



Information-technology
Promotion
Agency, Japan

セキュリティ要件リストとCCの動向

2014年9月29日

情報処理推進機構

技術本部セキュリティセンター

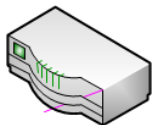
IT製品の利用でセキュリティを考慮すべき場面

IT製品

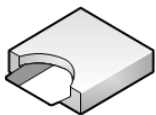
OS、DBMS



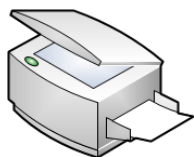
FW、IDS/IPS



ICカード



デジタル複合機



USBメモリ



①-1【製品調達時】
製品に必要な
セキュリティ機能は？
- セキュリティ要件
（要求仕様）の検討



②【運用・保守時】
セキュリティ機能を
正しく動作させる
- 適切な設定値、
パッチの適用

①-2【納品検査時】
要求仕様通りのセキュ
リティ機能が実装され
ていることの確認



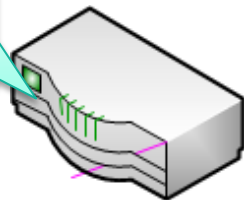
③【更改・廃棄時】
機密情報を抹消した
上で廃棄・リース返却



IT製品毎に適切なセキュリティ機能が必要 ～セキュリティ要件の検討～

製品分野毎に考慮すべき脅威は異なる

管理機能への不正アクセスによるポリシー侵害



FW

IDS/IPS

利用者識別認証機能 等

許可されないリソース・機能への不正アクセス



OS

DBMS

アクセス制御機能 等

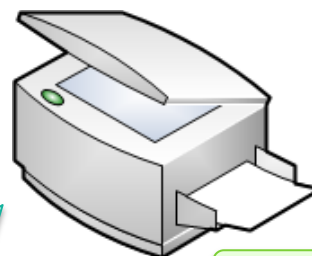
暗号化機能 等

放置・紛失・盗難等による機密情報の漏えい



USBメモリ

リース返却後の文書データの漏えい

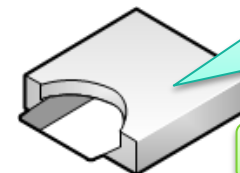


複合機

HDD完全消去機能 等

耐タンパ機能 等

ICチップへの攻撃(不正なデータ読み出し)



ICカード

政府機関の情報セキュリティ対策のための 統一管理基準群(平成24年度版)

1.5.1.1 情報システムのセキュリティ要件

遵守事項

(1) 情報システムの計画

(d) 情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器及びソフトウェアについて、IT セキュリティ評価及び認証制度に基づく認証取得製品を調達する必要性については、「IT セキュリティ評価及び認証制度に基づく認証取得製品分野リスト」を参照し、必要があると認めた場合には、当該製品の分野において要求するセキュリティ機能を満たす採用候補製品が複数あり、その中に要求する評価保証レベルに合致する当該認証を取得している製品がある場合において、**当該製品を情報システムの構成要素として選択すること。**

