電子入札コアシステムにおける最近の取り組み

システムエンジニアリング部
遠藤　卓也

2023/11/8

本日の話題

- 電子入札コアシステムと各種取り組みのための検討体制

- 政府等の動向とコアシステムの取り組み
  - ・社会全体のデジタル化の推進
  - ・暗号強度要件の変更

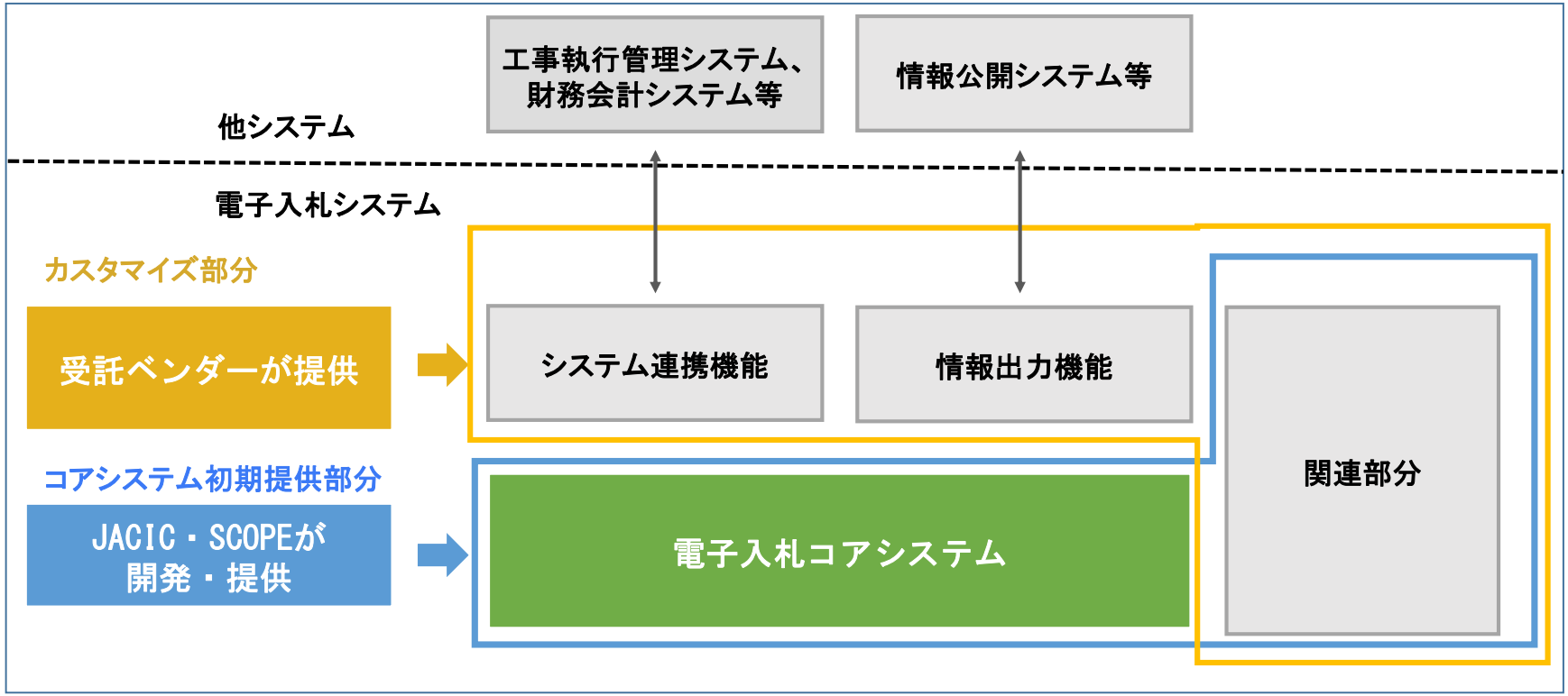
電子入札コアシステムと各種取り組みのための検討体制

JACIC 一般財団法人 日本建設情報総合センター

・電子入札コアシステムとは

国土交通省の電子入札システムをベースとして、基本となる汎用性の高い機能（認証・署名、案件の管理等）を搭載したパッケージソフトウェア。

発注機関毎に環境構築・独自のカスタマイズ（機能拡張や他システムとの連携等）を行うことで電子入札システムの構築が可能。



