

# 第 1 回 CRYPTREC の在り方に関する検討グループ

日時：平成 27 年 6 月 3 日(水) 10:00～12:00

場所：経済産業省別館 1 階 101-2 共用会議室

## 議 事 次 第

### 1. 開 会

### 2. 議 事

- (1) 「CRYPTREC の在り方に関する検討グループ」開催要綱について
- (2) CRYPTREC に関する現状について
- (3) その他

### 3. 閉 会

(資料番号)	(資料名)
資料 1	「CRYPTREC の在り方に関する検討グループ」開催要綱(案)
資料 2	CRYPTREC に関する現状について
参考資料 1	暗号技術検討会における小グループの設置について
参考資料 2	CRYPTREC の在り方に関する検討グループ 構成員・オブザーバ名簿

## 「CRYPTREC の在り方に関する検討グループ」開催要綱(案)

### 1 目的

暗号技術を取り巻く環境やサイバーセキュリティ基本法の施行といった社会情勢の変化を鑑み、一般社会における適切な暗号技術の利用促進に向けた日本の暗号政策に関する議論を踏まえ、「暗号技術検討会」の下に設置される検討グループとして、今後の CRYPTREC の活動内容及び対象範囲について集中的な検討を行うことを目的として開催する。

### 2 名称

本会合は「CRYPTREC の在り方に関する検討グループ」と称する。

### 3 検討事項

- (1) CRYPTREC の活動内容及び対象範囲について
- (2) 暗号技術の安全性確保等に係る活動の在り方
- (3) 暗号技術の普及促進、産業振興及び人材育成に係る活動の在り方
- (4) その他、日本の暗号政策に係る事項

### 4 構成及び運営

- (1) 本会合の構成は、別紙のとおりとする。
- (2) 本会合には、座長を 1 名置く。
- (3) 座長は、構成員の互選により定める。
- (4) 座長は、本会合の議事を掌握する。
- (5) 座長は、必要に応じ、構成員以外の者の出席を求め、意見を聞くことができる。
- (6) 関係する政府機関等で、座長が特に認めた者については、オブザーバとして本会合に参加することができる。
- (7) 座長は、必要があると認めるときは電子メールによる審議を行うことができる。
- (8) その他本会合の運営に関し必要な事項は、座長が定めるところによる。

### 5 議事の公開

本会合は非公開とするが、本会合で使用した資料及び本会合の議事概要については、次の場合を除き、公開する。

- (1) 公開することにより当事者又は第三者の権利、利益や公共の利益を害するおそれがあると座長が認める場合
- (2) その他、非公開とすることが必要と座長が認める場合

## 6 スケジュール

本会合は、平成27年7月を目途に報告をまとめることとする。

## 7 事務

本会合の事務は、総務省情報流通行政局情報セキュリティ対策室及び経済産業省商務情報政策局情報セキュリティ政策室が行う。

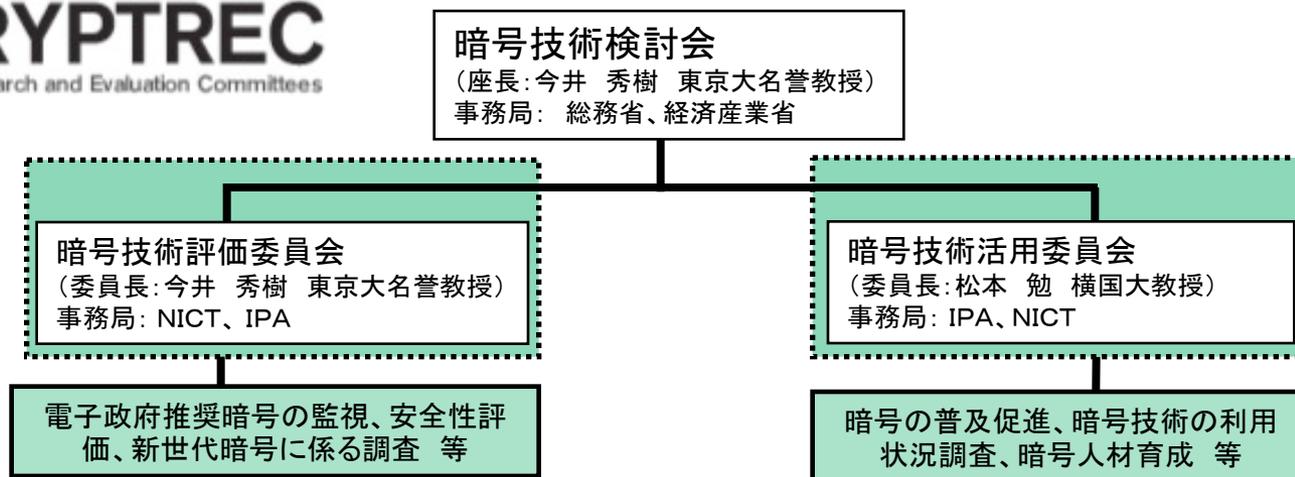
# CRYPTRECに関する現状について

平成27年6月3日

総務省情報セキュリティ対策室  
経済産業省情報セキュリティ政策室

# 1. 日本の暗号政策を巡る現状 (CRYPTRECについて)

- 必ずしも安全でない暗号アルゴリズムが乱立する中、安全な暗号の利用環境を整備するため、CRYPTRECを設立し、2003年に電子政府推奨暗号リストを策定。
- 電子政府推奨暗号リスト作成後、暗号技術の監視活動を中心に運営。
- 2013年、10年ぶりに電子政府推奨暗号リストを改定 (CRYPTREC暗号リスト)。
- リストの改定にあわせ、暗号技術検討会のもと、安全性・実装評価等の技術的な検討を行う暗号技術評価委員会及び、暗号技術の利用促進及び産業化等の検討を行う暗号技術活用委員会の2委員会体制とした。
- 事務局は、総務省、経産省、NICT、IPAの4者共同で運営。



※2014年度の体制図

# (参考) 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)

- ・ 暗号研究の進展や国内外の情勢変化を踏まえて、10年ぶりにリスト改定を実施。2013年3月に総務省・経済産業省による共同発表。
- ・ 2015年3月、注釈の一部を変更(注10の128-bit RC4)

