ISO/IEC 15408セキュリティ評価の意義と適用

ISO/IEC 15408 : Its Meaning and Application for IT Security Evaluation

山里拓己* 吉府研治* 伊東真理*
Takumi Yamasato Kenji Yoshifu Mari Itoh

要　旨

2001年4月，わが国の電子政府のセキュアな基盤構築に向けて，国際的な評価基準ISO/IEC 15408に基づくITセキュリティ評価及び認証制度が創設されました。本制度は欧米諸国などと相互承認を行える国際的なものです。しかしながら，わが国ではまだまだ十分な理解と推進がなされていない状況です。

本稿では，筆者の本制度における認証者としての経験を踏まえ，ISO/IEC 15408を適用することの意義，現在のセキュリティ評価の現状と課題，そしてISO/IEC 15408をより適切に推進するための取り組みについて述べていきます。

The Information Technology Security Evaluation and Certification Scheme in Japan based on the international criteria ISO/IEC 15408 was established in April, 2001. However, this scheme has not been used enough in Japan.

This paper describes the current state and the problems of the security evaluation and how to deal with the problems from the experience as a certifier of the scheme.

1．まえがき

企業におけるセキュリティは，セキュアな運用管理体制の確立，第三者による運用管理体制のチェックなど運用管理面のほか，そこで用いられる製品・システムのセキュリティ機能の安全性についても考慮しなければなりません。

製品や運用システムのセキュリティ機能が適切なものであるかを，その製品・システムの開発者あるいは運用者が自ら宣言し，その内容を第三者が検証するための評価基準がISO/IEC 15408であり，その基準を用いた「ITセキュリティ評価及び認証制度」が，わが国でも2001年度より運営されてきました。しかしながら，一般的にはISO/IEC 15408を導入することがどのような効果を生むのかは理解されているとはいいがたい状況です。また，評価は対象となる製品やシステムのセキュリティ機能のみならず，その製造過程の管理にまで及ぶため，開発者あるいは調達者にとって多大な工数がかかるととらえられています。

今後，企業のセキュリティが組織的，人的な管理・運用に加え，安全措置としてのIT手段の的確な把握と第三者への説明責任がより要求されるようになるなか，ISO/IEC 15408がどのようにそれらに寄与し，どのようにすれば適切な適用が可能となるのでしょうか。

2．セキュリティ評価をすることの意義

ISO/IEC 15408を評価基準とするITセキュリティ評価及び認証制度において，評価を実施するということはどのような意義があるのでしょうか。ISO/IEC 15408では大きく3つのフェーズに分けて評価が行われます。

第一にセキュリティターゲット（Security Target：ST）と呼ばれるセキュリティ設計方針に関する評価，第二にSTで識別されたセキュリティ環境（評価の対象となる製品・システムはどのような環境において運用され，そこにはどのような脅威が存在するのか）に対応するセキュリティ機能の十分性・妥当性の評価，第三にそれらのセキュリティ機能が正しく実装されていることの評価が実施されます。

ここでは，それぞれのフェーズがどのような意義を持つかについて述べていきます。

2.1　セキュリティターゲット

IT製品・システムの評価は，まずその製品がどのような環境で使用されることを想定しており，またそこにはどのような脅威が存在するかを識別することが出発点となります。ここで重要なのは，識別された環境においてその製品が何を保護するか，つまり保護資産を明確にすることがISO/IEC 15408の特徴です。資産の具体的な存在場所や，守ろうとする資産の価値が第三者に理解される必要があります。開発者あるいは調達者は，これらのセキュリティ環境を出発点とし，脅威（誰が何をどのように攻撃するか）に対抗すべくセキュリティ対抗策を策定し，それらを機能

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

要件と呼ばれるセキュリティ機能にまでブレイクダウンしていきます。この一連の説明が述べられているものが，STと呼ばれるセキュリティ設計方針をまとめたドキュメントです。評価においては，このSTの内容を吟味し，矛盾がなく妥当なものであることを第三者が検証します。

