ISO/IEC 15408とは

2003年2月28日

情報処理振興事業協会(IPA)　セキュリティセンター
評価認証グループ　　久田　俊哉

目　次

◆*ISO/IEC 15408とは*

◆ISO/IEC 15408の内容

ISO/IEC 15408が解決しようとする課題

ユーザ

機能が豊富そうだから、導入してみたけど・・・

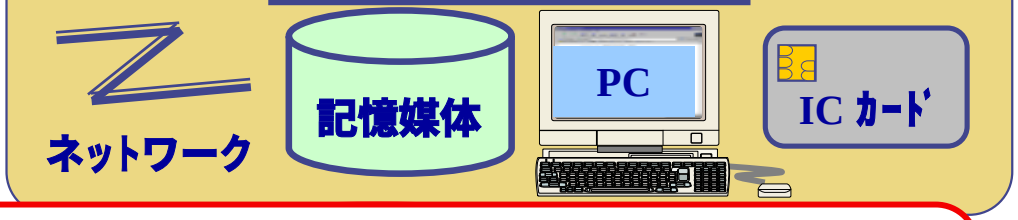
「肝心な機能が無かった」

「もっと安い製品でも十分だった」

客観的な判断基準

ISO/IEC 15408

IT製品・システム



セキュリティ機能の提供

個別技術がクローズアップされがち

セキュリティ機能
暗号化
認証。。。

開発者

IPA

ISO/IEC 15408の考え方(1)

◆セキュリティ設計を、体系的、網羅的に実施

➢セキュリティターゲット(ST：Security Target)の作成

✧ セキュリティ設計仕様書

✧ 開発者が、開発に先立ち、作成

✧ 使用環境想定 -> 脅威分析 -> 対策 -> セキュリティ機能

✧ 機能は、規格に定義された網羅的な機能カタログ集から選択

セキュリティ機能の必要性が順を追って示される
標準化された共通の言葉

✧ ユーザは、これを読むことにより、セキュリティ機能を把握できる

➢セキュリティターゲットをブレークダウンする形で、設計、実装

✧ セキュリティターゲット -> 概要設計書 -> 詳細設計書 -> プログラム

ISO/IEC 15408の考え方(2)

- ◆セキュリティターゲットの内容、及び、それが正しく実装されていることを第三者が客観的に評価
  - ➢開発、製造、運用に関わる資料を検査
    - ✧ セキュリティターゲット、各種設計書、ソースコード、オブジェクトコード、テスト仕様書、マニュアル など
  - ➢評価保証レベル ー EAL(Evaluation Assurance Level)
    - ✧ 検査対象物の範囲、検査の程度(セキュリティ強度を示すものではない)
    - ✧ より広く、より深く検査したから、より大丈夫(大きな保証)

ISO/IEC 15408の歴史

日本では最近だが、欧米では10数年前から(軍用、政府調達主体)

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

*CC*と呼ぶことが規格で認められている。

IPA

セキュリティ評価・認証済み製品件数

	TCSEC	ITSEC	CC	合計(年)
1990以前	20	1		21
91	4	0		4
92	6	1		7
93	5	7		12
94	19	25		44
95	11	17		28
96	4	18		22
97	7	28	1	36
98	5	32	3	40
99	2	41	14	57
2000	3	31	31	65
01	0	34	26	60
02	0	17	44	61
評価中	0	9	68	77
合計	86	261	187	534

基本方針：CCへ移行

米国：移行済み　欧州：移行中

＊CCRA加盟国の認証機関が公開しているリストより集計（2002年11月現在）。

◆ISO/IEC 15408とは

◆***ISO/IEC 15408の内容***

ISO/IEC 15408の構成

◆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
- ➢セキュリティターゲット(ST：Security Target)に書くべき内容、目次
- ➢プロテクションプロファイル(PP：Protection Profile)に書くべき内容、目次

