寄稿

三菱総合研究所

MONTHLY REVIEW

NOVEMBER.2017

Content

【特 集】

1 横行するサイバー攻撃からインフラを守るために

Point

- インフラに対するサイバー攻撃の接点が増えて被害の範囲は拡大。
- モノとICTが融合したシステム全体のセキュリティ確保が急務。
- 企業の課題は、サイバーと事業を統括するリスク評価・設計と人材の確保。

1 社会インフラに対するサイバーセキュリティの重要性

社会インフラや生産設備を狙ったサイバー攻撃の脅威

2017年5月、WannaCryというマルウェア（不正なプログラム）によるシステム利用停止が世界各地で同時多発的に発生した。トップニュースとして報道されたとおり、多くの国で通信、医療、鉄道事業者に感染が広がり、オフィスのパソコンのほか、屋内外の電光掲示板が使えなくなった。日系企業でも感染が確認され、自動車などグローバルに事業展開する製造業では生産ラインの停止などの損害を被る例が発生した。

WannaCryは感染したシステムを利用停止にして身代金を要求するランサムウェアというマルウェアであるが、自己増殖しネットワークを通じて拡散するワーム型と呼ばれる機能も有していた。それが爆発的な感染となった要因である。WannaCry以外にも、2010年6月にはイランの核燃料施設を標的にしたといわれるStuxnetや、2015年12月の停電にサイバー攻撃が起因していたとウクライナ政府が発表したケースなど、インフラ設備へのサイバー攻撃の事例は多く発生している（表1）。

社会インフラはICT（情報通信技術）に深く依存し、ネットワークでつながる利便性の反面には重大なセキュリティの脅威が潜む。これまで日本は他国に比べて被害が小さかった印象がある。サイバー攻撃は軍事的理由によるものが多く、日本がその攻撃対象の中心ではなかったことに加えて、ネットワークが狭い範囲で閉じていることが、結果的に功を奏したと考えられる。しかし、過去には、日本の幹線交通網で原因不明のシステムダウンが発生し、サイバー攻撃が要因として疑われた例もある。大規模な被害にこそなっていないが、いつ国内の重要インフラがサイバー攻撃を受けて、都市や国家の機能が麻痺してもおかしくないとみるべきである。

[表1]インフラ設備へのサイバー攻撃

事例		被害	原因
2010年	Stuxnet（スタックスネット）	イランの核燃料施設の遠心分離機の制御装置が不正操作で稼働不能になり、核開発計画が約3年遅延。	USBメモリを通じて不正プログラムがシステムに侵入。ウラン濃縮用遠心分離器の回転速度を不正操作し、稼動不能状況にした。
2014年	Havex（ハーベックス）	欧州電力会社の制御システムを管理するサーバーの情報が不正取得された。	制御ソフトウェア更新用サイトを改ざんし、保守用PCに不正プログラムをインストールさせた。制御システム管理サーバーの情報を取得し、外部に送信。
2014年	ドイツ製鉄所の操業停止	溶鉱炉を制御する装置が不正操作され、溶鉱炉を正常に停止できず生産設備が損傷。	メールで不正プログラムを送り開封させ製鉄所のネットワークに侵入。生産設備の制御システムに感染して不正操作。
2015年	ウクライナの大規模停電	ウクライナの電力供給会社のシステムが不正プログラムに感染し、停電が発生。140万人に影響が及んだ。	メールで不正プログラムを送り開封させネットワークに侵入。電力システムの監視・制御システムに侵入したと考えられている。
2017年	WannaCry（ワナクライ）	鉄道運行情報表示、駐車場、ATM、自動車工場などのシステムが使用不能になった。	Microsoft製品の既知の脆弱性を衝いた不正プログラム。ファイルを暗号化し、復元する代わりに金銭を要求。自己増殖機能があり、感染が拡大。

