システムのライフサイクル全体でセキュリティを確保するセキュアSI

Secure SI Ensuring Security in Entire Life Cycles of Systems

内田　祐介　　小村　昌弘　　三輪　稔則

あらまし

近年，サイバー攻撃は増加傾向にあり，お客様にセキュアなシステムを提供するシステムインテグレーターの責務はますます大きくなっている。この責務を果たすためには，企画・要件定義から運用・保守にわたるシステムインテグレーション（SI）全体にセキュリティを取り入れる必要がある。そこで，富士通は「セキュアSI」に取り組んでいる。セキュアSIとは，品質の保証を目的としたこれまでのSIに，セキュリティの確保を加えるものである。このセキュアSIを実践できる人材を発掘・育成して，セキュリティマイスターとして認定し，お客様のプロジェクトへの貢献を目指している。

本稿では，セキュアSIの具体的な取り組みについて述べる。

Abstract

In recent years, cyberattacks have been on the rise, and the responsibility of system integrators offering secure systems to customers is becoming all the greater. In order to fulfill this responsibility, security must be incorporated into entire system integration (SI) that covers all processes, from planning and requirements definition to operation and maintenance. That is why Fujitsu is working on secure SI. Secure SI is ensured security added to conventional SI for the purpose of assuring quality. Fujitsu is discovering and developing human resources capable of practicing this secure SI and certifying them as Security Meisters to contribute to customers' projects. This paper describes specific secure SI activities.

1. まえがき

近年，情報システムへのサイバー攻撃が増加している。システムインテグレーターは，お客様に安心してシステムを活用いただくために，よりセキュアなシステムを提供しなくてはならない。システムインテグレーション（SI）の企画・要件定義，設計・構築，テスト，運用・保守といった各工程にセキュリティを取り入れることが，最適なセキュリティを確保するために重要である。

例えば，企画・要件定義工程においては，目的とする機能要件の定義と同時に，セキュリティ要件の定義がセキュリティ向上につながる。仮に，目的とする機能要件の定義のみを先行させた場合，後続するセキュリティ要件で定義できる内容が制限されることがある。設計・構築工程においても，初めからセキュアコーディングを実践していなければ，コーディング終盤における修正は保守性の低いコードを生み，セキュリティ強度の弱いコードにつながることがある。

これらの背景を踏まえて，富士通では「セキュアSI」を進めている（図-1）。セキュアSIとは，SIの各工程をセキュアな工程に変革させるものである。また，このセキュアSIを実践できる人材をセキュリティマイスターとして発掘・育成している。

本稿では，各工程におけるセキュアSIの具体的な取り組みについて述べる。更に，セキュリティ人材の発掘・育成について述べる。

2. セキュアSI

これまで富士通は，システム構築の標準プロセス体系（以下，SDEM）を整備してきた。[1] SDEMは，SIにおける作業漏れの防止，品質の保証，およびノウハウの整理・蓄積・再利用を目的としており，セキュリティは作業の一つとして定義されている。例えば，要件定義工程におけるリスク分析や設計工程におけるセキュリティ基盤設計，テスト工程におけるセキュリティ監査などがある。セキュアSIでは，セキュリティは作業の一つではなく，品質の保証と同じく，目的の一つと定義する。

次節以降では，各工程におけるセキュアSIの具体的な取り組みについて述べる。

2.1 企画・要件定義工程のセキュリティ

企画・要件定義工程のセキュリティとして，セキュリティ・バイ・デザイン（以下，SBD）[2] の考え方を推進している。昨今，SBDはIoTにおけるセキュリティとして注目を集めている。[3], [4] 富士通はIoTだけではなく，どのようなシステムであっても，SBDは必要と考えている。総務省では，脆弱性対策に係る体制の整備として，SBDの意識啓発・支援を実施している。[5] 今後，SBDの考え方を踏まえて設計された製品には認証マークを付与し，認証マークを付与された製品の使用を推奨することも検討されている。[5]

