人間とシステムの協調で社会インフラにレジリエンスを

高橋 信　東北大学大学院工学研究科 技術社会システム専攻 教授
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
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
中野 利彦　日立製作所 インフラシステム社 情報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
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

近年，サイバー攻撃をはじめ，情報セキュリティに対する脅威が拡大している。
また，自然災害やテロなどへの懸念が高まる中，それらへの十全な対策が社会的な課題となっている。
社会インフラシステムの安全を維持するには，増大する脅威に備えるとともに，適切な対処で被害を最小化することが求められる。
日立グループは，社会インフラ分野やフィジカルセキュリティ分野などにおいて，あらゆるセキュリティ関連技術を培ってきた。
それらを生かした統合セキュリティソリューションで，より安全で安心な社会の実現に貢献していく。

多層防御で「想定外」にも備える

新井　社会の安全・安心に対する脅威が増大する中で，社会インフラのセキュリティへの関心も高まっています。高橋先生は，日立も組合員として参加している技術研究組合制御システムセキュリティセンターの東北多賀城本部長を務めておられますが，社会インフラのセキュリティでは，どのような点に注目されていらっしゃいますか。

高橋　私の主な研究分野は，例えば原子力発電所や航空管制システムなど，ひとたびトラブルが起きると社会的影響が大きい大規模システムの安全です。その中でも特に，ヒューマンファクターを含むシステム全体の安全性の向上に注目しています。東日本大震災では「想定外」がキーワードになりました。さまざまな状況を考慮して対策しても，やはり想定外の事象というのは起こりうるものです。その対処は，いくらシステムを作り込んでいても，最終的には人間の適応能力，フレキシビリティに頼らざるをえない部分があり，そういう人間的な要素を，どのようにシステム全体の安全性向上につなげるかを研究しています。

瀬野尾　サイバーセキュリティの場合は，新種のウイルスやマルウェアなどが次々と生み出されていて，最初からすべてのリスクを想定できるわけではありません。そのため想定外を前提として，それをどう減らすか，もし被害が起きた場合はいかに最小限にとどめるかという，いわゆる「減災」の観点が重要となっています。

三村　サイバーセキュリティで最近問題となっているのは，標的型攻撃です。特定の端末を狙って，あまり知られていないような脆（ぜい）弱性を突いて攻撃するというものです。従来は広範囲にウイルスをばらまく方法が主流でしたから，すぐに脆弱性が判明して対処できました。ところが，標的型攻撃では狙いが限られているために気づきにくく，知らないうちに被害が拡大しやすいのです。そうした新しい脅威に対応するためには，脆弱性をなくすことと並行して，やはり被害をできるだけ減らすというリスクヘッジが重要ですね。

高橋　そういう意味では，「多層防御（Defense in Depth）」という視点も重要だと思います。これは軍事の世界では基本的な考え方ですが，防護壁を二重三重にするといったことではなく，1つの防御ポイントが破られても，ほかの防御ポイントが機能するように備えておくというものです。そうした現実的な考え方を基本として取り入れていくことが，最終的な被害を減らすことにつながると思います。

高橋 信
東北大学大学院工学研究科
技術社会システム専攻 教授
1986年東北大学工学部原子核工学科卒業，1991年同大学大学院工学研究科（原子核工学専攻）博士課程修了。2000年東北大学大学院工学研究科助教授などを経て，2011年より現職。工学博士。現在，技術研究組合制御システムセキュリティセンター東北多賀城本部長を兼務。日本原子力学会理事，ヒューマンインタフェース学会理事。専門は，認知工学，システム工学，ヒューマンエラー解析。

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
1984年日立製作所入社，官公庁や自治体などのシステム構築を手がける公共部門のシステムエンジニアを経て，2002年よりセキュリティに関する現行業務に従事。

日頃の訓練の充実と，緊急時の情報活用を

新井　ヒューマンファクターによるリスクを低下させるには，指揮命令系統の訓練も重要ですね。特に大規模災害のような緊急事態には，OODA［Observe（監視），Orient（情勢判断），Decide（意思決定），Act（行動）］ループをしっかり回すことなど，平時とは異なるオペレーションが必要になりますから，意識の切り替えも鍵を握ります。

