社会インフラを支える制御システムセキュリティ

中野 利彦 Nakano Toshihiko
清水 勝人 Shimizu Katsuhito
山田 勉 Yamada Tsutomu
鍛 忠司 Kaji Tadashi

近年の社会インフラのネットワーク化に伴い，そこに供される制御システムのセキュリティリスクが高まっている。このような状況に対応するため，国際標準化団体や業界団体では，制御システムへのセキュリティ要件を定める活動が進められている。
日立グループは，サイバー攻撃の潮流，長期間の運用など社会インフラに求められる要件を整理するとともに，これらの要件を実現するためのソリューションと製品を提供している。また，制御システムのセキュリティ向上のために産官学が連携して設立した技術研究組合制御システムセキュリティセンター（CSSC）に設立当初から参画し，制御システムにおけるセキュリティ向上のための施策を連携して進めている。

1. はじめに

近年，社会インフラのネットワーク化が進展し，サイバー攻撃の脅威が現実のものになってきている。そのため，社会インフラシステムでも多種多様なサイバー攻撃に対するセキュリティ対策を実装することが必要不可欠になっている。

このようなセキュリティ対策は，漏れやむだがないように実装されることが求められるため，国際標準化団体においてセキュリティに対する要件やセキュリティを評価するための軸の検討が進められている。例えば，IEC（International Electrotechnical Commission）では，制御システム向けのセキュリティ規格IEC 62443[1)]において，セキュリティ要件の整理，リスク分析の軸として安全衛生や環境（HSE：Health Safety Environment）への影響の観点での分析要求，セキュリティ対策の強度を評価する軸としてセキュリティ保証レベル（SAL：Security Assurance Level）を規定している。また，ITU（International Telecommunication Union）では，Cyber Security Indicator[2)]やGlobal Cybersecurity Index[3)]といった評価軸の開発・標準化に取り組んでいる。そのほか，ETSI（European Telecommunications Standards Institute）でも，Information Security Indicators[4)]という評価軸の開発を進めている。

これらの評価軸には，ある時点（多くは設計段階）の静的なセキュリティ対策の強靭（じん）さを数値化あるいは評価しているものが多い。しかし，社会インフラに供される制御システムは，長期間にわたって稼働し続けることが大前提であり，社会インフラシステムは長期間運用することから多種多様なシステムが混在する。また，昨今のサイバー攻撃技術の急激な進展により，これまで全く予期しなかった攻撃が瞬く間に攻撃手法として一般化するという状況が頻繁に発生するようになってきている。

このような背景を鑑みると，社会インフラのセキュリティは，各構成システムの設計段階での対策だけでは十分とは言いがたく，長期間運用におけるサイバー攻撃技術の進歩を踏まえ，対策を適宜強化できるようにすることが必要である。日立グループは，サイバー攻撃の潮流および長期間運用などの社会インフラの特徴を踏まえ，社会インフラに求められる新たなセキュリティ要件として，適応性（Adaptive），即応性（Responsive），協調性（Cooperative）という3つの要件を整理してきた。

ここでは，社会インフラにおけるセキュリティの要求レベル（水準）と，その要求レベルの実現方針，実現に向けたシステムレベル・コンポーネントレベルでの取り組み，および制御システムのセキュリティ確保を目的として設立されたCSSC（Control System Security Center：技術研究組合制御システムセキュリティセンター）の活動を紹介する

とともに日立グループの取り組みについて述べる。

2. 社会インフラにおけるセキュリティの要求レベル

まず，IEC 62443で定義されている「セキュリティ強靭性」について概観するとともに，日立グループが独自に整理している「適応性」,「即応性」,「協調性」という3つの軸の要件とそれぞれの要求レベルについて説明し，その必要レベルを定義する。

(1) セキュリティ強靭性要件とその要求レベル

IEC 62443では，セキュリティ対策の強度を評価する軸であるセキュリティ保証レベル（SAL：Security Assurance Level）を定義している（**表1**参照）。

