「H-ARCコンセプト」の国際標準化活動とそれに基づく社会インフラセキュリティ

中野 利彦 Nakano Toshihiko
外岡 秀樹 Tonooka Hideki
佐藤 雅史 Sato Masashi
鍛 忠司 Kaji Tadashi
野中 洋一 Nonaka Yoichi

近年の社会インフラのネットワーク化により，社会インフラに供されるシステムにおいてもセキュリティリスクが高まっている。これらのリスクの高まりに対応し，国際標準化団体や業界団体において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。
日立は，サイバー攻撃の潮流への対応および長期間の運用など，社会インフラとして求められる要件を「H-ARCコンセプト」として整理し，IECで検討を進めてきた。その要件は将来のファクトリー像および必要な技術を示すホワイトペーパー「Factory of the future」に提案し，現在採択されている。
今後のIoTの進展などにより，セキュリティは一層重要となる。日立は，誰もが安心して利用できる安全な社会インフラ実現のため，セキュリティソリューションを提供していく。

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大規模かつ深刻な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への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。

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，脅威の進化やIoT（Internet of Things）などの進展による多様なシステム連携に対応し，発生した攻撃に迅速に対処できる必要がある。

日立は，サイバー攻撃への対応の潮流および長期間運用などの社会インフラの特徴や，オープンイノベーションの動向を踏まえ，社会インフラに求められる適応性（Adaptivity）・即応性（Responsivity）・協調性（Cooperativity）という3つの新たなセキュリティ要件を「H-ARCコンセプト」として整理した。国際標準化団体であるIEC（International Electrotechnical Commission）[1]で検討を進めた将来のファクトリー像および必要な技術を示すホワイトペーパー「Factory of the future」[2]にこれらの要件を提案し，採択された。

本稿では，第2章で社会インフラシステムにおけるセキュリティ動向を鳥観したうえで，第3章で日立が社会インフラシステムにおけるセキュリティ要件として提唱する「H-ARCコンセプト」[3]を示し，第4章でその実現に向けたソリューションを紹介する。

2. 社会インフラシステムにおけるセキュリティ動向

本章では，社会インフラシステムにおけるセキュリティを実現するうえで必要となる，脅威，システム構成，対策の動向について鳥観する（図1参照）。

セキュリティ脅威は絶えず変化しているが，近年はゼロデイ攻撃や複合攻撃など攻撃が多様化するとともに，内部

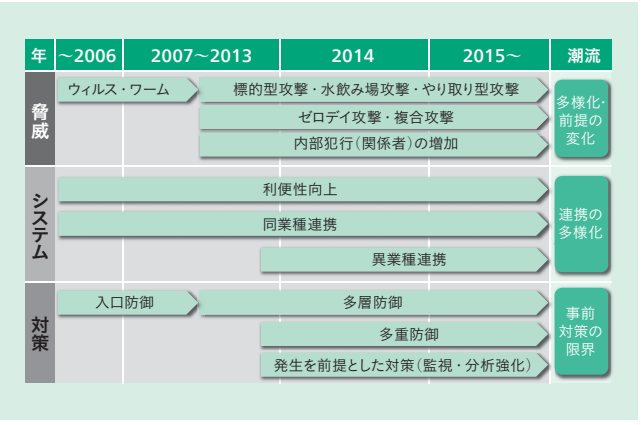


図1 | セキュリティ動向
近年，セキュリティ脅威の多様化が進むとともに，社会インフラシステム自体も種々の連携が進んでいる。このため対策技術も新たな考え方が必要である。

犯行など従来前提としていた条件から変化した攻撃がみられる。また，前提となるシステム構成においても，IoTやサプライチェーンの進展，さらに現場データの解析など業種や業務の垣根を越えて相互にシステムが接続する，日立が提唱する共生自律分散システムが進むと考えられる。これらのことからセキュリティ脅威を的確に予測することが難しく，事前の対策が困難になりつつある。

