リスト改訂スキームについて

山村　明弘（秋田大学）

リスト改訂の背景

現在の電子政府推奨暗号リスト（現リスト）

電子政府で利用可能な”安全な”暗号アルゴリズムを推奨

環境の変化・現リストの課題

- 暗号技術危殆化への対応
- 新しい技術への対応
- ISOにおける暗号技術標準化の進展
- 安全なシステム構築とリストの間のギャップ

新しい電子政府推奨暗号リスト（新リスト）

電子政府における安全な暗号技術の利用の促進する標準の提供

リスト改訂への要望

新たなリストへの要望や現リストに対する意見を有識者から聴取した(2007-2008年)

技術の経年劣化と新しい技術への対応

- 現リストの策定から5年経ち、暗号技術も大きく変化している
- 新しい技術にも目を向けることの必要性

安定した技術、市場で十分な利用実績がある技術

- 安全性に加えて、競争力(信頼性、商品の供給、価格)のあるもの
- 調達者、開発者、利用者にとってのわかりやすさ

リストの目的の明確化と情報提供や啓発

- 関連活動との協力による電子政府のセキュリティ確保
- 暗号技術を利用した調達者、開発者、利用者への情報提供を強化

新リストにおける基本方針

電子政府システムにおいて安全な暗号利用を促進することを目的として、
以下の3つの考え方を導入

暗号技術のライフサイクルへの対応

- 暗号技術の経年劣化にも柔軟に対応できる
- 公募機会の拡大

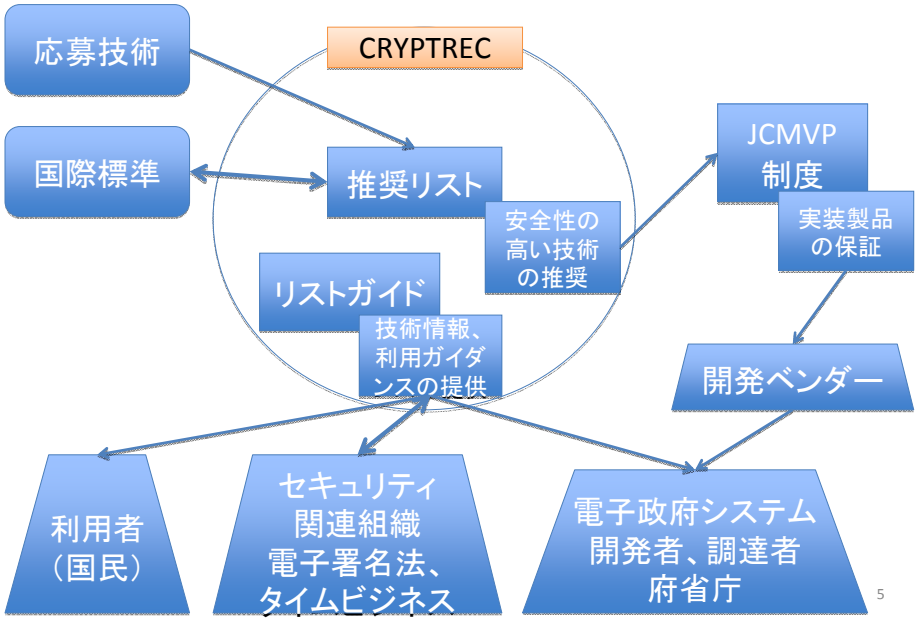
安定している技術の採用と国際動向への注意

- 電子政府における調達にあたり、製品化、利用実績を重視
- 国際標準との整合性を配慮

十分な情報発信

