スマートコミュニティシステムのための セキュアシステム構築技術 セキュアSI$_{TM}$

SecureSI$_{TM}$ Secure System Development Methodology for Information Systems of Smart Communities

小田原　育也　　小島　健司
■ODAHARA Ikuya　■KOJIMA Kenji

ICT（情報通信技術）を活用した新しい社会インフラシステムとして，エネルギー利用効率の最適化などを実現するスマートコミュニティが注目されている。そこでは，情報系と制御系のシステムが連携し，収集した様々なセンサ情報に基づく情報の見える化やコミュニティ最適化のための機器の制御を行う。このため，情報系システムで要求されるデータ機密性に加えて，制御系システムで要求されるサービス可用性といった，異なるシステム要求特性に起因するセキュリティ脅威への新たな対応が必要となる。

東芝ソリューション（株）は，制御系システムに要求される特性を考慮し，情報系と制御系のシステムの接続によるセキュリティ脅威に対応できるセキュアシステム構築技術“セキュアSI$_{TM}$（SI：System Integration）”の開発を進めている。

Smart communities, which represent the next-generation social infrastructure system, have been attracting considerable attention as a solution for the optimization of energy use efficiency.　A smart community system, consisting of both information systems and control systems, offers information visualization based on data collected by various sensors and controls equipment so as to optimize the community.　It is therefore necessary to protect such systems against new types of security threats resulting from different requirements, such as the priority given to data confidentiality in information systems versus the priority given to availability of services in control systems.

In response to this situation, Toshiba Solutions Corporation has been developing SecureSI$_{TM}$, a secure system development methodology for information systems taking the characteristics of smart community systems into consideration.

1　まえがき

電気，水，交通などの利用状況の見える化や，それらに基づくエネルギー供給量の制御など，ICTを活用して社会全体のエネルギー利用効率を最適化するスマートコミュニティへの期待が高まりつつある。スマートコミュニティの実現のためには，センサなどからの情報の収集と機器の制御を行う制御系システムと，収集した情報の見える化や最適化を実現する情報系システムとの接続が不可欠である。

しかし，物理的な隔離や，独自のインフラ及び通信プロトコルなどによるセキュリティ確保を前提とする制御系システムを，インターネットなどと接続された情報系システムに接続することは，社会インフラシステムを標的とするサイバー攻撃を受けるおそれがある[(1)]。このため，情報系システムと制御系システムの接続によるセキュリティ脅威への新たな対応が求められる。

東芝ソリューション（株）は，情報システムのセキュリティ確保のため，ライフサイクルを通じてセキュリティを作り込み維持するためのセキュアシステム構築方法論[(2)]及び，それを情報系システム向けに具体化したセキュアシステム構築技術“セキュアSI$_{TM}$（SI：System Integration）”を開発し，適用を推進している[(3)]。更に当社は，制御系システムに要求される特性を考慮し，前述のスマートコミュニティの課題に対応できる構築技術としてセキュアSI$_{TM}$の拡張を進めている。

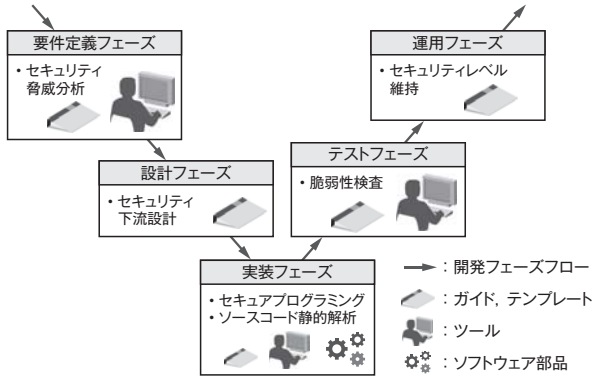

図1．セキュアSI$_{TM}$のフェーズとタスク ― 情報システム構築の各フェーズでセキュリティを確保するためのタスクを定義し，ノウハウを具体化したガイド，テンプレート，ツール，及びソフトウェア部品を提供する。
Development phases and tasks in SecureSI$_{TM}$

