

第 2 回 CRYPTREC の在り方に関する検討グループ

日時：平成 27 年 6 月 24 日(水) 18:30～20:30

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（資料確認等）

2. 議 事

- (1) 前回議事確認と本日の議論の進め方について
- (2) CRYPTREC に関する問題意識[上原構成員]
- (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]
- (4) サービス視点からの暗号技術(の重要性)[松本泰構成員]
- (5) 全体を通しての意見交換
- (6) その他

3. 閉 会

(資料番号)	(資料名)
資料 1-1	第 1 回議事概要(案)
資料 1-2	第 1 回議事録(案) ※関係者限り
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)

第 1 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 3 日 (水) 10:00~12:00

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)、太田和夫、近澤武、手塚悟、松本泰、盛合志帆

オブザーバ：NISC (奥山剛、森安隆、大川伸也)

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 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

5. 議事概要

1 開会

事務局から開会の宣言があり、構成員の欠席 (上原構成員) の報告があった。

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

資料 1 に基づき、事務局より説明が行われた。質疑はなし。原案どおり承認された。

続いて、構成員の互選により松本勉構成員が座長に選出され、ご挨拶があった。

(2) CRYPTREC に関する現状について

資料 2 に基づき、事務局より説明が行われた。続いて行った自由討論の内容は以下のとおり。

○自由討論

NISC：マイナンバー等、政府として重要なシステムの構築がこれから行われるところ、暗号技術について考え方を整理し、示すことができる場合は CRYPTREC しかないのではないかと考えている。また、近年量子計算機などの新しい技術の研究が進んでおり、現行暗号が効力を失うことも想定されるが、その際の移行をどうすればよいか不安がある。ぜひ構成員の方々の知見をいただきたい。

近澤構成員：「政府機関の情報セキュリティ対策のための統一基準」(以下「統一基準」

という。)では、使用可能な場合には「電子政府推奨暗号リスト」に掲載された暗号技術を使用することとなっているが、リストに掲載されていない暗号が使用される場合もあると考えてよいか。

NISC：知っている限り無い。

松本座長：安全なシステムを構築するためには、適切に実装されていることが重要。統一基準では、暗号プロトコル等について具体的な基準はないと考えてよいか。

NISC：一般論としての記載はあるが、具体的な基準はない。

松本座長：昨年度 CRYPTREC が作成した「SSL/TLS 暗号設定ガイドライン」のような文書は、NISC から見て有用だと思うか。

NISC：有用だと思う。

松本座長：CRYPTREC として政府システムの安全性向上に貢献できたらと考えているが、NISC としてどのような成果物があると望ましいと考えるか。

NISC：提案できるほど暗号技術に関する知見がないので、ぜひ CRYPTREC から提案してもらいたい。

松本座長：CRYPTREC と NISC が今後も継続的にコミュニケーションを取っていく枠組みが必要。属人的なつながりに依存するのではなく、長く続く仕組みを作りたい。

NISC：そのとおり。CRYPTREC 事務局（総務省、経済産業省、NICT、IPA）の4者は NISC と密に連携を取っており、その関係性を活用してほしい。

手塚構成員：政府システムを構築するにあたり、必要な要素の全体像を明確化し、どこまでが CRYPTREC の担当範囲で、それ以外の範囲を誰が担当するのかといった、俯瞰的な立場に立った議論が必要。現状では、暗号技術のうち、どの部分について基準がないためにベンダ依存になっているのかといったことが分からない。また、NISC には政府システム全般のリスト化、現状把握を行っていただきたい。どのような暗号技術を使用しているのか把握しておくことは、危殆化などの問題が生じた際に大変重要。政府内にシステムに熟知した人材が乏しくベンダへの依存度が高いが、安全なシステムを構築するために、基準や使用するべき規格などを定めることが必要。

松本座長：何についてどの程度基準を決めるべきか、という点は使う側と技術を提供する側で意見が異なっている。CRYPTREC として統一基準にどのようなインプットを行うか、本検討グループにおける重要な論点。また、CRYPTREC の範囲をどの程度広げるかという論点もある。

松本泰構成員：2点ある。1点目は、統一基準に関して、米国においてよく見受けられるデータセキュリティに基づく分類が議論の参考になるということ。移動中のデータ、保管中のデータ、利用中のデータ、消去されたデータの4つの状態に基づき分類され、こういった技術・文書があり、何が不足しているか分かり易い。2点目は、暗号研究の出口戦略が不明確であること。暗号がセキュリティのための技術であるというイメージが強いが、トラストのための技術としての意味合いの方が重要である。今後の IoT

社会においてイノベーションを起こすための技術として暗号技術を位置づけ、暗号技術の出口を考え直すべき。

松本座長：暗号研究に関して、CRYPTREC としてどのようにコミットしていけば良いか。

松本泰構成員：暗号政策全体の観点になるが、日本に足りないものは米国の NIST に相当する組織。基礎研究と実社会を結び付ける NIST のような組織がないため、暗号技術の社会への還元が不足している。CRYPTREC が NIST 相当の機能を担うべきかという点には様々な意見があると思うが、NIST 相当の機能の必要性は広く認められているところ。

太田構成員：信頼性の高いシステムを構築するという観点では、電子政府のみならず、例えば医療系システム等の重要なシステムも適用先としてアプローチできないか。医療系システムであれば厚生労働省の所管であるが、NISC ではこのような分野にもアプローチしているのか。

NISC：医療分野は重要インフラの 1 分野であり、NISC として安全基準等の策定指針を示したりしているが、NISC が政府統一基準への遵守を求められるのは政府機関のシステムまでである。セキュリティに限らず医療分野を含む各業界のルールは各所管省庁等で作っており、セキュリティだけを切り出して NISC が各業界を直接担当するという形にはなっていない。

松本座長：その点、米国の NIST は連邦情報セキュリティマネジメント法による位置づけがあり、豊富な標準規格を用意することで、各業界、世界各国から参照されている。日本でもかなり参照されているが、日本が自ら規格を定めることも必要。広く使われるような魅力ある成果物を作る必要がある。

事務局（経産省）：経済産業省では「IT 製品の調達におけるセキュリティ要件リスト」を作成している。現在は世界で標準的な基準に基づいて審査を行っているが、将来的に日本から基準そのものを発信していきたい。

事務局（経産省）：情報セキュリティ全体における暗号の位置づけを明確化し、さらに政府における役割分担も明確化するべきだと思う。法律上の所掌では、NISC が総合調整機能を果たし、総務省及び経済産業省が、暗号に関する取組を提案していく形だと思われる。

手塚構成員：CRYPTREC の活動を考えるうえで、技術と実装を分けて考えることが必要。従来の CRYPTREC は暗号技術の評価・監視など技術的な観点からの取組が中心であった。製品やシステムといった実装のレベルとは異なる段階である。技術から実装まで全体の流れを俯瞰し、それぞれの範囲をどの組織が担当するか、整理することが重要。その点、JCMVP 等も連携先として十分考えられるのではないか。

松本座長：技術に関する取組には必要な人的リソースの確保が CRYPTREC の重要な課題の 1 つ。とはいえ、人的リソース等の体制面での議論はひとまず置いておき、CRYPTREC としてやるべきことについて、最初に議論したい。現時点での CRYPTREC の取組は、

暗号技術の一部の側面しか対象となっていない。何が必要で何を作るべきか、改めて検討すべき。今日、実装やプロトコルレベルでの脆弱性への対処が重要な課題。また、CRYPTREC が電子政府や電子政府以外の領域でどのように貢献できるかも論点の1つ。

盛合構成員：CRYPTREC はこれまで、提案者から評価の申し出があった技術について評価し、結果を公表してきた。政府に近い立場である CRYPTREC が、勝手に個別の実装に対して問題点を指摘することになるというのがこれまでと異なる点である。また、現状の国内の脆弱性関連情報の届出の体制は、暗号技術に関する脆弱性等の情報に対応していない。さらに、現状の CRYPTREC の人的リソースは限られているので、より製品に近い部分については、既存の団体との連携を強化することが必要。

松本座長：ユーザ側の立場から判断する内容を示すだけなので、特段問題ないのではないか。

盛合構成員：製品レベルで推奨・非推奨といった評価を行う場合、全ての製品を評価対象とすることは出来ないので、限られたリソースに基づき調査をするとやはり不公平感が生じてしまい、中立性の担保が難しいのではないかと。

手塚構成員：ご意見もとてもだが、解決方法もある。例えば、基準となるガイドラインを作り、その基準に従って評価する制度を作るという方法が考えられる。

事務局（上村）：懸念点はあっても、必要なことであれば解決策を探るべき。

松本座長：人材リソースに関する論点は重要だが、CRYPTREC のミッションに関する議論の後に議論したい。

近澤構成員：暗号技術に関して脆弱性などの問題が明るみになった際、CRYPTREC のホームページにその問題に関する見解等が記載されていると、活動の存在意義が高まって良いのではないかと。IPA は電子政府に限らず全ての領域を対象としており、全ての領域を対象とすることの重要性は認識しているが、CRYPTREC で扱うべきかという点は議論が必要。また、ISO/IEC JTC1 で標準化活動にも関わっているが、利用者に近いテーマの規格文書やガイドラインでないともあまり読んでもらえないという実感がある。

松本座長：ホームページを通じた情報発信はぜひやっていきたい。情報の早さではマスクミ等のサイトに敵わないが、信頼性のある情報を素早く出すことに意義がある。ユーザに活用してもらえる情報を出すためには、リソースを考慮しつつ、どの分野で何を出すかという点が重要。

3 閉会

事務局から、次回会合の詳細については別途連絡する旨の説明が行われた。

以上

CRYPTRECについての問題意識



RITSUMEIKAN

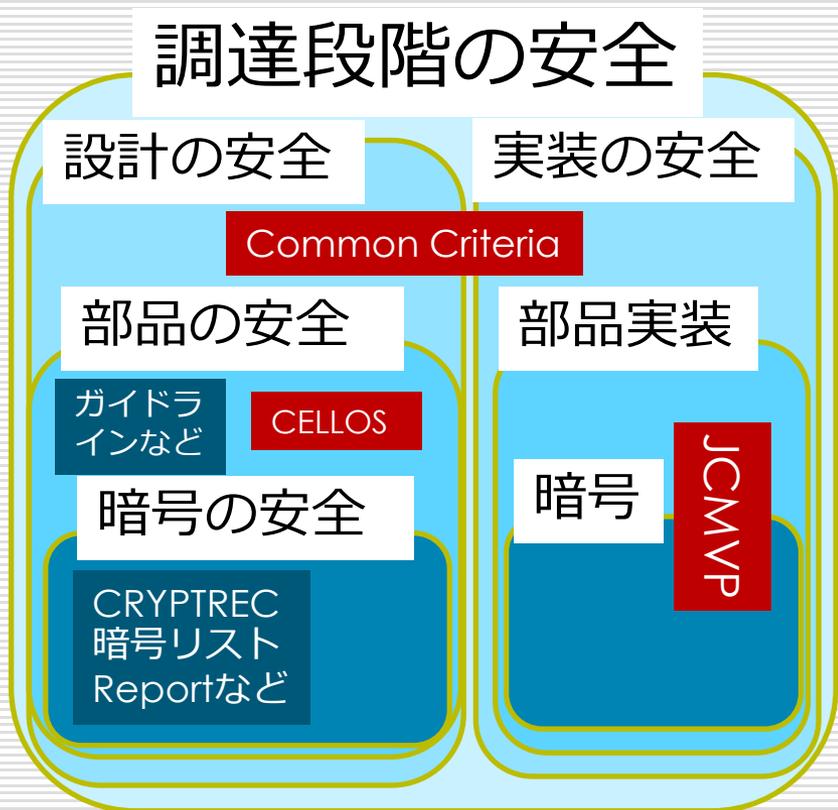
立命館大学
上原哲太郎

CRYPTRECの「元々の」ミッション

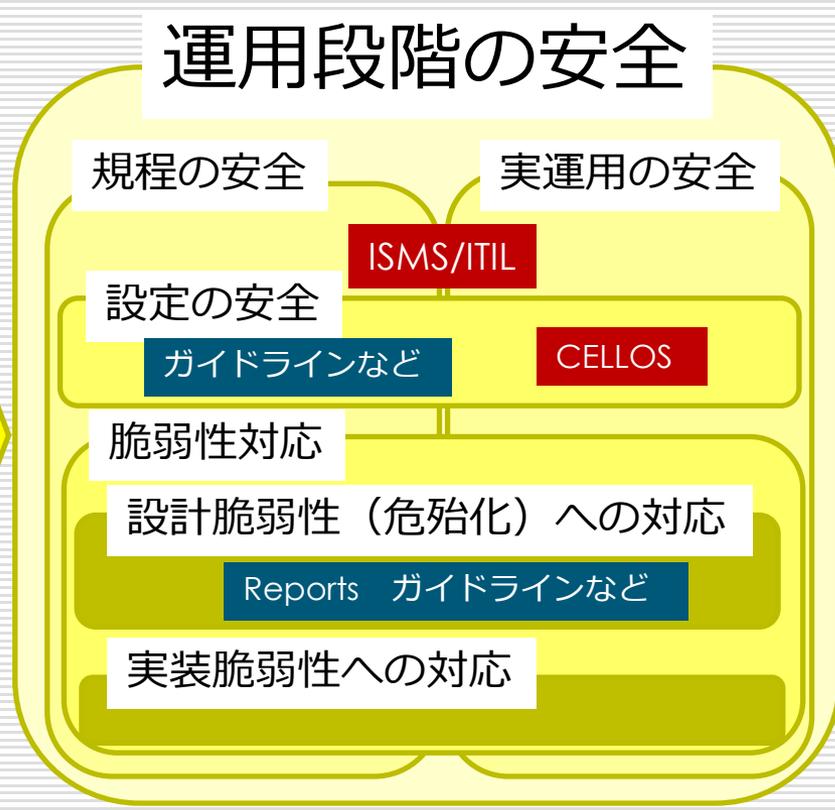
- 「電子政府」の安全性確保を「暗号」の観点から行うもの
 - 電子政府
 - ≡ 「各省庁が導入し運用する情報システム」
(政府情報システム)
- 主な出口はCRYPTREC暗号リスト
 - 公開鍵・共通鍵・ハッシュ関数
 - ・ 暗号利用モード・MAC・エンティティ認証
 - いずれもアルゴリズムのみについて安全性検証
 - そのほかガイドライン・レポートなど

