IPA
Information-technology
Promotion
Agency, Japan

ST作成講座

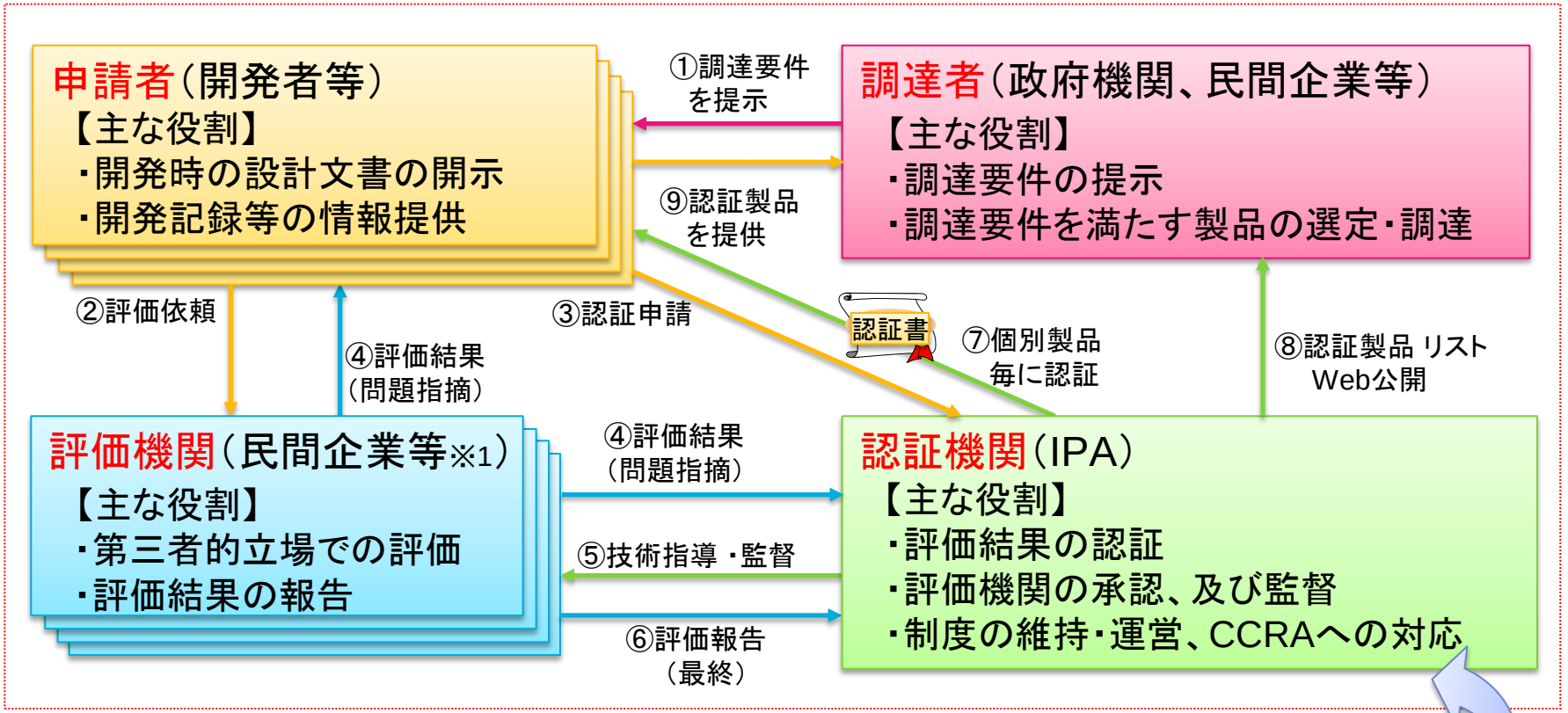
～オープニング～

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
情報セキュリティ認証室

ITセキュリティ
評価・認証制度

ITセキュリティ評価・認証制度

・国際標準ISO/IEC 15408 (CC:Common Criteria、JIS X 5070)に基づいてIT製品(ソフトウェア、ハードウェア)や情報システムを評価・認証する制度
・セキュリティ機能の必要・十分性、及びそれが正しく実装されていることを第三者(評価機関)が客観的に評価

