セキュアシステムインテグレーション

Secure System Integration

小田原　育也　■ ODAHARA Ikuya
秋山　浩一郎　■ AKIYAMA Koichiro
島田　毅　■ SHIMADA Tsuyoshi

情報システムのインテグレーションにおいて，セキュリティの向上は重要な課題である。これは単に，最新のセキュリティ技術・製品を導入するだけで実現できることではなく，要求分析やアーキテクチャ設計の段階から包括的にセキュリティを作り込むことを意識したシステム構築が必要となる。東芝は，セキュアシステム構築の方法論を開発し，情報システムのインテグレーションへの適用を進めている。また，国際規格ISO/IEC15408（ISO：国際標準化機構，IEC：国際電気標準会議）の評価認証取得に応用し，コンサルテーションサービスを行っている。

Security design is an important issue in information technology (IT) system integration. In designing security functions for the target system, it is necessary to employ not only advanced technologies and products but also a method focusing on security integration according to the customer's requirements and system architectures.

Toshiba has developed such a security design method and applied it to IT system integration. We have also employed this method to a consultation service for acquiring ISO/IEC 15408 certification of the target system.

1 まえがき

情報システムのセキュリティは，その必要性がクローズアップされるようになって久しい。政府は，世界に冠たる電子政府を実現するうえで情報セキュリティの向上が必要だとして，IT（情報技術）セキュリティ評価・認証制度や情報セキュリティマネジメントシステム（ISMS）適合性評価制度など，セキュリティ関連の各種施策を打ち出している。またIT企業も，製品のセキュリティに関する情報を一般に公開したり，セキュリティ診断や監視など新しいサービスビジネスを提供し，情報セキュリティを高める取組みを強めている。

情報システムのセキュリティを高めるため，今まで同様，暗号技術などのセキュリティ要素技術やコンポーネント技術の研究開発を続けなれければならない。しかしそれだけではなく，システムアーキテクチャ設計の段階から包括的にセキュリティを作り込むことを意識したシステム構築や，セキュリティを維持するためのシステム運用ルール・体制作りが必要である。これらがあいまって初めて可能になるもの，それが情報システムの包括的なセキュリティである。

ここでは，東芝が開発・実践している，セキュリティ作り込みのためのシステムインテグレーション，すなわちセキュアシステムインテグレーションの方法論について述べる。加えてこの方法論の応用として，情報セキュリティ評価のための国際規格ISO/IEC15408[(1)]（JIS X5070）に基づく認証を取得するための，支援コンサルテーションについて述べる。

2 セキュアシステムインテグレーションの考え方

セキュリティ技術が進歩している一方で，それら個々の技術を統合した情報システムにおいて，期待したほどにはセキュリティが高まらないという事態が起きている。多発する情報セキュリティ関連の事件を見ると，導入したセキュリティ技術や機器が，そのシステム固有の特性や置かれている環境に応じて適切に設定運用されず，有効に機能しなかったというケースの多さが目につく。例えば，ファイアウォールのフィルタリングルールや無線LAN機器の設定ミスがそうした事例に該当する。システムのセキュリティを理解するには，個別技術を見るのではなくシステム全体を見なければならない[(2)]。

情報システムの構築では，特別にセキュリティが重要視されるシステムを除くと，アプリケーション機能だけに注意が集中しセキュリティには十分な時間や労力が費やされないという傾向がある。セキュリティも，本来はアプリケーション機能同様，そのシステムの目的や要求性能，使用環境を前提条件として，分析・設計・実装が行われるべきである。当社は，情報システム構築におけるセキュリティの方法論を開発するにあたって，以下を基本的な考え方に据えて取り組んでいる。

(1) “保護すべきもの”を定義することからスタートする。

情報資産の機密性，完全性，可用性を保護することが情報セキュリティの目的である。したがって“何を”守るべきなのかが明確でなければ，包括的なセキュリティは

議論できない。また従来は，実装するセキュリティ機能が何を守っているのか不明確な場合もあった。

⑵ 担当者スキルに左右される度合いを極力低くする。

情報セキュリティ技術は，ほかの分野に比べて習得のチャンスが少ない。このため，情報セキュリティの分析・設計・実装の品質は，担当技術者のスキルに左右される度合いが強い。情報セキュリティの包括性を扱うには，担当者のスキルに左右される度合いを極力排除する定式的な方法論にしあげる必要がある。また，分析・設計・実装の結果を，客観的に評価する手法も重要になってくる。

⑶ ソフトウェア工学の成果を活用する。

分析・設計では，要求分析から始めて徐々に下流工程へと進みながら，上位の概念をブレークダウンしていく。適用できそうなセキュリティの個別技術がわかっていても，最初からシステム設計あるいは実装をスタートさせない。ソフトウェア工学の重要な成果は，抽象レベルから始めて少しずつ詳細化するというステップワイズリファインメントの考え方である。抽象レベルでは，漏れのない分析・設計が目標となるし，また具体レベルでは，抽象レベルで扱ったすべての事項を正確に具体化することが目標となる。

