CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会活動報告

暗号鍵管理ガイダンスWG活動報告

2024年9月2日

暗号技術活用委員会 委員長
（産業技術総合研究所 フェロー、
横浜国立大学 上席特別教授） 松本　勉

暗号鍵管理ガイダンスWG　主査
（立命館大学 教授） 上原　哲太郎

目次

目次

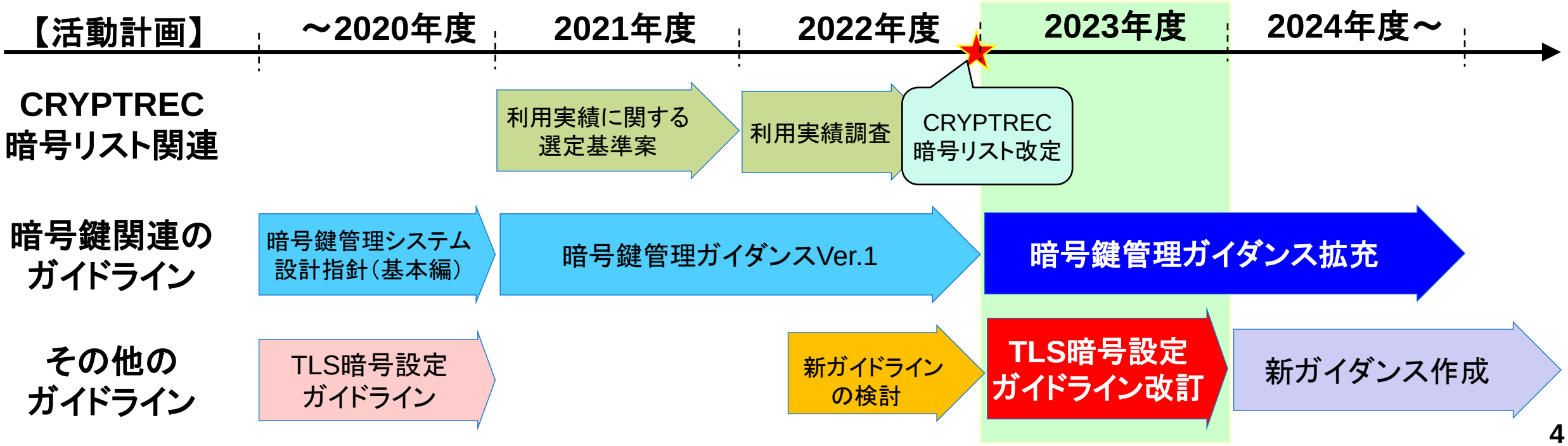
暗号技術活用委員会の活動目的および計画

【活動目的】

暗号技術活用委員会は、**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、実運用におけるセキュリティ確保の観点から、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



CRYPTREC活動体制（2023年度）

暗号技術検討会

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

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 （耐量子計算機暗号）

暗号技術活用委員会

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

暗号鍵管理ガイダンスWG

暗号技術活用委員会委員

CRYPTREC
Cryptography Research and Evaluation Committees

（注）2024年3月末時点

委員長	松本　勉	横浜国立大学　教授
委員	上原　哲太郎	立命館大学　教授
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティプログラムマネージャー
委員	菊池　浩明	明治大学　教授
委員	佐藤　直之	SCSK株式会社　シニアプロフェッショナルコンサルタント
委員	佐藤　雅史	セコム株式会社　主幹研究員
委員	須賀　祐治	株式会社インターネットイニシアティブ　シニアエンジニア
委員	田村　裕子	日本銀行　企画役
委員	手塚　悟	慶應義塾大学　教授
委員	寺村　亮一	GMOサイバーセキュリティ by イエラエ株式会社　執行役員
委員	三澤　学	三菱電機株式会社　グループマネージャー
委員	満塩　尚史	デジタル庁　セキュリティアーキテクト
委員	山口　利恵	東京大学　准教授
委員	渡邊　創	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

暗号鍵管理ガイダンスWG委員（2023年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2024年3月末時点

主査	上原　哲太郎	立命館大学　教授
委員	泉　雅明	シスコシステムズ合同会社　システムズアーキテクト
委員	漆嶌　賢二	GMOグローバルサイン株式会社　部長
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティプログラムマネージャー
委員	菅野　哲	GMOサイバーセキュリティ by イエラエ株式会社　取締役CTO of Development
委員	菊池　浩明	明治大学　教授
委員	小林　浩二	パナソニック　オートモーティブシステムズ株式会社　係長
委員	須賀　祐治	株式会社インターネットイニシアティブ　シニアエンジニア
委員	舟木　康浩	タレスDIS ジャパン株式会社　セールスエンジニアマネージャー
委員	程吉　英仁	株式会社NTTデータグループ　課長代理
委員	満塩　尚史	デジタル庁　セキュリティアーキテクト

目次

1. 暗号技術活用委員会　概要

2. 2023年度暗号技術活用委員会　活動概要
   - TLS暗号設定ガイドライン改訂版(v3.1)作成
   - 暗号鍵管理ガイダンス拡充の検討

3. 暗号鍵管理ガイダンスWG　活動概要（上原主査より）
   - 暗号鍵管理ガイダンス拡充の検討

2023年度 暗号技術活用委員会審議状況

回	開催日	議案
第一回	2023年7月11日	• 2023年度暗号技術活用委員会活動計画について • 2023年度暗号鍵管理ガイダンスWG活動計画について • TLS暗号設定ガイドライン改訂について
メール	2024年1月12日～2月15日	• TLS暗号設定ガイドライン改訂案v3.1のメール審議
第二回	2024年3月5日	• TLS暗号設定ガイドライン改訂内容について • 2023年度暗号鍵管理ガイダンスWG活動報告 • Triple DESに関する扱いについて • 2023年度暗号技術活用委員会活動報告案について

