情報セキュリティ
日立のサイバー攻撃対策ソリューション

川嶋 雄大 Kawashima Takehiro
本川 祐治 Motokawa Yuji
米光 一也 Yonemitsu Kazuya
濵田 紘幸 Hamada Hiroyuki
川嶋 一宏 Kawashima Kazuhiro

近年，社会インフラではIoT活用に向けた公開・広域ネットワーク接続が始まる一方，サイバー攻撃は技術的高度化や激化が進み，その脅威が懸念されている。
日立のサイバーセキュリティソリューションは，多層防御・早期検知・早期対応の3つのポイントについて，顧客の対策フェーズ全般にわたってメニューを整備している。アセスメントサービスなどの事前計画から，SOCサービスなどの監視・運用管理，CSIRT構築支援などのインシデント対応までの一貫したソリューションを提供してサイバー攻撃から顧客を守っている。
今後，未知のサイバー攻撃の脅威がますます増大することが予想される中で，日立はインテリジェンス情報共有によって集団防御を実現するための情報連携基盤構築や，セキュリティ人材の育成と活用などの幅広い活動によって社会インフラのセキュリティ維持・向上をめざす。

1. はじめに

21世紀に入って以来，サイバー空間の活用による社会イノベーションが次々と起こってきた。それと同時に犯罪やテロリズムの世界においてもサイバー空間の悪用は広まっている。その波は社会インフラの安全・安心に対する脅威となり，さらなる社会イノベーションにあたってサイバーセキュリティの確保が欠かせない状況となった。

ここでは近年のサイバー攻撃動向を踏まえ，日立のサイバー攻撃対策ソリューションの概要について述べる。

2. 社会インフラを取り巻くサイバー攻撃の動向

2.1 近年のサイバー攻撃動向

近年のサイバー攻撃は，ターゲットや攻撃手法など，さまざまな面で拡大，多様化の傾向を見せている。かつては個人による愉快犯的な攻撃が多く見られたのに対し，明確な目的を持ってサイバー攻撃を行うケースが増えてきている。

例えば，金銭を目的とした犯罪者集団が個人や企業，公的機関を狙って個人情報や企業情報を窃取しようとする攻撃や，ハクティビズムやサイバーテロのターゲットとして社会インフラ施設などを狙う攻撃がこれにあたる。企業がターゲットとなった場合に対処を誤れば企業価値を損なうおそれもあり，サイバーセキュリティはもはや企業にとって経営課題となったと言っても過言ではない。

これらの攻撃は目的とターゲットが明確であるため，ターゲットに最適化された攻撃手法が用いられる。代表例である標的型攻撃は，標的に定める人間に向け，その人間が最も受け入れやすい形で攻撃を仕掛ける手法である。攻撃の技術的手段は標的に合わせてさまざまな形を取るため，侵入を完全に阻むことは事実上困難である。

2.2 社会インフラにおけるサイバー攻撃の危険性

社会インフラではIoT（Internet of Things）活用やメンテナンス性・利便性向上のニーズが増大しており，公開・広域ネットワークへの接続が求められている。これによって従来は隔離されていた制御系システムが，情報系ネットワークや媒体経由で間接的に外部へ接続するケースが出てきている。社会インフラへのサイバー攻撃については，諸外国ではすでに攻撃のターゲットとなって被害が発生した事例があり[1)]，日本でも同様の事象が起こってもおかしくない状況と言える。

3. 日立のサイバーセキュリティへの取り組み

3.1 日立のサイバーセキュリティ対策の変遷

組織（企業・各種団体）におけるサイバーセキュリティ対策は，単なるセキュリティ機能（ウイルス対策ソフトウェアなどの製品）の導入だけでは完結せず，絶えず周辺状況を分析し，自組織において「現在」,「何が」最も適切なセキュリティ対策であるかを考え，変化させる必要がある。