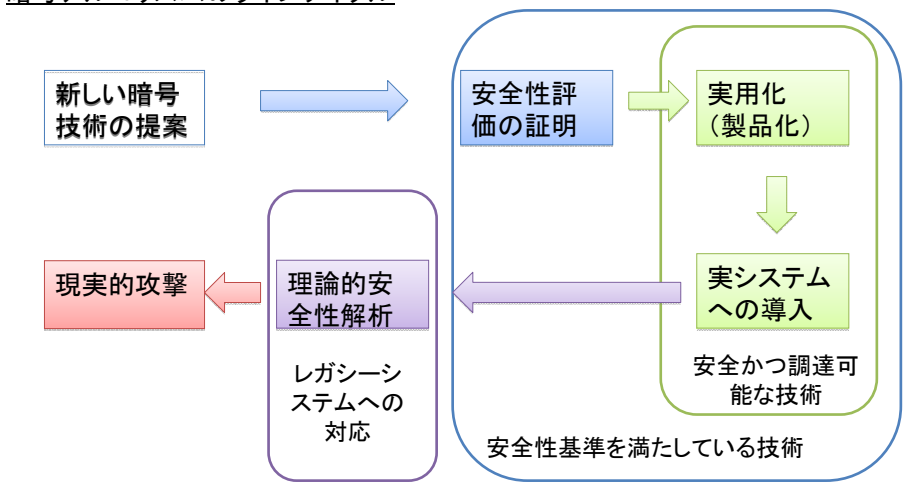
- リストの利活用に必要な技術情報の提供

新リストの利用/運用イメージ



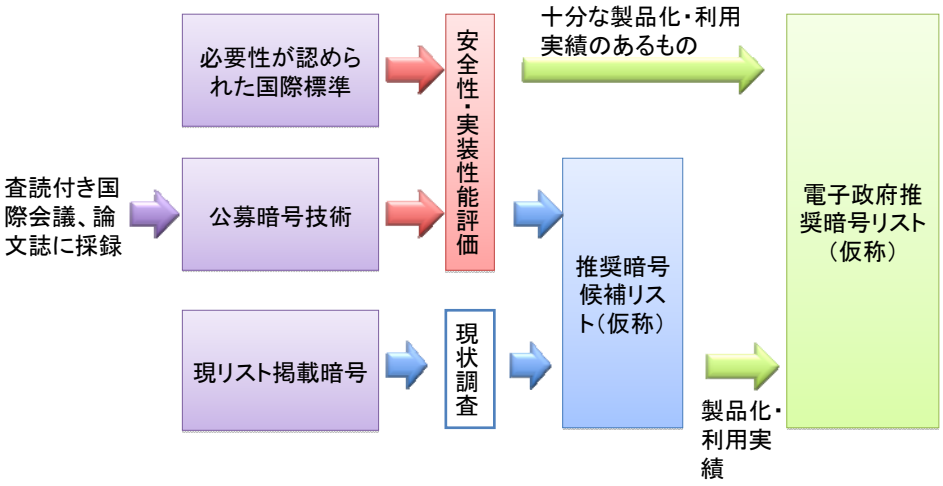
暗号技術のライフサイクルへの対応

暗号アルゴリズムのライフサイクル

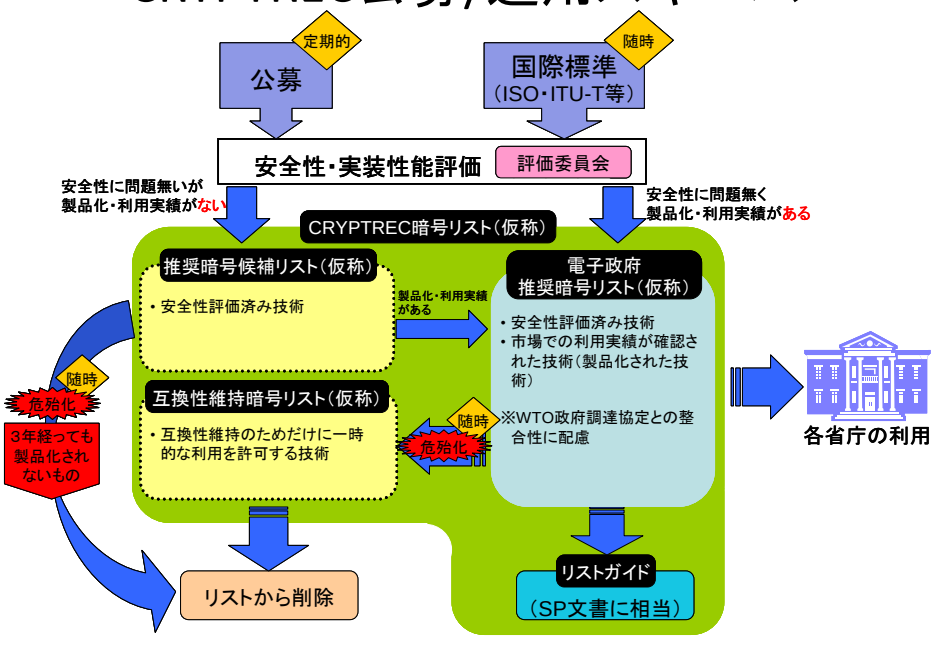


リストに3つのカテゴリを設け、ライフサイクルに応じて柔軟に変動

リスト入りまでの基本的な流れ

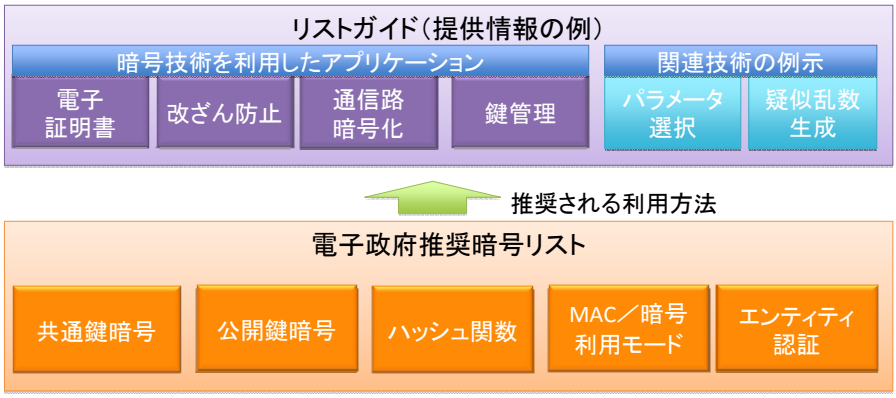


CRYPTREC公募/運用スキーム



リストガイドによる情報発信

- 利用方法に応じた暗号アルゴリズムの適切な利用方法を示す
- 疑似乱数生成のような、標準化は必要がないが、安全な技術が必要とされているアルゴリズムについての指針を示す
- 暗号技術の経年劣化等の技術情報の提供



電子政府推奨暗号リスト（仮称）の選定

<u>電子政府推奨暗号リスト（仮称）</u>

CRYPTRECにより安全性が確認され、かつ市場において利用実績が十分である技術リスト。電子政府構築（政府調達）の際には、当該技術の利用を推奨する（現リストと同等）。ここに登録される技術は、国際標準化期間等により標準化されていることが望ましい。

<u>選定の考え方</u>

- 推奨暗号候補リストの中で、電子政府における調達が可能になった技術であると確認された場合に、電子政府推奨暗号リストに登録
- 詳細な基準については、次年度検討

互換性維持暗号リスト（仮称）の考え方

互換性維持暗号リスト（仮称）

