Visionaries 2015

しなやかな強さへ

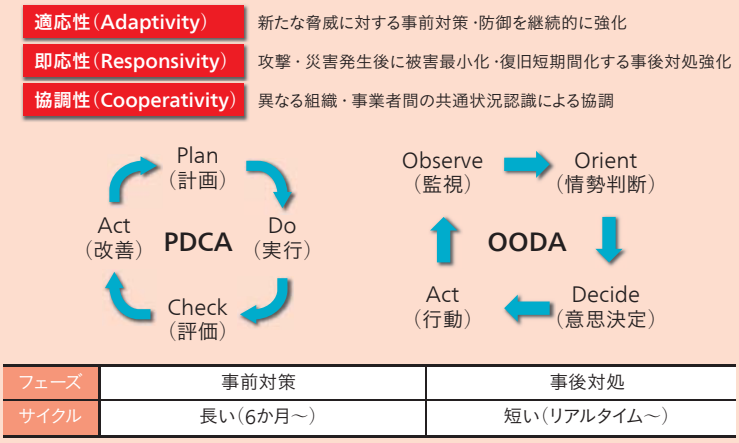
―社会インフラセキュリティ―

**社会インフラは，例えばエネルギーと交通のように互いに連携しながら高度化し，利便性を高めている。
それは同時に，社会インフラが多くの組織とシステムで成り立つ巨大な複合システムであることをも意味する。
現在，自然災害やサイバーテロなど，社会インフラを取り巻く脅威は急速に増大しており，有事の際の影響も拡大している。
日立は，多方面で培ってきた安全・安心を守る技術を結集し，社会インフラセキュリティに取り組んでいる。
適応性，即応性，協調性を柱としたコンセプトの下で，セキュリティの全体最適化をめざして動き始めている。**

「被害は発生する」を前提に

現代社会では，利便性と快適性の裏側にさまざまなリスクが存在する。電気，ガス，水道，鉄道，道路，公共施設，情報通信網といった，日々の生活やビジネスを支える社会インフラは，相互連携の拡大によってサービスを拡充してきた。反面，ひとたびトラブルが起こると，その影響は広範囲に波及する。トラブルの原因は故障やヒューマンエラーだけではない。異常気象や自然災害は，地球規模の気候変動によって今後も増え続けると予想される。グローバル化を背景に武力テロ攻撃への懸念も高まり，情報化の進展に伴うサイバーテロの増加は，すでに対岸の火事ではなくなっている。

24時間365日動き続ける社会を支えるインフラには，トラブルに際しても最低限必要なサービスを提供し続けることが求められる。しかし，このように多様化し，増大していく脅威のすべてを想定して対策をとってお



フェーズ	事前対策	事後対処
サイクル	長い（6か月～）	短い（リアルタイム～）

社会インフラのセキュリティ対策に求められる要件を適応性，即応性，協調性の3つに整理している。適応性はPDCAサイクルに，即応性は軍事的活動で用いられる意思決定理論のOODAプロセスにそれぞれ対応する。

くことは，もはや現実的とは言えない。想定外の災害や攻撃による被害が発生しうることを前提に，適切な事後対処によって被害の拡大や波及を抑え，迅速なサービスの復旧をめざすという柔軟な考え方が必要である。

こうした社会インフラ特有の事情を踏まえたセキュリティ対策に求められる要件を，日立は，適応性（Adaptivity），即応性（Responsivity），協調性（Cooperativity）という3つに整理している。その概念について，グループ内のセキュリティ技術全般を取りまとめる新井利明（日立製作所 ディフェンスシステム社 主管技師長・CTO）は次のように説明する。

「適応性は，新たな脅威の把握と対策方法の立案，対策の計画，導入，評価を継続的に実施し，その強化を図ることを意味します。つまり，事前対策力に関わる要素です。それに対して，事後対処力を高める要素が即応性です。今あるリソースの中で最良の対処を行うことに主眼を置いており，災害や攻撃などの発生後に，被害の最小化，復旧の短期間化を図ります。そして協調性は，相互連携の拡大に対応する要素です。異なる組織や事業者の間で情報を共有し，互いの状況を認識し合い，その後の対処に生かすことを意味します。」