調達・運用する立場からみると？

調達段階の安全



運用段階の安全



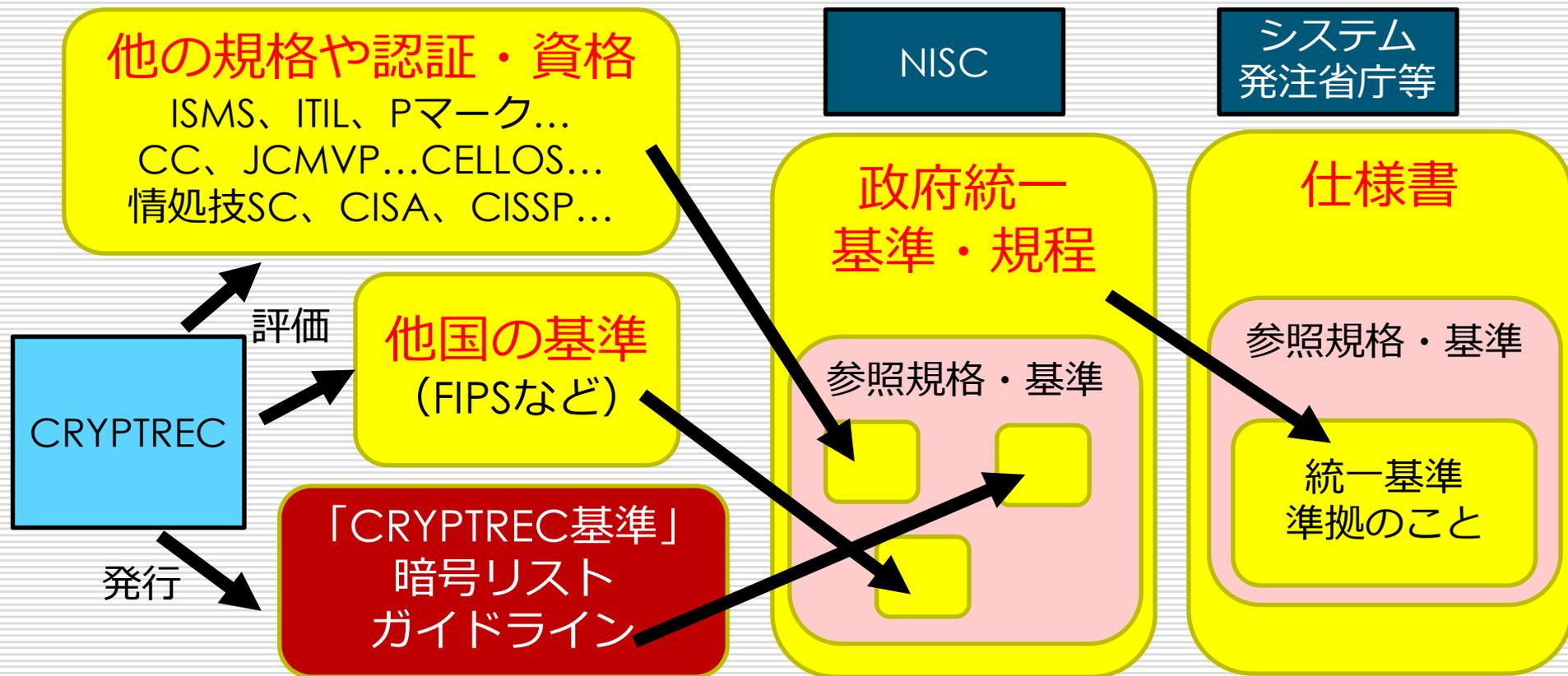
NISC政府統一基準・規程が求める領域

調達時に仕様書で書き込める領域

公共調達現場感からすると...

- 政府調達ではCRYPTREC暗号リストは比較的広く認識されている
 - 仕様書に一文書き込むだけで担保できる有難さ
 - 自治体レベルでは認識自体にやや不安あり
- 一方で部品レベルや運用に資するはずのガイドラインなどは認識が薄い
 - NISCの統一基準・規程に明文化されていない
→自動的に参照される存在ではない
 - 認識があっても仕様書にどう反映するか悩む
 - CCやISMSなどの「認証」は多用されるのと対照的
 - **セキュリティ担保の観点では網羅性が不明**

政府情報システムの調達にとって CRYPTRECに望まれる機能



CRYPTREC成果物に不足するもの

- 仕様書への反映のしやすさ
 - NISTのFIPSに比べて参照が難しい
- 政府情報システム調達向けの要件の網羅性
 - 設計の安全のうち「部品の安全」に関して他の規格等でカバーできてない領域でかつ必要なセキュリティ要件があるはず
 - 特にプロトコルと認証方式
- 実装・運用に対するセキュリティ担保機能
 - OSS活用にともなう問題など

方向性の提案

- 暗号技術およびそれを基とした部品の「設計上の」安全性の担保に関し網羅性を確保したうえで従来通り評価と監視を続ける
 - 評価の結果をより参照しやすくまとめる
- 実装と運用、特に脆弱性対応については外部機関の力を借りながら安全性評価に絞った活動を行う
 - 評価の信頼性vs迅速さ

具体案として

- これまで出したガイドライン類に附番
 - より短いサイクルでの再評価・改訂
 - 改訂時には積極的に分割して小さな単位で参照できるように
- IPA/CELLOSへの一部機能の委譲や委任
 - 速報性をとにかく重視する
 - 実装や運用ガイドについては任せる
 - CRYPTRECは安全性について追認する機能に絞る

暗号プロトコル評価技術 コンソーシアム (CELLOS)の概要

東京工科大学

手塚 悟

コンソーシアムの目的

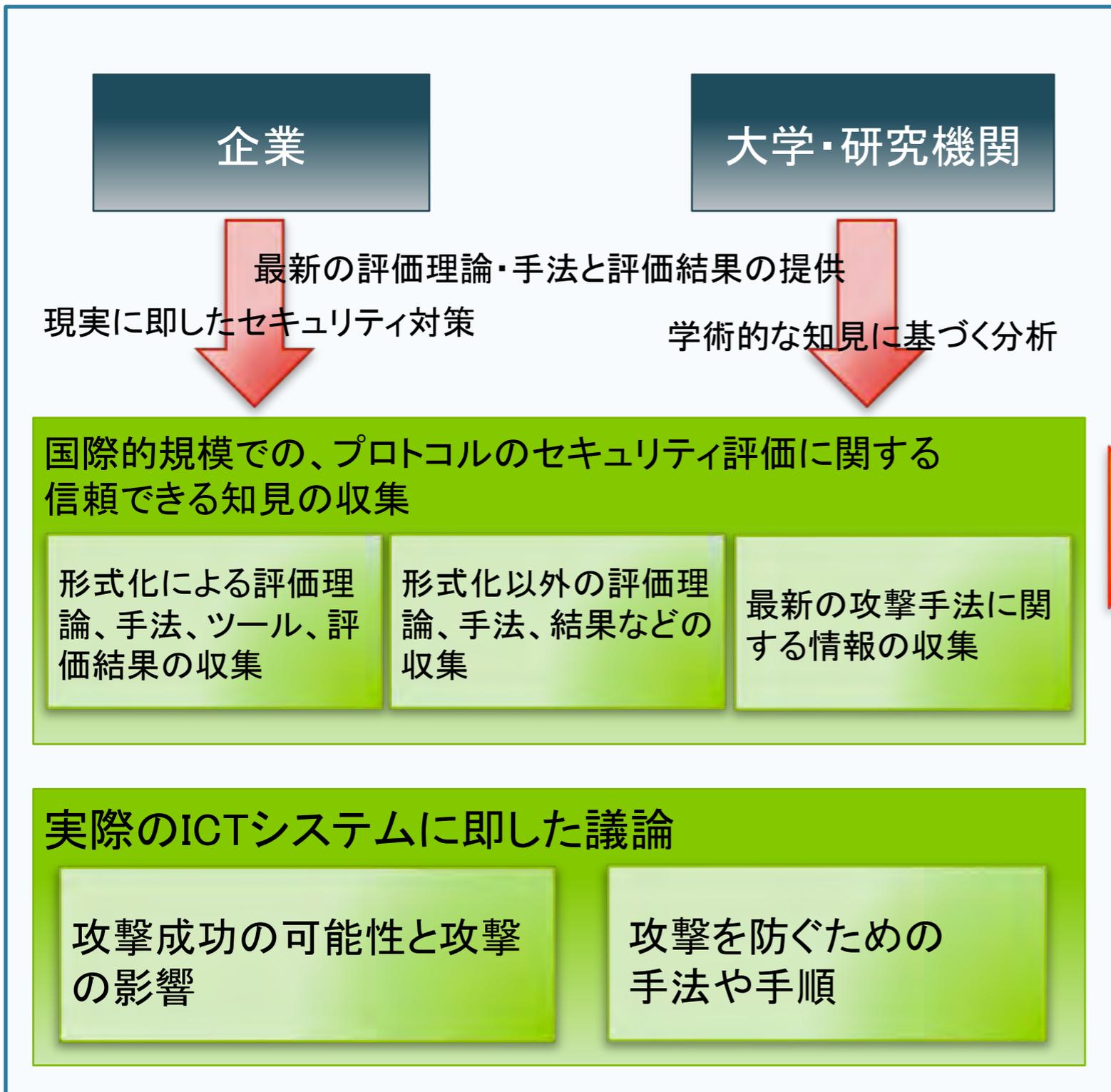
国際的に信頼できる基盤として、このコンソーシアムでは、ICTで利用される暗号プロトコルを評価するとともに、暗号プロトコルの評価結果を収集し、公開することを目的とする。

特徴

- ・ 国際的に中立であること
 - ・ 日本のみならず国際的な研究者からの知見の集約
- ・ 最新の情報を、即座に機動的に共有し、提供する

コンソーシアムの役割

CELLOS



参照者

大学・研究機関

研究・教育への利用

システムベンダ
(開発者視点)

プロトコル開発への利用

システムベンダ
(利用者視点)

システム設計における利用

国際標準

国際標準における安全でないプロトコルの修正など

議論の手順

総会

- 技術の見解に関するオンラインでの審議
- (活動方針に関する年次総会)


実システムに
即した見解など

 実システムでの見解などの審議
(必要に応じて)

技術WG

- 脆弱性などの技術的問題に関するオンラインでの議論
- 攻撃の可能性について論文、技術的文書のチェック、
およびメンバによる評価を経た上での技術的事実の確認
- 実システムに対する影響に関する報告案の作成
(必要に応じて)
- 評価手法・理論に関する知見の蓄積
- 重要な課題に関する勉強会(TLS1.3など)


技術的事実に関
する速報
レポート

Webサイト
での情報公開

CELLOSのオンライン議論システム

The screenshot displays the CELLOS online discussion system interface. At the top, the browser address bar shows 'cellos-consortium.org'. The navigation menu includes 'Home', 'My page', 'Projects', 'Administration', and 'Help'. The user is logged in as 'smatsuo@nict.go.jp'. The main heading is 'Technical Working Group » Protocol Vulnerability Discussions'. A search bar and a dropdown menu for 'Protocol Vulnerability Discussions' are visible. The 'Issues' tab is selected in the navigation bar. The main content area shows 'Vulnerability Report #14' with actions like 'Update', 'Log time', 'Watch', 'Copy', and 'Delete'. The report title is 'Comment on Heartbleed Bug on OpenSSL -1.0.1f'. It includes metadata such as 'Status: Discussion', 'Priority: Urgent', 'Start date: 04/11/2014', and 'Due date: 04/13/2014'. The description section contains text about proposing an announcement through the CELLOS website and refers to news about a vulnerability on OpenSSL. A sidebar on the right lists 'Issues' with options like 'View all issues', 'Summary', 'Calendar', and 'Gantt', and shows 'Watchers (1)' including 'Kazumasa Taira'.

cellos-consortium.org

Home My page Projects Administration Help

Logged in as smatsuo@nict.go.jp My account Sign out

Technical Working Group » Protocol Vulnerability Discussions

Search: [] » Protocol Vulnerability Discussions

Overview Activity **Issues** New issue Gantt Calendar News Documents Wiki Files Settings

Vulnerability Report #14 Update Log time Watch Copy Delete

Comment on Heartbleed Bug on OpenSSL -1.0.1f < Previous | 2 of 4 | Next >

Added by Shin'ichiro Matsuo 8 months ago. Updated 8 months ago.

Status:	Discussion	Start date:	04/11/2014
Priority:	Urgent	Due date:	04/13/2014
Assignee:	Technical WG members	% Done:	0%
Category:	-	Spent time:	-
Target version:	-		

Description Quote

As discussed in the "News". I would like to propose issuing an announcement through CELLOS web site as soon as possible, though it is not protocol specification issue. SO, now, I move this discussion to this issue in the "Technical Working Group » Protocol Vulnerability Discussions".

Please refer the following comments in the "news" and give comments for the announcement. In my plan, the announcement will be issued in one or two days. I will give the draft of the announcement in several hours including comments from WG members.

--

Heartbleed Bug on OpenSSL -1.0.1f

Added by Yuji Suga 3 days ago

Yesterday we got a lot of news about a vulnerability on OpenSSL with the specific versions. OpenSSL announced the following security advsory:
https://www.openssl.org/news/secadv_20140407.txt

This vulnerability is a matter of implementation, not a matter of specification of TLS. Patches (1.0.1g or 1.0.2-beta2) are available, so we can fix it easily. Alternative choice is recompiling OpenSSL with an option -DOPENSSL_NO_HEARTBEATS.

Issues

View all issues
Summary
Calendar
Gantt

Watchers (1) Add

Kazumasa Taira

現在の会員

組織会員

- ・ Internet Initiative Japan
- ・ KDDI R&D Labs.
- ・ National Institute of Information and Communication Technology
- ・ SECOM CO., Ltd.
- ・ NEC Corporation
- ・ Nippon Telegraph and Telephone Corporation
- ・ Hitachi Ltd.
- ・ Cybernetica AS
- ・ Royal Holloway, University of London
- ・ Information Promotion Agency

個人会員

- ・ Hideki Imai (Tokyo University)
- ・ Tetsuya Izu (Fujitsu)
- ・ Tetsutaro Uehara (Ritsumeikan University)
- ・ Akira Otsuka (AIST)
- ・ Yusuke Kawamoto (AIST)
- ・ Ryoichi Sasaki (Tokyo Denki University)
- ・ Satoru Tezuka (Tokyo University of Technology)
- ・ Shin Nakajima (NII)
- ・ Hagihara Shigeki (Tokyo Institute of Tech.)
- ・ Masami Hagiya (Tokyo University)
- ・ Yoshikazu Hanatani (Toshiba)
- ・ Kanta Matsuura (Tokyo University)
- ・ David Basin (ETHZurich)
- ・ Cas Cremers (Oxford)
- ・ Thomas Hardjono (MIT)
- ・ Shigeo Mitsunari (Cybozu Lab.)
- ・ Kenichi Arai (Tokyo University of Science)

日本以外の会員の分布



2014年の活動内容

- ・ 暗号プロトコルの仕様に関する脆弱性に関する議論とレポートの発行
 - * 速報レポート
 - * 国際標準化への報告
- ・ コンソーシアムメンバーの新規提案プロトコルの評価
- ・ プロトコル評価結果の知識ベースProtocol Zooの作成

2014年度の脆弱性に関する議論

Date	Title	Action taken
02/16/2014	Attack on mechanism in ISO/IEC 11770-4	議論の結果レポートの必要無しと判断
03/04/2014	New attack on TLS?	速報レポートを発行
03/19/2014	Attacking the iOS 7 early_random() PRNG	重大な議論はなし
03/24/2014	WPA2 wireless security cracked	重大な議論はなし
04/08/2014	Heartbleed Bug on OpenSSL -1.0.1f	速報レポートを発行
05/02/2014	Exposing WPA2 Paper	重大な議論はなし
05/27/2014	Some supersingular curve DLP algorithms broken	重大な議論はなし
06/05/2014	CVE-2014-3466 (GNUTLS-SA-2014-3)	速報レポートを発行
06/06/2014	OpenSSL patches are available	速報レポートを発行
08/06/2014	The BEAST Wins Again. (Blackhat)	速報レポートを発行
10/14/2014	Hearing whispers we're going to hear about flow in SSLv3. (POOLDE)	速報レポートを発行
12/11/2014	The POODLE bites again	速報レポートを発行
03/04/2015	FREAK Attack	速報レポートを発行
03/20/2015	New vulnerability on OpenSSL	速報レポートを発行