「IT セキュリティ評価及び認証制度等に基づく 認証取得製品分野リスト」の問題点

製品分野名	デジタル複合機 (MFP)	不正侵入検知/防止システム (IDS/IPS)	データベース管理システム (DBMS)
製品分野定義	プリンタ機能を標準で有しスキャナ、FAX、コピーのいずれか2つ以上の機能を標準で装備している製品	ネットワークやシステムの稼働状況を監視し、組織内のコンピュータネットワークへの外部からの侵入を報告、防御する製品	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
利用用途	保護すべき重要度の高い情報の複写やデジタルデータ化、送信等に利用される	ネットワーク上の通信を監視するなどにより、インターネットからの不正アクセスを検知し防止する	国民の個人情報等保護すべき重要度の高い情報をデータベースとして保管するために利用される (サーバOS 環境下で稼働するものに限り)
準拠すべき規格・制度	ISO/IEC15408 (Common Criteria)	ISO/IEC15408 (Common Criteria)	ISO/IEC15408 (Common Criteria)
一般的に必要なセキュリティ機能	セキュリティ監査、送受信の否認不可、暗号化サポート機能、アクセス制御、データ認証、送出データ保護、情報フロー制御、入力データ保護、内部転送データ保護、残存情報保護、ロールバック、蓄積データ完全性、転送データ機密性、転送データ完全性、識別・認証、セキュリティ管理、プライバシー保護、セキュリティ機能保護、資源利用管理、TOE アクセス制御、高信頼パス/チャネルの各セキュリティ機能について、調達者のニーズに応じて選択。個別製品ごとにどのセキュリティ機能が認証されているかについては、IPA ポータルサイトを参照。		
参照 PP	2600.X, Protection Profile for Hardcopy Devices Controlled Access System - System for Basic Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/PPes/pp_hcd_br_v1.0.pdf)	U. S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments (http://www.commoncriteriaportal.org/files/ppfiles/pp_ids_sys_br_v1.7.pdf)	U.S. Government PP for Database Management Systems (http://www.commoncriteriaportal.org/files/ppfiles/PPDBMS-BR_V1.1-PP.pdf)
標準 EAL	EAL3 以上	EAL3 以上	EAL2 以上

