資料7

CRYPTRECにおける検討状況について
～量子コンピュータ時代に向けた 暗号の在り方検討タスクフォース～

CRYPTREC事務局
（総務省 サイバーセキュリティ統括官室）

CRYPTREC暗号リスト

- **総務省**及び**経済産業省**（NICT及びIPA）は、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト「**CRYPTREC**」を実施。
  ※CRYPTREC：Cryptography Research and Evaluation Committees
- 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、電子政府での利用を推奨するものとして**CRYPTREC暗号リスト**※を公表。
  ※平成15年2月20日に「電子政府推奨暗号リスト」として策定し、平成25年3月1日に「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）」として改定し、現在再改定のための検討を実施中。

CRYPTRECの体制

暗号技術検討会
座長：松本 勉　横浜国立大学教授
（事務局：総務省、経済産業省）

量子コンピュータ時代に向けた暗号の在り方検討タスクフォース（2019年度新設）

暗号技術評価委員会
委員長：高木 剛　東京大学大学院教授
（事務局：NICT、IPA）

(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

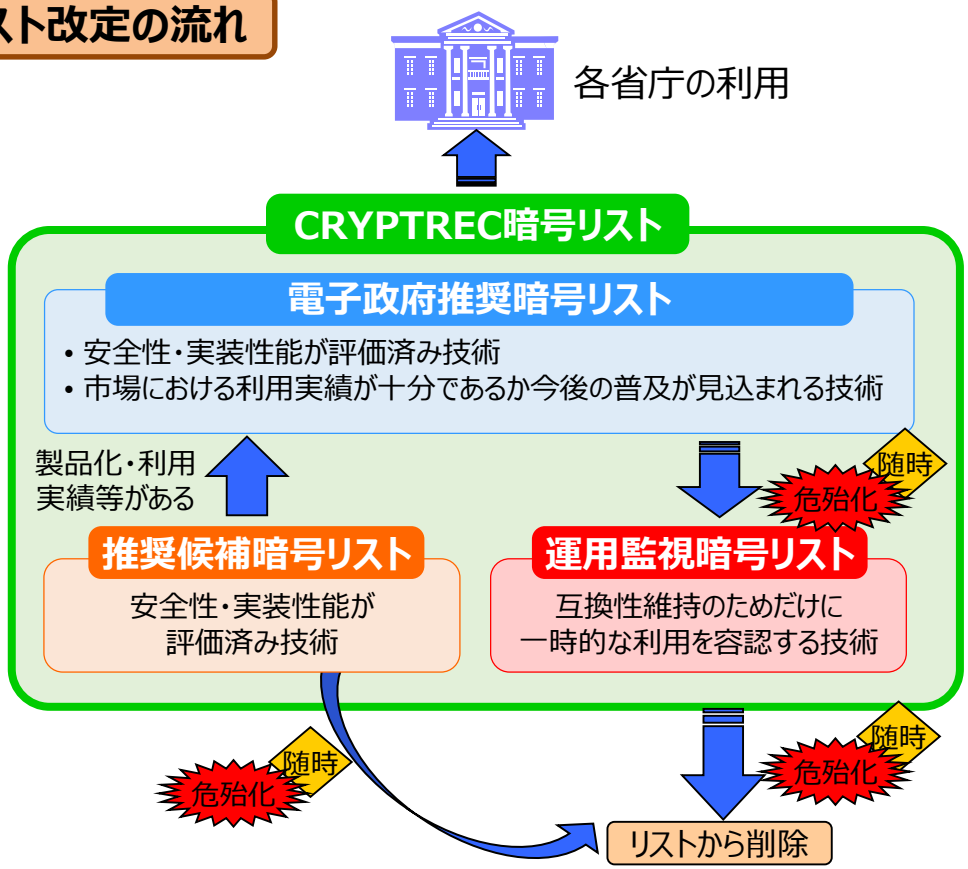
暗号技術調査WG

暗号技術活用委員会
委員長：松本 勉　横浜国立大学教授
（事務局：IPA、NICT）

(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

TLS暗号設定ガイドラインWG

リスト改定の流れ



（参考）CRYPTREC暗号リスト

電子政府推奨暗号リスト

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	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
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