## 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

技術分類		名称	
公開鍵暗号	署名	DSA	
		ECDSA	
		RSA-PSS <sup>(注1)</sup>	
		RSASSA-PKCS1-v1_5 <sup>(注1)</sup>	
	守秘	RSA-OAEP <sup>(注1)</sup>	
鍵共有	DH		
	ECDH		
共通鍵暗号	64ビットブロック暗号 <sup>(注2)</sup>	3-key Triple DES <sup>(注3)</sup>	
	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 <sup>(注4)</sup>			
メッセージ認証コード		CMAC HMAC	
エンティティ認証		ISO/IEC 9798-2 ISO/IEC 9798-3	

技術分類		名称	
公開鍵暗号	署名	該当なし	
	守秘	該当なし	
	鍵共有	PSEC-KEM <sup>(注5)</sup>	
共通鍵暗号	64ビットブロック暗号 <sup>(注6)</sup>	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
	ハッシュ関数		
	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
	エンティティ認証		ISO/IEC 9798-4

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5 <sup>(注8)</sup> <sup>(注9)</sup>
	鍵共有	該当なし
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	該当なし
	ストリーム暗号	128-bit RC4 <sup>(注10)</sup>
ハッシュ関数		RIPEND-160 SHA-1 <sup>(注8)</sup>
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 <sup>(注11)</sup>
	エンティティ認証	該当なし

(注1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1 及びRSA1024 に係る移行指針」(平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定)を踏まえて利用すること。  
[http://www.nisc.go.jp/active/general/pdf/angou\\_ikoushishin.pdf](http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf) (平成25年3月1日現在)

(注2) より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。

(注3) 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。  
 1) NIST SP 800-67として規定されていること。  
 2) デファクトスタンダードとしての位置を保っていること。

(注4) 初期化ベクトル長は96ビットを推奨する。

(注5) KEM(Key Encapsulating Mechanism) - DEM(Data Encapsulating Mechanism) 構成における利用を前提とする。

(注6) より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。

(注7) 平文サイズは64ビットの倍数に限る。

(注8) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1 及びRSA1024 に係る移行指針」(平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定)を踏まえて利用すること。  
[http://www.nisc.go.jp/active/general/pdf/angou\\_ikoushishin.pdf](http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf) (平成25年3月1日現在)

(注9) SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

(注10) 互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。

(注11) 安全性の観点から、メッセージ長を固定して利用すべきである。

# (参考) CRYPTRECの歴史

・これまでCRYPTRECは、担うべきタスクに合わせ、体制見直しを実施。

(2001年度～2002年度)

- 総務省技術総括審議官及び経済産業省商務情報政策局長の私的研究会に位置付け



(2003年度～2009年度)

- CMVP標準化対応の「暗号モジュール委員会」、調査テーマを決めて実務を行う「暗号技術調査WG」を新設



(2009年度～2012年度)

- リスト改定に向けて3委員会体制を発足



## 2-1. CRYPTRECの見直し(本検討グループの設置)

### CRYPTREC見直しの背景について

○CRYPTRECの基本ミッション: 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

・2013年3月の「CRYPTREC暗号リスト」への改定に伴い、CRYPTREC暗号の安全性及び信頼性確保のための調査・検討、CRYPTREC暗号リストの改定に関する調査・検討に加え、暗号技術の普及による情報セキュリティ対策の推進検討を追加。

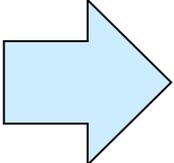
→「CRYPTREC暗号リスト」掲載の暗号アルゴリズムを念頭においた活動

○上記体制での2年間の活動により、以下の課題が顕在化

・暗号プロトコルによる通信が主流になり、様々な製品やサービスに暗号技術が当たり前前に組み込まれ、適用される領域は大幅に拡大(社会インフラ化)

→暗号ビジネスや普及促進といった観点からは、暗号アルゴリズムは差別化要因になりにくくなり、製品やサービスレベルを含めた対応が重要に。

→安全性確保という観点からは、暗号アルゴリズムを利用したプロトコルやアプリケーションの安全性評価や脆弱性対応等を含めた運用の重要性が増加。

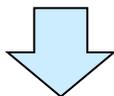


CRYPTRECのミッションを見直すための検討グループを設置

## 2-2. ミッション見直しの上で考慮すべき事項(企業)

### 暗号製品に関する市場動向(現状)

- 暗号アルゴリズムの実装先の1つである暗号ライブラリ市場は直近数年間横ばい。
- ベンダーは、暗号アルゴリズムの選択に当たり、実装性や実用化スケジュール等の観点から製品ベースで選択。(製品に使用されている暗号はデファクト暗号。)



### 方向性(たたき台)

- 安全な暗号技術の利用促進には、製品・サービスレベルで役に立つ推進策(ガイドライン等)が必要ではないか

(参考)2014年第3回暗号技術活用委員会報告(2015.3.10)

「暗号普及促進・セキュリティ産業の競争力強化に向けた課題分析と見解」 ー抜粋ー

① セキュリティ製品の視点からみる暗号アルゴリズムの選択に関する現状について

一般的なベンダは、暗号ライブラリを使う際に、(略)、暗号アルゴリズムそのものはブラックボックスとして使っているのが現実である。また、暗号アルゴリズム自身の安全性だけでなく、実装難度が低く実装しやすいかとか、実用化のスケジュールとかといったことも含めて検討することになる。

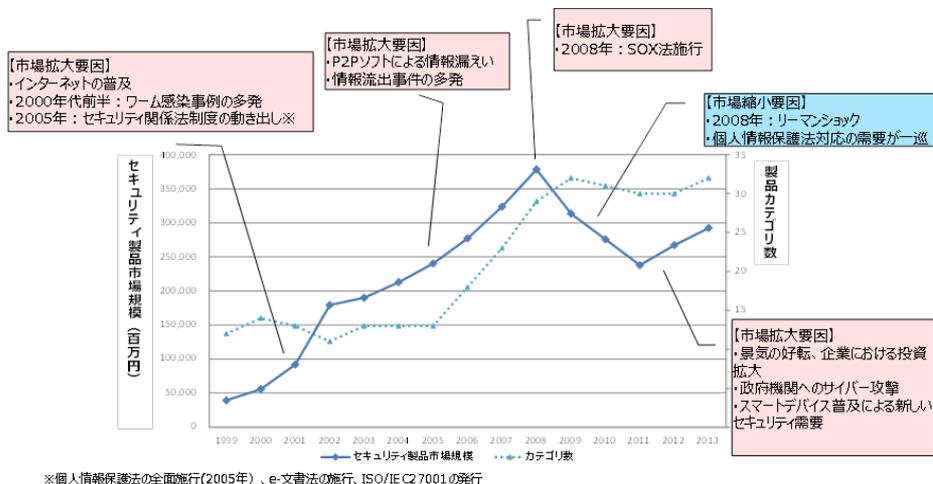
② ビジネスとしての暗号ライブラリ市場の成長鈍化について

暗号アルゴリズムの主な実装先として想定されているのは暗号ライブラリであるが、ヒアリングの結果からは、以前とは異なり暗号ライブラリ市場がビジネスとしては成立しにくくなっているのが現実である。(略)