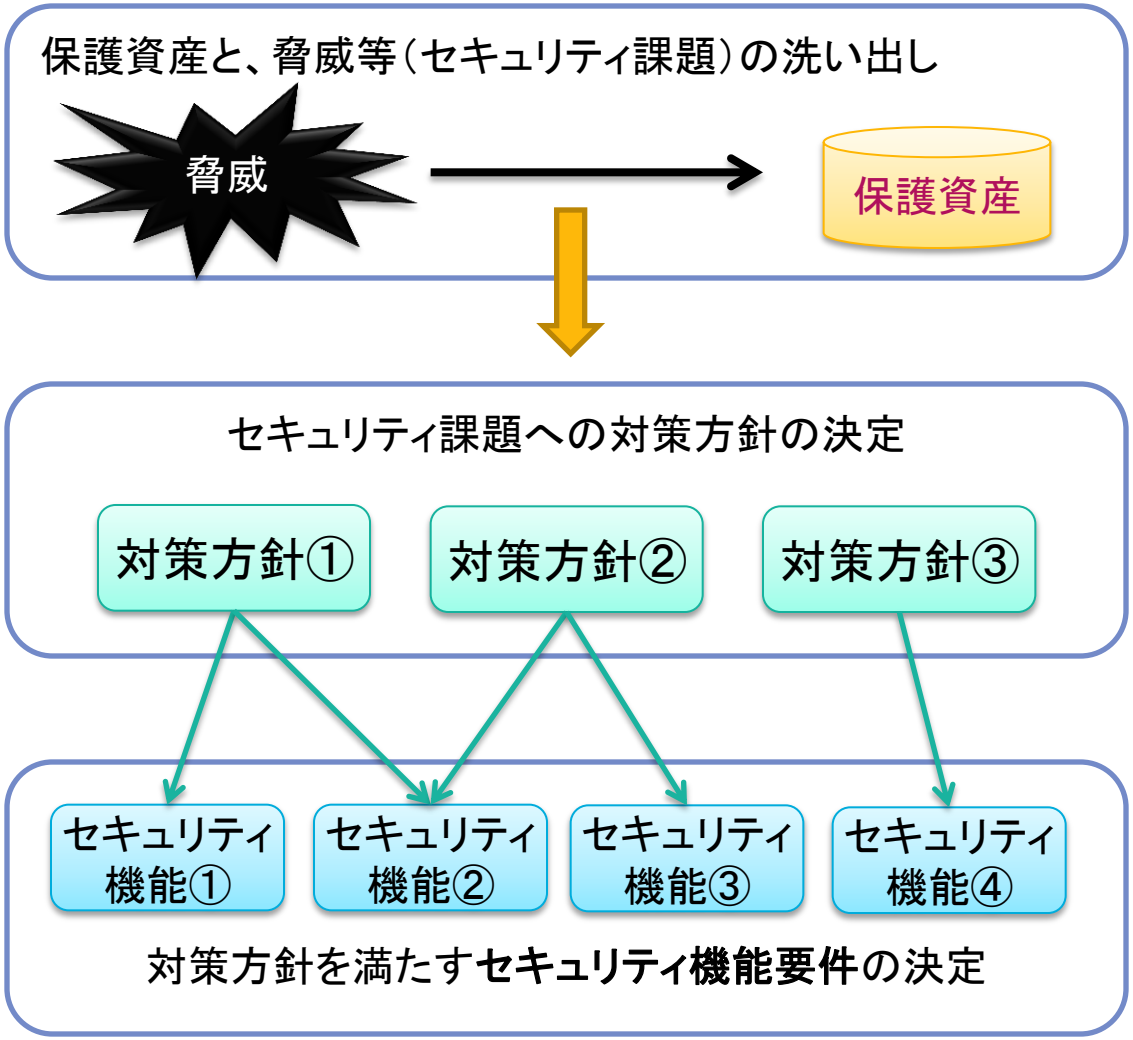


※1: 評価機関 (2012年5月現在、以下の4社)
ITSC :一般社団法人ITセキュリティセンター 評価部
ECSEC:株式会社電子商取引安全技術研究所 評価センター
MHIR :みずほ情報総研株式会社 情報セキュリティ評価室
TÜViT :TÜV Informationstechnik GmbH Evaluation Body for IT-Security

ITセキュリティ評価及び認証制度の運営を監督

経済産業省

セキュリティ機能の必要十分性(適切性)

