知創の杜

FUJITSU

2016 Vol.12

「しなやか」で「したたか」なレジリエンス強化
―サイバーの風に吹かれても倒れない―

shaping tomorrow with you
社会とお客様の豊かな未来のために

株式会社 富士通総研
FUJITSU RESEARCH INSTITUTE

富士通総研のコンサルティング・サービス

社会・産業の基盤づくりから個社企業の経営革新まで。
経営環境をトータルにみつめた、コンサルティングを提供します。

個々の企業の経営課題から社会・産業基盤まで視野を広げ、課題解決を図る。
それが富士通総研のコンサルティング・サービス。複雑化する社会・経済の中での真の経営革新を実現します。

お客様企業に向けたコンサルティング

課題分野別コンサルティング

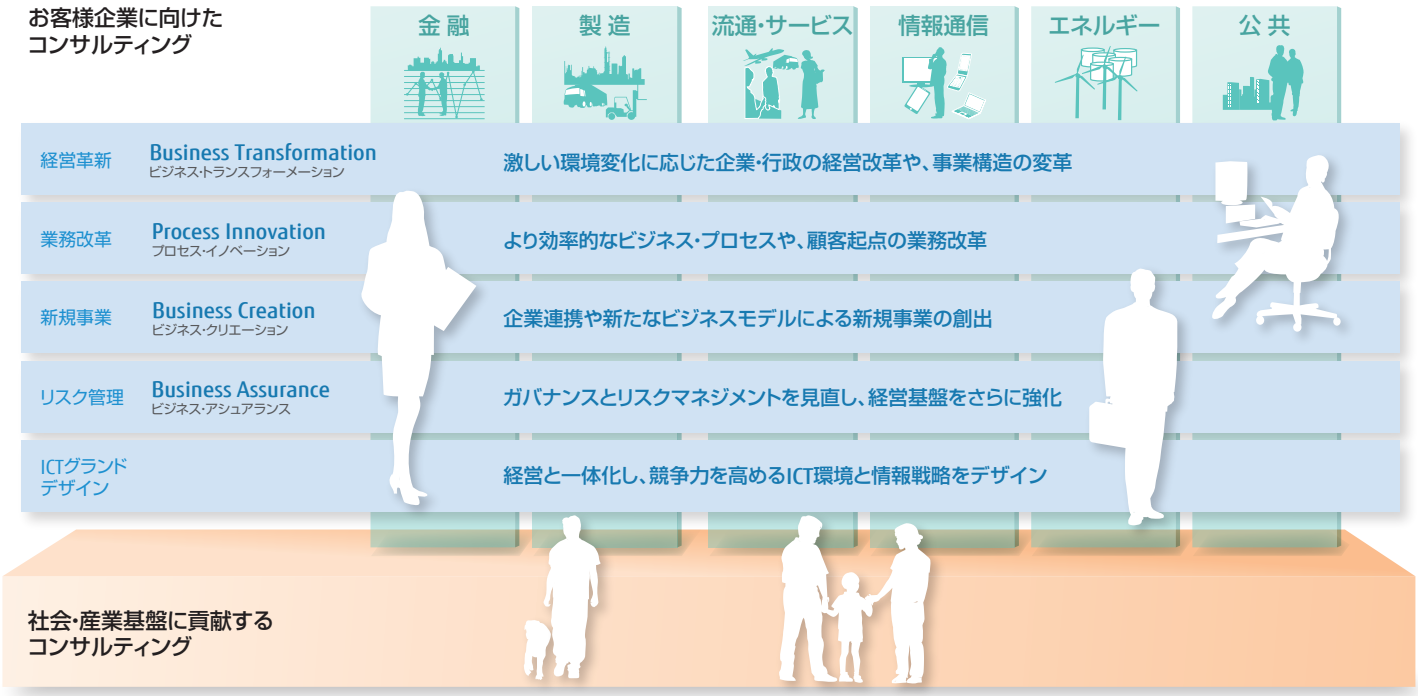
お客様のニーズにあわせ、各産業・業種に共通する、多様な業務の改善・改革を図ります。経営戦略や業務プロセスの改善などマネジメントの側面、そしてICT環境のデザインを通して、実践的な課題解決策をご提案します。

業種別コンサルティング

金融、製造、流通・サービスなど、各産業に特有の経営課題の解決を図ります。富士通総研は、幅広い産業分野で豊かな知識と経験を蓄積しており、あらゆる業種に柔軟に対応するコンサルティング・サービスが可能です。

社会・産業基盤に貢献するコンサルティング

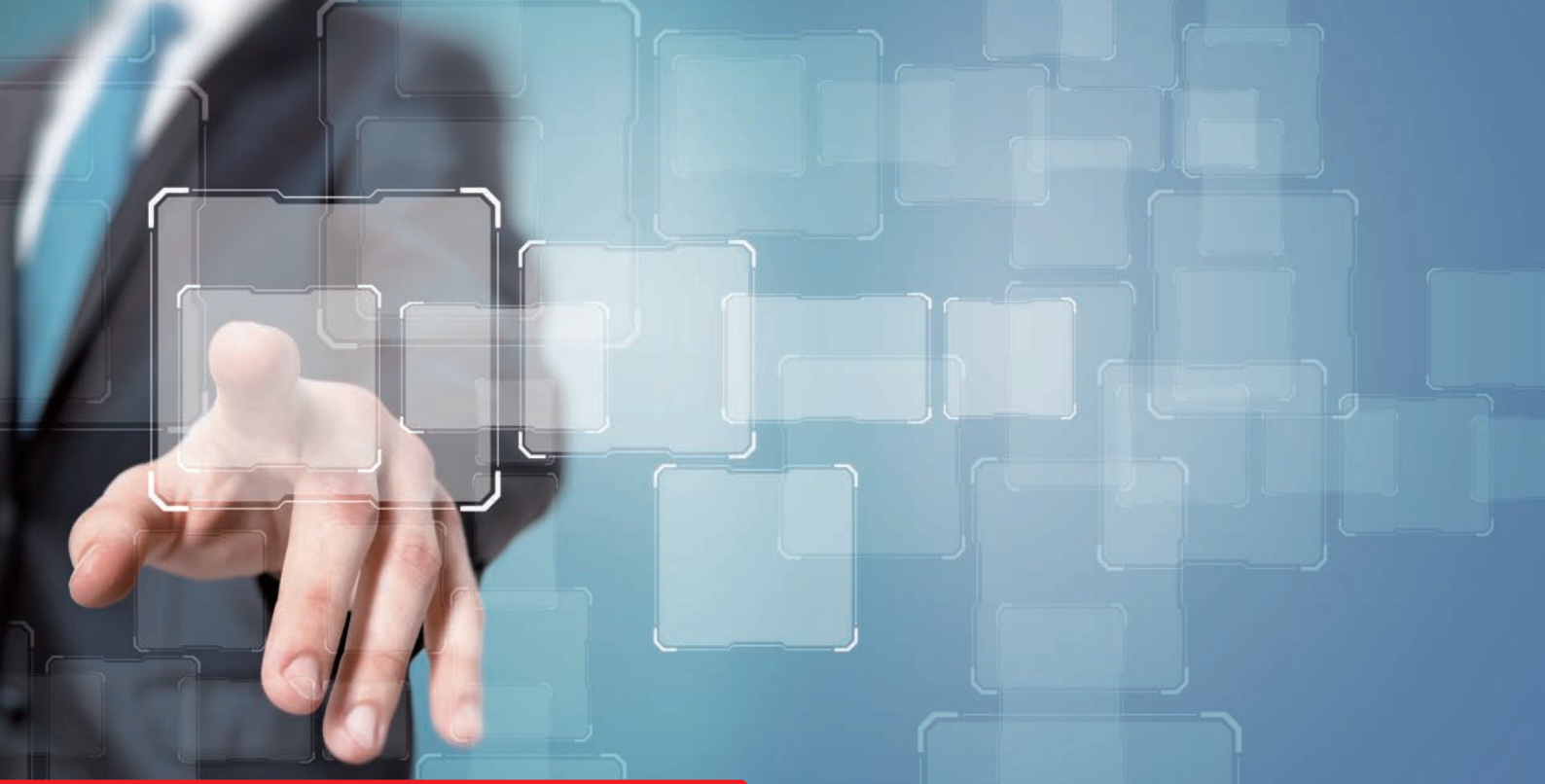
国や地域、自然環境などの経営の土台となる社会・産業基盤との全体最適を図ることで、社会そのものに対応する真の経営革新、業務革新を実現します。



知創の杜

2016　Vol.12

CONTENTS



特 集

サイバー戦の備え
―安全保障の視点から見たサイバーセキュリティ―

株式会社富士通システム統合研究所
主席研究員
田中　達浩

政治・経済・安全保障等のあらゆる分野における不安定・不確実な世界情勢の中、既存の枠組みでは対応できない、対テロの戦い、非対称型の戦い、ハイブリッドな戦いが繰り広げられている。そしてそれらの戦いはサイバー攻撃のような見えない手段を巧妙に使用する。そのような戦いにおけるサイバーセキュリティを、国家～組織～個人がそれぞれの立場に応じて安全保障の視点から準備する必要がある。

執筆者プロフィール

田中　達浩（たなか　たつひろ）

株式会社富士通システム統合研究所　主席研究員

1975年 防衛大学校卒業、陸上自衛隊入隊。統合幕僚会議事務局3室防衛情報通信基盤（DII）管理運営室長、陸自研究本部第3研究課長（装備体系担当）、統幕3室（運用訓練）、5室（防衛政策・計画）、第2師団副師団長兼旭川駐屯地司令の勤務を経て、通信学校長兼久里浜駐屯地司令を最後に退職、元陸将補。
米国海兵隊指揮幕僚大学留学のほか、米国スティムソンセンター、ハーバード大学アジアセンターにおいて国家安全保障およびサイバー安全保障の研究に従事。

1. サイバー戦において守るべき対象

最初に、サイバー戦において守るべき対象について考えてみる。

「サイバー空間」の説明にはいくつかの方法がある。ここでは簡単に、海底ケーブル、地上ケーブル、衛星・無線通信網およびそれらの管理施設から成る「物理的な通信層」、インターネットの基本構造たる「IPネットワーク層」、そして各種のサービスを提供する「システム層」によって構成される空間を「サイバー空間」と捉える。

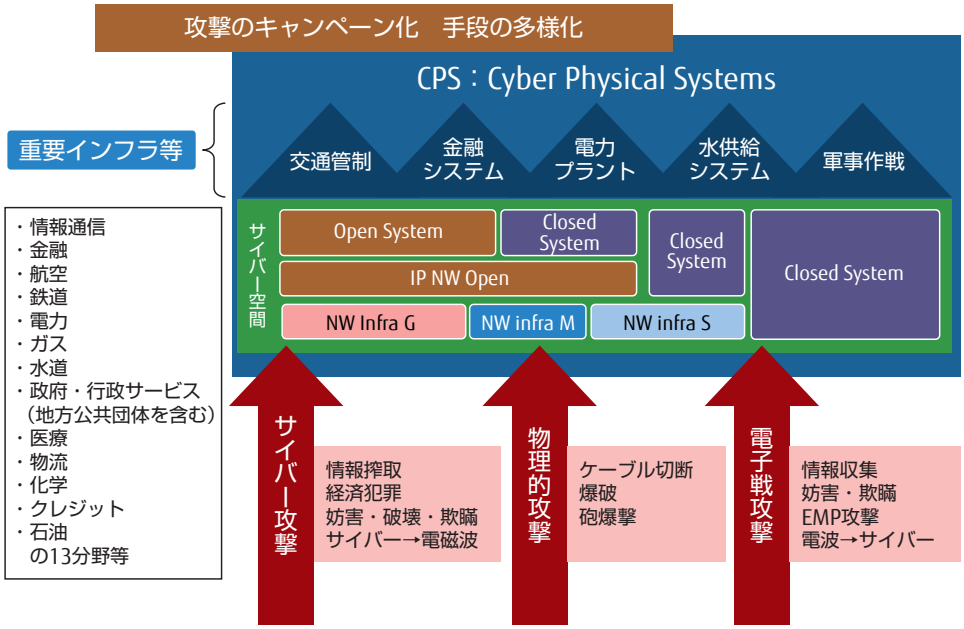
政府、企業や市民が使用者として直接関わるのは、経済活動、社会活動およびサービスを提供されるシステム等である。これらに対し、「サイバー空間」がサービスを提供し、サポートしている。特に、交通、ガス、水道、電気および金融システム等のいわゆる「重要インフラ」（13分野）等はその管理、供給、制御等のフィジカルな装置、フィジカルなシステム等が、サイバー空間のサービスおよびサポートに依存している。

