CRYPTREC Report 2025

令和８年３月

独立行政法人情報処理推進機構
国立研究開発法人情報通信研究機構

「暗号技術活用委員会報告」

目次

はじめに

本報告書は、デジタル庁、総務省及び経済産業省が主催する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構が共同で運営する暗号技術活用委員会の 2025 年度の活動を報告するものである。

暗号技術活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。2015 年度に、暗号技術活用委員会の活動目的の軸足を、「暗号技術を主軸とした検討」から「情報システムのセキュリティ確保に寄与する暗号技術等に係る成果物の提供」に移すことに定義し直し、2016 年度から新たな目的に基づいて活動している。特に、実運用におけるセキュリティ確保の観点から、運用面でのセキュリティマネジメントに関するガイドライン群の作成に注力している。

近年はクラウドサービスを活用して情報システムを構築するケースが増えており、そのようなシステムでは安全な暗号利用のために暗号鍵管理が今まで以上に重要になる。そこで、クラウドサービスにおいて利用する暗号鍵管理システムに特化したガイダンスを作成すべく、ワーキンググループを 2025 年度より設置して当該ガイダンスの作成を開始した。ガイダンスの完成は 2026 年度末の予定である。

また、近年の量子コンピュータの進展を契機に、耐量子計算機暗号（PQC）への移行について各国で検討が進展している。我が国でも 2025 年 6 月に関係府省庁連絡会議が設置され、政府機関等における耐量子計算機暗号（PQC）への移行に係る検討が本格的に開始された。暗号技術活用委員会は、その動きと連携して耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方について検討した。検討結果の一部は 2025 年度末に改定した CRYPTREC 暗号リストに反映されている。

耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの改定や耐量子計算機暗号（PQC）を安全に利用するためのガイドラインの作成は、2026 年度以降も精力的に検討すべき課題である。暗号技術活用委員会ではこのような課題に注力して、情報システムのセキュリティ確保の底上げ、暗号の普及促進・セキュリティ産業の競争力強化、より安心・安全な情報化社会の実現に引き続き貢献できればと考えている。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

2026 年 3 月

暗号技術活用委員会 委員長　松本 勉

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、2025 年度の暗号技術活用委員会の活動内容と成果概要を記述した。

2024 年度以前の CRYPTREC Report は、CRYPTREC 事務局（デジタル庁、総務省、経済産業省、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）が共同で運営する下記の Web サイトから参照できる。

https://www.cryptrec.go.jp/
CRYPTREC 報告書

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任を負わない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

委員会構成

暗号技術活用委員会（以下「活用委員会」という。）は、図１に示すように、デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（以下「IPA」という。）と国立研究開発法人情報通信研究機構（以下「NICT」という。）が共同で運営している。

活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。

なお、活用委員会と連携して活動する「暗号技術評価委員会」も暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。

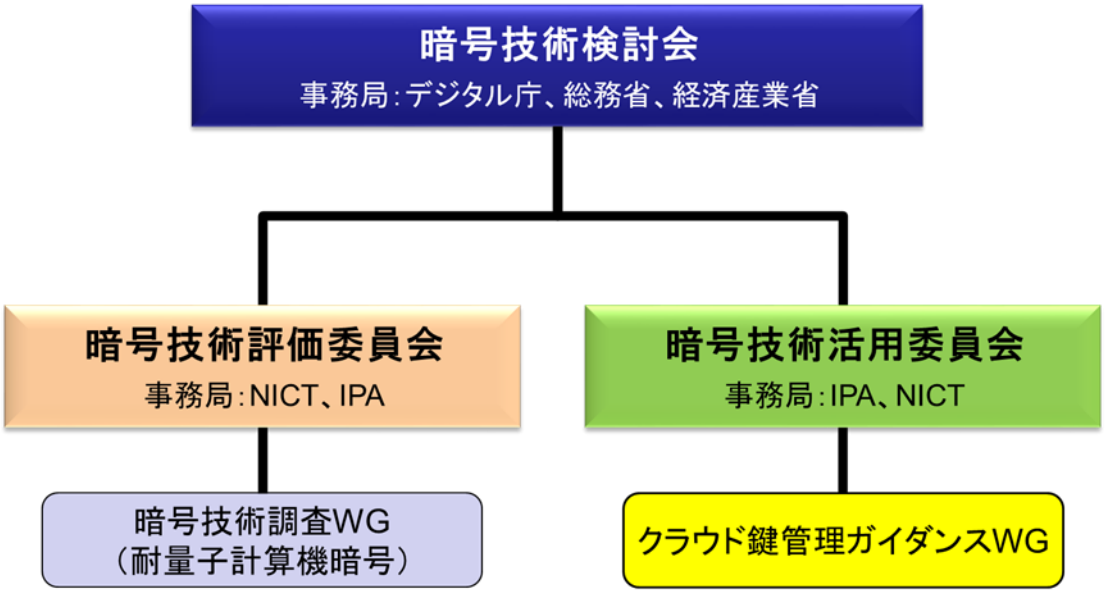


図１　2025 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

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 先端科学高等研究院 上席特別教授
委員	上原 哲太郎	立命館大学 情報理工学部 情報理工学科 教授
委員	垣内 由梨香	日本マイクロソフト リージョナルセキュリティチーム リスクマネージャー
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	佐藤 直之	SCSK セキュリティ株式会社 コンサルティング本部 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 IS 研究所 デジタルプラットフォームディビジョン 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 インターネットサービス事業本部 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	田村 裕子	日本銀行 金融研究所 情報技術研究センター 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（最高管理責任者） サイバーセキュリティ事業本部 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 情報管理・セキュリティソリューション統括室 セキュリティ技術部 製品セキュリティソリューショングループマネージャー
委員	満塩 尚史	順天堂大学 健康データサイエンス学部 健康データサイエンス学科 准教授
委員	山口 利恵	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 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 研究部門長

（所属：2026 年 3 月末時点）

クラウド鍵管理ガイダンス WG

主査	上原 哲太郎	立命館大学 情報理工学部 情報理工学科 教授
委員	漆嶌 賢二	GMO グローバルサイン株式会社 事業企画部 フェロー
委員	垣内 由梨香	日本マイクロソフト リージョナルセキュリティチーム リスクマネージャー
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	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 インターネットサービス事業本部 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	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, Security
委員	畠中 亮	デジタル庁 クラウドマイグレーションユニット ユニット長
委員	舟木 康浩	タレス DIS 株式会社 サイバーセキュリティプロダクト事業本部 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 ソリューション事業本部 セキュリティ＆ネットワーク事業部 サイバーセキュリティ統括部 課長代理
委員	満塩 尚史	順天堂大学 健康データサイエンス学部 健康データサイエンス学科 准教授

（所属：2026 年 3 月末時点）

オブザーバー

吉村 康志	内閣官房 国家サイバー統括室
加茂 聡	内閣官房 国家サイバー統括室
櫻井 駿	内閣官房 国家サイバー統括室
上野 浩理	内閣官房 国家サイバー統括室
北井上 礼樹	デジタル庁 デジタル社会共通機能グループ
山之上 隆広	デジタル庁 デジタル社会共通機能グループ
池田 晃輝	デジタル庁 デジタル社会共通機能グループ
梅城 崇師	総務省 サイバーセキュリティ統括官室
内藤 めい	総務省 サイバーセキュリティ統括官室
竹之内 玲	総務省 サイバーセキュリティ統括官室
山口 航輝	総務省 サイバーセキュリティ統括官室
木村 悠生	総務省 サイバーセキュリティ統括官室
橋本 勝国	経済産業省 商務情報政策局
石坂 知樹	経済産業省 商務情報政策局
東 亨佳	経済産業省 商務情報政策局
木下 誠	外務省 大臣官房 情報通信課
石丸 光宏	防衛省 整備計画局
河合 舜	防衛省 整備計画局
石山 優貴	警察庁
松崎 泰之	警察庁
多賀 文吾	警察大学校
髙橋 知義	警察大学校
井上 智樹	警察大学校