◆Part 2 セキュリティ機能要件

- ➢セキュリティ機能要件集(11分類)
  - ✧セキュリティ機能カタログ集 (監査、通信、暗号、データ保護、認証、・・・)
  - ✧ST、PPでは、ここから取捨選択

◆Part 3 セキュリティ保証要件

- ➢セキュリティ保証要件集(10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
  - ✧通常、EALの形で使われる
- ➢評価保証レベル ー EAL(Evaluation Assurance Level)
  - ✧保証要件のセット(EAL1～EAL7の7段階)
  - ✧検査対象物の範囲、検査の程度(セキュリティ強度を示すものではない)
  - ✧より広く、より深く検査したから、より大丈夫(大きな保証)

IPA

セキュリティターゲット(ST)とプロテクションプロファイル(PP) (1)

◆セキュリティターゲット(ST)

- ➢個々の製品･システム毎に、開発者が作成
- ➢セキュリティ設計仕様書

◆プロテクションプロファイル(PP)

- ➢製品･システムのカテゴリ毎に、業界団体やユーザが作成
  - カテゴリの例：OS、DBMS、ICカード、PKI
- ➢セキュリティ要求仕様書
- ➢内容は、セキュリティターゲット(ST)のサブセット

◆PPに個々の製品固有の記述を追加することで、STを作成できる

IPA

セキュリティターゲット(ST)とプロテクションプロファイル(PP) (2)

◆ISO/IEC 15408のPart 1に基づき、次のような内容で記述。

セキュリティターゲット（ST)

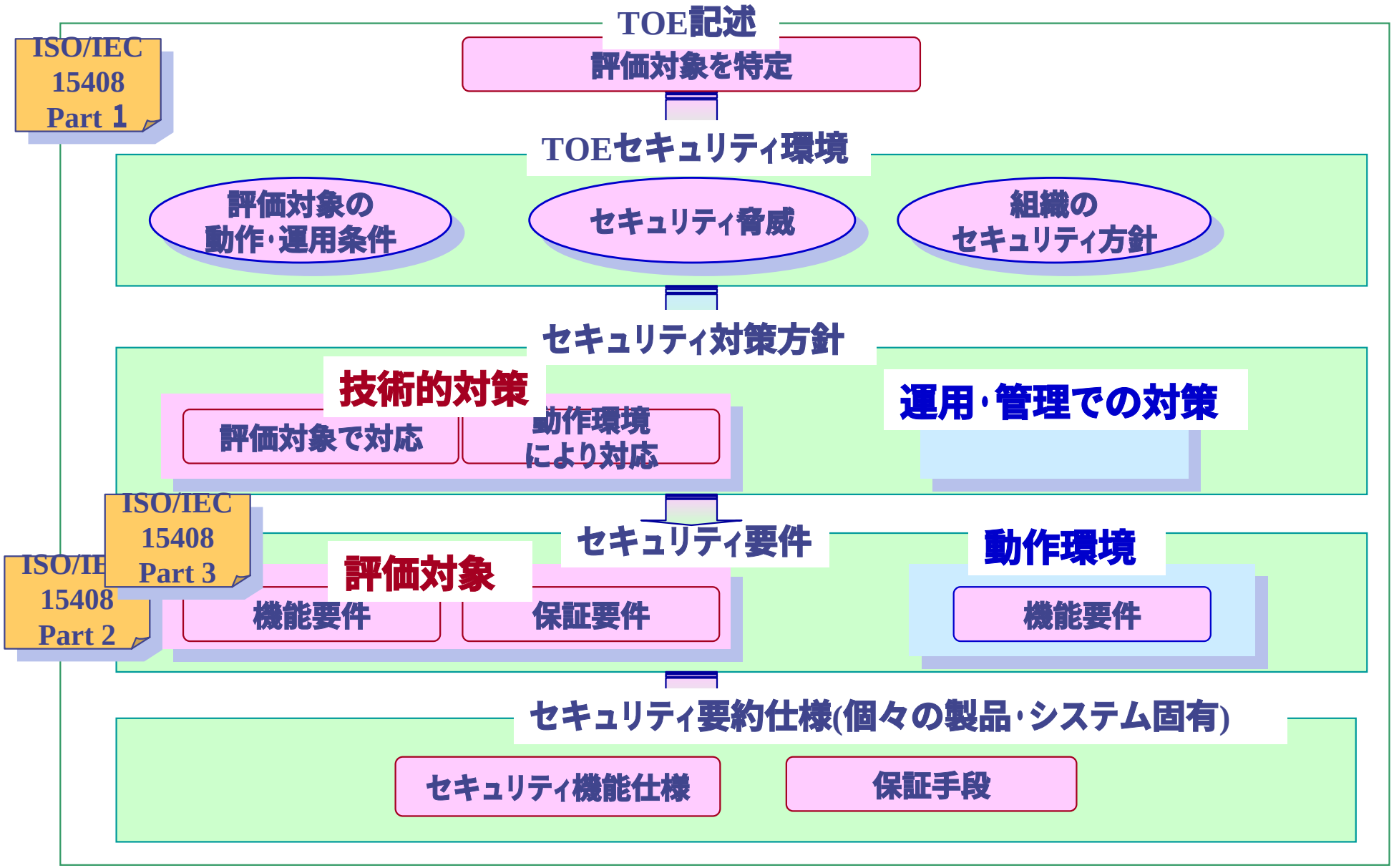
- TOE記述
- TOEセキュリティ環境
- セキュリティ対策方針
- セキュリティ要件
- セキュリティ要約仕様
- PP主張
- 根拠

