「ITセキュリティ評価及び認証制度」に関する説明会

2017年3月17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

説明会について

内容：
ISO15408(CC)及びそれを用いた認証制度の概要
対象：
CCや認証制度に関する知識を有していない方

- 第1部：認証制度と評価基準
  制度の目的、相互承認、CCの概要
- 第2部：制度の活用
  政府調達の現状
- 第3部：認証制度の手続き
  認証の申請、評価機関の承認
- 第4部：制度に関する情報
  関連URL等

IPA Better Life with IT

第1部

認証制度及び評価基準の概要

セキュリティ評価制度とは

- ITセキュリティ評価及び認証制度
  - 国際的なセキュリティ評価標準ISO/IEC 15408(Common Criteria)に基づきIT製品を認証する制度
  - セキュリティ機能の妥当性及び実装の正確性を第三者（評価機関）が評価し、その評価がCCに基づいて行われたことを認証機関（公的機関*）が確認する

*国から委託された民間機関も可

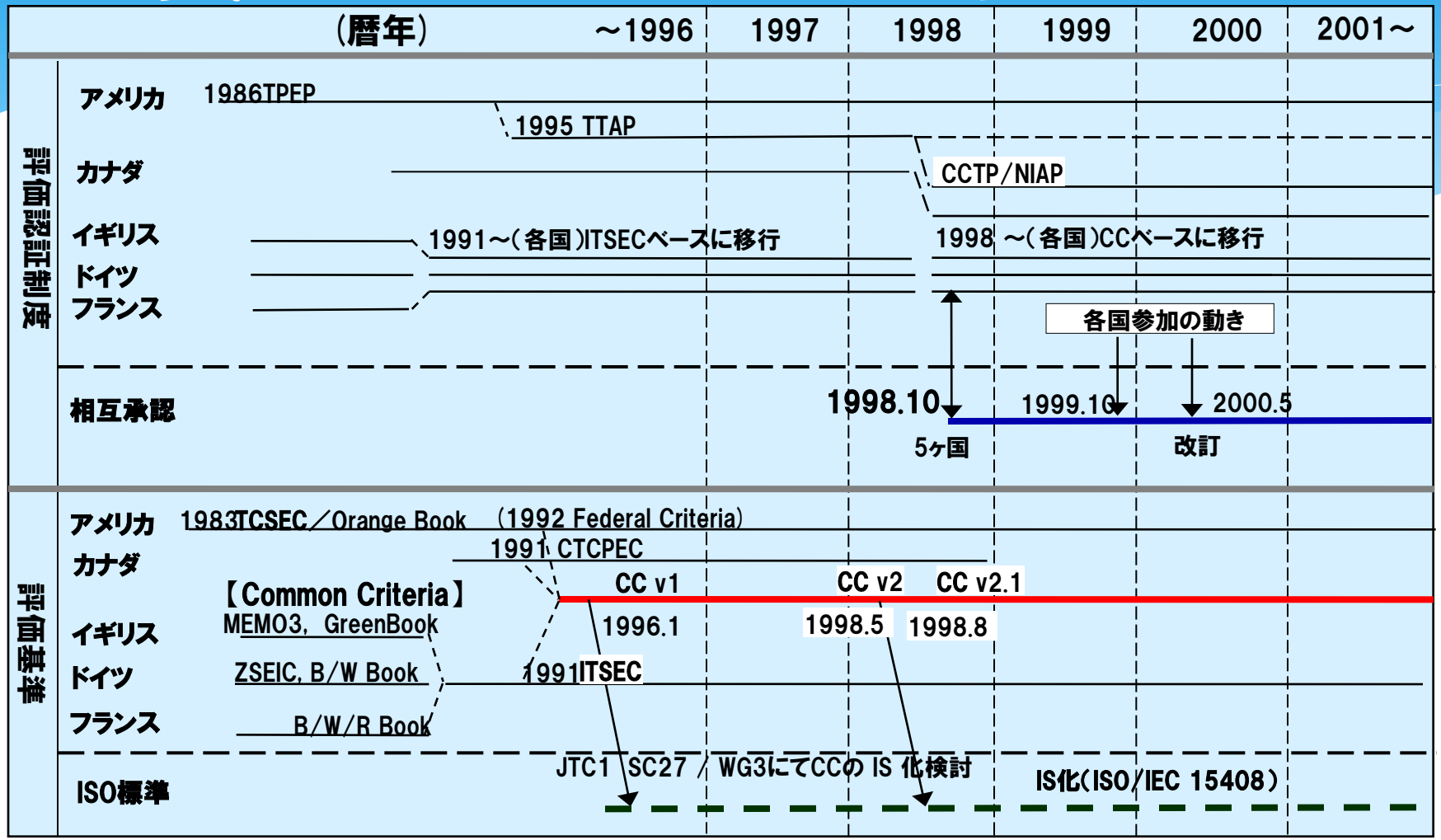
- 目的
  - 政府の民需製品調達におけるセキュリティの確保

セキュリティ評価制度とは

経緯

- 欧米諸国、ロシアによる自国でのセキュリティ評価・認証制度
  →非関税障壁化・相互接続性、調達コスト・効率の懸念
- CCプロジェクトの結成
  カナダ、フランス、ドイツ、オランダ、イギリス、アメリカ6ヵ国
- CCのISO化
  1999年6月にISO/IEC 15408として承認
- 相互承認の拡大
  1998年 オランダを除く5ヵ国で相互承認
  2000年相互承認協定の拡大(CCRA)
  2003年日本参加
  2017年現在27ヵ国が参加