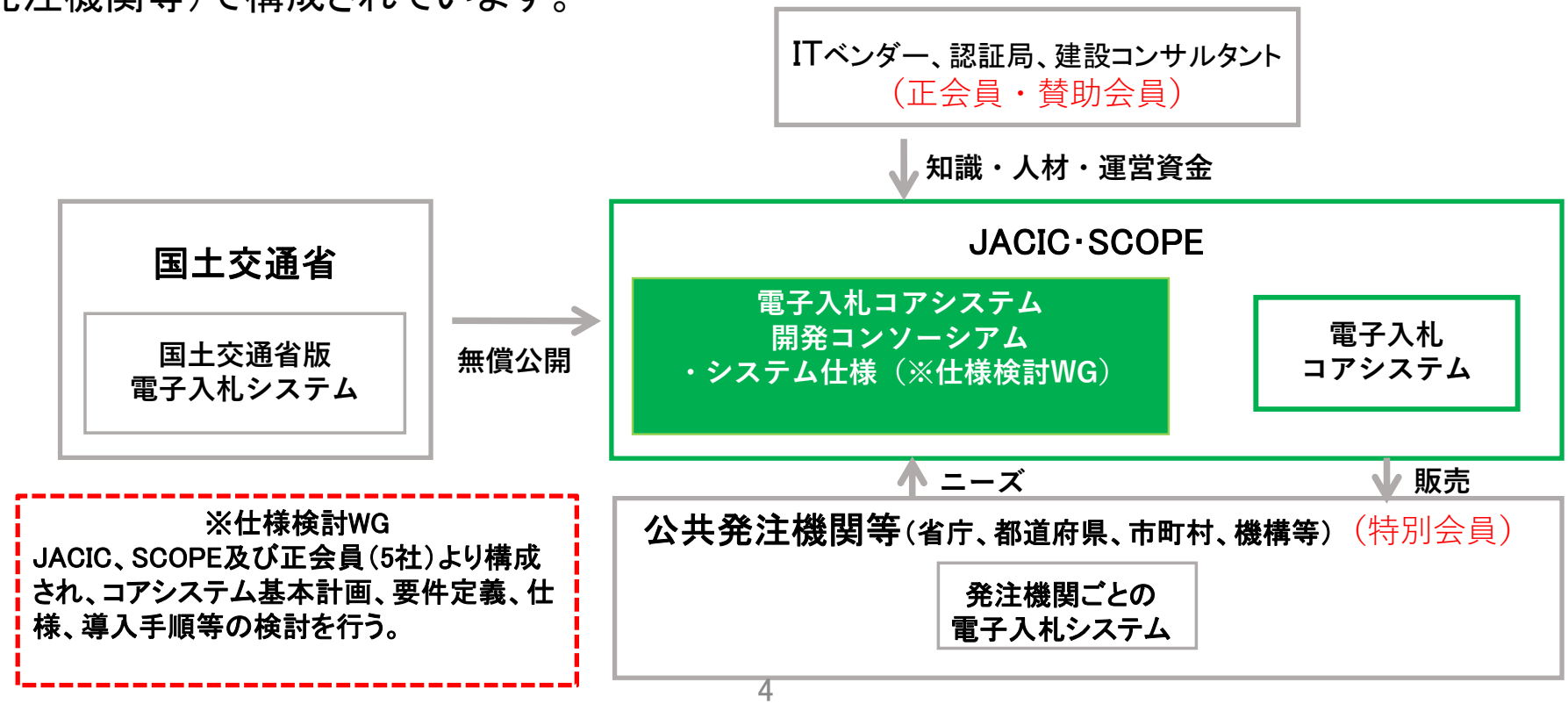
SCOPE ：一般財団法人　港湾空港総合技術センター

電子入札コアシステムと各種取り組みのための検討体制

JACIC 一般財団法人 日本建設情報総合センター

・電子入札コアシステム開発コンソーシアムについて

電子入札コアシステムの開発・運用支援のためにコンソーシアムを平成13年7月に設立、コンソーシアムは開発および改良するための仕様検討、開発および改良成果の検証並びに運用支援に関する検討を行うために正会員（電子入札システムの開発意欲を有するITベンダー）、賛助会員（ITベンダー、認証局、建設コンサルタント）および特別会員（電子入札を導入（予定を含む）府省、独法等、地方公共団体などの公共発注機関等）で構成されています。



