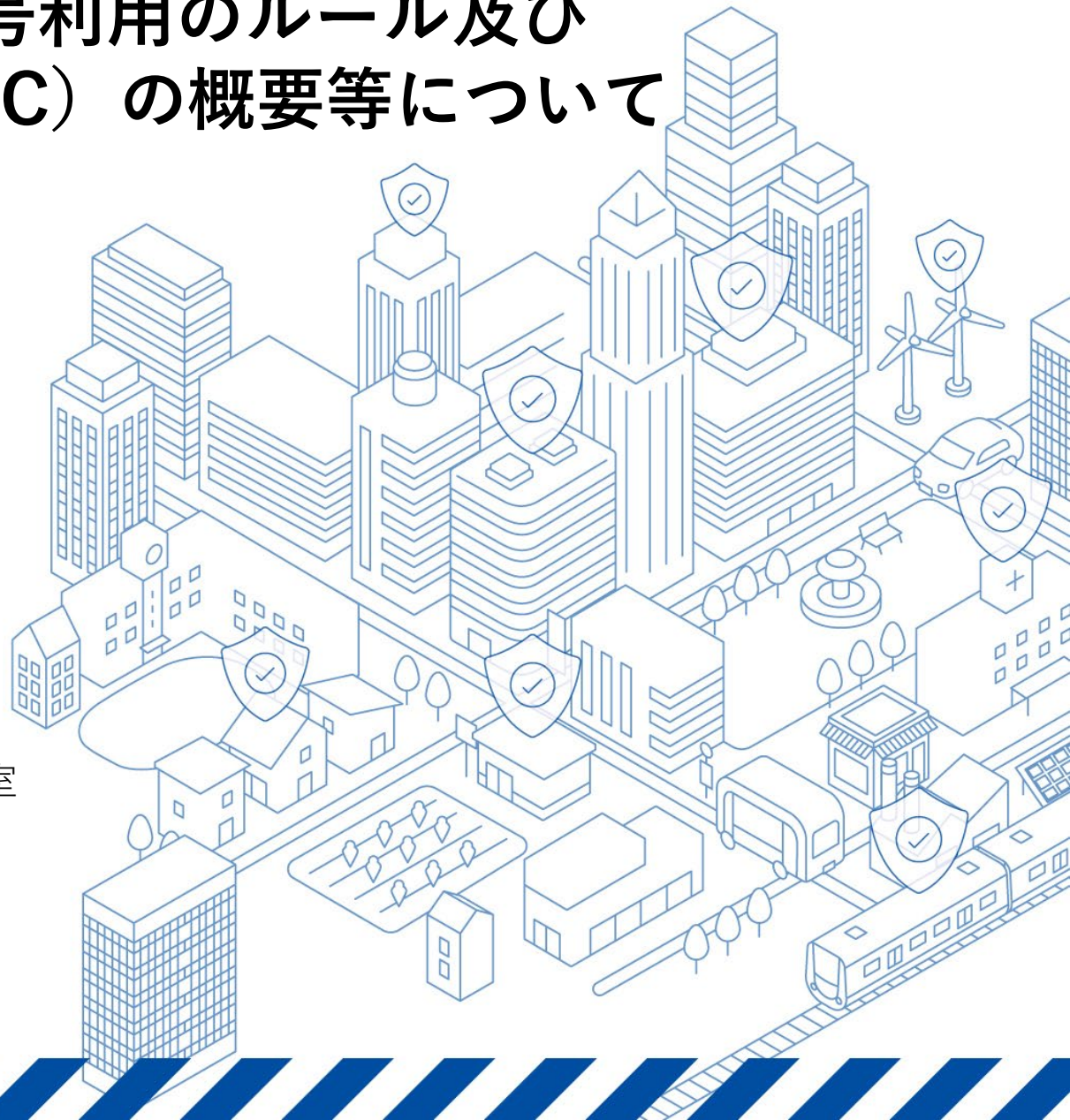
政府機関等における暗号利用のルール及び耐量子計算機暗号（PQC）の概要等について



令和７年７月31日　国家サイバー統括室

1　政府機関等における暗号利用のルールについて

政府機関等は、政府統一基準において**「暗号技術検討会及びその関連委員会(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、使用する暗号等を定める**こととされている。

