資料38－3－1

IPA Information-technology Promotion Agency, Japan

ITセキュリティ評価及び認証制度

2018年4月27日

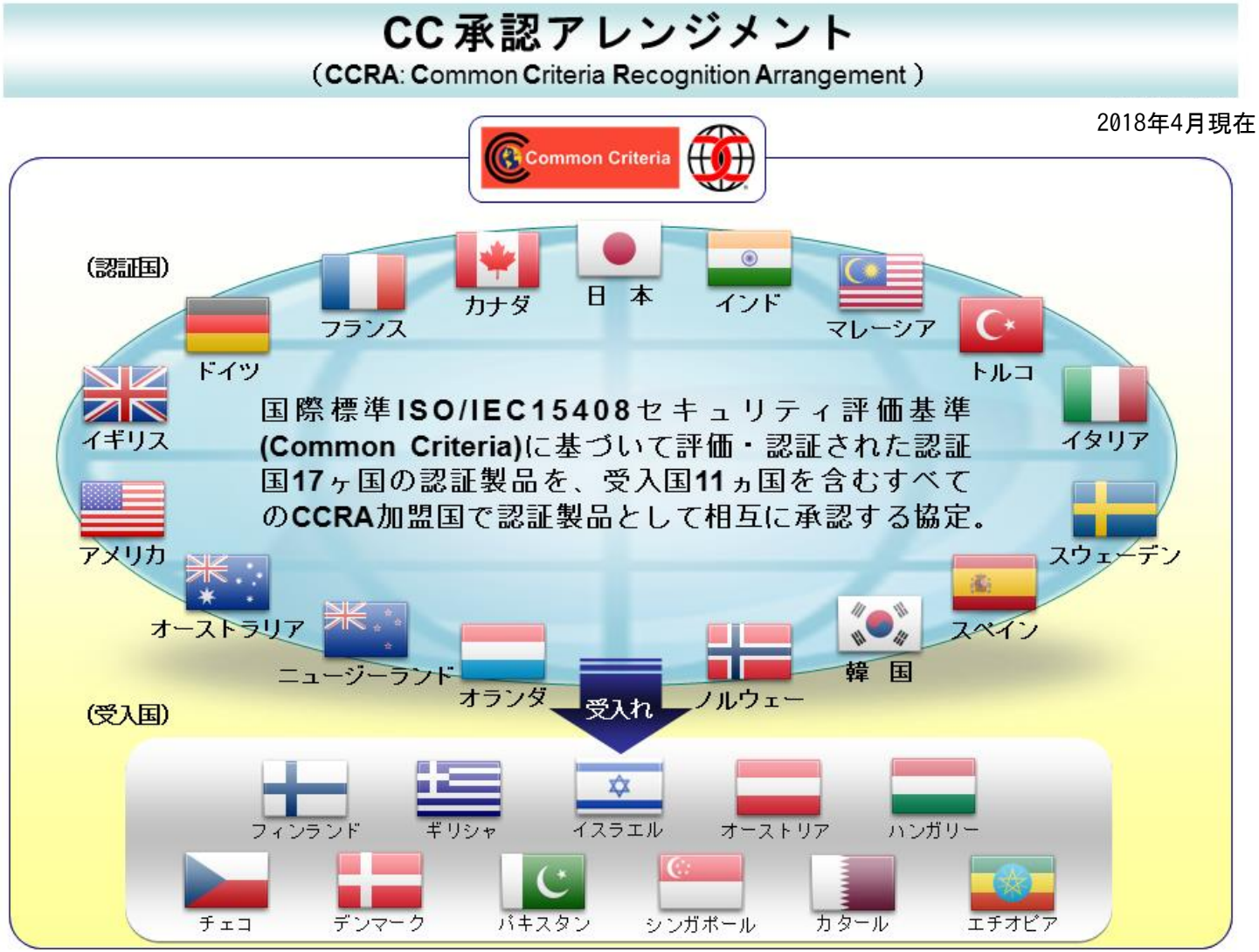
情報処理推進機構
技術本部セキュリティセンター

ITセキュリティ評価及び認証制度（CC認証）

（JISEC : Japan Information Security Evaluation and Certification scheme）

- ISO/IEC 15408（Common Criteria:CC）に基づき、IT製品のセキュリティ機能や品質を技術的な観点から評価し、評価結果を認証する制度
- 経済産業省の監督の下、情報処理推進機構（IPA）が制度を運営

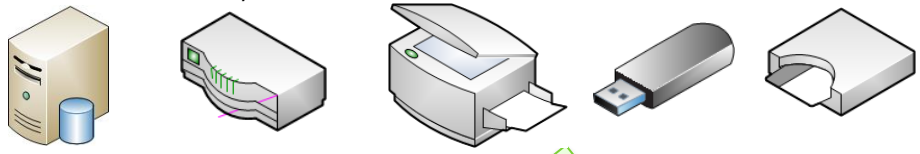
CCRA
(Common Criteria Recognition Arrangement)