電子入札コアシステムと各種取り組みのための検討体制

JACIC 一般財団法人 日本建設情報総合センター

・コンソーシアムの取り組み

平成13年7月　電子入札コアシステム開発コンソーシアム設立

（平成13年10月　国土交通省　電子入札運用開始）

（平成13年11月　国土交通省による電子入札システムの無償公開）

■平成14年6月　電子入札コアシステム Ver.1 提供

（平成15年度　国土交通省　直轄事業（工事・業務）対象に電子入札全面実施）

・

・

・

■令和元年11月　クライアント側でJREを利用しない方式の電子入札コアシステムを提供

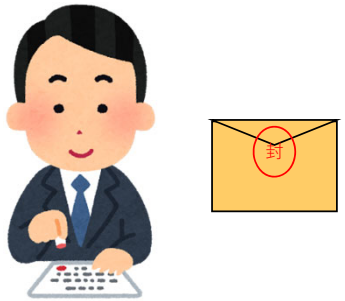
■令和3年4月　複数ブラウザ対応モジュール 提供

電子入札コアシステムと各種取り組みのための検討体制

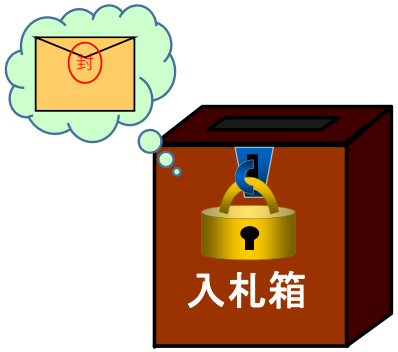
JACIC 一般財団法人 日本建設情報総合センター

・紙入札と電子入札の違い（イメージ）

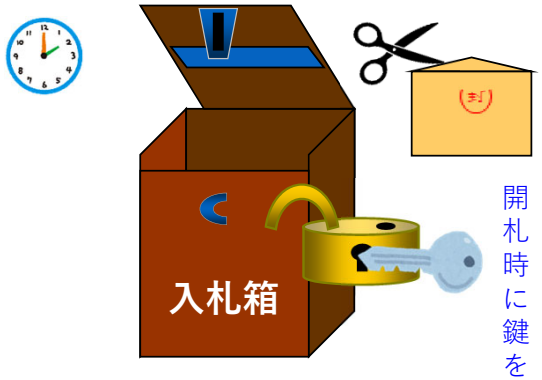
紙入札の場合



入札書の準備

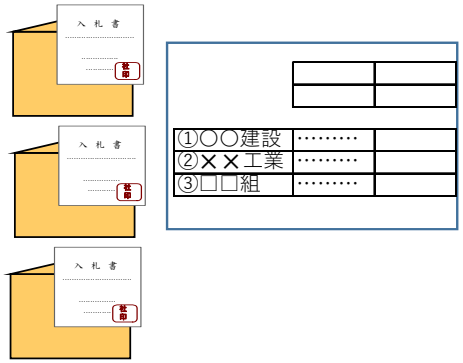


入札書の投函



開札時に鍵を取り出し

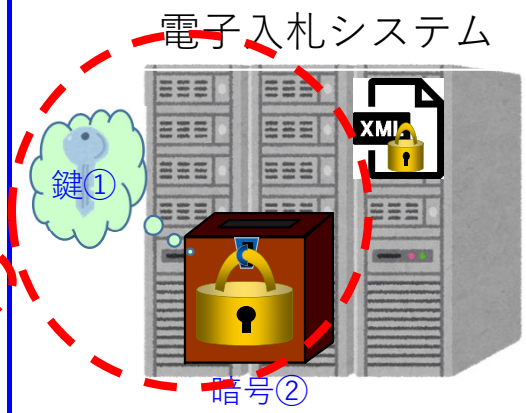
開札



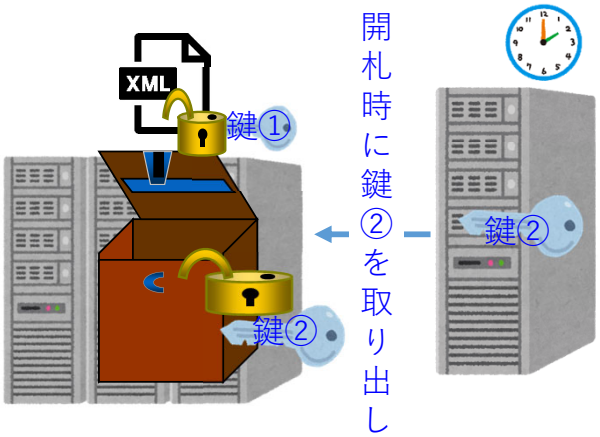
落札業者決定

電子入札の場合

入札データの暗号化



入札書の受付



開札時に鍵②を取り出し

開札（復号）

落札業者決定

政府等の動向とコアシステムの取り組み

①社会全体のデジタル化の推進
デジタル社会の実現に向けた重点計画（R5.6.9　閣議決定）

第１ 安全・安心で便利な国民の生活や事業者の活動に向けた重点的な取組
　３．国・地方公共団体を通じたDXの推進
　（７）国・地方公共団体のガバメントクラウド移行
　　2023年度（令和５年度）は、2022年度（令和４年度）に引き続き、地方公共団体による先行事業等の整備を実施するともに、各府省庁や地方公共団体の情報システムについて、業務の見直し及び費用削減の努力を徹底した上でのガバメントクラウドへの移行を進めるほか、ガバメントクラウドテンプレートや各府省庁向け利用ガイド等の整備、クラウド移行支援体制の整備等を実施する。