本稿では、サイバー空間と重要インフラ等のフィジカルなシステム全体を「サイバー・フィジカル・システム（CPS）」[注1]として扱う。従来は、サイバーセキュリティの確保要件をサイバー空間における「情報保証」として捉えていたが、現在では、フィジカルなシステムの継続・維持の重要性を認識した「事業継続（軍事的には任務保証）」として経営者のリーダーシップの問題として強調されている。

このCPSに対する攻撃手段は、サイバー空間内の「サイバー攻撃手段」に限らず、ケーブルの切断、重要インフラやサイバー空間の維持管理施設の爆破、エネルギー兵器による砲爆撃のような「物理的攻撃手段」、通信妨害・欺瞞等の「電子戦の手段」のような多様な手段が考えられる。したがって、安全保障の視点から見た「サイバー戦の対象」は、サイバー空間だけでなく、「CPSおよびそれらの活動全体」を守るべき対象として考える必要がある。（**図1**）

2. サイバー脅威の変化と特性

現在のサイバー脅威の変化をどのように捉えるのか？1つはサイバー空間における「サイバー攻撃の技術的変化」である。



●図1　サイバー・フィジカル・システムに対する攻撃

1980年代初めに、コンピュータウイルスが登場した。当初の悪意ある活動は、コンピュータ技術の争いであり、相手のシステムへの侵入、ウイルス感染、データ改ざん・削除等の「使用妨害が中心」で、「一時性」の、かつ攻撃者が成果を公表するような「成果誇示型」の攻撃であった。

しかし、現在は、「明確な攻撃目的」を持ち、「攻撃対象を絞って」「周到に準備」し、「複数の突破口を利用」した一時性ではない「高度で」「持続性のある」、いわゆる「APT（Advanced Persistent Threat）攻撃」あるいは「標的型攻撃」が大きな脅威となっている。

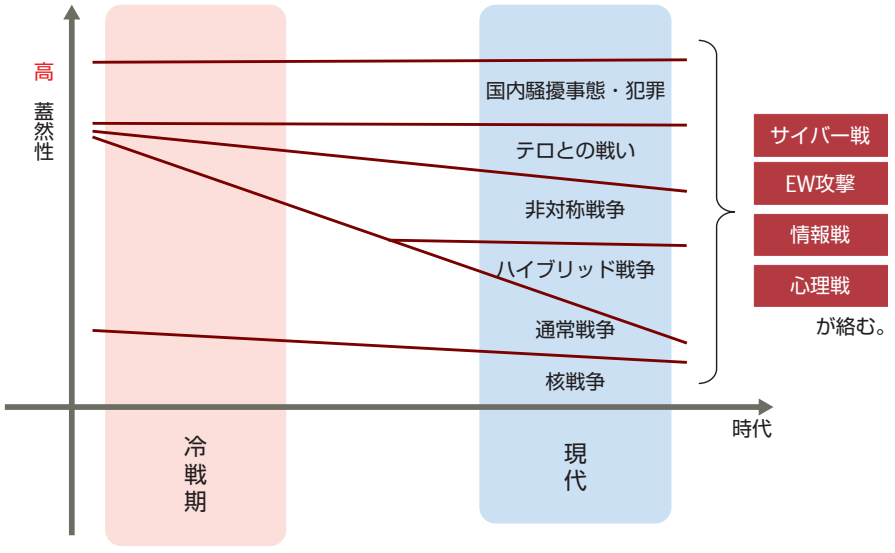
もちろん心理的な効果を狙った成果誇示型の攻撃もあるが、標的型攻撃の大きな特徴は、「隠密にシステム内に潜入後、システム内部で周到に準備を重ね、必要な時期まで潜伏またはシステム内を移動して隠ぺいを図る」極めて高度な戦いを仕掛けてきている点である。潜入に当たっては、「システムの脆弱性を突く方法」からシステム使用者側の「人的ミス等を悪用する方法」のような「内部脅威型」まで、「多様な攻撃方法を複数準備する」綿密周到な極めて大きな悪意を持った攻撃である。そして、多種多所に同時に攻撃を仕掛け、弱いところから侵入して成果を他に拡大していくような「キャンペーン化」の特徴が、さらに対応を難しくしている。

そのようなサイバー攻撃が、不確実・不安定な安全保障環境における「国家の戦い」の手段として重要な意義を持ち始めているのが、もう1つのサイバー脅威の変化である。

冷戦期における「国家の戦い」は、核戦争、通常戦力による戦争を中心に捉えていたが、冷戦崩壊後のポスト冷戦期においては、国家間の大規模紛争の生起する蓋然性が低下することとなった。そして現在では、生物化学兵器のような大量破壊兵器等を用いる「非対称戦」、非正規軍との戦いである「ゲリラとの戦い」、そして対テロ防護やテロリストの根拠地を掃討する「テロとの戦い」および国際法の適用を回避するために敢えてグレーゾーンの曖昧さを突いた「ハイブリッドの戦い」が「国家の戦い」の中心的なテーマとなっている。

以上のような国家間のハードな争いに「国内騒擾事態」および「国内外経済犯罪」を加えた「国家の戦い」のすべてのスペクトラムにおいて、「開発が容易で、安価かつ見えない手段」であるサイバー攻撃が重要な意義をもって用いられる。

加えて、無線通信に依存するシステムにおいては電子戦攻撃が「サイバー攻撃の準備手段」およびシステム使用の「直接的な妨害手段」等として用いられる。（**図2**）



●図2　「国家の戦い」の変化

攻撃を仕掛けるもの、すなわち「攻撃主体（アクター）」については、その一般的分類は、「国家主体」、テロ組織等を含む「非国家主体」、および犯罪者・ハクティビスト（Hactivist）(注2)を含む「個人」である。

「国家は地政学上の国益の追求目的」から、「テロリストおよびハクティビストは、宗教、信条等の政治的な目的」から、そして「犯罪者は主としていたずらや経済目的」から「サイバー戦（サイバー攻撃、電子戦攻撃等を含む）」を仕掛けてくる。これらの攻撃は、システムあるいはシステムがサポートする活動に対する直接的・物理的な効果および攻撃の結果がもたらす政治的・心理的な効果を狙って行われる。

以上のような、サイバー脅威の変化と特性から、攻撃の結果として生起する事象や被害状況、すなわち直接見える状況は、必ずしも攻撃者の最終的な目的を達成した結果ではないことがわかる。しっかりとした情報と分析をもって、攻撃者の特定、真の攻撃目的と標的を見極めることが重要となる。

3. CPSをいかに守るか
―安全保障の視点からの対応―

インターネットフリーダムの考えによりICTは十分に進化し、情報化時代を迎えた。しかし一方で、この善意に基づく仕組みを悪用した攻撃の進化も止まるところを知らない。現在および今後は、サイバー空間におけるセキュリティのみならず、国家として、あるいは、国際的な友好・同盟国も含めた「CPS全体としてのレジリエンス」を確保するため、安全保障的な視点を持って準備することが求められている。

最初に、「自己防護の原則」がある。

個人および組織は自らを防護する責任を有する。爆破等の物理的なテロ攻撃の可能性もサイバー戦の対象と考えると、システムおよび施設等が防護対象となる。この際、組織、企業等が防護すべきものについて理解していることが必要である。

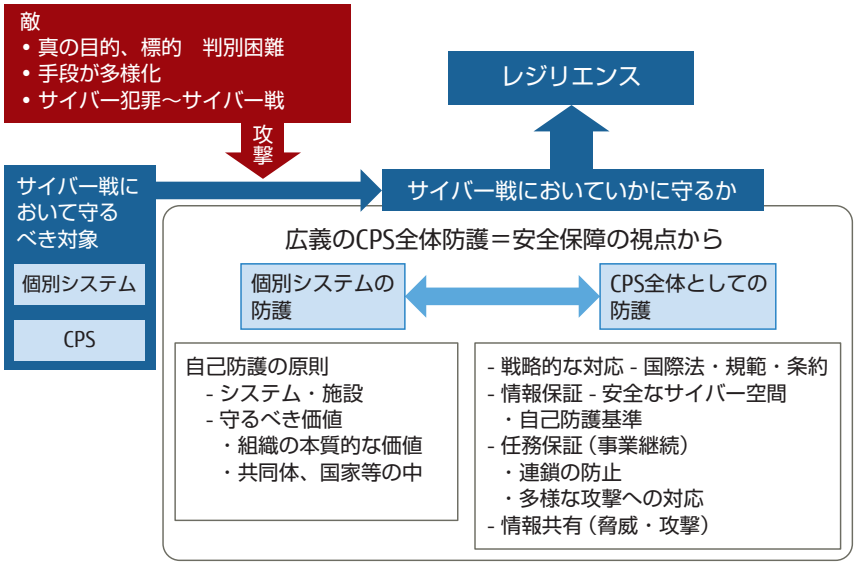
「企業等が社会に提供するもの」の「価値そのものがまず重要な防護対象」である。そして、「企業等およびその提供するものが、国家や世界、共同体、地域体の中で占める意義と役割が持っている価値が防護対象」となる。特に、重要インフラの障害による影響は大きく、例えば、電力については、その供給が停止することによる影響は他の多くのシステムおよび活動が影響を受ける。一方、規模の小さな企業であっても、その製品が高度・独自の技術であって、その製品供給停止は、他の重要な製品の生産に大きな影響を及ぼす場合も同様に、その企業は重要な防護対象となり得る。

企業等は、そのような視点で「自らの価値を認識」し、「サイバーセキュリティに対する投資」を適切に行って価値を高めなければならない。それは、利益に対するコストとは異なる。自らの価値に基づいてサイバー脅威に対する「リスクを分析」し、「リスクを回避し顕在化させない準備と投資」およびサイバーインシデントが生起した場合の「対処メカニズムの確立」が、企業としての価値を高め信用を確立することになる。

「CPS全体の防護」の考え方については、CPSの「相互依存性の特性」を理解する必要がある。「1つのシステムの障害・停止が他のシステムの障害へ連鎖しない」ための方策を準備することが重要である。また、CPS全体として、代替手段や迂回手段を準備することも考えなければならない。共同体やサプライチェーンおよび国家としての「リソース配分」も含めた守るべき対象の「優先順位」についても予め議論しておくことが「重大なサイバー攻撃に際しても即応」し、「CPS全体としてのレジリエンス」を確保するために必要なことである。

さらに、CPS全体の中で、攻撃者が狙う真の目的の達成を阻止するため、「サイバー攻撃の情報（攻撃者、技術、要領等）の共有」は、他への連鎖の防止、対処段階の国内および国際法的対応のため不可欠であり、政府系機関、企業等の積極的な参加が期待される。

サイバーセキュリティの分野に対し、企業等の経営者、政府首脳、防衛・危機管理担当者の高い見識に基づく安全保障の視点からの「リーダーシップの発揮」が今の日本にとっては重要である。（**図3**）



●図3　サイバー・フィジカル・システムの防護

(注1) サイバー・フィジカル・システム（CPS）：Cyber Physical System。コンピューティングおよび通信コアによって、その操作が監視され、コーディネートされ、制御され、統合されている物理的および工学的システムである。

(注2) ハクティビスト：サイバー犯罪に関する用語で、社会的・政治的な主張を目的としたハッキング活動（ハクティビズム）を行う者のこと。主な目的は、現実世界におけるアクティビスト（積極行動主義者）と同様、自分たちの主張を声明として発表したり、政治的に敵対する政府や企業へ攻撃したり、といったもの。

セキュリティレジリエンスへの取り組み

IoT時代に向け、セキュリティマネジメントリスクが再認識されています。サイバー攻撃は防御と検知も重要ですが、発覚後の対処を考えて備えることの重要性が高まっています。どのような心構えで備えの方針を考えるべきでしょうか？ 訓練と演習の違いを踏まえ、人材育成につなげるセキュリティレジリエンスへの取り組みを語っていただきました。

対談者は、名古屋工業大学大学院社会工学専攻の渡辺教授、富士通株式会社グローバルマーケティング部門の太田エバンジェリスト、株式会社富士通総研（以下、FRI）の三浦チーフシニアコンサルタント、進行役はビジネスレジリエンス事業部の細井事業部長です。（対談日：2016年7月21日）