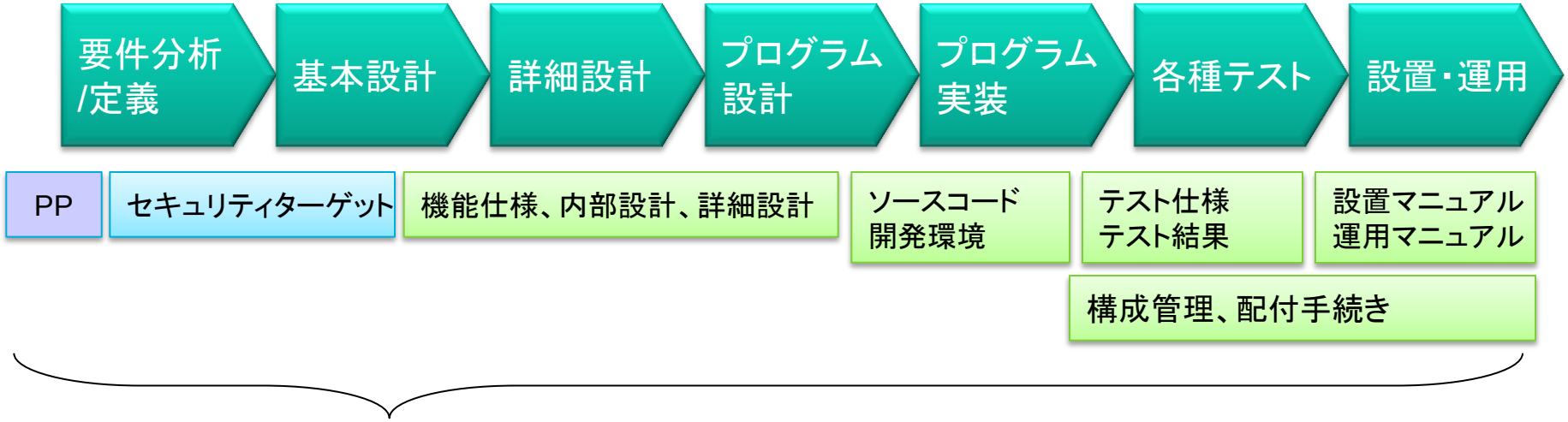


PP：プロテクションプロファイル
（セキュリティ要件定義）

ST：セキュリティターゲット
（セキュリティ設計仕様）

PP/STで論理展開し
セキュリティ機能の
必要十分性を評価
↓
適切性の保証

セキュリティ機能の正確性



セキュリティ機能の正確性を
ライフサイクル全体として保証

→ 脆弱性を生み出さない仕組み作り

定義された機能要件の正確性を
・どの範囲まで評価して保証するのか
・どこまで詳細に調査するのか

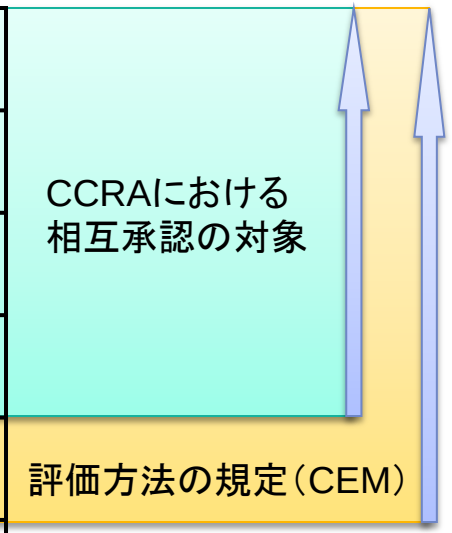
→ 正確性の保証における
厳密さを規定するための指標

EAL：保証レベル
（Evaluation Assurance Level）

セキュリティ保証レベル（EAL）

EAL ： Evaluation Assurance Level

	保証範囲
EAL1	機能仕様（外部I/F）、利用者ガイダンス 等
EAL2	内部設計、配付手続き、開発者テスト、開発資料からの脆弱性分析 等
EAL3	開発現場のセキュリティ、開発者テストの深さ（詳細度）分析 等
EAL4	ソースコード、開発環境（ツール） 等
EAL5	準形式的（フローチャート等の図式を用いた曖昧ではない）設計資料 等
EAL6,7	各国の制度による （軍需品など特別な用途のため）



