CC (ISO 15408)の基礎

平成１８年２月

独立行政法人情報処理推進機構
セキュリティセンター
情報セキュリティ認証室

目次

CC評価認証に係わる政府の施策　2005年12月

内閣官房より、
「政府機関の情報セキュリティ対策のための統一基準」が公表（12月13日）された。
（http://www.bits.go.jp/active/general/feedback.html）

本基準は、今後政府調達に反映されます。特に、CC評価認証に関連する箇所は以下。

4．3.1情報システムのセキュリティ要件
基本遵守事項（必須要件）として、
*情報システムの開発に際しては、CCによるST評価確認を受けることが求められます。「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に重要なセキュリティ要件があると認めた場合には、当該情報システムの**セキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST: Security Target）のST評価・ST確認を受けること。**」*

強化遵守事項（推奨）として、
*構築する情報システムのために調達する**製品はCC認証を取得**していること。*（概要のみ記載）

6．1.1　機器等の購入
基本遵守事項（必須要件）として、
*総合評価落札方式により購入する場合、**CC認証の取得**を評価項目として活用すること。*（概要のみ記載）

6．1.3　ソフトウェア開発
基本遵守事項（必須要件）として、
*ソフトウェアの開発に際しては、CCによる**ST評価確認を受ける**こと。*（概要のみ記載）

経済産業省より、平成18年度税制改正が発行され、この中で、CCの評価認証を受けたOS,DBMS,ファイアウォールを購入する際には、税額控除が適用されます。

2．産業競争力のための情報基盤強化税制の創設（法人税、所得税、住民税、事業税）

グローバル大競争を勝ち抜くためには、部門や企業を越えた戦略情報の共有･活用が鍵となるが、我が国企業では未だ不十分。
加えて、情報セキュリティ対策は米国等に対して大きく劣後しており、社会全体の情報セキュリティリスクが顕在化するおそれ。
このため、情報セキュリティを確保しつつ、国際競争力を強化するための新税制を創設する。

【制度の概要】

○情報セキュリティ強化と国際競争力強化の観点から、高度な情報セキュリティが確保された情報システム投資を促進し、情報基盤を強化するための税制上の措置を講じる。

（税額控除（10％）又は特別償却（50％）の選択適用）

【対象投資の内容】

①OS※及びこれと同時に設置されるサーバー
②データベース管理ソフトウェア※及びこれと同時に設置されるアプリケーションソフトウェア
③ファイアーウォール※（①または②と同時に取得されるものに限る）

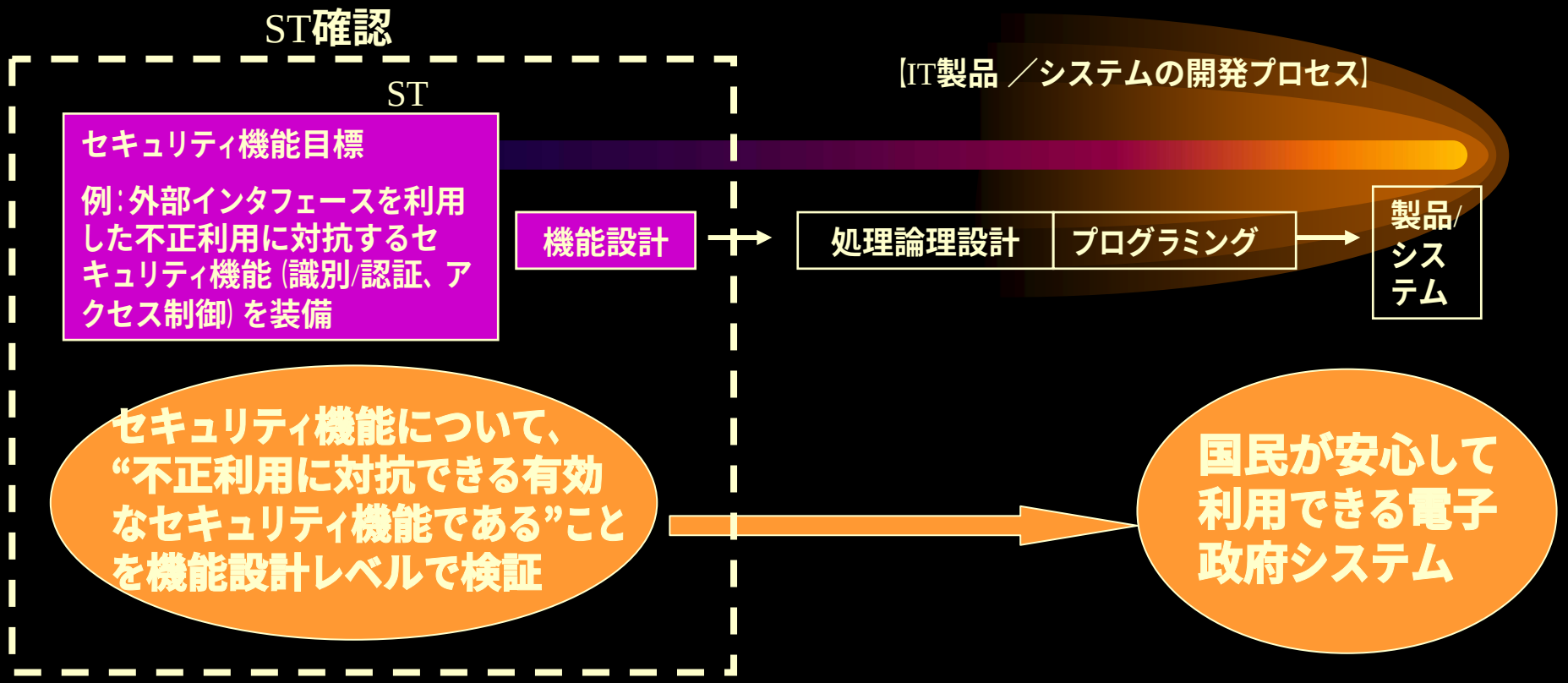
※ISO/IEC 15408に基づいて評価･認証されたもの。

（注1）年間投資額：1億円以上（資本金1億円以下：３００万円以上、資本金1億円超１０億円以下：3,０００万円以上）
（注2）資本金1億円以下の法人については、リース投資も税額控除の対象。（リース費用の総額：４２０万円以上）
（注3）適用期限は2年間。
（注4）税額控除について、法人税額の２０％相当額を限度とし、控除限度超過額については1年間の繰越しを認める。

＜改正の効果＞

制度の概要 高度な情報セキュリティが確保された情報システムの導入により、企業の部門間、企業間の情報共有･活用を促進し、抜本的に国際競争力を強化する。

ST確認の目的：「セキュリティ機能の設計について評価・確認する。」



ST確認のための保証コンポーネント

＝ ASEクラス(CC V3の場合のLow assurance STは除く)

＋ ADV_FSP.1 (CC V2.3の場合は依存性として要求されているADV_RCR.1を含む)

評価用証拠は「ST」と「機能仕様」

注：適用は、原則として、平成18年5月1日以降の申請分から。

セキュリティ評価（ST確認）の意義

電子政府システム

システム提供者の義務

電子政府システムにおいて個人情報などの秘密情報が確実に保護されていることの保証（ST確認）を利用者に通知

国民は安心して電子政府システムを利用
⇒システムの利用促進が図れる

電子政府システム利用者
＝国民

STの評価とは？

セキュリティ目標（ST） ← 開発者が作成

リスクの識別

例えば、顧客情報を不正に利用

セキュリティ対策

例えば、“利用者の本人確認”、“データに対する利用権限のチェック”、など

セキュリティ機能

正確に要求する機能の要件を記載するために、要件の記述内容を規定

例：アクセス制御

セキュリティ保証

正確に要求する保証の要件を記載するために、要件の記述内容を規定

例：脆弱性分析

セキュリティ機能仕様の概要

必要十分性を評価

STに準拠を検証

製品 / 情報システム

開発生産物（設計書など）

選択

保証要件
信頼性の確保

機能要件

具体化

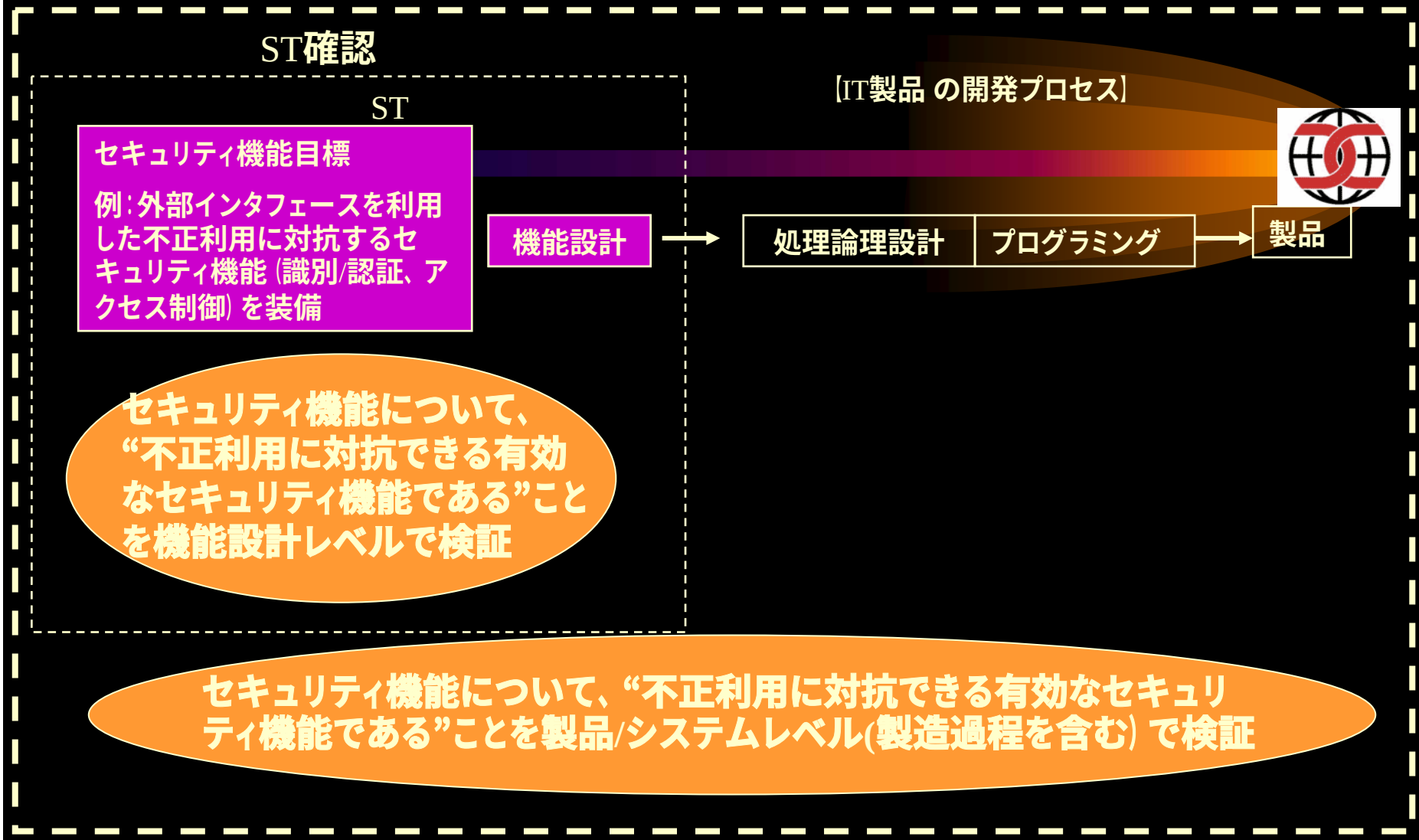
アクセス制御に関して：
個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

個人情報保護のためのガイドライン

アクセス制御に関して：

情報システムは、*顧客情報管理業務者*に対して、*業務サーバAの顧客情報管理データベースを参照する*権限を付与し、アクセス時にその妥当性をチェックするアクセス制御を実施しなければならない

ST確認とCC認証


ST確認
ST
セキュリティ機能目標
例：外部インタフェースを利用した不正利用に対抗するセキュリティ機能（識別/認証、アクセス制御）を装備
機能設計
【IT製品 の開発プロセス】
処理論理設計
プログラミング
製品
セキュリティ機能について、“不正利用に対抗できる有効なセキュリティ機能である”ことを機能設計レベルで検証
セキュリティ機能について、“不正利用に対抗できる有効なセキュリティ機能である”ことを製品/システムレベル(製造過程を含む）で検証
ＣＣ(Common Criteria)認証

１．セキュリティ評価の意義

なぜセキュリティ評価が必要なのか？

利用者はIT機能がカタログどおりに動作することを確認できる。

ところが

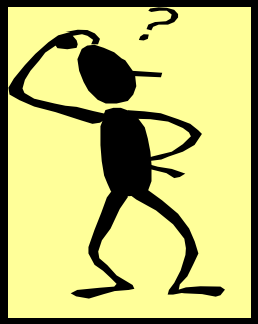
セキュリティ機能（ルールに従った処理だけが許可されることを確保）は、

動作しなかったり、不当な干渉を受けたり、動作不能に陥ったりなどすることなく動作することが求められる。

データが暗号化されないことは無いでしょうね？

データが記憶装置から削除されないことは無いでしょうね？

アクセスルールがチェックされないことは無いでしょうね？



利用者が、「機能が正確かつ有効に動作しないことは無いこと。」を確認することは困難。

「情報システム／製品のセキュリティは大丈夫？」と開発者に問う！

ISO 15408の考え方

情報システム／製品のセキュリティは

大丈夫？

開発者・運用者を信用

監査者がチェック

ISO 15408

大丈夫であることを開発者・運用者が宣言（セキュリティ目標）する。

開発（運用）生産物に基づいて、宣言内容の正当性（セキュリティ機能の正確性と有効性）を利用者に成り代わって第三者が検証する。

宣言する内容の形式や用語、および検証する内容を規格化したものがISO 15408:セキュリティ評価基準（これはCC：コモンクライテリアとも呼ばれる）

セキュリティ評価とは？

セキュリティ目標(ST)が妥当であることを検証

セキュリティ対策は必要かつ十分か

脅威（リスク）

↕

セキュリティ機能

情報システム/製品はセキュリティ目標に準拠して開発・構築・運用されていることを検証

準拠：信頼性を確保するために必要な証拠（ST、機能設計、構成設計、テスト結果、監査ログなど）を検証

証拠に関わる要求を保証要件（機能仕様、構造設計、テスト内容、マニュアル記載事項などの検証）として規定

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

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作成時に、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

