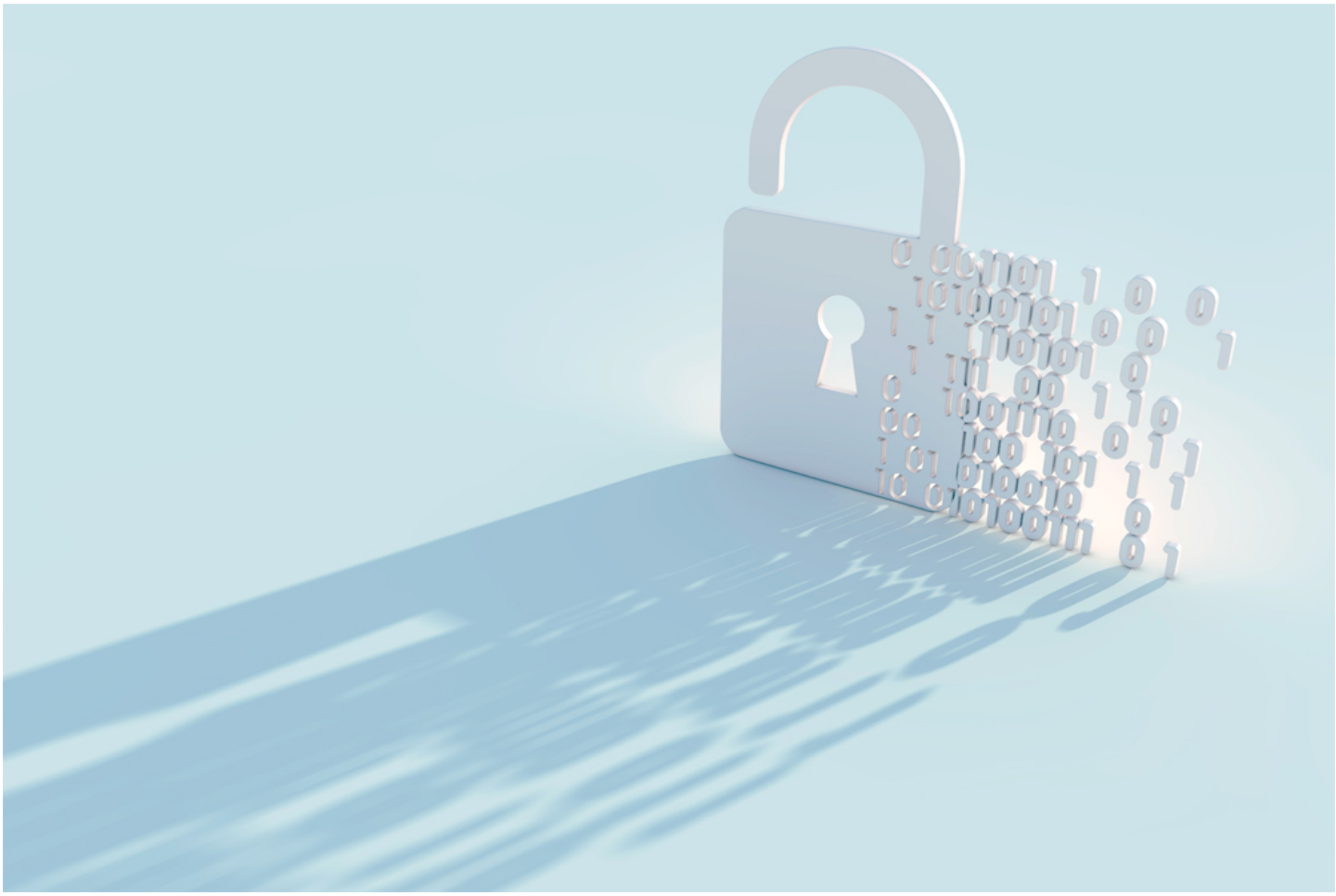
事業継続を支えるIT部門の役割とは ～セキュリティ・レジリエンス～

FUJITSU JOURNAL / 2019年1月23日



企業活動における安心・安全の取り組みは古くて新しいテーマであり、特にセキュリティ・レジリエンスは企業にとって最重要の課題です。昨今、攻撃の高度化や複雑化により完全なセキュリティ対策・防御は不可能になり、いかに早く攻撃を検知し被害拡大を局所化するか、安全に事業復旧するかという組織のレジリエンスが求められています。本対談では、「セキュリティ・レジリエンス」というテーマで、東北電力様をお招きし、富士通総研（FRI）のコンサルタントを含む5名の有識者の方に語っていただきました。（対談日：2018年2月14日）

