CRYPTREC
Cryptography Research and Evaluation Committees

# 暗号技術活用委員会活動報告

# クラウド鍵管理ガイダンスWG活動報告

2026年7月31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

クラウド鍵管理ガイダンスWG 主査
（立命館大学 教授）
上原　哲太郎

# 目次

# 目次

# CRYPTREC活動体制（2025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

クラウド鍵管理ガイダンスWG

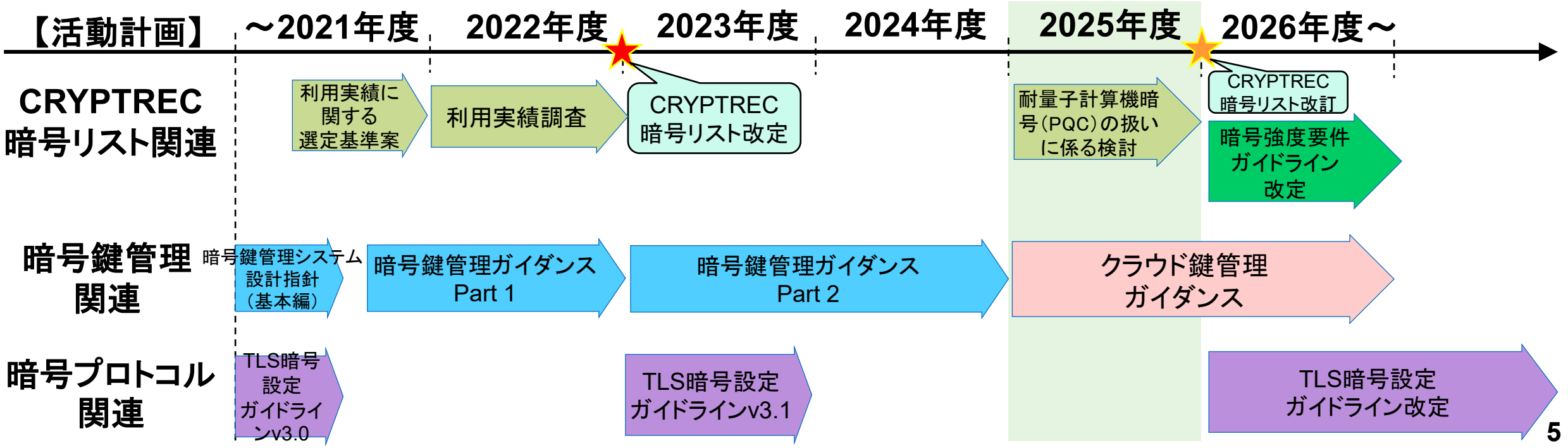
# 暗号技術活用委員会の活動目的

**【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



# 目次

# 暗号技術活用委員会委員（2025年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2026年3月末時点

| | | |
|---|---|---|
| 委員長 | 松本　勉 | 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 |
| 委員 | 上原　哲太郎 | 立命館大学　教授 |
| 委員 | 垣内　由梨香 | 日本マイクロソフト　リスクマネージャー |
| 委員 | 菊池　浩明 | 明治大学　教授 |
| 委員 | 佐藤　直之 | SCSKセキュリティ株式会社　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 | 寺村　亮一 | GMOサイバーセキュリティ by イエラエ株式会社　上席執行役員 CMO　サイバーセキュリティ事業本部長 |
| 委員 | 三澤　学 | 三菱電機デジタルイノベーション株式会社　グループマネージャー |
| 委員 | 満塩　尚史 | 順天堂大学　准教授 |
| 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部門長 |

※2026年度も委員メンバーには変更なし

# クラウド鍵管理ガイダンスWG委員（2025年度）

CRYPTREC Cryptography Research and Evaluation Committees

（注）2026年3月末時点

| | | |
|---|---|---|
| 主査 | 上原　哲太郎 | 立命館大学　教授 |
| 委員 | 漆嶌　賢二 | GMOグローバルサイン株式会社　フェロー |
| 委員 | 垣内　由梨香 | 日本マイクロソフト　リスクマネージャー |
| 委員 | 菊池　浩明 | 明治大学　教授 |
| 委員 | 税所　達朗 | さくらインターネット株式会社　社長室　特務　リーダー |
| 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 | 中島　智広 | アマゾン ウェブ サービス ジャパン合同会社　Sr. Specialist Solutions Architect |
| 委員 | 畠中　亮 | デジタル庁　ユニット長 |
| 委員 | 舟木　康浩 | タレスDIS株式会社　セールスエンジニアマネージャ |
| 委員 | 程吉　英仁 | 株式会社NTTデータ　課長代理 |
| 委員 | 満塩　尚史 | 順天堂大学　准教授 |

※2026年度も委員メンバーには変更なし

# 2025年度の活動概要

## ■ 耐量子計算機暗号（PQC）の扱いに係る検討

耐量子計算機暗号（PQC）をめぐる社会的動向を踏まえ、耐量子計算機暗号（PQC）の取扱い基準や位置づけ・暗号リスト記載内容等について検討を行い、暗号技術活用委員会としての見解を取りまとめた。

- 各国政府・公的機関等が公表している「PQCへの移行方針」や関連ガイドラインについて政策的側面から整理。
- 「CRYPTREC暗号リスト」での耐量子計算機暗号（PQC）に関する位置づけや移行ルールを変更すべきかどうかを検討。

