ISO/IEC 15408 ITセキュリティ評価基準，制度とその活用

ISO/IEC 15408, Information Technology Security Evaluation, Certification Scheme and NEC Activities

吉府研治* 伊東真理* 山里拓己*
Kenji Yoshifu Mari Itoh Takumi Yamasato
支倉健一* 杉浦 昌*
Kenichi Hasekura Masashi Sugiura

要 旨

国際規格であるISO/IEC 15408は，わが国においてもセキュリティの技術的手段に対する客観的評価基準として期待されています。本稿では，ISO/IEC 15408およびセキュリティ評価制度の概要と動向，そしてNECの取り組みについて具体的に述べます。

The international standard ISO/IEC 15408 is a common criteria for IT security technical measures evaluation. It is expected as one of the means that keeps IT security products/systems secure. This paper concretely describes the ISO/IEC 15408, IT security evaluation scheme, trends, and NEC activities.

1．まえがき

ITの普及とともに情報資産の価値が増し，企業・団体活動では，IT製品・システムへの脅威から資産を保護するセキュリティ対策が不可欠となりました。開発者はIT製品・システムのセキュリティ機能およびその実装を明確にし，導入者はIT製品・システムのセキュリティ品質を理解し，品質・機能に合った使用を心がけなければなりません。IT製品やシステムが備えるべきセキュリティ機能の設計および実装に関する国際規格を活用すれば，開発者・導入者双方がIT製品・システムのセキュリティ品質を確保できます。

本稿では，ISO/IEC 15408の概要，制度動向およびNECの取り組みについて解説します。

2．ISO/IEC 15408の概要

2.1 ISO/IEC 15408とは

IT製品・システムのセキュリティ機能が適切に設計され，その設計が正しく実装されているかどうかを客観的に評価する基準がISO/IEC 15408であり，ISO/IEC 15408に適合しているかどうかを検証し，認定する制度がITセキュリティ評価および認証制度です。

2.2 活用のメリット

ISO/IEC 15408には，セキュリティ機能要件集が含まれています。これをISO/IEC 15408をセキュリティ機能体系として活用すれば，IT製品・システムのセキュリティ機能の網羅性が向上します。適切な脅威分析を行い，技術対策と運用対策を明確にして，必要なセキュリティ機能を実装できます。開発者の作成するST（セキュリティ設計仕様書）を読むことにより，導入者は当該IT製品・システムが必要なセキュリティ機能を持つかどうかを判断できるため，適正なコストで必要なセキュリティ機能を持つものを購入できます。公的に認められた機関で，国際規格に則った評価を受けたIT製品・システムを導入することで，導入者の顧客に対し，情報資産（入札情報，企業情報，個人情報ほか）を確実に保護し，その保護方法が第三者の評価を受けているという安心感を与えることができます。情報資産の保護方法に関する説明責任を果たすことにもなります。

2.3 ISO/IEC 15408の歴史

欧米には独自のセキュリティ評価基準が存在し（欧州：ITSEC，米国：TCSEC（通称Orange Book)），それらを統合して作られたのがCC（Common Criteria）です。CCはISO化され国際規格ISO/IEC 15408となり（1999年12月発行)，日本ではJIS X5070としてJIS化されました（2000年7月制定，パート1：日本語翻訳，パート2およびパート3：要約JIS)。CC Version2.1の内容は，ISO/IEC 15408と同一です。

2.4 規格の概要

CCは，以下の3つのパートから構成されます[1)]。

① パート1（概説と一般モデル）：約60ページ
・基本概念，適用範囲など
・PP（Protection Profile）の仕様
・ST（Security Target）の仕様

＊ IT基盤システム開発事業部
IT Platform Systems Development Division

② パート2（セキュリティ機能要件）：約360ページ
・セキュリティ機能要件集（11分類：監査，通信，暗号，利用者データ保護，識別認証ほか）
③ パート3（セキュリティ保証要件）：約210ページ
・セキュリティ保証要件集（10分類：設計，テスト，マニュアル，構成管理，開発セキュリティ，脆弱性評定ほか）
・ 評価保証レベル（EAL）の規定（EAL1～7）