『TLS暗号設定ガイドライン』とは

■ 有識者の知見を集約したTLSを安全に使うためのBest Practice

- TLSの**安全性と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」
- 設定確認のための「チェックリスト」
- OpenSSLやWindows等の「サーバ設定方法例」

利用環境の実態を考慮して設定方法をアップデート

2015年
SSL/TLS暗号設定ガイドライン（第1.0/1.1版）

2018年
SSL/TLS暗号設定ガイドライン（第2.0版）

2020年
TLS暗号設定ガイドライン（第3.0版）

今回
2024年
TLS暗号設定ガイドライン（第3.1版）
2024年6月公開

■ 主な想定読者

暗号のエキスパートではない想定読者層が対象

- 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

TLS暗号設定ガイドライン改訂の背景

「TLS暗号設定ガイドライン（現行版ver3.0）」作成時点（2020年7月）以降のCRYPTREC成果および関連団体の動向を反映

- 「CRYPTREC暗号リスト」の改定
  - 「電子政府推奨暗号」への昇格：
    EdDSA, SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256, XTS,
    ChaCha20-Poly1305, ISO/IEC 9798-4
  - 「運用監視暗号」への降格：**3key-Triple DES**
  - 「運用監視暗号」からリスト外への降格：**RC4**, SC2000

  ※下線のアルゴリズムは IANA TLS registryに登録されているもの
- 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の策定
  - 「ビットセキュリティ基準」を導入し、これに基づいてアルゴリズムごとに強度要件を規定
  - 鍵長表現ではX25519などのCurve25519を用いた楕円曲線暗号アルゴリズムの採用可否が不明確
- TLSに関連するIETFでの動向や利用（サポート）状況の変化

TLS暗号設定ガイドラインで扱っている設定項目

■ 安全性への寄与度を考慮し、より現実的かつ実効性が高い要求設定に区分
- ●最低限の安全性を確保するために必ず満たさなければならない「遵守項目」
- ●よりよい安全性を実現するために満たすことが望ましい「推奨項目」

要求設定	遵守	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	**利用する暗号アルゴリズムと鍵長の設定**
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	**利用禁止暗号アルゴリズムを利用不可にする設定**
			公開鍵暗号の鍵長の設定
	推奨	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」でのセキュリティ強度要件の基本設定方針

CRYPTREC Cryptography Research and Evaluation Committees

ビットセキュリティ	利用上の条件	利用期間		
		2022～2030年	2031～2040年	2041～2050年
112ビット	新規に処理をする場合	移行完遂期間2)	利用不可	利用不可
	過去に処理したものを利用する場合		許容1)	
128ビット	新規に処理をする場合	利用可	利用可	移行完遂期間2)
	過去に処理したものを利用する場合			
192ビット	特になし	利用可	利用可	利用可
256ビット	特になし	利用可	利用可	利用可

1) “許容”とは、そのセキュリティ強度の暗号技術では必要なセキュリティ（暗号学的安全性）を確保するには必ずしも十分ではないレベルであると想定され得るが、その正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、過去に暗号保護が施された保護済みのデータに対して復号や検証の処理を行うことを許容する期間であることを示す。

2) “移行完遂期間”とは、そのセキュリティ強度の暗号技術では必要なセキュリティ（暗号学的安全性）を確保するには必ずしも十分ではないレベルになりつつあると想定され、この期間中に、よりセキュリティ強度の高い暗号技術及び鍵長への移行を完遂させなければならない期間であることを示す。そのため、利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定すべきであり、新規調達や更新調達を行うシステムにおいて、既存の電子政府システムとの互換性・相互接続性維持が必要でない場合や代替手段がある場合には、利用を許容すべきではないことに留意されたい。

TLS利用環境の変化

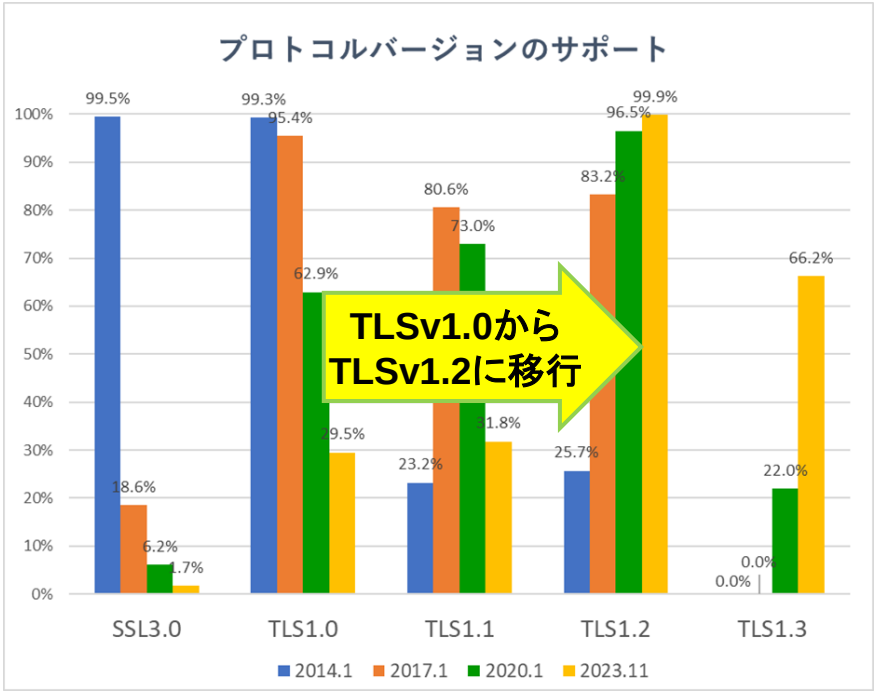
TLS1.0／1.1が排除され、TLS1.2に移行。TLS1.3のサポートが進展