システムとしての強じん性をベースに，この3つをコンセプトとして，日立はフィジカル（物理空間）とサイバー（情報空間）の両面から広範囲なセキュリティ対策に取り組んでいる。

利便性と安全性を両立させる

コンセプトの具現化に向け，フィジカルセキュリティでは，都市に流入する航空機，船舶，車両，人を対象に，各種システムの連携によって水際でのセキュリティチェックを実現する都市丸ごと安全・安心ソリューションや，各種センサー情報とシミュレーション技術を活用した災害対応支援ソリューションなどの提供を進めている。

フィジカルセキュリティは，従来，施設や


新井利明


影広達彦

エリアごとに個別のシステムが整備され，運用されてきた。しかし，社会インフラシステムが高度に連携・協調する都市においては，セキュリティシステムも相互に連携・協調することにより，人やモノの動きを可視化でき，さらに大きな効果を発揮する。

その一例として挙げられるのが，大規模公共施設・エリアのセキュリティ対策向けに開発されたトレーサブルフィジカルセキュリティシステムである。開発を取りまとめる影広達彦（日立製作所 中央研究所 情報システム研究センタ 知能システム研究部 主任研究員）は，このシステムの特徴を次のように説明する。

「めざしたのは，利便性と高い安全性の両立です。これまでは，セキュリティを高めようとすると認証や検査の手間や負担が増えてしまうのが課題でしたが，このシステムでは，入場時などのタッチパネル操作と同時に指静脈認証と顔画像の撮影を行うことで，利便性を損なわない認証を可能にしました。」

例えば，あらかじめ同意を得て登録してある個人情報と照合することにより，個人に向けた情報やサービスの提供にも活用できる。また，手荷物検査の際に手荷物の画像を撮影しておき，その画像を基に施設内各所に設置した監視カメラ映像から手荷物の移動経路を追跡するシステムと，質量分析技術を用いて対象エリア内にある爆発物の原料物質を検知し，爆発物の位置を短時間に特定できる装置を組み合わせることにより，個々の手荷物の安全性チェックも可能になる。

もし，爆発物の設置といった犯罪行為が起こった場合には，目撃情報などを基に，監視カメラの膨大な画像データから迅速に不審人物を見つけ出さなければならない。その際に力を発揮するのがマルチパースペクティブサーチである。

「私たちが以前から取り組んできた類似画像検索技術を生かし，顔だけでなく，上半身・下半身・手荷物の色，移動ルートといった断片的な検索条件でも，蓄積した画像データの中から類似度の高いものを瞬時に検索できます。」（影広）

このシステムは，監視カメラ映像からの人物追跡の効率を飛躍的に向上させるものと期待されている。

早期発見・早期対策で耐攻撃性を

一方のサイバーセキュリティは，情報系と制御系に大別される。



タッチパネル型指静脈認証装置の試作機。タッチパネルを操作している間に指静脈の認証と顔画像の撮影を同時に行うことで，アンコンシャス認証（事前同意を得たユーザー向けの無意識の認証）を実現し，利便性を向上させる。

類似画像検索技術を応用したマルチパースペクティブサーチ。開発メンバーの一人である渡邉裕樹（日立製作所 中央研究所 情報システム研究センタ 知能システム研究部 研究員）は，不審人物の追跡などにおける有用性を強調する。