推奨候補暗号リスト

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128
		SHAKE256
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

運用監視暗号リスト

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4
ハッシュ関数		RIPEMD-160
		SHA-1
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC
認証暗号		該当なし
エンティティ認証		該当なし

＜参考：政府機関等の対策基準策定のためのガイドライン（平成30年度版）（平成30年7月25日 内閣官房 内閣サイバーセキュリティセンター）＞

6.1.5 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**」を参照した上で、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並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

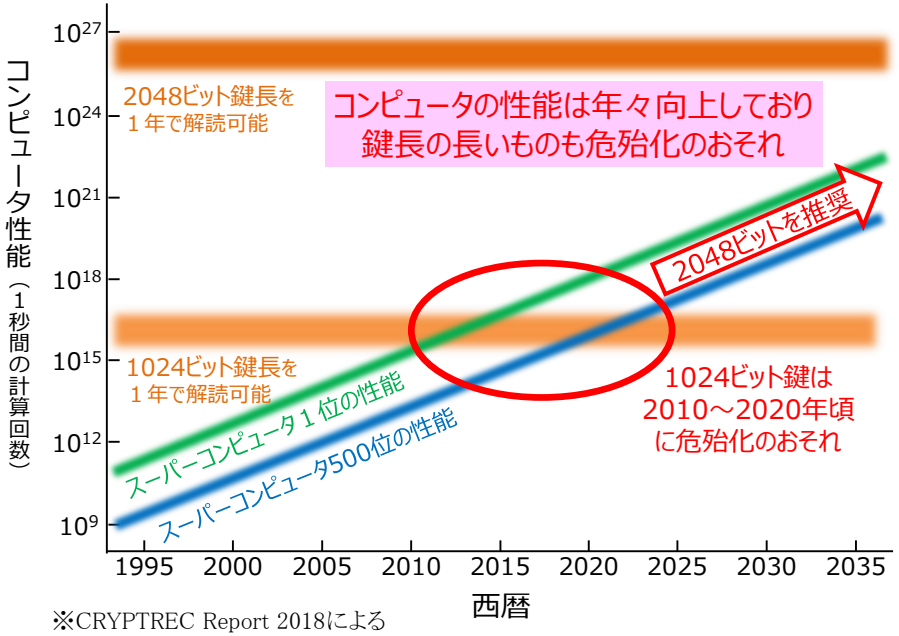
(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「**電子政府推奨暗号リスト**」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「**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それを利用した安全なプロトコルを採用すること。