【一般的に必要なセキュリティ機能】

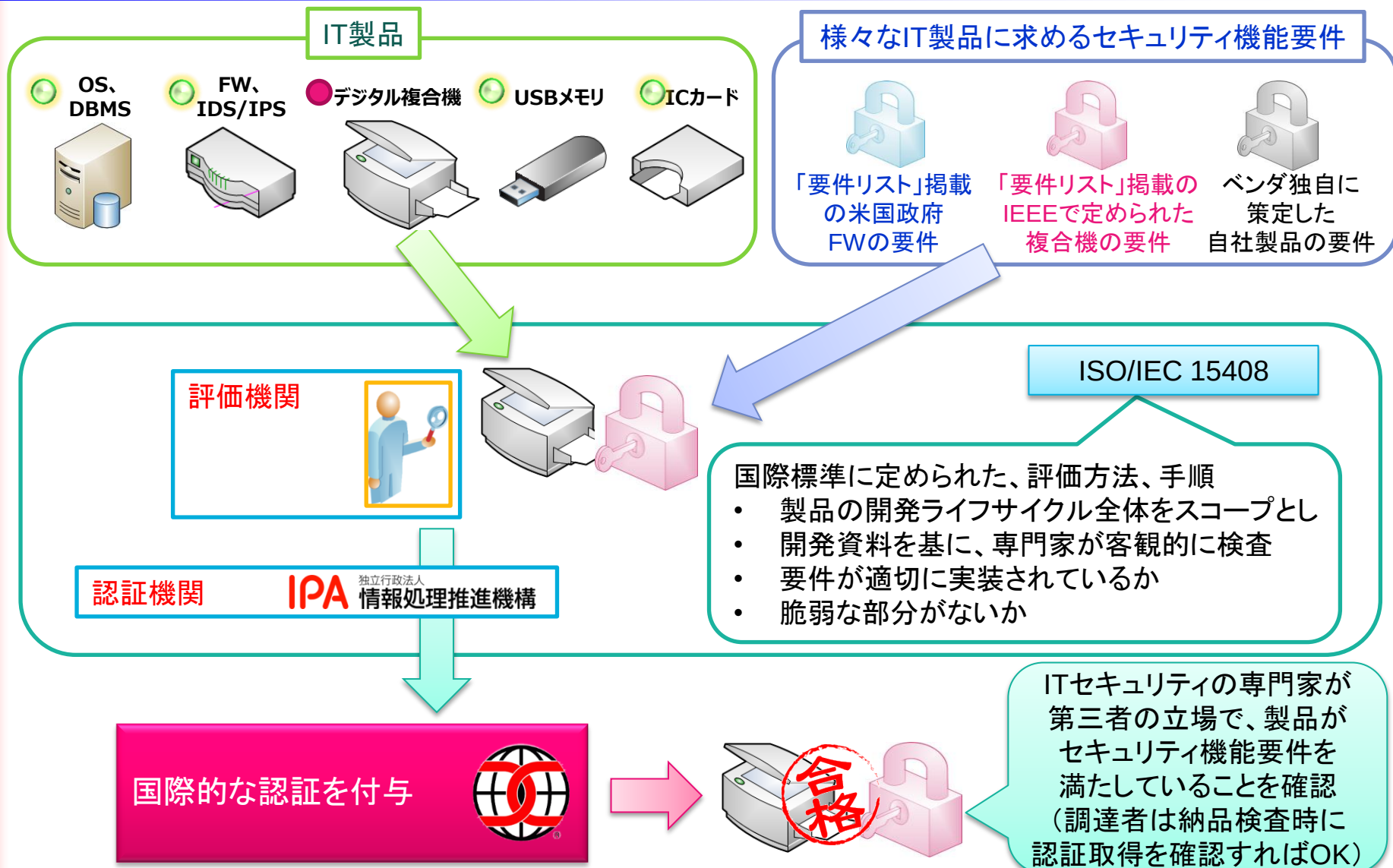
脅威分析⇒セキュリティ要件の策定は調達者におまかせ

とにかくISO/IEC15408 (Common Criteria)の認証取得製品を調達することを求める



部分的な脅威にだけ対抗できる【認証取得製品】の方が、幅広い脅威に対抗できる【認証未取得製品】よりも優先的に調達されてしまう可能性も...

ISO/IEC15408 (Common Criteria) の概要 ～ITセキュリティ評価及び認証制度 (JISEC)～



ISO/IEC15408 (Common Criteria) の概要 ～ITセキュリティ評価及び認証制度 (JISEC)～

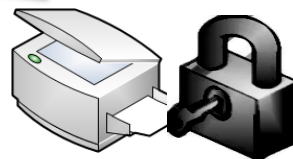
IT製品



様々なIT製品に求めるセキュリティ機能要件



評価機関



ISO/IEC 15408

・製品の一部の機能しか要件化 していない。
例えば、HDD完全消去機能だけを要件化。
(実際には、識別認証機能、アクセス制御機能、暗号化機能等を実装しているにも関わらず。)

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



一部の機能しか
セキュリティ評価
されていない製品でも、
認証は付与される。

平成24年度版統一基準での 「製品分野リスト」活用のロジック

認証取得製品分野リストを参照し

必要があると
認めた場合

機能を満たす候補製品が

複数存在

要求する評価保証レベルに

合致する認証
を取得してい
る製品がある

当該製品を

構成要素とし
て選択する

製品分野リスト

- ・ 認証製品が複数ある6分野について一般的なセキュリティ機能を羅列
- ・ 製品分野毎の脅威分析⇒セキュリティ要件の策定は調達者に丸投げ
- ・ 参考程度に国際標準に基づくセキュリティ要件(**PP: Protection Profile**)を提示

問題点

- ①リストを参照し「必要があると認めた場合」の判断基準が不明確
- ②リストの使い方が不明確(脅威分析⇒セキュリティ要件に役立たない)
- ③国際標準に基づくセキュリティ要件(**Protection Profile**)の必要性が不明確

政府機関の情報セキュリティ対策のための 統一基準群(平成26年度版)

5.2.1 情報システムの企画・要件定義

遵守事項

(2) 情報システムの
セキュリティ要件の
策定

(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。**

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

平成26年度版統一基準での 「セキュリティ要件リスト」活用のロジック

セキュリティ要件リストを参照し

該当する分野
の製品である
場合

~~機能を満たす候補製品が~~

~~複数存在~~

~~要求する評価保証レベルに~~

~~合致する認証
を取得してい
る製品がある~~

記載の脅威が

存在する場合
には対抗する

要件リスト

- ・ 製品分野毎に対抗すべき脅威を提示
- ・ 脅威に対抗できる国際標準に基づくセキュリティ要件(Protection Profile)を選択肢の1つとして推奨
- ・ 随時分野を拡大していく

問題点の解消

- ① リストを参照し「必要があると認めた場合」の判断基準が不明確
⇒ 脅威が存在する場合
- ② リストの使い方が不明確
⇒ 脅威分析に活用可能
- ③ 国際標準に基づくセキュリティ要件(Protection Profile)の必要性が不明確
⇒ 脅威に対抗するためのセキュリティ要件

