CYBER GRID JOURNAL

特集
伊勢志摩サミットとサイバーセキュリティ

LAC

Vol.1 | 2016 AUTUMN

巻頭言

三木俊明
取締役 常務執行役員
サイバー・グリッド・ジャパン GM

サイバー・グリッド・ジャパンが得た知見を皆さまに発信していきます

振り返ってみると、ラックは日本のインターネット創成期である 1995 年にセキュリティ事業を社内ベンチャーとして立ち上げ、2000 年の九州沖縄サミットでは公式サイトにおける不正アクセス監視・対応を支援しました。以来 15 年以上の間、日本のセキュリティビジネス強化に取り組み、日本の発展に尽力してきました。

昨今の報道からもわかるとおり、サイバー攻撃による脅威は深刻の度合いを増しています。ラックでは診断サービスや緊急対応サービス「サイバー 119」などを通じて、常にセキュリティインシデントの現場に寄り添い、事案解析に努めてきました。そして、この積み重ねこそがラックの大きな資産であり強みでもあると信じています。

サイバー・グリッド・ジャパンは事象解析の中心的な組織であると同時に、複数のセキュリティ企業との連携・機能補完による多面的な研究開発の提供を目的としたフレームワークとしても機能しています。

サイバー・グリッド・ジャパン内ではこれまで「サイバー・グリッド研究所」「ナショナルセキュリティ研究所」「データコンピューティング研究所」の 3 つの組織を運営してきましたが、2016 年 4 月、新たにモラル・教育・啓発の研究拠点として「ICT 利用環境啓発支援室」を設立しました。

これまでもセキュリティ関連コミュニティや社会貢献活動の支援を行ってきましたが、新組織を立ち上げることで、コミュニティとの情報共有を強化するとともに、社会のセキュリティ向上の一翼を担ってまいります。

また、2016 年 8 月に実証実験などによる研究開発成果の実用化を志向するため「次世代技術開発センター」を新設し、「データコンピューティング研究所」を機能統合しました。これらの組織による多面的な研究開発活動、これらを通じて得られた豊富な情報をベースに、ラックならではの見立てによる分析・予見・仮説提示を「CYBER GRID JOURNAL」として経営層・マネジメント層の方々をターゲットに情報発信していきます。

第 1 号となる今回は「伊勢志摩サミットとサイバーセキュリティ」をお届けします。公開されている日本のセキュリティ政策を読み解くことで、組織が取り組むべき対策の方向が見えてくる内容となっています。ぜひご一読ください。

CYBER GRID JOURNAL Vol.1 AUTUMN

TABLE OF CONTENTS

特集
伊勢志摩サミットとサイバーセキュリティ

文＝川口洋
（サイバー・グリッド研究所 所長、チーフエバンジェリスト）

サミットにおいてサイバー空間の安全が論じられるようになったことからもわかるように、サイバーセキュリティを巡る情勢はここ十数年で大きく変化した。本稿では、日本のサイバーセキュリティ政策や、社会・企業の意識や対応の変容を追い、今後さまざまな組織がなすべきこと、特に目前に控えた2020年東京オリンピック・パラリンピックに関連した攻撃やその対応策を論じる。

伊勢志摩サミットから見える サイバーセキュリティの課題

変化するサイバーセキュリティ政策 組織は何をすべきなのか

本年5月26日、27日に三重県志摩市で開かれた主要国首脳会議（通称 伊勢志摩サミット）は2日間の日程を無事に終え、閉幕した。この伊勢志摩サミットでは、討議の成果などを盛り込んだ「G7伊勢志摩首脳宣言」[i]が採択され、主に世界経済の課題が内容の中心となっていたが、首脳宣言と共に興味深い付属文書も公開されている。「サイバーに関するG7の原則と行動」というこの付属文書は、目指すべきサイバー空間のあり方やサイバー空間の安全の確保、デジタル経済の促進という内容が盛り込まれたものだ。「世界経済」だけでなく、「サイバー」もまた今回のサミットで議論された話題なのである。これまで日本で開催された2回のサミット（2000年の九州沖縄サミット、2008年の洞爺湖サミット）の時代から考えると大きな変化であると言える。

