Information-technology
Promotion
Agency, Japan

CCRA/ICCC 2013報告

～IT製品の国際的な政府調達要件の開発推進について～

平成25年11月14日

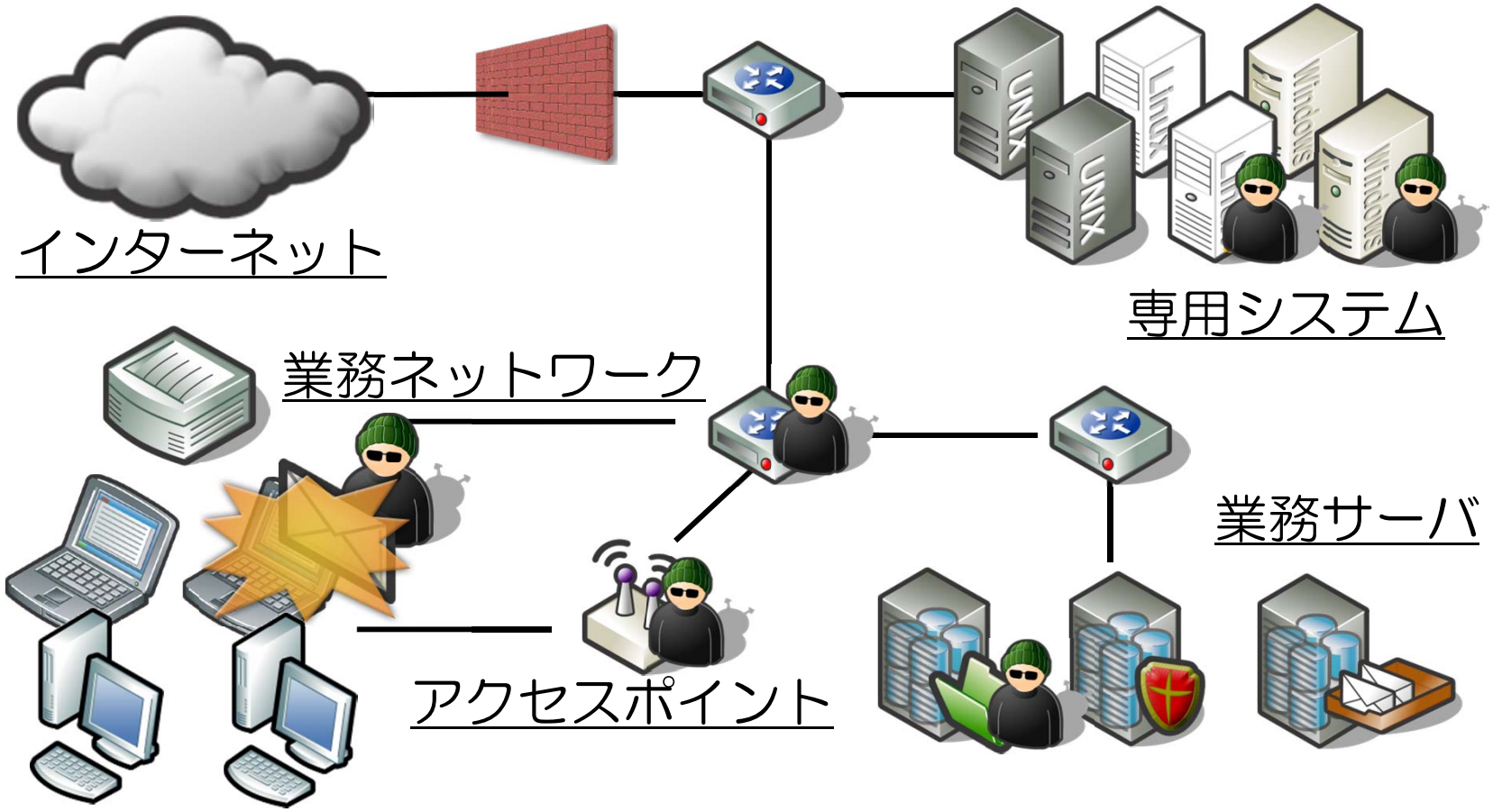
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

アジェンダ

1. イントロ
   - 最近の話題から
   - 今回の改革へ
2. CCRAの改革（サマリー）
   - CCRA会合／ICCC 2013の報告
   - 改革のポイントについて
3. cPP開発に向けた取り組み
   - cPPとは
   - cPP開発プロセス
   - 現在の状況
4. 今後の対応についての提案

事例(3) 政府調達システム等での脅威

- 堅牢な情報システムに、たった1つの問題であって管理者権限を取得されると、システム全体が知らないうちにやられている



脅威の識別について

- 脅威とは
  - 重要な情報資産（保護すべき資産）に対して
    盗られる（C）、壊される（I）、使えなくされる（A）
  - ポータブルメディア、電子メール、印刷物からの漏えい
  - 成りすまし（パスワード・暗証番号等の詐取）
  - 標的型攻撃メール、
  - ウィルス、
  - 不正アクセス、
  - DDoS攻撃、
  - フィッシング、
  - Webサイトへの攻撃、電子証明書を悪用した攻撃、など

