セキュリティとコンピュータ
~ 攻撃に強いソフトウェアをいかにして作るか ~
セキュリティ保証と評価

2009年6月11日

みずほ情報総研
情報セキュリティ評価室
室長　金子浩之

ソフトウェア開発者による保証の宣言

『セキュリティは大丈夫です』ということを相手に納得してもらうための方法

＜保証の信頼性を高める方法＞

- 開発者自ら「大丈夫です、私を信用してください」という
- 信頼できる第三者に確認してもらい、問題ないという結果報告を受けたことを相手に示す
- **セキュリティ評価の共通の基準**に基づいて **開発者自ら保証を宣言** し、認可された第三者がそれを評価することで保証に信頼を与え、別の信頼できる第三者によりその評価が基準に適合していることが確認済みであることを相手に示す

共通の基準:
Common Criteria (ISO/IEC15408)、CEM (ISO/IEC18045)

開発者による保証の宣言:
CC適合宣言 (保証レベル(EAL)及び保証コンポーネントによる適合宣言)

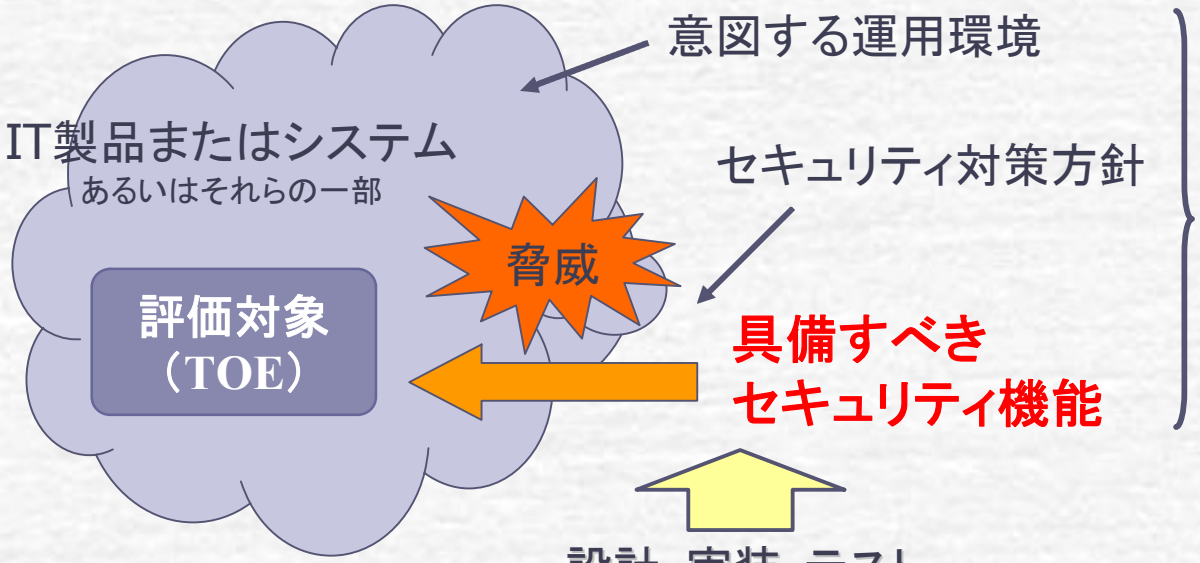
Common Criteriaのコンセプト

CCが求めるセキュリティを高めるコンセプトとは・・・・

セキュリティの枠組みを明確に定義
⇒保護資産、脅威、対抗策、要件、機能の関係を定義し、
これを正当化する根拠を示す

**「確かにセキュリティ機能が設計され、
実装された」ことの信頼性を「保証」し「評価」する**
⇒開発のライフサイクル全般を対象にする

Common Criteriaによる評価のコンセプト



セキュリティターゲット
（ST）

セキュリティターゲット評価

TOE評価

設計・実装・テスト

ST宣言通りの適切な設計・実装・テストの保証
許容できない脆弱性が残らないことの保証

保証エビデンス

テスト環境

ライフサイクルの保証

ST宣言通りの開発プロセス保証

ガイダンスの保証

ST宣言通りの機能性を保証するための運用ガイダンス

保証　**評価**

「保証」と「評価」の相互補完関係

- CC保証を導入するモチベーション
  - セキュリティ機能がきちんと設計、実装されていることを開発者が「保証」すること
  - メリット
    - セキュアな開発プロセスが定着することにより、製品のセキュリティ品質を本質的に高めるための体制ができる
    - 市場・顧客のセキュリティ要求に合致した製品を提供するためのトップダウンアプローチをマスターできる
    - 高品質の製品を確実に市場提供していくことで企業価値を高める

- 第三者評価を受けるモチベーション
  - セキュリティ機能が開発者の主張どおり、きちんと設計、実装されていることを第三者が「評価」すること
  - メリット
    - 製品セキュリティについて世界標準に基づいて客観的に検証される
    - 第三者評価・認証を求める調達に対し、企業としての説明責任が果たせる

CC及びCEMの全体構成

CCは、3つのパートにより構成される
機能要件、保証要件がカタログ化されている「要件」

CC

Part1 「概説と一般モデル」	CCの考え方、開発・評価の一般モデル
Part2 「セキュリティ機能要件」	機能要件パラダイムの解説 セキュリティ機能要件のカタログ
Part3 「セキュリティ保証要件」	評価保証レベル（EAL1～7）の定義 セキュリティ保証要件のカタログ
共通評価手法（CEM）	EAL5までの評価手法の定義

CCVer3.1の各パートの内部構成

Part1　概説と一般モデル

・一般モデル
・コモンクライテリアの要件と評価結果
・プロテクションプロファイルの仕様
・セキュリティターゲットの仕様

Part2　セキュリティ機能要件

・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)
・TOEセキュリティ機能の保護 (FPT)
・資源利用 (FRU)
・TOEアクセス (FTA)
・高信頼パス・チャネル (FTP)