JISECにおける評価・認証プロセスの流れ

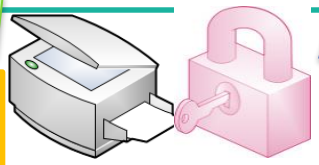
評価したいIT製品

OS、DBMS　FW、IDS/IPS　**デジタル複合機**　USBメモリ　ICカード



IT製品のセキュリティ要件

複合機のセキュリティ要件　FWのセキュリティ要件



評価機関
IT製品のセキュリティ要件に従い
・正しく実装されていることを確認
・セキュリティ機能に脆弱性がないことを確認

ISO/IEC 15408（CC）

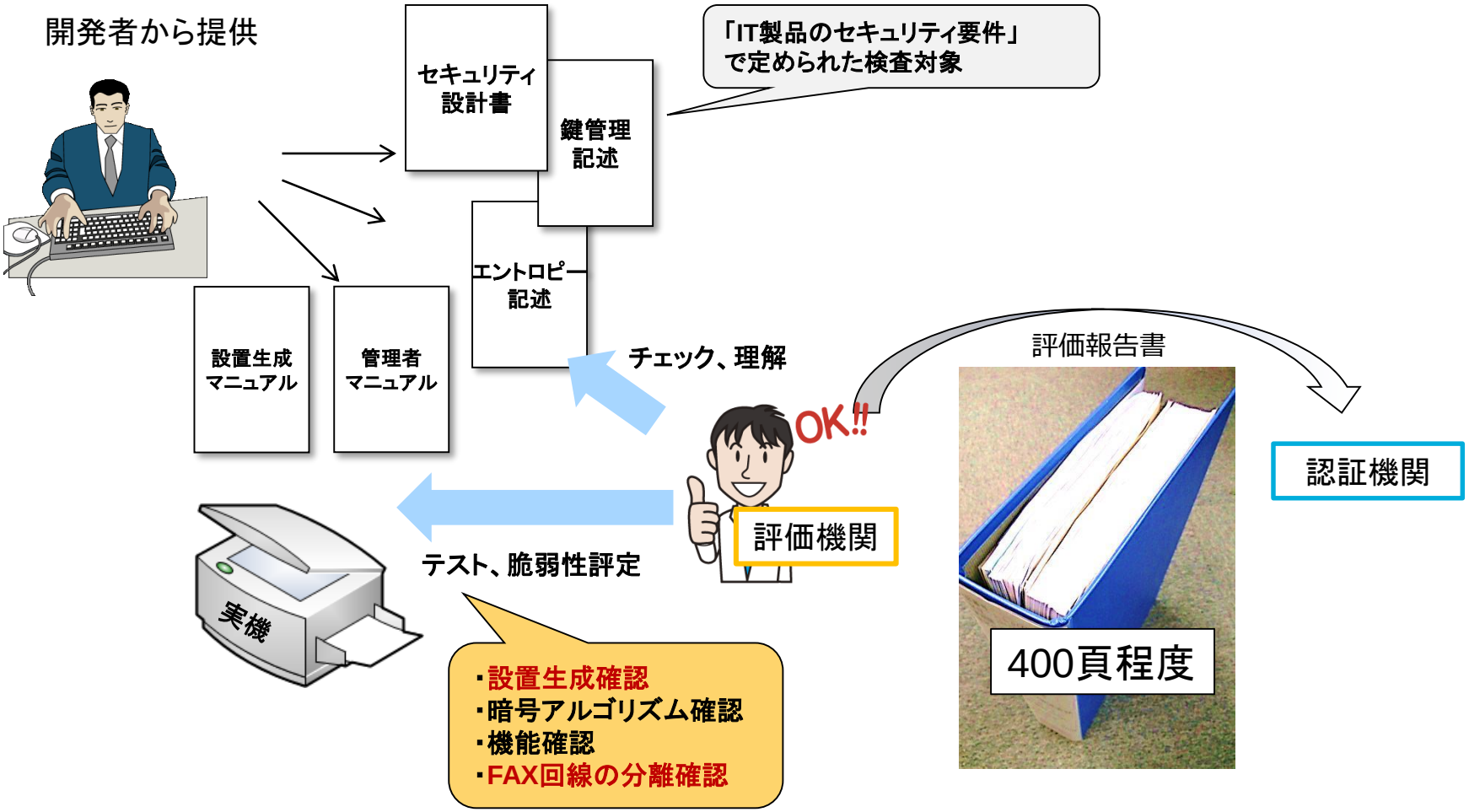
国際標準に定められた、評価方法、手順
- 製品の開発ライフサイクル全体をスコープ
- 証拠資料を基に、専門家が客観的に検査

