顧客協創により安全・安心を実現する日立の社会インフラセキュリティ

宮尾 健 Miyao Takeshi
中野 利彦 Nakano Toshihiko

社会インフラシステムの進化と増大する危険

日々の暮らしやビジネスを支える社会インフラには，トラブルに際しても常にサービスを提供し続けることが求められる。電力，ガス，水道，鉄道をはじめ，政府，金融，医療などのさまざまな分野のサービスにおいて，24時間365日停止することなく，あるいは，どんなときにも最低限の必要なサービスを提供することが期待されている。

社会インフラシステムでは，広域での運用や事業者間での連携，IoT（Internet of Things）技術のシステム適用が始まっており，システムが日々進化し，効率化が図られている。その一方で，海外ではテロに近い事象も増加し，またサイバー攻撃の手法も多様化しており，社会インフラシステムが実際に攻撃を受け，被害が発生する事案も出てきているのが現状である。

本稿では，このような状況において，日立が掲げる「協創」を基に，社会インフラ事業者と共に考え，セキュリティの脅威から社会インフラを協調して守るための取り組みについて概観する。

社会インフラを取り巻く環境

政府，業界団体における セキュリティに関する取り組み

政府では，社会インフラに対するサイバー攻撃への対策について，**内閣サイバーセキュリティセンター（NISC）**[a]を中心に各府省庁が連携して取り組んでいる。例えば，2015年1月に「**サイバーセキュリティ基本法**[b]」[1]が施行され，さらに2015年5月に，「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第4版）」[2]が，また2015年12月に，「**サイバーセキュリティ経営ガイドライン**[c]」[3]が経済産業省により策定された。産業界においても，一般社団法人日本経済団体連合会より，2016年1月に，「サイバーセキュリティ対策の強化に向けた第二次提言」[4]が出されており，これらの法制やガイドラインに従い，サイバーセキュリティへの対応が進められている。

セキュリティに関する国際標準化の動向

セキュリティに関する国際標準化は，従来からの情報システムセキュリティに加え，社会インフラを支える観点で，制御システムセキュリティに関する規格化が進んでいる。例えば，国際電気標準会議（IEC：International Electrotechnical Commission）において，制御システムセキュリティに関する標準化活動が行われており，汎（はん）用的な制御システム向けのセキュリティ標準規格として，IEC62443の策定が進められている。この規格の中で，特にIEC62443-2-1では，制御システムに関するマネジメントシステムを「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）」とし

(a) 内閣サイバーセキュリティセンター（NISC）
2014年11月に成立したサイバーセキュリティ基本法に基づき，2015年1月に内閣官房情報セキュリティセンターを改組，設置された組織。内閣のサイバーセキュリティ戦略に基づき，サイバーセキュリティ政策に関する総合調整を行いつつ，世界を率先する，強じんで活力あるサイバー空間の構築に向けた官民一体の活動を展開している。NISCはNational center of Incident readiness and Strategy for Cybersecurityの略称。

(b) サイバーセキュリティ基本法
サイバーセキュリティに関する施策を総合的かつ効果的に推進することを目的に，基本理念や国の責務を明確にし，基本的な取り組みやサイバーセキュリティを推進する体制の設置などを定めた法律。2014年11月6日の衆議院本会議で可決・成立し，2015年1月9日に全面施行された。

(c) サイバーセキュリティ経営ガイドライン
サイバーセキュリティを企業の経営問題と位置づけ，IT（Information Technology）の利活用が不可欠な企業の経営者を対象に，サイバー攻撃から企業を守るために認識する必要がある「3原則」と，経営者がCISO（Chief Information Security Officer）などの情報セキュリティ対策の責任者に指示すべき「重要10項目」をまとめたもの。

て規定している。CSMSでは，リスクアセスメントの実施のほか，演習の実行，フィジカルセキュリティ，セキュリティ組織の確立などの項目が規定されている。CSMSにおける認証制度は，日本が世界に先駆けて構築し，運用を開始した。

