セキュアSI$_{TM}$と流通ソリューションへの適用

SecureSI$_{TM}$ Innovative System Integrator and Its Application to Retail Solutions

西　真弓　■ NISHI Mayumi
山田　辰也　■ YAMADA Tatsuya
小田原　育也　■ ODAHARA Ikuya

東芝ソリューション（株）は，昨今のセキュリティ技術者の急激な需要の増加に対応するため，既に報告した“セキュアシステム構築方法論”を手順レベルまで具体化した“セキュアSI$_{TM}$”を開発し，当社ソリューションへの適用拡大とセキュリティ技術者の増強を進めている。当社の流通ソリューションの一つである“ポイント・顧客ソリューション”の構築への適用では，システムの構築に一定の経験を持つ技術者によるセキュリティ脅威分析の結果，ソリューションの提案に生かせる，体系的に整理されたセキュリティ対策が策定された。

Toshiba Solutions Corporation has developed SecureSI$_{TM}$, an innovative system integrator that materializes our security design methodology to the procedures level in order to ease the rapidly growing demand for security engineers. We are promoting the extensive application of SecureSI$_{TM}$ to our solutions development in parallel with the reinforcement of security engineers' capabilities. For example, we have applied SecureSI$_{TM}$ to the development of a "point service system for customers," one of our retail solutions, and have successfully drawn up and systematically deployed security measures for the system taking customers' proposals into consideration. The security threat analysis was carried out by a systems development engineer who was not greatly experienced in security engineering but was significantly assisted by SecureSI$_{TM}$.

1　まえがき

情報システムのインテグレーションでは，情報システムのライフサイクルを通じて包括的なセキュリティを実現することが重要である。東芝ソリューション（株）は，情報システムのインテグレーションにおけるセキュリティの向上という課題に対応するために，セキュアシステム構築方法論[(1)]の開発を行い，情報システムを含むソリューション構築やコンサルテーションサービスなどへの展開を実践してきた。

近年，情報システムへの依存度が高まるなかで，個人情報を含む機密情報漏えい事故の被害の増加[(2)]や，セキュリティ対策が不十分な情報システムの存在などが報告されている。更に，個人情報保護法や日本版SOX法[(注1)]などの法規制により厳密な情報管理が企業に求められるようになり，情報システムのセキュリティへの需要が増大している。

このような背景から，情報システム構築にかかわるセキュリティ技術者の増強が緊急の課題となっているが，急速なセキュリティの需要に応えられる人材を短期間で養成することは容易ではない。

当社は，この課題に対応するため，前述のセキュアシステム構築方法論を更に発展させ，セキュリティの専門スキルは持たないが情報システムの構築に一定の経験を持つ技術者がセキュリティの作り込みに活用できるレベルにまで具体化した“セキュアSI$_{TM}$（SI：System Integration）”を開発し，当社ソリューションへの適用拡大を進めている。ここでは，セキュアSI$_{TM}$の概要と，その流通ソリューションへの適用事例について述べる。

（注1）　米国のサーベンス・オクスリー法（SOX法）にならって整備された日本の法規制で，企業の会計監査制度の充実と内部統制強化を求めている。

2　セキュアSI$_{TM}$の概要

セキュアSI$_{TM}$では，**図1**に示すように情報システムのライフサイクルを七つのフェーズに分け，それぞれのフェーズでセキュリティ強化のために必要なタスクを定義している。全体として，セキュリティの提案，構築，及び維持を継続的に実現できる構成となっている。以下に，セキュアSI$_{TM}$で定義しているフェーズごとに，各タスクにおいて実施する内容を述べる。

(1)　業務分析フェーズ　　“業務リスク分析”では，分析対象業務の現状分析を行い，業務リスク（業務遂行上のリスク）の低減を実現した将来のシステム化の姿を策定し，移行のための計画を策定する。業務リスクを定量化し，施策によるリスク低減効果の検証を行うことで，効率的な分析作業をサポートする。

