制御セキュリティ
制御システムのライフサイクル保護を実現するセキュリティソリューション

大久保 訓 Okubo Satoshi
山口 耕平 Yamaguchi Kohei
中三川 哲明 Nakamikawa Tetsuaki
内山 宏樹 Uchiyama Hiroki

社会インフラシステムで利用される制御システムの汎用化やネットワーク接続範囲の拡大に伴い，制御システムにおけるセキュリティ上の問題が次々と発見されている状況となっている。しかし，制御システムは長期間にわたる安定稼働を優先させるため，容易にはセキュリティパッチ適用などの対応ができない。このため，脆弱性の有無の把握や脆弱性を突く攻撃の早期検知・対処といったセキュリティ運用管理が求められてきている。
このような背景の下，日立は，社会インフラシステムの安全・安心を実現するため，制御システムにおけるセキュリティ運用管理の負荷低減につながるセキュリティソリューションを整備しており，ライフサイクル全般にわたるセキュリティ確保をめざしている。

1. はじめに

電力，鉄道，ガス，水道といった社会インフラシステムや自動車で利用される制御システムは，これまで専用OS（Operating System）や専用プロトコルを利用しており，インターネットなどの外部ネットワークからアクセスできない環境に設置されているため，サイバー攻撃の影響は受けないと考えられてきた。しかし，近年，コスト削減のために，Windows※1）やLinux※2）といった汎用OSやTCP（Transmission Control Protocol）/IP（Internet Protocol）などの汎用プロトコルの利用が進んでいる。また，効率性向上のために生産管理システムなどの情報システムとの接続が進んでおり，従来，セキュリティを考慮する必要がなかった制御システムにおいても情報システムと同様にセキュリティ対策が求められている。

一方，制御システムは可用性や長期保守性といった，一般の情報システムとは異なる要件があり，情報システム向けのセキュリティ技術・製品をそのまま制御システムに適用することは困難であるという課題がある。例えば，制御システムでは，脆（ぜい）弱性などのセキュリティ上の問題が発生しても，制御システムの稼働への影響が不明なパッチなどの対策は，容易には実施できない。また，仮にセキュリティ対策製品を導入したとしても，システム稼働後のシステム構成の変更による既知の脆弱性の顕在化，新しい脆弱性の発見などにより完全には対処できないという課題もある。

情報システムにおいてはセキュリティ運用管理に関して，ISO/IEC 27001で規定される情報セキュリティマネジメントシステム（ISMS：Information Security Management System）があり，認証制度が整備されている[1)]。ISMSでは顧客情報や機密情報といった情報資産の保護を目的とし，セキュリティリスク分析，リスクへの対処（予防策），運用組織体制の構築，インシデント発生時の対応手順の策定（検知策，対処策）などの実施を要求しており，組織において，セキュリティライフサイクル（現状把握→予防→検知→対策）のループを構築することを求めている。このようなセキュリティ運用管理は，今後，情報システムだけではなく，制御システムにおいても同様に必要になってくると考えられる。

ここでは，社会インフラシステムの安全・安心を実現するため，制御システムに対して求められるセキュリティ運用管理の必要性とそのコンセプトおよびセキュリティ運用管理を支えるソリューションについて述べる。

※1）Windowsは，米国Microsoft Corporationの米国およびその他の国における登録商標である。
※2）Linuxは，Linus Torvaldsの米国およびその他の国における登録商標または商標である。

2. 制御システムのセキュリティ運用管理の必要性

制御システムのセキュリティ運用管理の重要性が高まる中，その要件を規定した制御システム向けのセキュリティ標準規格や政府のガイドライン策定が進められている。本章では，これらの動向について示す。

2.1 セキュリティ標準規格の動向

汎用的な制御システム向けセキュリティ標準規格として，IEC 62443[2]の策定が進められている。IEC 62443は13の規格群から構成されており，事業者向け要件，システムインテグレータ向け要件，コンポーネントベンダ向け要件がそれぞれ規定されている。これらの規格群の中でIEC 62443-2-1[3]では，サイバーセキュリティマネジメントシステム（CSMS：Cyber Security Management System）が規定されている。ISMSとCSMSの相違点を**表1**に示す。ISMSと同様にCSMSにおいても，2014年に世界に先駆けて認証制度が整備されており[4]，今後社会インフラ事業者において認証取得が拡大していく可能性がある。

2.2 政府ガイドラインの動向

経済産業省は，独立行政法人情報処理推進機構とともにIT（Information Technology）に関するシステムやサービスを提供する企業や経営戦略上ITの利用が必須である企業の経営層向けのサイバーセキュリティガイドラインを策定している[5]。本ガイドラインには，以下の4項目が経営上重要な実施項目として記載されている。