SBDは企画段階からセキュリティの検討を始め

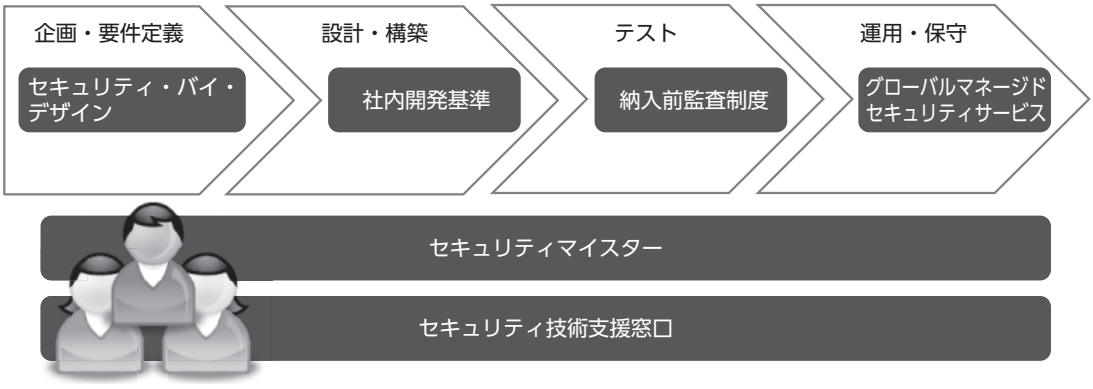

図-1　セキュアSI

るため，主要機能の設計などに起因した制約によってセキュリティ対策を妥協することはない。最適なセキュリティ対策を実現するために，主機能の果たす目的を変えることなく実現方法の変更を視野に入れる。例えば，金融系のWebアプリケーションでは，ソフトウェアキーボードを導入した。ハードウェアキーボードにより入力するシステムでは，キーボード操作を盗み取るキーロガーは脅威である。そのため，セキュリティを確保するためにキーロガーの対策を実施することが不可欠である。これに対しソフトウェアキーボードでは，キーロガーの脅威自体を排除している。

富士通では，SIに関わる全てのSEがSBDによる企画・要件定義を主体的に実践し，よりセキュアなシステムを提案・構築できるよう教育している。その一環として，これまで役員・本部長を含め，約15,000人のSEを対象にSBDの考え方や効果，重要性の認識を広める教育を実施してきた。現在は，SBDの実践的手法を習得する教育の展開に取り組んでいる。そして，この思想に基づいてお客様に最適なセキュリティを提案している。

2.2 設計・構築工程のセキュリティ

設計・構築工程のセキュリティとして，社内開発基準（セキュアWebガイド，お客様インターネット接続システムにおけるセキュリティ必須要件）を策定している。[6]

現在，国内外には，Payment Card Industry Data Security Standard（PCI DSS）やNIST SP-800シリーズをはじめとした多種多様なセキュリティ基準がある。業種によって準拠すべき基準も異なっている。この多種多様なセキュリティ基準を包含する基準を策定することで，あらゆる業種・業態への適合を可能にしている。

国内外のセキュリティ基準は設計要件にとどまっており，構築工程の基準となるものではない。構築工程における社内開発基準として，具体的な防御方法にまで踏み込んだ基準を規定した。

社内開発基準は常に最新動向に追随できる体制を取っている。この社内開発基準は，2005年に第1版を発行してから，原則6か月ごとに改版を続けている。定期の改版以外にも社会的影響の大きい攻撃方法が出現したり，効果的な防御技術が開発されたりした際には，速やかに調査・検証を行った上で改版している。

2.3 テスト工程のセキュリティ

テスト工程のセキュリティとして，お客様に納入するシステムに脆弱性がないか，アプリケーション脆弱性検査ツールで診断し，検査部門が診断結果を確認している。[7] 従来の脆弱性診断は，診断のためにシステム外部からアクセスして脆弱性を検知するものであった。そしてこの方法は，システムの構築が完了した最終テスト工程でなければ実施できなかった。

一方，セキュアSIでは，詳細かつ高精度にシステムの内部を直接診断できるソースコード診断を導入し，脆弱性を検知している。従来の脆弱性診断では検知結果から原因箇所を探す必要があったが，ソースコード診断では原因箇所を特定した的確な対応が可能となる。またソースコード診断は，構築工程の途中でも実施できる。これによって，セキュアなコードが作り込まれていることを確認しながら効率的にシステムを構築できる。

2.4 運用・保守工程のセキュリティ

運用・保守工程のセキュリティとして，アメリカ国立標準技術研究所（NIST）がサイバーセキュリティフレームワーク（CSF）[8] で定義している，攻撃の検知・対応・復旧のフェーズに対応する仕組みを構築している。この仕組みを築いた背景には，世界のサイバー攻撃の激化がある。従来は，防御強化がセキュリティ対策の中心であったが，今日では，仮にシステムの防御を突破されたとしても，速やかに攻撃を検知し，影響範囲を見極めて封じ込め，更に阻害された機能やサービスを回復させるという考え方が，システムの安全な運用には必要不可欠となっている。運用・保守強化の仕組みの中心となるのは，人材とサービスである。