このように脅威やシステムが絶えず変化することを前提としたセキュリティ対策が不可欠である。

3. H-ARCコンセプト

本章では，日立が提唱する「H-ARCコンセプト」について説明する（図2参照）。

社会インフラシステムのセキュリティを確保するためには，対象システムの構成をベースにした，想定する脅威に対する強じん性（Hardening）の確保が前提となる。そのうえで，絶えず変化する脅威やシステム構成に対して，セキュリティ対策についても的確に適応していく適応性（Adaptivity），セキュリティ脅威が発生した場合に社会インフラシステムへの影響を最小限とする対応を実現する即応性（Responsivity），さらに，セキュリティ脅威の早期把握を実現するために複数の組織で相互に連携する協調性（Cooperativity）をセキュリティの新たな要件として提唱している。

これら3つの要件は，社会インフラシステムや産業システムを実現するうえで重要であり，国際的に共有する必要があると判断し，国際標準化団体であるIECで検討を進め，将来のファクトリー像および必要な技術を示すホワイトペーパー「Factory of the future」に提案して採択された。

以下に詳細を説明する。

(1) 強じん性（図3参照）

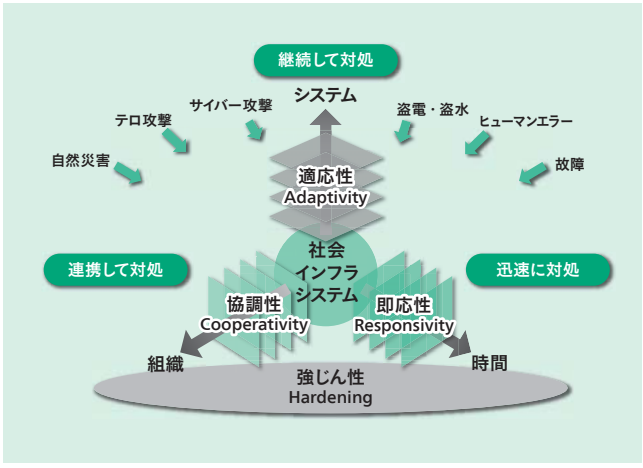


図2｜H-ARCコンセプト
日立は社会インフラシステムにおけるセキュリティ確保をするうえで必要となる要件を「H-ARCコンセプト」として提唱している。

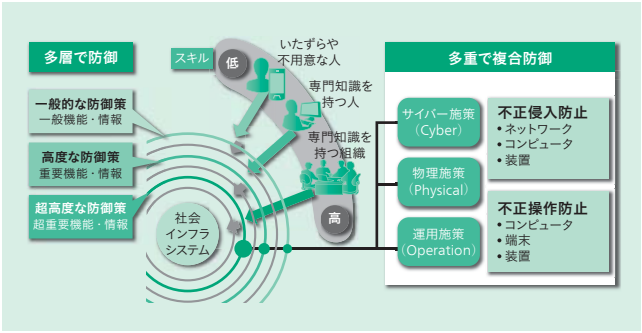


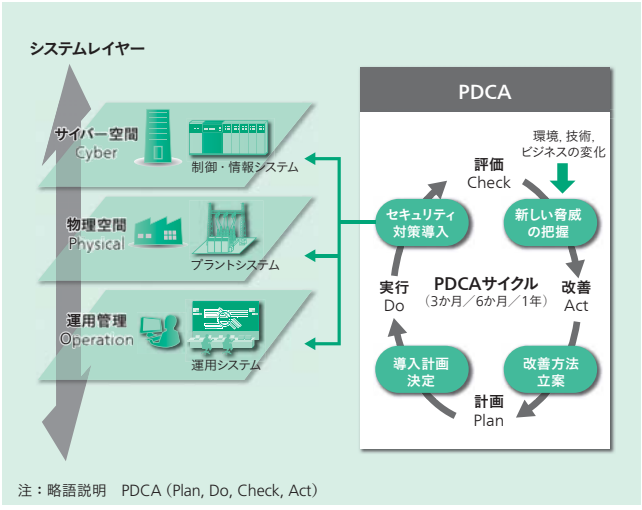
図3｜強じん性の確保
多様な脅威に対する強じん性を確保するためには，多重・多層での防御策が重要である。