なお、IPA「暗号利用環境調査」報告書でも、暗号ライブラリ市場の成長は2008年頃に止まり、現在横ばいになっていることが指摘されている。

# (参考)暗号に関する市場動向

## 情報セキュリティ製品市場の経年推移



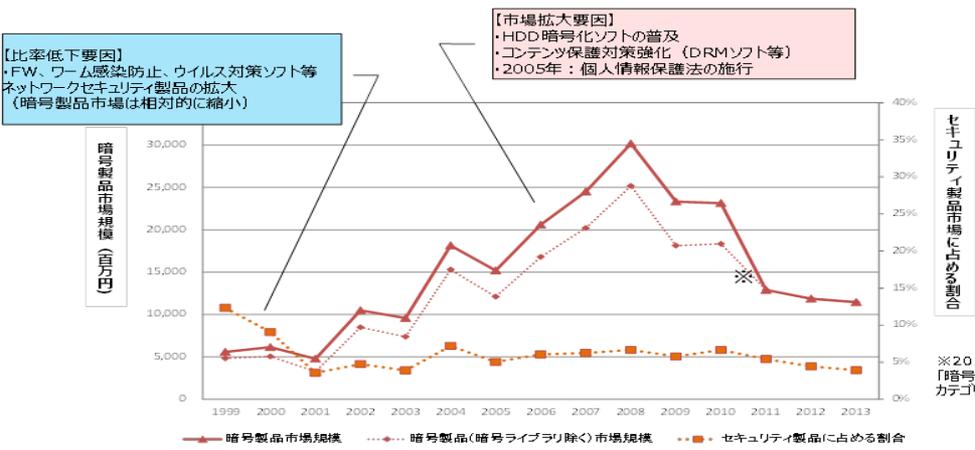
## 市場カテゴリーの分類

### <情報セキュリティ市場>

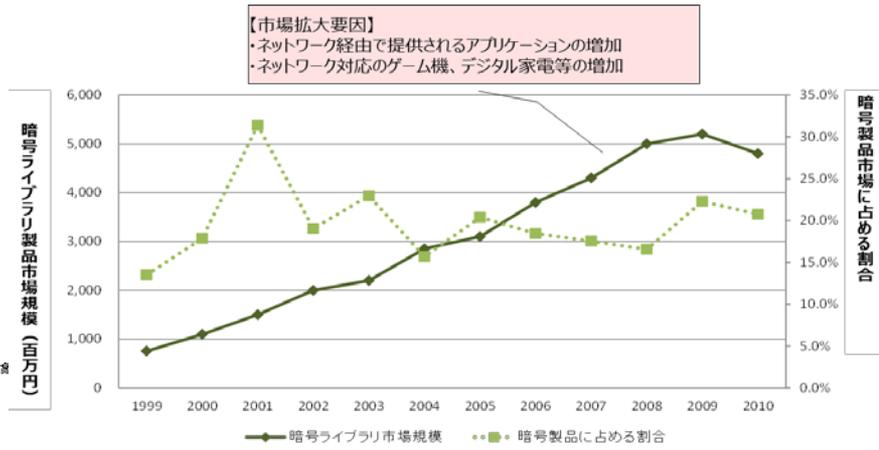
- ◆ ワンタイムパスワード
- ◆ デバイス認証ツール
- ◆ 認証デバイス(ICカード、USBトークン、バイオメトリクス)
- ◆ シングルサインオン
- ◆ **PKI関連製品**
- ◆ 統合ID管理ツール
- ◆ 特権ユーザ管理ツール
- ◆ 検疫ツール(トークン、不正接続防止、検疫ツール)
- ◆ フォレンジックツール
- ◆ 統合ログ管理ツール
- ◆ シンククライアント
- ◆ ファイアウォール/VPN/UTM関連製品
- ◆ DDoS対策ツール
- ◆ ウイルス対策ツール
- ◆ 標的型攻撃対策ツール
- ◆ Webフィルタリングツール
- ◆ メールフィルタリング
- ◆ **メール暗号化(暗号機能、誤送信防止)**
- ◆ 電子メールセキュリティアライアンス
- ◆ 電子メールアーカイブ
- ◆ Webセキュリティアライアンス
- ◆ Webアプリケーションファイアウォール
- ◆ データベースセキュリティ製品
- ◆ 端末管理・セキュリティツール  
 (IT資産管理、端末操作ログ収集、持出制御、**ファイル暗号化、ディスク暗号化**)
- ◆ **DRM**
- ◆ DLP
- ◆ USBメモリセキュリティ
- ◆ モバイルウイルス対策
- ◆ モバイルフィルタリングツール
- ◆ **モバイル暗号化ツール**

