第 4 回 CRYPTREC の在り方に関する検討グループ

日時：平成 27 年 8 月 3 日(月) 17:00～19:00
場所：経済産業省 本館 9 階 西 8 共用会議室

議　事　次　第

１．開　会（資料確認等）

２．議　事
(1) 前々回の議事確認と今回の進め方について
(2) CRYPTREC の在り方に関する検討グループまとめ案
(3) 全体を通しての意見交換

３．閉　会

（資料番号）	（資　料　名）
資料１－１	第２回議事概要（案）
資料１－２	第２回議事録（案）　※関係者限り
資料２	CRYPTREC の在り方に関する検討グループまとめ案 ※関係者限り
参考資料１	CRYPTREC に関する現状について（第２回事務局配布資料）

資料１－１

第２回　CRYPTREC の在り方に関する検討グループ　議事概要（案）

１．日時　平成２７年６月２４日（水）　１８：３５～２０：４０

２．場所　経済産業省別館１階　１０１－２会議室

３．出席者（敬称略）

構成員：松本勉(座長)、上原哲太郎、太田和夫、近澤武、手塚悟、松本泰、盛合志帆

事務局：総務省（赤阪晋介、筒井邦弘、中村一成）

経済産業省（上村昌博、上坪健治、中野辰実、中村博美）

４．配布資料

（資料番号）	（資　料　名）
資料１－１	第１回議事概要（案）
資料２	「CRYPTREC に関する問題意識」（上原構成員）
資料３	「暗号プロトコル評価技術コンソーシアム(CELLOS)の概要」（手塚構成員）
資料４	「サービス視点からの暗号技術(の重要性)」（松本泰構成員）
参考資料１	CRYPTREC に関する現状について（第２回会合版）

５．議事概要

１　開会

事務局から開会の宣言があった。参考資料１に関して、前回会合での構成員意見を追記した旨説明があった。

２　議事

（１）前回議事確認と本日の議論の進め方について

前回議事概要については、文書の体裁についてコメントがあり、事務局が修正のうえ後日再度構成員にメールにて展開することとなった。

（２）CRYPTREC に関する問題意識

資料２に基づき、上原構成員より説明が行われた。

（３）暗号プロトコル評価技術コンソーシアム(CELLOS)の概要

資料３に基づき、手塚構成員より説明が行われた。

（４）サービス視点からの暗号技術（の重要性）

資料４に基づき、松本泰構成員より説明が行われた。

（５）全体を通しての意見交換

議事（２）～（４）までの発表に対して行った意見交換の内容は以下のとおり。

〇意見交換

①上原構成員プレゼンに対する質疑

松本座長：ガイドラインに附版したり小さい単位に分割したりといった利便性向上のための工夫を行うべきという提案には、全く同感である。これらの工夫はガイドラインの改定に当たっても便利である。CELLOS に一部機能を委譲するという資料の記載中、CRYPTREC が情報の正確性を追認するとあるが、具体的にどのようなイメージか。

上原構成員：CELLOS 等が速報性を重視して情報発信を行うが、調達の仕様等に使うためには正確性の担保がない。議論が固まった段階で、CRYPTREC として情報の正確性を追認するイメージである。

手塚構成員：調達要件として標準が採用されることも多い。欧州では ETSI で盛んに標準化が行われているのに対し、日本でも JIS などの標準規格で暗号を上手くひも付けできないか。

松本座長：例えば米国の調達では FIPS が仕様を定め、CMVP が製品を指定している。日本の調達では、調達のための参照規格や基準という意味で、暗号に関わる部分は後発であり、あまり整備されていない。

上原構成員：日本は標準化にかけているリソースが欧州と比較して少ないと感じている。国際標準化と調達の関係では、デジュール標準以外の規格を仕様に入れると非関税障壁扱いとなってしまうという問題もある。

近澤構成員：情報セキュリティは安全保障に関係してくるため、特に国際標準を使う必要はないという考えもある。

松本座長：いずれの場合であっても、調達の部分毎に標準やリストといった参照すべき文書が用意されているが、網羅的でないという問題があるのだと思う。

太田構成員：資料２の最後から２頁目の「設計上の安全性の確保」はどういう意味だったか。

上原構成員：実装物の安全性確保は JCMVP 等に頼るとして、アルゴリズムやプロトコルといった仕様の部分はこれまで CRYPTREC が担当してきており、その部分でもまだ「認証プロトコル」等の取り組むべき課題がある、ということ。暗号を基礎とする部品の安全性について、現在足りない部分に注力するべきではないかと考える。暗号の安全性についても当然従来どおり注力するべき。

盛合構成員：CRYPTREC では、仕様だけでなく実装の安全性確保も重要であるという議論があり、暗号モジュール委員会や JCMVP の立ち上げに繋がった。CMVP の製品数が大きく増えているのに対し、JCMVP の製品数があまり伸びていないと感じる。JCMVP の認