## ■ クラウドにおける鍵管理ガイダンスの骨子検討

暗号鍵管理ガイダンスの拡充活動として、クラウドサービスを利用した情報システム構築を対象とした「クラウド鍵管理ガイダンス」の作成を開始。2025年度はガイダンスの骨子を整理。

- 本活動は2025年度より設置したクラウド鍵管理ガイダンスWGにて実施。

## ■ 「暗号鍵管理システム設計指針（基本編）」の改訂

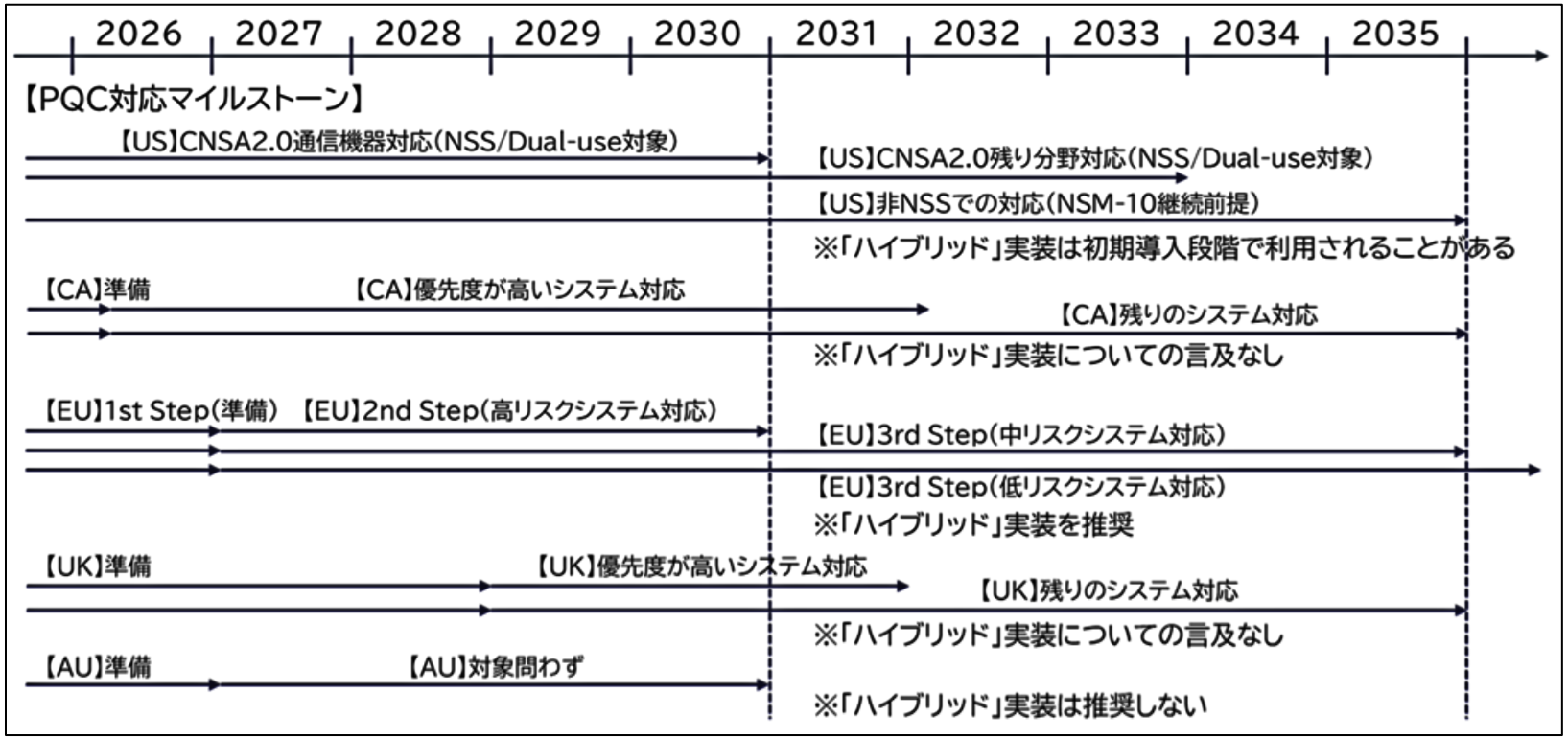
作成から約5年が経過し、記載の古さや誤記などを解消するための小改訂を実施。

# 耐量子計算機暗号（PQC）の扱いに係る検討：「PQCへの移行方針」の政策やガイドラインについて（1）

CRYPTREC
Cryptography Research and Evaluation Committees

■ 各国政府・公的機関等のPQC移行に関する政策やガイドラインの情報を収集し、時系列的観点での分析を実施

- 移行の優先度が高い、国家安全保障システムや高セキュリティシステムなどは2030年頃、その他のシステムは2035年を移行期限の目途としている




各国のPQC移行スケジュール

- US Executive Order 14306 (2025.6)
- NIST SP800-131A Revision 3 draft
- カナダ, “Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)”
- EU, “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography”
- 英国, “Timelines for migration to post-quantum cryptography”