※暗号製品市場は下線  
 富士キメラ総研「ネットワークセキュリティビジネス調査総覧」を利用

## 暗号製品市場の経年推移



## ライブラリ市場の経年推移



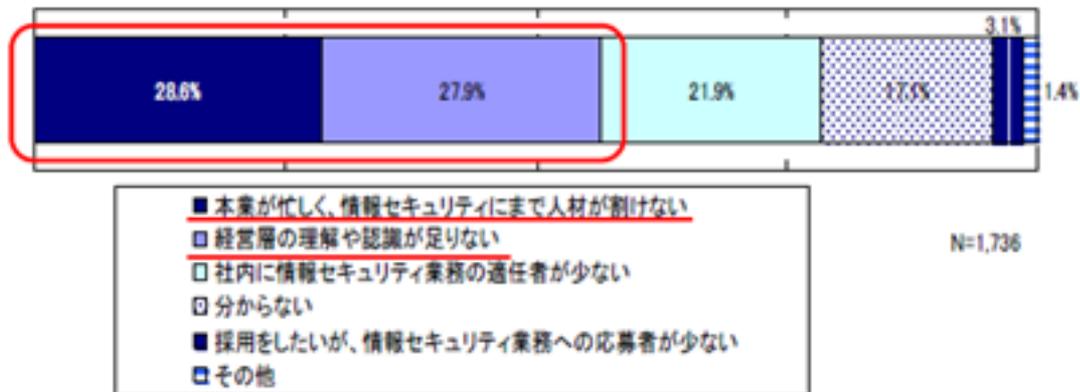
近年、情報セキュリティ製品市場が拡大する一方、暗号に関する市場が伸び悩み

出展：IPA「暗号利用環境に関する動向調査」2014年7月

# (参考) 企業における情報セキュリティ対策の現状

- 企業では情報セキュリティに関する業務に従事する人員が不足。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。
- 経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が6割程度。

人材不足の原因  
(社内向け業務)



企業経営層の  
情報セキュリティに  
対する理解度



(経営層以外からの回答)

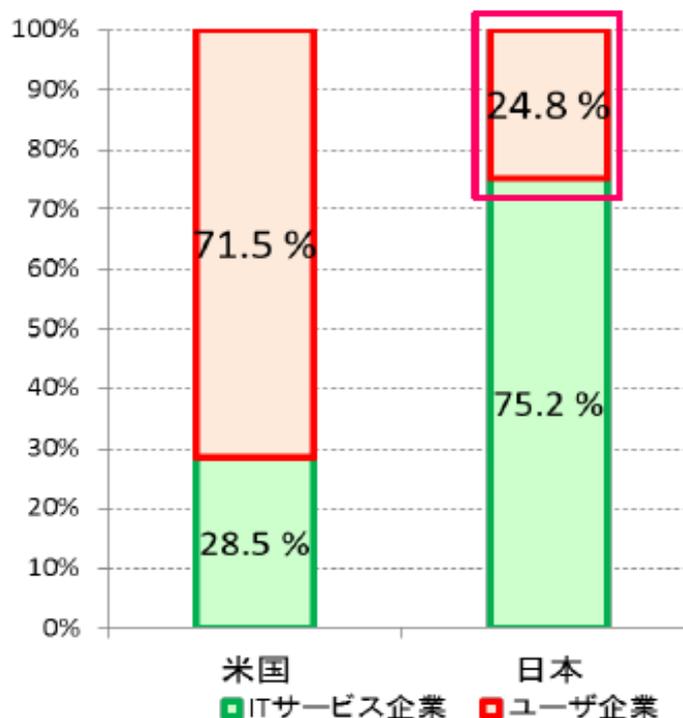
出典: 独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2012年4月

# (参考)企業における情報セキュリティ対策の現状

## 経営層を支える人材の問題

日本ではIT技術者がITサービス企業に偏っており、ユーザ企業に十分なIT技術者がいない。  
→ 情報システムの作成・管理が外注先に丸投げになっている可能性

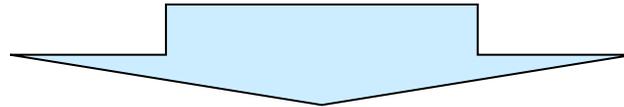
日米のIT技術者の分布状況



## 2-3. ミッション見直しの上での検討事項(政府)

### 政府における暗号利用について(論点)

- 我が国のセキュリティ対策は、「サイバーセキュリティ基本法」に基づき、サイバーセキュリティ戦略本部が担う。具体的には、同本部事務局であるNISC(内閣官房サイバーセキュリティセンター)が司令塔としてサイバーセキュリティに関する企画・立案、総合調整等を行い、各省が実施。
- 政府では、「政府機関の情報セキュリティ対策のための統一基準」により、情報システムで使用する暗号アルゴリズム等は電子政府推奨暗号リストを参照することが規定。
- また、政府の「サイバーセキュリティ戦略」(パブコメ中)においても、保持すべきサイバーセキュリティ技術として暗号技術が挙げられている。



### 方向性(たたき台)

- 安全な暗号技術の利用促進のため、プロトコルや製品・サービスレベルでのガイドライン等を政府統一基準に追加し、政府の受入れ拡充が必要ではないか
- 暗号技術検討会での普及促進に係る取組を実施。

## 2-4. 暗号技術を巡る環境変化

○暗号アルゴリズム等の技術はデファクトが普及

→安全な暗号アルゴリズムの選定に加え、脆弱性や新たな攻撃等への対応(方針の策定等)も重要

○プロトコル・製品・サービスでの暗号リスクの増大

→「デファクトスタンダード」における仕様の曖昧さ・多様さにより発生する、仕様・実装の脆弱性、運用時の課題や攻撃に対応することが重要。暗号技術が社会基盤の重要な1要素となった為に、問題発生時の社会的影響が非常に大きくなっている。

CRYPTREC暗号リストに掲載された暗号技術だけでなく、CRYPTRECとして活動の対象とするべき技術領域について再検討が必要

(参考)JNSAが発表した2014年度のセキュリティ十大ニュースでも「4月7日 Heartbleedなど脆弱性が次々と」としてHeartbleedなどの脆弱性が社会的に影響を与えた事案として【第3位】に。

具体的に言及された暗号技術関連としては以下

・OpenSSLというオープンソースの暗号ソフトウェアライブラリ上で発見された脆弱性(Heartbleed) [2014年4月7日]

・暗号化通信の一部を解読される可能性があるSSL V3.0の脆弱性(Poodle)[2014年10月]

