# 第 3 回 CRYPTREC の在り方に関する検討グループ

日時：平成 27 年 7 月 3 日(金) 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) 前回議事確認と本日の議論の進め方について
(2) CRYPTREC で取り組む新しい暗号技術[盛合構成員]
(3) これからの CRYPTREC について [近澤構成員]
(4) 第１回、第２回の発言ポイントまとめ
(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 | 第 2 回議事概要（案） |
| 資料２ | 「CRYPTREC で取り組む新しい暗号技術」（盛合構成員） |
| 資料３ | 「これからの CRYPTREC について」(近澤構成員) |
| 資料４ | 第１回、第２回の発言ポイントまとめ |

# 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） |

５．議事概要

１　開会

事務局から開会の宣言があり、参考資料１に関して、前回検討グループでの構成員意見を反映させた旨説明があった。

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、議事録について確認が行われた。議事概要については、発言者の記載方法をこれまでの研究会に合わせて修正し、後日事務局から修正版を再度構成員にメールにて流すこととなった。

（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：上原構成員のプレゼンでガイドラインの附版をつける提案は、ガイドライン見直しに当たっても便利である。

上原構成員：附版をつけることで最終版の確認が容易である。

手塚構成員：欧州の標準化は ETSI が強い。日本では JIS が標準規格であり、暗号を上手く JIS にひも付けできないかと考える。

松本座長：米国調達では FIPS が CMVP を指定している。日本の調達では、暗号はなぜかうまくいっていない。

上原構成員：日本は標準化にかけているリソースが海外と比較して大幅に少ない。国際調達ではデジュール暗号以外は非関税障壁扱いとなってしまうなど制約がある。

近澤構成員：情報セキュリティは例外的に扱っていると思う。

太田構成員：設計上の安全性の確保はどういう対応なのか。

上原構成員：暗号アルゴリズムではない、暗号製品の部品の安全性の確保である。モジュールは JCMVP が審査している。

盛合構成員：JCMVP の利用実績があまりよくないと感じる。CRYPTREC の暗号リストを必須条件にすれば利用が進むのではないか。

松本座長：JCMVP が対象とするスコープの中に、CRYPTREC 暗号リストが入っているというイメージ。CRYPTREC 暗号リストに記載されたアルゴリズム以外のものを実装した製品の評価は JCMVP でも確認しておらず、別途独自に行うことになる。また、審査も相当厳密に行っている。

②手塚構成員プレゼンに対する質疑

近澤構成員：CELLOS は脆弱性など発表後、１、２日後にはレポートがでている。全てコンセンサスがとられているのか。

手塚構成員：細部は答えられないが、CELLOS から発信する速報の対応は、最終的には総会座長の私が全て判断している。

松本座長：どのようなプロトコルを対象としているのか。

手塚構成員：CELLOS で活動の対象としているプロトコル

とは、暗号アルゴリズムも加味した仕様（具体的なコード）であり、CELLOS では標準化団体が出している標準プロトコルの安全性などを調べている。

松本座長：CELLOS の活動を引き続き継続していくにあたっては、若い人材も巻き込んでいった方がよいと思われる。協力範囲を明確にして役割分担を行えば、活動が広がっていくのでは。

手塚構成員：CELLOS 内では、それぞれの得意な分野においてすでに役割分担はできている。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。

松本座長：連携の方向に当たり、攻撃手法情報の集約、安全性評価といった分野など、速報性が求められるものを意図されているのか。

手塚構成員：そのとおり。CRYPTREC の認知度は高く、HP にリンクを張ることもあり得ると考えている。純粋な技術の部分は CRYPTREC の方で、是認していただく流れが良い。

③松本泰構成員プレゼンに対する質疑

手塚構成員：標準化の考えを確認したい。

松本泰構成員：セコム社の暗号技術の取り組みとして目指しているデジタル時代のフレームワークにおいて、標準化とは電子署名や電子政府を意識したもの。

盛合構成員：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った方がよい。

松本座長：暗号技術を広く活用する方向であると認識している。

松本泰構成員：米国の医療分野の個人情報保護法にあたる HIPAA では、暗号技術に関して 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。日本の個人情報保護法については、守る対象と守る方法が整理されたガイドラインがないので、技術的なガイドラインのレファレンスがあってもよい。暗号化しても個人情報か？という議論は以前からあるので、アメリカでの実施状況も参考にして、日本の対応を検討すべき。

松本座長：鍵管理は大問題。実装面までチェックできることが大事だがまだ困難。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。日本でも NIST の翻訳版で良いか疑問がある。

