27	● SSL/TLSに関する動向及び鍵管理に関する公募調査の中間報告
第2回	2018.03.15	● SSL/TLS暗号設定ガイドラインのアップデート案について **SSL/TLS暗号設定ガイドライン改定の紹介** ● 鍵管理に関する運用ガイドライン作成に向けた今後の計画について

「SSL/TLS暗号設定ガイドライン」とは①

CRYPTREC Cryptography Research and Evaluation Committees

2013～2014年にSSL/TLSで色々な問題が起こっていた

背景1: スノーデン事件とフォワードセキュリティ

- Edward Joseph Snowden
  - 元米中央情報局CIA職員、米国家安全保障局NSAへ出向していた
  - 2013年6月13日、香港英文紙に、米国政府が世界中の数万の標的を対象に電話記録やインターネット利用を極秘裏に監視していたことを暴露
- Perfect Forward Secrecy (PFS)の重要性が再認識

背景2: BEAST, POODLE攻撃

- BEAST攻撃
  - CBCモードの脆弱性。ブロックの一部を解読。メッセージの分割などにより対処可
- POODLE攻撃
  - SSL 3.0のパディングの脆弱性。2014年12月に発見

SSL/TLS への攻撃方法に対する耐性	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
ダウンを独制的					
バージ的に使					
ブロッを利用					

背景3: 新しいプロトコル

- TLS 1.2 (RFC5246, 2008)
  - SHA-256, SHA-384のサポート
  - CBCに代わる認証付暗号利用モード(GCM, CCM)をサポート
  - 必須暗号スイート TLS_RSA_WITH_AES_128_CBC_SHA
  - 普及はそれほど進んでいない (54.5%, 2015年2月)

利用できる暗号アルゴリズム	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
128 ビットブロック暗号 (AES, Camellia)	可	可	可	不可	不可
認証付暗号利用モード (GCM, CCM)	可	不可	不可	不可	不可
楕円曲線暗号	可	可	可	不可	不可
SHA-2 ハッシュ関数 (SHA-256, SHA-384)	可	不可	不可	不可	不可

ウェブサーバ管理者の苦悩

- BEAST、POODLEなどの攻撃が次々に出てきて、自分のサイトは安全に運用されてだろうか？
- PFSは重要らしいが、どうしたらそれを満たされるだろうか？
- 携帯電話やゲーム機などのSSLしか話せないブラウザの利用者を無視できない。セキュリティとのトレードオフをどうしたらよいか
- 上司がセキュリティ技術を理解してくれない。最新のTLS1.2の重要性を納得してもらうにはどうしたらよいか

CRYPTREC Cryptography Research and Evaluation Committees

暗号に関するリテラシーがあることを前提とせずに、SSL/TLSを安全に使うためのガイドラインを作ろう

引用：CRYPTRECシンポジウム2015より

「SSL/TLS暗号設定ガイドライン」とは②

CRYPTREC Cryptography Research and Evaluation Committees

- **主な想定読者**
  - 具体的な構築・設定を行うサーバ構築者
  - サービス提供に責任を持つサーバ管理者
  - サーバ構築を発注するシステム担当者

暗号のエキスパートではない想定読者層が対象

- **2015年3月時点でのSSL/TLSの安全性と可用性（相互接続性）のバランスを踏まえた推奨暗号設定方法をガイダンス**
  - ユースケースに応じた3段階の設定基準を用意

    「高セキュリティ型」
    「推奨セキュリティ型」
    「セキュリティ例外型」

2014年後半の利用環境の実態も考慮した設定を採用

  - OpenSSLやWindows等の「設定方法例」をAppendixに記載
  - 設定確認するための「チェックリスト」も用意

大ヒット御礼

2015年5月公開後、180，000件以上のダウンロード

設定ガイドラインアップデートの必要性

CRYPTREC Cryptography Research and Evaluation Committees

3段階の設定基準

設定基準	概要	安全性	相互接続性の確保
高セキュリティ型	漏えいすると致命的または壊滅的な悪影響を及ぼすと予想される情報を通信するような場合に採用 ※とりわけ高い安全性を必要とする明確な理由があるケースが対象で、非常に高度で限定的な使い方	標準的な水準を上回る高い安全性水準を達成	最近のOSやブラ でなければ接続で ない可能性が高い
推奨セキュリティ型	漏えいすると何らかの悪影響を及ぼすと予想される情報を、安全性確保と利便性実現をバランスさせて通信するような場合に採用 ※ほぼすべての一般的な利用形態で使うことを想定	標準的な安全性水準を実現	本ガイドラインで対 とするブラウザで ば問題なく相互接 性を確保
セキュリティ例外型	脆弱なプロトコルバージョンや暗号が使われるリスクを受容したうえで、安全性よりも相互接続性に対する要求をやむなく優先させて通信するような場合に採用 ※推奨セキュリティ型への早期移行を前提として、暫定的に利用継続するケースを想定	推奨セキュリティ型への移行完了までの短期的な利用を前提に許容可能な最低の安全性水準を満たす	最新ではないフィー チャーフォンやゲー 機などを含めた、 んどのすべての機 について相互接続 を確保