3 セキュアシステム構築方法論

セキュアシステム構築方法論は論理設計，システム設計，実装，運用の四つの段階に分かれる。ここでは運用段階以外の三つの段階の構築手法を**図1**に沿って説明する。

3.1 論理設計段階

この段階では顧客要求に従った初期システムを作成することが目標であり，三つのステップから成る。

⑴ システム機能要件の決定　　当該システムに望まれる機能を洗い出す。

⑵ システム構成要素と関与者の決定　　システム機能要件に基づいて，**図2**に例示したように，必要な機器（システム構成要素）とシステムにかかわる人（関与者）を決定する。図2は顧客管理システムの例で，社内のオペレータと社外の外交員が顧客データベース（DB）へアクセスすることが想定されている。

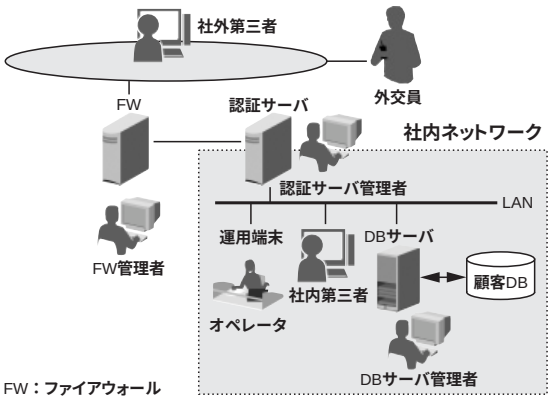

図2．顧客管理システムの初期システム ― オペレータと外交員がそれぞれ社内，社外から業務上必要となる顧客情報の登録，検索，変更ができることを機能要件としたシステム。社外からのアクセスを正当なものだけに制限するため認証サーバやFWの設置をあらかじめ検討している。また，各システム構成要素には，それを管理する管理者がいるほか，社内外にはシステムとは関連のない第三者も想定しなくてはならない。

Example of draft design for target system

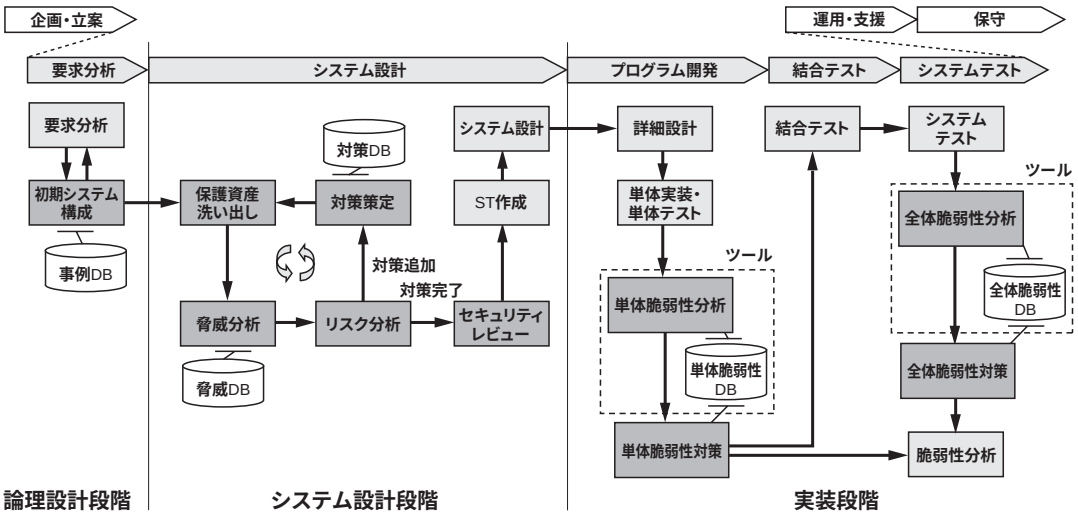

図1．方法論の全体 ― セキュアシステムインテグレーションの方法論は，論理設計段階，システム設計段階，実装段階の三つの部分から成る。

Methodology for secure system integration

⑶ 詳細なプロトコルの決定　　前記システム構成要素と関与者に基づいてシステム機能要件を満たすために，どのようなデータがどこを流れるかを決定する。

3.2 システム設計段階

この段階では保護資産洗い出し，保護資産に対する脅威分析，脅威に対するリスク分析，対策すべき脅威に対する対策策定を行うことによって，顧客のセキュリティポリシーを明らかにし，ポリシーに基づいてシステム設計を行う。なお，対策策定で新たな保護資産が生じることが多く，通常は数回これらのプロセスを繰り返す。

