セキュリティ基盤
社会インフラを支える日立のセキュリティソリューション基盤

中野 利彦 Nakano Toshihiko　小野寺 剛 Onodera Takeshi　上脇 正 Kamiwaki Tadashi　宮尾 健 Miyao Takeshi

近年，社会システムに対するセキュリティ脅威では，より目的を持った攻撃を仕掛けてくる標的型攻撃や社会生活へ影響を与える攻撃などが増加してきている。さらにIoT技術の進展により，広範囲からのサイバー攻撃の可能性が高まっている。また内部犯行の増加や，テロに近い事象も増加してきている。
日立は，これらの脅威から社会システムを守るためのセキュリティ要件を「H-ARCコンセプト」として整理し，マネジメント，運用，現場システムにおいて必要となる種々の施策をセキュリティソリューション基盤として整備を進めている。誰もが安心して利用できる安全な社会システムを実現するため，セキュリティ脅威やオープンアーキテクチャの伸展など種々の変化に的確に対応できるソリューションを提供していく。

1. はじめに

近年，社会システムに対するセキュリティ脅威はサイバー空間・フィジカル空間ともに増大し続けている。具体的にはサイバー空間では，より目的を持った攻撃を仕掛けてくる標的型攻撃や社会インフラシステムを制御する装置への攻撃などが増加してきている。さらにIoT（Internet of Things）技術の進展によってシステムの相互連携が加速し，より広範囲からのサイバー攻撃が業務と密接に関連する機能に影響する可能性がより高まっている。一方，フィジカル空間では，内部犯行の増加や，テロに近い事象も増加してきている。

日立は，これら脅威の潮流および守るべき社会システムの特徴や，IoTをはじめとするオープンイノベーション技術の動向を踏まえ，社会システムに求められるセキュリティ要件を，適応性（Adaptive）・即応性（Responsive）・協調性（Cooperative）という3つの要件に整理し「H-ARCコンセプト」として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]に提案し採択された。日立は，このコンセプトに基づいた各種のセキュリティソリューション基盤の整備を進めている。

本稿では，社会システムにおけるセキュリティ動向を，想定する社会システムの例を含め鳥瞰し，社会システムにおけるセキュリティ要件として日立が提唱する「H-ARCコンセプト」[3]について述べたうえで，このコンセプトに基づき提供するセキュリティソリューション基盤の概要について紹介する。

2. セキュリティを取り巻く動向

本章では，社会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の認識，システム構成，対策の動向などについて鳥瞰する（図1参照）。