手塚構成員：CRYPTREC の在り方を検討するにあたり、ベンダのシステムを作っている人をもっと巻き込むべき。新しいレイヤーでの議論が必要。CRYPTREC は、NIST（レイヤ別に分け、サービス、通信、デバイス、暗号といった体系）のような構造を考えてよいのでは。

松本座長：暗号をどう使うのか。日本では体系立っていない。

手塚構成員：トラストは複数のステークホルダーがいて成り立つもの。暗号は個別案件。このギャップを埋めるのが課題。

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。

事務局（総務省）：サービスの運用コストを最適化するために、鍵管理をしっかり実施できるガイドラインがあれば安心だが、CRYTREC として対応することにはハードルがある。日本では、Data at Rest もまだ対応できていないので、こちらの方が手をつけやすいのでは。

松本座長：第３回は、近澤構成員と盛合構成員にプレゼンをお願いしたい。IPA や NICT の一員としてではなく、暗号に詳しい人として問題意識の共有や提案をしてほしい。第３回で CRYPTREC の今後の活動の方向性を出していき、第４回でまとめを行う。

３　閉会

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。

資料2

# CRYPTRECで取り組む新しい暗号技術

国立研究開発法人 情報通信研究機構

盛合 志帆

# これまでの議論で出てきたポイント

- 暗号プリミティブだけではなく、プロトコル等、より上位まで含めた安全性の担保をめざす
- 暗号技術が、電子政府システムだけでなく、今後の社会でどのように使われていくべきかを視野に検討すべき

# 今後社会で活用される暗号技術とは

- 情報利活用のための暗号技術
  - Internet of Things
  - セキュアな情報流通 (保存, 消去を含む)
  - セキュアな情報分析
  - プライバシー保護