(2)　上流設計フェーズ　　“業務機能セキュリティ分析”では，保護すべき情報資産と業務環境から，TC（Threat Countermeasure）リストを活用して，想定されるセキュリティ脅威の洗い出しと，セキュリティ脅威に対抗するためのセキュリティ対策を策定する。TCリストは，保護す

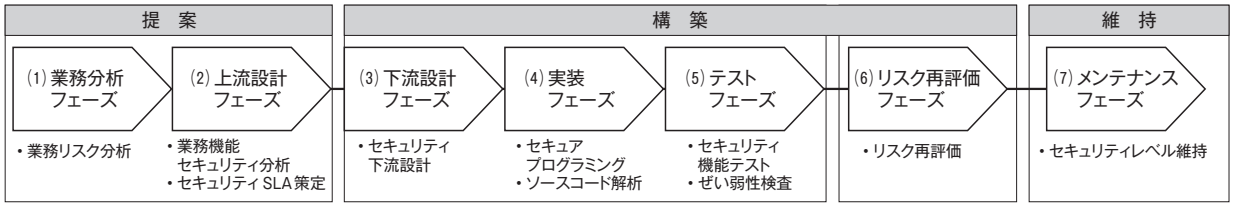


図1. セキュアSI$_{TM}$の七つのフェーズとタスク — セキュアSI$_{TM}$では，情報システムのライフサイクルを七つのフェーズに分類し，各フェーズにおけるタスクを定義している。各タスクの実施のために，ガイド，テンプレート，及びツールを提供する。

Seven phases and their tasks in SecureSI$_{TM}$

べき情報資産の種別，セキュリティ脅威発生箇所，典型的な脅威のパターン，及びISMS（Information Security Management System）詳細管理策や個人情報保護法など，各種基準や法制度で要求されるセキュリティ対策と関連付けられている。対策はIT（情報技術）又は運用によるもの，抑止，予防，検出，及び回復によるもの，などに分類される。このため，セキュリティの専門スキルを持たない技術者でも，業務環境で想定すべきセキュリティ脅威と，脅威に対抗するセキュリティ対策を効率的に導き出すことができる。

また，セキュリティ対策の実現責任範囲について，発注者の十分な理解と合意を得るために“セキュリティSLA（Service Level Agreement：責任範囲についての合意文書）の策定”を行い，内容について合意したうえで，セキュリティ対策の具体化に着手する。

(3) 下流設計フェーズ　“セキュリティ下流設計”では，セキュリティSLAで合意したセキュリティ対策のうち，ITによるセキュリティ対策を具体化する。設計で必要となるパラメータを定義したテンプレートや，設計レベルのぜい弱性の混入を防止するチェックシートの活用で，技術者のスキルに依存しない，一定のセキュリティ品質の確保を実現している。

(4) 実装フェーズ　“セキュアプログラミング”では，実装レベルでぜい弱性の混入を防止するために，アプリケーションの実装ノウハウをルール化したチェックリストを活用して詳細設計とコーディングを行うことで，セキュリティ品質の確保を実現する。

“ソースコード解析”は，単体テスト済みのソースコードに対して，検出パターンとして前述の実装ルールを定義した静的解析ツールを用い，客観的に実装ルールに違反した部分を検出する。

(5) テストフェーズ　“セキュリティ機能テスト”では，セキュリティ対策がふるまいとして正確に実現されていることをテストするため，システマティックなテスト項目の洗い出しをサポートし，セキュリティ機能の確実なテストを実現する。

“ぜい弱性検査”では，アプリケーションとインフラを対象として，公知のぜい弱性の混入を防止する。アプリケーション32項目とインフラ42項目のぜい弱性項目と，それらに対応した検査パターンが定義されており，検査補助ツールを活用して効率的なぜい弱性の検出ができる。

検出されたぜい弱性への対応は，前述のセキュリティ下流設計とセキュアプログラミングのノウハウに関連付けられたチェックリストを活用することで，技術者スキルに依存しない確実な対応を実現できる。

(6) リスク再評価フェーズ　“リスク再評価”では，構築の過程で確認された技術的課題や，運用環境で確認された課題を再評価し，それらがシステム運用上のぜい弱性とならないようにセキュリティSLAを見直し，合意を得る。

