特集

セキュリティ

社会インフラを守る日立のセキュリティ

サイバー攻撃の対象がITシステムだけでなく社会インフラにも拡大し始めています。人々の生活を支える社会インフラがひとたび機能停止に陥れば、その影響は計り知れません。日立は2017年に世界中で発生したランサムウェアの被害を受けた教訓を生かし、セキュリティビジョン「Evolving Security for changing IoT world.（進化するセキュリティ）」の下、社内堅ろう化の取り組みと広範なセキュリティ人財の育成を進めるとともに、サイバー・フィジカルの両面から、お客さまの事業継続を支えるセキュリティソリューションを提供しています。

IoTの進展によって現れた脅威

さまざまなものがインターネットにつながるIoT※1の進展は、社会やビジネスに新たな価値の創出をもたらしました。しかしその一方で、従来ネットワークから隔離されていた電力や鉄道などもIoTを活用した効率的なサービスの提供により、セキュリティ上の脅威にさらされるリスクを顕在化させています。

2017年、世界的に猛威を振るったランサムウェア「WannaCry（ワナクライ）」がその一例です。

Windows®のぜい弱性を悪用して拡散するWannaCryは、感染したシステムのファイルを暗号化し、その暗号解除の鍵と引き換えに金銭を要求するウイルスです。確認されているだけでも150か国以上、数十万台のコンピュータに感染し、銀行、病院、物流、通信会社などに大きな被害を与え、日立グループでも欧州現地法人の検査機器から社内ネットワークのサーバなどが次々と感染してグローバルな被害を受けました。

現在も特定組織や団体を狙ったサイバー攻撃は日々増加の一途をたどっており、今後IoTがグローバルな社会で広がっていくなか、新たな観点からセキュリティの脅威に立ち向かう必要に迫られています。

このような状況の下、政府は、国際的なスポーツイベントなどに備え、サイバー攻撃の被害により社会的に多大な影響が想定される業界に対し企業間連携を呼びかけています。例えば、国土交通省は社会の重要インフラである鉄道・航空・物流などへのサイバー攻撃を連携して阻止すべく、すでに設立されている金融・情報通信・電力分野のISAC※2（セキュリティ人財育成や先進的な対策事例を同じ業界で共有する民間組織）に続く交通ISACの設立支援を行うなど、活発な取り組みを進めています。

一方、こうしたサイバーセキュリティ対策を担う人財の不足も社会的な課題となっており、今後はITシステムだけでなく、社会インフラシステムにも対応できるセキュリティ人財を、いかに育成・確保していくかが国を挙げた重要なテーマとなっています。

※1 Internet of Things
※2 Information Sharing and Analysis Center

IoT時代を迎え、インシデント発生時の経営インパクトは、より増加
⇒ サイバーセキュリティは経営課題としてとらえることが必須

1. イントラ内部は、利便性を最優先したフラットネットワークのため、拡散型のワーム型ウイルスへの耐性がない。

- IoT時代に接続するものが多様化しており、一部弱いところから拡散する
- 接続されている機器のすべてが見えていない

2. サーバに対するセキュリティ対策の徹底不足が露呈した。

- 業務都合でパッチを当てられない
- 複雑な仮想環境運用を実施しているため、迅速に対応できなかった

3. IoT機器へのセキュリティ対策が困難であることを再認識した。

- パッチを適用することが想定されていない
- 導入する側もそもそもOSをアップデートする意識がない

4. 災害BCPとサイバー攻撃を想定したBCPの違いを再認識した。

- 災害BCPとはRecovery Time Objective (RTO) が明らかに異なる
- インシデントレスポンスとサイバー攻撃を想定したBCPは連続性がある

BCP：Business Continuity Plan

表1 サイバー攻撃から得た教訓

日立がサイバー攻撃事案から得た教訓

WannaCryによるサイバー攻撃事案の教訓は、4点あります（表1）。これらを踏まえた今後の対策として、IoT時代における大規模システム（ネットワーク）運用のあり方を見直し、セキュリティインシデントの発生時に事業継続の観点からどのように対応すべきかの予防措置を事前に講じておくことの重要性をあらためて確認しました。その気づきと対策をお客さまと共有し、ともに検討・推進していくことで、より安全・安心なIoT時代の社会インフラを協創していきたいと考えています。

日立は社内の堅ろう化を図るため、セキュリティガバナンス強化の取り組みとして6要素に焦点を当てています（表2）。これらの要素の実現に向け、2017年10月、これまでCIO※3が兼務していた情報セキュリティの責任を分離し、CISO※4が日立グループ全体のセキュリティを統括するガバナンス体制と、そのための情報セキュリティ統括組織を設置しました（図1）。

CISOと情報セキュリティ統括組織は、日立グループのネットワークにつながる、すべての製品や社内設備を対象に、情報セキュリティのガバナンスを行います。これにより、システムの実装・運用の設計において、最初からセキュリティを考慮した“セキュリティファースト”を確立するとともに、サイバーセキュリティ対策のPDCA※5から得られた知見を、お客さま向けの製品やサービス、システム構築などにも順次フィードバックしていきます。