定を調達の必須条件にすれば利用が進むと思うが、今後の展望についてどう考えるか。

上原構成員：プロトコルや認証方式（パスワード認証の要件等）にも広げられるのではないか。本当はもっと JCMVP の製品が参照されるようになればいいが、今は不十分と感じる。

手塚構成員：仕様の部分は仕様のリストで規定し、実装の部分は製品リストから製品を選ぶ形が望ましい。複数社が同じ仕様に基づいて作成しても、ある社の製品は安全性に疑問があるといったことがあり得るので、調達の要件としては仕様のリストで規定する一方で、実際に選択する製品群は製品のリストの中から選び、それ以外のところから選ばないようにすることが必要。

松本座長：JCMVP では、使用して良い暗号アルゴリズムは JCMVP Approved のものとなっており、電子政府推奨暗号リストに掲載されている暗号技術は当然対象であるが、他のものも入れることができる。CRYPTREC よりスコープが広いので、CRYPTREC で評価していない暗号については、独自で評価を行う必要が出てくるが、我が国における暗号専門家の人材リソースが限られていることを考えると、色々と改善の余地がある。

松本泰構成員：資料４の参考の部 60 頁に CMVP と JCMVP の比較を書いている。日本のベンダ数が米国に比べ少ないということもあるが、情報セキュリティ製品の競争力の縮図とも言えるかもしれない。

松本座長：調達における強制力の有無がやはり大きいのではないか。

②手塚構成員プレゼンに対する質疑

近澤構成員：CELLOS は、脆弱性情報が発表されてから１，２日後にはレポートが掲載されており CRYPTREC でも見習いたいところだと感じているが、何人ぐらいで作業し、どのような承認プロセスを取っているのか。

手塚構成員：中心的な数人がドラフトを作成し、メーリングリストでの審議を経て、最終的に私や、WG リーダーの松尾氏が判断する形となっている。

松本座長：CELLOS の活動対象としている「プロトコル」はどういったものをいっているのか。

手塚構成員：CELLOS で活動の対象としているプロトコルとは、主に標準化団体が規定しているプロトコルで、具体的なコードも含むが、主に仕様レベルである。実装レベルまで確認することはリソース的に難しい。例えば、形式的手法による評価の実績は、３種類のツールを使って 33 個のプロトコルを評価した。活動を通じて見えてきたものとしては、標準化団体における認定のスキームが必ずしも十分ではないということ。標準化に際してしっかりと評価手法を導入していくことを推進していきたいと考えている。プロトコルの評価と脆弱性情報に対する対応が活動の大きな２本柱といえる。

松本座長：CELLOS は、大変有能な方々が集まっていることは理解したが、現時点ではまだ、組織として作業を発注できるような体制はとれていないと理解してよいか。

手塚構成員：現時点ではそのとおり。

松本座長：CELLOS の活動を引き続き継続していくにあたって、人的資源確保のためにうまく連携していけないかと思う。若い人材も巻き込んでいった方がよい。継続的な活動としていくために、CRYPTREC との協力範囲を明確にして役割分担を行えば、より一層活動が広がっていくのでは。

手塚構成員：プロトコルの部分は CELLOS で評価し、純粋に暗号アルゴリズムに関する部分は CRYPTREC で評価するという役割分担の構造ができると CELLOS にとってもありがたいところ。CELLOS 内では、脆弱性の速報を作成する人やプロトコル評価をする人など、それぞれの得意な分野を活かして役割分担はできている。ただ、ボランタリーな活動に基づいているので、仕事として活動に参加できるようになるとよい。また、CRYPTREC との連携としては、CELLOS の速報情報のページへのリンクを CRYPTREC のウェブページに貼るようなことでも十分に意義がある。プロトコル評価結果知識データベースを拡充し、海外にも発信していきたい。また、海外の人材もどんどん巻き込んでいきたいと考えている。

<u>③松本泰構成員プレゼンに対する質疑</u>

手塚構成員：資料８頁の「標準化」はどのような意味か。

松本泰構成員：例えば ETSI の標準化は、欧州の競争力を念頭においた活動であるとの認識しているが、技術標準の仕様だけでなく、相互運用性の確保や法制度との調整なども行っている。そのような広い意味での「標準化」活動だと考えているが、これは欧州における電子政府の活動にも深い関係がある。

盛合構成員：これまでの CRYPTREC は、過去の取組や電子政府という枠組に囚われすぎる傾向があったと思う。今後、CRYPTREC の活動範囲を広げていくのであれば、こういう風に変わります、ということをもっと打ち出して行く必要があると感じた。