量子コンピュータ時代に向けた暗号の在り方の検討

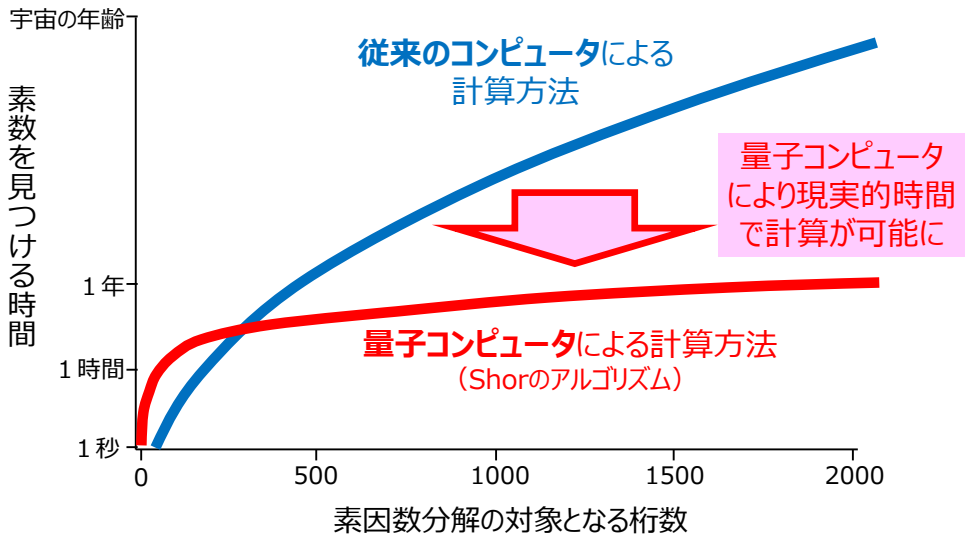
- **実用的な量子コンピュータ**の登場により、遠くない将来に**現在の公開鍵暗号**（RSA暗号や楕円曲線暗号）が**容易に解読されるおそれ**があり、大規模システムの改修・更改には10年以上を要する。
  ※RSA暗号：大きな桁数の素因数分解は困難なことを安全性の根拠とした公開鍵暗号。インターネット通信における暗号化等で広く利用されている。
- こうした状況を踏まえ、CRYPTRECの暗号技術検討会の下に「**量子コンピュータ時代に向けた暗号の在り方検討タスクフォース**」を設置し、量子コンピュータ時代の推奨暗号の在り方について検討を開始（2019年６月～）。

コンピュータの性能向上による影響
例：RSA暗号の安全性評価



※CRYPTREC Report 2018による

実用的な量子コンピュータによる影響
例：RSA暗号の安全性評価



※Quantum Computing (Stolze and Suter)に基づく

（参考）量子コンピュータ時代に向けた暗号の在り方検討タスクフォース

検討事項

✓大規模な量子コンピュータの動向を踏まえた次期CRYPTREC暗号リストに求められる要件等の検討
✓その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

構成員

	宇根 正志	日本銀行金融研究所情報技術研究センター 情報技術研究グループ長
	國廣 昇	筑波大学システム情報系教授
	高木 剛	東京大学大学院情報理工学系研究科教授
	松井 充	三菱電機株式会社開発本部役員技監
(座長)	松本 勉	横浜国立大学大学院環境情報研究院教授
	松本 泰	セコム株式会社IS研究所 コミュニケーションプラットフォームディビジョンマネージャー
	満塩 尚史	内閣官房情報通信技術(IT)総合戦略室政府CIO補佐官

＜オブザーバ＞ 内閣サイバーセキュリティセンター、警察庁、個人情報保護委員会事務局、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、防衛省、警察大学校、国立研究開発法人産業技術総合研究所

＜事務局＞ 総務省、経済産業省、国立研究開発法人情報通信研究機構、独立行政法人情報処理推進機構

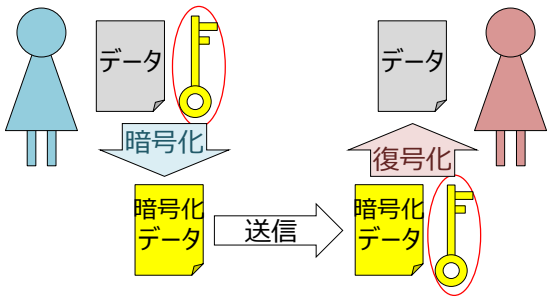
開催概要

第１回	令和元年６月24日	量子コンピュータの動向について 耐量子計算機暗号の動向について
第２回	令和元年９月６日	CRYPTREC暗号リストにおける耐量子計算機暗号の扱いについて 軽量暗号の動向について CRYPTREC暗号リストにおける軽量暗号等の扱いについて
第３回	令和元年12月24日	CRYPTREC暗号リストに関する論点等について