POODLEのケースにおける対応

日時 (JST)	Action
10/14, 18:39	POODLE攻撃に関する情報をTwitterで把握。技術WGのオンライン議論システムに投稿し、影響の議論を開始。
10/15, 14:04	速報レポートの作成開始
10/15, 15:28	速報レポートドラフト第1版
10/15, 21:48	速報レポートドラフト第2版 攻撃成功の条件と可能性についての重要な記述を追加
10/15, 22:20	速報レポートドラフト第3版、製品名の追加
10/15, 22:20	英語版、日本語版の修正
10/15, 22:52	最初の速報レポートの公開(約28時間後)
10/15, 23:09	OpenSSLの新しいバージョンに関する情報の追加
10/16, 10:07	エディトリアルな誤りの訂正

CELLOSにおける速報レポート

英語版と日本語版を同時リリース



国際標準化への報告

- ・ ISO/IEC standardsに関する2つの脆弱性について検討
- ・ 修正に関するレポートをISO/IEC SC27/WG2に提出(日本エキスパートを通じて)

ISO/IEC標準	レポートの内容と対応	ISO/IEC SC27/WG2でのアクション
ISO/IEC 11770 (Key-management mechanisms)における攻撃	ETH Zurichの修士論文で指摘されたISO/IEC 11770の脆弱性. 指摘の正しさをCELLOSで確認	セキュリティ要件に関するStudy periodに対して、確認した内容を寄書として提出
ISO/IEC 11770-2/3	Dr. Cas Cremers(Oxford)が形式検証を行った結果攻撃を発見し、プロトコルの修正と安全性の定義の修正提案。内容の正しさをCELLOSで確認.	11770-2/3に対するTechnical Corrigendumの作成と、新たなセキュリティ要件についてのDefect Reportを寄書として提出。修正中。

コンソーシアム会員提案のプロトコルの評価

- ・ コンソーシアム会員から提案があったプロトコルについて、WG内で評価。
- ・ WG内で、提案者を除く評価チームを組織し、形式検証を実施
- ・ 評価レポートはWebサイトで公開予定
- ・ コンソーシアム会員は、将来の標準化提案における補助資料として活用可能

プロトコル評価結果知識ベース“Protocol Zoo”の構築

- ・ 技術標準となっている暗号プロトコルのリスト
- ・ 各プロトコルについて、現状のセキュリティの状況（攻撃の有無など）を示す。（オンライン検索可能に）
- ・ 最初のバージョンとしてSSL/TLS関連について構築中



2015年度以降の活動

- ・ 標準の暗号プロトコルの脆弱性に関する論文、技術文書の継続的な監視、事実の確認と速報レポートの発行（CELLOSの機動的な体制を活かした活動）
- ・ 技術WGにて、TLS1.3勉強会を実施し、プロトコル評価結果を11月のIETF Meeting(@横浜)に入力。（CELLOSの国際的中立性を活かした活動）
- ・ コンソーシアム会員からの新規提案プロトコルの評価
- ・ “Protocol Zoo”の作成と拡充
- ・ CRYPTRECとの連携（評価結果の迅速な共有など）

CRYPTRECとの連携方策(私案)

CELLOSの活動のうち、以下の活動についてはCRYPTRECとの連携が有効と考えられる。

① 暗号プロトコルの攻撃手法情報の集約・安全性評価

CELLOSで実施している活動

- 学会発表等、情報を集約し「速報」として発表
- 「速報」として報じた情報に対する詳細検討・安全性評価結果の提示

⇒CRYPTRECとの連携が可能ではないか

例えば、CRYPTRECに入力された速報等をもとに、対応策を審議するなど

② 安全な暗号プロトコルの利用促進(普及・広報活動)

CELLOSで実施している活動

- 安全性の評価結果が活用されるための方策を検討

⇒CRYPTRECとの連携が可能ではないか

例えば、CRYPTRECに提示された評価結果をもとに、暗号技術の利用促進の観点から安全な暗号プロトコルの利用促進に努める活動を実施するなど

サービス視点からの暗号技術（の重要性）

2015年 6月 24日

松本 泰 セコム（株）IS研究所



松本の自己紹介

- 所属 セコム(株) 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
- 1984年 UNIX上のビデオテックス・パソコン通信システムの開発に従事
- 1994年 各種インターネットサービスの設計、開発、運用に従事
- 1999年 サイバーセキュリティ事業の立ち上げに従事
- 2003年-2007年
 - 工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授
- 2005年 金融庁 偽造カード問題に関するスタディーグループ・メンバー
- 2007年 経済産業省商務情報政策局長表彰「情報セキュリティ促進部門」受賞
- 2007年-2012年 IPA 情報セキュリティ分析ラボラトリー非常勤研究員
- 2011年-2012年
 - 社会保障・税に関わる番号制度 情報連携基盤技術WG 構成員
 - 社会保障・税に関わる番号制度 社会保障分野サブWG 構成員
- 2015年3月現在
 - 内閣官房 パーソナルデータに関する検討委員会・技術検討ワーキンググループ構成員
 - 日本データセンター協会 セキュリティWGリーダ、ファシリティインフラWGサブリーダ
 - 保健医療福祉情報システム工業会: JAHIS セキュアトークンWGメンバー
 - IEC/AAL (Ambient Assisted Living) 国内委員会 委員
 - NPO 日本ネットワークセキュリティ協会 PKI相互運用技術WGリーダ
 - 暗号技術検討会 (CRYPTREC) 構成員、暗号技術評価委員会委員
 - 電子署名法研究会 構成員

サービス視点からの暗号技術

- 「CRYPTRECの在り方」を考える上で、暗号技術が、現在の社会においてどのように使われているか。また、今後の社会においてどのように使われていくべきなのか。こうした暗号技術と社会との関わりが俯瞰された上で検討されることが望ましい。
- しかし、暗号アルゴリズム評価等の暗号技術に要求される高度な専門性や、暗号技術が既に社会基盤に深く広く取り込まれているという現実等から、この「暗号技術と社会との関わりの俯瞰」は容易ではない。
- ここでは、「サービス視点からの暗号技術」を説明することにより、「暗号技術と社会との関わりの俯瞰」の手助けとなることを考えたい。

サービス視点からの暗号技術 目次

- (1) セコム（株）IS研究所における暗号技術の取り組み
 - サービス視点からの暗号技術へのアプローチ
- (2) IoT/CPS時代の暗号技術の考察
 - オープン化や情報連携に対応するための「暗号技術によるトラスト」
- (3) 暗号技術とデータセキュリティ
 - 暗号技術によるデータセキュリティの分類
- 参考

セコム（株）IS研究所における 暗号技術の取り組み

サービス視点からの暗号技術への アプローチ

セコム（株）IS研究所における サイバーセキュリティと暗号技術の取り組み

- Security - 主に「サイバーセキュリティグループ」
 - インシデント情報の収集
 - 脆弱性対策
 - セキュリティ・バイ・デザイン
- Trust - 主に「暗号・認証基盤グループ」
 - 暗号技術によるトラスト（信頼関係）の構築
 - 認証、署名、暗号化 技術等
- Privacy - 主に「スマートコンピューティンググループ」
 - ビッグデータ、パーソナルデータの対応
 - 様々な情報連携における個人情報保護と利活用
 - プライバシー・バイ・デザイン

「暗号技術の取り組み」で目指しているところ 社会基盤としての暗号技術 Big Picture

デジタル時代の
日本の社会？



効率的で、透明性があり
競争力のある社会？



デジタル時代の
社会サービス

Trust が必要な様々な社会サービス

デジタル時代の
社会基盤

暗号技術を利用したエコシステム(のための基盤)

デジタル時代の
(信頼のための)
フレームワーク

標準化

実装

法制度

デジタル時代の
要素技術

コアとなる暗号技術 etc..

IoT/CPS時代の暗号技術の考察

オープン化や情報連携に対応するための「暗号技術によるトラスト」

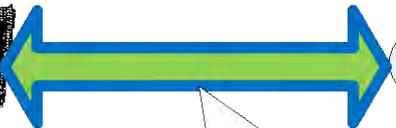
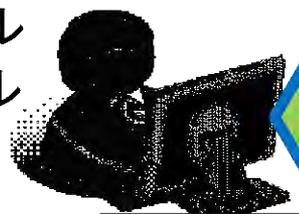
IoT/CPS時代の暗号技術の考察

暗号技術によるトラスト

- 暗号技術は、セキュリティのためというよりは、様々なサービスにおけるステークホルダーを結びつけるトラストのために必要になる。
- トラストは、多くの場合、物理セキュリティ環境と、暗号技術による暗号鍵の関係性等により構築されている。
- IoT時代において、IoT機器は「弱い物理セキュリティ環境」において多く利用されることが想定され、そのため暗号技術によるトラストが重要になる。
- 「弱い物理セキュリティ環境」で使用するIoT機器は、物理的攻撃に強い、耐タンパーなセキュリティエレメント等に格納された暗号鍵・クレデンシャルが非常に大きな役割を果たす。
- IoTのサービスモデル・ビジネスモデルは、暗号技術によるトラストの構造であるトラストモデル（信頼関係モデル）と非常に関係が深い。
- こうしたことも含め、暗号技術は、IoTのセキュリティというよりは、IoT自体の実現、また、IoTによるイノベーションのために重要になる。

暗号技術によるトラストの典型例

サービスモデル
ビジネスモデル



インターネット上で、人とサービス間の
トラスト(信頼関係)を作りたい

ビジネスレイヤー

実装レイヤー - 暗号技術等によるトラスト

家という物理的環境(物理的なトラスト)

データセンターという強固な物理的環境
(物理的なトラスト)

脳に記憶され
た秘密の鍵
(弱い鍵・
パスワード)



ROOT証明書

TLS

TRUST

Web証明書

プライベート鍵

ユーザの
秘密の鍵
パスワード

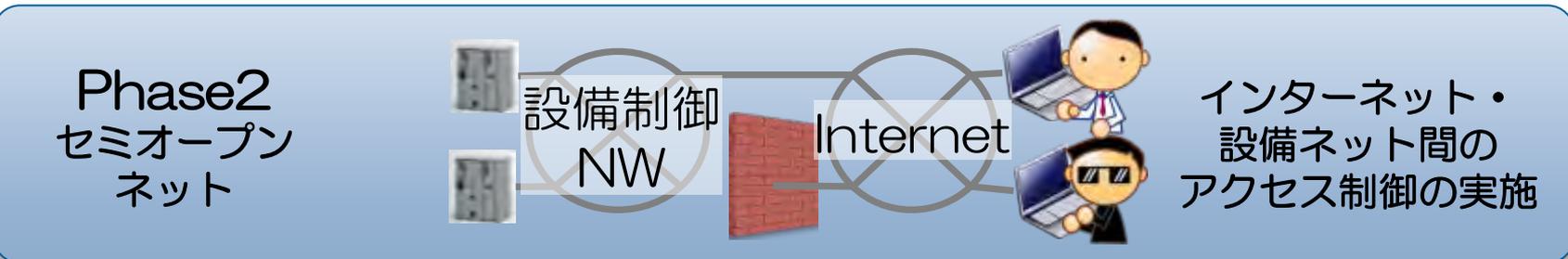


端末(PC等)に格納されたトラ
スタアンカーとなるルート証明書
(証明書に格納された公開鍵)

暗号鍵の関係で構築さ
れるトラスト・信頼関係。
利用者がサービスを
信頼(認証)する

Web証明書に格納され
る公開鍵に対応する
プライベート鍵

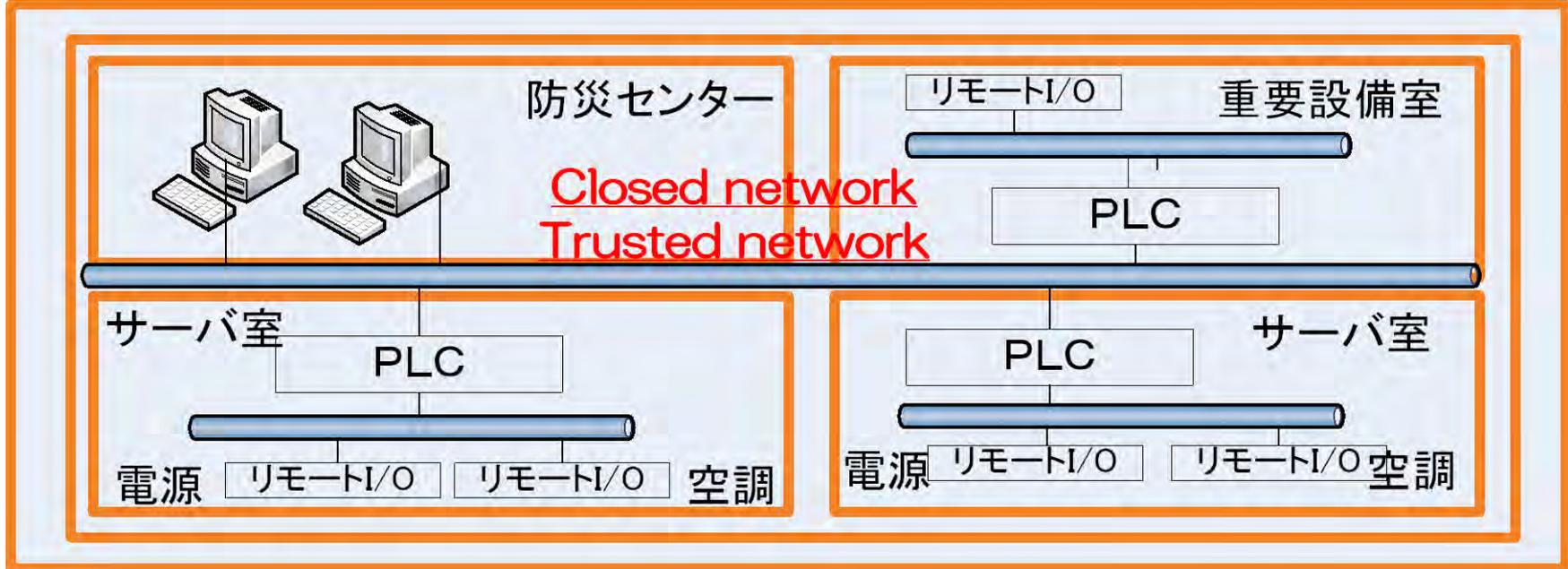
- 設備制御システムのネットワークセキュリティの現状調査と基準作り
- M2M時代のデータセンターを見据えた、設備制御システムのアーキテクチャとセキュリティの検討



典型的な制御システムにおけるトラスト

≡ 暗号技術を使わないトラスト・Trusted network
 (→ ボーダーを突破されると非常に脆弱)

