社会インフラを支えるIoT時代のエリアセキュリティ

近年，社会情勢の不安定化に伴って，テロ・犯罪などの脅威は増加かつ多様化しており，人々の暮らしを支える社会インフラには，より強固な安全・安心が求められている。
日立は，これらの脅威から社会インフラを守るため，IoTの活用によってセキュリティを進化させ，より強固な安全・安心を実現するとともに，デジタルトランスフォーメーションによって新たな価値を創出するセキュリティソリューションを提供していく。
本稿では，日立が開発したプラットフォームを活用し，フィジカルセキュリティシステムやIoTセンサーで取得したフィジカル空間の情報を見える化・分析することで，人やモノの動態管理を行い，社会インフラのセキュリティ強化やビジネス進化へつなげるエリアセキュリティの取り組みについて紹介する。

下条 智貴 | Shimojo Tomotaka
宮澤 泰弘 | Miyazawa Yasuhiro
仲田 智 | Nakata Satoshi
小屋 博 | Koya Hiroshi

1. はじめに

近年，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は，社会情勢の不安定化やテクノロジーの発展などにより，さまざまなテロや犯罪の脅威にさらされている。

日本国内においては国際的な大規模イベントを控え，また世界では事業継続に大きな影響を与えるサイバーテロや人々が集う場所を狙った爆破・銃撃テロが発生するなど，社会インフラにおけるセキュリティ強化は急務となっている。

本稿では，社会インフラにおけるセキュリティ対策の課題を背景にIoT（Internet of Things）を活用したセキュリティ進化の方向性を述べ，日立が推進するエリアセキュリティの取り組みについて紹介する。

2. IoT時代におけるセキュリティ進化

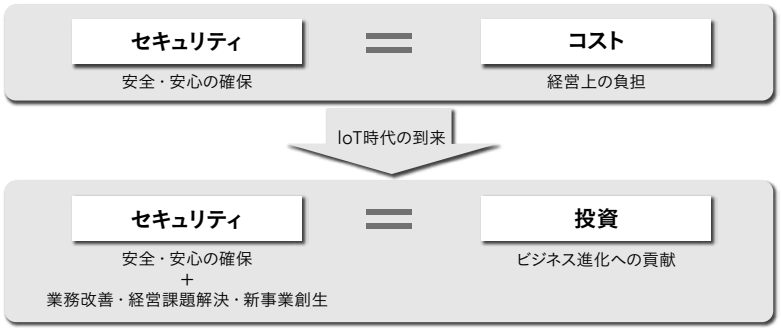
2.1 セキュリティ対策の課題

社会インフラにおけるセキュリティ対策の考え方は，国・業界あるいは事業者自身によって各種セキュリティガイドラインとして策定されている。これらのガイドラインに従ってセキュリティ対策を行う場合，事業者としての基本方針を決定し，リスクの洗い出しや脆（ぜい）弱性診断を行い，優先順位を付けて対策していく必要がある。特に，セキュリティの強靭（じん）化を図るためには，サイバーセキュリティおよびフィジカルセキュリティの技術・運用面での対処を組み合わせ，多層・多重で防御することが重要である。

しかし，セキュリティ対策費用は社会インフラ事業者

図1｜社会インフラにおけるセキュリティ対策の課題と進化の方向性

社会インフラ事業者にとってセキュリティ対策は単なるコストではなく投資と位置づけ，新たな価値を創出するための仕組みが必要である。



注：略語説明
IoT（Internet of Things）

にとって単なるコストであり，過剰な対策は経営上の負担であるという見方から，対策の決定には慎重な検討が重ねられる。その結果，適切な対策範囲を判断できず，脆弱性や老朽化の問題を抱えたまま，セキュリティ対策・強化を先送りしてしまうケースもある。

社会インフラにおける安全・安心の確保にセキュリティは不可欠であるが，セキュリティ対策・強化を加速させるためにも，これらの費用をコストではなく投資と位置づけ，業務改善・経営課題解決・新事業創生など，事業者のビジネス進化に貢献していくことが，IoT時代のセキュリティソリューションに求められる新たな価値であると考える（**図1**参照）。