第２ 重点計画の基本的考え方
　２．デジタル社会の実現に向けての理念・原則
　（４）クラウド・バイ・デフォルト原則
　　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・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とともに、共通的に必要とされる機能は共通部品として共用できるよう、機能ごとに細分化された部品を組み合わせて適正（スマート）に利用する設計思想に基づいた整備を推進する。

「デジタル社会の実現に向けた重点計画」（2023年6月9日　閣議決定）より抜粋

政府等の動向とコアシステムの取り組み

①社会全体のデジタル化の推進
デジタル社会推進標準ガイドライン　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
（R4.12.28デジタル社会推進会議幹事会決定）

２　基本方針

２.１　クラウド・バイ・デフォルト原則

政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、クラウドサービスの利用を第一候補として、その検討を行うものとする。その際、「３　具体方針」に基づき、単にクラウドを利用するのではなく、クラウドをスマートに利用するよう検討するものとする。

２.２　モダン技術の利用

クラウドをスマートに利用するためには、アプリケーションのモダン化が必要となる。新規システムについては当初から、移行システムについてはアプリケーションのライフサイクルにおける刷新タイミングにおいて、「３.５アプリケーションとシステム刷新について」に基づき、アプリケーションのモダン化を検討するものとする。

「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」
（2022年12月28日 デジタル社会推進会議幹事会決定）より抜粋

政府等の動向とコアシステムの取り組み

①社会全体のデジタル化の推進
コアシステムの現在の取り組み

現行のコアシステム設計思想

- オンプレミス環境での利用を前提
- サーバOSに依存しない汎用性の高いシステム
- カスタマイズが容易なシステム

主な課題：開発から20年が経過しコアシステムがクラウド環境に最適化していない

取り組み：仕様検討WGにおいて以下を議題に検討中

- クラウドサービスでの利用を想定したコアシステムの検討
  - ・DB構造やフレームワークを含めた旧技術に関する見直し
  - ・メールの送信・データベース等のマネージドサービスの適応性

②暗号強度要件の変更

政府機関等のサイバーセキュリティ対策のための統一規範（R3.7.7　サイバーセキュリティ戦略本部決定）

（暗号・電子署名）

第二十条

　機関等は、自組織における暗号・電子署名の利用について、必要な措置を定め、実施しなければならない。

政府機関等のサイバーセキュリティ対策のための統一規範（R5.7.4　サイバーセキュリティ戦略本部決定）

（暗号・電子署名）

記載なし

（統一基準への委任）

第二十三条

　本規範に定めるもののほか、本規範の実施のため必要な要件は、統一基準で定める。

「政府機関等のサイバーセキュリティ対策のための統一規範 」（令和３年７月７日　サイバーセキュリティ戦略本部決定）及び
「政府機関等のサイバーセキュリティ対策のための統一規範 」（令和５年７月４日　サイバーセキュリティ戦略本部決定）より抜粋

②暗号強度要件の変更

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（令和5年度版）（R5.7.4　サイバーセキュリティ戦略本部）

7.1.5 暗号・電子署名

遵守事項

(1) 暗号化機能・電子署名機能の導入

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

「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 （令和５年度版）」
（令和５年７月４日　サイバーセキュリティ戦略本部）より抜粋