2　セキュアSI$_{TM}$の概要

情報システム構築の各フェーズにおけるセキュリティ確保のためのタスクと，セキュアSI$_{TM}$が提供するガイド，テンプレート，ツール，及びソフトウェア部品の対応を**図1**に示す。セキュアSI$_{TM}$の活用により，セキュリティ技術の専門家でないシステム構築技術者であっても，構築対象システムに対するセキュリティの作込みと維持を効率的に実施し，一定のセキュリティ品

質を確保できる。

各フェーズのタスクの概要と特長について以下に述べる。

(1) 要件定義フェーズ　セキュリティ脅威分析では，構築対象システムの要件に含まれる保護すべき情報資産や，関与者，業務機能，システム構成などの項目から，セキュリティ脅威分析ツール SecuScope$_{TM}$を用いて，想定されるセキュリティ脅威の抽出と対策を策定する。

(2) 設計フェーズ　セキュリティ下流設計では，(1)のセキュリティ脅威分析で策定した対策の実現方式の具体化と，脆弱（ぜいじゃく）性の混入防止に必要な作業を行う。対策の実現方式の具体化では，仕様記述に必要となる各種セキュリティ機能のパラメータを定義できる対策策定シートを用いる。更に，OS（基本ソフトウェア）やミドルウェアなどのインフラに関わる脆弱性の混入を設計段階で防止するためのチェックリストを活用する。これらにより，セキュリティ設計の品質を確保する。

(3) 実装フェーズ　セキュアプログラミングでは，アプリケーションレベルで脆弱性混入を防止する実装ノウハウをルール化した実装チェックリスト，及び実装チェックリストの内容をソフトウェア部品化して実装スキルへの依存を低減するセキュリティコンポーネントを用いる。

ソースコード静的解析では，前述の実装チェックリストに対する違反やセキュリティコンポーネントの誤った使用を検出する。この仕組みは，オープンソースソフトウェアをベースとするツールとして実現しており，問題点の検出に関してスキル依存を低減できる。

(4) テストフェーズ　脆弱性検査では，アプリケーションと，OSやミドルウェアなどのインフラを対象とし，既知の脆弱性を検出する。ツールによる効率的な脆弱性の検出に加えて，専門家による検査手順を具体化したチェックリストやガイドによってきめ細かな検査もできる。

(5) 運用フェーズ　セキュリティレベル維持では，運用段階に入った情報システムのセキュリティレベルを，ベースラインに基づいて維持するための方法と体制を定義したガイドを提供している。これに基づき運用することによって，セキュリティレベルの低下傾向が見られた場合の適切な予防保守，及びインシデント対応を実施できる。

3　スマートコミュニティシステムのセキュリティ課題

スマートコミュニティシステムの構成例を**図2**に示す。

情報系システムでは，アクセス権限を持つ利用者や外部システムに対して，制御系システムから得られた電力使用量などの見える化機能を提供する。制御系システムでは，フィールド機器のセンサから電力使用量などの監視データをリアルタイムに収集する。更に，外部システムから得られた情報と合わせて

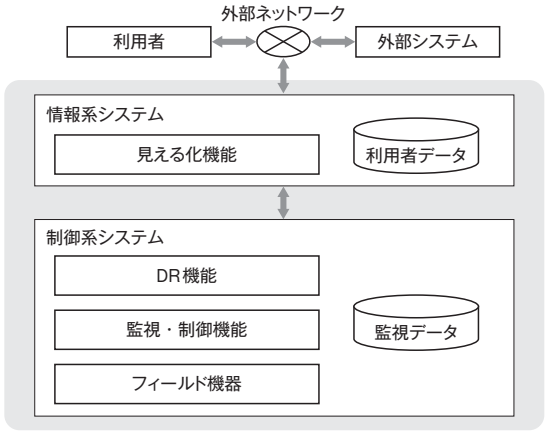

図2．スマートコミュニティシステムの構成例 — 情報系システムと制御系システムを接続することで，見える化やDRなどのサービスを提供する。
Typical configuration of smart community system

デマンドレスポンス（DR）機能で決定した電力消費の制御方針に従って，監視・制御機能がフィールド機器を制御する。このようにして，制御系システムと情報系システムが接続した構成で電力使用量の最適化などのサービスを実現する。