保証レベルはセキュリティ機能の確かさ（保証の度合い）**を示す。**
保証レベルが高くなるほど確認される範囲（証拠資料）が広くなり、確認される詳細度が深くなる。

CCRA (Common Criteria Recognition Arrangement)

- ITセキュリティ評価・認証制度を運用し、試行認証審査に合格した国（認証書生成国）が発行する認証書を相互に承認する枠組みとして「CCRA」が創設された
  - ➢ 日本で認証された製品は、他の加盟国でも同等に扱う
  - ➢ 海外の認証書生成国で認証された製品は、日本でも同等に扱う

CCRA公式サイト
http://www.commoncriteriaportal.org/

2014年6月現在

政府機関の情報セキュリティ対策のための統一基準

5.2 情報システムのライフサイクルの各段階における対策
5.2.1 情報システムの企画・要件定義

遵守事項

(2) 情報シ

(a) 情報

業務等

下の事

(ア

(イ

(ウ

(b) 情報

のオン

価及び

(c) 情報システムセキ 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。

(d) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

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。

http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf

IT製品の調達におけるセキュリティ要件リスト

製品分野名	デジタル複合機（MFP）

セキュリティ上の脅威	① **他の利用者による不正な操作** 各利用者が複合機を操作するにあたり、取り扱う文書データに適切な保護（データアクセス権、各種操作の制御等）を行うことができなければ、蓄積される文書及び文書関連データの漏えい、情報の改ざんなどが発生する。
	② **通信データの盗聴、改ざん** 複合機を利用（プリント、スキャン等）するために使用するPCやファイルサーバと複合機の間でやりとりされるネットワーク上の通信データが盗聴、改ざんされる可能性がある。
	③ **管理機能への不正なアクセス** 取り扱う文書データに対する設定された規則（セキュリティポリシー）や複合機の利用者情報を管理する機能等に対して、操作できる者を適切に識別認証できない場合には、不正に操作される可能性がある。
	④ **複合機のソフトウェアの改ざん・破損** 複合機のソフトウェアが改ざん・破損された場合、設定されたセキュリティポリシーが適切に実施されない可能性がある。
	⑤ **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。
	⑥ **複合機内に保存された文書データの漏えい（リース終了返却、または廃棄処理時）** プリントやコピー、FAX機能で扱われる文書データは、複合機のHDD/SSD等の記憶媒体に一時的または継続的に保存される場合があり、リース終了返却、または廃棄処理となった複合機から、それらの文書データが漏えいする可能性がある。これらの文書データは、物理的に消去されていない場合、表面的にはアクセスできないようになっていても復元される可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：IEEE Std 2600.1™-2009,Protection Profile for Hardcopy Devices,Operational Environment A Version 1.0 [3] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤, ⑥
[2]：U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009) [4] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤, ⑥

- 製品分野特有の「セキュリティ上の脅威」を列挙
  - ➢ 何が保護資産なのか？
  - ➢ 保護資産に対する脅威は何か？

対象製品分野	製品分野定義
デジタル複合機（MFP）	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
OS(サーバOS に限る)	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（DBMS）	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（IC 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