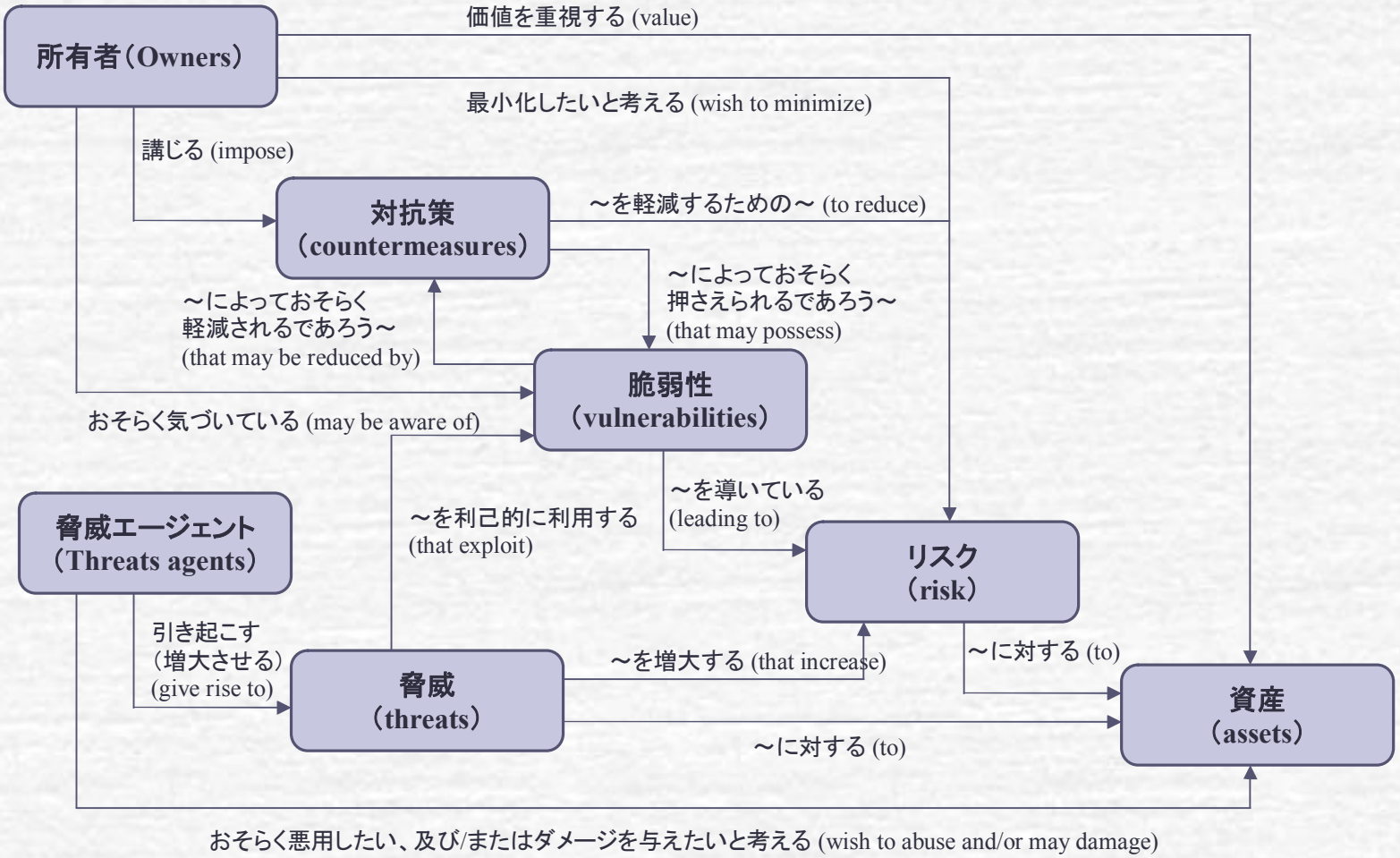
※F**の3文字で機能クラスを表す

Part3　セキュリティ保証要件

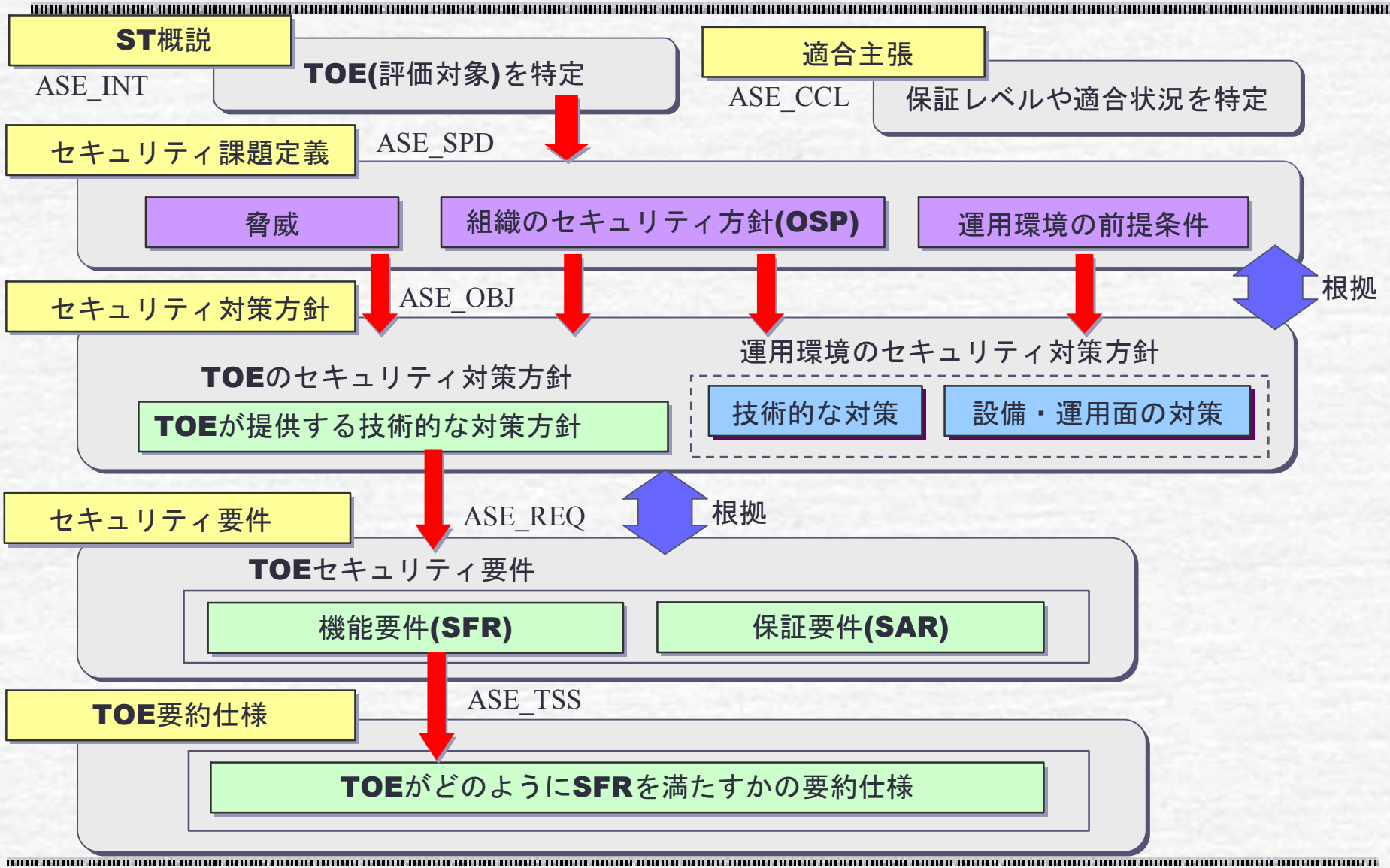
・評価保証レベル（EAL）
・統合保証パッケージ（CAP)
・プロテクションプロファイル評価 (APE)
・セキュリティターゲット評価 (ASE)
・開発 (ADV)
・ガイダンス文書 (AGD)
・ライフサイクルサポート(ALC)
・テスト (ATE)
・脆弱性評定 (AVA)
・統合 (ACO)
・付属書 (ADV、ACO、相互参照)