- ➢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)

機能要件（CCパート2）の例

利用者

識別と認証

- 認証情報の秘密性確保
- 認証のタイミング
- 多重認証
- 再認証
- 一意の識別

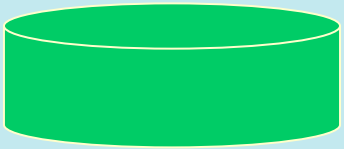
利用管理

- 利用条件の設定
- 離席対策
- 利用状況の表示

信頼パス

アクセス管理

- 利用者とアクセス権限（規則、操作、許可／禁止）と 資源（利用最小単位）のルールを管理



保管データの秘匿性と完全性
残存データの管理

情報フロー管理

- 利用主体と属性（ID，操作、セキュリティレベル、業務権限）と 資源のルールを管理

転送データの秘匿性、完全性

不正再送／削除／挿入防止

信頼パス

証拠性の確保

監査ログデータの収集

- 収集事象、収集データの内容、障害対策

セキュリティ管理

プライバシ保護

暗号鍵管理

セキュリティ機構の保護

機能要件事例：アクセス制御に関して

規定

FDP_ACC.1 サブセットアクセス制御

FDP_ACC.1.1

TSF は、[*割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[*割付: アクセス制御SFP*]を実施しなければならない。

評価対象に対して割付部分を設定

情報システムは、*顧客情報管理業務者*に対して、*業務サーバAの顧客情報管理データベースを参照する権限を付与し、アクセス時にその妥当性をチェックするアクセス制御*を実施しなければならない。

保証要件（CCパート3）の例

構成管理

・自動管理ツールによるソースコード／オブジェクトコードの管理

・設計書、テスト関連ドキュメント、マニュアルのログ管理

ライフサイクルサポート

・設計や作成時の物理、運用、人の管理

・障害修正管理

開発

・セキュリティポリシーモデル（機能との関連、規則／特徴、無矛盾性／完全性）の完備

・機能仕様書（機能詳細、外部ｲﾝﾀｰﾌｪｰｽ（目的、利用方法、例外、ｴﾗｰﾒｯｾｰｼﾞ、機能説明）の完備

・構成設計書（セキュリティ関連のハード／ファーム／ソフト、サブシステム機能／インターフェース，）の完備

・論理設計書（モジュール機能／インタフェース）の完備

・セキュリティ機能上重要な部分のソースコードの完備

ガイダンス

・システム管理者向け（安全な運用方法）

・利用者向け（安全な利用方法）

テスト

・テストドキュメント（計画、手順、期待結果、実施結果）の完備

・機能やサブシステムの構造／インターフェースのテスト実施

脆弱性分析

・利用環境分析からの対策の完備性，・セキュリティ機能の強度分析の実施、侵入テストの実施

・検出された脆弱性の評価

保証要件事例

TOE:評価対象（評価を受ける者がその範囲を規定する）

AVA_VLA.2 独立脆弱性テスト

開発者アクションエレメント：

AVA_VLA.2.1D 開発者は、TOE提供物件に対して、利用者がTSPを侵害し得る方法を探す分析を行い、証拠資料を提出しなければならない。

AVA_VLA.2.2D 開発者は、識別された脆弱性の処置について証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_VLA.2.1C 証拠資料では、識別されたすべての脆弱性に対して、TOEの意図した環境においてはそれらの脆弱性が悪用され得ないことを示さなければならない。

AVA_VLA.2.2C 証拠資料は、識別された脆弱性について、TOEが明白な侵入攻撃に耐え得ることを正当化しなければならない。

評価者アクションエレメント：

AVA_VLA.2.1E 評価者は、提出された情報が、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。

AVA_VLA.2.2E 評価者は、開発者脆弱性分析に基づき侵入テストを行い、識別された脆弱性への対処が行われていることを保証しなければならない。

AVA_VLA.2.3E 評価者は、独立脆弱性分析を行わなければならない。

AVA_VLA.2.4E 評価者は、独立脆弱性分析に基づき、意図した環境において、新たに識別された脆弱性が悪用され得るかどうかを決定するため、独立侵入テストを実施しなければならない。

AVA_VLA.2.5E 評価者は、低い攻撃能力を持つ攻撃者による侵入攻撃にTOEが耐えられるこ

とを決定しなければならない。

評価保証レベル (EAL) に応じた評価対象物

濃色にいくほど必要とされる情報 (要件) が多い。(視覚的に理解できるように表現したもの)

EAL	評価に必要な情報										
	FS	HLD	LLD	IMP	TE	CM	LC	GD	DEL	IGS	VLA
1											
2											
3											
4											
5											
6											
7											

FS: 機能仕様
HLD: 上位レベル設計書
LLD: 下位レベル設計書
IMP: ソースコード
TE: テストに関する文書
CM: TOEの構成管理
LC: 開発環境、開発工程
GD: 利用者・管理者へ提供するガイダンス文書
DEL: 開発元から利用者への配付
IGS: 利用者における導入、起動
VLA: 脆弱性分析、誤使用分析、隠れチャネル分析書

ISO 15408に基づくセキュリティ評価の効果

開発者・運用者が宣言したセキュリティ目標（特に、セキュリティ機能）が脅威などに十分対抗できることが確認できる。

セキュリティ機能が正確、かつ、有効に機能するように実装されていることが確認できる。（利用されるような脆弱性は存在しない。）

セキュリティ機能が有効に動作するための前提条件が、マニュアルに記載されていることが確認できる。

製品／情報システムのセキュリティは

大丈夫！

セキュリティ評価の対象　(いずれもJIS X 5070の定義による)

IT製品:

単独での使用又は様々なシステム内への組込みを目的に設計された機能性を提供するITのソフトウェア、ファームウェア、及び/又はハードウェアの集まり。

ITシステム:

特定の目的及び運用動作環境を伴う特定のIT設備。

プロテクションプロファイル:

ある評価対象の分野に関して、利用者の要求を満たす、実装に依存しないセキュリティ要件を記述した文書。

セキュリティターゲット:(日本固有の制度)

識別されたTOEの評価に用いられるセキュリティ要件及び仕様を記述した文書。

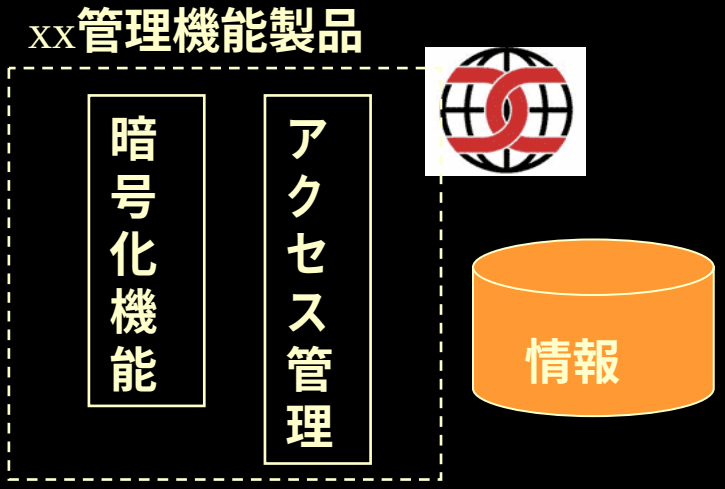
情報製品のセキュリティ評価

xx管理機能製品の開発

↓

セキュリティ評価認証

製品としてセキュリティが大丈夫であることを確認する

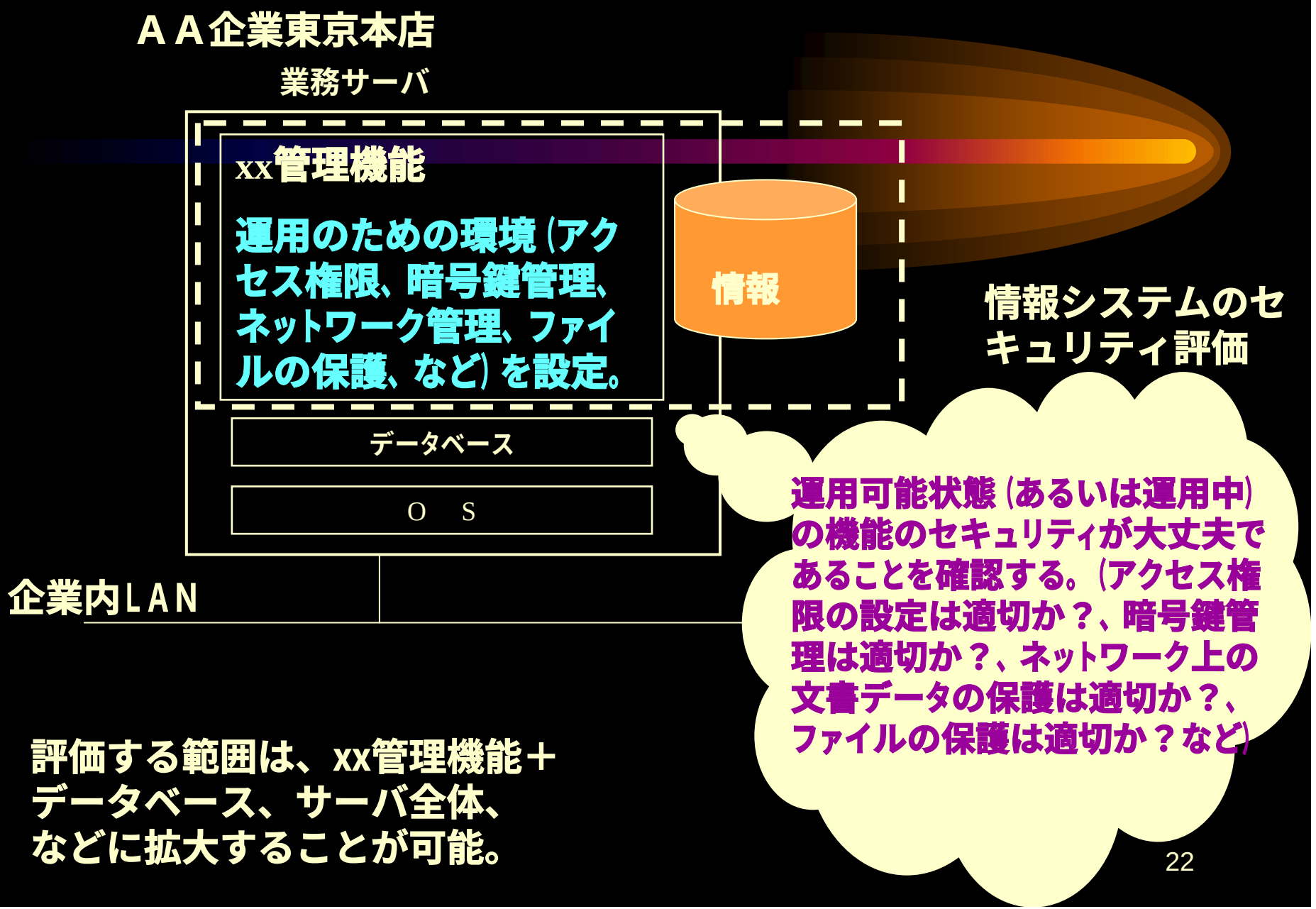


前提:

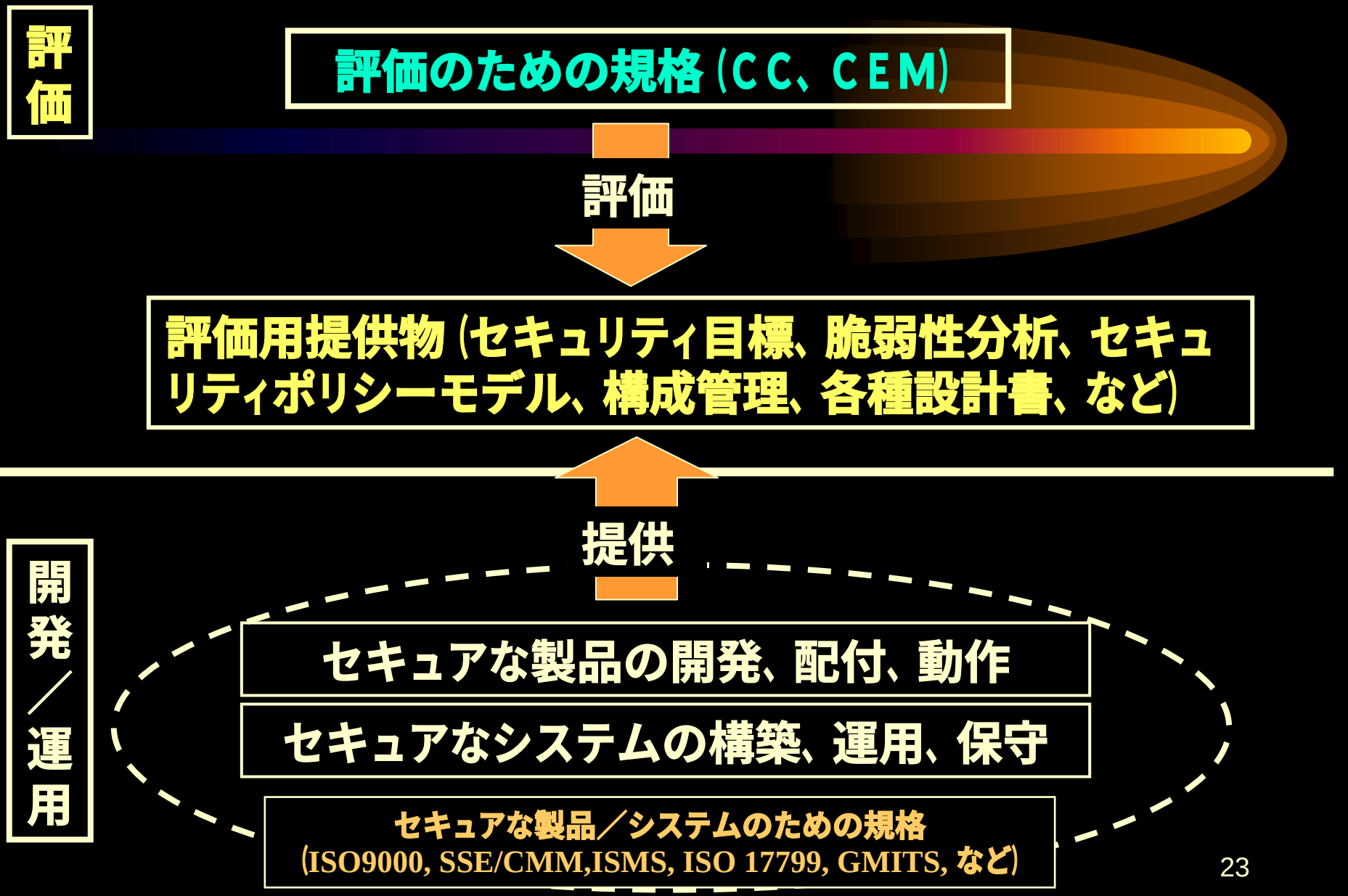
-アクセス権限設定は適切に行う。

- 暗号鍵の管理は適切に行う。
- ネットワークの管理は適切に行う。

情報システムのセキュリティ評価



評価の位置づけ


評価
評価のための規格（CC、CEM）
評価
評価用提供物（セキュリティ目標、脆弱性分析、セキュリティポリシーモデル、構成管理、各種設計書、など）
提供
開発／運用
セキュアな製品の開発、配付、動作
セキュアなシステムの構築、運用、保守
セキュアな製品／システムのための規格
（ISO9000, SSE/CMM,ISMS, ISO 17799, GMITS, など）