事務局

独立行政法人情報処理推進機構（高柳大輔、神田雅透、鷲見拓哉、新保淳、伊藤忠彦、白岩裕子、川名優香、渡邊由香利）

国立研究開発法人情報通信研究機構（井上大介、青野良範、伊藤琢真、伊藤竜馬、大久保美也子、小川一人、金森祥子、木村隼人、黒川貴司、髙和真、田村千代、松井充、吉田真紀）

第1章　2025 年度活動内容

1.1. 活動内容

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、運用ガイドライン／ガイダンスの作成等の活動を行っている。

2025 年度の活動概要は以下の通りである。

（1）耐量子計算機暗号（PQC）の扱いに関わる検討

PQC をめぐる社会的動向を踏まえ、PQC の取扱い基準や位置づけ・記載内容等について検討を開始した。具体的には各国政府・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し、また「CRYPTREC 暗号リスト」での 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した。これらの検討結果を踏まえて、暗号技術活用委員会としての見解を取りまとめた。

（2）クラウドにおける鍵管理ガイダンスの作成

暗号鍵管理ガイダンスの拡充活動の一環として、クラウドサービスを利用したシステム構築を対象とする「クラウド鍵管理ガイダンス」の作成のため、クラウド鍵管理ガイダンス WG を設置した。同 WG では、作成するガイダンスの位置づけや内容を検討し、2026 年度末でのガイダンス完成を目標に、今年度はガイダンスの骨子を整理した。

（3）「暗号鍵管理システム設計指針（基本編）」の改訂

暗号鍵管理システムの設計に関わる解説書として作成した「暗号鍵管理システム設計指針（基本編）（以下「設計指針」と表記）」について、作成から約５年が経過したことに伴い、記載の古さや誤記の指摘などの問題があったため、改訂を行うこととした。修正の必要な箇所を洗い出し、改訂版となる「設計指針 第 1.1 版」を作成した。

1.2. 開催状況

2025 年度に開催された暗号技術活用委員会での審議概要は表 1-1 のとおりである。

表 1-1　2025 年度暗号技術活用委員会　開催概要

回	開催日	議案
第一回	2025 年 7 月 18 日	● 2025 年度暗号技術活用委員会活動計画の確認 ● 2025 年度クラウド鍵管理ガイダンス WG 活動計画の審議 ● PQC の扱いに関する検討 ● 「暗号鍵管理システム設計指針（基本編）」の修正について
第二回	2026 年 2 月 24 日	● PQC の扱いに関する検討 ● 2025 年度クラウド鍵管理ガイダンス WG 活動状況及び活動報告の審議 ● 「暗号鍵管理システム設計指針（基本編）」の修正案の審議 ● 2025 年度暗号技術活用委員会活動報告案について

第2章　成果概要

2.1. PQC の扱いに係る検討

2.1.1. 「PQC への移行方針」の政策やガイドラインについて

各国政府・公的機関等が発行している PQC 移行に関する政策やガイドラインの情報を収集・最新化し、時系列的観点での分析を行った。

2025 年 4 月の G7 会合で「Accelerating the Transition to Quantum-Safe Communication: A Call for Global Collaboration and Action 」が取りまとめられたことを受け、G7 各国は協調して PQC への移行を進めるため、明確な期限を定めた移行スケジュールを策定し、進捗状況を管理することが謳われた。欧米諸国では、PQC 移行スケジュールの策定・改定が進められており、代表例として以下を整理した。

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

このほかドイツ、フランス、オーストラリアなどでも同様の文書が公表されている。これらの情報をまとめたのが以下の図である。

各国とも、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については 2030 年頃、その他のシステムについては 2035 年を移行期限の目途としていることが分かる。一方で、既存暗号、特に現行の公開鍵暗号との関連では、利用を止めるのかどうか、ハイブリッド実装を活用するのかどうかについては国ごとに違いがある。

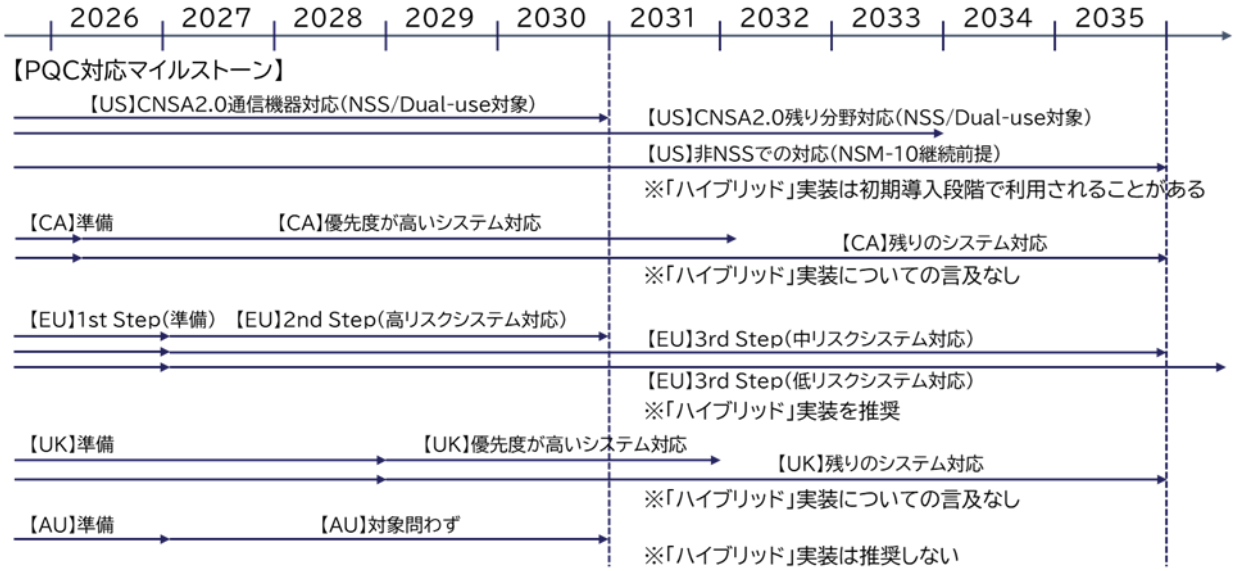


図 2-1　各国の PQC 移行スケジュール

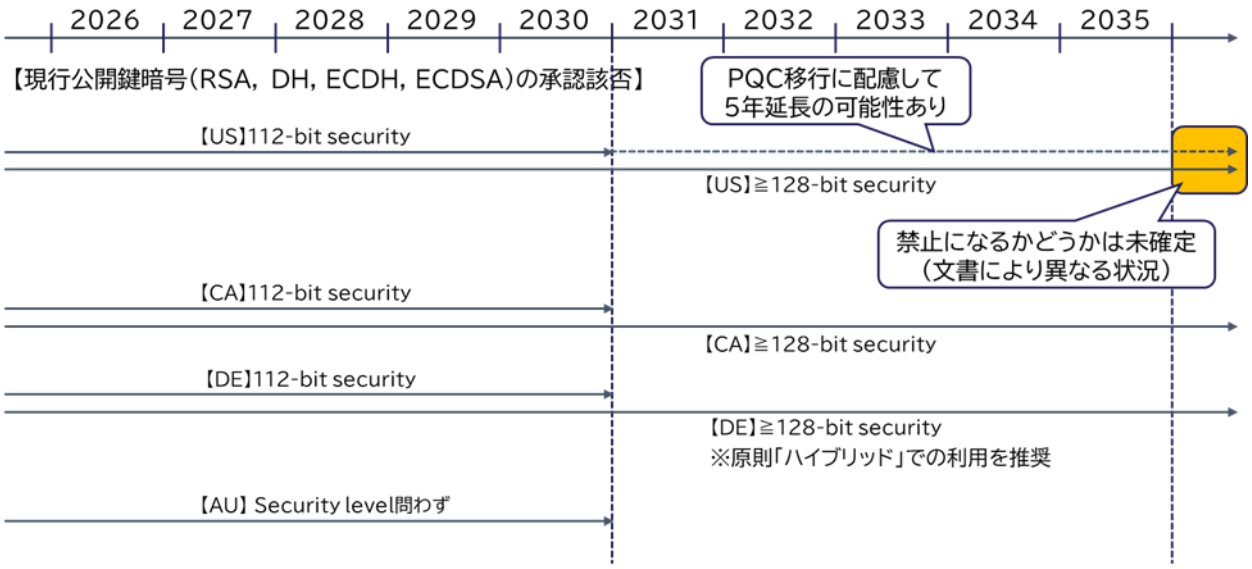


図 2-2　既存暗号（特に現行の公開鍵暗号）の利用可否

2.1.2.　「CRYPTREC 暗号リスト」上の PQC の位置づけや移行ルールについて

PQC に対応した CRYPTREC 暗号リストの在り方について議論し、以下のとおり、暗

号技術活用委員会としての見解をまとめた。また、これらの見解を踏まえつつ作成された「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)」の内容を確認し、暗号技術活用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