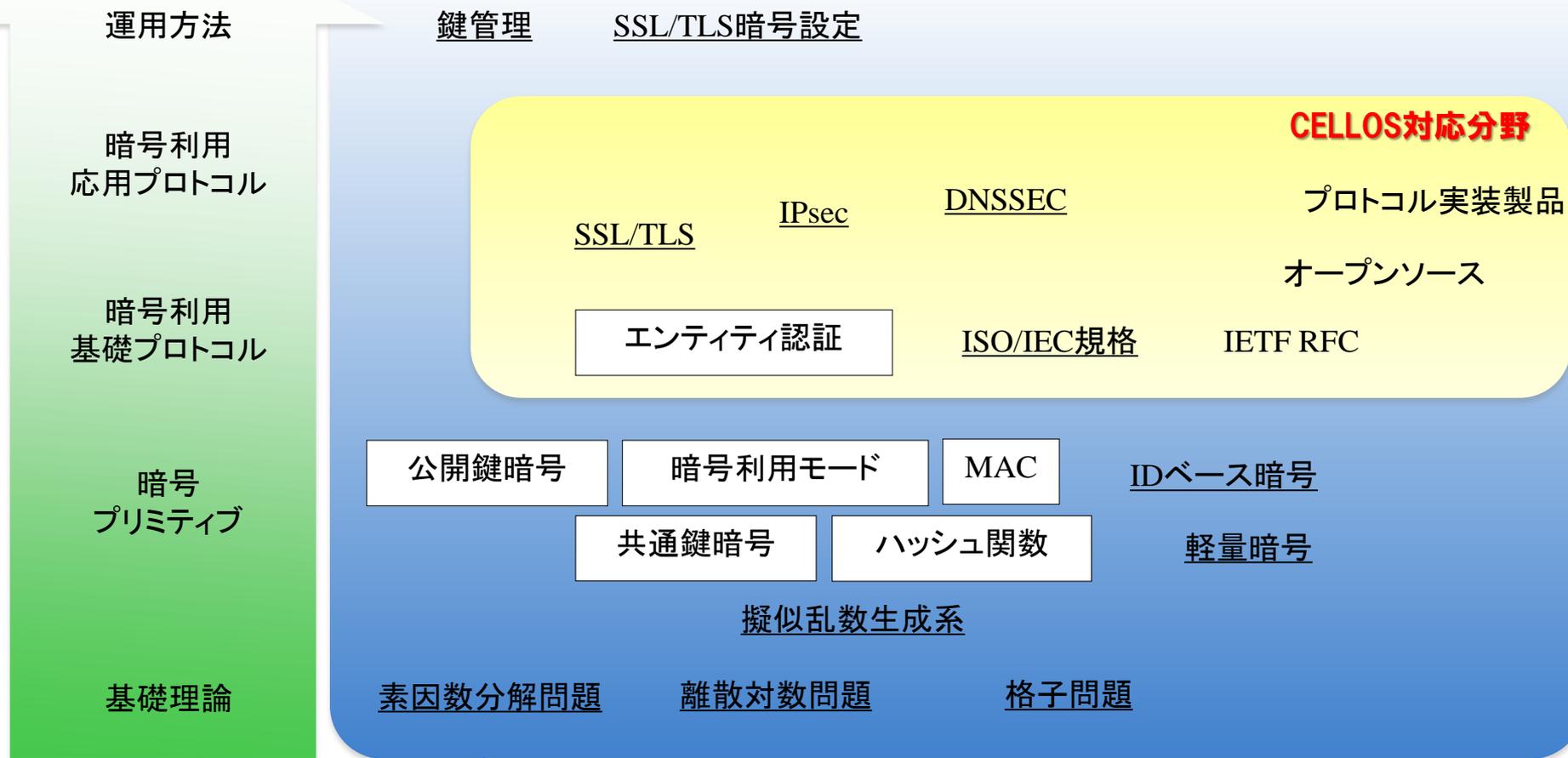
その他はApache Struts2の脆弱性、Internet Explorer(IE6~IE9)、Unixのbashシェルの脆弱性(Shellshock)の3つ。



# (参考)暗号技術の俯瞰図

プロトコルレベルでは

- ISO/IEC等で仕様が規格化されているもの
- IETF RFC等をもとにオープンソース化されたり各社の製品として実装され広く利用されているものがある。



**CRYPTREC対応分野**

枠線

CRYPTREC暗号リストにある技術分類

下線

CRYPTRECがWGやガイドライン等で扱った技術

### 3. 論点

○CRYPTRECが担うべきタスクについて、以下の論点を踏まえた検討が必要。

- ・目的 : 従来のミッションから変更すべきか、何を追加すべきか
- ・対象とする活動領域 : 暗号アルゴリズム等従来のものに加えて何を対象とするか
- ・主な適用範囲 : 電子政府に加えて一般向けのシステムも対象とするか
- ・成果物 : CRYPTREC暗号リストに加え、どのような成果物が考えられるか

○上記を踏まえ、現在担うタスクの棚卸しを行い、必要な体制を検討することが必要

#### 考慮すべき具体的観点

○現在の以下のミッションを修正すべきかを検討する。

「CRYPTREC暗号の安全性及び信頼性確保のための調査・検討、CRYPTREC暗号リストの改定に関する調査・検討に加え、暗号技術の普及による情報セキュリティ対策の推進検討」