出所：三菱総合研究所

IoT機器や自動運転の普及によりリスクは高まる方向へ

今後はさらに、あらゆるモノにセンサーや通信機能を備えるIoT（モノのインターネット）が普及し、ネットワークに接続される機器数が爆発的に増加する。シスコシステムズ社の調査では、2013年時点で100億個であった接続数が、2020年までに500億個になると予測されている。IoT機器は小型・省力型であるためセキュリティ対策機能を搭載しにくい。その上、機器が無数に上るため人手で管理することが困難である。加えて利用期間は数年間に及び、機器交換のタイミングでは対策が後手に回る。こうしたことから、パソコンやサーバーなど従来型のICT機器と同様の方法を適用することは難しく、対策は容易ではない。

2015年に開催されたセキュリティカンファレンスBlack Hat USA 2015では、ある自動車のシステムに対するハッキング（不正侵入）手法が公開され、それを受けて140万台がリコールの対象となった。医療機器でも、近年ネットワークに接続する機器の脆弱性情報が増えている。いずれも、製品が市場に出てからソフトウェアの脆弱性が発見されている事象である。2016年10月には、Mirai というマルウェアに感染した無数のIoT機器が、一斉に膨大なデータ通信を発生させ、多くのネットワークやウェブサイトに障害を発生させている。

社会インフラにおけるICTへの依存度は今後も高まり、IoT機器や制御システムの利用機会や利用範囲がさらに拡大する。結果、社会インフラが攻撃を受ける接点は格段に増加し、インフラを介した社会被害の広がる範囲とスピードは一気に増大する。サイバー攻撃の脅威とリスクは高まり、社会インフラに対するサイバーセキュリティの確保は重大かつ差し迫った社会的な要請となっている。

2 モノとICTが融合したシステムのセキュリティ対策

わが国では、2015年9月に閣議決定されたサイバーセキュリティ戦略のもとで、重要インフラのセキュリティに加え、安全なIoTシステムを確保することを目標として、IoTシステムのセキュリティに係る制度整備・技術研究開発・人材育成などが進められている。例えば、総務省および経済産業省などでは、IoT推進コンソーシアムを通じて、IoTセキュリティガイドラインを策定し普及に努めている。重要インフラを支える制御システムについては、2012年に技術研究組合制御システムセキュリティセンター（CSSC）が設立され、三菱総合研究所も参加して、電力をはじめとする社会インフラや産業機器のセキュリティに関する研究開発が実施されている。電力分野では制御システムのセキュリティを確保する要件が技術基準省令に含まれるようになった。

折しも2020年、モノとICTが融合したシステムのセキュリティが問われるオリンピック・パラリンピックがある。前述の閣議決定でも大会の開催と運営を支えるインフラのサイバーセキュリティを確保することの重要性が謳われている。これに基づき、内閣サイバーセキュリティセンターを中心に、組織委員会、開催都市である東京都、電力事業者、鉄道事業者などを交えながら、体制構築や演習・訓練の取り組みが進められている。オリンピックで得られた知見をレガシーとして、全国に展開していくことが望まれる。

3 企業におけるセキュリティ対策の考え方

政府や業界によるモノとICTが融合したシステムに対するサイバーセキュリティ対策が推進される一方、重要インフラの管理主体や製造業にも対応が求められる。多様な主体と連携し継続して事業活動を推進しなければならないため、インフラなどの制御システムに対するきめ細かい分析と対策が必要だ（表2）。

専門家の連携によるリスク評価（脅威分析）

インフラなどの制御システムへの攻撃の経路は多岐にわたる。注意を要するのは、プラントや製造設備が直接インターネットに接続していなければ安全とは限らないことだ。USBなどの記憶媒体を介して制御システムのネットワークに侵入する手法も多発している。