対策の必要性について

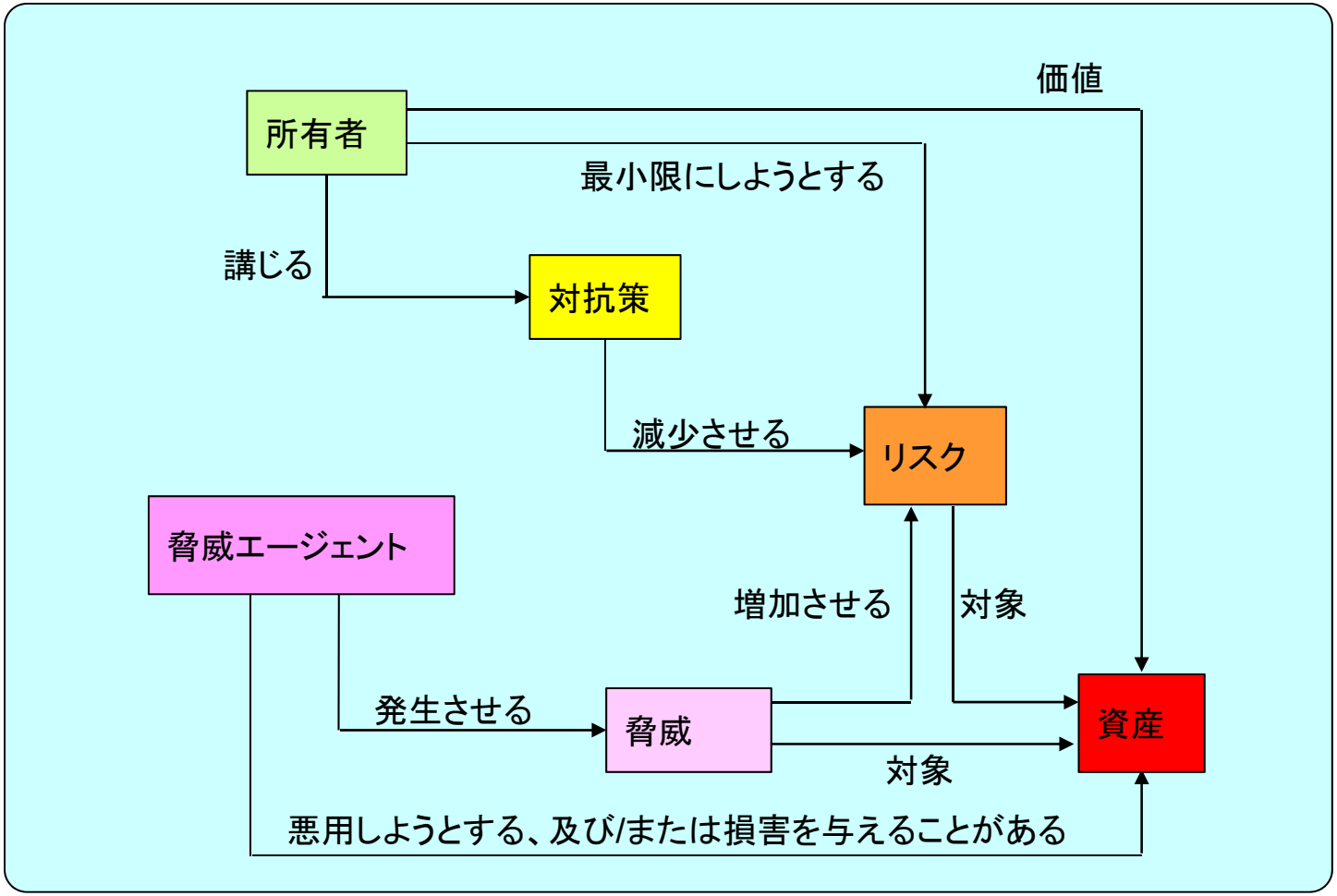
- 脅威から保護資産を守るために(対策方針)

  たとえば、

  - 情報の流れを制御
  - 情報資産に対するアクセス制御
  - アクセス権限の付与(利用者の役割)
  - 利用者の識別(ID)と認証(パスワード・証明書)
  - データの暗号化
  - 通信路の暗号化と真正性
  - 残存情報の保護
  - 最新のセキュリティパッチを適用、など

セキュリティ課題定義

- セキュリティの概念と関係（CCパート1より）

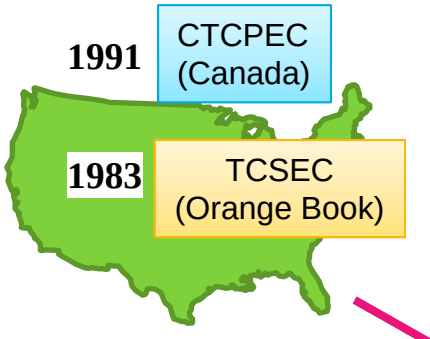


海外での政府調達

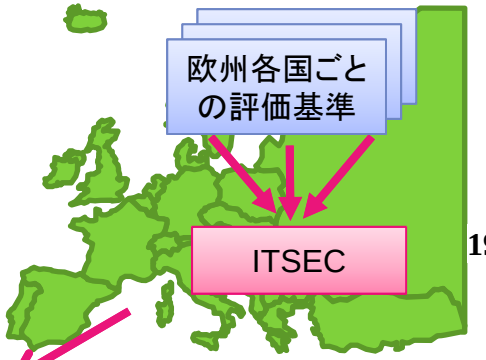
- 米国
  - 1983~2000：TCSEC（オレンジブック）クラスC1,C2,B1,B2,B3,A1,A1超
  - 2000~現在：PP適合によるCC評価
- カナダ
  - 1991~2000： CTCPEC
  - 2000~現在： PPへ適合したCC評価（US、UKと協調）
- 欧州（UK）
  - 1985: CESGが政府系コンピュータシステムの評価機関設立
  - 1987：DTIが商用IT製品のセキュリティ評価開始（Green Book）
  - 1990：両制度をITSECに一本化
  - 1997：EU15か国がMRAに合意
  - 2000~現在：PPへ適合したCC評価（UKは独自のCPAによる調達を実施）