2.2
デジタルトランスフォーメーションの取り組み

セキュリティが社会インフラ事業者のビジネス進化に貢献するためには，内閣府がSociety 5.0の推進に向けて提唱しているICT（Information and Communication Technology）を活用したサイバー／フィジカル空間の融合がキーワードになると考える。

具体的には，人やモノを監視するフィジカルセキュリティシステムによってフィジカル空間の情報をデジタルデータとして密に収集し，断片的かつ離散的にしか把握できなかった人やモノの動きや状態をサイバー空間上で見える化・分析する。これにより，人やモノのシームレスな監視だけでなく，事業者にとって有用な情報へ変換したり，フィジカル空間へフィードバックを掛けたりするなど，新たな価値の創出につなげることができると考える。

日立は，このようなデジタルトランスフォーメーションを実現する基盤として，フィジカルセキュリティ統合プラットフォームを開発した。

3. フィジカルセキュリティ統合プラットフォーム

3.1
プラットフォームの概要

今回開発したフィジカルセキュリティ統合プラットフォームは，防犯カメラや入退室管理などのフィジカルセキュリティシステムや位置情報計測・環境計測などのIoTセンサーによって，社会インフラの現場におけるフィジカル空間（監視対象や業務オペレーションなど）の情報を収集・蓄積・見える化し，AI（Artificial Intelligence）やアナリティクスソフトウェアを活用して人やモノの動態（動線・動作・状況）を分析することで，セキュリティ強化や業務改善・経営課題解決・新事業創生などの価値創出に貢献するソフトウェア基盤である（**図2**参照）。

3.2
プラットフォームの構成

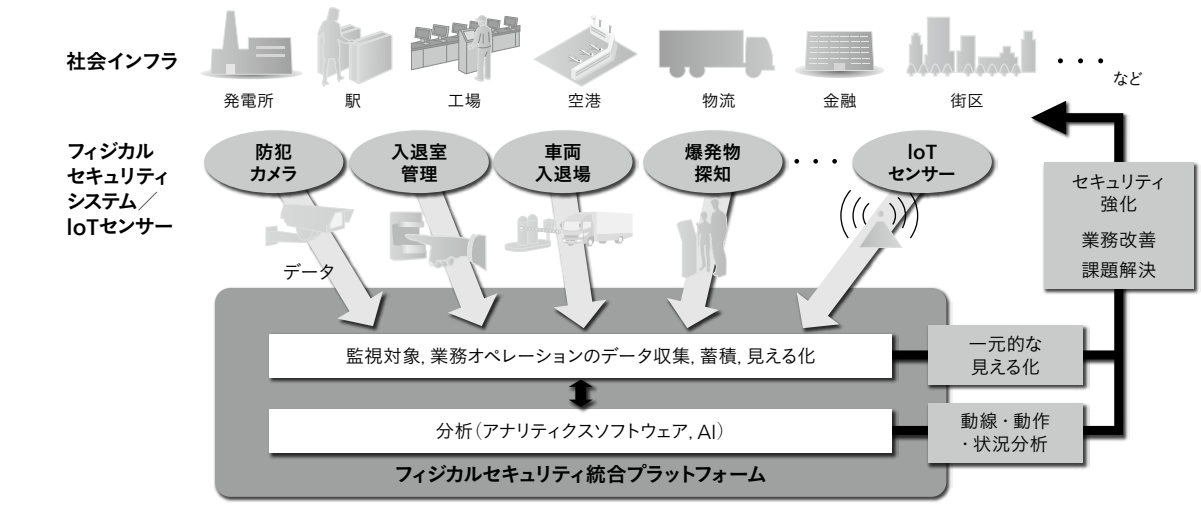
本プラットフォームのソフトウェア基盤は，大きく分けて3つのフィールドで構成される（**図3**参照）。