(7) メンテナンスフェーズ　“セキュリティレベル維持”では，セキュリティSLAに基づいて，発注者とベンダーのそれぞれの責任範囲でセキュリティレベルを監視し，セキュリティレベルの低下の傾向が見られた場合，これを是正する予防保守を実施する。是正作業がセキュリティSLAによる合意の範囲を超える場合は，次期システム提案として，業務分析フェーズ又は上流設計フェーズを開始する。

以上に述べたセキュアSI$_{TM}$の七つのフェーズを繰り返すことで，情報システムの継続的なセキュリティの維持を実現する。

3　流通ソリューションへの適用事例

近年の情報技術の急速な進展とインターネットなどの普及で，流通業においても情報システムを活用したサービスの需要が高まっている。特に，小売業界では，顧客情報や売上情報などの機密性の高い情報を取り扱う一方で，インターネットを活用した顧客サービスへのニーズが高い。

このようなニーズのなかで，以下に述べる“ポイント・顧客ソリューション”をはじめとする当社の流通ソリューションについても，セキュリティに関する方針を確立するとともに，官公庁や企業からの要求に応えられるセキュリティ技術者の育成が急務となった。以下に，この活動の一環として進めてきたソリューションのセキュア化の事例として，ポイント・顧客ソ

リューションへのセキュアSI$_{TM}$の適用と今後の展開について述べる。

3.1 ポイント・顧客ソリューションの概要

ポイント・顧客ソリューションの構成を**図2**に示す。

ポイント・顧客ソリューションは，ポイントカードを持つ会員情報の管理と，購買に応じて付加されるポイントの管理を統合したグループ企業向けのソリューションである。

図2に示すように，このソリューションでは，機密性を要する会員情報（個人情報を含む）を取り扱い，かつインターネットを介した顧客サービスを提供するため，体系的なセキュリティの作り込みが不可欠である。

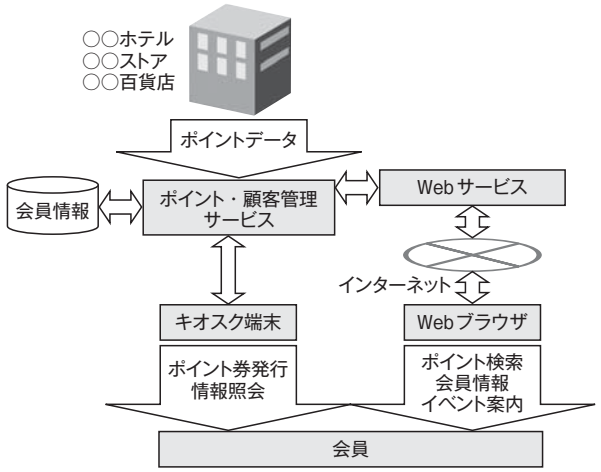


図2. ポイント・顧客ソリューション ― 会員がグループ企業のサービス（ホテル，店舗，など）を利用すると，利用内容に応じたポイントが付与される。ポイントは会員情報とともに管理されており，それらは会員自身がインターネットを介して参照及び更新できる。

Point service system for customers

3.2 業務機能セキュリティ分析の適用

今回適用したセキュアSI$_{TM}$のうち，上流設計フェーズで実施した業務機能セキュリティ分析について述べる。

一般に，体系的なセキュリティ対策の策定のためには，セキュリティ脅威分析などを実施するが，この実施には相応のスキルとコストを必要とする。業務機能セキュリティ分析では，手順レベルで示されたガイドやテンプレートを活用して，効率的に分析を実施できる。以下に，定義された手順に従い実施した今回の分析内容について述べる。

(1) 業務環境の抽出　　この手順では，システムが対象とする業務から，保護すべき情報資産，提供サービス（業務機能），及び関与者を洗い出す。具体的には，要求定義書の内容から各要素を抽出し，提供されるテンプレートを埋めていけばよい。

保護すべき情報資産としては会員情報（個人情報を含む），関与者としては会員，加盟店店員，加盟店管理者，システム管理者，システム保守者などを挙げた。また，業務機能としては，下記を含む168件を抽出した。

