e-Japan構想における暗号評価の位置づけについて

２００２年１月２８日

経済産業省情報セキュリティ政策室長
大野　秀敏

CRYPTREC：暗号技術検討会（座長：今井秀樹東大教授）

電子政府における暗号に関する利用方針の策定のため、経済産業省及び総務省（旧郵政省）の共同事業として、我が国の暗号技術者を集結し、専門的な見地から、暗号技術評価を実施（IPA、TAOが評価事務局）。内閣官房、警察庁、防衛庁、法務省、財務省、外務省とも連携。本検討会は、両省の担当局長により開催される。

対象：共通鍵暗号（ブロック、ストリーム）、公開鍵暗号、ハッシュ

等

評価基準：　暗号アルゴリズムに関する、Security, Flexibility, Efficiency等について評価。

公募形式：　公募により広く透明に受付（外国からも受付）。
（＋その他暗号も評価）

CRYPTREC：暗号技術検討会活動内容

１　電子政府推奨暗号リストの策定

電子申請システム等の電子政府システムで利用される暗号アルゴリズムに関する推奨暗号リストを作成し、安全性及び信頼性の高いシステム構築に貢献。そのために昨年度に引き続き、継続評価及び新規評価を行うとともに、電子政府に求められる暗号要件に関する調査をWG（ﾘｰﾀﾞ：佐々木電機大教授）において実施。

２　電子署名法に基づいて利用される暗号に関する助言

①　電子署名法第2条第3項の電子署名基準（暗号に関するもの）への反映、及び見直し。

②　電子署名法第33条に基づく暗号技術の評価に関する調査研究。

３　暗号技術に関する国際標準化への対応

ISO、ITU等の場における暗号の国際標準化に関する活動について支援を行う。

e-Japan重点計画における位置づけ
（平成１３年３月２９日　IT戦略本部）

６．高度情報通信ネットワークの安全性及び信頼性の確保
（３）具体的施策
①情報セキュリティに係る制度・基盤の整備

ウ）暗号技術の標準化の推進（総務省及び経済産業省）

　客観的にその安全性が評価され、実装性で優れた暗号技術を採用するため、２００２年度までに、ISO、ITU等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