※この記事は、富士通総研発行の情報誌「知創の杜 2018 Vol.3」（2018年5月28日発行）に掲載されたものです。

対談者（敬称略 左から）※所属・役職は対談当時のもの

三浦 良介：株式会社富士通総研 ビジネスレジリエンスグループ チーフシニアコンサルタント

山下 眞一郎：富士通株式会社 サイバーセキュリティ事業戦略本部 部長

大友 洋一：東北電力株式会社 ビジネスサポート本部情報通信部 情報セキュリティ課長

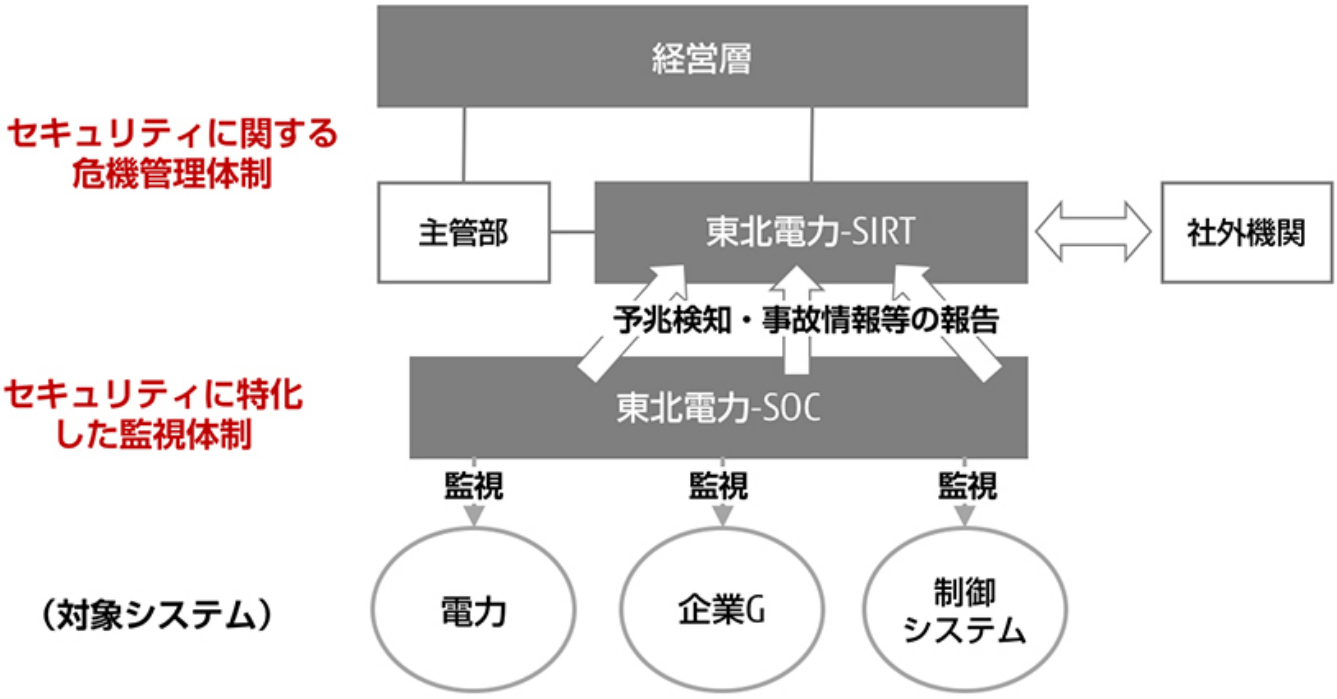
藤本 健：株式会社富士通総研 ビジネスレジリエンスグループ プリンシパルコンサルタント

細井 和宏：株式会社富士通総研 エグゼクティブコンサルタント（司会）

情報系システム・制御系システムが歩み寄って事業を守る

―事業経営とITとはますます一体化しています。事業継続を支えるためのサイバーセキュリティ、我々はこれを「セキュリティ・レジリエンス」と表現していますが、サイバー戦略という観点で、情報部門は従来よりもミッションが拡大していますね。