開発者は，CCパート1～3の規定に従って，IT製品・システムの設計・実装を行い，開発文書（設計書，マニュアル，テスト報告書，脆弱性分析書など）を作成します。なお，CCに基づいて作成された開発文書一式は証拠資料と呼ばれます。開発者は，最初にCCパート1に規定されるSTを作成します。STは，TOE（評価対象となるIT製品・システム）の概要・考えられる脅威・それに対するセキュリティ対策方針・製品のセキュリティ機能などを記載した文書であり，他の証拠資料のベースとなります。**図1**にSTの基本的な構成を示します。CCパート2は，IT製品・システムが備えるべきセキュリティ機能要件集であり，PP/STの機能要件選択時に参照されます。11の大分類（機能クラス）があり，それらはさらに細かく135の機能コンポーネントとして規定されています。規格中に当該IT製品・システムにふさわしい機能コンポーネントがない場合，PP/STにおいて独自の機能コンポーネントを定義することも可能です。**表1**に機能クラスの一覧およびその概要を示します。

1. ST概説
  1.1 ST識別（ST名称，バージョン，作成日，作成者など）
  1.2 ST概要（STおよびTOEの概要）
  1.3 CC適合主張（CCへの適合形態，CCのバージョンなど）
2. TOE記述
  製品種別，TOEの物理的範囲（HW/SW構成），
  TOEの論理的範囲（セキュリティ機能）
3. TOEセキュリティ環境
  3.1 前提条件（使用環境，物理的・人的・接続性側面）
  3.2 脅威（保護資産，脅威エージェント，攻撃方法）
  3.3 組織のセキュリティ方針
4. セキュリティ対策方針
  4.1 TOEセキュリティ対策方針
    TOEで対処するセキュリティ対策
  4.2 環境セキュリティ対策方針
    IT環境，運用で対処するセキュリティ対策
5. ITセキュリティ要件
  5.1 TOEセキュリティ要件
    5.1.1 TOEセキュリティ機能要件
    TOEに関する機能要件をCCパート2から選択
    5.1.2 TOEセキュリティ保証要件
    TOEに関する保証要件，EALをCCパート3から選択
  5.2 IT環境セキュリティ要件
    IT環境に関する要件をCCパート2, 3から選択
6. TOE要約仕様
  6.1 TOEセキュリティ機能（具体的な実装機能）
  6.2 保証手段（具体的な保証文書）
7. PP主張（PPの参照内容）
8. 根拠（セキュリティ対策，セキュリティ要件，TOE要約仕様，
    PP主張の根拠）

図1 STの構成
Fig.1 Contents of ST.

（1）保証要件

保証要件は，設計から製品化に至る過程で，セキュリティ機能が確実に実現されていることを保証するための要件であり，CCパート3で規定されています。機能要件と同様，PP/STの保証要件選択時に参照されます。**表2**に保証クラスの一覧およびその概要を示します。

表1 機能クラスの一覧と概要
Table 1 Functional classes.

機能クラス	概　要
セキュリティ監査	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
通信/否認防止	否認防止のためのデータ通信への参加者の識別に関する要件
暗号利用	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
利用者データ保護	アクセス制御，情報フロー制御，転送データ秘匿/保全，保管データの秘匿/保全，残存データ管理など，ユーザデータを保護するための要件
識別と確認	ユーザを特定し，ユーザ本人であることを確認する要件
セキュリティ管理	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
プライバシー	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
セキュリティ機能保護	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
可用性とリソース管理	一定の資源サービスを保証するための，資源の耐障害性や資源割当などに関する要件
TOEアクセス管理	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
高信頼性経路	セキュリティ機構とユーザとの間のセキュアな通信路を確保するための要件

表2 保証クラスの一覧と概要
Table 2 Assurance classes.