1990年当時はセキュリティといえば組織と外界との間の境界防御を多層化し，常に進化させることが最適であった。そこで，日立は1996年にSOC（Security Operation Center：セキュリティオペレーションセンター）サービスを立ち上げ，MSS※)（Managed Security Service）の日本における先駆者として顧客に境界防御のためのサービスを提供した。その後，時代や技術によって変化する脅威と，攻撃者・犯罪者の意図分析を行ってきた。その結果，ショッピングサイトなどのWebアプリケーションへの攻撃，フィッシング詐欺，DDoS（Distributed Denial of Service）攻撃，標的型攻撃などの手法に対して，入り口・出口対策などの対策手法とIoT機器などに対する監視対象の拡大など，常にMSS自身を変化させてきた。一方，複雑化するサイバーセキュリティ情勢により顧客側にもセキュリティ対策を行う仕組みが必要となっている。具体的にはBCM（Business Continuity Management：事業継続マネジメント）の見地から，経営と現場をサイバーセキュリティの観点でつなぐCSIRT（Computer Security Incident Response Team：コンピュータセキュリティインシデント対応チーム）が必要となってきている（図1参照）。

日立は，MSSの延長線上に顧客のCSIRT活動を支援するサービスや，人と組織をつなぐ情報連携基盤と，基盤上で必要となるインテリジェンス情報の提供など，サイバーセキュリティソリューション全般を常に進化させている。

3.2 日立のサイバーセキュリティソリューション

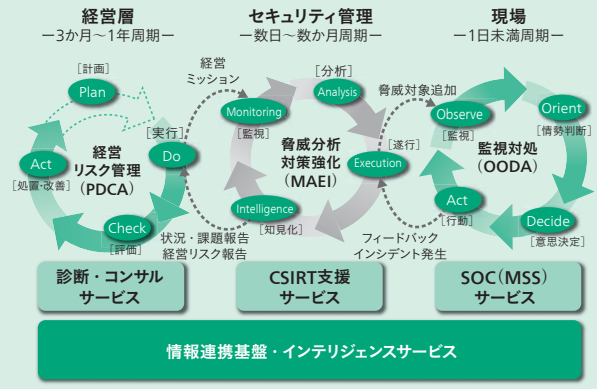
日立のサイバーセキュリティソリューションは，サイバー攻撃やマルウェアの侵入を前提として，多層防御・早期検知・早期対応の3つのポイントで整備している。

多層防御とは，入り口のみなどの局所的対策ではなく，入り口・出口・内部と多層を守ることでリスクを極小化し，事故を抑制することである。マルウェア・不正通信検知やWeb・メールなどの入り口・出口対策，サーバ・エンドポイントなどの内部の拡散対策を複合的に行う（図2参照）。

早期検知は，攻撃の兆候を早期発見し，被害を最小限に抑える仕組みを実現することである。イベント監視・SOC構築などにより攻撃の流れ・マルウェアの活動を把握し，監視する仕組みを構築することが重要である。

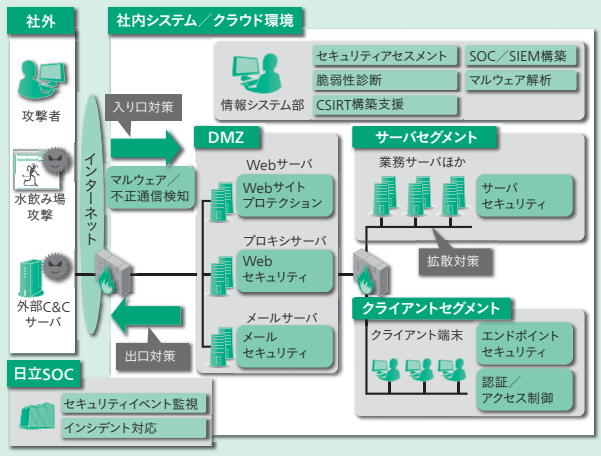
早期対応については，サイバー攻撃をはじめとした組織内の情報セキュリティインシデントに対応できる体制を整えることが重要である。CSIRTを構築し運用することが具体的施策の一例となる。これらのポイントについて，日立は「事前計画」から「対策・保護／監視・運用管理」,「事後対応」までの一貫したソリューションを提供する（図3参照）。