松本座長：そのとおり。

松本泰構成員：HIPAA は、米国の医療分野の個人情報保護法にあたるものであり、保護医療情報（PHI）等の守る対象について規定しているが、暗号技術等によりの「どうやって守るか」に関しては、個別に記述している訳ではなく NIST が発行している技術ガイドラインを参照している。米国においては、包括的な個人情報保護法は存在しないが、技術ガイドラインについては、このように共通のものが参照されている。日本では、包括的な個人情報保護法が存在するが、それぞれの主管省庁ごとに業界にあったガイドラインを作成している。技術ガイドラインについては、米国において NIST のガイドラインを参照しているように、統一的な技術ガイドラインが参照するべきではないか。現在の主管省庁ごとの個別のガイドラインが技術的に必ずしも全て練られているとは思えない。

松本座長：その意味では、鍵管理なども同様の例。IoT において鍵管理は重要であるが、

CRYPTREC において鍵管理に関する文書はない。従っておくべき事項を規定する文書があり、かつ、その文書に沿って、実装されているかまでチェックできることが理想的だがまだまだ困難である。NIST が膨大な資料を作成してはいるが、それはあくまで米国モデルのものであるが、日本でも NIST の翻訳版で良いかは疑問があり、しっかり吟味する必要がある。

手塚構成員：CRYPTREC の活動範囲を実装などの方向に広げるのであれば、それらのレイヤーに知悉したベンダのシステムエンジニアなどの人をもっと巻き込むべき。CRYPTREC は今後、社会において暗号技術がどう活用されていくか議論し、活動範囲を自律的に決定していくべきであり、暗号よりもっと広い視野に立つ上位のレイヤーからインプットを受けて活動する構造になった方がよりよい。

松本座長：暗号技術を部品単位で評価する体制は整っているが、鍵管理、トラスト構築といったより上位のレイヤーについても CRYPTREC の活動範囲としていくべき。

手塚構成員：そのとおり。そのレイヤーの議論が不十分であり、部品レベルの議論のあと、いきなりアプリケーションや調達のレイヤーに議論が飛んでしまう。

事務局（経済産業省）：松本泰構成員の発表にもあるように、クラウドサービスやプライバシー保護等における暗号技術の応用についての検討は社会的な関心も高い。

松本泰構成員：Date at Rest において、日本では、暗号鍵を消去することでデータを消去するという手法が制度上明確でないことが、技術開発を促していない面がある。今後有望な技術だと考えられる Data in use のプライバシー保護データマイニングについても法制度との調整が考慮されないと技術開発の発展を阻害する可能性があるかもしれない。

事務局（総務省）：NIST のガイドラインのうち Data at Rest の分類にあるものは、内容によっては日本でも取組やすいものがあるのではないか。

松本泰構成員：CCRA に用いる PP と同様の記載であるので、日本にも文書としては存在する。ただ、基準を満たす製品の導入が進んでいない。

３　閉会

松本座長より、第３回会合について、近澤構成員と盛合構成員によるプレゼンを依頼した。また、議論の進め方として第３回で CRYPTREC の今後の活動の方向性について検討し、第４回でとりまとめを行う旨説明があった。

事務局から、第３回及び第４回の日程について連絡があった。

参考資料1

CRYPTRECに関する現状について

平成27年6月24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）

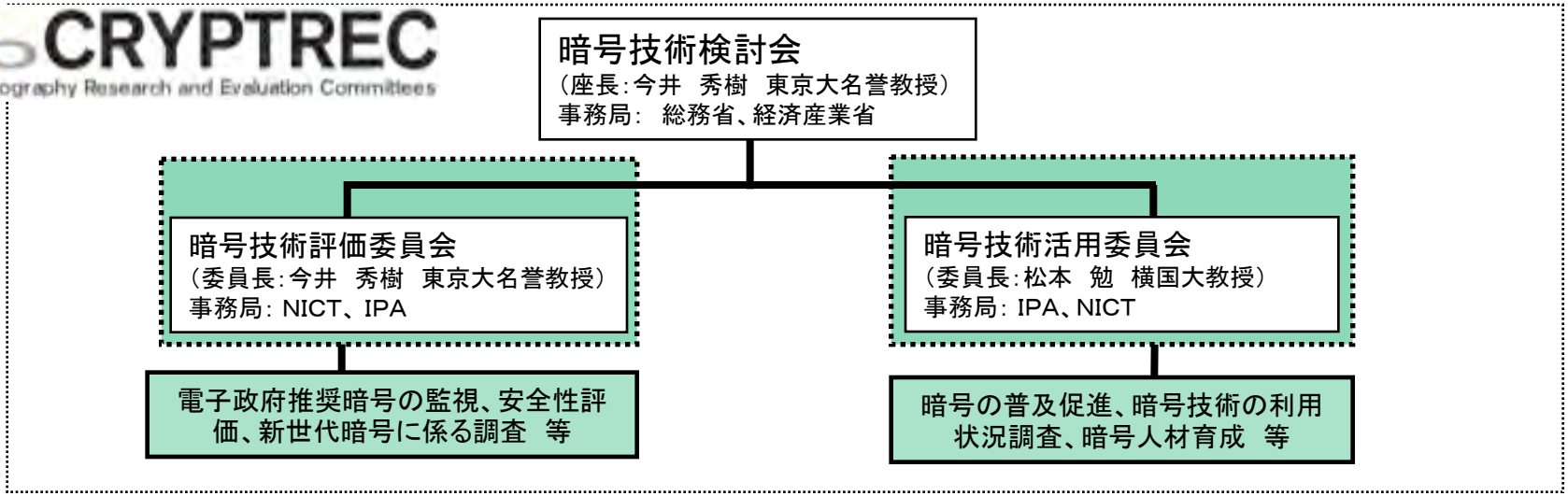
○必ずしも安全でない暗号アルゴリズムが乱立する中、安全な暗号の利用環境を整備するため、CRYPTRECを設立し、2003年に電子政府推奨暗号リストを策定。