人材面では，セキュリティマイスターという制度に基づいた人材育成・強化を実施している。近年では，ログ分析などを自動化する動きも広まってきているが，今後も人による運用・保守は欠かせない。防御を突破するほど巧妙かつ複雑になっている高度

サイバー攻撃に対処するには，検知・対応・復旧において自動化できない臨機応変な分析・判断が求められるからである。この分析・判断できる人材をセキュリティマイスターとして育成している。この詳細については，次章で述べる。

サービス面では，グローバルマネージドセキュリティサービス（GMSS）による運用品質の強化を実施している。富士通の保有する最新セキュリティ技術，お客様に寄りそう実システムでの運用経験，高度な分析・判断スキルを持つ人材のノウハウを統合し，社内の運用の標準化を図るとともに，お客様への提案・提供を可能にしている。詳細については，本誌掲載の「お客様のICT環境を守るグローバルマネージドセキュリティサービス」を参照されたい。

3. セキュリティマイスター

3.1 体制と役割

2014年以降，富士通はセキュリティ人材の発掘・育成を目的に，セキュリティマイスター認定制度を導入している。[9] セキュリティ人材の発掘とは，社内に点在する各技術分野のセキュリティ知識・ノウハウを持つ人材を探し出すことである。育成では，発掘してきた人材をお客様にセキュリティの専門技能という付加価値を提供できるセキュリティマイスターとして育て上げる。2019年3月時点で約4,000人をセキュリティマイスターとして認定している。今後，2021年3月末までに11,000人の認定を目指している。この目標を達成することによって，全てのお客様プロジェクトに対して，複数名のセキュリティ要員をバランス良く配置できると考えている。セキュアSIを担うセキュリティマイスターを図-2に示す。以下，セキュリティマイスターを前章で述べたSIの四つの工程に当てはめて，その役割を紹介する。

(1) 企画・要件定義工程

企画・要件定義工程では，セキュリティプロダクトエキスパートが活躍する。この人材は，セキュリティプロダクトのメリット，デメリットを熟知しており，システム構成，お客様のニーズに合わせた製品選定を行う。また，セキュアネットワークコーディネーターが活躍する。この人材は，ネットワークプロダクトとその構成について熟知しており，ネットワーク構成の提案を行う。

(2) 設計・構築工程

設計・構築工程では，サイバーセキュリティエンジニアが活躍する。この人材は，社内開発基準をはじめ，業務・業種固有のガイドラインやフレームワークの知識・スキルを保持しており，基準に準拠したシステムを設計・構築する。

(3) テスト工程

テスト工程では，設計・構築工程と同じくサイバーセキュリティエンジニアが活躍する。ソースコード診断の導入により，構築と並行してテストを行うようになった。この工程では，ペネトレーションテスターも活躍する。ペネトレーションテストとは，実際の攻撃手法を用いて脆弱性の有無を確認する手法である。ペネトレーションテストのスキルを活かし，サーバおよびネットワーク機器，アプリケーションに脆弱性がないことを攻撃者視点から確認している。

(4) 運用・保守工程

運用・保守工程では，セキュリティアナリストが活躍する。この人材は，ネットワーク上のログやパ

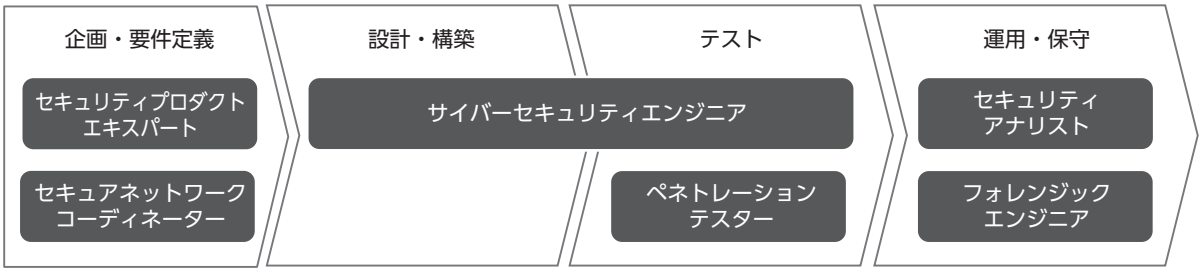

図-2　セキュアSIを担う人材像

ケットを分析するスキルに長けており，どのような攻撃が行われているのか突き止める。また，システムに対する影響範囲を特定し，暫定対処案の提示から恒久対処の実行支援まで行う。