社会インフラシステムのサービスや機能を守るための基本的な施策である。絶えず変化するセキュリティ脅威に対して，完全なサイバーセキュリティ施策を実現することは困難である。このため，物理施策や運用施策を組み合わせたバランスのよい多重防御を実現することが必要である。また，多重防御を実装することにより，重要な機能を司るシステムへの攻撃リスクを低減することが求められる。

日立は，制御システムを中心に長期間の安定した運用を実現するための制御システム向けのセキュリティ製品を提供するとともに，国際規格や業界基準などに準拠し，業務知識を活用したシステムを実現する。

(2) 適応性（図4参照）

セキュリティ脅威はより巧妙に変化している。システムアーキテクチャの構成も，オープンイノベーションによる公開提供技術の活用や，新たなビジネスを実現するためのシステム相互連携など常に変化している。このため社会インフラシステムは，絶えず新たな脅威にさらされていると考えられる。強じん性においても示したが，制御システムを中心に安定した長期間の運用を実現することが不可欠で



注：略語説明　PDCA（Plan, Do, Check, Act）

図4｜適応性の確保
脅威や技術などの変化に対して迅速に適応していくためのPDCAプロセスが重要である。

あるため，実際に脅威が発生する以前に脅威の取り扱いを評価することが望ましい。すなわち，システムを取り巻く変化に対応するためのセキュリティマネジメントを実現することが重要となる。

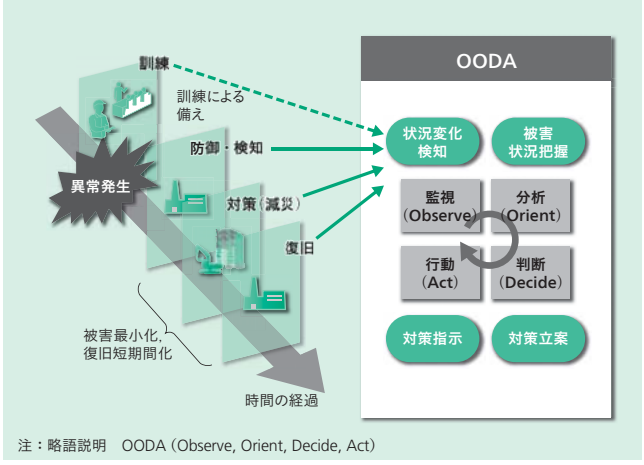
そのためには，経営層，エンジニアリング部門，運用部門，スタッフ部門が一体となり，PDCA（Plan, Do, Check, Act）サイクルを継続的に実施することが必要である。具体的には，新たな脅威などシステムを取り巻く変化を組織的に把握し，把握した脅威に対するリスク評価を実施することで改善項目を選択するとともに，「サイバー空間」，「物理空間」，「運用管理」の3つの軸で改善方法を立案し，改善方法に基づいて導入計画を策定することが求められる。このときのポイントは，客観的なリスク評価を実施することである。

日立は，この適応性を実現するため，制御システムのセキュリティマネジメントシステムであるCSMS（Cyber Security Management System）をベースに今までの制御システム構築ノウハウを生かしたエンジニアリングを提供している。

(3) 即応性（図5参照）

セキュリティ脅威から完全に防御することは困難であるため，社会インフラシステムを守って被害を最小限にするためには，発生時の対応が重要である。そのため，システムの状況変化を絶えず把握し，さらに状況変化がセキュリティ脅威によるものかを判断するとともに，セキュリティ脅威の影響範囲把握と対応策の策定に基づいた迅速な対策が必要である。これには，システムの状況変化を把握するための仕組みをシステムに具備するとともに，対応策などを策定する専門家組織が不可欠となる。

日立は，これらに対してシステムの状況変化をITレベルおよび業務レベルで早期に検知する技術を提供するとともに，専門家組織を支援するために最新のセキュリティ情報の提供やセキュリティ脅威の種別解析を行う専門家サービスを提供している。