【資料】セキュリティ評価の遍歴



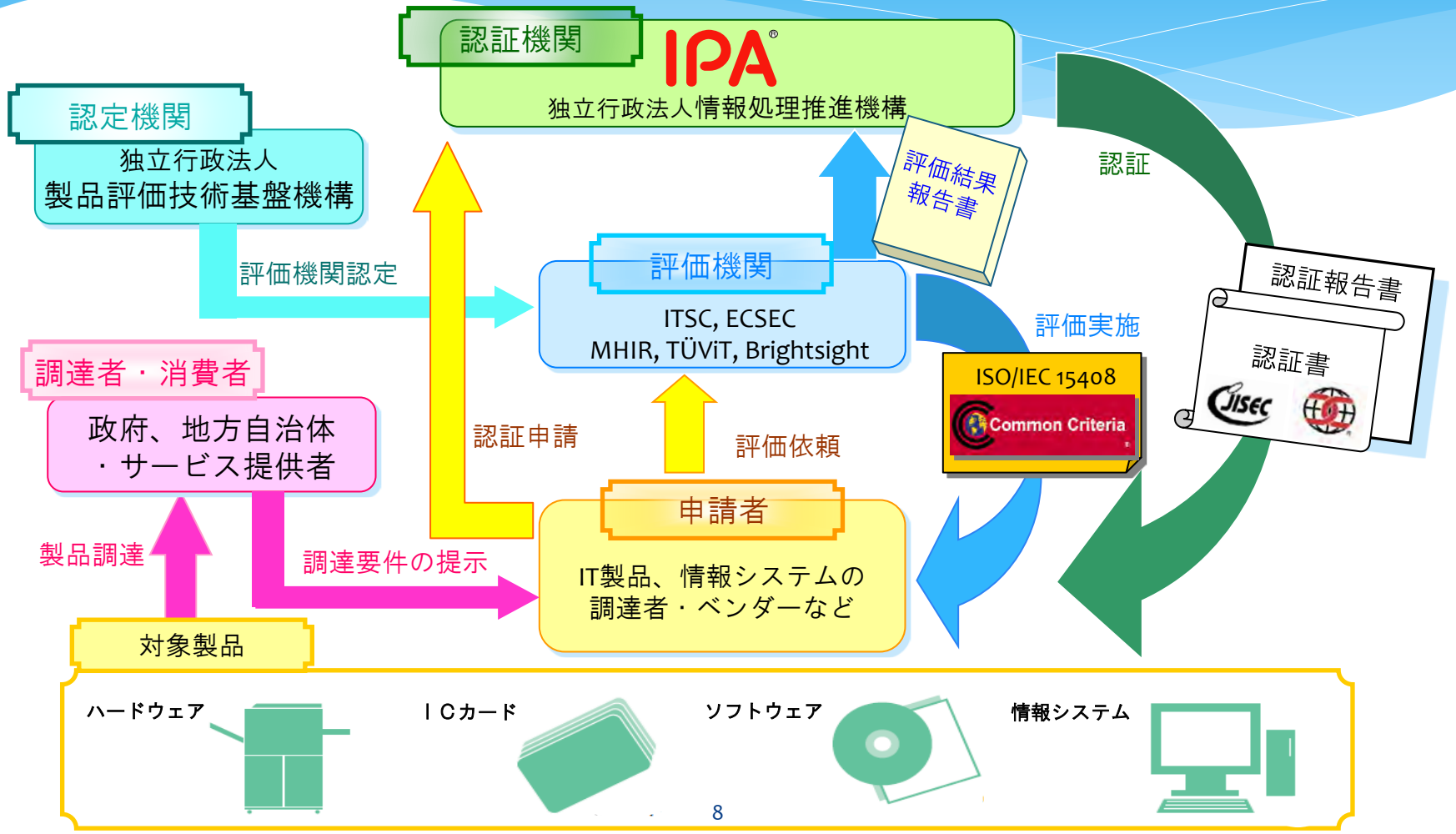
JISEC

Japan Information Security Evaluation and Certification Scheme

- 日本のITセキュリティ評価及び認証制
  - 日本政府のセキュアな基盤構築におけるIT製品調達のため2001年創設
  - 2003年に国際的なCC相互承認アレンジメント(CCRA)に参加
- IPAの役割
  - 評価機関が実施した評価結果を検証し認証する認証機関としてJISECを運営
  - 国際的なCC相互承認アレンジメント(CCRA)における日本唯一の加盟機関

JISEC

Japan Information Security Evaluation and Certification Scheme



CCRA

Common Criteria Recognition Arrangement

（認証国）

（受入国）

受入れ

ARRANGEMENT on the Recognition of Common Criteria Certificates In the filed of Information Technology Security

IPA Better Life with IT

CC(Common Criteria)とは

要求仕様と製品仕様

- 要求仕様

  調達者A：

  - セキュアな製品であること

  調達者B：

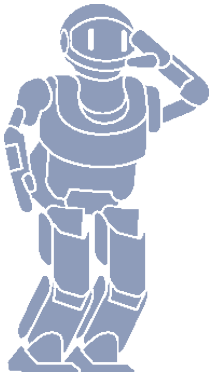
  - 誰かが不正なアクセスを試みた場合、追跡可能なセキュリティログをとること
  - …

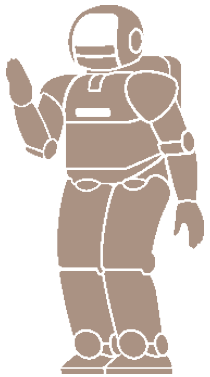
要求仕様と製品仕様

- 要求仕様
  セキュリティログをとること

- 製品仕様

  製品A：
  - 認証失敗時にIDと時間のログをとる
  - 管理者はログを閲覧・削除できる
  - ログ領域がなくなったら停止する
  - …





  製品B：
  - 認証の失敗と成功時にIDと時間のログをとる
  - 管理者はログを閲覧のみ、監査者はログを閲覧・削除できる
  - ログ領域がなくなったら古いデータから上書きする
  - …

CCによる機能の指定
監査データ生成(FAU_GEN.1)の例

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;
b) 監査の[選択: 最小、基本、詳細、指定なしから1つ選択]レベルのすべての監査対象事象;及び
c) [割付:上記以外の個別に定義した監査対象事象]

FAU_GEN.1.2 TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗);及び
b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査情報]

CCによる機能の指定
監査データ生成(FAU_GEN.1)の例

- 依存する機能の提示

FAU_GEN.1 監査データ生成

依存性： FPT_STM.1 高信頼性タイムスタンプ

- 関連する監査事象の提示

FIA_SOS.1 秘密の検証

監査： セキュリティ監査データ生成(FAU_GEN)がPP/STに含まれていれば、以下のアクションを監査対象にすべきである;

a) 最小: TSFによる、テストされた秘密の拒否;

b) 基本: TSFによる、テストされた秘密の拒否または受け入れ;

C) 詳細: 定義された品質尺度に対する変更の識別

CCによる機能の指定

- セキュリティ監査 (FAU)
- 通信 (FCO)
- 暗号サポート (FCS)
- 利用者データ保護 (FDP)
- 識別と認証 (FIA)
- セキュリティ管理 (FMT)
- プライバシー (FPR)
- TSF保護 (FPT)
- 資源利用 (FRU)
- TOE アクセス (FTA)
- 高信頼パス/チャネル (FTP)

CC Part 2 セキュリティ機能要件集

CCによる機能の指定

セキュリティ監査 (FAU)

- FAU_ARP
  セキュリティ監査自動応答
- FAU_SAR
  セキュリティ監査レビュー
- FAU_GEN
  セキュリティ監査データ生成
- FAU_SEL
  セキュリティ監査事象選択
- FAU_SAA
  セキュリティ監査分析
- FAU_STG
  セキュリティ監査事象格納

PP(要求仕様)とST(製品仕様)