（参考）量子コンピュータ時代の暗号関係技術

共通鍵暗号

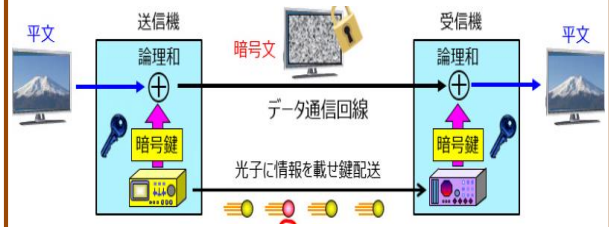
同一の暗号鍵を事前に双方で共有



N人が通信する際、**N×(N-1)通りの鍵**が必要

鍵の共有(運搬)がセキュリティリスクになりうる

量子力学の原理（物理法則）に基づき、盗聴が不可能な方法により鍵共有が可能

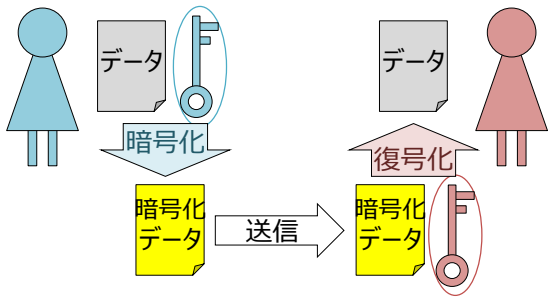


(2) 量子鍵配送(量子暗号)
Quantum **K**ey **D**istribution

ネット利用の進展に伴い鍵管理が煩雑化

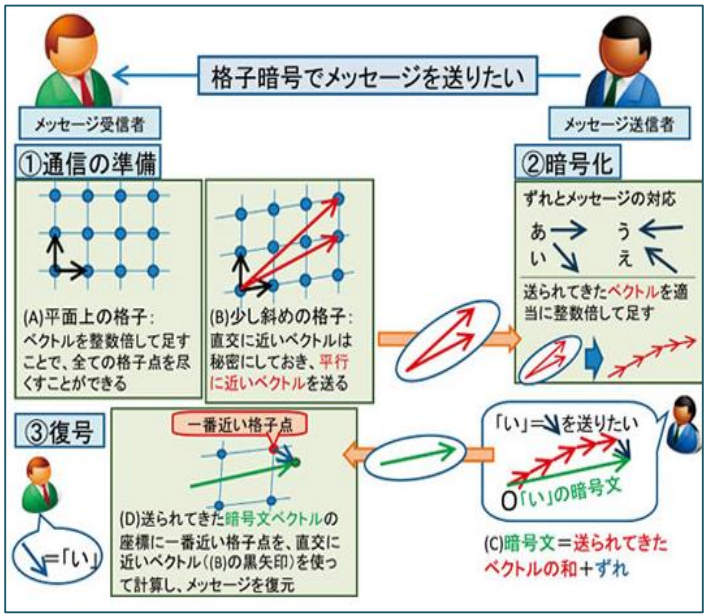
公開鍵暗号

公開鍵を公開し、**秘密鍵**は自身で保有



N人が通信する際、**N通り**の**鍵**で足りる

＜格子に基づく耐量子計算機暗号の例＞



＜公開鍵暗号の代表例：RSA暗号＞

素因数分解

$$n = p \times q$$

合成数＝公開鍵　素数×素数＝秘密鍵

例：公開鍵＝23449／秘密鍵＝131、179
（実際には数百桁程度の数を使用）

古典コンピュータ　解読は実質不能

量子コンピュータ　解読の可能性

量子コンピュータに耐えうる暗号の必要性

量子コンピュータでも効率的な計算方法が発見されていない数学的計算問題を活用した暗号方式が各種提案

- ✓格子に基づく暗号技術
  （CRYSTALS-KYBER、FrodoKEM、LAC、NewHope、NTRU、NTRU Prime、Round5、SABER等）
- ✓符号に基づく暗号技術
  （BIKE、Classic McEliece、HQC、LEDAcrypt、NTS-KEM、ROLLO、RQC等）
- ✓その他
  （SIKE、Three Bears等）