  現行の CRYPTREC 暗号リスト（「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」）の技術分類をそのまま使うか、「PQC」カテゴリを追加するか、あるいは、それらのリストとは別の独立した「量子計算機耐性を備えた暗号方式に関わる独立したリスト（PQC リスト)」を作るべきかを議論した。

  その結果、現時点においては既存の CRYPTREC 暗号リストに PQC を加えるのではなく、新たに量子コンピュータに耐性のある暗号方式のみを記載する独立したリストを作成したほうがよいとの見解で一致した。

  また、新たなリストに掲載するアルゴリズムについて、量子計算機耐性を備えた公開鍵暗号だけではなく、共通鍵暗号やハッシュ関数なども含めて、量子計算機耐性を備えた暗号方式全般を含むリストとするのがよいとの見解で一致した。さらに、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もあった。

  これは、PQC リストを参照することで量子計算機耐性を備えた暗号方式を包括的に選択可能にし、利用者にとって利便性が高いと考えられるためである。

- 移行ルール・選定ルールについての検討

  「PQC リストを新たに作成すること自体は妥当であり、そのための移行・選定ルールが設けられることも理解できるが、電子政府推奨暗号リストとの関係は整理すべき」との指摘があった。これは、「電子政府推奨暗号リスト」を参照して暗号方式を選択するようにしている事例が政府機関のみならず民間事業者にも多いため、「電子政府推奨暗号リスト」の中に「現行暗号リスト」と新たな「PQC リスト」の２つのリストが併存する形になった場合、両リストの関係について分かりやすい説明をすべきとの観点での指摘である。例えば、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ていくのか、両リストに掲載されるアルゴリズム、片方にしか掲載されていないアルゴリズムについてどのように考えればいいのか、PQC リストでも将来は監視暗号リストが必要である、などである。

  これらの意見は、「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)」を作成する際の参考としてもらうこととした。

- 「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」の説明文に関連して、例えば、現行の電子政府推奨暗号リストにのみ掲載されている方式について、いずれ PQC リストにも掲載される可能性があるのか、あるいは PQC リストには掲載されない方式であるのかが明確でない等の課題があるため、誤解が生じないように修正したほうがよいとの指摘があった。

また、ハイブリッドモードの取扱いについて、PQC リストではプリミティブとなるアルゴリズムだけにとどめるほうがよいのではないかとの意見があった。これは、ハイブリッドモードを含めると暗号リストとして複雑になることが予想されるため、例えば TLS 暗号設定ガイドラインのようなプロトコルやアプリケーションを対象に作成するガイドラインの中で対応するのがよいのではないかとの指摘である。

この点については、「耐量子計算機暗号（PQC）リスト検討タスクフォース（仮称）」にて検討を継続することとなった。

2.1.3. 産業界における PQC への移行状況

各国政府・公的機関による PQC 移行方針を受けた、産業界の取り組み事例についてマイクロソフト社の状況を同社委員により共有した。共有された情報の概要は以下のとおり。

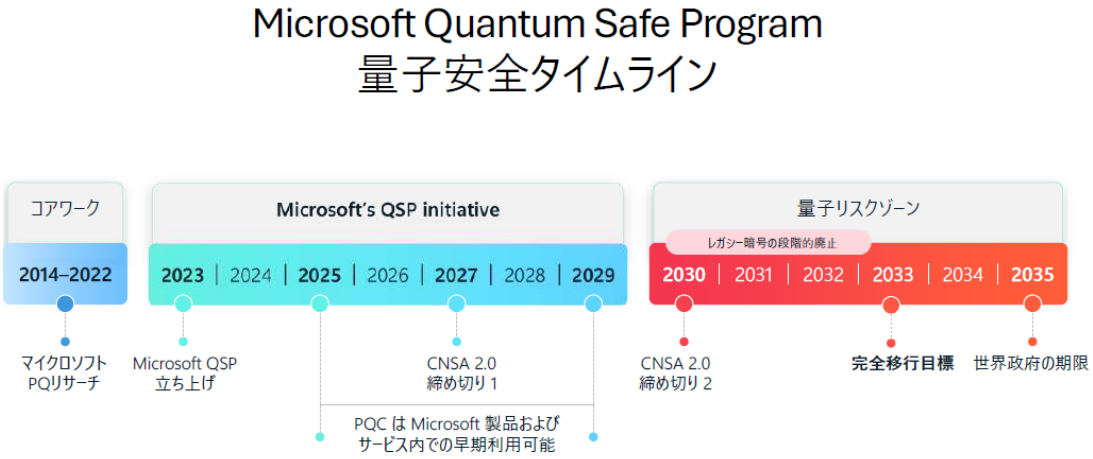
マイクロソフトは、社内に大規模な IT 環境を構築している他、プラットフォーマとしてクラウドや Windows、IoT、ゲームなど様々なサービスを提供している事業者である。これらに対して、QSP（Quantum Safe Program）なる耐量子技術の取り組みを全社として推進しており、膨大なエコシステムを適切に更新していくことを目標としている。詳細は同社ブログを参照のこと[1]。

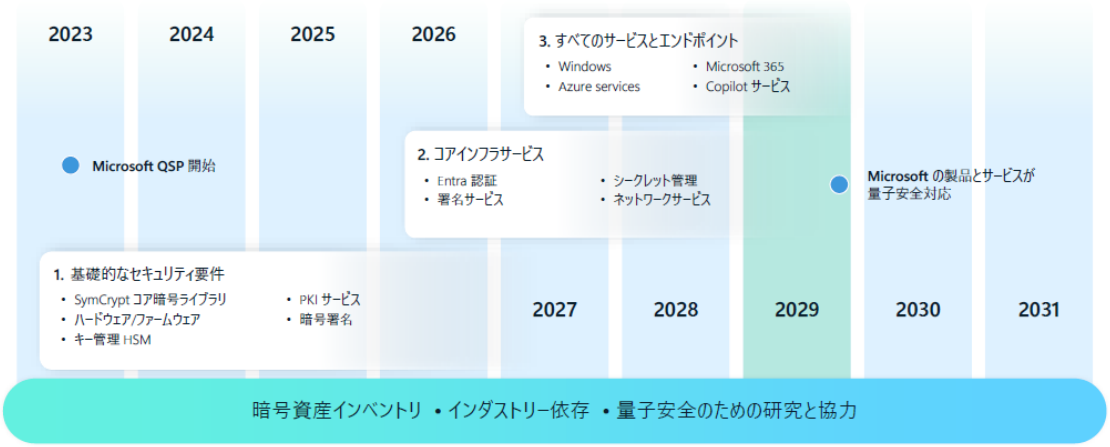
- マイクロソフト QSP の量子安全タイムライン

  2030 年に PQC 移行のマイルストンを設定する国・地域が多い中、1 年前倒しの 2029 年をターゲットに PQC 利用が可能となるように対応を進めている。また、現行の公開鍵暗号を段階的に廃止し、2035 年から 2 年前倒しした 2033 年を PQC への完全移行の目標と設定している。