ISO/IEC 15408は，組織全般のセキュリティをめざすためのものではありません。個々のモラルや全体のポリシーではなく，IT手段が守る保護資産に着目し，それをどのような条件のもと，どこまで守ることができるかを，STのなかで明らかにし，第三者に理解できるかたちで提示しなくてはなりません。この考え方を導入することで，開発者あるいは調達者は次のような効果が得られます。

(1) セキュリティ効果・要件の明確化

セキュリティはその効果を第三者に提示することが難しい分野です。その製品・システムを導入することで，どのようなセキュリティが向上するのか，またそのセキュリティが利用者にとって本当に必要であるか，これらの判断材料を示すことは重要です。

ISO/IEC 15408は，何を何からどのような状況で守るかということを明確にします。利用者や調達者は，提示された環境が自分たちの運用環境にかなっているか，また自分たちが守ろうとする資産の重要性（資産価値）に合致したシステムであるかを，STを通じて判断することができます。開発者やベンダーは自分たちの製品やシステムがもたらすセキュリティをより明確に第三者に説明でき，調達者はこれを具体的な調達要件として開発者やベンダーに示すこともできます。

(2) セキュリティコストの集中

漠然とセキュリティを向上させることは，その投資対効果が見えにくく，また何をどの程度まで守ればいいかという目安がないとセキュリティのためのコストを維持しにくい面があります。組織において，最低限守るべき必要のある資産が何かを分析し，ISO/IEC 15408を適用することで，本来不要であるセキュリティへの投資を抑制することも可能です。

またISO/IEC 15408は，脅威への対抗策が妥当であることのみならず，その対抗策に対し不要なセキュリティ機能が紛れ込むことを検査します。想定する運用環境に寄与しない機能（つまり，脆弱性が紛れ込む可能性）の排除も評価の対象となります。これにより必要最小限の機能を実現することとなり，余分な開発コスト，導入コストの発生を抑制します。

2.2 機能要件

開発者は，識別された脅威への対抗策をセキュリティ機能レベルまでブレイクダウンします。ISO/IEC 15408ではセキュリティ機能を分類して（認証機能，監査機能，プライバシー，アクセス制御など），さらにその分類のなかで機能レベルを階層的に定義した機能要件と呼ばれるカタログを規格として提供しています。

この機能要件は実装に依存しない抽象レベルで機能を記述してあり，開発者はこの機能要件から適切なセキュリティ機能を選び，STに記述することができます。機能要件は，さらにその機能の実現に必要と考えられる他の機能要件への依存性（たとえば監査イベントの記録という機能については，正確なタイムスタンプを提供するという機能が依存性として示されています）や，機能にかかわらず考慮すべきセキュリティ機能自体の保護要件も含まれます。評価は開発者が記述したこの機能要件のセットが脅威への対抗策，そして脅威へとさかのぼれることを検査します。

ISO/IEC 15408がこれらの機能要件を用意し，開発者あるいは調達者がその機能要件を通じてセキュリティ機能を述べることは以下の利点があります。

(1) セキュリティ機能の共通理解

脅威への対抗策がどのようなセキュリティ機能によって実現されるかを，設計書や実装言語そのもので理解させることは困難です。また，同じような機能説明でも受け手の知識の差によりその理解が異なることもあります。

ISO/IEC 15408では，実装に依存しない形でかつ規格という共通の言語でセキュリティ機能を表すことで，セキュリティ機能の正確で共通な理解を与えることができます。これにより開発者が調達者にあるいは調達者が開発者に，提供あるいは要求するセキュリティ機能を正確に伝えることが可能となります。また，第三者による評価を受ける際，対抗策から実装レベルへのブレイクダウンが正確になされていることを理解する大きな手助けとなります。