コモンクライテリアとCCRA

欧米では20数年前から、政府機関が調達するIT製品について
自国独自の基準に基づいたセキュリティ評価・認証が行われていた



IT製品市場の国際化により
セキュリティ評価基準統一の必要性



米加英仏独蘭の6か国が開発

Common Criteria

V1.0：1996
V2.0：1998／V2.1：1999

評価結果の相互承認
（2000年5月にCCRAを創設）

13か国が加盟し、政府調達での
活用を開始した。

(ISO/IEC JTC 1／SC 27／WG 3へ提案)

ISO/IEC 15408

1999年6月に国際規格(ISO/IEC)として承認。12月発効。

規格上*CC*と呼ばれている。

TCSEC ：Trusted Computer System Evaluation Criteria
ITSEC ：Information Technology Security Evaluation Criteria

これまでのCC評価での問題点

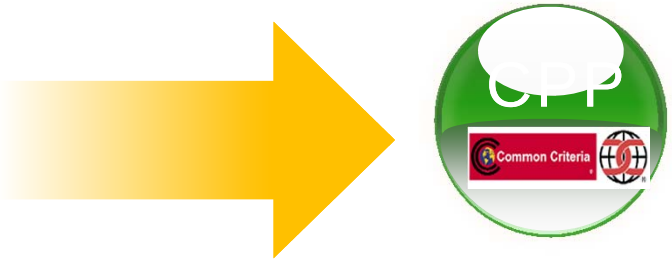
- 各国独自のPPによる重複した評価
  - 同じ製品分野で各国から異なるPP（セキュリティ要件）が作成されたため、一つの製品についてそれぞれのPPに適合sる評価が求められる
- 評価機関・評価者による評価品質のバラツキ
  - CEM（評価方法）は、さまざまな製品に対応するため、抽象的な記述となっており、技術分野に対応した具体的な評価方法がないため、加盟国間・評価機関間で評価品質の均一性を維持することが困難であった
- PP適合でないベンダー独自仕様（ST）に基づく認証製品
  - その製品本来のセキュリティ機能が評価対象から外されていたり、実現不可能な前提条件や運用環境、組織のセキュリティ方針などをもとに評価されることがあり、調達対象として活用できない認証製品があった
- EAL4等の評価では、評価コスト・期間がかかり過ぎる
  - 評価に18か月程度かかることがあり、新製品をタイムリーに調達できない
  - 製品ベンダーにとって、販売機会を逸することがあった

今回のCCRAにおける「CC改革」

**各国がバラバラなセキュリティ要件（PP）で調達していたが、
一つの技術分野に一つの共通要件（CPP）に統一され、
IT 製品が「海外から日本へ」、そして「日本から海外へ」**

各国がバラバラなセキュリティ要件で調達

セキュリティ要件が統一へ



【EAL】から【CPP適合】へ

2. CCRAの改革（サマリー）

- CCRA会合の報告
  - 会期：2013年9月3日（火）～9日（月）
  - 会場：米国フロリダ州オーランド市（主催：米国認証機関NIAP）
  - 参加国：18か国(US、UK、SE、GE、FR、AU、CA、JP、NL、NO、SK、SP、IT、TK、MY、IN、DK、FI)
  - 決定事項：

    CCRA MC Vision Statement（2013年9月）にもとづくCCRAアレンジメント（規約）の改訂案V15に基本合意。今後、各国でリーガルチェック、批准作業を開始する。
  - 改訂の主な内容：
    - 相互承認の適用範囲：

      cPP適合評価（EAL4+ALC_FLRまで）、独自ST（EAL2+ALC_FLRまで）
    - 承認の条件等：適合規格の修正（サポート文書の追加）
    - cPP関連：cPPの定義、認証報告書・認証書のcPP対応、用語の追加修正
  - 検討中の課題：