リスクを正しく認識するためには、攻撃の糸口やアクセス経路、考えられる攻撃手法だけでなく、インフラ

[表2]インフラを支える制御システムのセキュリティ対策

	課　題	対　策
リスク評価	■サイバー攻撃は多様であり、時間とともに高度化。 ■現状のシステム内容、運用方法に加え、攻撃の糸口・アクセス経路、最新の攻撃手法などを十分理解していないとリスク対策は困難。	■適正なリスク評価、最適な対策検討のためには、インフラや設備の設計・管理・運用に携わる専門家と、セキュリティの専門家の連携が必要。
設計思想見直し・リスク低減	■制御システムのセキュリティ対策を開発ライフサイクルの中でどのように考慮するか、方法論は確立していない。	■開発ライフサイクルの早期よりセキュリティに配慮した設計に取り組むとともに、技術的対策以外の代替策やリスク低減策の検討も必要。
セキュリティマネジメント	■制御システムのセキュリティがリスクと認識されても、その責任・所掌があいまいな場合が多い。 ■制御システムとセキュリティの双方を理解するリーダー人材は稀で、育成も容易ではない。	■計画的な技術者の採用や人材育成プログラムへの参加など、外部の知見を自社の開発手順、運用ルールに取り入れる活動の継続が必要。

出所：三菱総合研究所

や設備の個別システム、ネットワーク構成、運用方法など、被害を受けるシステムの全体像を把握した上で、セキュリティリスクを評価する必要がある。これを脅威分析と呼ぶ。

ポイントは、セキュリティとインフラの両分野の専門家の連携である。セキュリティの専門家は、システムの機能障害がどの程度甚大な事象（人命に関わるなど）を引き起こすかまでは想定できない。一方、インフラの専門家は、セキュリティがどこから何によって破られるかについて十分な知識がない。脅威分析では、セキュリティとインフラの専門家がタッグを組み、さまざまなサイバー攻撃による被害可能性と影響範囲・規模を想定し、対策の投資規模、優先順位などを検討することが重要となる。

システム設計思想の見直しとIT以外のリスク低減

制御系など影響範囲の広いシステムでは、開発の早い段階からセキュリティに配慮した設計（Secure by Design）思想をもって取り込むことが必要である。

一般的なITのセキュリティ対策は、城郭が内堀や外堀を張り巡らせて天守閣を守るように、ネットワークを分割・隔離して最も重要な情報を守るという考え方がある。ところが、従来からの制御システムはセキュリティの脅威がさほど強く認識されず、利便性とコストを重視した障壁の少ないフラットな構造が志向されがちであった。システムの詳細設計や仕様検討が進んだ後からセキュリティ対策を検討すると、対策の選択肢が制限され、費用対効果が悪くなるなどの問題が発生する。

また、制御システムは、パソコンやサーバーといった一般的なIT（InformationTechnology）とは異なる技術（ITと区別してOT＝Operational Technology＝という）も用いられており、システムの使用環境や求められる機能に特殊性がある。このため、ITのセキュリティ対策製品が適用できない場合もあり、IT以外の対策や運用方法の工夫によるリスク低減を図ることも重要である。

IT部門と事業部門の統括リーダー

どの企業でも課題となるのが、制御システムセキュリティへの取り組みを社内に浸透し定着化させるマネジメントの進め方である。制御システムのセキュリティが重大リスクと認識されても、IT部門と事業部門で責任や所掌の押し付け合いとなることが多い。インフラや設備の仕組みとセキュリティの双方を理解して横断的にリーダーシップを発揮できる人材は極めて稀であるが、高い視点から両部門を統括できる人材を採用し、育成を続けることが安全確保の鍵となろう。

三菱総合研究所には、セキュリティ分野、各種インフラおよび安全分野で豊富な知見と実績がある。これを活かし、セキュリティ対策の技術的な検討、マネジメントプロセス、マネジメント態勢などのソリューションを提示し、拡大するサイバー攻撃に対するインフラ・企業の安全確保を積極的に支援していく。

【業務改革】

2 建設現場の生産性革命

次世代インフラ事業本部　竹末 直樹

Point

- 建設現場の生産性向上を目的とした「i-Construction」が活況。
- 最終ゴールはデジタル技術による「働き方改革」の実現。
- 新しい現場の姿を描き、その実現に向けて技術開発を進めることが重要。