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・破壊 複合機のソフトウェアが改ざん・破壊された場合、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。



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

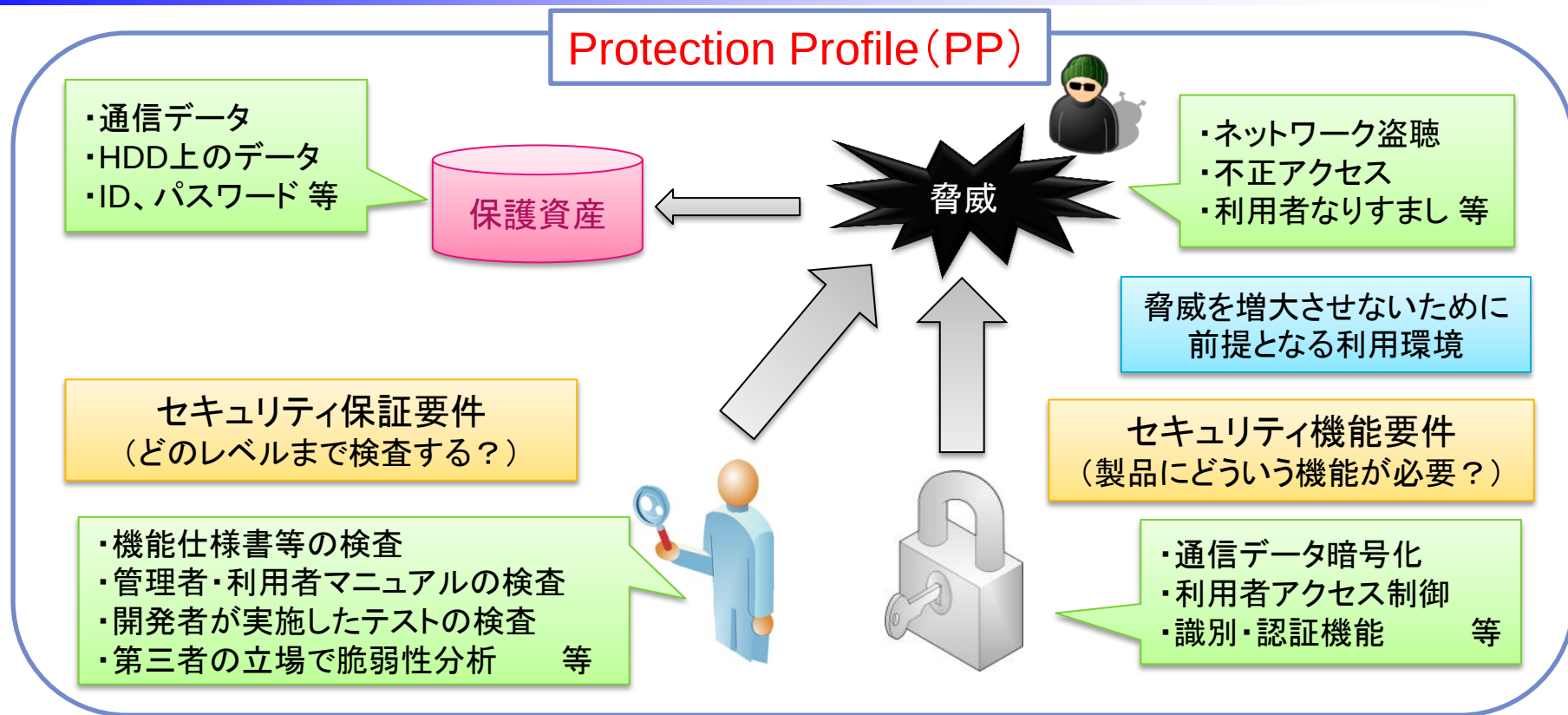
- ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様（**Protection Profile**）
- ISO/IEC19790(暗号モジュール対するセキュリティ要求事項)も活用