※A**の3文字で保証クラスを表す

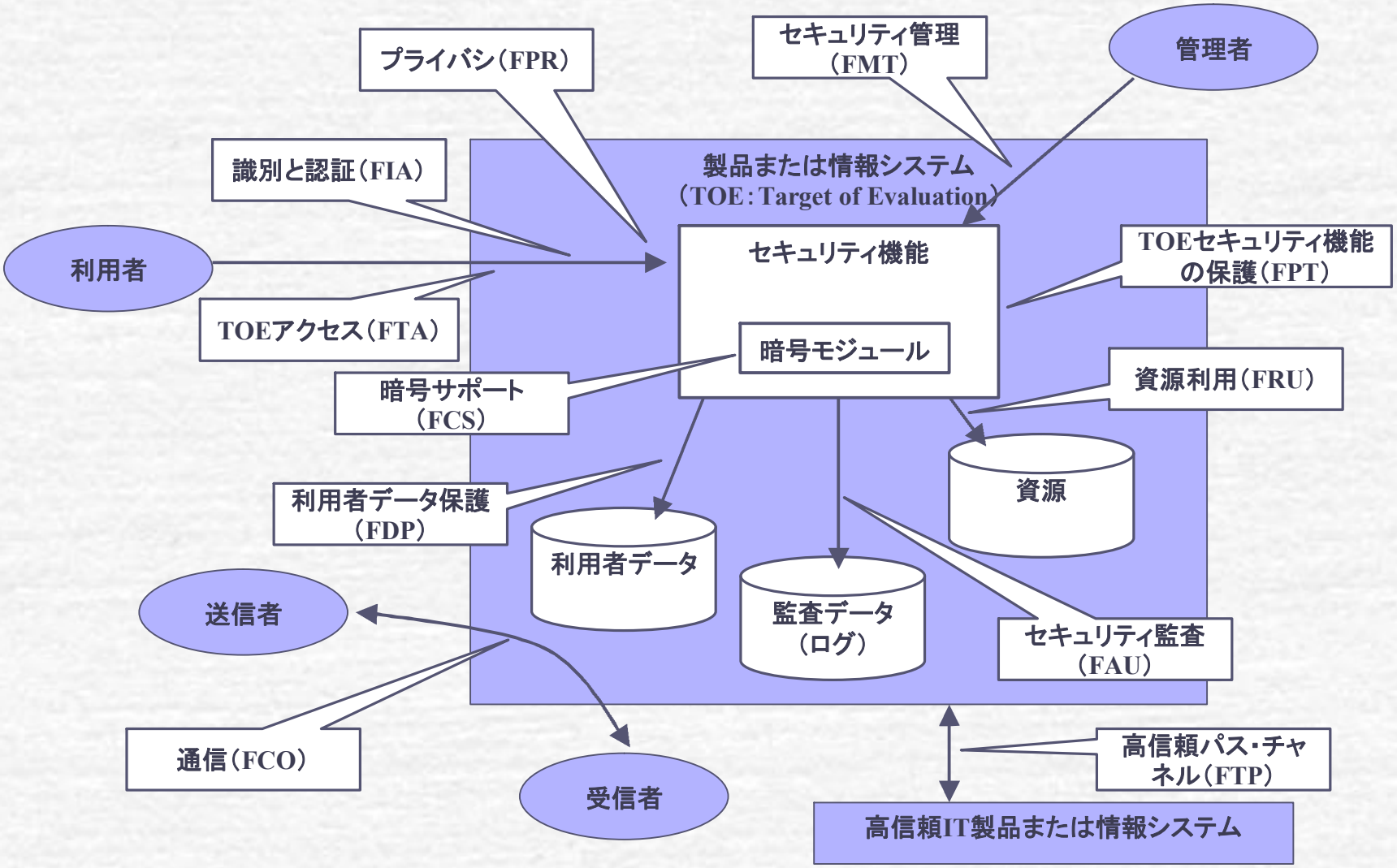
Part1 セキュリティ構造を分析するためのセキュリティ概念



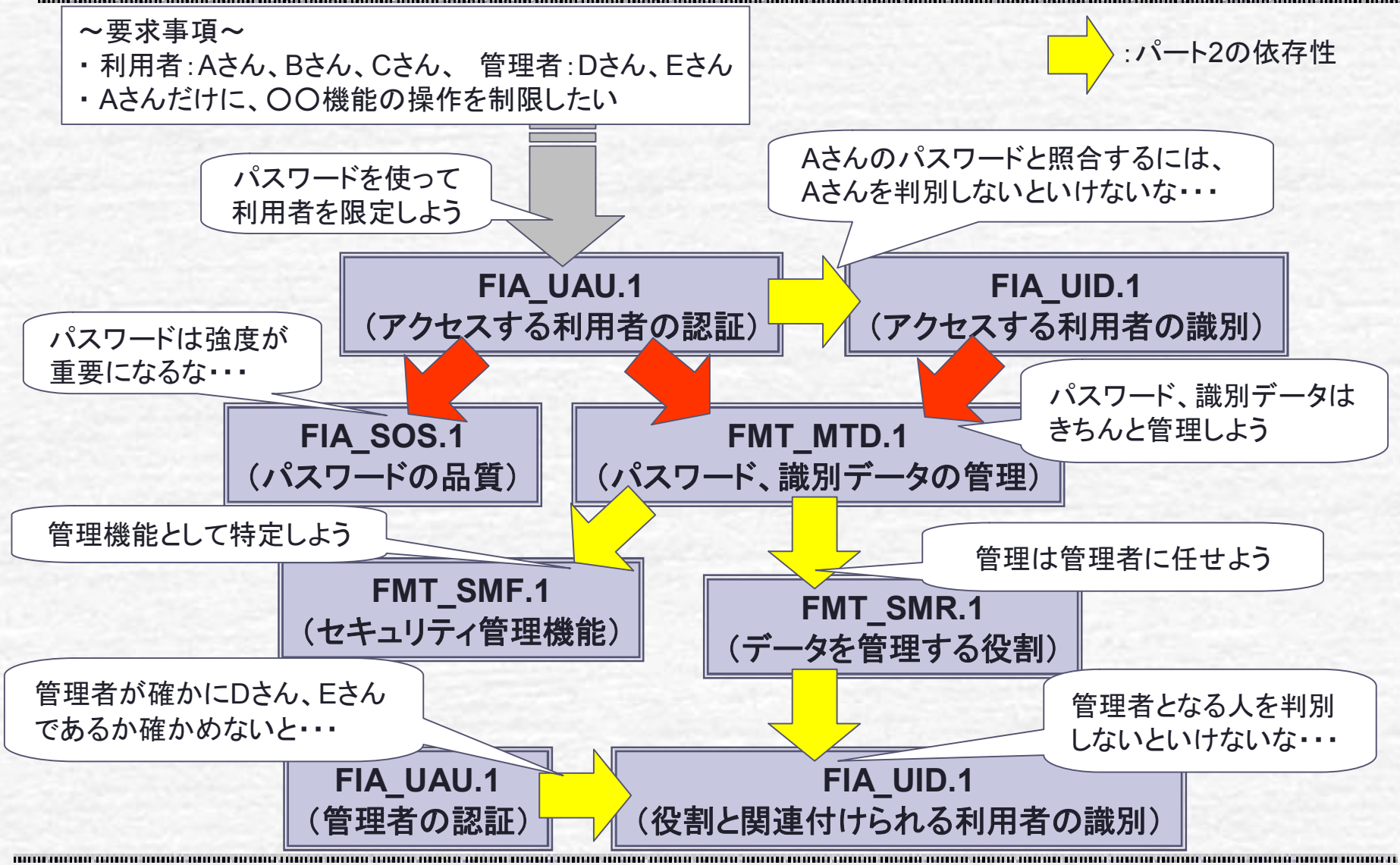
Part1 セキュリティターゲットの構造



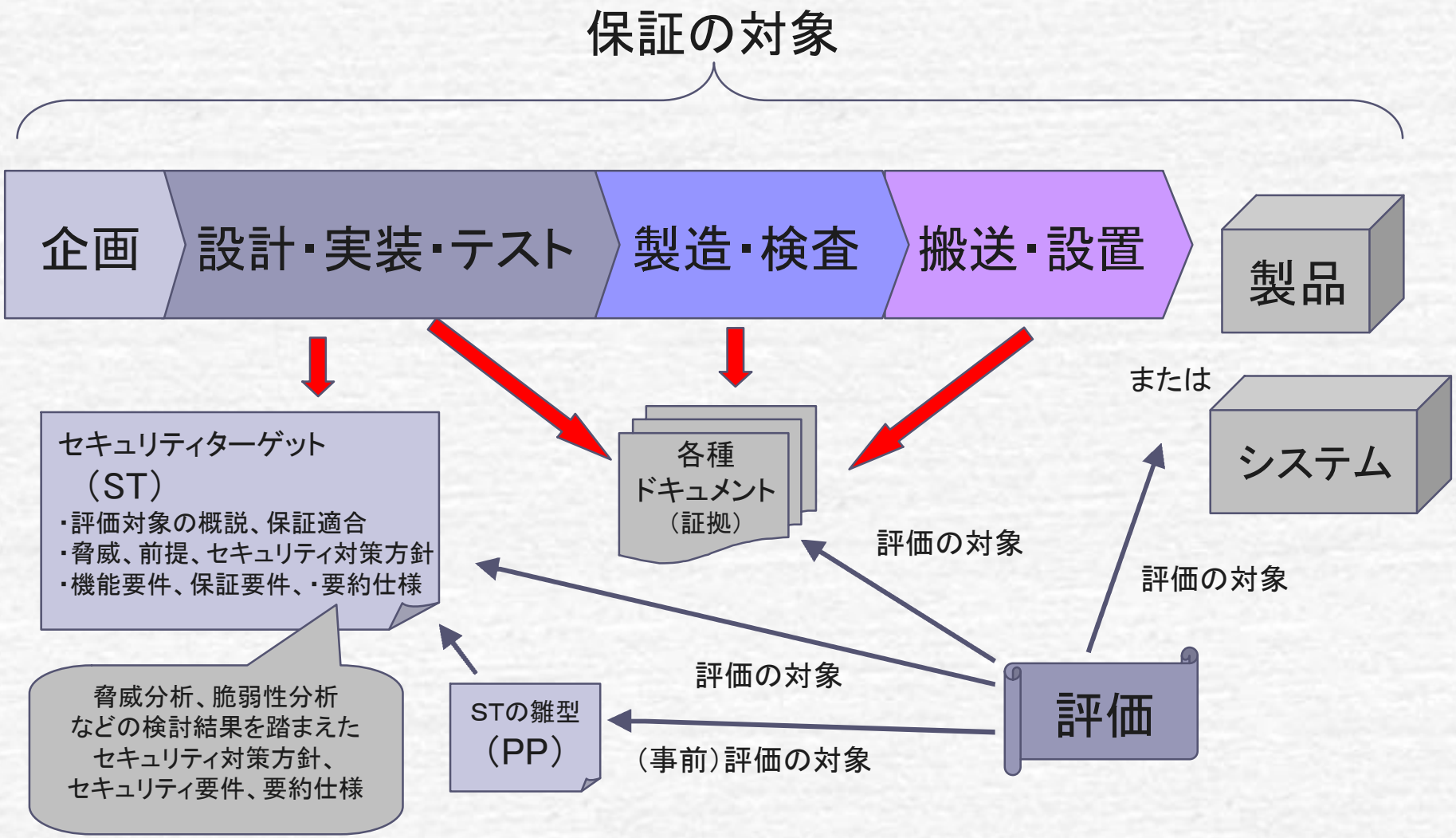
Part2 セキュリティ機能要件の概念



Part2 セキュリティ機能要件の適用例 （識別認証）



Part3 開発ライフサイクル上の保証すべき範囲



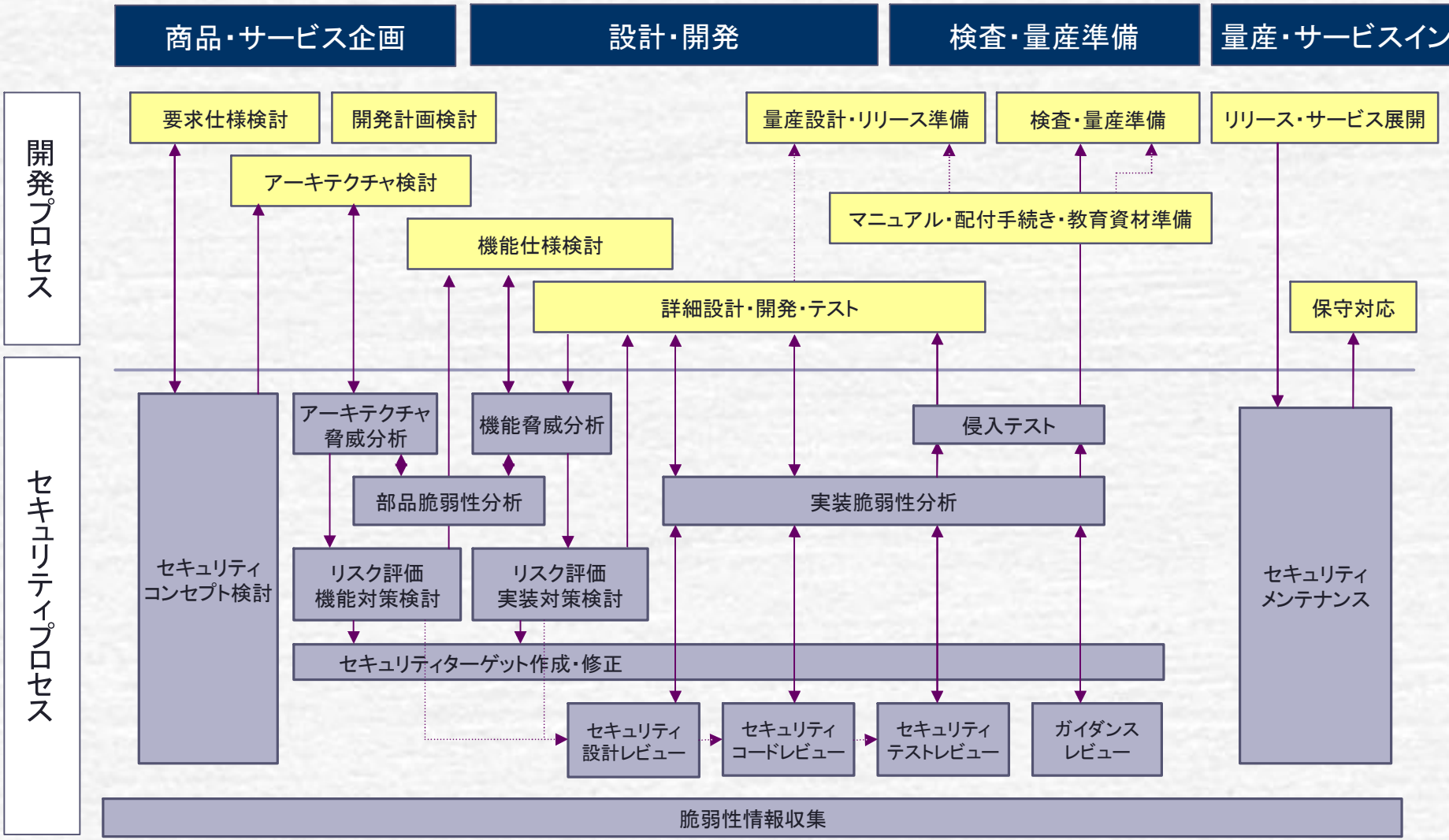
CCVer3.1のEALと保証コンポーネントの関係

保証クラス	保証ファミリ	省略名	評価保証レベル(EAL)/保証コンポーネント						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ASEクラス	ST概説	ASE_INT	1	1	1	1	1	1	1
セキュリティターゲット評価	適合主張	ASE_CCL	1	1	1	1	1	1	1
	セキュリティ課題定義	ASE_SPD		1	1	1	1	1	1
	セキュリティ対策方針	ASE_OBJ	1	2	2	2	2	2	2
	拡張コンポーネント定義	ASE_ECD	1	1	1	1	1	1	1
	セキュリティ要件	ASE_REQ	1	2	2	2	2	2	2
	TOE要約仕様	ASE_TSS	1	1	1	1	1	1	1
ADVクラス	セキュリティアーキテクチャ	ADV_ARC		1	1	1	1	1	1
開発	機能仕様	ADV_FSP	1	2	3	4	5	5	6
	実装表現	ADV_IMP				1	1	2	2
	TSF内部構造	ADV_INT					2	3	3
	セキュリティ方針モデル化	ADV_SPM						1	1
	TOE設計	ADV_TDS		1	2	3	4	5	6