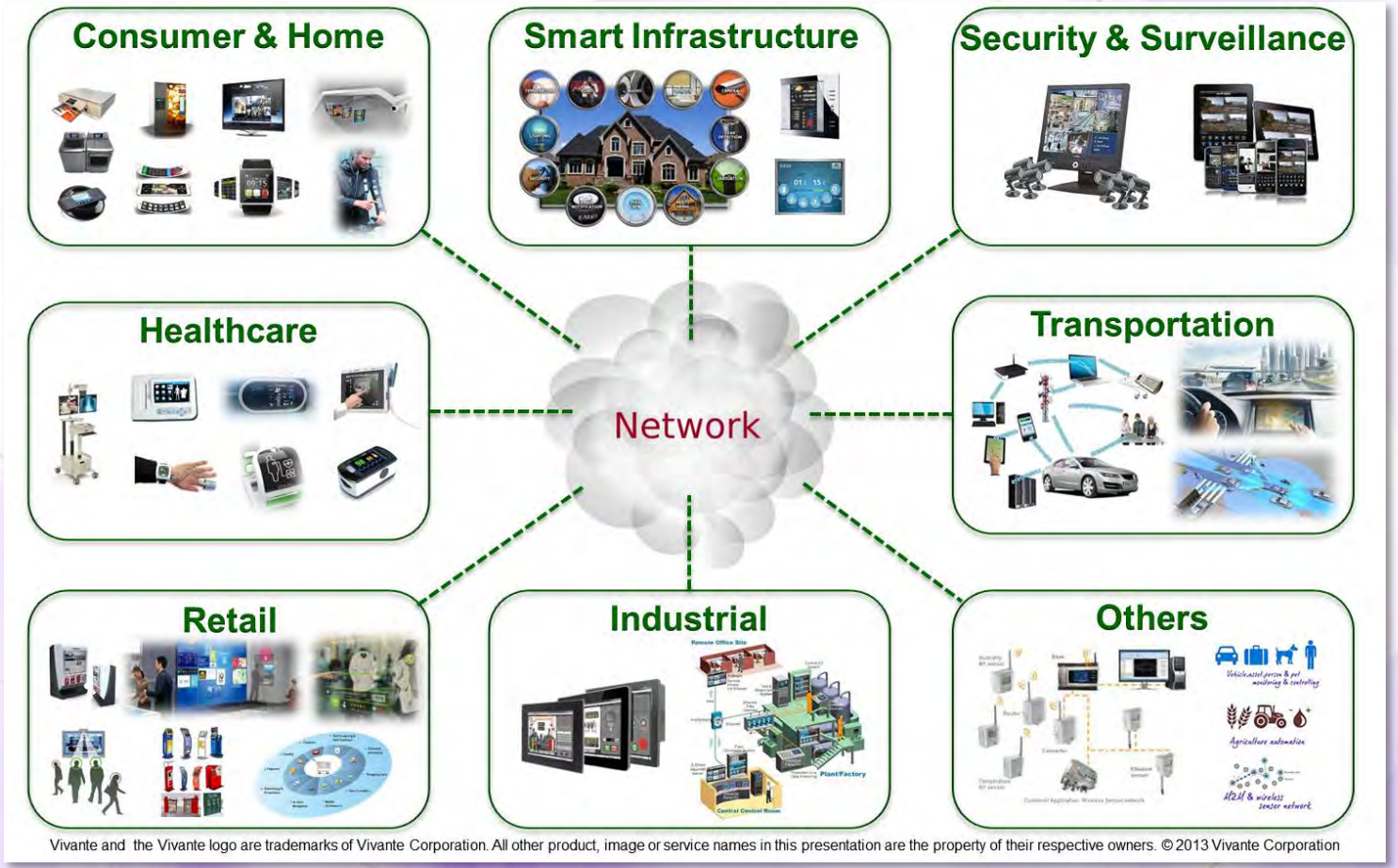
  などを実現するための暗号技術

# 技術トピックスの例

- 軽量暗号 ← 今日はこの2つを取り上げます
- 軽量プロトコル
- 鍵管理
- 高機能暗号 (検索可能暗号, 代理再暗号化etc)
- 耐量子計算機暗号技術 (準同型暗号)
- プライバシー保護/匿名化技術 ←

