INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

暗号アルゴリズムと認証制度の動向
～国産暗号技術はどこに向かえばいいのか？～

IPA　技術本部　セキュリティセンター
暗号グループ
神田 雅透

はじめに

「システム」や「製品」として「セキュア」であるためには

暗号アルゴリズムが安全 ― 一番、基盤になるものですから

＋

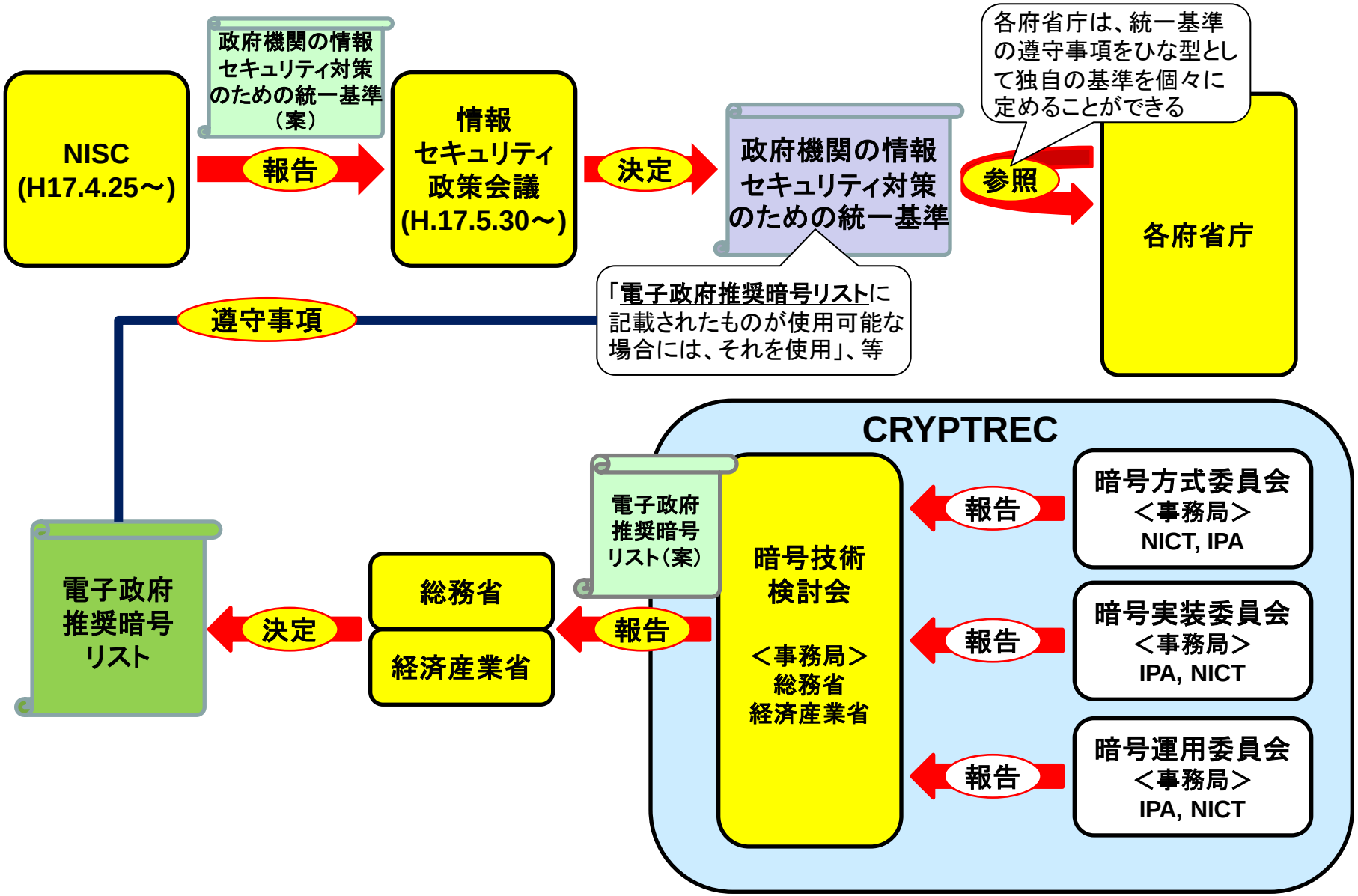
実装物が安全 ― 穴が開いてては意味ないよね

＋

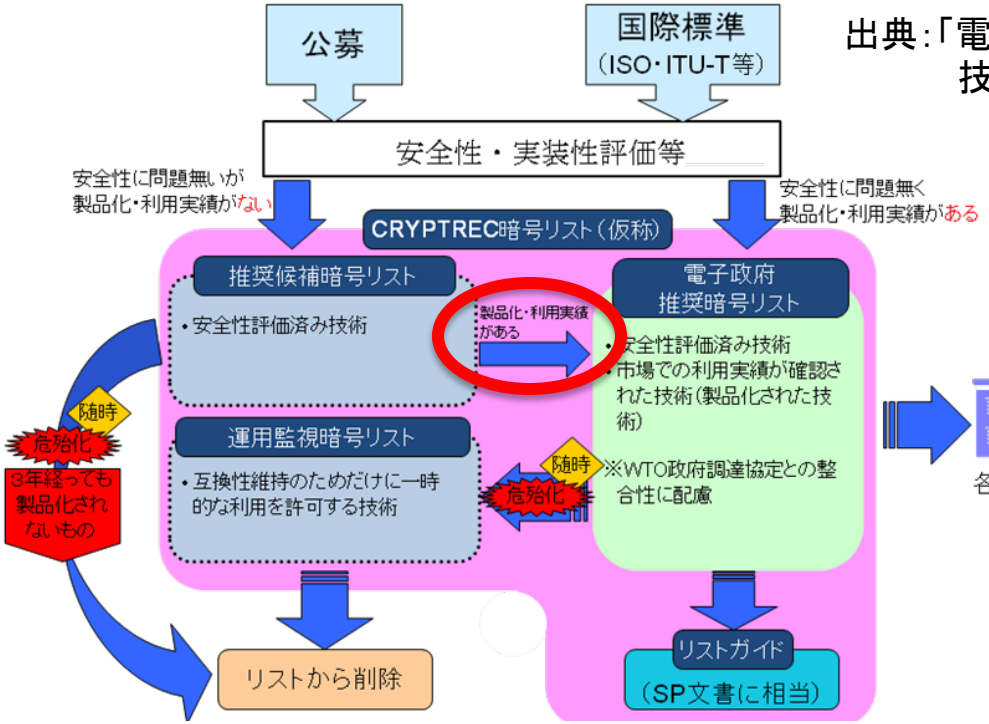
鍵管理がしっかり ― 鍵をほったらかしてはダメだよね

ここは今までにたくさん話があったから ・・・ 飛ばす

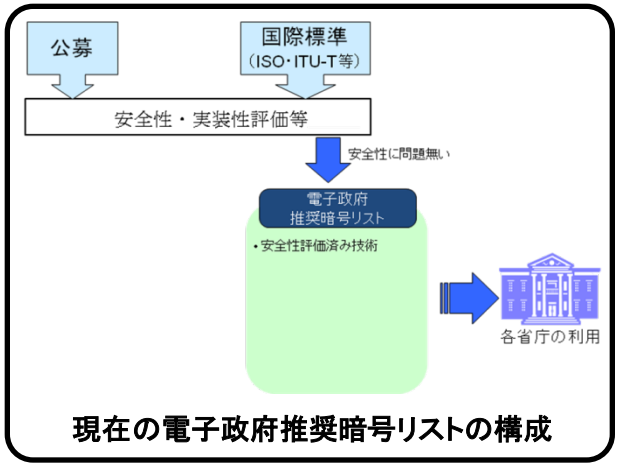
安全な暗号アルゴリズムを選ぼう



次期のCRYPTREC暗号リスト(仮称)の構成



出典:「電子政府推奨暗号リスト改訂のための暗号技術公募要項(2009 年度)」 P.5



現在の電子政府推奨暗号リストの構成

(1) 電子政府推奨暗号リスト

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**である暗号技術リスト。電子政府構築(政府調達)の際には当該技術の利用を推奨します(現リストと同等の位置づけ)。ここに登録される技術は国際標準化機関等により、標準化されていることが望まれます。

(2) 推奨候補暗号リスト

CRYPTREC により安全性が確認されているが、**市場において利用実績が十分でない普及段階**にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類されます。電子政府構築(政府調達)の際には当該技術も利用することができます。

本リストに登録された技術は、一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リストに登録されます。また、利用実績が十分であると認められなかった場合にはここから削除されます。危殆化が生じた暗号技術については、随時ここから削除されます。

