エレクトロニックコマース・セキュリティ特集

UDC　342.738：681.324(100)：006.88.032

情報セキュリティ国際標準化動向

Trends of International Standard for Information Security

山本　明　Akira Yamamoto
宮井貴志　Takashi Miyai

要　旨

製品およびシステムに対する情報技術セキュリティ評価基準が1999年6月に国際標準ISO/IEC15408として採択された。本稿は，ISO/IEC15408の制定の背景，概要，および沖電気の取組みについて述べている。

1．まえがき

電子メール，電子商取引，あるいはサプライチェーンマネジメントなどの利用拡大に伴い，企業におけるコンピュータのネットワーク接続が急速に拡大されてきている。しかし，これに伴ってインターネットを経由した不正侵入，メール爆弾，コンピュータウィルス等による業務妨害などのコンピュータ犯罪の脅威が身近な問題となってきている。このため，多くの企業は情報セキュリティ管理・運用の強化を図りつつあり，企業にとって必要な情報セキュリティのレベル，およびそのレベルを達成するための適切な情報セキュリティ製品選定基準の作成が望まれている。

このような中，製品およびシステムに対する情報技術セキュリティ評価基準が，1999年６月に国際標準ISO/IEC15408として採択された。

ここでは，ISO/IEC15408の制定の背景，概要，および沖電気の取組みについて述べる。

山本　明

システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部

宮井貴志

システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部　開発第四チーム

2．ISO/IEC15408制定の背景

欧米では，以前からTCSEC（Trusted Computer System Evaluation Criteria），ITSEC（Information Technology Security Evaluation Criteria）など各国が独自に情報技術セキュリティ評価基準を制定し運営していた。しかし，その評価基準や運用方法はまちまちであり，インターネットで機器が相互接続される場合に統一した基準に基づくセキュリティを確保できないことや，ベンダーは国ごとに各国評価基準に合わせた評価・認証を取得する必要がある等の不都合があった。このため，国際間で共通に利用できる情報技術セキュリティ評価基準の作成が望まれていた。

この問題の解決のため，カナダ，フランス，ドイツ，オランダ，イギリス，アメリカによる協議会が結成され，国際標準を作成するプロジェクトが開始された。この協議会で作成された成果が，1999年６月に国際標準ISO/IEC15408として採択され，同12月には正式に発刊された。

3．ISO/IEC15408の概要[1)2)]

ISO/IEC15408は，情報技術を用いた機器やシステムに対するセキュリティ評価標準であり，機器あるいはシステムが備えるべきセキュリティ機能の要件（機能要

件)と，設計開始から納入に至る開発過程で実行すべきセキュリティ管理の要件(保証要件)とを規定している。

機能要件では，機能クラスと呼ばれる以下の11項目が定義されており，情報技術セキュリティに必要な機能が網羅されている。

- セキュリティ監査
- セキュリティ通信
- 暗号サポート
- ユーザデータ保護
- 識別と認証
- セキュリティ管理
- プライバシー
- セキュリティ機能保護
- 資源利用
- 評価対象アクセス
- 信頼経路／チャネル

開発に際しては，対象とする機器(システム)のセキュリティ対策に必要な機能を機能クラスから選んで使用する。

また，保証要件は，保証クラスと呼ばれる以下の10項目で構成されており，開発の各工程で実行すべきセキュリティ管理の内容が定義されている。

- プロテクションプロファイル(PP)の評価
- セキュリティターゲット(ST)の評価
- 構成管理
- 配布と運用
- 開発
- ガイダンス文書
- ライフサイクルサポート
- テスト
- 脆弱性評価
- 保証の保守

保証要件では，開発時のセキュリティ管理の厳しさに従って評価保証レベルと呼ぶ7段階のレベル(EAL１～７)を定めている。レベル１(EAL１)がもっともセキュリティ管理レベルが低く，レベル７(EAL７)がもっとも厳しいセキュリティ管理を要求する。また，機能要件とは異なり，各評価保証レベルごとに，実行すべき保証要件が決まっている。

各レベルと保証内容は以下のように定義されており，通常の商用製品ではEAL4以下を使用し，軍事用あるいはそれに準じた非常に高レベルのセキュリティが要求される分野ではEAL５以上が向いていると言われている。

- EAL1；機能的なテストの保証
- EAL2；構造的なテストの保証
- EAL3；系統的なテストおよび確認の保証
- EAL4；系統的な設計，テスト，レビューの保証
- EAL5；準形式的な設計およびテストの保証
- EAL6；準形式的な設計の検証およびテストの保証
- EAL7；形式的な設計の検証およびテストの保証