共通評価方法論(ISO 18045: CEM)

- ◆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～EAL4までの保証要件の評価用ガイダンス

事例

AVA_VLA.2 独立脆弱性テスト

評価者アクションエレメント：

AVA_VLA.2.1E 評価者は、提出された情報が、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。

評価者アクションエレメントに対して
CEMに具体的な評価方法を規定

AVA_VLA.2-2 評価者は、識別された各脆弱性が記述されていること及びTOE の意図する環境でそれが悪用されることがない理由に対する根拠が示されていることを決定するために、開発者の脆弱性分析を検査しなければならない。

脆弱性は、次の1 つまたはいくつかの条件が存在する場合、悪用される可能性がないと呼ばれる。

a) （IT またはIT 以外の）環境のセキュリティ機能または手段が意図する環境の脆弱性の悪用を阻止する。例えば、TOE への物理的アクセスを許可利用者だけに制限することにより、効果的にTOE の脆弱性が改ざんに悪用されないようにすることができる。

b) 脆弱性は、悪用可能であるが、攻撃能力が中程度または高い攻撃者のみが悪用可能。例えば、セションハイジャック攻撃への分散TOE の脆弱性は、低を超えた攻撃能力を必要とする。ただし、そのような脆弱性は、残存脆弱性としてETR に報告される。

以下、省略

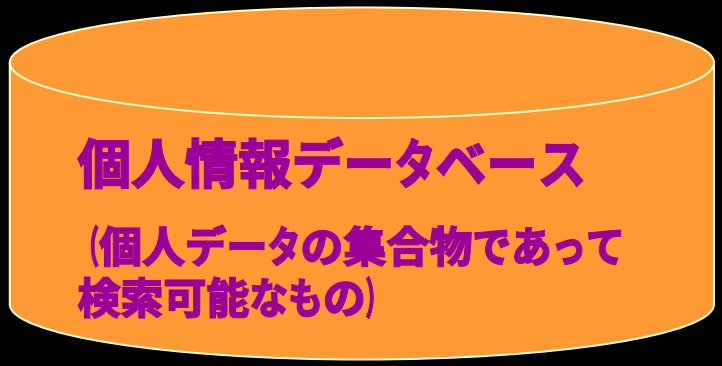
２．個人情報保護法対策としてのセキュリティ評価

「個人情報の保護に関する法律」とは

個人情報取扱事業者の義務等（第４章）が平成１７年４月から施行

個人情報取扱事業者

政令で定める件数（５０００件）以上の個人情報で構成される個人情報データベース等を事業の用に供している者



個人情報：生存する個人に関する情報であって、特定の個人を識別可能なもの（他の情報と容易に照合でき、それにより特定の個人を認識できることとなるものを含む。）（第２条第１項）

従業員、その家族、取引先企業などのインハウス情報を含む。

個人情報取扱事業者の義務等

・利用目的に関わる事項

・データ内容の正確性に関わるもの

・安全管理措置、従業者・委託先の監督

①安全管理措置

個人データの漏洩、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。（第２０条）

②従業者、委託先に個人データを取り扱わせる場合

・従業者を監督する義務（第２１条）

・委託先を監督する義務（第２２条）

企業活動にとっての「個人情報保護法」

コンプライアンス（法令遵守）：基本的人権の尊重

- 事業者規制法：違反した場合に是正勧告、従わなければ罰金。
- 事故が発生すると、民事上の損害賠償請求に発展。例：氏名/住所/本籍：30万円以上、顔写真/履歴書：平均140万円
- 同時に、消費者の事業者に対する信頼が損なわれ、企業の売り上げ低下。

CSR (Corporate Social Responsibility；　社会的責任）

- 情報システムは社会基盤。その基盤への侵害（基本的人権の侵害、フィッシング詐欺、ICカード偽造、など）対処は社会責任。
- 情報開示は企業の義務。このため、リスク情報の開示（リスク対策要）を求められる。
- リスク対策は消費者の信頼を得る上で必須

情報は企業資産

- 情報は人／もの／金を支える。適切な企業資産の管理が企業利益を生む。
- 個人情報の適切な管理は企業の利益に直結。誤れば、影響が甚大であり、経営破たんに直結。

適切な個人情報の管理を行わないことは、企業経営を放棄することと同義。

適切な「個人情報」の管理を検証（セキュリティ評価）することの意義

事業者は安全管理に係わる契約責任

＝顧客は、事故発生の事実と被害内容を主張すればいい。事業者は契約上の義務違反や注意義務違反が無い事を立証しなければならない。

従来は、被害者が被害内容と違法行為の事実を立証しなければならなかった。（プライバシー侵害を理由とする不法行為）

適切な管理を行う事業者には、消費者からの信頼が高まる。

積極的に、適切な管理状況にあることを広報することが、経営上必要となる。

個人情報漏洩事故の大部分は顧客からの通報で発覚。修復は不可能。

事故が発生しないことを常に検証することは企業活動の基本である。

「個人情報」の管理に問題が無い事を継続的に検証し、結果を広報

＝

セキュリティ評価

さらに、適切な「個人情報」の管理のためのセキュリティ評価の意義

企業活動の利便性や作業効率とのバランスを踏まえた情報管理

↓

リスクに応じた必要最小限の情報管理を実施

情報は経営資産であるから、事故前提のアプローチはあたりまえ

企業資産の管理は経営活動

↓

情報管理の内容はすべての関係者が誤りなく理解

セキュリティ評価

適切な情報管理目標（セキュリティターゲット）の設定とその妥当性の検証

正確な情報管理内容の規定（セキュリティターゲット）と実態の検証（TOE評価）

適切な個人情報管理のためのセキュリティ評価　事例

個人情報の取り扱いの明確化

個人情報の棚卸し
(顧客情報、採用時の応募者情報、他インハウス情報、など)

個人情報の企業への受け入れ
(Webサーバ、電話、Fax,郵便、書類持参、など)

個人情報の保管
(サーバのデータベース、バックアップ、コピー、ダウンロードPC、など)

個人情報の処理
(業務サーバ、他のサーバ/クライアント、ネットワーク回線、印刷、など)

個人情報の廃棄
(記憶媒体)

攻撃

- システムの脆弱性を利用してシステムに侵入
- ルート権限を奪取
- 侵入の痕跡を抹消
- 攻撃用コマンドを入力（例えば、クレジットカード番号を探し出すために、Visa/Mastercard などの文字列を含むファイルを検索
- 必要な情報を入手
- 情報入手の痕跡を抹消

利用できる脆弱性は？

ルート権限奪取阻止対策の十分性は？

データベース構造の脆弱性は？

データベースアクセス権限の妥当性は？

個人情報の取り扱いシステム評価のための保証要件　事例

保証コンポーネント	要求概要	適用の可否
ACM_CAP.1	TOE構成要素の識別	関連資材の識別なので工数上の問題は稀少
ADO_IGS.1	セキュアな構築と運用	インテグレーション関連文書と運用手引書
ADV_FSP.1	TSFとその外部インタフェース	運用/操作/利用手引書
ADV_RCR.1	TOE要約仕様とFSPとの対応	作成工数は稀少
AGD_ADM.1	運用/操作手引書	既存の文書
AGD_USR.1	利用手引書	既存の文書
ATE_IND.1	評価者によるセキュリティ機能テスト	評価者の技量
AVA_VLA.2	評価者による独立脆弱性テストの実施	ADV_HLD.2, ADV_IMP.1, ADV_LLD.1の依存性は無視 代わるものを考慮要
ST	個人情報の処理空間をTOE	TOEの識別は容易

基本的には、システムの開発と運用で作成/使用する文書に基いて評価が可能

「本当に“個人情報保護法”への対処は大丈夫？」に応えるアプローチ方法

運用システム

①セキュリティ目標(ST)の作成

運用システムの構成及び業務に基づいてSTを作成

・個人情報の処理および管理に関わる脅威（リスク）の識別

・個人情報に関わる問題を発生させないためのセキュリティ対策

・必要なセキュリティ機能

③評価結果を運用システムに反映

例：パスワード管理機能を追加

アクセス管理機能が持つアクセス権限に関わる規則を修正

④評価のために必要な資材を準備

例：

・運用システムが提供するセキュリティ機能仕様書（パスワードの管理機能、アクセス管理機能のアクセス権限、など）

・システムへの侵入テストの結果報告書

評価

②セキュリティ目標(ST)の規定内容の妥当性を検証

・セキュリティ対策は必要かつ十分か

・セキュリティ機能は正確に規定されているか

例：

「パスワードは他人に推測されないようなものを設定し、定期的に変更すること。」（利用規程」

⇒評価の結果、規程だけでは不十分。パスワードの構文を既定し、適合しないものは登録不可とする機能を導入要。変更も、強制的に実施できるような機能を導入要。

⑤運用システムがセキュリティ目標に準拠していることを検証

個人情報処理システムの評価を支援するために、

「個人情報処理システム用セキュリティターゲット 」
を公開している。

http://www.ipa.go.jp/security/jisec/jisec_system_st.html

３．ITセキュリティ評価・認証制度

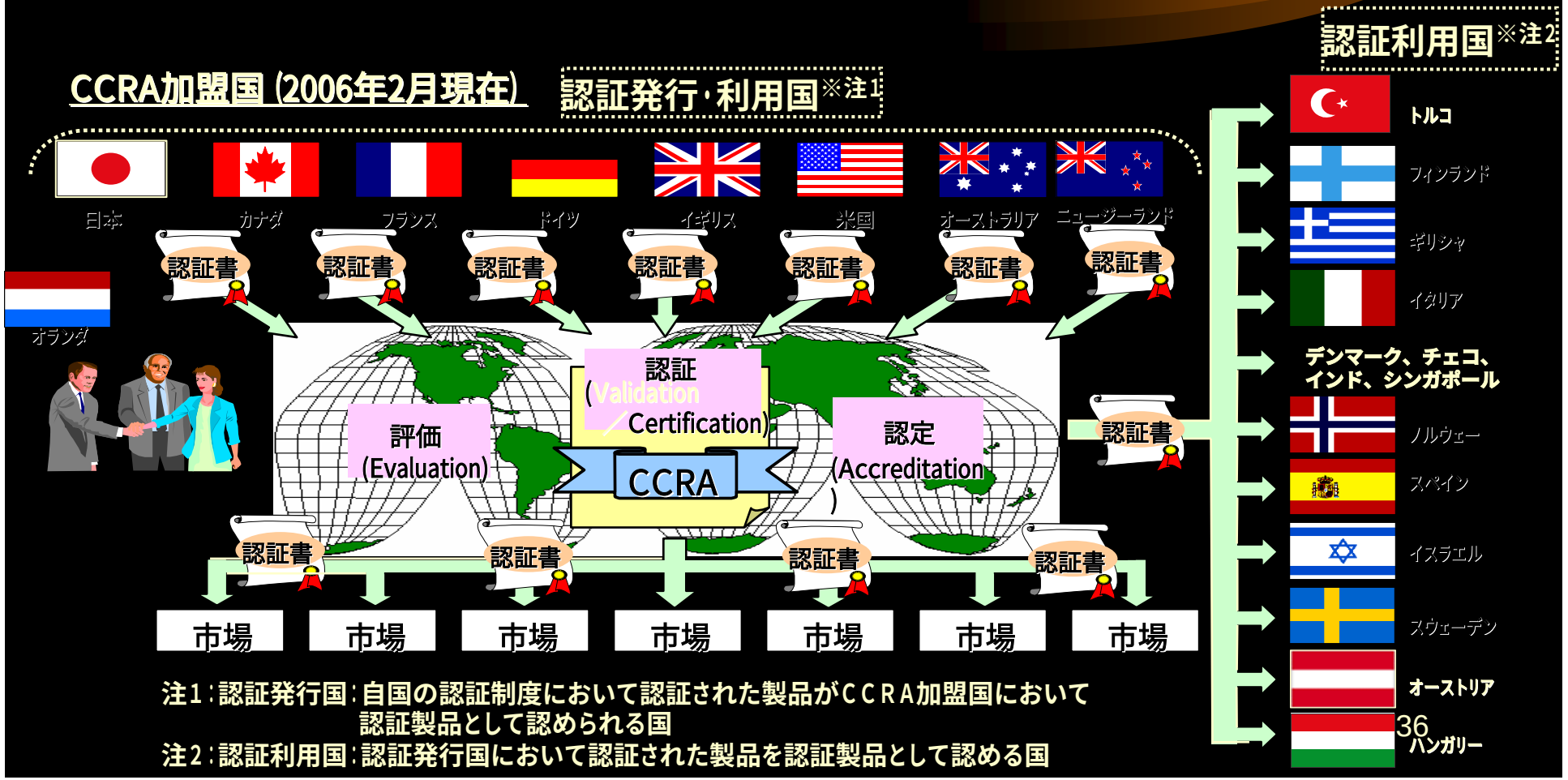
ITセキュリティ評価及び認証制度とは？

情報処理の促進に関する法律（昭和45年5月22日法律第90号)第20条第5項（情報処理に関する安全性及び信頼性の確保を図るため、情報処理システムに関する技術上の評価を行うこと。）に基づき経済産業省の監督のもと、独立行政法人情報処理推進機構(IPA)がCCRA（コモンクライテリア承認アレンジメント）及び関連する国際基準に適合させたITセキュリティ評価及び認証を行う制度。