プロテクションプロファイル（PP)

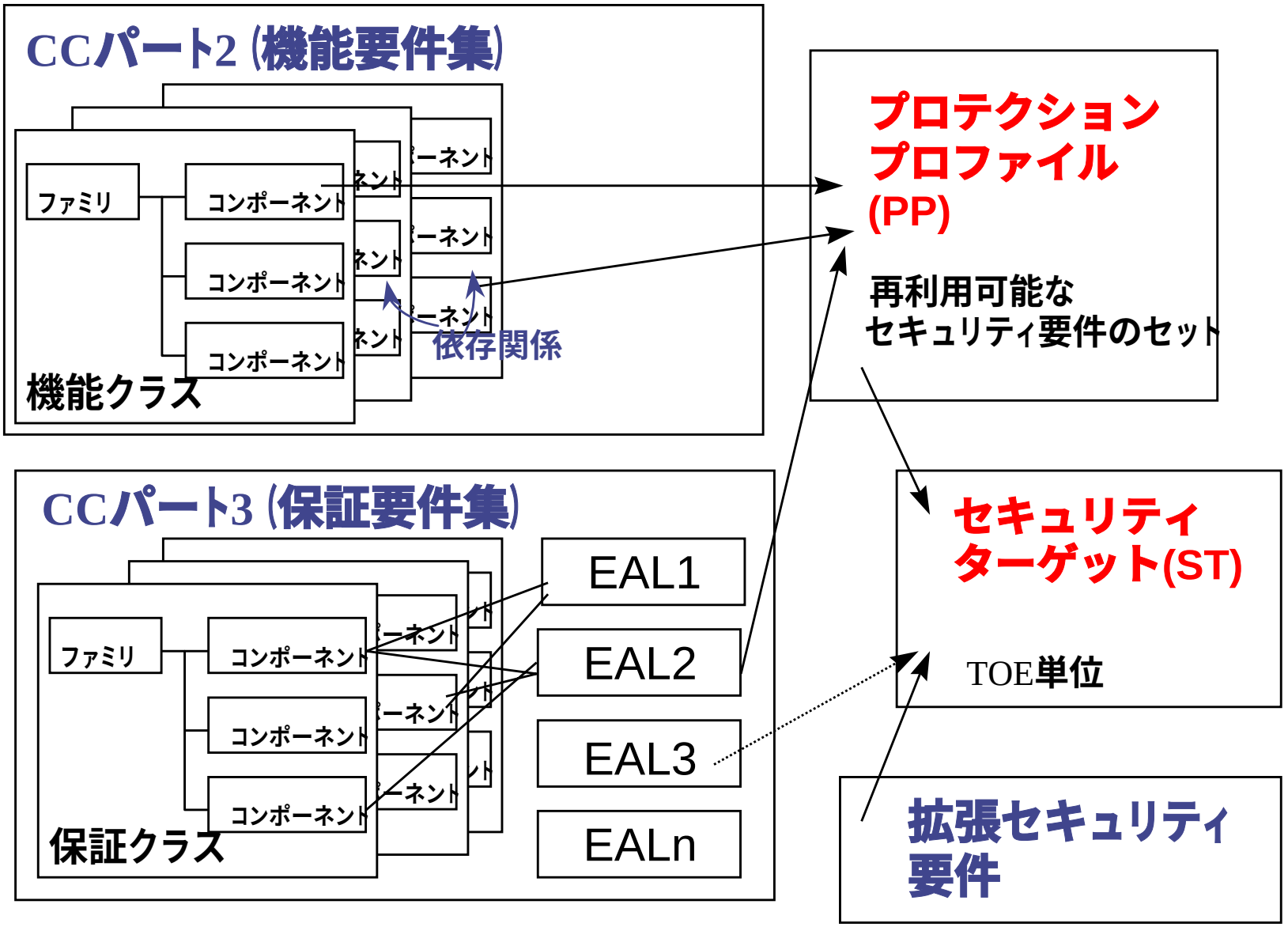
- TOE記述
- TOEセキュリティ環境
- セキュリティ対策方針
- セキュリティ要件
- 根拠