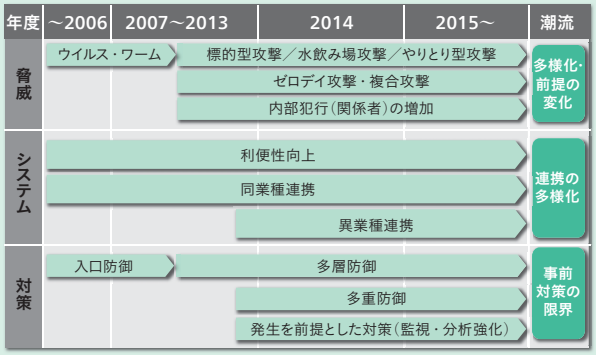


図1｜セキュリティ動向
近年，セキュリティ脅威の多様化が進むとともに，社会システム自体も種々の連携が進んでいる。このため対策技術も新たな考え方が必要である。

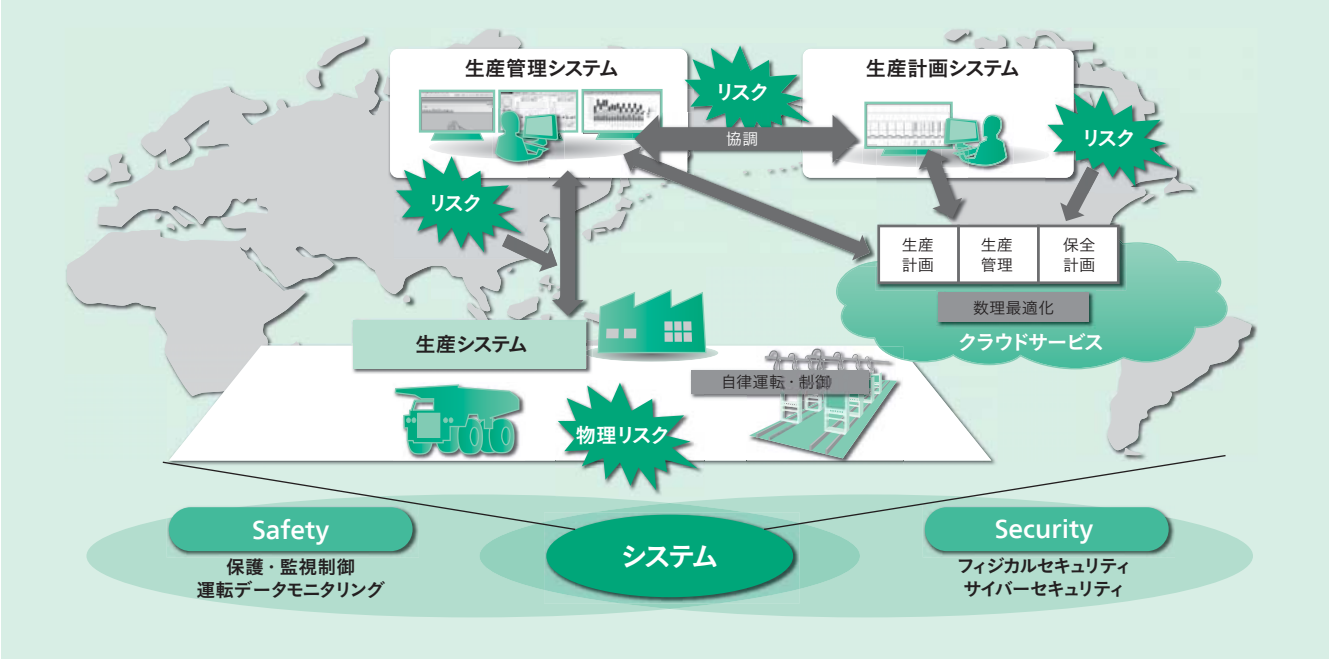


図2｜社会システムにおける安全・安心の確保
オープンアーキテクチャによりシステムが相互に連携する。「Safety」と「Security」の確保が重要である。

セキュリティ脅威は絶えず変化しているが近年はサイバー空間でのゼロデイ攻撃や，サイバー攻撃とフィジカル攻撃を複合した攻撃など攻撃が多様化している。さらに関係者が攻撃者となる内部犯行の考慮も必要となってきている。また，前提となるシステム構成についても，IoTやサプライチェーンの伸展などにより，業種や業務，さらに国の垣根を越えてシステムが相互に接続する「共生自律分散システム」化が進むと考えられる。**図2**に複数のシステムがオープンアーキテクチャにより相互に連携して動作する社会システムの例を示す。それぞれのシステムは地域を越えて動作するだけでなく，計画情報や稼働実績などのデータを効果的に活用すべく種々のサービスを利用する。このような社会システムにおいては，個々のシステムが自律的に稼働することがポイントであり，セキュリティにおいても個々のシステムで自律的に確保されることが重要である。結果として社会システム全体としてもセキュリティが確保されていることが必要である。

しかし，相互連携が伸展するほど，セキュリティ脅威の発生や影響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。このようなセキュリティ動向への対策を検討するうえで重要となるのが，脅威の発生を前提にセキュリティ対策を策定することと，現場におけるSafetyの確保を実現することである。これは社会システムが守るべき対象物（人，製品，情報，環境など）の安全を守ることであり，この要件を満足したサイバー空間およびフィジカル空間に対するセキュリティ施策を持つ複数の視点で対象物を守るシステムが不可欠である。

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。

社会システムのセキュリティを確保するために必要な要件をH-ARCコンセプトとしてまとめた（**図3**参照）。具体的には，対象システムの構成をベースに想定する脅威に対する強じん性（Hardening）を確保する。これをベースに，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（Adaptive），セキュリティ脅威が発生した場合に社会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（Responsive），さらにセキュリティ脅威の早期把握を実現