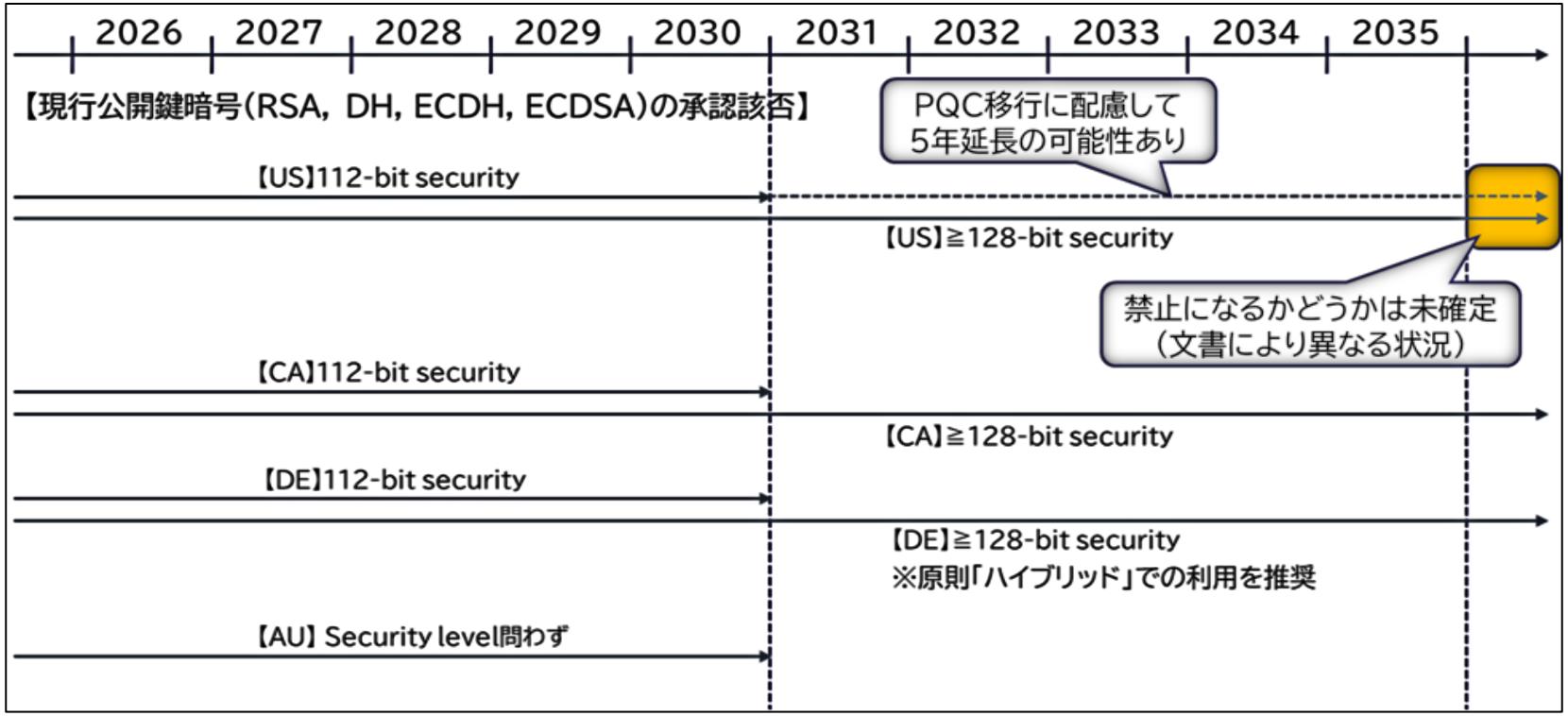
などを参照

# 耐量子計算機暗号（PQC）の扱いに係る検討：「PQCへの移行方針」の政策やガイドラインについて（2）

CRYPTREC
Cryptography Research and Evaluation Committees

■ 各国政府・公的機関等のPQC移行に関する政策やガイドラインの情報を収集し、時系列的観点での分析を実施（続き）

- 現行の公開鍵暗号の利用を止めるかどうか、ハイブリッド実装を活用するかどうかは国ごとに違いあり




既存暗号（特に現行の公開鍵暗号）の利用可否

# 耐量子計算機暗号（PQC）の扱いに係る検討：
# 「CRYPTREC暗号リスト」上の耐量子計算機暗号（PQC）の位置づけや移行ルールについて

CRYPTREC
Cryptography Research and Evaluation Committees

■ PQCに対応したCRYPTREC暗号リストの在り方を議論し、暗号技術活用委員会の見解をまとめた。
「耐量子計算機暗号（PQC）に対応したCRYPTREC暗号リストの在り方（案）」を確認し、委員会として同意した。

- PQCを取り込んだCRYPTREC暗号リストの形式
  - 現行暗号リストにPQCを加えるのではなく、量子計算機耐性を備えた暗号方式を記載したPQCリストを新たに作成するのがよい。
  - PQCリストは、量子計算機耐性を備えた公開鍵暗号に加え、共通鍵暗号やハッシュ関数等も含む暗号方式全般とするのがよい。
  - アルゴリズムの強度を規定するパラメータもリスト中に記載するのがよいとの意見あり。