電子政府推奨暗号・応募暗号一覧

技術分類		電子政府推奨暗号リスト（平成15年2月20日版）		2次評価対象の 今回の応募暗号	今回の事務局選出暗号
		前回の応募暗号	前回の事務局選出暗号		
公開鍵暗号	署名	なし	DSA ECDSA RSASSA-PKCS1-v1_5 RSA-PSS		
	守秘	なし	RSA-OAEP RSAES-PKCS1-v1_5(注1)		
	鍵共有	PSEC-KEM(注2)	DH ECDH		
共通鍵暗号	64ビットブロック暗号(注3)	CIPHERUNICORN-E Hierocrypt-L1 MISTY1	3-key Triple DES(注4)		
	128ビットブロック暗号	Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000	AES	CLEFIA	
	ストリーム暗号	MUGI MULTI-S01	128-bit RC4(注5)	Enocoro KCipher-2	
その他	ハッシュ関数	なし	RIPEMD-160(注6) SHA-1(注6) SHA-256 SHA-384 SHA-512		
	擬似乱数生成系	なし	（省略）(注7)		
	MAC			PC-MAC-AES	CBC-MAC・CMAC・HMAC CBC・CTR・CFB OFB・CCM・GCM
	エンティティ認証			なし	ISO/IEC 9798-2 ISO/IEC 9798-3 ISO/IEC 9798-4

ところで・・・・

こんなにたくさんの

暗号アルゴリズムが本当にいるの？

きちんと調べてみましょう

- 「暗号モジュールの市場動向等に関する調査研究」
  - 調査協力企業数：１１０社・３７２製品（回収率４９．６％）
- 国内外の主要暗号製品ベンダ・システムインテグレータを主な対象とした実態調査アンケート

CRYPTREC Report 2010 暗号運用委員会報告書付録2より

  - 暗号搭載製品の開発製造、情報システムの構築等における暗号利用（選択プロセス）に関する実態を把握

ベンダ（全39社、67プロダクト）

凸版印刷株式会社
オーセンテック株式会社
キヤノン株式会社
KDDI株式会社
大日本印刷株式会社
三菱電機インフォメーションシステムズ株式会社
日本電気株式会社
株式会社PFU
ルネサスエレクトロニクス株式会社
EMCジャパン株式会社
一般社団法人 Mozilla Japan
インフィニオンテクノロジーズジャパン株式会社
株式会社リコー
株式会社東芝
富士ゼロックス株式会社
富士通株式会社
ソニー株式会社
アマノビジネスソリューションズ株式会社
株式会社ACCESS
ヤマハ株式会社
マイクロソフト株式会社
セコムトラストシステムズ株式会社
日本ベリサイン株式会社
株式会社バッファロー
タレスジャパン株式会社
シスコシステムズ合同会社
インテル株式会社

他、全39社・67プロダクト

注：応募ベンダ　：**応募企業の事業部門**及び応募企業の出資率が50%超のグループ企業
　　非応募ベンダ：応募ベンダ以外の企業

SIer（全8社、11システム）

三菱電機株式会社
東芝ソリューション株式会社
新日鉄ソリューションズ株式会社
三菱電機インフォメーションシステムズ株式会社
株式会社日立製作所

他、全8社・11システム

政府機関

総務省

他、全4府省・6システム

応募者（応募企業の研究開発部門）

株式会社ローレルインテリジェントシステムズ
三菱電機株式会社
株式会社富士通研究所
日本電信電話株式会社
ソニー株式会社
株式会社日立製作所
KDDI株式会社

他、全9社

電子政府推奨暗号の実装率（2009年度調査）

- 「暗号モジュールの市場動向等に関する調査研究」

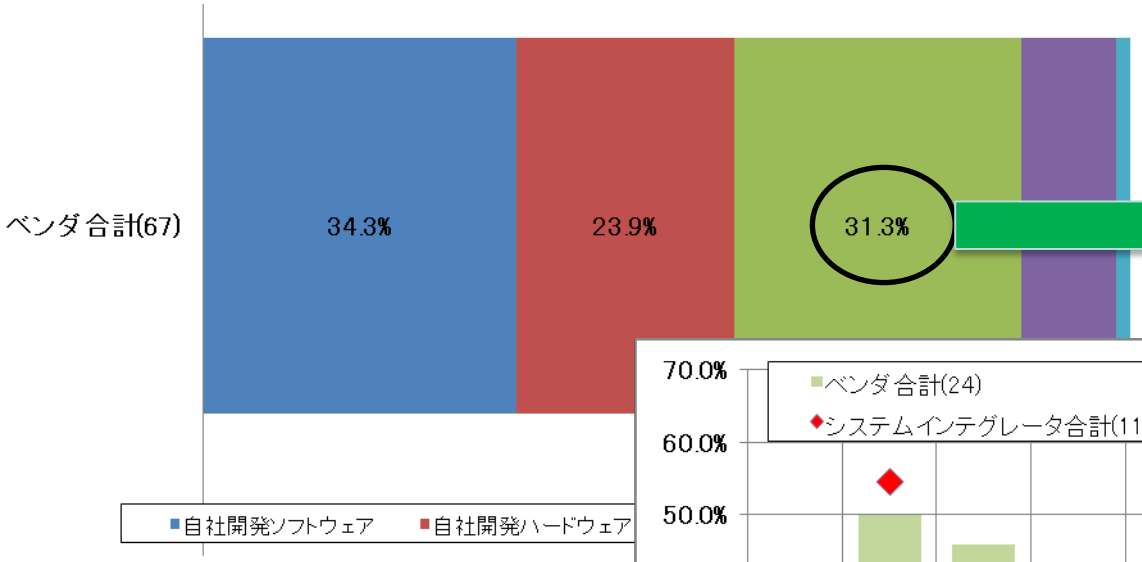
http://www.meti.go.jp/meti_lib/report/2010fy01/E001139.pdf

暗号分類	暗号アルゴリズム	2003年度実装率%（製品数）	2009年度実装率%（製品数）	増減
128ビットブロック暗号	AES	**24.9% (62)**	**72.5% (222)**	**+47.6%**
	Camellia	**0% (0)**	**14.4% (44)**	**+14.4%**
	CIPHERUNICORN-A	**0% (0)**	**0.3% (1)**	**+0.3%**
	Hierocrypt-3	**0% (0)**	**0% (0)**	**+0%**
	SC2000	**0.4% (1)**	**0.3% (1)**	**△0.1%**
64ビットブロック暗号	CIPHERUNICORN-E	**0% (0)**	**0.3% (1)**	**+0.3%**
	Hierocrypt-L1	**0% (0)**	**0% (0)**	**+0%**
	MISTY1	**4.0% (10)**	**2.0% (6)**	**△2.0%**
	TDES	**45.0% (112)**	**47.4% (145)**	**+2.4%**
ストリーム暗号	MUGI	**0% (0)**	**1.0% (3)**	**+1.0%**
	MULTI-S01	**0% (0)**	**0% (0)**	**+0%**
	RC4 (128bit)	**14.1% (35)**	**5.9% (18)**	**△8.2%**