保証クラス	概　要
PPの評価	PPの内容の妥当性を評価するための要件
STの評価	STの内容の妥当性を評価するための要件
構成管理	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
配付と運用	製品やシステムがユーザに安全に提供され，運用されるための要件
開発	製品やシステムの設計内容が，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
ガイダンス文書	システム管理者および一般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
ライフサイクルサポート	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対策に関する要件
テスト	製品やシステムのテストを漏れなく実施し，テスト結果を十分に確認するための要件
脆弱性評定	運用時に発生し得るセキュリティ上の問題（誤用，脆弱性）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

表3　評価保証レベルの概要
Table 3　Evaluation assurance level.

EAL	概　要
1	評価者は,マニュアルや機能仕様書の分析,独立テストを実施
2	開発者は,機能仕様（外部インタフェース）のテスト,明白な脆弱性の分析を実施。評価者は,上位レベル設計書を用いたプログラム構造の検証,サンプリングテスト,明白な脆弱性に関する侵入テストを実施
3	開発者は上位レベル（サブシステムレベル）までのテスト,誤使用分析を実施。評価者は,開発セキュリティや開発生産物の構成管理状況の評価,独自の脆弱性分析を実施
4	開発者は構成管理の自動化を実施。評価者は下位レベル設計書を使用し,処理内容を検証。重要な部分はソースコードも検証
5	開発者は半形式的記述言語を用いた上位レベル設計書を作成。評価者は,全ソースコード,隠れた情報漏えいルートを分析
6	開発者は,半形式的記述言語を用いた下位レベル設計書を作成
7	開発者は,半形式的記述言語を用いた検証方法に基づく設計とテストを実施

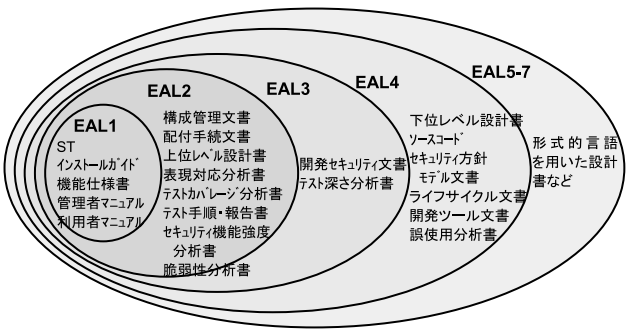


図2　TOE評価に必要な証拠資料
Fig.2　Deliverables.

（2）評価保証レベル（EAL）

評価保証レベル（Evaluation Assurance Level：EAL）は，評価の深さ/厳格さのレベルを示します。セキュリティ機能の強度を示すものではないので注意が必要です。規格では，保証要件のサブセットという形でパッケージ化され，7つのレベルが規定されています。上位（番号の大きい方）レベルは，下位レベルの要件を含みます。**表3**に評価保証レベルの一覧およびその概要を，**図2**に評価保証レベルごとに必要とされる証拠資料を示します。

3．ITセキュリティ評価認証制度

日本でISO/IEC 15408を評価基準とするITセキュリティ評価および認証制度がスタート（2001年）してから数年が経過しました。日本独自のST確認制度，評価機関の認定，CCRA（ITセキュリティ評価・認証の相互承認に関する協定。第3.2節参照）への加盟，認証機関の移管など，制度普及のため，様々な取り組みが行われています。

3.1　ITセキュリティ評価および認証制度の仕組み

ITセキュリティ評価および認証制度[2)]は，情報システム・製品のセキュリティ品質を客観的に評価・認証する国際的にも認められた制度で，評価機関，認証機関，認定機関の3つの機関があります（**表4**）。日本のITセキュリティ評価および認証制度は，**図3**のように経済産業省の指導のもとで運用されています。

表4　認証制度における機関
Table 4　Organizations in Certification Scheme.