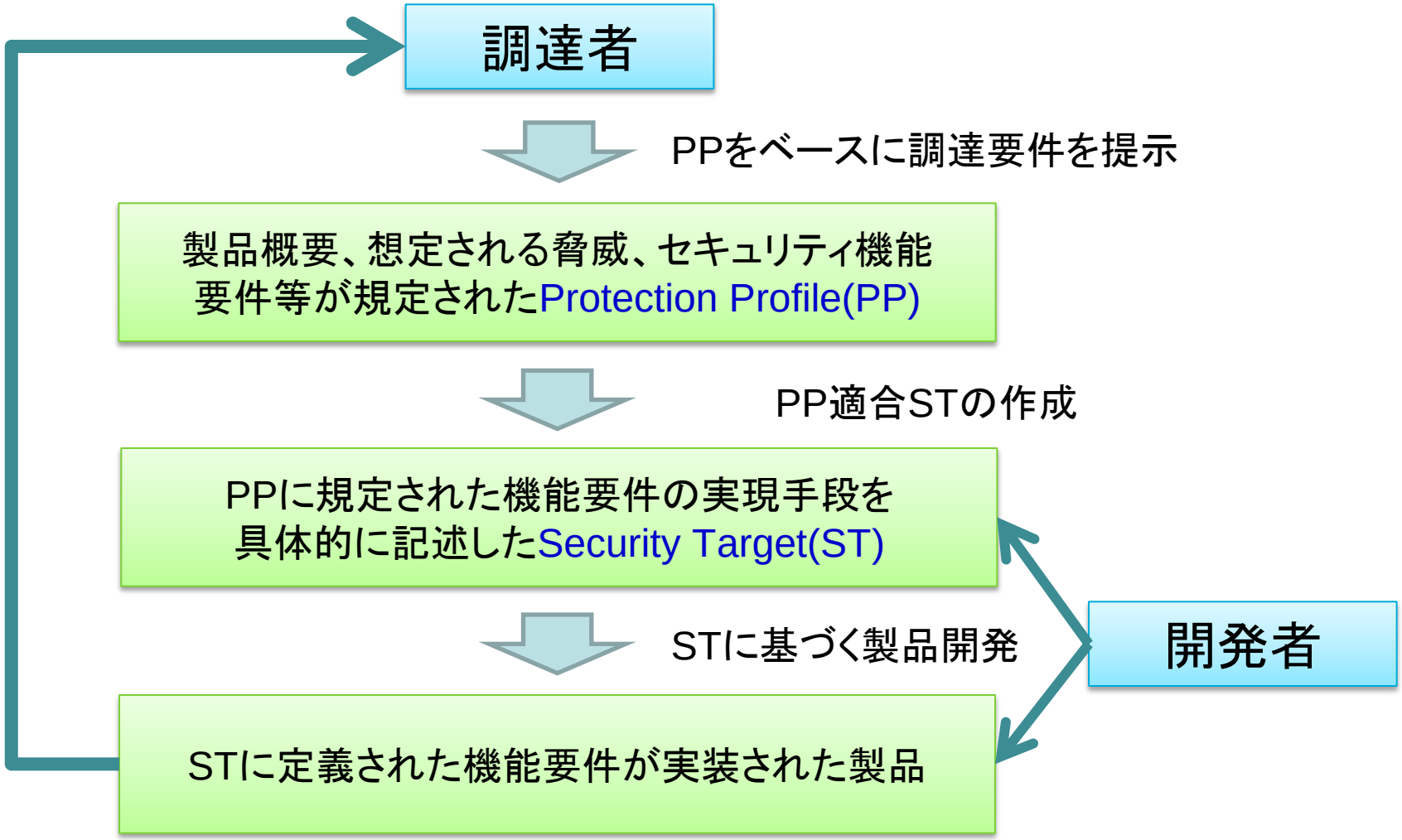
対象候補	製品分野定義
USB メモリ	製品自体に USB コネクタを備えており、別途 USB 接続ケーブル等を用いる必要がない、フラッシュメモリを内蔵した持ち運び可能な記憶装置

- 上記脅威に対抗できる「国際標準に基づくセキュリティ要件」を提示
  - ➢ ISO/IEC15408（Common Criteria)に基づくProtection Profile等の活用

http://www.meti.go.jp/policy/netsecurity/cclistmetisec2014.pdf

Protection Profileを活用した製品調達

要件を満たすセキュアな製品の提供



CCの構成

Common Criteria の構成と概要

- 情報技術セキュリティ評価のためのコモンクライテリア
  - Part.1　概説と一般モデル
    - セキュリティ評価の背景、考え方、開発/評価モデル

    （参考情報）
    - ST（セキュリティターゲット）に書くべき内容、目次
    - PP（プロテクションプロファイル）に書くべき内容、目次
      - ＰＰはＳＴ作成時に参考になるもので、内容はＳＴのサブセット
  - Part.2　セキュリティ機能コンポーネント
    - セキュリティ機能要件集（11分類）
      - セキュリティ機能のカタログ集であり、ST、PP作成時にはここから取捨選択する
      - 監査、暗号、データ保護、識別と認証、など
  - Part.3　セキュリティ保証コンポーネント
    - セキュリティ保証要件集（８分類）
      - セキュリティ機能が正しく実装されていることを確認するための検査項目カタログ集