社会インフラシステムに対する昨今の攻撃の動向を考慮すると，強い悪意を持った組織的な攻撃の対象となっていることは明らかであり，レベル3ないしは4相当のセキュリティ対策が必要である。

(2) 適応性要件と要求レベル

適応性は，多種多様な脅威への対策の柔軟性を定義したものである。

従来，設計段階で想定した脅威に対応できるようにセキュリティ対策を実装することが要求されてきた。しかし，攻撃手法の進展などにより，時々刻々と新たな脅威が発生する状況が出現しており，「設計段階では想定していなかった脅威」への対応能力が求められるようになってきている。

このような適応性の要件の達成度合いをレベル化したものを**表2**に示す。

社会インフラに供される制御システムは，設計段階では予期していなかった攻撃に直面する可能性が高く，適応性要件に対する要求は情報システムなどよりも強い。そのため，レベル3の対策が求められ，さらに，レベル4に向けた組織的な対策が必要である。

(3) 即応性要件と要求レベル

即応性は，脅威が発生した場合の対処の迅速性を定義したものである。

従来，セキュリティ対策では脅威の予防が重要視されてきたが，最近の高度な脅威に対してはその発生をいち早く検知し，脅威に有効な対処を講じる能力が求められるようになってきている。

このような即応性の要件の達成度合いをレベル化したものを**表3**に示す。

社会インフラに供される制御システムは，サービスを提供し続けることが求められ，セキュリティ脅威が発生した場合においても迅速な対応が不可欠である。このため即応性要件は，サービスを提供し続けながら対処を可能とするレベル3の対策が必要であり，さらに，絶えず変化する脅威に対応するべくレベル4に向けた組織的な対策が必要である。

(4) 協調性要件と要求レベル

協調性は，相互に依存し合う他のシステムから受ける影響の程度を定義したものである。

影響については，正の影響（例：脅威情報の共有によって未知の脅威を検出できる）と負の影響（例：他システムがマルウェアに感染し，攻撃を受ける）が考えられる。

このような協調性の要件の達成度合いをレベル化している（**表4**参照）。

社会インフラシステムは，長期間継続的に運用することから多種多様なシステムが混在しており，セキュリティ対策の強度が全体としては均一にならない。このような状況において，最も弱い部分に対する攻撃を防ぐためには，レベル2相当の対策によってシステム全体のセキュリティ強度を維持することが求められる。

表1｜セキュリティ強靭性レベル

ある時間単位で見た瞬間の静的なセキュリティ対策の強靭（じん）さを評価するレベルを示す。

レベル	内容
1	不注意から発生する脅威を防御
2	汎用的なスキルと単純な手段での攻撃を防御
3	専門知識と強い悪意を持つ者による攻撃を防御
4	高度な専門知識と非常に強い悪意を持つ組織の攻撃を防御

