CRYPTREC
Cryptography Research and Evaluation Committees

# CRYPTREC暗号リスト改定に向けた動向及び暗号強度要件設定基準の紹介

CRYPTREC事務局
（デジタル庁・総務省・経済産業省・NICT・IPA）

# 目次

1. CRYPTREC暗号リスト改定に向けた動向
   - ●CRYPTREC暗号リスト改定方針
   - ●CRYPTREC暗号リスト移行ルール
   - ●暗号利用実績調査による選定基準
   - ●スケジュール

2. 「暗号強度要件（アルゴリズム及び鍵長）に関する設定基準」の紹介
   - ●設定基準作成の背景・位置づけ
   - ●設定基準の概要

# CRYPTREC暗号リスト

## 各省庁での利用

サイバーセキュリティ戦略本部決定、「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」の遵守事項に記載

**CRYPTREC暗号リスト**

**電子政府推奨暗号リスト**

- 安全性・実装性能評価済み技術
- 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技術

製品化・利用実績がある

危殆化 随時

**推奨候補暗号リスト**

安全性・実装性能評価済み技術

**運用監視暗号リスト**

互換性維持のためだけに一時的な利用を容認する技術

安全性・実装性評価等

公募

国際標準 (ISO・ITU-T等) 随時

利用実績 随時

危殆化 随時

定期的 長期の利用実績なし

危殆化 随時

容認不要 随時

リストから削除

CRYPTREC Cryptography Research and Evaluation Committees

# タスクフォースの検討結果（CRYPTREC暗号リスト関係）

抜粋再掲

## CRYPTREC暗号リストの構成

✓ CRYPTREC暗号リストについて、次の**3リスト構成は維持**し、リスト間の**遷移ルールを明確化**。

① **電子政府推奨暗号リスト**（安全性・実装性能が確認され、利用実績や普及見込みがあると判断されたもの）

② **推奨候補暗号リスト**（安全性・実装性能が確認され、今後①のリストに掲載される可能性のあるもの）

③ **運用監視暗号リスト**（危殆化等により推奨すべき状態ではなく、互換性維持のために継続利用を容認するもの）

✓ 各暗号技術は十分成熟しているため、技術分類※は変更せず、新たな暗号技術の公募も実施しない。

※7分類：公開鍵暗号／共通鍵暗号／ハッシュ関数／暗号利用モード／メッセージ認証コード／認証暗号／エンティティ認証

## CRYPTREC暗号リストの今後の改定

✓ 2003年に作成、2013年に改定を行い、**今般、2023年目途に改定作業中**であり、10年単位で改定。

✓ 常に危殆化等の監視を行い、必要に応じた暗号技術の加除等も行っており、10年単位とする必要もない。

→ 次の改定以後は、改定後5年以内を目途に暗号技術検討会において改定是非を判断することとする。

CRYPTREC Cryptography Research and Evaluation Committees

# CRYPTREC暗号リスト移行ルール

再掲

## ①電子政府推奨暗号リスト

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

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

※電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

標準化等により将来的な
利用が見込まれ、安全性や
実装性能が十分にあると
暗号技術検討会が決定した場合
（公募や事務局提案等）

## ②推奨候補暗号リスト

## ③運用監視暗号リスト

安全性維持が困難(危殆化した)と判断した場合

CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの

**（2019年度暗号技術検討会　決定事項）**
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、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。
1. 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2. 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3. その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