(2) セキュリティ機能の網羅性

脅威に対する直接的なセキュリティ機能を設計する場合，そのセキュリティ機能を支えるための二次的なセキュリティ機能を考慮する必要があります。たとえば，先に示した例のように，セキュリティ事象にかかわるイベントのログの採取には，正確なタイムスタンプの提供が不可欠です。特定の資源に制限値を設ける場合には，その制限値の変更に関する管理も必要となります。そしてこれらのセキュリティ機能自体の改ざん，迂回をも考慮する必要があります。

ISO/IEC 15408では，それぞれの機能要件に関連する依存性や管理項目が示されており，開発設計者は脅威への対抗策をセキュリティ機能へとブレイクダウンする際，その機能に関連するセキュリティ事項にかかわるセキュリティ機能要件も網羅することができます。また，調達者や第三者による評価時にも，関連するセキュリティ事項が顧慮されていることを確信するための客観的根拠としてこれらの機能要件を用いることができるのです。

2.3 保証要件と評価手法

ISO/IEC 15408では，その製品・システムのセキュリティ機能が適切であることを検証するとともに，正確にその機能が実装されたこと，設計・開発から配送・導入までにその機能が損なわれる機会がないことを検証します。具体的には，STで述べられた機能要件が仕様，設計そしてソー

スコードへと対応付けられていること，適切なテスト・脆弱性評定がなされていること，開発環境がセキュアであること，ガイダンスにセキュリティ維持に必要な指示がなされていることなど，保証要件と呼ばれるセキュリティ機能が実現されるための要件のカタログが用意されています。評価者は評価の対象となる製品・システムの要求分析の段階から製品導入に至るライフサイクルにおいて，これらの保証要件を検証します。

この評価では，評価を受ける側が自らその評価をどのくらい厳密に行うか（評価保証レベル）を宣言します。たとえば脆弱性評定において機能仕様をもとに外部インタフェースからの攻撃を想定するレベルと，ソースコードを含む論理設計をもとに処理論理の欠陥による脆弱性を利用した攻撃までを想定するレベルでは，セキュリティ機能実現の確実性の度合いは後者の方が高いといえるでしょう。この評価保証レベルはどのような証拠をどこまで検査するかというセキュリティ機能の実現の確実さの検証度合いを示すものであり，セキュリティ機能の強度ではない点に注意が必要です。

また，ISO/IEC 15408で宣言された評価保証レベルに対応した評価手法も規定されています（現在ISO/IEC FCD 18045）。保証要件で述べられた評価基準を評価者は具体的にどのように評価すればよいかという評価手法が示されているため，評価者や開発案件の違いによる評価結果の振れが抑えられます。

ISO/IEC 15408の保証要件を評価手法に従って評価することで以下の効果が得られます。

（1）多岐にわたる評価項目と客観的な評価結果

ISO/IEC 15408では，製品やシステムの最終的なセキュリティ機能のふるまいにのみ焦点を当てるのではなく，その製造過程においてセキュリティを脅かす要因が紛れ込まないこと，あるいは運用時にそのセキュリティ機能が損なわれるようなガイダンス記述がないことといった，妥当とされるセキュリティ機能の確実な実現をも視野にいれています。また，特定の評価手法に沿って第三者により評価が実施されるため，その評価結果は客観的であり，かつ製品や評価者の違いによらない均質なものとなります。したがって，開発者あるいは調達者が利用者にその評価結果を示すことは，利用者に対して大きな安心を与えることとなります。

（2）適切な評価レベルの選択

評価をより深く厳密に行えばそれだけ信頼度は増しますが，その一方で開発費用や負荷は増大します。ISO/IEC 15408では，評価をどの程度の深さまで実施するのかを，評価を依頼する側（開発者や調達者）が宣言します。開発者や調達者は，STで識別された資産価値，使用環境をかんがみて，適切な保証レベルを任意に決定できます。

これにより開発者，調達者は，その製品やシステムにとって保証が必要だと考える範囲で評価を受けることができ，無駄なコストを抑えるとともに，製品やシステムにかなった保証を利用者に示すことが可能となるのです。