表2｜適応性レベル

多種多様な脅威への対策の柔軟性を評価するためのレベルを示す。

レベル	内容
1	セキュリティ脅威に未対応
2	設計段階で想定した脅威に対応
3	新たな脅威が出現した場合にも対応
4	新しい脅威へのマネジメントシステムが確立

表3｜即応性レベル

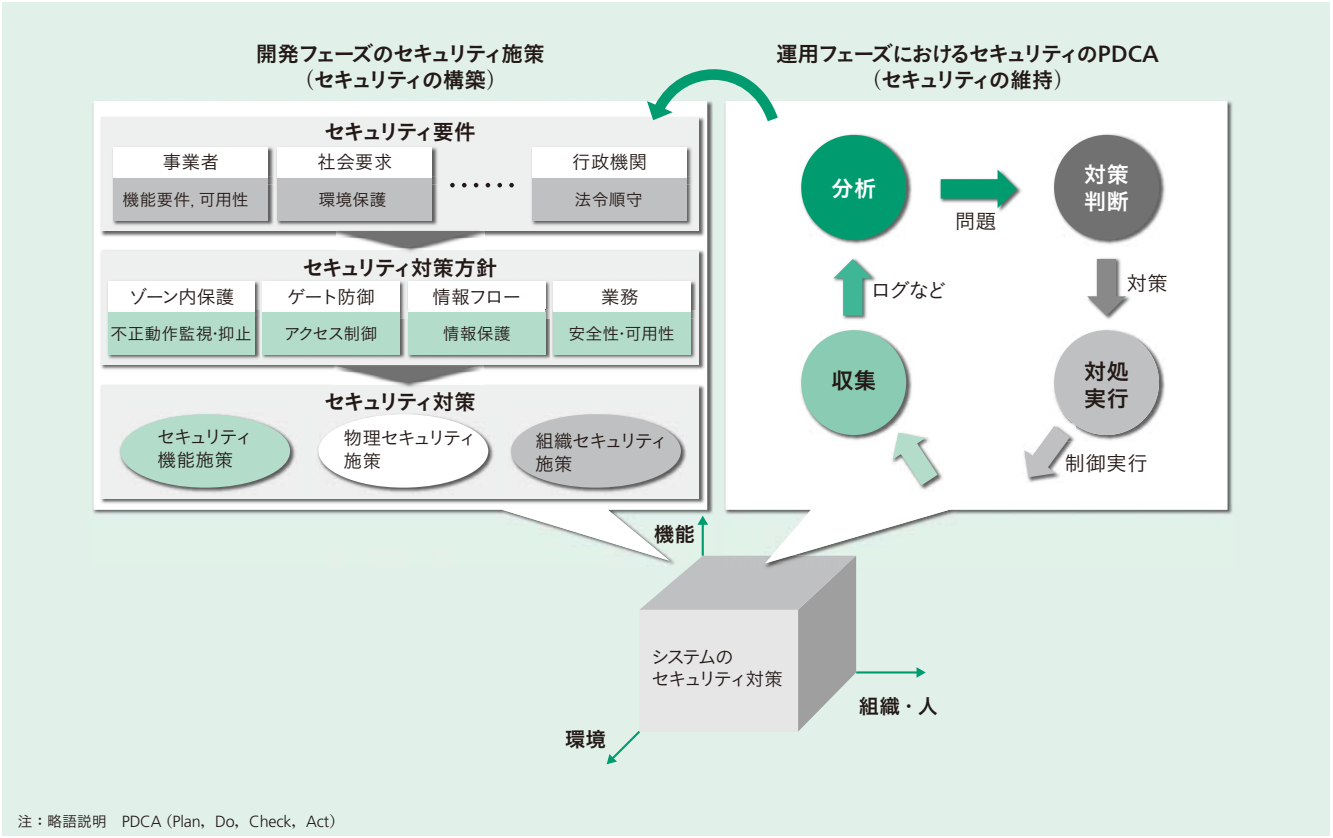
脅威が発生した場合の対処の迅速性を評価するためのレベルを示す。

レベル	内容
1	脅威発生の検知手段が未整備
2	脅威発生の検知手段を具備
3	脅威発生後の対策手段を具備
4	脅威発生から対策までのマネジメントシステムが確立

表4｜協調性レベル

相互に依存し合う他のシステムとの間の影響を評価するためのレベルを示す。

レベル	内容
1	負の影響への防御策が未整備
2	負の影響への防御策を整備
3	正の影響を与える策を具備
4	相互の影響を継続評価するマネジメントシステムが確立



注：略語説明　PDCA（Plan，Do，Check，Act）

図1｜2×3セキュリティ実現モデル

開発と運用という2つのフェーズにおいて，機能，環境，組織・人という3つの観点で脅威に対策・対処し，漏れのないセキュリティを実現する。

3.　制御システムセキュリティの実現方針

日立グループは，これまでに，社会インフラシステムのセキュリティをライフサイクル全体で確保する考え方を「2×3セキュリティ実現モデル」としてモデル化してきた[5]。このモデルは，開発フェーズと運用フェーズの2つのフェーズにわたって，機能，環境，組織・人という3つの観点で脅威に対処・対策し，漏れのないセキュリティを持続的に実現するという考え方である（**図1**参照）。