電子政府の情報セキュリティ確保のためのアクションプラン（平成13年10月10日　情報セキュリティ対策推進会議決定）

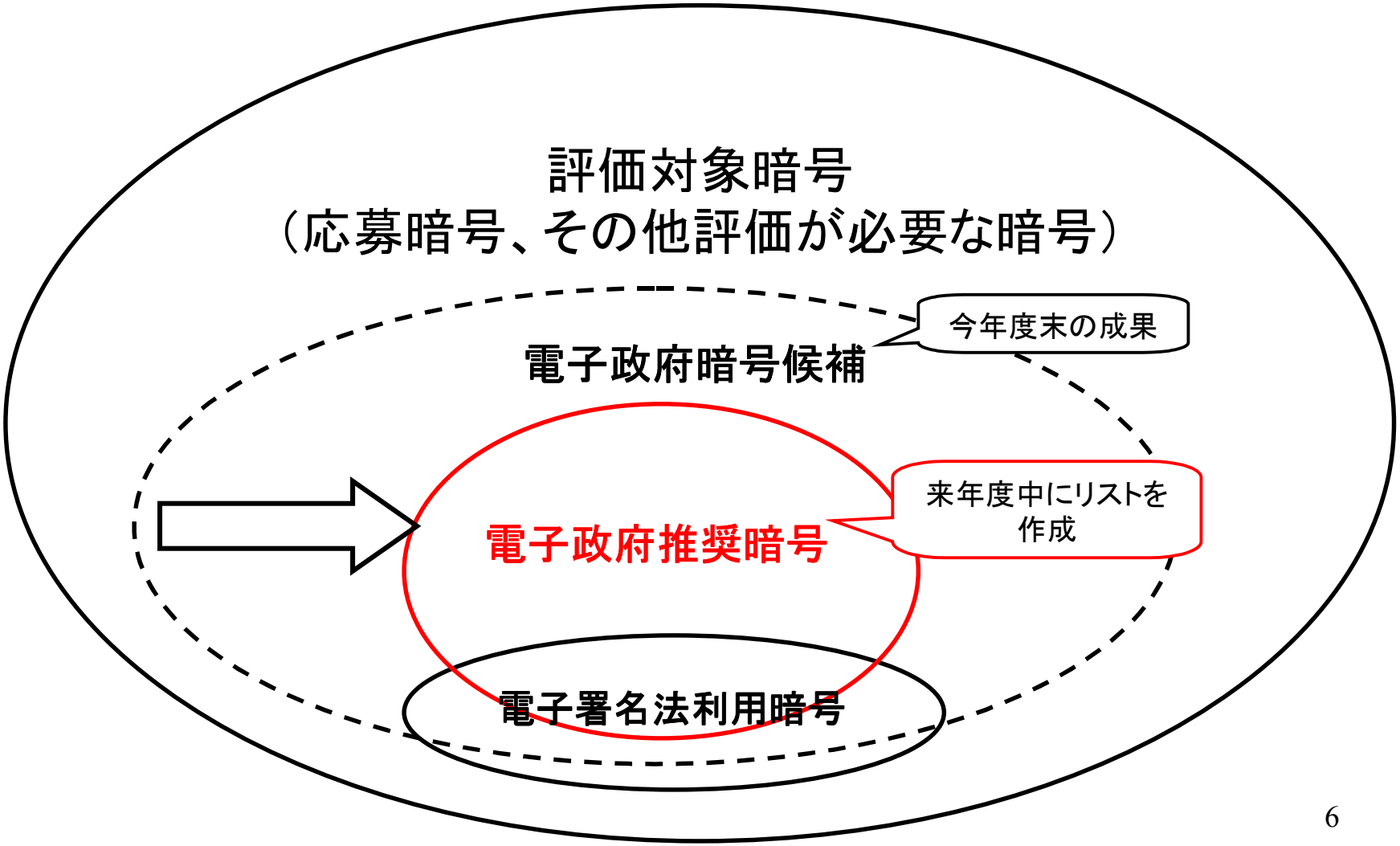
２．具体的な方策

（２）暗号の標準化の推進

・「電子政府」におけるセキュリティ確保のためには、政府調達における一定水準のセキュリティ確保のための情報機器等に関する基準（具体的にはISO/IEC15408）を可能な限り利用することと同様、暗号についても、一定水準以上の安全性及び信頼性を有するものの利用が不可欠であり、これを推進することが必要である。

・このため、総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す。

電子政府推奨暗号


評価対象暗号
（応募暗号、その他評価が必要な暗号）
今年度末の成果
電子政府暗号候補
来年度中にリストを
作成
電子政府推奨暗号
電子署名法利用暗号

今後のスケジュール

平成13年度の成果

電子政府暗号要件調査（カテゴリー及び要件）

暗号評価（電子政府暗号候補）

現在利用されている暗号に関する評価

平成14年10月

電子政府暗号要件及び電子政府暗号候補の一致、リストの作成（カテゴリー：電子署名、送信、保存、etc）

平成15年3月

電子政府推奨暗号リストの提示、調達への反映、省庁間の合意

利用方針の合意

関係の整理

利用方針案のイメージ

利用方針レベル

…(略)…
・各省庁は、セキュリティに関する信頼性の高い情報システムの構築を図る観点から、今後の情報システムの構築にあたっては、可能な限り、別添に掲げるような暗号技術を利用することとする。

別添

	暗号技術	要件)
電子署名	A暗号、B暗号	安全性、実装性等
通信	C暗号、D暗号、E暗号	安全性、実装性等
保存	F暗号、G暗号	安全性、実装性等
その他	H暗号、I暗号	安全性、実装性等

＋調達ガイドブック

（実際の利用に際しての調達者向けの解説本。）