大友　私の今のミッションは、セキュリティの方針・計画、教育・啓発、点検・モニタリング活動、電力制御系のセキュリティ確保です。特に電力制御系のセキュリティはIT系とOT（Operational Technology：制御）系が力を合わせないと完結しないので、IT側からアプローチして関係を作りながら、共有事項を増やしてきました。セキュリティインシデントも監視するほど検知の数が増え、インシデントへの対応と監視体制の強化という両輪を回す必要があるため、SIRT（Security Incident Response Team）（注1）SOC（Security Operation Center）（注2）の機能を社内で立ち上げ、体制づくりをしてきました。また、経営層にセキュリティの有効性やリスクへの対応を理解いただいて推進する必要もあるため、「情報通信戦略委員会」という会議体を活用しながら活動を進めています。



●図1 東北電力様情報セキュリティ事故などへの対応力強化

―なぜセキュリティの「求心力」が必要だと感じられたのですか？

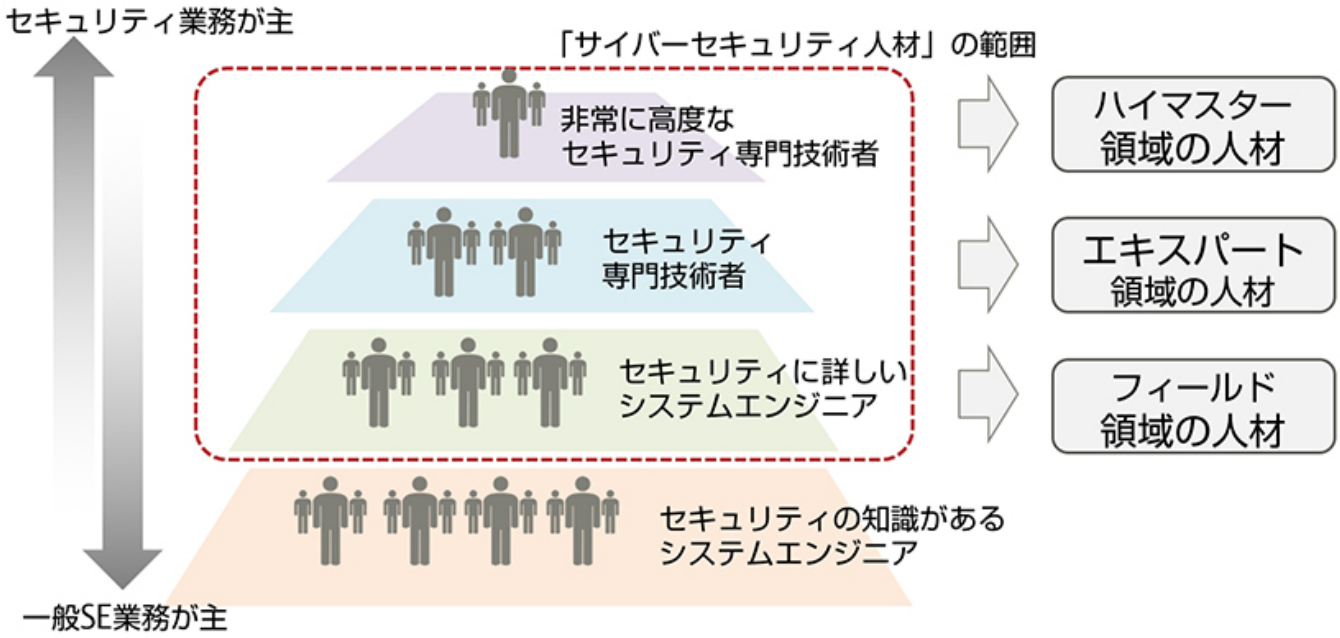
大友　今までは個人情報の保護やセキュリティのPDCAサイクルを回すのがセキュリティ担当の主なミッションでした。しかし、私が担当になった時点では、制御系の対策やサイバー攻撃への備え、リアルタイムの運用などについて十分に検討されていませんでした。それを立ち上げる課題認識だけではなく、企画段階で、何名で何をやり、どんな効果があるかを経営層に説明するまでがセキュリティ担当の業務範囲なのです。セキュリティ体制の強化によって、ICT部門の価値を高め、経営への貢献度を高められると考え、求心力を確保して、継続のレールを敷いていけるように進めたいと思いました。