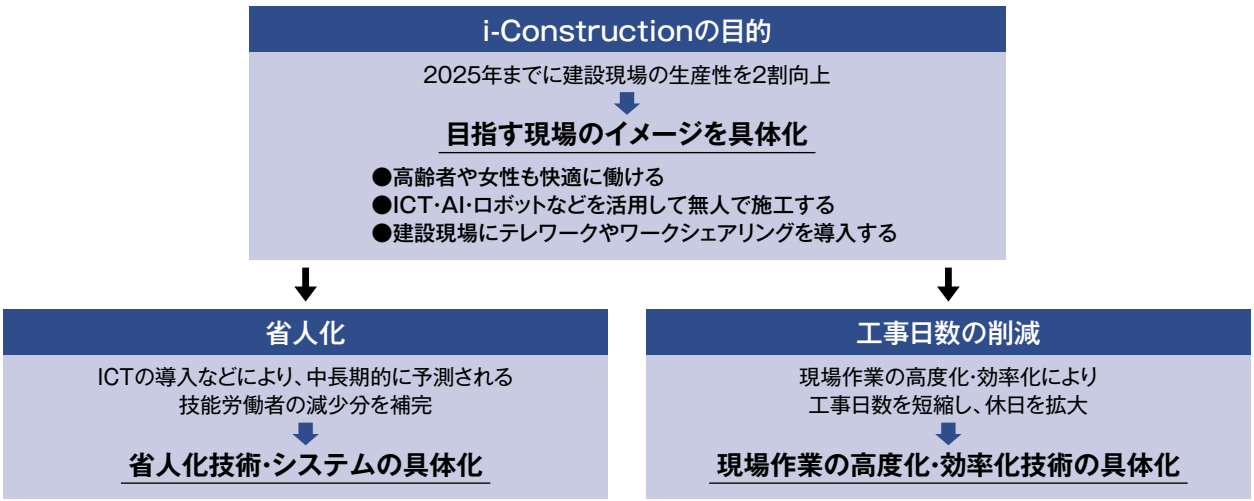
高齢化が進み、今後10年間に建設現場で働いている技能労働者340万人のうち110万人が減少する。建設現場の生産性向上と新たな働き手の確保は日本の喫緊の課題である。国は人工知能（AI）、IoT、ロボットなどの最先端技術により、建設現場の生産性を2025年までに2割高める「i-Construction」を加速させている。

狙いは工事日数の削減と省人化にある。これまでより少ない日数と人数で同じ量の工事を実施する。建設は、設計、施工、維持管理に加え、解体や素材への還元など守備範囲が広く、特にメンテナンスを含めると仕事は限りなくある。省人化が進んでも大量失業につながる心配はない。まさに建設産業の生産性革命である。

最終ゴールは、結局のところ「働き方改革」といえる。デジタル化による業務改革を進める建機メーカーのコマツは、測量の際にドローンを飛ばして地形の3次元点群データを収集し、完成形との差異を重機が認識して半自動的に施工する革新的なしくみを構築している。これまでは、「丁張り」や「遣り方」などと呼ばれる目印を人が測量機器を用いて設置した後、測量図に従って重機で掘削・整形していた。今では、データを読み込んだIT重機を経験の浅いオペレーターが運転して、熟練オペレーターの手を借りることなく施工できる。建設現場から極力人手を減らし、高齢者や女性など新たな働き手の活躍を促す、i-Constructionが目指す姿の一つといえる。

今後、多くの企業に必要なのは、働き方が変わった新しい建設現場の姿を描くことだ。技術開発、システム開発などを進める場合も、「高齢者や女性も快適に働ける」、「ICT・AI・ロボットなどを活用して無人で施工する」、「建設現場にもテレワークやワークシェアリングを取り入れる」、「その結果として平均総労働時間が減少する」といった関係者が具体的にイメージしやすい現場の姿を共有するべきである。日本の技術開発ではニーズよりもシーズが先行し、目先の細かな課題解決に走りがちな点にも留意するべきだ。生産性2割向上という目標が働き方改革につながる具体的なイメージに置き換えて、官民協働で新技術の開発・導入に取り組むことが必要である。