  PQC 移行の具体的な取り組みとして、まず Windows や Microsoft Azure で利用する基盤となる暗号ライブラリ SimCrypt の PQC 対応等を進めてきた。次の段階として、コアとなる認証や署名のサービス、ネットワークサービスの PQC 対応を進め、さらに最終段階として、あらゆるサービスに PQC 対応を広げる方針である。

[1] https://news.microsoft.com/ja-jp/2025/08/22/quantum-safe-security-progress-towards-next-generation-cryptography/





- 顧客との連携

  PQC 移行は単なる暗号アルゴリズムの置き換えではなく、レガシーシステムの近代化の取り組みと捉えるべきであることを顧客トップ層に伝えている。必要によってはクラウドに移行するなど、システム全体の暗号アジリティを確保できる体制づくりを顧客と共に進めることをゴールとしている。

2.2. クラウドにおける鍵管理ガイダンスの作成

今年度はクラウド鍵管理ガイダンスの骨子となる資料を作成した。以下に、骨子の概要をまとめる。

2.2.1. クラウド鍵管理ガイダンスの目次案

本ガイダンスの目次案は以下のとおりである。

1. はじめに
2. 基礎知識
3. クラウド鍵管理サービスについて
4. クラウド鍵管理サービスに関わる責任分界
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
6. その他

Appendix. 参考資料

1 章では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 章では、クラウド鍵管理に関わる技術や政府システムにおける要件などの基礎知識をまとめる。3 章では、クラウド鍵管理サービスを体系化して比較する。4 章では、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 章では、NIST SP 800-130 を基に鍵管理における管理策を抽出して、クラウド鍵管理サービス利用時の責任分界の適用例や利用者側の実施事項について説明する。6 章では、本ガイダンスでとりあげていない周辺事項に触れる。

以降では、ガイダンスの中核となる 1 章、3 章、5 章の概要を説明する。

2.2.2. 「1．はじめに」の概要

本ガイダンスの目的、位置づけ、想定読者、スコープは以下のとおりである。

<u>目的・位置づけ</u>

- 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た解説書を作成し、クラウド環境で安全に暗号を運用するための一つのガイダンスとする。
- 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」

を作成しており、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 事業者等）、運用者。本ガイダンスで「利用者」と表記した場合は、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、情報システムを構築するケースを対象に、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、どのようにクラウド鍵管理サービスを利用するかをターゲットとする。なお、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。

2.2.3. 「３．クラウド鍵管理サービスについて」の概要

クラウドに利用者が保存するデータの保護を対象として、CSP が提供する鍵管理サービスを体系化する。それらの違いや選択時の考慮事項を整理する。

クラウド鍵管理サービスの分類

クラウド鍵管理サービスを分類する要素を示し、一般に使われるクラウドネイティブ鍵管理、BYOK（Bring Your Own Key）、HYOK（Hold Your Own Key）、BYOE（Bring Your Own Encryption）等の用語との関係を説明する。

図 2-3 に各方式の構成概要を示す。鍵の統制権、鍵の保管場所、データの暗号・復号処理の実行場所、の 3 点に着目することでそれぞれの特徴を整理できる。

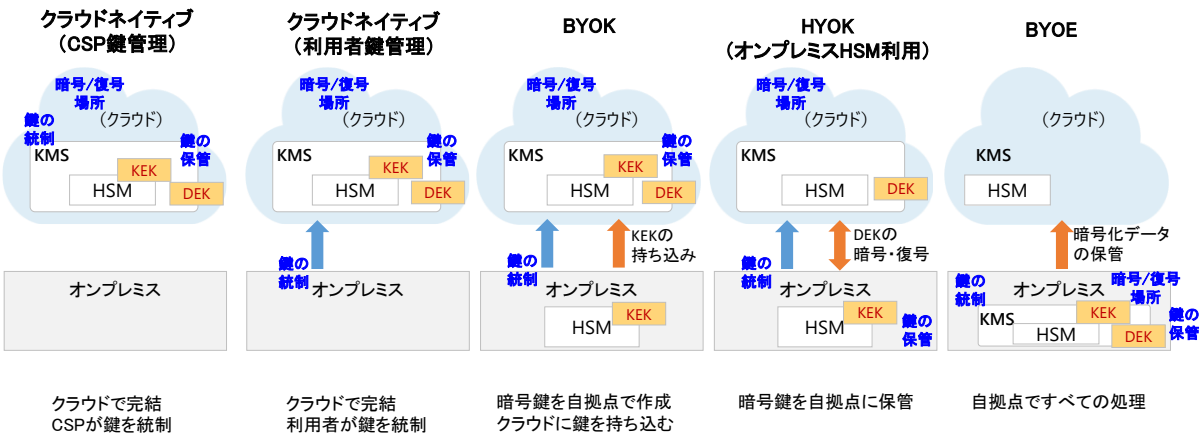


図 2-3　クラウド鍵管理サービスの構成概要

<u>クラウド鍵管理サービスの比較</u>

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。

一般に図 2-3 の右側の方式になるほど暗号鍵に関わる利用者の管理レベルが上がる一方で、利用者側の鍵管理基盤の構築や運用に関わるコストが増加する。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り、他の方式はそれぞれの方式の特徴に関わる要件が自組織のポリシーとして存在する場合に選択候補として考えるのが適当である。また、HYOK や BYOE は対象とする IaaS や PaaS におけるクラウドサービスとの連携がされていない場合が多く、選択できないケースがあることにも注意すべきである。

2.2.4.　「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」の概要

クラウドサービスを導入した場合でも暗号鍵管理システムの設計・運用において検討すべきことは変わらないが、オンプレミスでの構築と比べて利用者が重点的に検討すべきことは変わる。本章では、利用者から見てどのような項目に重点が置かれるかを NIST SP 800-130 の検討項目の視点から整理する。

<u>CKMS フレームワーク要求の適用について</u>

NIST SP 800-130 のフレームワーク要求（FR）は CKMS 設計者を主対象に書かれており、FR として扱うと CSP が検討すべき内容が多数となる。そこで、同文書を元に暗号鍵管理システムの管理策として項目を整理する。このようにして、クラウド鍵管理サー

ビスを利用する場合の責任分界の検討や利用者側の実施項目の抽出において参照可能となる管理項目一覧を作成する。

CKMS 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例

上記のように作成した管理項目一覧を基に、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）の３方式において利用者の実施項目を抽出した例を説明する。ここでは、クラウドネイティブ（利用者鍵管理）における責任分界の例を表 2-１に示す。

表 2-1　クラウドネイティブ（利用者鍵管理）における責任分界の例

管理項目	設計指針の該当節/番号	責任分界（実施責任）※	クラウド鍵管理での実施内容
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	[利用者]	DEK の暗号化及びデータ保護に利用する暗号アルゴリズム・暗号利用モード・鍵長は、CSP の提供方式の中から利用者が選択する。
メタデータの管理	7.2	[利用者]	メタデータ（特に鍵のタイプや保護対象とするデータ）は CSP の選択メニューから利用者が設定する。
ライフサイクルの定義と管理	5.2, 5.3		
暗号機能の実行場所	5.3 ③	CSP	KEK 及び DEK を利用した暗号処理の実行場所は CSP の提供サービスに依存する。KEK を利用した暗号処理はクラウド HSM 内で実行され、DEK を利用した暗号処理はクラウドサービス環境において実行される。
鍵生成	5.3 ⑧	[利用者]	KEK の生成は利用者がクラウド KMS を操作して実施する。DEK はクラウド側で自動的に生成される。
鍵情報の破壊	5.3 ⑦	[利用者]	KEK の破壊（消去）は利用者がクラウド KMS を操作して実施する。KEK の破壊（消去）によって、DEK 及び保護対象データの暗号化消去が行われる。
鍵更新（＝鍵ローテーション）	5.3 ⑨	[利用者]	KEK のローテーションは利用者がクラウド KMS を操作して実施する。DEK のローテーションは原則として行われない。
鍵活性化、鍵非活性化、鍵失効、鍵の一時停止	5.3 ② ,④,⑤,⑥	[利用者]	KEK の非活性化や一時停止等の状態管理は、クラウド KMS の提供機能に基づいて利用者が操作して実施する。
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	[利用者]	鍵情報へのアクセス権限は利用者が設定する。クラウドにおける IAM 機能と連携してアクセス管理が実施される。
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	CSP	KEK 及び DEK のストレージ保管とそこで実施されるセキュリティは、CSP の提供サービスによる。KEK はクラウド HSM での保管、DEK は KEK で暗号化してクラウドサービス環境における保管などの形態がとられる。
鍵情報のバックアップ	5.4 ③	CSP	鍵情報のバックアップは CSP の提供サービスによる。
鍵情報のアーカイブ	5.4 ④	CSP	古い世代の鍵情報の保存（アーカイブ）は CSP の提供サービスによる。