AGDクラス	利用者操作ガイダンス	AGD_OPE	1	1	1	1	1	1	1
ガイダンス	準備手続	AGD_PRE	1	1	1	1	1	1	1
ALCクラス	CM能力	ALC_CMC	1	2	3	4	4	5	5
ライフサイクルサポート	CM範囲	ALC_CMS	1	2	3	4	5	5	5
	配付	ALC_DEL		1	1	1	1	1	1
	開発セキュリティ	ALC_DVS			1	1	1	2	2
	欠陥修正	ALC_FLR							
	ライフサイクル定義	ALC_LCD			1	1	1	1	2
	ツールと技法	ALC_TAT				1	2	3	3
ATEクラス	カバレージ	ATE_COV		1	2	2	2	3	3
テスト	深さ	ATE_DPT			1	2	3	3	4
	機能テスト	ATE_FUN		1	1	1	1	2	2
	独立テスト	ATE_IND	1	2	2	2	2	2	3
AVAクラス　脆弱性評定	脆弱性分析	AVA_VAN	1	2	2	3	4	5	5

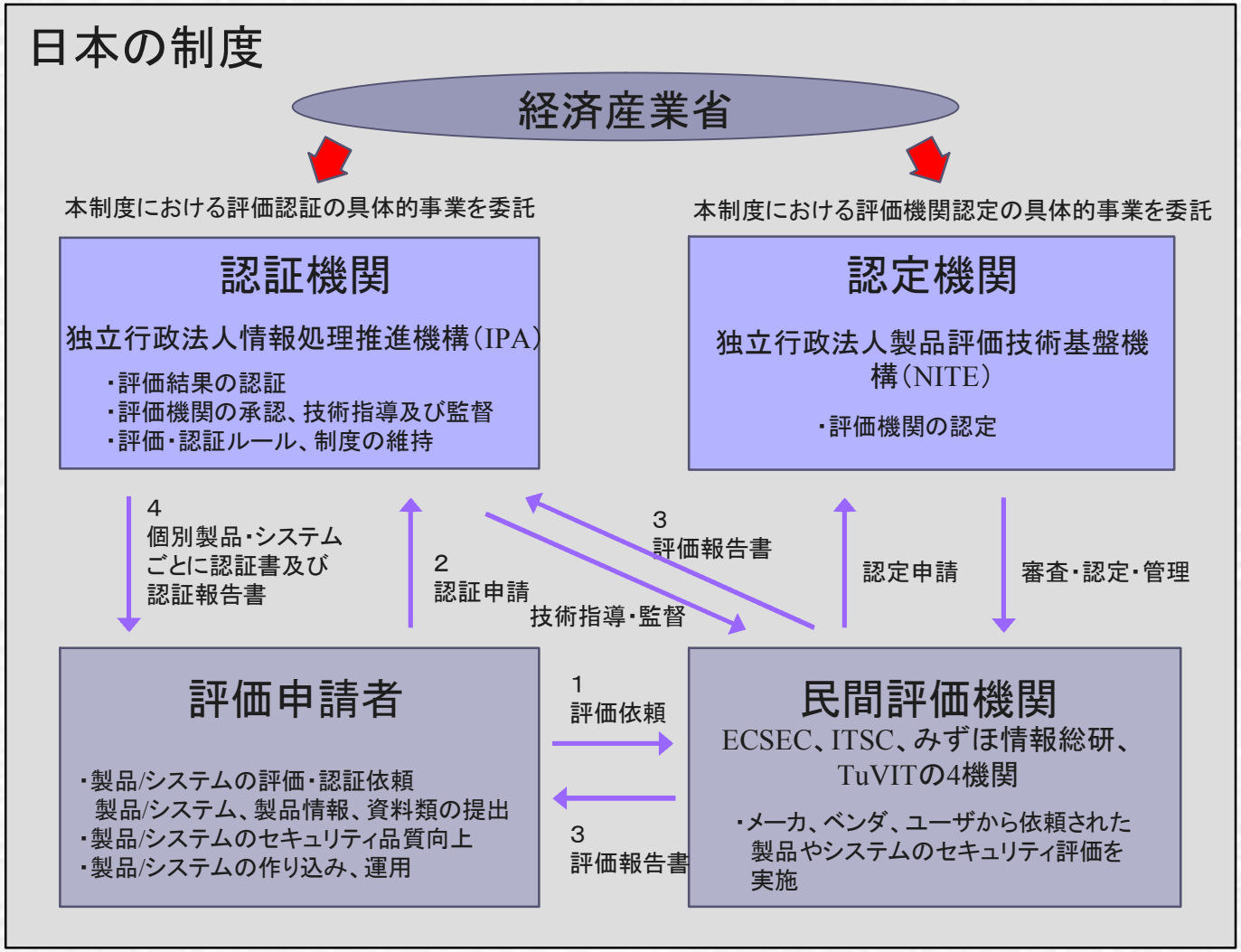
EALの選定（製品評価への適用傾向）

評価保証レベル	保証度合い	適用傾向
EAL1	セキュリティ機能が正しく利用できることを保証	運用システムやセキュリティがそれほど重視されない一般IT製品等に適用 初めて評価認証を行う場合や早期認証取得を目指す必要性がある場合などに適用効果あり CCVer3.1では、EAL1は特定機能保証と呼ばれる。STをEAL2相当にしたEAL1+として評価可能。
EAL2	設計情報と開発者によるテストが正しいことを保証	セキュリティ機能が要求される一般OA製品（機器、ソフトウェア）等に適用 製品開発が終了した後での評価証拠資料を作成して評価することも可能 CC導入コストを抑えつつ、設計開発成果を保証する場合などに適用効果あり
EAL3	設計、開発が方式的に適切に行われたことを保証	セキュリティ品質が要求されるネットワーク接続製品（機器、ソフトウェア）等に適用 開発拠点セキュリティなど組織的対応を含め、製品開発段階で保証すべき項目も含まれる セキュアな開発体制の保証を満たすことをアピールする場合などに適用効果あり