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

国際標準に基づくセキュリティ要件

～ ISO/IEC15408におけるProtection Profile～



- 製品分野毎に、「保護資産」、「保護資産に対する脅威」、「脅威に対抗するため必要となるセキュリティ機能要件」、「第三者が検査すべき項目(セキュリティ保証要件)」等が、専門家により定義・策定されている。

政府機関の情報セキュリティ対策のための 統一基準群(平成26年度版)

5.2.1 情報システムの企画・要件定義

遵守事項

(2) 情報システムのセキュリティ要件の策定

(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。**

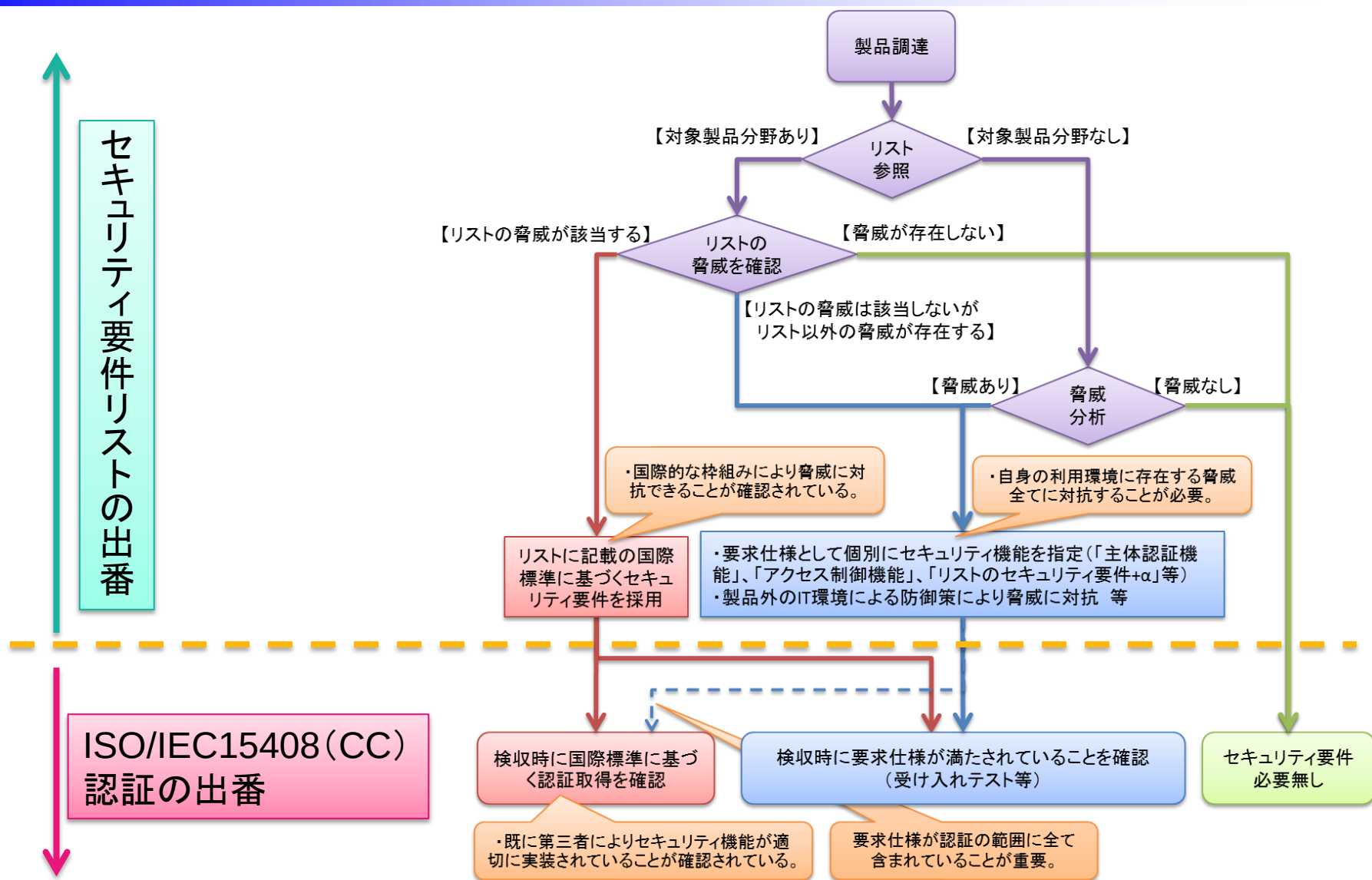
5.2.2 情報システムの調達・構築

遵守事項

(3) 納品検査時の対策

(a) 情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。

セキュアなIT製品を調達するためのフロー



国際的な認証制度

～世界各国で認証された製品が調達対象～

CCRA (Common Criteria Recognition Arrangement)