○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

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注１)
		RSASSA-PKCS1-v1_5(注１)
	守秘	RSA-OAEP(注１)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注２)	3-key Triple DES(注３)
	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(注４)
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

推奨候補暗号リスト

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(注５)
共通鍵暗号	64ビットブロック暗号(注６)	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	Enocoro-128v2
		MUGI
		MULTI-S01(注７)
ハッシュ関数		該当なし
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

運用監視暗号リスト

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注８)(注９)
	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(注１０)
ハッシュ関数		RIPEMD-160
		SHA-1(注８)
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(注１１)
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 （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 （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ての対応が重要に。

→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）

〇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。

〇ベンダーは、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）

〇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１）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」　－抜粋－

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２）第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)

・CRYPTREC暗号リストは、政府機関のシステム以外の分野（医療、農業等）にも活用・展開できるのではないか。

・CRYPTRECによる活動成果は、現在のアウトプットに加え、利用者に近いテーマ・話題に関するものが望まれる。

（参考）暗号に関係する市場動向

情報セキュリティ製品市場の経年推移

※個人情報保護法の全面施行(2005年）、e-文書法の施行、ISO/IEC27001の発行

市場カテゴリの分類

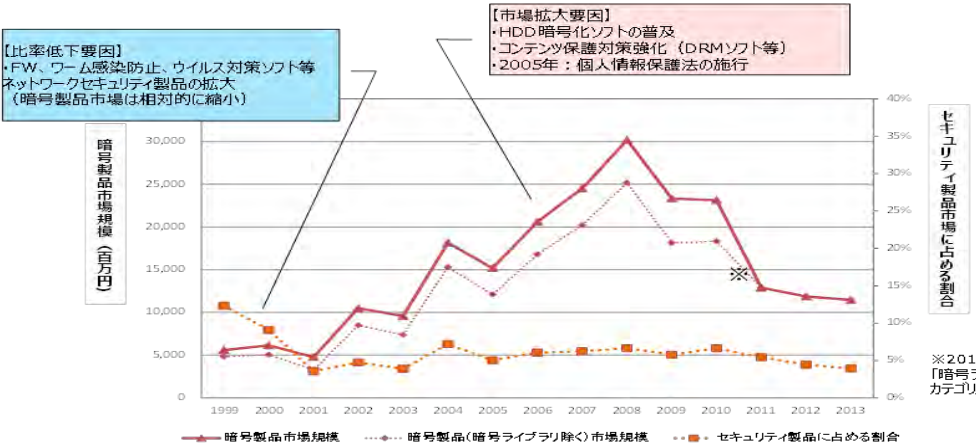
＜情報セキュリティ市場＞

- ◆ 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プライアンス
- ◆ 電子メールアーカイブ
- ◆ Webセキュリティアプライアンス
- ◆ 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