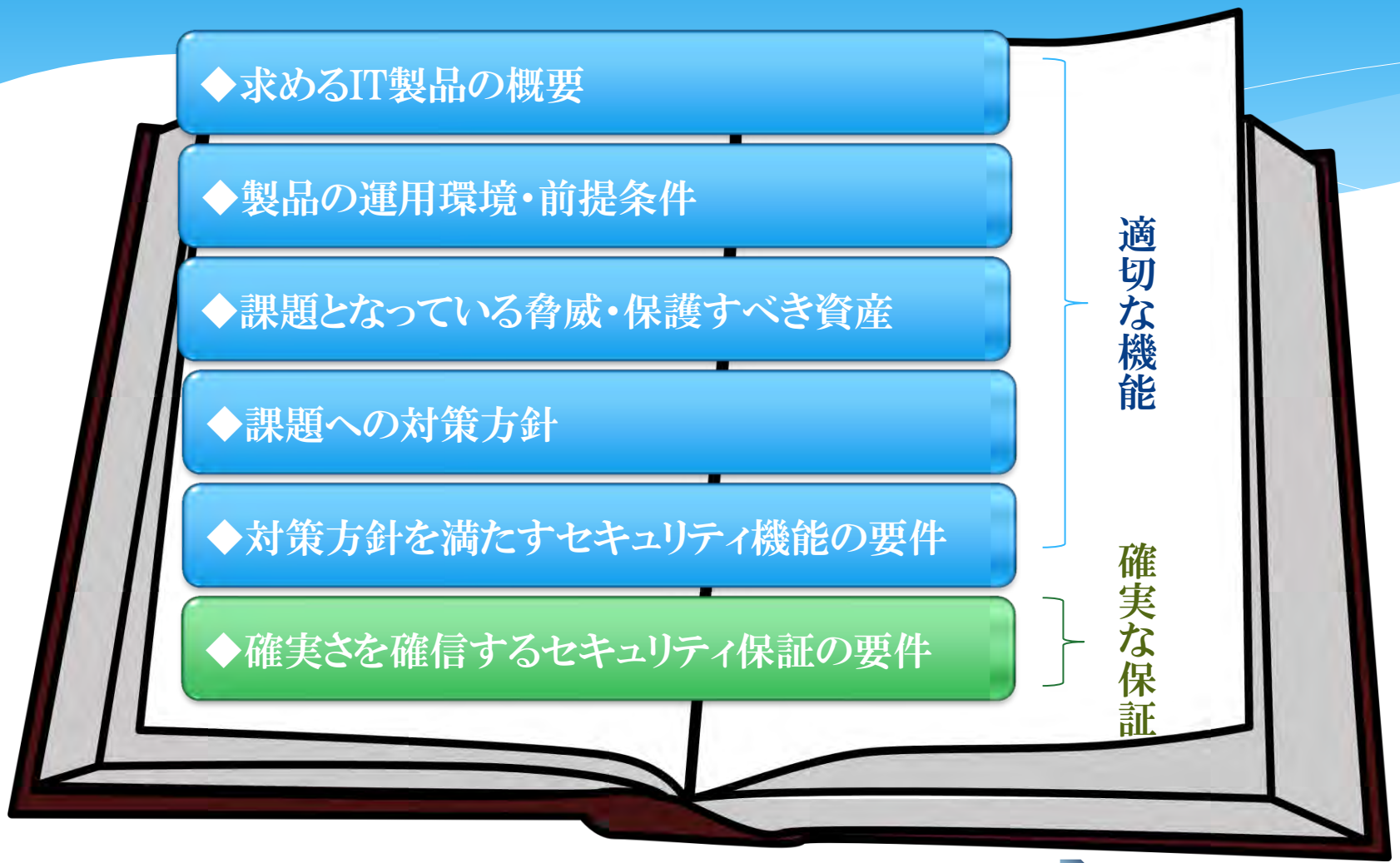
- PP：Protection Profile

  調達側が、IT製品への適切な機能（使用する環境や対抗する脅威、対応するセキュリティ機能）と保証すべきレベルをCCに従った方法で指定する

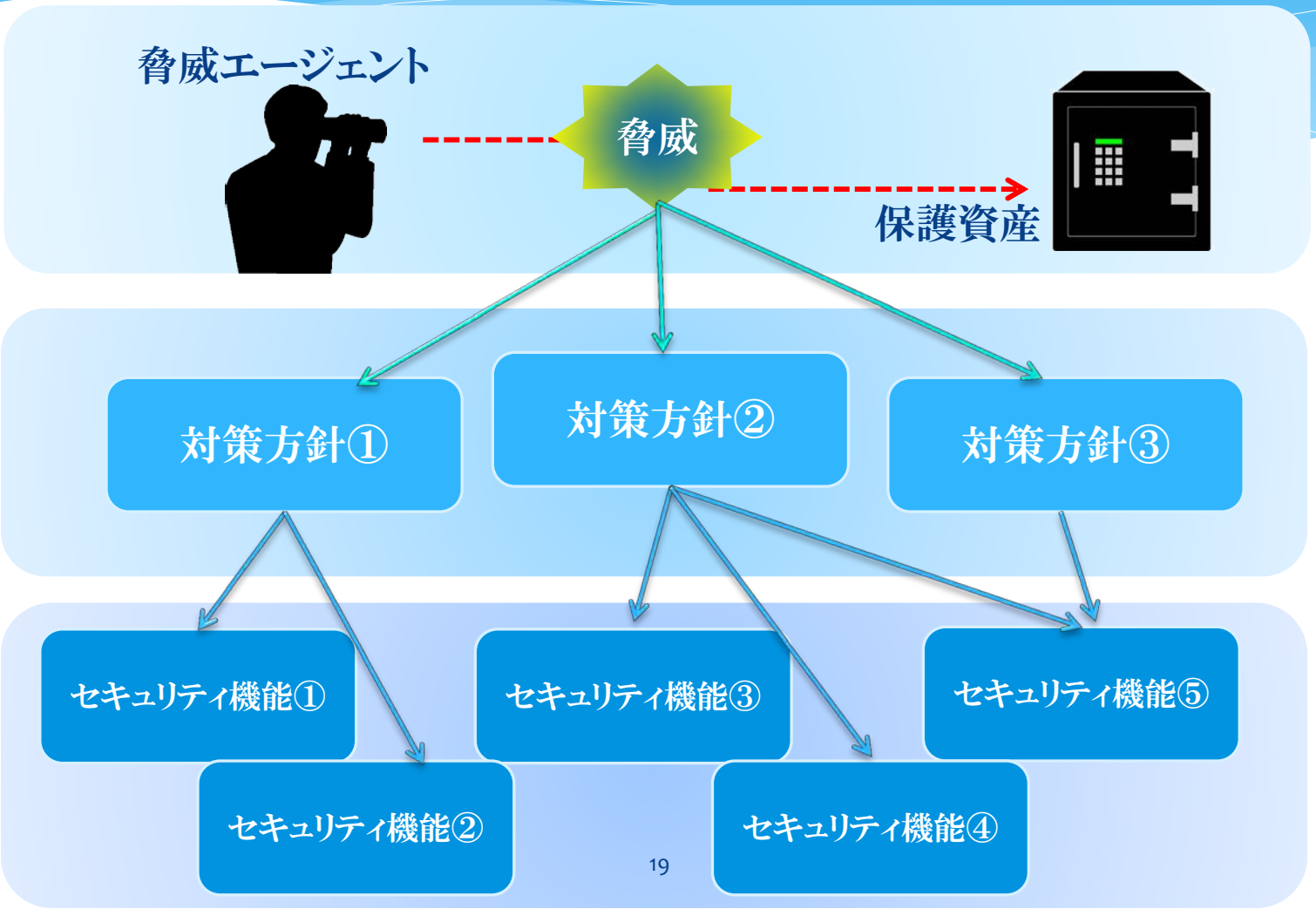
- ST：Security Target

  IT製品提供者が、IT製品のセキュリティ要件が調達者要件を満たす(PPに適合)ことを宣言する

PPの構成


◆求めるIT製品の概要
◆製品の運用環境・前提条件
◆課題となっている脅威・保護すべき資産
◆課題への対策方針
◆対策方針を満たすセキュリティ機能の要件
◆確実さを確信するセキュリティ保証の要件
適切な機能
確実な保証

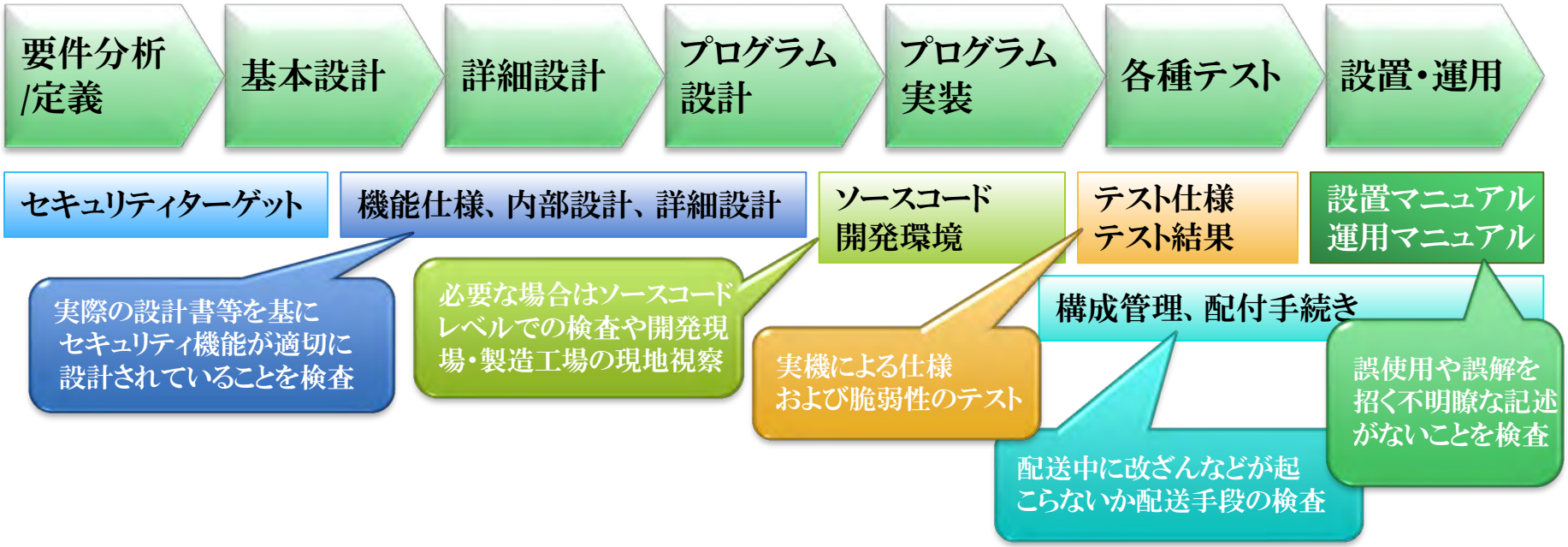
PPの構成


脅威エージェント
脅威
保護資産
対策方針①
対策方針②
対策方針③
セキュリティ機能①
セキュリティ機能②
セキュリティ機能③
セキュリティ機能④
セキュリティ機能⑤