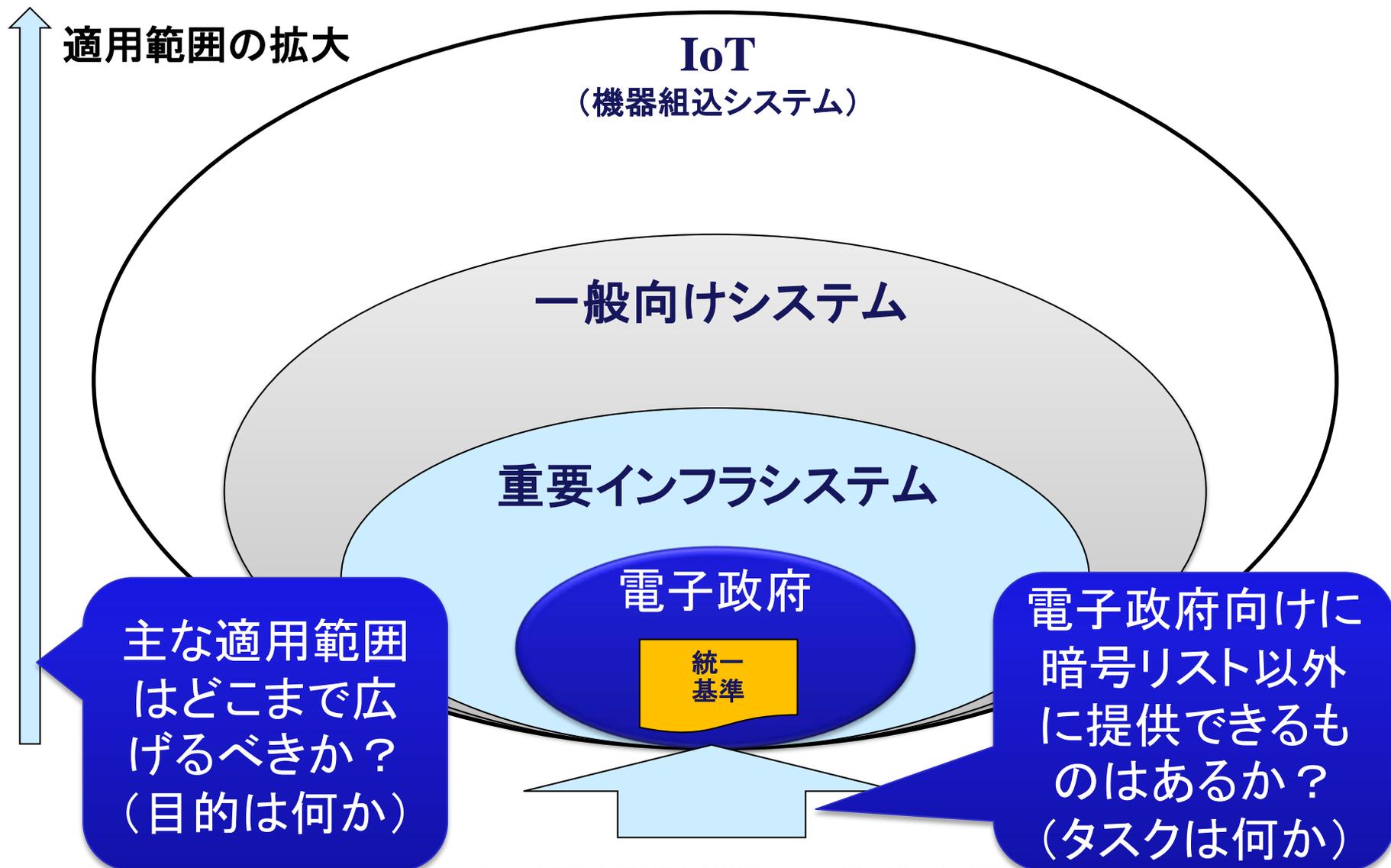
○対象とする活動領域を検討する場合、既存の他団体の活動(プロトコルの安全性(CELLOS)、製品(ソフトウェア)の脆弱性(JVN)等)との関係を考慮する。

○主な適用範囲については、ビジネスの現状や今後のIoT社会の到来などの変化も踏まえて、技術的な安全性は前提としながらも、厳密性と運用上の制約とのバランスを考慮しながら検討する必要がある。

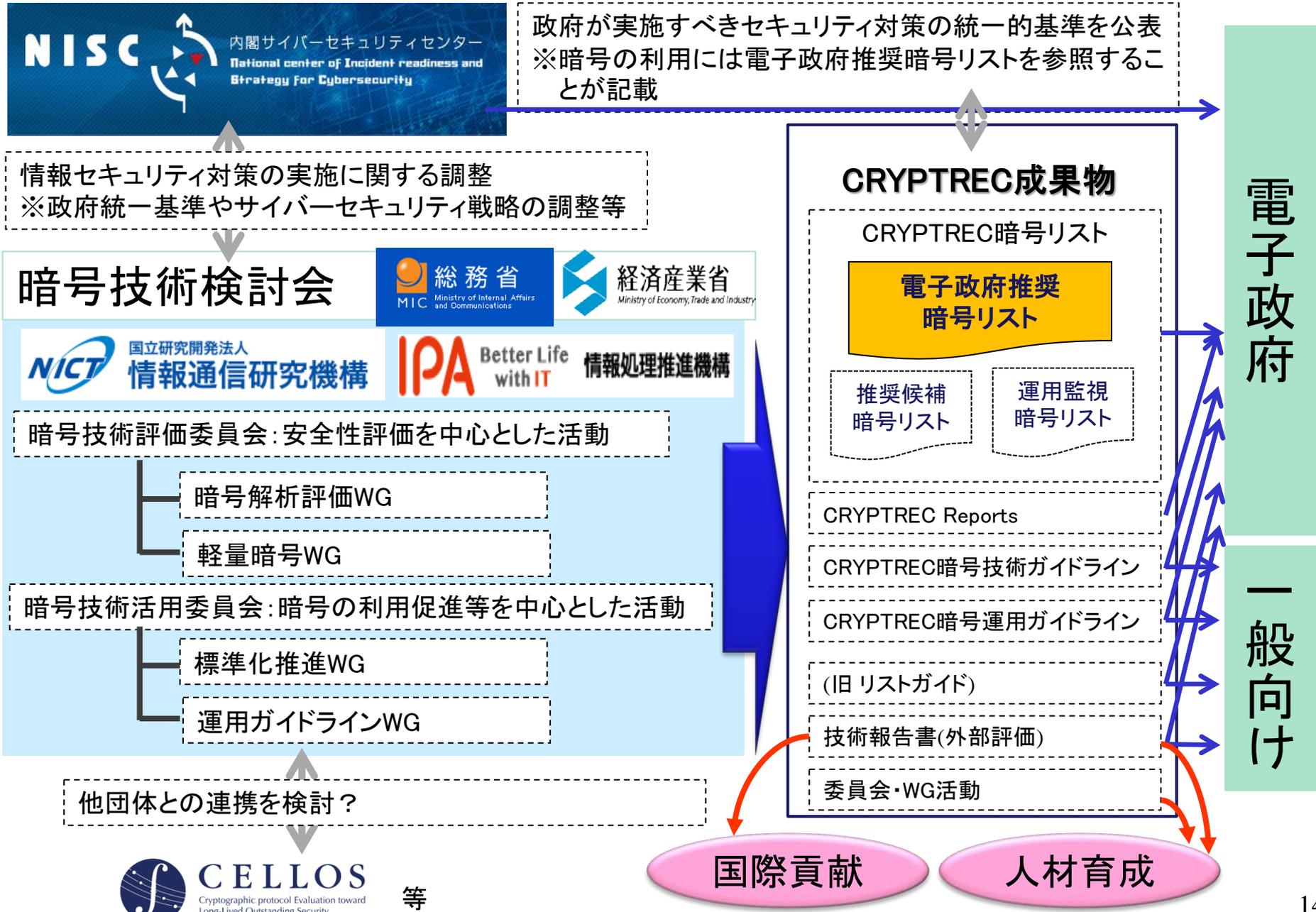
○成果物として、まずは電子政府向けでも現状の暗号リスト以外に柱となるべきものがないか検討が必要。