鍵情報の復元	5.4 ⑤	CSP	バックアップやアーカイブされた鍵情報を復元して利用可能とする機能は、CSP の提供サービスによる。
鍵確立	5.5	CSP	クラウドシステム内やインターネットにおける各種通信に関わる保護機能（鍵確立を含む）は、CSP の提供サービスによる。
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	CSP	鍵情報の喪失や破損に関わる対策は、CSP の提供サービスによる。クラウド HSM を含めて冗長構成などがとられる。
鍵情報の危殆化時の対策	5.7	CSP	鍵情報の危殆化対策は、CSP の提供サービスによる。
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	利用者	CKMS のセキュリティポリシーは利用者側の要件であり、それに適合したクラウド鍵管理サービスを選択する。クラウド鍵管理に関わるエンティティ及び役割は、CKMS セキュリティポリシーに基づいて利用者側が定める。
暗号モジュール	8.1.2	CSP	KEK 管理に用いる HSM の暗号鍵保護メカニズムや HSM の第三者認証は、CSP の提供サービスによる。
CKMS のセキュリティコントロール	9.1	CSP	CKMS のシステムとしてのセキュリティコントロール（物理的セキュリティコントロール、コンピュータシステム・セキュリティコントロール、ネットワーク・セキュリティコントロール）は CSP の提供サービスによる。利用者鍵（KEK）の操作に関わるログ機能は CSP の提供サービスによる。
CKMS の障害・災害対策	9.5	CSP	CKMS のシステムとしての障害・災害対策は CSP の提供サービスによる。
将来的な移行対策	4.7	[利用者]	暗号アルゴリズム及び鍵長の移行（PQC を含む）、鍵確立プロトコルの移行、鍵管理デバイス（HSM など）の移行といった対策は、CSP の提供サービスによる。暗号アルゴリズムや鍵長の移行のコントロールは、利用者が行う。

※[利用者]は CSP の基盤上で利用者側での操作・設定などの運用が要求される項目。[ ]がないものは運用以外に設計や構築も要求される項目。

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をより詳しく解説する。以下の事項等について説明を行う予定である。

- クラウド鍵管理方式の選択
- 暗号アルゴリズムと鍵の生成パラメータの設定、選択
- 鍵のライフサイクル
- 鍵へのアクセス管理
- ログ管理、監視

2.3. 「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）」の修正について検討した。検討の背景は、2023－2024 年度に実施した「暗号鍵管理ガイダンス Part 2」の作成過

程で、同ガイダンスの親文書に相当する設計指針に対する修正意見が幾つかあったことである。さらに、設計指針の執筆から約５年が経過し、記載内容の最新化や明確化を行った方がよい箇所や誤記も見つかっているため、修正すべき箇所と修正案を議論し、「設計指針 第 1.1 版」として改訂を行う方針とした。

以下に、記載内容の最新化や明確化に関わる主な修正箇所をまとめる。この他の修正箇所については記載を省略する。

改訂版は、CRYPTREC の暗号運用ガイドラインのサイトを参照されたい。

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

該当箇所	「設計指針」記載内容の問題	「設計指針」の修正方針及び修正内容
「2.1 暗号鍵管理の必要性」、本文（p.10）	「政府機関の情報セキュリティ対策のための統一基準（平成 30 年度版）」（平成 30 年 7 月 25 日、サイバーセキュリティ戦略本部）が参照されている。 また、**「「統一基準」でも暗号鍵の管理手順を定めることになっているように、データが保護される期間中、その暗号アルゴリズムが使用する暗号鍵もセキュアに管理されている必要がある。」**と書かれているが、最新の「統一基準」に暗号鍵の管理手順を定める記載はない。	最新の統一基準（令和 7 年度版）を参照する。また、暗号鍵の管理手順を定めることが基本対策事項として書かれている「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）の一部改定（令和 7 年 9 月）」を参照して、該当箇所の本文及び引用内容を更新する。 「「対策基準策定のためのガイドライン」でも暗号鍵の管理手順を定めることが基本対策事項になっているように、…」とする。
「2.2.4 Guidance」、本文（p.15）、及び図 2-2（p.12）	Guidance 文書に**「リストガイド（鍵管理）」**と書かれているものがあるが、対象文書が明確でない。	「リストガイド（鍵管理）」を**「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」**の 2 文書に変更する。
「2.6.1 SP800-57」、本文（p.24）	SP 800-57 Part 1 の最新の更新版 rev.5 が書かれていない。**「2005 年に初版が発行され、2006 年、2007 年、2012 年（revision 3）、2016 年（revision 4）に改訂されている。」**と書かれている。	**「…、2012 年、2016 年、2020 年（revision 5）に改訂されている。」**と修正する。

該当箇所	「設計指針」記載内容の問題	「設計指針」の修正方針及び修正内容
「4.7 将来的な移行対策の必要性」、 ②、 本文（p.52）	暗号解読に関わる量子コンピュータやPQC について 2020 年当時の状況が書かれている。現状を踏まえて更新した方がよい。 **「・新しい計算機技術の発展** **現状の脅威で最も高い関心が払われているものは、暗号鍵を復元するのに十分な能力を持つ量子コンピュータの発展である。** **例えば、大きなキュービットの量子コンピュータが構築されれば、既存の公開鍵暗号アルゴリズムのセキュリティが脅かされるかもしれず、これらのアルゴリズムに暗号鍵の確立を依存する CKMS に対して重大な影響を与える可能性がある。** **一方、量子コンピュータに耐性がある公開鍵暗号アルゴリズム（耐量子計算機暗号）についての研究や標準化が現在進行中であるが、現時点で広く受け入れられている解はまだ見出されていない。」**	以下の記載に変更する。 **「・新しい計算機技術の発展** **現状の脅威で最も高い関心が払われているものは、現在広く使われている暗号の秘密鍵を復元するのに十分な能力を持つ量子コンピュータの発展である。** **そのような量子コンピュータによる攻撃にも耐性がある公開鍵暗号（耐量子計算機暗号）について各国の組織で研究や標準化活動が進展しており、米国 NIST では複数の標準方式が選定された。」** さらに、脚注を設けて「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」のリンクを記載する。 https://www.cryptrec.go.jp/tech_guidelines.html
「6.1.1 暗号アルゴリズムのセキュリティ強度」、 本文及び表 6-1 （p.79 - 81）	ビットセキュリティの表 6-1 を SP 800-57 Part 1 を参照して記載しているが、CRYPTREC では後に「暗号強度要件に関する設定基準」を発行している。同表には「強度要件」では推奨されていない方式やセキュリティ強度も記載されている。 また、表 6-1 について本文に以下のように書かれている。 **「そこで、暗号アルゴリズムの選択においては、“x ビットセキュリティ”の“x ビット”に着目して、長期的な利用期間の目安とする使い方ができる。例えば、NIST SP800-57 Part 1 revision 4 を参考にすると、電子政府推奨暗号リストに記載の暗号アルゴリズムのビットセキュリティは表 6-1 のように表現できる。」**	「暗号強度要件に関する設定基準」に沿った表記に更新する。 具体的には、表 6-1 を強度要件に記載されているセキュリティ強度と暗号アルゴリズムに変更する。 さらに、表 6-1 に関わる本文を以下の記載に修正する。 **「「暗号強度要件に関する設定基準」において、CRYPTREC 暗号リストに掲載されている暗号アルゴリズムのビットセキュリティによるセキュリティ強度、並びに、電子政府システムにおけるセキュリティ強度要件の基本的な設定方針が示されている。同文書に基づいて CRYPTREC 暗号リストに掲載されている暗号アルゴリズムと基本的な利用期間の設定方針をまとめると表 6-1 のようになる。」**