相互承認アレンジメント
（CCRA(Common Criteria Recognition Arrangement)）とは

■ 参加国のITセキュリティ評価・認証制度の下で評価・認証されたIT製品を、受入れのみを行う参加国も含むすべての参加国で、その国内で評価・認証されたIT製品と同等に扱うことに同意するものである。

条件：
- 規格としてCCとCEMを利用。
- 対象はEAL4+ ALC_FLRまでのIT製品
- CC認証書、認証報告書、STを公開。



注1：認証発行国：自国の認証制度において認証された製品がＣＣＲＡ加盟国において認証製品として認められる国

注2：認証利用国：認証発行国において認証された製品を認証製品として認める国

日本の事情

平成13年3月の関係府省申し合わせ

政府利用方針（ポイント）

平成13年3月29日 行政情報化推進各省庁連絡会議了承

各省庁は、セキュリティに関する信頼度の高い情報システムの構築を図る観点から、今後の情報システムの構築に当たっては、可能な限り、次のような方法等により、ISO/IEC15408に基づいて評価又は認証された製品等の利用を推進するものとする。

・調達仕様書において、セキュリティ機能の全部又は一部がISO/IEC15408に基づいて評価・認証された製品等で実現されることを入札要件とする方法

政府の政策

内閣官房より、
「政府機関の情報セキュリティ対策のための統一基準（2005年12月版［全体版初版］）」
が公表（12月13日）されました。（http://www.bits.go.jp/active/general/feedback.html）

本基準は、今後政府調達に反映されます。特に、CC評価認証に関連する箇所は以下です。

4．3.1情報システムのセキュリティ要件
基本遵守事項（必須要件）として、
情報システムの開発に際しては、CCによるST評価確認を受けることが求められます。「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に重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST: Security Target）のST評価・ST確認を受けること。」

強化遵守事項（推奨）として、
構築する情報システムのために調達する製品はCC認証を取得していること。（概要）

6．1.1　機器等の購入
基本遵守事項（必須要件）として、
総合評価落札方式により購入する場合、CC認証の取得を評価項目として活用すること。（概要）

6．1.3　ソフトウェア開発
基本遵守事項（必須要件）として、
ソフトウェアの開発に際しては、CCによるST評価確認を受けること。（概要）

アメリカの事情

政府システムに適用する製品の調達要件の内容

●国家の安全に係わる情報の処理を行うシステム（注：国防総省(DoD)が所有または管理するシステムを実際は意味している。）で使用する製品に対して、2つの要件がある。

- 2002年7月以降、製品が情報を入力、処理、保管（記憶）、表示、通信する機能のいずれかを持っている場合は、当該製品をシステムで使用する前に、必ず認証を得なければならない。

(http://www.nstissc.gov/Assets/pdf/nstissp_11_fs.pdf)

- NSAがPPを規定している製品種別(OS，ファイアウォール、IDSなど)に該当する製品の場合には、そのPPに適合していなければならない。

(http://www.dtic.mil/whs/directives/corres/html/85001.htm)

●国家の安全に係わる情報以外の情報を処理している政府システムに対しては、認証製品の適用が好ましいとの指針が提示されている。

(http://www.nstissc.gov/Assets/pdf/nstissp_11_fs.pdf)

韓国事情

現在は、CCRAに認証国として加盟の準備中。

認証状況

年度	日本			韓国*		
	ST確認	CC認証	日本計	Domestic	CC	韓国計
1998	0	0	0	1	0	1
1999	0	0	0	2	0	2
2000	0	0	0	5	0	5
2001	0	0	0	10	0	10
2002	3	2	5	21	0	21
2003	6	5	11	17	3	20
2004	15	17	32	8	4	12
計	24	24	48	64	7	71
	(日本は2005.3.31.)			(* How dose IT security certificate affect business and technology of IT security in Koria? (2004 ICCC))		

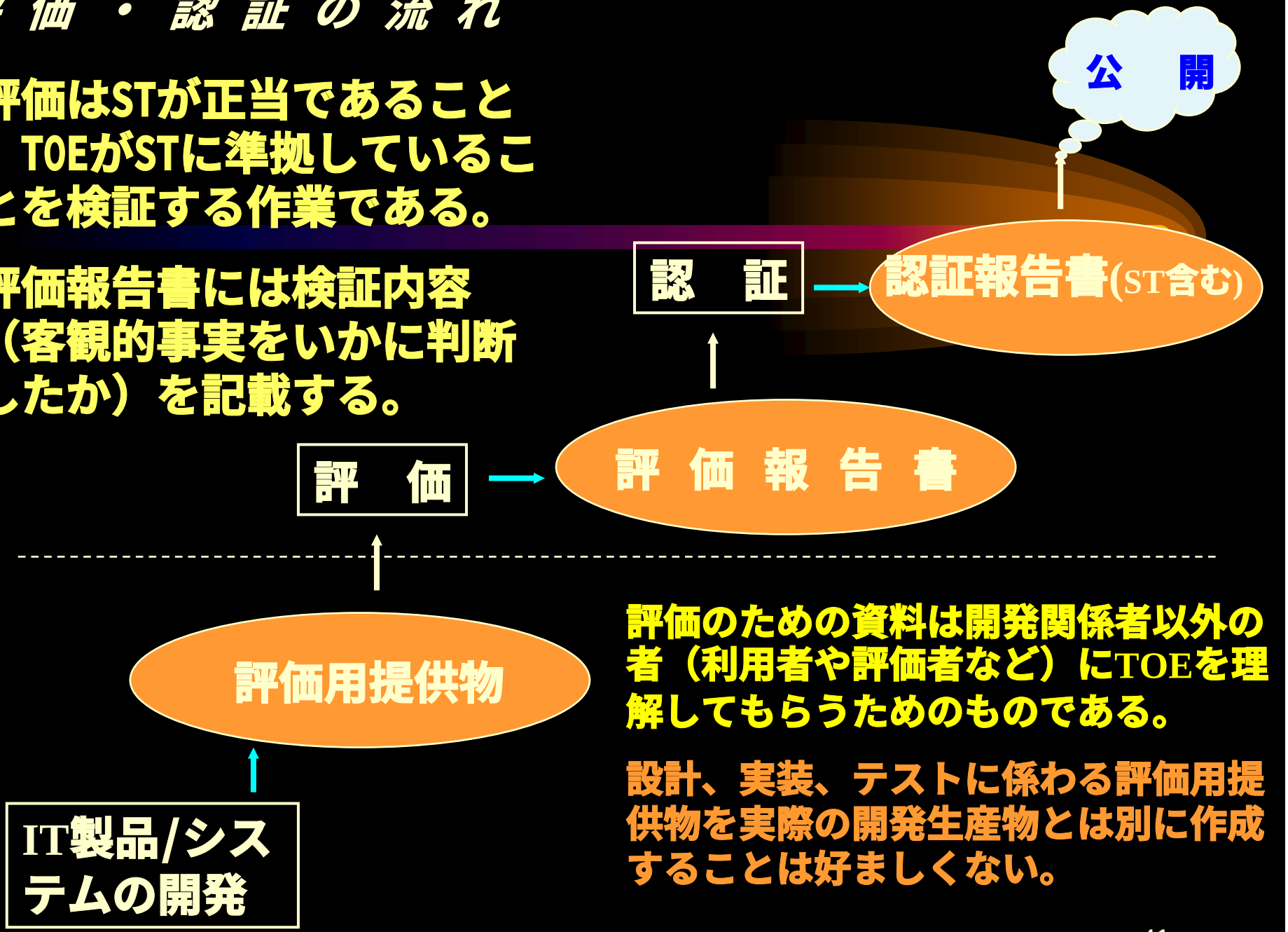
・政府関連システム（軍関連を含む）に対して、セキュリティ認証製品の適用が法的に義務づけられている。ただし、現在は、強い要請というのが実情。（製品の品揃えが可能なファイアウォールやIDSは必須になっている。）

→ **CCRA加盟（2006年春予定）以降は、実質的に、政府関連システムで使用する製品のCC認証が必須になる。**

評 価 ・ 認 証 の 流 れ

評価はSTが正当であること、TOEがSTに準拠していることを検証する作業である。

評価報告書には検証内容（客観的事実をいかに判断したか）を記載する。



評価のための資料は開発関係者以外の者（利用者や評価者など）にTOEを理解してもらうためのものである。

設計、実装、テストに係わる評価用提供物を実際の開発生産物とは別に作成することは好ましくない。

CC認証製品の公開

利用者

CCプロジェクトのWebページ
www.commoncriteriaportal.org

CCRA加盟認証機関の
CC認証製品リスト

CC Certified Product

- -Product Name
- -Product type
- -Vendor
- -Contact
- -Conformance claim
- -PP Identifier
- -Certification date
- -Evaluation facility
- -TOE Description

評価･認証のための規格

認証機関より公開

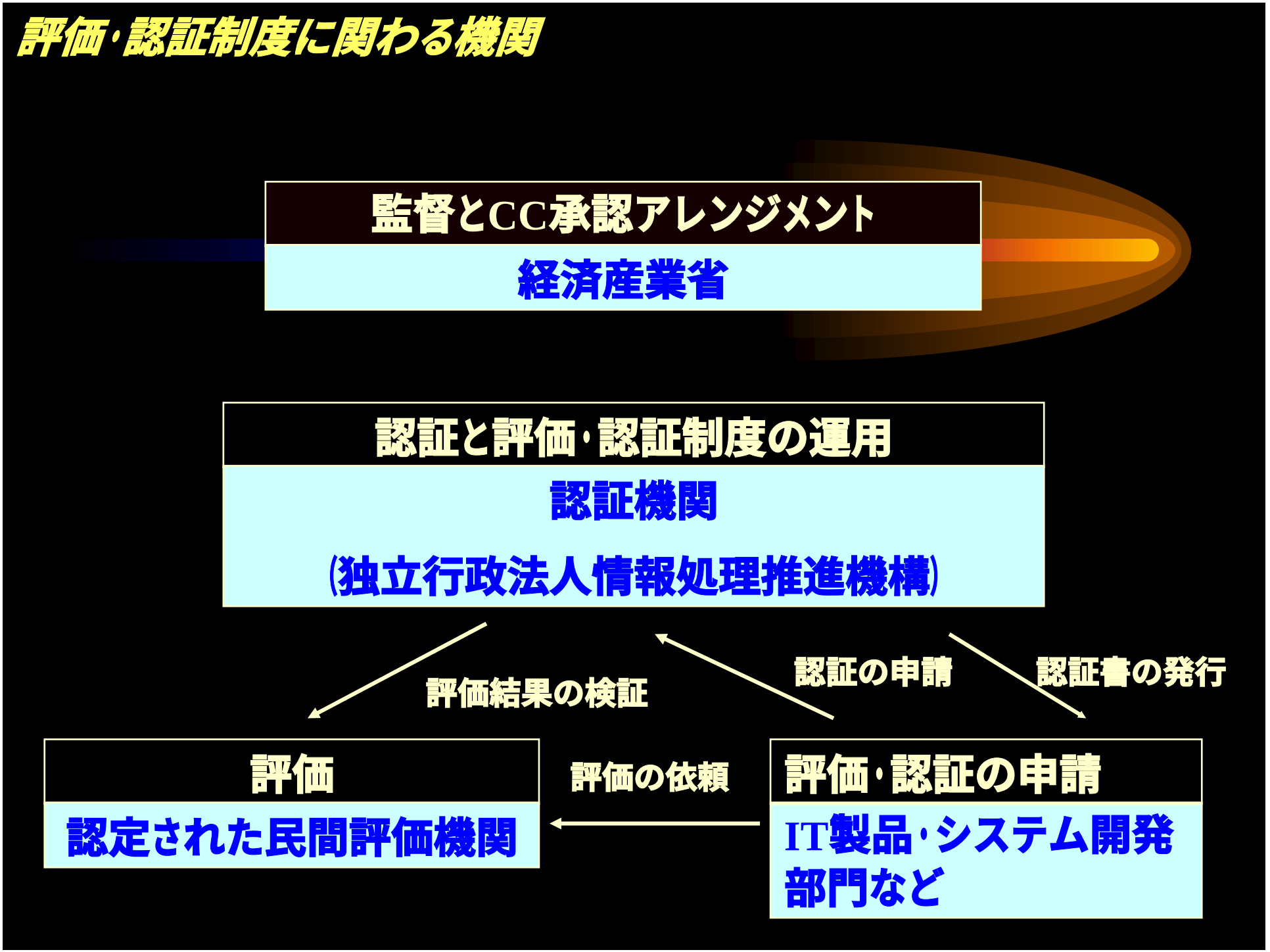
①ITセキュリティ評価基準

- ISO/IEC 15408　Evaluation criteria for IT security
- JIS X 5070　セキュリティ技術 ― 情報技術セキュリティの評価基準
- Common Criteria for Information Technology Security Evaluation
- 認証機関が公開する、上記の規格の翻訳文書
- 認証機関が公開する、評価基準補足文書
  （CCIMB Interpretations- 0407、補足-0210第2版、補足-0407）

②ITセキュリティ評価方法

- Common Methodology for Information Technology Security Evaluation
- TR　X0049　情報技術セキュリティ評価のための共通方法
- 認証機関が公開する、上記の規格の翻訳文書
- 認証機関が公開する、評価方法補足文書
  （CCIMB Interpretations-0407、補足-0210第2版、補足-0407）

評価・認証制度に関わる機関



評価認証プロセス　1/3

ステップ1：評価用提供物の作成　(開発者の作業)