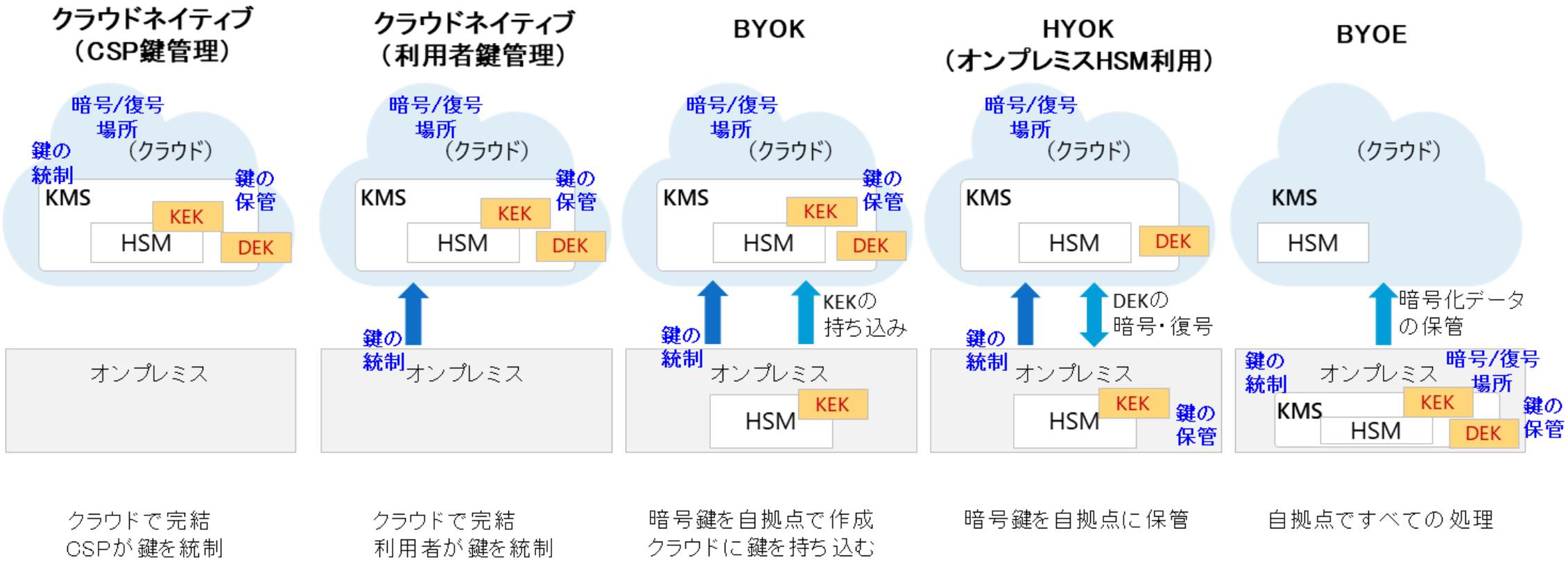
- 移行ルール・選定ルールについて
  - 電子政府推奨暗号リスト内に現行暗号リストとPQCリストが併存する場合、両リストの関係を分かりやすく説明すべきである。
    両リストの使い分けをどうするのか、両リストは将来的に一本化されるのか、など。

- 「耐量子計算機暗号（PQC）に対応したCRYPTREC暗号リストの在り方について（案）」に対する意見
  - 「耐量子計算機暗号（PQC）リスト」の説明文を誤解が生じないように修正したほうがよい。
    例えば、現行リストにのみ掲載の方式は、いずれPQCリストにも掲載される可能性があるか否かが明確でない。
  - ハイブリッドモードの取扱いについて、PQCリストはプリミティブとなるアルゴリズムにとどめるのがよい。
    TLS暗号設定ガイドラインなどのプロトコルやアプリケーションを対象にしたガイドラインの中で対応するのがよい。

【参考】CRYPTREC暗号リスト最新版（2026年3月）
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r2.pdf

# クラウドにおける鍵管理ガイダンスの骨子検討

- クラウドサービスを利用したシステムにおいて、クラウドに預ける情報を保護する上でクラウド鍵管理サービスを適切に選択・構築・利用するために考慮すべき点を解説するガイダンス
  - 骨子の詳細はクラウド鍵管理ガイダンスWG活動報告（上原主査）にて紹介




| クラウドで完結<br>CSPが鍵を統制 | クラウドで完結<br>利用者が鍵を統制 | 暗号鍵を自拠点で作成<br>クラウドに鍵を持ち込む | 暗号鍵を自拠点に保管 | 自拠点ですべての処理 |
|---|---|---|---|---|

# 「暗号鍵管理システム設計指針（基本編）」の改訂

■ 2020年に発行した「暗号鍵管理システム設計指針（基本編）」の小改訂版 v1.1 を発行

https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.1.pdf

- 改訂１：記述の最新化
  - 耐量子計算機暗号（PQC）の標準化動向、及び量子コンピュータの脅威の記述修正
  - 「政府機関の情報セキュリティ対策のための統一基準」 最新版の参照
  - NIST SP 800-53 Part 1 最新版の参照
  - CRYPTREC文書「暗号強度要件（アルゴリズム及び鍵長選択）」「暗号鍵設定ガイダンス」との整合、など

- 改訂２：誤記の修正
  - 本書がベースとするNIST SP 800-130の記述との齟齬修正
  - 不明瞭な記述の修正
  - 単純な記述誤りの修正、など

# 暗号技術活用委員会 2026年度の活動計画

## ■ 暗号強度要件ガイドラインの見直し

5年ごとの見直し時期にあたること、耐量子計算機暗号（PQC）移行方針がとりまとめられる状況から、耐量子計算機暗号（PQC）の取り扱いを含めた形での見直しを行う。2026年度末での完成を目指す。

## ■ TLS暗号設定ガイドラインの見直し

耐量子計算機暗号（PQC）のサポートに向けたTLS1.3への移行、耐量子計算機暗号（PQC）関連技術の取り込み、証明書有効期限の短縮化、現行のセキュリティ例外型の削除などを含む記載内容の見直しを行う。2027年度末での完成を目指す。