# 軽量暗号

- Internet of Things (IoT)
  あらゆるモノがネットに繋がる時代



# 軽量暗号

- IoT接続デバイス数の予測

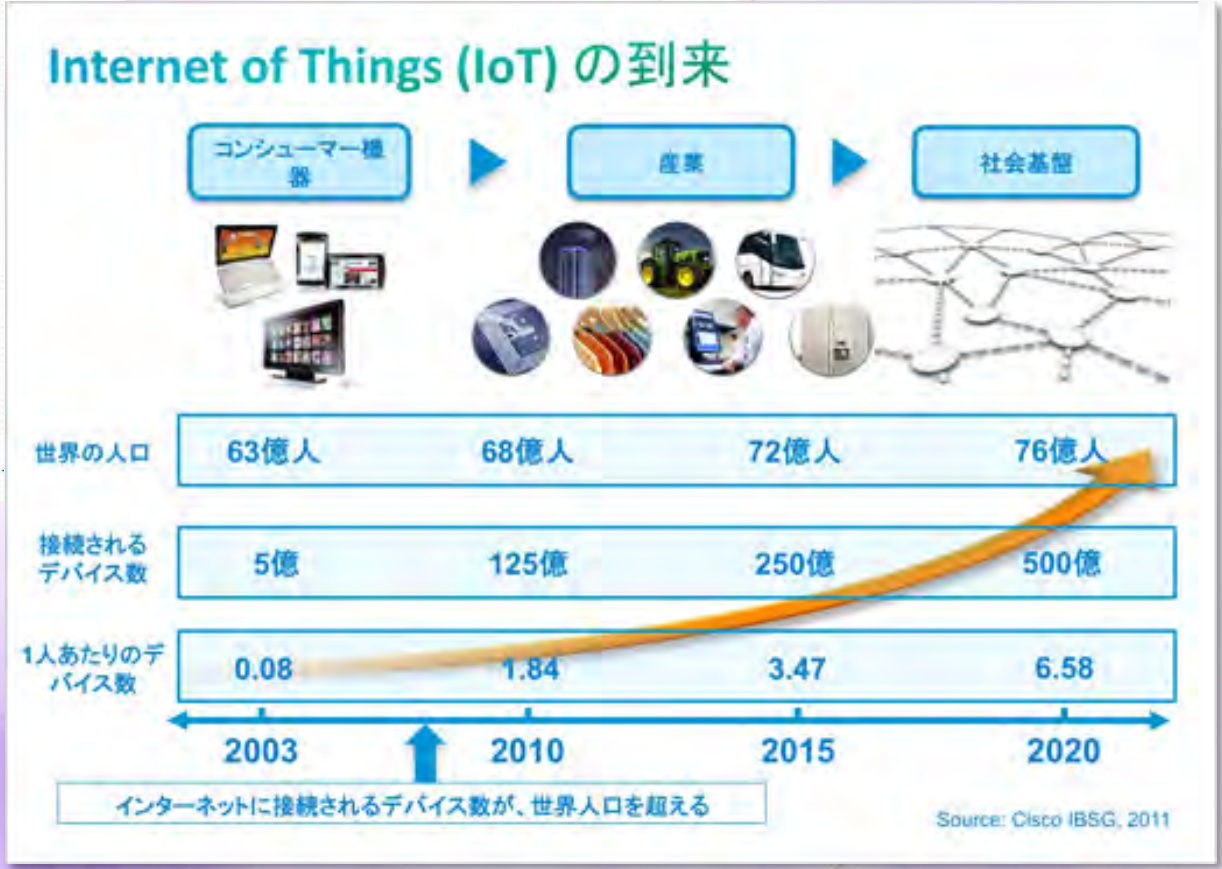
Gartner 2020年に260億

IDC Analyze the Future 2020年に300億

cisco 2020年に500億

intel 2020年に2兆

森山,「IoTの実現に有効なRFID認証技術」
情報セキュリティシンポジウム道後2015




http://cisco-inspire.jp/issues/0010/cover_story.html

# 軽量暗号

- 全てのデバイスに、データのセキュリティやプライバシーを守るための十分なリソースがあるわけではない
- IoT時代に「電子政府推奨暗号」だけで十分か？

- 実装できないデバイスをいかに守るか？

# 軽量暗号:海外動向

- 欧州
  - EU FP6, 7の研究プロジェクトECRYPT I, II(2004- )のテーマとして盛んに研究されてきた
- 米国
  - 従来は取り上げられてこなかったが、近年、NSAが軽量暗号を設計し国際標準化を推進、NISTも積極的に取り組み始めている
- 国際標準
  - ISO/IEC 29192 (ブロック暗号, ストリーム暗号, 非対称メカニズム, ハッシュ関数, MAC?)

# 軽量暗号:国内動向

- 多くの軽量暗号アルゴリズムが提案されている

# 軽量暗号：CRYPTRECでの活動

- 暗号技術評価委員会「軽量暗号WG」での活動
  - 昨年度までの活動：軽量暗号の現状と今後の活動方針を報告書にとりまとめ(134ページ)
  - 今後の活動方針：IoT等の次世代ネットワークサービスにおいて軽量暗号の活用が期待されることから、方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的として、暗号技術ガイドラインを作成

# プライバシー保護/匿名化技術

- 背景
  - 情報利活用による経済再生：政府の成長戦略
    - プライバシーを保護しつつもパーソナルデータを利活用した新産業・新サービスの創出が求められている
  - 個人情報保護制度見直し
    - 改正個人情報保護法の成立
    - 個人情報保護委員会の発足

# プライバシー保護/匿名化技術

個人特定性低減データ

- 「骨子案」における匿名加工情報(仮称)
  - 匿名加工情報を作成する際には予め個人情報保護委員会への届出が必要
  - 匿名加工基準は委員会規則で定める

# プライバシー保護/匿名化技術

- プライバシー保護技術の活用促進する制度が未整備
  - 日本では「個人情報」は暗号化しても「個人情報」
    - 暗号化等の情報保護手段を講じるインセンティブがない
  - 米国HIPPA/HITECH法, SOX法
    - 暗号化することで情報漏洩時の通報義務が軽減される
  - 暗号技術やプライバシー保護技術の活用を促進する制度や法律・ガイドラインの整備につなげる活動ができないか

# 手段とアウトプット

- 手段
  - 社会ニーズ/制度を調査・検討するWG
  - 暗号技術専門家によるWG
  - 外部評価(調査)
- アウトプット
  - 専門家向け最新技術動向調査
  - 一般向けのガイドライン
  - 政策提言につなげるレポート

# まとめ

- 暗号技術が今後社会で活用されるために取り組むべきこと
  - 情報利活用のための暗号技術
    - 特に、IoTやプライバシー保護を実現する暗号技術
  - 暗号技術の活用を促進する制度や法律・ガイドラインの整備につなげる活動