    cPPの早期開発、Modular PPのCC/CEMへの導入、暗号評価サポート文書作成、評価結果の有効期限と定期的なサーベイランス（再評価）の導入

2. CCRAの改革（サマリー）

- 製品ベンダーが独自に定めたセキュリティ仕様に対する評価（EALベース）からの脱却

- 技術分野に対応した「統一セキュリティ要件(cPP)」を開発し、cPP適合の認証を相互に承認

- cPPに最新技術を盛り込むために、国際的なテクニカル・コミュニティを作り、英知を結集

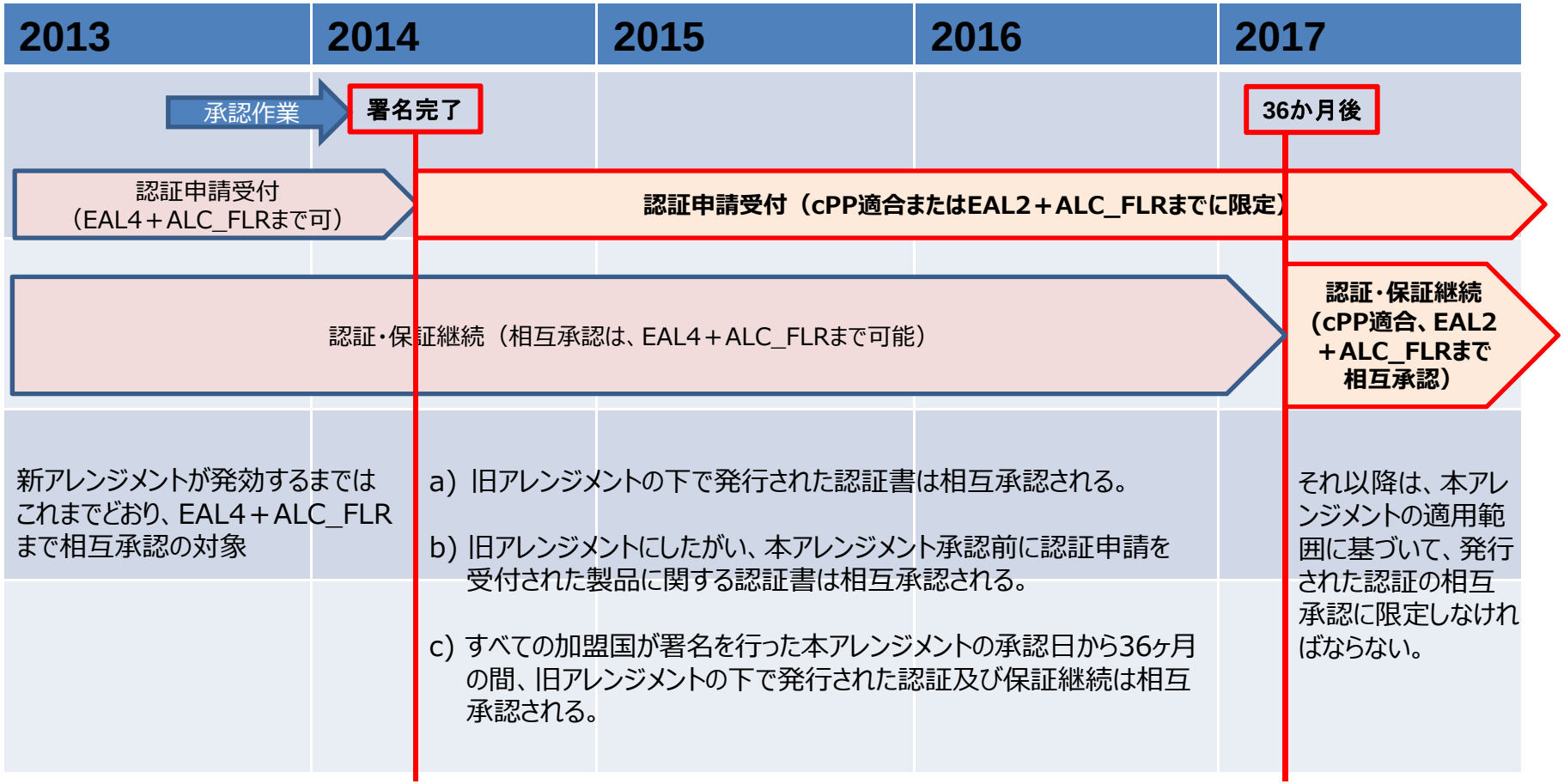
- cPPを適用できない場合は、EAL2＋ALC_FLRまでを相互承認

2. CCRAの改革（サマリー）

- 今後の方向性
  - 定期的なサーベイランス
    （最新の脆弱性情報に基づく再評価）の実施
  - CC/CEMの改訂
    モジュラーPPの導入
  - CCRAアレンジメント改訂
    新アレンジメントの批准・発効
    発効から3年後の完全実施へ
  - 各技術分野のcPP開発と政府調達での活用推進

2．CCRAの改革（サマリー）

- 移行スケジュール



2. CCRAの改革（サマリー）

- ICCC 2013の報告
  - 会期：2013年9月10日（火）～12日（木）
  - 会場：米国フロリダ州オーランド市（主催：米国認証機関NIAP）
  - 参加者：約300名
  - キーノート： 米国NSA Information Assurance Director, Ms. Debora Plunkett
    めまぐるしい技術革新の環境における規格としてCCを政府調達に活用し、
    相互承認を推進するために、cPPに基づく評価がその第一歩となる。
    2013年7月に米国政府の新調達ポリシーCNSSP-11が施行された。
    https://www.cnss.gov/Assets/pdf/CNSSP-11.pdf
  - 主なプレゼン内容：「CC活用の改革」、「技術」、「コラボレーション」の3テーマ
    - 各国の認証機関の最新状況報告、インドの認証国への昇格セレモニー
    - 米国政府承認PPに基づく評価の実際についての報告（NDPP評価など）
    - cPP開発に向けた取り組み、高保証レベル評価の報告、ほか
  - 日本からの発表：5件（IPA 3件、ECSEC Lab 1件、ECSEC 1件）
  - 認証書授与式：日本から、3社に授与

2. CCRAの改革（サマリー）

- 米国の新調達ポリシー CNSSP-11の概要
  - 発効：2013年7月一部修正（2013年6月10日付文書）

    https://www.cnss.gov/CNSS/issuances/Policies.cfm
  - 対象：米国政府機関における情報保証IT製品の調達
  - 第4章 ポリシー

    第5条　NSS（国家安全保障システム）における情報保護用に調達されるすべての市販の情報保証IT製品はNSA承認プロセスにしたがいNIAPプログラムの要求事項を満たさなければならない、また適用可能な場合FIPS暗号認証プログラム（CMVP、CAVP）の要求事項についても満たさなければならない。
  - 第5章 責任

    第8条　米国政府機関の長は、

    a) 本ポリシーの要求事項への適合を確実に実施しなければならない；

    b) NIAP適合製品リスト（PCL）から評価済の認証製品（市販の情報保証IT製品）を選択しなければならない；

    （以下省略）

Snap shots at ICCC 2013 in Orlando

3. cPP開発に向けた取り組み

- cPPとは？
- cPPを必要とする技術分野
- 誰がcPPを作るのか？
- どうやってcPPを作るのか？
- cPP開発の現状について
- 日本の対応は？

3. cPP開発に向けた取り組み

cPPとは？

- 定義
  - 「統一セキュリティ要件（cPP）と関連するサポート文書は、共通のセキュリティ機能要件・達成可能な保証レベルのミニマムセットとして定めるもので、認証製品がこのレベルを確実に達成するための脆弱性分析の要件を含む。
- 原則
  - EAL2＋ALC_FLRまでの保証コンポーネントとする。
  - ただし、各国で再現できるという根拠が示され、CCRAで承認を得た場合のみ、EAL4までの保証コンポーネントを含むことができる。
- CC/CEM
  - cPPは、CC/CEMに適合しなければならない。サポート文書は、CEMに対する解釈を与えるために作成される。CCRA承認の下、CC/CEMを修正することができる。
- 相互承認
  - cPP適合の認証は、cPPに適宜された機能要件、保証要件のみをカバーしなければならない。