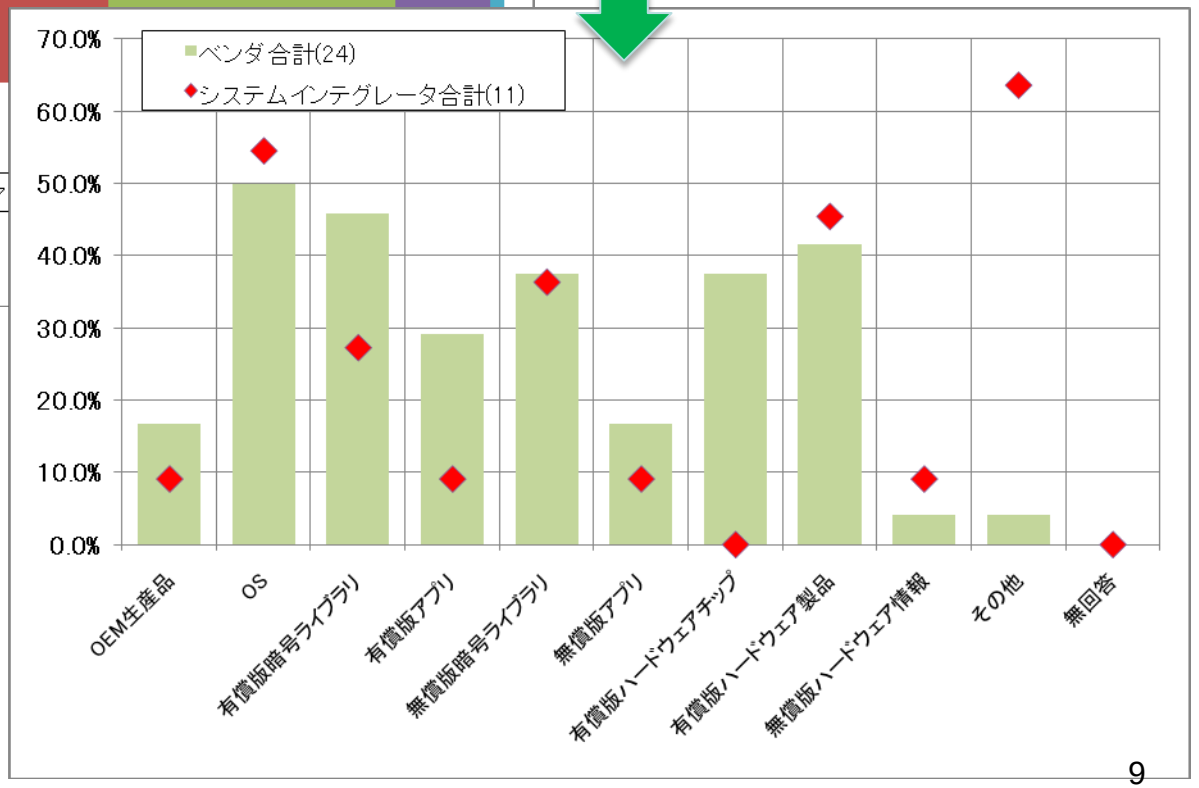
暗号分類	暗号アルゴリズム	2003年度実装率%（製品数）	2009年度実装率%（製品数）	増減
公開鍵署名	DSA	**13.7% (34)**	**14.1% (43)**	**+0.4%**
	ECDSA	**4.8% (12)**	**9.5% (29)**	**+4.7%**
	RSASSA-PKCS1-v1_5	**29.3% (73)**	**34.6% (106)**	**N/A**
	RSA-PSS	**7.6% (19)**		
	RSAES-PKCS1-v1_5	**16.1% (40)**		
	RSA-OAEP	**9.2% (23)**		
ハッシュ関数	RIPEMD-160	**2.0% (5)**	**9.2% (28)**	**+7.2%**
	SHA-1	**49.4% (123)**	**28.8% (88)**	**△20.6%**
	SHA-256	**4.4% (11)**	**14.4% (44)**	**+10.0%**
	SHA-384	**3.2% (8)**	**7.2% (22)**	**+4.0%**
	SHA-512	**3.2% (8)**	**9.2% (28)**	**+6.0%**
鍵共有	DH	**27.7% (69)**	**22.2% (68)**	**△5.5%**
	ECDH	**2.0% (5)**	**7.5% (23)**	**+5.5%**
	PSEC-KEM	**0% (0)**	**0.3% (1)**	**+0.3%**

アンケート結果 (1)

暗号搭載製品で利用する暗号アルゴリズムをどのような方法で実現しているか？

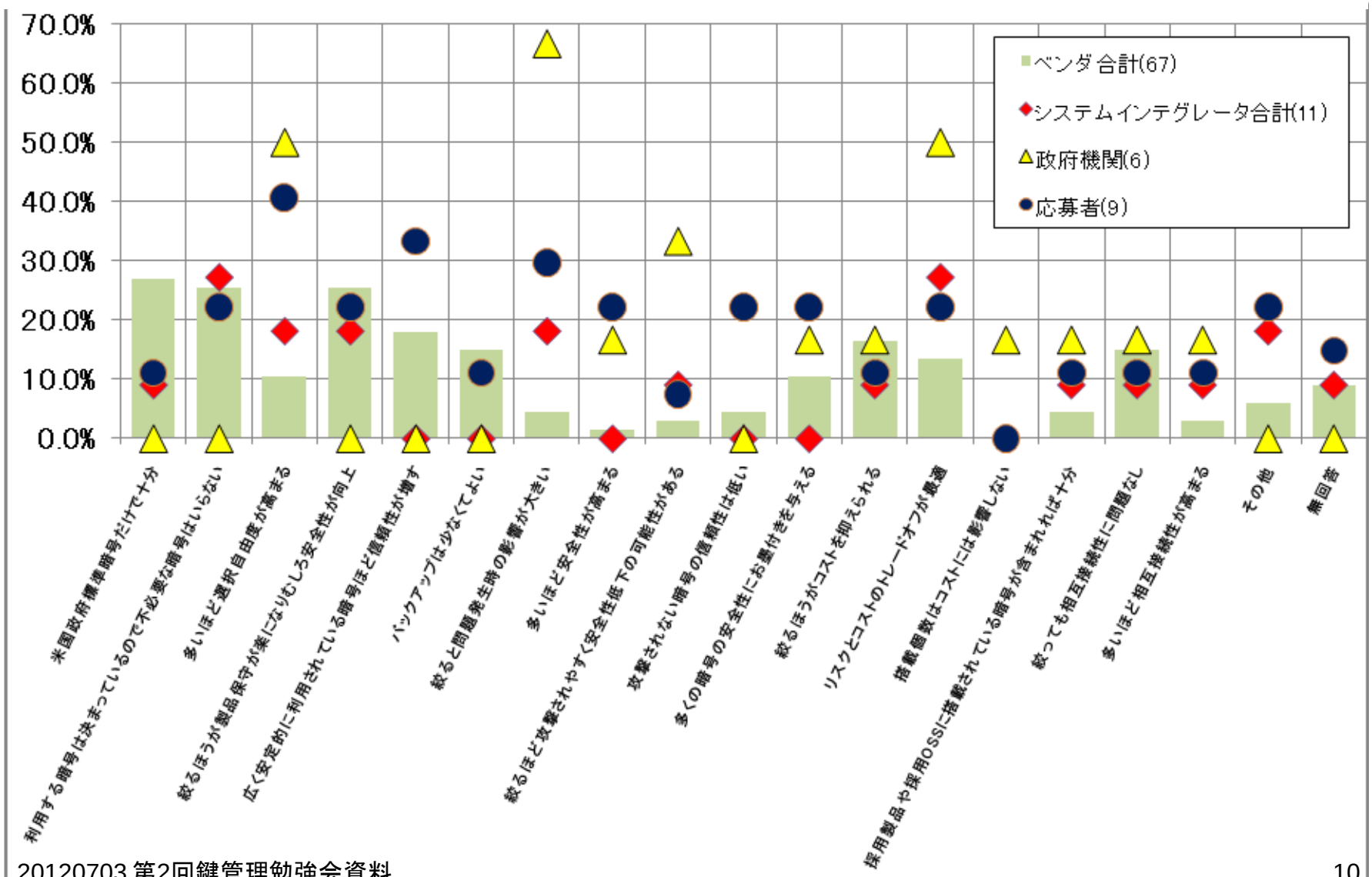


他社製品を利用している場合、どのような他社製品に搭載されている暗号アルゴリズムを利用しているか？



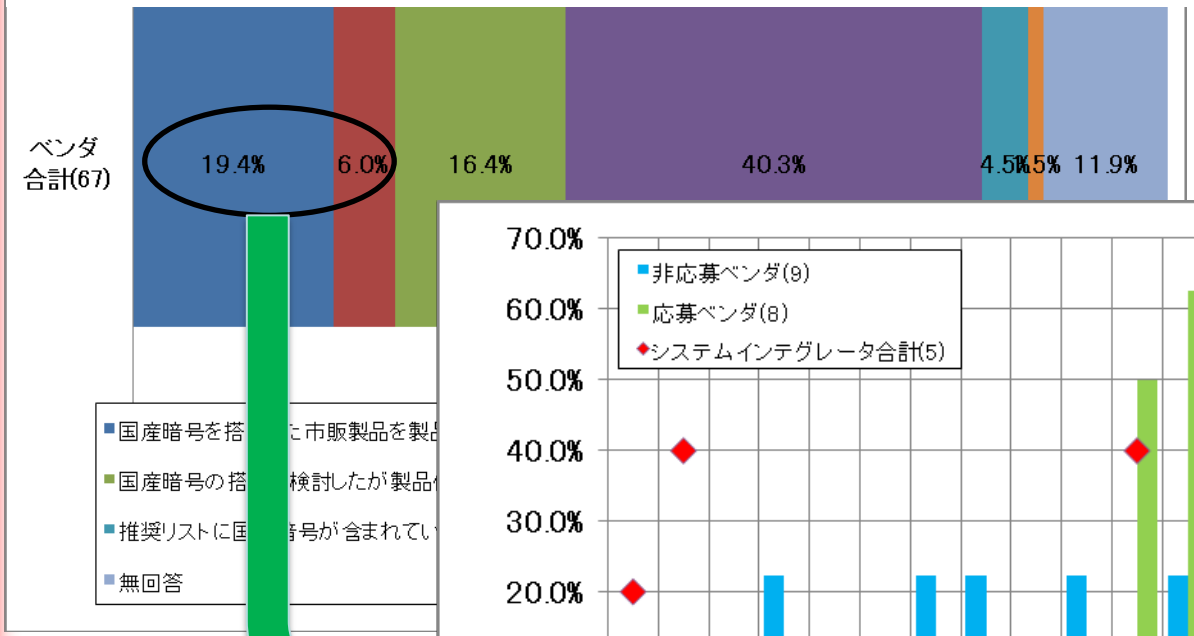
アンケート結果 (2)