# (参考) CRYPTRECの現在の活動


CRYPTREC暗号リスト

CRYPTREC Report

技術報告書

CRYPTREC
暗号運用ガイドライン

CRYPTREC
暗号技術ガイドライン

IPA Better Life with IT

# これからのCRYPTRECについて

2015年7月3日

独立行政法人 情報処理推進機構 (IPA)
技術本部　セキュリティセンター
近澤　武

# CRYPTRECは…

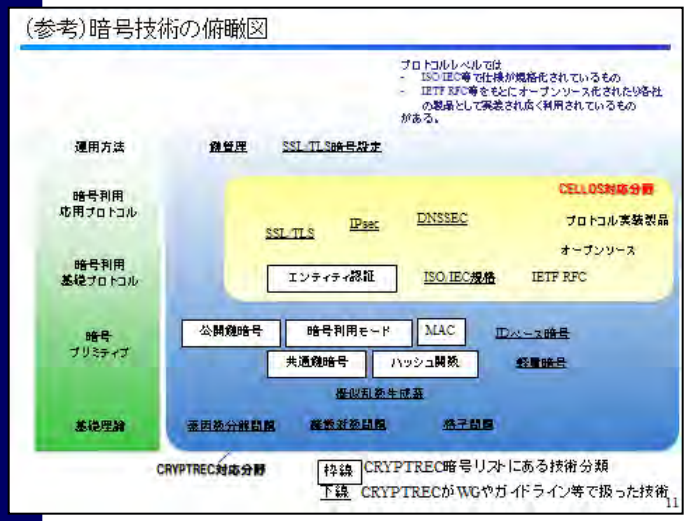
- 暗号関係の情報、専門家の知見が集約する

  日本の**総本山**

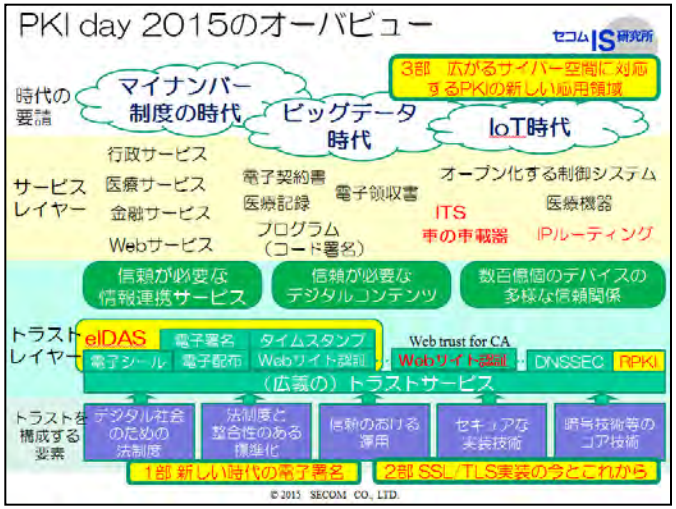
  となるべき

- そのためには、以下について明確にすべき
  - スコープ（まずは俯瞰図の整理・意思統一から）
  - 中立性（どういった視点・立場での中立性か）
  - 体制（他組織との連携を含む）
  - 情報発信のやり方