CEMの概要

- 情報技術セキュリティ評価のための共通方法
  - CC Part.3のセキュリティ保証要件に対する、具体的な評価方法を規定
    - 評価者により評価結果が異ならないように
  - PP、ST、EAL1～EAL5までの保証要件の評価用ガイダンス
  - 評価要件を満足（評価合格）するためには、CEMに規定される「必須」及び「強い要請」について満足しなければならない
    - 必須：「評価者は～しなければならない。（The evaluator shall ～.）」と記述されている。
      - 評価においては、必ず満たさなければならない事項
    - 強い要請：「評価者は～すべきである。（The evaluator should ～.）」と記述されている。
      - 評価において、除外するに積極的な理由があり、それが妥当なものである場合を除き、満たさなければならない事項

CEM：Common Methodology for Information Technology Security Evaluation

CC Part.2の記載例

FAU_GEN.1	**監査データ生成**
	下位階層: なし
	依存性: FPT_STM.1 高信頼タイムスタンプ
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: • 監査機能の起動と終了; • 監査の[選択: ***最小***、***基本***、***詳細***、***指定なし***: から1つのみ選択]レベルのすべての監査対象事象;及び • [割付: ***上記以外の個別に定義した監査対象事象***]。

FIA_AFL.1	**認証失敗時の取り扱い**
	下位階層: なし
	依存性: FIA_UAU.1 認証のタイミング
FIA_AFL.1.1	**TSF** は、[割付: ***認証事象のリスト***]に関して、[選択: ***[割付: 正の整数値]***、***[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値***]回の不成功認証試行が生じたときを検出しなければならない。
FIA_AFL.1.2	不成功の認証試行が定義した回数に達するか上回ったとき、**TSF** は、[割付: ***アクションのリスト***]をしなければならない。

CC Part.3の記載例

11.3	**セキュリティ課題定義(ASE_SPD)**
	目的
180	ST のこの部分は、TOE 及び TOE の運用環境によって対処されるセキュリティ課題を定義する。
181	セキュリティ課題定義の評価は、TOE 及び TOE の運用環境によって対処されることが意図されているセキュリティ課題が明確に定義されていることを実証するために必要である。
ASE_SPD.1	**セキュリティ課題定義**
	依存性:　　なし
	開発者アクションエレメント:
ASE_SPD.1.1D	**開発者は、セキュリティ課題定義を提供しなければならない。**
	内容・提示エレメント:
ASE_SPD.1.1C	**セキュリティ課題定義は、脅威を記述しなければならない。**
ASE_SPD.1.2C	**すべての脅威は、脅威エージェント、資産、及び有害なアクションの観点から記述しなければならない。**
ASE_SPD.1.3C	**セキュリティ課題定義は、OSP を記述しなければならない。**
ASE_SPD.1.4C	**セキュリティ課題定義は、TOE の運用環境についての前提条件を記述しなければならない。**
	評価者アクションエレメント:
ASE_SPD.1.1E	**評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない*。**

CEMの記載例

ADV_FSP.1.1C	***機能仕様は、SFR 実施及びSFR 支援の各 TSFI の目的と使用方法を記述しなければならない。***
ADV_FSP.1-1	評価者は、機能仕様が SFR 支援及び SFR 実施の各 TSFI の目的を記述していることを決定するために、その仕様を***検査しなければならない。***
548	TSFI の目的とは、インタフェースによって提供される機能性を要約する一般的なステートメントである。そこで意図されているのは、インタフェースに関連するアクション及び結果の完全なステートメントではなく、そのインタフェースが何のために使用されるものなのかを読者が大まかに理解できるようにするためのステートメントである。評価者は、目的が存在することだけでなく、そこに TSFI が正確に反映されていることも、パラメタの記述など、インタフェースに関するその他の情報を考慮に入れて決定するべきである。この作業は、このコンポーネントの他のワークユニットと組み合わせて行うことができる。
549	インタフェースを通じて利用可能なアクションが、TOE のセキュリティ方針を実施するうえで何らかの役割を果たしている場合(TSF に課されている SFR のいずれかにたどれるアクションがインタフェースにある場合)、そのインタフェースは *SFR 実施*である。ここで言う方針とは、アクセス制御方針に限定されるものではなく、ST に含まれている SFR のいずれかで特定されるあらゆる機能性を指す。なお、インタフェースには様々なアクション及び結果が含まれている可能性があり、その中には、SFR 実施のものもそれ以外のものもあるので注意する必要がある。