- ISO/IEC15408を利用する国際的な枠組み(CCRA)に加盟しているのは26カ国
 - ある国で評価・認証された製品は、他の加盟国でも相互に通用
 - 海外を含む様々なベンダから調達可能
 - 欧米諸国の政府調達要件に広く活用



2014年8月現在

CCRA現行制度における課題

- CCRA加盟国毎に、各種IT製品（例：Firewall、OS、DBMS等）において、各国独自の「セキュリティ要件（PP: Protection Profile）」を作成し、調達要件としているケースが多い
 - ベンダは、各国の調達要件となっているPP毎に評価認証を受ける（例えば、A国のPP、B国のPP、C国のPPで別々に認証を取得）
 - 相互承認のメリットが半減
 - 評価認証費用は製品の価格にも影響（調達側・供給側とも不利益）

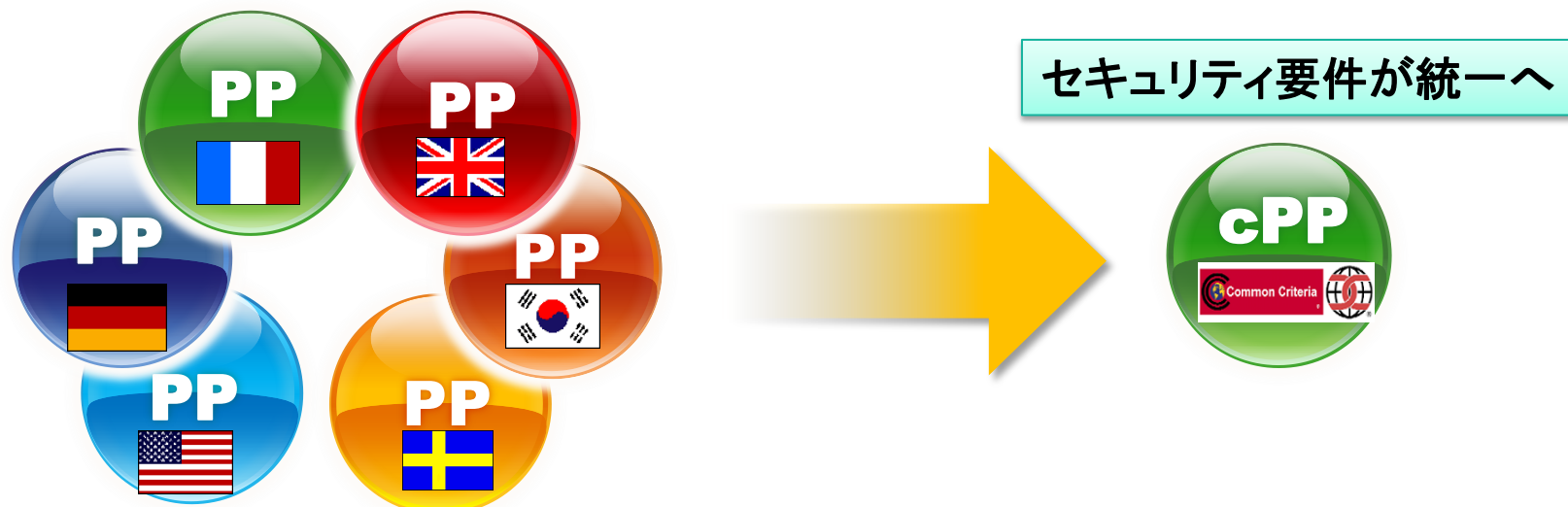


各国がバラバラなセキュリティ要件で調達



世界共通のセキュリティ要件(cPP)へ

- 共通化されたベースラインとなるセキュリティ要件
 - cPP (Collaborative Protection Profile)
CCRA加盟国が共同で作成する政府調達のための世界共通のセキュリティ要件
- cPPのコンセプト
 - 今までのPPでは過剰な評価内容になっていたものも存在していた
 - 必要最小限の評価でコスト削減、認証取得までの時間短縮
 - ただしテスト方法を具体的に記載することで評価品質確保