対談者
前列左から　渡辺　研司：名古屋工業大学　大学院社会工学専攻　教授
　　太田　大州：富士通株式会社　グローバルマーケティング部門　エバンジェリスト
後列左から　細井　和宏：株式会社富士通総研　ビジネスレジリエンス事業部　事業部長
　　三浦　良介：株式会社富士通総研　ビジネスレジリエンス事業部　チーフシニアコンサルタント

1. 経営者に対してセキュリティリスクの危機感を演習で醸成する

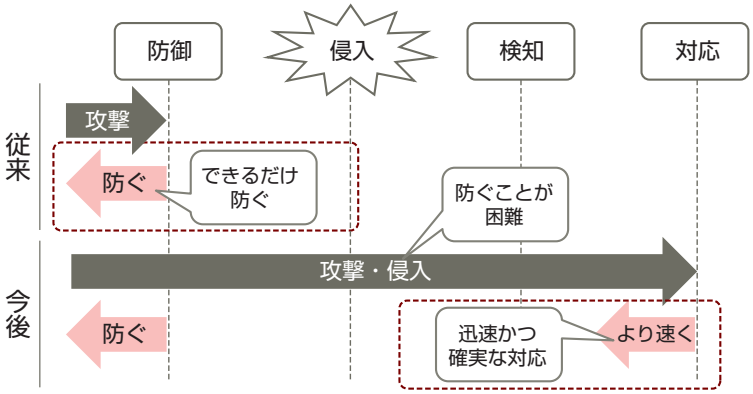
細井　IoTの進展に伴いサイバー攻撃の脅威とともに、セキュリティリスクがクローズアップされています。しかし、自然災害とは異なり、発生後の自社にとっての影響度合いが企業のトップに認識されにくいのが実態です。攻撃目的も、機密性に関わる情報流出から、可用性に関わるPLC（programmable logic controller）に代表される制御系インフラまで、IoT（Internet of Things）も相まって範囲が広がっています。当然その防御と検知は重要ですが、それ以上に、検知後のインシデントレスポンスの構えが重要です（**図1**）。FRIでは事業継続（BCM）では発災後の行動力が重要だと考え、そのための平時の心構えや備えについてコンサルティングを行っていますが、サイバー攻撃への取り組みも事業継続の考え方と根本は同じと考えています。それをセキュリティレジリエンスと呼んでいます。本日はそういった観点で、サイバーセキュリティに対する企業の心構え、インシデントレスポンスの重要性、平時の構えなどを話していただきたいと思います。

早速ですが、渡辺先生は事業継続に精通され、また数多くサイバー演習をされていますが、最近特に感じられている課題はどういったことでしょうか？

渡辺　重要インフラ企業や個別企業と演習をご一緒させていただいておりますが、ようやく訓練から演習に変えなければという意識を経営者の方々も持ち始めてきた気がします。訓練は決められたことを時間内に手順どおりできるかをチェックする、いわゆるドリルです。訓練は世の中で多く実施されていますが、私は正解がないところで各ポジションの役割で臨機応変に考え意思決定を行う、頭の筋肉を鍛えるような演習に注力しています。参加者が的確に状況把握して、自身がカバーすべき目標への距離感を測り、残ったリソースを見て、選択肢を考えて意思決定を重ねていくことがレジリエンスの基本だと思います。演習シナリオとして作り出された想定外の事象で、いかに断片的な情報を掻き集め、限られた時間内で意思決定して次に進められるか。落とし穴も仕込まれた周到なシナリオが準備された演習を体験し、皆さん恥をかきながら「何ができていないのかがわかって良かった」というモードに変わってきました。御社も貢献されていますが、いわゆる圧迫訓練も含めた試行を通じて、一部の意識の高い企業や業界が追いついてきたところです。

太田　今、先生が仰った訓練から演習へって素晴らしい考えだと思います。各省庁にサイバーセキュリティ情報化審議官が4月に設定されました。その方々の課題

■ 防御困難なサイバー攻撃の増加
■ インシデント発生の際は、迅速・確実な「対応」がポイント



●図1　セキュリティに対する意識の変化

認識の1つに人材育成があります。世の中ではテクニカルな面での人材育成、ホワイトハッカー(注1)がいると世の中は救われるみたいなイメージが強く、8万人足りない、20万人足りないといった話が多いのです。技術であればエンジニアがセキュリティを学べばいいだけのこと。教育体系だけを変えても人は育たない、まさに演習をやる仕組みを作らねばと痛切に思います。道具の話ではなく、頭を鍛える演習の場を用意しないといけません。

渡辺　まずトップが演習の重要性を理解しないといけなくて、トップに危機感がない会社はいくらやってもダメですね。何か起きた時「想定外のことでございました。あいすみません、再発防止に努めます。」で記者会見を終えてはいけませんね。

渡辺　研司（わたなべ　けんじ）
名古屋工業大学　教授
1986年 京都大学卒業、同年 富士銀行入行、米国駐在（ストラクチャード・ファイナンス）、システム開発・企画他。1997年プライスウォーターハウスクーパースに移籍、国内外企業向け金融ビジネスに関わるコンサルティングに従事。2003年 長岡技術科学大学准教授（経営情報系）。2010年4月より現職。内閣官房重要インフラ専門調査会・会長、内閣府事業継続計画策定促進に関する検討会・委員、経済産業省ISOセキュリティ統括委員会・委員、ISO/TC292（Security and resilience）・エキスパート、日本政策投資銀行BCM格付けアドバイザーなどを兼務。工学博士、MBA。

三浦　CSIRT（Computer Security Incident Response Team）を構築している企業の方と話していて、トップダウンでCSIRTを作っている企業はシステム部門だけでなく他も巻き込んでいるケースが多いです。ボトムアップで作っている企業はシステム部門内に閉じたCSIRTを構築しているケースが多く、横連携に課題があります。やはり経営層がサイバー攻撃をリスクとして認識して対応することが重要だと思います。

太田　昨年12月に経済産業省から「サイバーセキュリティ経営ガイドライン」が出たおかげで、そういう考え方を持たなければという意識が多くの企業で広がっていますね。

三浦　7月に総務省からも「IoTセキュリティガイドライン」が出されましたが、経営層がやるべきことが徐々に定義されてきているかと思います。

渡辺　「安心安全の対策はきちんと考えてあります、大丈夫です」と言っている企業は信用できません。リスクをきちんと認識し、自社の脆弱性に対し、それが起きたらどういうビジネスインパクトがあるかを想定し、それに対して今対応できるのはここまでで、残存リスクについては、例えばバックアップシステムへ切り替えたり、定義された重要業務に沿ってサービスラインを減らします、と言える企業だけが信用できます。この考え方は事業継続と全く同じですね。

2. 経営者にビジネスインパクトを明示する

細井　事業継続ではリソースの相互依存性をサプライチェーンなどの概念で理解しやすいですが、セキュリティリスクの文脈で危機感を醸成するために工夫すべきポイントは何でしょうか？

渡辺　やはりビジネスインパクトで示すことですね。例えば、情報漏洩すればコストがいくらとか、どれだけマーケットシェアが落ちるとか、経営者に数値インパクトを示すことが有効です。やはりBC（Business Continuity）は自然災害もセキュリティも同じなので、CSIRTは情シスだけでは無理で、事業部門が入って、この事象は事業にどうインパクトがあるか翻訳し、きち

んとCEOに伝えなければいけません。事故が起きた際、データベースをシャットダウンするか、システムを全部止めるか、どれをやってもお客様は困るし風評被害が出るけど、これ以上続けるともっと酷いことになると、番頭さんのような立場の人が翻訳してあげないと、経営者はわからないですね。

三浦　地震などの災害では時間が経つと被害状況がわかってくるのに対し、サイバー攻撃は悪意をもって行われるため、証跡の改ざんや証拠隠滅がある点が違います。だからこそ、CSIRTは今何が起きているかを断片的な情報から組み立てて、経営者にわかりやすく伝えることが重要です。フォレンジック（forensic）[注2]で原因を完全に調査するまで1、2か月くらいかかってしまい、調査結果を待っていては手遅れになります。

渡辺　さらに、同時多発的に攻撃された際に個社では潰しきれないので、CSIRT協議会等の横軸で見る人たちと連携して、断片に散発する事象群から組み立てたインテリジェンスを経営者に伝える必要があります。攻撃は肉眼では見えませんし、攻撃目的も一般企業の人にはわからないので、専門団体と連携しないといけません。

3. セキュリティ防御技術の進化

太田　今までセキュリティの防御方法の多くはアメリカで形成され、検知装置やフォレンジックツールが生まれています。富士通も社内のサイバーセキュリティに取り組む中で、そういう装置を運用してきています。しかし、そのためには大勢の優秀なセキュリティ専門家がいて、あらゆる情報を全件調査できる体力が必要です。フォレンジックでは大量の通信パケットデータを集めて、相関分析をかける。分析エンジンも凄くパワーが求められます。こんなマルウェアが来たら、どこかにバックドアが開いていないのか、そのIPアドレスが前に悪いことに使われていたURLだ、というふうに攻撃者の手段に着眼して調査していました。しかし結局は後追いのセキュリティ対策なのです。そこで、我々は2011年から攻撃者の行動に着眼しました。攻撃者は必ず入ってくる努力をして、内部調査をする努力をして、最終的に見つけた情報を持ち出すという動きをします。この行動には法則があります。それを研究して、ようやく昨年モデル化できました。

太田　大州（おおた　たいしゅう）
富士通株式会社　エバンジェリスト
1980年 富士通株式会社入社。複合情報通信システム分野の商品開発、東京シティホールや東京国際フォーラムなどインテリジェントビルシステム構築に従事。1995年より全国の消防指令管制システムの開発に従事、2005年より情報セキュリティ、事業継続（BCM）のビジネスを担当し、お客様・社会の安心安全イノベーションを促進。2014年1月「FUJITSU Security Initiative」としてサイバー攻撃への対応に向けてサービス・製品を体系化。セキュリティイニシアティブセンター長として、お客様起点でICTの安心安全を実現する継続的な取り組みを開始。2015年6月より初代エバンジェリストとして、社会的な視点でのサイバーセキュリティの課題解決に向けて、「国産セキュリティ自給率の向上」を目標に国産技術の醸成・普及、人材育成支援に関する活動を強化推進中。

渡辺　FBIとか犯罪捜査系のですよね。

太田　こんな行動とあんな行動とが組み合わさった場合には、どれくらいの確度で攻撃の可能性があるというトリアージの技術を作っています。個別のパケットを見ていないのです。また、各PCが外と横にどう通信して業務的に何をやっているかを全部トレースすることで、通信のパケットキャプチャーより1万分の1程度のボリュームのログを解析すればよく、結果的に凄いスピードで解析できます。例えば年金機構の事件は調

査に3か月近くかかりましたが、我々の技術では1時間で相関が全部出ます。攻撃者の行動特性に着目し、すぐに調査できるスピード感がサイバーセキュリティの世界を大きく変えていけると思っています。すでにお客様や富士通で使われて良い成果が出ていて、今後は情報系だけでなく制御系でも適用研究したいと考えています。

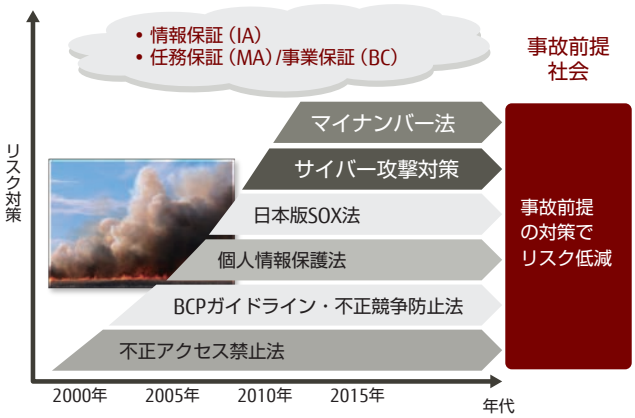
渡辺　マネーロンダリングやSNS系の関係性を抽出するようなロジックですよね。コミュニケーションの相手や頻度、方向を分析するような。

細井　IoTが広がれば、そういった行動をより正確に集めることができて、制御系への展開も現実味が増しますよね。一方、複雑に絡まったシステム系で、どこかで情報量が増えると意図しない連鎖障害が起きる。渡辺先生は攻撃者がそこを突いてくる可能性もあると警鐘を鳴らされています。それは意図的に再現される危険性もありますか？