## ■ クラウドにおける鍵管理ガイダンスの作成

クラウド鍵管理ガイダンスWGにおいてガイダンスの位置づけや内容を確定し、クラウド鍵管理ガイダンスを作成する。2026年度末での完成を目指す。

# 目次

# クラウドにおける鍵管理ガイダンスの目次案

■ クラウドサービスを利用したシステムにおいて、クラウドに預ける情報を保護する上でクラウド鍵管理サービスを適切に選択・構築・利用するために考慮すべき点を解説するガイダンス

1. はじめに★
   イントロダクションとして、本ガイダンスの位置づけや想定読者をまとめる。
2. 基礎知識★
   クラウド鍵管理に関わる技術や、政府システムにおけるクラウド利用時の要件などの基礎知識をまとめる。
3. クラウド鍵管理サービスについて★
   クラウド鍵管理サービスを体系化して比較する。クラウド鍵管理サービスの選択基準について説明する。
4. クラウド鍵管理サービスに関わる責任分界
   クラウド鍵管理サービスにおけるクラウドサービスプロバイダ（CSP）と利用者の責任分界の原則を説明する。
5. 暗号鍵管理システムのフレームワーク要求からの整理★
   NIST SP 800-130を基に鍵管理システムにおける管理策を抽出し、クラウド鍵管理サービス利用時の責任分界の例や、利用者側の実施事項について説明する。
6. その他
   クラウド鍵管理に関わる本ガイダンスの周辺事項に触れる。

Appendix.
参考文献や補足資料をまとめる。

★：以降のスライドでピックアップ

# 1章　本書の目的及び位置づけ、想定読者、スコープ

■ 目的

- クラウドサービスの活用では、情報をクラウドサービスに預けることから情報の保存に関し、オンプレミスとは異なる考慮事項も生じる。
  クラウドサービスにおける暗号鍵管理サービスを適切に選択・構築・運用することによって、そのような事項に対処できる部分がある。
- クラウドサービスにおける暗号鍵管理の仕組みや注意事項をまとめ、クラウド環境で安全に暗号を運用するためのガイダンスとする。

■ 位置づけ

- CRYPTRECでは、NIST SP 800-130 (A Framework for Designing Cryptographic Key Management Systems)に基づいて暗号鍵管理システムを設計する際の解説書として「暗号鍵管理システム設計指針（基本編）」及び「暗号鍵管理ガイダンス」を作成している。
  今回作成する解説書は、これらのCRYPTREC文書を補強する位置づけにもなる。

■ 想定読者

- クラウドサービスを利用した情報システムの構築者（SI事業者など）、運用者。
  本ガイダンスで「利用者」とはこれらの情報システム構築者や運用者を指す。

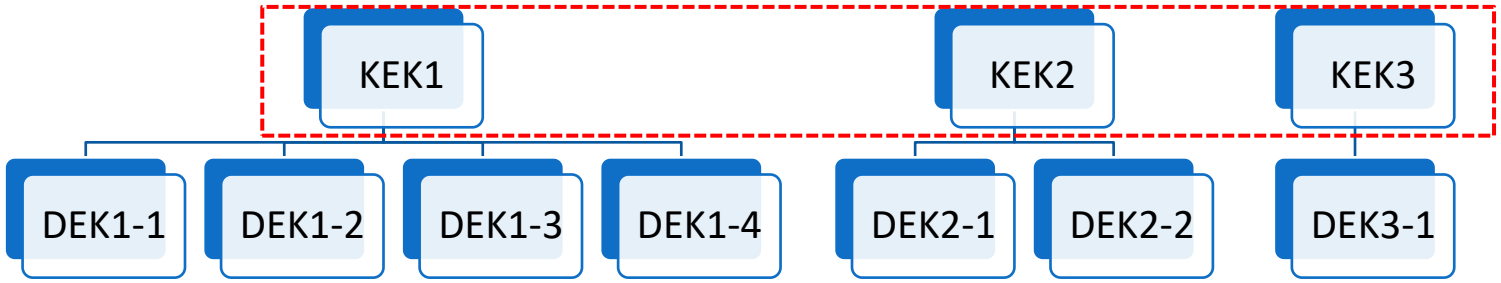
■ スコープ

- IaaSやPaaSのクラウドサービスを利用して、情報システムのプラットフォーム構築を行うケースを対象に、クラウドサービスに保存するデータ及び鍵情報の機密性及び完全性を確保する観点から、どのように鍵管理サービスを利用するかをターゲットとする。
- SaaSや利用者が開発するアプリケーションにおいて、暗号鍵管理サービスのSDKを組み込んで実装する形態は、本ガイダンスの直接の対象外とする。ただし、関連する概念や留意点については理解促進のために限定的に言及する。

# 2章　クラウド鍵管理サービスにおける暗号鍵の階層管理

■ クラウド鍵管理における暗号鍵階層の基本構成を説明する。

- 鍵暗号化鍵KEK（Key Encryption Key）とデータ暗号化鍵DEK（Data Encryption Key）の2階層で構成される場合が多い。
  KEKとDEKの2段階の鍵を用いたデータの暗号化を「エンベロープ暗号化」と呼ぶ。
- 利用者が意識するのはKEKである。
  暗号化対象のデータの機密性レベルやアクセス権の範囲に応じてKEKを生成する。
  KEKのアクセス権限がDEKのアクセス権限に継承される。
- DEKはクラウド側で自動的に生成される場合が多い。
  KEKから鍵導出関数によって生成されるなどの形態がとられる。
- KEKはHSMで管理され、DEKは暗号化されて（HSM外の）クラウドサービスに保存される場合が多い。
- 暗号化消去では、KEKを消去することによってDEK及びDEKで暗号化されたデータが無効化される。