［図］「i-Construction」による働き方改革



出所：三菱総合研究所

【安全安心】

「日本版フードディフェンス」導入のコツ 3

科学・安全事業本部　山口 健太郎

Point

- 食品への異物混入防止策（フードディフェンス）の必要性が高まっている。
- 性悪説を前提とする従業員管理は日本の食品現場にはなじまない。
- 工場の経営効率化と両立できる取り組みを。

「食の安全」に関して、米国が新たな動きに出ている。2011年制定の「食品安全強化法」で関連事業者に対し、製造加工・包装・保管の各工程において、従業員などによる意図的な異物混入行為の防止対策（フードディフェンス）を求めた。適用期限は原則2019年7月であるため、今後、従業員による犯行の防止策が確実に進むとみられる。

一方で、日本の食品製造現場では近年、多品種化と大量製造を求められ、作業場が手狭になり従業員の身体的負担も増大するなどの状況が目立っている。背景には、個人消費低迷にもかかわらず、コンビニエンスストアの売上高と来客数が2008～2016年に約3割増えたことがある。少子高齢化で一人暮らし世帯が増え、「おいしいものを手軽に、いつでも食べたい」というニーズが急速に強まったからだ。

こうした状況では、「放っておくと悪事を働く」という性悪説を前提に、従業員を信頼しないまま管理を強化しても、逆効果にしかならないだろう。工場内部の防犯対策の強化と作業環境の改善、生産性の向上を同時に達成させるという難しい課題を解決するには、別の手法が必要になる。

フードディフェンスに関わる取り組みを、工場経営の効率化にも役立てる発想が欠かせないだろう（表）。例えば、工場内のカメラが記録した映像や、センサーがとらえた従業員の移動データを保存する目的を、監視の強化ではなく、製造工程における無駄の発見や、作業手順の改善に設定する。

同様に、冷蔵庫や保管庫の施錠に関しても、非接触型ICカード形式のキーを従業員に配布する方法がある。開閉作業が簡略化されて利便性が大いに高まる一方、開閉を行った人物を簡単に特定して、責任の所在を明確にできる。

方策の一つひとつを、工場経営の効率化や生産性向上の取り組みと読み替え、活かしていくこと。この発想が、日本におけるフードディフェンス導入のコツである。2020年の東京オリンピック・パラリンピックを見据えた独自の「食の安全」確保策として、国際社会へのアピールにもなり得る。

［表］フードディフェンスと工場経営効率化を両立させる取り組みの例

具体的な方策	フードディフェンスの方向性	工場経営効率化への効果
カメラ、センサーによる従業員の移動履歴の保存	工場内の監視	作業における無駄の発見、作業改善
非接触型ICカードと連動する電子錠の採用	冷蔵庫や保管庫の施錠	開閉作業の効率化
	製造工程にアクセス可能な従業員の限定	電子錠の開閉データを基に、従業員の配置計画や勤怠管理を自動化
洗剤や薬物などをあらかじめ定めた場所で一括管理	食品への混入防止	在庫管理や使用量の把握が容易になる
私物保管を工場の責任下に置く	従業員の私物持ち込みの禁止	私物を盗難から守る

出所：三菱総合研究所

【海外戦略】

4 価値観への関心を促す

コンサルティング部門
経営イノベーション本部　丸貴 徹庸

Point

- 海外子会社の企業統治が苦戦。
- グループ全体への価値観の浸透が欠かせない。
- 従業員の自主性に基づく意識改革に結びつける。

海外進出している日本企業の損失計上や現地撤退が目立つ。海外子会社の内部統制システムが機能せず、リスク管理が行き届かないなど、企業統治に苦戦しているようだ。親会社が海外の子会社を管理するには、国内以上の工夫が必要となる。