渡辺　再現可能ですね。証券系は1,000分の1秒単位の取引なので、人の入る余地はないわけですが、システム同士がつながって、お互いの利益を最大化し始めると連鎖的に障害（輻輳）が伝播します。日本の証券市場はサーキットブレイカーという仕組みをすでに入れていて、特定時間内にある価格幅を外れた銘柄は売買停止になりますが、米国にはなかった。2010年に米国で発生したフラッシュクラッシュ(注3)は完璧に再現可能です。ああいう情報をシステムに投げ込んでやればよいのです。センシティビティ(注4)が上がっているので、そこに悪さをしようと思ったら、様々なことができてしまいます。

4. 事故前提での取り組みの必要性、情報保証から任務保証へ

太田　サイバー攻撃というと情報漏洩だと思う経営者が多すぎます。私は任務保証（ミッションアシュアランス）が要だと言い続けています。事業継続を保証すべき、そのためには事故前提で考えるべきです。今までは情報保証という観点が強すぎて、任務保証とのつながりがありませんでした。自然災害は目に見えてわかるので、経営者も理解しやすい。しかし、サイバー攻撃の本質は任務保証であることを理解してもらう意味で、演習はわかりやすい気づきが得られる手段だと思います。経済産業省に作られることが計画されている産業系のサイバーセキュリティ推進センターの機能として入れて普及させていかなければいけません。（**図2**）



●図2　これからの危機管理の考え方

渡辺　担当者ではなく経営者に来て欲しいですね。すでに攻撃されている、盗られている前提で、攻撃者にここまではくれてやって、どこから先を守るという、身を切ってでも守るべき所を守ることですね。そういった感覚を持つことが必要です。

細井　FRIでは事業継続の領域でシナリオ非提示型の演習を10年以上やってきており、これは演習で気づきを得ていただくことを目的にしています。今年7月より事業継続演習で培った考え方を応用してサイバーインシデント演習を開始しました。その演習シナリオでこだわった点は何でしょうか？

三浦　演習シナリオでは参加者に情報を提供しすぎない点にこだわっています。サイバー攻撃の全容が明白にわかるには、数週間から数か月ほど時間がかかります。初動時には断片的な情報しかわかりません。その断片的な情報から状況を推測して、事業経営にどんなインパクトがあるのか考えて、エスカレーションして意思決定してもらうところにポイントを置いています。

三浦　良介（みうら　りょうすけ）
株式会社富士通総研　チーフシニアコンサルタント
2002年 株式会社富士通ビー・エス・シー入社以来、公共分野におけるインフラ構築から運用・保守設計を実施。2005年から富士通株式会社にて個人情報保護および情報セキュリティに関するマネジメントシステム構築および認証取得を多種多様な業種で実施。2007年から株式会社富士通総研にて情報セキュリティに加え、ITガバナンスやリスクマネジメント分野のコンサルティングを実施。直近ではサイバーセキュリティ関連コンサルティング（サイバー演習、CSIRT構築等）に携わっている。

細井　お客様ごとに事業は異なりますが、どのような観点で影響把握すべきかは共通点がありそうですね。また、演習シナリオにリアリティがあるか、情報系と制御系に同時に何か起きたらどうなるかといったところも考え所ですね。

太田　先日、工場側のセキュリティ責任者とお話ししたら、オフィス系と工場系のセキュリティで全く違うのは、止めるとすぐに売上に影響を及ぼすことで、そのため、止める時の判断基準が必要だと言われていました。マルウェアが見つかっても、それが悪さをするかわからず、悪さするなら当然止めなければいけない。どの条件で止めるかについて、「ここまでならこうする」というのが事前に準備できるといいと思いました。そういうことを気づかせるサイバーセキュリティ演習もあると思います。

三浦　昨年のNISC（内閣サイバーセキュリティセンター）様の分野横断的演習で制御系システムの担当者にインタビューしたところ、「止まったシステムをリカバリする手順書は多数準備できている。しかしながら、システムは稼動しているもののコンピュータの負荷が高く制御できない状況のとき、誰がシステムを止める判断をするのか決まっていない」という話がありました。今後の制御系システムに関する演習では、システムが稼動しているものの制御できないようなシナリオを検討したいと思います。

細井　最近IoT関連の見える化、故障予測といった事例でも、生産ラインのマシンの様々な情報が取れるようになっています。日常的に発生する局所的な停止への対応と、攻撃で停止した際の対応はレベルが異なるだけと言えます。平時の状況変動に対応する構えまでカバーするシナリオを策定していけるでしょうか？

渡辺　生産管理システムとつなげればシミュレーションできます。意思決定で重要なのは、今止めると回復の時間がどれだけかかり、在庫がどれだけ減るか、お客様との取引関係もあるので1時間後に判断するかどうか。「これが起こると出社できる従業員が50%超えない、となれば生産体制をシフトしていく」というように、すべて通常業務にインパクトを落とし込む発想はインフルエンザもサイバーも同じです。振り返りの際に、「社長、あと30分判断が早くなっていれば、もっとこうなっていました」と言って学習していくことも重要ですね。

5. 日本を強靭化するためにはセキュリティ技術の国産自給率の向上が必要

細井　サイバー攻撃に企業1社で対応するのは難しいと

のことでしたが、共助の重要性とか、日本を強靭化することを考えていくために何を考えればよいでしょうか？我々が普段から取り組めること、サイバーセキュリティ演習で取り込んでいくべきこと、留意していくべきことはどんなことでしょうか？

太田　先ほど国産技術と言いましたが、モノを作れるということは、そこに技術者が存在するということです。技術者はモノを作るだけでなく、フォレンジックもできる人に変われる能力を持っている。でも日本には国産技術を育成するプログラムはない。例えば、国家安全保障の観点で独自にサイバー空間を守るものを開発していない。米国ではベンダーと開発し、それを運用する人が軍を退役して民間企業に戻り、オペレーションを手伝い、意思決定のための人材として人材マーケットを回る。この官と民が人材を回していく仕組みが日本にはない。米国で作られたものが日本に輸入されています。セキュリティビジネスは年率7%で伸びていると言いますが、伸びてはいけない世界だと思います。ICTの運用費用は今の低い経済成長率では増やせないし、そこにサイバー投資が割って入ると景気は悪くなる一方です。だからICTの投資範囲で実現しなければならない。となると、高い技術を自分たちで創り出さず他国にすべて頼るのは間違っている。

細井　太田さんはセキュリティ技術の国産自給率の向上と表現されていますね。

太田　政府にも働きかけていますが、総務省の研究外郭団体のNICT（National Institute of Information and Communications Technology; 情報通信研究機構）がダークネット(注5)の監視や研究等において海外製品でテストベッドを作り評価しています。その活動の中で、何らかのコアがないと技術者が育たないという課題認識は一致しているので、協力をお願いしています。

三浦　大企業ではそれなりのセキュリティ体制がとられていますが、中小企業を含めた全体の底上げが必要だと思います。中小企業が踏み台にされるケースも多く、サイバー攻撃は弱い所が狙われます。企業単体で弱い所、日本全体で弱い所が狙われています。中小企業でもセキュリティに関する情報を集めやすいとか、サイバー演習をバーチャルで受けられるといったことが現実にならないと、日本全体としてセキュリティのレベルは上がらないと思います。

太田　技術的な側面や、運用で誰に頼るかは、サービスで補完するしかないと思います。自社のリスクを経営者が捉えて、それに対処するリソースに限りがあるなら外部に頼るべきです。頼るべき領域が分かり、そのリソースをどこに頼もうと気づける演習もある。しかし、やはり日本にセキュリティの産業がないと思います。セキュリティ自給率を高める必要がある。

渡辺　個別の中小企業は人も金もないので、ある程度外部の専門サービスに監視をしてもらうことです。これは横軸を通して監視することになりますので、特定の産業や特定のツールを使っている企業群の攻撃が捕捉できるようになるため、補助金を出すことなど、割り切りが必要でしょう。英国の金融機関の決済系ネットワークも、大きな銀行は各々やっているけど、それ以下の銀行は当局が外部サービスを入れさせて監視し、同時多発的な攻撃やタッピングの段階から横軸で捕捉して、攻撃者をある程度特定し、攻撃目的を交渉するとかやっています。ネットワークやシステムが全部つながっていて脆弱性が高い部分から攻撃されるため、横にサービスを入れて網を張るしかないので、ある程度国が支援すべきでしょう。

太田　それを富士通がやると提案してもいいですか？逆に、横軸で監視するサービスが国のためにレピュテーションを集める。アメリカは民間企業が情報を集めてレピュテーション情報として売買しています。それが国家レベルで集められるというのは国の強靭化という

面では非常に意味があります。

渡辺　中小企業は必ずプロバイダーを選んでいるので、プロバイダー同士が情報を集める共同センターを作っていくというやり方もありますね。

6. セキュリティレジリエンス人材育成は次世代経営者の育成そのもの

細井　人材の底上げに関連して、検知段階や通信監視ではAIの活用や、先ほどの行動分析など、ITでの対応領域が広いですが、その後工程を担う人材が重要ということです。オリンピックも絡めて国レベルの強靭化を加速するには、どのように人材育成していけばよいでしょうか？

細井　和宏（ほそい　かずひろ）
株式会社富士通総研　執行役員　ビジネスレジリエンス事業部長
1983年 富士通株式会社入社以来、電力・製造業のSEとしてプロマネを実践。06年から株式会社富士通総研でビジネスコンサルティングを開始。海外駐在経験も活かし、製造業のお客様を中心とした経営戦略立案、業務プロセス革新、グローバルERP戦略策定などを深耕。 直近ではワークスタイル変革、IoT、事業継続マネジメント、CSIRT構築などに注力し、お客様の経営・業務課題解決に携わっている。

渡辺　報告を躊躇しないということと、報告したことに対してアプリシエイトすることが重要です。エスカレーションすることを推奨し、それがネガティブなことにつながったとしても、あなたには責任ありませんと言う。これは普通の危機管理でもやられていることです。上がってくる流れを作っておかないと、見えるものも見えない。例えば「あなたはあのとき、この兆候を見逃しましたね」、「気づいたのに報告しませんでしたね」といった感じで、報告しなかったことによる影響が出る演習を組むのもよいと思います。エスカレーションを是とする演習です。サイバーの事例ではないですが、ある企業で中堅社員を集めて生産や供給や企画のチームを作り、1年くらいかけて様々に連鎖するシナリオを考えました。すると、各々の業務を学んでいきますし、違う業務の中堅が集まる会議なので次世代の経営陣を育てることになる。「渡辺さん、これは演習も大事だけども、次の経営陣を育てるためのネットワークだから、当日はどうでもいいけど、それまでのプロセスを大事にしてくれ」と、そこの会長からも言われました。

太田　会社の風土を作り替えるという意味では、企業の危機管理能力は企業の底力であり、平時にもその危機管理能力は発揮できる。その部分がこれから市場で試されると、もっと活性化するかと思います。

渡辺　ドリルは手順を体で覚えるという面では必要ですが、それだけではダメです。事業継続と称して手順を確認する訓練だけをやっていると、その手順が本番で足枷になるケースがあります。ステップ1の次にステップ2とやるとスキップできないのです。

三浦　各手法には検証目的があるので、作った手順がきちんと実行できることを目的とした訓練も大事ですが、想定外の事象に対応できるかを検証する訓練も重要です。目的に応じていくつかあるパターンの訓練や演習を織り交ぜてやるのが一番よいかと思います。

渡辺　現業の人たちが自分の業務を持ち寄って、社内の相互連鎖を見て、何が起きるとどうなるかというインパクトを想像していく。それが中堅から経営陣に上がっていくのが条件ですね。

細井　ビジネスレジリエンスもセキュリティレジリエ

ンスも、「いざ鎌倉」状態から臨機応変に判断をしていくことが求められます。しかし、有事の際には考える能力が低下し、最悪の場合パニックに陥ります。役職が上がると、そういう姿を見せたくないのか、判断を間違えることが心配なのか、演習に参加されない経営者もいらっしゃいます。その状態で経営者に最終報告しても臨場感・危機感が伝わらないことが多いのですが、ご指摘のとおり、イベント当日ではなくプロセスの中で連鎖のシナリオ検討に巻き込むことで、危機管理の人材育成、次世代経営者育成として取り組んでいきたいと思います。本日はありがとうございました。