ISO/IEC15408に従って機器(システム)を開発する場合の手順は以下のようになる。

1)評価対象とセキュリティ要求条件を明確にする。(評価対象：開発しようとしている製品あるいはシステム)
2)評価対象に対する脅威分析を行なう。
3)脅威分析結果をもとに，セキュリティ対策方針を立てる。
4)セキュリティ対策方針を実現するためにセキュリティ要件を選択する。
5)セキュリティ要件に従って評価対象の開発を実施する。
6)テストを実施する。
7)出荷する。

上記手順の４)では，開発する機器(システム)に必要なセキュリティ機能要件をISO/ICE15408で定義している機能要件の中から選び出す。また，開発段階でのセキュリティ管理についてもISO/ICE15408で定めるセキュリティ保証レベルをもとに決定する。

開発者は，開発にあたって機器(システム)に対するセキュリティ設計仕様書ST(Security　Target)を作成する。このSTは，開発の基本となるものであり，評価・認証を受ける際にももっとも重要視されるものである。STには，上記開発手順１)～４)で検討した内容をもとに，以下の項目について記述する。

1)STの概要
2)評価対象の情報
3)評価対象に対するセキュリティ上の脅威
4)脅威に対する対策方針
5)セキュリティ要件
6)製品の具体的なセキュリティ仕様
7)脅威，対策方針，機能要件，セキュリティ仕様選定それぞれの妥当性

STは，上記手順に従って最初から作成することも可能であるが，一般的にはPP(Protection Profile)と呼ばれる仕様書をもとに作成した方が効率が良い。PPは，

同じ製品群に共通に適用できるように作成されたセキュリティ要求仕様書であり，業界団体，ユーザ等が事前にISO/ICE15408に従って作成する。STを作成する際に，PPをもとにすることによって，上記手順2）～4）を簡素化することができる。しかし，PPは同じ製品群に共通なセキュリティ要件のみを定義しているため，セキュリティについての他製品との差別化機能や付加機能を持つ製品では，STを作成する際にPPで規定されたセキュリティ要件以外に，追加のセキュリティ要件が必要な場合もある。その場合には，ISO/IEC15408の機能要件，保証要件から必要な要件を選んで，STに追加するか，まったく新しい要件を追加することができる（図1参照）。

なお，現在，ICカード，ファイアウォール，オペレーティングシステム等に関するPPが，各国で開発されている。

4．評価・認証制度

ISO/IEC15408は，情報技術セキュリティ評価基準として新たに制定されたものであるが，評価・認証の運用の仕組み自体は，ITSECやTCSECなどで行なっている評価・認証制度をそのまま利用している。

この制度を利用した評価・認証は，評価を評価機関に依頼することから始まる。評価機関は，製品がISO/IEC15408の機能要件・保証要件に従って開発されていることを，対象とする機器あるいはシステムのST，開発ドキュメント，工程管理証拠等をもとに評価する。また，実際の製品あるいはシステムそのものについても評価を行なう。評価機関の評価結果は，認証機関で審査され，問題がなければSTで規定されたセキュリティ機能および評価保証レベルが認証される。

ISO/IEC15408に基づく評価・認証は個別の機器やシステムを評価対象としており，ISO9000のようにプロセスを評価対象とするものではない。

5．ISO/IEC15408の今後の動向と課題

現在ISO/IEC15408に基づいて，ある国で受けた評価・認証結果を他の国でも有効とする国際相互認証協定がカナダ，イギリス，フランス，ドイツ，アメリカ間で結ばれている。しかし，この協定が実質的に意味のあるものになるためには，各国の評価手法が同じでなければならない。このため，現在CEM(Common Criteria Evaluation Method)[3]と呼ばれる評価手法のための仕様書が作成されている（図2参照）。

また，PPの開発が各国で行なわれており，これらを1個所に登録し，国際的に利用できるようにするための枠組がISO（国際標準化機構）で議論されている。

日本においても，日本工業規格協会が，ISO/IEC15408の日本工業規格（JIS）化作業を急ピッチで進めており，今年の夏にはJIS化される見込みである。また，ICカード取引システム研究開発事業組合(ICCS)は，1999年度に日本最初のIC カードPPを作成した。

しかし現在，日本には情報技術セキュリティの評価・認証制度はなく，日本のベンダーが製品の評価・認証を取得するためには海外の評価機関・認証機関を利用するしかない。このため，評価・認証を受けるには，ドキュメントの英語化などによる費用の発生，海外で評価を行なうことによる開発の長期化等の問題が発生