―情報システム部門の枠では、OTという制御系に入りにくいと思うのですが、どのようにして巻き込まれたのですか？

大友 洋一（おおとも よういち）
東北電力株式会社 ビジネスサポート本部情報通信部
情報セキュリティ課長

大友　OTのセキュリティの取り組みにはITの基礎知識が必要ですし、逆にIT側はOTのシステムの仕組みやビジネスを知らないので、どこかで線を引いてしまうと、空白領域が生じて、大きなリスクになります。当社ではIT側から積極的にアプローチし、OT側と連携する体制を構築し、取り組みが加速しました。

山下　富士通ではお客様向けクラウドサービスを専門に集中管理する「富士通クラウドCERT」（Computer Emergency Response Team）を2010年に設置しました。そのサービスは、①脆弱性診断やモニタリングなどの情報セキュリティ運用、②万一のインシデント発生時の分析や対処などの緊急対応、③情報セキュリティマネジメントの運営、からスタートし、今ではインシデント緊急対応チームとしてのフルサービスを提供しています。多くの事象に粛々と冷静に対応しています。グローバルにセキュリティ監視をスタートして以降、今ではデジタルフォレンジックとマルウエア解析、実際に侵入してみるレッドサービスと呼ばれる脆弱性診断も実施しています。
さらに、グローバルを対象にしたCTI（Cyber Threat Intelligence）という、サイバー脅威情報収集・分析も含めてセキュリティインシデント緊急対応チームとしてのフルサービスでやっています。
今の課題は人材育成です。富士通では、NICT（National Institute of Information and Communications Technology：情報通信研究機構）が策定した人材フレームワーク（NICE）をベースにアレンジし、セキュリティスキルのあるエンジニアを認定する「セキュリティマイスター認定制度」を2013年に開始しました。人材像をフィールド、エキスパート、ハイマスターの3領域に分け、どういう教育をして何をもって認定するかを決め、グループ内の1万人を対象に推進しています（図2）。