※利用実績調査の具体的な実施内容・評価基準は、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

## リストから削除

# 電子政府推奨暗号リストへの選定方法

暗号技術評価委員会で**安全性及び実装性の評価を実施**し、
その結果により暗号技術検討会が**推奨候補暗号リストに含めると決定**

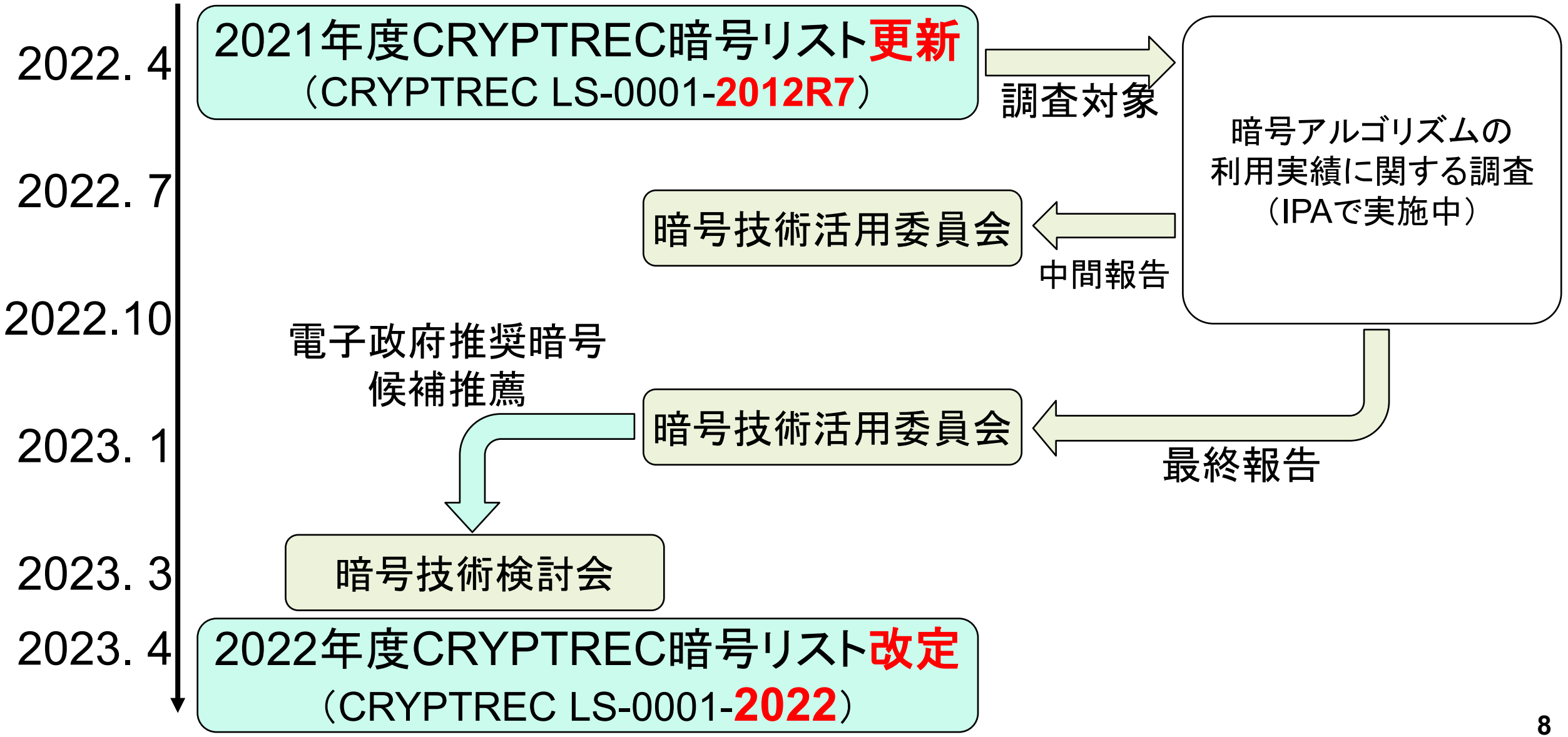
**利用実績による選定基準**（次ページ）に基づき、暗号技術活用委員会にて
電子政府推奨暗号リストへの**昇格検討対象の暗号技術を検討・選定**し、
暗号技術検討会に推薦

推薦された暗号技術について、暗号技術検討会では、その**根拠となった利用実態を再度確認・審議**を行い、電子政府推奨暗号リストへの昇格に問題がないと判断した場合に**電子政府推奨暗号リストに選定**