IPA Better Life with IT

製品仕様と実装の検査

- ✓ 実際の製品は要求仕様に準拠しているか？
- ✓ 実装において潜在的な脆弱性はないか？



セキュリティ機能の正確性と脆弱性をライフサイクル全体を通して確認

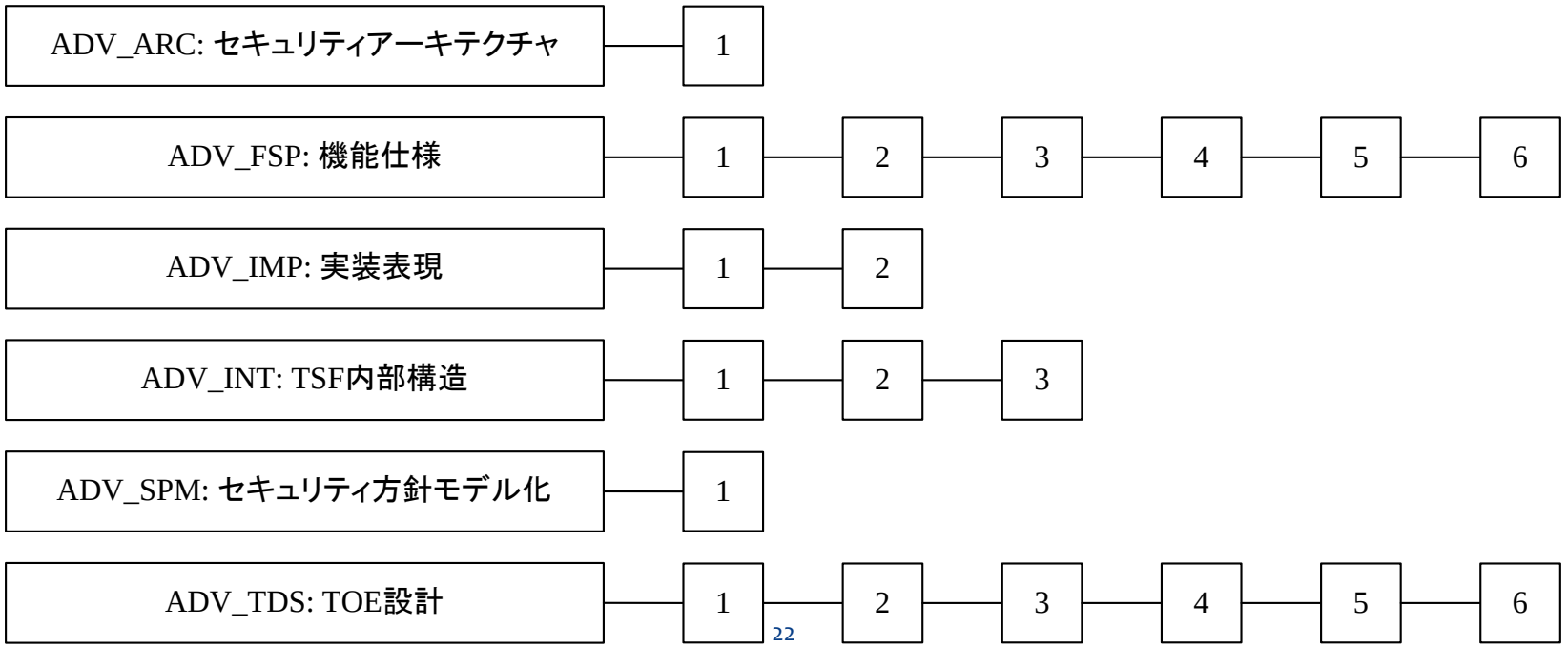
CCによる保証の指定

保証クラス	保証ファミリ	保証クラス	保証ファミリ
開発	ADV_ARC	セキュリティターゲット評価	ASE_CCL
	ADV_FSP		ASE_ECD
	ADV_IMP		ASE_INT
	ADV_INT		ASE_OBJ
	ADV_SPM		ASE_REQ
	ADV_TDS		ASE_SPD
ガイダンス文書	AGD_OPE		ASE_TSS
	AGD_PRE	テスト	ATE_COV
ライフサイクルサポート	ALC_CMC		ATE_DPT
	ALC_CMS		ATE_FUN
	ALC_DEL		ATE_IND
	ALC_DVS	脆弱性評定	AVA_VAN
	ALC_FLR		
	ALC_LCD		
	ALC_TAT		

CC Part 3 セキュリティ保証要件集

開発
ADVクラス

セキュリティ機能の仕様やセキュリティ機能自体の保護に関する保証要件



ガイダンス文書
AGDクラス

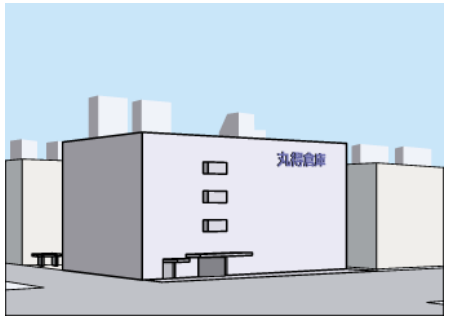
ガイダンスが利用者や管理者等がセキュアに準備・操作するために適切であるかの保証要件

AGD_OPE: 利用者操作ガイダンス	1
AGD_PRE: 準備手続き	1

ライフサイクルサポート
ALCクラス

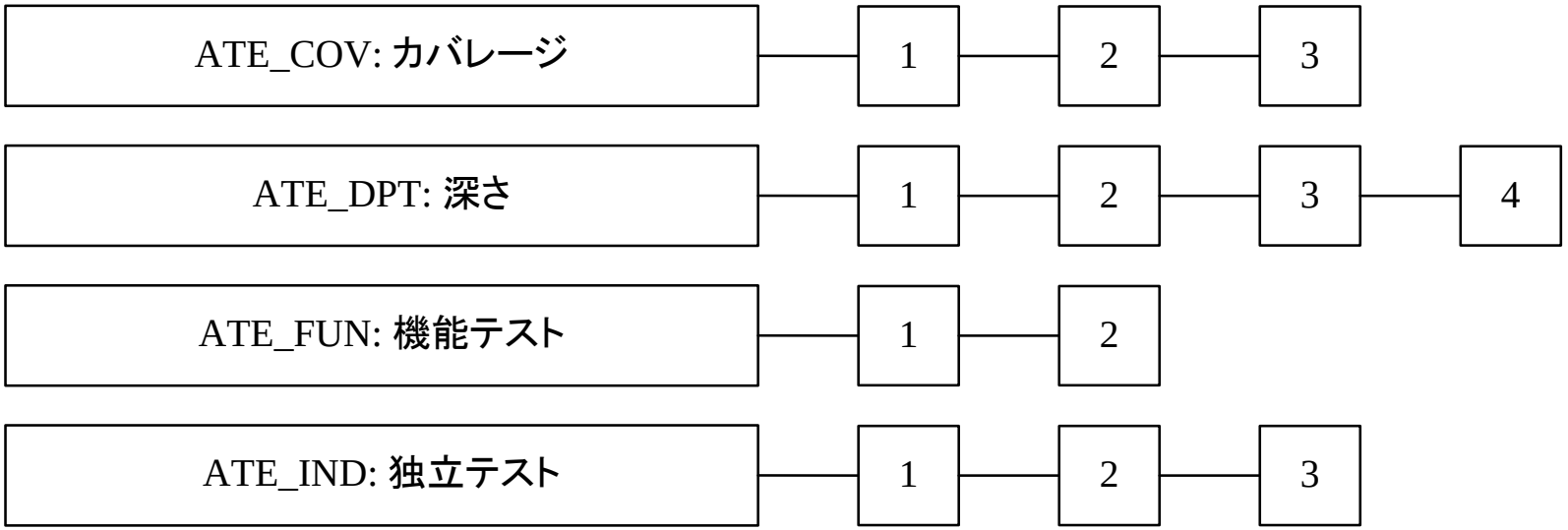
開発及び保守におけるセキュリティ確保に関する保証要件

ALC_CMC: CM能力	1	2	3	4	5
ALC_CMS: CM範囲	1	2	3	4	5
ALC_DEL: 配付	1				
ALC_DVS: 開発セキュリティ	1	2			
ALC_FLR: 欠陥修正	1	2	3		
ALC_LCD: ライフサイクル定義	1	2			
ALC_TAT: ツールと技法	1	2	3		



