CRYPTREC シンポジウム 2025

ガバメントクラウドにおける暗号鍵管理

2025/7/25

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　畠中 亮

デジタル庁
Digital Agency

はたなか りょう

畠中 亮

デジタル庁 ガバメントクラウドチーム
クラウドマイグレーションユニット ユニット長

職務概要

2023年よりデジタル庁にて国の行政機関や地方公共団体等のシステムの稼働環境となるガバメントクラウドへの移行支援組織の運用、ガバナンス&セキュリティ施策を担当している。

デジタル庁までの経歴

- 外資系SIer インフラアーキテクト (2003～2014)

  自社セキュリティ製品やデスクトップ仮想化製品(VDI)を中心に全業種の顧客に対してプリセールスやアーキテクトとして活動。

- 事業会社 セキュリティコンサルタント/Unit Leader(2014～2016)

  50社を超えるグループ会社へのセキュリティ施策の展開責任者を担当し、計画立案から数万台の端末ログ取得やビッグデータ基盤からの個人情報削除等を実現。

- 外資系クラウドサービスプロバイダー マネージャー(2016～2023)

  自社クラウドのセキュリティサービス/機能活用に関するコンサルティングサービス部門を立ち上げ、マネージャーとして組織とビジネスを拡大。自身も96のコンサルプロジェクトを担当。

資格

CISSP/CISA/CISM/CCSP
AWS/さくらのクラウド/Google Cloud 等

著作

「AWSではじめるクラウドセキュリティ」(共著)
「Amazon Web Services企業導入ガイドブック[改訂版]」(共著)

本日の内容

1. ガバメントクラウドと利用状況
2. 暗号化実施時の重要な考慮ポイントと暗号鍵管理の位置付け
3. 公共情報システムに求められる暗号化関連要件
4. ガバメントクラウドの技術要件
5. 鍵管理の留意事項とガバメントクラウド

まとめ

1. ガバメントクラウドと利用状況

1.1 デジタル庁の概要

2021年9月に発足したデジタル庁は、次のミッションを掲げ、デジタル社会の実現を通じて、国民の皆様にさまざまなメリットを受け取っていただけるよう、各種施策を推進しています。

ミッション

誰一人取り残されない、人に優しいデジタル化を。

一人ひとりの多様な幸せを実現するデジタル社会を目指し、世界に誇れる日本の未来を創造します。

ビジョン

優しいサービスのつくり手へ。

Government as a Service

国、地方公共団体、民間事業者、その他あらゆる関係者を巻き込みながら有機的に連携し、
ユーザーの体験価値を最大化するサービスを提供します。

大胆に革新していく行政へ。

Government as a Startup

高い志を抱く官民の人材が、互いの信頼のもと協働し、多くの挑戦から学ぶことで、
大胆かつスピーディーに社会全体のデジタル改革を主導します。

1.2 デジタル社会を実現する施策としてのクラウド利用

クラウドの検討や利用はデジタル社会を実現するための施策として位置付けられています。

クラウド第一
（クラウド・バイ・デフォルト）
原則

重点計画の「デジタル社会の実現に向けた理念・原則」の1つ

「各府省庁において必要となる情報システムの整備に当たっては、迅速かつ柔軟に進めるため、クラウド第一原則（クラウド・バイ・デフォルト原則）を徹底し、クラウドサービスの利用を第一候補として検討する」(2017年)

政府情報システムにおける
クラウドサービスの適切な
利用に係る基本方針

デジタル社会推進標準ガイドラインの1つ

「本方針は、デジタル・ガバメント推進標準ガイドラインが適用されるサービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理に関する事項に適用するものとする。」

情報通信技術を活用した
行政の推進等に関する法律

ガバメントクラウド利用の検討(2024年12月に法改正)

「国の行政機関等は、（中略）クラウド・コンピューティング・サービス（中略）を利用することについて検討を行い、その結果に基づいて当該公共情報システムの整備を行わなければならない。」
「国の行政機関等以外の行政機関等は、（中略）クラウド・コンピューティング・サービスの利用に関する検討及びその結果に基づく当該公共情報システムの整備に係る取組を行うよう努めなければならない。」

1.3 ガバメントクラウドの概要と利用状況

デジタル庁は国の行政機関や地方公共団体、準公共分野向けに共通のクラウドサービス利用環境として「ガバメントクラウド」を整備しています。

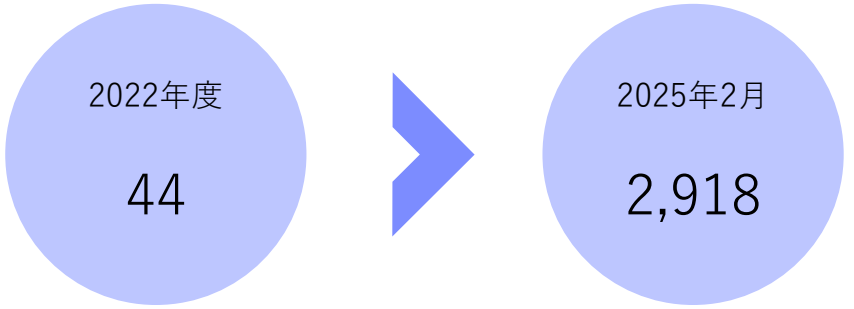
特徴

- 利用者は、自身で**調達することなくデジタル庁が予め選定した複数社のクラウド**から選んで、既成のクラウドサービスを使うことができる
- デジタル庁は、ルールやガイド、IaCテンプレート、セキュリティ統制等の**ガバナンスに必要な機能を利用者に提供**し、**クラウド最適でモダンなシステム構成の採用を推進**する
- デジタル庁はクラウドサービスの利点を最大限に活用して、**迅速、柔軟、かつセキュアでコスト効率の高い**システムの実現を目指すことのできる環境の提供に注力する