TOE：Target Of Evaluation（評価対象）
製品・システムのうち、評価対象となる範囲

セキュリティターゲット(ST)とプロテクションプロファイル(PP) (3)



セキュリティターゲット(ST)とプロテクションプロファイル(PP) (4)



IPA

PP開発の動向

◆ NIST-NSA Protection Profile (PP) Development Project

- 米国のNISTとNSAが中心となって重要な技術領域（OS,PKI,VPN等）のPP開発を促進し、その利用を奨励しようというもの
- http://niap.nist.gov/niap/projects/pptest-proj.html

NIST : The National Institute of Standards and Technology

NSA : The National Security Agency

◆ ISO/IEC 15292に基づくPP登録

- ISOにより任命される国際登録機関(フランスの標準機関 AFNORを予定)にPPを登録
- 誰でもインターネット経由で利用可能
- 登録は有料、利用は無料

IPA

セキュリティ機能要件(1)

◆ ISO/IEC 15408 Part 2にて、11クラスに分類

1. **セキュリティ監査** (*Security audit：FAU*)
   セキュリティ監査ログデータの収集と管理に関する要件
2. **通信** (*Communication：FCO*)
   送受信否認防止に関する要件
3. **暗号サポート** (*Cryptographic support：FCS*)
   暗号鍵の管理や暗号操作(暗号化、復号、ディジタル署名など)に関する要件(暗号アルゴリズムは対象外)
4. **利用者データ保護** (*User data protection：FDP*)
   アクセス制御、情報フロー制御、転送データの秘匿/保全、保管データの秘匿/保全、残存データ管理など、利用者データを保護するための要件
5. **識別と認証** (*Identification and authentication：FIA*)
   利用者を特定し、利用者本人であることを確認する要件

IPA

セキュリティ機能要件(2)

6. **セキュリティ管理** (*Security management：FMT*)

   セキュリティ属性や業務権限の管理など、セキュリティ機能を正常に動作させるための管理に関する要件

7. **プライバシー** (*Privacy：FPR*)