○CRYPTRECの活動範囲を拡大する場合、限られたリソースの現状に鑑み、CRYPTRECで新たなタスクを行うことの是非をCRYPTRECのあり方・リソースに照らし検証し、それを実施するために適切な体制を検討する。

# (参考) CRYPTRECの成果の適用範囲



# (参考)現在のCRYPTREC体制・成果物と展開先



○我が国においては、政府の調達基準を規定している「政府機関の情報セキュリティ対策のための統一基準」(情報セキュリティ政策会議決定)において、情報システムで使用する暗号は、電子政府推奨暗号リストを参照することが規定されている。

○政府機関の情報セキュリティ対策のための統一管理基準 (抜粋)

(平成26年5月29日 情報セキュリティ政策会議決定)

## 第6部 情報システムのセキュリティ要件

### 6.1 情報システムのセキュリティ機能

#### 6.1.5 暗号・電子署名

#### 目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用するアルゴリズムが適切であること、運用時に当該アルゴリズムが危殆化した場合の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

#### 遵守事項

##### (1) 情報システムの運用・保守時の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。

(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及び運用方法について、以下の事項を含めて定めること。

(ア) 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズムについて、「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) ~ (エ) 略

# (参考)サイバーセキュリティ戦略本部の概要

## 設置根拠

○ 設置根拠：サイバーセキュリティ基本法（平成26年11月成立）

※ IT戦略本部長決定（平成17年5月）による「情報セキュリティ政策会議」が、同法に基づきサイバーセキュリティ戦略本部へ格上げ。

○ 本部の所掌事務：

- ① 政府全体のサイバーセキュリティ戦略の案の策定、同戦略の実施推進
- ② 各省及び独法が守るべきセキュリティ基準の策定、それに基づく各省等の施策評価
- ③ 各省に対する重大なサイバー攻撃事案に関し原因究明のための調査等の実施
- ④ 重要な施策の調査審議、関係行政機関の経費の見積もり方針の作成、その他総合調整

## 構成（※従来の「情報セキュリティ政策会議」の構成員を引継）

本部長：内閣官房長官

副本部長：IT担当大臣

本部長員：国家公安委員会委員長、**総務大臣**、外務大臣、**経済産業大臣**、防衛大臣、有識者

### <有識者本部長員>

遠藤 信博 日本電気株式会社（NEC）代表取締役執行役員社長

小野寺 正 KDDI株式会社 代表取締役会長

中谷 和弘 東京大学大学院法学政治学研究科 教授

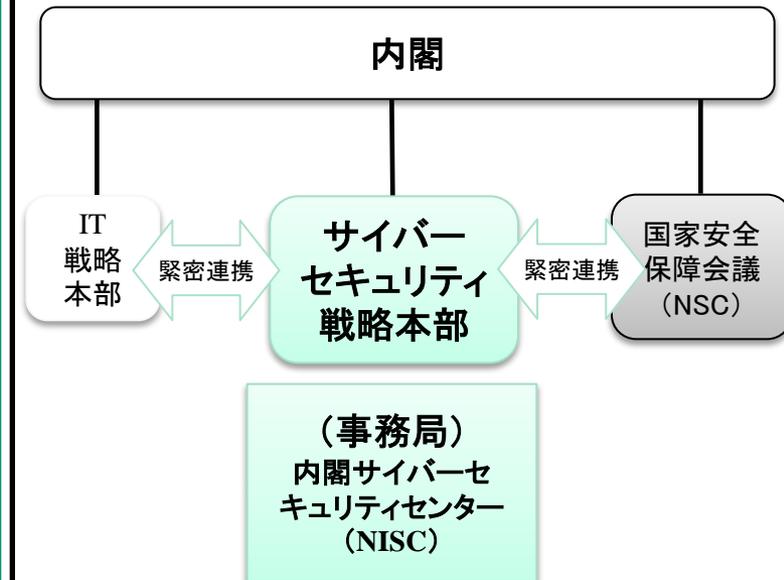
野原佐和子 株式会社イプシ・マーケティング研究所 代表取締役社長

林 紘一郎 情報セキュリティ大学院大学 教授

前田 雅英 首都大学東京法科大学院 教授

村井 純 慶応義塾大学 教授

本部等の法制化により、事務・権限を強化



## (参考)サイバーセキュリティ戦略本部の下での各府省庁の役割分担

内閣官房

総合調整、サイバーセキュリティ戦略の策定、各省施策の評価

警察庁

サイバー犯罪の防止

総務省

情報通信ネットワークの安全な利用の確保、  
ネットワークセキュリティに関する研究開発

外務省

サイバーセキュリティに関する諸外国との協力調整

経済産業省

重要インフラ<sup>\*</sup>を含む民間企業の対策促進、サイバーセキュリティ人材の育成、  
制御システムセキュリティ等に関する研究開発。

※ 政府指定の重要インフラ13業種<sup>注</sup>のうち、当省所管は5業種：電力、ガス、石油、化学、クレジットカード

防衛省

防衛関連施設に対するサイバー攻撃の防御

金融庁、国交省、厚生労働省  
等

金融、運輸、医療等の重要インフラ分野のサイバーセキュリティ対策促進

(注) 平成26年5月、情報セキュリティ政策会議において決定。13業種は、情報通信、金融、航空、鉄道、電力、ガス、石油、化学、クレジット、政府・行政サービス（地方公共団体を含む）、医療、水道、物流。

# (参考)新サイバーセキュリティ戦略の策定について

## 1 サイバー空間に係る認識

- サイバー空間は、「無限の価値を産むフロンティア」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがインターネットに接続され、サイバー空間と実空間との融合が高度に深化した「**接続融合情報社会**」が到来同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