社会インフラ事業者における課題認識

社会インフラに関わるサービスを提供する事業者にとって，サイバー攻撃の多様化・高度化はセキュリティ上の脅威となっている。これらのセキュリティ脅威に対応するため，ガイドラインや標準規格を活用し，マネジメントとシステムそれぞれの観点から対応を進めている状況である。システムの観点では，リスクアセスメントを実施し，社会インフラシステムにおけるセキュリティ脅威と万一事象が発生した場合の影響を評価し，そのリスクの大きさに応じて優先順位をつけながら対策を実施している。しかし，システムにおける対策だけでなくマネジメントの観点での対応も重要となっている。社会インフラ事業者においては，セキュリティ対策に責任を持つ全社セキュリティ統括組織を設立する動きが出てきているが，実際のシステム運用に責任を持つ現場部門との意識合わせ，具体的な連携方法や，事業者間など業界を巻き込んだ連携などを模索している。このような状況で，セキュリティ対策・運用は，企画部門，情報部門，現場部門の連携が必要であり，さらには各業界を巻き込んだ活動が必要となることから，真に経営課題の1つと認識されるようになっている。

日立のセキュリティコンセプト

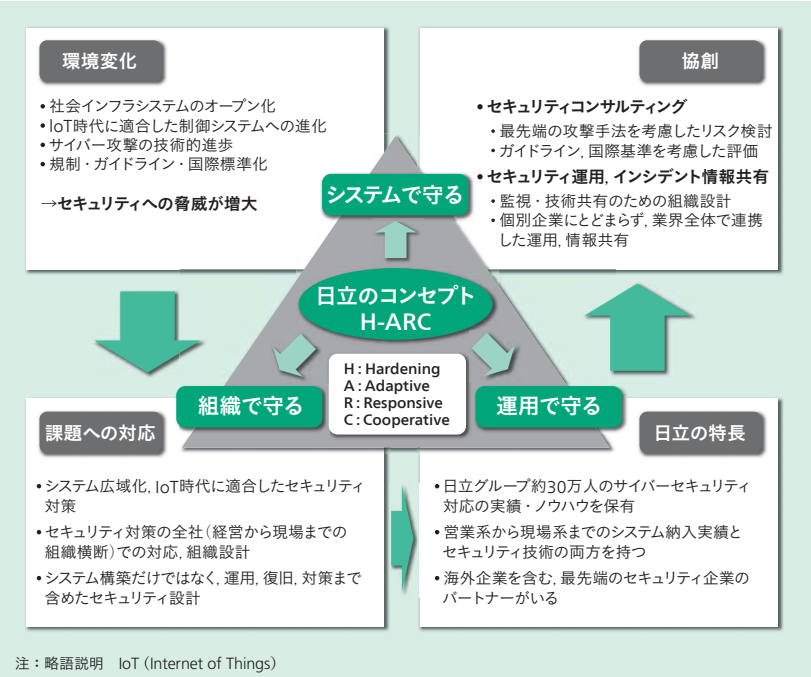
システム対策から，組織・運用対策へ

社会インフラをセキュリティの脅威から守るためには，システム上の対策はもちろん重要であり必要条件であるが，必ずしもそれだけでは十分と言えない。サイバー攻撃手法は日々進化しており，システムの継続的な改善が必要である。さらには，万一事象が顕在化した場合に，迅速に問題箇所を特定し，対策・復旧できる体制を構築しておくことが大切である。

日立では，「システムで守る。組織で守る。運用で守る。」をコンセプトに，「H-ARC」という考え方を用いてそのコンセプト実現に取り組んでいる。「H-ARC」は，セキュリティ対策を実現するための強固な基盤（H：Hardening＝強じん性）を基に，「システム」で新たな脅威に対する事前対策・防御を継続的に強化・実施し（A：Adaptive＝適応性），「運用」で攻撃発生後の被害を最小化・復旧を短時間化し（R：Responsive＝即応性），「組織」で異なる組織・事業者間の協調（C：Cooperative＝協調性）をすることにより，社会インフラを守るという考え方である（図1参照）。

社会インフラシステム構築実績を セキュリティ運用へ応用

日立は，電力，ガス，水道，鉄道，金融，行政といった各分野で社会インフラシステムを構築し，社会インフラ事業者に提供してきた実績がある。社会インフラ事業者が品質の高いサービスを提供していくうえで必要なのは，システムの高い信頼性と高可用性である。昨今のサイバー攻撃の脅威



注：略語説明　IoT（Internet of Things）

図1｜日立のセキュリティコンセプト
「システムで守る。組織で守る。運用で守る。」をコンセプトに，世の中の環境変化に対応し，社会インフラ事業者との協創を進めることで，安全・安心な社会インフラシステム実現に貢献する。