（注1）ホワイトハッカー（white hacker）：コンピュータやネットワークに関する高度な知識や技術を持つ者を指す呼び名である「ハッカー」のうち、特にその技術を善良な目的に活かす者のこと。
（注2）フォレンジック（forensic）：証跡管理。コンピュータやネットワークシステムのログや記録、状態を詳細に調査し、過去に起こったことを立証する証拠を集めること。
（注3）フラッシュクラッシュ（flash crash）：株価の瞬間的な急落。米国市場で2010年5月6日に起きた株価の急変が代表的。わずか10分ほどの間にダウ平均株価が9%の下げ幅を記録した。
（注4）センシティビティ（sensitivity）：センシティビティ分析とは分析対象の要素をパラメータ化し、ある変数の変動に対して他の変数がどのように変化するかを調べるリスクマネジメントの分析手法。
（注5）ダークネット：インターネット上で到達可能なIPアドレスのうち、特定のホストコンピュータが割り当てられていないアドレス空間のこと。

キーワード1

サイバーリスク時代のセキュリティレジリエンス

株式会社富士通総研
ビジネスレジリエンス事業部
シニアマネジングコンサルタント
藤本　健

ビジネスや行政の様々な分野で「レジリエンス」というキーワードが使われる場面が増えています。この事象は、私達が直面する環境が複雑かつ変化の激しいものであり、「組織としての適応力」が求められる時代になっていることを示唆しています。セキュリティ分野においてもICTの発達やIoTの進展に比して、サイバーリスクの脅威が年々高まり、すべてを防御するのは難しい時代に突入しています。本稿では、現在、私たちが取り組むべき「セキュリティレジリエンス」についてご紹介します。

執筆者プロフィール

藤本　健（ふじもと　たける）
株式会社富士通総研　ビジネスレジリエンス事業部　シニアマネジングコンサルタント
1996年 富士通株式会社入社後、コーポレート部門を経てコンサルティング部門に異動、2007年より株式会社富士通総研。主な専門は、リスクマネジメント、ITガバナンス、環境・エネルギーなど。近年はICT部門の電力・ガスシステム改革対応のほか、サイバーセキュリティ経営に関するコンサルティングに従事。

1. セキュリティレジリエンスとは

ビジネスや行政の分野で「レジリエンス」という用語が広く使われるようになったのはWEF(注1)の「グローバルリスク2013」が契機です。この報告書により日本でも内閣府の国土強靭化の取り組みが始まっています。その一方で「レジリエンス」の定義は使われる分野によっても異なるため、共通言語として扱うレベルまで一般的には浸透していないのが現状です。そのような中でISO22300における「レジリエンス」の定義は「複雑かつ変化する環境下での組織の適応能力」と訳すことができます。

「レジリエンス」という用語の浸透の時間軸と同期して、セキュリティ分野では、サイバーリスクの脅威が経営課題として認識され始めています。ビジネスにおけるICTの利活用・依存の進展に伴い、サイバーリスクの多様性・複雑性が増し、実際に企業、行政いずれの組織においてもインシデント発生件数、損害額が年々増加しているのです。それだけでなく、サイバー攻撃の攻撃者も「愉快犯」から「営利犯」や「テロリスト」へと変貌するのに伴い、攻撃手法もAPT(注2)などのように高度化し、完全な防御が困難な時代になってきています。

このように現在のセキュリティのトレンドは、インシデント発生前提の考え方に基づき、想定外の事態や動的な状況変化に適応できる組織としての能力が求められるようになってきました。いわゆる「セキュリティレジリエンス」の構築です。セキュリティレジリエンスの構築として、金融や通信、電力などの重要インフラ事業者を中心に現在取り組みが盛んになっているのが、サイバーインシデントへの対応力の強化であり、CSIRT(サイバーインシデント対応チーム)の整備です。

2. サイバーインシデント対応の要諦

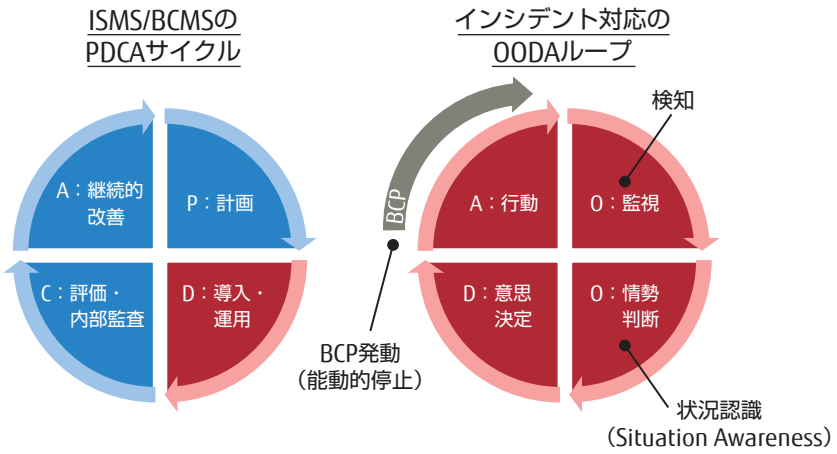
従来のBCP/ICT-BCPでは、インシデント対応チームのミッション(例えば、災害対策本部など)は早期復旧でしたが、サイバーインシデントの場合は、迅速かつ適切な初動対応による被害拡大抑制(ダメージコントロール)と顧客や監督官庁とのコミュニケーション、広報部門・法務部門と連携しながらの危機時のIR対応(レピュテーションマネジメント)が加わります。このダメージコントロールとレピュテーションマネジメントにおいて、インシデント対応チームは、収集した断片的かつ不確実な情報に基づいて、経営者の意思決定の材料となり得るインテリジェンスを組み立てて、迅速なエスカレーションをすることが求められます。

このインシデント対応では、「動的な状況変化の監視と不確実な情報に基づく情勢判断、迅速な意思決定のサイクル」をリアルタイムでループさせるOODAループ(Observe(監視)－Orient(情勢判断)－Decide(意思決定)－Act(行動))の確立が不可欠です。OODAループは、リアルタイムの意思決定を行うモデルとしてアメリカ空軍で理論化されたモデルですが、将来予測が困難な近年のビジネスシーンにおいても取り入れられています。セキュリティレジリエンスの構築では、従来から取り組んでいるISMS(注3)やBCMS(注4)サイクルの中で、このインシデント対応のOODAループの訓練や演習を積み重ね、有事の適応力を高めることが肝要となってきます。(**図1**)

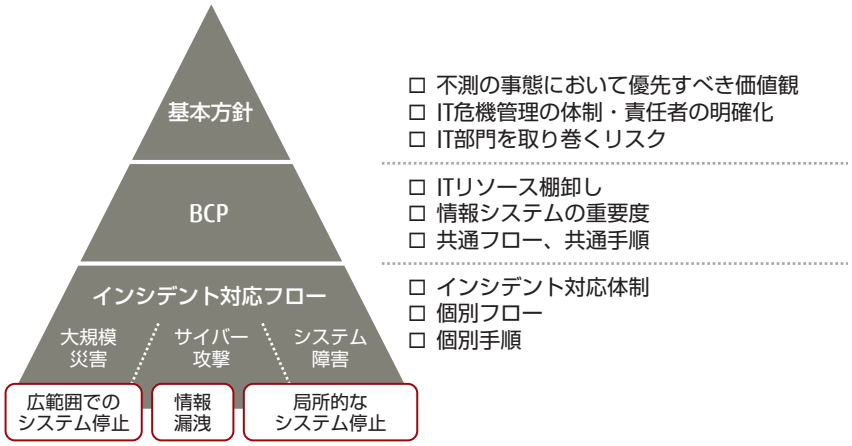
また、セキュリティレジリエンスの構築の際には、組織内に新たに作り上げるのではなく、多くの企業ですでに導入されているBCPの取り組みを補完、再構築するアプローチを富士通総研では提唱しています。(**図2**)

3. 経営としての取り組み

このようなセキュリティレジリエンスの構築は、ようやく先進的な企業においても取り組みが始まっているところですが、そこから得られるケーススタディは、いかに経営者を関与させ、経営課題として位置づけられるかです。今年に入ってからもサイバー攻撃の被害がメディアで取り沙汰されていますが、それでも多くの組織において経営者の危機感はまだまだ希薄と言えます。一方で、昨年末以降、経済産業省からは「サイバー



●図1　平時のPDCAサイクルと有事のOODAループ



●図2　BC観点のセキュリティレジリエンス構築ポイント

セキュリティ経営ガイドライン」、内閣サイバーセキュリティセンターからは「企業経営のためのサイバーセキュリティの考え方」などの指針が出され、経営者が経営課題としてサイバーセキュリティに取り組むべきという潮流になりつつあります。

では、経営者がサイバーセキュリティに取り組む際のポイントは何でしょうか？ 富士通総研では、「ビジネスインパクト」、「セキュリティガバナンス」の2つが重要であると考えます。

(1) ビジネスインパクト：経営の意思決定支援

多くの経営者にサイバーセキュリティの取り組みを聞くと、「対策は考えている/している」という言葉が返ってくるでしょう。しかし、今後求められるサイバーセキュリティの説明責任は、「自社としてのサイバーリスクを認識している」、「現時点での脆弱性を把握し、インシデント発生時のビジネスインパクトを影響展開できる」、「残存リスクが顕在化した際の戦略オプションを立てている（例えば、バックアップシステムに切り替えるのか、二次被害を抑えるために業務サービスを停止するのか）」といったことを経営者が答えられるのか？ といったことです。

(2) セキュリティガバナンス：現場と経営の橋渡し

次に必要となるのは、CISOなどの経営層が主体的にセキュリティリスクを管理する仕組みを構築・運用できているかということです。特に組織構造が多層化されている企業においては、「ガバナンス」と「マネジメント」を分離し、責任分界点を明確にしなければ、危機時の迅速かつ適切な意思決定は困難になるでしょう。一方で、CISOは情報システム（IT）のセキュリティだけでなく、制御システム（OT）のセキュリティも含めて全社的観点でセキュリティ投資や危機時の意思決定に取り組むことが今後求められます。

セキュリティレジリエンスの取り組みはまだ始まったばかりで、手本となるモデルがありませんが、それぞれの組織がこれまで行ってきた、セキュリティやBCPの取り組みの延長線上として位置づけ、経営者と現場の意識啓発から始めることが最初の一歩でしょう。

（注1）WEF：世界経済フォーラム（World Economic Forum）
（注2）APT：標的型攻撃の一種で、特定ターゲットに対して持続的に攻撃・潜伏を行い、様々な手法を駆使して執拗なスパイ行為や妨害行為などを行うタイプの攻撃の総称（Advanced Persistent Threat）
（注3）ISMS：情報セキュリティマネジメントシステム
（注4）BCMS：事業継続マネジメントシステム

キーワード 2

平時からの事業継続能力を高める演習起点のESAサイクル

株式会社富士通総研
ビジネスレジリエンス事業部
プリンシパルコンサルタント
浅野　裕美

東日本大震災では、想定外の結果事象への対応が不十分であり、柔軟な対応実現の課題が浮き彫りとなりました。被災時対応において、想定外の事象にも「迅速」かつ「柔軟」に重要業務を継続できる対応能力（＝有事の実効性）が、事業継続マネジメント（BCM）として求められています。被災時の初動においては、実際に対応を行うメンバーが、被災時に起こり得る事象や状況イメージを共有し、自らの役割を理解しておくことが前提となります。

執筆者プロフィール

浅野　裕美（あさの　ゆみ）
株式会社富士通総研　ビジネスレジリエンス事業部　プリンシパルコンサルタント
1990年 富士通株式会社入社、アウトソーシングサービス事業の企画業務を経て、2005年から富士通グループの事業継続マネジメント（BCM）構築を担当。2008年度より株式会社富士通総研において、BCMコンサルティングに従事。2010年4月開設の「BCM訓練センター」副センター長として、様々な業種における危機対応能力強化と、BCMの普及啓発に従事。NPO法人事業継続推進機構理事。

1. 計画ありきの「訓練」から人の対応能力を高める「演習」へ

従来の「訓練」の目的は、策定した計画（BCP）どおりに行動するための準備を行うことでした。BCMのマネジメントサイクルでは、事業継続計画を作り（P）、事前対策を実施（D）、計画どおりに動けるかを訓練で試し（C）、評価改善（A）を行う流れで、平時の運用に取り組んでいました。この方式では「人」が、作成された「計画」に合わせる形となります。その訓練手法は、想定した状況をシナリオに落とし込み、予定調和型で読み合わせを行うものが主流でした。決められた手順に習熟することや、発生可能性の高い想定内の状況への対応を試す場合は、従来の訓練でも対応が可能です。しかしながら、計画ありきのこの訓練形式では、あらかじめ決められた事象の体験が主軸であるため、想定外の事象への柔軟な対応能力を高めることは困難です。