一方セキュリティの観点で見ると，制御系システムでは，これまでの物理的な隔離や，独自インフラ，独自通信プロトコルなどを前提としたシステム保護の方針を見直していく必要がある。すなわち，情報系システムを介した外部ネットワークとの接続と，インフラや通信への標準技術の採用により，情報系システムと同様に外部からの侵入に対抗するセキュリティ対策が必要になる。また制御系システムでは，リアルタイム性が要求されるなど，情報系システムとは異なるシステム要求特性も考慮する必要がある。したがってシステム構築では，接続する個々のシステムのシステム要求特性の違いに着目し，これらに起因するセキュリティ脅威に対抗することが重要である。

情報系システムと制御系システムで考慮すべきシステム要求特性の比較を**表1**に示す。制御系システムでは，セキュリティ特性として可用性が重視され，提供機能や機器の保護が求められる。また，利用できるリソースが少ない，処理遅延が許容されないといった制約があることから，セキュリティ対策の策

表1．情報系システムと制御系システムのシステム要求特性の比較
Comparison of required characteristics of information system and control system

システム要求特性	情報系システム	制御系システム
セキュリティ特性優先順	機密性重視	可用性重視
保護対象	情報	機能，機器
稼働条件	計画停止が容易	連続稼働が前提
リソース制約	十分なリソース	最小限のリソース
処理遅延	許容できる	許容できない

定の際に，これらの制約を考慮する必要がある。

一方，制御系システムについては，昨今のセキュリティリスクの高まりから国内外の各種団体によりセキュリティ基準や，規格，ガイドラインの策定が進められている。その中でも代表的なものがIEC 62443（国際電気標準会議規格62443）[4]であり，制御系システムのセキュリティを確保するために必要な原則や実現の手段がまとめられている。次章で述べるスマートコミュニティシステムのためのセキュアSI$_{TM}$を考える際にも，それらの考え方を取り入れている。

4　スマートコミュニティシステムへの対応

3章で述べたスマートコミュニティシステムに対するセキュリティ課題及びセキュリティ規格を考慮し，スマートコミュニティシステムに対しても適用できるセキュアシステム構築技術セキュアSI$_{TM}$の開発を進めている。

4.1　要件定義フェーズの対応

スマートコミュニティシステムでは，表1に示すようにシステム要求特性が異なるシステムや，物理的に離れて設置されたシステム，オーナーが異なるシステムなど，統一的なセキュリティ方針を適用できないシステムが互いに有機的に連携してサービスを提供するという特徴がある。このような多数のサブシステムが連携した大規模システムを安全に構築するためには，個々のサブシステムを安全に構築したうえで，サブシステム間を安全に接続するというアプローチが有効である。

このアプローチに対応したセキュリティ脅威分析手法とセキュリティ脅威分析ツールSecuScope$_{TM}$について以下に述べる。

4.1.1　セキュリティ脅威分析手法　セキュリティゾーンの分割，脅威の抽出，及び対策の策定の手順によって行う。

(1)　セキュリティゾーンの分割　構築対象システムをシステム要求特性や，物理的な設置場所，システムオーナーなどの違いに基づきセキュリティゾーンに分割する。

(2)　脅威の抽出　セキュリティゾーンを対象に，想定されるセキュリティ脅威（以下，脅威と呼ぶ）を洗い出す（**図3**）。

(a)　セキュリティゾーン内の脅威抽出　セキュリティゾーン内に存在する機器の故障，盗難，ウイルス感染，及び情報の不正持出しといった脅威Aを抽出する。

(b)　セキュリティゾーン間の脅威抽出　この脅威は，セキュリティゾーン外部からセキュリティゾーンの外部インタフェース（I/F）へのアクセスにより発生する脅威Bと，セキュリティゾーン間を流れるデータに対する脅威Cに分類される。Bの例として，セキュリティゾーンが提供する機能への第三者による不正アクセスなどが，Cの例として，通信の盗聴や改ざんなどが該当する。