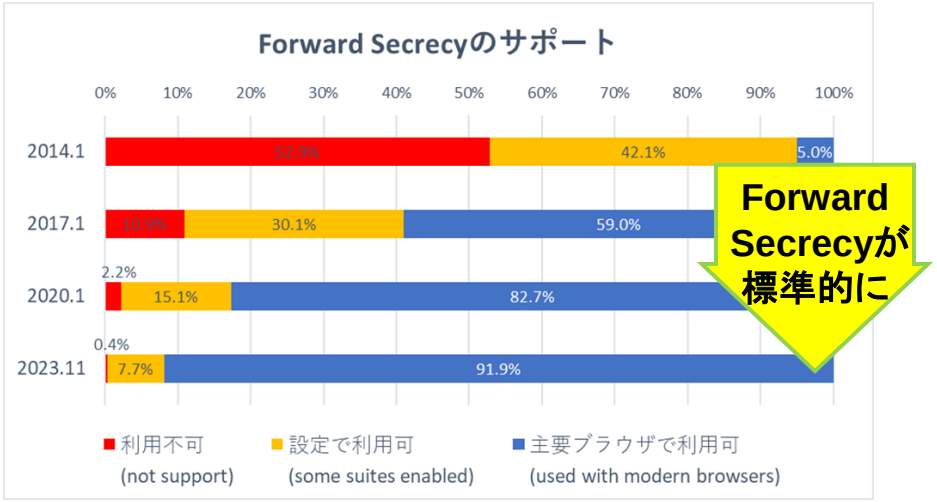
- 「Deprecating TLSv1.0 and TLSv1.1」のRFC8996発行（2021年3月）
- 主要ブラウザベンダが2020年前半にTLS1.0/1.1を無効化するアナウンス
- サポート率（2014年 → 2020年 → **2023年**）：
  TLS1.0（99.3% → 62.9% → **29.5%**）、
  TLS1.1（23.2% → 73.0% → **31.8%**）、
  TLS1.2（25.7% → 96.5% → **99.9%**）、
  TLS1.3（ー → 22.0% → **66.2%**）

Perfect Forward Secrecy*)のサポートが進展

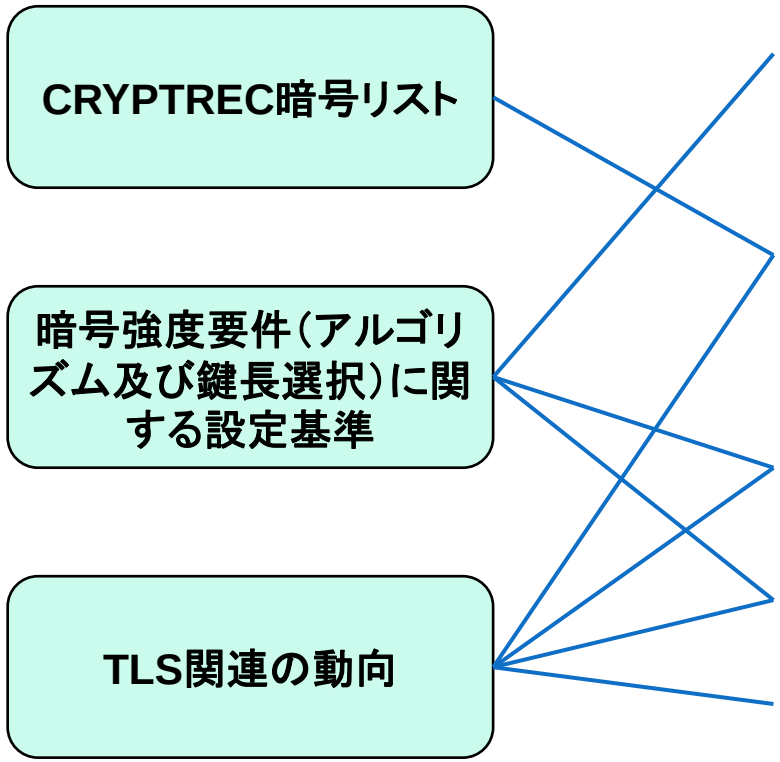
- 主要ブラウザデフォルト有効率：
  2014年 5.0% → 2020年 82.7% → 2023年 91.9%

*) 鍵交換に固定的な秘密鍵を用いず、あるセッションが危殆化しても他のセッションに影響しない。DHE/ECDHEで実現





TLS暗号設定ガイドラインv3.1での主な改訂内容



① 「鍵長」基準から「ビットセキュリティ」基準への変更

② TLSでの利用を推奨／禁止する暗号アルゴリズムの更新

③ 「セキュリティ例外型」の取り扱い

④ DHEの強度設定について推奨要件の改訂

⑤ その他の改訂項目

①「鍵長」基準から「ビットセキュリティ」基準への変更

- 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」に従い、現行版v3.0の「鍵長」をそのまま「ビットセキュリティ」に置き換え
  - ➢ [例外] セキュリティ例外型のDH／DHEの1024ビット鍵長は、対応するビットセキュリティが存在しないため、鍵長表現のままとした
- 利用する楕円曲線は「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」に記載のものから選択することを明記