そこで富士通総研では対応能力の強化を目的として「模擬演習」形式の取り組みを進めてきました。「演習」の目的は、迅速かつ柔軟に重要業務を継続するための対応能力を試し、課題を抽出することです。有効な課題を抽出するためのポイントは、起こり得る状況を「被害想定（インフラ被害）」「事業継続の阻害要因（重要リソースの枯渇等）」「意思決定（判断が必要な事象）」といった構成要素を踏まえたうえで、リアリティのあるシナリオ設計をすることです。同時に、求められる想定時間までに重要業務の復旧を行う「時間軸」の考慮も重要です。模擬演習は、参加者には事前にシナリオ内容を開示しないスタイル（シナリオ非提示型）で進めます。被災時さながらにその場で情報・状況を把握しながら、様々な判断を行います。様々な状況をリアルにイメージしながら、組織の危機対応能力を見える化し、対応への想像力・判断力を養うことで、人・組織の想定外への対応能力を強化することができます。

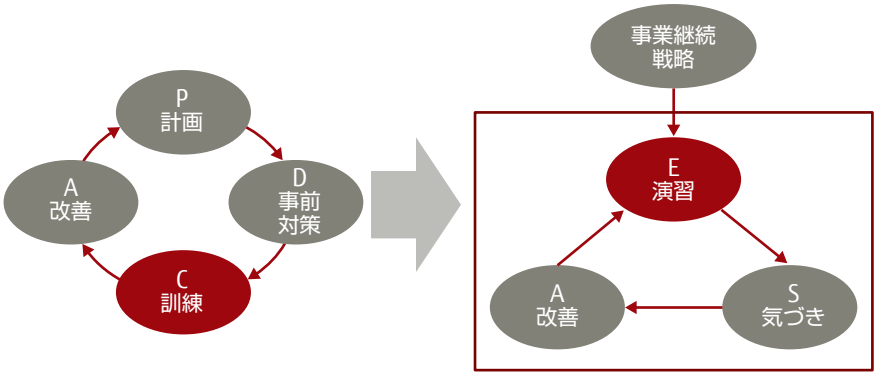
すなわち、対応能力強化を重視したBCMサイクルでは、従来の計画における手順やプロセスを確認するPDCAサイクルではなく、演習（Exercise）から気づき（Sense）、改善（Action）に着手するプロセス「ESAサイクル」が重要と考えています。有事、平時にかかわらず速いスピードでの環境変化への迅速な対応を行うには、ESAサイクルによるプロセスマネジメントが有効です。（**図**）

すでに様々な分野において、演習を気づきの起点としたBCMの取り組みが行われ、評価され始めています。

2. 演習を起点とした取り組みの事例

（1）石油業界における実効性の高い演習と評価の仕組み

石油業界ではインフラ企業としての強い使命感を背景に、官民が一体となって、災害時の迅速な石油供給を実現する取り組みの実効性を高めることが課題でした。災害時には資源エネルギー庁と協調し、石油連盟共同オペレーションルームを経由して、元売各社連携によ



●図　BCMはPDCAサイクルからESAサイクルへ

る速やかな石油供給がなされる仕組みの強化に取り組まれています。災害時のオペレーションシステムを迅速に機能させるためには、具体的な供給再開目標を関係者が理解し、その達成に向けた模擬演習が不可欠です。BCPで体制やルールを設定していても、有事のリアルな状況や脆弱性課題を反映したシナリオを検討し、シナリオ非提示型の模擬演習で試しておかないと、迅速かつ柔軟な対応を実現することはできないからです。

BCPによって具体的な供給再開目標時間とレベルを設定し、様々な被災想定シナリオに基づく演習を行い、想定時間内での供給達成を検証し、有識者が第三者的に格付け評価をしています。このような演習起点の評価制度を導入することにより、平時から元売各社のモチベーションを維持しています。そして想定外の事象にも「迅速」かつ「柔軟」に供給継続できる対応能力を高めるための改善活動につなげています。先般発生した熊本地震の際には、素早くBCPを発動し、迅速な供給再開を実現されました。

(2) 演習を起点としたBCP策定で地域強靭化に取り組む

岐阜県・商工政策課では2015年からの3ヵ年事業として「岐阜県BCP研修・訓練センター」を設置され、県下の企業のBCP策定を推進されています。ここでも模擬演習を起点としたBCP策定への取り組みがポイントです。様々な被災状況をリアルにイメージしたうえで、各社の戦略に則って決められた重要業務を迅速に継続するための計画づくりを実践し、有事の実効性を高めようとしています。岐阜県下では製造業を中心に2年ですでに約200社がBCPを策定・改訂しています。

この活動は、全国的にも岐阜モデルとして注目を集めています。県下企業が、業界団体であるNPO法人事業継続推進機構のアワードを受賞しています。また2016年4月にスタートした、事業継続に積極的に取り組む企業を認証するレジリエンス認証において、東京に続き全国で最も多い4社が認証を取得しています。県下企業が、災害をはじめとする様々な環境変化に対して柔軟に対応していくしなやかな強さを持つことで、エリア全体での産業競争力強化につなげていくことを目指しています。

3. 変化に柔軟に対応できる組織対応能力の獲得へ

BCPを作り想定内の訓練を繰り返すという従来の活動方式では、組織内の活動意欲を維持しにくく、また訓練を行うことが目的化（イベント化）するケースも散見されました。模擬演習により、常に想定外を経験することで、組織構成員の想像力を刺激し活動への取り組み意欲を向上させるとともに、平時におけるワークスタイルそのものへの気づきを与えることができます。同時に、組織構成員の対応能力を鍛えるための人材育成としても非常に有効です。ここに共感されて、マネージャー向けの人材育成メニューに位置づける企業も増えつつあります。

グローバル化の進展によりサプライチェーンをはじめとした事業の相互依存性が複雑化する中、経営環境を取り巻くリスクは、自然災害やコンプライアンスリスク以外にも取引先の倒産、原材料の高騰、為替の変動など、日々山積し拡大しています。経営環境が激変する中で、変化に柔軟に対応できる人材を育成し、自らの組織の変革を促すことで、真の事業継続戦略の果実として企業の持続的な成長を実現していくことが可能となります。

ケーススタディ 1

サイバーセキュリティを推進するグループガバナンスの再構築

サイバーリスクの脅威が年々増す一方、完全な防御が困難であることが認識される中で、インシデント前提の考え方に基づいた危機対応能力の強化が公共部門、民間部門を問わずに求められている。このような環境変化を背景にCSIRT（インシデント対応チーム）の立ち上げが重要インフラ事業者を中心に進んでいる。

サイバーセキュリティを巡るこのような潮流の中、重要インフラ事業者でもあるA社様は、サイバーインシデントへの対応体制の構築と並行して、グループ全体のセキュリティガバナンスを再構築された。本稿では、サイバーリスクに対応するための、セキュリティガバナンスモデル再構築のコンサルティングについて紹介する。

執筆者プロフィール

藤本　健（ふじもと　たける）

株式会社富士通総研　ビジネスレジリエンス事業部　シニアマネジングコンサルタント

1996年 富士通株式会社入社後、コーポレート部門を経てコンサルティング部門に異動、2007年より株式会社富士通総研。主な専門は、リスクマネジメント、ITガバナンス、環境・エネルギーなど。近年はICT部門の電力・ガスシステム改革対応のほか、サイバーセキュリティ経営に関するコンサルティングに従事。

三浦　良介（みうら　りょうすけ）

株式会社富士通総研　ビジネスレジリエンス事業部　チーフシニアコンサルタント

2002年 株式会社富士通ビー・エス・シー入社以来、公共分野におけるインフラ構築から運用・保守設計を実施。2005年から富士通株式会社にて個人情報保護および情報セキュリティに関するマネジメントシステム構築および認証取得を多種多様な業種で実施。2007年から株式会社富士通総研にて情報セキュリティに加え、ITガバナンスやリスクマネジメント分野のコンサルティングを実施。直近ではサイバーセキュリティ関連コンサルティング（サイバー演習、CSIRT構築等）に携わっている。

1. 従来のセキュリティガバナンスの限界

■インシデント発生前提の考え方

ビジネスにおけるICTの利活用の進展や依存度の高まりに伴い、サイバーリスクの脅威は年々高度化・複雑化しており、サイバーセキュリティの対応はビジネスにおける最重要課題の１つになりつつある。サイバーセキュリティにおけるレジリエンス力の要諦は「防御・検知・対応」だが、近年では「防御の困難性」を前提としたレジリエンス力の向上、具体的には「サイバーインシデントへの対処体制」の見直しが不可欠と認識されるようになった。求められるのは、サイバー攻撃によるビジネスへの影響の大きさを認識し、想定外の事態や動的な状況変化に適応できる組織能力を平時より備えておくことである。（**図1**）

■従来のセキュリティガバナンス

従来の情報セキュリティの取り組みは、PCの紛失や操作ミスなどの人為的偶発的脅威に対する規程整備や従業員教育などによる人的対策、ロッカー施錠や入退管理などの物理的対策を現場部門に徹底させる「防御」に重点を置き、それらの取り組みを組織全体に浸透、定着させるためのPDCAサイクル、いわゆるISMS（情報セキュリティマネジメントシステム）として運用されてきた。

事前にすべてを完全に防御すること（完璧主義）は重要であるが困難であることを認識したうえで、リスクを考慮した社会意識、社会行動へ転換すること、また、このようなサイバー攻撃に迅速に対応できるよう、対処体制を抜本的に見直すことが必要

出所：「総務省における情報セキュリティ政策の推進に関する提言」H25.4.5

セキュリティレジリエンスとは…

サイバー攻撃等に対する防御の困難性と影響の大きさを認識のうえ、インシデント発生前提の考え方に基づき、想定外の事態、動的な状況変化に適応できる組織能力

●図1　富士通総研の考えるセキュリティレジリエンス

このISMSは、一般的には年1回のモニタリングにより点検・改善するサイクルである。また、グループを構成する子会社に対しても親会社のセキュリティ監査チームが年1回程度のサイクルで定型的なチェック項目について点検・改善指導を行うのが多くの会社で採られる方法である。

A社様においても同様であり、グループ全体を対象とした「Aグループ情報セキュリティ方針」を制定し、本体の各部門とグループ子会社各社に対してそれぞれ年1回のチェックシートを用いたモニタリングを実施されていた。また、同時にAグループの情報システム子会社がファイアーウォールや侵入検知、ウイルス対策、認証システムなど技術的対策をAグループの共通ネットワーク基盤の運用業務の1業務として担い、「防御」という観点では、グループ全体の水準の維持と運用により、グループ全体のセキュリティレベル向上を進めてこられた。

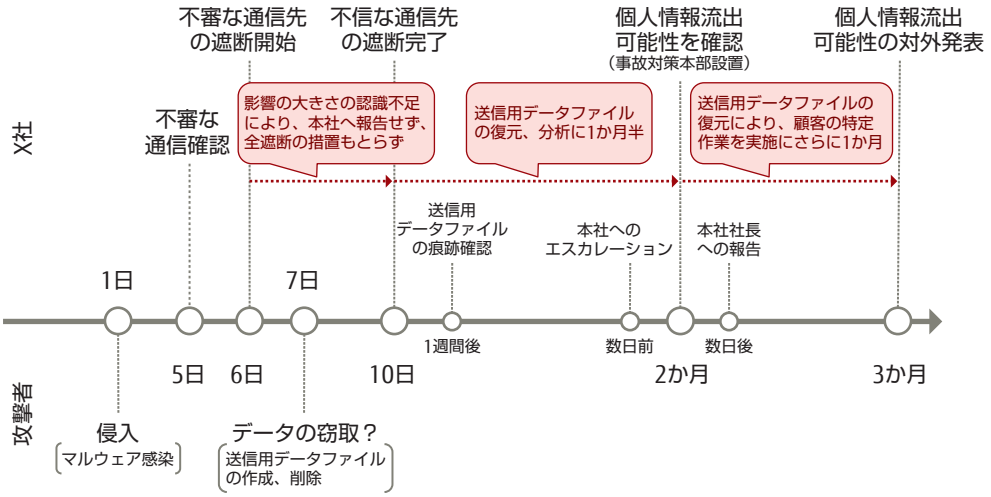
しかし、このような従来の情報セキュリティのガバナンスモデルでは「サイバーインシデントへの対応」に際しては有効に機能しないことが明らかになってきており、これは最近メディアでも取り沙汰されているX社事案からも学ぶことができる。