注：略語説明　OODA（Observe, Orient, Decide, Act）

図5｜即応性の実現

セキュリティ脅威によるシステムへの影響を最小限にするためには，脅威の兆候を迅速に把握し対処することが重要である。

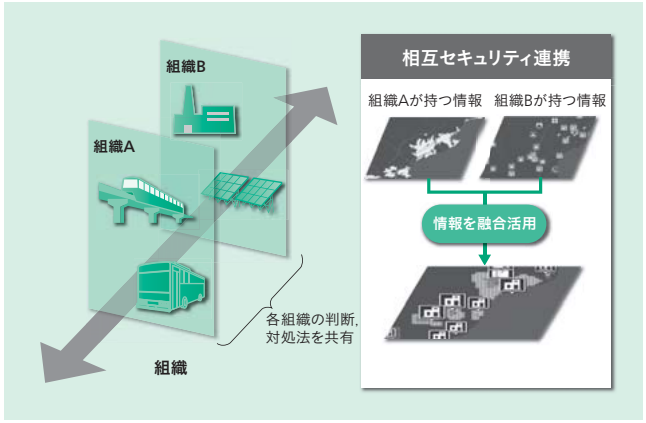


図6｜協調性の実現

社会インフラシステムを守るためには，自システムの周りに発生しているセキュリティ脅威の状況を迅速に把握する仕組みが重要である。

(4) 協調性（図6参照）

社会インフラシステムを脅威から守るためには，セキュリティ脅威の状況を事前に把握することが重要である。さらに，複数のシステムが連携している場合は，1か所のシステムのセキュリティ脅威が他のシステムに伝播（ぱ）していく可能性がある。

このため社会インフラシステムにおいては，システム間でのセキュリティポリシーや施策の協調が必要であるとともに，セキュリティ脅威情報の共有が重要である。

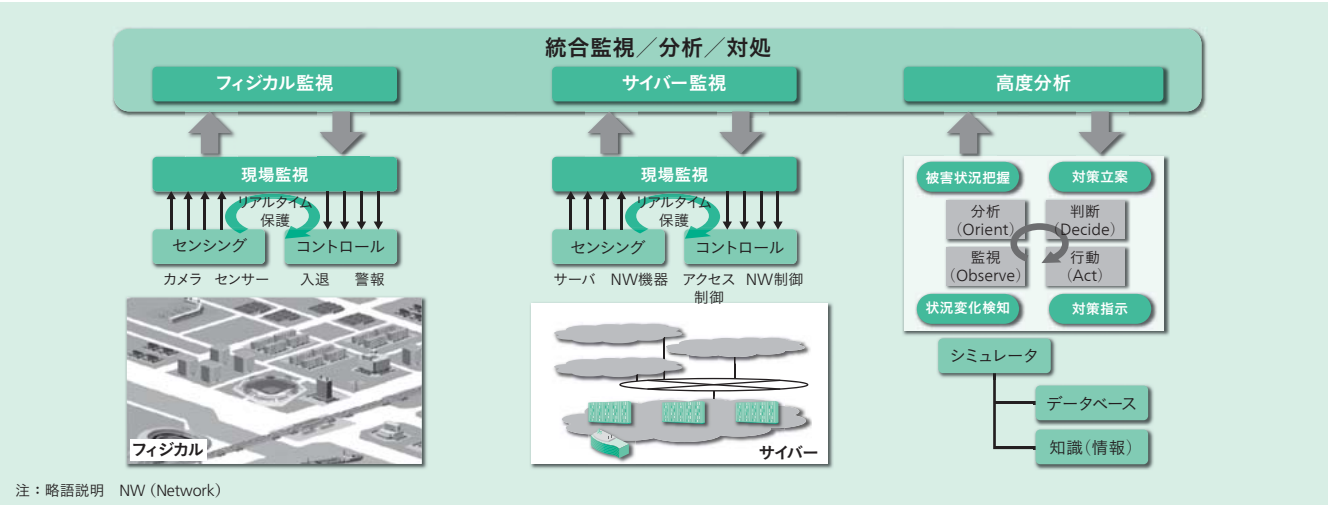
日立は，この協調性を実現するため，各種のゲートウェイ装置を用意するとともに，組織間での情報連携を可能にするためのソリューションを提供している。