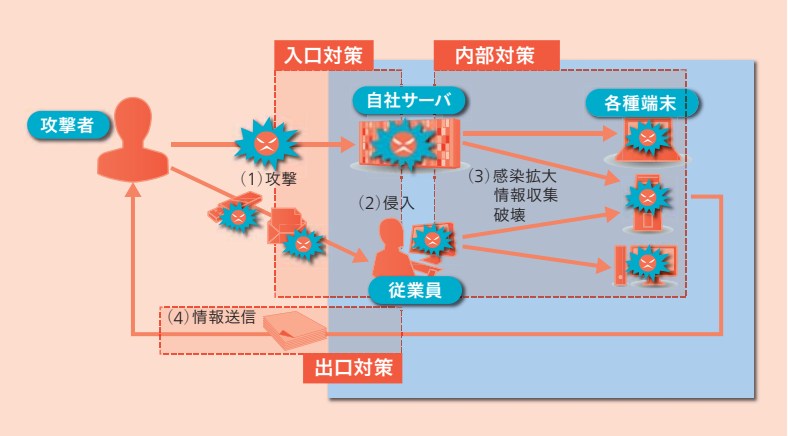
情報セキュリティの先端技術に精通する瀬野尾修二（日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティ先端技術本部 本部長）は，年々高度化，組織化が進むサイバー攻撃への対処について，次のように話す。

「個人をターゲットとする『標的型攻撃』などの新種のマルウェアが次々と発生している現状では，システムへのすべての侵入を防ぐのは実質的に不可能です。したがって，そのことを前提に，OODAの概念に基づいて，いかに早期発見・早期対策を行うかが，今の情報セキュリティの基本であると考えます。例えば，これまでの入り口対策に加えて，不正な情報送信の出口を絶つことで実質的な被害発生を防ぎつつ，内部の検知と対策を迅速に行うことが肝要です。」

こうした考え方に基づき，日立の情報セキュリティソリューションは，不正アクセスやマルウェアを検知・防御する監視サービスや，PC（Personal Computer）の不正接続を自動的に監視・排除する技術などを組み合わせ，多層的なモニタリングと防御を提供している。検知されたマルウェアは，多種類の環境で自動実行させてその構造を解析する独自の自動解析技術で特性を解明され，事後対処に役立てられる。

発電所や基幹産業などの社会インフラを支える制御システムでも，近年，情報システムとの連携が進み，サイバー攻撃のリスクが高まっている。中野利彦（日立製作所 インフラシステム社 制御プラットフォーム開発本部 制御プラットフォーム設計部 制御セキュリティセンタ センタ長）は，自身が統括する制御セキュリティの特徴について次のように話す。

「日立は，産学官連携によって設立した技術研究組合制御システムセキュリティセンター（CSSC）に当初から参画し，制御セキュリティの強化に取り組んでいます。制御分野においてもセキュリティ脅威が出現する可能性が高まっており，システム全体の耐攻撃性をいかに強化するかが重視されています。」



最近の情報セキュリティでは，マルウェアの侵入をすべて防ぐのは不可能ということを前提とせざるを得ない。こうした状況では，従来の入口対策に加えて，組織の内部や出口での対策が求められる。

基幹産業インフラの制御システムへのサイバー攻撃に備えるための各種装置。耐攻撃ソリューションの一環として提供している。

日立は，制御用コントローラでいち早くEDSA認証[※1)]を取得した製品を開発し，ネットワーク経由でのサイバー攻撃に対するリスクを軽減した。特に重要度の高いシステムには，外部ネットワークからのアクセスを遮断する一方向中継装置を提供することにより，高いセキュリティを実現する。また，ネットワークに不正な装置を接続することによって発生するセキュリティ脅威を防ぐため，不正PC監視＆強制排除装置を提供している。さらに，システムの中に「デコイ」と呼ばれるおとりサーバを置き，侵入したマルウェアを早期に把握するとともに，捕獲して解析するソリューションを提供している。不正アクセス検知装置とセットで運用することにより，既知と未知の両方の脅威に素早く対応できる。


瀬野尾修二

社会インフラセキュリティの向上へ，技術を育て，人を育てる


新誠一 氏

宮城県多賀城市に本部を置く技術研究組合制御システムセキュリティセンター（CSSC）は，社会インフラを支える制御システムのセキュリティ強化をめざし，セキュリティ認証，研究開発，教育，普及・啓発活動を行う産学官連携の組織として2012年3月に発足した。その理事長を務める新誠一氏（電気通信大学 情報理工学研究科 知能機械工学専攻 教授）は，制御工学を専門とし，マイコン制御の第一人者として知られる。