該当箇所	「設計指針」記載内容の問題	「設計指針」の修正方針及び修正内容
「7.1 鍵情報の種類」、 表 7-1（p.83）	「表 7-1 鍵タイプ一覧」が SP 800-130(2012 年)に基づいて書かれており、表内に**「乱数生成プライベート鍵」**と**「乱数生成公開鍵」**が含まれているが、最新の SP 800-57 Part 1, rev.5(2020 年)ではこの 2 つの鍵タイプは削除されている。本文に**「SP800-130 で分類する鍵タイプは表 7-1 の通りである」**と書かれている。	表 7-1 から**「乱数生成プライベート鍵」**と**「乱数生成公開鍵」**を削除する。併せて、本文を**「SP 800-57 Part 1, rev.5 で分類する鍵タイプは表 7-1 のとおりである。」**と修正する。
「9.2 システム保証」 ② 見出し及び本文（p.107）	**「セキュアな配付」**と書かれているが、SP 800-130 では「secure delivery」となっている。	製品配送に関わる記載であり、**「セキュアな配送」**と変更する。
「9.2 システム保証」 ④ 本文（p.108）	**「欠陥修正能力に関する検知、報告、修正」**と表記されている中で、「報告」については**「通知」**の表記も混在している。SP 800-130 では「report」と書かれている。	**「報告」**に用語を統一する。
「9.3 セキュリティアセスメント」 ② 見出し及び本文（p.110 - 111）	**「定期的なセキュリティアセスメント」**と書かれているが、SP 800-130 では「security review」となっている。FR の表内では「セキュリティレビュー」と書かれており、表記が混在している。	**「定期的なセキュリティレビュー」**に表記を変更し、用語を統一する。

第3章　今後に向けて

2026 年度は以下の活動を実施する予定である。

1)　暗号強度要件ガイドラインに PQC の取り扱いを含める形で見直しを実施し、2026 年度末での完成を目指す。

2)　TLS 暗号設定ガイドラインについては、PQC サポートに向けた TLS1.3 への移行や PQC 関連技術の取り込み、現行のセキュリティ例外型の削除など、現在の TLS 暗号設定ガイドラインの前提条件が大きく変わりつつことを踏まえ、記載内容の見直し検討を 2026 年度より開始する。2027 年度末でのガイドライン見直しの完成を目指す。

3)　引き続き、「クラウド鍵管理ガイダンス」の作成を進め、2026 年度末に完了する予定である。

【別紙】

2025 年度クラウド鍵管理ガイダンス WG 活動報告

1. 2025 年度の活動概要

1.1. 活動目的と活動概要

CRYPTREC では、情報システム設計者やシステム調達者が暗号の利活用を適切に行うためのガイドライン作成を進めており、暗号技術活用委員会では 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（CKMS：Cryptographic Key Management System）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）」を 2020 年度に発行した。さらに、本文書の副読本として 2023 年度に「暗号鍵管理ガイダンス Part 1」を、2025 年度に「暗号鍵管理ガイダンス Part 2」をそれぞれ発行した。これらの文書はオンプレミス環境において CKMS を設計する場合を暗黙に想定している。

一方、クラウドサービスを活用して効率的に情報システムを構築することは一般的になっている。その場合には、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システムを適切に選択・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。そこで、今年度よりクラウド鍵管理ガイダンス WG を設置して、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解説した「クラウド鍵管理ガイダンス」の作成を開始した。今回作成する解説書は、これまでに発行した暗号鍵管理システムの設計に係る CRYPTREC 文書を補強する位置づけにもなる。

1.2. クラウド鍵管理ガイダンス WG の委員構成及び開催状況

クラウド鍵管理ガイダンス WG の委員構成は表 1-1 のとおりである。また、2025 年度の開催状況は表 1-2 のとおりである。

表 1-1　クラウド鍵管理ガイダンス WG　委員構成

主査	上原　哲太郎	立命館大学　情報理工学部　情報理工学科　教授
委員	漆嶌　賢二	GMO グローバルサイン株式会社 事業企画部 フェロー
委員	垣内　由梨香	日本マイクロソフト　リージョナルセキュリティチーム リスクマネージャー
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	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 インターネットサービス事業本部　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	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, Security
委員	畠中　亮	デジタル庁　クラウドマイグレーションユニット　ユニット長
委員	舟木　康浩	タレス DIS 株式会社 サイバーセキュリティプロダクト事業本部 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　ソリューション事業本部 セキュリティ＆ネットワーク事業部 サイバーセキュリティ統括部　課長代理
委員	満塩　尚史	順天堂大学　健康データサイエンス学部 健康データサイエンス学科　准教授

（2026 年 1 月 26 日現在）

表 2-2　クラウド鍵管理ガイダンス WG　開催状況

回	開催日	議事概要
第一回	2025 年 9 月 8 日	■ 2025 年度クラウド鍵管理ガイダンス WG 活動計画の説明 ■ クラウド鍵管理ガイダンスの骨子に係る検討（審議）
第二回	2026 年 1 月 19 日	■ クラウド鍵管理ガイダンスの骨子に係る検討（審議） ■ 2025 年度クラウド鍵管理ガイダンス活動報告（審議）

2. 成果概要

今年度はクラウド鍵管理ガイダンスの骨子となる資料を作成した。以下、骨子の概要をまとめる。

クラウド鍵管理ガイダンスの目次案

本ガイダンスの目次案は以下のとおりである。

1. はじめに
2. 基礎知識

3. クラウド鍵管理サービスについて
4. クラウド鍵管理サービスに関わる責任分界
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
6. その他

Appendix. 参考資料

1章では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章では、クラウド鍵管理に関わる技術や政府システムにおける要件などの基礎知識をまとめる。3章では、クラウド鍵管理サービスを体系化して比較する。4章では、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章では、NIST SP 800-130 を基に鍵管理における管理策を抽出して、クラウド鍵管理サービス利用時の責任分界の適用例や利用者側の実施事項について説明する。6章では、本ガイダンスでとりあげていない周辺事項に触れる。

2.1. ガイダンス１章「はじめに」

ガイダンス 1 章では、ガイダンスの目的、位置づけ、想定読者、スコープ等をまとめる。

<u>目的・位置づけ</u>

- 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た解説書を作成し、クラウド環境で安全に暗号を運用するための一つのガイダンスとする。
- 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」を作成しており、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。

<u>想定読者</u>

- クラウドサービスを利用した情報システムの構築者（SI 事業者等）、運用者。以降、本ガイダンスで「利用者」と表記した場合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、情報システムを構築するケースを対象に、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、どのようにクラウド鍵管理サービスを利用するかをターゲットとする。なお、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。

2.2. ガイダンス 2 章「基礎知識」

ガイダンス 2 章では、以降の章を理解する上で必要となる基礎的な事項をまとめる。次の 3 つの節で構成する。

- 暗号鍵管理とは
- クラウドサービスにおける暗号技術
- クラウドサービス利用に関わる要件及び認証制度

「暗号鍵管理とは」の節では、一般に暗号鍵管理として要求される事項である、暗号鍵へのアクセス権限管理、暗号鍵のライフサイクル管理、暗号鍵の保管について NIST SP 800-57 part 1 を参照しながら説明する。さらに、NIST SP 800-130 に基づいて CKMS を設計する際の推奨事項として、CKMS の対象範囲を適切に定めたモジュール設計を行うことを説明する。これらの観点について、クラウドシステムではどのようにクラウド鍵管理サービスが設計されているかを概説する。