・フィジカルフィールド（現場側インタフェース）
・情報＆制御フィールド（管理側インタフェース）
・データフィールド（収集・蓄積・連携）

どのフィールドもオンプレミス（自社運用型）とすることが可能であるが，管理・運用面などの観点から情報＆制御フィールドとデータフィールドをクラウドに構成してフィジカルフィールドと連携させることもできる。

本プラットフォームには，各種のシステム・装置・機能と連携する標準プラグインモジュールを多数用意しており，必要なセキュリティ対策や顧客のニーズ・課題に合わせ，各フィールドにモジュールを選択実装すること

図2｜フィジカルセキュリティ統合プラットフォームの概要
フィジカル空間の情報を収集・蓄積・見える化し，人やモノの動態を分析することで，セキュリティ強化や業務改善・経営課題解決を行う。



注：略語説明
AI（Artificial Intelligence）

で各種ソリューションを提供する。

フィジカルフィールドにはフィジカルセキュリティシステム・IoTセンサー・映像解析機能などと連携するモジュールを実装し，情報＆制御フィールドにはレポート出力・設備制御といった人やモノの動態を見える化・分析・制御するモジュールを実装する。そして，データフィールドでは，データの収集・蓄積を行うとともに，フィジカルフィールドと情報＆制御フィールドを連携させることで管理側での動態管理や現場側へのフィードバックを可能とする。

3.3 プラットフォームの特長

本プラットフォームには，前述の構成やプラグイン方式により，以下の3つの大きな特長がある。

(1) 利便性

各種モジュールを実装するためのインタフェースを標準的に多数具備しており，迅速かつ安価にシステム・機能を提供することが可能である。

(2) 機能性

多数の映像解析機能（顔認証，作業逸脱検知，動線検知，不審者・不審物検知など）と連携することで，人や

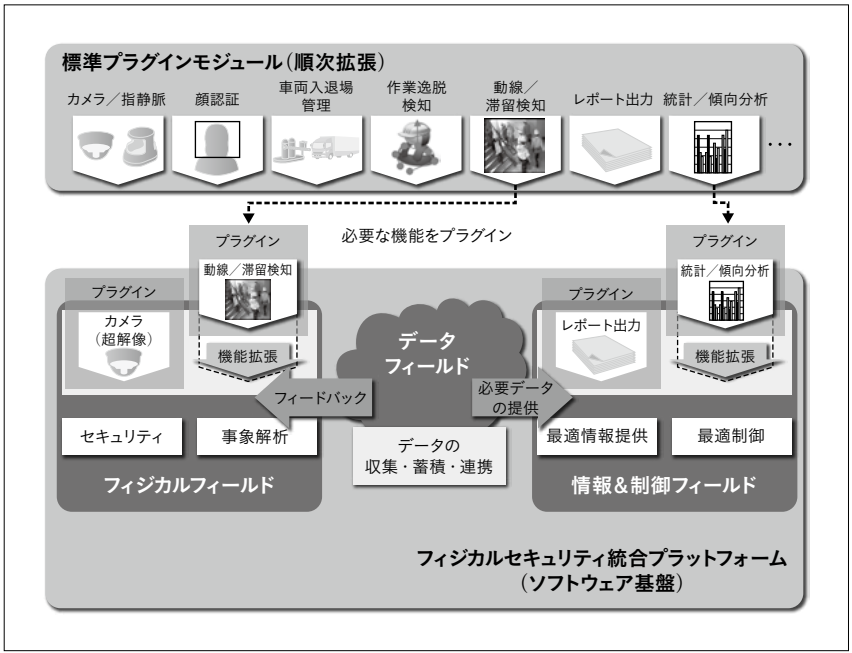


図3｜フィジカルセキュリティ統合プラットフォームの構成
フィジカルフィールドと情報＆制御フィールドに必要な機能をプラグイン（実装）し，データフィールドでデータの収集・蓄積・連携を行う。