ガバナンス体制の強化と並行し、攻撃の早期検知と迅速な対処の実現に向け、監視およびインシデント対応についてテクニカル面での強化も進めています。日本だけでなく欧州、米国、中国といったグローバル拠点でのセキュリティ監視強化を実現する体制づくりも行っており、SOC※6による24時間365日の監視とHIRT※7によるインシデント対応の強化で、初動対応から対策までを迅速化し、サイバー攻撃による被害を最小限に抑える環境を実現していきます。

※3 Chief Information Officer：最高情報責任者
※4 Chief Information Security Officer：最高情報セキュリティ責任者
※5 Plan-Do-Check-Act
※6 Security Operation Center
※7 Hitachi Incident Response Team

社内で実証を重ねたセキュリティをお客さまへ

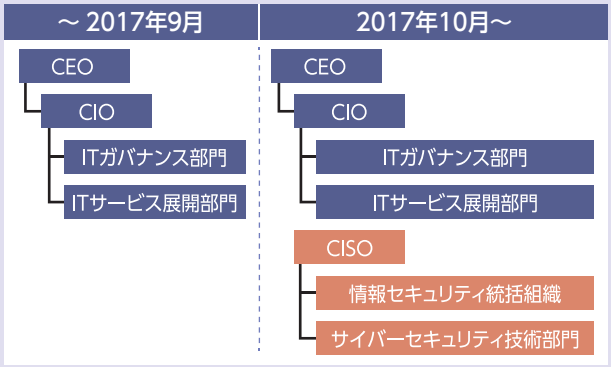
日立は、一連の堅ろう化施策で蓄積したノウハウや、社内で実証を重ねたセキュリティ技術を、社会インフラを中心としたお客さま向けに、サイバー・フィジカル両面からのセキュリティソリューションとして提供します。

例えば、ITシステムだけでなくOT※8/IoTシステムまで含めたセキュリティ運用・監視や事業継続計画の実現をトータルに支援するのが「セキュリティ統合監視ソリューション」です。これにより、お客さまに適したセキュリティ運用環境を実現するため、上流のセキュリティコンサルティングからシステム構築、運用・監視にいたるまでのバリューチェーン

1. **サイバー攻撃を想定したBCP設計**
   災害に加え、サイバー観点・グローバル観点を設計
2. **事業リスク分析に基づいたITでの対策**
   情報資産の重み付けを意識したITでの対策
3. **パッチマネジメントにおけるセキュリティパッチ強制適用**
   IoT機器、物理セキュリティほか、現場機器もすべて管理できる体制構築
4. **IT責任者の管理範囲・権限の見直しによる一元管理体制構築**
5. **セキュリティマネジメントのグローバルガバナンス**
   各国のリージョンを含めた体制再検討
6. **IoTセキュリティガイドラインの制定**

➡ **グループ横断での情報セキュリティ専門部門の設置**

表2 ガバナンス強化の取り組み



【CISO/セキュリティ統括組織の役割】

a) サイバー /情報セキュリティマネジメントの継続的実行
b) 日立グループ全体に影響を及ぼす事案へのシステム停止判断と提言
c) 経営インパクト、残存リスクへの対策の日立経営会議へ定期的な答申および実行

図1 CISOの体制と役割

をカバーした、付加価値の高いソリューションを提案していきます。

また、日立独自の「指静脈認証」技術を適用したフィジカルセキュリティも進化させ、柔軟かつ強固な本人認証の仕掛けを提供します。

※8 Operational Technology

広範なセキュリティ人財の育成にも注力

日立は、社会インフラを担うセキュリティ人財の育成にも力を入れています。セキュリティの確保は一部のセキュリティ専門家だけでは実現不可能であり、組織の構成員が担当業務に応じて、それぞれセキュリティ面で求められる役割を果たす必要があります。

そこでグループ内の人財育成では、経済産業省が定めた「ITSS」※9（ITスキル標準）と社内認定制度などの仕組みを利用して、人財状況の見える化と効果的な育成を推進。情報系だけでなく、産業システムや制御システムに携わる従業員にも、IoT時代に求められるセキュリティスキルを学ばせ、インシデント発生時には専門部署と連携しながら現場で対応できるセキュリティ人財の育成を図っています。

また日立は、セキュリティを速やかに社会に導入するための活動にも貢献してきました。例えば、独立行政法人情報処理推進機構（IPA）が発足させた産業サイバーセキュリティセンターや、重要インフラ分野を中心に企業約30社が参加する「産業横断サイバーセキュリティ人材育成検討会」にも中核的な立場で参画。サイバーセキュリティ対策の根幹を担う人財育成を、政府や産業界とともに積極的に推進しています。

※9 Information Technology Skill Standard

社会インフラの事業継続を支え続ける

サイバー攻撃がサプライチェーンに及ぼす影響が拡大している現在、事業継続の観点から強固なセキュリティ対策を講じることが、すべての企業にとって重要な経営課題となっています。日立は社会インフラシステムの構築・運用実績とノウハウを生かし、どのレベルまで対策すればよいかを短期・中期・長期に分けて提案し、新たな脅威に向け、進化するセキュリティで事業継続を力強く支えていきます。

お問い合わせ先

（株）日立製作所 セキュリティ事業統括本部
http://www.hitachi.co.jp/security-inq/