「クラウドサービスにおける暗号技術」の節では、クラウドサービスで扱われるデータが保存中データ、移動中データ、使用中データの 3 つの状態を遷移する中でクラウド鍵管理サービスが対象とするのは保存中データの暗号化に関わる鍵の管理であることを説明する。また、クラウド鍵管理で採用されている技術として、エンベロープ暗号化、鍵の階層管理、暗号化消去によるデータ廃棄があることを説明する。

「クラウドサービス利用に関わる要件及び認証制度」の節では、我が国の政府機関におけるクラウドサービス利用に関わる要件の中でクラウド鍵管理に関連する事項を説明する。ここでは、国家サイバー統括室（NCO）の「政府機関等のサイバーセキュリティ対策のための統一基準群」、デジタル庁の「クラウドサービス利用基本方針」、「政府情報情報システムのためのセキュリティ評価制度（ISMAP）」を参照する。クラウドサービスの利用においては、情報の暗号化に用いる鍵の管理主体を基本的に利用機関とすること、扱った情報の廃棄について確実に消去できる方法を採用すること等が要求されている。

これらに対応して、ISMAP にはクラウドサービスで扱う暗号鍵の利用者管理及び消去機能等の要件があり、政府機関等ではクラウドサービスの選定において、原則としてISMAP に登録されたサービスから選定することが定められている。

2.3. ガイダンス 3 章「クラウド鍵管理サービスについて」

ガイダンス 3 章では、クラウドに利用者が保存するデータの保護を対象として、CSP が提供する鍵管理サービスを体系化する。それらの違いや選択時の考慮事項を整理する。以下の節で構成する。

- クラウド鍵管理サービスの分類
- 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の分類」の節では、クラウド鍵管理サービスを分類する要素を示し、一般に使われるクラウドネイティブ鍵管理、BYOK（Bring Your Own Key）、HYOK（Hold Your Own Key）、BYOE（Bring Your Own Encryption）等の用語との関係を説明する。

- クライアントサイド暗号化とサーバサイド暗号化

クラウドに保存するデータの暗号化・復号の実行場所によって 2 つの方式がある。クライアントサイド暗号化は、暗号化・復号の処理を利用者のアプリケーションまたはプロセスが実行し、クラウドには暗号化済みデータのみが保存される方式である。BYOE はこの典型例である。他方、サーバサイド暗号化は、暗号化・復号の処理をクラウドサービス側が実行する方式である。そこで利用される暗号鍵の管理をクラウド鍵管理サービスとして CSP が提供している。

- クラウド鍵管理サービスの分類

クラウド鍵管理サービスの分類として、クラウドネイティブ鍵管理、BYOK、HYOK が使われることが多い。

- クラウドネイティブ鍵管理はクラウド側で暗号鍵を保管し、クラウドサービスと統合された方式。鍵管理を CSP 側で全て行うものと鍵管理のコントロールを利用者側で行うものがある。以降では「クラウドネイティブ鍵管理（CSP 鍵管理）」と「クラウドネイティブ鍵管理（利用者鍵管理）」と表記する。
- BYOK はオンプレミス側で生成した暗号鍵をクラウド側に持ち込むもの。鍵管理のコントロールは利用者側で行う。
- HYOK は利用者専用に設置された HSM において暗号鍵（鍵暗号化鍵 KEK）が管理され、クラウド側での暗号・復号処理において一時的に暗号鍵（データ暗号化鍵 DEK）が提供されるもの。オンプレミスの HSM を利用する場合と CSP が用意し

た顧客専用のクラウド HSM を利用する場合がある。以降では前者を取り上げ「HYOK（オンプレミス HSM 利用）」と表記する。

図 2-1 に各方式の構成概要を示す。鍵の統制権、鍵の保管場所、データの暗号・復号処理の実行場所、の 3 点に着目することでそれぞれの特徴を整理できる。

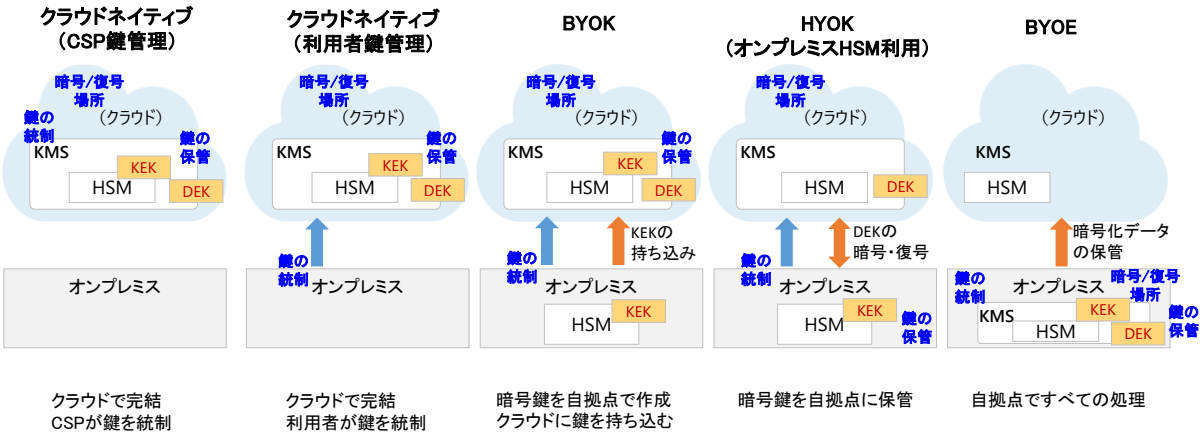


図 2-1　クラウド鍵管理サービスの構成概要

「クラウド鍵管理サービスの比較」の節では、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。

表 2-1 にクラウド鍵管理サービスの方式の比較を示す。表中、▲を記した箇所は方式採用時の懸念点である。一般に表の右側の方式になるほど暗号鍵に関わる利用者の管理レベルが上がる一方で、利用者側の鍵管理基盤の構築や運用に関わるコストが増加する。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方式であり、他の方式はそれぞれの方式の特徴に関わる要件がある場合に選択候補として考えるのが適当である。また、HYOK や BYOE は対象とする IaaS や PaaS におけるクラウドサービスとの連携がされていない場合が多く、選択できないケースがあることにも注意すべきである。

表 2-3　クラウド鍵管理サービスの比較

	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	☆ 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	☆☆ 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	☆☆ 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	☆☆☆ 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	☆☆☆☆ 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
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

2.4. ガイダンス 4 章「クラウド鍵管理サービスに関わる責任分界」

ガイダンス 4 章では、クラウド鍵管理サービスに関わる利用者と CSP の間の責任分界の原則を整理する。

クラウドサービスは CSP が情報処理の基盤を提供するマネージドサービスであり、利用者と CSP は実施責任（responsibility）をそれぞれの責任範囲に基づいて分担しているが、最終的な説明責任（accountability）は利用者が負っていることに注意すべきである。クラウド鍵管理サービスにおいて、鍵管理の機能構築に関わる項目は CSP が担当し、提供された機能を適切に運用する項目は利用者が担当するのが原則である。このように CSP と利用者の責任分界を示すモデルが前提となるため、利用者はクラウド鍵管理サービスの方式ごとの違いや責任分界の境界に関わる事項に注意すべきである。