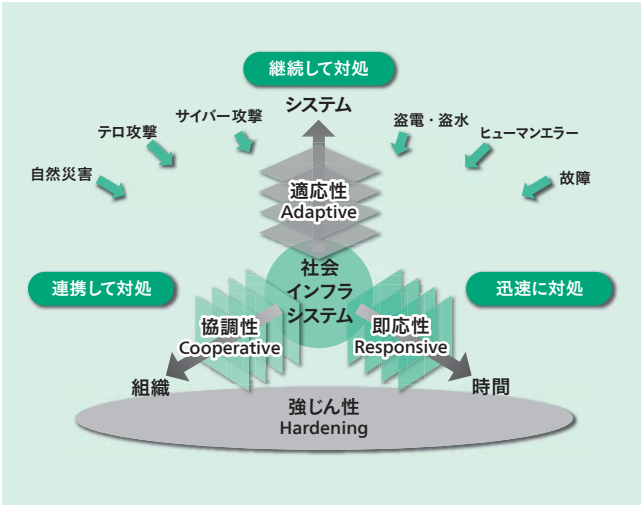


図3｜H-ARCコンセプト
日立は，社会システムにおけるセキュリティ確保をするうえで必要となる要件を「H-ARCコンセプト」として提唱している。

表1｜H-ARCでの実現内容

H-ARCの各軸において実現すべき内容を示す。

対策種別	概　要
システムの強じん化（Hardening）	システムを管理可能な単位（ゾーン）にゾーニングし，ゾーン内への不正侵入やゾーン内での不審な挙動を検知
脅威への持続的適応（Adaptive）	脅威の動向を踏まえ，システムが内包するリスクを定期的に把握，システム強じん化対策を更新／強化
脅威への迅速な対応（Responsive）	システム強じん化対策の状態を常時監視／分析し，脅威がシステム内に侵入した場合迅速に対処
脅威の情報共有（Cooperative）	現場と経営層，同業他社，顧客などのステークホルダーと脅威やリスクを共有（リスクコミュニケーション），事案発生に備える

するために複数の組織で相互に連携する協調性（Cooperative）をセキュリティの新たな要件として提唱している。

これらの軸は社会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，本要件を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」に提案し採択された。各軸で実現すべき内容について**表1**に示す。

4.　セキュリティソリューション基盤

前章で「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実現するためのセキュリティソリューション基盤について述べる。

「Safety」と「Security」を兼ね備えたシステムを実現するために，日立は標準的なセキュリティソリューションだけでなく，それぞれのシステムが実現するサービスや業務知識を生かしたセキュリティソリューションを提供する。個々の社会システムに対して分野共通のセキュリティソリューションを基に個々の社会システムに最適なセキュリティソリューション基盤を提供する（**図4**参照）。

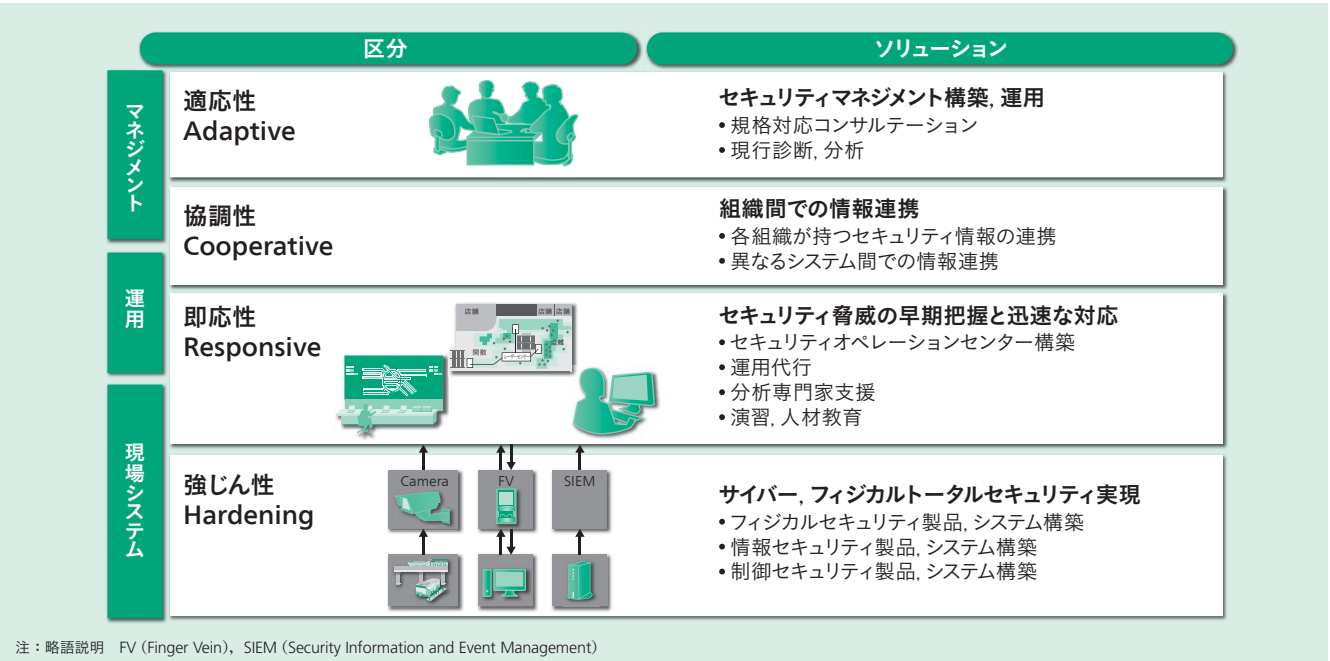
セキュリティソリューション基盤は，現場システムのセキュリティを実現するソリューションだけでなく，計画段階のセキュリティマネジメントから日々のセキュリティ運用までを見据えたソリューションを提供する。以下に提供するソリューションの概要について示す。