セキュリティ要件との関係は，開発フェーズにおけるセキュリティ施策によってセキュリティ強靭性要件および適応性要件を達成し，運用フェーズにおけるセキュリティのPDCA（Plan, Do, Check，Act）サイクルを確立することで即応性要件および協調性要件を達成する。特に，即応性レベル3以上や協調性レベル2以上のシステムを実現するには，システムのセキュリティ状態を常時監視してセキュリティインシデントを検出するとともに，検出された場合にサービスを維持しつつそれに対処するためのセキュリティ運用体制を整備する必要があり，運用フェーズを想定した開発が不可欠である。

4.　システムレベルでのセキュリティ実現の取り組み

ここでは，2×3セキュリティ実現モデルに基づいた，開発フェーズに対して制御システムを開発するうえでの施策と，運用フェーズに対する施策について述べる。

4.1　開発フェーズ

制御システムを開発するうえでは，セキュリティ上の脅威を洗い出して評価し，実装すべきセキュリティ対策を導出することが重要になる。日立グループは，その一連の手順をIEC 62443が提唱しているセキュリティコンセプトを活用したシステム構築ガイドとして整備している。このガイドは，システムの重要度や顧客要件に応じた適切なセキュリティ対策を実装するためのものである。

具体的には，次の手順を実施する。

(1) システムにおけるリスク分析に基づき，同一のセキュリティポリシーを適用する範囲（ゾーン）にシステムを分割する。

(2) ゾーン間の接続関係（コンジット：「導管」の意）を明確化する。

(3) セキュリティ施策を策定する。

(a) コンジットからゾーンへ不正な情報が入らない施策（コンジットゲートの設置）

(b) ゾーン内での不正な動作を防止する施策

(i) ネットワークへの対策

(ii) 装置への対策

前章で述べた要件レベルを満足するためにこのシステム

構築ガイドが示しているセキュリティ施策について，情報制御ゾーンに基づいて以下に述べる（図2参照）。

(1) コンジットゲートのセキュリティ施策（施策1）

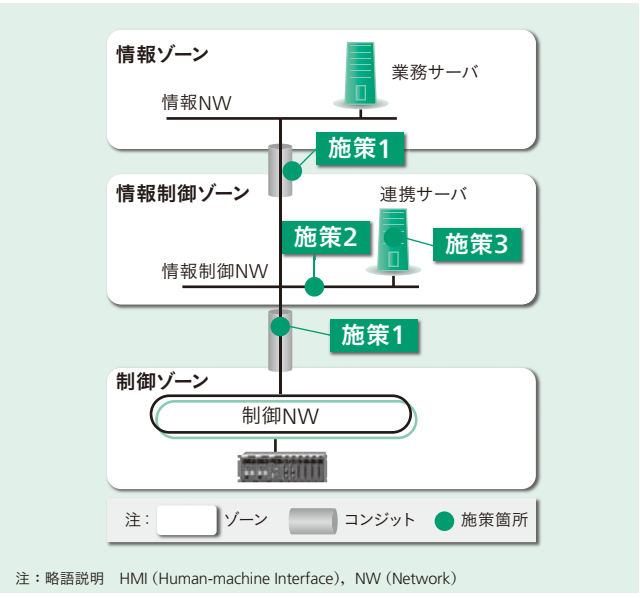
コンジットゲートのセキュリティ施策は，ゾーンへの不正侵入やゾーンからの漏えいを防止することが主な役割である。

システムがセキュリティ強靭性レベル3ないしは4を満足するためには，コンジットゲートにおいて必要な通信を識別し，不要な通信を遮断する。通信の識別にあたっては，通信相手だけではなく，通信の方向や内容にも応じて要・不要を判断する。適応性レベル3を満足するためには，通信の要・不要や不審な通信か否かを判断するロジックを提供できるようにすることが必要となる。即応性レベル3を満足するためには，通信を常時監視し，不審な通信が検出された場合には，制御システム運用者の対策判断が可能となるような施策が必要となる。この考え方に基づき，各ゾーンのセキュリティポリシーを考慮してシステムを開発する。