重要施設という物理的環境・物理的なゾーニングによるトラスト

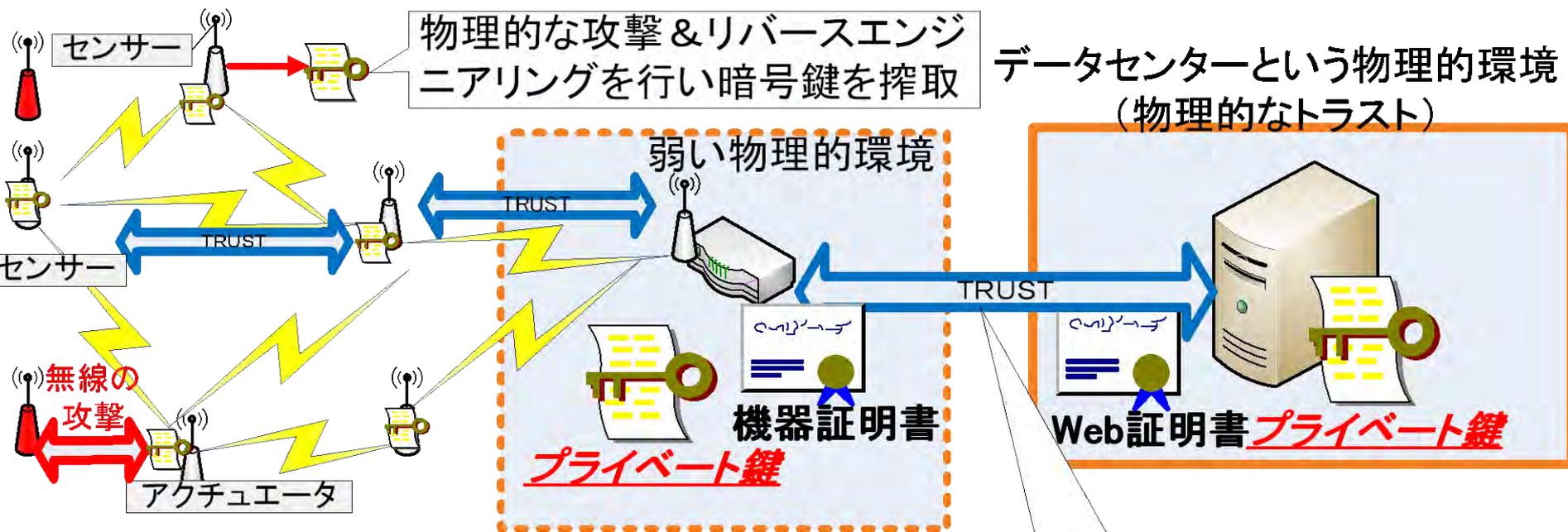


ファシリティ系のネットワークではBACnet等のプロトコルが利用されるが、多くの場合、暗号技術による機器認証等は実装されていない。



IoT/CPS時代の暗号技術によるトラスト

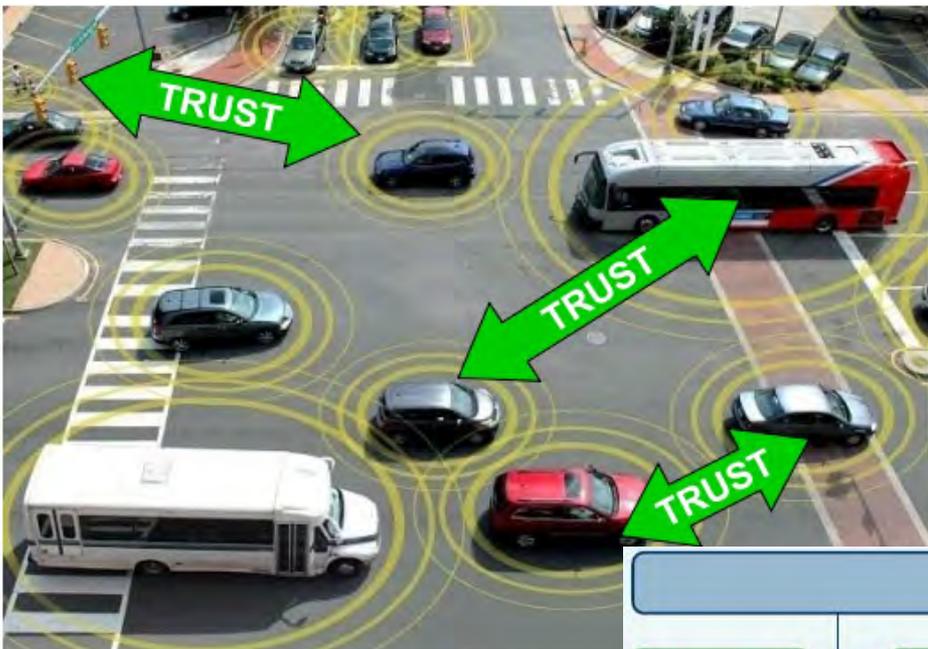
IoT機器が、「弱い物理セキュリティ環境」において多く利用されることが想定 → ハードウェアセキュリティの重要性



暗号鍵の関係で構築されるトラスト・信頼関係。機器がサービスを信頼(認証)し、サービスが機器を信頼する



自動車の場合（車車間、車載装置間のトラスト）



車載装置間の信頼 (Trust)

出典：Infineon社
Automotive (R)evolution: Defining a Security Paradigm in the Age of the Connected Car
https://www.infineon.com/dgdl/car_security_white_paper111914_lowres.pdf?filed=5546d4614bcaeb6014bef227039027d

PRESERVE : Preparing Secure Vehicle-to-X Communication Systems

出典：PRESERVE-Score@F Workshop

車車間、
車と外部の信頼
(Trust)
V2V, V2I

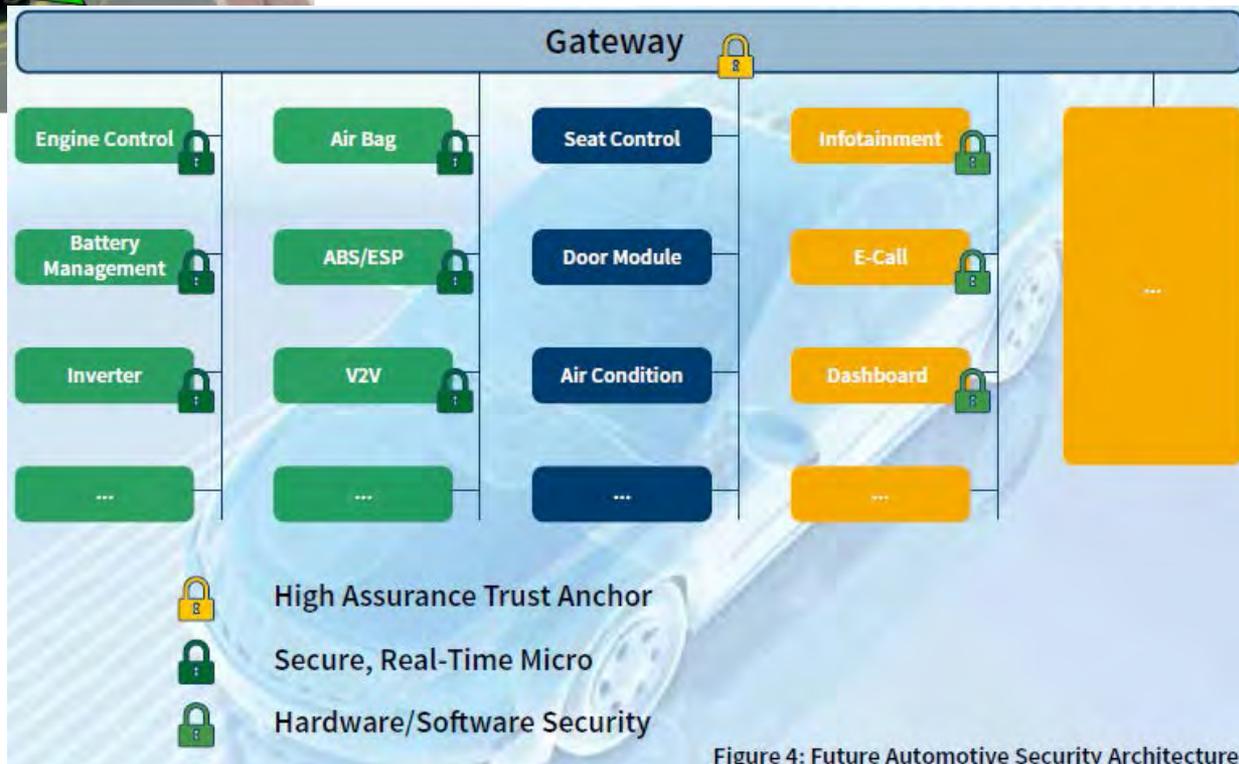
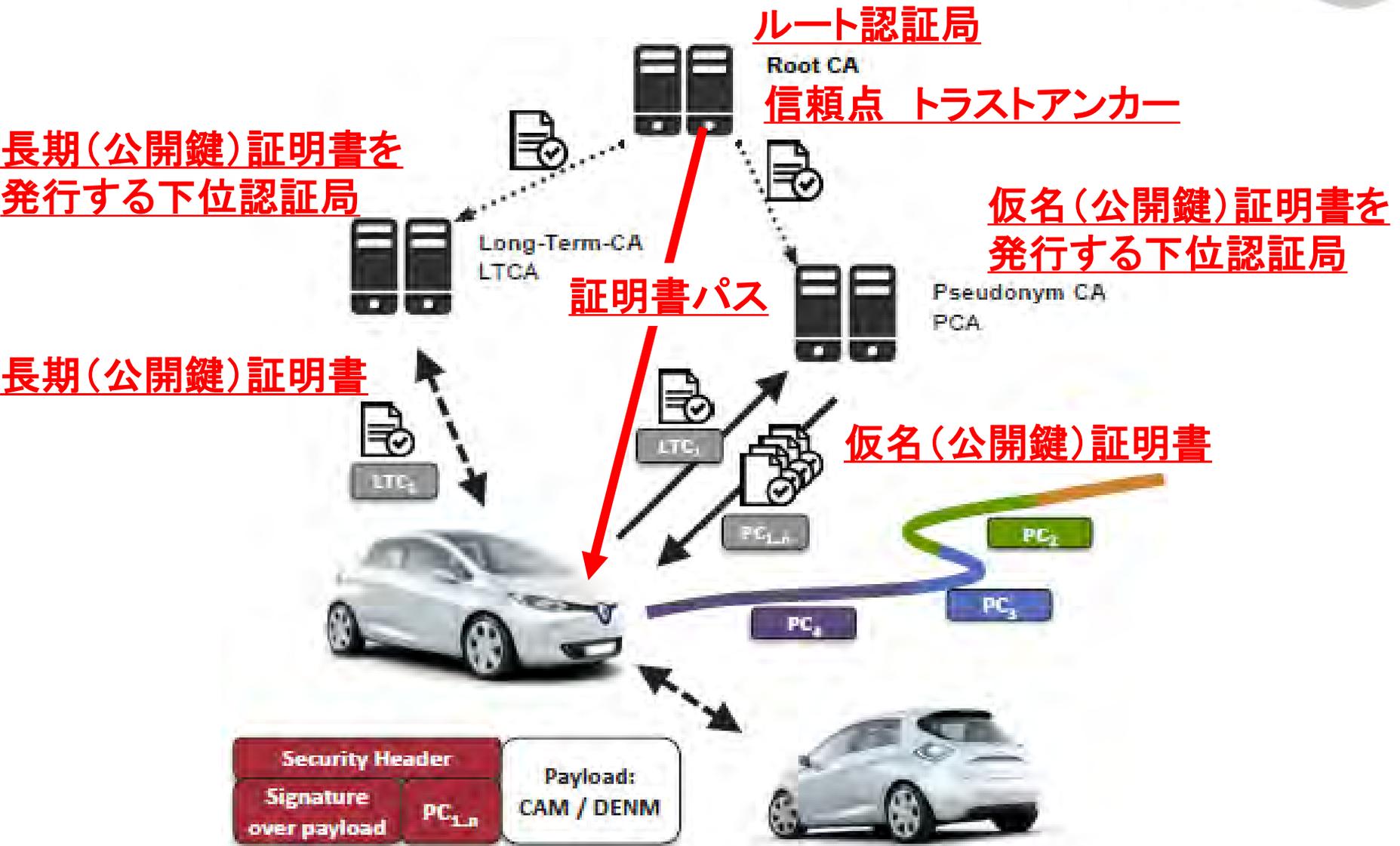


Figure 4: Future Automotive Security Architecture

自動車の場合（車車間、車と外部の信頼 TRUST） PRESERVE（欧州のプロジェクト）の実証実験



出典: PRESERVE-Score@F Workshop

自動車の場合 - パラダイムシフト イノベーションのために暗号技術が重要になる??

コスト削減、保守性の向上などの要求に対応する技術戦略

- 独自仕様の装置
- 独自のインターフェース

- コモディディ化した部品、装置の採用・調達
- オープンな標準化されたインターフェース (ex. OBD II ポート)

利用者ニーズに対応するビジネス戦略、サービス戦略

- 独自のサービスとの連携
- クローズドな専用の機器

- 外部の多様なサービスとの連携
- 利用者の多様な IT 機器の利用

攻撃者にとってもシステムを
類推しやすい状況へシフト

サイバーセキュリティの考え方のパラダイムシフト

- 物理的に守られた信頼関係
 - ex. 車の中、専用線
- 設計の秘密で守る

- 設計の秘密が最小限
- 暗号技術等によるトラストの構築
(= **ビジネス戦略でもある**)

自動車の場合 — 攻撃のシナリオと対策？

- (信頼できない) 外部のサービスAとの接続(V2V,V2I)
 - 信頼関係ない外部のサービスと接続されてしまう問題
 - ⇒ 外部のサービスとの間のトラストの確立 (暗号技術等)
- 外部のサービスに接続される脆弱な車載装置Bへの攻撃 (乗っ取り)
 - 脆弱な車載装置が組み込まれてしまう可能性
 - ⇒ 脆弱な車載装置を作らない (セキュリティ・バイ・デザイン)
 - ⇒ 車載装置の脆弱性対応 ⇒ プログラムコードの更新
 - ⇒ 信頼できるコードの検証 (コード署名の検証)
 - » ⇒ 車載装置のRoot of Trust の (ハードへの) 組み込み
 - 車載ネットワークのオープン化で、誰もが車載装置を作ってしまう問題
 - ⇒ 車載装置の認証 (Certification)
 - 認証 (Certification) された車載装置のみを接続する
 - ⇒ 車載装置間のトラスト等 (暗号技術等)
- 車載装置Bから、自動車の重要な制御を行う車載装置Cへの命令
 - ⇒ 車載装置間のトラスト等 (暗号技術等)

自動車のセキュリティのふたつの戦略？

#現実には、（たぶん）折衷案になる?????