もっとも、2000年の九州沖縄サミットにおいて採択された「グローバルな情報社会に関する沖縄憲章」[ii]でも、犯罪のない安全なサイバー空間を強化するための協調行動を目指し、産業界との対話をさらに推進することがうたわれていた。しかし、サミット直後に制定された「高度情報通信ネットワーク社会形成基本法」[iii]（通称 IT基本法）の第7条では「高度情報通信ネットワーク社会の形成に当たっては、民間が主導的役割を担うことを原則とし」と記載されており、これまでわが国のサイバー空間は民間主導で発展が進められてきた。

しかし、最近のサイバー空間における事件事故の報道を見てもわかるように、今や民間企業だけの問題として捉えることが難しいものが多くなっている。九州沖縄サミットやその関連会合[1]では想定されていなかった、民間企業に対するサイバー攻撃が国家の安全保障や危機管理に影響する事態も発生しており、民間企業のみの問題として片づけることはできない。また、国家またはそれに準ずるような集団による攻撃と疑われる事案も発生しており、一民間企業だけの努力では守ることが難しいのは自明の理といえる。

そして、2020年の「東京2020オリンピック・パラリンピック競技大会」[iv]を控え、政府としてもサイバーセキュリティを国家の安全保障や危機管理の問題の一部として捉え、民間の活力や国民の財産を損なわないような配慮をしつつも、さまざまな施策を講じている。

2014年に制定された「サイバーセキュリティ基本法」[v]（以下、基本法）、重要インフラの行動計画をまとめた「重要インフラの情報セキュリティ対策に係る第3次行動計画」[vi]、経営者のサイバーセキュリティへの関与を求めた「サイバーセキュリティ経営ガイドライン」[vii]など、一連の動きはいずれも把握しておきたい。今後、ますます国家による関与が強まることが予想される中、読者の方々がそれぞれの組織で備えておくべきことについて解説する。

[1] G8ハイテク犯罪対策政府・産業界合同会合（2000年5月パリ）、G8リヨングループ・ハイテク犯罪対策に関する政府・産業界合同ワークショップ（2000年10月ベルリン）及び第2回G8ハイテク犯罪対策・官民合同ハイレベル会合（2001年5月東京）

サイバー空間を取り巻く状況の変化

サイバー空間における現状理解のため、ここでは「社会」「政府機関」「企業」の変化について解説する。

社会の変化：インターネット人口の増加とセキュリティへの関心の高まり

総務省の「平成 26 年通信利用動向調査」[viiii] によると携帯電話の保有率は 90% を超え、パソコンの保有率も 80% 前後を維持している。近年、スマートフォンやタブレット端末の普及によりパソコンの保有率は減少傾向にあるが、「インターネットの利用者数及び人口普及率の推移」を見ても多くの人がインターネットに接続し、サイバー空間で生活していると言える(**図 1**)。このことは統計データを見るまでもなく、多くの人の肌感覚と同じであろう。