ガバメントクラウド ＝ 技術要件を満たした民間クラウド ＋ ITガバナンス機能

デジタル庁が契約したクラウドサービス
Amazon Web Services
Google Cloud
Microsoft Azure
Oracle Cloud Infrastructure
さくらのクラウド（条件付き*で選定）

利用状況

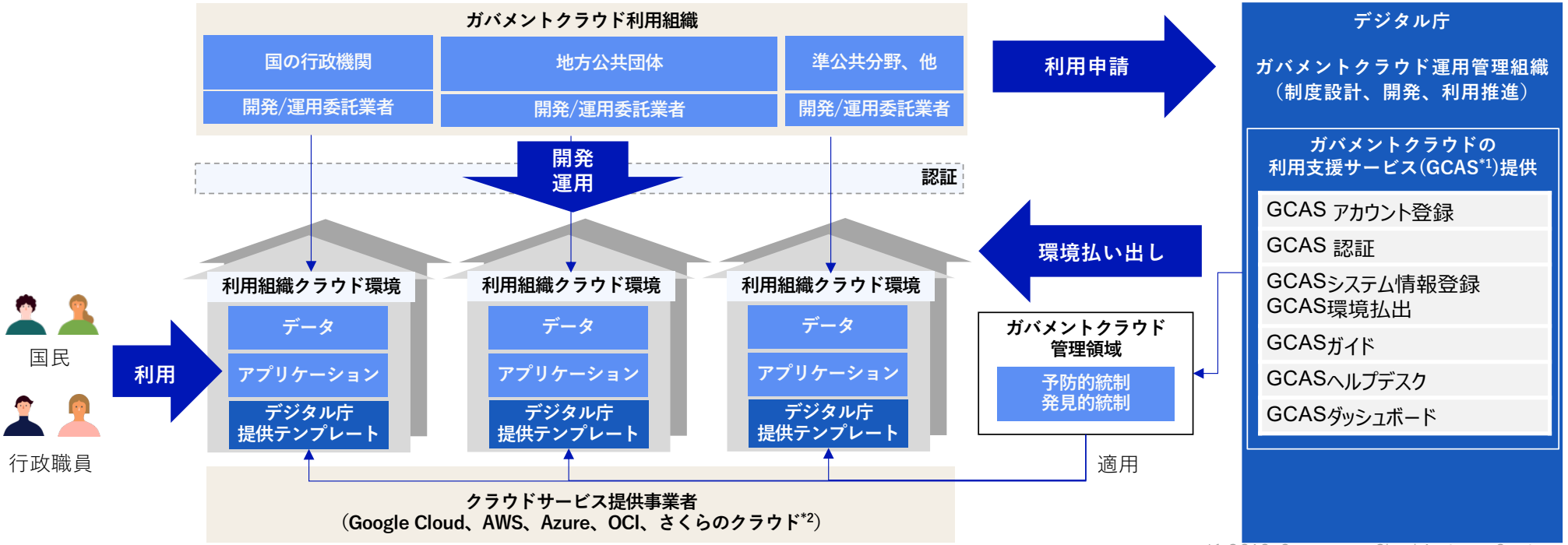


*さくらのクラウドは2025年度末までに全ての技術要件を達成することの条件付き

1.4 ガバメントクラウドの全体像

ガバメントクラウドでは利用組織の申請により、各クラウドサービスの利用が可能な環境が払い出されます。

- 利用組織の申請単位（システム/環境種別)に、他の環境から**独立した環境とその管理権限**を提供
- 利用組織（および開発・運用業務の委託を受けた事業者）が、各環境で**公共情報システムを構築、運用**
- 利用組織の管理者は、GCAS*1を使って、**ガバメントクラウドに関わる各種申請(ユーザー登録等)**が可能



*1 GCAS: Government Cloud Assistant Service

*2さくらのクラウドは2025年度末までに全ての技術要件を達成することの条件付き

1.5 公共情報システム運用基盤としてのガバメントクラウドの取り組み

ガバメントクラウドでは利用組織の公共情報システムの運用基盤の受け皿になることを目指し、主に次に挙げる3点を考慮して環境の整備に取り組んでいます。本講演では暗号鍵管理に関連し、その取り組みについて取り上げます。

公共情報システムに 求められる要件の把握と クラウドサービスの調達	統制を施した クラウド環境の提供	クラウド利用に 関するガイドの提供
公共情報システムに 求められる各種要件の 調査・把握、 クラウドサービスの調達に 関わる技術要件の調査、 定義、調達	**ガバメントクラウドとして 必要な統制を 維持するための 仕組みの開発・運用**	**利用組織が各種要件を 充足できるよう、 ガバメントクラウドの 利用手順や構築・運用時の 推奨事項を明示** **(例:リファレンスアーキテクチャーの提供など)**