• その1

- 技術戦略 独自技術
 - 独自のインターフェース
- ビジネス戦略、サービス戦略
 - 限られた（コントロールされた）外部のサービスとの連携
 - クローズドな周辺製品。
- セキュリティ（トラスト）の戦略？
 - （車の内部という）物理的に守られた信頼関係
 - 設計の秘密で守る

• その2 — より暗号技術によるトラストが重要

- 技術戦略 オープンな技術
 - オープンな標準化されたインターフェース
 - コモディティ化した部品、装置の調達
- ビジネス戦略、サービス戦略
 - 多様な外部のサービスと連携する
 - 利用者の多様なIT機器を利用する
- セキュリティ（トラスト）の戦略？
 - 暗号技術で守る
 - 暗号技術によるトラストの構築（＝ビジネス戦略）

IoTサービスのレイヤーと暗号技術

サービスの観点	暗号技術の観点	セキュリティの観点	備考
IoTサービスの運用	暗号技術が組み込まれたシステムの運用。特に暗号鍵のライフサイクル管理、長期的な運用	<ul style="list-style-type: none"> セキュアな運用 脆弱性対応 PDCA 	信頼できる暗号鍵・トラストアンカーを基点にプログラム更新等を行う（Root of Trust の重要性）
IoT機器・クラウドサービスの設計・開発・実装	<ul style="list-style-type: none"> 暗号技術を組み込んだ機器などの実装 耐タンパー性 	<ul style="list-style-type: none"> セキュリティ・バイ・デザイン プライバシー・バイ・デザイン 	暗号技術特有の実装の難しさの問題等がある
ビジネスモデル サービスモデル	暗号技術による信頼モデル(信頼関係モデル)	物理セキュリティと暗号技術による信頼モデル	サービスのライフサイクルと暗号鍵のライフサイクル等の基本設計

- IoTは、「物理セキュリティによるトラスト」から「暗号技術によるトラスト」へのパラダイムシフト → 自動車の場合 slide 17
 - 大量のIoT機器を接続するラストワンマイル、ラストワンメートル等での無線の要求 → 必然的に暗号技術によるトラストが重要になる
- IoTサービス -- 多くのステークホルダーを結びつけるトラストの重要性
 - 自動車の場合（車車間、車載装置間のトラスト） slide 15
 - エコシステムにおけるステークホルダー間のトラスト
 - ⇒ 参考 「暗号技術とビジネスモデルの関係」
- IoT機器における暗号技術の要求
 - 限られたリソースでの暗号技術の実装、様々なトレードオフが必要な環境下での実装 -- 省電力無線+省電力暗号、軽量暗号、低遅延暗号、etc.. の要求
 - 「弱い物理セキュリティ環境」で使用を想定したハードウェアセキュリティ、プログラムコードの更新等のためのRoot of Trust の重要性
- IoTサービスの運用 -- 信頼における暗号鍵の運用と運用コストの最適化
 - 大量のIoT機器・大量の暗号鍵の管理、信頼における鍵配布の重要性
 - Trust provisioning チップの設計、製造からサービス運用まで
 - 「セキュリティ」と「サービス容易性」のトレードオフの設計
 - サービスの運用コストを最適化するための暗号技術、暗号鍵管理
- IoTにおけるプライバシー保護技術 -- 仮名証明書、グループ署名・匿名認証等

暗号技術とデータセキュリティ

- 移動中のデータ Data in Motion
- 保管データ Data at Rest
- 使用中のデータ Data in Use
- データの処分 Data Disposed

データセキュリティのドメインに対応した NISTガイドラインの例

ドメイン	ガイドラインの例	対象・備考
移動中のデータ (Data in Motion)	NIST SP800-52	TLS
	NIST SP800-77	IPsec VPNs
	NIST SP800-113	SSL VPNs
保管データ (Data at Rest)	NIST SP800-111	Storage Encryption for End user
使用中のデータ (Data in Use)	なし ?	クラウドサービスにおける暗号技術の応用のほか、プライバシー保護データマイニング (PPDM) 等の応用が考えられる
データの処分 (Data Disposed)	NIST SP800-88 Rev.1	電子メディアの破壊等 2.6節 Use of Cryptography and Cryptographic Erase

HITECH Breach Notification Interim Final Rule

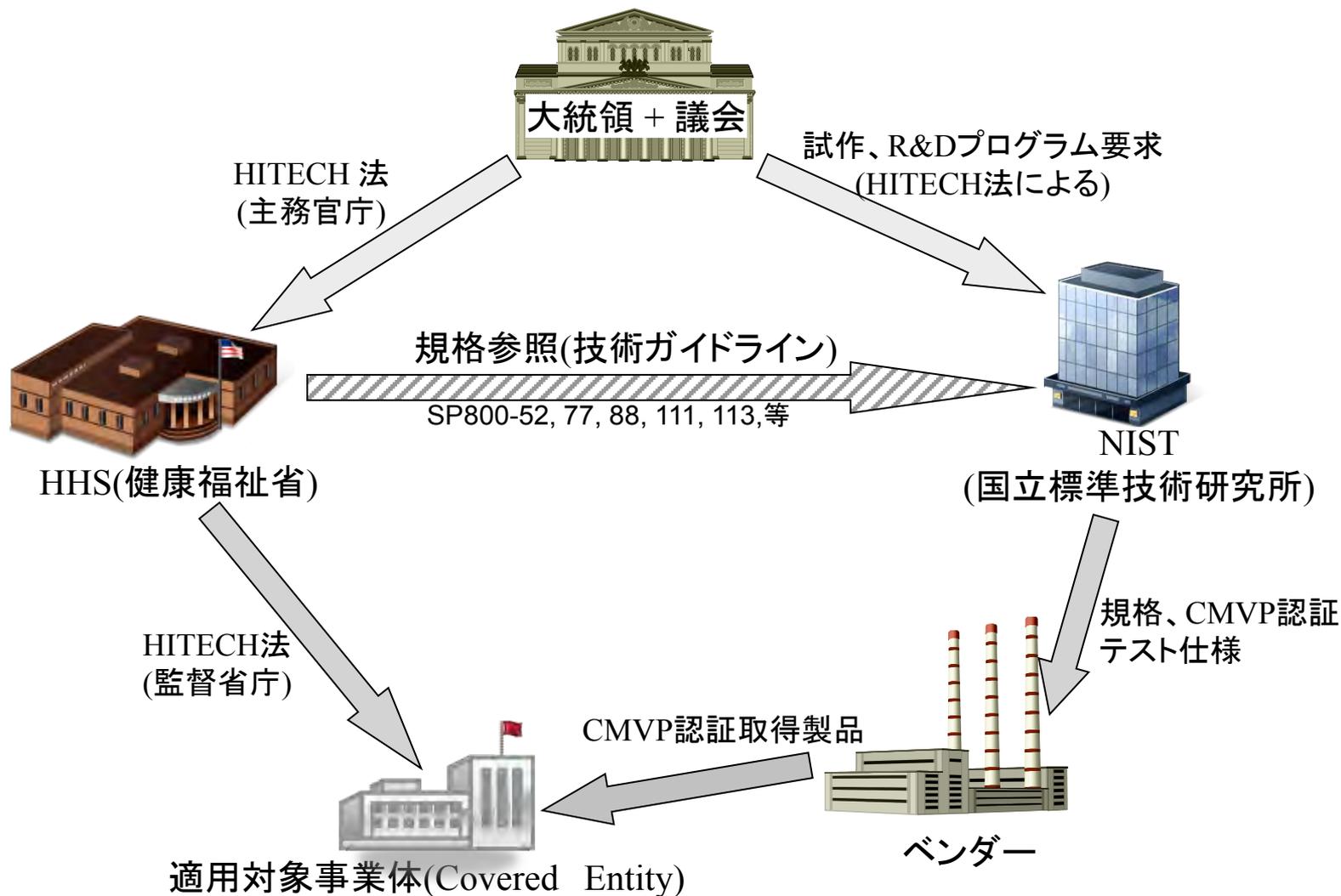
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html>

- ・ (a) HIPAA遵守義務で記述される **暗号化された電子PHI** について、… (略)
 - (i) 有効な手続きで暗号化された「**保管データ (data at rest)**」は **NIST SP800-111** “Guide to Storage Encryption Technologies for End User Device” が該当する
 - (ii) 有効な「**移動中のデータ (data in motion)**」は、 **NIST SP800-52** “Guideline for the Selection and Use of Transport Layer Security (TLS) Implementation”, **800-77** “Guide to IPsec VPNs”, **800-113** “Guide to SSL VPNs”, その他 **FIPS 140-2** 認定を適切に使う事により満たす
- ・ (b) PHIが保存または記録された媒体は、以下の方法の何れかで破壊されないといけない、これは「**データの処分 (data destruction)**」を意味する
 - (ii) 電子媒体は、 **NIST SP800-88** “Guidelines for Media Sanitization” により、PHIが復元できないように、削除、消去、又は破壊されなければならない。

PHI : protected health information

HIPPAの主務官庁はHHS（健康福祉省）であるが、NISTのガイドラインが参照され重要な役割を果たしている。またHIPPAにおけるPHIの漏えいに対する厳しい罰則などから、ガイドラインの遵守等の強制力が働いている。

米国におけるスキーム 重要なNISTの（ガイドラインの）役割



参考資料

- 暗号技術とビジネスモデルの関係
 - 「暗号技術によるトラスト」と「ビジネスモデル」の関係の説明
- PKI Day 2015「サイバーセキュリティの要となるPKIを見直す」
 - 2015年4月10日に開催されたPKI day 2015での松本の発表資料 (http://www.jnsa.org/seminar/pki-day/2015/data/0_matsumoto.pdf) の抜粋
- 暗号技術による個人情報保護の制度と技術の動向
 - 2012年10月25日に開催された中央大学研究開発機構・情報通信技術研究会での松本の発表資料の抜粋
 - NPO JNSAの機関誌 JNSA Pressの寄稿「暗号技術による個人情報保護の制度と技術の動向」
 - http://www.jnsa.org/jnsapress/vol34/3_kikou.pdf

暗号技術とビジネスモデルの関係

「暗号技術によるトラスト」と
ビジネスモデルの関係

SSL証明書に関連したステークホルダー

- (1) PC利用者等
 - PC利用者、携帯利用者、機器利用者
 - モチベーション：Webサービスを安心して利用したい。
- (2) Webサーバ提供者・SSL証明書利用者
 - 様々なサービス：民間、金融、行政、etc..
 - モチベーション：利用者に安心してサービスを提供したい
- (3) SSL証明書を発行する認証局
 - 古くからの認証局、比較的新しい認証局
 - モチベーション 証明書発行による収益
- (4) 信頼点（ルート証明書）を組み込むベンダー
 - PCのOS/ブラウザベンダー、携帯キャリア/ベンダー、その他の機器ベンダー（ゲーム機、地デジ）
 - モチベーション：提供する端末等を利用者に安心して利用してもらいたい
- (5) その他のステークホルダー
 - 認証局の監査会社等、業界毎の管轄官庁等

信頼点（ルート証明書）を組み込むベンダー

Microsoft ルート証明書プログラム - Microsoft の場合

- OS (MS-Windows) に組み込むルート証明書の基準を明確にした
- Windows-XP のリリース時より (2002 年)
 - つまり 2002 年以前は、基準と言えるものがなかった
- 「**Web Trust for CA**」による認証局の監査スキーム
 - しかし、SSL 証明書発行のための「審査の基準」などは規定していない
- 現時点の登録されているルート証明書
 - **300 以上** 非常に多くのルート証明書が登録されている
- 適用範囲外
 - マイクロソフトの製品である Windows Mobile
 - MS-Windows 版の Firefox 等
 - MS-Windows 以外のプラットフォーム、携帯。。。 Etc...