※) セキュリティ対策装置の監視や運用を通じて，IT（Information Technology）システムのセキュリティに関する異常を検知し，保護を行うサービス。



注：略語説明　PDCA（Plan, Do, Check, Act），
MAEI（Monitoring, Analysis, Execution, Intelligence），
OODA（Observe, Orient, Decide, Act），
CSIRT（Computer Security Incident Response Team），
SOC（Security Operation Center），MSS（Managed Security Service）

図1｜セキュリティ対策の周期と対応するサービスの関係
組織におけるセキュリティ対策は階層ごとに周期がある。周期はリンクする。中でもセキュリティ管理はCSIRTが担う。各階層に対し日立のセキュリティソリューションはワンストップで対応する。



注：略語説明　DMZ（Demilitarized Zone），C&C（Command and Control），
SIEM（Security Information and Event Management）

図2｜サイバーセキュリティにおける多層防御ソリューション
サイバー攻撃に対し，入り口対策，出口対策，内部拡散対策の多層防御によってリスクを極小化し，事故を抑制する。

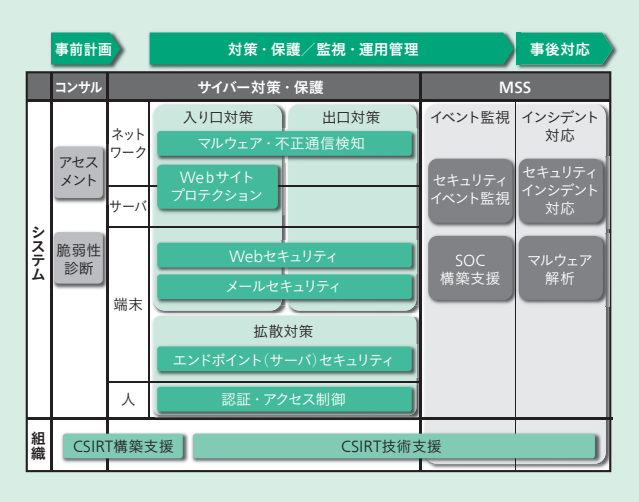


図3｜顧客の対策フェーズに応じたソリューションメニュー
「事前計画」,「対策・保護／監視・運用管理」,「事後対応」の対策フェーズに応じて一貫したソリューションを提供する。

3.3　サイバー攻撃対策事例：アセスメントサービス

サイバー攻撃対策では「守るべき資産は何か」,「どのような脅威があるのか」,「現状の対策状況はどこまで実施できているか」などの現状を分析し，対策方針を決める計画策定が重要である。

現状分析から対策方針を提案したアセスメントサービスの事例を以下に示す（図4参照）。高度なサイバー攻撃への耐性について専門家であるコンサルタントによる机上評価を行い，今後の対策方針を決定するためのサービスである。

日立は実際のサイバー攻撃の手法の類型化を行い，独自の評価手法を用いたアセスメントサービスを提供している。このサービスの特徴は，セキュリティに関する評価を専門に行う技術者だけでなく，ネットワーク・データベース・ハッキングなどの専門スキルを有する技術者が，豊富な経験を基に専門家の視点で評価する点にある。例えばネットワーク技術者の場合は,「顧客のネットワーク構成図の俯瞰（ふかん）」,「業務内容の簡単なヒアリング」により，ネットワーク構成上の問題点，ネットワークの入り口／出口／内部それぞれにおけるセキュリティ上の問題点を指摘することができる。

評価結果は，複数のセキュリティ上の問題点を提示し，それらを解決する優先度の高い対策案を列挙する形にまとめる。対策案は2種類あり，1つは「重要なセグメントにL7ファイアウォールを設置する」,「URLフィルタリング機能を持つプロキシを導入する」といった，対策にある程度の投資が必要な提案，もう1つは「ネットワーク構成の見直し」,「CSIRTの緊急時対応プロセスの事前整備」といった，投資を抑えて対策できる提案である。

顧客はこれらの評価結果を基にセキュリティ対策に優先順位を設定することで，投資対効果の最も高い対策から順に実行する，実現性・実効性の高いセキュリティ対策計画を策定し，遂行することができる。