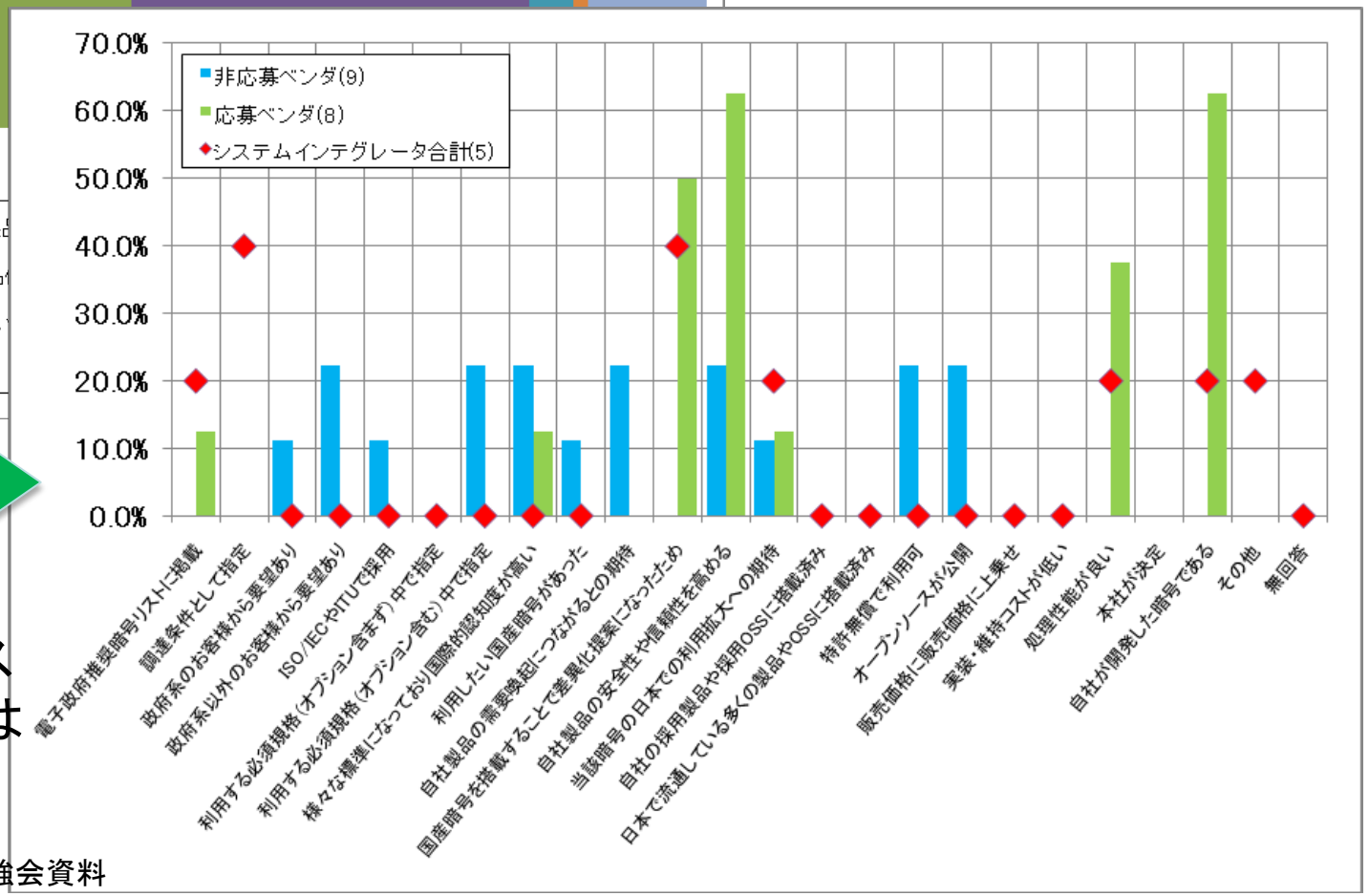
（推奨暗号リストに掲載されるアルゴリズムの個数はどの程度がよいかの質問に続いて）
なぜそのように考えるのか？



アンケート結果 (3)

電子政府推奨暗号である国産暗号を搭載した製品を出荷した実績があるか？

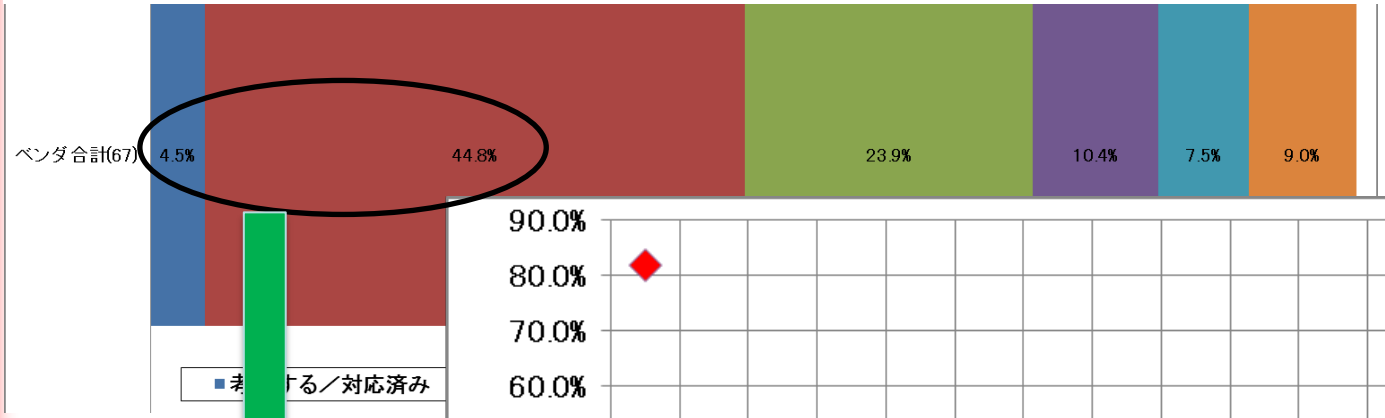




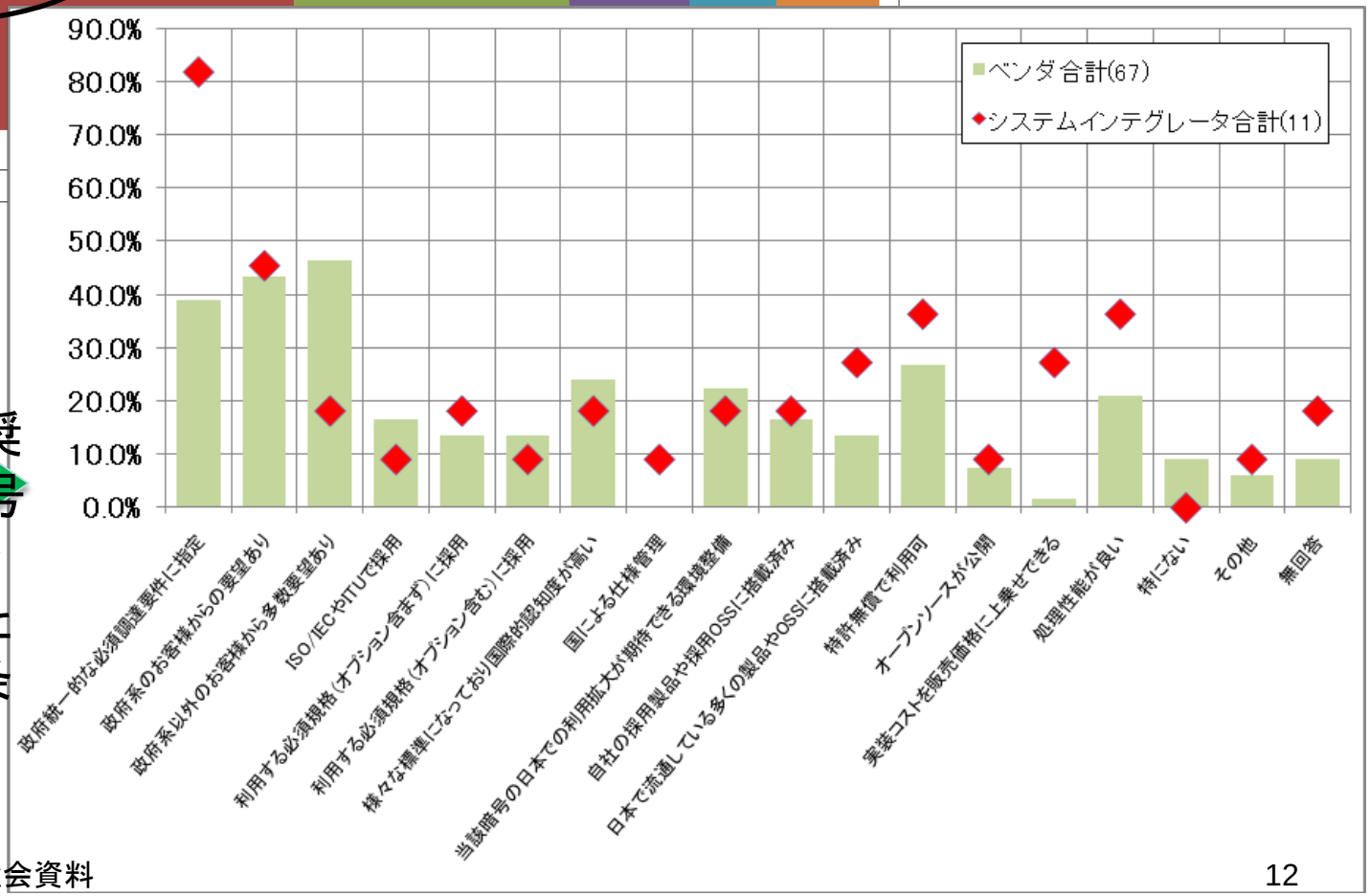
電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用したのはなぜか？