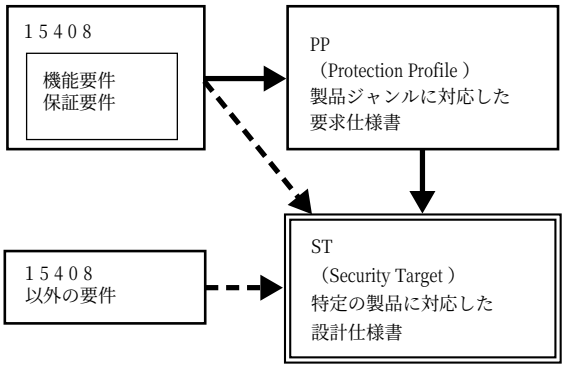

図1　15408、PPおよびSTの関係
Fig. 1　Relation between 15408, PP and ST

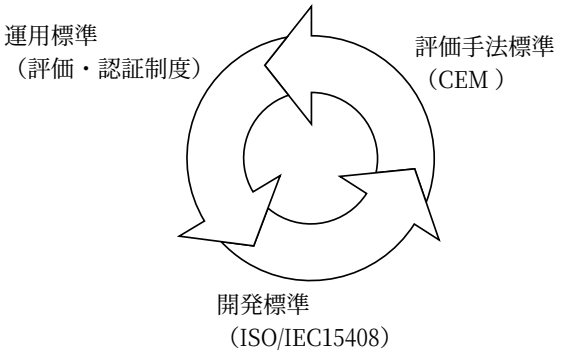

図2　評価・認証制度
Fig. 2　Evaluation and certification system

する。この問題を解決するため，現在日本に評価機関および認証機関を設立するために必要な技術蓄積が，情報処理振興事業協会（IPA）を中心に行なわれている。

6．沖電気の取り組み

当社は，機器あるいはシステムがISO/IEC15408の評価・認証を取得する必要のある場合に備えて，ISO/IEC15408に対応した開発手法の評価と技術蓄積を行なってきた。その結果，ISO/IEC15408は情報技術セキュリティを必要とする各種製品設計の際の情報セキュリティ品質を一定に保つためにも有効であるとの認識を得た。そのため，ISO/IEC15408をもとに社内の新しい情報セキュリティ設計規定を作成し，製品開発に適用している。

特に，脅威分析およびその対策は製品計画の早い段階から実施するように規定することにより，製品の情報技術セキュリティ品質ついて一層の向上を目指している。さらに，STレベルの仕様作成時には，その記述内容を情報セキュリティの有識者が参加してチェックしている。

評価保証レベルについては，すべての製品に対して高いレベルを設定するとコストに影響を与える恐れがあるため，個々の製品あるいは製品群のセキュリティ要求条件によって保証要件を設定するようにしている。

今後は，ISO/IEC15408に基づく情報セキュリティ設計の経験を蓄積するとともに，開発をより効率的に行なえる手法を開発していく予定である。

当社は，このほかに，日本工業規格協会による，ISO/IEC15408のJIS化委員会，（社）日本電子工業振興協会セキュリティ評価技術委員会等での活動をはじめ，ICカード取引システム研究開発事業組合で行なったICカードPP作成等の活動にも積極的に参加してきた。さらに，ISO/IEC15408に準拠したセキュリティ評価機関設立を目指した電子商取引安全技術研究組合（ECSEC）等にも積極的に参加している。

7．あ と が き

昨年６月に国際標準として採択されたISO/IEC15408について，その背景，概要，今後の課題および沖電気の取り組みについて報告した。

現在，ハッカーによるネットワークを経由した不正侵入等が，深刻な問題となっている。このため，政府でも使用する情報システムの高いセキュリティの実現を目指しており，「ハッカー対策等の基盤整備に係る行動計画」[4]の中で，情報機器等の政府調達におけるISO/IEC15408の活用方針について，平成13年５月までを目途に検討すると述べている。当社は，このような状況にも充分対応できるように準備を進めている。

なお，ISO/IEC15408は，製品およびシステムの情報セキュリティに関する標準である。しかし，情報資産およびそれを扱う情報システムのセキュリティは人的管理，システム管理，物理的管理などを含めたトータルなセキュリティが重要である。このため，当社は，情報セキュリティポリシーの作成，システムセキュリティ診断をはじめ，インターネット時代に対応した総合的な情報セキュリティサービスをさらに充実させ，ユーザに提供していく予定である。

8．参 考 文 書

1）情報処理振興協会セキュリティセンター：ISO/IEC15408「情報セキュリティ評価基準」のご紹介，Ver.1.02，平成11年
2）ISO/IEC：Information technology -Security techniques - Evaluation criteria for IT security -, ISO/IEC15408, 1999
3）The Common Evaluation Methodology Editorial Board：Common Evaluation Methodology for Information Technology Security, Ver.1.0, 1999
4）情報セキュリティ関係省庁局長等会議決定：「ハッカー対策等の基盤整備に係る行動計画」，平成12年