# 利用実績による選定基準

| 考慮項目 | | 選定目安 |
|---|---|---|
| 採用実績 | 以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、<br>• 5年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」<br>• 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」<br>により確認するものとする。 | |
| | ① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合 | 電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。 |
| | ② **利用実績調査**又は**利用実態確認**の結果、**電子政府システムや重要インフラ等日本の基幹システム**においてすでに利用されていることが確認された場合 | 必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。 |
| | **利用実績調査**又は**利用実態確認**の結果、③～⑤のいずれかが確認された場合：<br>③ **利用者が多い主要な汎用製品群の複数**に搭載されるなど、明らかに採用が進展していると判断された場合<br>④ **利用者が多い主要なオープンソースソフトウェアの複数**に搭載されるなど、明らかに採用が進展していると判断された場合<br>⑤ **利用者が多い主要なサービスやプロトコルの複数**で利用されるなど、明らかに採用が進展していると判断された場合 | 「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。<br>※「複数」の意味は、必要条件として「2個以上が必要」ということであって、「2個以上あればよい」という十分条件としての意味ではないことに留意 |
| 標準化実績 | 以下を満たす場合、昇格の検討対象に含める。 | |
| | ⑥ **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合 | 電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討対象とする。 |

# CRYPTREC暗号リストの改定スケジュール



# タスクフォースの検討結果（CRYPTREC暗号リスト関係）

抜粋再掲

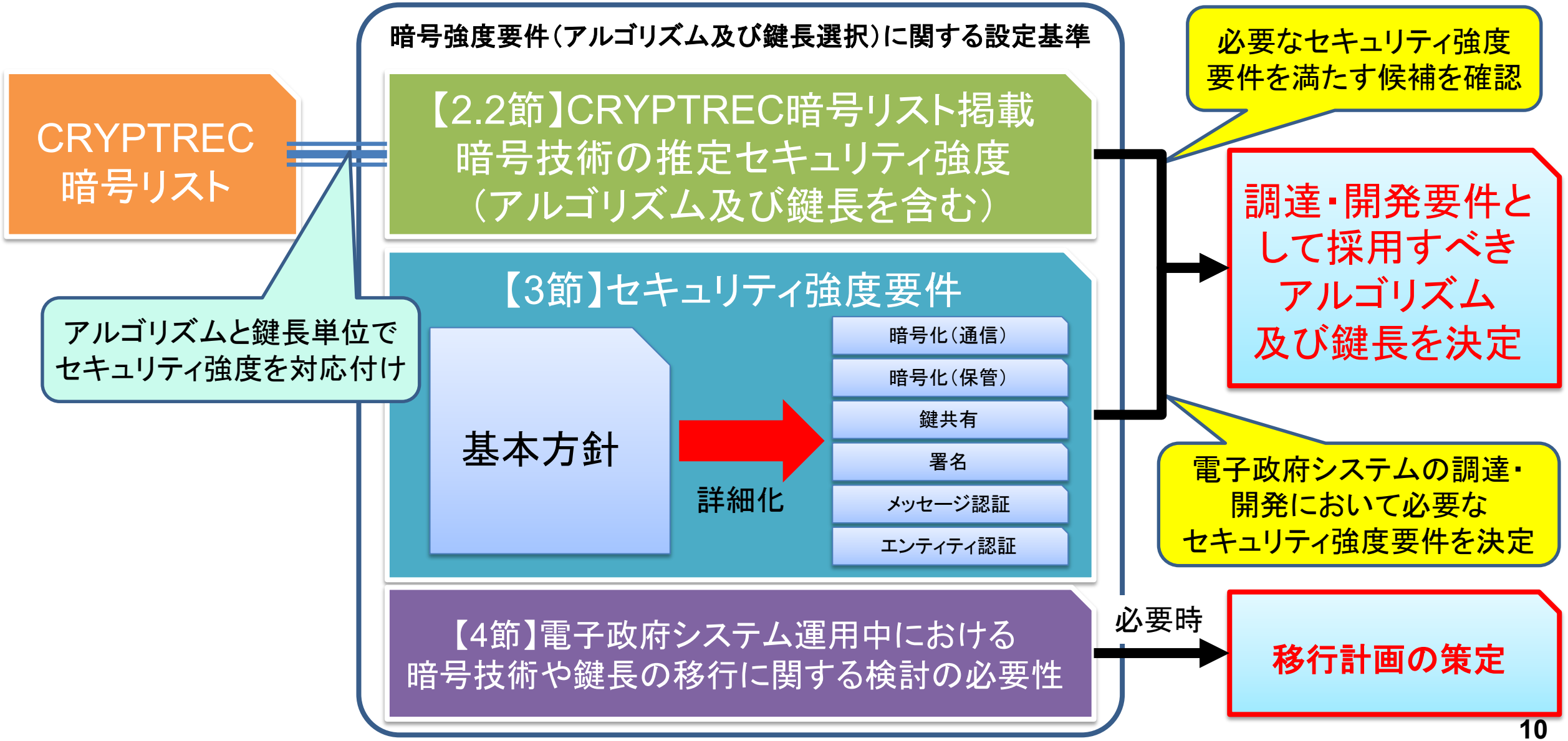
## 暗号技術のパラメータ

- ✓ CRYPTREC暗号リストでは推奨する暗号技術（暗号アルゴリズム）を示してきたが、パラメータは提示していない。
- ✓ 推奨パラメータの明示は、安全なシステム構築や計画的な暗号技術の移行を促進するために有用。

→ **推奨パラメータを規定する別の文書を新たに作成**する。
（CRYPTREC暗号リストから当該文書を参照する構成とする。）

（暗号技術活用委員会にて作成に向けた検討を実施し、「**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**」を策定。）

