Overview

IoT時代へつなぐ 防災・セキュリティソリューション

宮尾 健 | Miyao Takeshi
中野 利彦 | Nakano Toshihiko

1. IoT時代の光と影

IoT（Internet of Things）の出現により，あらゆるものがインターネットにつながる世界になりつつある。スマートフォンやセンサー，カメラなどを用いて，モノやヒトの動向はデータ化され，インターネットにつながる。現実世界をデジタルにモデル化し，サイバー空間上で分析・試行するIoTは，これまでにないスピードで新たな価値を発見し，現実世界へフィードバックすることを可能にする。これにより，産業の在り方，社会インフラ自体の在り方までもが大きく変わろうとしている。

このように，IoTの出現により新しい価値が生み出される一方で，新たな脅威が出現している。

例えば電力や鉄道など，従来は外部ネットワークから隔離されたシステムを用いていたために攻撃の対象とならなかったシステムが，IoTを活用したより高度なサービス提供の実現に伴い，セキュリティ上の脅威にさらされるようになってきている。さらに，システムのつながりが拡大し，巨大なエコシステムやサプライチェーンが構築される中で，セキュリティの弱い部分を入り口としてシステム全体が攻撃にさらされるなど，単体の企業や組織では発生しなかった新たな課題・脅威が生じている。

IoT時代において，人々が安全・安心に過ごすための生活基盤を築き，レジリエントな社会を実現するためには，IoTによる利便性と脅威を見極めたうえで，十分なセキュリティ対策を実施することが不可欠となっている。

2. IoTとともに進化する 防災・セキュリティへの取り組み

日立は，IoT時代における顧客のビジネス進化を実現するために，IoTを活用したデータ分析，経営課題を解決するソリューションを提供していく。その基盤となるのが，日立のIoTプラットフォームLumadaである。Lumadaはオープンかつ段階的なアプローチを提供するIoTプラットフォームであり，顧客の持つさまざまなシステムやデータとつながり，高度な分析を行うことで，業務改善や事業創生に有用なインサイトを生み出し，ビジネスの進化を加速する。

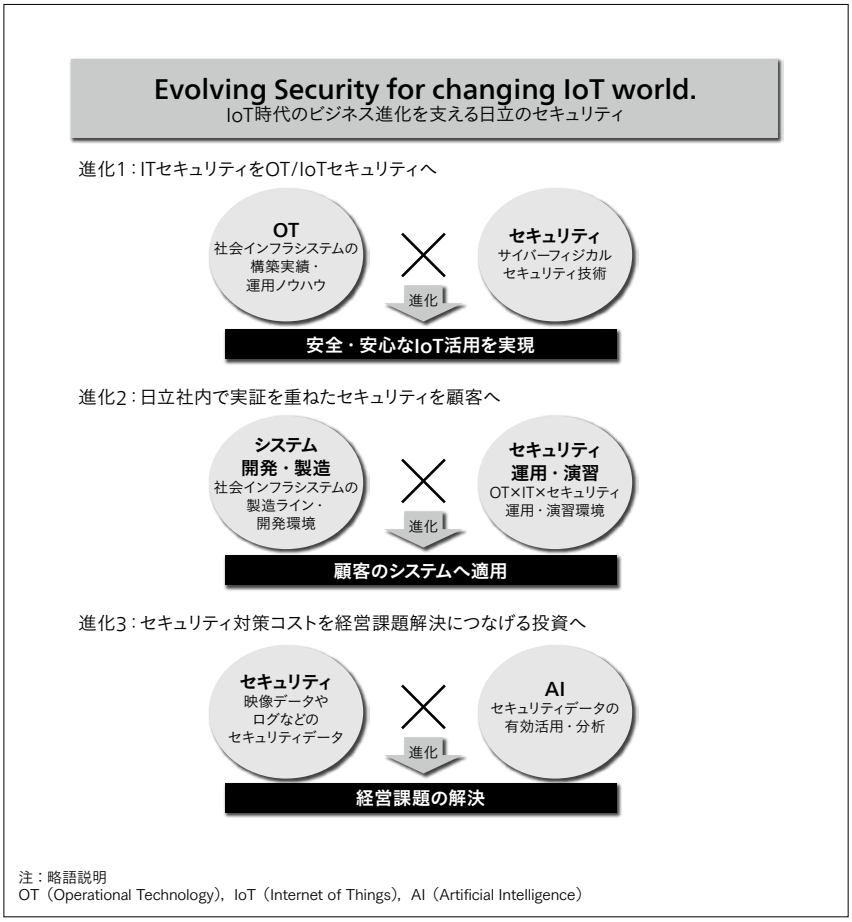
そして，「安全」で「安心」なビジネス進化のために，IoT時代に必要なセキュリティをLumadaの基盤技術の一つとして提供していく。変化するIoT時代において，顧客のシステムやサービスを守るため，日立はセキュリティのビジョンとして，「Evolving Security for changing IoT world.」を掲げ，セキュリティを進化させる。その方向性について以下に紹介する（**図1**参照）。