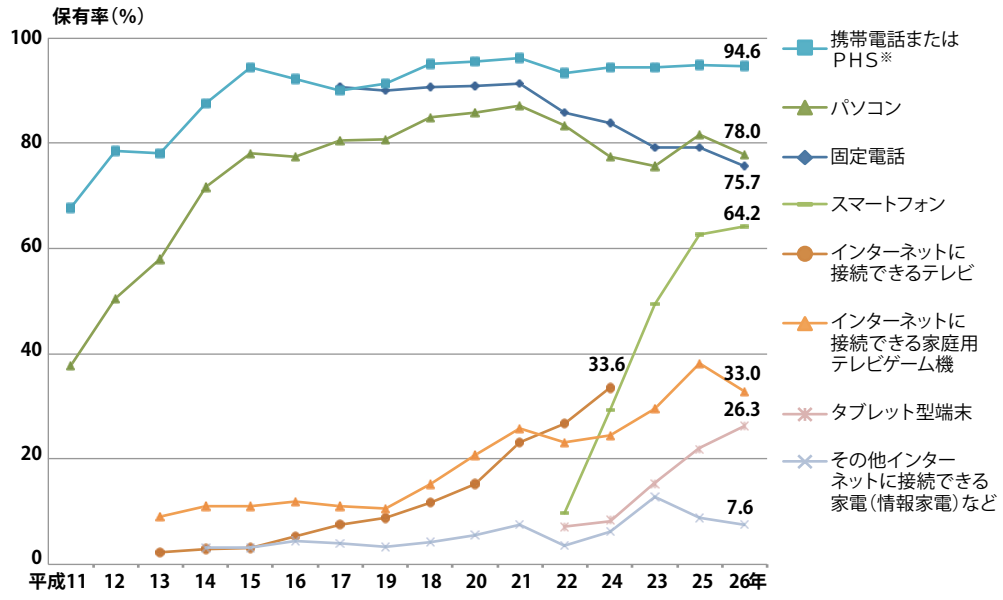
また、国民の代表である国会議員が議論する国会における「サイバー」という発言の数の変化を見ても、近年サイバー空間の問題が多く論じられていることがわかる（**図 2**: 次頁）。

2000 年以降、日本の IT 社会は民間が主導する形で発展し、同時にセキュリティ対策も個々の企業や個人の責任で実施されるものと見なされてきた。その後、Web サーバーへの不正アクセスによる機密情報漏えいや、ファイル交換ソフトによる個人報漏えいなどの事件が発生し、技術者や IT を積極的に利用するユーザーの間においてはセキュリティの関心は徐々に高まりつつあった。しかし、2008 年に開催された洞爺湖サミットにおいても IT やセキュリティが議論のそ上に載ることはほとんどなく [2]、社会全体に及ぶほどの動きではなかった。

しかし 2011 年に大手重工業や衆参両院などに対するサイバー攻撃が報道され、安全保障や政策立案に関わる組織が狙われているという事実が明らかになったことで、再びセキュリティに関する議論が行われるようになった。これらの事件では、外部より遠隔操作するコンピューターウイルスを添付したメールを、攻撃対象に関連する組織からのもののように装って送り付けるという攻撃手法が用いられた。これらの攻撃は「標的型サイバー攻撃（または標的型メール攻撃）」と呼ばれ、サイバー空間での攻撃や犯罪に関する言葉が一般社会に広まる契機となった。

2012 年の衆議院議員総選挙で自民党が政権を奪還、その後、政府は安全保障および危機管理を重視し、「国家安全保障戦略」[ix] を定めた。この国家安全保障戦略の中に「サイバーセキュリティの強化」という項目があり、国家の安全保

1



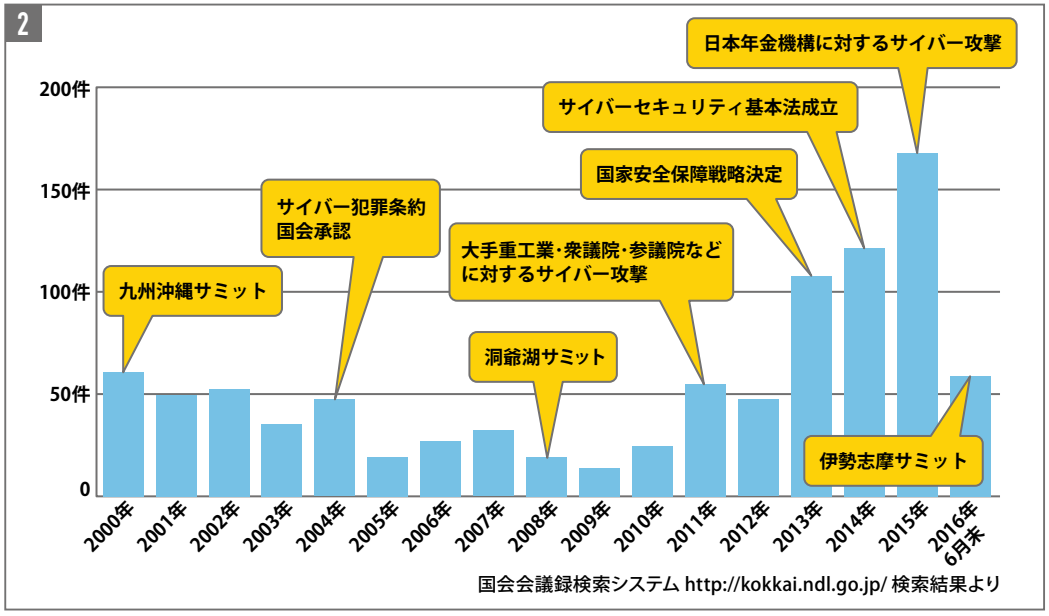
※「携帯電話・PHS」には、平成 21 年末以降は携帯情報端末（PDA）、平成 22 年末以降はスマートフォンも含む。「スマートフォン」は「携帯電話・PHS」の再掲