# 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準概要

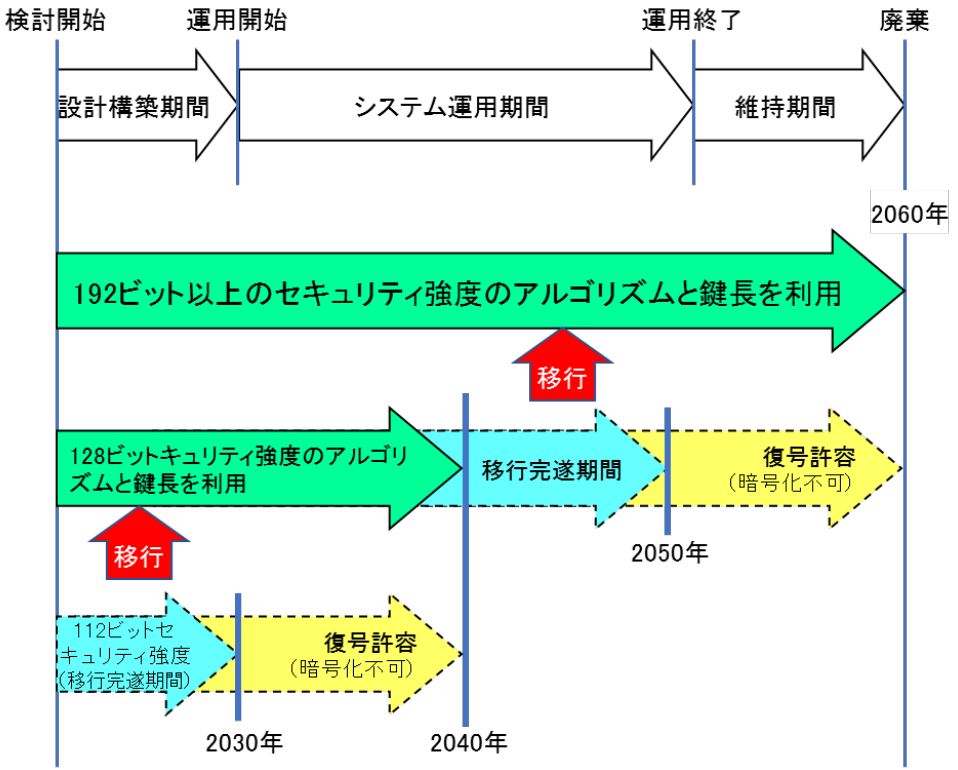


# セキュリティ強度要件の基本設定方針概要(1/2)

■ 電子政府システムを調達又は開発する際は、その**システムの運用寿命全体と、その期間に実現するセキュリティ強度の関係を考慮**してセキュリティ強度要件を設定し、その強度要件を満たすアルゴリズムと鍵長の組合せを調達・開発要件としなければならない。

- 設定されたセキュリティ強度要件と同じかそれ以上のセキュリティ強度を満たすアルゴリズム及び鍵長の組合せをサポート(実装)しなければならない
- 設定したセキュリティ強度要件以下の安全性のアルゴリズム及び鍵長をサポート(実装)すること自体は妨げない。ただし、サポート(実装)されたアルゴリズム及び鍵長の利用期間については、そのセキュリティ強度に応じて、セキュリティ強度要件に従って定めなければならない
- データのセキュリティ寿命は利用するアルゴリズムのセキュリティ寿命に包含されなければならない

想定廃棄年を2060年に予定しているシステムにおける保管時の暗号化の場合



# セキュリティ強度要件の基本設定方針概要(2/2)

■ 必要なセキュリティ強度要件は以下の表をベースとして、**システムの想定運用終了・廃棄年又は利用期間の終了年を基準**に設定する

| 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*1) | 移行完遂期間*4) | 利用不可 | 利用不可 | 利用不可 | 利用不可 |
| | 処理*2) | | 許容*3) | | | |
| 128ビット セキュリティ | 新規生成*1) | 利用可 | 利用可 | 移行完遂期間*4) | 利用不可 | 利用不可 |
| | 処理*2) | | | | 許容*3) | |
| 192ビット セキュリティ | 新規生成*1) | 利用可 | 利用可 | 利用可 | 利用可 | 利用可 |
| | 処理*2) | | | | | |
| 256ビット セキュリティ | 新規生成*1) | 利用可 | 利用可 | 利用可 | 利用可 | 利用可 |
| | 処理*2) | | | | | |

*1) 新規に暗号処理を実行する場合(例:暗号化、署名生成)

*2) 処理済みのデータに対して処理を実行する場合(例:復号、署名検証)

*3) 処理済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等(暗号技術によるものとは限らない)を併用している場合

*4) よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させなければならない期間。利用する暗号処理が短期間で完結する場合(例:エンティティ認証)、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定

注) 2021年末時点での暗号技術の安全性評価の現状等を踏まえたうえで、2070年までの予測可能なセキュリティマージンを持った基準として定めたものである。
したがって、精度の高い実現時期の予測が困難な、画期的な暗号解読手法の発明や大規模量子コンピュータの実現によるアルゴリズムの危殆化等については考慮していない。

# （参考）CRYPTREC暗号リスト上の暗号技術とセキュリティ強度との対応

CRYPTREC Cryptography Research and Evaluation Committees

注) **今後、暗号解読手法の進展や大規模量子コンピュータの実現等により、暗号アルゴリズム及び鍵長によっては推定セキュリティ強度が見直される可能性がある（少なくとも5年ごとに再確認される）。**