電子政府推奨暗号リスト（仮称）に登録されていたが、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もののうち、互換性維持のために継続利用を容認するもののリスト。

- 暗号の国際学会などで、暗号技術に関する脆弱性が報告された場合に、暗号技術監視委員会において、報告内容を吟味した上で、互換性維持暗号リストへ移行する
- 互換性維持暗号リストへの移行の際には、（可能な限り）安全な技術への移行のタイミングの検討に資する情報を注釈として付ける
- 上記のタイミングになったら互換性維持暗号リストから削除する

公募実施の考え方

公募対象となる技術カテゴリ

以下のいずれかの条件を満たす技術カテゴリについて、定期的に公募を行う。

- 電子政府で利用されており標準化の必要性があるが、リストに掲載されていない
- すでにリストに掲載されている技術に比べ優位性のある新技術が存在し、電子政府での利用が見込まれる
- 実用化技術が確立されており、近い将来において電子政府で利用される見込みがある

2009年度における公募対象カテゴリ

- すでに電子政府で利用されているがリストにないカテゴリ
  - ✓メッセージ認証コード
  - ✓暗号利用モード
  - ✓エンティティ認証
- 既存技術に比べ優位性のある新技術が登場しているカテゴリ
  - ✓128bitブロック暗号
  - ✓ストリーム暗号

スケジュールと今後の進め方

- 2013年に、2009年度版の公募カテゴリに対するリストを公表する。
- 2013年までに、並行してリストガイドを完成させる。
- 新しいカテゴリ・技術の公募については、暗号技術の監視結果のフィードバックとして必要性を検討し、随時行う。