(3)　対策の策定　洗い出した脅威に対して必要な対策を検討する。この際，セキュリティゾーンに対するシステム要求特性を考慮し，脅威への対策優先度を決定する。例えば，機密性重視のセキュリティゾーンでは，処理する情報の漏えいを引き起こす脅威のリスクが高いため，アクセス制御や暗号化といった対策が優先される。これに対し，可用性重視のセキュリティゾーンでは，システムのサービス停止を引き起こす脅威のリスクが高いため，ネットワークやサーバの多重化といった対策が優先される。

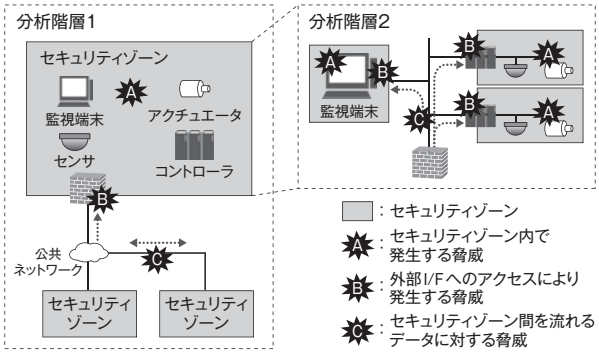

図3．セキュリティ脅威分析の考え方 — 構築対象システムを，システム要求特性などに基づきセキュリティゾーンに分割して分析を行う。セキュリティゾーンを階層的に扱うことで，システム仕様の明確さに応じた分析が可能である。

Concept of security threat analysis

この手法により，複数のセキュリティゾーンから構成されたシステム全体の安全性を確保するために必要な対策を策定できる。

また，図3の例に示すように，分析階層1の粒度でセキュリティゾーンを分割しセキュリティ脅威分析を実施したうえで，更にそのゾーンを分析階層2のように複数のゾーンに分割し，再帰的にセキュリティ脅威分析を行うことができる。これを利用して，システム仕様が明確でない段階では粗い粒度でセキュリティゾーンを定義し，システム仕様が明確になった段階で粒度を細かくして分析するというように，システム仕様の明確さに応じたセキュリティ脅威分析を実施できる。

4.1.2　SecuScope$_{TM}$　セキュリティ脅威分析手法を支援するためのツールで，分析を効率的に進めるだけでなく，分析担当者による分析精度のばらつきを排除することを目的としている。脅威抽出処理の概要を**図4**に示す。

SecuScope$_{TM}$は，分析エンジンと脅威-対策データベース（DB）から構成される。脅威-対策DBは，システムに存在する典型的なセキュリティ脅威とその対策をリスト化し記録したものである。具体的には，図3に示した3種類の脅威A，B，Cに関して典型的なものを，発生箇所（どこで），保護資産（何を），関与者（誰が），脅威内容（どうする）の組で表現しており，各脅威に対して有効な対策（どう守る）を示している。この内容は，セキュリティ専門家のノウハウや各種セキュリティガイドラインの内容を集めたもので，これを用いることでセキュリティ専門家以外の技術者でも質の高いセキュリティ脅威分析

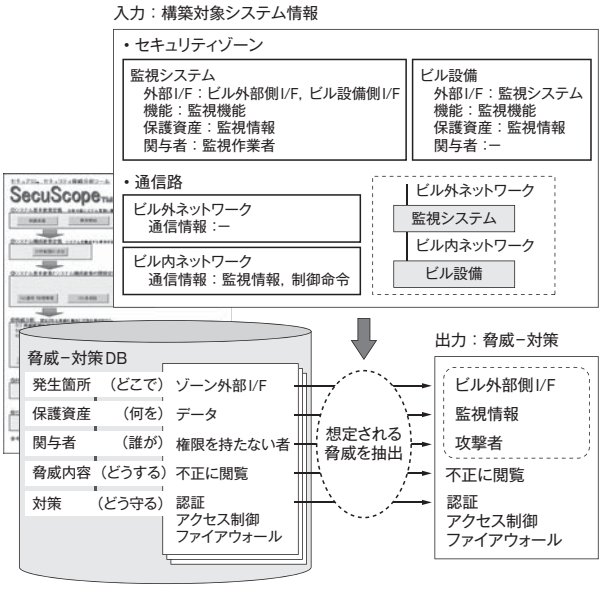

図4．SecuScope$_{TM}$によるセキュリティ脅威分析 — SecuScope$_{TM}$では，構築対象システム情報を入力し，脅威－対策DBの情報を用いて，構築対象システムに存在するセキュリティ脅威及びそれに対する対策を出力する。