「これまで私たちは，さまざまなモノをつなげることで，社会を便利にしようと努力してきました。その結果として，時間どおりに動く鉄道，安全な飲み水，停電しない電力システムなど，世界に類を見ない高度な社会インフラを作り上げてきました。それらがきちんと動いていて当たり前という世界を維持するために，日立をはじめとする企業のさまざまな技術が貢献しているのは言うまでもないことですが，近年では特に，セキュリティが重要な要素となっています。

サイバーテロ行為は，かつては愉快犯だったものが営利目的の組織的犯罪になっており，社会インフラの制御システムをターゲットとするものも増加しています。それらに対抗していくためには，セキュリティ技術はもちろん，それを適正に活用する指針やマネジメント力が欠かせません。

そこで重要になるのが国際標準規格と，その認証制度です。セキュリティ認証はCSSCの設立目的の一つであり，EDSAの日本国内での認証機関となっています。国際規格の技術動向を捉え，国内企業に採用を促すことで，日本の優れた社会インフラシステムの輸出を後押ししたいと考えています。

さらに，意識と行動の両面から社会インフラのセキュリティ向上を図るため，CSSCでは，火力発電所，電力広域制御，下水処理場，ビル制御システム，部品組立工場，ガスプラント，石油化学プラントのオペレーターを対象にサイバー攻撃の演習を行っています。欧米やアジアのサイバーセキュリティ普及啓発機関などと連携して，グローバルな情報共有や研究開発も推進しています。

また，もう一つ重要な点が人材です。CSSCでも，電気通信大学でも，今後ますます求められる，情報セキュリティと制御システムの両方を理解できる人材の育成に力を入れています。社会インフラの安全・安心は，技術力だけでなく，倫理観にも支えられています。その両面に優れた優秀な人材を呼び込むためにも，この分野に関わる人々がきちんと評価されることを願っています。それが結果的に，社会全体の安全・安心を高めることにつながるのですから。

サイバーセキュリティは，世界ではすでに軍事技術の一つと見なされて，日本のように民間主導で重要インフラを守る体制を整えている国は，ほかにありません。日立には，ぜひ，その中心となって社会インフラセキュリティの向上に貢献していってほしいと思います。」（新氏）


中野利彦

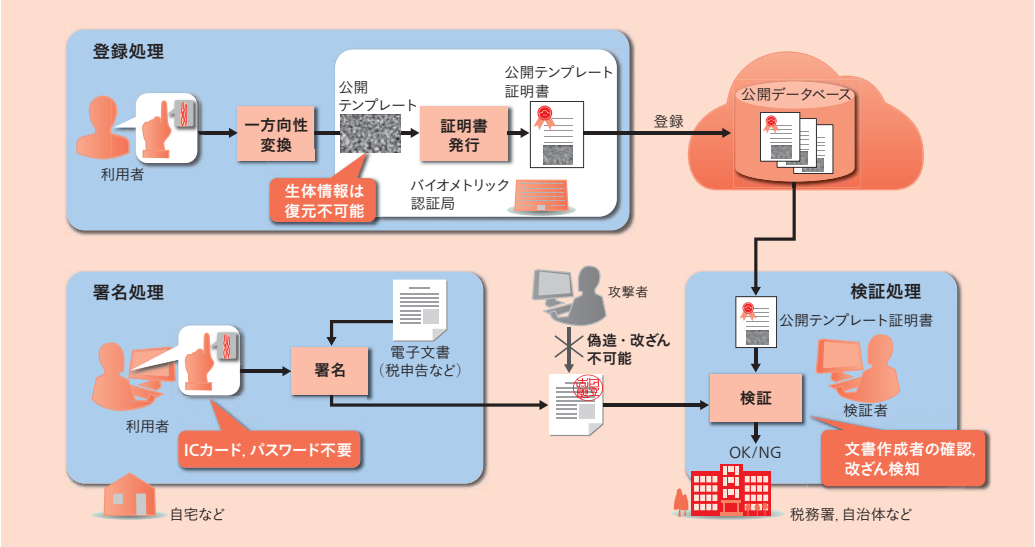
情報と制御は社会インフラシステムの基盤である。日立は，ここに挙げたような個別の技術をベースに，リスク分析，コンサルティングから，システム構築，運用支援までカバーする総合的なセキュリティサービスを提供している。