TLSにおいて鍵交換アルゴリズムとして利用実績の多いX25519 (ECDHE)の許容を明確化

「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」における暗号アルゴリズム・パラメータに対する推定セキュリティ強度

セキュリティ強度（ビットセキュリティ）		112	128	192	256
公開鍵暗号（署名・守秘・鍵共有）	素因数分解型（RSA暗号・RSA署名）	鍵長2048ビット	鍵長3072ビット	鍵長7680ビット	鍵長15360ビット
	離散対数型（DH(E)、DSA）	鍵長2048ビット (L, N) = (2048, 224)	鍵長3072ビット (L, N) = (3072, 256)	鍵長7680ビット (L, N) = (7680, 384)	鍵長15360ビット (L, N) = (15360, 512)
	楕円曲線暗号（ECDH(E)、ECDSA、EdDSA）	P-224 B-233 K-233	P-256 B-283 K-283 W-25519 Curve25519 Edwards25519	P-384 B-409 K-409 W-448 Curve448 Edwards448	P-521 B-571 K-571
共通鍵暗号	ブロック暗号	なし	鍵長128ビットのAES、Camellia	鍵長192ビットのAES、Camellia	鍵長256ビットのAES、Camellia
	認証暗号	なし	なし	なし	ChaCha20-Poly1305
ハッシュ関数	HMACで使う場合	なし	SHA-1	なし	SHA-256 SHA-384 SHA-512

② CRYPTREC暗号リスト改定等を踏まえた TLSでの利用を推奨／禁止する暗号アルゴリズムの更新

CRYPTREC
Cryptography Research and Evaluation Committees

暗号アルゴリズム	改訂内容
DSA	現行版v3.0での「本ガイドラインでは積極的には利用を勧めない」から、改訂版v3.1では「今後、新規・更新時にDSAを利用すべきではない」に修正 ● FIPS186-5から削除された状況を反映
RSA-PSS	「サーバ証明書で利用可能な署名アルゴリズム」として、「推奨セキュリティ型」および「高セキュリティ型」に追加 ● 現行版v3.0ではサーバ証明書でのRSA-PSSの記載が漏れていたため
EdDSA	「サーバ証明書で利用可能な暗号」及び「暗号スイートでの利用推奨暗号アルゴリズム」への追加は行わない ● サーバ証明書ではCA/ブラウザフォーラムの規定によりEdDSAはCA署名アルゴリズムとしても、subject公開鍵としても設定できない状況にある。このため、TLSでの鍵交換時に付与する署名のアルゴリズムとしてもEdDSAを利用できないため。
ChaCha20-Poly1305	現行版v3.0で利用推奨アルゴリズムに記載済みであり、対応不要
3-key Triple DES	現行版v3.0で利用禁止アルゴリズムに記載済みであり、対応不要
RC4	現行版v3.0で利用禁止アルゴリズムに記載済みであり、対応不要
SM2（署名）、SM3、SM4	CRYPTREC暗号リストにないため、利用禁止アルゴリズムに追加

③「セキュリティ例外型」の取り扱い

- 移行を明確に促す観点から移行期限を明記した表現に変更

現行版v3.0:「推奨セキュリティ型への移行完了までの暫定運用を想定している。」

改訂版v3.1:「本ガイドラインで記載されているセキュリティ例外型の設定内容は、2029年度を目途とした改訂時に終了させる予定である。速やかに推奨セキュリティ型への移行を完了させるべきである。」

④ DHEの強度設定について推奨要件の改訂

設定基準	改訂内容
高セキュリティ型	現行版v3.0での「112ビットセキュリティ以上の鍵長（2048ビット以上）」から改訂版v3.1では「128ビットセキュリティ以上の鍵長（3072ビット以上）」に変更 ● 高セキュリティ型では、先行して「128ビットセキュリティ以上の鍵長（3072ビット以上）」にすべきであるため
推奨セキュリティ型	「112ビットセキュリティ以上の鍵長（2048ビット以上）」で変更しない ● 依然として2048ビット鍵が主流であるため
セキュリティ例外型	「1024ビット以上の鍵長」で変更しない ● 112ビットセキュリティよりはるかに弱い設定だが、以下の理由から変更しない ➢ セキュリティ例外型で設定内容を変更させるよりも、推奨セキュリティ型への変更に誘導するほうがよい ➢ 設定内容を変更すると「セキュリティ例外型」の継続利用を容認したかのように誤解される恐れがある ● 「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」に対応するビットセキュリティ基準がないため、例外的に鍵長表現のままとした

⑤ その他の改訂項目および参考意見

- 「Certificate Transparency（全世界のサーバ証明書が確認できる仕組み）」の節を追加
  - サーバ認証用証明書の誤発行や不正発行のインシデントが相次いで発生した。Certificate Transparency（CT）は、それらのインシデントを受けて実施された取り組みの1つ
- 「ブラウザを利用する際に注意すべきポイント」について、Microsoft、Google、Mozilla、Appleの各社ブラウザの最新情報を反映
  - サポート中のバージョン情報、TLSに関わる設定項目
- IoT普及の観点から組み込み系に向けた補足文書検討の意見があったが、本ガイドラインの主たる読者層とは対象者が異なると想定され、今回の改訂対象とはしていない
  - 今後の新規ガイドラインの作成や拡充の候補とする