2. 暗号化実施時の重要な考慮ポイントと暗号鍵管理の位置付け

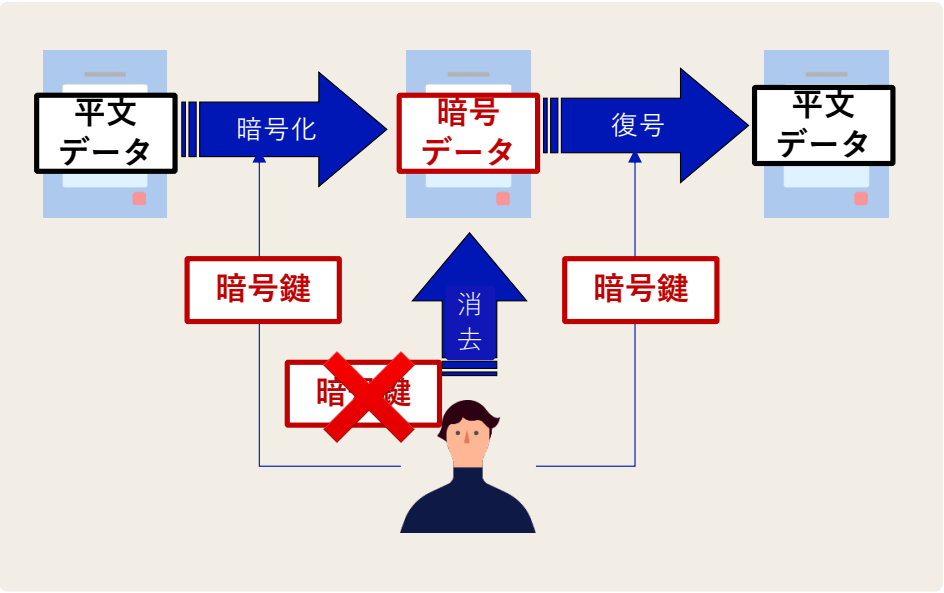
2. 暗号化実施時の重要な考慮ポイントと暗号鍵管理の位置付け

データを秘匿化するために暗号化を実施する際はアルゴリズムや鍵長の選択が重要になります。
さらに、データの暗号化、復号は暗号鍵を用いて実施するため、暗号鍵管理を適切に実施する必要があります。

堅牢なアルゴリズムの選択	適切な鍵長の選択	暗号鍵の適切な管理 *本講演では保管データの暗号化に用いる鍵を対象とします
元データを鍵を利用して別のデータに置き換える計算の処理方式が脆弱であると、鍵を予測されてしまう	鍵の長さが短いと予測されてしまう 但し、暗号化処理の負荷に留意	アルゴリズムや鍵長が堅牢であっても暗号鍵を入手することで暗号化データを復号できてしまう 暗号鍵の保護 / 暗号鍵のライフサイクル管理 / 暗号鍵の可用性

【補足】クラウドにおけるデータ消去方法としての暗号化消去

従来よりストレージ機器からのデータ漏えいを防ぐため記録媒体の物理的破壊や論理的消去とその証拠となる証明書の発行が行われています。クラウド環境は個別対応が難しく暗号鍵の削除によるデータ消去が求められています。



物理的破壊	細断、分解、粉砕、焼却など
論理的消去	新しい値で書き換えるなど **暗号鍵の削除による「暗号化消去」**

クラウド上の利用者データを事前に暗号化しておく対応が求められている

3. 公共情報システムに求められる暗号化関連要件

3.1 政府統一基準における暗号鍵関連の要件

国の行政機関及び独立行政法人等のセキュリティ対策基準のベースラインとして活用されている「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」では、暗号鍵に関連する以下の対策事項が挙げられています。

❑基本対策事項2.1.2(1)-1q)「情報の暗号化に用いる鍵の管理主体」について

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をする主体を明確にしておく必要がある。利用するクラウドサービスの形態及び仕様によっては、暗号鍵の管理をクラウドサービス提供者自身によって行っているサービスも存在し、クラウドサービス提供者がクラウドサービス利用者の情報を復号できてしまう可能性もある。また、クラウドサービスの利用を終了する際に、クラウドサービスで取り扱った情報の廃棄方法として、暗号化消去等も考えられるが、暗号化に用いた鍵の管理を確実に実施していることを確認する必要がある。そのため、利用するクラウドサービスにおいて暗号鍵の管理主体を事前に把握しておく必要がある。

鍵の管理主体

❑基本対策事項4.2.2(1)-9「暗号化に係る基本方針」について

クラウドサービスにおいて要機密情報を扱うには情報の流通経路全般において暗号化の対策が必要となるが、クラウドサービスの個々の構成要素において対策を採ることは容易ではないため、**クラウドサービス提供者が提供する暗号化機能を利用して対応することが推奨される。**暗号化の対策は7.1.5「暗号・電子署名」のオンプレミスの対応と基本的には同じであるが、鍵の管理をクラウドサービス提供者が行う場合は注意が必要である。**基本的に鍵の管理はクラウドサービス利用者側で行う必要があるが、鍵の管理をクラウドサービス提供者が提供するサービスを利用せざるを得ない場合は、詳細な情報をクラウドサービス提供者に要求し、リスク評価を行った上でクラウドサービスに情報を保存する前に機関等が用意した別暗号鍵を用いて保存するなどのリスクを低減するための措置を検討する**よう基本方針として運用規程に含めることが求められる。