4. セキュリティソリューション

前章では「H-ARCコンセプト」の概要を示した。本章では，このコンセプトを活用したセキュリティソリューション例について述べる（図7参照）。

適応性の観点からセキュリティを実現するために，保護する対象物を中心にしてリスク評価を行い，リアルタイムで保護に必要となるサイバーセキュリティ対策およびフィジカルセキュリティ対策を策定することで，最適なセキュリティ防護策を提供する。また，即応性の視点では，侵入した脅威や新たな脅威へ迅速に対応するための体制へのエンジニアリング支援，およびセキュリティ脅威の分析環境を提供する。

さらに，セキュリティ施策の実施は，今まで以上の精度や粒度で情報を取得することであり，また，取得した情報が正しいか正しくないかの判断知識を明確化することでもある。これらの情報を活用することは，企業価値の向上に



注：略語説明　NW（Network）

図7｜「H-ARCコンセプト」を活用したセキュリティソリューションの例

サイバーセキュリティ，フィジカルセキュリティとしてリアルタイムに保護し，さらにこれらを統合監視／分析／対処することで社会インフラシステムのセキュリティを確保する。

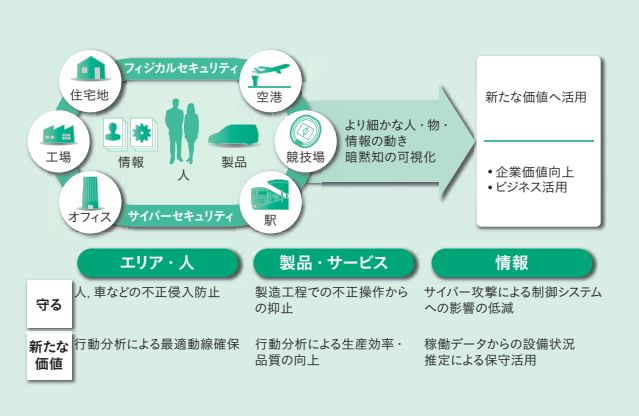


図8｜セキュリティによる価値向上

セキュリティシステムから得られる情報を有効活用することで，守るだけでなく新たな価値を創生することが可能となる。

つながり，新たなサービスとしての可能性が広がる。このため，セキュリティ対策によって得られる情報を有効活用することも併せて提案を進めている（図8参照）。

5.　おわりに

本稿では，社会インフラシステムを支える制御システム実現のために必要となる新たなセキュリティ要件について述べた。

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一つである。日立は，誰もが安心して利用できる安全な社会インフラの実現のために，今後も巧妙化を続ける脅威に対抗すべく，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を行っていくとともに，開発した技術を活用した製品を提供していく。また，社会インフラ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，さらには運用支援までトータルなサービスを提供していく。

参考文献など

1）　IEC, http://www.iec.ch/
2）　IEC：Factory of the future, http://www.iec.ch/whitepaper/futurefactory/
3）　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

中野 利彦
日立製作所 インフラシステム社 大みか事業所 セキュリティ推進室 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

外岡 秀樹
日立製作所 インフラシステム社 大みか事業所
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製品のマーケティング・商品開発に従事

佐藤 雅史
日立製作所 インフラシステム社 産業ソリューション事業部
産業ユーティリティソリューション本部
セキュリティエンジニアリング部 所属
現在，統合セキュリティのソリューションビジネスに従事

鍛 忠司
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，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 CS会員

野中 洋一
日立製作所 研究開発グループ 生産イノベーションセンタ 所属
現在，SCM，生産制御，デジタルエンジニアリングの研究に従事
博士（工学）
精密工学会会員，計測自動制御学会会員，日本機械学会会員，国際生産工学アカデミー（CIRP）会員