暗号鍵管理ガイダンスの拡充

■ 暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計において考慮する点を解説するガイダンス

● 詳細は暗号鍵管理ガイダンスWG活動報告（上原主査）にて紹介

■「暗号鍵管理ガイダンスVer.1.0（2022年度発行）」に記載していない章をまとめる

● 2023年度は**2章分（赤字部分）**の記載ダイジェストを作成、今年度にガイダンス拡充分を完成予定

暗号鍵管理システム設計指針（基本編）	暗号鍵管理ガイダンスVer.1.0（2022年度発行）	暗号鍵管理ガイダンス拡充分（別冊時）
1. はじめに	1. はじめに	1. はじめに
2. 暗号鍵管理の在り方	（1章に集約）	（1章に集約）
3. 本設計指針の活用方法	（1章に集約）	（1章に集約）
4. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー	←----------	**2. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー**
5. 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	2. 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	
6. 暗号アルゴリズムの選択	3. 暗号アルゴリズムの選択	
7. 暗号アルゴリズム運用に必要な鍵情報の管理	4. 暗号アルゴリズム運用に必要な鍵情報の管理	
8. 暗号鍵管理デバイスへのセキュリティ対策	←----------	**3. 暗号鍵管理デバイスへのセキュリティ対策**
9. 暗号鍵管理システム（CKMS）のオペレーション対策	←----------	4. 暗号鍵管理システム（CKMS）のオペレーション対策

目次

1. 暗号技術活用委員会　概要

2. 2023年度暗号技術活用委員会　活動概要
   - TLS暗号設定ガイドライン改訂版(v3.1)作成
   - 暗号鍵管理ガイダンス拡充の検討

3. 暗号鍵管理ガイダンスWG　活動概要（上原主査より）
   - 暗号鍵管理ガイダンス拡充の検討

暗号鍵管理ガイダンスWG委員（2023年度）

CRYPTREC Cryptography Research and Evaluation Committees

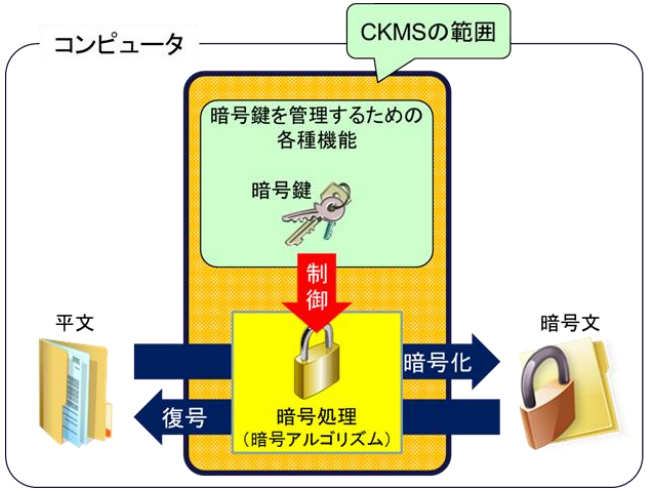
（注）2024年3月末時点

主査	上原　哲太郎	立命館大学　教授
委員	泉　雅明	シスコシステムズ合同会社　システムズアーキテクト
委員	漆嶌　賢二	GMOグローバルサイン株式会社　部長
委員	垣内　由梨香	マイクロソフト株式会社　セキュリティプログラムマネージャー
委員	菅野　哲	GMOサイバーセキュリティ by イエラエ株式会社　取締役CTO of Development
委員	菊池　浩明	明治大学　教授
委員	小林　浩二	パナソニック　オートモーティブシステムズ株式会社　係長
委員	須賀　祐治	株式会社インターネットイニシアティブ　シニアエンジニア
委員	舟木　康浩	タレスDIS ジャパン株式会社　セールスエンジニアマネージャー
委員	程吉　英仁	株式会社NTTデータグループ　課長代理
委員	満塩　尚史	デジタル庁　セキュリティアーキテクト