アンケート結果 (4)

今後、電子政府推奨暗号である国産暗号を搭載するつもりがあるか？



今後、電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用するために必要と考える条件は何か？



推奨暗号リストの考え方の明確化に向けて(1)

- 電子政府推奨暗号リストに「何を求める」のか

  ⇒　それぞれの設定意図を参考に4つのシナリオを設

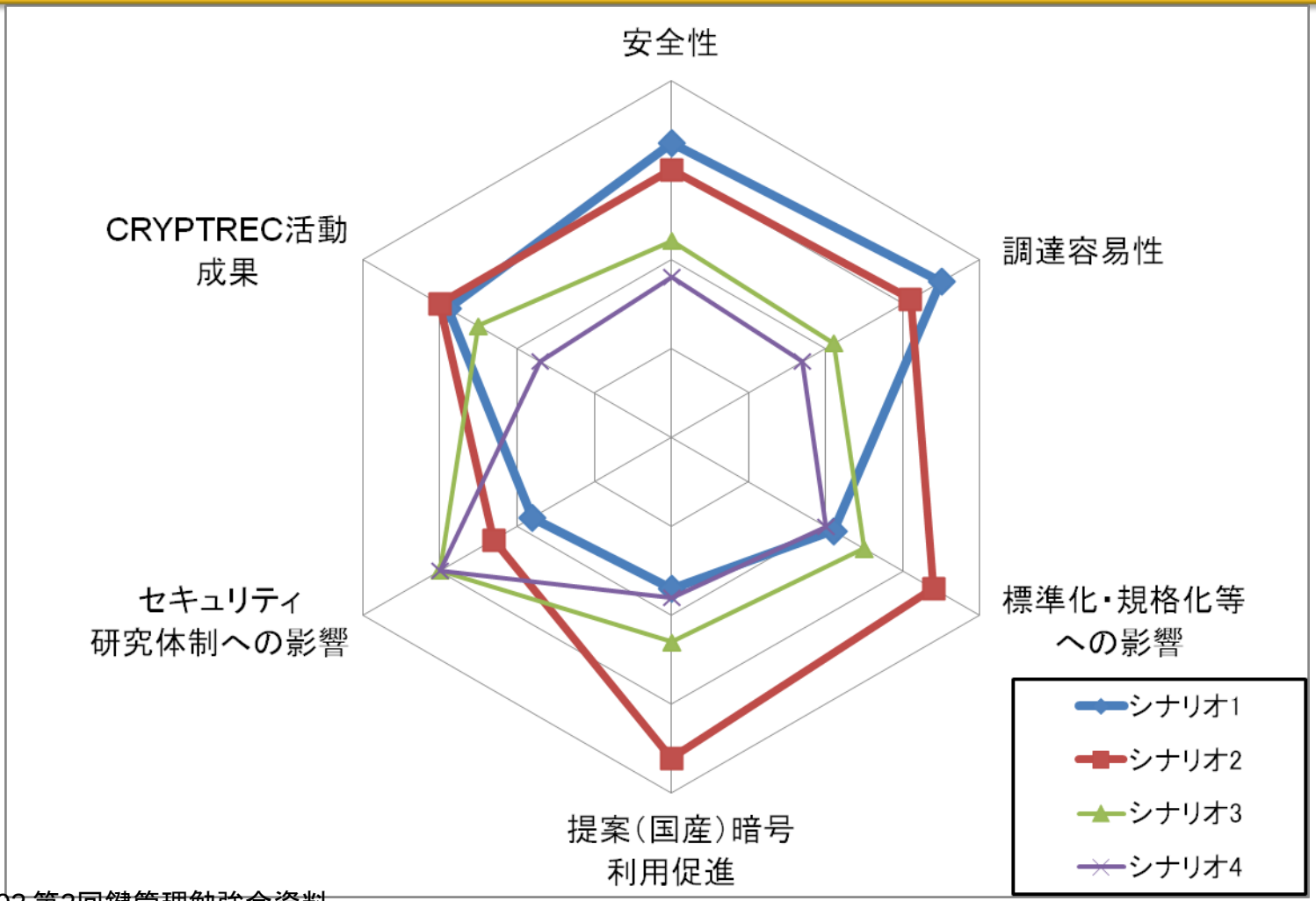
シナリオ			推奨リスト例	シナリオの設定意図
No. 1	実際に利用されている暗号だけを電子政府推奨暗号に選定	実際に利用されている暗号だけを電子政府推奨暗号リストに限定することでリストの有効性を高めるために**「現状の調達容易性（利用実績）」を主たる判断材料**としたうえで、有力な標準化規格で必須実装に指定されているなどの「純技術的なその他要件」を考慮	米国政府標準暗号のみ	調達容易性の観点から、特定の暗号アルゴリズムが政府システムにおいて広く利用されている実態を考慮
No. 2	国際標準化・製品化促進の手段として電子政府推奨暗号リストを活用	「安全性」、「現状の調達容易性（利用実績）」、「将来的な調達容易性（利用実績）」の見通しを踏まえつつ、電子政府推奨暗号リストの掲載個数を限定したうえで、提案暗号の普及展開をどのように進めるべきかといった**「非技術的なその他要件」を最大限加味**	米国政府標準暗号＋国産暗号（1 or 少数）	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 提案暗号に対する国としてのバックアップの明確化

推奨暗号リストの考え方の明確化に向けて(2)

シナリオ			推奨リスト例	シナリオの設定意図
No. 3	一定期間経過後の利用実績不振による電子政府推奨暗号からの降格	当初は電子政府推奨暗号リスト入りさせるが、一定期間経過後の普及状況を厳格に判定する**「将来的な調達容易性（利用実績）」を重要視**	短期的にはシナリオNo. 4。中長期的にはシナリオNo. 1, 2, 4のいずれにもなりうる	提案暗号の普及展開を強力に実施するモチベーションを応募企業に持たせる一方、一定期間経過後の普及展開が思わしくない提案暗号には電子政府推奨暗号リストから降格してもらうルールを新たに導入
No. 4	政府調達の選択肢としての提示	電子政府推奨暗号リストと推奨候補リストとの区分は**「安全性」を主たる判断基準**として行うことにより、現状とほぼ同様の構成	現状とほぼ同様	「調達容易性」を判断することは難しいうえ電子政府推奨暗号リストの掲載個数を削減することによる効果も定かではない点、ならびに暗号研究体制に与えるマイナス影響を考慮

評価点比較のまとめ

「CRYPTREC Report 2010 暗号運用委員会報告書」をご覧ください　(http://www.cryptrec.go.jp/report.html)