# CRYPTRECのスコープ
# まず統一した俯瞰図の整理が必要

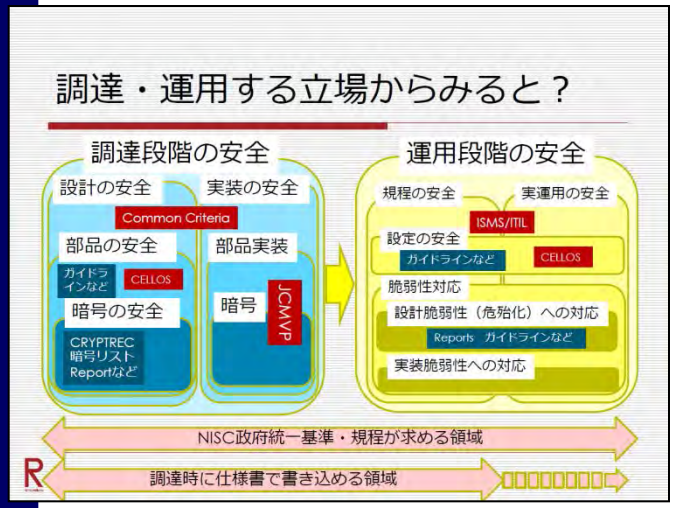



第2回委員会事務局プレゼン資料

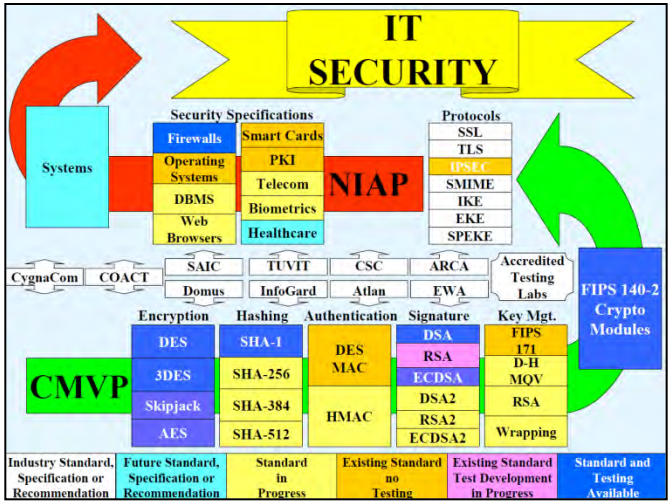



第2回委員会松本(泰)委員資料

| | |
|---|---|
| システム | システムに必要な要件すべてを実装し、セキュリティ認証を受けたもの。この認証を受けたものが政府調達の対象となる（例：CC認証、プロテクションプロファイル作成など） |
| セキュリティ仕様 | 具体的なセキュリティ機能を実現するために必要となる仕様を規定するもの（例：ファイアウォール、OS、データベース、ブラウザ、バイオメトリクス、ICカード、ヘルスケアシステム等に必要なセキュリティ機能の規定など） |
| プロトコル | 基本的に外部の産業標準を流用する（例： IETF標準プロトコル、IEEE標準プロトコル、など） |
| 暗号モジュール | 暗号アルゴリズムを含め、実装された暗号モジュールが安全に使えるための必要な要件を実装し、セキュリティ認証を受けたもの（CMVP認証） |
| 暗号アルゴリズム仕様 | CMVP認証の対象となる暗号アルゴリズムの仕様を規定したもの |