(1) リーダーシップの表明と体制の構築
(2) サイバーセキュリティリスク管理の枠組み決定
(3) リスクを踏まえた攻撃を防ぐための事前対策
(4) サイバー攻撃を受けた場合に備えた準備

国内外の制御システムの標準動向，ガイドライン動向により，ITの利用が必須となっている社会インフラ事業者は，長期間にわたってセキュリティ運用管理を実施することが求められている状況である。

表1｜ISMSとCSMSの違い
ISMSとCSMSで求められる要件の違いを示す。

相違点	ISMS	CSMS
保護対象	情報資産	IACS（情報資産，人的・物理的資産，運用）
想定脅威	保護対象の機密性，完全性，可用性（CIA）が損なわれること	保護対象のCIAが損なわれることに加えて，HSEが損なわれること
対象ライフサイクル	運用面主体	システムライフサイクル全般

注：略語説明　IACS (Industrial Automation and Control System)，CIA (Confidentiality, Integrity, Availability)，HSE (Health, Safety, Environment)，ISMS (Information Security Management System)，CSMS (Cyber Security Management System)

3. 制御システムのセキュリティ運用管理のコンセプト

3.1 社会インフラセキュリティコンセプト：H-ARC

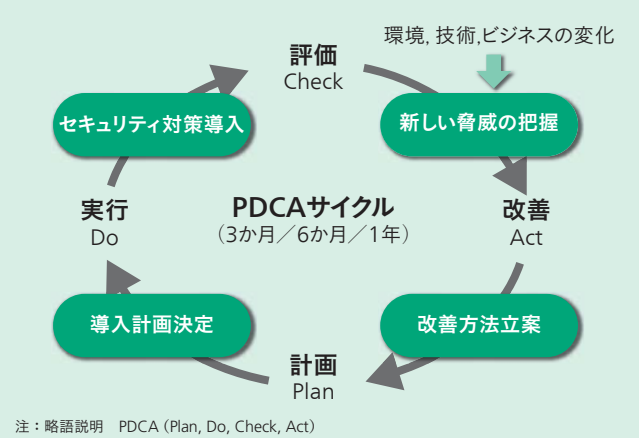
日立は，社会インフラを自然災害やサイバー攻撃，テロなどの脅威から守るために必要なセキュリティ要件を，H：Hardening（強じん性），A：Adaptive（適応性），R：Responsive（即応性），C：Cooperative（協調性）の観点で，「H-ARCコンセプト」[6]として整理している。

(1) H（強じん性）：攻撃者が持つ攻撃スキルに対抗できる防御力の準備
(2) A（適応性）：新たな脅威に対する事前対策・防御の継続的な強化
(3) R（即応性）：攻撃発生後に被害最小化・復旧短時間化する事後対処力の強化
(4) C（協調性）：異なる組織・事業者間の共通状況認識による協調

3.2 制御システムのセキュリティ運用管理の考え方

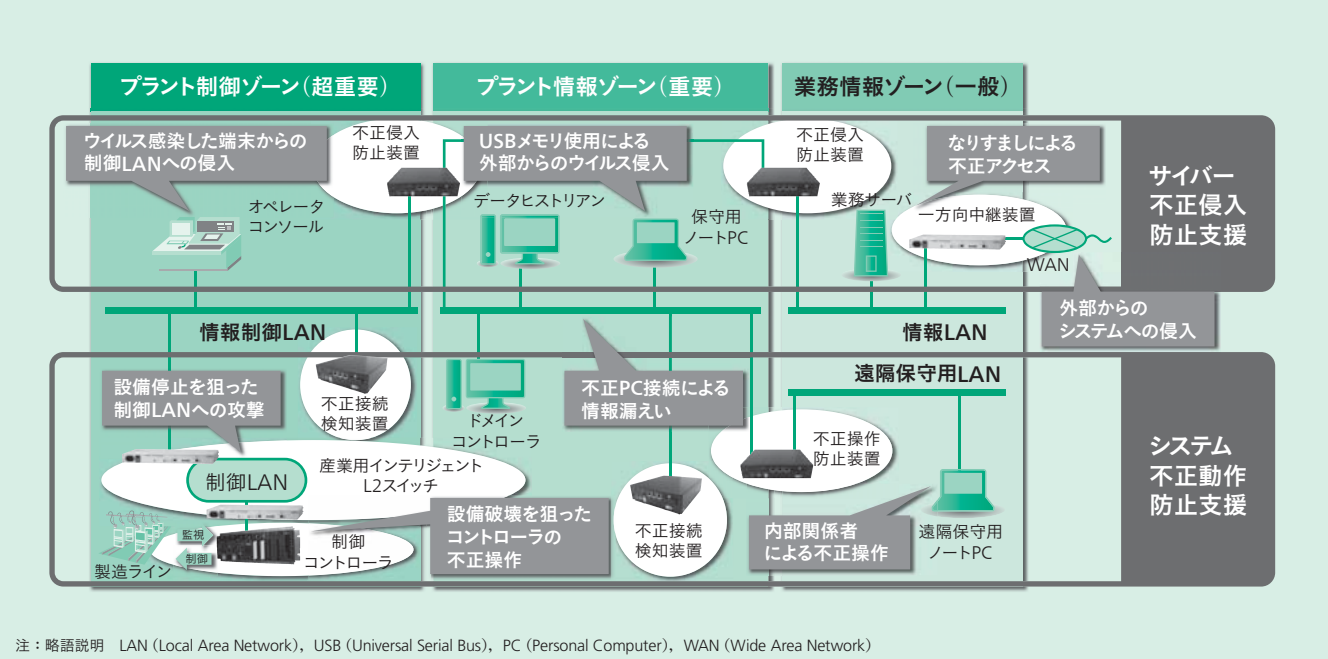
日立は，「H-ARCコンセプト」により，新しい脅威の対応をPDCA（Plan, Do, Check, Act）で継続的に強化することで，制御システムのセキュリティ運用管理を実施する（**図1**参照）。