3．セキュリティ評価の実情と適切な適用

ここまで述べてきたように，ISO/IEC 15408を適用することは，開発者や調達者による必要かつ十分なセキュリティレベルの選択と，それに対する国際的判断基準に基づく第三者の客観的評価により，必要最小限のセキュリティ機能の具備とその保証を示すことが可能となるのです。

今後の社会的要求から，開発者が提供するあるいは運用者が用いるITセキュリティ手段の安全に関する説明責任が重要となってくるでしょう。しかしながら，現在ではまだISO/IEC 15408を用いたセキュリティ評価が一般的に認知され，普及しているとはいえない状況にあります。

ここでは，筆者の経験をもとに，現在のセキュリティ評価の現状・課題と，適切にセキュリティ評価を適用するためにはどうすればよいかについて述べていきます。

3.1　セキュリティ評価の現状

セキュリティ評価の最大の課題として挙げられていることは，その期間とコストです。ISO/IEC 15408に基づくITセキュリティ評価及び認証制度において，実際の認証を受けるにはどのくらいの期間とコストがかかるのでしょうか。

過去の事例では，商用における最高の評価保証レベルで評価に半年，認証に半年，またその評価を受けるための事前の準備に半年をかけ，費用は数千万円という話も聞きました。セキュリティ製品といわれるものは，IT技術の進歩に対応し頻繁なバージョンアップを繰り返します。セキュリティ評価を実施している間に次のバージョンの製品が出荷されるようでは，開発者にとって魅力的な制度とはいえません。また，長い期間をかけて評価を行うことはコストも増大し，そのコストを製品で回収できるかという判断の結果，認証取得をあきらめるケースも多いようです。

（1）制度の過渡期

過去のこのような事例の原因としては，本制度が2001年度に立ち上がったばかりの過渡期であったことが挙げられます。本制度にかかわる評価者や認証者は，評価基準や評価手法についての知識を規格として理解していましたが，実際に開発された製品やシステムの証拠資料の検証には多くの困難がありました。

評価依頼者は，何を評価用の証拠資料とするのか十分な情報がなかったため，多くの資料の作成に試行錯誤し，評価の過程においても開発関連の資料が何度も見直され，認証フェーズでも評価報告に対する技術的指導が頻繁に行われました。加えて，実際の認証業務を遂行する調査機関が当時の認証機関（独立行政法人 製品評価技術基盤機構）とは異なっており，評価機関と認証業務者とのやりとりは，認証機関の窓口管理業務を経由しなければなりませんでした。このため，評価結果に対する認証側の技術指導が多いほど，累計的にお互いの応答期間が長くなり，認証取得ま

でさらに時間がかかることになったのです。

その後の制度の見直しにより，2004年度に認証機関と調査機関は統一され（独立行政法人 情報処理推進機構），評価報告に対する応答も改善されています。評価機関・認証機関の経験も増え，多くの判例を蓄積しています。評価開始時には評価依頼者，評価者，認証者により評価対象に対する共通の理解を得る機会を設けています。さらに評価機関・認証機関によるISO/IEC 15408に関する技術セミナーも開催され，多くの開発者がこれに参加してきました。このような制度改善努力により，認証取得までの期間は以前より短くなっています。

(2) 保証継続

改善されたといっても，評価の期間は現在のIT分野での製品ライフサイクルに追いつけるものではありません。多くのIT製品は，開発後にバージョンアップを頻繁に繰り返します。バージョンアップによる変更がセキュリティに影響を与えるものでないケースも多くあります。セキュリティ評価による認証の取得が，製品のバージョンアップに追いつかない，あるいはバージョンアップのたびに再評価を必要とするのでは，認証製品をタイムリーに市場に投入することはできませんし，コストの面からも現実的ではありません。これに対応すべく，ISO/IEC 15408に基づく評価結果の相互国際承認の協定に参加する各国が，保証継続と呼ばれる新しい枠組みを制度に追加しました。わが国でも2004年11月に保証継続が導入されています。