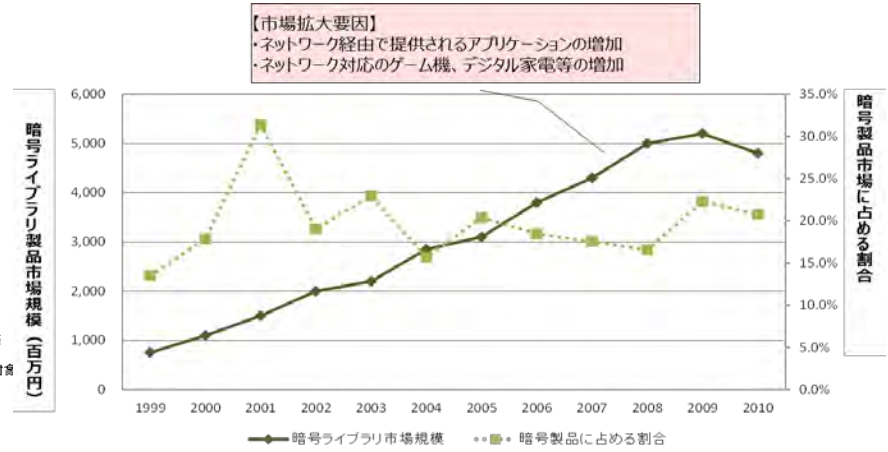
富士キメラ総研「ネットワークセキュリティビジネス調査総覧」を利用

暗号製品市場の経年推移



※2011年以降「暗号ライブラリ」カテゴリが集計対象

ライブラリ市場の経年推移



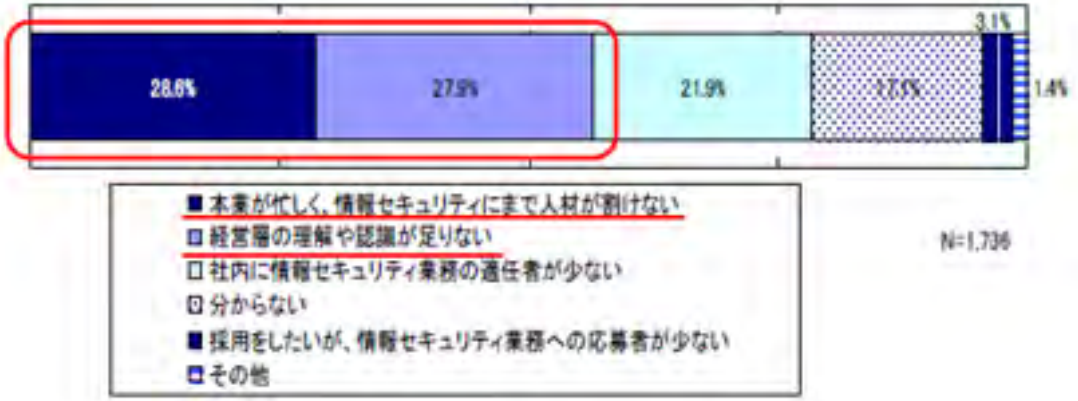
出展：IPA「暗号利用環境に関する動向調査」2014年7月

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

（参考）企業における情報セキュリティ対策の現状

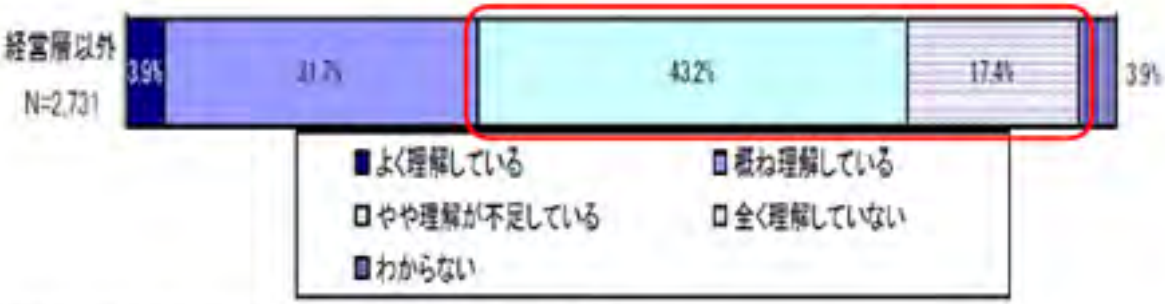
○企業では情報セキュリティに関する業務に従事する人員が不足。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。
○経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が6割程度。

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

（出典）米国労働省 労働統計局統計資料、NASCOMM、アジア情報化レポート、IPA IT人材白書2010 等

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、保持する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。

（参考）第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)

・政府の暗号利用のポリシーは、政府統一基準に掲載することで示される。

・政府統一基準への反映を念頭に、CRYPTRECとして、暗号リスト以外に何を作成すれば良いか検討すべき。

2-4. 暗号技術を巡る環境変化

〇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

〇プロトコル・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1）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]