テスト
ATEクラス

評価対象が機能仕様に従ってふるまうことを確認するための保証要件



脆弱性分析
AVAクラス

評価対象の開発・運用における脆弱性評定に係る保証要件

AVA_VAN: 脆弱性分析	1	2	3	4	5

保証の深さ
AVA_VANの例

AVA_VAN.1　脆弱性調査

依存性:ADV_FSP.1基本機能仕様
AGD_OPE.1 利用者操作ガイダンス
AGD_PRE.1 準備手続き

AVA_VAN.1.2E 評価者は、TOEの潜在的脆弱性を識別するために、公知の情報源の探索を実行しなければならない。

AVA_VAN.1.3E 評価者は、基本的な攻撃能力を持つ攻撃者からの攻撃にTOEが耐えられることを決定するために、識別された潜在的脆弱性に基づいて侵入テストを実施しなければならない。

保証の深さ
AVA_VANの例

AVA_VAN.3　焦点を置いた脆弱性分析

依存性:
- ADV_ARC.1 セキュリティアーキテクチャ記述
- ADV_FSP.4 完全な機能仕様
- ADV_TDS.3 基本モジュール設計
- ADV_IMP.1 TSFの実装表現
- AGD_OPE.1 利用者操作ガイダンス
- AGD_PRE.1 準備手続き
- ATE_DPT.1 テスト：基本設計

AVA_VAN.3.2E　評価者は、TOEの潜在的脆弱性を識別するために、公知の情報源の探索を実行しなければならない。

AVA_VAN.3.3E　評価者は、TOEの潜在的脆弱性を識別するために、ガイダンス証拠資料、機能仕様、TOE設計、セキュリティアーキテクチャ記述、及び実装表現を使用して、TOEの焦点を置いた独立脆弱性分析を実行しなければならない。

AVA_VAN.3.4E　評価者は、強化基本的な攻撃能力を持つ攻撃者からの攻撃にTOEが耐えられることを決定するために、識別された潜在的脆弱性に基づいて侵入テストを実施しなければならない。

第1部まとめ

- 認証制度
  - 民需製品の政府調達のために生まれた
  - 認証制度はその結果を国際的に相互に承認している
- Common Criteria
  - 要求仕様を適切に表すために、機能要件を形式化
  - 仕様が確実に実装されていることを確認するために、保証要件のカタログを規定
  - 持つべきセキュリティ機能を機能要件で、セキュリティ機能を確認する厳格さを保証要件で指定する

第2部

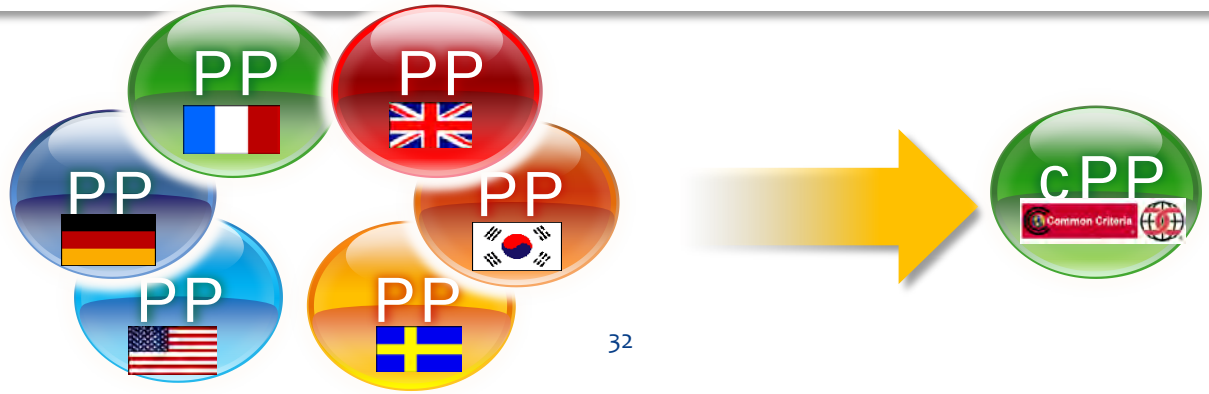
認証制度の活用

CCRA各国の活用

- 欧米のCCRA加盟各国ではPPを開発し、政府調達要件として使用
- PPに準拠した認証製品を調達

世界共通セキュリティ要件の開発

- 共通化されたミニマムなセキュリティ要件
  - cPP（Collaborative Protection Profile）
    CCRA加盟国が共同で作成し活用する、政府調達のための世界共通のセキュリティ要件
  - サポート文書
    cPPごとに具体的な評価手法を記載
- cPPのコンセプト
  - 要件開発や対応製品開発コストの削減
  - テスト方法を具体的に記載することで評価品質を確保



わが国の状況

2014年5月より調達時のセキュリティ要件を求める

- 政府機関の情報セキュリティ対策のための統一基準

- IT製品の調達におけるセキュリティ要件リスト

わが国の状況
統一基準

❑政府統一基準

- 2014年5月に、「政府機関の情報セキュリティ対策のための統一基準」が改訂され、内閣官房情報セキュリティセンターから発表
- 政府でのIT製品調達時の基準として、経済省の公開する「IT製品の調達における要件リスト」を参照し、セキュリティ要件を策定することを求めた。

■5.2.1 情報システム企画・要件定義

(c) 情報システムセキュリティ責任者は、機器等を調達する場合には、「IT製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

政府機関調達の情報セキュリティ対策のための統一基準(平成28年度版)
平成28年8月31日　サイバーセキュリティ戦略本部

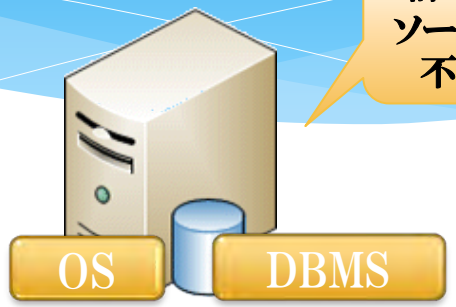
セキュリティ要件の策定

管理機能への不正アクセスによる設定の変更

FW

IDS/IPS

許可されないリソース・機能への不正アクセス

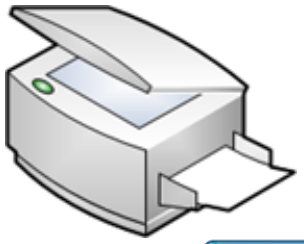


OS

DBMS

利用者識別認証機能 等

アクセス制御機能 等



暗号化機能 等

リース返却後の文書データの漏えい

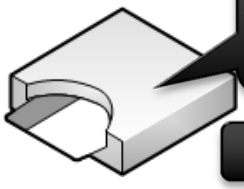
複合機

耐タンパ機能 等

放置・紛失・盗難等による機密情報の漏えい

USBメモリ

HDD完全消去機能 等



ICチップへの物理的攻撃による情報読み出し

ICカード

わが国の状況
要件リスト

❑セキュリティ要件リスト

- 2014年5月に、「IT製品の調達におけるセキュリティ要件リスト」が経済産業省から発表
- IT製品調達時にセキュリティ要件の確認手段を求める製品分野とその要件が掲載されている