第2回委員会上原委員資料



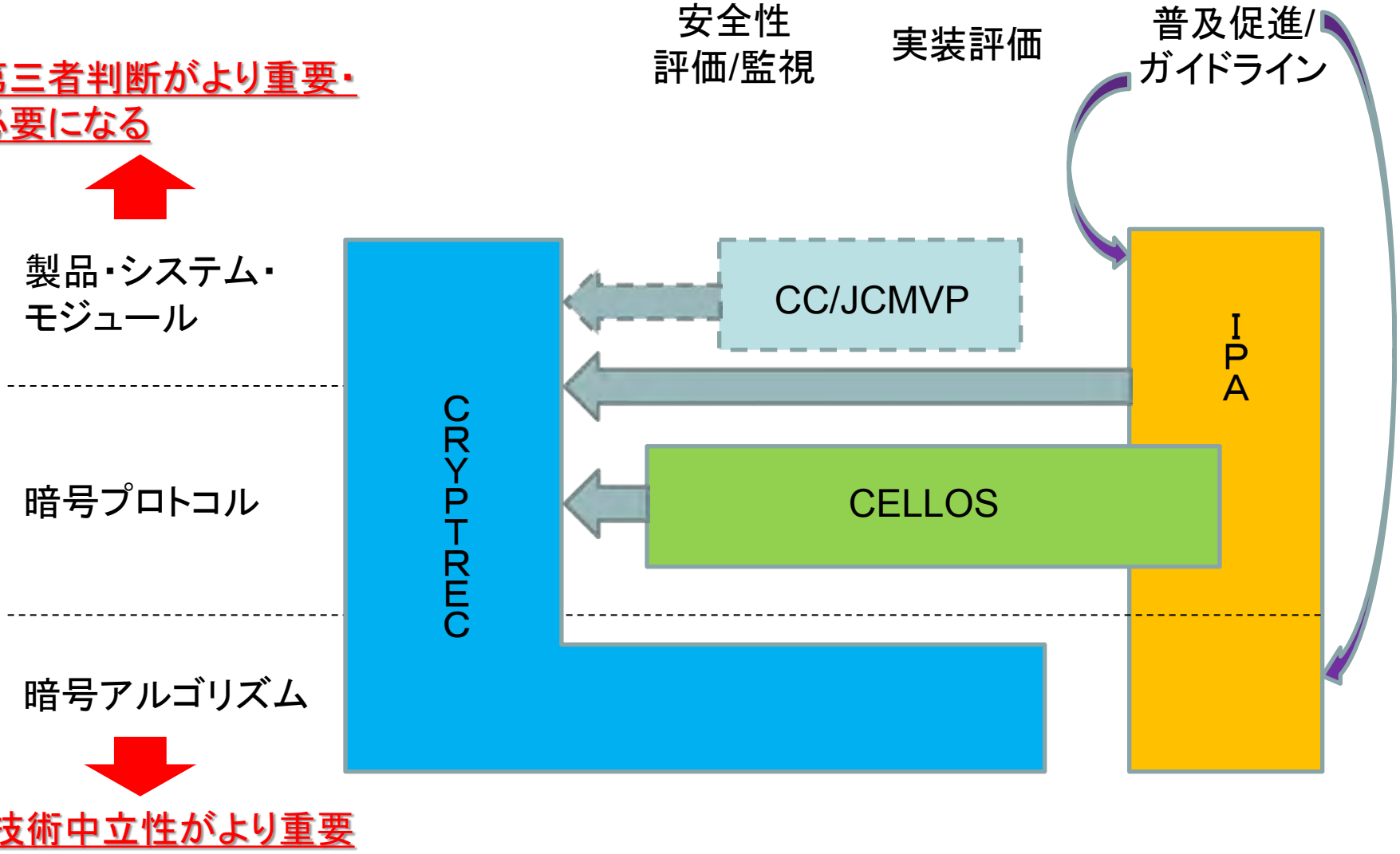

CMVP Status and FIPS 140-1&2

2014年度活用委員会報告書

# CRYPTRECの中立性

- 技術中立性
  - （使えるかどうかは別に）技術としていいものはいい、悪いものは悪い、とだけいえばよい
  - ただし、世の中がそれに追随するかはわからない
- 第三者判断
  - （世の中をよりよくするために）製品・設定として、こうするのがいい、こうしてはいけない、とのメッセージが伝わればよい
  - ただし、必ずしも技術中立性の視点でベストなわけではない

# CRYPTRECの体制と他組織との関係（1）



# CRYPTRECの体制と他組織との関係（2）

- 暗号技術評価委員会
  - 従来からの暗号アルゴリズムの安全性監視・実装評価
  - CELLOSからの暗号プロトコルに関する情報を受け、確認・議論
  - 暗号プロトコル専門家を若干追加？

# CRYPTRECの体制と他組織との関係（3）

- 暗号技術活用委員会
  - IPAに暗号技術の普及促進（運用ガイドライン作成を含む）を任せ、状況を報告させるのも検討してはいかがか
    - IPA作成の運用ガイドラインを審議し、委員会承認後（検討会も）、CRYPTRECのクレジットで発行
  - その他、暗号技術評価委員会で扱わない項目を担当
    - ただし、項目によっては、委員構成が適切になるよう調整が必要の場合が生じる

# 情報発信（1）ー目的と手段の再確認

- 今まで「想定読者」と「想定読者が必要とするコンテンツ」が合っていなかったのではないか
  - 想定読者をどこに置くかによって、必要とするコンテンツや暗号リテラシは全く異なる
  - 「脆弱性への対応策」、「脆弱性の解説（技術ガイドライン）」、「技術評価結果」、「最新動向」、「設定・運用ガイドライン」でコンテンツの性格が異なる
- 一般への独自の情報発信機能を持ちたい（＝情報の集約・発信ポータル）のか、情報発信機能を持つ組織が欲するような情報提供機能を持ちたい（＝コンテンツの充実）のか

# 情報発信（2）

- （適度な）速報性が重要
  - とにかく迅速に
- そのためには、数名の専門家をキープしておき、何か事象が生じた際に、（短い時間の）議論を行ってCRYPTRECとしてのコメント作成
  →時間をかけずに（1日程度で）委員会承認
  →CRYPTRECのコメントを発信
  - 「数名の専門家をキープ」:
    IPAには「専門委員」という制度があり、稼動分だけ対価を支払うことが可能

# 情報発信（3）

SSL/TLS暗号設定ガイドライン
CRYPTREC　　IPA

「活動成果物」との位置づけ

「脆弱性対策啓発資料」との位置づけ

REC
on Committees

ENGLISH

トピックス

2014年度CRYPTREC暗号運用ガイドラインの公開

平成27年5月22日
国立研究開発法人 情報通信研究機構
独立行政法人 情報処理推進機構

国立研究開発法人情報通信研究機構(略称NICT)と独立行政法人情報処理推進機構(略称IPA)が共同で運営する「暗号技術活用委員会」の2014年度の活動成果として、CRYPTREC 暗号運用ガイドラインを作成しましたので、公開いたします。

「SSL/TLS暗号設定ガイドライン」

本報告書に対するお問い合わせは、下記までお願いいたします。問い合わせ等の受付はe-mailのみといたします。
CRYPTREC事務局
E-mail : info@cryptrec.go.jp

このサイトについて　プライバシーポリシー

SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～

最終更新日　2015年5月12日
独立行政法人 情報処理推進機構
セキュリティセンター

「SSL/TLS暗号設定ガイドライン」は、SSL/TLSサーバの構築者や運営者が適切なセキュリティを考慮した暗号設定ができるようにするためのガイドラインです。「様々な利用上の判断材料も加味した合理的な根拠」を重視し、実現すべき安全性と必要となる相互接続性とのトレードオフを踏まえたうえで、実際に設定すべき「要求設定項目」として3つの設定基準（「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」）を提示しています。本ガイドラインは安全なウェブサイトの作り方とともに適切な暗号設定をする資料の一つとしてお使いいただけます。