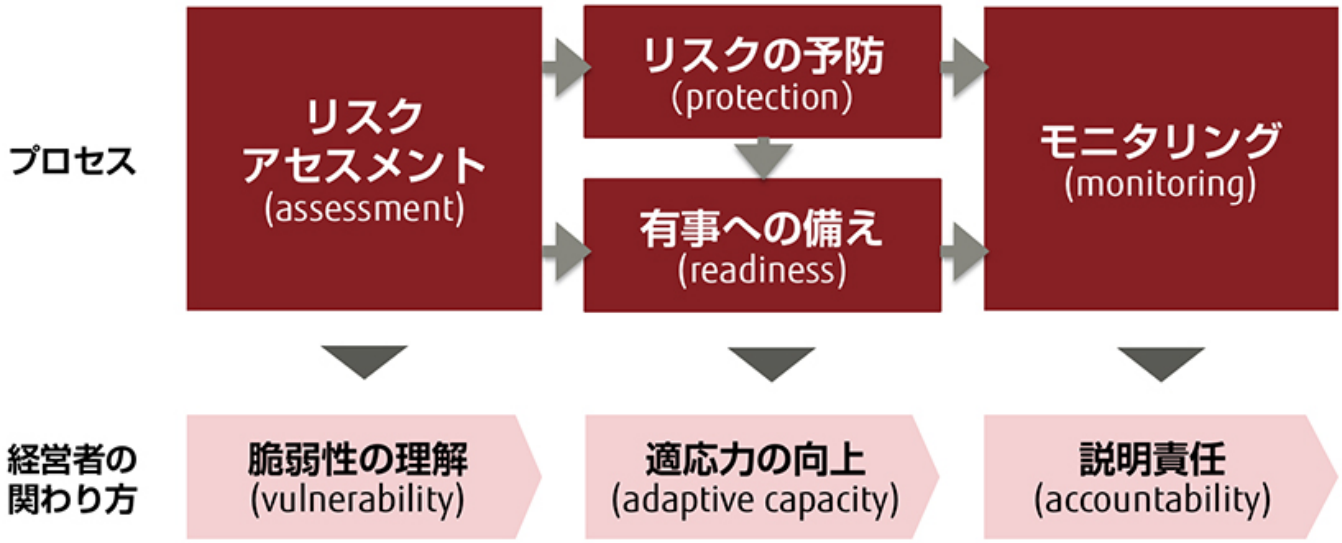


認定実績（2018年1月現在）

フィールド領域	エキスパート領域	ハイマスター領域	合計
2,554名	216名	8名	2,778名

●図2 セキュリティマイスターの人材像

藤本　FRIでは「事業継続」という、発現を前提に事業活動を早期再開する回復力、つまりレジリエンスの向上に取り組んできた背景を踏まえて、3年前から、発現前提のサイバーリスクにいかに備えるかの活動をしています。高度なサイバー攻撃の防御はもちろん大切ですが、発生前提で検知と対応という、SOCとCSIRTの組織能力を上げる、「セキュリティ・レジリエンス」という考え方です。最近注力しているのは「リスク評価」です。予防や有事への備えの必要はありますが、企業はリソースが限られる中で、すべての予防や備えは難しい。だからこそ、最初にリスク評価をして本当に予防や備えが必要なサイバーリスクは何かを特定して、優先順位づけすることが重要です（図3）。



●図3 セキュリティ・レジリエンスのプロセス

三浦　NISC（内閣サイバーセキュリティセンター）様の2つの事業をご紹介します。1つは「分野横断的演習」で、2015年より事務局ご支援に携わっています。重要インフラ13分野の事業者2,600名以上が参加したサイバー演習です。もう1つは「サイバーセキュリティ対処調整センター（注3）の環境構築に係る調査・検討」です。いずれの事業も情報共有に主眼を置いています。インシデント対応において個社での対応は限界があるため、事業者間またはセキュリティ機関等とどのように情報共有し、対応するかが課題です。また被害状況や脆弱性への対応について活発に情報共有することで、事業者のセキュリティ対策を底上げすることもできます。

組織を超えたサイバー情報共有の課題–実攻撃、ヒューマンエラー、脆弱性情報–

―セキュリティ対応は各企業で対応するのは難しく、国か業界か、団体戦で取り組まなければということですが、お客様がSOCやCSIRTを立ち上げる時、どんな課題を考えていけばよいのでしょうか？

山下 眞一郎（やました しんいちろう）
富士通株式会社 サイバーセキュリティ事業戦略本部
GMSS開発統括部 サービスデリバリ部 部長

山下　必要とされる機能と、自組織で持つべきコアスキルを明確にすることが立ち上げのポイントですが、それを明確にできないことが課題になりがちです。また、お客様自身のコアスキル以外はアウトソーシングするように、コアスキルとそうでないものを明確に見極めて育成していくのがポイントだと思います。

藤本　CSIRTの機能を最初からすべて実装するのは現実的ではなく、まずはスモールスタートで始めるべきです。東北電力様は2020年の分社化に向けて組織が大きく変わっていくので、中期的視点でどの機能をどのタイミングでCSIRTの業務機能として実装していくかという議論と、どの機能を外部にアウトソースし、どの機能を内部で持つべきかの議論もしました。

山下　グローバル展開においては、"Follow The Sun"という考え方で、世界を3拠点に分けたうえで、それぞれのビジネスアワーに合わせて8時間単位で引き継ぎしながら監視することもありますので、ここはアウトソースするけれど、経営インパクトを考慮したリスクコントロールだけは自分たちで行う、といった見極めも必要です。

―情報共有という話がありましたが、自然災害でも、支援側が受援側の要請を待たずして、タイムリーに必要なリソースを提供するにはどんな情報があればよいのかという議論があります。なぜなら、受援側は自助に一生懸命で先読みは難しいうえに、支援を求めにくいメンタリティも指摘されているからです。そのためにも、演習で被災を実体験し、有事の現場を体験することで、支援側として被災側が必要としているリソースを想像する力を養ってもらいます。

三浦　対処調整センターでも、情報共有に関するツールだけを提供しても活発な情報共有は難しいと考えています。インシデント情報は企業にとって機密情報であり、攻撃を受けている事実や被害状況は簡単に公開できません。外部に対して情報共有するためには、開示範囲をシステムで制御できる必要があります。例えば、特定の所管省庁にだけ開示するなどが考えられます。また、情報共有を後押しする法律の整備検討も重要だと考えています。

山下　情報共有は有益な情報が集まらないと使われなくなるので、いかに早く有益な情報を入れてもらうかがポイントです。1週間前の情報が来ても仕方ないので、有益な情報を入れる人のモチベーション、秘密が守られる保証、参加組織ごとの特性に応じた情報の開示レベル設定が必要かもしれません。