1．セキュリティターゲット(ST:セキュリティ目標)を作成する。

2．STで宣言した信頼性確保のために要求される評価用提供物(機能設計書、テスト仕様書、脆弱性分析書、セキュリティポリシーモデル、など)の整備や作成を実施する。

3．評価および認証を依頼する。

認証を開始するに際して、キックオフミーティングを開催(強制ではない)

- ST内容の確認
- 認証作業内容と手続きの確認
- 評価/ 認証スケジュールの確認

ステップ2：評価

システム運用者／開発者とは異なる第3者（評価者）が、提供された評価用提供物を検査する。

検査に使用する規格

- 評価基準
- 評価方法
- 補足文書

↓

評価の結果は「評価報告書」としてまとめる。

ステップ3：認証

「評価報告書」の内容が規格に準拠して正当であることを、認証機関が確認し、「認証報告書」を作成する。

評価機関、評価者、評価時期に関わらず評価結果が一致することを確保することが目的。

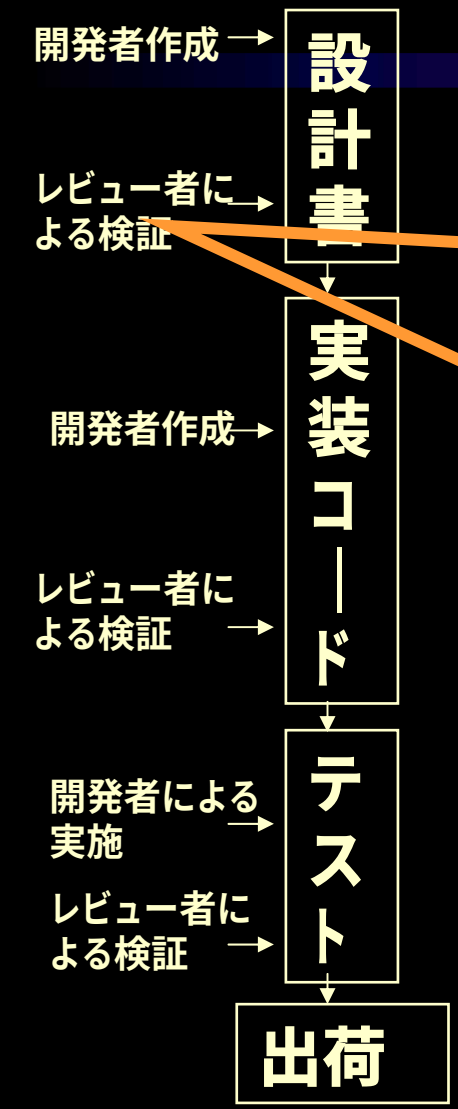
規格に適合していれば「認証書」を発行する。

YY株式会社データベース管理製品

CC認証の場合、認証報告書＋ST

開発とセキュリティ評価

【ＣＣに基くセキュリティ評価作業内容】



評価

作成に係った生産物（設計書、実装コードなど）を評価基準（ISO 15408/CC;実際は評価方法ISO 18045/CEMを使用）に基づいて検証する。

CEMに規定の例：評価者は、機能仕様が外部TOE セキュリティ機能インタフェースのすべて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。

評価者は(上記の機能設計の評価の例)；

- **機能仕様が記載されている設計書を探し、内容を理解し、**
- **外部セキュリティ機能インタフェースが記載されている箇所を識別し、**
- **上記のＣＥＭに記載の検査内容に従って検査し、**
- **検査結果を評価報告書に記載する。**

開発レビューで実施

同様の作業を、CEMの規定に従って、開発生産物に対して実施する。

４．保証継続

基本的な考え方

認証TOEの後続版において、最初の認証TOEの保証要件が維持されている場合、後続版の再評価は不要とする。この場合、後続版は維持追加情報（維持TOEの認証製品リスト）に記載し、公開する。

認証書は再発行する。

変更のあったTOEは最初のSTに記載の保証要件を満足していることを意味している。脅威や脆弱性に変化があった（あると想定される）場合には、再評価する。

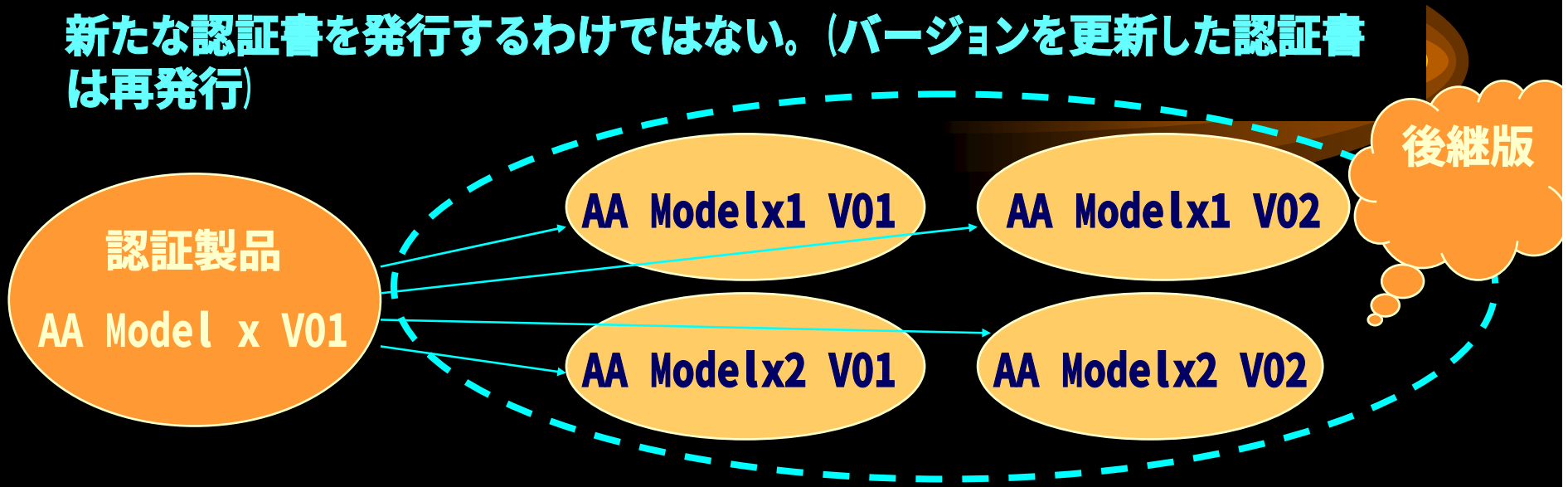
詳細は、規程「ITセキュリティ認証に係る保証継続の要件」を参照。

- CC V2.1のAMAはCC V2.2からは削除
- CCRAの保証維持の仕組みとして採用

保証継続が適用できる条件

1．認証製品の後継版に適用する。

新たな認証書を発行するわけではない。（バージョンを更新した認証書は再発行）

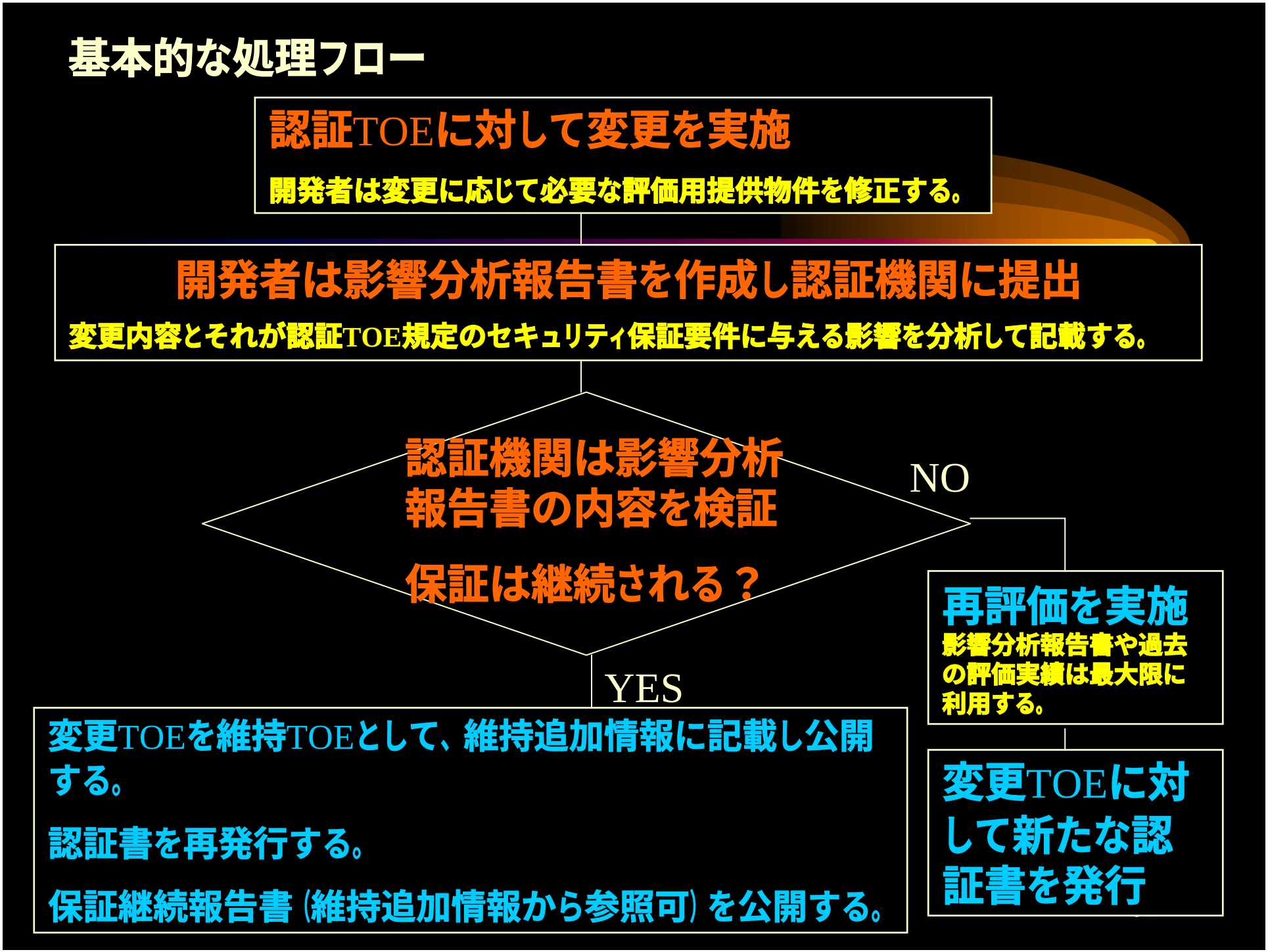


2．製品のバージョンを除いては、STの内容に変更が無い。

ST記載内容の保証が継続されることを意味している。

3．認証TOEからの変更が、認証時の評価提供物件に影響を与えない。（ただし、バージョン名称の変更とリグレッションテストの実施は除く）

基本的な処理フロー


認証TOEに対して変更を実施
開発者は変更に応じて必要な評価用提供物件を修正する。
開発者は影響分析報告書を作成し認証機関に提出
変更内容とそれが認証TOE規定のセキュリティ保証要件に与える影響を分析して記載する。
認証機関は影響分析報告書の内容を検証
保証は継続される？
NO
YES
再評価を実施
影響分析報告書や過去の評価実績は最大限に利用する。
変更TOEに対して新たな認証書を発行
変更TOEを維持TOEとして、維持追加情報に記載し公開する。
認証書を再発行する。
保証継続報告書（維持追加情報から参照可）を公開する。

影響分析報告書の概要（開発者が作成）

1．序説

認証TOE、名称、ST、関連ガイダンス文書、ETR、認証報告書など

2．変更の記述

3．影響する開発者証拠

変更が影響を与える評価用提供物件の一覧

4．証拠変更の記述

変更の内容

5．結論

各変更に対して、セキュリティ保証に与える影響の大小とその理由

リグレッションテストの結果

附属書　更新された開発者証拠

保証継続の作業フロー

ステップ1：開発者はTOEの認証時に提供した評価用提供物件を識別する。

ステップ2：開発者は変更箇所（TOE自体、開発環境など）を識別する。

ステップ3：開発者は影響分析報告書案（変更内容と影響を受ける評価用提供物件とその内容だけを記載したもの）を認証機関に提示する。

ステップ4：認証機関で保証継続の可否の一次きりわけを実施する。

ステップ5：開発者は変更を適用し、影響分析報告書を完成させる。

ステップ6：認証機関で保証継続の最終判断を行う。

ステップ7：認証機関で保証継続報告書を作成し、認証書を再発行する。

・ステップ３，４は省略も可能。

・ステップ５～ステップ７の所要期間は、影響分析報告書の内容に問題が無ければ、約２週間程度。

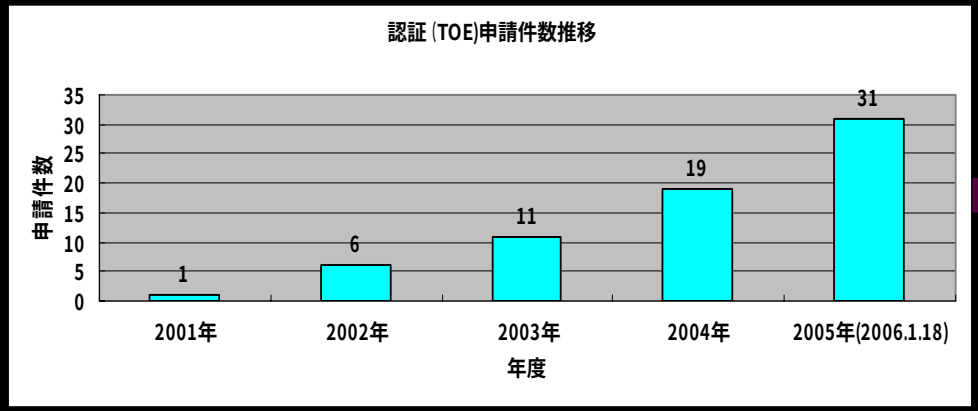
認証実績の継承についての考え方（保証継続ではない）

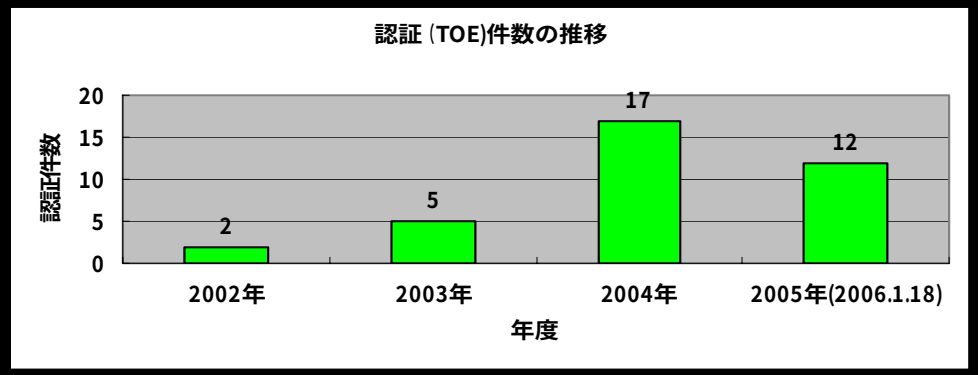
認証（＝評価結果は正当）した事実は他TOEの評価結果でも継承する。

注：ABC V1.0箇所に対する再評価を妨げるものではない

５．認証状況

認証状況





認証製品の種別

製品種別	認証件数 (18年1月20日)	17年度申請件数 (18年1月20日)
文書管理	1	1
ファイアウォール	1	1
データベース	1	2
電子申請ソフトウェア	1	0
PKI（認証局/登録局）	2	0
ICカード	3	2
デジタル複合機	24	22
デジタルカメラ	1	0
金融端末	1	0
運用システム	0	1
その他	1	1
合計	36	30