■最近の事案から学ぶこと（X社における標的型攻撃による個人情報流出）

今年6月に公表されたX社における標的型攻撃の事案について、「サイバーインシデントの対処体制」の観点より考察する。

この事案では、サイバー攻撃者の侵入（マルウェア感染）後から5日目という比較的短期間で不審な通信を確認し、X社の情報システム子会社が外部ベンダーと対応の協議を始めており、「検知」という観点では、迅速な動きであったと評価されている。一方で、その後のインシデント対応が後手に回り、企業ブランドを傷つける事態となっている。（**図2**）

X社では、グループCSIRTと情シス子会社CSIRTを設置していたが、各CSIRT間もしくはグループCSIRTと全社的な危機管理チームとの間での役割分担・連携/エスカレー



●図2　X社事案におけるインシデント対応のタイムライン

ションルールが定まっておらず、担当役員へのエスカレーションに2か月、外部公表まで、実に3か月を要している。この事案におけるインシデント対応の問題点は以下の3つであることが伺える。

(1) グループCSIRTと子会社CSIRTの連携、役割分担
(2) 顧客や監督官庁へのリスクコミュニケーション態勢
(3) 意思決定のためのエスカレーション態勢

前述のとおり、従来の「防御」としての情報セキュリティでは、PDCAを年間サイクルで運用することで問題はなかったが、ひとたびサイバー攻撃によりインシデントが発生すると、時々刻々と変化する状況下で、情報収集・分析、意思決定の繰り返しが必要となるが、従来の態勢では機能しないことが露わになった。このような従来のセキュリティガバナンスの課題をA社様も認識され、サイバーリスクに対応するためのセキュリティガバナンスモデルの再構築に取り組まれる契機となった。

2. サイバーリスクに対応するための セキュリティガバナンス

■ サイバーリスクへの対応

サイバーリスクは前述のとおり、インシデント発生を前提に考える必要があるが、その際にインシデント対応チーム（いわゆるCSIRT）が担うミッションは、被害拡大の抑制（ダメージコントロール）と風評被害の抑制（レピュテーションマネジメント）である。被害拡大や風評被害の抑制に際しては、原因特定と被害状況把握のための情報収集、分析等が必要となるが、これらの一連の役割は一般的に企業グループの中で以下のように分担されている場合が多い。

- 危機事象への対応
  - 対策本部…総務部門/危機管理部門
  - 危機広報…広報部門、法務部門
- 情報セキュリティ事故…情報システム部門基盤担当グループ
- ネットワークの監視…情報システム子会社/ICTベンダー

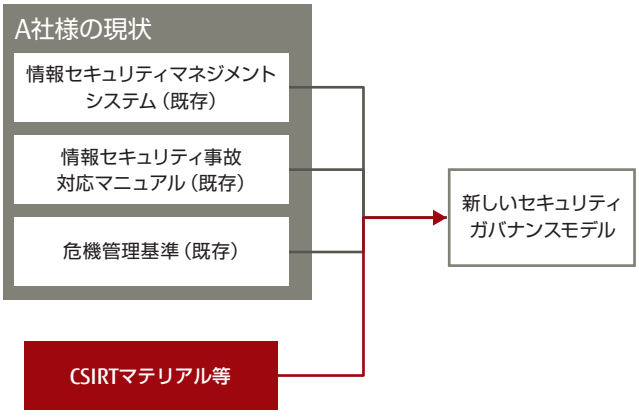
A社様でも従前より危機管理への体制は総務部門が主導し、危機レベルに応じて現場部門内に対策本部を立ち上げる体制となっており、さらにその中でも情報セキュリティに関する事案については情報システム部門が主体となる、といった体制が整備されていた。しかし、このケースでの情報セキュリティに関する事案は主にPC等の紛失や盗難などであり、高度なサイバー攻撃は想定されていなかった。したがって、ネットワークを

監視している情報システム子会社やICTベンダーとの連携が想定されていないほか、システムやネットワークの能動的な停止などの意思決定に係る取り決めは未整備であった。

■ セキュリティガバナンスモデルの再構築（組織内CSIRTの機能配置）

再構築の支援に際して富士通総研では、まずA社様における既存の取り組みを把握、整理しながらグループ全体として実装すべきCSIRT機能を抽出したうえで、その役割をどの部門が担うべきかの議論をA社様と行うといった段階的な検討により進めた。この際、特に論点となったのは、「ガバナンスの強度」である。従来のセキュリティガバナンスでは、グループ会社に対しては、比較的緩いケース（自立的取り組みを促すための支援やモニタリングを中心に実施）が多く見受けられたが、サイバーリスクに関しては特定のグループ子会社における脅威がグループ全体に影響を及ぼしかねないことまでを考慮し、より強固なガバナンスモデル（早期の親会社へのエスカレーション体制など）の構築を志向した。（**図3**）

一般論として、グループ子会社を複数擁する企業グループの場合は階層型の組織内CSIRTの整備が想定されるため、グループ内に配置する各CSIRTのサービススコープの整理（責任範囲の明確化）が必要となる。A社様においても「対象部門」×「対象システム」の“面のスコープ”に「危機レベル」を加えたマトリクスにより、責任分界点を明確化することで、危機時の迅速かつ適切な意思決定が行える体制を整備した。



●図3　セキュリティガバナンスモデルの再構築

このような組織内CSIRTに関しては、JPCERT/CCから発行されている「CSIRTマテリアル」などのガイダンスが多く出ているが、企業グループ全体のセキュリティガバナンスの再構築は、これまでの情報セキュリティや危機管理の取り組みなど、個社固有の状況も踏まえたうえで、検討・整備することが肝要である。

3. 演習を通じたサイバーセキュリティの実効性向上

■ 今後取り組むべき2つの課題

ここまで企業グループにおけるセキュリティガバナンスモデルの再構築について紹介してきたが、今後のサイバーセキュリティへの取り組みについては、2つの課題が挙げられる。

1つ目は、サイバーリスクによる事業インパクトの展開である。自社にどのようなサイバーリスクが潜在的にあり、顕在化したときの自社事業への影響がどの程度あるのかをあらかじめ把握したうえでの、インシデント対応における意思決定が求められる。富士通総研ではサイバーインシデント対応の模擬演習を定期的に実施しているが、情報システム部門のメンバーだけで演習を行うと、多くの場合システムやネットワークの停止判断になってしまう。しかし、実際の意思決定は事業を担う主管部との協議が不可欠である。X社事案においても検知後の原因追及や影響調査は速やかに行われていたが、意思決定については取り決めがなかったため、ネットワーク停止のタイミングを逸している。

2つ目は、グループ内に擁する情報システム子会社やICTベンダーとの平時からのサイバーセキュリティ推進体制の整備である。

多くの組織では、情報システム子会社やICTベンダーは運用委託業務の1業務として、監視業務やログ収集等を委託しており、危機管理としての認識が十分でないケー

スが多い。例えば、同一グループ内の親会社と子会社が個別に運用業務を委託する場合、ログ収集の頻度・方法にもバラツキがあり、インシデント発生時に原因特定ができなかったり、時間を要したりということも起こっている。したがって、子会社のネットワーク監視がどのように行われているかまで親会社は統制をかけることが今後必要となる。

■ サイバーセキュリティ分野における富士通総研の取り組み

サイバーセキュリティに関する課題抽出や対策の検討方法として、富士通総研では事業継続コンサルティングで培った演習ノウハウを適用している。特にサイバー演習では、富士通グループで蓄積してきた最新の攻撃動向もシナリオに反映することで、お客様のセキュリティレジリエンス向上に努めている。

また、制御系システムを持つ企業では、これまでは全く管轄外であった制御系システムのサイバーセキュリティについても一定のガバナンスが必要となってくる。近年の制御系では、Windowsなどの汎用系OSの採用もあり、それらの脆弱性についてはCSIRTが情報系と併せて管理するだけでなく、全社的観点でのセキュリティ投資や危機時の意思決定の取り組みも含めた新たなセキュリティガバナンスの中で管理することが必要になる。特にIoTの活用が進めば進むほど、サイバーリスクを想定した企業グループ全体、さらにはサプライチェーンまで俯瞰したセキュリティガバナンスモデルの再構築が求められる。

富士通総研では、ICTを安心して利活用いただけるよう、今後もお客様のサイバーセキュリティの取り組みをご支援していく。

ケーススタディ 2

サプライチェーンにおける レジリエンス強化の取り組み ―企業連携型BCPによる事業継続能力の強化事例―

株式会社富士通総研
ビジネスレジリエンス事業部
シニアマネジングコンサルタント
大谷　茂男

サプライチェーンの高度化や広域化などに伴い、自然災害やテロ・紛争、取引先倒産等によりサプライチェーンが寸断され、直接的な被害を受けない企業のビジネスにも大きな影響が生じる事例を数多く経験している。国土強靭化アクションプランでは、レジリエンスの強化対策として企業ごと・企業連携型でのBCP(注1)策定を進めているが、サプライチェーンにおけるレジリエンス強化の仕組みの確立までは至っていない。

本稿では、民間主導でサプライチェーンの強化に取り組む「佐川急便株式会社様（以下、佐川急便様）」を事例として取り上げ、企業連携型BCP等、レジリエンス強化の取り組みを解説する。

■ 執筆者プロフィール

大谷　茂男（おおたに　しげお）

株式会社富士通総研　ビジネスレジリエンス事業部　シニアマネジングコンサルタント

1998年 富士通株式会社入社、2007年 株式会社富士通総研出向。主に製造業や流通業を対象にサプライチェーンマネジメントや調達改革等の業務改革、情報戦略のコンサルティング業務に従事。東日本大震災以降は現組織にて事業継続マネジメントやサプライチェーンBCP、地域連携等のレジリエンス強化のコンサルティング業務に従事。

1. サプライチェーンを構成する生産や物流停止等における組織対応力強化の必要性

平成28年4月14日、16日に熊本で最大震度7の大規模地震（平成28年熊本地震）が発生した。この震災においても東日本大震災と同様に、被災していない企業のビジネスにもサプライチェーンの停止により影響が生じた。例えば、東海エリアの自動車下請企業では受注減による資金繰りの悪化が発生している。

企業は、世界各地で発生する自然災害やテロ・紛争などがいつどこで起こるか予測できないため、サプライチェーン寸断による不測の事態を想定して対策を検討する必要がある。とりわけ、企業内での取り組みだけでは実効性の確保が難しいため、顧客や取引先、地域でのBCP策定の重要性が高まっている。

2. 国土強靭化基本計画における指摘

昨年閣議決定された「国土強靭化基本計画」では、企業連携型BCP/BCM[(注2)]の構築促進が盛り込まれている。また、基本計画を受けた「国土強靭化アクションプラン」では、起きてはならない最悪の事態の例として、サプライチェーンの寸断等による企業の国際競争力低下も懸念されている。

一方、BCPの策定状況を見ると、大企業では60.4%が、中堅企業では29.9%が「策定済み」と回答しているが、100名以下の中小企業では1割程度にとどまっている。

大企業だけが事業継続に取り組んでも、そのサプライチェーン上には中堅・中小企業、インフラ事業者や行政も大きく関係しており、サプライチェーン上のウィークポイントの存在は事業継続のボトルネックになり得る。そのため、企業内のBCP策定に加え、サプライチェーンや地域連携型のBCP策定が急務である。

3. サプライチェーンにおけるレジリエンス強化の取り組み

レジリエンス強化の意義は、「急激な環境変化に対する組織的な危機対応力強化」にある。今後BCPの策定は進んだとしても、「被害が起きることを前提にして、回復をできるだけ早くすること」に対し、取引先や顧客、地域等を含めた企業連携型BCPの取り組み強化が重要である。

企業連携型BCPの取り組みには、市場への製品・サービスの安定供給を目的としたビジネスチェーンの観点（サプライチェーン、デマンドチェーン）と、地域復旧・復興を目的とした地域内外（地域連携、広域連携）の観点が重要であり、その観点から4つに分類した取り組みを以下に解説する。（**図**参照）