2.1 進化1：ITセキュリティをOT/IoTセキュリティへ

日立は，電力，鉄道，ガス，水，製造，情報通信，金融，公共などの社会インフラシステムを構築し，顧客に提供している。この経験と実績は，セキュリティ対策を実施するうえで重要な要素と考える。社会インフラシステムのセキュリティ対策は，セキュリティ技術のみならず，システムがどのように運用されているか，そのうえでどのように守ればよいかを理解して初めて有効である。特に，OT（Operational Technology）/IoTセキュ

図1｜日立のセキュリティビジョン

変化するIoT時代において，顧客のシステムやサービスを守るために，図に示す3つの方向にセキュリティを進化させる。



注：略語説明
OT（Operational Technology），IoT（Internet of Things），AI（Artificial Intelligence）

リティには，「安全」と「事業継続」が重要となる。システムが正しく動き，サービスを安全に，かつ継続的に提供することが大切であり，インフラ構築の経験がセキュリティ適用に生かされるポイントである。

2.2
進化2：日立社内で実証を重ねたセキュリティを顧客へ

日立は，多種多様なセキュリティの実証環境を構築・保有している。IT系においては，日立グループ約30万人の社内ユーザーに対するITインフラの運用実績を持っている。また，1998年に日本国内で他社に先駆けて組織内CSIRT［Computer Security Incident Response Team（HIRT：Hitachi Incident Response Team)］を発足し，実績を蓄積している。

OTセキュリティにおいては，大みか事業所にセキュリティの実証・演習設備を構築し，セキュリティ演習を通して顧客と協創する環境を整えた。

フィジカルセキュリティ関連では，ウォークスルー型指静脈認証装置を実際の入退館に活用・実証している。

このように，社内で実証を行ってセキュリティ技術を進化させ，その成果を顧客に提供している。

2.3
進化3：セキュリティ対策コストを経営課題解決につなげる投資へ

日立は，AI（Artificial Intelligence）やアナリティクスの技術をセキュリティに応用することで，セキュリティ対策費用を業務効率化など経営課題解決への投資に進化させていく。

例えば，セキュリティの監視運用は，膨大なログを常にチェックしなければならず，高負荷であるとともに，セキュリティの技術を持った人材でないと対応が難しい作業である。しかし，AI技術をログ解析に活用することで，業務の効率化を図ることができる。

また別の例では，同時に大量発生する映像データに対してAI技術を活用することで，目視では困難なリアルタイムの監視が可能となる。さらには人の動作を分析することで，安全性や作業効率を向上できる可能性がある。

AI技術を活用した予兆検知，行動分析により，セキュリティインシデントへの事前対策が可能となる。事故発生後のシステム・サービス停止からの復帰，経営品質のリカバリーにかかる費用は膨大であるため，小さな異変を検知し，先手を打って対策することで事業継続性を高め，経営の品質を守っていく。

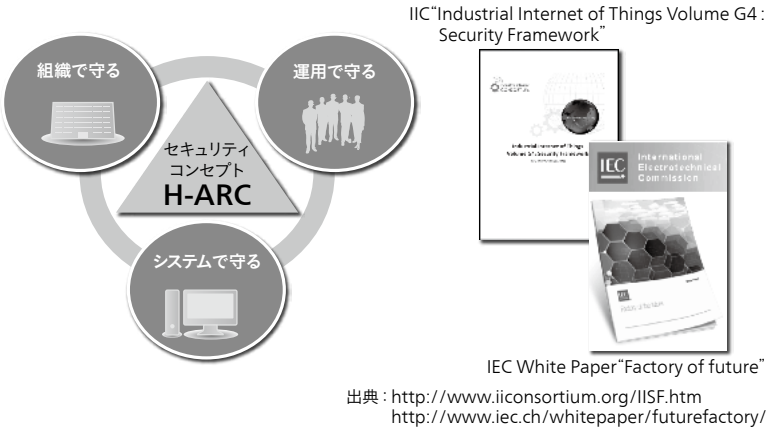


図2｜日立のセキュリティアプローチと国際標準化活動

「組織で守る，システムで守る，運用で守る」というアプローチで顧客の安全・安心を実現していく。また，日立のセキュリティコンセプト（H-ARC）が国際標準機関のホワイトペーパーに採択されるなど，OT/IoTセキュリティの国際標準化へ貢献している。

3. 安全・安心を支える日立の防災・セキュリティソリューション

日立は，顧客の安全・安心を実現するため，「組織で守る，システムで守る，運用で守る」というセキュリティアプローチを取っている。セキュリティシステムの構築はもちろん，それらの対策を継続的に維持するためのマネジメントシステムや，異常な挙動を監視・検知するための対応策を提供している。それらを実現し，支えるための考え方としてセキュリティコンセプトH-ARCを創出し，その内容を国際標準機関のホワイトペーパーに提案して採択されている。日立はセキュリティアプローチに従い，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，運用監視に至るまでのバリューチェーンをカバーする形でソリューションを提供している。また，ITシステムに対するソリューションを，OT/IoTシステムに対するソリューションに進化させ，サイバーセキュリティとフィジカルセキュリティを融合させた形での解決策を提案する（**図2**参照）。