Process of security threat analysis using SecuScope$_{TM}$

を実施できる。

分析時にはまず，構築対象システムの情報として，セキュリティゾーンや通信路の情報を入力する。セキュリティゾーンに関しては，セキュリティゾーンが持つ外部I/F，機能，保護資産と関係する関与者及びその権限を，通信路に関しては，通信路で受け渡す通信情報を定義する。次にこの入力に基づき脅威－対策DBに登録された脅威の絞込みを行い，脅威の項目を構築対象システムの情報で置換していくことで，構築対象システムのセキュリティ脅威とそれに対する対策候補を出力する。

現在，SecuScope$_{TM}$の実システム適用を進めるとともに，効率的な対策策定を目的として，抽出脅威への対応優先度を示すリスク値を，システム要求特性を考慮して算出するリスク評価技術の導入を検討している。

4.2　設計フェーズと実装フェーズの対応方針

これらのフェーズでは，要件定義フェーズで策定した対策を具体化し実装する。特に制御系システムでは，表1で示したように機器のリソースや処理のリアルタイム性が問題となることが多く，これらを考慮した方式設計や実装が重要になる。

したがって，セキュリティ下流設計，セキュアプログラム，及びソースコード静的解析といったタスクに対しては，情報系システム向けの開発成果をベースに，制御系システムの環境を考慮したチェックリストの拡充や，低リソースの機器でも利用できる軽量セキュリティライブラリの提供を検討している。

4.3　テストフェーズと運用フェーズの対応方針

情報系システムに対する脆弱性については，各種の機関が公開している情報を参考に，構築時に参照可能なチェックリストやガイドを整備するとともに，オープンソースソフトウェアの活用による脆弱性検査ツールの整備を行ってきた。これに対して，制御系システムの脆弱性に関しては，一般的にもまだ十分な取組みがなされていない。制御系システムの機器は，管理が行き届かない場所に設置される場合も多くリスクが高いうえに，連続稼働が求められパッチ適用などによる一時的な停止も許されないといった制約から，開発段階から既知の脆弱性に対して漏れなく対応しておくことが重要になる。

このため，脆弱性検査とセキュリティレベル維持に対しては，制御機器に対する脆弱性検査技術，制御系システムの特性を考慮した予防保守，及びインシデント対応のためのガイドラインの提供を検討している。

5　あとがき

当社は，スマートコミュニティシステムの実現において不可欠となる情報系システムと制御系システムが接続することによるセキュリティ課題を整理し，それらに起因するセキュリティ脅威に対抗できるセキュアシステム構築技術 セキュアSI$_{TM}$の開発に取り組んでいる。

今後は，当社のスマートコミュニティ関連ソリューションや実証実験システムなどへのセキュアSI$_{TM}$の適用を進め，得られた知見をフィードバックして更に実践的な構築技術とするとともに，社会インフラシステムの信頼性向上に寄与していく。

文　献

(1) 情報処理推進機構（IPA）. “2010年度制御システムの情報セキュリティ動向に関する調査報告書”. IPAホームページ. ＜http://www.ipa.go.jp/security/fy22/reports/ics_sec/index.html＞,（参照2011-10-01）.

(2) 小田原育也 他. 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.

(3) 西　真弓 他. セキュアSI$_{TM}$と流通ソリューションへの適用. 東芝レビュー. **62**, 7, 2007, p.7－10.

(4) IEC. IEC 62443: 2010. Industrial communication networks - Network and system security.

小田原　育也　ODAHARA Ikuya

東芝ソリューション（株）IT技術研究所 情報セキュリティラボラトリー主任研究員。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.

小島　健司　KOJIMA Kenji

東芝ソリューション（株）IT技術研究所 アドバンストソリューションズリサーチラボラトリー研究主務。情報セキュリティ技術及び応用システムの研究・開発に従事。

Toshiba Solutions Corp.