3．cPP開発に向けた取り組み
cPPを必要とする技術分野

- cPP開発プロジェクトとして提案が予測される分野

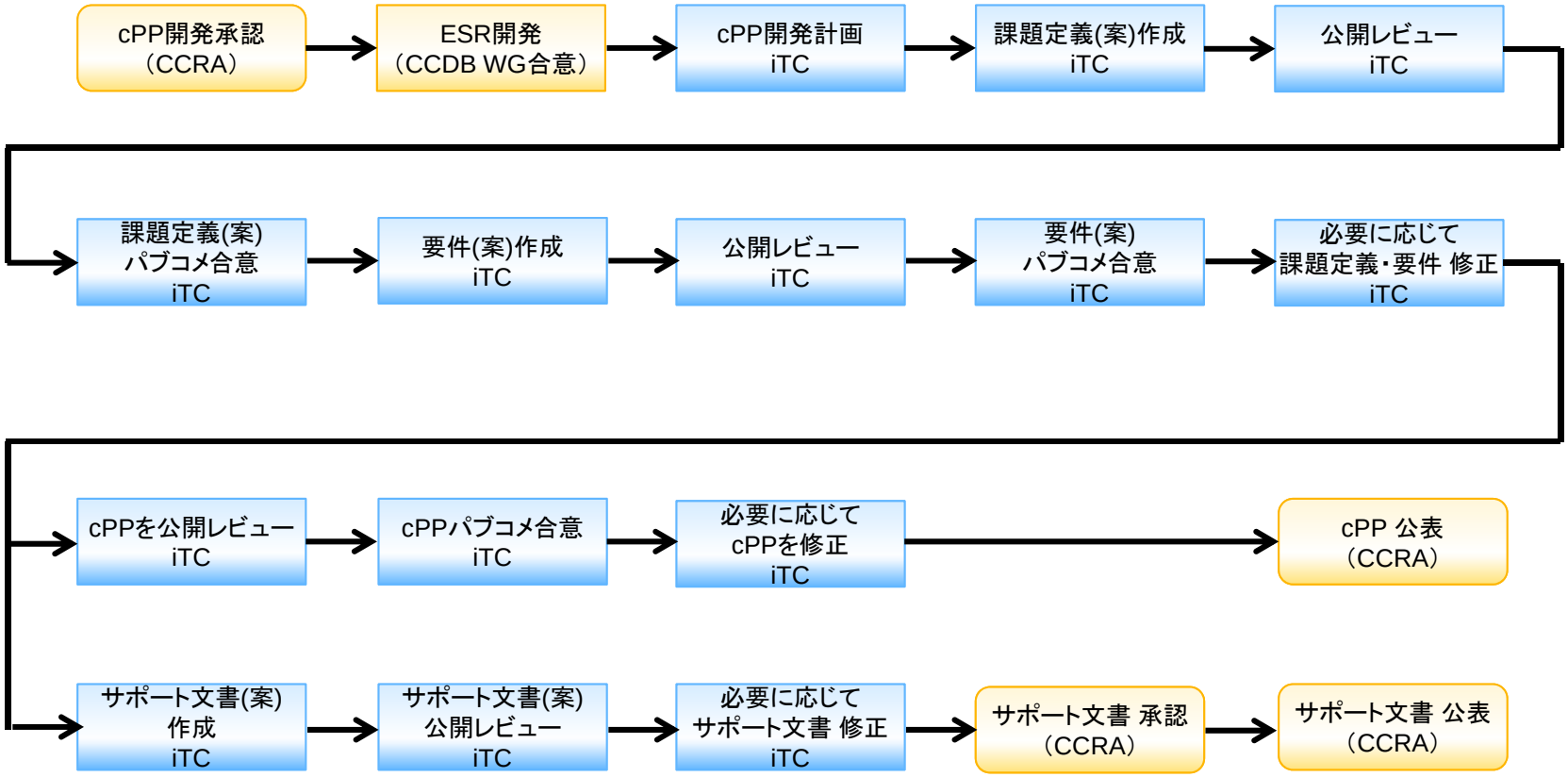
セキュリティ要件	参加国	状況
USB Portable Storage Devices	SE, US, UK, GE, AU, JP, etc.	US, GE, SE, SKのPPあり
Operating System	GE, US	GEとUS共同開発のGPOSあり
Multifunction Printers	JP, US, KR, SE, UK, GE	MFP-PPを日米で開発中
Mobile Gateway	UK, US, etc.	USG PPあり
Mobile Client Devices	UK, US, KR, etc.	USG PPあり
Network Device Firewall Extended Package	US, UK, etc.	USG PPあり
DBMS	未定（US,JP,GE,UK,・・・）	CCUF TCにて開発を開始
Encryption	US	USG PPあり
Applications	US	