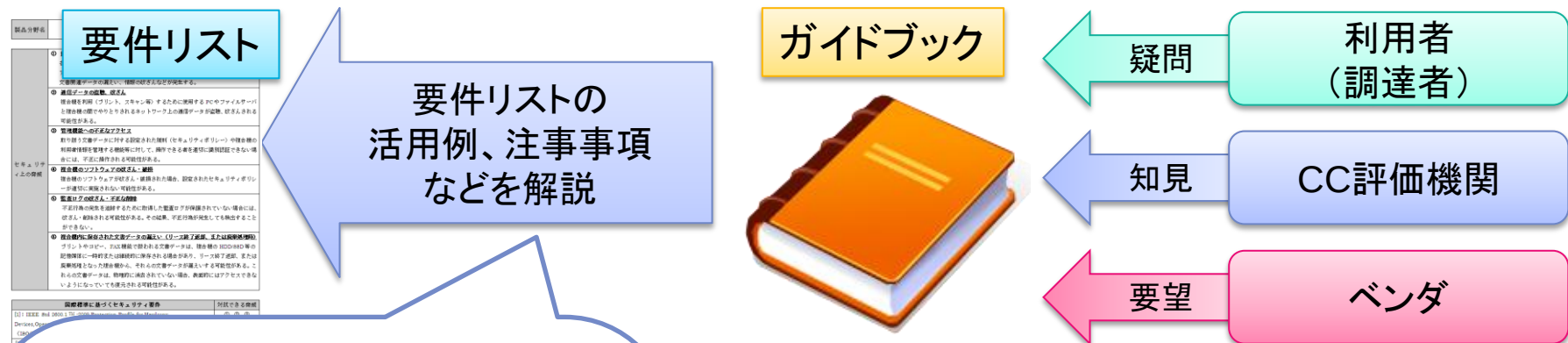


CCRAの新たなアレンジメントが発行(9/8)

・【経産省・ニュースリリース】<http://www.meti.go.jp/press/2014/09/20140910001/20140910001.html>

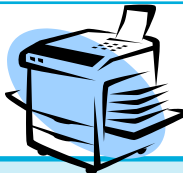
・【IPA・プレスリリース】<http://www.ipa.go.jp/about/press/20140910.html>