②暗号強度要件の変更

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

（2022.3　デジタル庁・総務省・経済産業省）

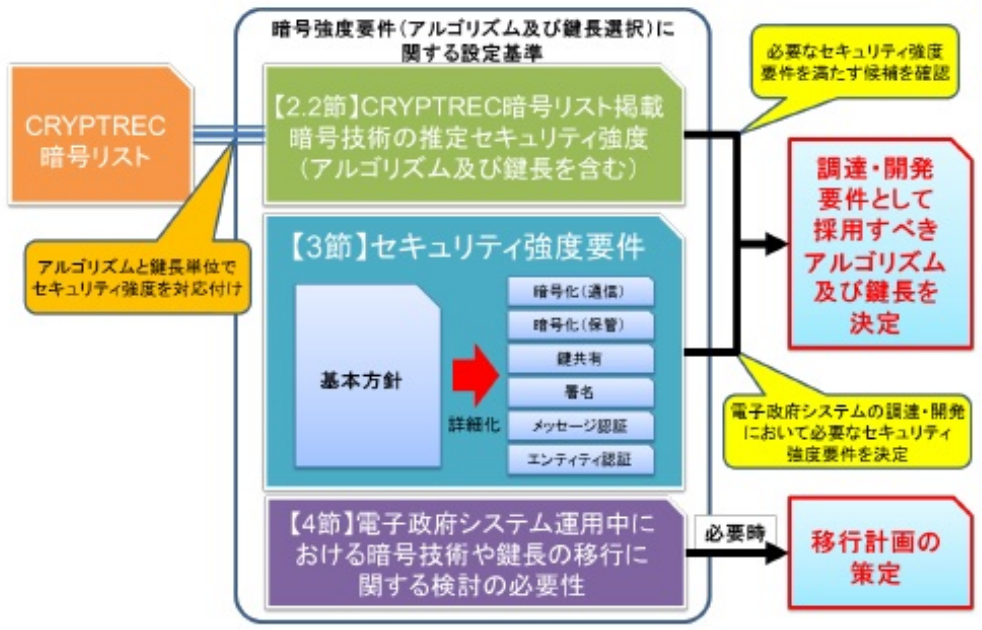


図 1　CRYPTREC 暗号リストと本書の関係

1.はじめに

本書は、CRYPTREC暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定したものであり、CRYPTREC暗号リストとの関係を図 1に示す。

したがって、利用する鍵長について、本書の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

「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」
（2022年３月 （Ver1.0）デジタル庁　総務省　経済産業省）より抜粋

②暗号強度要件の変更

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

（2022.3　デジタル庁・総務省・経済産業省）

表 5　セキュリティ強度要件の基本設定方針

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビット セキュリティ	新規生成 ((a)参照)	移行完遂期間 ((c)参照)	利用不可			
	処理 ((b)参照)		許容			
128 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	期間 ((c)参照)		利用不可
	処理 ((b)参照)				許容	
192 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					
256 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					

2031年以降は、新規生成が「利用不可」となるため事前の対応完了が必要

セキュリティ強度要件の基本設定方針（抜粋）

電子政府システムの調達・開発にあたっての基本方針として、3.1節の考え方に基づき、最低限のセキュリティ強度要件を以下の方針で設定し、その強度要件を満たすアルゴリズム及び鍵長を選択（3.3節参照）することを調達・開発要件としなければならない。

なお、本書では、標準文書保存期間基準[12]を参考に、最長想定運用終了・廃棄年を2070年（本書発行後、約50年間）とした。

[12] https://www.kantei.go.jp/jp/singi/genshiryoku_bousai/pdf/hozonhyou.pdf
「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」
（2022年３月（Ver1.0）デジタル庁　総務省　経済産業省）より抜粋

②暗号強度要件の変更

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）（R5.3.30　デジタル庁・総務省・経済産業省）

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP（注１）
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注12)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)

技術分類		暗号技術
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS(注17)
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

（注１）「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びSA1024に係る移行指針」（平成20年４月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）　を踏まえて利用すること。
https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf
（平成25年３月１日現在）

（注２）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注４）初期化ベクトル長は96ビットを推奨する。

（注12）ハッシュ長は256ビット以上とすること。

（注13）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注17）ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」
（令和5年3月30日　デジタル庁・総務省・経済産業省）より抜粋

②暗号強度要件の変更
コアシステムの取り組み

課　　題：コアシステムが利用している暗号アルゴリズムの今後の危殆化が想定されるため暗号アルゴリズムの見直しが必要

取り組み：ICカードの提供者として、暗号強度要件の変更の影響があるコアシステム対応認証局との関係者会議において以下を議題に検討中

- 認証局が採用するICカードの暗号アルゴリズムの動向を踏まえた検討（P6暗号①）
  - ・コアシステムで実装が可能なアルゴリズムであるか及びその実装方法
- 入札書の保管及び開札のために利用する暗号アルゴリズムの検討（P6暗号②）
  - ・コアシステムで実装が可能なアルゴリズムであるか及びその実装方法
  - ・暗号アルゴリズムの変更に伴う影響（処理速度への影響や開発工数等）

より利便性の高いサービスの提供を目指していきます

ご清聴いただきありがとうございます