＜政府機関等におけるサイバーセキュリティ対策について＞

- ✓ 政府機関等におけるサイバーセキュリティ対策の水準の維持・向上のため、サイバーセキュリティ基本法に基づき、**「政府機関等のサイバーセキュリティ対策のための政府統一基準」（令和７年６月サイバーセキュリティ戦略本部決定）を策定**。
- ✓ 政府統一基準では、政府機関等が講ずるべき**情報セキュリティ対策のベースラインを定めており、政府機関等においては政府統一基準に準拠しつつ**、組織及び取り扱う情報の特性等を踏まえ**各組織の情報セキュリティポリシーを策定**。

○　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）
①電子政府推奨暗号リスト、②推奨候補暗号リスト、③運用監視暗号リストの３つのリストで構成

②推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。

次の条件のいずれかを満たすと暗号技術検討会が決定した場合
1．５年ごとの利用実績調査により、複数の利用実績を確認した場合
2．その他、普及していることが明らか又は急速な普及が大いに見込まれる場合

①電子政府推奨暗号リスト

CRYPTRECにより安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

安全性維持が困難（危殆化した）と暗号技術検討会が決定した場合

③運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。

※暗号技術検討会及び関連委員会（CRYPTREC）　暗号技術に関する専門家の会合。デジタル庁・総務省・経産省が共同で事務局を運営。

2　耐量子計算機暗号（PQC）の概要について

■ 現在の公開鍵暗号（RSAや楕円曲線暗号等）は、素因数分解問題や離散対数問題といった、従来型の電子計算機では解読に膨大な時間がかかる数学的困難性を利用している。
■ ソフトウェアを含めた量子計算機技術の進展に伴い、将来的にショアのアルゴリズムのような公開鍵暗号を解読する量子アルゴリズムを量子計算機で実行することにより、現在広く用いられている公開鍵暗号を効率的に解読できるとされている。
■ 耐量子計算機暗号（PQC（Post-Quantum Cryptography））とは、量子計算機及び従来型の電子計算機の双方に対して安全性が確保される暗号のことである。量子計算機でも解読が困難な数学的問題（格子問題、符号理論、多変数多項式、ハッシュ関数ベースなど）を利用することで、量子計算機による攻撃に耐性を持つとされている。

【耐量子計算機暗号（PQC）の例（米国NISTによる標準化 2025年７月時点）】

FIPS	名称	方式	分類
FIPS　203	CRYSTALS-Kyber(ML-KEM)	格子問題	鍵共有
FIPS　204	CRYSTALS-Dilithium(ML-DSA)	格子問題	署名
FIPS　205	Sphincs+(SLH-DSA)	ハッシュ関数	
FIPS　206(予定)	FALCON（FN-DSA）	格子問題	

※FIPS：Federal Information Processing Standards（連邦情報処理標準）の略。国立標準技術研究所（National Institute of Standards and Technology（NIST））が公表している米国連邦政府が定める情報処理及びセキュリティの標準規格。

【公開鍵暗号の例（CRYPTREC電子政府推奨暗号リスト）】

技術分類	暗号技術
署名	DSA
	ECDSA
	EdDSA
	RSA-PSS
	RSASSA-PKCS1-v1_5
守秘	RSA-OAEP
鍵共有	DH
	ECDH

3　耐量子計算機暗号（PQC）の移行に係る背景等について

■ 量子計算機技術の進展に伴い、従来型の電子計算機に対して安全性を有している公開鍵暗号について、将来的な安全性の低下（危殆化）の懸念。

■ 米国をはじめ、欧州（EU）などの諸外国においても、量子計算機に耐性を持つ耐量子計算機暗号（PQC）への移行に向けて、ロードマップやタイムラインを公表。

■ 我が国においては、2025年３月の暗号技術検討会（CRYPTREC）を受けて、耐量子計算機暗号（PQC）について、技術的な安全性等の評価に向けた検討が開始。

■ 耐量子計算機暗号（PQC）への移行については、サイバーセキュリティ確保のほか、産業政策、安全保障、サービスの安定供給、国際連携・標準化の観点等の多岐にわたる課題があり、広範囲の検討が必要。

■ これらの状況を踏まえ、「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」が設置され、第１回の会議を開催。