EAL4	設計、テスト、レビューが系統的に行われたことを保証	高度なセキュリティ品質が要求されるセキュリティ製品・部品、セキュリティソフトウェア等に適用 コード分析や評価者による脆弱性検査において製品種別特有の評価方法がとられる そのため、保証手段が確立されていない製品分野には適用しにくい
EAL5以上	セキュリティ品質が最優先されるような製品を対象	高いレベルの脅威への対抗が求められる製品や軍事目的など限定された分野の製品実績のみ 今後、設計開発方法論や開発ツールが整備されたセキュリティ製品分野への適用が予想される

CCライクなセキュリティ保証を実現するためのプロセス



CCに基づくITセキュリティ評価及び認証制度



他国制度（日本以外）
アメリカ、カナダ、
フランス、ドイツ
イギリス、オーストラリア
ニュージーランド、
オランダ、ノルウェー、
韓国、スペイン、スウェーデン

CCRA
相互認証

制度は持たないが、
認証結果を認める国
フィンランド、ギリシャ、
イタリア、イスラエル、
オーストリア、トルコ、
ハンガリー、チェコ、
インド、シンガポール、
マレーシア、デンマーク
パキスタン

ITセキュリティ評価及び認証制度が定める規格・標準

◈ 「ITセキュリティ評価及び認証制度」で認める評価基準や評価方法を適用する

◈ 評価基準（通称、CC）

- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision2

＜以下の同類規格は上記CCのバージョンに追随していない＞

- **ISO/IEC 15408**:2005 Information Technology - Security Techniques Evaluation Criteria for IT Security.
- **JIS X 5070**:2000 セキュリティ技術・情報技術セキュリティの評価基準