   プライバシーを確保するための、匿名性やペンネーム利用に関する要件

8. TOE**セキュリティ機能保護** (*Protection of the TSF：FPT*)

   不正再送(リプレイ)/不正削除/不正挿入など、不正な干渉からセキュリティ機構を保護するための要件

9. **資源利用** (*Resource utilisation：FRU*)

   一定の資源サービスを保証するための、資源の対障害性や資源割当などに関する要件

10. TOE**アクセス** (*TOE access：FTA*)

    利用条件の設定、離席対策、利用状況の表示など、不正利用を防止するための要件

11. **高信頼パス/チャネル** (*Trusted path/channels：FTP*)

    セキュリティ機構と利用者との間のセキュアな通信路を確保するための要件

IPA

セキュリティ保証要件(1)

◆ ISO/IEC 15408 Part 3にて、10クラスに分類

1. PP評価 (*PP evaluation：APE*)
   PPの内容の妥当性を評価するための要件
2. ST評価 (*ST evaluation：ASE*)
   ST の内容の妥当性を評価するための要件
3. 構成管理 (*Configuration management：ACM*)
   製品やシステムの設計書、ソースコード、オブジェクトコードなどの管理に関する要件
4. 配付と運用 (*Delivery and operation：ADO*)
   製品やシステムが利用者に安全に提供され、運用されるための要件
5. 開発 (*Development：ADV*)
   STに書かれたセキュリティ設計仕様が、プログラムのモジュール構成やソースコードに正しく反映されていることを保証するための要件

＊ 2から9の保証要件に基づきTOEを評価する。

IPA

セキュリティ保証要件(2)

6. **ガイダンス文書** (*Guidance documents：AGD*)

管理者および利用者向けのマニュアルやガイドラインの記述内容に関する要件

7. **ライフサイクルサポート** (*Life cycle support：ALC*)

開発から保守に至るまでの各工程で必要なセキュリティ手段に関する要件

8. **テスト** (*Tests：ATE*)

セキュリティ機能要件が正しく実現されていることをTOEのテストによって確認するための要件

9. **脆弱性評定** (*Vulnerability assessment：AVA*)

製品やシステムに内在するセキュリティ上の問題を漏れなく分析し、それに対する対策が施されていることを保証するための要件

10. **保証維持** (*Maintenance of assurance：AMA*)

機能拡張などの保守作業において、セキュリティレベル低下などを防止するための要件

＊ 2から9の保証要件に基づきTOEを評価する。

IPA

評価保証レベル

(EAL：Evaluation Assurance Level)

◆上位（番号の大きい方）レベルは、下位レベルを含む
◆検査対象物の範囲、検査の程度(セキュリティ強度を示すものではない)
◆より広く、より深く検査したから、より大丈夫(大きな保証)

レベル	評価の概要	
EAL1	セキュリティ機能仕様、マニュアルの確認、評価者によるテスト	商用
EAL2	サブシステムレベルまでセキュリティ機能設計の確認、構成管理の確認、開発者による機能強度・脆弱性分析、評価者による侵入テスト	商用
EAL3	サブシステムレベルまで開発者テスト結果の確認、構成管理システム使用の確認、開発環境の確認、開発者による誤使用分析	商用
EAL4	モジュールレベルまで確認、実装表現レベル(最も具体レベルの設計: 例えばソースコードレベル)の部分的確認、普通程度の攻撃に対抗	商用
EAL5	実装表現レベルのセキュリティ機能を全て確認、サブシステムレベルまでの設計が半形式的表現、隠れチャネル分析、高度の攻撃に対抗	軍用
EAL6	モジュールレベルまでの設計が半形式的表現、非常に高度の攻撃に対抗	軍用
EAL7	サブシステムレベルまでの設計が形式的表現、開発者による分析・テストのすべてを評価者が再確認	軍用

IPA

評価保証レベルの内容(1)