3．cPP開発に向けた取り組み
誰がcPPを作るのか？

- cPPに求められる要求事項
  - 技術分野における最新技術を取り入れる
  - 具体的な評価方法を明確にする
  - 政府調達のミニマム・ベースライン保証要件とする
- CCRA各国の技術者、評価者の参画が必要
  - IT製品の製造者・開発者
  - 評価機関の評価者
  - セキュリティ技術者（コンサルタント）
  - 認証機関、政府機関
- CC Users Forumを創設（2012年7月）

3. cPP開発に向けた取り組み
どうやってcPPを作るのか？

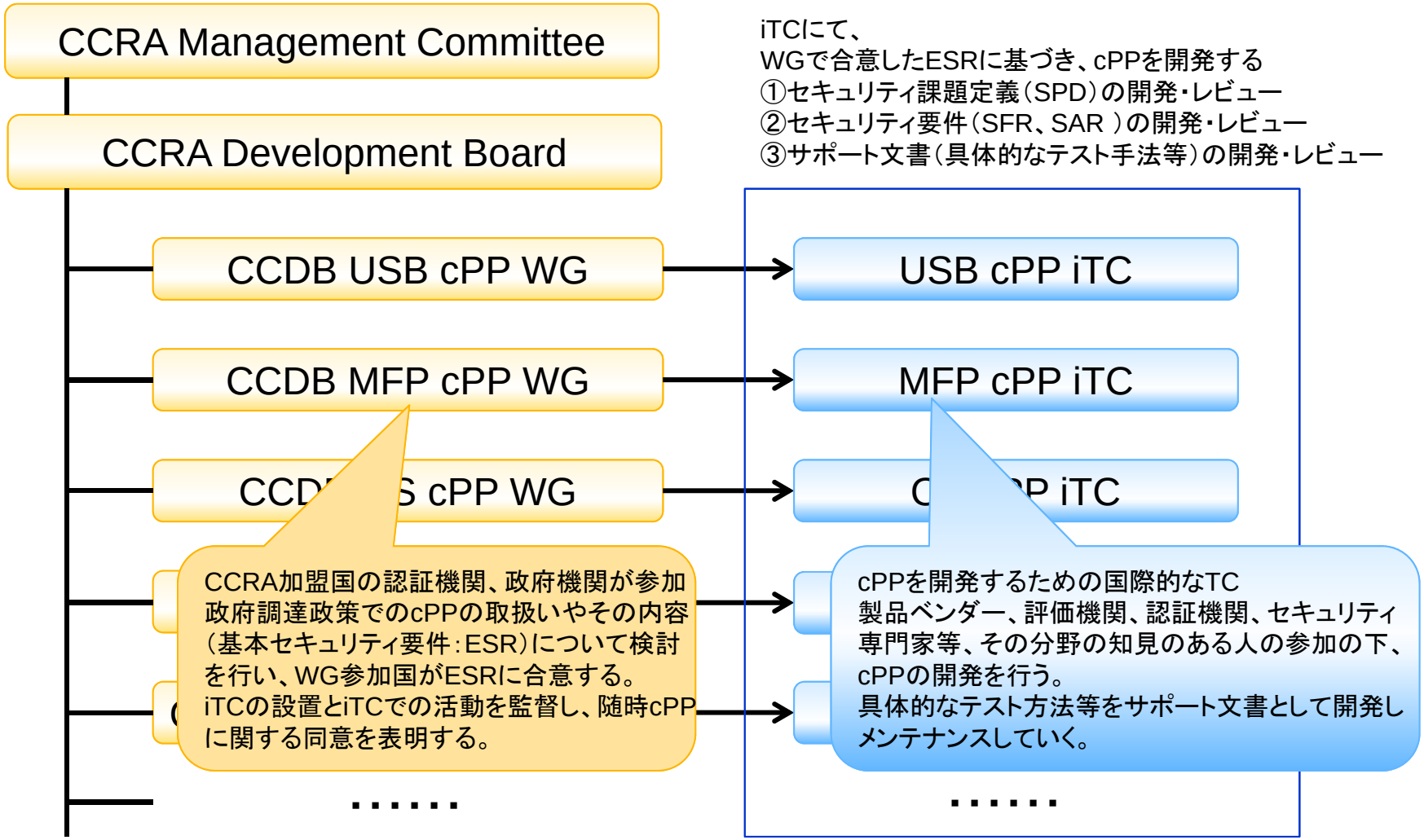
- cPP開発プロセス



3．cPP開発に向けた取り組み

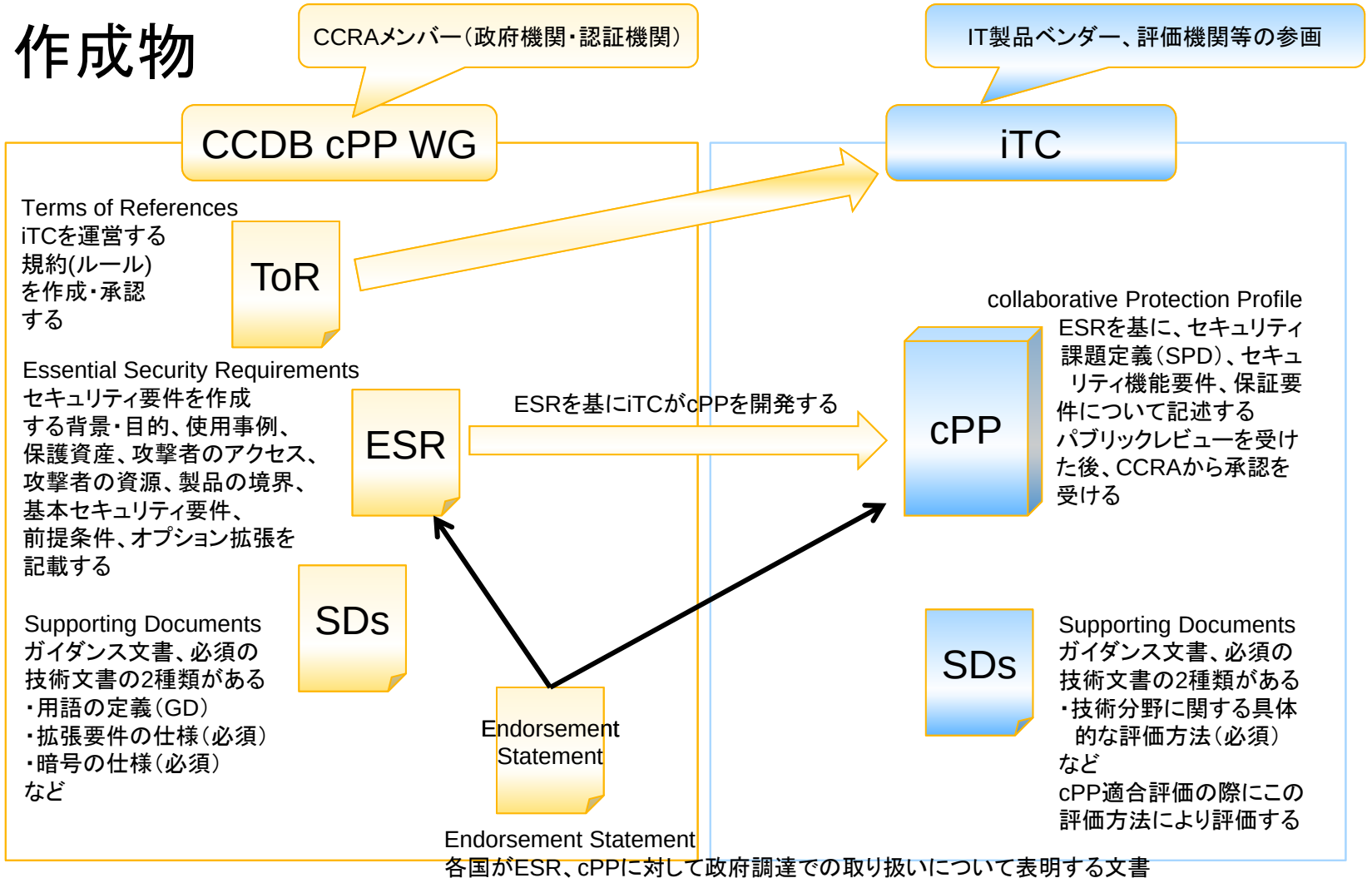
どうやってcPPを作るのか？

cPP開発体制



3. cPP開発に向けた取り組み
どうやってcPPを作るのか？

- 作成物



3．cPP開発に向けた取り組み
現状は？

- CC Users Forumとの協力
  - Chair：Alicia Squires（Cisco Systems）
  - Board Members:7名（投票により選出）
  - 参加者　約480名
    各国の評価機関、ベンダー、コンサルタント、認証機関、政府機関
  - ツール
    www.teamlab.comをポータルサイトとして活用
    TCごとに、電話会議（GotoMeeting, WebEx等）を活用
  - 参加費　無料（旅費、日当、通信費は各自負担）
  - 会議　年3回（春・秋 CCUF Workshop（CCRAと合同会議）、
    2月サンフランシスコ（RSAカンファレンス））

3．cPP開発に向けた取り組み
現状は？

- CCDB USB cPP WG（パイロットプロジェクト）
  - 参加国（2013年11月現在）

    SE, US, UK, GE, JP, DK, FI, SG, AU, NL, TRの11か国
  - 作業内容（毎週電話会議を開催し、年6回会合）

    cPP開発プロセスの検討（White Paper：解説書の作成）