❑基本対策事項4.2.2(2)-6c)「暗号化に用いる鍵の保管場所等の管理」について

基本対策事項4.2.2(1)-9a)において定めている運用規程に基づき、クラウドサービス管理者は、情報の暗号化に用いる鍵の保管場所に関するセキュリティ要件を定める必要がある。**例えば、暗号鍵の保管場所については、暗号化した情報とは別の場所で管理することや、適正なかつ透明性のある手続き（例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で暗号鍵が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場所には保管しない**などが考えられる。暗号鍵の管理については、基本対策事項7.1.5(1)-3b)「管理手順を定めること」を参照するとよい。

鍵の保管箇所

❑基本対策事項4.2.2(2)-6d)「暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理」について

基本対策事項4.2.2(1)-9c)において定めている運用規程に基づき、クラウドサービス管理者は、**情報の暗号化に用いる鍵の生成から廃棄に至るまでのライフサイクルにおける管理に関するセキュリティ要件を定める必要**がある。暗号鍵の管理は重要であり、暗号鍵の複製の可否や暗号鍵の利用者を特定するための要件なども含めると良い。暗号鍵の管理については、基本対策事項7.1.5(1)-3b)「管理手順を定めること」についてを参照するとよい。

暗号鍵管理要件

「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」

https://www.nisc.go.jp/policy/group/general/kijun.html

3.2 クラウド利用基本方針における暗号化要件

「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」では暗号鍵管理の運用方式と実装を検討の必要性を示す一方で、クラウド以外で暗号鍵管理を行う場合の運用負荷等について注意喚起しています。

❑3.6 セキュリティについて
❑7) データ保護に関する暗号化技術の利用

クラウド環境では、データを暗号化する機能を提供するサービスが充実し ており、オンプレミス環境よりも容易かつ安全に暗号化技術を利用することができる。データの機密性や想定される脅威に応じて、通信中のデータや保管されているデータを暗号化することを検討する必要がある。暗号化を行う際には、「電子政府推奨暗号リスト」に基づいた暗号アルゴリズムを選択し、適切な方法で暗号鍵を管理する必要がある。

クラウドでは暗号鍵管理をクラウドの利用者が自ら実施できることを考慮し、取り扱うデータに求められるセキュリティ要件に基づいて運用方式と実装を検討する。例えば、クラウドの暗号鍵管理サービスの提供する利用者が主体的に管理可能な暗号鍵では、アクセス権の設定を含む鍵のライフサイクルを管理する。

「BYOK(Bring Your Own Key)」と呼ばれる方式では、利用者自身が作成した暗号鍵をクラウド環境に持ち込み、クラウドサービス事業者が提供する鍵管理サービスを利用して、その暗号鍵を管理し暗号化処理を行う。また、HYOK(Hold Your Own Key)と呼ばれる方式では、利用者が保有する鍵管理システム上で保管・管理されている暗号鍵をクラウドサービス事業者のサービスから利用して暗号化処理を行う。いずれの場合も、**利用者自身がクラウド以外で暗号鍵を作成・保管・管理する場合は、サービスに組み込まれた標準的な方法を利用する場合と比べて運用負荷や処理の複雑さが大幅に増すため、導入前に十分な検討が必要となる。**

暗号鍵の管理主体

クラウド以外の暗号鍵管理の運用負荷と処理の複雑さ

DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf

3.3 地方公共団体に求められる暗号化要件

地方公共団体において参照されている総務省のガイドラインや基幹業務システムの標準非機能要件における暗号化要件は以下のとおりです。

❑総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」(令和6年10月版)

（１６）電子署名・暗号化
①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密 性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、パス ワード等による暗号化等、セキュリティを考慮して、送信しなければならない。
②職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。 また、CISO が定めた方法で暗号のための鍵を管理しなければならない。
③CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全 に提供しなければならない。

①（オ）統括情報セキュリティ責任者は、運用・保守時における暗号化に係る規定を策定する場合、以下を含む内容を規定すること。
・暗号化に用いる鍵の管理者と鍵の保管場所

（イ）**鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価 ・鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価**

暗号鍵の管理

❑「地方公共団体の基幹業務システムの標準非機能要件」(令和4年8月)