| ビットセキュリティ | 112 | 128 | 192 | 256 |
|---|---|---|---|---|
| 公開鍵暗号 | RSA系*1)(鍵長2048ビット)<br>DSA(鍵長2048ビット/224ビット)<br>ECDSA(P-224,B-233,K-233)<br>DH(鍵長2048ビット/224ビット)<br>ECDH(P-224,B-233,K-233)<br>PSEC-KEM(P-224,B-233,K-233) | RSA系*1)(鍵長3072ビット)<br>DSA(鍵長3072ビット/256ビット)<br>ECDSA(P-256,B-283,Ed25519等)<br>DH(鍵長3072ビット/256ビット)<br>ECDH(P-256,B-283,Ed25519等)<br>PSEC-KEM(P-256,B-283,Ed25519等) | RSA系*1)(鍵長7680ビット)<br>DSA(鍵長7680ビット/384ビット)<br>ECDSA(P-384,B-409,Ed448等)<br>DH(鍵長7680ビット/384ビット)<br>ECDH(P-384,B-409,Ed448等)<br>PSEC-KEM(P-384,B-409,Ed448等) | RSA系*1)(鍵長15360ビット)<br>DSA(鍵長15360ビット/512ビット)<br>ECDSA(P-521,B-571,K-571)<br>DH(鍵長15360ビット/512ビット)<br>ECDH(P-521,B-571,K-571)<br>PSEC-KEM(P-521,B-571,K-571) |
| 共通鍵暗号 | 3-key Triple DES | ブロック暗号*2)(鍵長128ビット)<br>KCipher-2<br>Enocoro-128v2<br>MUGI | ブロック暗号*2)(鍵長192ビット) | ブロック暗号*2)(鍵長256ビット)<br>MULTI-S01 |
| ハッシュ関数 | | SHA-256<br>SHA-512/256<br>SHA3-256<br>SHAKE128<br>SHAKE256(ハッシュ長256ビット) | SHA-384<br>SHA3-384<br>SHAKE256(ハッシュ長384ビット) | SHA-512<br>SHA3-512<br>SHAKE256(ハッシュ長512ビット) |
| ハッシュ関数<br>(HMAC利用時) | | SHAKE128<br>RIPEMD-160<br>SHA-1 | | ハッシュ関数*3) |
| 認証暗号 | | | | ChaCha20-Poly1305 |

*1) 次の公開鍵暗号
- RSA-PSS
- RSASSA-PKCS1-v1_5
- RSA-OAEP
- RSAES-PKCS1-v1_5

*2) 次の共通鍵暗号（ブロック暗号）
- AES
- CIPHERUNICORN-E
- MISTY1
- CLEFIA
- SC2000
- Camellia
- Hierocrypt-L1
- CIPHERUNICORN-A
- Hierocrypt-3

*3) 次のハッシュ関数
- SHA-256
- SHA-512
- SHA3-256
- SHA3-512
- SHA-384
- SHA-512/256
- SHA3-384
- SHAKE256

［文字色の凡例］
- 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

# 運用中における暗号技術及び鍵長移行に関する検討の必要性

■ 新しいアルゴリズム及び鍵長に移行するのは、多くの場合、非常に時間とコストがかかる作業であることを念頭に置いておく必要がある。

- 利用しているアルゴリズムや鍵長がセキュリティ寿命を迎える**少なくとも5年前まで**には、より強力なアルゴリズム及び鍵長への移行計画を策定すべき。その際、いつからどのくらいの期間をかけてどのアルゴリズムや鍵長に移行するのかを明確にすべき。

■ 以下に該当する事象が発生した場合には、直ちに内容の確認を行い、必要に応じて移行計画を策定しなければならない。

- 電子政府システムの運用寿命の延長に伴う対応
- セキュリティ強度要件の設定変更に伴う対応
- 暗号技術の推定セキュリティ強度の変更に伴う対応
- 運用監視暗号リストに掲載されたアルゴリズムの継続利用にあたっての対応
- 突発的な理由に伴う緊急移行にあたっての対応
- 量子コンピュータの実現リスクへの対応

# CRYPTREC暗号リスト説明文の変更

## ■ 電子政府推奨暗号リスト

暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）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。**なお、利用する鍵長について、「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」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。**

## ■ 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。**なお、本リストに記載されている暗号技術を利用する際は、「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」の規定に合致する鍵長を用いることが求められることに留意すること。**

## ■ 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と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。互換性維持以外の目的での利用は推奨しない。**なお、本リストに記載されている暗号技術を利用する際は、「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」の規定に合致する鍵長を用いることが求められることに留意すること。**


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