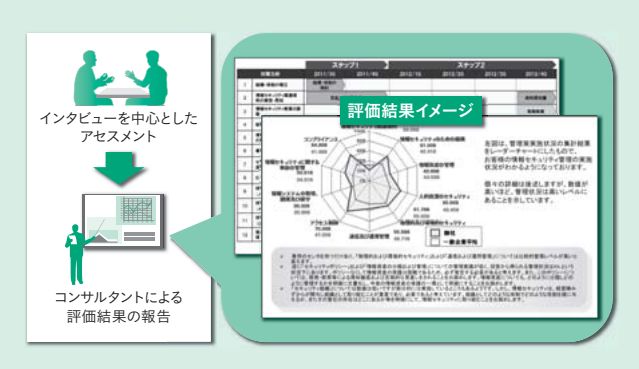


図4｜アセスメントサービスの評価結果イメージ
現状分析から対策方針を提案したアセスメントサービスの評価結果イメージを示す。

4.　社会インフラにおけるサイバーセキュリティの展望

4.1　社会インフラを守るためのインテリジェンス共有

日立はこれまで，社会インフラ・産業分野の顧客向けに，SIEM（Security Information and Event Management）によるログ相関分析機能を備えたSOC構築やCSIRT構築支援などを行ってきた。これらのセキュリティ監視基盤をより有効に機能させるためには，最新の脅威情報や脆（ぜい）弱性情報といったインテリジェンス情報を企業・組織の枠を超えてSOC/CSIRT他の関係者間で共有し，サイバー攻撃の被害が拡散する前に対策することが重要である。これが集団防御の基本的な考え方である（図5参照）。

具体的には，社会インフラ事業者や日立のSOCで検知したサイバー攻撃情報，セキュリティ関連ベンダから提供された脅威・脆弱性情報，セキュリティ技術者どうしの連携により得られた技術情報などを，インテリジェンス情報として情報連携基盤の上に集約する。この情報を解析することにより，各社のSOC/CSIRTに対するレポートや対策サービスの提供が可能となる。これによって社会インフラ

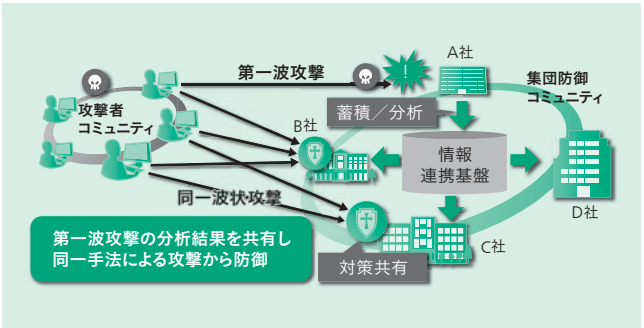


図5｜インテリジェンス情報共有の仕組み
第一波攻撃の分析結果をインテリジェンス情報として共有し同一手法による攻撃から防御する。

事業者は，新たに拡散しつつあるサイバー攻撃を未然に防ぐことが可能となる。

将来的に日立はこれらのサービス提供によって，平時のセキュリティシステム構築・監視運用・教育訓練から有事のインシデント対応まで包括的かつ継続的に社会インフラを支えるセキュリティサービスの確立をめざす。

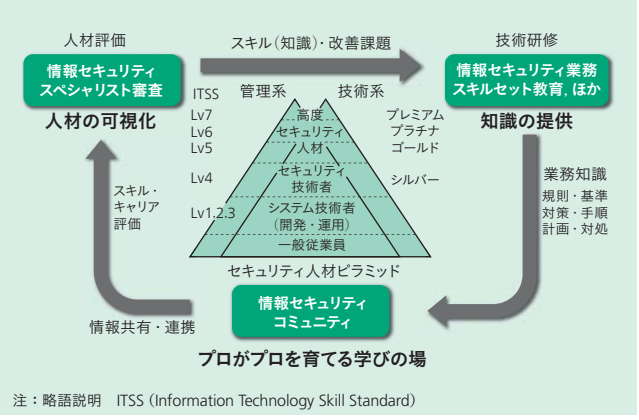
4.2　サイバーセキュリティ人材育成

激化するサイバー攻撃に対し，独立行政法人情報処理推進機構（IPA）の調査によれば情報セキュリティ人材は質，量共に不足が推計されている[2)]。日立は人材に関する課題をいち早く認識し，人材育成からコミュニティ活性化，キャリアパス構築まで一貫した取り組みをグループ内外で行っている。