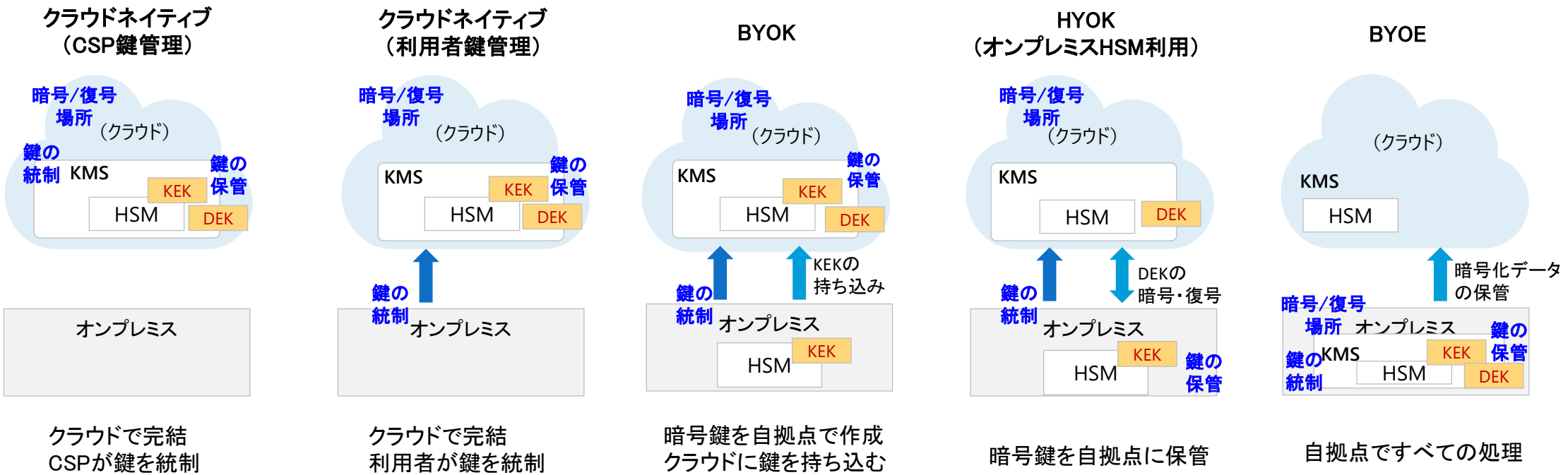



HSM（Hardware Security Module）で管理

# 3章　クラウド鍵管理サービスの構成概要

■ 鍵の統制（アクセス制御、ライフサイクルのコントロール）、鍵（KEK）の保管場所、データの暗号化・復号処理の実施場所に基づいてそれぞれの方式を分類。

- クラウドネイティブ：ストレージやデータベースなどのクラウドサービスでの暗号処理と密に統合された鍵管理方式。
  鍵の統制をクラウド側で行う方式と利用者側で行う方式に区分される。
- BYOK（Bring Your Own Key）：KEKを利用者側で生成し、クラウドに持ち込む機能を付加。
- HYOK（Hold Your Own Key）：KEKを利用者側で保管しながら、クラウドの管理基盤と連携させる方式。
- BYOE（Bring Your Own Encryption）：暗号鍵の保管及び暗号処理を利用者側で行う方式。



# 3章　クラウド鍵管理サービスの比較

■　クラウド鍵管理サービスを比較し、選択時の考慮事項をまとめる。

- 下表右側の方式ほど、利用者の鍵管理レベル（鍵の保有や実施すべき管理項目）が高まり、利用者の鍵管理基盤構築や運用コストも増加する。
- 各方式の中で「クラウドネイティブ（利用者鍵管理）」が選択上の基準となる。

| | クラウドネイティブ（CSP鍵管理） | クラウドネイティブ（利用者鍵管理） | BYOK | HYOK（オンプレミスHSM利用） | BYOE |
|---|---|---|---|---|---|
| 暗号鍵の利用者管理のレベル | ☆<br>マネージドサービス基盤を利用し、CSPに鍵管理を委任する | ☆☆<br>マネージドサービス基盤を利用し、利用者が鍵のライフサイクル管理を行う | ☆☆<br>クラウドネイティブ（利用者鍵管理）に加えて、オンプレミス環境でKEKを生成する | ☆☆☆<br>オンプレミス環境にKEKを保管した状態で、マネージドサービス基盤と連携する | ☆☆☆☆<br>オンプレミス環境で暗号鍵の保管及び暗号処理が行われる |
| 暗号鍵管理基盤の利用者構築コスト | ○フルマネージドサービスの利用になり、構築コストは不要 | ○マネージドサービスの利用になり、構築コストは不要 | ▲オンプレミス側に暗号鍵管理の基盤があることが前提 | ▲オンプレミス側に暗号鍵管理の基盤を構築することが必要 | ▲オンプレミス側に暗号鍵管理の基盤を構築することが必要 |
| 利用者の運用負荷 | ○フルマネージドサービスの利用になり、暗号鍵管理の運用負荷はない | ○マネージドサービスの利用になるが、利用者側でクラウドKMSのコントロールが必要 | ▲マネージドサービスの利用になるが、利用者側でクラウドKMSのコントロールに加えて、暗号鍵の生成・持ち込みが必要 | ▲クラウドKMSと連動したオンプレミス環境の暗号鍵管理基盤（HSM）の運用が必要 | ▲オンプレミス環境の暗号鍵管理基盤の運用が必要 |
| クラウド環境とオンプレミス環境のネットワーク可用性 | ○クラウド環境で暗号鍵管理の処理が行われ、ネットワークの可用性に影響しない | ○クラウド環境で暗号鍵管理の処理が行われ、ネットワークの可用性に影響しない | ○暗号鍵の持ち込み以降は、ネットワークの可用性に影響しない | ▲ネットワークの可用性確保が重要である | ▲ネットワークの可用性確保が重要である |
| 制約や要件への準拠 | ▲利用者による鍵管理を求める要件への準拠が困難 | ○クラウド鍵管理サービスの中で選択の基準となる方式である | ○鍵生成時のエントロピーソース要件やクラウド外にオリジナルの鍵を保有する要件がある場合等に選択候補となる | ○クラウド環境での保存データと暗号鍵の分離を行う要件がある場合等に選択候補となる | ▲オンプレミス環境で暗号に関わる処理が行われるため、クラウドサービスでのデータ利用は極めて限定される |