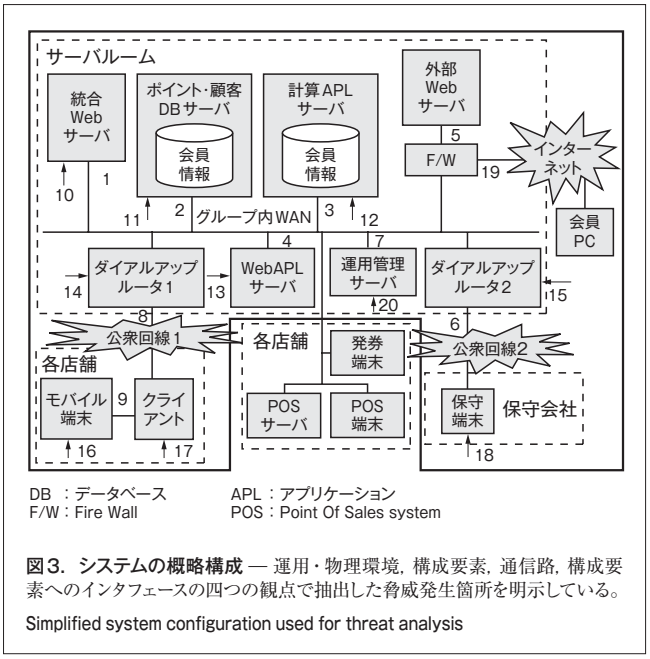
(a) 会員が，自身の会員情報を更新する。

(b) 加盟店店員が，顧客のポイントを更新する。

(c) 加盟店店員が，顧客の会員情報を閲覧する。

(2) 分析範囲の決定　　この手順では，物理的構成を示したシステム構成図を参照して，分析範囲を決定する。分析範囲は，責任分界点や環境の違い，保護すべき情報資産の位置，セキュリティポリシーといった要因から決定する。

今回の分析で使用したシステム構成を**図3**に示す。このソリューションでは，上記要因を考慮し，当社の構築責任範囲であり，かつ顧客情報の登録，閲覧，及び編集にかかわる部分（図3太線枠内）とした。



DB ：データベース　　APL：アプリケーション
F/W：Fire Wall　　POS：Point Of Sales system

図3. システムの概略構成 ― 運用・物理環境，構成要素，通信路，構成要素へのインタフェースの四つの観点で抽出した脅威発生箇所を明示している。

Simplified system configuration used for threat analysis

(3) 脅威発生箇所の抽出　　セキュリティ脅威分析では，想定するセキュリティ脅威を受入れ可能な範囲で洗い出すことが求められる。このため，業務機能セキュリティ分析では，まず，運用・物理環境，構成要素，通信路，構成要素へのインタフェースの四つの観点で，脅威発生箇所を網羅的に抽出する。

図3で，運用・物理環境はサーバルーム，各店舗，及び保守会社が該当し，構成要素は統合Webサーバなどのサーバ類，保守端末，モバイル端末などが該当する。通信路はグループ内WAN（Wide Area Network）及び公衆回線が該当し，また，図中の矢印と数字（1～20）は，抽出したインタフェースとその識別子である。

次に，抽出した脅威発生箇所における保護すべき情報資産の扱いを，それぞれテンプレートに記載する。例えば，インタフェース19については**表1**のように記載できる。

表1. インタフェースの記載例（抜粋）

Example of interface description (excerpt)

I/F名	利用法			
	アクセス元	関与者	対象（何を）	作用（どうする）
19	会員PC上のブラウザ	会員（顧客）	会員情報	閲覧・編集する

I/F：インタフェース

このように，保護すべき情報資産に対する，アクセス元，関与者，対象，及び作用を明らかにすることで，後述する脅威分析をシステマティックに実施することができる。また，この手順は，従来の要求定義とは別の視点から要件の妥当性を検証するためにも役だつ。

(4) 脅威分析　　脅威発生箇所における保護すべき情報資産の扱いから，どのようなセキュリティ脅威を想定すべきか，また，その脅威に対してどのような対策をとるべきか，TCリストとテンプレートを活用して分析する。