日々の運用まで考慮したセキュリティ設計が求められる

―最近感じられている課題、注力されているテーマはどんなことでしょうか？

大友　情報システム、制御システムと明確に括れるもの以外の、部門組織のニーズで独自に導入されたものが実は重要システムとリンクしていて、重要なお客様や制御に関わる重要度の高いものだったというのが散見されています。例えば、お客様システムからデータを抽出して加工して業務を行う時に、部門で独自にパソコンを調達してマクロを動かしてしまう業務などは、今後ルールで統制していく必要があります。制御システムもデータはPLC（Programmable Logic Controller）のプロトコルで守られていますが、そこから変換してデータを加工しやすいように業務を効率化しようとした仕組みもあります。また、管理されていないと世代が代わった時に誰が管理者で何が課題だったか引き継がれずリスクだけ高まってしまいます。

藤本　ビジネスのデジタル化や働き方改革は攻めとして進めていくけど、サイバー攻撃の脅威も捉えて、セキュリティ・レジリエンスを高めるところはセットで取り組む必要があります。他の重要インフラ事業者のお客様でも、IT部門に見えていないシステムや制御システムを全社的に管理するための可視化とリスク分析を現在ご支援しています。

三浦 良介（みうら りょうすけ）
株式会社富士通総研 ビジネスレジリエンスグループ
チーフシニアコンサルタント

三浦　多くのIT部門が行う資産管理はIT部門が導入した資産を管理するだけで、会社全体の資産を管理できていません。事業部で導入した資産を管理できていないことはセキュリティとして問題です。また、従来の資産管理では年1度しか棚卸しを実施しておらず、ビジネススピードと合っていません。短期間しか利用しない資産でも同等のセキュリティレベルを保つにはどうすべきかが課題です。

大友　最近クラウドの提案では「すぐに利用できます」という謳い文句でのアピールが多くあります。これらは、ビジネス目線でよい提案であるかもしれませんが、お試しで終わらず、業務で継続するとなった場合には、リスクを認識してどんな情報を取り扱い誰が管理するのか決めていく必要があります。このようなケースでは、情報共有しながら進める必要があり、そこはIT部門の重要な役割と考えています。

今後強化すべきは、「自律的」に動ける人づくりだ

―これからもセキュリティについては絶え間なく対応していかなければなりません。それぞれの立場から、強化すべきと感じられている点は何でしょうか？

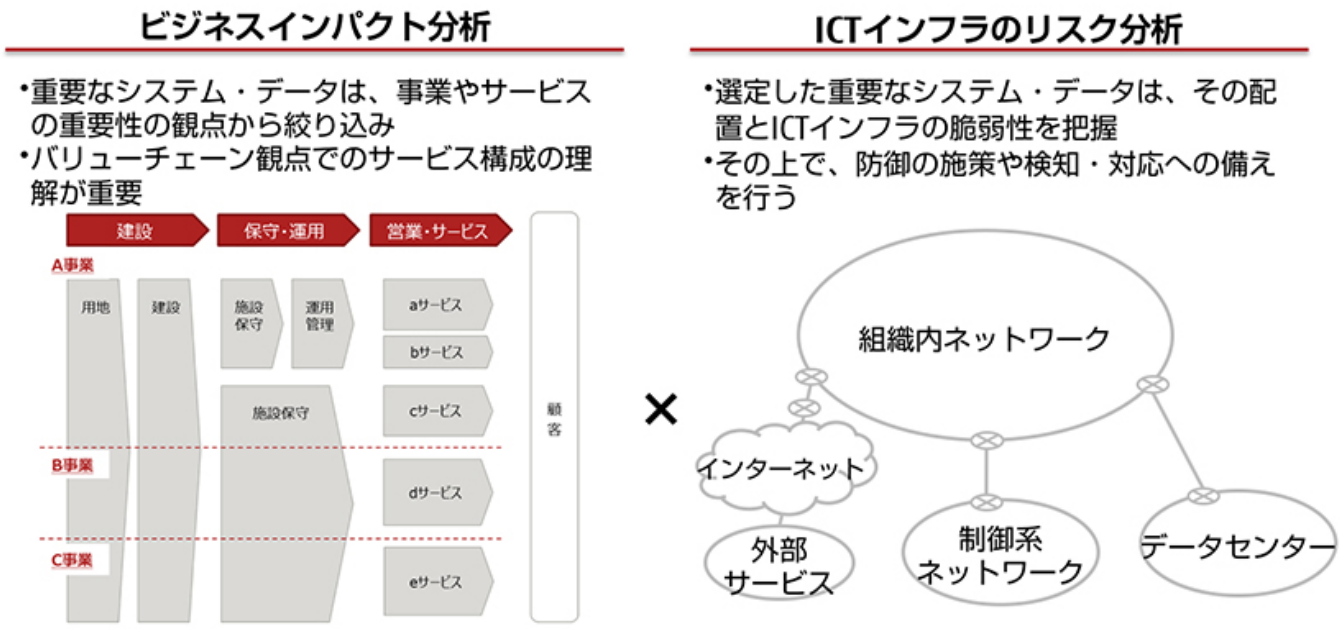
山下　2020年に向けて日本ではセキュリティ投資が高まっていきます。攻撃者は必ずモチベーションや背景があって攻撃してくるので、そのプロファイリングが重要です。富士通では、「エーキューブラボ」（FUJITSU Advanced Artifact Analysis Laboratory）というサイバーインテリジェンス専門の研究施設を作り、攻撃手法やキャンペーンの種類といった情報を収集しながら、スキルア