機関	説　明	日本の機関（2005.1現在）
評価機関	メーカ,ベンダ,ユーザから依頼された製品,システム,PPのセキュリティ評価を実施します	・社団法人電子情報技術産業協会ITセキュリティセンター ・株式会社電子商取引安全技術研究所評価センター ・みずほ情報総研株式会社情報セキュリティ評価センター
認証機関	評価機関でISO/IEC15408に基づいて正しく評価されたことを確認し,問題がなければ認証書をメーカ・ベンダ・ユーザに発行します。また評価・認証ルール,制度を維持します	独立行政法人　情報処理推進機構（IPA）セキュリティセンター 情報セキュリティ認証室
認定機関	ISO/IEC 17025（Guide25）に基づき,評価機関に評価業務を遂行する能力があることを審査,認定します	独立行政法人　製品評価技術基盤機構（NITE）認定センター

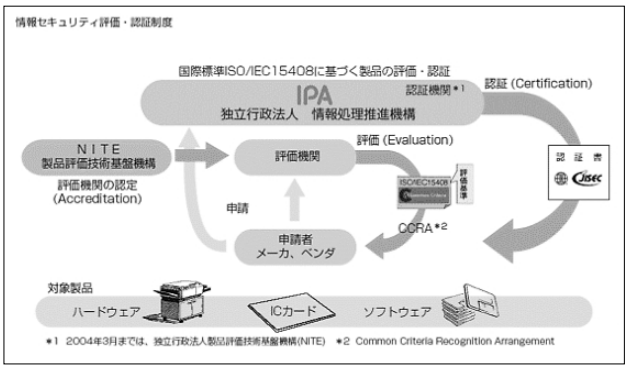


図3　日本におけるITセキュリティ評価および認証制度
Fig.3　Information Technology Security Evaluation and Certification Scheme in Japan（出典：IPA）.

認証機関による認証の種類には，STのみの認証である「ST確認」と，ST以外の証拠資料(機能仕様書，ガイダンス文書など）と評価対象（TOE）であるIT製品・システムの認証である「TOE認証」とがあります。ST確認はSTという1つの設計書のみの認証なので，同じ製品がTOE認証を取得する場合と比較して低コスト・短期間で取得できます。

最も大きな違いは，ST確認では，評価・認証機関はIT製品・システムが設計書どおりに実装されているかどうかを検証しないことです。「ST確認」は日本独自の認証であり，「TOE認証」は後述のCCRAにより海外でも認められた認証です。2005年1月現在，ST確認件数は22件，TOE認証件数は18件です。

3.2　CCRA（Common Criteria Recognition Arrangement）

CCRAとは，CCに基づいたITセキュリティ評価・認証の相互承認に関する協定です。この相互承認協定により，

ある国でCCに基づいて評価・認証されたIT製品・システムは，協定に合意した他の国においても認証製品・システムとして通用します。この協定への参加の形態には，CAP（Certificate Authorizing Participants），CCP（Certificate Consuming Participants）の2つがあります。CAPは相互承認を行う国であり，CCPは国内にITセキュリティ評価認証制度がないが，他の参加国で認証されたIT製品・システムを，その国でも認証済みのものとして受け入れるという国です。日本も2003年10月31日にCAPとしてCCRAに調印しました。2005年1月現在の加盟国は以下のとおりです。

・CAP：CCに基づいて評価・認証した製品を相互に承認
カナダ，フランス，ドイツ，英国，米国，オーストラリア，ニュージーランド，日本（8カ国）
・CCP：CCに基づいて評価・認証した製品を受入れ
フィンランド，ギリシャ，イタリア，オランダ，ノルウェー，スペイン，イスラエル，スウェーデン，オーストリア，トルコ，ハンガリー（11カ国）

4．動　向

4.1　認証取得の動向

認証取得製品の例を**表5**に示します。現在ではデータベース，通信，OS，スマートカードのみならず，コピー機・カメラなど幅広い製品が認証を取得しています。認証取得製品に関する情報は，CCプロジェクト[3]のサイトやCCRA加盟各国のサイトで入手できます。