(1) 耐量子計算機暗号
Post-**Q**uantum **C**ryptography

タスクフォースにおける検討内容①

量子コンピュータの現状について

- ✓ **暗号解読ができるような**（大規模でノイズの少ない）**量子コンピュータ※の実現時期は見えていない。**
  - ※ 素因数分解された最大の数は「21」であるが、その数に特化した方法で計算しており汎用的な素因数分解を実施したものではない。（暗号解読のためには、汎用的な方法により、数百桁程度の素因数分解が必要）
- ✓ 量子コンピュータの性能は、「量子ビット数」、「ノイズ（誤り）」※、「演算可能回数」※が重要な指標。
  - ※ 古典コンピュータには計算誤りの発生時に訂正する機能があり、何年も計算させ続けられるが、量子コンピュータでは誤り訂正の実現の難易度が高く、現在は誤り訂正をせずに計算を行う必要がある。そのため、コヒーレンス時間（状態が保たれている時間；現状はミリ秒程度）の中で計算を終わらせる必要があり、演算可能回数も制限されている。
- ✓ 量子ビット数は公表されているが、ノイズ等はあまり公表されないため、計算性能に関する将来予測は困難。
- ✓ そもそもゲート型量子コンピュータの量子ビット数が数千程度以上ないと（ノイズ等に関わらず）暗号解読はできないと見込まれているため、公表されている**量子ビット数の動向を確認し続けることが妥当。**
- ✓ ノイズがある場合※でも、**化学や金融の分野では活用できる**想定だが、現状のノイズは**暗号解読のための素因数分解に活用できる水準ではない。**
  - ※ NISQ（Noisy Intermediate-Scale Quantum Computer）。Google社、IBM社、Intel社等が開発している。

今後の予定

現在の**量子コンピュータの開発状況**を踏まえると、**近い将来**にCRYPTREC暗号リスト記載の**暗号技術が危殆化する可能性は低い**旨、近日中に**CRYPTRECホームページにて周知**予定

タスクフォースにおける検討内容②

CRYPTREC暗号リストにおける耐量子計算機暗号の位置付けについて

- ✓ **CRYPTREC暗号リスト**は、**安全性等の評価に加え、利用実績や普及見込みも考慮**した暗号リスト。
- ✓ 一方、「**耐量子計算機暗号(PQC)**」に関しては、多数の方式が提案され安全性等の検討が行われているが、利用実績や普及見込みについて評価できる段階にない。
- ✓ **PQC**については、CRYPTREC暗号リストには含めず、**ガイドライン等の別文書**とし、当該文書の**重要性がわかるようCRYPTREC暗号リストから参照**する。

高機能暗号や軽量暗号の位置付けについて

- ✓ 今後、利用が拡大すると想定される、IoT機器等に用いられる「**軽量暗号**」や、暗号状態での情報処理が可能となる「**高機能暗号**」は、利用環境やアプリケーションが限定され、従来暗号とは取り扱いが異なる。
- ✓ **軽量暗号・高機能暗号**についても、CRYPTREC暗号リストには含めず、**ガイドライン等の別文書**と、当該文書の**重要性がわかるようCRYPTREC暗号リストから参照**する。

CRYPTREC暗号リスト本体について

- ✓ **CRYPTREC暗号リスト**の改定（2023年目途）について、現行の**３リスト構成の在り方**については**引き続き検討**が必要であるものの、**技術分類**については**現行のものを踏襲**し、公募は行わない。
- ✓ **推奨される暗号のパラメータ**について、CRYPTREC暗号リストから参照する形で**別の文書としてまとめる**。

今後の予定

暗号技術検討会（2020年3月）において、上記の**検討結果をとりまとめ、来年度の活動方針※を決定**

※量子コンピュータや耐量子計算機暗号の状況をフォローするため、及び引き続き継続検討としたCRYPTREC暗号リスト改定等に関する議論を行うため、タスクフォースを継続設置
（PQCに関するガイドラインは、暗号技術評価委員会にてCRYPTRECリストの改定作業と並行して実施予定）