６．ST作成のポイント

Security Target （当初は、“セキュリティ目標”と解釈）

JISでは、「セキュリティ設計」

本来は？

やはり、「**セキュリティ目標**」

装備するセキュリティ機能を***正確***に表現する

パート2機能要件の操作規定を的確に行う

装備するセキュリティ機能が***必要かつ十分***である

必要性：運用に適用できる

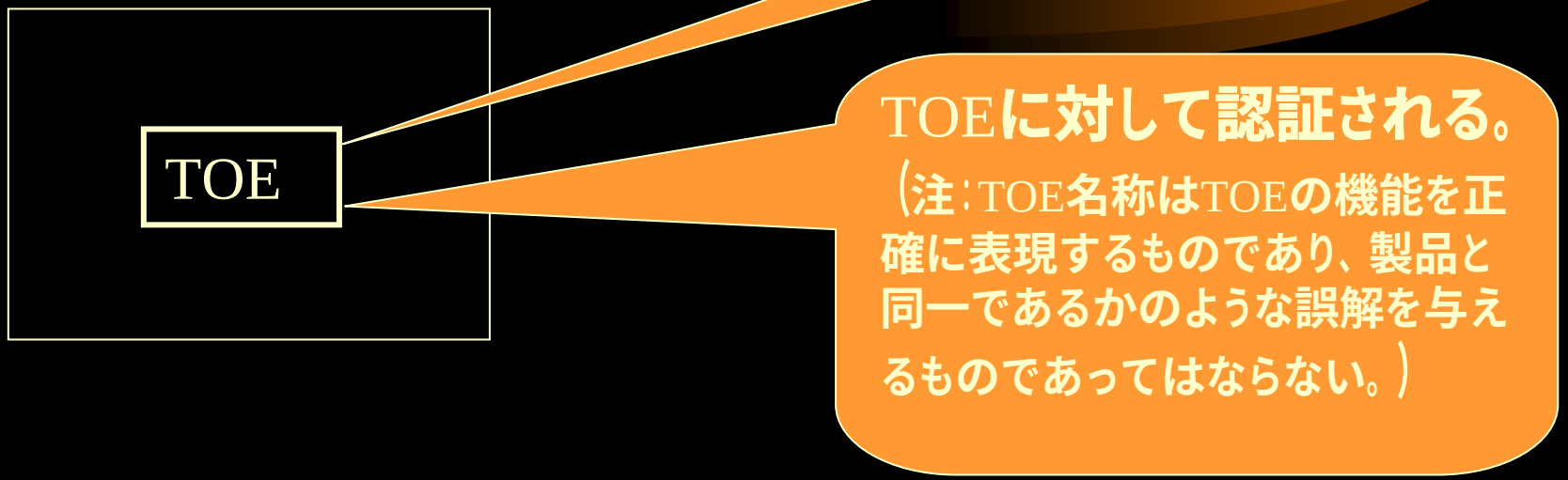
十分性：脅威に対抗できる

利用者が利用の可否を***判断***できる

一般読者が記述内容を理解できる

TOEの規定

製品≠TOEの場合



製品＝TOEが原則

- 評価はTOEの中のセキュリティ機能(TSF)に対してのみ実施する。
- 後継版に対しては保証継続の適用が可能。

（注：後続版であることが認識できるようにTOE名称を付与すること。）

セキュリティ目標(セキュリティターゲット：ＳＴ）の内容

1　セキュリティを確保する範囲（＝評価の範囲）を特定

例えば、“公開サーバ”、“企業ネットワークシステム”、など

2　セキュリティに関わる課題を記載

課題として、リスク、組織のセキュリティ方針（法律準拠など）、前提条件

3　課題を解決するためのセキュリティ対策

例えば、“利用者の本人確認”、“データに対する利用権限のチェック”、など

4　セキュリティ機能と信頼性（保証）

正確に機能や保証を記載するために、要件の記述形式を規定

上記３，４項の必要十分性の自己検証を含む

STを作成する意義は？

情報セキュリティに対する説明責任が果たせる。

必要最小限のセキュリティ対策の策定が可能になる。

ST:セキュリティ対策方針

必要十分なセキュリティ機能を明確にすることができる。

ST:セキュリティ機能要件

必要十分な信頼性を確保することができる。

ST:セキュリティ保証要件

既存の情報システムのセキュリティ問題を抽出して、最小の投資で有効な対策を策定できる。

ST:セキュリティ機能概要と現状の差分

セキュアな製品（認証製品）の有効な導入を実現できる。

基本的な考え方

原則：製品全体をTOEとする。
ただし、オプション的な機能を除外することは可。

現実には、バージョンアップによる再評価を避けるために、TOEの範囲を狭める傾向がある。（バージョンアップは保証継続で簡単に対応できる。）

製品のセキュリティ評価を行うのが目的である。

TOEは、対象機能およびプログラムを利用者が認識できなければならない。

秘密情報について

STは公開が原則（CC認証では必須）

秘密情報を含んではならない。

秘密情報の記載を要求していない。必要があれば、別資料にして、評価者に対してのみ提示。

暗号アルゴリズムの考え方

・暗号アルゴリズムの評価はCCの対象外

・選択された暗号アルゴリズムは、以下の場合に認める。

電子政府推奨暗号リストに掲載

NISTなどの信頼できる海外機関で実績

信頼できる機関で調査を実施

STの読者は？

１．TOE利用者／運用者

STによって何が評価されたのかを把握する。

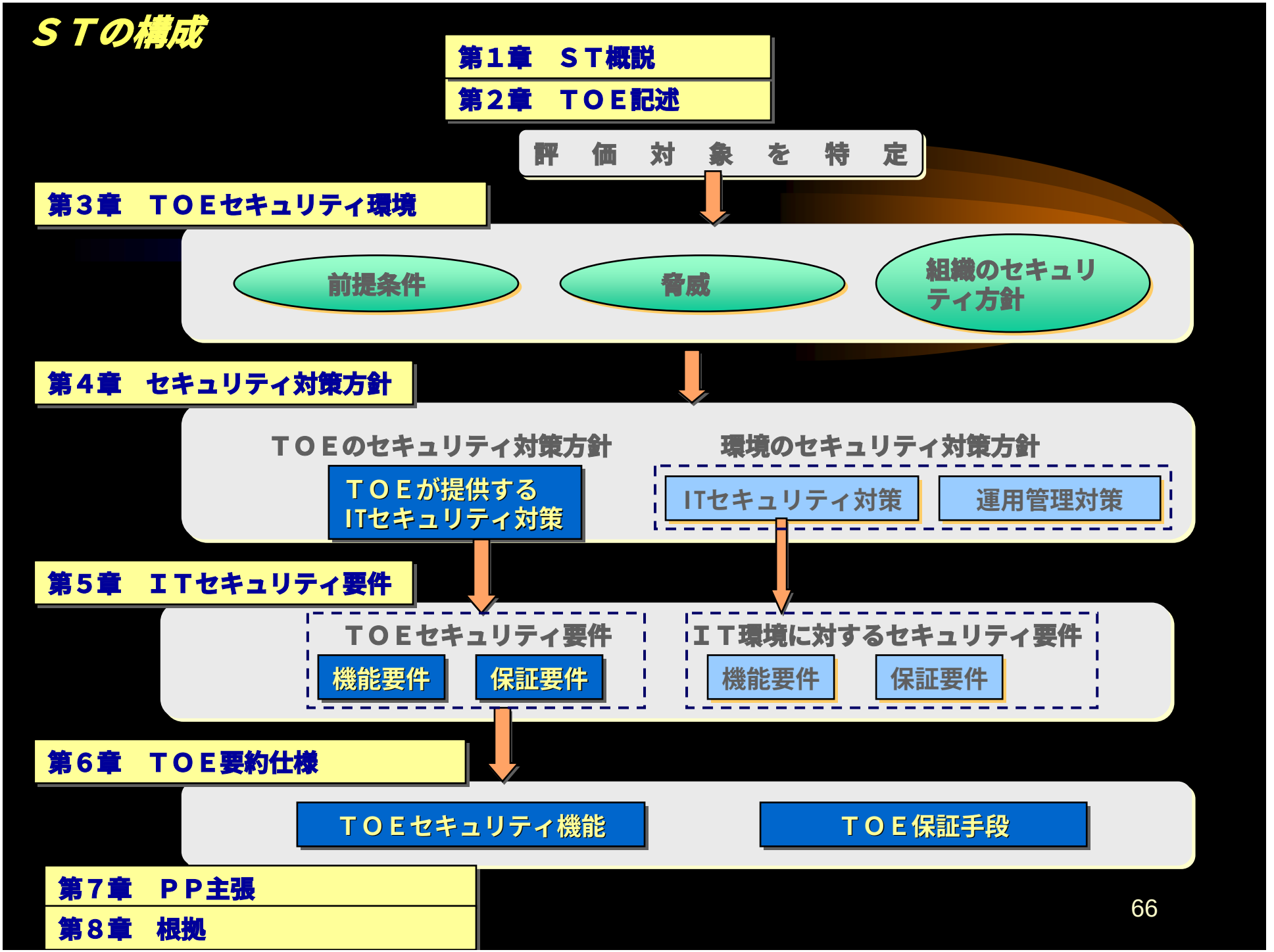
TOEのセキュリティ環境（保護資産、対抗する脅威、前提、組織のセキュリティ方針）とセキュリティ機能、および、保証内容を理解することが主な目的。

２．評価者

STによって何を評価すべきかを把握する。

TOEのセキュリティ特性や評価の範囲について、開発者と評価者が正しく認識し合意することが目的。

ＳＴの構成


第１章　ＳＴ概説
第２章　ＴＯＥ記述
評　価　対　象　を　特　定
第３章　ＴＯＥセキュリティ環境
前提条件
脅威
組織のセキュリティ方針
第４章　セキュリティ対策方針
ＴＯＥのセキュリティ対策方針
ＴＯＥが提供するITセキュリティ対策
環境のセキュリティ対策方針
ITセキュリティ対策
運用管理対策
第５章　ＩＴセキュリティ要件
ＴＯＥセキュリティ要件
機能要件
保証要件
ＩＴ環境に対するセキュリティ要件
機能要件
保証要件
第６章　ＴＯＥ要約仕様
ＴＯＥセキュリティ機能
ＴＯＥ保証手段
第７章　ＰＰ主張
第８章　根拠

1． ST概説

ポイント

・STの識別

タイトル、バージョン、作成者、発行日付

・TOEの識別

名称、バージョン、開発者

注：製品名称をTOE名称とする場合で、TOEが製品の一部の場合はその旨が明確にわかるようにする。

・TOE概説（←*要求する機能、セキュリティ、IT基盤を満たすTOEを選択したい*）

認証製品リストの抄録として利用。利用者が製品選択時に利用できる内容の情報を記載する。

利用内容と主なセキュリティ機能、TOE種別＊（OS、データベース、ファイアウォール、ICカード、など）、必要なTOE外のハードやソフト

＊TOE記述に記載

・適合主張（←*適合条件、信頼性の程度を理解したい*）

適合するCC（保証要件）、PP、パッケージ

2． TOE記述（←*利用者がTOEの機能およびそのセキュリティを理解したい*）

ポイント：

・TOEの範囲を特定

物理的な範囲と境界：TOEを構成するハード、ソフト、ファームのパーツ

論理的な範囲と境界：TOEが提供する機能、TOEのセキュリティ機能がカバーする範囲

TOEを利用者が、物理的、論理的に識別できることが必須。

・TOEの説明

以降の規定で参照するTOEに関わる事項（機能、構成、使用方法、使用環境など）については、本項で説明しておく。

・TOEが提供するセキュリティ機能の簡潔な要約

セキュリティ機能の概要が把握できるものにする。（読者が概要を理解できる程度の詳細度）

・TOEが提供するガイダンス文書

ガイダンス文書名と記載概要

3． TOEセキュリティ環境（←*利用者が現状の運用環境を満たすTOEを選択したい*）

目的：セキュリティに関わる与件を規定

注：規定の過程および内容はCCの範囲外（ただし、規定内容に矛盾が無いこと、および、CC規定項目の形式に従うこと）

ポイント（必ずしも下記の全ての項目を規定する必要は無い）

- **前提条件**（←*TOEが現状の運用環境に適合するか判断したい*）

  前提条件が利用者の意図する利用環境に対して妥当であるか否かを判断できる内容にする。 環境で対応することになる。

- **脅威**（←*TOEが現状のセキュリティ問題を解決してくれるかを判断したい*）

  セキュリティ対策の策定のために必要な内容を識別する。

- **組織のセキュリティ方針**（←*TOEが組織のセキュリティ要求事項を解決してくれるかを判断したい*）

  セキュリティ対策の策定に必要な詳細度の情報を記載する。

個別の与件（脅威、組織のセキュリティ方針、前提）を規定する前に、与件の考え方を記述することを推奨

（要件ではない）

記述する内容は以下。

- 何を保護するのか（保護対象資産）。
- 各保護対象資産はセキュリティ上何が（機密性、完全性、可用性、責任追跡性、など）求められるのか。
- 想定する攻撃力（許容する攻撃力）はどのようなものか。
- 各保護資産はどのような条件で、誰が利用/管理するのか。