モノの高度な動態分析が可能である。

また，多拠点を統合管理する場合，オンプレミス／クラウドの双方に機能分散し，ネットワークなどのリソースを有効活用することもできる。

(3) 拡張性

プラグイン方式により，顧客の優先順位や予算などに合わせてシステム・装置・機能を段階的に選択して導入することができる。

また，AI・BI（Business Intelligence）を活用した分析機能や他社システム／装置と連携するモジュールを拡充していくことで，最新機能への更新や既設システム／装置との連携も可能となる。

4. エリアセキュリティ

4.1 エリアセキュリティの定義

日立は，社会インフラのセキュリティ強化やビジネス進化を実現する各種セキュリティソリューションを「エリアセキュリティ」と称して展開していく。

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，社会インフラのさまざまなエリアを対象としている。以下に，フィジカルセキュリティ統合プラットフォームを活用したソリューション事例を紹介する（**図4**参照）。

4.2 セキュリティ強化への貢献

(1) 防犯強化

従来，防犯カメラや入退室管理などのフィジカルセキュリティシステムは個別に導入されることが多く，カメラ映像や入退室履歴などのデータは各システム内で独立して扱われ，監視情報が分断していた。

その結果，特に多拠点・大規模の現場では，網羅的に監視するためのオペレーションコスト増加や，網羅的に監視できないことによるインシデント（不審者・不審物など）の見逃しなどが発生していた。

しかし，本プラットフォームの活用により，各種フィジカルセキュリティシステムやIoTセンサーと連携することで，監視情報を一元的に集約・管理し，シームレスな監視によってオペレーションの効率化やインシデントの見逃し防止などにつなげることができる。また，映像解析機能との連携により，インシデントを目視検知ではなく自動検知することで，より堅牢（ろう）な監視と迅速対処にもつなげることができる。

(2) 防災強化

監視情報の一元的な管理は，エリア内にいる従業員・来訪者・業者などのシームレスな居場所の監視も可能となる。特に，入退室履歴・カメラ映像・位置計測などの情報から，危険区域への接近や災害発生時の避難状況を把握し，危険区域への侵入防止や避難者の誘導指示などに活用することができる。

4.3 ビジネス進化への貢献

(1) 業務改善

少子高齢化に伴う労働者の不足や働き方改革への取り組みなどを背景に，社会インフラにおける業務の効率化は非常に重要な課題となっている。

しかし，本プラットフォームを活用することで，各種フィジカルセキュリティシステムやIoTセンサーと連携した従業員や業者などのシームレスな監視が可能となるため，各種作業の動態を把握して非効率作業や異常行動

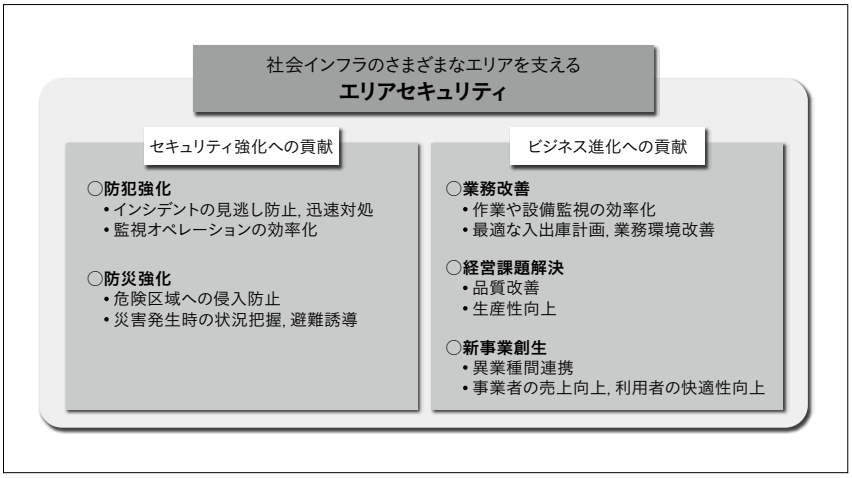


図4｜エリアセキュリティにおけるソリューション提供例

現場における人やモノの動態管理により，セキュリティ強化だけでなく，業務効率化や生産性向上などのビジネス進化にも貢献する。

を検知し，アラームや是正指示などのフィードバックによって業務を効率化することができる。

同様に，設備・在庫・業務環境などの動態を把握することで，人数と時間を掛けて行っていた設備異常監視の自動化，在庫状態の把握による最適な入出庫計画，劣悪な業務環境の検知による環境改善など，各種の業務効率化にも活用することができる。