競争の中でのトラストの維持

モバイル
キャリア

メモリの関係から、よく使われるルート証明書だけを格納したい。



認証局



「全ての端末をサポート」して欲しいというお客様がいる限り古いルート証明書を使うしかない。

ブラウザベンダ

基準を満たしている限り、証明書リストに入れていくけど、暗号のことはどうしましょーね。後、古いOSは、勘弁してね？



信頼できる証明書なんて分らないからブラウザを信頼するしかない



利用者

とにかくPCも携帯も全ての端末をサポートして欲しい

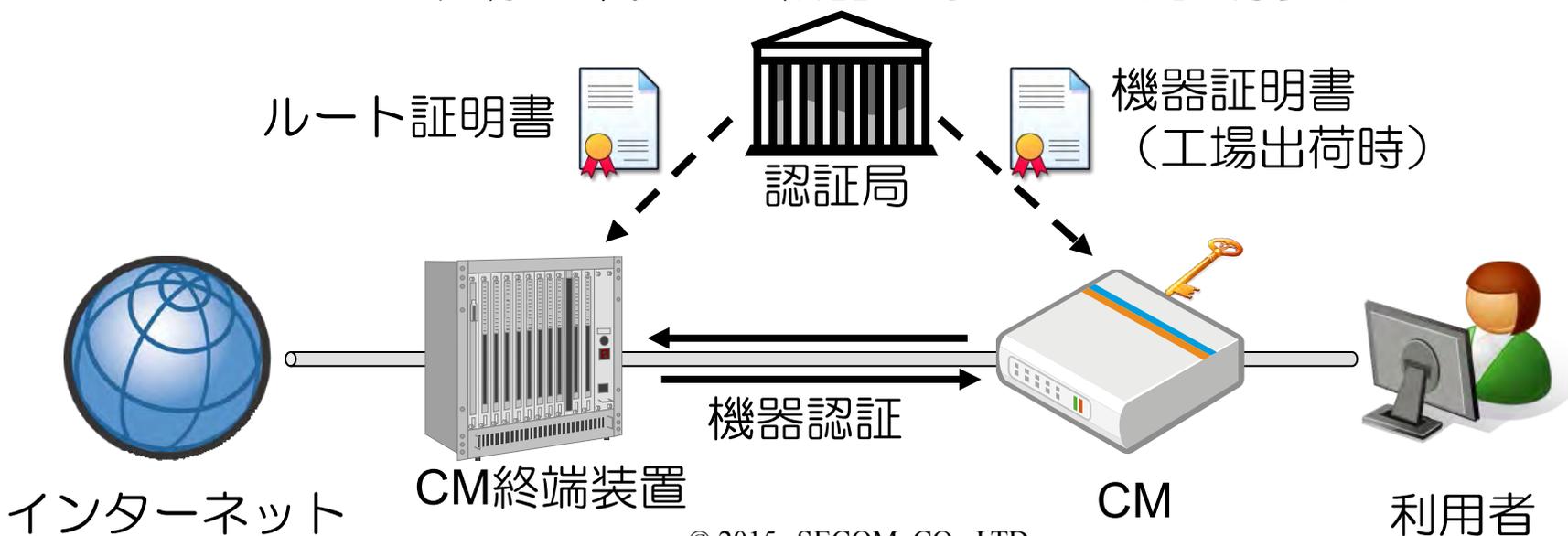


サーバ運営者



ケーブルモデム（CM）の機器証明書の事例

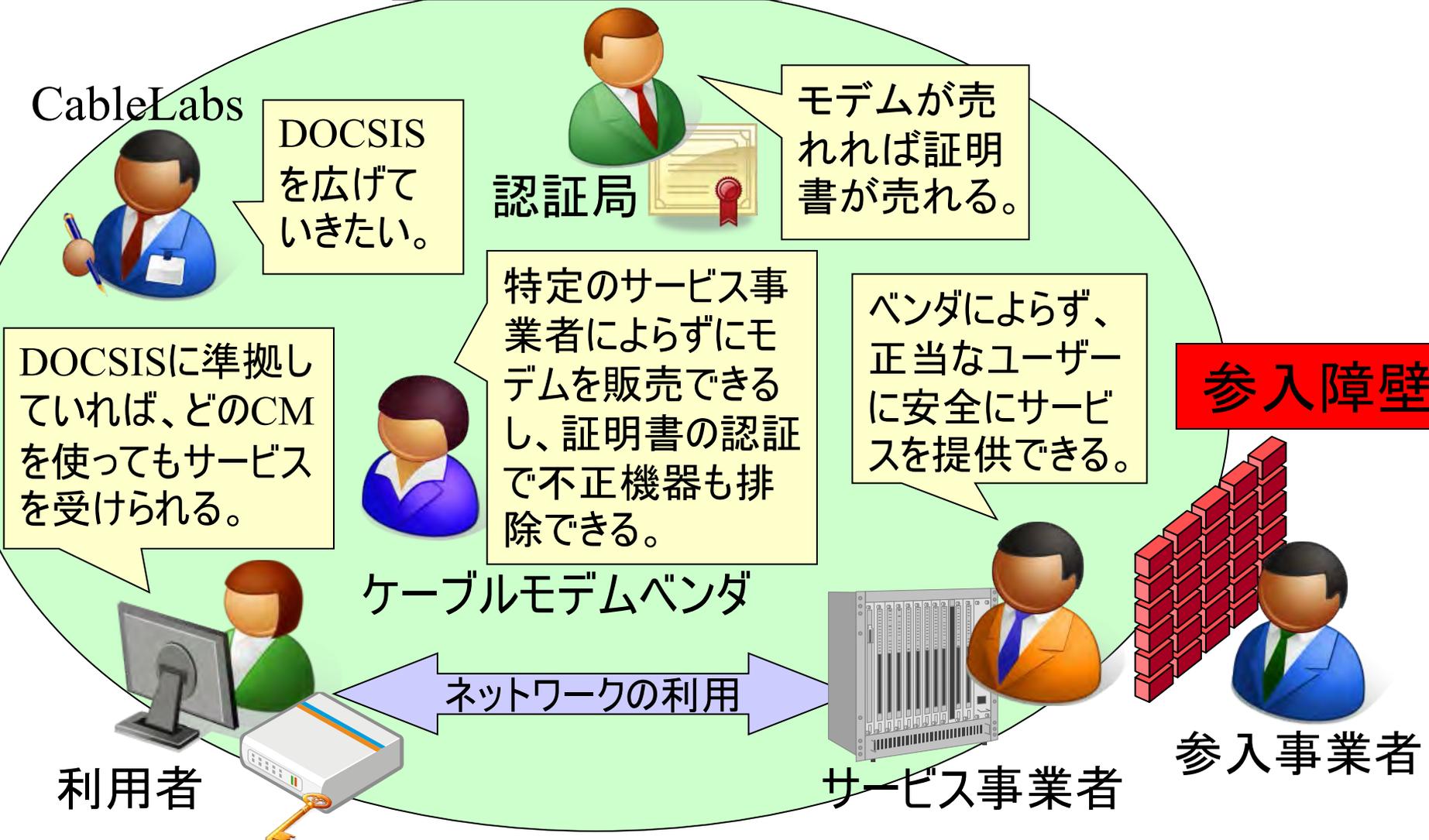
- ケーブルモデルの仕様
 - DOCSIS
 - Data Over Cable Service Interface Specifications
 - ケーブルテレビのネットワークを利用してデータ通信を行なうための技術仕様の業界標準
- Cable Labs(ケーブルラボ)
 - CATV機器の研究開発・認定のために設立された非営利団体
- ケーブルモデム（CM）の機器証明書
 - DOCSISの仕様に準拠した機器であることを証明する



- ケーブルモデム利用者
 - DOCSISに準拠した好みの機器（CM等）を利用できる
- CATVサービス事業者
 - CMの機器証明書の検証者
 - ルート証明書を保持している
 - 特定のベンダーに依存しないCM等の利用者にサービスを提供することができる
 - DOCSISに準拠したCMを識別できる
 - CM機器を特定できる（ベンダー、機器固有ID）
- ケーブルモデム（その他セットボックス）ベンダー
 - 工場出荷時にCMの機器証明書を組み入れる
 - 特定のCATVサービス事業者に依存せずに機器を利用者に提供できる
- Cable Labs(ケーブルラボ)
 - DOCSIS標準を広めることができる
- 認証局（証明書発行サービス）
 - 機器証明書を発行することによる売り上げ

CMとCATVキャリアに関する ステークホルダー

トラスの輪



2015年4月10日に開催されたPKI Day 2015
での松本のプレゼン資料からの抜粋
http://www.jnsa.org/seminar/pki-day/2015/data/O_matsumoto.pdf

PKI Day 2015 サイバーセキュリティの要となるPKIを見直す

2015年 4月 10日

松本 泰 セコム（株）IS研究所



サイバーセキュリティの要となるPKIを見直す 背景について

- サイバー空間の広がり、本格的なデジタル社会の到来
 - CPS (Cyber Physical System)、制御システム等のオープン化
 - 紙台帳前提の社会制度からデジタルデータ前提の社会制度へ
- サイバーセキュリティの重要性
 - 情報システムのための情報セキュリティだけでなく、より広範囲な制御システム、CPS等も含めたサイバーセキュリティ
- サイバーセキュリティの要であるトラストサービスの重要性
 - サイバー空間上のトラスト（信頼関係）の確立なくして、サイバー空間におけるセキュリティ確保はあり得ない。
- PKIの重要性
 - サイバー空間においてトラストを構築するための暗号技術の重要性
 - 多様なステークホルダー間のトラストを構築する公開暗号技術の重要性
 - 標準化された公開暗号技術であるPKIの重要性
- 多くの課題
 - 現状のトラストサービス(SSL/TLS関連等)の様々なほころび
 - トラストを構成する要素の整合（ビジネス・制度・技術等の整合）
 - 今後の社会における大量、多様なエンティティ間のトラスト

1部 新しい時代の電子署名

- 欧州のeIDAS
 - 欧州においては、1999年のEU電子署名指令 (Directive) から、より広範囲なトラストサービスを扱い、より強制力のあるeIDAS規則 (Regulation) へ
 - 欧州においては、個人情報保護法においても、EUデータ保護指令 から、より強制力のあるEUデータ保護規則 へ
 - EU域内におけるパーソナルデータの利活用と保護のためのEUデータ保護規則。同時に、パーソナルデータの利活用と保護・情報連携等を支えるトラストサービスのためのeIDAS規則
- 欧州におけるサイバーセキュリティ・トラストサービスの標準化と展開
 - eIDASのような規則（ないし規制）とETSI等での技術標準化がセットで検討されてきた
 - 強制力のある規則により、制度、技術、ビジネスの統合が難しいトラストサービスの展開を行っているように見える。
 - ex. 欧州における自動車のサイバーセキュリティ等も同様に見える？
- 欧州の規制モデル型 vs. 米国の市場モデル型
 - では、日本の立ち位置は？

第2部 SSL/TLS実装の今とこれから

- 近年のインターネット上の重要なトラストを提供しているSSL/TLSの様々な問題
 - 2008年 MD5不正CA証明書
 - 2011年 DigiNotar不正証明書発行事件、BEAST
 - 2012年 CRIME
 - 2014年 HeartBleed、POOLDE、CCS Injection
 - 2015年 FREAK
 - Etc……
- 背景
 - SSL/TLSの社会基盤化 → 攻撃対象へ
 - 暗号技術・暗号技術の組み込んだ実装の難しさ
 - トラストを構成する様々なステークホルダー
 - 競争の中でのトラスト、エコシステムによるトラストの難しさ
- では。。

3部 広がるサイバー空間に対応する PKIの新しい応用領域

- より社会基盤化するインターネットにおけるトラストの向上
 - インターネットは、暗号技術普及以前に広く普及したが、普及し社会基盤化する程に、より高いトラストが要求されるようになってきた
 - RPKI、DNSSEC
- 制御システム等のオープンネットワーク化
 - 従来の制御システム等は、物理的なセキュリティにより守られたクロードネットによりトラストを実現してきた
 - 閉じた世界の制御システム等に、多様な「繋がり」を求められている
→ 広く「繋がる」ためには、物理的なセキュリティだけでは実現できない (ex. 車の場合、ITS、自動運転等の要求で外部と接続)
 - 「繋がり」「オープンネットワーク化」では、PKI等の暗号技術によるトラストの構築が必要
- IoT時代の数百億のデバイス
 - 現在のSSL/TLSによるWebサイト認証やコード署名等以上に、大量で多様なエンティティ、そして多くのステークホルダー、そうした中での多様なトラストの構築

PKI day 2015のオーバビュー

3部 広がるサイバー空間に対応するPKIの新しい応用領域

時代の要請

マイナンバー
制度の時代

ビッグデータ
時代

IoT時代

行政サービス

医療サービス

金融サービス

Webサービス

電子契約書

医療記録

プログラム
(コード署名)

電子領収書

オープン化する制御システム

医療機器

ITS

車の車載器

IPルーティング

信頼が必要な
情報連携サービス

信頼が必要な
デジタルコンテンツ

数百億個のデバイスの
多様な信頼関係

トラスト
レイヤー

eIDAS

電子署名

タイムスタンプ

電子シール

電子配布

Webサイト認証

Web trust for CA

Webサイト認証

DNSSEC

RPKI

(広義の) トラストサービス

トラストを
構成する
要素

デジタル社会
のための
法制度

法制度と
整合性のある
標準化

信頼のおける
運用

セキュアな
実装技術

暗号技術等の
コア技術

1部 新しい時代の電子署名

2部 SSL/TLS実装の今とこれから

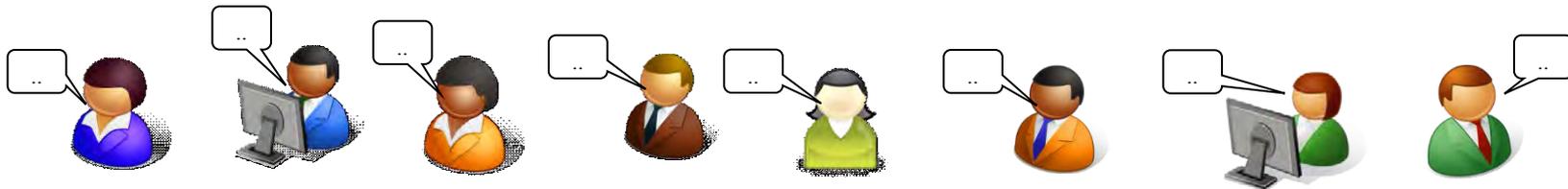
広義のトラストサービスへの期待と課題

- ニーズからのビュー（期待）
 - マイナンバー時代、ビッグデータ時代、IoT時代において、様々なトラスト（信頼関係）を必要としているサービスがある
- シーズからのビュー（課題）
 - 技術、制度、ビジネスの整合
 - トラストを構成する多くの要素の整合

暗号技術による個人情報保護の 制度と技術の動向

2012年10月25日

セコム(株)IS研究所 松本 泰



暗号技術による個人情報保護の制度と技術の動向

- ・ 個人情報を適切に保護するための暗号技術については、個人情報保護法が施行された当時から現在に到るまで、様々な議論があったようです。個人情報に限らず、暗号技術により情報を保護するためには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」、これらそれぞれが適切である必要があります。そうならば、暗号技術による個人情報保護は、非常に有用なものになります。
- ・ 7月3日に開催された「JNSA／第2回 鍵管理勉強会」ではこうした暗号技術・鍵管理技術のあるべき姿と、これらの技術が制度にどう組み込まれていくべきか等を念頭に、勉強会のひとつのテーマとして「暗号技術による個人情報保護の制度と技術の動向」を取り上げ、議論を行いました。
- ・ 本稿では、鍵管理勉強会の議論も踏まえ、日本と米国の状況を説明し、今後の日本における課題を考察します。

寄稿

暗号技術による個人情報保護の 制度と技術の動向

セコム株式会社 IS 研究所
松本 泰、伊藤 忠彦

1. はじめに

個人情報を適切に保護するための暗号技術については、個人情報保護法が施行された当時から現在に到るまで、様々な議論があったようです。個人情報に限らず、暗号技術により情報を保護するためには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」、それらすべてが適切である必要があります。

それにより特定の個人を識別することができることとなるものを含む。)をいう。

法第 20 条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

—http://www.jnsa.org/jnsapress/vol34/3_kikou.pdf

米国 HITECH法の個人情報漏通知ルール HITECH Breach Notification Interim Final Rule

- 個人情報漏洩に対して厳しい通知義務
- 「個人情報」が守られている状態の定義
- NISTが提供する技術ガイドライン

米国のHITECH法 - 厳しい通知義務

Health Information Technology for Economic and Clinical Health Act

- ・ 2009年に成立した米国再生・再投資法（American Recovery and Reinvestment Act、ARRA）の一部として成立したHealth Information Technology for Economic and Clinical Health（HITECH） Actでは、HIPAA遵守義務がある医療機関・保険者などの組織に対して、情報通信の機密性に関する追加要項が課せられている。
- ・ 中でも、特に個人情報・プライバシー保護との関連性が高い要項として、同法は保護医療情報（PHI）が漏洩した場合には対象者全員への通報を義務付けるとともに、うち500人以上のPHIの漏洩した場合に、HHS（Department of Health and Human Services）及びメディアに対して通報を行うよう義務付けている、という点がある。

PHI: protected health information

出典： ニューヨークだより 2012 年 6 月
米国における個人情報・プライバシー保護・活用の動向
<http://www.ipa.go.jp/about/NYreport/201206.pdf>

HITECH Breach Notification Interim Final Rule

- 情報が安全でなく(unsecure)、HHS 及び FTC (Federal Trade Commission)に通報義務が発生する事態を明示するため、HHSはPHIについてのガイドラインを更新し、認証されないユーザが使用、判読、または復号できなくするための、暗号化と破棄についての技術と方法論を記載している
- 上記でHHSとFTCは、それらの情報が漏洩しても、ガイドラインに記載される方法による暗号化又は破棄が施されているならば、安全(secure)な医療情報であるとしている

HITECH Breach Notification Interim Final Rule

- (a) HIPAA遵守義務で記述される暗号化された電子PHIについて、…（略
 - (i) 有効な手続きで暗号化された「保管データ (data at rest)」は NIST SP800-111 “Guide to Storage Encryption Technologies for End User Device” が該当する
 - (ii) 有効な「移動中のデータ (data in motion)」は、NIST SP800-52 “Guideline for the Selection and Use of Transport Layer Security (TLS) Implementation”, 800-77 “Guide to IPsec VPNs”, 800-113 “Guide to SSL VPNs”, その他 FIPS 140-2 認定を適切に使う事により満たす
- (b) PHIが保存または記録された媒体は、以下の方法の何れかで破壊されないといけない、これは「データ破棄 (data destruction)」を意味する
 - (ii) 電子媒体は、NIST SP800-88 “Guidelines for Media Sanitization” により、PHIが復元できないように、削除、消去、又は破壊されなければいけない。

データセキュリティのドメインに対応したガイドラインの例

ドメイン	ガイドラインの例	対象
移動中のデータ (Data in Motion)	NIST SP800-52	TLS
	NIST SP800-77	IPsec VPNs
	NIST SP800-113	SSL VPNs
保管データ (<u>Data at Rest</u>)	NIST SP800-111	Storage Encryption for End user
使用中のデータ (Data in Use)	なし **	処理中の秘密情報の扱いなど
データの処分 (Data Disposed)	NIST SP800-88 ***	電子メディアの破壊