なお、本ガイドラインは、暗号技術評価プロジェクトCRYPTRECで作成されました。

「SSL/TLS暗号設定ガイドライン」の内容

・第1章と第2章は、本ガイドラインの目的やSSL/TLSについての技術的な基礎知識をまとめています。

・第3章ではSSL/TLSサーバに要求される設定基準の概要について説明しています。

・第4章から第6章では、第3章で定めた設定基準に基づき、プロトコルバージョン、サーバ証明書、暗号スイートについての具体的なSSL/TLSサーバの要求設定項目について示しています。ここでの要求設定項目は別紙のチェックリストで確認が求められる項目となります。

・第7章では、チェックリストの対象には含めていませんが、SSL/TLSを安全に使うために考慮すべきことをまとめています。

・第8章は、クライアントの一つであるブラウザの設定に関する事項を説明しており、ブラウザの利用者に対して啓発するべき事項を取り上げています。

・第9章は、そのほかのトピックとして、SSL/TLSを用いたリモートアクセス技術（“SSL-VPN”とも言われる）について記載しています。

・Appendixには、4章から6章までの設定状況を確認するためのチェックリストや、個別製品での具体的な設定方法例を記載しています。

・チェックリストは、「選択した設定基準に対応した要求設定項目の設定忘れの防止」と「サーバ構築の作業受託先が適切に要求設定項目を設定したことの確認」を行うために利用できるように作られています。

資料のダウンロード

# 情報発信（4）

（参考）JPCERTからの情報をIPAのHPで掲載
JPCERTが「情報提供機関」、IPAが「情報発信機関」になっている例


CELLOSが「情報提供機関」・CRYPTRECが「情報発信機関」になる（なりたい）のか、
それともCRYPTREC独自に「情報発信機関」になる（なりたい）のか

# 第１回、第２回の発言ポイントまとめ

資料4

## CRYPTRECの活動成果の適用

- 基本的に電子政府に限られているCRYPTRECの適用範囲を、医療等の重要インフラ分野、ITS等のIoTといった範囲まで拡大した方がよいか。
- 利用者に近いテーマの文書でないと十分に読んでもらえないため、分かりやすいガイドライン等の文書を整備する必要があるか。
- 政府統一基準や仕様書へより反映しやすい成果物が必要。形式面でも、文書への付番や短周期での改定、小さい単位での文書作成等の工夫が考えられる。
- 実装やプロトコルなど、仕様書で参照する文書がない若しくは、認知されていない部分はベンダー依存になる。
- 暗号技術をデータセキュリティの観点で分類※し、作成するべき文書を整理することが有用かもしれない。

※NISTガイドラインでは、移動中のデータ（TLS、IPsec　VPNs等）、保管データ（storage Encryption for End user）、使用中のデータ（クラウドサービスにおける暗号技術の応用等）、データの処分（電子メディアの破壊等）に区分

# 第1回、第2回の発言ポイントまとめ

## CRYPTRECが対象する技術分野

- 今日の脆弱性の多くは実装やプロトコルレベルで生じているため、暗号アルゴリズムだけでなくこれらの領域も対象とする必要があるか。
- より製品に近い領域になってくると、評価の方法・コストや客観性の担保の観点で困難な部分があるため、どこまでを対象とするか検討が必要であるか。
- IoTの世界においては、リソースが少ない、物理セキュリティが乏しいといった新しい課題があり、CRYPTRECとして貢献できる部分があるのではないか。
- CELLOS、JCMVP等の他団体との連携を通じて、対象とする範囲を広げられるか。

## CRYPTRECの体制

- 関連する既存団体との連携を深めることは有用でないか。
- 速報性のある脆弱性情報の提供を行える体制作りが必要ではないか。すでに同様の取組を行っているCELLOS等との連携が有用か。
- 一般向けガイドラインの作成、プロトコルに関する安全性評価など、IPAやCELLOSに一部機能を委任することで、機動的に活動することができるのではないか。

# 第１回、第２回の発言ポイントまとめ

## 日本の暗号政策全体の俯瞰

- 一言で暗号技術といっても様々あるが、暗号技術のどの部分についてどのような取組を行うべきか、全体を俯瞰した議論が必要ではないか。
- 中心的な役割を担うのはCRYPTRECであるが、CRYPTRECの活動範囲や政府内での位置づけは適切か。
- 米国のNISTにおける法的位置づけ、成果物の出し方、政府調達との結びつけなど、NISTとの比較分析は有用ではないか。