◆各評価保証レベル(EAL)を構成する保証要件(保証クラス、ファミリ)

保証クラス	保証ファミリ		評価保証レベル			
			EAL1	EAL2	EAL3	EAL4
構成管理	ACM_AUT	CM自動化				1
	ACM_CAP	CM能力	1	2	3	4
	ACM_SCP	CM範囲			1	2
配付と運用	ADO_DEL	配付		1	1	2
	ADO_IGS	設置、生成、及び立上げ	1	1	1	1
開発	ADV_FSP	機能仕様	1	1	1	2
	ADV_HLD	上位レベル設計		1	2	2
	ADV_IMP	実装表現				1
	ADV_INT	TSF内部構造				
	ADV_LLD	下位レベル設計				1
	ADV_RCR	表現対応	1	1	1	1
	ADV_SPM	セキュリティ方針モデル化				1
ガイダンス文書	AGD_ADM	管理者ガイダンス	1	1	1	1
	AGD_USR	利用者ガイダンス	1	1	1	1
ライスサイクルサポート	ALC_DVS	開発セキュリティ			1	1
	ALC_FLR	欠陥修正				
	ALC_LCD	ライフサイクル定義				1
	ALC_TAT	ツールと技法				1
テスト	ATE_COV	カバレージ		1	2	2
	ATE_DPT	深さ			1	1
	ATE_FUN	機能テスト		1	1	1
	ATE_IND	独立テスト	1	2	2	2
脆弱性評定	AVA_CCA	隠れチャネル分析				
	AVA_MSU	誤使用			1	2
	AVA_SOF	TOEセキュリティ機能強度		1	1	1
	AVA_VLA	脆弱性分析		1	1	2

数字が大きくなると、検査の深さが増す

IPA

評価保証レベルの内容(2)

◆基本的な内容は全EALに含まれる

保証クラス	保証ファミリ		評価保証レベル			
			EAL1	EAL2	EAL3	EAL4
構成管理	ACM_AUT	CM自動化				1
	ACM_CAP	CM能力	1	2	3	4
	ACM_SCP	CM範囲			1	2
配付と運用	ADO_DEL	配付		1	1	2
	ADO_IGS	設置、生成、及び立上げ	1	1	1	1
開発	ADV_FSP	機能仕様	1	1	1	2
	ADV_HLD	上位レベル設計		1	2	2
	ADV_IMP	実装表現				1
	ADV_INT	TSF内部構造				
	ADV_LLD	下位レベル設計				1
	ADV_RCR	表現対応	1	1	1	1
	ADV_SPM	セキュリティ方針モデル化				1
ガイダンス文書	AGD_ADM	管理者ガイダンス	1	1	1	1
	AGD_USR	利用者ガイダンス	1	1	1	1
ライスサイクル サポート	ALC_DVS	開発セキュリティ			1	1
	ALC_FLR	欠陥修正				
	ALC_LCD	ライフサイクル定義				1
	ALC_TAT	ツールと技法				1
テスト	ATE_COV	カバレージ		1	2	2
	ATE_DPT	深さ			1	1
	ATE_FUN	機能テスト		1	1	1
	ATE_IND	独立テスト	1	2	2	2
脆弱性評定	AVA_CCA	隠れチャネル分析				
	AVA_MSU	誤使用			1	2
	AVA_SOF	TOEセキュリティ機能強度		1	1	1
	AVA_VLA	脆弱性分析		1	1	2

インストールマニュアル

ドキュメントの記述の一貫性

運用マニュアル

IPA

評価保証レベルの内容(3)