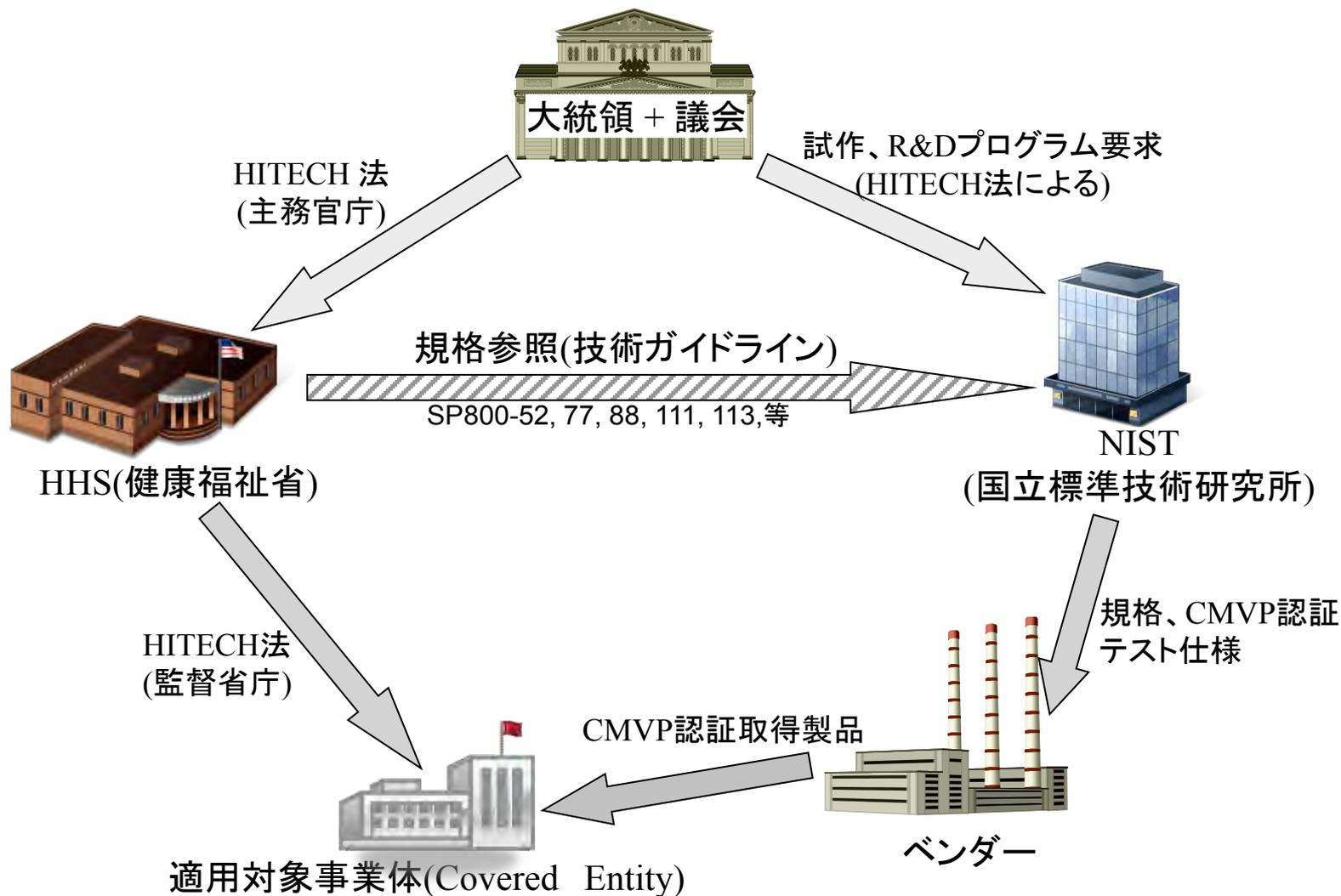
** 暗号状態処理などは、Data in Use に対応した技術になり得る。

*** NIST SP800-88 rev.1 draft 2012年9月 このDraftには、暗号技術による消去 Cryptographic Eraseが記述されている。

Data at Rest と 自己暗号化ストレージ ガイドライン、仕様、PP、認定製品、

- ・ ガイドライン
 - NIST SP800-111 Guide to Storage Encryption Technologies for End User Devices 2007年
- ・ 仕様
 - TCG OPAL 自己暗号化ディスク仕様
- ・ プロテクションプロファイル
 - NSAの「暗号化ストレージ (Encrypted Storage)」のプロテクションプロファイル 2011年
 - ・ フルディスク暗号化のプロテクションプロファイル、2011/12/1、バージョン1.0
 - ・ USBフラッシュドライブ用のプロテクションプロファイル、2011/12/1、バージョン1.0
- ・ 認定製品 FIPS140-2
 - TCG OPAL 仕様の自己暗号化ディスク
 - ・ Seagateのハードディスク、サムソンのSSDなどの製品
 - 暗号化USB
 - ・ Etc…

米国におけるスキーム 重要なNISTの役割



日本における今後の課題

「技術」「制度」「ビジネス」を統合させることは可能なのか？

日本における今後の課題 (JNSAの機関誌に記述した)

- ・ 個人情報保護法に関連する技術ガイドラインの統合
 - 組織、業界に対する管轄省庁毎のガイドラインが、レベルの低い曖昧な「技術」ガイドラインまで含んでいる。
 - NISTの役割を果たす組織的な課題
- ・ 「鍵管理」の重要性の認識
 - ##
- ・ 技術と制度と(ビジネス)の整合
 - 暗号技術は、一般的な「IT技術者」「情報セキュリティ関係者」にとってもブラックボックス。
 - 適切な技術を普及させるためのインセンティブの重要性

JCMVP・CMVPとISMSの日米比較

	JCMVP 日本	CMVP 米国
開始	2006年	1995年
試験機関	4	21 (日本に2)
認証取得 組織	10	485
2011年 認証数	0	186
2012年 認証数	4	70
総認証数	15	1733 (2012. 6. 20)

	ISMS 日本 (JIPDEC)	ISMS 米国 (ANAB)
認証機関	26	7
認証取得 組織	4061	104

2012年4月での情報
認証取得組織は世界全体で7840

日本における課題 その1

- ・ 暗号技術に対する誤解？
 - (学術系における) 「暗号が破られた」という意味
 - ・ ex. SHA-1が破られた。
 - 所詮、暗号は破られると言う認識
 - ・ B-CASの暗号が破られた！！
 - 「所詮、技術(だけ)では情報は守れない」という意見
 - ・ これは正しいが、「暗号鍵管理技術」による運用、管理(含む証跡管理)の重要さが認知されていない。
- ・ 暗号技術のバランスの悪さ(鍵管理の観点が希薄)
 - 「鍵管理」の観点の希薄
 - ・ なので、実際に暗号技術を応用したシステムのセキュリティが破られる。

日本における課題 その2

- ・ 強制力のないガイドラインや認定制度
 - 「民間を規制しない」「技術の中立性」等という理由
- ・ 技術のガイドラインも管轄官庁毎
 - 似て非なる技術ガイドライン
- ・ その結果??
 - 国内は、レモン市場化??、オレオレ化??
 - 対外的には、競争力のあるソリューションが出てこない?
- ・ 暗号技術に係る政策的判断の不在???
 - CRYPTRECの推奨暗号リスト, JCMVP, CC
- ・ その他
 - Cryptographic Eraseの法的な扱い

参考

- ・ JNSA Press 第34号 2012年9月発行
 - <http://www.jnsa.org/jnsapress/vol34/index.html>
 - 「暗号技術による個人情報保護の制度と技術の動向」
 - セコム株式会社 IS 研究所 松本 泰、伊藤 忠彦
 - http://www.jnsa.org/jnsapress/vol34/3_kikou.pdf
- ・ JNSA／第2回 鍵管理勉強会
 - <http://www.jnsa.org/seminar/seckey/120703/>

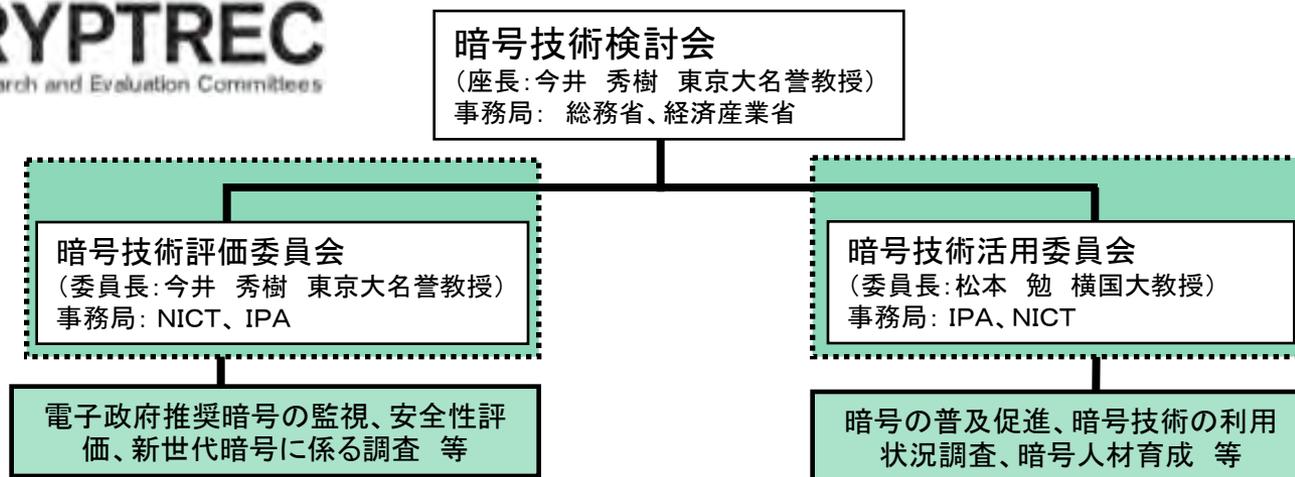
CRYPTRECに関する現状について

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

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 ^(注1)
		RSASSA-PKCS1-v1_5 ^(注1)
共通鍵暗号	守秘	RSA-OAEP ^(注1)
		鍵共有
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
暗号利用モード	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

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
	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 ^(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		RIPEND-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。

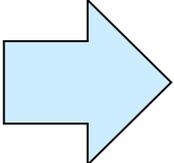
→「CRYPTREC暗号リスト」掲載の暗号アルゴリズムを念頭においた活動

○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。

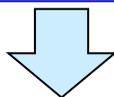


CRYPTRECのミッションを見直すための検討グループを設置

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。

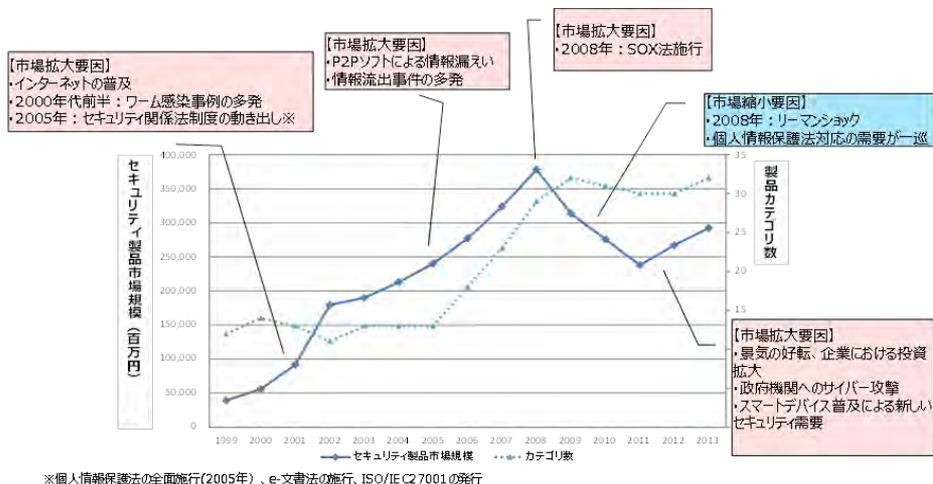
(参考2)第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)

・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



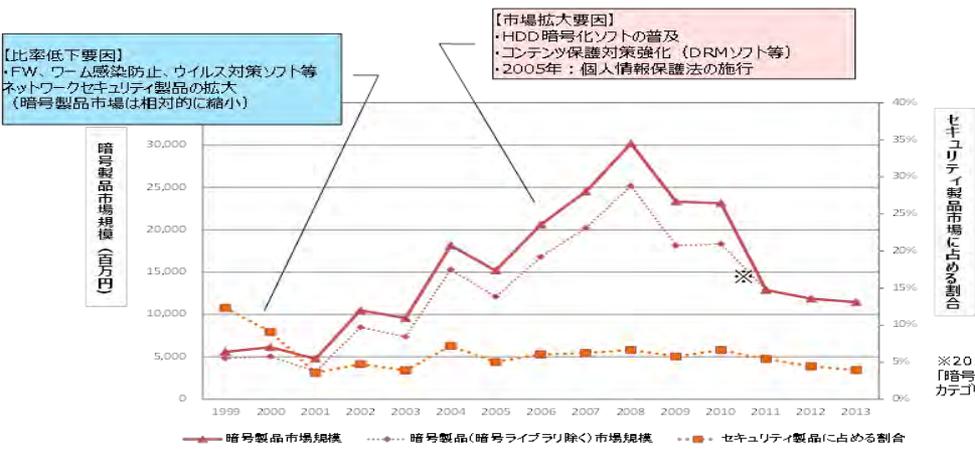
市場カテゴリーの分類

<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
- ◆ 検査ツール (トークン、不正接続防止、検査ツール)
- ◆ 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

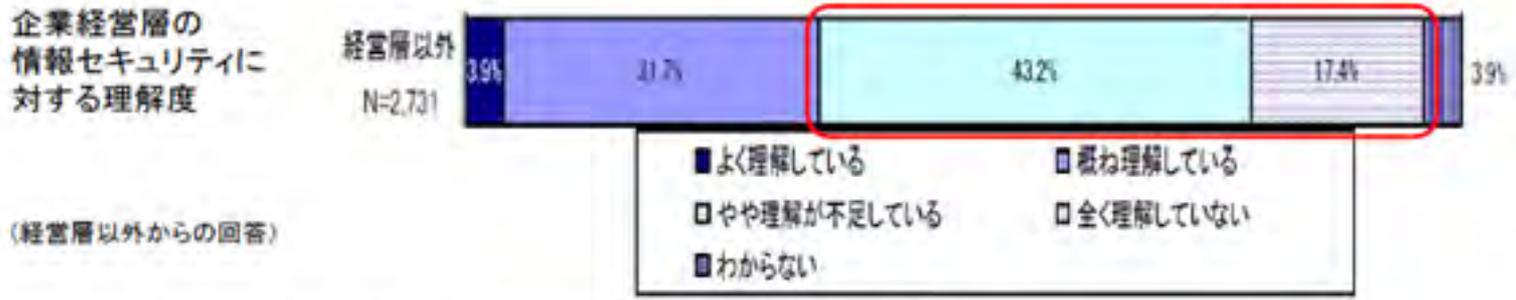
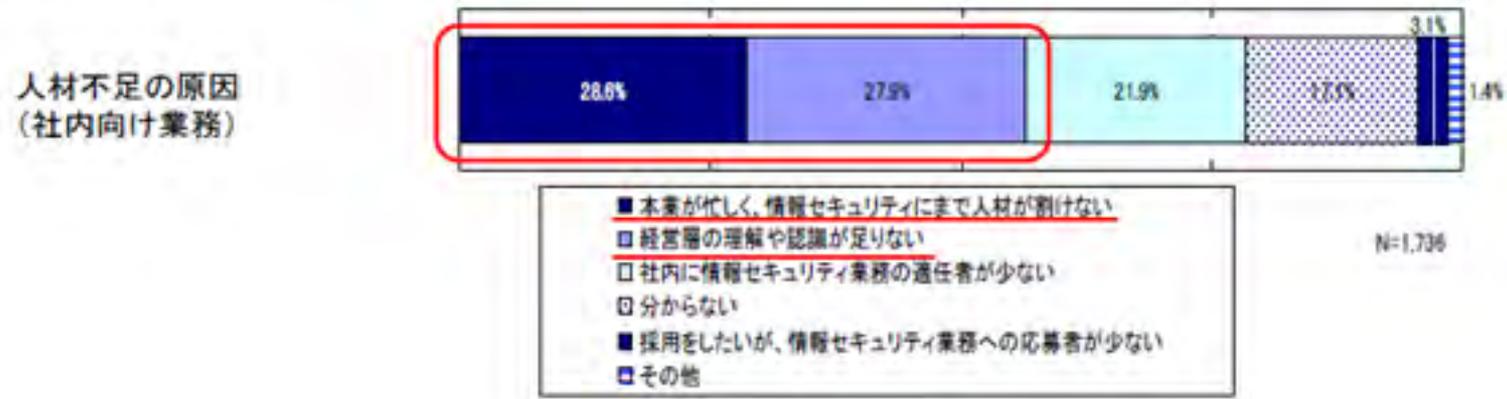