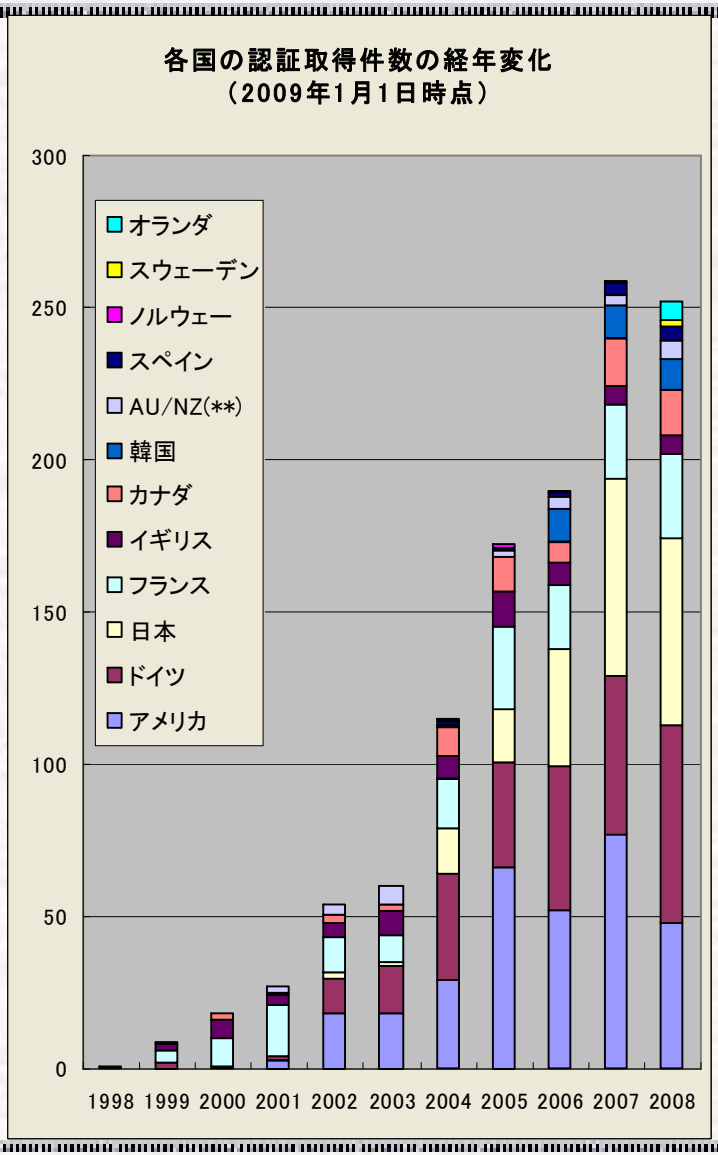
◈ 評価方法（通称、CEM）

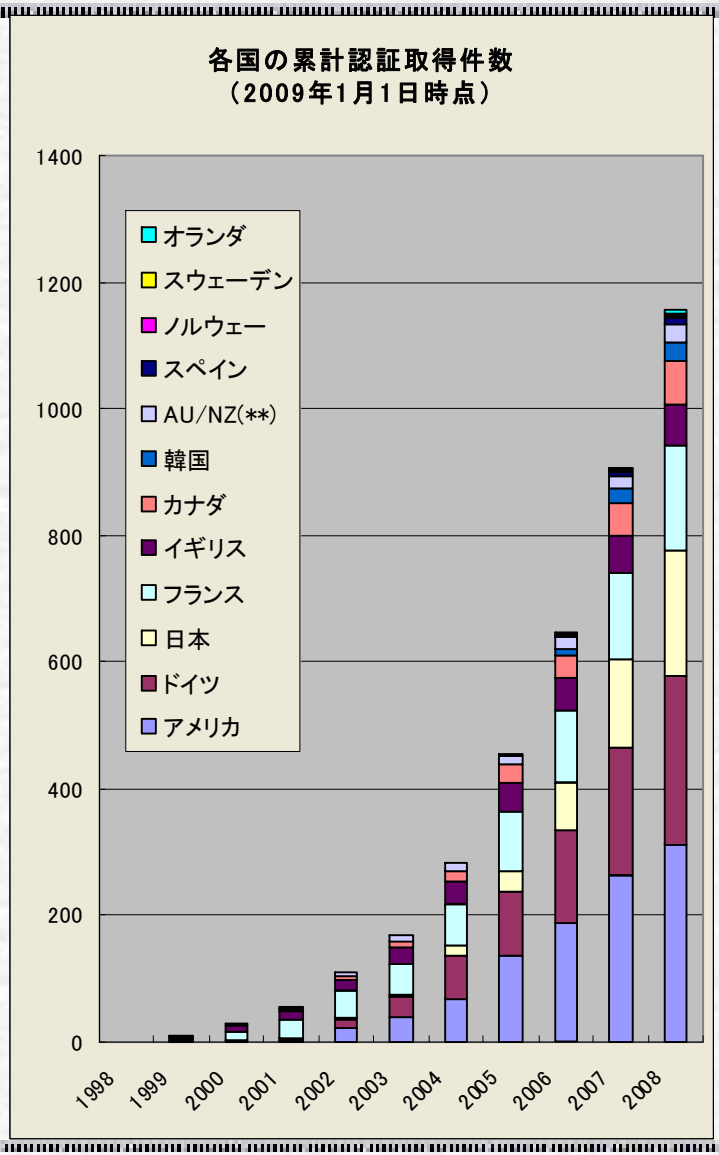
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision2

＜以下の同類規格は上記CEMのバージョンに追随していない＞

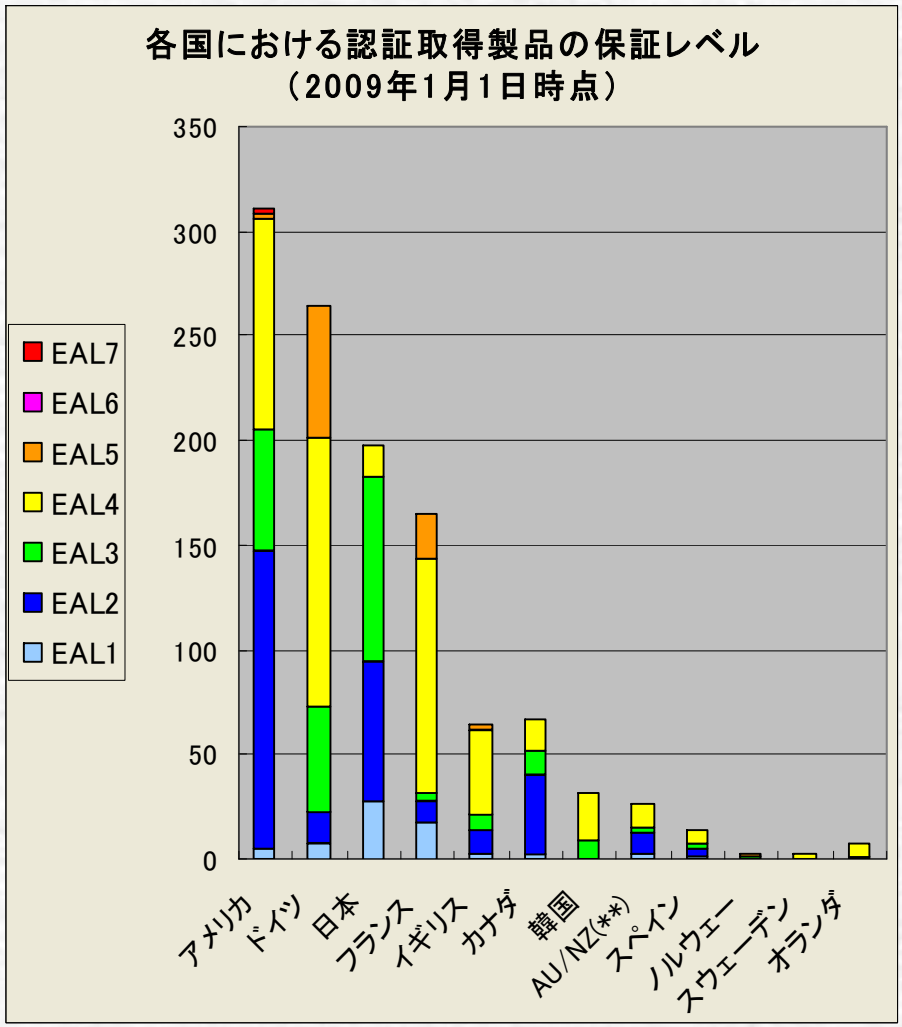
- **ISO/IEC 18045**:2005 Information Technology - Security Techniques - Methodology for IT Security Evaluation
- **JIS TR X 0049**:2001 情報技術セキュリティ評価のための共通方法