セキュリティ要件リスト（脅威と要件）

製品分野名	ファイアウォール

セキュリティ上の脅威	① **管理機能等への不正アクセスによる不正な通信の発生** 不正な通信を制御するための規則（セキュリティポリシー）等を管理する機能等に対してアクセス権限のない者が、正当な利用者になりすますことができれば、不正に操作される可能性がある。不正操作により、本来実施されるべき情報フロー制御が実施されず、組織内外からの不正な通信を排除できず、セキュリティ侵害に繋がる可能性がある。例えば、インターネット等のオープンな環境からの通信が、管理されるべき内部のネットワークへとアクセスされ、内部のネットワークに接続されるサーバ等が何らかの被害を受ける可能性がある。またインターネット等のオープンな環境に存在し、利用が禁止されているサービスに対して、内部のネットワークから通信し、秘匿されるべき情報が流失する等の可能性がある。
	② **ネットワーク処理の残存情報からの情報漏えい** 送信したネットワークパケットが使用しているバッファまたはメモリエリアに、パケットに含まれるデータが残存している場合、別のパケットがそのバッファを再利用することで、送信済みのデータが別のパケットに含まれ、機密情報（に関連したデータ）が漏えいする可能性がある。
	③ **リモートで管理する場合の通信データの盗聴、改ざん** 管理権限のある者が遠隔地からリモートで管理する際に、製品との間で通信されるセキュリティ関連情報を含むデータが盗聴、改ざんされる可能性がある。管理者パスワード等が盗聴により不正に取得された場合には、ファイアウォールの設定が不正に変更される恐れがある。
	④ **監査ログの改ざん・不正な削除** 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments Version 1.1 [6] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①，②，③，④
[2]：U.S. Government Approved Protection Profile – Protection Profile for Network Devices Version 1.1 [7] 及びU.S. Government Approved Protection Profile – Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall Version 1.0 [8]	①，②，③，④

確認すべきセキュリティ事項
・守るべき資産
・想定される脅威

上記脅威の対抗手段
（プロテクションプロファイル）

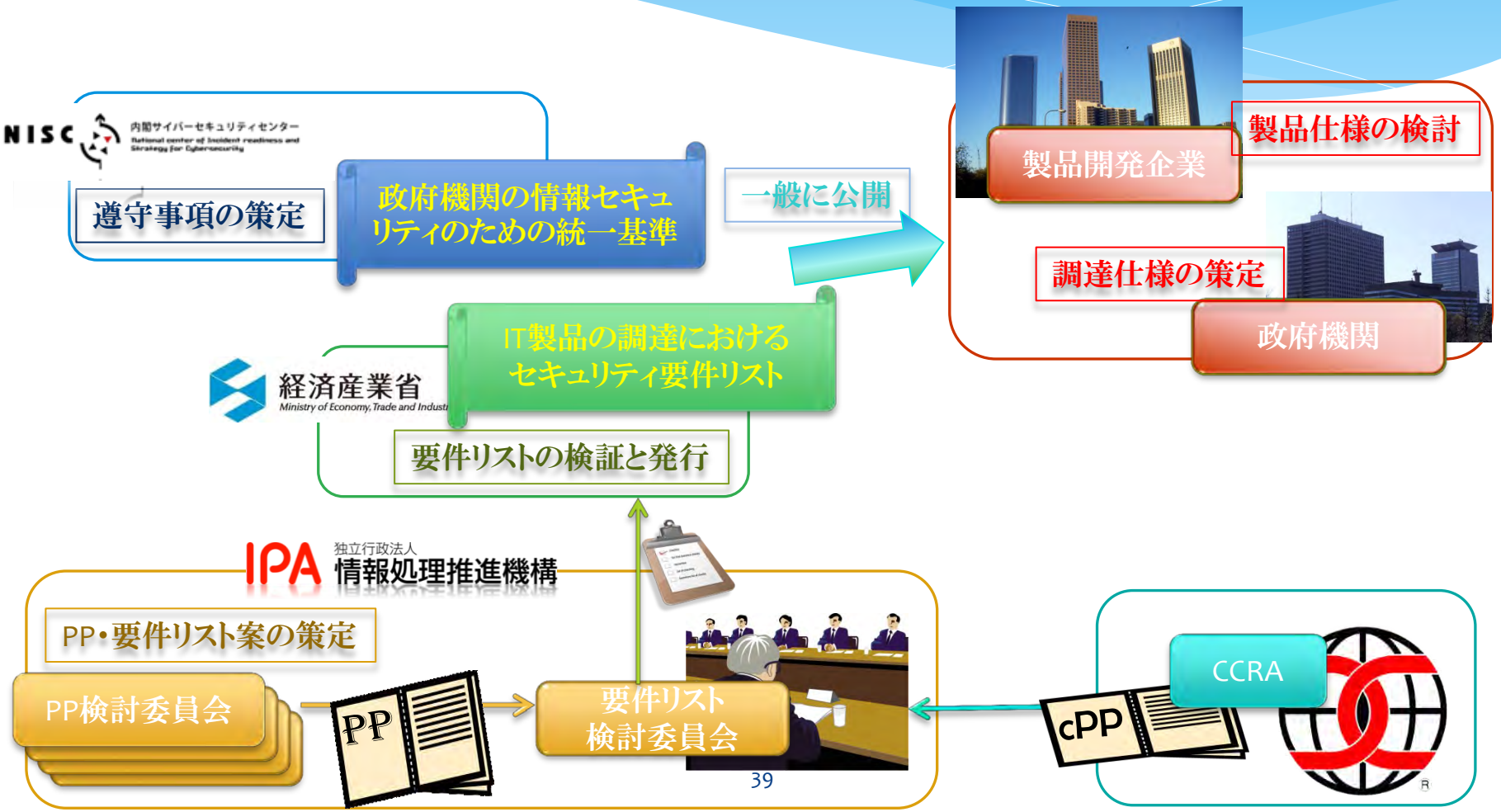
IT製品の調達におけるセキュリティ要件リスト
平成26年5月19日　経済産業省

セキュリティ要件リスト（対象製品分野）

対象製品分野	製品分野定義
デジタル複合機	プリント機能を有し、さらに、スキャン、FAX、コピー機能のうちいずれか2つ以上の機能を装備している製品
ファイアウォール	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品
不正侵入検知/防止システム（IDS/IPS）	ネットワークやシステムの稼動状況を監視し、組織内のコンピューターネットワークへの外部からの侵入を報告、防御する製品
サーバOS	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア
データベース管理システム	共有データとしてのデータベースを管理し、データに対するアクセス要求に応える製品
スマートカード	プラスチック製カード等にIC チップを埋め込み、情報を記録できるようにした製品
対象候補	**製品分野定義**
USBメモリ	製品自体にUSBコネクタを備えており、別途USB接続ケーブル等を用いる必要がない、フラッシュメモリを内蔵した持ち運び可能な記憶装置

IT製品の調達におけるセキュリティ要件リスト
平成26年5月19日　経済産業省

セキュリティ要件リストの検討



「デジタル複合機の賃貸借及び保守業務」に係る一般競争入札
IPA 2014年12月実施 入札説明書

(3) セキュリティ要件【共通要件】

ア　納入するデジタル複合機は，「IEEE Std 2600.1 TM - 2009, Protection Profile for Hardcopy Devices, Operational Environment A Version 1.0」又は「U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2 TM - 2009)」と同等以上のセキュリティ要件に適合したCommon Criteria（CC）認証（ISO/IEC 15408）取得している製品であること。なお，提案するデジタル複合機がCC認証の取得申請中の場合，当該製品がITセキュリティ評価及び認証制度（JISEC）のWebサイト（https://www.ipa.go.jp/security/jisec/index.html）にある「評価・認証中リスト」に掲載されている製品であり，かつ当該製品の一代前のモデルが当該認証を取得していることを証明すること。

第3部

認証制度の手続き

認証申請に係る手続き

- 評価対象・評価範囲の決定
- STの作成・製品開発
- 評価機関の選定
- 認証申請・評価開始

認証申請に係る手続き
評価対象の決定

- 製品のセキュリティ要件の決定
  - セキュリティ要件リスト対象分野であれば、PPに適合
  - 対象でなければ、調達者のセキュリティ要件や類似製品のセキュリティ要件(ST)を参考に決定