12

引用：CRYPTRECシンポジウム2015より

3つのセキュリティ型の整理

要件		高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
想定対象		G2G	一般	レガシー携帯電話を含む
暗号スイートの（暗号化の）セキュリティレベル		①256 bit ②128 bit	①128 bit ②256 bit	① 128 bit ② 256 bit ③ RC4, Triple DES
暗号アルゴリズム	鍵交換	DHE 2048 bit ECDHE 256 bit	DHE 1024 bit以上 ECDHE 256 bit RSA 2048 bit ECDH 256 bit	DHE 1024 bit以上 ECDHE 256 bit RSA 2048 bit ECDH 256 bit
	暗号化	AES 256, 128 CAMELLIA 256, 128	AES 256, 128 CAMELLIA 256, 128	AES 256, 128 CAMELLIA 256, 128 RC4 DES CBC3
	モード	GCM	GCM, CBC	
	ハッシュ関数	SHA384, SHA256	SHA384, SHA256, SHA1	
プロトコルバージョン		TLS1.2のみ	TLS1.2 ～ TLS1.0	TLS1.2～1.0, SSL 3.0
証明書鍵長		鍵長2048ビット以上のRSA または 鍵長256ビット以上のECDSA		
証明書でのハッシュ		SHA256		SHA256, SHA1

14

2015年3月時点ではバランスが取れていても
2017年ではバランスが取れているとは言えない状況に

設定ガイドラインアップデートの方向性

CRYPTREC
Cryptography Research and Evaluation Committees

- **セキュリティ例外型見直しに向けた環境が進展**
  - RC4及びSSL3.0利用禁止のRFC発行、Triple DES非推奨化への勧告
  - 認定認証事業者が発行する証明書ではSHA-1からSHA-256へ移行完了、パブリック証明書もSHA-1証明書の発行終了
  - 携帯キャリアがSHA-1証明書での接続はできないと注意喚起
- **セキュリティ例外型の利用を終了させる時期（EOL）は導入せず**
  - EOL導入で、EOLまでは利用を容認すると誤解される恐れあり

何らかの形でセキュリティ例外型の記述見直し
※ 推奨セキュリティ型以上への早急な移行を強く勧告する方向で

- **最新動向の反映**
  - TLS1.0/TLS1.1非推奨等のRFC発行
  - TLS1.2の標準搭載が大きく進展
  - TLS1.3 RFC発行に向けた作業が大詰め

高セキュリティ型についての情報提供
※ 高セキュリティ型の利用促進を図る方向で

設定ガイドラインアップデートの主なポイント①

CRYPTREC
Cryptography Research and Evaluation Committees

SSL3.0やRC4の利用を禁止するRFCが発行

TLS1.0/TLS1.1利用を非推奨化するRFCが発行

TLS1.2の標準搭載が大きく進展

TLS1.3のRFC発行＆サポートが始まる

セキュリティ例外型の利用制限を強化

「早期移行を前提とした暫定的な利用継続」
⇒「移行完了までの短期の暫定運用」

高セキュリティ型の適用範囲の拡大

「とりわけ高い安全性が必要、
非常に高度で限定的な使い方」
⇒「高い安全性が必要、高度な使い方」

TLS1.3の情報提供

本格的なプロトコルの世代交代への準備

設定ガイドラインアップデートの主なポイント②

CRYPTREC
Cryptography Research and Evaluation Committees

アップデートでの変更箇所

設定基準	概要	安全性	相互接続性
高セキュリティ型	漏えいすると**致命的または壊滅的な悪影響を及ぼす**と予想される情報を通信するような場合 ※**高い安全性を必要とする理由があるケース**が対象で、**高度な使い方**	標準的な水準を**大きく上回る高い安全性水準**を達成	**本ガイドラインで対象とするブラウザ**であれば問題なく相互接続性を確保
推奨セキュリティ型	漏えいすると**何らかの悪影響を及ぼす**と予想される情報を、安全性確保と利便性実現をバランスさせて通信するような場合 ※ほぼすべての**一般的な利用形態で使う**ことを想定	**標準的な安全性水準**を実現	**ほとんどのすべての機器**について相互接続性を確保
セキュリティ例外型	脆弱なプロトコルバージョンや暗号が使われるリスクを受容したうえで、**安全性よりも相互接続性に対する要求をやむなく優先**させて通信するような場合**であって、推奨セキュリティ型への移行完了までの短期の暫定運用としての設定基準** **※システム等の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合**	**最低限度の安全性水準を満たしているとは言えない状況。速やかな推奨セキュリティ型への移行を強く求める**	**ほとんどのすべての機器**について相互接続性を確保

3．2018年度暗号技術活用委員会　活動概要

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）』のドラフト版の紹介

2018年度 暗号技術活用委員会審議状況

CRYPTREC
Cryptography Research and Evaluation Committees

回	開催日時	主な議題
第1回	2018.09.06	● 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	2018.12.26	● 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	2019.03.14	● 鍵管理ガイドラインのドラフト素案の審議 **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）』の紹介** ● 次期CRYPTREC暗号リスト策定に向けた方針についての検討