※1）EDSAはEmbedded Device Security Assuranceの略。国際計測制御学会のメンバーを中心とした国際認証推進組織が提供している，制御機器の組込み装置向けのセキュリティ認証プログラム。

セキュリティの全体最適へ

社会インフラセキュリティでは，指静脈などの生体情報をはじめ，さまざまな個人情報，ビジネス上の重要なデータなどが扱われる。金融・公共向けセキュリティ技術の研究に携わる三村昌弘（日立製作所 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 部長）は，そうした情報を守る先端技術の一端を次のように挙げた。

「PBI（Public Biometric Infrastructure）と呼んでいるテンプレート公開型生体認証基盤は，生体情報（テンプレート）を復元できない形に変換して登録しておくことで，安全に公開し，暗号鍵と組み合わせて認証や署名に



テンプレート公開型生体認証基盤は，厳密なユーザー認証を必要とするシステムのクラウド化や，それらの関係する複数のシステム間でのID連携を低コストで実現することにつながる。

活用できる技術です。また，情報を暗号化したままで高速にデータの検索や照合・分析ができる秘匿情報処理技術もあります。」

PBIは，指静脈などの自分の生体情報を認証に利用できる利便性と，情報漏えいリスクの軽減を両立する。秘匿情報処理技術は，高い安全性を保ちながら，大容量データの処理を可能にする。これら最先端のセキュリティ技術は，クラウド上で社会インフラの重要な情報を扱う際のリスクを低減する。すなわち，日立の考える社会インフラセキュリティは，社会の利便性を損なうものではなく，利用者が特別に意識しなくても安全が守られている社会の基盤である。

前出のとおり，単にセキュリティを高めようとすると手続きや機器の操作が煩雑になるだけでなく，常時警戒を求められることにもつながりかねない。情報デザインを専門とする佐藤敦俊（日立製作所 デザイン本部 情報デザイン部 主任デザイナー）は，三村の話を補足するように，今後のセキュリティ施策に必要とされる視点をこう指摘する。

「セキュリティのために常に緊張を強いられる社会は，居心地が悪いはずです。デザインの力を応用すれば，求められるセキュリティレベルを満たしつつ，個人の快適性も損なわない最適なセキュリティ施策を見出すことができると考えています。」

例えば，ユーザーインタフェースの工夫によって機器の使い勝手を高め，人為的ミスを防ぐ。注意・警戒レベルを効果的に可視化し，危険と安心の切り替えを支援する。そうした試みに，エスノグラフィ※2)やExアプローチ※3)の手法を役立てようとしているのである。

社会を支えるインフラは，個別のシステムはもちろん，全体がセキュアに保たれなければならない。そのために日立は，こうしたデザインの観点も取り入れながら，多方面で培ってきた安全・安心を守る技術，それらを一体として運用するサービスの提供を進めているほか，セキュリティレベルの底上げや発展に向けた標準化活動も推進している。その根底にあるのは，セキュリティの全体最適化という視点である。

さまざまな脅威から気づかないうちに守られ，想定外の危機にもしなやかに強く対抗できる。そうした社会の実現を，日立の社会インフラセキュリティが支えていく。

※2)人間中心設計の最上流において，ユーザーの業務現場の実態を観察して潜在ニーズを発見する手法。人々の実際の行動を詳細に観察し，得られたデータに対して事実に基づく分析を行うことによって，人々が実際に行っていることの全体像，暗黙のうちに前提としている価値観，満たされないニーズや願望などを明らかにするもの。

※3)システム開発の超上流工程（構想・計画段階）において，利用者のエクスペリエンスを重視しながら合意形成を進めるための方法論。エクスペリエンスデザイン手法をベースとして日立が体系化した。


三村昌弘


佐藤敦俊