(2) ゾーン内での不正動作を防止する施策：ネットワーク（施策2）

ゾーン内ネットワークのセキュリティ施策は，ゾーン内に侵入した不正者やマルウェアが機能や情報にアクセスすることを防止するとともに，不正者を検知することを主な役割とする。

セキュリティ強靭性レベル3ないしは4を満足するためには，ゾーン内においてコンポーネントを識別し，不要なコンポーネントの接続を遮断する。日立グループは，このような機能を実現する製品を提供している。



注：略語説明　HMI（Human-machine Interface），NW（Network）

図2｜制御システムにおけるセキュリティ実装ポイント

制御システムをゾーン分割し，ゾーンの出入り口とゾーン内のネットワーク（情報制御ネットワーク），ゾーン内コンポーネントにセキュリティ施策を実施する。

即応性レベル4を満足するため，ゾーン内を常時監視し，不審な動作が検出された場合は，セキュリティ運用システムに警告を発するようにする。日立グループは，ゾーン内の監視を実現する新しいアプローチとして，おとりサーバを用いたソリューションを開発している。このソリューションは，意図的にセキュリティ対策を緩めたおとりサーバを設置し，マルウェアに感染させることでゾーン内へのマルウェアの侵入を早期検知するものである。

(3) ゾーン内での不正動作を防止する施策：装置（施策3）

ゾーン内にある制御コンポーネントのセキュリティ施策は，機器内に侵入したマルウェアが機能や情報にアクセスすることを防止することが主な役割である。

制御コンポーネント内で登録されたソフトウェア以外の動作を抑止する機能の提供や，セキュリティ強化した制御コンポーネントの利用が必要である。

制御コンポーネントへのセキュリティ強化については後述する。

4.2　運用フェーズ

制御システムの運用フェーズにおいて必要となるセキュリティ施策として，制御システムで発生するセキュリティインシデントの迅速な対処施策と，新たに発生するセキュリティ脅威などのリスクに対する組織的なセキュリティマネジメントについて紹介する。

(1) セキュリティインシデントの迅速な対処施策

コンジットゲートやゾーン内ネットワーク，ゾーン内にあるコンポーネントにおいてセキュリティ上の異常を検出した場合に，その異常がインシデントによるものなのか，単なる誤検知なのかを迅速に判断し，対処することが必要となる。日立グループは，情報システム向けにセキュリティ運用センター（SOC：Security Operation Center）を設置するとともに，セキュリティインシデントに対処するインシデント対策チームを組織し，インシデント対処のノウハウを蓄積している。一方，異常がインシデントによるものか否かを決定するには，業務に関する知識も必要である。

これらのインシデント対処と業務システムの構築・運用という双方のノウハウを踏まえ，セキュリティ運用システム・サービスを開発している。

(2) 組織的なセキュリティマネジメントシステム

制御システムの適応性レベル4，即応性レベル4を実現するためには，組織的なセキュリティマネジメントシステムが不可欠である。日立グループは，CSMS（Cyber Security Management System）に注目している。CSMSは，制御システム保有者が制御システムのリスク管理を実施

し，セキュリティを継続的に維持する管理システムである。システム保有者がセキュリティを維持するためには，システムインテグレータや製品提供者との連携が求められる。日立グループは，以前から高信頼かつセキュアな制御システムの提供に注力しており，CSMSへの対応についても取り組んでいる。

5. 制御コンポーネントレベルでの取り組み

セキュリティ強靭性レベル3以上のセキュアな制御システムを実現するには，システムを構成する各コンポーネントを安全かつ安定的に利用できることが重要である。日立グループは，制御コンポーネントの要塞化（ハードニング）やセキュリティ機能の強化を進めるとともに，セキュリティ対策を実施できない制御コンポーネントに対してセキュリティを強化するための製品を開発している。