3.2.1 保護資産洗い出し　　保護資産とは，情報資産やシステム構成要素などのシステム資産のうち保護すべきものを言う。顧客管理システムの例では，“顧客データ”と“システム可用性”などが保護資産となる。

3.2.2 脅威分析　　脅威とは保護資産の機密性，完全性，可用性のいずれかを損なう危険である。個々の脅威は“社外第三者がインターネット上で顧客データを盗聴する”などのように，“どの関与者がどこで保護資産に何をする”という形式で記述し，**表1**のような脅威リストにまとめる。

脅威分析のポイントは網羅性であり，このために構築経験から導き出した脅威を抽出するための勘所と実際の脅威事例がDB化されている。

表1．脅威リスト（抜粋）
Threat analysis table (excerpt)

保護資産	関与者	場　所	攻撃手法
顧客データ	オペレータ	ターミナル	改ざんする
			漏えいする
	社外第三者	インターネット	盗聴する
			改ざんする

3.2.3 リスク分析　　リスク分析では，各脅威に対するリスクを次のように評価する。

（脅威が起こった場合の被害額）×（脅威の発生確率）

ここで，脅威の発生確率を決定することは困難なので，関与者の資質と攻撃方法の困難さを勘案して数値化する。なお，リスク分析結果は，あくまでも参考データであり，最終的な対策要否は顧客との話し合いによって決定する。

3.2.4 対策策定　　対策策定では脅威に対応する具体的な対策を選択することが目的で，二つのステップから成る。

⑴ 対策の絞込み　　あり得ない対策を排除して，対策方式を絞る。

⑵ 対策の評価　　取りうる対策に対し，定量的評価を行う。

これらはすべて設計者（あるいは顧客）への質問という形式で行い，利用する暗号の種類やビット数など具体的な対策を決定する。

3.3 実装段階

実装段階では，適切な実装によりシステム設計どおりのセキュリティが実現されていることを確認する。まず，単体実装完了後に単体脆弱（ぜいじゃく）性分析を行い，ソースコードの不備を専用のツールによって洗い出す。ソースコードの不備が修正された段階で単体実装を結合し，全体脆弱性分析を行ってシステム全体としての不具合を専用ツールによって洗い出す。全体脆弱性分析ツールには，実際にネットワークから擬似攻撃する機能も含まれており，ハッカーによる攻撃に対する脆弱性もチェックすることができる。

4 ISO/IEC15408認証取得コンサルテーションへの応用

ISO/IEC15408認証取得への関心が高まっており，当社ではこれを受けて**図3**の体系に基づく具体的な支援サービスの開発を行い，手始めとして社内及びグループ会社にて活用を開始した。提供されるサービスには，図3の体系に対して，集中支援サービスとレビューサービスの二つの方式がある。

⑴ 集中支援サービス　　適用組織の既存の開発体制とISO/IEC15408規格要件とのギャップを分析し，個々の組織に合った支援を行う。開発規定の作成からシステム開発の体制作り，及びセキュリティ設計など，組織メンバーと共同での集中的な支援を実施する。

⑵ レビューサービス　　集中支援サービスを受けた組織を対象としたサービスで，対象組織で作成した認証取得のための証拠資料に対して，ISO/IEC15408規格要件との適合性についてのレビューを実施する。

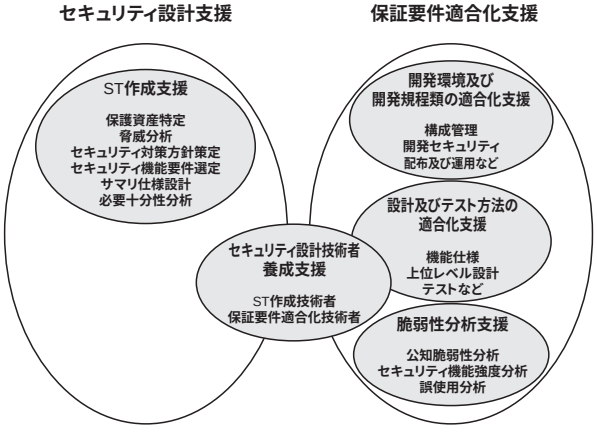

図3．ISO/IEC15408認証取得コンサルテーション体系 ― ISO/IEC15408認証取得支援のコンサルテーションサービスは，セキュリティ設計支援，セキュリティ設計技術者養成支援，保証要件適合化支援の三つから成る。

Consultation service menu for acquisition of security certification based on ISO/IEC15408

図3に示した項目のうち，セキュリティターゲット（ST）作成支援及び脆弱性分析支援については，セキュアシステム構築方法論を応用することによって，単にISO/IEC15408規格要件に適合するだけでなく，対象システムのセキュリティを高めることも考慮した効果的なコンサルテーションが可能となる。なお，ST作成支援と脆弱性分析支援以外の項目については，この論文の範囲を超えるため割愛する。