また、CSP が実施責任を担う事項に対して、利用者が説明責任を果たすために利用できる情報や手段としては、クラウドサービスのセキュリティ評価制度の認証取得状況確

認、第三者監査レポートの確認、CSP との契約条項の確認、利用者鍵の管理に関わるクラウド処理のログ確認、等がある。

2.5. ガイダンス 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」

クラウドサービスを導入した場合でも暗号鍵管理システムの設計・運用において検討すべきことは変わらないが、オンプレミスでの構築と比べて利用者が重点的に検討すべきことは変わる。ガイダンス 5 章では、利用者から見てどのような項目に重点が置かれるかを NIST SP 800-130 の検討項目の視点から整理する。以下の節で構成する。

- CKMS フレームワーク要求の適用について
- CKMS 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例
- クラウド鍵管理サービスにおける利用者の管理事項

「CKMS フレームワーク要求の適用について」の節では、NIST SP 800-130 のフレームワーク要求を基に暗号鍵管理システムの管理策として項目を整理した上で、クラウド鍵管理サービスを利用する場合の責任分界や利用者側の実施項目の抽出において参照可能な管理項目表を記載する。この管理項目表を表 2-2 に示す。

表 2-4　暗号鍵管理における管理項目

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。
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。 ・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。 ・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。 ・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。

「CKMS 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例」の節では、上記管理項目表を基に、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）の 3 方式において利用者の実施項目を抽出した例を説明する。

クラウドネイティブ（利用者鍵管理）における責任分界の例を表 2-3 に示す。表中、「責任分界」欄に、[利用者]とした項目は CSP が提供する鍵管理基盤上で利用者が操作・設定などの運用を担うものであり、[ ]のない項目は設計・構築及び運用を担うものである。

表 2-5　クラウドネイティブ（利用者鍵管理）における責任分界の例

管理項目	設計指針の該当節/番号	責任分界（実施責任）※	クラウド鍵管理での実施内容
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	[利用者]	DEK の暗号化及びデータ保護に利用する暗号アルゴリズム・暗号利用モード・鍵長は、CSP の提供方式の中から利用者が選択する。
メタデータの管理	7.2	[利用者]	メタデータ（特に鍵のタイプや保護対象とするデータ）は CSP の選択メニューから利用者が設定する。

ライフサイクルの定義と管理	5.2, 5.3		
暗号機能の実行場所	5.3 ③	CSP	KEK 及び DEK を利用した暗号処理の実行場所は CSP の提供サービスに依存する。KEK を利用した暗号処理はクラウド HSM 内で実行され、DEK を利用した暗号処理はクラウドサービス環境において実行される。
鍵生成	5.3 ⑧	[利用者]	KEK の生成は利用者がクラウド KMS を操作して実施する。DEK はクラウド側で自動的に生成される。
鍵情報の破壊	5.3 ⑦	[利用者]	KEK の破壊（消去）は利用者がクラウド KMS を操作して実施する。KEK の破壊（消去）によって、DEK 及び保護対象データの暗号化消去が行われる。
鍵更新（＝鍵ローテーション）	5.3 ⑨	[利用者]	KEK のローテーションは利用者がクラウド KMS を操作して実施する。DEK のローテーションは原則として行われない。
鍵活性化、鍵非活性化、鍵失効、鍵の一時停止	5.3 ②,④,⑤,⑥	[利用者]	KEK の非活性化や一時停止等の状態管理は、クラウド KMS の提供機能に基づいて利用者が操作して実施する。
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	[利用者]	鍵情報へのアクセス権限は利用者が設定する。クラウドにおける IAM 機能と連携してアクセス管理が実施される。
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	CSP	KEK 及び DEK のストレージ保管とそこで実施されるセキュリティは、CSP の提供サービスによる。KEK はクラウド HSM での保管、DEK は KEK で暗号化してクラウドサービス環境における保管などの形態がとられる。
鍵情報のバックアップ	5.4 ③	CSP	鍵情報のバックアップは CSP の提供サービスによる。
鍵情報のアーカイブ	5.4 ④	CSP	古い世代の鍵情報の保存（アーカイブ）は CSP の提供サービスによる。
鍵情報の復元	5.4 ⑤	CSP	バックアップやアーカイブされた鍵情報を復元して利用可能とする機能は、CSP の提供サービスによる。
鍵確立	5.5	CSP	クラウドシステム内やインターネットにおける各種通信に関わる保護機能（鍵確立を含む）は、CSP の提供サービスによる。
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	CSP	鍵情報の喪失や破損に関わる対策は、CSP の提供サービスによる。クラウド HSM を含めて冗長構成などがとられる。
鍵情報の危殆化時の対策	5.7	CSP	鍵情報の危殆化対策は、CSP の提供サービスによる。
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	利用者	CKMS のセキュリティポリシーは利用者側の要件であり、それに適合したクラウド鍵管理サービスを選択する。クラウド鍵管理に関わるエンティティ及び役割は、CKMS セキュリティポリシーに基づいて利用者側が定める。
暗号モジュール	8.1.2	CSP	KEK 管理に用いる HSM の暗号鍵保護メカニズムや HSM の第三者認証は、CSP の提供サービスによる。
CKMS のセキュリティコントロール	9.1	CSP	CKMS のシステムとしてのセキュリティコントロール（物理的セキュリティコントロール、コンピュータシステム・セキュリティコントロール、ネットワーク・セキュリティコントロール）は CSP の提供サービスによる。利用者鍵（KEK）の操作に関わるログ機能は CSP の提供サービスによる。
CKMS の障害・災害対策	9.5	CSP	CKMS のシステムとしての障害・災害対策は CSP の提供サービスによる。

将来的な移行対策	4.7	[利用者]	暗号アルゴリズム及び鍵長の移行（PQC を含む）、鍵確立プロトコルの移行、鍵管理デバイス（HSM など）の移行といった対策は、CSP の提供サービスによる。暗号アルゴリズムや鍵長の移行のコントロールは、利用者が行う。

※[利用者]は CSP の基盤上で利用者側での操作・設定などの運用が要求される項目。[ ]がないものは運用以外に設計や構築も要求される項目。

「クラウド鍵管理サービスにおける利用者の管理事項」の節では、利用者側の管理事項をより詳しく解説する。

- クラウド鍵管理方式の選択
  クラウド鍵管理方式の選択は利用者が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、クラウド鍵管理システムを含むインフラストラクチャ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選択すべき事項である。
- 暗号アルゴリズムと鍵の生成パラメータの設定、選択
  クラウド鍵管理サービスでは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、その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
  クラウド鍵管理サービスでは、暗号鍵のライフサイクルを支援する管理機能（鍵の生成・無効化・削除・ローテーション設定など）が提供されている。他方で、暗号鍵の有効期間（cryptoperiod）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
  暗号鍵のアクセス管理は、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。その目的は、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にある。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

暗号鍵のログ管理および監査は、情報システム全般に適用される監査・監視統制（NIST SP 800-53 の AU 系統制）を基盤とし、これに暗号鍵管理システムに対して NIST SP 800-130 が要求する監査機能を適用したものである。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にアクセスしこれら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。

2.6. ガイダンス 6 章「その他」

ガイダンス 6 章では、前章までに説明していない事項や関連動向をまとめる。説明を予定するトピックは以下のとおりである。

- SaaS における暗号鍵管理
- コンフィデンシャル・コンピューティング
- 使用中データの保護に関わる暗号技術（秘密計算や準同型暗号）

3. 今後に向けて

今年度は、クラウド事業に関わる委員の知見を活用し、クラウド鍵管理ガイダンスの骨子を整理した。記載方針や全体構成など議論の必要な部分は残っているが、来年度は骨子の見直しを行いつつ本文の作成を進め、ガイダンスを完成させることを目標とする。

また、現在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どのように扱うかについての検討も予定している。

以上

CRYPTREC Report 2025
(暗号技術活用委員会報告　CRYPTREC RP-3000-2025)

発行日　2026年6月30日 第1版（印刷版）
発行者
・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人情報処理推進機構
(セキュリティセンター 技術評価部 暗号グループ)
INNOVATION PLATFORM AGENCY, JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北町四丁目2番1号
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 セキュリティ基盤研究室)
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN