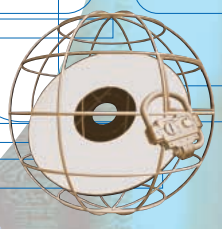
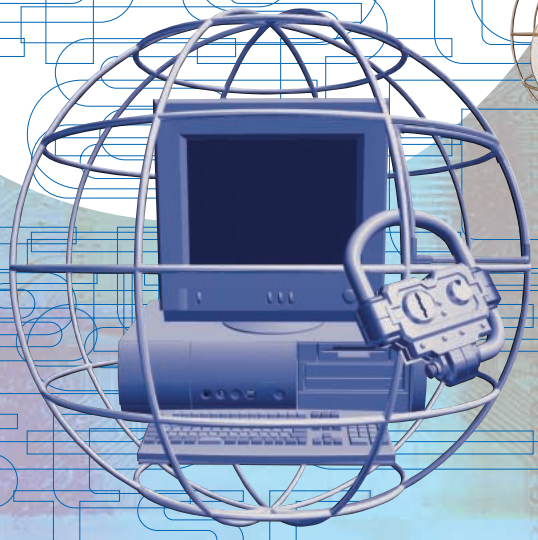
IT Security Center

ITSC

ITセキュリティセンターのご紹介

http://www.itsc.or.jp



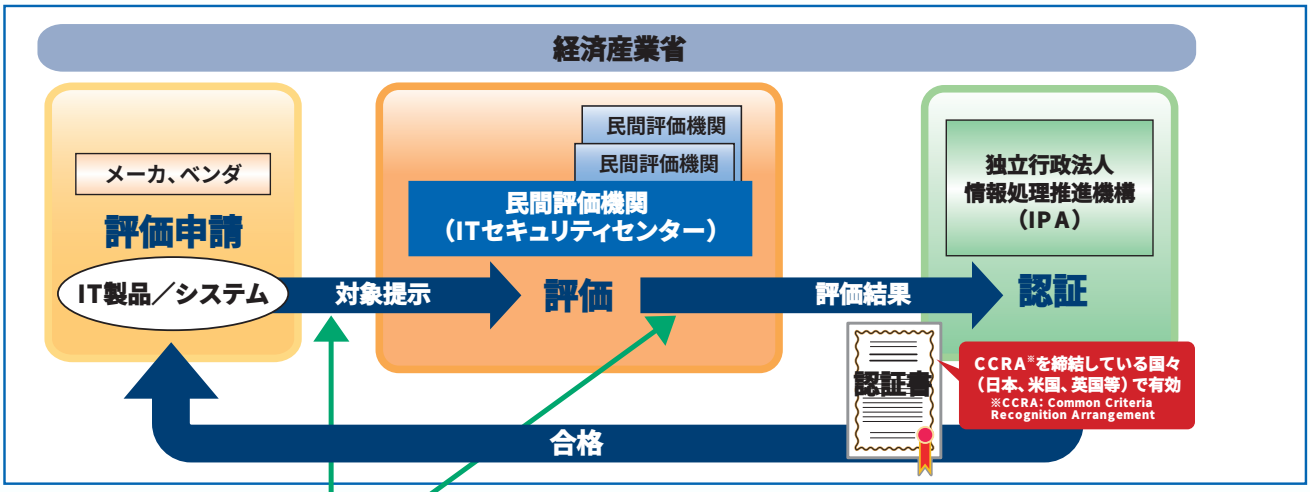


一般社団法人ITセキュリティセンター

無限の可能性を秘めたIT社会。
確かなセキュリティが成功を生み出します。

ITセキュリティセンターは、2007年11月に設立されましたが、
そのITセキュリティに対する取り組みの歴史は長く、日本電子工業振興協会（JEIDA）の時代から始まります。
1987年には既にISO/IEC15408の基になったCommon Criteriaの調査、研究を行っています。
2001年にはIT製品/システムのセキュリティ評価機関としての活動に重点を移した電子情報技術産業協会（JEITA）の
ITセキュリティセンタとして、高品質のセキュリティ評価と関連サービスの提供を開始しています。
これらの活動により蓄積されたセキュリティ評価技術をそのまま引き継いで設立されたITセキュリティセンターは、
IT製品/システムの信頼性を検証するセキュリティ評価、セキュリティ評価に伴うコンサルティング、セキュリティ開発者・セキュリティ技術者向けのセキュリティ教育のサービスを提供するとともに、セキュリティ評価に関する調査、研究開発も行っております。

日本のITセキュリティ評価及び認証制度



セキュリティ国際標準 ISO/IEC15408
（Common Criteria）

- ●Part1：概説、一般モデル
  - セキュリティターゲット
- ●Part2：機能要件
  - 利用者識別と認証
  - アクセス制御
- ●Part3：保証要件
  - 開発環境
  - 設計書
  - ソースコード
  - ガイダンス文書

欧米では1980年代からITセキュリティへの取り組みが行われてきました。また、グローバル化するIT製品/システムの効率的なセキュリティ品質向上のためにITセキュリティに関する国際標準化の努力が続けられてきました。この手法を定めた規格が1999年に制定された国際標準ISO/IEC15408です。ISO/IEC15408はハードウェア、ソフトウェアを問わず個々のIT製品/システムのセキュリティ機能を正しく実装し、かつ検証するためのルールです。この検証作業はISO/IEC15408に基づいて各国が定めるセキュリティ評価認証制度に従って実施されます。

日本では、2001年4月経済産業省により本制度が創設され、その運用が開始されました。本制度はIT製品/システムのセキュリティ機能を検証する「評価」とその評価結果を再検証する「認証」によって運営されます。ITセキュリティセンターは、本制度で定められる「評価」を実施するEAL4評価機関として公式に認定されています。また、本制度の「認証」を担当する機関は、独立行政法人情報処理推進機構（IPA）と定められています。

評価依頼の手順

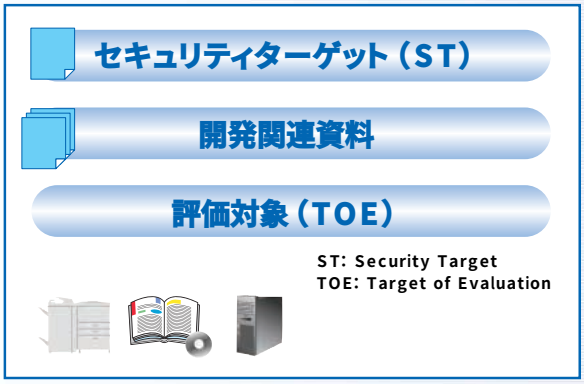
IT製品/システム開発方針
評価申請者は、EAL、スケジュール、体制、コンサルの必要性について、評価機関と検討

評価準備
STを評価機関に提出し、評価手順について評価申請者と評価機関で合意

評価認証申請
評価機関と評価契約締結。認証機関に認証申請書を提出し、評価・認証を依頼

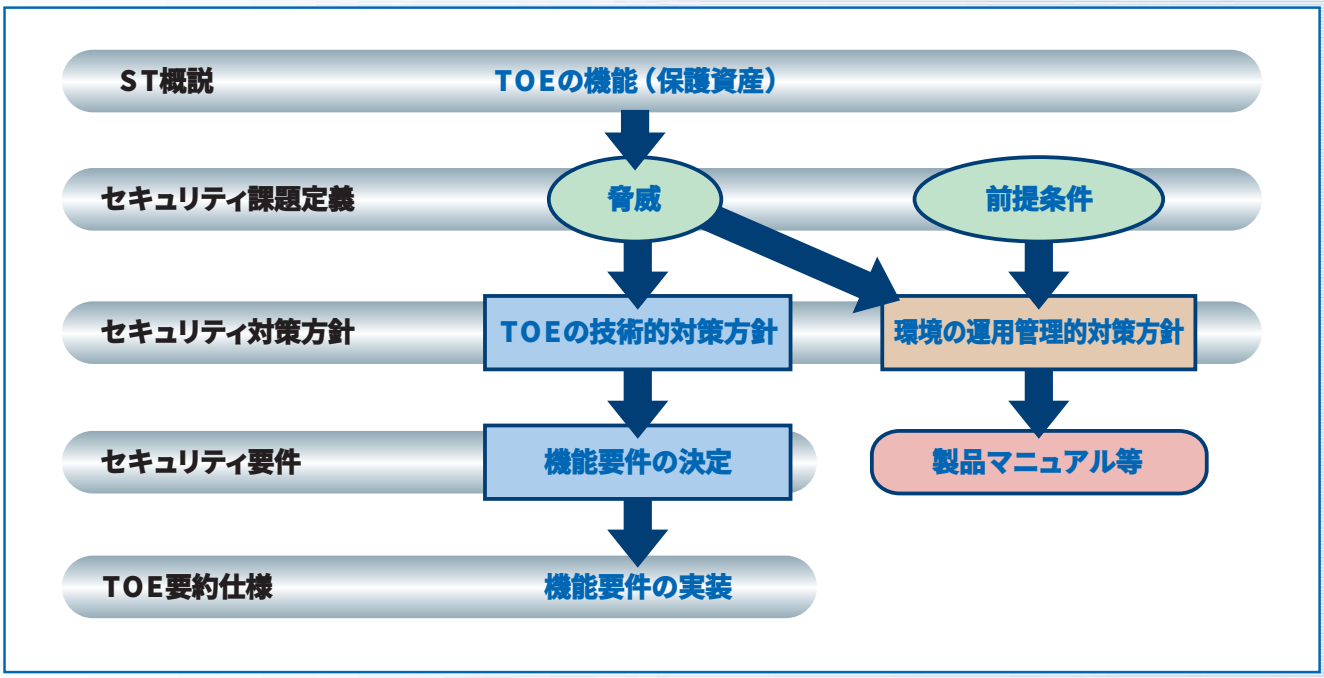
評価認証作業
評価機関は認証機関の監督の下に評価作業開始

セキュリティ評価に必要な資材



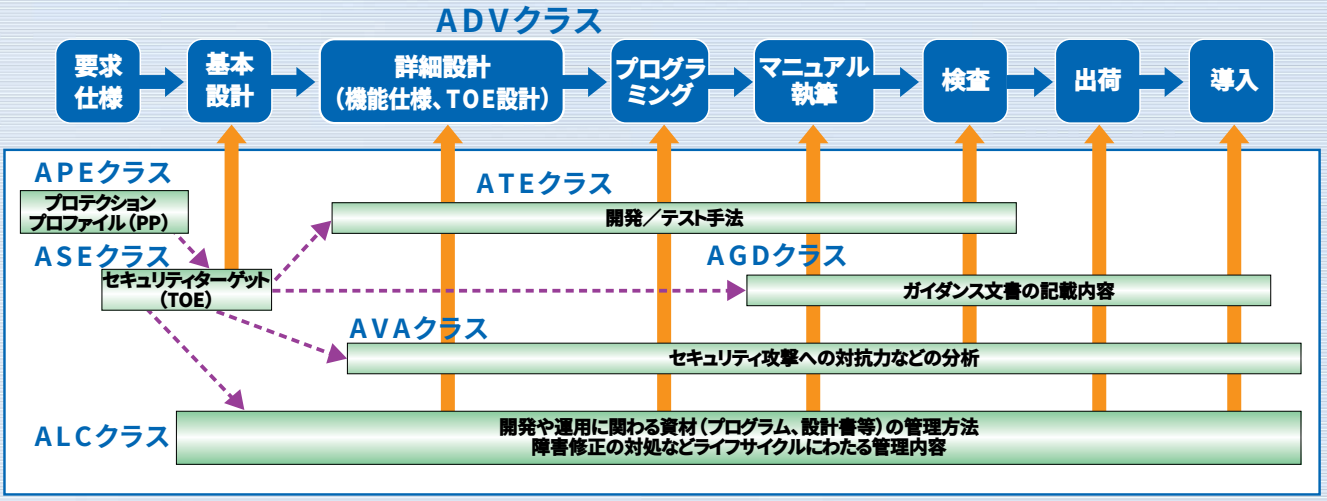
IT製品/システムの開発者がそのセキュリティ機能の評価及び認証を受けるためには、制度が定める評価機関（ITセキュリティセンタ等）に、評価対象（TOE:Target of Evaluationと呼ぶ）となるIT製品/システム、評価対象のセキュリティ機能を ISO/ IEC15408に基づいて記載した文書（ST: Security Targetと呼ぶ）、及び評価対象の開発関連資料を提出します。開発関連資料のほとんどは、開発作業で一般に作成される機能仕様書、テスト仕様書、ソースコード、マニュアル等の資料で、STに記載された機能要件および保証要件を明示的に実現していることを示す資料として提示が求められます。

セキュリティターゲットの構成



STはTOEに対するセキュリティ機能に関する基本設計書に位置付けられますが、単なる設計書ではありません。セキュリティ機能の根源を明らかにし、実装されるセキュリティ機能がなぜ正しいかを論理的に証明するための文書です。セキュリティ機能の根源とは、保護すべき資産（保護資産）です。STは保護資産に加えられる改ざん、破壊、漏洩といった脅威をいかに防ぐかを順序立てて記載、論証します。この論証が正しければ、STに記述されたセキュリティ機能の正当性が実証されたことになります。

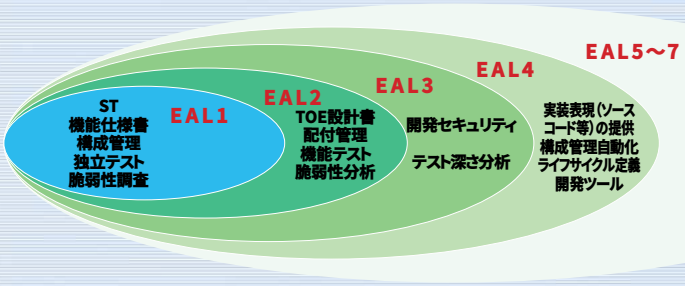
情報処理製品/システムの開発～保守



TOEのセキュリティ機能がSTのとおりに開発・実装されていることを検証します。ISO/IEC15408はSTに従った開発方法・実装方法についての要件（保証要件）を規定しています。保証要件はTOEに対して特殊な開発方法を要求しているわけではありません。STで定められたセキュリティ機能に基づき、外部インタフェースを記述する機能仕様書、TOEをサブシステム/モジュールに分割した機能インタフェースの仕様書（TOE設計書）といった開発文書、マニュアル（ガイダンス文書）、テスト仕様書/結果報告書、開発環境の規定（構成管理）等の開発関連文書を揃えます。

評価保証レベル（EAL）の考え方

EAL: Evaluation Assurance Level



保証要件は、評価保証レベル（EAL: Evaluation Assurance Level）に従って7段階（EAL1～EAL7）に分類されています。どのEALを選択するか、つまり、どれだけ詳細に開発関連資料を検証するかは、TOEの保護資産の価値、セキュリティ機能に要求される信頼度によって判断されます。例えば、国家レベルの機密を扱うTOEは最高レベルのEAL7が必要かも知れません。一方、それほど保護資産の価値が高くなければ、機能仕様書といくつかの開発関連資料を検証するEAL1で良いかも知れません。このようにEALはTOEの検証がどの程度まで行われたかを示す尺度であり、逆にどの程度の評価リスク（未検証の部分）が残っているかを示しているとも言えます。一般に商用ではEAL4が最高レベルと言われています。