高橋　大規模システムでは，シミュレータを活用して現実に近いレベルの訓練を行っています。何千万分の1というような確率の多重故障なども想定して行っていますが，実際にそれが役立つかは，訓練の内容にもよります。シナリオベースでは想定外のことに対しては無力ですから，やはり図上訓練という形で，ある部分から先はシナリオをブラインドにして行う訓練が実効的です。また，いくら訓練を積んでも，実際の災害時には情報の有無が生死を分ける要因ともなりますから，災害時の情報活用に備えておくことも重要ですね。

瀬野尾　米国では，政府がNIEM（National Information Exchange Model）という情報共有の標準モデル化を推進することで，災害やテロなどの緊急事態が発生した際に，政府と省庁や自治体などの間で情報を共有する環境がすでに作られていますし，関係する個々のシステム間での情報連携を円滑に進める仕組みも構築されています。日本でも，行政機関が収集・保有する公共データの公開と利用を促進するオープンデータに取り組んでいますが，まだいろいろと課題があります。改ざん防止などの技術を活用しながら，公共データを二次利用しやすい形で公開することが，災害時や非常時の適切なオペレーションに不可欠だと思います。

制御システムのセキュリティリスク

新井　ヒューマンファクターに関してもう一つ言うと，ISMS（Information Security Management System）をはじめとして，企業の情報システムにおける情報漏えいや改ざんなどへの対応は進んできましたが，制御システム分野ではセキュリティに対する意識改革が必要ですね。

中野　以前は，制御システムはクローズドであるためサイバー攻撃の心配はないと言われていましたが，汎用プラットフォームの活用やネットワーク化，外部メディアの利用が進んでおり，リスクが高まっています。制御システム分野での基本的なセキュリティの知識と危機意識の向上に，私たちも貢献していかなければならないと感じています。

瀬野尾　セキュリティの分野では，専門知識を持ったスペシャリストが必要なだけでなく，実務に携わる一般の人が最低限の知識を持っていないと，標的型攻撃メールを何の疑いもなく開けてしまうなど，防御が機能しないという問題があります。企業の場合には，SE（Systems Engineer）や技術者でない従業員とも普遍的なセキュリティ知識の共有化を図ることが課題になると思います。

三村　セキュリティには人手とコストがかかるという認識も根強いのではないのでしょうか。私たちもセキュリティの重要性を訴えるだけでなく，サイバー攻撃に対して，できるだけ人手をかけない対策方法，IT（Information Technology）による管理者への支援や自動化などに取り組んでいかなければならないと思います。

高橋　実際にサイバー攻撃が起きたときには，それが単なるシステムトラブルによる動作異常なのか，サイバー攻撃によるものなのかを早期に判別することが重要なポイントになるでしょう。システムで考えると，シグネチャを設定して自動的に検出するという方法もあると思いますが，COP（Common Operational Picture：共通状況図）などのように，管理している人間に対して適切な情報を提供し，状況認識や意思決定の支援をするという対処法が，1つの方向性として重要ではないかと思っています。

瀬野尾　特に制御システムの世界はセキュリティでは新しいフィールドですから，どんな未知の脅威が出現するか分かりません。そのため，できるだけ迅速に警告を発して管理者を支援する技術に力を入れています。例えば，システムの中に「デコイ」と呼ぶおとりのサーバを置き，そこでウイルスの進入と感染をいち早くキャッチし，管理者に対して適切なアラートを発することで感染拡大を防ぐソリュー

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

1997年日立製作所入社，生体認証をはじめとしたセキュリティ技術・システムの研究開発，金融システムの研究開発を経て，2012年より金融・公共向けソリューションとそれを支えるソフトウェア生産性技術，システムセキュリティ技術の研究開発に従事。
博士（工学）。情報処理学会会員。