(1) 適応性のソリューション

適応性の観点からは，組織としてセキュリティマネジメントシステムを確立することが重要である。このために日立はIEC 62443やISO 27000シリーズなど，規格に対応したセキュリティマネジメントシステムを組織内に構築するためのコンサルテーションを提供する。また，マネジメントを的確に実施できるように既存システムにおけるセキュリティの状況を診断するとともにセキュリティリスクの分析を支援する。

(2) 協調性のソリューション

協調性の観点からは，セキュリティ脅威からシステムを守るために社内外の組織間での情報連携を実現する。情報連携により(1)のセキュリティマネジメントシステムにおいて最新のセキュリティ脅威や対策情報などを組織間で連携することで，最新情報を活用したマネジメントを実施可能とする。さらに次に述べる即応性確保の視点で情報連携が必要である。攻撃者は絶えず新たな手法やルートを組織的に検討し攻撃を仕掛けてくる。このため守る側においても，攻撃の兆候を複数の組織で広く収集し共有すること



注：略語説明　FV（Finger Vein），SIEM（Security Information and Event Management）

図4｜セキュリティソリューション基盤

H-ARCを実現するためのセキュリティソリューション基盤を示す。

が不可欠である。特にサイバー空間だけでなく映像などのフィジカル空間の情報を連携して共有することが重要である。日立はサイバー空間だけでなくフィジカル空間におけるセキュリティ情報を共有する環境構築や運用を支援するソリューションを提供する。

(3) 即応性のソリューション

即応性の観点からは，セキュリティ脅威を早期に把握し迅速な対応を可能とするために，「現場からのタイムリーな情報収集」,「効果的な状況分析」,「的確な対応策の策定」,「迅速な実行」が不可欠である。日立は，これらを実行するセキュリティオペレーションセンターの構築や実際の運用代行，セキュリティ技術の専門家や自社でのセキュリティオペレーションセンターの運用ノウハウを持つ専門家による分析の支援，セキュリティ脅威に対する演習を含む人材教育について提供している。

(4) 強じん性のソリューション

強じん性の観点からは，現場システムを守るためにサイバーとフィジカル双方の視点を融合し，セキュリティ脅威から対象を保護する施策を現場システムに実装することが必要である。日立はフィジカル空間の保護やサイバー空間を保護するためのソリューションとしてセキュリティ製品および各種システム構築を提供している。

なお情報セキュリティにおけるソリューション，制御セキュリティにおけるソリューション，フィジカルセキュリティにおけるソリューション，IoTシステムにおけるソリューションについては，本特集掲載の別論文で詳述している。

5. おわりに

本稿では，社会システムの安全・安心を支える日立のセキュリティソリューション基盤について説明した。

社会システムに対するセキュリティ脅威は，従来以上に組織活動や人の活動，さらに社会生活へ影響を与えている。また社会の進歩やIoT技術の進展によって組織活動と人の活動はより広大な網として連携する。このためセキュリティ脅威の発生や攻撃，感染ルートを予測することは，より一層困難となってくる。このような状況における，セキュリティ対策では，組織と人が個々に実施するだけでなく，網として連携して対応することが重要である。このため政府や団体よりセキュリティに関連するガイドラインや情報連携のための体制が整備されている。また国際規格としての整備や認証制度の制定が進められている。

日立としても，これからも変化を的確に捉え，最適なソリューションを提供するとともに，多くの組織との協創を進めることで安全・安心な社会システム実現に貢献していく。

参考文献など

1) IEC：http://www.iec.ch/
2) IEC：White Paper，Factory of the future，http://www.iec.ch/whitepaper/futurefactory/
3) 中野, 外:「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，日立評論，98，3，197～200（2016.3）

執筆者紹介

中野 利彦
日立製作所 社会イノベーション事業推進本部
セキュリティ事業推進本部 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

小野寺 剛
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
情報プラットフォーム統括本部 事業開発本部 所属
現在，情報サービスプラットフォームの事業開発の統括業務に従事

上脇 正
日立製作所 社会イノベーション事業推進本部
セキュリティ事業推進本部 所属
現在，セキュリティ事業開発に従事

宮尾 健
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
セキュリティ事業推進本部 所属
現在，セキュリティ事業の統括業務に従事