『暗号鍵管理システム設計指針（基本編）』とは

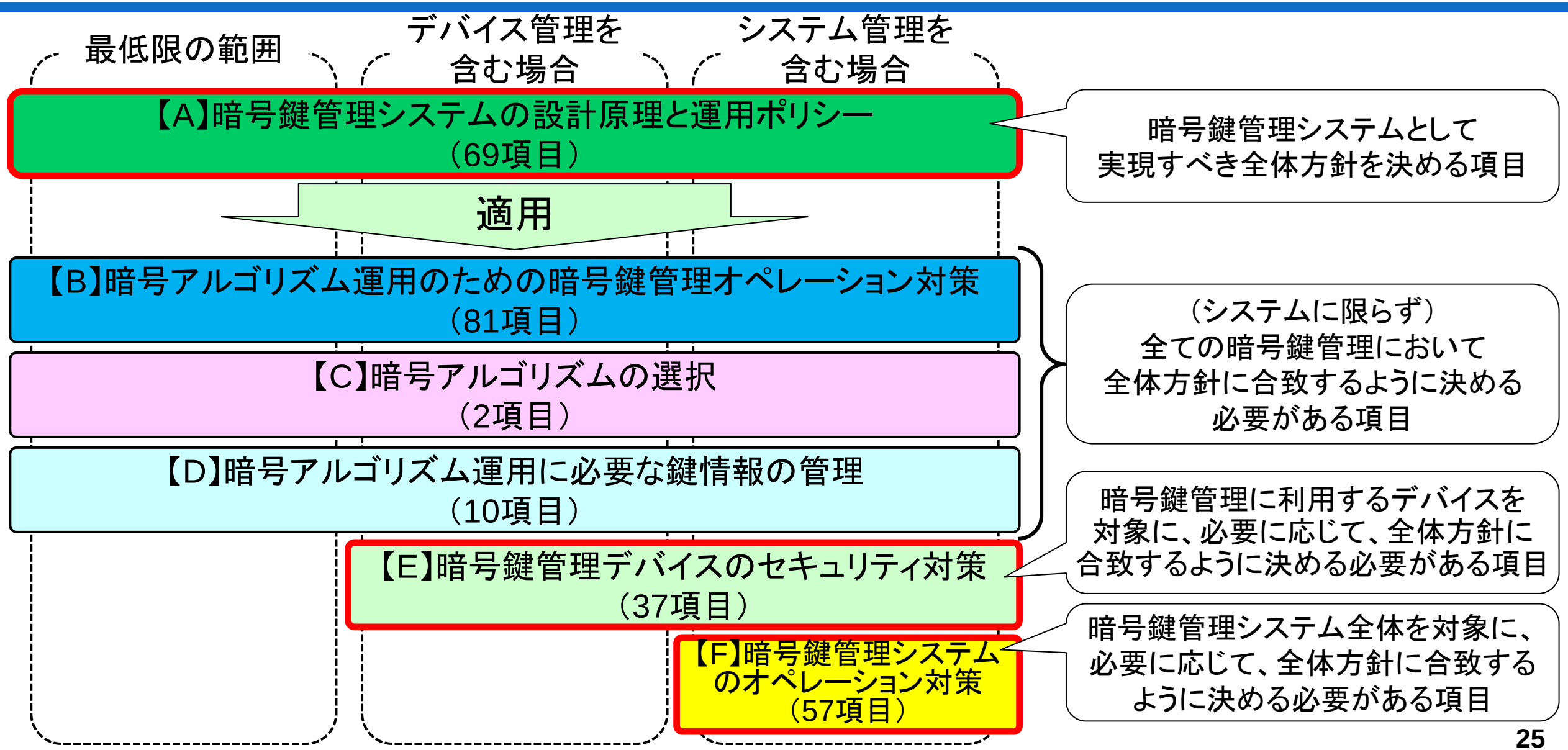
あらゆる分野／領域の暗号鍵管理システム（CKMS）を対象に
暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する
対応方針として考慮すべき検討事項（Framework Requirements）を網羅的にカバーする指針

- イントロダクション＞「鍵管理」の在り方／考え方の解説
- 技術的な中身＞NIST SP800-130*の理解を深める利用手引き
  - NIST SP800-130の 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
  - NIST SP800-130：A Framework for Designing Cryptographic Key Management Systems



- セキュリティ要求事項は定義せず、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

『暗号鍵管理システム設計指針（基本編）』の構成



『暗号鍵管理ガイダンス』とは

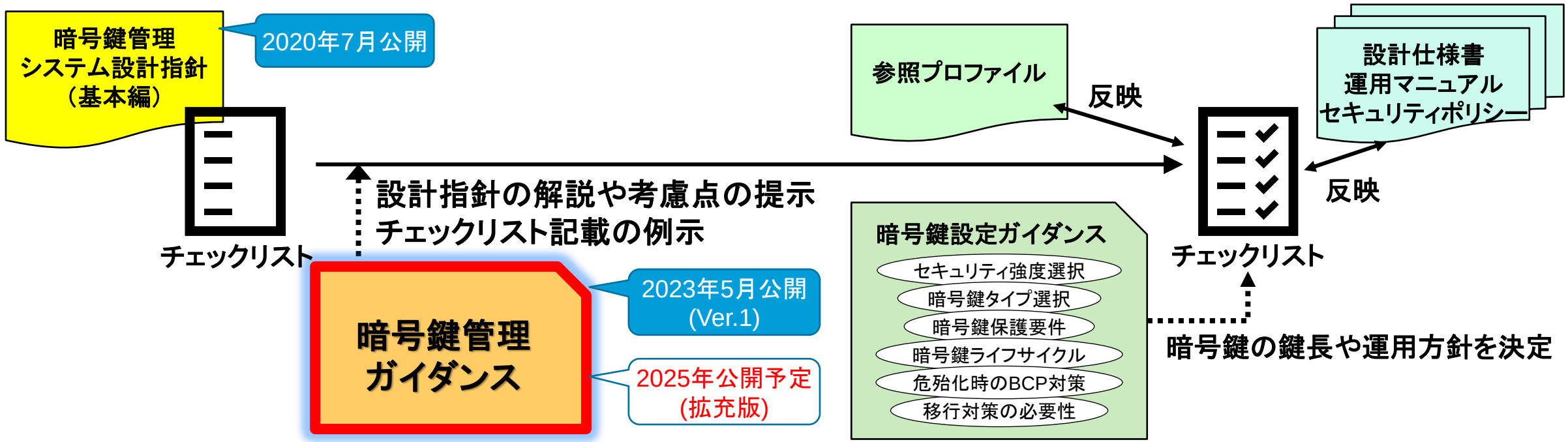
「暗号鍵管理システム設計指針（基本編）」の**解説書**

- 暗号鍵管理プロファイルを作成するためのガイダンス
- 暗号鍵管理で必要となる項目について、シンプルなモデルを例示し説明

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

Profile Requirements
Framework Requirementsに沿い、セクタ固有の特性／環境も考慮して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

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



暗号鍵管理ガイダンスの概要

■ 位置づけ

- 「暗号鍵管理システム設計指針（基本編）」を詳しく解説し、記載が求められる項目について検討する際の**有用な副読本**となることを目的とする
  具体的には、「暗号鍵管理システム設計指針（基本編）」で記載されている項目に関して、各検討項目についての**解説・考慮点を具体的に説明**する
- 理解を助けるため、**シンプルなモデル（トイモデル）を例示**し説明する
- トイモデルを用いた説明では、鍵管理における**要求や思想が理解できるような記載**を行う（**※“推奨しているわけではない”ことに注意**）
- 暗号鍵管理における特に注意すべきリスクを説明する