    ESR（Essential Security Requirement）の作成・合意

    Endorsement Statement案の作成・ESRライフサイクルの検討

    ToR（規約）の作成・合意

    cPP共通の暗号に関するサポート文書の開発（ガイダンス文書：用語の定義、必須サポート文書：拡張要件、暗号の仕様書）

    cPPの認証申請者の募集

    現在のUSB PPの比較検討

    iTC設立に向けた準備

3．cPP開発に向けた取り組み
現状は？

- MFP PP TC
  - 参加者　約70名（Chair：IPA、NIAP）

    評価機関　9社16名

    ベンダー　18社45名

    認証機関　3か国（IPA（JP）、NIAP（US）、NIS（SK））
  - MFP PP v0.6.3のSFRについて審議中
    - 監査ログ生成の項目について
    - OSPの記述の修正
    - セキュア通信の要件
    - 暗号要件
    - 暗号機能の評価方法

3．cPP開発に向けた取り組み
現状は？

❑OS PP TC

- 参加者　21名（Chair：Matthias Intemann：BSI）

  評価機関（atsec(2),saic,ewa-canada,cgi,TUViT(2),corsec,BAH）

  ベンダー（baesystems,bluecoat,windriver,oracle, IBM, microsoft(2), Redhat）

  認証機関（NIAP(2),BSI）
- 実績

  2012年 ドイツ・米国主導で、OSPP v3.9を開発
- 今後の課題

  暗号に関する要件は重要。

  ラベルセキュリティは重要な拡張パッケージとして検討

  ToR作成。cPP開発のためのiTC設立要請の決定
- 3社の新規参加ベンダー、1社の新規参加評価機関

3．cPP開発に向けた取り組み
現状は？

- DBMS PP TC（CCUF TCとして活動中）
  - 参加者　40名

    評価機関（atsec(2),SiVenture,corsec,cgi,saic,BAH,cygnacom(4),
    ewa-canada(4),epoche&espri,TUViT(2),）