暗号鍵管理システム設計指針（基本編）とは

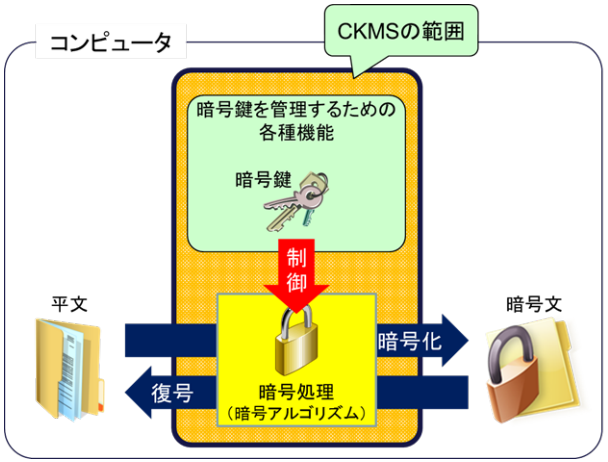
CRYPTREC
Cryptography Research and Evaluation Committees

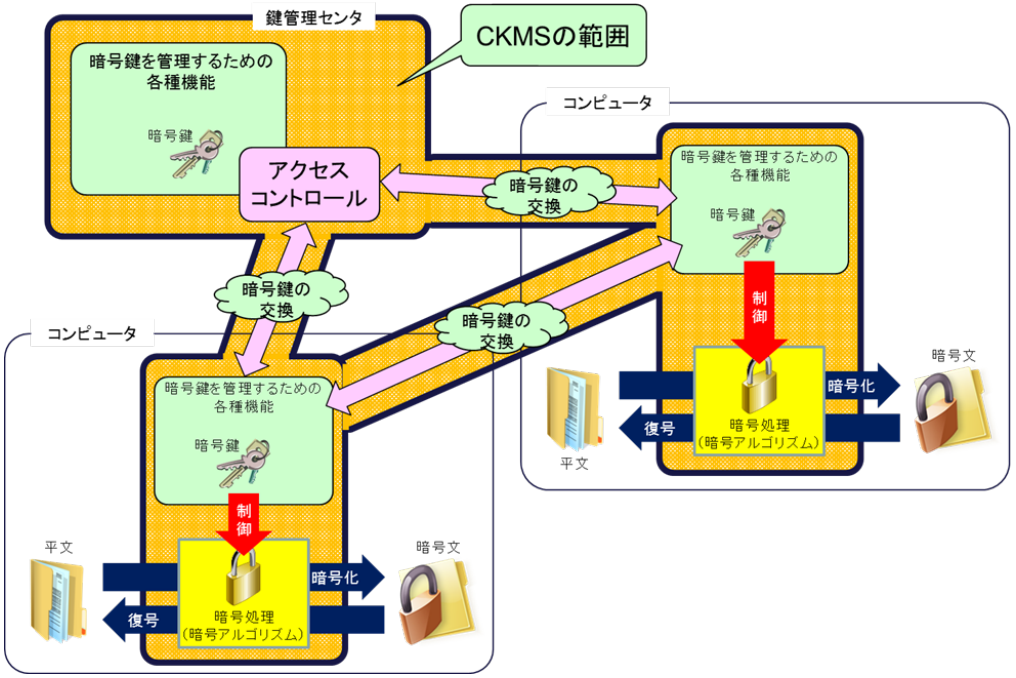
あらゆる分野／領域の暗号鍵管理システム（CKMS）を対象に暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき検討事項（Framework Requirements）を網羅的にカバーする指針

- **イントロダクションとして＞「鍵管理」の在り方／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**
  - SP800-130記載のトピックス／FR（Framework Requirements）を『暗号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
  - オリジナルな「鍵管理ガイドライン」ではない。SP800-130がベース
- **セキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能を義務づけない**
  - どのように要求事項に対応するか＞設計者に委ねられる
  - 対応方針が適正かどうかの判断＞運用管理者や調達責任者が行う