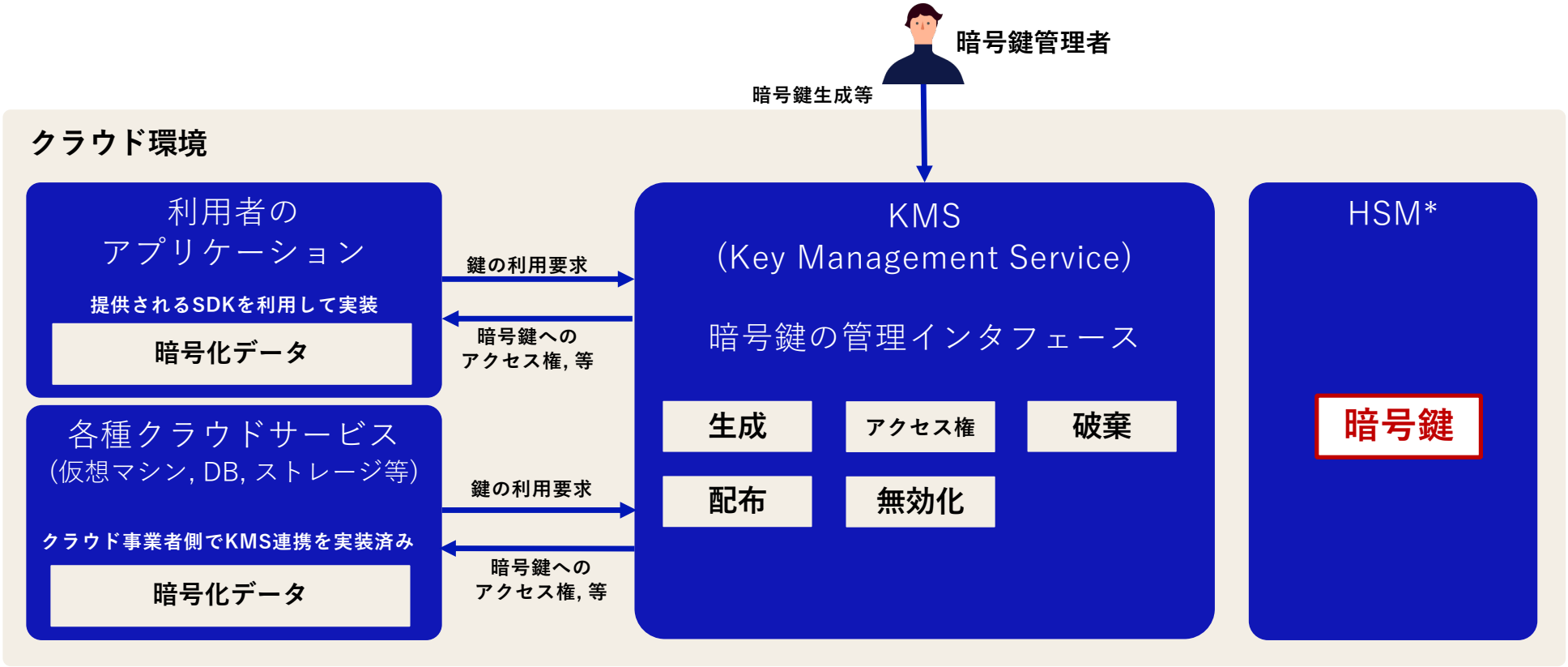
6.1.2 セキュリティ データの秘匿
蓄積データの暗号化の有無
ファイル・フォルダを暗号化するソフトウェア や、データベースソフトウェアの暗号化機能を使用して暗号化を行う。
選択レベル: 1（一般的な選択基準）
（補足2参照）
選択時の条件
蓄積するパスワード等については 第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合、又は、**クラウドサービスの仕様により暗号化消去 を行う場合**（後者については選択レベルを2上げる）

暗号化消去

4. ガバメントクラウドの技術要件

4.1 暗号化及び暗号鍵管理を効率的に行えるクラウド環境

主要なクラウド事業者の提供するクラウド環境では暗号鍵管理サービスが提供されています。通常、暗号鍵管理サービスと各クラウドサービスは連携され、サーバーやストレージのデータを容易に暗号化可能です。



*HSM: Hardware Security Module

4.2 ガバメントクラウドのクラウドサービス調達時の暗号化に関する技術要件

ガバメントクラウドでは暗号化に関する利用者の要件を満たせるよう、クラウドサービスの調達時に以下の要件*を提示し、契約しています。

❑統制	
環境一式に保管される業務データはユーザが所有権を持ち、ユーザが指定した場所に保管され、ユーザの許可なしに他所に移転・複写したりしないこと。ユーザ所有の暗号鍵で暗号化して保護できること。（以下、略）	暗号鍵管理主体
❑暗号鍵管理	
サーバやDB、ストレージで使用される暗号鍵は、FIPS 140-2等で認証された厳格に管理された鍵管理サービスで管理されること。	FIPS認証
利用者が独自に生成した暗号鍵を利用者自らが当該サービスにインポートできること（BYOK）。	BYOK
❑各サービス	
クラウド利用者からは完全に分離し暗号化された仮想マシンでデータの暗号化/復号が行えるサービスまたはサポートが提供されていること。	KMSとの連携
オブジェクトストレージは、BYOKを含む鍵管理サービスを使ってユーザ鍵で暗号化できること。	
ブロックストレージは、BYOKを含む鍵管理サービスを使ってユーザ鍵で暗号化できること。	
アーカイブストレージは、BYOKを含む鍵管理サービスを使ってユーザ鍵で暗号化できること。	
DBに保管するデータは、BYOKを含む鍵管理サービスを使ってユーザ鍵で透過的に暗号化できること。	