    ベンダー（oracle(5),Microsoft(3),IBM(3),

    認証機関ほか（TK(2),SK,mitre(2),nsa,IPA,BSI,opengroup,I3MLLC）
  - 活動

    Chair：Petra Manche（Oracle：UK）

    cPP化に向けたESRドラフトv0.4.4のレビュー中

    参加者のうち、韓国・日本以外は欧米のため、電話会議は
    日本時間午前3時となっている。（どこかが犠牲になる）

    3月のCCRA会合でのcPPプロジェクト承認を目指している

現状は？

- その他
- Network Devices TC（NIAP TeamLab）
- Enterprise Security Management TC（Google Groups）
- Mobile Devices TC（Mobile Devices TeamLab）
- Mobile Device Management TC（NIAP TC）
- Encrypted Storage TC（NIAP TC）

- 各TCへの参加希望の方は、

  jisec@ipa.go.jp までお願いします。

  登録されるまでサポートいたします。

4. 今後の対応についての提案

- おさらい
  - なぜ、今 CC改革が必要なのか？

調達者の視点	①最新版のIT製品をタイムリーに調達したい ②調達品のセキュリティ仕様（要件）をPPにより明確にしたい ③必要最小限のテストは確実に行われるようにしたい
利用者の視点	①利用環境にマッチしたIT製品かどうかを確認したい ②保護資産が確実に守れるIT製品を利用したい
IT製品製造者の視点	①セキュリティ評価のコストを低減したい。（国によって、何度も評価を受けることは避けたい） ②セキュリティ評価（EAL4）に多大な時間がかかり販売機会を失うことがある
認証機関の視点	①評価機関・評価者により評価品質にバラツキがある ②最新技術に対応したPP開発が困難（リソース・コスト） ③PPによる調達の法制化に時間がかかり、難しい

4. 今後の対応についての提案

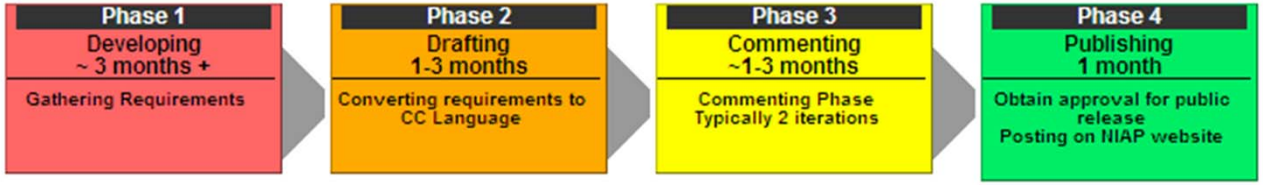
- おさらい
  - 今後の「安全なIT製品の政府調達」の成功は、
    ① 必要な技術分野に、cPPを開発し
    ② cPPをCCRA加盟国で共通に活用する
    ことに懸かっている

Protection Profiles in Development

https://www.niap-ccevs.org/pp/draft_pps/ (2013/11/14参照)

The following table lists all U.S. Government Protection Profiles currently being developed or modified and gives a general indication of their current status. For additional information, please send inquiries to niap@niap-ccevs.org.

Proposed Protection Profile Development Process



Protection Profile Status as of 13 November 2013

PP Name	Tech Type	Phase	Est. Completion
Protection Profile for Authentication Server Version 1.0	System Access Control	Phase 1	CY 2014, Q4
Protection Profile for Server Virtualization Version 1.0	Virtualization	Phase 1	CY 2014, Q3
Protection Profile for Applications on an Operating System Version 1.0	Applications	Phase 1	CY 2014, Q3
Protection Profile for Web Browsers Version 1.0	Applications	Phase 1	CY 2014, Q1
Protection Profile for Email Clients Version 1.0	Applications	Phase 1	CY 2014, Q1
Protection Profile for Redaction Version 1.0	Sensitive Data Protection	Phase 1	CY 2014, Q2
Protection Profile for Ethernet Security/Layer-2 Encryption Version 1.0	Network Encryption	Phase 1	CY 2014, Q2
Protection Profile for Certificate Authority Version 1.0	Certificate Management	Phase 2	CY 2014, Q1
Peripheral Sharing Switch for Human Interface Devices, Version 2.0	Peripheral Switch	Phase 2	CY 2014, Q4
Protection Profile for Multifunction Printer Version 1.0	Multi Function Device	Phase 2	CY 2014, Q4
Protection Profile for Software File Encryption Version 1.0	Encrypted Storage	Phase 2	CY 2014, Q2
Protection Profile for Intrusion Prevention Systems Version 1.0	IDS/IPS	Phase 2	CY 2014, Q4
Protection Profile for Enterprise Security Management-Access Control Version 2.1	Security Management	Phase 4	CY 2014, Q4

調達者の皆様へ

- cPP開発状況の共有について
  - 公開情報について

    IPAのホームページに、公開情報を掲載しますので、適宜、参照いただきたい

  - 非公開情報の共有について

    cPP WG、iTCでの検討中の情報を共有するためのメーリングリスト（ML）を立ち上げますので、MLへの参加を希望される方は、登録をお願いします

4. 今後の対応についての提案
各技術分野の製品ベンダーの皆様へ

- iTCへの参加
  - 直接、テクニカルコミュニティに参加していただき、積極的な活動をお願いします
- cPP開発状況の共有について
  - 公開情報について

    IPAのホームページに、公開情報を掲載しますので、適宜、参照いただきたい
  - 非公開情報の共有について

    技術分野ごとに創設される iTC に対応したメーリングリスト（ML）を立ち上げる予定です。MLへ登録をお願いします

ご清聴ありがとうございました。