日立グループ外との連携としては，産学連携によるセキュリティ公開セミナー[3)]のような人材供給の取り組み，国内最大級のセキュリティコンテストであるSECCONやコンピュータセキュリティシンポジウム／マルウェア対策研究人材育成ワークショップ［CSS（Computer Security Symposium）/MWS（anti Malware engineering WorkShop）］の協賛，大学連携チームでのMWS Cup2015出場（チーム優勝）といった研究者コミュニティ活性化の取り組みを行っている。

日立グループ内においては，ITスキル標準におけるレベルと専門性（管理系，技術系など）に応じた人材育成とキャリアパス構築を推進している（**図6**参照）。具体的には，人材の発掘・評価，育成・活用をねらいとして，情報セキュリティスペシャリスト審査による人材の可視化，情報セキュリティと業務スキルのセット教育他による知識の提供，情報セキュリティコミュニティによる「学びの場」提供などの施策で人材育成を加速する。

日立はこれらの取り組みによって，マルウェアなどの解析が可能な高度セキュリティ人材100人を含め，2018年度までにITSS（Information Technology Skill Standard）Lv4以上のセキュリティ技術者を1,000人規模へ拡大し，サイバーセキュリティソリューションの根幹となる人材育成サイクルを確立していく。



注：略語説明　ITSS（Information Technology Skill Standard）

図6｜日立のセキュリティ人材育成サイクル
人材評価，技術研修，情報共有・連携の3つの観点から，セキュリティ人材育成施策を推進し，人材育成サイクルを確立する。

5.　おわりに

今後，ナショナルイベントの開催などを契機として未知の攻撃手法による国内社会インフラへの攻撃が激化することも想定される。日立はこのため，社会インフラのセキュリティ維持・向上に向けてセキュリティ事業強化を推進していく。サイバーセキュリティ対策に終わりはない。

参考文献など

1)　SANS Industrial Control Systems Security Blog: Confirmation of a Coordinated Attack on the Ukrainian Power Grid,
https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
2)　独立行政法人情報処理推進機構：「情報セキュリティ人材の育成に関する基礎調査」報告書について（2014.7），
https://www.ipa.go.jp/security/fy23/reports/jinzai/
3)　日立システムズ ニュースリリース：産学連携・協創による情報セキュリティ人材不足解消への取り組みを強化（2016.1），
http://www.hitachi-systems.com/news/2016/20160125.html

執筆者紹介


川嶋 雄大
日立製作所 ICT事業統括本部 IoT・クラウドサービス事業部
事業推進本部 事業企画部 所属
現在，情報セキュリティ事業の企画業務に従事


本川 祐治
株式会社日立システムズ クラウドICTサービス事業グループ 所属
現在，Hitachi Incident Response Team（HIRT）ならびにサイバーセキュリティ技術取りまとめに従事
ISACA東京支部教育委員会委員長，
JNSA（NPO日本ネットワークセキュリティ協会）幹事


米光 一也
株式会社日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部
トータルセキュリティソリューション部 所属
現在，情報セキュリティコンサルタント事業に従事
情報処理技術者試験試験委員


濵田 紘幸
日立製作所 ICT事業統括本部 サービスプラットフォーム事業本部
IoT・クラウドサービス事業部 エンジニアリングサービス本部
セキュリティソリューション部 所属
現在，サイバーセキュリティ事業のソリューション開発業務に従事


川嶋 一宏
日立製作所 ICT事業統括本部 サービスプラットフォーム事業本部
サイバーセキュリティ事業統括本部 セキュリティ先端技術本部
セキュリティ先端技術部 所属
現在，情報セキュリティ人材育成業務に従事
博士（情報科学）