*要件は技術動向等に合わせて見直しが行われます

4.2 ガバメントクラウドのクラウドサービス調達時の暗号化に関する技術要件

ガバメントクラウドでは暗号化に関する利用者の要件を満たせるよう、クラウドサービスの調達時に以下の要件*を提示し、契約しています。

❑暗号鍵管理サービス		
1	暗号鍵の生成、利用、ローテーション、破棄等の一般的に暗号鍵の管理に必要となる管理機能が利用可能であり、FIPS 140-2 レベル1に準拠していること。	FIPS認証
2	暗号鍵に関しては利用者が生成した暗号鍵を持ち込めるBYOK(Bring Your Own key)が可能であること。	BYOK
3	クラウド環境で利用するストレージやデータベースのデータの暗号化についてBYOKで持ち込んだ暗号鍵を指定して即座に利用可能であること。	
4	FIPS 140-2のレベル3認証済みのHSMと連携し、HSMから暗号鍵を取り込んで利用可能であること。	HSM連携
5	暗号鍵サービスの動作やオペレーションに関してはセキュリティ上の監査に利用可能な詳細ログを出力可能であること。	ログ
6	暗号鍵サービスに格納された暗号鍵はSDKを介して利用でき、利用者独自のアプリケーションにもSDKを介して暗号鍵サービスの機能を実装し利用可能であること。	SDK
❑HSMサービス		
7	HSMの物理的な設置、ソフトウェアへのパッチ適用、可用性・クラスタ構成等、物理（低）レイヤーに近いHSMの管理タスクについては、クラウドサービス側が利用者の要求によって管理し、暗号鍵そのものに係るHSMの高レイヤーの操作（暗号鍵の生成、破棄等）については利用者に完全な統制権が提供され、利用者の任意のタイミングで操作が即座に可能であること。	HSM運用責任分界
8	FIPS 140-2 のレベル3認証済みのHSMを、利用者が占有するHSMサービスとして提供可能であること。	FIPS認証
9	以下の暗号鍵の作成、利用、暗号鍵のローテーション、および破棄が可能であること。 対称暗号鍵：AES256、非対称暗号鍵：RSA 2048、RSA 3072、RSA 4096、ECC P256、ECC P384	暗号アルゴリズム
10	HSMの可用性を確保するためにクラスターを構成して提供可能であること。	HSM可用性

*要件は技術動向等に合わせて見直しが行われます

5. 鍵管理の留意事項とガバメントクラウド

5.1 暗号鍵管理の留意事項とガバメントクラウド利用の前提

暗号鍵管理の要件への対応を進める際には、以下に挙げる留意事項と前提があります。

	留意事項	ガバメントクラウド利用の前提 （後述）
暗号鍵の管理主体	暗号鍵の管理主体によっては 各種要件への対応が困難	暗号鍵の作成や廃棄等の運用は 利用者の責任範囲* （運用管理組織では一元管理はしない）
暗号鍵管理の実装方式	実装方式によっては 構築・運用負荷が増大	暗号鍵の保管・利用に関する実装は 利用者の責任範囲*、 CSPマネージドサービスの利用を推奨 （共通の鍵管理基盤は提供していない）

*取り扱うデータの規制要件や利用組織の定めるポリシーに準拠することを想定

5.2 暗号鍵管理の主体とガバメントクラウドにおける推奨

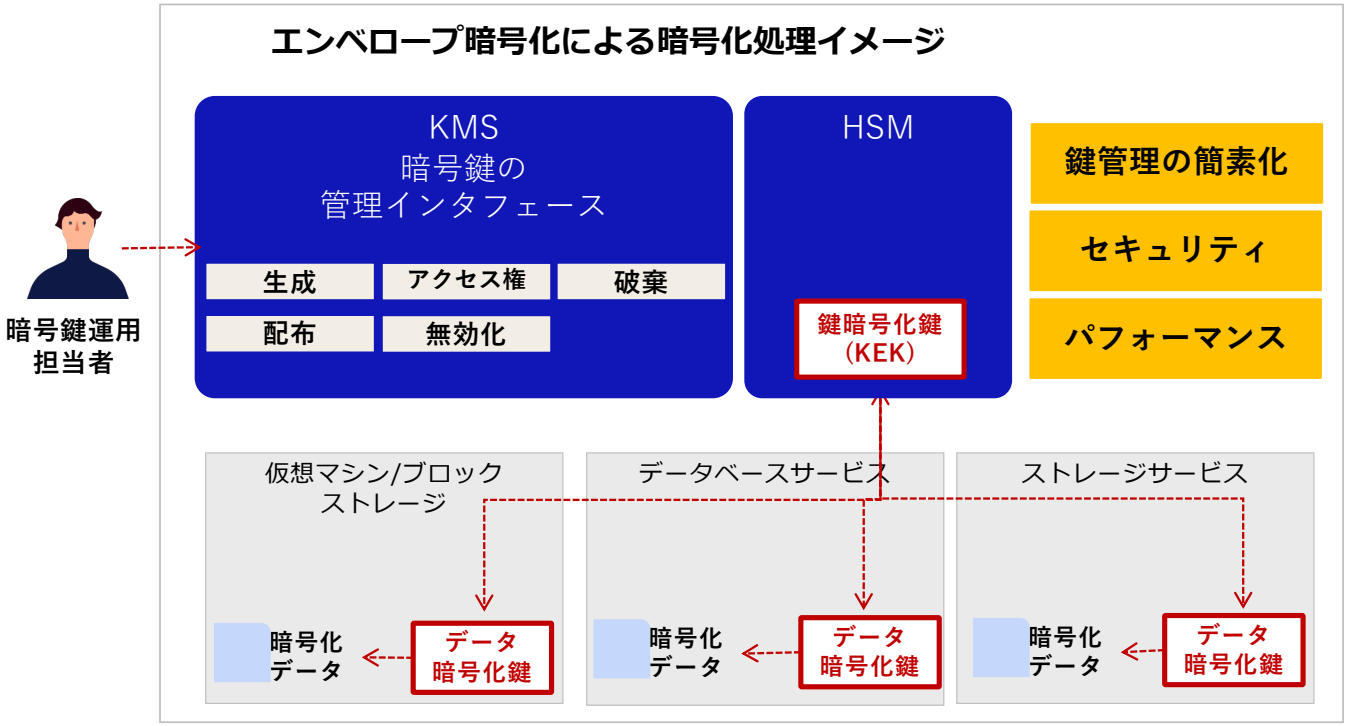
暗号鍵の管理主体によって特徴が異なります。ガバメントクラウドの各クラウド環境では、暗号鍵管理の主体を選択可能です。ガバメントクラウドではクラウド利用者による鍵管理を推奨しています。