○：方式採用時の利点、▲：懸念点、☆数：利用者の鍵管理レベルの高さ

# 5章　暗号鍵管理システムのフレームワーク要求からの整理

■ クラウドサービスでもCKMSの設計・運用において検討すべきことは変わらないが、利用者が検討すべきことは変わる。利用者視点の重点項目をSP 800-130のフレームワーク要求に基づいて整理する。

- SP 800-130フレームワーク要求のクラウド鍵管理サービスへの適用
  - SP 800-130はCKMS設計者向けにフレームワーク要求を網羅。クラウド鍵管理サービスの利用者視点では適用が難しい。
  - SP 800-130を再構成した「暗号鍵管理システム設計指針（基本編）」の章・節・小項目から、「暗号鍵管理の実施項目（管理策）」を抽出する。
  - 抽出した「暗号鍵管理の実施項目」に対して、CSP実施事項と利用者実施事項を検討する。

- 暗号鍵管理の実施項目のクラウド鍵管理サービスへの適用
  - クラウドネイティブ（利用者鍵管理）、BYOK、HYOKの3方式を対象に、利用者とCSPの責任分界、利用者実施事項の違いを説明する。

- クラウド鍵管理サービスにおける利用者の管理事項
  - クラウドネイティブ（利用者鍵管理）を主対象に、利用者の管理事項における注意点を説明する。

# 5章　暗号鍵管理の実施項目（管理策）

■「暗号鍵管理システム設計指針（基本編）」におけるフレームワーク要求から、クラウド鍵管理サービスでの責任分界の検討に利用可能な管理項目一覧を抽出。

| 管理項目 | 設計指針の該当節/番号 | 設計指針から抽出した管理項目の内容 |
|---|---|---|
| **暗号アルゴリズム及びメタデータの選択** | 6章, 7章 | |
| 暗号アルゴリズム・鍵長選択 | 6.1 | 要求される保護レベル（セキュリティ強度）に対応した暗号アルゴリズムを選定する。 |
| メタデータの管理 | 7.2 | CKMSが取り扱う全ての鍵タイプ、メタデータ、信頼関係、保護方針、等を定める。 |
| **ライフサイクルの管理** | 5.2, 5.3 | |
| 暗号機能の実行場所 | 5.3 ③ | 暗号機能の実行場所を定める。 |
| 鍵生成 | 5.3 ⑧ | 鍵生成機能への要求事項を定める。 |
| 鍵情報の破壊 | 5.3 ⑦ | 鍵情報の破壊機能への要求事項を定める。 |
| 鍵更新（＝鍵ローテーション） | 5.3 ⑨ | 鍵導出機能／鍵更新機能（=鍵ローテーション機能）への要求事項を定める。 |
| 鍵活性化、鍵非活性化、鍵失効、鍵の一時停止 | 5.3 ②, ④, ⑤, ⑥ | ・鍵活性化機能への要求事項を定める。・鍵非活性化機能への要求事項を定める。・鍵失効機能への要求事項を定める。・暗号鍵の一時停止機能及び再活性化機能への要求事項を定める。 |
| **鍵情報へのアクセスコントロール** | 8.1 | |
| アクセスコントロールシステム | 8.1.1 | 鍵情報へのアクセスコントロールの要求事項を定める。 |
| **鍵の保管・鍵の確立** | 5.4, 5.5 | |
| 保管中の鍵情報のセキュリティ | 5.4 ① | 保管中の鍵情報のセキュリティを確保するための手段を定める。 |
| 鍵情報のバックアップ | 5.4 ③ | 鍵情報のバックアップ方法を定める。 |
| 鍵情報のアーカイブ | 5.4 ④ | 鍵情報のアーカイブ方法を定める。 |
| 鍵情報の復元 | 5.4 ⑤ | 鍵情報の復元方法を定める。 |
| 鍵確立 | 5.5 | ・鍵確立機能の利用局面を定める。・鍵配送/鍵合意における要求事項を定める。・利用する鍵確立プロトコルを定める。 |