* 前提条件、脅威（資産・脅威エージェント）を識別
* 評価対象は調達可能な単位

認証申請に係る手続き
評価範囲の決定

- 製品の評価範囲の決定
  - セキュリティ要件リスト対象分野であれば、PPに適合
  - 対象でなければ、調達者のセキュリティ要件やコスト対効果により決定

* 外部インタフェース～ソース、開発現場セキュリティ、構成管理ツール、脆弱性評定等々
* 広く詳細な評価は高い保証を与えるが費用・時間もかかる
* 関連する部門との調整（外部委託先等）

認証申請に係る手続き
STの作成

- STの作成
  PPに従い（なければ独自に）作成
  - 脅威や保護資産を「セキュリティ課題定義」として記述
  - それらの対抗手段を「セキュリティ対策方針」として記述
  - 対策方針を満たすセキュリティ機能をCC part2を用いて記述
  - 評価する詳細さと広さをCC part3を用いて指定

* 独自STにおける評価の4割がST評価に費やされる
  → 要件からではなく機能ありきの開発

認証申請に係る手続き
STの構成

第1章　ST概説
- ST参照
- TOE参照
- TOE概要
- TOE記述

第2章　適合主張
- CC適合主張
- PP主張
- パッケージ主張
- 適合根拠

第3章　セキュリティ課題定義
- 脅威
- 組織のセキュリティ方針（OSP）
- 前提条件

第4章　セキュリティ対策方針
- TOEのセキュリティ対策方針
- 運用環境のセキュリティ対策方針
- セキュリティ対策方針根拠

第5章　拡張コンポーネント定義
- 拡張コンポーネント定義

第6章　セキュリティ要件
- セキュリティ機能要件
- セキュリティ保証要件
- セキュリティ要件根拠

第7章　TOE要約仕様
- TOE要約仕様

認証申請に係る手続き
製品の開発

- ST/PPに基づく製品開発
  - セキュリティ機能要件の外部インタフェースの識別
  - セキュリティ基本設計～詳細設計～実装の対応
  - 開発・構成管理ツールの活用
  - テスト方針や網羅性の提示
  - 開発現場、出荷等のセキュリティ手段実施と記録
  - 製品マニュアルにおけるセキュリティ事項の明確化

    ….

  STに示した機能要件・保証要件を満たすことを確認

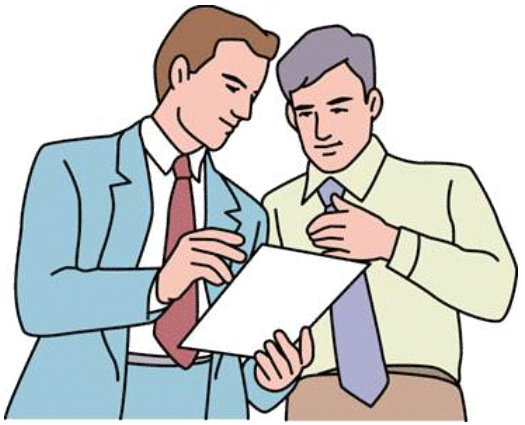
認証申請に係る手続き
評価の依頼

- 評価機関の選定
  - 評価機関へ訪問
    評価対象を評価する設備やツール等の確認
  - 評価者へのインタビュー
    評価対象分野のスキルを専門家とともに確認
  - サービスレベルについて
    認証機関はセキュリティ品質のみに関心

* 基本的には開発者が評価内容を理解し責任を負う

認証申請に係る手続き
評価・認証の実施

- 認証申請
  - 評価用の資料が揃った状態で認証を申請
    （申請後2年以内に評価完了しない場合は取り下げ）
  - 申請時には作成したST/PPとともに書類を提出
- 評価の開始
  - 申請者・評価機関・認証機関でキックオフ実施
  - 評価機関がCCに従い評価
  - 評価過程における指摘事項への対応
- 認証審議委員会
  - 産・学・官の有識者による審議



認証申請に係る手続き
認証取得

❑認証書発行

- IPA及びCCRAのサイトに掲載
- 認証マークのプロモーション使用が可能

JISEC

評価機関承認に係る手続き

- 評価機関の役割・要件
- 認定機関による認定
- 認証機関による承認

評価機関の役割と要件

- 役割
  - 調達者の代わりに対象製品のセキュリティ機能の妥当性、実装の正確性及び脆弱性に関する判定
  - （セキュリティ評価の結果への責任）

- 要件
  - 管理的要件（主に認定機関による認定対象）
    - 文書管理、記録管理、内部監査等ISO/IEC 17025を満たす
  - 技術的要件（主に認証機関による承認対象）
    - 一般的なIT及びITセキュリティに精通
    - 対象製品分野の技術的知見とテストツール
    - 国際的なセキュリティ評価基準(CC)の理解

評価機関の認定

- 認定機関による認定審査
  - NITE(独立行政法人製品評価技術基盤機構)又はCCRA加盟国の定める認定機関によるISO/IEC 17025(JIS Q 17025)に基づく認定審査

* ISO/IEC 17025(JIS Q 17025)
  - 「試験所及び校正機関の能力に関する一般要求事項」
  - 試験所及び校正機関が特定の試験又は校正を実施する能力に関する一般要求事項を規定

評価機関の認定
一般要求事項

1. 管理上の要求事項

- 組織
- マネジメントシステム
- 文書管理
- 依頼、見積仕様書及び契約の内容の確認
- 試験・校正の下請負契約
- サービス及び供給品の購買
- 顧客へのサービス
- 苦情
- 不適合の試験・校正業務の管理
- 改善
- 是正処置
- 予防処置
- 記録の管理
- 内部監査
- マネジメント・レビュー

2. 技術的要求事項

- 一般
- 要員
- 施設及び環境条件
- 試験・校正の方法及び方法の妥当性確認
- 設備
- 測定のトレーサビリティ
- サンプリング
- 試験・校正品目の取扱い
- 試験・校正結果の品質の保証
- 結果の報告

評価機関の認定
NITEによる認定

- 試験事業者(IT)の認定
  - 認定区分：
    情報技術（コモンクライテリア評価・暗号モジュール試験・システムLSI試験）

* 「ASNITE試験事業者IT 認定の一般要求事項」
  - 当該認定区分の事業者の認定及び認定維持に関する要求事項
  - 当該認定区分におけるISO/IEC 17025適用解釈を含む
* 「ASNITE試験所IT 認定の取得と維持のための手引き」
  - 当該認定区分の試験事業者の認定及び認定維持に必要な手続き

評価機関の承認

- 認証機関(JISEC)による承認審査
  - 運営審議委員会での審議
  - 教育訓練プログラムの確認
  - 評価者資格の付与

評価機関の承認
運営審議委員会

評価機関の認定・承認手続きに先立ち、運営審議委員会による制度参入の妥当性を判断

- 事前確認
  - 認定審査に先立ち、認証機関に評価機関として参入希望する旨を通知
  - 参入目的、製品分野、事業情報を提供
- 運営審議委員会での審議
  - 参入の妥当性や必要性を官・学の有識者により事前に判断

評価機関の承認
教育訓練プログラム

評価機関として適切な訓練プログラムを有し、定期的に実施されることを確認

- 確認事項
  - 評価技術に関する教育プログラム
  - 最新のセキュリティ技術情報の共有手段
  - 脆弱性分析、侵入テスト等の訓練状況
  - 対象分野のPP等の教育状況