保証継続では，開発者がすでに認証を取得した製品やシステムからの変更個所を識別し，それらの変更がセキュリティにどのような影響を及ぼすかを分析します。その結果，セキュリティを保証する要件への影響が小さい（つまり，すでに認証済みの製品やシステムの保証が継続されている）と判断した場合，開発者はその分析結果を認証機関に提出します。認証機関が，その影響分析内容が妥当で保証が継続されると判断した場合，そのバージョンアップされた製品やシステムは認証済みとして扱われます。このように，すでに実施された評価・認証をそのまま利用し，再度同じプロセスを必要としないため，開発者にとって認証取得のための期間とコストは格段に短縮・軽減されました。

3.2 課題への取り組み

保証継続はセキュリティへの影響がある場合には適用できません。現在のセキュリティ評価にかかる期間および費用は，まだまだ多くのITセキュリティ製品にとって，セキュリティ評価を受ける妨げとなっていることは事実です。それでは，このコストを縮小させるためには，どうすればよいのでしょうか。

(1) 評価範囲と目標の明確化

セキュリティ評価を受ける際，その製品やシステムのどの範囲を対象とするのかを明確にしなければなりません。組織全体のセキュリティの目標とセキュリティ評価の対象となる製品・システムの目標との関係，評価の対象となる製品・システムとそれを包含するシステムとの境界，さらに評価対象となる製品・システムのなかの評価範囲を明確に示すことは，セキュリティ評価の第一歩として非常に重要です。セキュリティ評価の現状でも，評価全体に占めるST評価の割合は大きく，これらの範囲を明確に意識せずにSTが作成された結果生じた誤解の解決に費やされています。

STを作成する開発者や調達者は，製品やシステムを用いて構築された全体（組織やシステム）のセキュリティを意識しますが，そのなかで用いられるIT手段としての製品と，全体から見えるセキュリティの方針が一致しないこともあります。ST作成者にとって，あるデータがシステム全体から非常に重要なものであり，セキュリティの要となるものであったとしても，評価の対象である製品自体は，その内容を意識せず単純なデータとして扱うべきものかもしれません。評価の範囲を大きくすることで，このデータは重要な資産となるかもしれません。さらに大きく範囲をとれば，セキュリティ機能のふるまいにかかわるセキュリティ属性として扱うべきデータかもしれません。このように，評価の対象・範囲・目標を明確に示すことができなければ，評価すべき対象の前提条件・脅威・かかわるセキュリティ方針を固定することができず，開発者・評価者・認証者がそれぞれの異なった理解で評価が進んでしまいかねません。また，セキュリティ機能についても，その機能が何に寄与するかを理解しないまま開発がなされている場合があります。

ISO/IEC 15408ではセキュリティ機能の必要性がまず示され，その妥当性と実装の正しさを検証します。最先端の機能のサポートや製品カタログ上の見栄えから選択された機能を評価の対象とし，その利用目的や手段に対する十分な示唆を利用者に与えられない（特に資産とその価値を特定できない）ようなケースでは，何を持って妥当と判断するかの根拠にさかのぼれず，期待すべき評価結果が得られないこともあります。

STは評価の出発点です。STの作成には，評価の対象範囲を物理的・論理的に明確に示し，評価の対象の利用目的を客観的に理解できる記述にすること，またST段階で開発者・評価者・認証者にこれらの共通理解を十分に図ることが，評価期間短縮の大きな鍵といえるでしょう。

(2) セキュアな開発体制の維持

評価を受ける側にとって，その工数の多くが開発過程の評価のための証拠資料の提供（作成）に関するものといわれています。開発者は，STで述べたセキュリティ機能の実装を確実とするために，どのような保証がなされているかの資料を評価者に提供する必要があります。その内容は，機能仕様書，テスト仕様書のように開発やテストにかかわるものから，開発資材や開発環境の管理，開発物の配付手順，設置や立上げの留意点など製品の開発から保守まで多岐にわたっています。