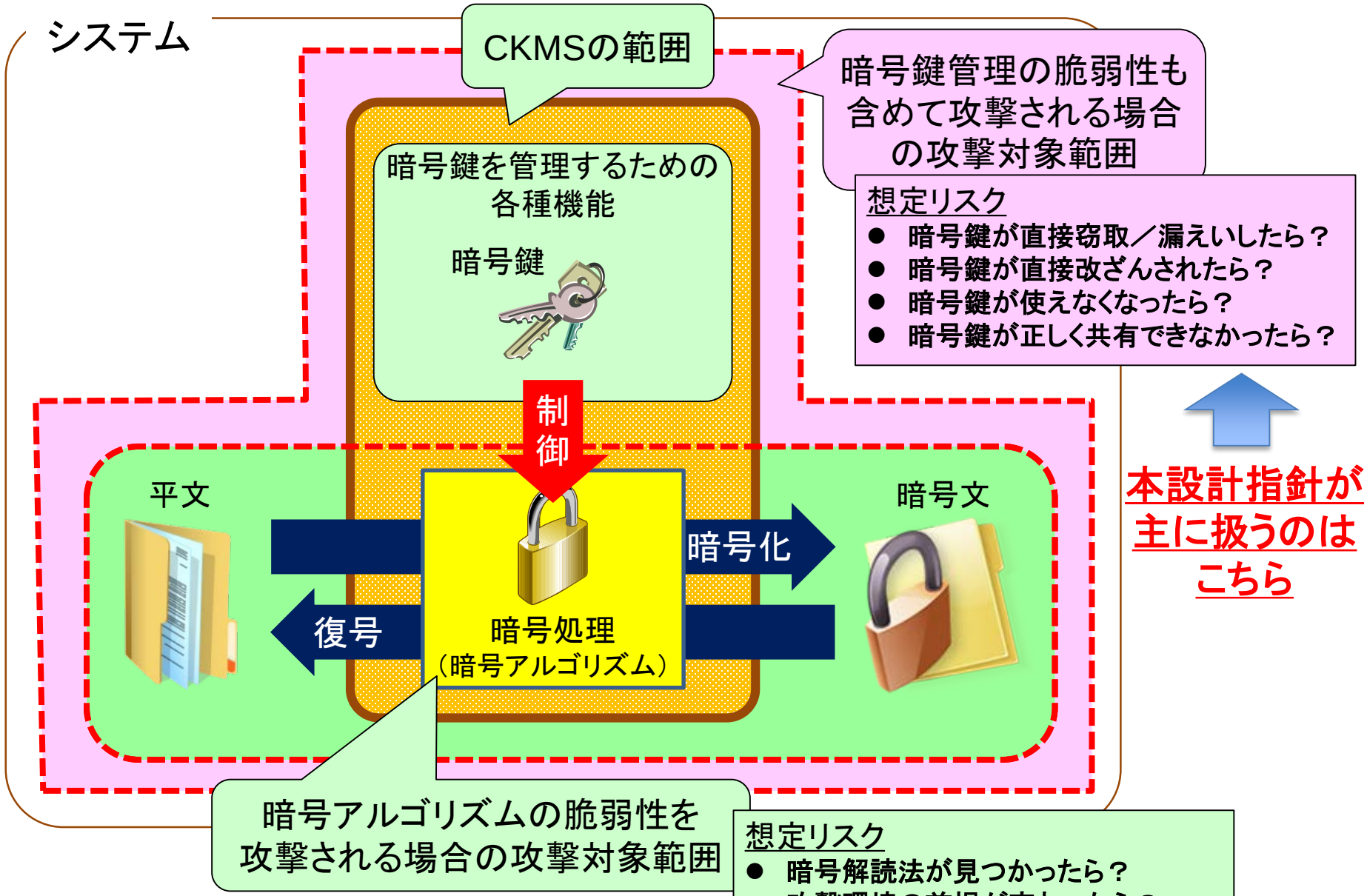
適用範囲

- あらゆる分野・あらゆる領域の全てのCKMSを対象
  - 暗号処理及びその処理で利用する暗号鍵を管理するシステム全体を包含
    - ただし、暗号処理及び暗号鍵を管理・運用するのに必要な機能以外の部分は対象外
  - 適用範囲にCKMSのシステム規模は問わない
    - どの範囲をCKMSの対象とするのかは、「暗号鍵管理システムの設計原理と運用ポリシー」の中でCKMS設計者によって具体的に定義される





暗号鍵管理の必要性


システム
CKMSの範囲
暗号鍵管理の脆弱性も含めて攻撃される場合の攻撃対象範囲
想定リスク
● 暗号鍵が直接窃取／漏えいしたら？
● 暗号鍵が直接改ざんされたら？
● 暗号鍵が使えなくなったら？
● 暗号鍵が正しく共有できなかったら？
暗号鍵を管理するための各種機能
暗号鍵
制御
平文
暗号化
復号
暗号処理
（暗号アルゴリズム）
暗号文
本設計指針が主に扱うのはこちら
暗号アルゴリズムの脆弱性を攻撃される場合の攻撃対象範囲
想定リスク
● 暗号解読法が見つかったら？
● 攻撃環境の前提が変わったら？