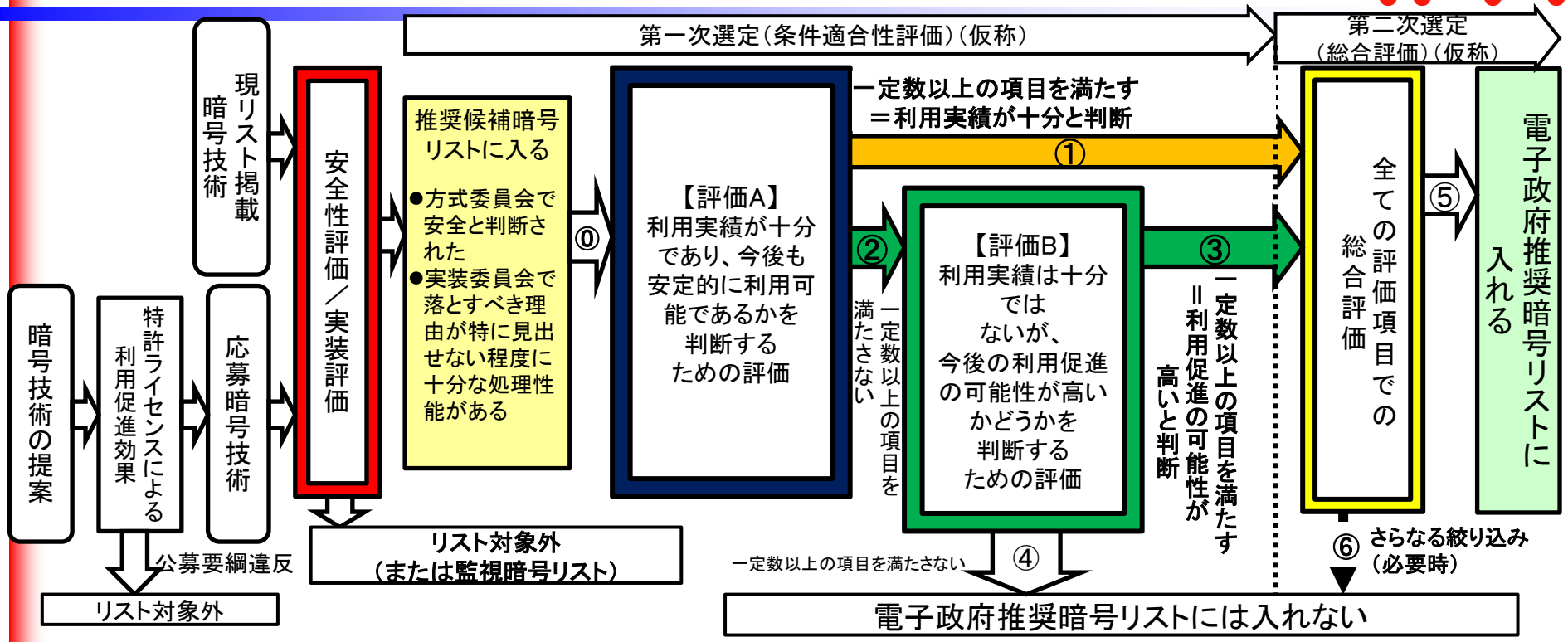
暗号技術検討会の審議の結果

- 2010年度暗号運用委員会の検討において、4つの電子政府推奨暗号リストの設定意図を設定し、効果を評価
  - 実施時のメリット・デメリット・留意点を参考に評価点を採点

- 暗号技術検討会での審議の結果、電子政府推奨暗号リスト改訂にあたっては以下の方針で推進するよう答申

No.2	**国際標準化・製品化促進の手段**として電子政府推奨暗号リストを活用	**米国政府標準暗号＋国産暗号（1 or 少数）**	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 **提案暗号に対する国としてのバックアップの明確化**

明示的な選考基準で絞り込みを行います



【ルート①】 すでに現状の利用実績が十分に高く、かつ将来的な安全性にも十分な余裕度があって今後も安定して利用できる見込みがある暗号技術

【ルート②③】 現状の利用実績は十分に高いとは言えないものの以下の条件すべてを満たす暗号技術

- 最も高い安全性を有するものと同等かそれ以上の安全性を有すると評価される
- 普及展開支援によって国際標準化・製品化促進が図られると期待できる根拠がある
- 普及展開支援によって将来的な利用実績が十分に高くなると期待できる根拠がある

選定ルールのフレームワーク（詳細）

第一次選定（条件適合性評価）（仮称）

第二次選定
（総合評価）（仮称）

推奨候補暗号リストに入る

- 方式委員会で安全と判断された
- 実装委員会で落とすべき理由が特に見出せない程度に十分な処理性能がある

⓪

【評価A】
利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価

- 市販製品での採用実績（販売会社数・種類・種別）
- オープンソースプロジェクトでの採用実績
- 政府系システム規格での採用実績
- 国際的な民間メジャー規格での採用実績

一定数以上の項目を満たす
＝利用実績が十分と判断

①

②
一定数以上の項目を満たさない

【評価B】
利用実績は十分ではないが、今後の利用促進の可能性が高いかどうかを判断するための評価

- 市販製品での採用実績（販売会社数・種類・種別）
- オープンソースプロジェクトでの採用実績
- 政府系システム規格での採用実績
- 国際的な民間メジャー規格での採用実績
- 利用促進を図る際の障壁の除去
- 標準化・規格化の促進を図るハードルの低さ
- 実装コスト低減を図るハードルの低さ
- 調達コスト低減を図るハードルの低さ