4①　耐量子計算機暗号（PQC）の移行について（検討すべき論点）

1．量子計算機の開発・普及状況及びそれに伴い危殆化する公開鍵暗号等の特定とその時期について

2．諸外国の動向の把握について

3．耐量子計算機暗号（PQC）の安全性等の評価・確認とその時期について

4．耐量子計算機暗号（PQC）への移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期について

5．政府機関等の移行への対応に必要な支援策等について

6．政府機関等の移行に向けた工程表（ロードマップ）の策定について

7．その他

※出典：第１回政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（令和７年６月30日）資料より

4②　耐量子計算機暗号（PQC）の移行について（検討スケジュール（案））

令和７年６月30日　　第１回　関係府省庁連絡会議

令和７年７月31日　　第１回　幹事会
（議事内容）検討すべき論点について

令和７年８月　　第２回　幹事会
（議事内容（案））有識者からのヒアリング

令和７年９月　　第３回　幹事会
（議事内容（案））工程表（ロードマップ）の骨子（案）について

令和７年10月～11月　　第４回　幹事会
（議事内容（案））工程表（ロードマップ）の骨子（案）とりまとめ

令和７年10月～11月　第２回　関係府省庁連絡会議
（議事内容（案））工程表（ロードマップ）の骨子のとりまとめ

令和８年度中　　第３回　関係府省庁連絡会議
（議事内容（案））工程表（ロードマップ）の策定について

（参考１）政府統一基準における暗号利用に関する記載

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７年度版）＜抜粋＞

7.1.5 暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用する暗号アルゴリズム及び鍵長に加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズム又は鍵長が危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

(1)暗号化機能・電子署名機能の導入

(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。

一 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

二 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

(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。

(c) 情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム、鍵長及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な**公的な公開鍵基盤が存在する場合はそれを使用する**など、目的に応じた適切な公開鍵基盤を使用するように定めること。

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）＜抜粋＞

【 基本対策事項 】

＜7.1.5(1)(b)関連＞

7.1.5(1)-2 情報システムセキュリティ責任者は、職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合において、情報システムで使用する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、「電子政府推奨暗号リスト」に基づき定めること。

7.1.5(1)-3 情報システムセキュリティ責任者は、基本対策事項7.1.5(1)-2で定めた事項の運用方法について、以下を全て含めて実施手順として定めること。

a) 暗号化及び電子署名に使用する**アルゴリズム又は鍵長が危殆化**した場合又はそれらを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

b) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、**管理手順を定めること**。

（解説）

遵守事項7.1.5(1)(b)「「電子政府推奨暗号リスト」に基づき」について

職員等が暗号や電子署名を利用する場合、あるいは情報システムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合においては、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長を定めることが原則である。

しかし、職員等が利用するソフトウェアや連携する他の情報システム側が「電子政府推奨暗号リスト」に記載されたアルゴリズム又は鍵長に対応していない等の場合は、利用実績が不十分であること、また、今後の普及が見込めない可能性があることによる影響を踏まえた上で、「推奨候補暗号リスト」に記載されたアルゴリズム及び鍵長を利用するとよい。

なお、「運用監視暗号リスト」に記載されたアルゴリズム及び鍵長は互換性維持以外の目的での利用をしてはならない。また、互換性維持の目的であったとしても、暗号が解読される等のリスクが考えられるため、「電子政府推奨暗号リスト」に記載されたアルゴリズム及び鍵長への移行を検討する必要がある。

（参考２）政府統一基準に係る法令等

サイバーセキュリティ基本法（平成26年法律第104号）＜抜粋＞

（国の行政機関等におけるサイバーセキュリティの確保）

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又　は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第八号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十三条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

（設置）

第二十五条　サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部（以下「本部」という。）を置く。

（所掌事務等）

第二十六条　本部は、次に掲げる事務をつかさどる。

一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

三　～　六　（略）

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７年６月27日サイバーセキュリティ戦略本部決定）＜抜粋＞

（目的）

第一条　本規範は、サイバーセキュリティ基本法（平成二十六年法律第百四号。以下「法」という。）第二十六条第一項第二号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）におけるサイバーセキュリティに関する対策の基準として、機関等がとるべき対策の統一的な枠組みを定め、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。

（適用対象）

第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。

一　国の行政機関 法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関

二　独立行政法人 独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人

三　指定法人 法第十三条に規定する指定法人

２　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。

３　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び情報システムに入力された書面に記載された情報を含む。）及び情報システムの設計又は運用管理に関する情報とする。

（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。