暗号鍵管理の考え方の枠組み

本設計指針が取扱う範囲

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

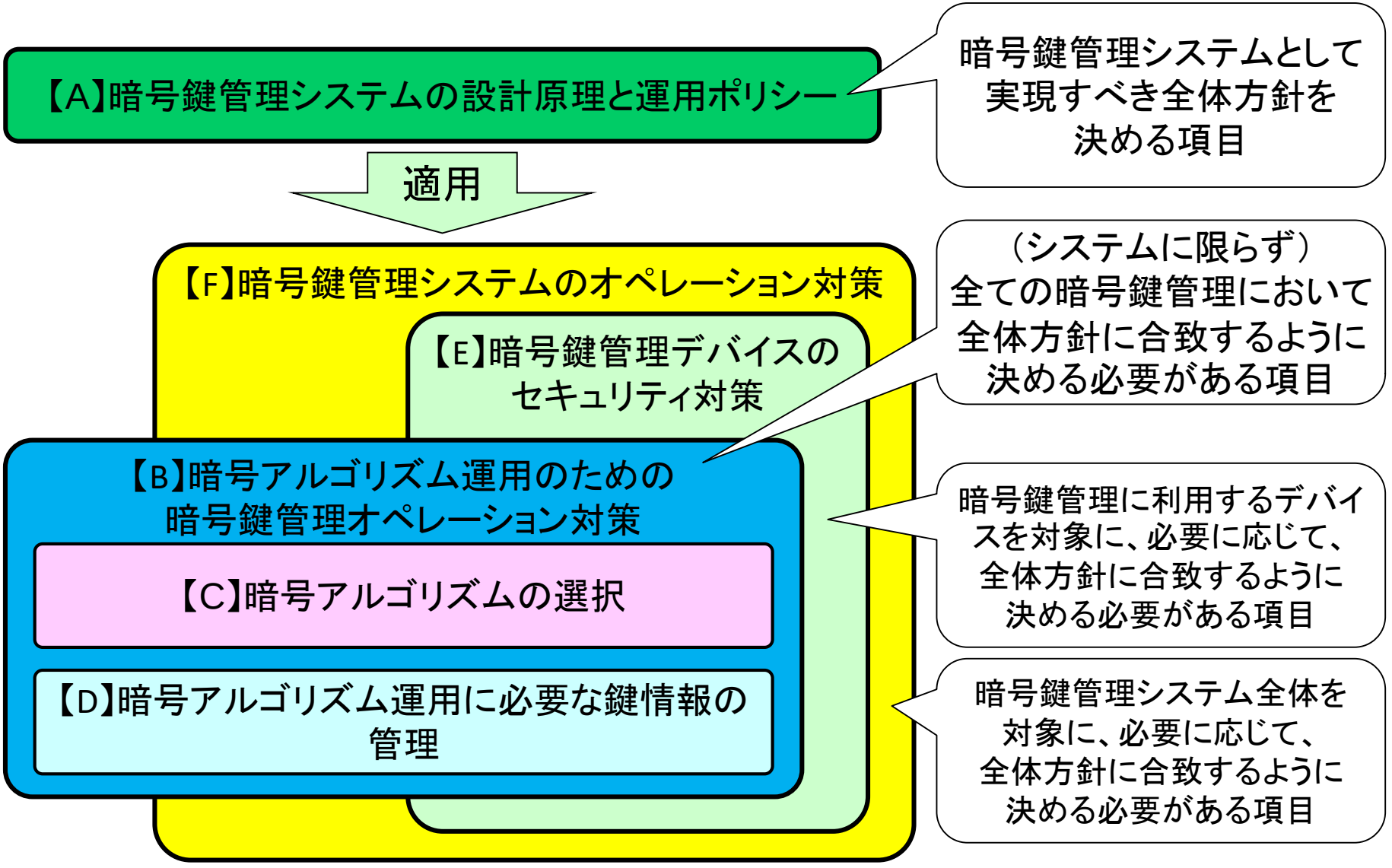
SP800-57 Part1、CRYPTREC暗号リスト、リストガイド（鍵管理）