前提条件：

ここで規定（ TOEのセキュアな運用に係る事項）の下でTOEは動作。規定事項の実現はTOEの責任範囲外。（TOE自体の動作条件の規程は不要）

TOEの環境で実現する。実現が無理なことは規定しない。

組織のセキュリティ方針：

脅威以外の理由でセキュリティ装備を必要とする要求事項を規定。
利用者からのRFPなどが例。

他に、TOE機能をセキュリティ機能として評価したい、個人情報保護法などの法律や規則などが想定される。

脅威：

保護すべき資産を識別。この資産に対して想定される脅威を漏れなく列挙する。

対策の必要性と十分性が検証できるだけの具体的（脅威エージェント、攻撃方法など）な記載が必要。

次のセキュリティ対策で必要かつ十分性を説明するに必要な情報が必要。

組織のセキュリティ方針には、脅威から導かれる事項は記載しない。

組織のセキュリティ方針に；

「＊＊データの機密性を確保すること。」

本要求は、機密性を確保できないような脅威が存在するための要求であるから、脅威として記載する。これによって、セキュリティ対策の必要性が理解できる。

注：＊＊データがTOEの保護資産ではなく、他の機能の保護資産である場合は、この限りではない。

脅威、前提条件、組織のセキュリティ方針を策定するためのアプローチ方法の事例

ステップ１：TOE（評価対象）自身の機能として、セキュリティ機能（暗号、通信データのフィルタリング、署名機能、など）を提供する場合は、「方針（OSP）」として規定する。この場合、準拠すべき標準規格などがあれば規定する。

ステップ２：TOEが正常に動作するために保護しなければならない資産（利用者データ、ハードウェア、など）を識別する。

ステップ３：識別した資産に関連する脅威を抽出する。

参考情報として、「脅威データベース」を認証機関より公開している。

ステップ４：TOEの開発/インテグレーション環境に関連する脅威を抽出する。（CC2.1では必須ではない。）

ステップ５：抽出した脅威を分析し、下記に分類する。

a) TOEにセキュリティ機能を装備して対抗する。

b) TOEでは対抗する機能は提供しない（提供する必要が無いので）。関連する製品（OSやミドルウェアなど）のセキュリティ機能を利用する。

c) TOEでは対抗する機能は提供しない（提供する必要が無いので）。運用（教育・訓練、契約、など）、または、物理的な装備（ハードウェア特性、施設管理、など）で対処する。

d) 保証要件に反映する。（ステップ４で抽出された脅威。CC2.1では必須ではない。）

ステップ６：

a) に係わる脅威は、「TOEへの脅威」として規定する。

b) に係わる利用機能を、「前提」（IT環境）として規定する。

c) に係わる対処方法を、「前提」（運用管理）として規定する。

d) に係わる脅威は、「開発環境への脅威」として規定する。（CC2.1では必須ではない。）

4． セキュリティ対策方針

ポイント

- **対策方針の記載**

  セキュリティ環境で記載の与件への対策は何かと、その目的を記載する。

  TOEガイダンス文書記載内容は把握できる程度の知識保有の利用者が理解できる内容であること。（用語の定義に注意。セキュリティ環境の繰り返しはセキュリティ対策方針としては不適切。）

- **脅威の除去、軽減、緩和に貢献**

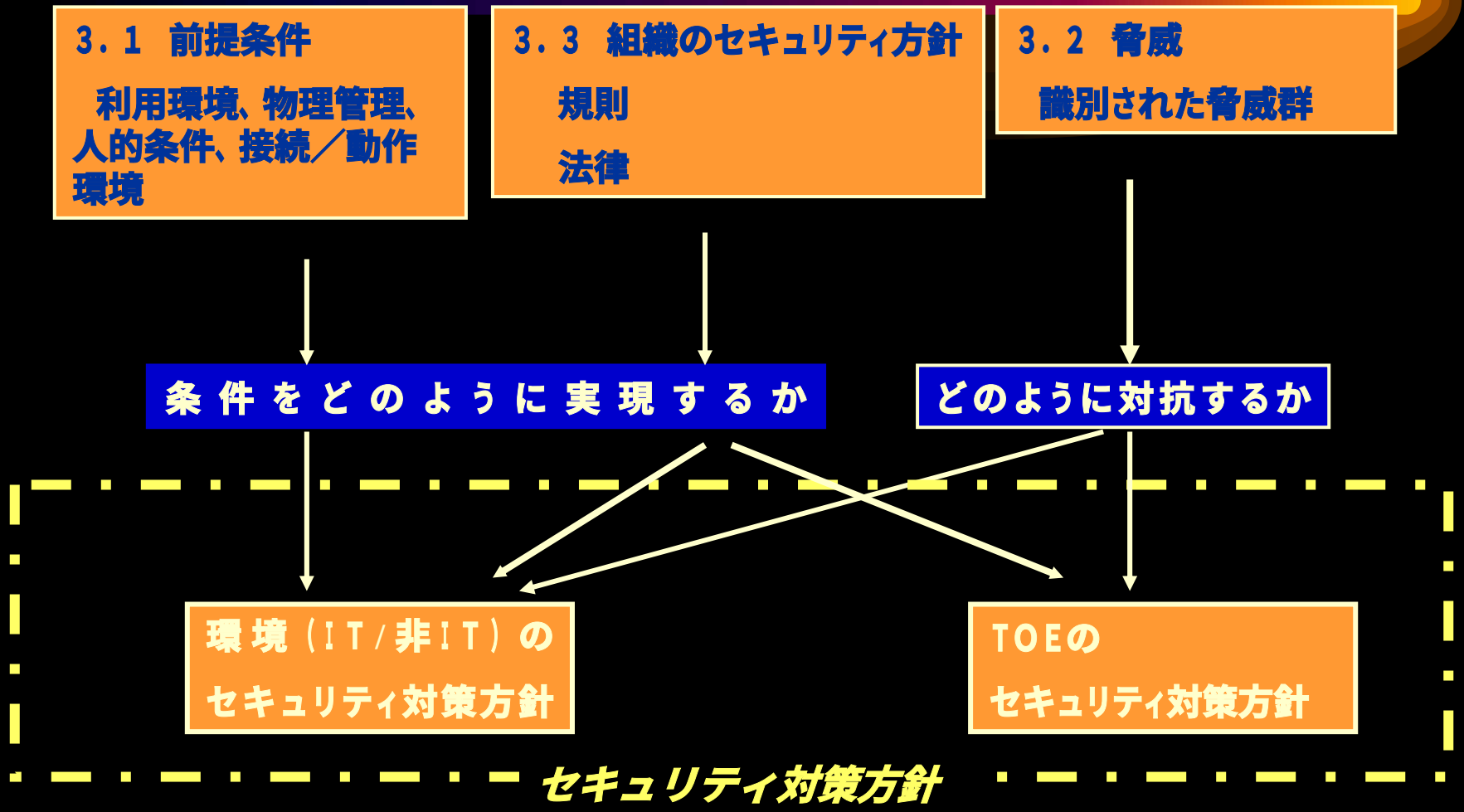
  根拠の記載と合わせて、対抗できることを説明する。

- **対策方針の必要性と十分性の説明**

  根拠の記載と合わせて必要かつ十分であることを説明する。

  脅威への対策の場合、対抗できる理由を説明する。

セキュリティ対策方針の策定手順



セキュリティ対策方針を策定するためのアプローチ方法の事例

ステップ１：セキュリティ環境（前提、方針）の中で、非IT環境で実現するセキュリティ対策方針を規定する。

規定したセキュリティ対策方針は実現性のあるものでなければならない。

ステップ２：セキュリティ環境（前提、方針）の中で、IT環境で実現するセキュリティ対策方針を規定する。

規定したセキュリティ対策方針はIT環境のセキュリティ機能によって、実現されなければならない。

ステップ３：セキュリティ環境（脅威、方針）の中で、TOEが提供する機能に係わるセキュリティ対策方針を規定する。

明確に、脅威への対抗、方針の実現が理解できるように記載する。あわせて、実現性、運用性、利便性、有効性について考慮する。

ステップ４：セキュリティ環境（前提、方針）の中で、TOEの開発に係わる（保証）セキュリティ対策方針を規定する。（CC2.1では必須ではない。）

規定したセキュリティ対策方針は実現性のあるものでなければならない。

セキュリティ対策方針として、

必要かつ十分であることを説明する。

不必要なセキュリティ対策方針は避ける。

セキュリティ対策方針（機能、管理）によって、脅威が確実に許容レベルに達することが理解できる。

セキュリティ対策方針によって、組織のセキュリティ方針が実現できる。

TOEの利用、運用環境において前提条件が可能である。

5． ITセキュリティ要件（←*セキュリティ技術者がTOEのセキュリティを理解したい*）

ポイント

- **新規要件の定義**

  適用可能な要件が無い場合は、新規の要件を定義する。

- **保証要件**

  必要最小限の信頼性を確保することが目的

  必要な保証要件の選択

  妥当性、有効性を配慮

機能要件：

セキュリティ機能設計の正確性を確保することが目的

操作（割付、選択、詳細化、繰返し）

規格に準拠する。特に、割付のパラメタ（サブジェクト、オブジェクトなど）。

パート2の附属書（規格）を参照のこと。

支援機能要件

機能としての依存性を配慮する。

セキュリティ機能の保護（バイパス防止、干渉阻止、動作不能防止、問題検出、など）のための機能要件を考慮する。

機能強度

AVA_SOF.1を含む場合、最小限の機能強度を記載する。

機能強度レベルは脅威エージェントの攻撃力によって決まる。

最悪のケースを検証する。

事例：パスワードの規則に係わる機能

脅威　T. Access：許可されていない人がTOEを利用する。

↓

対策方針　O.PASS.LEN：パスワードは8文字以上の長さのもので、少なくとも1文字以上の特殊記号を含めなければならない。

このセキュリティ対策方針は、利用者の識別・認証に係わるもの(FIA)であることは明白。

このクラスの中で、パスワードの機能に関連のあるファミリーは(FIA_SOS：秘密の規定）と（FIA_UAU：利用者の認証）。

このうち、パスワードの指定文字の規則に係わるコンポーネントはFIA_SOS.1：秘密の検証

機能要件　FIA_SOS.1 ― 秘密の検証

FIA_SOS.1.1　TSFは、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

この[割付: 定義された品質尺度]として、

“パスワードは8文字以上の長さのもので、少なくとも1文字以上の特殊記号を含めたものとする”　と規定する。

保証要件パッケージ(EAL)の内容

脆弱性の分析と評価が目的

	脆弱性識別のための評価対象物	想定する攻撃力	保証内容
EAL1	機能仕様	公開の外部インタフェースを使用した攻撃 *(例:辞書攻撃、IPアドレススプーフィング)*	公開の外部インタフェースを使用した攻撃によって利用される脆弱性は無い
EAL2	構造設計だが機能仕様の補完	全ての外部インタフェースを使用した攻撃 *(例: DoS攻撃)*	全ての外部インタフェースを使用した攻撃によって利用される脆弱性は無い
EAL3	構造設計	処理機能の不備を利用した攻撃 *(例:リプレイアタック)*	処理機能の不備を利用した攻撃によって利用される脆弱性は無い
EAL4	論理設計	処理論理の欠陥を利用した攻撃 *(例:バッファオーバフロー)*	処理論理の欠陥を利用した攻撃によって利用される脆弱性は無い
EAL5	ソースコード	全ての処理論理の欠陥を利用した攻撃 *(例:隠れチャネル)*	全ての処理論理の欠陥を利用した攻撃によって利用される脆弱性は無い

6． TOE要約仕様（←*利用者およびセキュリティ技術者がTOEのセキュリティ機構を理解したい*）

ポイント

- ITセキュリティ機能
  - 機能は何かを記載する。
  - 機能要件を満足していることを、読者が理解できる内容にする。
  - TOE記述のセキュリティ機能にトレースできること。
- 保証手段
  - 開発者が使用する文書の概要説明と、保証要件との対応。