は，その品質を脅かす1つのリスク要因ではあるが，それがすべてではない。セキュリティリスクは単独で存在するわけではなく，装置故障や人為的ミス，災害など，他のリスク要因と併せて評価・対策されるべきものである。そのため，システム全体の運用の中に，セキュリティ運用をどのように組み込んでいくかが課題である。社会インフラシステムを運用している現場部門にセキュリティ運用機能を追加しながら，事業者全体での運用との整合性を取る必要があると考える。

多層防御とサイバー・フィジカルを融合した予兆検知技術

社会インフラシステムは，間接的にインターネットのような外部ネットワークに接続される場合が増えてきている。そのため，外部から社会インフラシステムに直接侵入されることはないものの，いくつかのゲートを徐々に通過・侵入し，最終的に社会インフラシステムに到達される可能性は残されている。

そこで，社会インフラシステムを守るために，多層防御と予兆検知の考え方を採用している。

多層防御は，外部から社会インフラシステムに到達するまでに複数のゲートを多層的に設けることである。サイバー空間，フィジカル空間を問わず，ゲートを多層化することで，システムへ侵入されるリスクを極小化し，侵入までの時間を稼ぐことができるため，その間に兆候を検知する可能性を高めることができる（**図2**参照）。

予兆検知は，多層化されたゲートにおいて，攻撃を受けていること，あるいは，社会インフラシステムに侵入はされていないものの，いくつかのゲートが突破されたことなどの，脅威の予兆を検知することである。**マルウェア**[(d)]検知技術や**ホワイトリスト型**[(e)]装置などを活用し，さらには複数の技術を組み合わせて予兆を検知する技術を開発している。特に，社会インフラシステムを運用しているオペレータを認識し，そのオペレータの操作であることと具体的な操作内容の整合性を取ることで正しい操作かを判定する技術によって，遠方からのサイバー攻撃に対して，フィジカルセキュリティの技術を応用して不正を検知することが可能となる。

日立グループ内での運用実績

日立グループでは，約30万人の社内ユーザーに対してITインフラサービスを提供しており，外部からのサイバー攻撃に対して，日々対応・対策を実施している。これは，国内最大規模のITインフラであり，セキュリティの専門要員により24時間365日監視を続けている。1998年に日本国内において他社に先駆けて組織内CSIRT（Computer Security Incident Response Team）を発足し，現在に至るまでセキュリティ運用を実施している。この運用実績と経験は，日立が社会インフラ事業者に提供するソリューションにも応用している。

顧客協創

日立は，顧客との協創により，社会イノベーション事業を推進している。セキュリティもその中の重要なテーマの1つであり，社会インフラ事業者におけるセキュリティに関する課題を，システム，組織，運用の観点より，顧客と共に考え，対応を進めている。