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

暗号鍵管理における検討項目の目的別分類



本設計指針の目次①

CRYPTREC
Cryptography Research and Evaluation Committees

SP800-130該当節

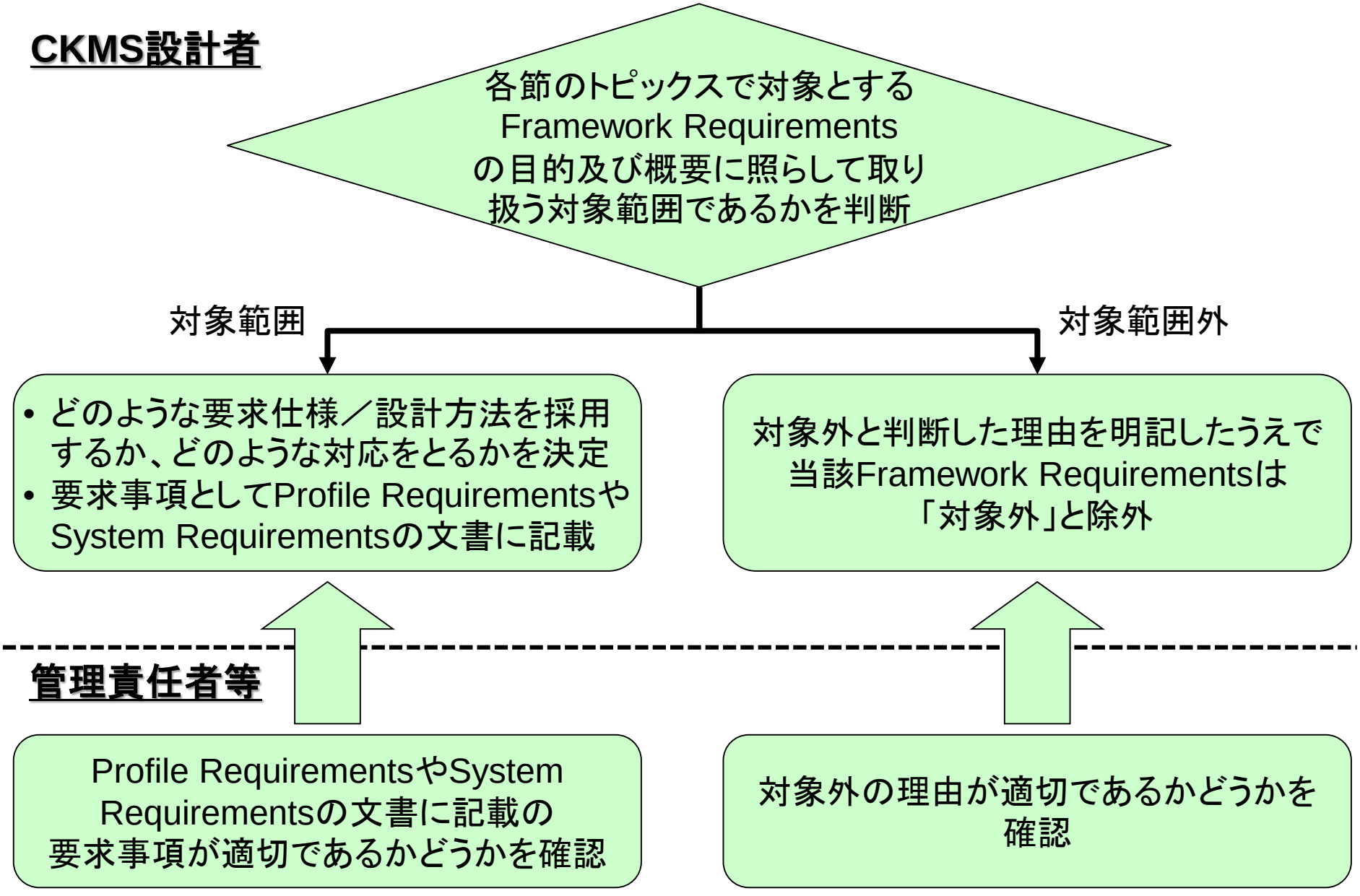
A	(4章)暗号鍵管理システムの設計原理と運用ポリシー	(4.1節)CKMSセキュリティポリシー	4.3, 4.4, 4.5
		(4.2節)情報管理ポリシー等からの要求事項	4.6, 4.7
		(4.3節)セキュリティドメインポリシー	4.9
		(4.4節)CKMSにおける役割と責任	5
		(4.5節)CKMSの構築環境／実現目標	2.10, 3.1, 3.2, 3.4, 3.5, 6.2, 7
		(4.6節)標準／規制に対する適合性	3.3, 4.8
		(4.7節)将来的な移行対策の必要性	7, 12
B	(5章)暗号アルゴリズム運用のための暗号鍵管理オペレーション対策	(5.1節)CKMS設計	2.5
		(5.2節)鍵情報のライフサイクル	6.3
		(5.3節)鍵情報のライフサイクル管理機能	6.4, 6.8
		(5.4節)鍵情報の保管方法	6.4, 6.5
		(5.5節)鍵情報の鍵確立方法	6.4, 6.6
		(5.6節)鍵情報の破損時のBCP対策	10.7
		(5.7節)鍵情報の危殆化時のBCP対策	6.8
C	(6章)暗号アルゴリズムの選択	(6.1節)暗号アルゴリズムのセキュリティ	2.1
		(6.2節)CRYPTREC暗号リスト	－

本設計指針の目次②

CRYPTREC
Cryptography Research and Evaluation Committees

			SP800-130該当節
D	(6章／7章)暗号アルゴリズム運用に必要な鍵情報の管理	(7.1節)鍵情報の種類	2.2, 6.1, 6.2
		(7.2節)鍵情報の選択	6.1, 6.2
		(7.3節)鍵情報の保護方針	6.2
E	(8章)暗号鍵管理デバイスのセキュリティ対策	(8.1節)鍵情報へのアクセスコントロール	6.4, 6.7, 6.8, 8.4
		(8.2節)セキュリティ評価・試験	9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7
		(8.3節)暗号モジュールの障害時のBCP対策	10.6
F	(9章)暗号鍵管理システムのオペレーション対策	(9.1節)CKMSへのアクセスコントロール	8.1, 8.2, 8.3
		(9.2節)システム保証	9.8
		(9.3節)セキュリティアセスメント	11.1, 11.2, 11.3, 11.4
		(9.4節)CKMSのアクセスコントロールの危殆化時のBCP対策	6.8
		(9.5節)CKMSの障害・災害発生時のBCP対策	10.1, 10.2, 10.3, 10.4, 10.5

本設計指針の活用方法


CKMS設計者
各節のトピックスで対象とする
Framework Requirements
の目的及び概要に照らして取り
扱う対象範囲であるかを判断
対象範囲
対象範囲外
• どのような要求仕様／設計方法を採用するか、どのような対応をとるかを決定
• 要求事項としてProfile RequirementsやSystem Requirementsの文書に記載
対象外と判断した理由を明記したうえで
当該Framework Requirementsは
「対象外」と除外
管理責任者等
Profile RequirementsやSystem
Requirementsの文書に記載の
要求事項が適切であるかどうかを確認
対象外の理由が適切であるかどうかを
確認