認証機関　IPA 独立行政法人 情報処理推進機構

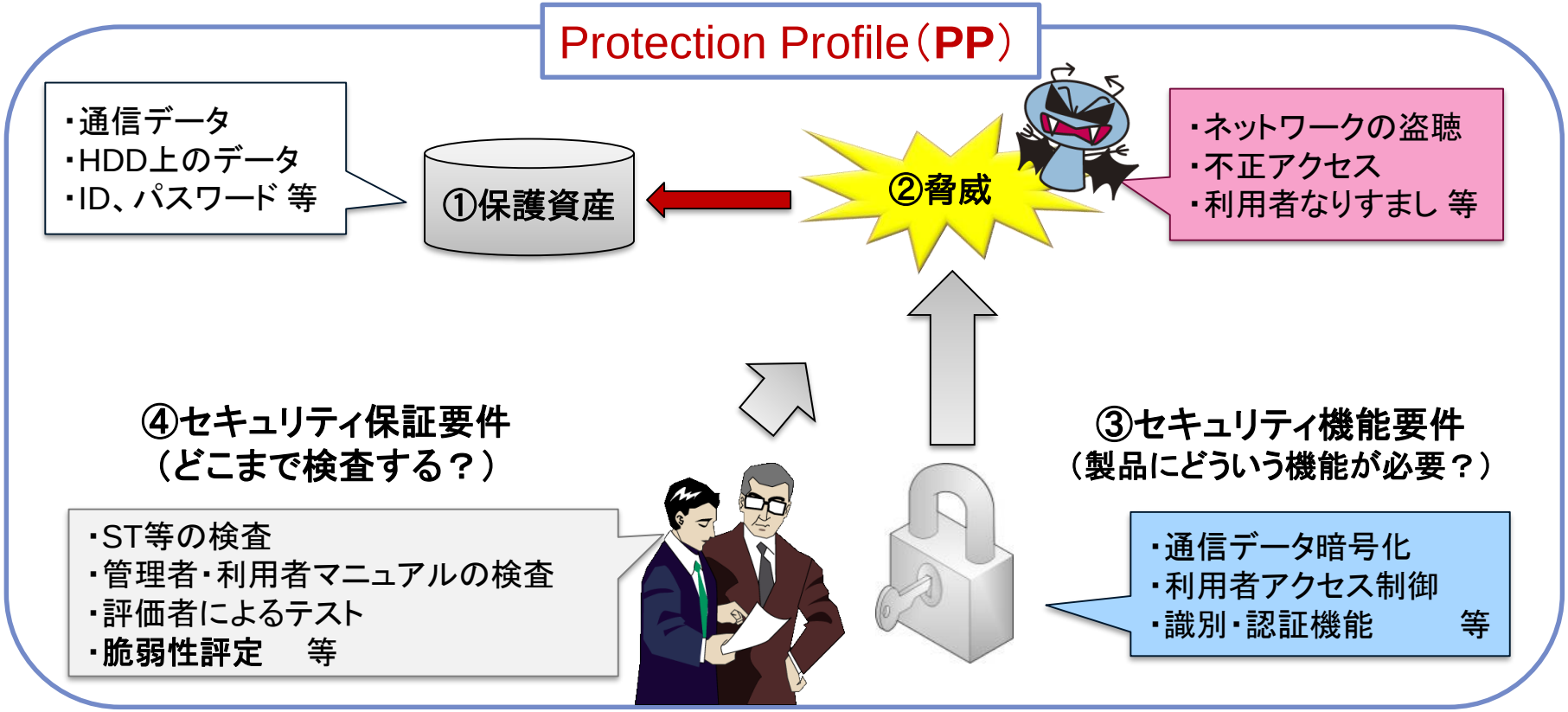
国際的な認証を付与

（調達者は納品検査時に認証取得を確認すればOK）

複合機の評価の例


開発者から提供
セキュリティ設計書
鍵管理記述
エントロピー記述
「IT製品のセキュリティ要件」で定められた検査対象
設置生成マニュアル
管理者マニュアル
チェック、理解
評価報告書
OK!!
評価機関
認証機関
実機
テスト、脆弱性評定
400頁程度
・設置生成確認
・暗号アルゴリズム確認
・機能確認
・FAX回線の分離確認

IT製品のセキュリティ要件
～ Protection Profile（**PP**）～



「①保護資産」、「②保護資産に対する脅威」、「③脅威に対抗するため必要となるセキュリティ機能要件」、「④セキュリティ保証要件」が定義されている。

対象機器
「IT製品の調達におけるセキュリティ要件リスト」第2版

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
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
暗号化USBメモリ	製品自体にUSBコネクタを備えており、フラッシュメモリを内蔵した持ち運び可能な記憶装置に暗号化機能を有する製品
ルータ/レイヤ3スイッチ	OSI基本参照モデル第3層を利用し、情報システム及びネットワークの基盤においてデータを中継する機能を持った通信回線装置
ドライブ全体暗号化システム	ノートPC等のハードディスクドライブ、半導体ドライブなどのデータストレージ全体を暗号化するシステム
モバイル端末管理システム	スマートフォン、タブレット等のモバイル端末を安全に運用・管理するシステム
VPNゲートウェイ	公共ネットワークを利用した、仮想的なプライベートネットワークシステムにおける終端装置

参考：
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) 情報シス

(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。

参考：
セキュリティ要件リスト（デジタル複合機の例）

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、情報の改ざん等が発生する。
	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、又は廃棄処理時） 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又は継続的に保存される場合があり、リース終了返却、又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、暗号化されていない、又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？
  - ➢ 考慮すべき脅威のベースライン

- 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（CC）に基づいたセキュリティ要求仕様