特に，IoT時代に対応するため，「セキュリティ統合監視（Integrated Security）」，「エリアセキュリティ」，および「IoTセキュリティ」の3つのソリューションを開発した。

「セキュリティ統合監視」は，ITシステムだけでなくOT/IoTシステムまで含めたセキュリティの運用・監視，セキュリティ運用組織の統合・効率化およびインテリジェンス情報の共有・活用といったIoT時代に必須となる運用課題を，AI活用を含めて網羅的かつ効率的に解決するソリューションである（**図3**，**図4**参照）。

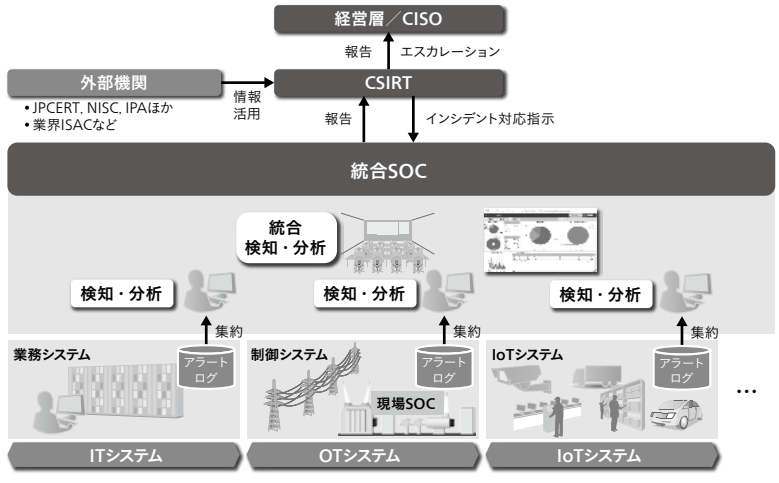


図3｜セキュリティ統合監視の全体像

ITシステムだけでなくOT/IoTシステムまで含めたセキュリティ運用・監視，セキュリティ運用組織の統合・効率化，インテリジェンス情報の共有・活用といったIoT時代に必須となる運用課題を，CSIRTや経営層も巻き込んで解決していく。

図4｜統合SOC監視画面の例

ワールドワイドに展開している製造業の工場をモデルとした監視画面の一例を示す。OT・IT・IoTシステムのアラートやログ情報などを集約し，AIも活用しながら網羅的に情報を表示している。

「エリアセキュリティ」は，発電所・空港・駅・街区・工場・テーマパークなど，人々の暮らしを支える社会インフラのさまざまなエリアにおいて，セキュリティ強化とビジネス進化（業務改善・経営課題解決・新事業創生など）を実現するソリューションである。

「IoTセキュリティ」は，IoT時代の到来に伴って生じる，今までにないセキュリティ上の重要課題を解決するため，日立が独自の視点でIoTシステムを捉え，提案するセキュリティソリューションである。

4. 顧客との協創と経営課題解決

日立は，変化するIoT時代に合わせてセキュリティを進化させ，顧客の提供するサービスや事業を守っていく。これは，顧客が提供するサービスがどのように構築・運用されているかを知ったうえで，顧客と共に考え，サービスを進化させることで，真の経営課題の解決に努めるということである。

セキュリティ対策費用は，単なるコストではない。課題解決を通して業務効率化や品質向上に貢献し，投資の一環として経営に貢献するものである。日立は，投資の極小化・最適化を図るため，社会インフラシステムの構築・運用のノウハウを生かし，どのレベルまで対策すればよいかを，短期・中期・長期の3つの視点から提案していく。また，初期投資を抑え，スモールスタートをしながら段階的にシステムを構築することが可能なプラットフォームを提供している。

日立はセキュリティを経営者の視点で捉え，顧客のすぐそばで，その事業を進化させていく。

5. おわりに

本稿では，IoT時代に求められる防災・セキュリティソリューションの取り組みの考え方について説明した。

これらの考え方に基づく具体的なソリューションや研究開発，および防災・セキュリティに関する適用事例については，本特集掲載の別論文で詳述しているので参照されたい。

参考文献など

1）IoT推進コンソーシアム，総務省，経済産業省：IoTセキュリティガイドラインver 1.0（2016.7），
http://www.soumu.go.jp/main_content/000428393.pdf

2）宮尾健，外：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，日立評論，98，6，394～398（2016.6）

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
サービスプラットフォーム事業本部 セキュリティ事業統括本部
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 サービス＆プラットフォームビジネスユニット
サービスプラットフォーム事業本部 セキュリティ事業統括本部
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