◆EAL1のその他の内容

製品と一般的な添付文書さえあればチェック可能なレベル

保証クラス	保証ファミリ		評価保証レベル			
			EAL1	EAL2	EAL3	EAL4
構成管理	ACM_AUT	CM自動化				1
	ACM_CAP	CM能力	1	2	3	4
	ACM_SCP	CM範囲			1	2
配付と運用	ADO_DEL	配付		1	1	2
	ADO_IGS	設置、生成、及び立上げ	1	1	1	1
開発	ADV_FSP	機能仕様	1	1	1	2
	ADV_HLD	上位レベル設計		1	2	2
	ADV_IMP	実装表現				1
	ADV_INT	TSF内部構造				
	ADV_LLD	下位レベル設計				1
	ADV_RCR	表現対応	1	1	1	1
	ADV_SPM	セキュリティ方針モデル化				1
ガイダンス文書	AGD_ADM	管理者ガイダンス	1	1	1	1
	AGD_USR	利用者ガイダンス	1	1	1	1
ライスサイクル サポート	ALC_DVS	開発セキュリティ			1	1
	ALC_FLR	欠陥修正				
	ALC_LCD	ライフサイクル定義				1
	ALC_TAT	ツールと技法				1
テスト	ATE_COV	カバレージ		1	2	2
	ATE_DPT	深さ			1	1
	ATE_FUN	機能テスト		1	1	1
	ATE_IND	独立テスト	1	2	2	2
脆弱性評定	AVA_CCA	隠れチャネル分析				
	AVA_MSU	誤使用			1	2
	AVA_SOF	TOEセキュリティ機能強度		1	1	1
	AVA_VLA	脆弱性分析		1	1	2

バージョン管理

機能仕様書

マニュアルや機能仕様書の確認

評価保証レベルの内容(4)