例えば、日本たばこ産業（ＪＴ）は買収した海外のたばこ事業について、経営陣を多国籍としながらも放任はせず、責任の範囲を明確にして、多様性の維持と事業拡大を両立させた。現地経営陣に対し、的確な目標を示してグリップを効かせることが求められる。

では海外で企業統治を機能させる要件は何か。適切な制度・人材配置・規則に基づく権限委譲が挙げられるが、その前提条件が整わないとうまく機能しない。より重要なことは、基本的な価値観を企業グループ全体に浸透させることである。

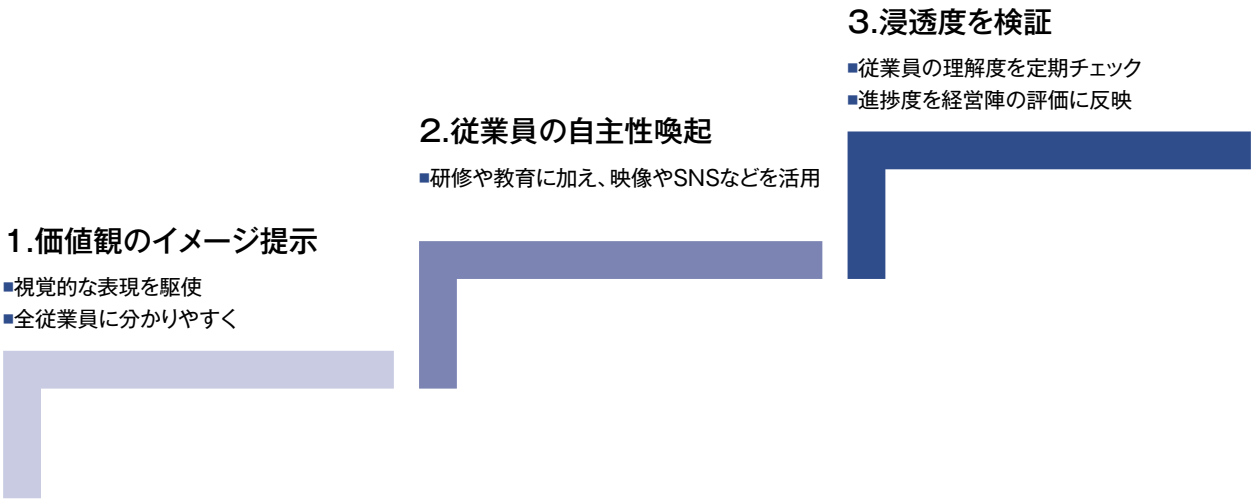
歴史・言語・文化的な背景が異なる海外子会社の隅々にまで、共感できる形で基本的な価値観を浸透させるのは容易ではない。特に、明確な意思表示が苦手な日本人にとっては、ハードルが高いとされてきた。

しかし、人種や使用言語が多様なグローバル企業は、この難題を段階的な取り組みによってクリアしている。まずは、基本的な価値観をアイコン（※1）やインフォグラフィック（※2）によって表現し、誰もが視覚的に理解可能にすることから始まる。第2段階は、教育や研修だけではなく、映像やＳＮＳも駆使して、従業員が自主的に価値観への関心を強める仕掛けだ。そして第3段階で、従業員の理解度を定期的にチェックし、その結果を経営陣の評価に組み入れている。この3つのステップを通じて、全組織への価値観の浸透を徹底させている（図）。

米国のゼネラル・エレクトリック（ＧＥ）は、さらに価値観への関心を促すため、社外向けの情報開示を可能な限り拡充することで、外部からのフィードバックを従業員の意識改革に結びつけている。日本企業についても、グローバル企業が講じている工夫の数々を採り入れて、海外進出をうまく加速させることを期待したい。

（※1）特定の人物や出来事などを端的に表すイラスト。
（※2）情報、データ、知識などを効率的に表現したグラフや図。

［図］海外子会社に価値観を浸透させるステップ



出所：三菱総合研究所