4.2　調達の動向

電子政府推進に当たり，2001年3月総務省を事務局とする各省庁会議の場で「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」[4]が示され，各省庁の情報システム構築に当たっては，可能な限りISO/IEC 15408に基づいて評価または認証された製品などの使用を推奨しています。

経済産業省は，政府調達においてISO/IEC 15408の活用を促進するため，調達のガイドブックを発行しています（2004年8月 Ver2.0発行）[5]。この調達ガイドブックには，ISO/IEC 15408を活用した調達要件の例が示されています。

・ST確認またはTOE認証取得済み製品を納入する。
・納入物に関し，STを作成するまたはST評価を受検するまたはST確認を取得する。
・納入物に関し，証拠資料を作成するまたはTOE認証を取得する。
・（調達側が提示する）PPに準拠した機能要件・保証要件を満たす。

これらの要件は，入札側の開発期間・費用に大きく影響するので，予算・納期を十分考慮して調達要件を決める（調達側），入札するか否かを決める（入札側）ことが必要です。**図4**に某官庁のISO/IEC 15408調達仕様の具体例を示します。

表5　認証製品リスト
Table 5　List of evaluated products.

製品･システム名（略称）	種　別	提供者	EAL	取得年月	国
Oracle 9i Release 9.2.0	DB	Oracle	EAL4	2003.9	英
Entrust/RA from Entrust/PKI 5.1	PKI	Entrust	EAL3	2001.2	英
Check Point VPN-1 /Firewall-1	VPN/Firewall	Nokia	EAL4	2003.9	英
Windows2000 SP3	OS	Microsoft	EAL4+	2002.10	米
Sun Trusted Solaris Version 8 4/01	OS	Sun Micro systems	EAL4	2004.3	英
GemXpresso Pro E64PK	IC SW	Gemplus	EAL5+	2002.2	独
EOS−1D MarkⅡファームウェア	カメラ	キヤノン	EAL2+	2004.8	日
データセキュリティキット AR−FR4 version M.20	コピー機※	シャープ	EAL4	2004.9	日

※コピー機全体でなく,部分的に（ディジタル複合機内データ保護機能のみ）について認証を取得

システムのセキュリティ品質を高めるために，電子政府が推進している「ITセキュリティ評価及び認証制度」に基づく評価・認証を受けること。
具体的には，
下記の手順に従うこと
A．受注者によるセキュリティターゲットの作成
B．独立行政法人評価技術基盤機構が定める評価機関によるセキュリティターゲットの評価
C．セキュリティターゲットに基づくシステムの構築
D．独立行政法人情報処理推進機構（IPA）による認証書の交付

図4　某官庁の調達仕様具体例
Fig.4　Example of a request for proposal for a government.

5．NECの取り組み

5.1　評価機関・認証機関へ派遣，情報収集を継続実施

NECは，海外での制度の創設段階よりISO/IEC 15408の重要性を認識しており，国内のITセキュリティ評価認証制度の準備段階から参画し，調査研究を行ってきました。国内制度が本格稼働した現在も，認証機関のIPA，評価機関のECSECに研究員を派遣し，認証業務および評価業務を実施しています。評価機関に常駐していた筆者（吉府）は，ITセキュリティ評価者資格（EAL4）を取得しています。

5.2　5件の認証（確認）取得実績

NECは，国内のITセキュリティ評価および認証制度において，ST確認を3件取得しています。また，フランスの評価認証制度において，TOE認証を2件取得しています。これらの取得内容一覧を**表6**に示します。

筆者（吉府）は，表6内のPKIソフトウェアのST確認取得をコンサルティングしました。この製品のSTを，ST確認を取得した製品としては国内で初めて認証機関のホームページに公開しました。このSTは見本として参照され，制度の活性化に貢献しています。

5.3　評価経験に基づくコンサルティングサービス

NECは，これまでのISO/IEC 15408に関する経験を踏まえたISO/IEC 15408コンサルティングサービスを**表7**のよ

表6　NECの取得したST確認/TOE認証一覧
Table 6　List of NEC's certified products/systems.