③
一定数以上の項目を満たす
＝利用促進の可能性が高いと判断

全ての評価項目での総合評価

⑤

電子政府推奨暗号リストに入れる

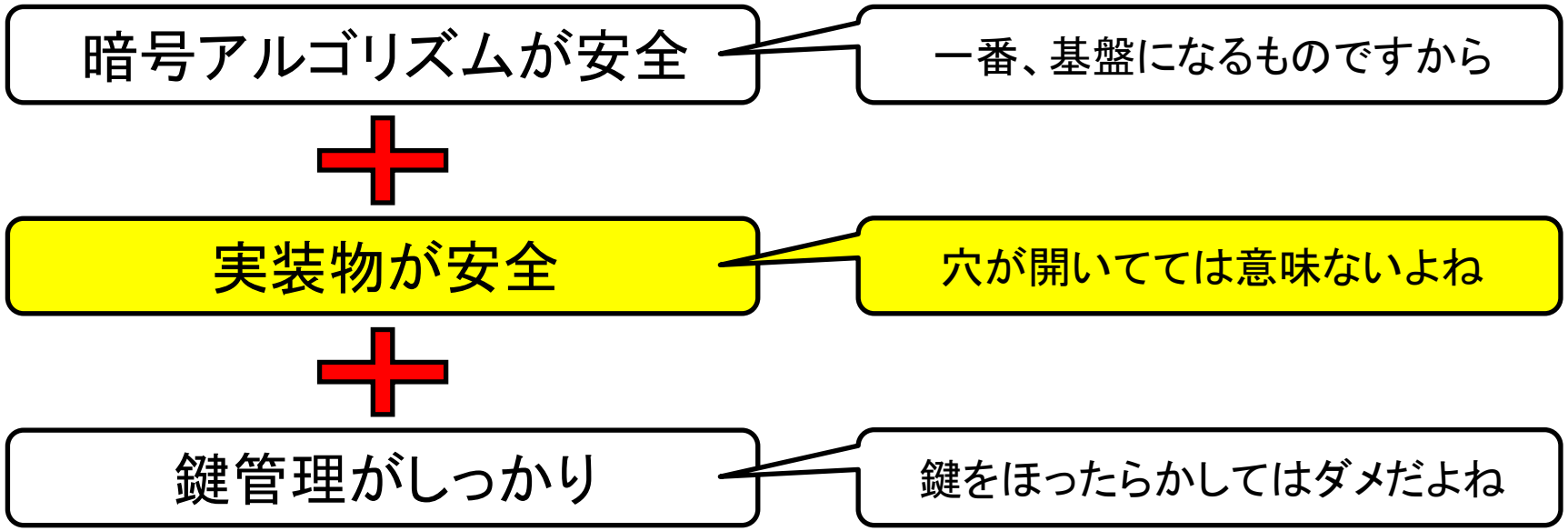
⑥ さらなる絞り込み（必要時）

一定数以上の項目を満たさない

④

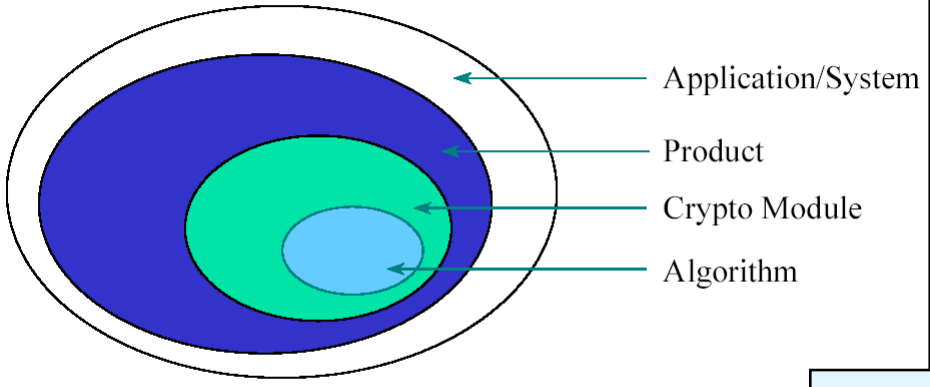
電子政府推奨暗号リストには入れない

せっかく絞り込んだとして・・・・
本当に使われるようになるんだろうか？
認証制度への対応不備が足を引っ張らないか？



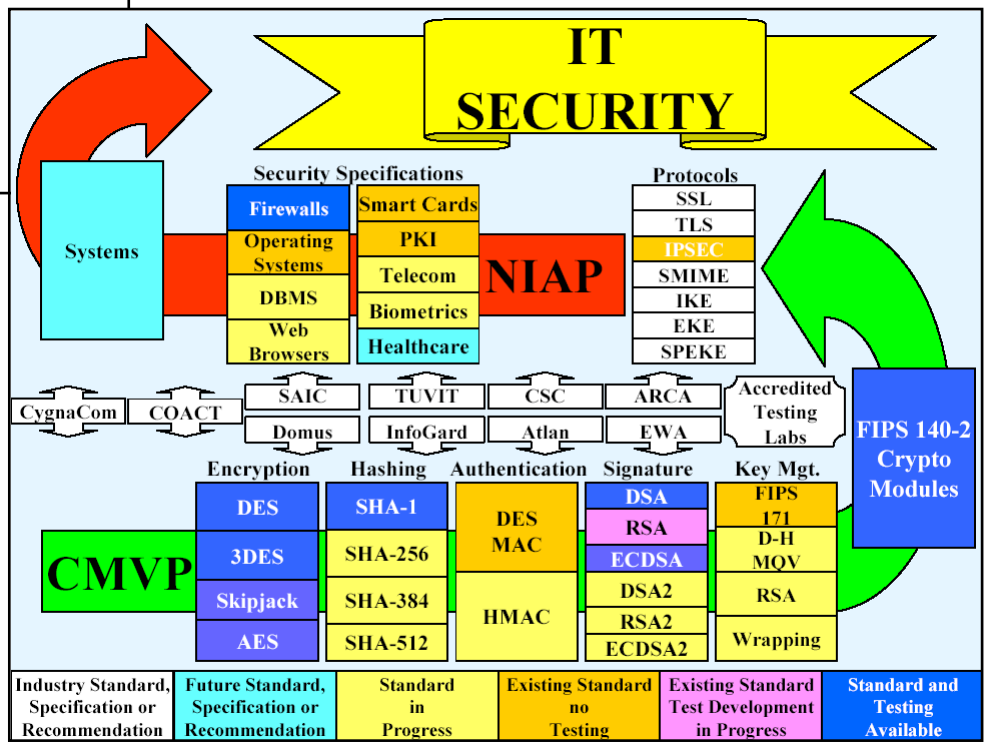
米国では1990年代からすでに・・・

Testing - Algorithms to Systems



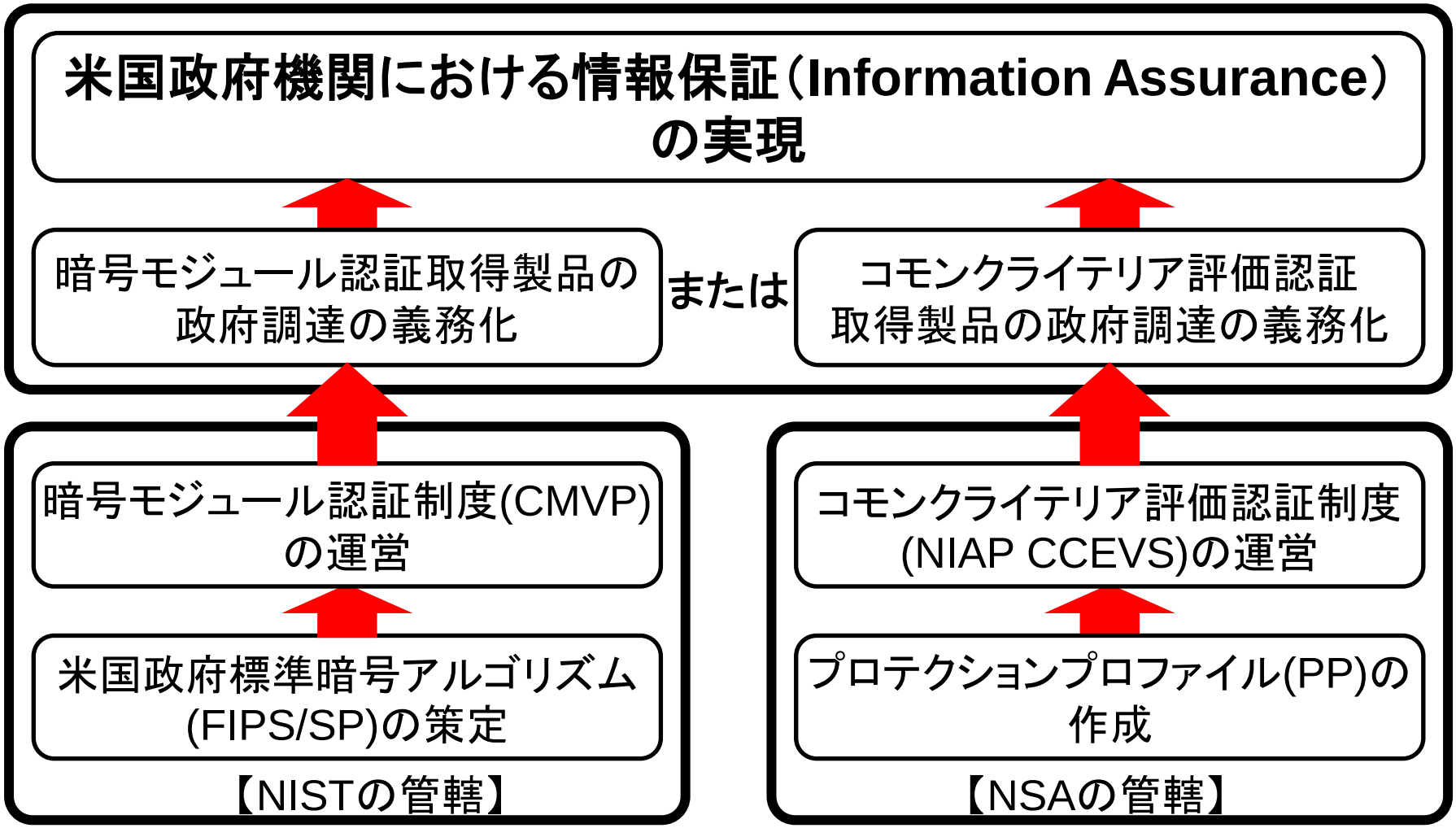
Level	Example	Specification
Application	Air Traffic Control	?
Product	Firewall	Common Criteria
Security Module	Crypto Module	FIPS 140-2
Algorithm	AES	FIPS 197

CMVP Conference 2002の資料から



アルゴリズムから政府調達まで管轄

- 国家安全保障通信・情報システムセキュリティ委員会（議長：国防総省）による**国家情報保証調達ポリシー**



英国政府の取り組み

IPA

- 組織

政府通信本部(GCHQ)

通信電子セキュリティグループ(CESG)

- 暗号アルゴリズムから政府調達まで管轄

英国政府機関における情報保証の実現

CAPS認証取得製品の政府調達の義務化

CAPS認証制度の運営

CESG承認暗号アルゴリズム（非公開）の策定

【CESGの管轄】

オープンな仕様に基づく電子政府システム

電子政府相互接続フレームワーク(eGIF)に準拠

米国政府標準暗号主体

※ 政府情報区分の“Classified”に入らないセンシティブ情報を取り扱う場合のみに限定

中国政府の取り組み

- 組織
  - 国家情報化指導グループ
  - 情報セキュリティ国家重点実験室
  - 国家情報センター
  - 公安部情報安全等級保護評価センター
  - 国家コンピュータネットワーク応急処理技術調整センター
- 中国の暗号アルゴリズム
  - SM2 (楕円暗号), SM3 (ハッシュ関数), SMS4 (ブロック暗号)
- 戦略的に自国標準暗号を推進
  - 標準化
    - 無線LAN: WAPI
    - TCG (Trusted Computing Group): Trusted Cryptography Modules (TCM; TPM (Trusted Platform Module)の中国版)
    - 中国強制製品認証制度（CCC：China Compulsony Certification）
  - 市場形成
    - 中国市場規模を全面的にアピール
    - 途上国（特にアフリカ）への通信インフラ輸出とセット

中国国内でのWi-Fi解禁とセット

ところで、日本では？

- 「政府機関の情報セキュリティ対策における政府機関統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」が改定

昨年度まで	今年度から
基本遵守事項 ● 必須として実施すべき対策事項を列挙	遵守事項 ● 必須として実施すべき対策事項を列挙 ● 対策候補案についての実施の必要性の有無を検討し、必要と認められるときに追加で実施
強化遵守事項 ● （対策事項についての実施の必要性の有無を検討し、）必要と認められるときに、追加で選択実施すべき対策事項を列挙	

ところで、日本では？

■ 暗号関係の遵守事項

- CC認証製品の調達要件（管理基準1.5.1.1）
  - IT セキュリティ評価及び認証制度に基づく認証取得製品分野リストを参照し、必要があると認めた場合には、要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、当該製品を情報システムの構成要素として選択

認証取得製品分野リスト

製品分野名	製品分野定義
スマートカード（IC カード）	プラスチック製カード等にIC チップを埋め込み、情報を記録できるようにした製品
ファイアウォール	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品
OS（サーバOS に限る）	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア
デジタル複合機（MFP）	プリンタ機能を標準で有しスキャナ、FAX、コピーのいずれか2つ以上の機能を標準で装備している製品
不正侵入検知/防止システム（IDS/IPS）	ネットワークやシステムの稼動状況を監視し、組織内のコンピューターネットワークへの外部からの侵入を報告、防御する製品
データベース管理システム（DBMS）	共有データとしてのデータベースを管理し、データに対するアクセス要求に応える製品