# 5章　暗号鍵管理の実施項目（管理策）（表の続き）

■ 「暗号鍵管理システム設計指針（基本編）」におけるフレームワーク要求から、クラウド鍵管理サービスでの責任分界の検討に利用可能な管理項目一覧を抽出。

- 管理項目のカテゴリーを「暗号アルゴリズム及びメタデータの選択」、「ライフサイクルの管理」、「鍵情報へのアクセスコントロール」、「鍵の保管・鍵の確立」、「鍵の喪失・危殆化の対策」、「その他（システムレベルの管理策）」と整理した。

| 管理項目 | 設計指針の該当節/番号 | 設計指針から抽出した管理項目の内容 |
|---|---|---|
| **鍵の喪失・危殆化の対策** | 5.6, 5.7 | |
| 鍵情報の喪失・破損時の対策 | 5.6 | 鍵情報の喪失・破損に対するBCP対策を定める。 |
| 鍵情報の危殆化時の対策 | 5.7 | 鍵情報の危殆化に対するBCP対策を定める。 |
| **その他（システムレベルの管理策）** | 4章, 8章, 9章 | |
| CKMSセキュリティポリシー | 4.1、4.4、4.5、4.6 | ・CKMSセキュリティポリシーを作成する。<br>・CKMS参加者（責任者／管理者／運用者／ユーザ、等）の役割と責任を定める。<br>・CKMSが使用される地域・国家の法律、ルール及び規制、適合すべき標準を定める。 |
| 暗号モジュール | 8.1.2 | ・暗号モジュールのセキュリティポリシーを定める。<br>・鍵情報の暗号モジュールへの入出力のための機能及び制限を定める。 |
| CKMSのセキュリティコントロール | 9.1 | ・CKMSコンポーネント及びデバイスに対する物理セキュリティの方法を定める。・OSに対するセキュリティの要求事項を定める。・監査機能に対する要求事項を定める。・セキュリティ境界をコントロールするためのネットワークセキュリティコントロールデバイスに対する要求事項を定める。 |
| CKMSの障害・災害対策 | 9.5 | ・CKMS設備への物理的損害発生時におけるBCP対策を定める。・ハードウェア障害発生時におけるBCP対策を定める。・ソフトウェア障害発生時におけるBCP対策を定める。 |
| 将来的な移行対策 | 4.7 | ・使用中の暗号アルゴリズムを拡張又は置き換えができるように実装することを検討する。・技術の進歩に起因する潜在的な脅威（暗号アルゴリズム及び鍵確立プロトコルに対する新しい攻撃、鍵管理デバイスに対する新しい攻撃、新しい計算機技術、等）について考慮する。 |

# 5章　クラウド鍵管理サービスにおける利用者の管理事項

■ 利用者側の管理事項及び利用上の注意点を解説する。

- **クラウド鍵管理方式の選択**
  自組織のセキュリティポリシーを基にどの範囲を安全に管理できるかを基準に考え、CSPのセキュリティアシュアランス（第三者評価や認証を通じて、クラウドシステムのセキュリティを証明している状況）や運用容易性も考慮した上で方式を選択すべきである。

- **暗号アルゴリズムと鍵の生成パラメータの設定、選択**
  暗号アルゴリズムと鍵の生成パラメータは原則としてCSPが定義した暗号ポリシーに基づいて選択、設定する。他方で、利用者がBYOK等でHSMを利用する場合は暗号アルゴリズムと鍵の生成パラメータを利用者自身で設定可能であるが、安全性と品質の保証責任は利用者にある。

- **鍵のライフサイクル**
  暗号鍵のライフサイクルを支援する管理機能が提供されており、暗号鍵の有効期間や更新のタイミングおよび方針は、利用者が自組織の鍵管理ポリシーに基づいて決定すべき事項である。また、クラウド鍵管理サービスの仕様によっては、暗号鍵の有効期間設定や自動ローテーション機能の有無・周期が異なるため、利用前にCSPの提供仕様を確認することが望ましい。

- **鍵へのアクセス管理**
  情報システム全体のアクセス制御原理（NIST SP 800-53）を基礎に、暗号鍵への適用を具体化している。認証・認可・最小権限・職務分離・監査といった原則に基づき、暗号鍵を不正利用や漏えいから保護し、鍵管理プロセス全体の信頼性と説明責任を確保することが目的である。クラウドにおけるアクセス制御は、CSPが提供するアクセス制御機能（IAM：Identity and Access Managementなど）を用いて設定及び管理する。

- **ログ管理、監視**
  鍵管理に関するすべての操作（生成、使用、削除、権限変更など鍵の状態や権限制御に関わる操作）は、鍵ポリシーへの準拠状況の確認や不正利用の検知を目的として監査ログとして記録される。CSPが提供する監査ログを定期的に確認して、不正な利用や鍵ポリシーで定めた設定・運用ルールからの逸脱がないかを監視するのは利用者の役割である。

# クラウド鍵管理ガイダンスWG 2026年度の活動計画

## ■ クラウドにおける鍵管理ガイダンスの作成

- クラウド鍵管理ガイダンスWGにおいてガイダンスの位置づけや内容を確定し、クラウド鍵管理ガイダンスを作成する。2026年度末での完成を目指す。
- 作成中のガイダンスで十分にカバーできていない事項を今後どのように扱うかの検討も予定している。

# おわりに

■ 2025年度暗号技術活用委員会／クラウド鍵管理ガイダンスWGの活動報告・成果物

- CRYPTREC Report 2025　暗号技術活用委員会報告
  https://www.cryptrec.go.jp/report/cryptrec-rp-3000-2025.pdf

- 暗号鍵管理システム設計指針（基本編）v1.1
  https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.1.pdf


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