■ 想定読者

- 暗号鍵管理機能を持つシステム設計者

暗号鍵管理ガイダンスの拡充

■「暗号鍵管理ガイダンスVer.1.0（2022年度発行）」に記載していない章をまとめる

- 2023年度は**2章分（赤字部分）**の記載ダイジェストを作成、今年度にガイダンス拡充分を完成予定

暗号鍵管理システム設計指針（基本編）	暗号鍵管理ガイダンスVer.1.0（2022年度発行）	暗号鍵管理ガイダンス拡充分（別冊時）
1. はじめに	1. はじめに	1. はじめに
2. 暗号鍵管理の在り方	（1章に集約）	（1章に集約）
3. 本設計指針の活用方法	（1章に集約）	（1章に集約）
4. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー	←----------→	**2. 暗号鍵管理システム（CKMS）の設計原理と運用ポリシー**
5. 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	2. 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	
6. 暗号アルゴリズムの選択	3. 暗号アルゴリズムの選択	
7. 暗号アルゴリズム運用に必要な鍵情報の管理	4. 暗号アルゴリズム運用に必要な鍵情報の管理	
8. 暗号鍵管理デバイスへのセキュリティ対策	←----------→	**3. 暗号鍵管理デバイスへのセキュリティ対策**
9. 暗号鍵管理システム（CKMS）のオペレーション対策	←----------→	4. 暗号鍵管理システム（CKMS）のオペレーション対策

4章　暗号鍵管理システム（CKMS）の設計原理と運用ポリシー

CKMS設計において実現すべき全体方針を定める

- 4.1 CKMSセキュリティポリシー
- 4.2 情報管理ポリシー等からの要求事項
- 4.3 ドメインのセキュリティポリシー

} CKMSのセキュリティポリシー（CKMSセキュリティポリシー、他の関連するセキュリティポリシー）

- 4.4 CKMSにおける役割と責任
- 4.5 CKMSの構築目標及び実現目標
- 4.6 標準・規制に対する適合性

} CKMSの概要設計（エンティティと権限の定義、構築目標、関連する標準・規制）

- 4.7 将来的な移行対策の必要性

} 将来の移行対策（暗号アルゴリズムや鍵管理デバイスの移行、技術の進歩に起因する課題評価）

「4章 CKMSの設計原理と運用ポリシー」の検討項目の解説・考慮点（1）

節番号	FR番号	「解説・考慮点」の説明概要
4.1節 CKMS セキュリティポリシー	A.01-A.05	セキュリティポリシーとはCKMSが実現するセキュリティ機能や運用方針の概要を定めたものである。CKMSを利用するシステムやCKMSが構築されるIT環境のポリシーなどと矛盾がないことが前提である。
4.2節 情報管理ポリシー等からの要求事項	A.06	個人の説明責任が求められるケース（監査、リスクマネジメントの観点）を想定してCKMSでのサポートメカニズムを記載する
	A.07-A.13	匿名性、連結不可能性、観測不可能性のサポート有無とサポートする場合のメカニズムを記載する。一般に、匿名性、連結不可能性、観測不可能性を要求するのは特殊なケースである。
4.3節 ドメインのセキュリティポリシー	A.14-A.19	異なるセキュリティドメイン間での鍵情報の交換がなければ対象外である。GPKIは異なるセキュリティドメイン間での鍵交換の事例である。
	A.22-A.26	マルチレベルのセキュリティドメインでの鍵情報の交換がなければ対象外である。一般に、マルチレベルのセキュリティドメインでの鍵情報の交換は特殊なケースである。
4.4節 CKMSにおける役割と責任	A.27-A.28	CKMSの運用に関わるエンティティを定め、エンティティに割り当てる役割と実行できる鍵情報の管理機能へのアクセス権（権限）を定義する
	A.29-A.31	不必要な権限の割り当てや権限の分離が不十分な場合、内部犯行を誘発するリスクがある
4.5節 CKMSの構築環境及び実現目標	A.32	CKMSを構成する主要なデバイスおよびコンポーネントの一式を定める
	A.33-A.36	CKMSが要求する時刻の精度や利用する権威時刻ソース、第三者タイムスタンプの要求有無を定める
	A.39-A.42	初期及び将来を想定してユーザ数やCKMS性能面の目標、負荷増大時の対応策を定める
	A.43-A.46	CKMS内デバイスやCKMS間の相互運用を可能とするため、インタフェース、プロトコル、コマンド仕様を定める
	A.47-A.50	使いやすいユーザインタフェースを検討し、ヒューマンエラーを防止する
	A.51-A.53	どのような商用既製品を利用してどのようなセキュリティ機能を実行するかを定める

「4章 CKMSの設計原理と運用ポリシー」の検討項目の解説・考慮点（2）

節番号	FR番号	「解説・考慮点」の説明概要
4.6節 標準／規制に対する適合性	A.54-A.55	暗号アルゴリズム、暗号モジュール、セキュリティ認証などの標準への準拠性を明確にする
	A.57	CKMSが使用される国家・地域の法的規制を明確にする。欧州のサイバーセキュリティ法、中国のデータセキュリティ法、各国のデータ規制などが関係する。
4.7節 将来的な移行対策の必要性	A.58-A.61	CKMSは暗号アルゴリズムのセキュリティライフタイムを超えたサービス提供や、危殆化により、暗号アルゴリズムの置き換えが必要になる。そのため、複数の暗号アルゴリズムや異なる鍵長をサポートするケースも多い。
	A.62-A.69	技術の進歩をウォッチすると共に、予め潜在的な脅威に対する影響評価の実施を推奨する