セキュリティ脅威を考える場合は，ガイドに従って，(3)でまとめた脅威発生箇所での関与者を悪意のある第三者に，また，本人を他人などに置き換えることで，効率的に実施できる。表1で示したインタフェース19の例では，“会員パソコン（PC）上のブラウザから第三者が会員情報を閲覧・編集する”，“会員PC上のブラウザから会員が他人の会員情報を閲覧・編集する”といった脅威を機械的に導き出すことができる。また，TCリストには，発生箇所以外に，データ，プログラム，機器類などの対象に応じた想定すべき脅威と対策が整理されており，これを活用することで，網羅的な脅威分析を実現できる。TCリストを活用して実施した脅威分析の結果，143件のセキュリティ脅威をシステマティックに抽出できた。最終的に，143件すべてのセキュリティ脅威に対抗できる67件の対策を策定した。**表2**は，その結果の一部を示したものである。

表2. 脅威分析結果（抜粋）

Results of threat analysis (excerpt)

対象I/F	脅威内容				対策			
	アクセス元（どこから）	関与者（誰が）	対象（何を，何に）	作用（どうする）	抑止・予防	検出	回復	運用
19	会員PC上のブラウザ	会員（顧客）	他人の会員情報	不正に閲覧・編集する	識別+認証（WebAPL） アクセス制御（WebAPL） 情報フロー制御（WebAPL）	ログ・監査（F/Wのログ）	バックアップ／リストア	契約（罰則）
19	会員PC上のブラウザ	非会員	他人の会員情報	不正に閲覧・編集する	情報フロー制御（F/W） 識別+認証（WebAPL） アクセス制御（WebAPL）	ログ・監査（F/Wのログ）	バックアップ／リストア	—

3.3 得られた効果と今後の展開

従来は専門スキルと経験を要したセキュリティ脅威分析を，セキュアSI$_{TM}$で示された手順どおりに実施することで，ソリューションとして盛り込むべきセキュリティ対策を効率的に策定できた。分析結果として，保護すべき情報資産，セキュリティ脅威，及びセキュリティ対策の論理的な関連付けがなされるため，セキュリティ対策の方針や効果の説明を含めた，効果的な提案活動の展開が可能となった。

セキュリティを差異化要素として，積極的なPRを行うとともに，今回の適用のノウハウや知見を共有し，技術者の増強と，他のソリューションへの展開を図っていく。

4 あとがき

当社は，セキュリティ技術者の急激な需要に対応するため，セキュリティの作り込みと維持のノウハウの形式知化を実現したセキュアSI$_{TM}$技術を開発した。個人情報の取扱いやインターネットの利用など機密性を要するソリューションを中心に，段階的な適用拡大を進めている。ここで紹介した流通業以外にも，官公庁，鉄道，道路，小売業など，既に多くのソリューションへの適用実績があり，高い評価を得ている。

今後は，適用ソリューションの拡大と，セキュアSI$_{TM}$を活用する技術者の増強を進め，セキュリティを当社のソリューションの強みとし，官公庁や企業が安心して業務やビジネスに活用できるセキュアソリューションの提供に貢献していく。

文　献

(1) 小田原育也，ほか．セキュアシステムインテグレーション．東芝レビュー．58，8，2003，p.11－14.

(2) JNSA.Japan Network Security Association. <http://www.jnsa.org/result/2005/20060803_pol01/index.html>，（参照　2007-03-09）.

西　　真弓　NISHI Mayumi

東芝ソリューション（株）IT技術研究所 研究開発部主任。システム・セキュリティ技術の研究・開発に従事。

Toshiba Solutions Corp.

山田　辰也　YAMADA Tatsuya

東芝ソリューション（株）ソリューション第一事業部 流通ソリューション部主任。流通業向けシステムの設計・開発に従事。

Toshiba Solutions Corp.

小田原　育也　ODAHARA Ikuya

東芝ソリューション（株）IT技術研究所 研究開発部主務，システム開発プロジェクト管理技術を経て，システム・セキュリティ技術の研究・開発に従事。

Toshiba Solutions Corp.