## 2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」「**国民が安全で安心して暮らせる社会の実現**」「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

## 3 基本原則

- ① 情報の自由な流通の確保    ② 法の支配    ③ 開放性    ④ 自律性    ⑤ 多様な主体の連携

## 4 目的達成のための施策

①後手から**先手**へ / ②受動から**主導**へ / ③サイバー空間から**融合空間**へ

### 経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

- **安全なIoTシステムの創出**  
安全なIoT活用による新産業創出
- **セキュリティマインドを持った企業経営の推進**  
経営者の意識改革、組織内体制の整備
- **セキュリティに係るビジネス環境の整備**  
ファンドによるセキュリティ産業の振興

### 国民が安全で安心して暮らせる社会の実現

～ 2020年・その後にに向けた基盤形成 ～

- **国民・社会を守るための取組**  
事業者の取組促進、普及啓発、サイバー犯罪対策
- **重要インフラを守るための取組**  
防護対象の継続的見直し、情報共有の活性化
- **政府機関を守るための取組**  
攻撃を前提とした防御力強化、監査を通じた徹底

### 国際社会の平和・安定 及び 我が国の安全保障

～ サイバー空間における積極的平和主義 ～

- **我が国の安全の確保**  
警察・自衛隊等のサイバー対処能力強化
- **国際社会の平和・安定**  
国際的な「法の支配」確立、信頼醸成推進
- **世界各国との協力・連携**  
米国・ASEANを始めとする諸国との協力・連携

### 横断的 施策

- **研究開発の推進**  
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- **人材の育成・確保**  
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

## 5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会に向けた対応

# (参考) 世界各国の政府使用暗号の現状

- 政府で使用する暗号アルゴリズムを統一(=標準暗号方式):アメリカ、英国、韓国、中国、CIS(ロシア)
- 汎用製品主流で構築するシステムと、製品認証等を受けた高セキュリティシステムとに分離。汎用製品は米国政府標準を採用。高セキュリティシステムでは自国暗号アルゴリズムをしている場合もある: 欧州
- 政府で使用する暗号アルゴリズムをリスト形式で提示、調達官庁に選択を委ねる(=推奨暗号リスト方式): 日本

## 欧州



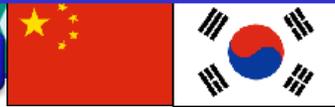
- ・高セキュリティシステムでは自国暗号(非公開)を採用した製品調達に指定(英国)
- ・汎用製品中心のシステムと高セキュリティシステムの製品調達方法を分離(ドイツ、フランスなど)

## ロシア



- ・国際経済活動国家規制局(DSRIEA: Department for State Regulation of International Economic Activity)が暗号関連のライセンス交付機関
- ・「GOST」をCISで標準暗号として指定。

## 中国・韓国



- 中国: 中国暗号管理局が指定する暗号アルゴリズムを使用  
「SM2」「SM3」「SMS4」  
(1カテゴリー1アルゴリズム)
- 韓国: 「SEED」「ARIA」「KC-DSA」が標準暗号アルゴリズム。  
GtoG、GtoCで利用。金融も準拠。  
「HIGHT」はB(ビジネス)での利用(軽量暗号)

## 日本



- ・2013年「CRYPTREC暗号リスト(電子政府推奨暗号)」作成。
- ・公募等により一定の基準を満たしたものを掲載。自国暗号、デファクト暗号を差別せず。
- ・標準暗号方式を採用せず。

## 米国



### 国立標準技術研究所(NIST)

- ・1990年代後半以降、全世界オープンで受け付けし、選定されたものを連邦政府標準として指定することが多い。  
(例) AES(Advanced Encryption Standard)
- ・ハッシュ関数(SHA-3)を選定済み、連邦政府標準にするための作業中。

## 暗号技術検討会における小グループの設置について

平成 27 年 3 月 27 日  
暗号技術検討会事務局

## 1. 設置目的

2001 年に CRYPTREC が発足した当初の目的は、安全でない暗号アルゴリズムが乱立する中で、電子政府において利用が推奨される安全な暗号アルゴリズムを確定させることであり、活動成果として 2003 年に「電子政府推奨暗号リスト」を策定し、2013 年にその改定版である「CRYPTREC 暗号リスト」を策定した。

また、2013 年のリスト改定を契機として、従来からの「CRYPTREC 暗号リストの安全性維持に係る取組」に加え、新たな試みとして「新しい暗号技術の調査」、「暗号技術の普及促進に係る取組」、「中長期的視点に立った暗号政策に係る検討」等を行った。

上記活動を通じて明らかにされた、暗号技術を取り巻く環境、サイバーセキュリティ基本法の施行といった社会情勢の変化等を鑑みると、CRYPTREC が果たすべき役割は、CRYPTREC 暗号リストの策定及び維持に限られるものではなく、より柔軟に活動することが望ましいと考えられる。

よって、暗号技術検討会に小グループを設置し、今後の CRYPTREC の活動内容及び対象範囲について集中的に検討を行うこととする。

## 2. 検討項目

- ・ 我が国の暗号技術を取り巻く環境の変化に応じた CRYPTREC の活動内容及び対象範囲について
- ・ 暗号技術の安全性確保等に係る活動のあり方
- ・ 暗号技術の普及促進、産業振興及び人材育成に係る活動のあり方等

## 3. 参加メンバー

暗号技術検討会の構成員、総務省、経済産業省、NICT、IPA を想定。必要に応じて関係省庁のオブザーバの参加を認める。

## 4. 検討スケジュール（予定）

2015 年度上半期中の早期に検討を行い、検討結果を暗号技術検討会に報告する。

## CRYPTREC の在り方に関する検討グループ 構成員・オブザーバ名簿

2015. 6. 3 現在

## (構成員)

上原 哲太郎	立命館大学 情報理工学部情報システム学科 教授
太田 和夫	電気通信大学大学院 情報理工学研究科 教授
近澤 武	独立行政法人情報処理推進機構 セキュリティセンター暗号グループ グループリーダー (ISO/IEC JTC 1/SC27/WG2 Convenor (国際主査))
手塚 悟	東京工科大学 コンピュータサイエンス学部 教授
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
盛合 志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長

## (オブザーバ)

内閣官房内閣サイバーセキュリティセンター

(五十音順、敬称略)