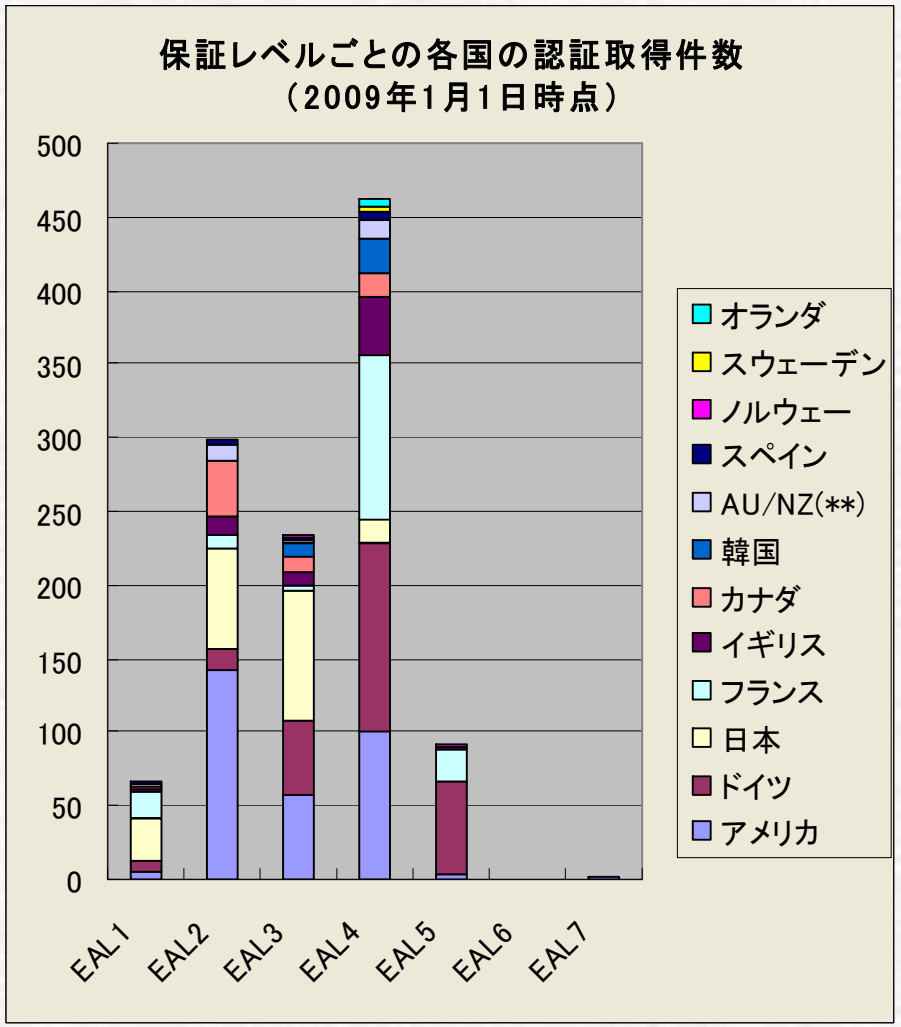
CC認証取得件数の推移



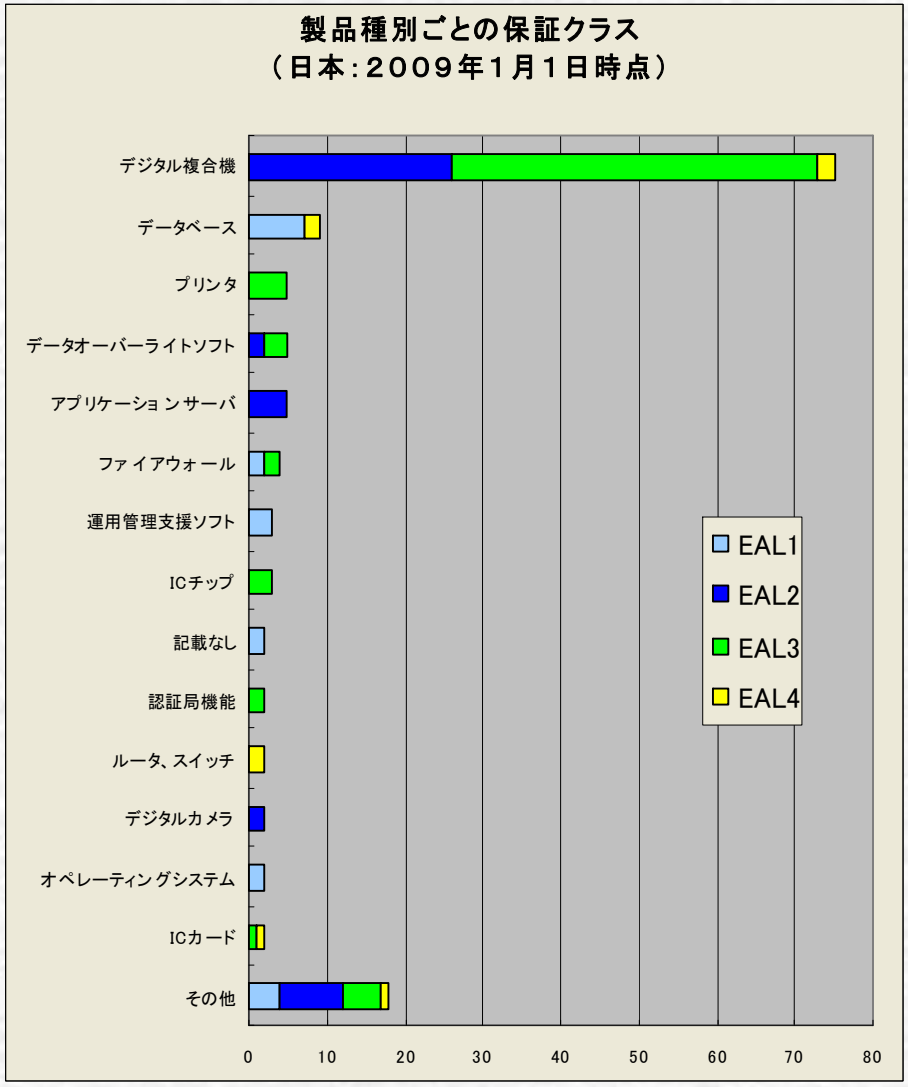


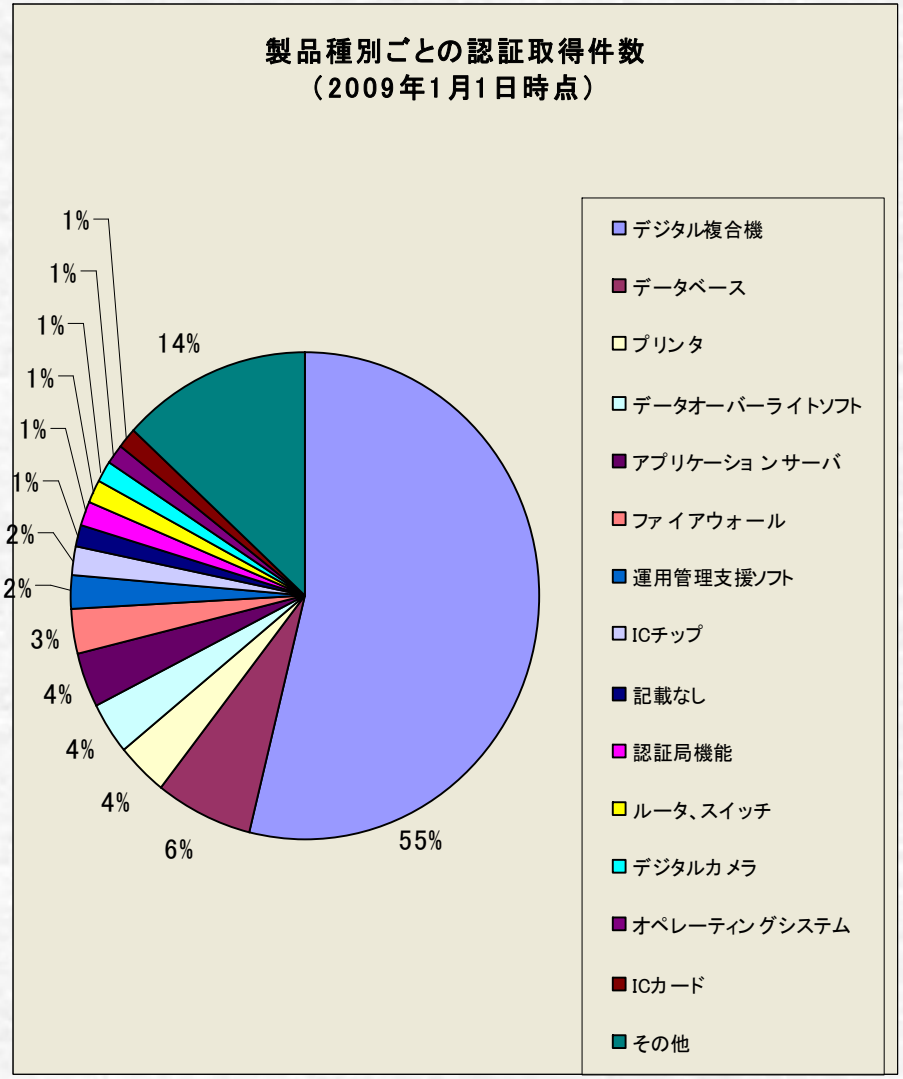
保証レベル毎のCC認証取得



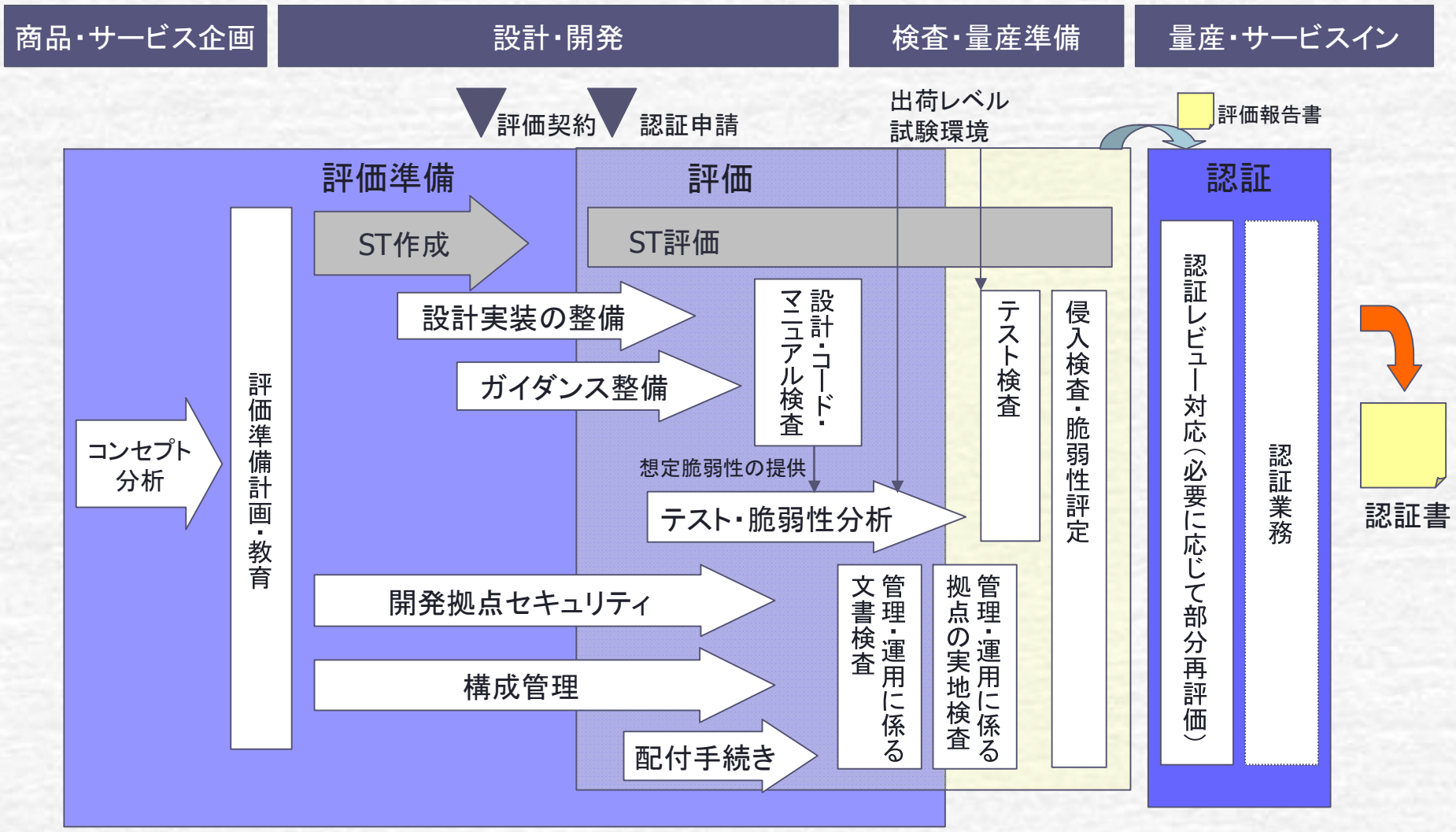


日本におけるCC認証取得製品内訳





セキュリティ保証と評価・認証タスクの関係



CCが関係する日本の最近の取り組み

- 政府機関のセキュリティ対策　(NISC)
  - 「政府機関の情報セキュリティ対策における統一基準（第4版）」
  - 「第2次情報セキュリティ基本計画」
  - 「セキュアジャパン2009（案）」 など
- CCタスクフォース：CCTF　(IPA)
  - 「ITセキュリティ評価及び認証制度」の制度運営状況、改善施策、プロモーション、技術課題等に関する協議体
- ICシステムセキュリティ協会 (ICSS-RT)
  - ICチップ及びICシステムのセキュリティ評価に関する協議体
  - 欧州と同等のICシステムセキュリティ体制構築を目指す
  - AISTのRCISにハードウェア評価設備を設置、技術開発をスタート