ところで、日本では？

- 暗号関係の遵守事項
  - 暗号アルゴリズムの調達要件（管理基準1.5.2.5）
    - 電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用
  - 暗号・JCMVP認証製品の調達要件（技術基準2.2.1.6 ）
    - 以下の各措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずる
      - （ア）暗号モジュールの交換可能なコンポーネント化による構成
      - （イ）複数のアルゴリズムを選択可能にする構成
      - （ウ）選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、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及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択
      - （エ）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の耐タンパー性を有する暗号モジュールへの格納

CC認証の仕組み

専門知識を持つ第三者による客観的なセキュリティ評価の必要性

セキュリティ機能に求められること

適切性
情報資産を守るために必要十分な機能を持っているか

正確性
機能は正しく実装され確実に動作するのか

- 保護資産の洗い出し
- 脅威等（セキュリティ課題）の洗い出し
- セキュリティ課題への対策方針の決定
- 対策方針を満たすセキュリティ機能要件の決定

セキュリティターゲット

ソースコード
設計書
機能仕様

セキュリティ機能の正確性をライフサイクル全体として保証するための情報

EAL: 保証レベル
Evaluation Assurance Level

- 特定分野の製品について必要とされる典型的なセキュリティ要件、環境などを抽象的なレベルで記述した要求仕様書（STのテンプレートのようなもの）

プロテクションプロファイル

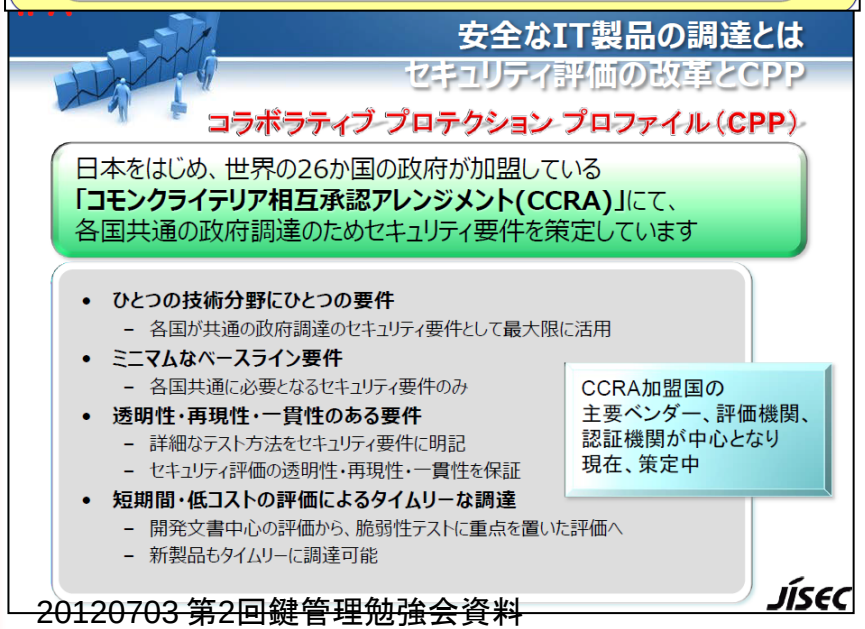
保証範囲

EAL1	機能仕様（外部I/F）、利用者ガイダンス 等
EAL2	内部設計、配付手続き、開発者テスト、開発資料からの脆弱性分析 等
EAL3	開発現場のセキュリティ、開発者テストの深さ（詳細度）分析 等
EAL4	ソースコード、開発環境（ツール） 等
EAL5	準形式的（フローチャート等の図式を用いた曖昧ではない）設計資料 等
EAL6,7	各国の制度による （軍需品など特別な用途のため）

CCRAにおける相互承認の対象

評価方法の規定（CEM）

CCRAの大規模変革

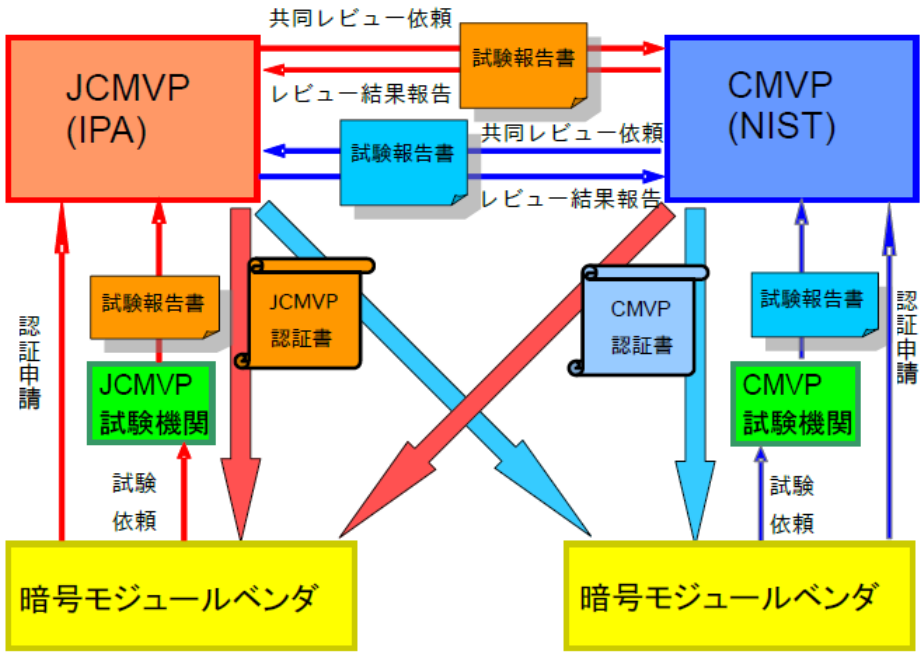


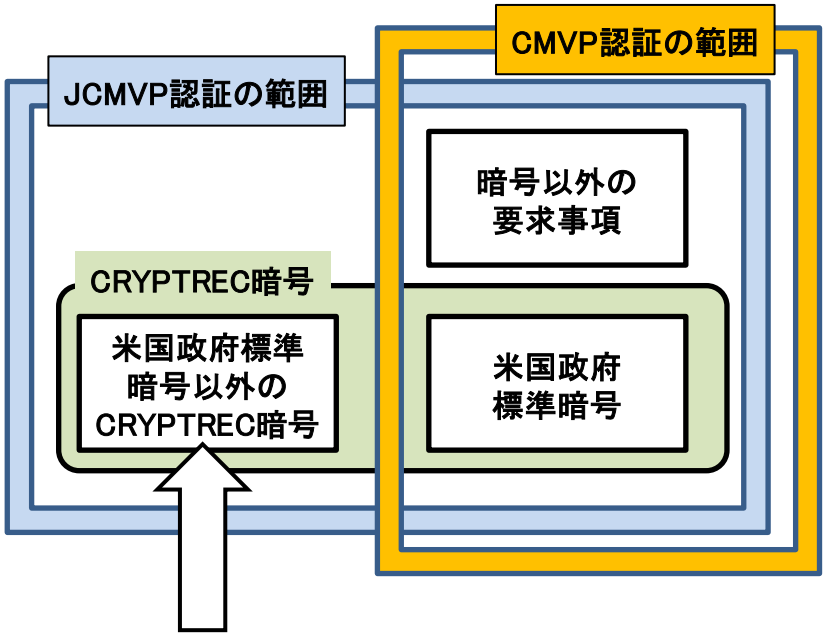
暗号アルゴリズムの統一規定なし

特定の暗号アルゴリズムが指定されているようなCPPもいくつか作られ始めている

これに国産暗号が入っていけないとCC認証でも圧倒的に不利な状況に

CMVP/JCMVPの共同認証





この部分だけが差分となると・・・

共同認証を JCMVP に申請した場合の流れ

共同認証を CMVP に申請した場合の流れ

認証書の発行。共同認証をどちらに申請しても両方の認証書が発行される

ちなみに認証製品数は・・・

CMVP認証（1995/10/12～）：1752製品
（1995/10/12～2000/12/31: 130製品）
JCMVP認証（2007/3/30～）： 17製品

まとめにかえて

「技術力が高い」ことを売りにして世界を席巻していた
家電業界は今や青色吐息・・・

↓

「コモディティ化した（＝標準化が進んだ）技術」では
「技術力」とは違う力学でビジネスが進んでいく

↓

認証制度の強化・標準化の進展に伴い、
暗号アルゴリズムも急速に「コモディティ化」が進行中

↓

早急に国としての暗号アルゴリズムの出口戦略を
定まらないと、国産暗号全滅の憂き目にも・・・
～コモディティ化に乗り遅れた暗号アルゴリズムは使われない～