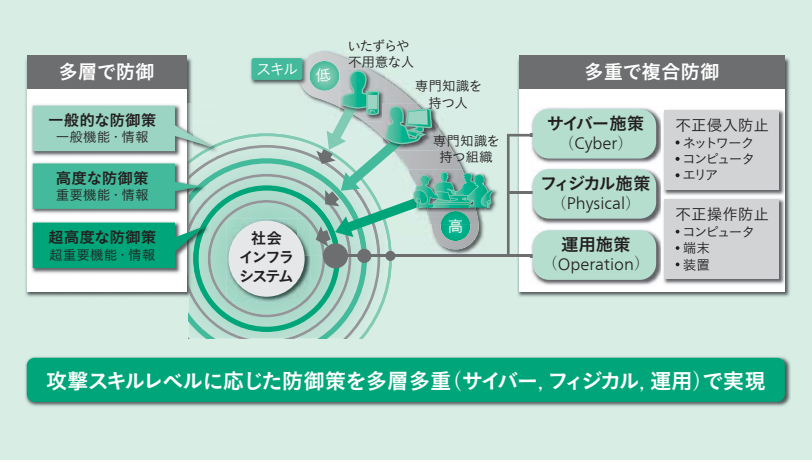


図2｜多層防御
防御策を多層化し，さらにサイバー・フィジカル・運用の各施策を多重化することで社会インフラシステムを守る。

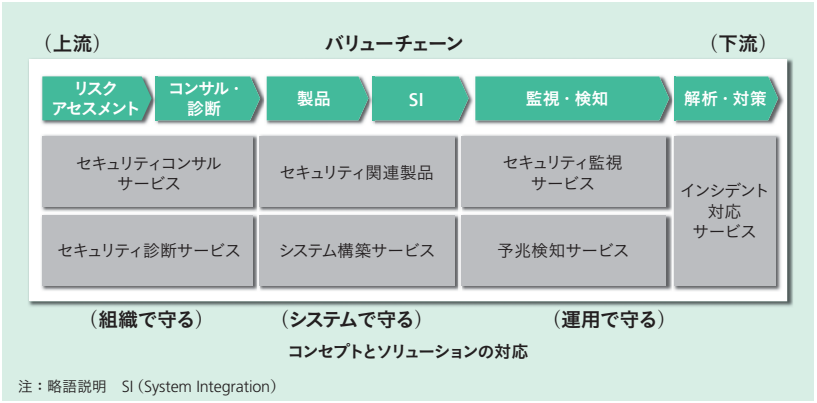
(d) **マルウェア**
Malicious Software（悪意あるソフトウェア）を略したことばで，コンピュータウイルス，スパイウェア，トロイの木馬などの悪意ある攻撃に利用されるソフトウェアの総称。近年は，特定の標的から機密情報を盗むなどの明確な目的を持った，標的型攻撃を行うものが増加している。

(e) **ホワイトリスト型**
デバイスをサイバー攻撃から保護する方法の1つで，承認されたプログラムのみを利用する方式。未知のマルウェアが侵入しても，プログラムの実行が禁止されるため，安全が守られる。これに対し，過去に確認された悪意のあるコードやデータを登録しておき，検出，駆除する方式をブラックリスト型などと呼ぶ。

日立のセキュリティソリューション

日立のセキュリティコンセプトに基づくソリューションの提供

日立は,「システムで守る。組織で守る。運用で守る。」をコンセプトに，社会インフラ事業者と共にセキュリティに関する課題に取り組むことを方針としている。そのため，セキュリティソリューションについても，バリューチェーンの観点を取り入れながら，コンセプトに沿ったソリューションを提供している（図3参照）。バリューチェーンの上流においては,「組織で守る」を具現化するためのセキュリティコンサルティングをサービスとして提供する。「システムで守る」の観点では，社会インフラシステムをセキュリティの脅威から守るための製品を提供し，システムとして構築する。バリューチェーンの下流では,「運用で守る」の観点より，セキュリティの監視・検知・情報共有・対策のためのソリューションを提供する。社会インフラ事業者の立場になって，トータルなバリューチェーンを構成するソリューションを提供している点が特長である。それぞれのソリューションの概要について，次項以降で紹介する。



注：略語説明　SI（System Integration）

図3｜日立のセキュリティソリューション
バリューチェーンの観点を取り入れながら，コンセプトに合ったソリューションを提供する。

セキュリティコンサルティング

セキュリティコンサルティングとしては，リスクアセスメントや国際規格に基づくコンサルティングを実施している。セキュリティコンサルティングを提供するうえで，セキュリティ技術を熟知していることはもちろんであるが，さらに重要なのは，対象となる社会インフラに関する業務知識やシステム構成，運用についても熟知していることである。日立は，社会インフラシステムの納入実績を多数持ち，また社内でもITインフラサービスを運用している経験を持っている。それらのノウハウを活用したコンサルティングを顧客に提供している点が特長である。

製品・システム構築

セキュリティ製品として，サイバー・フィジカル両面から製品を提供している。例えば，サイバーセキュリティでは，顧客のシステムを守るクラウドセキュリティサービスをはじめ，不正アクセスをネットワークレイヤで守るネットワークセキュリティや，情報資産を守るためのデータセキュリティに関する製品やシステム構築サービスを提供している。