近年、情報セキュリティ製品市場が拡大する一方、暗号に関する市場が伸び悩み

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。



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

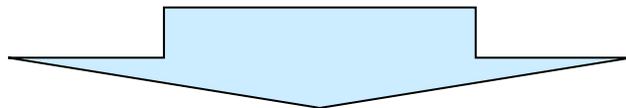


2-3. ミッション見直しの上での検討事項(政府)

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。

(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

○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

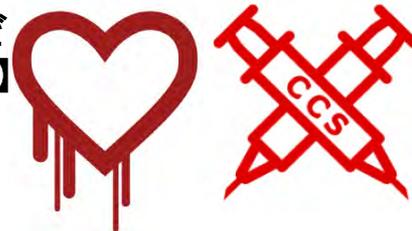
→「デファクトスタンダード」における仕様の曖昧さ・多様さにより発生する、仕様・実装の脆弱性、運用時の課題や攻撃に対応することが重要。暗号技術が社会基盤の重要な1要素となった為に、問題発生時の社会的影響が非常に大きくなっている。

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



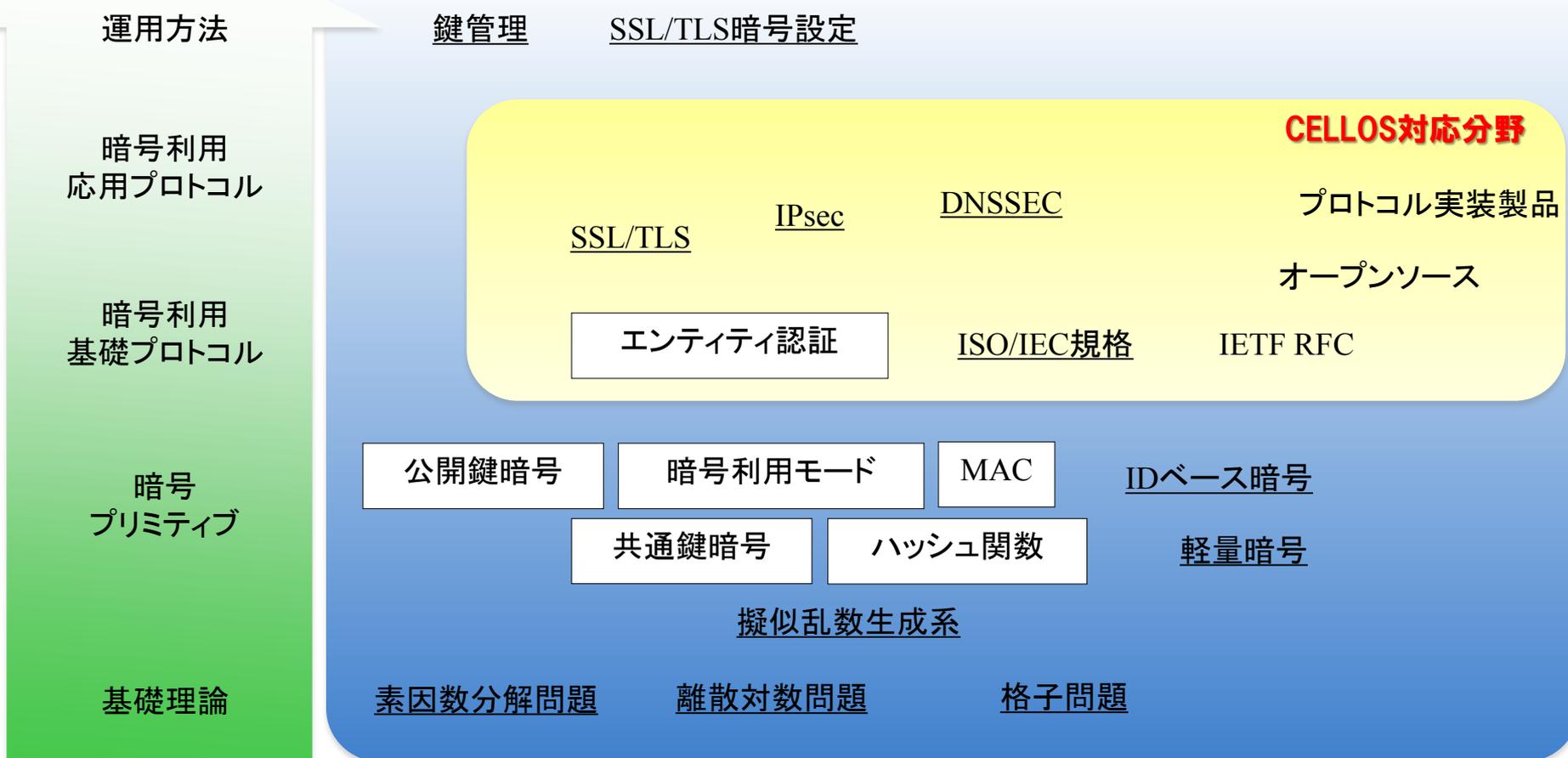
(参考2)第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)

・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。⑩

(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。

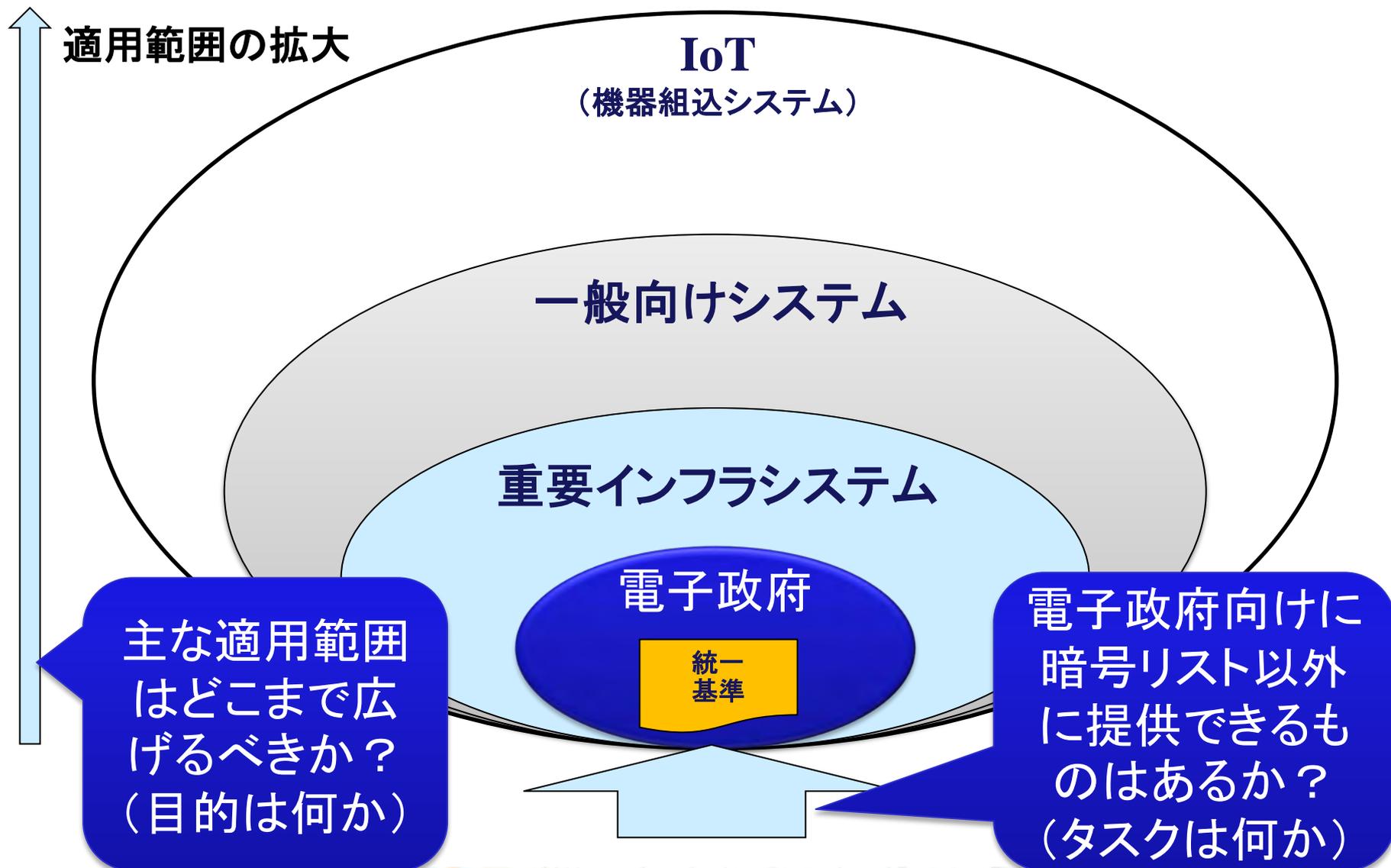
○成果物として、まずは電子政府向けでも現状の暗号リスト以外に柱となるべきものがないか検討が必要。

○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。

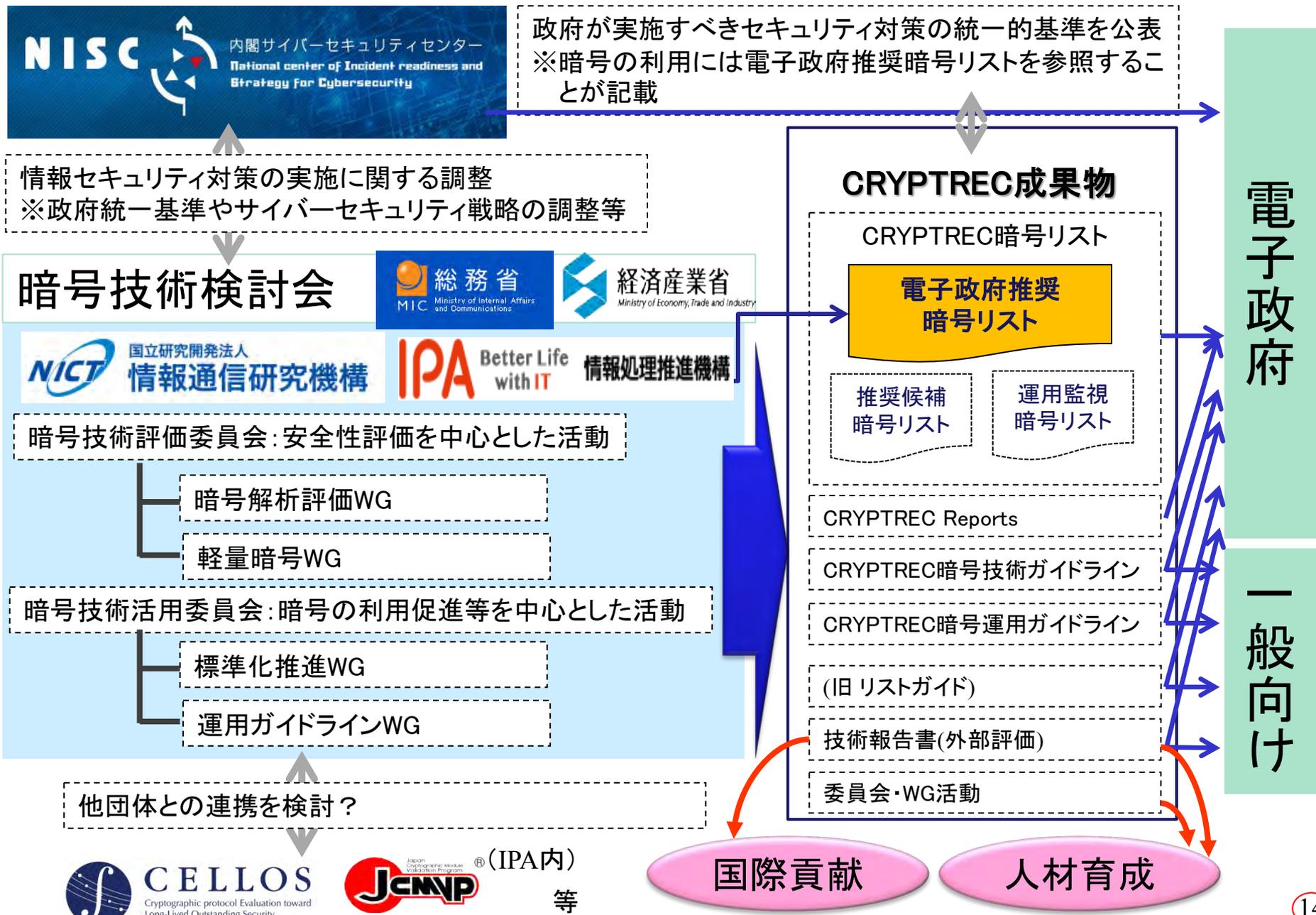
(参考2) 第1回CRYPTRECの在り方に関する検討グループでの構成員発言(2015.6.4)

・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に留意することが重要。

(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



(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

本部長：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>

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

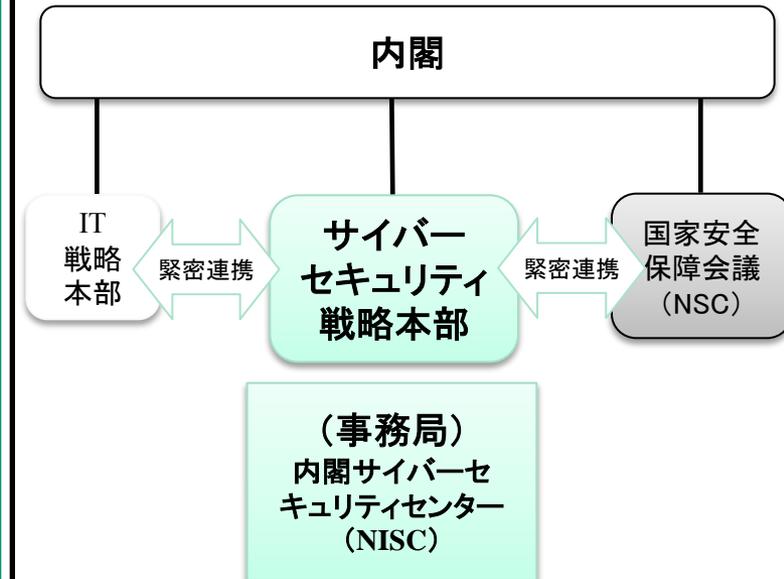
野原佐和子 株式会社イプシ・マーケティング研究所 代表取締役社長

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



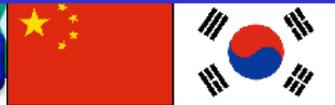
- ・高セキュリティシステムでは自国暗号(非公開)を採用した製品調達に指定(英国)
- ・汎用製品中心のシステムと高セキュリティシステムの製品調達方法を分離(ドイツ、フランスなど)

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。