(1) 新しい脅威の把握
システム構成の変更などに伴い検討すべき新しい脅威を抽出し，対象システムへの影響をリスク分析などにより，把握する。
(2) 改善方法立案
(1) で抽出したリスク分析結果により，想定脅威に対する改善方法を検討する。
(3) 導入計画決定
(2) で検討した改善方法に対する導入計画を決定する。
(4) セキュリティ対策導入
(3) で決定したセキュリティ対策を実施する。



注：略語説明　PDCA (Plan, Do, Check, Act)

図1｜セキュリティ運用管理のPDCAによる対策
新しい脅威への対応をPDCAで継続的に強化する。



注：略語説明　LAN（Local Area Network），USB（Universal Serial Bus），PC（Personal Computer），WAN（Wide Area Network）

図2｜制御システムセキュリティソリューション
幅広い制御システム向けのセキュリティ製品を組み合わせることで，2つの制御システムセキュリティソリューションを提供している。

4.　セキュリティ運用管理を支える制御セキュリティソリューション

制御システム向けのセキュリティ対策では，システムを守るべきセキュリティレベルごとに領域（ゾーン）に分割したうえで，各ゾーンの出入口と各ゾーンをつなぐ通信路に対して，セキュリティ施策を実施することが必要である。

日立の制御システムセキュリティ対策は，H-ARCコンセプトに基づき，「サイバー不正侵入防止支援」，「システム不正動作防止支援」の2つのソリューションを提案している（**図2**参照）。

4.1　サイバー不正侵入防止支援

サイバー不正侵入防止支援は，各ゾーンの出入口において，サイバー空間経由での不正侵入防止（H：強じん性），および不正侵入検知後のセキュリティ問題の拡散防止（R：即応性）を実現するソリューションである。

不正侵入防止装置は，あらかじめ定義したホワイトリストに合致しない不正パケットを遮断する。この装置を保護したい制御システムの出入口に設置することで，制御システムへの不正侵入を防止できる。また，試運転時のアクセスログを活用することで，前述のホワイトリストを生成するツールを準備しており，これらの特長から，制御システムへの導入が容易になっている。さらに，不正侵入防止装置は，制御システムと連携している他システムでセキュリティ問題（例えば，マルウェア感染など）が発生した場合，他システムからの通信パケットを遮断することで，制御システムへの問題の拡散を未然に防止できる。

また，一方向中継装置NX Oneway-Bridgeは，ソフトウェアレスでデータダイオード（ダイオードのように片方向のみ通信を許可する）機能を実現し，基幹システムの情報を外界へ伝達する際に，外界からの不正アクセスを物理的に遮断し，基幹システムを守ることができる。また，ソフトウェア更新不要，長寿命化などの特長によって運用時の負担を軽減した（**図3**参照）。

4.2　システム不正動作防止支援

今後，制御システムには，さまざまなIoT（Internet of Things）機器がネットワークを介して接続されることが予想される。特に，製造現場に無線ネットワークが導入されると，管理者が把握していないIoT機器や従業員の個人端末など，無許可の機器が制御システムに接続される可能性が高まり，マルウェア感染や情報漏えいといった新たなリスク発生源となる。システム不正動作防止支援は，このようなシステム内部での不正機器接続による脅威からの制御システムの防御（H：強じん性），および許可された機器のマルウェア感染などによる不正な動作の検知・排除（R：即応性）を実現するソリューションである。