また，フォレンジックエンジニアが活躍する。この人材は，GMSS内で証拠を保全および解析し，攻撃者によって何が行われたかタイムラインを作成する。タイムラインを用いた顧客報告も担っている。

上記では6種類の人材像を紹介したが，セキュリティマイスターでは全14種類の人材像を定義している。これらの人材像は，統合セキュリティ人材モデル[10]にも採用されている。

3.2 セキュリティ技術支援窓口

セキュリティマイスター向けの支援窓口を設置している。セキュリティマイスターは，各技術分野のセキュリティ知識･ノウハウを持つ専門家であるが，ときには専門外の技術分野まで含めた幅広い知識・ノウハウを求められることもある。このような場合にセキュリティ技術支援窓口を活用することで，セキュアな設計に関する疑問やセキュリティ技術全般に関する疑問を解消し，幅広いセキュリティ知識を持った技術者と連携しながらお客様のプロジェクトを推進できる。

4. むすび

本稿では，SIの各工程にセキュリティを取り入れるセキュアSIの取り組みについて述べた。また，セキュアSIを実践する人材の発掘・育成について述べた。

今後，AIが台頭するにつれて，システムはますます複雑になっていくと予想される。セキュアSIでは，セキュアなシステムの骨格にあたるアーキテクチャーの定義にも取り組み始めている。これからも，富士通はセキュアなシステムをお客様に提供し続けることで，お客様のビジネスを支えていく。

参 考 文 献

(1) 室中健司ほか：システム構築の標準プロセス体系：SDEM．FUJITSU, Vol.63, No.2, p.193-199（2012）．
http://img.jp.fujitsu.com/downloads/jp/jmag/vol63-2/paper15.pdf

(2) 内閣官房情報セキュリティセンター（NISC）：「情報セキュリティの観点から見た行政情報システムの望ましいあり方」と「行政情報システムの企画・設計段階からのセキュリティ確保に向けた取組み（セキュリティ・バイ・デザイン［SBD］）」について．
http://www.nisc.go.jp/conference/seisaku/dai15/pdf/15siryou02.pdf

(3) IoT推進コンソーシアム，総務省，経済産業省：IoTセキュリティガイドラインver1.0．p.6.
http://www.soumu.go.jp/main_content/000428393.pdf

(4) 内閣サイバーセキュリティセンター（NISC）：安全なIoTシステムのためのセキュリティに関する一般的枠組．p.2.
https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf

(5) 総務省：IoTセキュリティ総合対策プログレスレポート2018．p.3-5.
http://www.soumu.go.jp/main_content/000566458.pdf

(6) 富士通：富士通グループ情報セキュリティ報告書2014．お客様の情報資産を守るための富士通グループの取り組み．p.13.
http://www.fujitsu.com/downloads/JP/archive/imgjp/jcsr/csr/management/security/2014/security2014.pdf

(7) 富士通：富士通グループ情報セキュリティ報告書2016．セキュリティ向上への取り組み．p.13.
http://www.fujitsu.com/jp/imagesgig5/security-2016.pdf

(8) アメリカ国立標準技術研究所（NIST）：サイバーセキュリティフレームワーク（CSF）．p.6-8.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

(9) 富士通：セキュリティマイスター認定制度．
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-meister/certification/index.html

(10) 富士通：NEC・日立・富士通、サイバーセキュリティ技術者の共通人材モデル「統合セキュリティ人材モデル」を策定．
http://pr.fujitsu.com/jp/news/2018/10/24-1.html

著者紹介

内田　祐介（うちだ　ゆうすけ）
富士通（株）
サイバーセキュリティ事業戦略本部
セキュアSIの定義と推進，セキュリティマイスターの技術支援に従事。

小村　昌弘（こむら　まさひろ）
富士通（株）
サイバーセキュリティ事業戦略本部
セキュアSIの定義と推進，セキュリティマイスターの技術支援に従事。

三輪　稔則（みわ　としのり）
富士通（株）
サイバーセキュリティ事業戦略本部
セキュアSIの定義と推進，セキュリティマイスターの技術支援に従事。