現在，制御コンポーネントのセキュリティを評価する手段として，EDSA（Embedded Device Security Assurance）認証[6]に注力している。EDSA認証は，国際認証推進組織ISCI［ISA（International Society of Automation）Security Compliance Institute］が運営する制御機器のセキュリティ保証に関する認証制度であり，以下の3つの評価項目が存在する。

（1）セキュリティ機能の実装評価（FSA：Functional Security Assessment）

（2）ソフトウェア開発の各フェーズにおけるセキュリティ評価（SDSA：Software Development Security Assessment）

（3）通信の堅牢（ろう）性テスト（CRT：Communication Robustness Testing）

6. CSSCと日立グループの取り組み

CSSCは，制御システムのセキュリティ強化を目的に，産官学の連携により2012年3月に設立された。具体的には，「制御システムセキュリティ技術の研究開発」，「制御機器のセキュリティ検証」，「模擬プラントによる普及啓発・人材育成」を主な目的としている。制御機器のセキュリティ検証については，EDSA認証に着目し，ISCIのアソシエートメンバーとして加入するとともに，CSSCにおいて評価認証の準備を進めている。

日立グループは，設立当初より組合員として参画し，制御システムにおけるセキュリティ強化策の共同研究，模擬プラントを活用した制御システムにおけるセキュリティ演習，制御機器のセキュリティ検証を，それぞれCSSCと連携して実施している。今後も，CSSCの組合員として，制御システムにおけるセキュリティ強化技術の研究開発や施策へ積極的に貢献していく。

7. おわりに

ここでは，社会インフラシステムを支える制御システムの実現のために必要となる新たなセキュリティ要件，および要件を実現するためのセキュリティ技術について述べた。

制御システムにおけるセキュリティ施策は，社会インフラシステムを守るために重要な要件の1つである。今後も日立グループは，進化を続ける脅威に対抗すべく，CSSCをはじめとする国内外の組織との連携を進め，必要となる技術の研究開発と，開発した技術を活用した製品の提供に取り組む。また，制御システムにおけるセキュリティリスク分析からシステム構築，さらに運用支援までのトータルなサービスを提供していく。それにより，誰もが安心して利用できる安全な社会インフラの実現に貢献できるものと考える。

参考文献など

1） IEC: Industrial Network and System Security, IEC 62443（2013）
2） ITU-T: A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies, Recommendation ITU-T X.1208, 1204
3） ITU-D: Global Cybersecurity Index, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
4） ETSI: Information Security Indicators, http://www.etsi.org/images/files/ETSITechnologyLeaflets/InformationSecurityIndicators.pdf
5） 鍛，外：社会インフラの安全・安心を確保するサイバーセキュリティ技術，日立評論，95，4，318～321（2013.4）
6） ISCI: Embedded Device Security Assurance（EDSA），http://isasecure.org/ISASecure-Program.aspx

執筆者紹介

中野 利彦
日立製作所 インフラシステム社 情報制御プラットフォーム開発本部 制御プラットフォーム設計部 制御セキュリティセンタ 所属
現在，社会インフラシステムのセキュリティ開発に従事
博士（工学）
電気学会会員

清水 勝人
日立製作所 インフラシステム社 情報制御プラットフォーム開発本部 制御プラットフォーム設計部 所属
現在，情報制御システム向けのサーバとコントローラの開発・設計に従事

山田 勉
日立製作所 日立研究所 エネルギー・環境研究センタ エネルギーマネジメント研究部 所属
現在，組込み計算機・ネットワークアーキテクチャ，制御系セキュリティの研究開発に従事
技術士（情報工学部門）
IEEE会員，ISA会員，電子情報通信学会会員，計測自動制御学会会員

鍛 忠司
日立製作所 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，情報セキュリティ技術の研究開発に従事
博士（情報科学）
IEEE Computer Society会員