	クラウド事業者が管理する鍵	クラウドの利用者が管理する鍵
名称例	(CSP) マネージドキー	CMK(カスタマーマネージドキー)*
利用例	• CSP側でデフォルトで行う暗号化 • KMSによる暗号鍵作成時（指定）	• KMSにて暗号鍵作成時（指定） • BYOK(後述)
メリット	• 鍵の管理不要	• 鍵へのアクセス権管理可能 • 鍵へのアクセスログの取得可能 • 鍵の明示的な利用停止、削除可能
デメリット	• 鍵の主体的かつ明示的な管理不可 • 鍵へのアクセスログ取得不可 利用者の指示による暗号化消去不可	鍵の管理負荷発生
ガバメントクラウドにおける推奨	非推奨	推奨

CMK: Customer Managed Key

5.3 2種類の暗号鍵 - エンベロープ暗号化

クラウド環境におけるデータの暗号化では主に2種類の鍵が用いられます。暗号鍵の管理主体以外にこれらの鍵をどこで保管して利用するかという実装方式が鍵管理の構築・運用負荷に影響します。



鍵暗号化鍵
(KEK: Key Encryption Key)

データを暗号化するために使われる「データ暗号化(DEK)」の暗号化/復号に使用

データ暗号化鍵
(DEK: Data Encryption Key)

データを暗号化するために使用される暗号鍵

(暗号化されて保管, 平文はすぐに削除)