4.1 ST作成支援への応用

ST作成支援では，ISO/IEC15408で要求されている，保護資産洗い出し～脅威分析～セキュリティ対策方針策定～セキュリティ機能要件選定～サマリ仕様設計～必要十分性分析といった一連のST作成の流れに基づく技術支援を行う。

上記ST作成の流れのうち，保護資産特定～脅威分析～セキュリティ対策方針策定は，対象システムで何を保護し，保護対象がどのような脅威にさらされ，脅威に対してどのような対策を行うかといったシステム全体のセキュリティ設計方針を決定する意味で大変重要な部分と言える。しかし，この部分に対して，ISO/IEC15408では具体的な手法は示されておらず，必ずしも認証取得のための活動が対象システムのセキュリティを高めることにつながらないという問題がある。

セキュアシステム構築方法論のシステム設計段階でのアウトプットは，この問題を解決するために有効である。対象システムで何を保護資産とするかについては，本来保護資産が攻撃された場合の顧客事業へのインパクトに基づいて決定されるべきである。また，保護資産に対する脅威や対策方針についても，顧客事業を取り巻く環境や顧客組織のセキュリティポリシーに基づいて決定されるべきである。

セキュアシステム構築方法論は，設計事例とリスク分析に基づくセキュリティ対策方針の策定が可能である。

このように，ISO/IEC15408認証取得コンサルテーションに，セキュアシステム構築方法論を応用することにより，ISO/IEC15408認証取得のための活動と，対象システムのセキュリティを高める活動を両立し，最終顧客への付加価値を増大させることが期待できる。

4.2 脆弱性分析支援への応用

脆弱性分析支援では，ISO/IEC15408で要求されている，以下に示した設計にかかわる脆弱性分析及び公知脆弱性分析に対して技術支援を行う。

⑴ 設計にかかわる脆弱性分析　　機能仕様書や上位レベル設計書などの設計情報やソースコードの中に潜む脆弱性を検査し，脆弱性対策の策定及び実施を行う。

⑵ 公知脆弱性分析　　インターネットなどで公開された基本ソフトウェア（OS）やミドルウェアに関連する脆弱性情報，及び進入テストツールによる結果に基づいて，対象システムの脆弱性を検査し，脆弱性対策の策定及び実施を行う。

しかし，ISO/IEC15408では脆弱性分析に関して具体的な手法は示されておらず，分析者の経験やスキルに依存する面が大きいという問題がある。

セキュアシステム構築方法論の実装段階での単体脆弱性分析及び全体脆弱性分析で提供されるツール群は，この問題を解決するために有効である。単体脆弱性分析はソースコード及び関連する設計情報に潜む脆弱性と対策のDBを，また全体脆弱性分析はシステムに関する脆弱性と対策のDBをそれぞれ参照し，これらに基づいた脆弱性検査及び脆弱性対策の策定を行う。

このように，ISO/IEC15408認証取得コンサルテーションにセキュアシステム構築方法論を応用することで，担当者の経験やスキルに依存しない脆弱性分析を実現することが期待できる。

5 あとがき

当社では，システムへの包括的なセキュリティの作り込みを実現するためにセキュアシステム構築方法論を開発した。更に，セキュリティ機能実装の完全性を保証するための規格であるISO/IEC15408に関して，現在進めている認証取得コンサルテーションの中で，ISO/IEC15408に適合する開発プロセスに応用した。

この成果により，ISO/IEC15408で定義された手法の弱点を補った，システムへのセキュリティの作り込みが可能となった。現在，社内及びグループ会社を中心にこの成果の適用を進めており，官公庁向け総合的文書管理システムのST作成をはじめ，他に数件の案件への適用を進めている。

文　献

⑴ ISO/IEC. ISO/IEC15408: 1999 Information technology -Security techniques-Evaluation criteria for IT security. 1999, 639p.

⑵ Schneier,B. Secrets & Lies:Digital Security in a Networked World. New York, John Wiley & Sons, Inc., 2000, 412p.

小田原　育也　ODAHARA Ikuya

e-ソリューション社 SI技術開発センター SI技術担当主務。システム開発プロジェクト管理技術を経て，現在，システムセキュリティ技術の研究開発に従事。

Systems Integration Technology Center

秋山　浩一郎　AKIYAMA Koichiro

研究開発センター コンピュータ・ネットワークラボラトリー研究主務。セキュリティ技術の研究開発に従事。電子情報通信学会会員。

Computer & Network Systems Lab.

島田　　毅　SHIMADA Tsuyoshi

e-ソリューション社 SI技術開発センター SI技術担当主務。システム セキュリティの研究開発に従事。IEEE，米国プロジェクト管理学会会員。

Systems Integration Technology Center