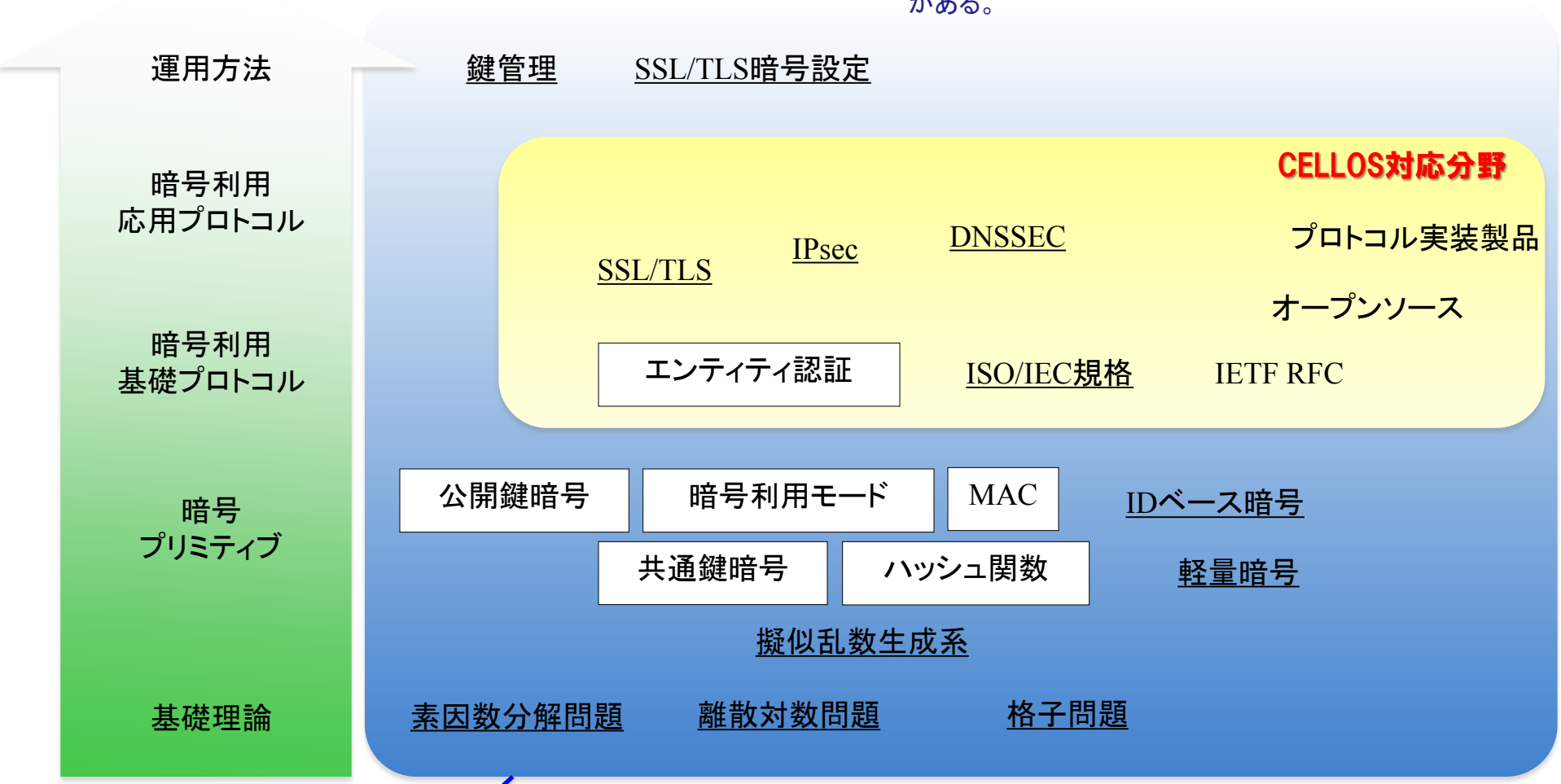
その他はApache Struts2の脆弱性、InternetExplorer（IE6～IE9）、Unixのbashシェルの脆弱性（Shellshock）の3つ。

（参考2）第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)