図3｜一方向中継装置NX Oneway-Bridge
ソフトウェアレス化することで，設定誤りのリスク，運用時の負担を軽減した。

図4｜不正接続検知装置NX NetMonitor
未登録の機器がネットワークに接続しようとするのを検知し，自動的に排除することで，サイバー攻撃の脅威を防ぐ。

不正接続検知装置NX NetMonitorは，あらかじめ登録された機器以外がネットワークに接続したことを検知し，ネットワークから排除する機能を持つ。無線ネットワーク経由での接続にも対応しており，無許可の機器が制御システムに接続されることを防止する（図4参照）。

また，近年増加している標的型攻撃に対しては，サイバー攻撃に気付かない，ウィルス対策ソフトで未対応のマルウェアの感染など，システムへの不正侵入を完全に防止するのは困難，という前提での対応が必要である。サイバー攻撃を検知するため，情報システムで実績のある振る舞い検知製品と前述の不正接続検知装置NX NetMonitorを連携することで，不正な動作をしている機器を検知し，ネットワークから排除する。

さらに，サイバー攻撃を受けた際の影響を最小化するため，サイバー攻撃に対するロバスト性を高める対策を採用している。

制御コントローラHISEC 04/R900Eは，ISA（International Society of Automation）セキュリティ適合性協会（ISCI：ISA Security Compliance Institute）が運営する制御コンポーネントのセキュリティ保証に関する認証制度であるEDSA（Embedded Device Security Assurance）認証を取得し，サイバー攻撃への耐性を高めた（図5参照）。

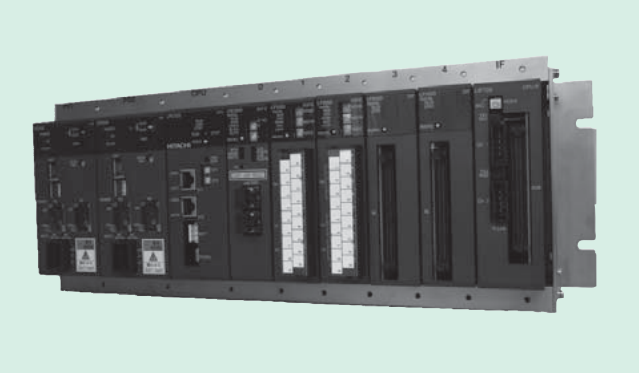


図5｜EDSA認証取得コントローラHISEC 04/R900E
あらかじめ決められたセキュリティ要件を満たすことで，サイバー攻撃への耐性を保有していることを示している。

5. おわりに

本稿では，国内外の動向を踏まえた制御システムのセキュリティの運用管理の必要性およびそのコンセプトとコンセプトを支えるソリューションについて紹介した。

今後も制御システムは，社会インフラを支える基盤として最新のITの導入，情報システムやIoT機器との連携により，発展していくとともに，サイバー攻撃のリスクも増大すると予測される。日立は，引き続き安全・安心な社会インフラシステムの実現に向け，制御セキュリティの技術開発を進め，付加価値の高いソリューションを提供していく。

参考文献など

1） 一般財団法人日本情報経済社会推進協会：ISMS適合性評価制度，http://www.isms.jipdec.or.jp/isms.html
2） IEC（International Electrotechnical Commission）:IEC TS 62443-1-1, Terminology, concepts and models（2009.7）
3） IEC（International Electrotechnical Commission）:IEC 62443-2-1, Establishing an industrial automation and control system security program（2010.11）
4） 一般財団法人日本情報経済社会推進協会：CSMS適合性評価制度，http://www.isms.jipdec.or.jp/csms.html
5） 経済産業省：サイバーセキュリティ経営ガイドラインVer 1.0（2015.12）
6） 三村，外：H-ARCコンセプトに基づく日立グループの社会インフラセキュリティ，日立評論，96，3，160～167（2014.3）

執筆者紹介

大久保 訓
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 セキュリティセンタ 所属
現在，制御セキュリティ技術の研究開発に従事

山口 耕平
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 セキュリティセンタ 所属
現在，制御セキュリティ技術の研究開発に従事

中三川 哲明
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 制御プラットフォーム開発部 所属
現在，制御システムのコンポーネント開発に従事
技術士（情報工学部門）
情報処理学会会員

内山 宏樹
日立製作所 研究開発グループ システムイノベーションセンタ
セキュリティ研究部 所属
現在，制御セキュリティ技術の研究開発に従事
博士（情報学）
電気学会会員，情報処理学会会員