	製品・システム名	種別	取得年月	取得国
ST確認	Carassuit 電子政府版Ver2.0	PKIソフト	2002.12	日本
	Carassuit 電子政府版Ver1.1	PKIソフト	2003.7	日本
	ファイアウォール コアユニット Ver.1.0	ファイアウォール	2004.8	日本
TOE認証	CZ6 production line on the NEC site in Yamaguchi	ICカード生産ライン	2001.11	フランス
	Smart Card IC Development flow, Smart Card IC Development section in Kumamoto, NEC	ICカード設計ライン	2002.8	フランス

表7　NECが提供するISO15408コンサルティングサービス
Table 7　ISO15408 Consulting Services by NEC.

サービス名	内　容
調達仕様作成支援	ISO15408を適用した調達仕様書の作成をご支援します
方針立案	製品・システム開発者向けに認証取得の方針立案コンサルティングを行います
教　育	ISO15408のパート1からパート3までの解説と,公開PP/STの解説を行います
証拠資料作成支援	STやTOE証拠資料の作成をご支援します
認証取得支援	ISO15408認証取得コンサルティング(評価・認証機関対応を含む)を行います

うに提供しています。

NECが提供するコンサルティングサービスの特長は，実際の評価・認証業務の経験者がコンサルティングを実施することです。コンサルタントが評価・認証作業の内容を知り尽くしているので，評価・認証のポイントを押さえた証拠資料の作成の支援や，評価・認証機関からの指摘事項に速やかに対応することができ，評価・認証にかかるコストや期間を低減します。

5.4　製品開発にISO/IEC15408開発ガイドライン適用

NECは，ISO/IEC 15408の手法を取り入れた社内の開発ガイドラインを策定中です。今後開発する製品・システムはこのガイドラインに沿って開発を進めていく予定です。
また，このガイドラインに沿った開発ができているかどうかを内部監査する仕組みも検討しています。たとえ認証取得をしない製品・システムであっても，社内の高い基準をクリアすることになりますので，NECが提供する製品・システムはセキュリティ水準が高いということで，お客様に安心してお使いいただけるようになります。

6．むすび

ISO/IEC 15408 ITセキュリティ評価および認証制度の動向とNECの取り組みについて述べました。製品，システムのセキュリティ水準を高める仕組みとして，ISO/IEC 15408に基づく開発・認証取得は今後さらに重要になります。

NECは，ISO/IEC 15408の認証取得製品を増やしていくとともに，認証取得コンサルティングを提供し，お客様の認証取得を支援します。

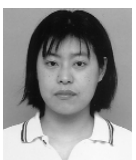
＊本稿に記載されている会社名，製品名は，各社の商標または登録商標です。

参考文献

1) 情報技術セキュリティ評価のためのコモンクライテリア パート1～3
(http://www.ipa.go.jp/security/jisec/evalbs.html)
2) JISEC Webサイト
(http://www.ipa.go.jp/security/jisec/index-j.html)
3) CCプロジェクトWebサイト
(http://www.commoncriteriaportal.org/)
4) 各省庁の調達におけるセキュリティ水準の高い製品等の利用方針
(http://www.soumu.go.jp/gyoukan/kanri/010425_9.htm)
5) 経済産業省 調達のガイドブック
(http://www.meti.go.jp/policy/netsecurity/downloadfiles/CCguide_ver2_0.pdf)

筆者紹介

Kenji Yoshifu
吉府　研治　1991年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター主任。コモンクライテリア プロフェッショナル。



Mari Itoh
伊東　真理　1992年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター主任。

Takumi Yamasato
山里　拓己　1988年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー。コモンクライテリア プロフェッショナル。

Kenichi Hasekura
支倉　健一　1991年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー。

Masashi Sugiura
杉浦　昌　1983年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター センター長。