・CRYPTRECとして、信頼性の高い情報の発信は重要であるが、早期に脆弱性情報等を発信できる体制作りも重要。

（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。



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

〇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**

〇上記を踏まえ、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

〇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」

〇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。

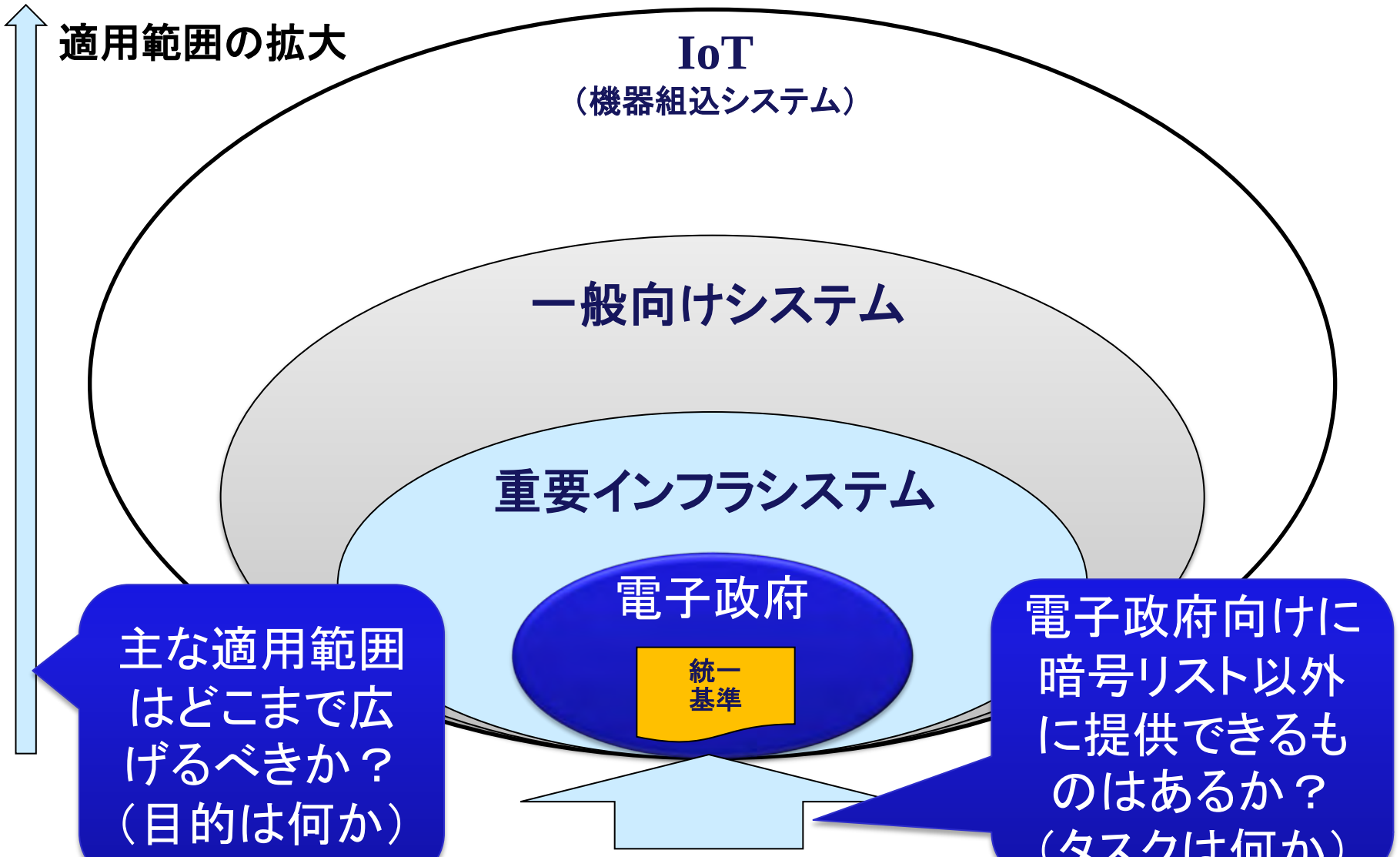
〇主な適用範囲については、ビジネスの現状や今後のIoT社会の到来などの変化も踏まえて、技術的な安全性は前提としながらも、厳密性と運用上の制約とのバランスを考慮しながら検討する必要がある。

〇成果物として、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。

〇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2）第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)
・CRYPTRECが個別製品の評価に関与する場合、網羅性や対象選定で不公平感が出ないよう留意することが重要。

（参考）CRYPTRECの成果の適用範囲



CRYPTREC
Cryptography Research and Evaluation Committees

（参考）現在のCRYPTREC体制・成果物と展開先

政府が実施すべきセキュリティ対策の統一的基準を公表
※暗号の利用には電子政府推奨暗号リストを参照することが記載

情報セキュリティ対策の実施に関する調整
※政府統一基準やサイバーセキュリティ戦略の調整等

暗号技術検討会

総務省 MIC Ministry of Internal Affairs and Communications

経済産業省 Ministry of Economy, Trade and Industry

国立研究開発法人 情報通信研究機構 NICT

IPA Better Life with IT 情報処理推進機構

暗号技術評価委員会：安全性評価を中心とした活動
- 暗号解析評価WG
- 軽量暗号WG

暗号技術活用委員会：暗号の利用促進等を中心とした活動
- 標準化推進WG
- 運用ガイドラインWG

他団体との連携を検討？

CELLOS Cryptographic protocol Evaluation toward Long-Lived Outstanding Security

JCMVP Japan Cryptographic Module Validation Program ®（IPA内）

等

CRYPTREC成果物

CRYPTREC暗号リスト

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

CRYPTREC Reports

CRYPTREC暗号技術ガイドライン

CRYPTREC暗号運用ガイドライン

(旧 リストガイド)

技術報告書(外部評価)