（参考）【A】4.1　CKMSセキュリティポリシー

- **CKMSがサポートしなければならない暗号鍵及びメタデータの保護のためのルールを規定**
  - 全ての暗号鍵及びメタデータの機密性、完全性、可用性、ソース認証を保護
    - 鍵ライフサイクル全体にわたってカバー
  - 組織のより高位レベルのポリシー群と整合する必要あり
  - セキュリティ機能がCKMSセキュリティポリシーをサポートするためにいつどのように使用されるのかをCKMS設計文書に記述
  - ポリシーを守ることに責任を持つ役員・従業員がポリシーを容易に理解して自らの役割及び責任を正しく実行できるようにCKMSセキュリティポリシーは書かれるべき

#A.01	FR4.1 （4.3節）	CKMS設計は、実行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。
#A.02	FR4.2 （4.3節）	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行されるのか（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。

- 他のセキュリティポリシーや組織の様々なポリシーの依存に留意

#A.03	FR4.4 （4.4節）	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。
#A.04	FR4.5 （4.5節）	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】5.2　鍵情報のライフサイクル

■ CKMSとそのアプリケーションに適切な鍵状態と遷移条件を選択し定義

- 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

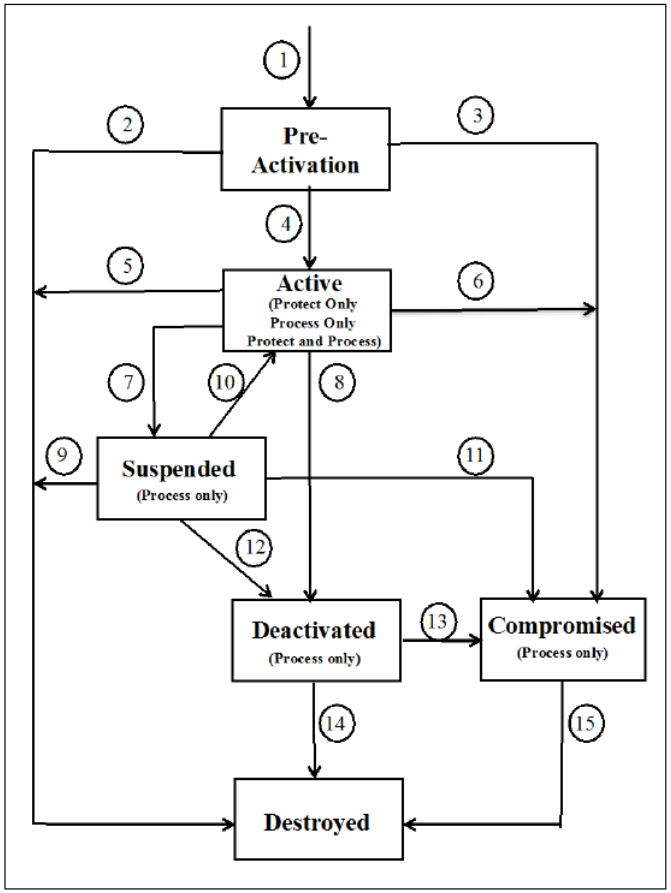


Figure 3: Key state and transition example.

#B.02	FR6.15（6.3節）	CKMS設計は、CKMSの鍵が取り得る全ての状態を**明記**しなければならない。
#B.03	FR6.16（6.3節）	CKMS設計は、全てのCKMS鍵状態間の遷移、及び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。