(2) 経営課題解決

製造ラインや作業現場などにおいて，品質劣化による信用失墜の防止や若手への熟練技術継承は，事業継続にあたって非常に重要な課題となっている。

しかし，本プラットフォームの活用により，各種作業の動態を把握することで，異物混入や未熟動作を検知・是正したり，熟練者の作業を手本として見える化し，若手へ技術継承したりすることで，品質改善や生産性向上につなげることができる。

(3) 新事業創生

警備員・清掃員・設備監理員などの異業種が集うエリアにおいて，人やモノの動態やインシデント情報を業者間で共有することで，これまで把握・対処できなかった情報・業務を異業種間で補完し合い，互いの業務をサポートし，リソースを共有できると考える。

また，利用者が集う公共空間においては，動態情報をマーケティング活用して商業活性化を図ったり，混雑状況などの情報や利用者個々の状況を把握して最適サービスを提供したりするなど，事業者の売上向上や利用者の快適性向上にも貢献が期待できる。

5. プライバシー保護の取り組み

人の動態管理にあたっては，プライバシー保護に十分な注意を払う必要がある。特に，カメラ映像（画像）の利活用については，産官学が参画するIoT推進コンソーシアムにおいてガイドブックを策定し，事業者が配慮すべき事項を整理するといった動きもある。

日立は，カメラ映像に限定せず，データの利活用に取り組む事業者として，独自のチェックリストに基づくプライバシー影響評価を実施しており，その内容は最新の動向も踏まえて継続的に改善している。

日立は，このような取り組みを通じ，顧客のビジネス運用を支援する際にも適切なパーソナルデータの取り扱いに努めており，プライバシー侵害が問題化することを未然に防止している。

6. おわりに

本稿では，日立が推進するエリアセキュリティの取り組みについて紹介した。

顧客の状況や課題を十分に把握し，顧客と一体になって適切なソリューションの選択や導入計画・運用方法の検討を行うことが重要である。

今後も，価値創出に向けた最先端技術の研究開発など，日立はセキュリティを進化させ，社会インフラのセキュリティ強化とビジネス進化を支えていく。

参考文献など

1) 内閣府：第5期科学技術基本計画（平成28～平成32年度)，http://www8.cao.go.jp/cstp/kihonkeikaku/index5.html
2) 佐川達人，外：多様化する顧客ニーズに応えるフィジカルセキュリティ統合プラットフォームの構想，日立評論，98，6，432～436（2016.6）
3) 株式会社日立産業制御ソリューションズ，フィジカルセキュリティソリューション・課題解決ソリューション，http://www.hitachi-ics.co.jp/product/pss/index.html
4) IoT推進コンソーシアム：「カメラ画像利活用ガイドブックver1.0」の公表，http://www.iotac.jp/wg/data/

執筆者紹介

下条 智貴
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
セキュリティ戦略本部 セキュリティ企画部 所属
現在，セキュリティ事業の企画業務に従事

宮澤 泰弘
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
マネジメント本部 事業管理部 所属
現在，プライバシー保護対策の運用に従事

仲田 智
株式会社日立産業制御ソリューションズ
セキュリティ・画像ソリューション事業部 PSS本部 PSS設計部
所属
現在，フィジカルセキュリティおよび経営課題解決のビジネスに従事

小屋 博
株式会社日立産業制御ソリューションズ
セキュリティ・画像ソリューション事業部
セキュリティ事業企画本部 ソリューション企画部 所属
現在，フィジカルセキュリティ全般のビジネス企画に従事
技術士（情報工学），防犯設備士