委員会・WG活動

電子政府

一般向け

国際貢献

人材育成

（参考）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

○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

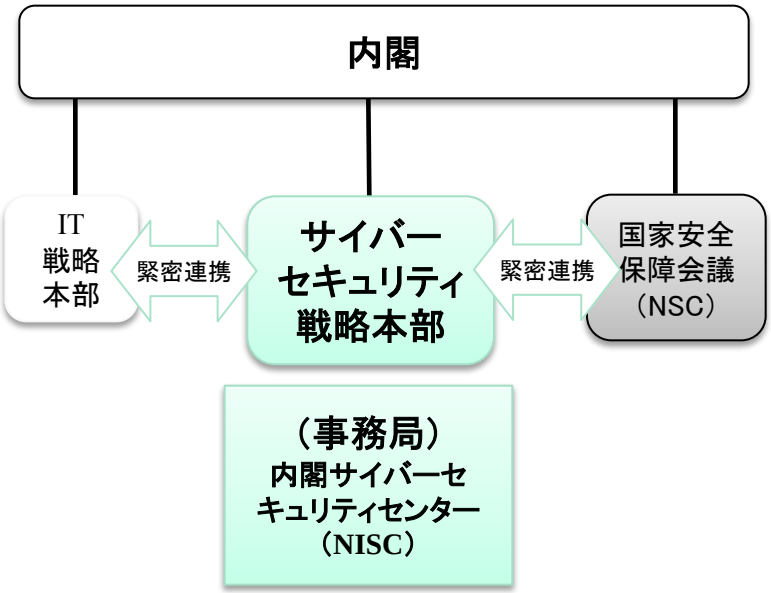
副本部長：ＩＴ担当大臣

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※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[注]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連接され、サイバー空間と実空間との融合が高度に深化した「**連接融合情報社会**」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

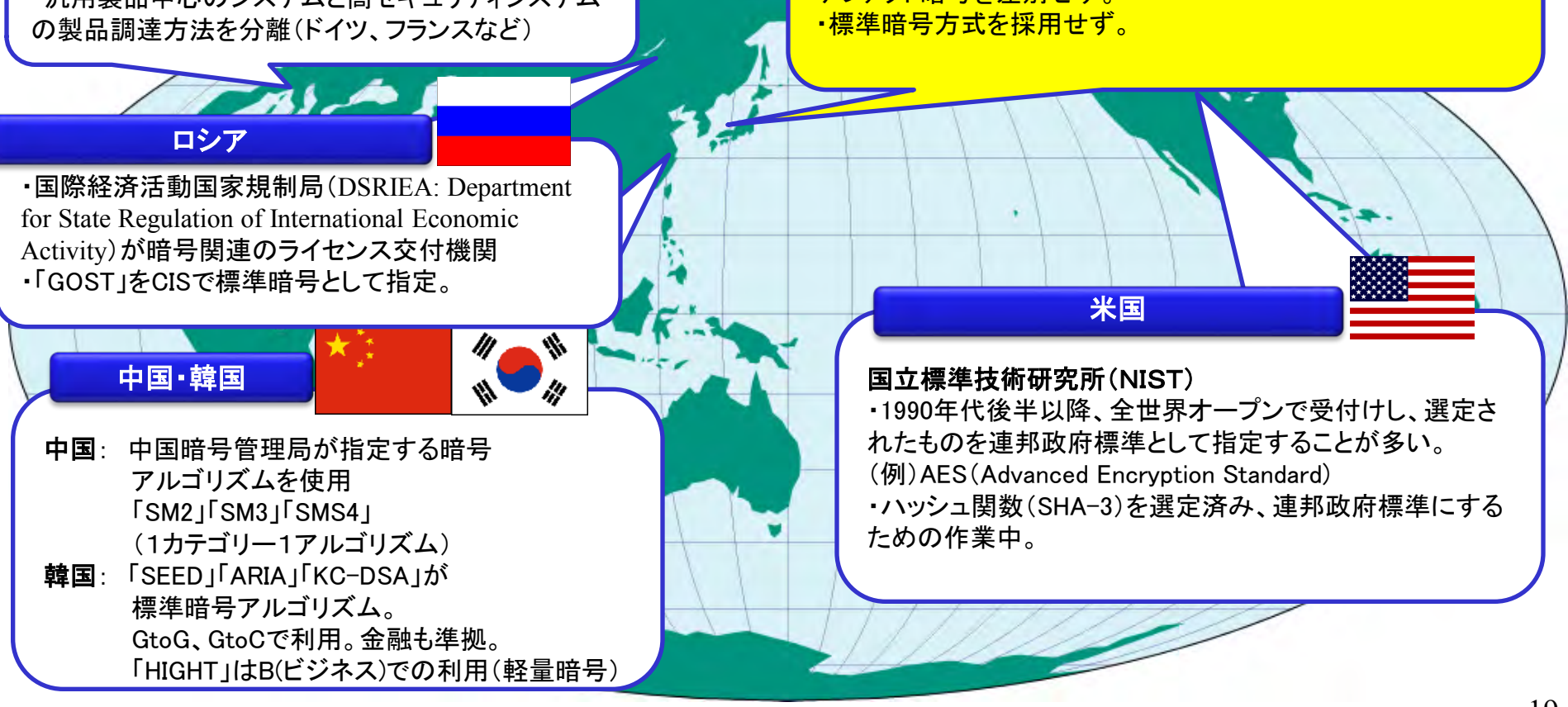
- ■ 研究開発の推進
  攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- ■ 人材の育成・確保
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

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）

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。

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）

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。