しかしながら，セキュリティ評価を受ける段階になり，

どのような資料が必要となるかを開発者が理解し，それらの準備にとりかかるケースもあるようです。開発がすべて終了し，評価やコンサルを受ける段階で，開発過程においてなされなければならない保証が実はされていなかったことが発覚した場合，その製品やシステムが確実にセキュリティ機能を実装した確証を評価から得ることはできません。また，開発過程においてなされている保証が，評価の証拠としてうまく流用できないこともあります。たとえば，セキュリティ機能の識別がなされておらず，その他の膨大な機能仕様のなかにセキュリティ事項が埋没しており，結局は新たにセキュリティ機能仕様を作り直すのではコストが増大します。

セキュリティ機能が正しく実装されるための保証は，開発過程だけではありません。ガイダンスの記載内容，利用者への配付手順など多くの部門に関連してきます。製品開発部門が中心となって評価を依頼してみたが，実はその他の部門の管理内容を十分に把握しておらず，評価が滞る例もあります。またこのような対応をセキュリティ評価のたびに行っていては，製品開発に対する評価コストは大きくなってしまいます。

ISO/IEC 15408で求めている保証要件は，開発セキュリティ確保のための手法として全部門で取り組むべき基準です。セキュリティ製品・システムの開発段階から導入までにセキュリティ評価に必要となる証拠資料の内容をあらかじめ理解し，開発プロセスに反映することは，認証取得の有無にかかわらずセキュリティ品質の高い製品を提供する仕組みとして活用できます。また開発者サイトのセキュリティ管理・監査の具体的手法としても活用できます。

セキュリティ評価を，特定の製品のコストととらえず，開発のガイドラインとして取り組むことにより，評価コストを分散し，開発者・調達者双方が製品・システムのセキュリティ品質の向上を図れるとともに，第三者に対し国際的基準を満たしていることを示すことができるのです。

4．NECのISO/IEC 15408への取り組み

NECはISO/IEC 15408に深くかかわった活動をしてきました。特長としては，わが国のITセキュリティ評価及び認証制度における認証機関・評価機関においてそれぞれ認証者・評価者として従事したコモンクライテリア プロフェッショナル（独立行政法人 情報処理推進機構が付与するCCに関する資格）保有者を有し，ISO/IEC 15408に関する高度な技術を展開していることです。また，IT製品ベンダー・サービスベンダーの立場から，セキュリティ評価の本質であるIT製品のセキュアな開発体制の確立と運用環境での製品・システムに対する脆弱性診断などのサービスを提供することができます。

セキュリティ評価は，ISO/IEC 15408で規定された規格・手法の正しい理解と，それを実際に展開するIT技術が必要となります。前者が抜ければやみくもな評価となり，後者が抜ければ形式的な評価に終始します。

NECでは，セキュリティコンサルティングとIT技術の両側面から，ISO/IEC 15408技術を認証取得支援にとどまらず，総合的なセキュリティソリューションの有用な手法として活用していきます。

5．むすび

情報セキュリティ対策が，情報を扱う企業の社会的責任と認識される今，適切なセキュリティ管理・運用と安全措置としてのセキュアなIT手段を講じていることを利用者に説明する責任が生じています。

本稿では，国際的なセキュリティ基準であるISO/IEC 15408がどのようにそれらに寄与するかについて述べてきました。NECでは，ISO/IEC 15408を始め，お客様の情報セキュリティ対策を，管理と技術の両側面からサポートできる体制を整えています。

筆者紹介

Takumi Yamasato
山里　拓己（やまさと　たくみ） 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。

Kenji Yoshifu
吉府　研治（よしふ　けんじ） 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（いとう　まり） 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。