8章　暗号鍵管理デバイスへのセキュリティ対策

暗号鍵管理デバイス（暗号モジュール）に対する検討項目を定める

- 8.1 鍵情報へのアクセスコントロール
  - アクセスコントロールへの要求事項
  - 暗号モジュールのセキュリティポリシー
  - 人間による入力のコントロール
  - マルチパーティコントロール

　→ 鍵情報へのアクセスコントロール及び暗号モジュールによる保護

- 8.2 セキュリティ評価・試験
  - 機能テスト、セキュリティテスト、環境テスト、セルフチェックテスト、第三者テスト

　→ CKMSシステム及びデバイスに対するセキュリティ評価・試験

- 8.3 暗号モジュールの障害時のBCP対策

　→ 障害発生に対する検知・回復

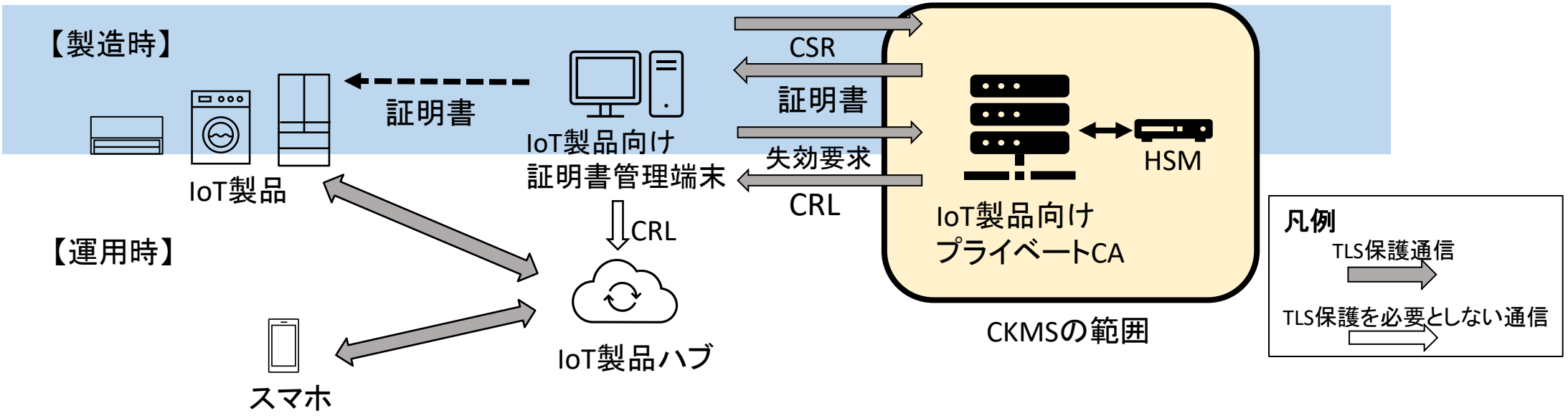
「8章 暗号鍵管理デバイスへのセキュリティ対策」の検討項目の解説・考慮点

節番号	FR番号	「解説・考慮点」の説明概要
8.1節 鍵情報へのアクセスコントロール	E.01-E.04	暗号モジュールの各機能の実行を認可されたエンティティに限定する。実行権を管理するアクセスコントロールシステム（ACS）は暗号モジュールと連動して動作する
	E.05	ACSによるエンティティ識別、認証、認可の粒度や機能を明確にする
	E.07-E.20	暗号モジュールとは、暗号境界内で暗号処理を実行するハードウェアもしくはソフトウェアの集合である。暗号境界内で利用される暗号鍵の保護機能を有する
	E.08-E.14	暗号モジュールへの鍵情報の入出力を平文形式で行うことは望ましくない。出力は暗号化して行うことが望ましく、主に外部での保管（バックアップなど）目的である
	E.21	鍵情報の入力を人間が行う場合、その正確さとセキュリティ面の問題がある。こうした入力がない場合は対象外である
	E.22-E.25	マルチパーティコントロールを利用する機能を明確にする。暗号鍵分割（K out of N秘密分散）やマルチパーティ機能をベンダに確認する
8.2節 セキュリティ評価・試験	E.26-E.34	いずれもシステムレベルの試験項目であるが、特に暗号モジュール（HSMなど）にも関連するものはベンダテスト、機能テスト、セキュリティテスト、環境テスト、セルフチェックテスト、第三者テストである
	E.26-E.34	FIPS140などの認証試験で上記テストをカバーするものが多い
8.3節 暗号モジュールの障害時のBCP対策	E.35	暗号モジュールはセルフテスト機能を備えることが望ましい。FIPS140-2/-3の要件に動作前や条件付きのセルフテスト機能がある
	E.37	回復可能なエラー発生時のセルフテストを含む回復の手順、回復困難なエラー発生時の暗号モジュールの交換手順（鍵情報のバックアップや破壊を含む）を明確にする

設定したトイモデル

IoT製品（家電想定）向けに公開鍵証明書を発行するプライベートCAシステム

- CKMSの範囲はCAサーバとHSMまでとする
- IoT製品向けのID管理、プライベート鍵生成、発行された証明書の機器埋め込みは工場内で行う
- IoT製品はネット接続され、スマホ内専用アプリからIoT製品ハブ経由でセンシングや制御が行われる。証明書は専用アプリとIoT機器の接続（TLSでの認証と秘匿通信確立）に利用される
- 証明書の失効管理はプライベートCAが発行するCRLによって行う



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