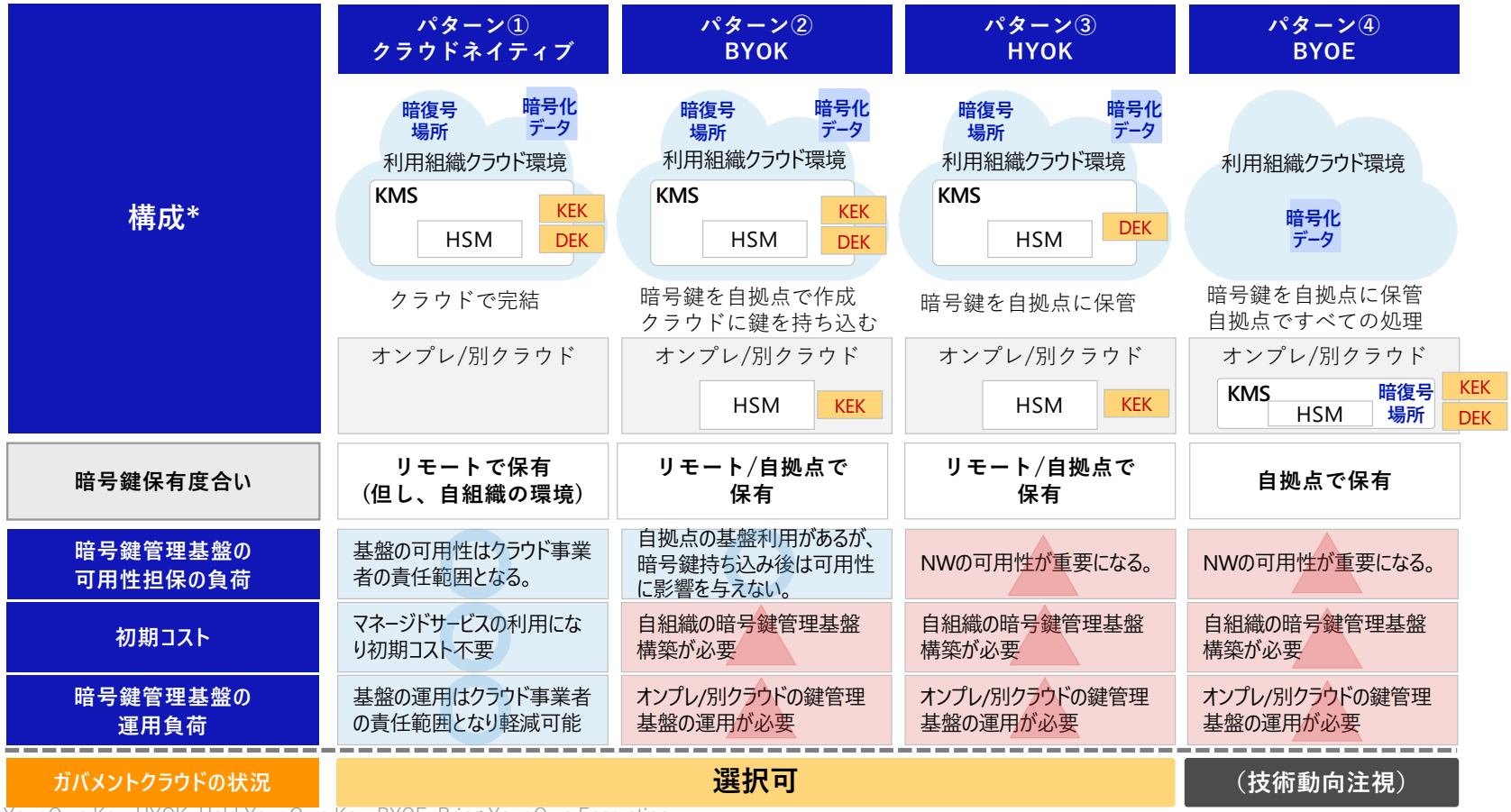
5.4 暗号鍵管理の実装方式の概要

暗号鍵管理方式は、暗号鍵の保有度合い（生成場所・保管場所、暗復号場所）によって主に次の種類に分けられます。

*BYOK: Bring Your Own Key, HYOK: Hold Your Own Key, BYOE: Bring Your Own Encryption

5.4 暗号鍵管理の実装方式の特徴

暗号鍵管理の方式ごとに構築・運用負荷が異なります。ガバメントクラウドでは実装方式は利用者選択になります。



*BYOK: Bring Your Own Key, HYOK: Hold Your Own Key, BYOE: Bring Your Own Encryption
BYOKは、オンプレミス環境の暗号鍵の継続利用や暗号鍵を利用するクラウド環境以外の自組織の環境にも暗号鍵を保有するなどの利用組織のポリシーに応じた利用をユースケースとして想定

5.5 ガバメントクラウドの事業者内に保管する暗号鍵の保護

ガバメントクラウドのクラウド事業者における暗号鍵の保護については、クラウドサービス調達時における以下の技術要件の提示により対応を求めています。

クラウド事業者

FIPS 認証済のKMS, HSMの提供

米国国立標準技術研究所（NIST）が暗号モジュールのセキュリティ要件を定めた規格

例「FIPS 140-2* のレベル3認証済みのHSMを、利用者が占有するHSMサービスとして提供可能であること」（技術要件）

政府情報システムのためのセキュリティ評価制度（ISMAP）認証取得

「ISMAP制度の認証（監査終了）を「機能等証明明細書」提出時点までに取得していること」（技術要件）

第三者監査レポートの提示

「AICPA SOC2又は日本公認会計士協会が定める同等の監査フレームワークに対応し、第三者監査人の監査を受け実施されている旨の証明の提出ができること」等(技術要件)

**ガバメントクラウドの技術要件を上回る暗号鍵の保護要件がある場合には、
取り扱うデータの性質や規制を考慮し、
暗号鍵の管理方式を検討し、独自のプラットフォームを調達する必要がある**

*FIPS 140-2の後継規格としてFIPS 140-3が策定済み

まとめ

まとめ – ガバメントクラウドにおける暗号鍵管理

本講演では、ガバメントクラウドにおける暗号鍵管理について、以下のポイントでご紹介しました。

ガバメントクラウドでは
暗号化関連の
技術要件を提示

利用組織は各種規制/
ガイドラインに準拠し
暗号化要件を定義

暗号鍵の管理に関する
実装は利用組織の責任範囲

ガバメントクラウドでは
利用者の主体的な
暗号鍵管理を推奨

暗号鍵管理方式は
各種要件を踏まえ
構築/運用負荷を考慮し選択

暗号関連の設定に関する
発見的統制

ガバメントクラウドにおける暗号鍵管理の今後の取り組み

暗号鍵管理において現在、検討しているテーマは次のとおりです。引き続き、今後の技術動向を踏まえてガバメントクラウドにおける暗号鍵管理の推奨事項を充実し、利用システムの安全性向上への寄与を目指します。

BYOK用HSM基盤の構築効率化	発見的統制機能の拡充	暗号鍵管理の運用ガイド
BYOK利用を選択する際のHSM基盤構築を効率化するサンプルIaCファイル、運用設計ガイドの提供を検討	暗号鍵の利用状況の確認を効率化する機能の実装を検討	暗号鍵管理の運用は学習コストが高いため、利用ガイドの拡充を検討

デジタル庁

Digital Agency