7． 根拠

ポイント

・規定事項が必要であること

上流工程の要求事項にトレースできる。

・規定事項が十分であること

上流工程の要求事項を満足できること。

十分性を読者に納得させられる記述内容にする。

評価のための支援として、下記を認証機関から公開している。

- ST事例
  - ICカード用ST

  その他、ST確認/認証製品のSTが多数公開されている。

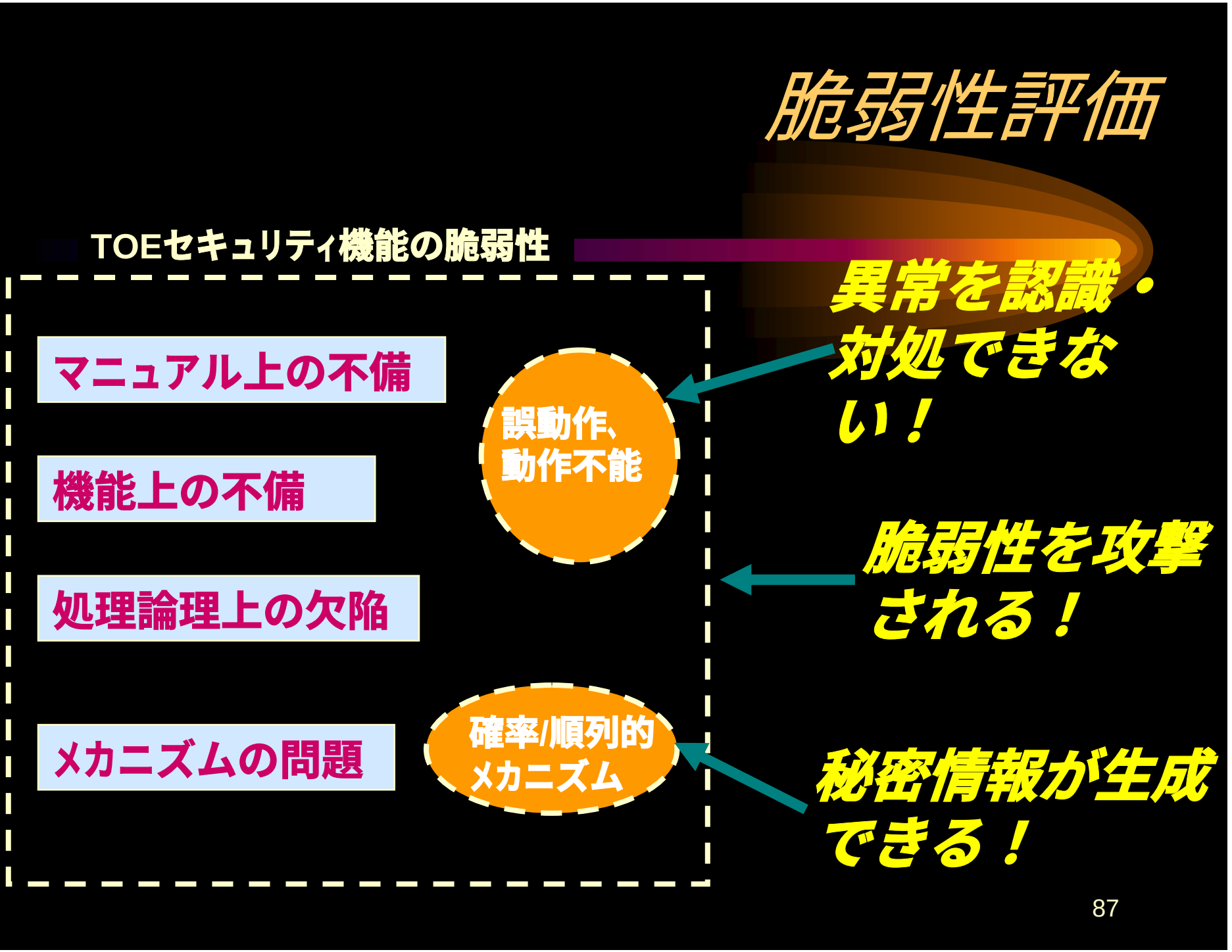
- 「ST作成ガイダンス」

７．脆弱性評価のポイント

脆弱性：資産や操作に影響を与える設計や実装上の問題や弱点。

脅威ではない。

脆弱性評価


TOEセキュリティ機能の脆弱性
マニュアル上の不備
機能上の不備
処理論理上の欠陥
メカニズムの問題
誤動作、
動作不能
確率/順列的
メカニズム
異常を認識・
対処できな
い！
脆弱性を攻撃
される！
秘密情報が生成
できる！

脆弱性評価

脆弱性を攻撃される！

脆弱性の分析

TOEのセキュリティ機能に係わる脆弱性の存在を確かめ、TOEが意図する環境において悪用されないこと、明白な侵入攻撃に対抗できることを検証する。「**脆弱性分析書**」を作成する。

異常を認識・対処できない！

TOEの誤使用や設定を誤る危険性の最小化

TOEが正常に動作していないことを認識・対処できない危険性を最小にする。「**誤使用分析書**」を作成する。

秘密情報が生成できる！

確率的・順列的メカニズムが破られる危険性の分析

確率的・順列的メカニズムの強度が、STに定義された最小強度レベルと同等以上であることを検証する。
「**機能強度分析書**」を作成する。

脆弱性評価で開発者が作成する分析書

脆弱性分析書

脆弱性の識別

- マニュアルに係わる脆弱性
- 基本設計に係わる脆弱性
- 機能設計に係わる脆弱性
- 論理設計に係わる脆弱性
- 保守に係わる脆弱性
- 運用に係わる脆弱性

誤使用分析書

利用者や管理者が認識すべき脆弱性への対応（ガイダンスへの記述など）が十分であることを分析

想定する攻撃力（低位、中位、高位）に対して、脆弱性が顕在化しないことを分析

機能強度分析書

確率/統計的メカニズムに係わる脆弱性に対する強度を分析

脆弱性分析書の作成 (AVA_VLA)

目的

TOEのセキュリティ機能を侵害する脆弱性を分析する。

識別された脆弱性に関して、明白な侵入攻撃に耐えうることを検証する。

明白な侵入攻撃：TOEに関する最小限の理解、技能、技術、資源によって可能な攻撃

脆弱性の識別

情報源
- 製造に係わった資材 (設計書、テスト、など)
- 脆弱性情報データベース
- 一般情報 (Internet、書籍・雑誌等)

TOEのすべてのセキュリティ機能に対して、脆弱性を識別する。

脆弱性事例(1)　マニュアル

【脆弱性の内容】

前提条件が正確に運用者や利用者に伝わらないため、セキュリティが確保されない環境で、TOEが動作する。

【攻撃方法】

前提条件が満足されない環境でTOEを使用し、保護資産を不正に利用する。

【対策】

前提条件を正確にガイダンス文書に記載し、運用者や利用者に認識させる。（「xxの条件を満足しないと、セキュリティが確保されない。」と記載する。多数の注意書きの中に、単に「xxすること。」と記載しただけでは、その重要性を読者は認識できないことがある。）

脆弱性事例(2)　基本設計

【脆弱性の内容】

TOEの想定する運用環境では、前提条件を満足させるには無理があり、セキュリティが確保されない環境で、TOEが動作する。

（製品によっては、利用者がガイダンス文書を読まないで、機能を使用する場合がある。）

【攻撃方法】

前提条件が満足されない環境でTOEを使用し、保護資産を不正に利用する。

【対策】

前提条件が満たされていなければ、TOEの処理を中断して、警告メッセージを表示する。

脆弱性事例(3)　機能設計

【脆弱性の内容】

エラー処理（ハード障害、他機能からのエラーリターン、操作ミス、入力パラメタのミス、暗号秘密鍵の取得/参照不可、などへの対処）の不備で、セキュリティ機能が動作不能になる。

【攻撃方法】

誤操作、異常なパラメタ値の設定、ハード障害などを誘発し、セキュリティ機能を動作不能にして、保護資産を不正に利用する。

【対策】

エラーによって、セキュリティ機能の正常な動作が不可ならば、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。

脆弱性事例(4)　論理設計

【脆弱性の内容】

物理的な干渉によって、TOEの処理回路を変更したり、参照したりできる。

【攻撃方法】

- 配線加工装置などを使用して処理回路を改ざんし、セキュリティ機能を無効にする。
- 物理的プロービング（探針）により、処理回路を暴露して、同等の機器を偽造する。
- 電子顕微鏡などで回路構成を解析し、機器を偽造する。
- 機器の樹脂や絶縁膜を除去して、回路構成を暴露して、機器を偽造する。

【対策】

- 探針検出機能を装備する。
- 改ざん検出機能を装備する。
- 物理的ストレスの検知機能を装備する。

脆弱性事例(5)　保守

【脆弱性の内容】

追加の機能やパッチを、保護しないで利用者に配付している。

【攻撃方法】

不正プログラムを、追加機能やパッチとして配布し、保護資産を不正に利用する。

【対策】

追加機能やパッチに電子署名を添付し、適用側で検証する。

脆弱性事例(6)　運用

【脆弱性の内容】

セキュリティ機能が動作するために必要な資源が枯渇すると、そのタイムリーな動作が保証できなくなる。

【攻撃方法】

Ｄｏｓ攻撃

【対策】

- セキュリティ機能の動作に必要な資源（各種のバッファ領域など）は、動作環境に応じて、必要な量を確保できるようにしておく。
- 枯渇した場合には、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。

脆弱性の分類と対処

識別したすべての脆弱性

明白な脆弱性

TOEの公開外部インタフェース(＊)を使用すれば、顕在化する脆弱性

(例：パスワードの推測、APIの利用、パネル操作、など)

TOEの公開外部インタフェースを使用しただけでは顕在化しない脆弱性

セキュリティ対策や前提によって対処していることを検証

TOEの公開外部インタフェースを駆使した攻撃では顕在化しないことを検証

＊：インターネットなどで流通/公開されているもので、簡易に使用できる攻撃方法も含めることを推奨

脆弱性分析書

識別された脆弱性を記載する。

- 脆弱性の内容（関連するTOEセキュリティ機能の識別を含む）
- 脆弱性の分類（明白な脆弱性か、残存する脆弱性か）
- 検出の情報源と検出に係わった作業
- 関連する脅威

明白な脆弱性に対しては、前提、または、TOEのセキュリティ対策によって対処していることを検証し、その結果を記載する。

他の脆弱性（残存脆弱性）に対しては、TOEの公開外部インタフェースを駆使した攻撃（低レベルの攻撃）では、顕在化しないことを検証し、その結果を記載する。

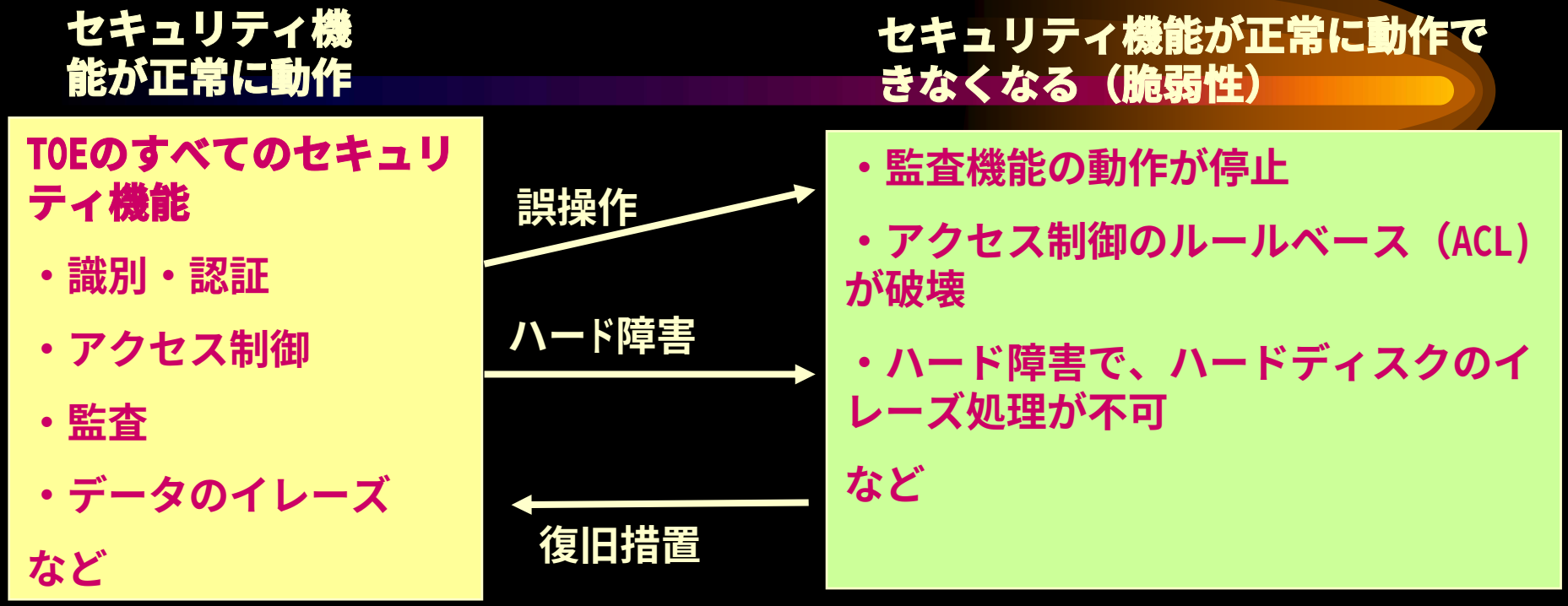
誤使用分析書の作成

目的

TOEの運用管理者や利用者向けのガイダンス文書に必要十分な事項が記載されていることを、誤使用に対する分析により、実証する。

注）ガイダンス文書の作成については、
AGD・ADOを参照。

誤使用分析



TOEのすべてのセキュリティ機能に対して、下記を分析して、誤使用分析書に記載する。

- セキュリティ機能が正常に動作できなくなる脆弱性の識別
- 脆弱性が顕在化する条件（誤操作，ハード障害など）
- 復旧措置

ガイダンス文書への記載

TOEの全てのセキュリティ機能の動作に関して、運用管理者や利用者が認識できなければならない事項を、ガイダンス文書に明記する。

- 正常な動作、あるいは、異常な動作状態にあることを認識（検知）できる。
- 正常な動作が維持できる。
- 異常な動作状態から正常な動作に復旧できる。
- セキュリティ機能の仕様とすべての操作を理解できる。
- セキュリティ機能の構成、導入、起動手順を理解できる。
- TOE動作のすべての前提条件や環境に係わるセキュリティ対策（物理対策、管理対策など）を理解できる。

操作方法、操作の内容、操作に伴うレスポンス（表示メッセージなど）や確認方法を記載する。

誤使用分析書

- 誤使用の分析結果

- 誤使用の分析結果にもとづいて、TOEの運用管理者や利用者が認識しなければならない事項はすべて、正確に、漏れなく、明確にガイダンス文書に記載されていることを検証

評価のための支援

「ITセキュリティ評価・認証業務における判断事例」を認証機関から公開している。

現在公開内容の一部：

・ハッシュ関数のアルゴリズムは評価の対象範囲外だが、演算結果の確率的側面は機能強度評価の対象になる。

・TOEの利用者が1名しか存在し得ない場合、認証要件の依存関係にある識別要件(FIA_UID)は必ずしも必須ではない。

・依存性で指定の要件が不要な場合は、その理由を明記（OR条件の場合も）

・強度分析（SOF)では、前提条件の下での、ワーストケースを考慮

評価のための支援として下記の講座を開催している。

- CC基礎：CCの基本的な考え方と技術動向の紹介
- ST作成：ST作成手法
- 評価のためのエビデンス作成：保証要件で要求されている
  エビデンスを作成するための手法
- 評価認証制度セミナー：制度の紹介

上記の講座や評価機関、認証製品、規格などの情報は、

http://www.ipa.go.jp/security/jisec/index.html