ドラフト版を公開します

- **暗号鍵管理システム設計指針（基本編）ドラフト版**

  CRYPTREC HP:
  https://www.cryptrec.go.jp/op_guidelines.html

- **SP800-130日本語訳　ドラフト版**

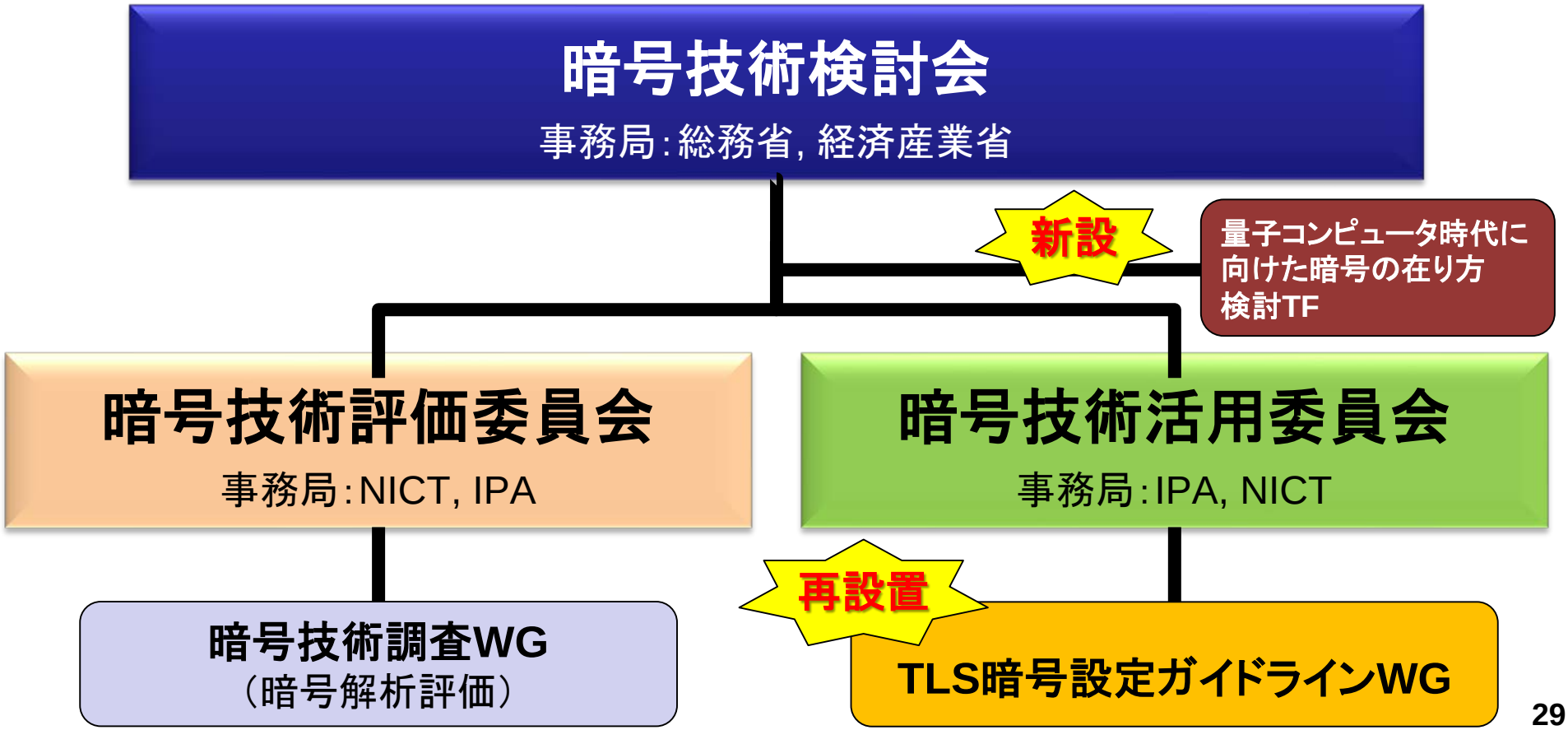
  IPA HP:
  https://www.ipa.go.jp/security/publications/nist/index.html

2019年10月31日までコメント募集！

4．2019年度暗号技術活用委員会　活動計画紹介

2019年度 暗号技術活用委員会活動計画

- **暗号鍵管理システム設計指針（基本編）の作成**
  - 外部からの意見も踏まえつつ、ガイドライン正式版を作成
  - SP800-130の日本語訳正式版も公開
- **SSL/TLS暗号設定ガイドラインの改訂**
  - SSL3.0利用禁止／TLS1.3リリースを踏まえ内容を大幅に見直す方針



2019／2020年度 暗号技術活用委員会委員

CRYPTREC
Cryptography Research and Evaluation Committees

全委員
留任

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　主査
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	株式会社NDIAS　自動車セキュリティ事業部　マネージャー
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　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	国立研究会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

（注）2019年6月末時点

TLS暗号設定ガイドラインWG　委員

CRYPTREC
Cryptography Research and Evaluation Committees

主査	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	漆嶌　賢二	富士ゼロックス株式会社　CS品質本部　品質保証部　マネージャー
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	菅野　哲	株式会社レピダム　代表取締役
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	北村　英治	グーグル合同会社　デベロッパーリレーションズ　デベロッパーアドボケイト
委員	島岡　政基	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　主任研究員
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	杉原　弘祐	セコムトラストシステムズ株式会社　情報セキュリティサービス本部　セキュアサービス2部
委員	松本　照吾	アマゾンウェブサービスジャパン株式会社　パブリックセクター コンサルティング本部 シニアセキュリティコンサルタント

（注）2019年6月末時点

乞、ご期待

CRYPTREC
Cryptography Research and Evaluation Committees

- **TLS暗号設定ガイドライン改訂の主な論点（予定）**
  - 推奨プロトコルバージョンの見直し
  - 推奨暗号スイートの見直し
  - サーバ証明書の利用方法の見直し
  - ブラウザでの標記に関する留意点の追加
  - 常時HTTPS化に伴う留意点の追加
  - 現行ガイドラインでは情報提供として記載している内容
    （鍵生成、サーバ証明書の種類や有効期間、鍵管理など）に
    ついての見直し、要求事項への格上げ、あるいは削除
  - IoT機器やSSL-VPN、クラウド利用など、
    サーバ―ブラウザ以外の利用形態での利用方法の追加
  - 代表的な製品・OSSについて具体的な設定方法の見直し

https://www.cryptrec.go.jp/