(1) サプライチェーンBCP

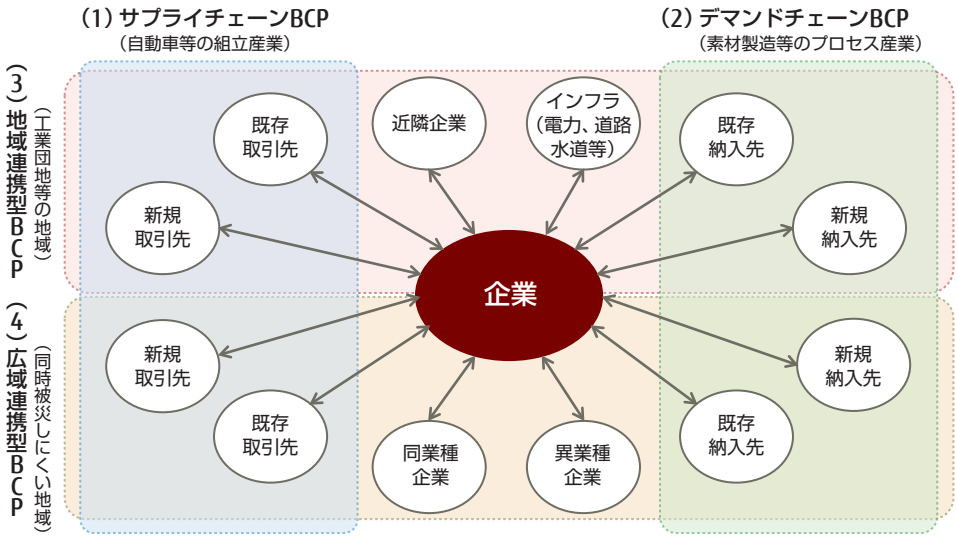
自動車や航空機産業等の組立産業では、部材の安定供給を実現するため、平時から多段階の取引先（既存・新規）の取り組み状況を可視化し、樽型構造でボトルネックとなる取引先への対策の検討と実行を促す。

(2) デマンドチェーンBCP

銅やアルミ等の素材産業では、素材の安定供給を実現するため、平時から多段階の納入先（金属加工、商社等）の構造を分析し、重要顧客が求めるニーズに対し、優先的に支援する取り組みや、供給側としての対応を検討する。

(3) 地域連携型BCP

地域の工業団地や商業施設では、広域災害による地域の経済損失の最小化のために早期復旧・復興を実現することが重要であり、電気・道路等の重要インフラ事業者との連携や、近隣企業間での情報連携等の方策を議論し、有事の際の地域連携の仕組みを検討する。



●図　企業連携型BCPの取り組み

(4) 広域連携型BCP

上述の地域連携に加え、同時被災の可能性が低い地域との連携を行うことで、被災時の代替拠点として互いに機能することを検討し、事業停止リスク最小化の対策を講じる。また、同業種・異業種との交流を通じて平時のビジネス強化にもつなげる。

本ケーススタディでは、上記4つの企業連携型BCPの取り組みの重要ポイントについて、製品の安定供給と、地域の早期復旧・復興を支える佐川急便様の事例を踏まえながら解説する。

●写真1　佐川急便様における訓練の様子

4. サプライチェーンBCP

供給側の事業継続における重要ポイントは、「マネジメントと対策実施の両面からサプライチェーン組織の評価・改善を行うこと」である。

マネジメント面では、推進体制や、BCP策定・訓練状況、業務改善等の成果を、対策実施面では、重要業務の目標復旧時間や、現状復旧時間、課題、改善状況を可視化して継続的改善を支援する。改善の進捗状況に応じて、マルチファブ化(注3)やマルチソース化、在庫保有等の代替調達も検討する。

これまでは、取引先へのアンケート等で形式的な取り組みによる点数評価が中心だったが、実効性を高めるためには取引先の行動能力(本当に早期に事業再開できるかという能力)の評価が重要である。取引先を巻き込んだシミュレーション演習や、顧客の訓練に参加して実効性を評価する等の取り組みが開始されている。

佐川急便様では、社長・役員を含めた全社対策本部のBCP検証訓練に、行政や顧客・取引先を招き、行動能力の可視化と、BCPの実効性向上のための課題解決ワークショップを共同で実施、経営トップ主導でのサプライチェーンの組織の評価・改善に取り組んでいる。

5. デマンドチェーンBCP

需要側の事業や業務の継続を考慮した重要ポイントは、「重要顧客（納入先）のニーズの可視化」である。

有事の際に優先的に対応が必要な顧客・商品、需要、流通在庫等を事前に調査し対策を検討する。重要顧客が選定できない場合は、BCPの緊急時対応計画にビジネスインパクト分析の方法論を定義する。

また、企業が直接的に被害を受けなくても、重要顧客が被災し事業停止が長期となった場合の対策も重要である。特に、特定顧客への依存度が高い場合は、顧客に代替拠点を持つようBCP策定を支援することや、ビジネスポートフォリオの見直しが重要である。

佐川急便様では、有事の際に需要が増大する行政からの緊急支援物資輸送対応のニーズを可視化し、「災害時相互連携協定」の締結や、平時からの関係構築・実効性の確認を目的とした協働訓練を行っており、自治体が運営する防災拠点備蓄基地の保管・管理の方法を具体化している。

6. 地域連携型BCP

地域の早期復旧・復興の重要ポイントは、「インフラ事業者との連携」と「民間主体での体制構築」である。

インフラ事業者との連携では、電力、道路等の被災状況を早期に把握する仕組みを工業団地等で構築することが重要である。インフラの情報は、現状把握ができても、復旧予定等の迅速な把握は困難であるため、平時からのコミュニケーションが重要である。

また、有事の際は公助機能が働きにくいため、工業団地内等の地域企業主体での体制作りが重要である。地域力、市民力、リーダーシップを発揮するため、リーダー企業を中心とした組織体制作りや、上下関係ではない横の関係構築、地域とつながる仕組み作りが重要である。

佐川急便様では、インフラ事業者や民間企業を巻き込み、BC（事業継続）[注4]活動に関する「BC企業交流会」や、

●写真2　BC交流会の様子

●写真3　佐川急便様のレジリエンス認証

地域連携の重要課題である「備蓄品の共同利・活用」や「物流と気象」、「BC教育・訓練（人材育成）」といった、テーマ別の研究会を立ち上げ、地域連携におけるリーダーシップを発揮している。

7. 広域連携型BCP

地域内での早期復旧・復興が困難な場合も想定し、「支援/受援の仕組み構築」も考える必要がある。同時被災しない地域との連携では、ビジネス拠点の代替策や、取引先の代替策に加え、強みである地域資源を活用した新規事業開発等、既存ビジネスの枠を超えた、業界や業際連携の取り組みが重要である。

広域連携型BCPを通じて、新規顧客の開拓や、新規事

業の創造等に取り組む企業も出始めている。例えば、熊本地震で被災した企業への支援を通じて、熊本地域資源を活用した首都圏や海外への販路開拓や、新規市場のニーズに対応した製品開発である。

佐川急便様は、今年8月に内閣官房国土強靭化推進室が国土強靭化貢献団体として認証する制度「レジリエンス認証」において、運輸業・郵便業として第1号の認証を取得した。 重要な社会インフラの1つである物流を担う企業として、広域地域での支援/受援の仕組み構築を全国で積極的に実施している。

8. サプライチェーンの対応力強化に向けて

サプライチェーンにおけるレジリエンス強化の取り組みは、まだ具体的なモデルが確立されていない状況ではあるが、佐川急便様をはじめとして、点から線、線から面への展開が開始されつつある。今後も、サプライチェーン寸断のリスクは回避できないため、国土強靭化計画に基づく官主導の取り組みをはじめ、佐川急便様のように民間主導での企業連携型BCPの取り組みが進んでいくと考えている。

(注1) BCP：Business Continuity Planning 事業継続計画
(注2) BCM：Business Continuity Management 事業継続マネジメント
(注3) マルチファブ化：製造工場をファブ(fabricationの略)と呼ぶことから、代替生産に着手するプロセス
(注4) BC：Business Continuity 事業継続

◆参考

- 内閣府「平成28年熊本県熊本地方を震源とする地震に係る被害状況等について」
- 内閣府防災担当「平成27年度企業の事業継続及び防災の取組に関する実態調査」
- 一般社団法人レジリエンスジャパン推進協議会ウェブサイト
  http://www.resilience-jp.org/certification/
- 佐川急便株式会社　CSRレポート
  (Corporate Social Responsibility Report)
- 佐川急便株式会社ウェブサイト
  「【佐川急便】物流業界初「レジリエンス認証」を取得(2016/08/23)」
  http://www2.sagawa-exp.co.jp/newsrelease/detail/2016/0823_1141.html

知創の杜バックナンバーご紹介

知創の杜　検 索

http://www.fujitsu.com/jp/group/fri/resources/magazine/


マガジン

富士通総研のエコノミストやコンサルタントによる、トレンド予測、提言、コンサルティング事例など情報を紹介する情報誌です。
冊子体の販売はしておりませんのでご了承下さい。

2015年

知創の杜 2015 Vol.9

地方の元気の素をつなぎ育てる
2015年12月25日発行
ダウンロード（3.22 MB）

- 【特集】
  今なぜ地方創生なのか？
  －課題と想定される方向性－
- 【フォーカス】
  どう向き合う？ 地域課題と地方創生
- 【あしたを創るキーワード】
  地域経済分析の活用による"地域が実感できる"施策の立案
- 【ケーススタディ1】
  會津 as Oneとしての価値創造に向けて
  －會津価値創造フォーラムによる地域活性化の取り組み－
- 【ケーススタディ2】
  地域の経済循環を生み出すサービスモデルの構築に向けて
  －地域エネルギー事業により内発型産業の創出を目指す米子市の挑戦－

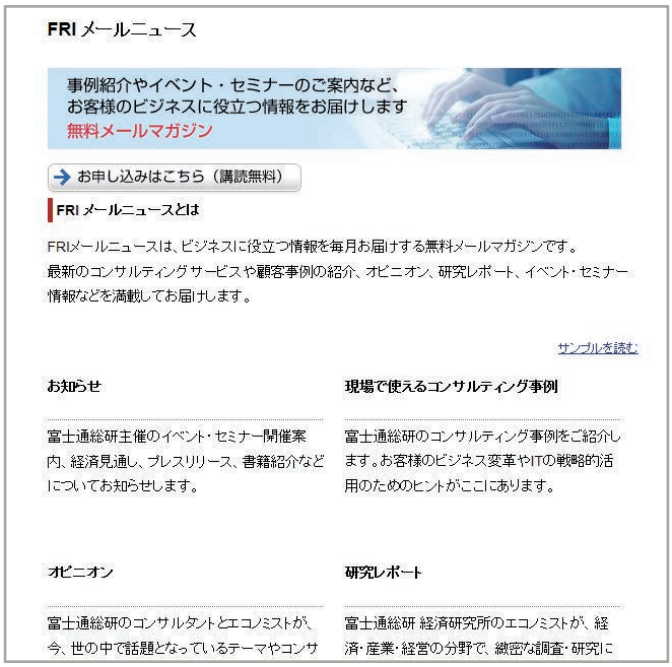
メルマガ会員登録

FRIメールニュース　検 索

http://www.fujitsu.com/jp/group/fri/resources/news/FRImailnews.html

ビジネスに役立つ情報を
毎月第1火曜日にお届けします。

- オピニオン
- 研究レポート
- コンサルティング事例
- サービス紹介
- セミナー案内


FRI メールニュース

事例紹介やイベント・セミナーのご案内など、
お客様のビジネスに役立つ情報をお届けします
無料メールマガジン

お申し込みはこちら（購読無料）

FRI メールニュースとは

FRIメールニュースは、ビジネスに役立つ情報を毎月お届けする無料メールマガジンです。
最新のコンサルティングサービスや顧客事例の紹介、オピニオン、研究レポート、イベント・セミナー情報などを満載してお届けします。

サンプルを読む

お知らせ

富士通総研主催のイベント・セミナー開催案内、経済見通し、プレスリリース、書籍紹介などについてお知らせします。

現場で使えるコンサルティング事例

富士通総研のコンサルティング事例をご紹介します。お客様のビジネス変革やITの戦略的活用のためのヒントがここにあります。

オピニオン

富士通総研のコンサルタントとエコノミストが、今、世の中で話題となっているテーマやコンサ

研究レポート

富士通総研 経済研究所のエコノミストが、経済・産業・経営の分野で、緻密な調査・研究に

www.fujitsu.com/jp/fri/

株式会社 富士通総研
FUJITSU RESEARCH INSTITUTE

〒105−0022　東京都港区海岸1丁目16番1号　ニューピア竹芝サウスタワー
TEL：(03) 5401−8391　FAX：(03) 5401−8395

通巻第24号