評価機関の承認
評価者資格

評価者は認証機関との評価業務に係る窓口

評価機関には1名以上の評価者資格保持者を要する

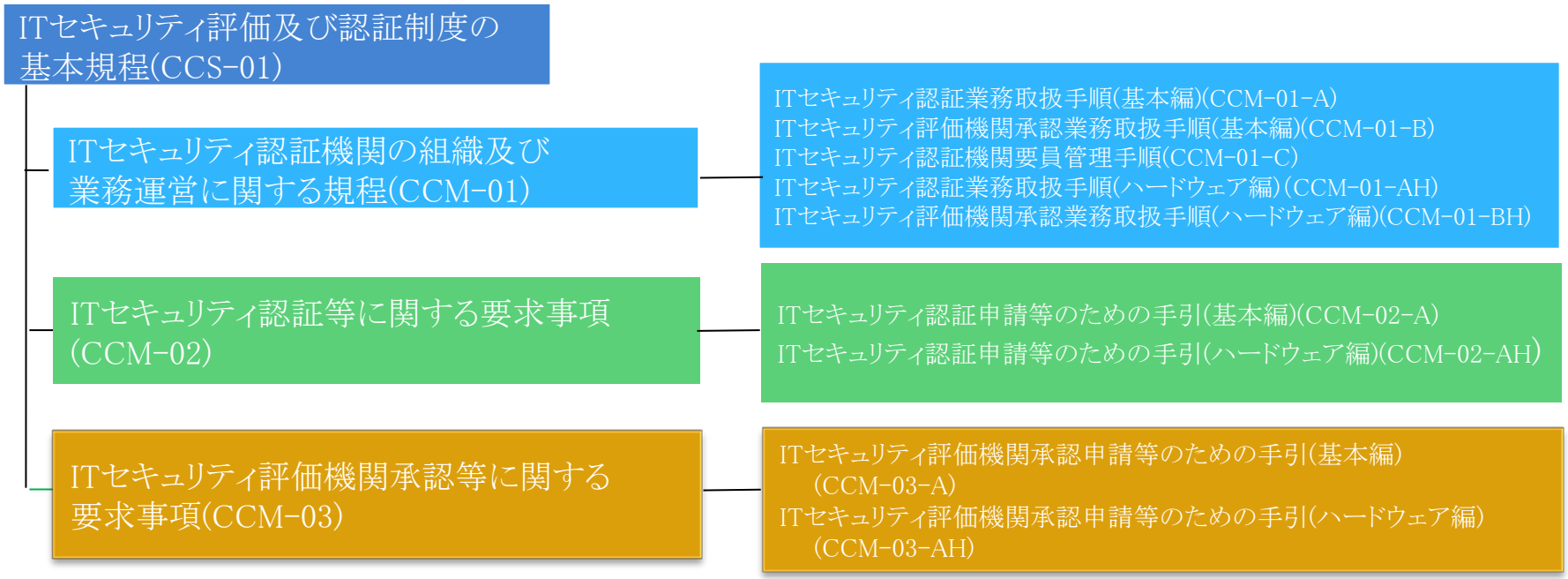
- 評価者要件
  - 情報技術処理の専門知識、脆弱性や侵入テストの経験
  - 制度規程を理解
  - 試行評価において評価ならびに報告書作成が適切に実施できる
  - 公平性・コミュニケーション能力

第4部

制度に関する情報

認証制度に係る手続き

JISCの規程に手続きに関する要求事項と手順を記載



対象者：　制度に係るすべての人　認証機関　申請者　評価機関

制度や規格に関する情報

JISEC Japan Information Technology Security Evaluation and Certification Scheme

JISECポータルサイト
https://www.ipa.go.jp/security/jisec/index.html/

- 一般情報
  - 認証制度概要
  - セキュリティ評価基準(CC/CEM)
  - 国際承認(CCRA)
- 調達者向け情報
  - 認証製品リスト
  - 活用方法
- 申請者・評価者向け情報
  - 申請手続き
  - 規程集
  - 参考資料

調達関連情報

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

政府の情報セキュリティ対策のための統一基準群(平成28年度版)
http://www.nisc.go.jp/active/general/kijun28.html

経済産業省
Ministry of Economy, Trade and Industry

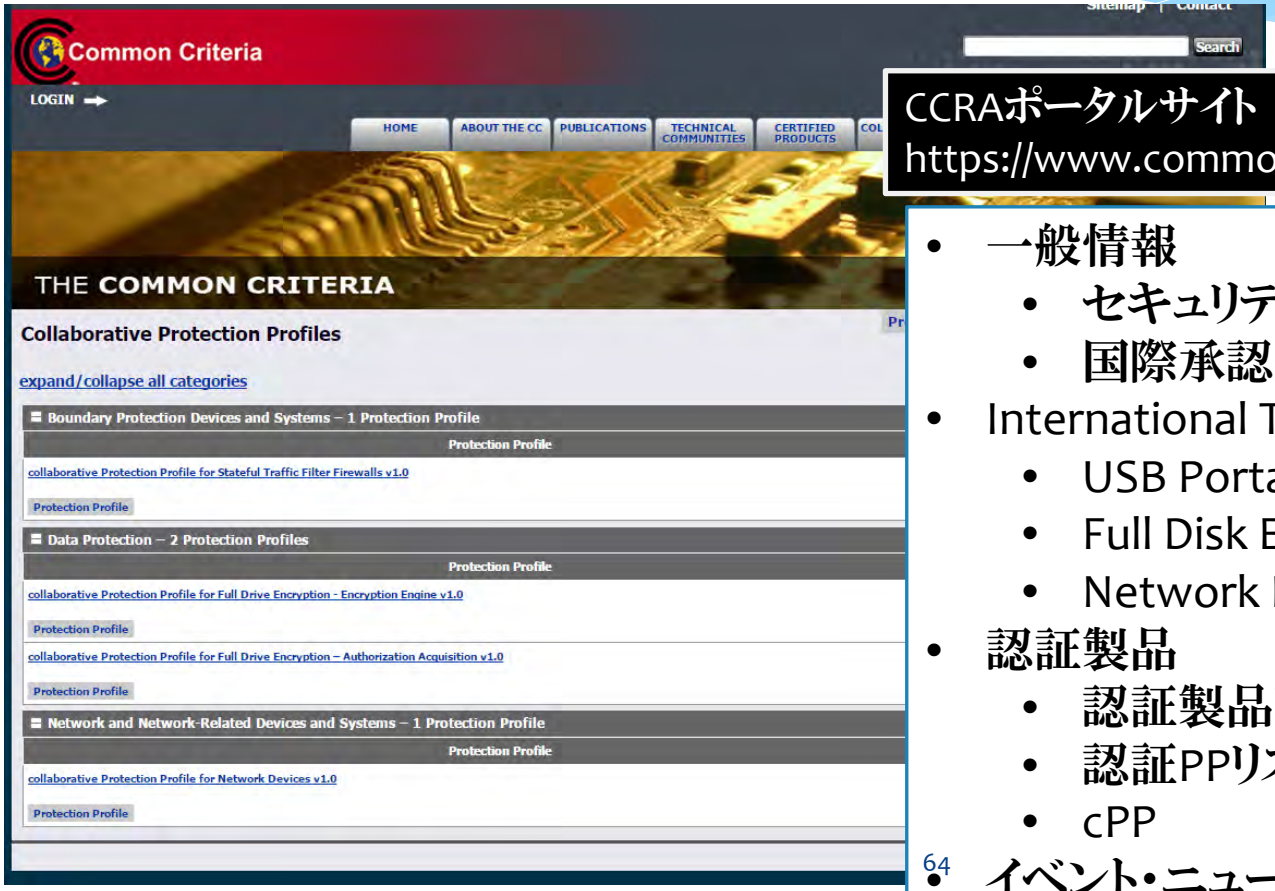
IT 製品の調達 におけるセキュリティ要件リスト
http://www.meti.go.jp/press/2014/05/20140519003/20140519003.html

IPA Better Life with IT

IT 製品の調達 におけるセキュリティ要件リスト活用ガイドブック
https://www.ipa.go.jp/security/it-product/guidebook.html

海外のプロテクションプロファイルの翻訳
https://www.ipa.go.jp/security/publications/pp-jp/index.html

CCRAに関する情報



CCRAポータルサイト
https://www.commoncriteriaportal.org/

- 一般情報
  - セキュリティ評価基準(CC/CEM)
  - 国際承認(CCRA)
- International Technical Community
  - USB Portable Storage
  - Full Disk Encryption
  - Network Fundamentals and Fire Walls
- 認証製品
  - 認証製品リスト
  - 認証PPリスト
  - cPP
- イベント・ニュース

評価機関認定に係る情報

製品評価技術基盤機構認定制度（ASNITE）
http://www.nite.go.jp/iajapan/asnite/

ASNITE試験所IT 等関連文書
http://www.nite.go.jp/iajapan/asnite/documents/

評価機関（ASNITE試験所IT）
- **申請手続き**
- **認定の一般要求事項**
- **認定取得・維持の手引き**