ップを図っています。また、セキュリティマイスター制度で現場のニーズに基づくセキュリティ技術者人材像を作り、どの分野で何人育成するという目標のもとに、人材育成しています。

―実際の運用まで意識するためには、スキルだけでなく「自分事」として考えるマインドも必要で、それを私どもは演習ベースで高めようとしています。

山下　お客様と向き合うフィールドはシステム開発するSEやお客様とともに運用するSEなど最も人が多いのですが、スキルとマインドの両方の観点でインシデントのハンドリング力を高めていきます。「普段と違う。バグではないみたいだ」と感じた時に、サイバー攻撃ではないかを素早く見極め素早くエスカレーションすることが重要なので、「気づく力」もセットで育成しています。

藤本　コンサルタントの立場としては2つのテーマを持って活動しています。1つは冒頭でも触れたリスクアセスメントを起点にしたセキュリティ・レジリエンスの最適化です。具体的には、「ビジネスインパクト分析」と「ICTインフラのリスク分析」の取り組みです（図4）。もう1つはインシデント対応力の強化です。CSIRT、SOC、サイバーに限らない危機管理体制がどう連携していくのかが重要になるため、CSIRTの整備だけでなく、危機管理対策本部との役割分担、連携フローの整備、連携のための演習などに取り組んでいます。



●図4 リスクベースアプローチによる取り組み

大友　電力会社にとって2020年の法的分離は非常に大きなインパクトがあります。分社化の際には、事業持株会社と送配電会社の双方にICTもセキュリティ機能も持たなければなりません。しかし、大幅な要員増は難しいことから、今いる人間で凌がなければなりません。今あるネットワークは活かし、社内にないリソースはパートナーさんやメーカーさんの力を借りながら進めるつもりです。今一番注力しなければいけないのはベースとなるフレーム作りで、それはルール、体

制、アクティブな情報共有です。IoTやAIの技術を有効活用しながら、自律的な活動と有機的な連携をバランスよく図っていくことが最も必要なことと考えています。

［司会］細井 和宏（ほそい かずひろ）
株式会社富士通総研 執行役員
エグゼクティブコンサルタント

―自律的に動ける人というのが肝ですね。

大友　主管部については自律的な活動につなげる人材を啓発・育成していくことにしていますし、ICT部門では自ら企画を考えて調整してやり抜くというメッセージも含めて人材育成を図っていきたいと考えています。今回、我々だけでは新しい企画や知見が足りないので、FRIさんに入っていただいて加速したと思っています。

―本日はありがとうございました。

（注1）SIRT（Security Incident Response Team）：コンピュータやネットワーク上で何らかの問題（主にセキュリティ上の問題）が起きていないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称。

（注2）SOC（Security Operation Center）：企業などにおいて情報システムへの脅威の監視や分析などを行う、役割や専門組織。

（注3）サイバーセキュリティ対処調整センター：政府機関・重要サービス事業者等に対するサイバーセキュリティに係る脅威・事案情報の収集・提供および対処支援調整を行う中核組織としてNISCで準備を進めている。

知創の杜

フォーカス

「セキュリティ・レジリエンス
ー事業継続を支えるIT部門の役割ー」

当記事の詳細をPDFでご覧いただけます。

資料ダウンロード

コンサルタントやエコノミストの知見・ノウハウをご紹介する情報誌「知創の杜」 はこちら

FUJITSU JOURNAL / 2019年1月23日