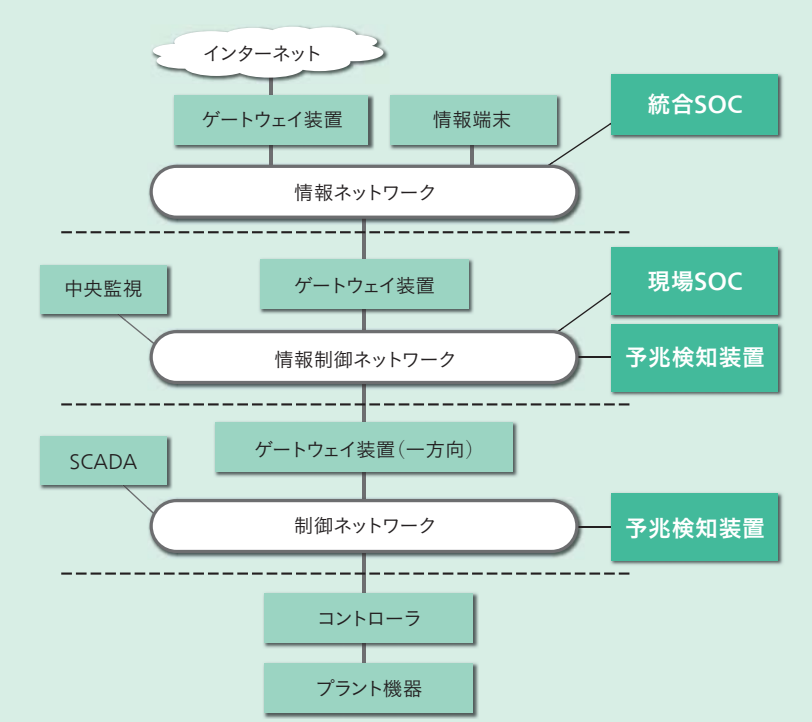
一方，フィジカルセキュリティでは，**指静脈認証**(f)を用いた入退室管理システムやカメラを応用した映像監視ソリューション，さらには爆発物を探知するためのゲート内蔵型爆発物探知システムを提供している。サイバーとフィジカルを融合させた製品としては，サイバー空間での不正侵入を防止するために，外界からの不正アクセスを物理的に遮断し，社会インフラシステムを守ることができる一方向中継装置を提供している。

(f) **指静脈認証**
体の一部を利用して個人の特定を行う生体認証の1方式。近赤外線を指に透過させて得られる指の画像から，静脈部分を構造パターンとして検出し，あらかじめ登録した静脈の構造パターンとマッチングさせて個人認証を行う。

セキュリティ運用サービス

社会インフラを守るためには，セキュリティ要件を満たしたシステムを構築した後も，継続的な監視が必要である。的確なセキュリティ運用を設計し，セキュリティへの脅威を早期に把握し，迅速な対応を可能としなければならない。そのためには,「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（SOC：Security Operation Center）の構築，実際の運用代



注：略語説明　SOC（Security Operation Center），SCADA（Supervisory Control And Data Acquisition）

図4｜セキュリティ監視アーキテクチャ

制御システム向けのセキュリティ運用・監視，検知のアーキテクチャで，現場設置するSOC，予兆検知装置と統合SOCを連携する。

行，セキュリティ技術の専門家や自社のセキュリティオペレーションセンターで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関するサービスを提供している。

また，社会インフラシステムの中でも，特に制御システムを対象としたSOCの構築，運用代行についてサービス開発を進めている。制御システムの場合には，SCADA（Supervisory Control And Data Acquisition）のような監視システムを持っているため，セキュリティ監視との機能分担や，予兆検知・状況分析・原因特定のためのデータログ収集，および迅速なシステム復旧のためのバックアップ復元などの機能が必要となる。そのため，社会インフラ事業者の現場部門をサポートするセキュリティ運用サービスを拡充していく（図4参照）。

安全・安心な社会システムを守るために

IoT時代に入り，社会インフラシステムも進化を続ける状況で，セキュリティの脅威も大きくなるばかりである。

日立は，「システムで守る。組織で守る。運用で守る。」をコンセプトに，社会インフラシステムを提供してきた実績と経験を生かしながら，社会インフラ事業者をはじめ，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） 内閣サイバーセキュリティセンター（NISC），関連法令等，
http://www.nisc.go.jp/law/
2） 内閣サイバーセキュリティセンター（NISC），活動内容，重要インフラの情報セキュリティ対策に関する主な資料，
http://www.nisc.go.jp/active/infra/siryou.html
3） 経済産業省，サイバーセキュリティ経営ガイドラインを策定しました，
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html
4） 一般社団法人日本経済団体連合会，サイバーセキュリティ対策の強化に向けた第二次提言，
https://www.keidanren.or.jp/policy/2016/006.html

執筆者紹介

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

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