◆より上位のEALでは、

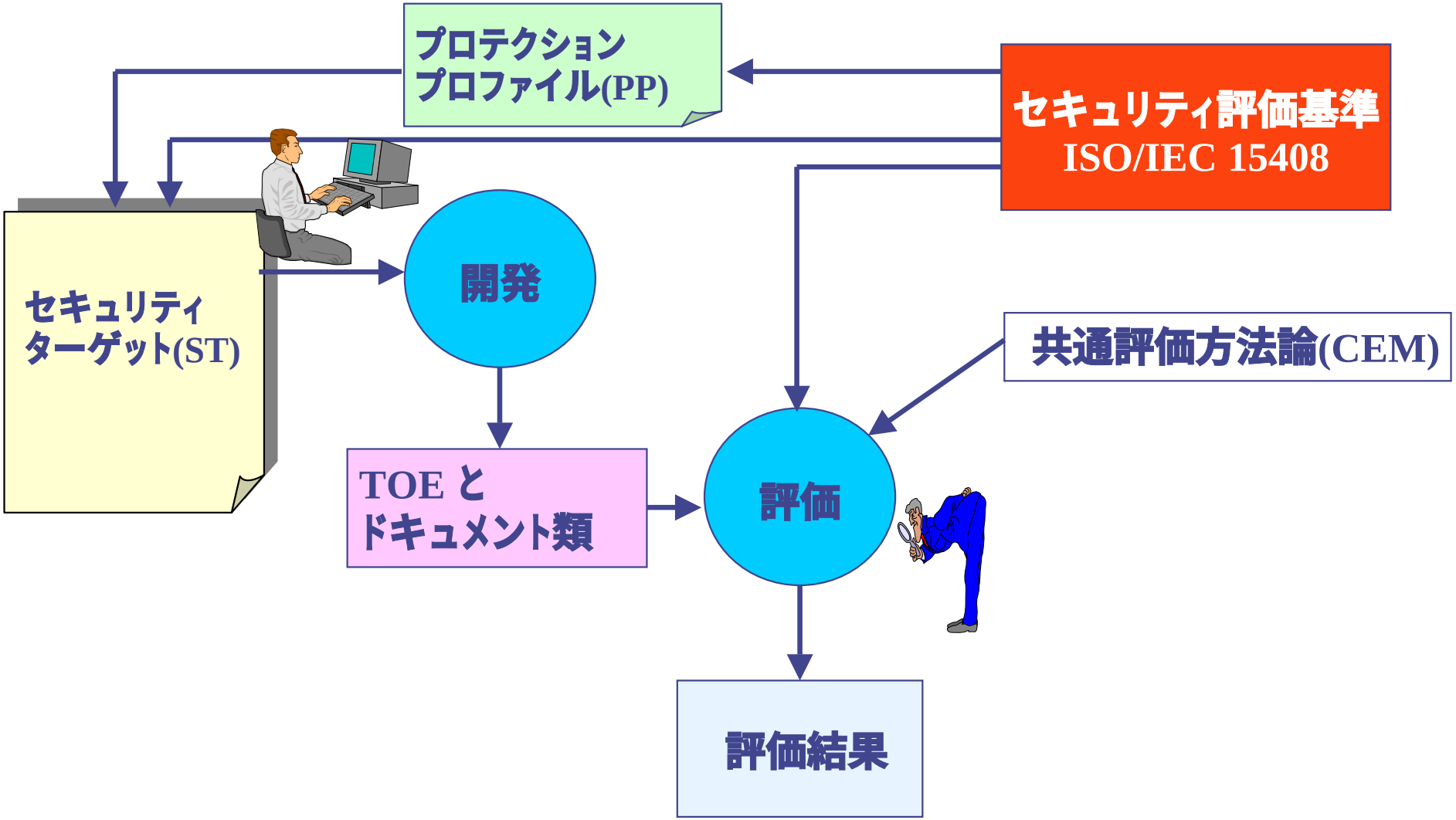
同一項目でも、深さが増す

1	2	3	4

保証クラス	保証ファミリ		評価保証レベル			
			EAL1	EAL2	EAL3	EAL4
構成管理	ACM_AUT	CM自動化				1
	ACM_CAP	CM能力	1	2	3	4
	ACM_SCP	CM範囲			1	2
配付と運用	ADO_DEL	配付		1	1	2
	ADO_IGS	設置、生成、及び立上げ	1	1	1	1
開発	ADV_FSP	機能仕様	1	1	1	2
	ADV_HLD	上位レベル設計		1	2	2
	ADV_IMP	実装表現				1
	ADV_INT	TSF内部構造				
	ADV_LLD	下位レベル設計				1
	ADV_RCR	表現対応	1	1	1	1
	ADV_SPM	セキュリティ方針モデル化				1
ガイダンス文書	AGD_ADM	管理者ガイダンス	1	1	1	1
	AGD_USR	利用者ガイダンス	1	1	1	1
ライスサイクル サポート	ALC_DVS	開発セキュリティ			1	1
	ALC_FLR	欠陥修正				
	ALC_LCD	ライフサイクル定義				1
	ALC_TAT	ツールと技法				1
テスト	ATE_COV	カバレージ		1	2	2
	ATE_DPT	深さ			1	1
	ATE_FUN	機能テスト		1	1	1
	ATE_IND	独立テスト	1	2	2	2
脆弱性評定	AVA_CCA	隠れチャネル分析				
	AVA_MSU	誤使用			1	2
	AVA_SOF	TOEセキュリティ機能強度		1	1	1
	AVA_VLA	脆弱性分析		1	1	2

項目数が増加

開発者と評価者から見たST、PPの位置付け



共通評価方法論(CEM)

- 評価方法を規定 － 評価者により評価結果がぶれないように
- PP、ST、EAL1～EAL4までの保証要件の評価用ガイダンス

- 歴史
  - CCプロジェクトにて1999/8発行
  - 我が国では標準情報(TR) として、2001/11公表
    TR X 0049:2001 情報技術セキュリティ評価のための共通方法
  - ISO/IEC SC27 WG3にて、CEMのTR化を審議中

参考情報

◆情報処理振興事業協会 セキュリティセンター

http://www.ipa.go.jp/security/

お問い合わせ：info-cc@ipa.go.jp

[ご参考]

◆Common Criteria Project

http://www.commoncriteria.org/