セキュリティ要件リスト活用ガイドブック

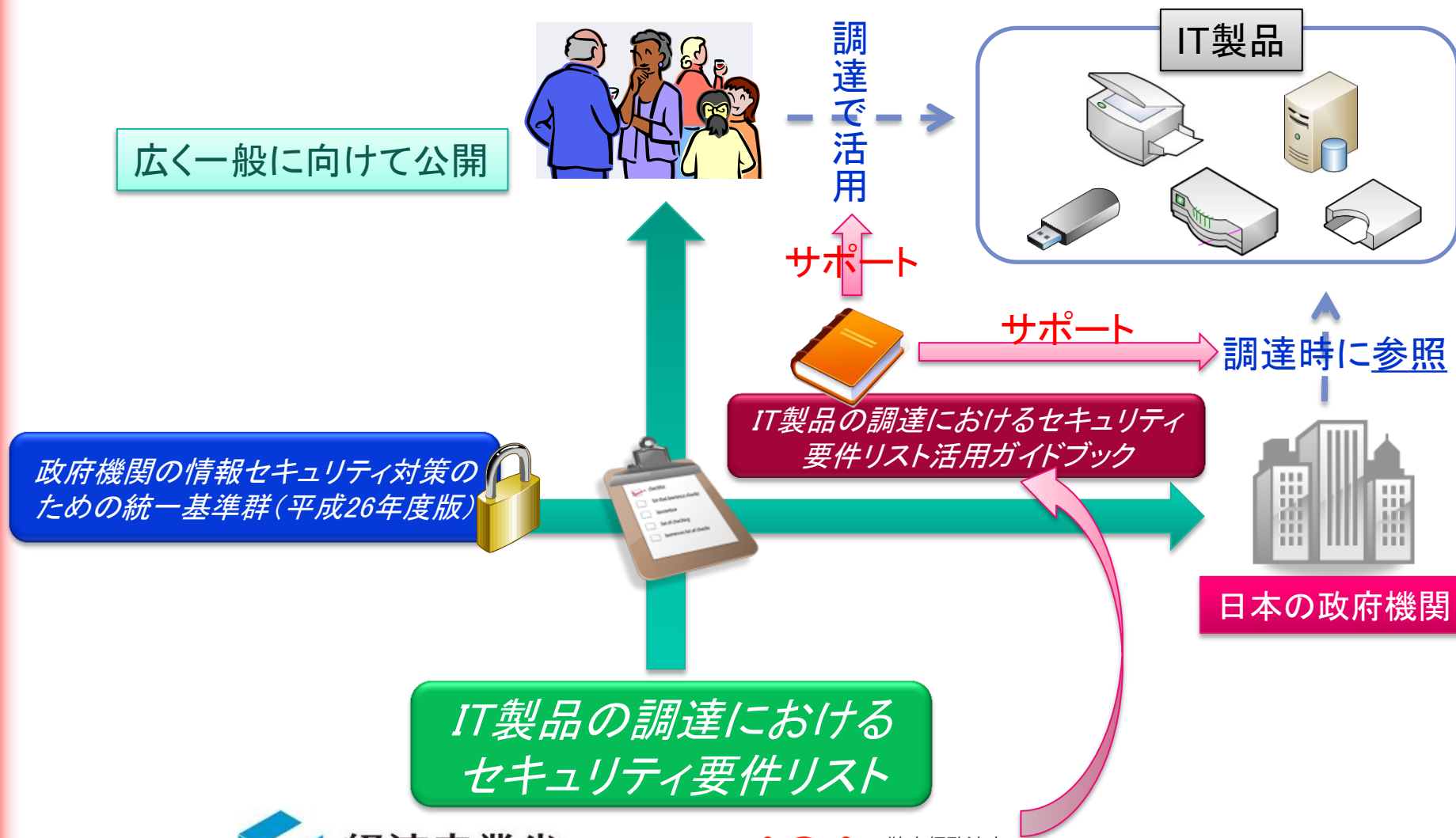


- 想定される事情への対処
 - 要件リストに提示されているものより厳しい要件が必要な場合
- 認証取得製品の調達
 - 認証取得見込み(セキュリティ評価中)製品を調達する場合
- 製品分野に特有な、注意事項
 - 分野に該当するかどうかの判断、該当しない場合の考え方
 - ベンダ独自のセキュリティ要件でのISO/IEC15408認証製品の活用
- 調達時、運用時の注意点
 - 単体調達ではない場合の仕様記述
 - 設置環境や、パッチの適用等

例えば:複合機のモデル毎の活用例・注意点

		
オフィス向け大型機	SOHO向け小型機	インクジェットプリンタ
ISO/IEC15408 認証取得製品 多数	ISO/IEC15408 認証取得製品 少数	ISO/IEC15408 認証取得製品 皆無
要件リストをそのまま活用可能。 (ISO/IEC15408認証製品の活用を推奨)	脅威分析に要件リストを活用可能。	要件リストの活用は困難なため、別途調達時の注意事項を解説。

「セキュリティ要件リスト」「統一基準」 「活用ガイドブック」の関係



対象とする製品分野を拡充していきます

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



まずは6つの
製品分野を対象
(今後拡充予定)

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



セキュリティへの需要がありつつも、市場に要件を満たす製品、ISO/IEC15408認証取得製品が揃っていない分野は「対象候補」と位置付け。
状況を検討し、「対象製品分野」に移行していく。
(今後拡充予定)