中野 利彦
日立製作所 インフラシステム社
情報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

1980年日立製作所入社，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。

ションを開発しました。特に可用性が求められる社会インフラ分野での適用にあたっては，長期間連続的な稼働に耐えうる実装を行っています。

中野　制御システムでは，セキュリティの国際基準IEC 62443への準拠が広がり始めています。培ってきた信頼性の高い技術をスタンダード化していくことを視野に，そうした標準化の動きに貢献して，個々のコンポーネントから，システム全体，オペレーション，そして社会まで含めた全体がセキュアに保たれる世界をめざしていかなければならないと思います。

ヒューマンファクターで「レジリエンス」を高める

高橋　最近私は，レジリエンスエンジニアリングに注目しています。レジリエンス(resilience)は「弾力性」や「復元力」といった意味のことばですが，セキュリティの分野でもそうした概念が重要になっていると感じます。従来の安全対策は，事故が起きたらその原因を取り除くことで再発防止をめざすというものです。それは決して否定しませんが，まれにしか起きない失敗事例にこだわるよりも，時々刻々と変化する状況の中で，物事がうまくいっている要因を分析して実行するほうがよいケースもあります。なぜうまくいっているのかに注目し，人間による的確な予測や，対応力，フレキシビリティといったヒューマンファクターによってレジリエンスを高め，事故の予防プロセスを創造していくという考え方も，セキュリティ技術の進展には必要なのではないでしょうか。

中野　一生に一度というような大災害やトラブルが起きれば，たとえ訓練を積んだ人でもパニックになる可能性があります。そうしたときのために，過去の成功・失敗事例を分析して，人間の判断を支援するために最適な情報を，タイムリーに提供できるようなシステムが必要なのかもしれないですね。

高橋　人間とシステムとの協調が，今後ますます大事になるでしょう。機械やシステムが，そのときの人間の精神状態を生体情報などから読み取って，普段は人間を優先し，人間の状態が限界に近づいて信頼性が低下する可能性のある状況では機械が支援する。そうしたシステムが可能になれば理想的です。私たちはそれを適応インタフェースと呼び，その基礎的な技術について研究を始めています。

新井　2020年の東京五輪に向け，国内でますます重要となるフィジカルセキュリティでも，人間と機械との協調が鍵になるでしょう。監視カメラと画像認識との組み合わせなど，日立グループの得意とするIT活用によるフィジカルセキュリティの高度化に貢献したいと考えています。

瀬野尾　指静脈認証などの生体認証も活用できると思います。また，最近では「人流」と呼ばれる人の動きや，携帯電話の位置情報などを解析し，サービス向上やセキュリティに活用していく動きもあります。プライバシーの確保と情報活用についての国としての指針が明確に打ち出されれば，私たちも活用のための技術開発が進めやすくなります。

三村　日立では，社会インフラセキュリティにおいては「適応性」,「即応性」,「協調性」という3つのキーワードが必要であると考えています。適応性とは，個々の部品から，それをまとめているミドルウェア，その上のアプリケーションなど，システムのすべてのレイヤーでセキュリティ対策をしておくという考え方です。しかし，それでもウイルスに侵入されて被害が起きる可能性はありますから，どんな場合にも迅速に対処できるようにするという考え方が即応性です。そして協調性とは，例えばウイルスや脆弱性の情報をつかんだとき，それをできるだけ素早く，IPA（独立行政法人情報処理推進機構）やJPCERT（Japan Computer Emergency Response Team）をはじめとするコミュニティの中で共有するという動きです。実際にそうした活動はあるのですが，もう一歩進めて，ITシステムや物理セキュリティはもとより，社会インフラの根幹となる制御システムまで含めた社会全体のセキュリティの向上に必要となる情報を，お互いにもっと出し合って共有する仕組みを構築すべきではないかと考えています。これらのキーワードは，他の分野のセキュリティにおいても重要なのではないでしょうか。

新井　日立グループはIT，制御システム，そしてフィジカルまで，幅広い分野のセキュリティを支える技術を基に，統合セキュリティソリューションを提供しています。今回の議論も生かしながら，社会の安全・安心を高めることに貢献していきたいと思います。本日はどうもありがとうございました。

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
1978年日立製作所入社，システム開発研究所（当時）での情報システムの研究開発などを経て現職。
工学博士。