ファミリ	証拠資料	EAL1	EAL2	EAL3	EAL4
AGD_OPE	利用者操作ガイダンス	●	●	●	●
AGD_PRE	利用者準備ガイダンス	●	●	●	●
ADV_ARC	セキュリティアーキテクチャ記述		●	●	●
ADV_FSP	機能仕様	●	●	●	●
ADV_IMP	実装表現				●
ADV_TDS	TOE設計		●	●	●
ALC_CMC	構成管理証拠資料	●	●	●	●
ALC_CMS	構成リスト	●	●	●	●
ALC_DEL	配付証拠資料		●	●	●
ALC_DVS	開発セキュリティ証拠資料			●	●
ALC_LCD	ライフサイクル定義証拠資料			●	●
ALC_TAT	開発ツール証拠資料				●
ATE_COV	テストカバレージ証拠		●	●	●
ATE_DPT	テスト深さ分析			●	●
ATE_FUN	テスト証拠資料		●	●	●
ATE_IND	テスト資材	●	●	●	●
AVA_VAN	テスト資材 潜在的脆弱性情報	●	●	●	●

IT社会を支えるセキュリティサポート

●開発経験者からなる、システムノウハウ豊かなサービスの提供
●単体製品から、情報処理システムまで幅広い専門分野の人材を結集

日本におけるセキュリティ評価の先駆的活動

●Common Criteria V1.0による日本最初のセキュリティ試行評価
●セキュリティ国際標準のJIS規格作成に参画
●日本のITセキュリティ評価および認証プログラム制度設立作業に参画

提供サービス

セキュリティ評価（EAL1～EAL4、PP）

■ ISO/IEC15408認証取得向けセキュリティ評価

IT製品やシステム（TOE）のISO/IEC15408に基づいた認証取得を目的としたセキュリティ評価サービスを提供します。お客様より提供された評価資料の中で、まずセキュリティターゲット（ST）の妥当性を検証し、続いてIT製品やシステムがSTで記述されたとおりに開発されているかを検査します。

■ ST評価確認向けセキュリティ評価

日本政府の「ST評価確認」制度に基づいたST評価確認の取得を目的としたセキュリティ評価サービスを提供します。セキュリティ評価は、IT製品やシステム（TOE）のセキュリティ機能設計の妥当性を検証するため、ISO/IEC15408の一部（ASEクラスおよびADV_FSP.1）に基づいて、セキュリティターゲット（ST）と機能仕様書の内容を検査します。

TOE（Target of Evaluation）

●ハードウェア／ソフトウェア製品
●単体製品から情報処理システムまで
例
単体製品:ファイアウォール、会計ツール、ICカード製品 等
情報処理システム:経理システム、電子商取引システム 等

セキュリティコンサルティング

■ セキュリティ評価・認証取得支援サービス

IT製品やシステムのセキュリティ評価には、STに従ったIT製品やシステムの設計資料、テスト仕様書、各種分析資料等を用意する必要があります。必要な評価保証レベルを満たすにはどのような評価証拠資料が必要か、その評価証拠資料の書き方は、といったご相談にお応えします。また、評価証拠資料のレビューや、お客様に代わってプロテクションプロファイル（PP）やセキュリティターゲット（ST）の作成も行います。

■ セキュリティ機能設計支援サービス

単にコストをかけるだけでは、強固なセキュリティ機能は実現できません。漏れがなく、かつコストパフォーマンスに優れたセキュリティ機能を構築するためには、系統的な脅威分析から効果的な対策の立案が必要となります。お客様の立場にたって、適切なセキュリティ機能設計の提案や設計支援サービスを提供します。

セキュリティ教育

■ ISO/IEC15408 技術者教育

ISO/IEC15408に関するセキュリティの基礎から、機能設計/生産管理/検査/評価などのIT製品やシステムの開発段階に必要となるセキュリティ技術の習得を目的とした豊富な教育プログラムを用意しています。

教育プログラム

1. ISO/IEC 15408 概論
2. ST作成手法
3. ST作成演習
4. 開発/検査/評価手法