総務省「平成 26 年通信利用動向調査」
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/26honpen.pdf より項目を抜粋

図 1 情報通信機器の保有状況の推移

[2] 2000 年九州沖縄サミットで初めてサイバーセキュリティ（当時の文書には「secure cyberspace」と表現されている）について議論され、2001 年 7 月に開催されたジェノヴァサミットにおいても「サイバー犯罪との闘い」との表現で継承された。しかし、2001 年 9 月 11 日のアメリカ同時多発テロ事件を機に実空間のテロリスト対策が急務となるとともに、2001 年 11 月の「サイバー犯罪に関する条約」署名式典により当面の成果が得られたこともあって、2002 年カナナスキスサミット以降、IT やサイバー空間に関する議論は低調となった。洞爺湖サミットでは、「テロ対策に関する G8 首脳声明」において、（テロリズムによる）情報通信技術の濫用（the abuse of information/communication technology）という表現で言及されているだけである。

図 2　国会会議録から「サイバー」をキーワードに検索しヒットした数の推移



障の一環としてサイバーセキュリティの確保が必要であると明言されている。世の中が「情報セキュリティ」から「サイバーセキュリティ」に大きく舵を切った瞬間だ。

そして特にここ数年、基本法の審議や日本年金機構へのサイバー攻撃に関する議論が活発に行われるようになった。衆参本会議や各委員会での国会議員による質疑が増えれば、政府機関も多くの取り組みを行うようになる。同時にサイバーセキュリティの話題がメディアに取り上げられる機会が増え、世間の人の目に触れることも多くなった。

政府機関の変化：セキュリティ専門機関の創設と法整備

2000 年には、国際的な競争力のある IT 立国を目指すため IT 基本法が制定され、その後「情報通信技術戦略本部[ix]（IT 戦略本部）」が設置された。そして、同じ 2000 年に情報セキュリティ対策の企画、立案並びに総合調整を行うため、内閣官房に「情報セキュリティ対策推進室」[xi]が設置される。この時点ではセキュリティ政策に関する実行力を持った組織ではなく、各府省庁の対策を取りまとめ調整する役目を担っていた。

2005 年には内閣官房に「情報セキュリティセ

COLUMN ドローン規制の二の舞を踏まないために

2015 年 4 月に首相官邸にドローンが落下した事件を覚えているだろうか。あの事件を契機に航空法の改正やドローン規制法の制定が行われた。以前から多くの人がドローンの安全上の問題を指摘していたが、大きな事故もなかったことや、経済的な側面から大きな規制は行われていなかった。ところが、首相官邸に落下し、多くのメディアが取り上げたことで、法規制が一気に進むこととなったわけだ。十分な議論をし尽くす前に法規制が行われたことは、ドローンに関係する人や業界にとっては大きな痛手であろう。

日本社会の特徴として、メディアが事件を大きく取り上げると、それにより法規制などの展開も変わるということがある。これには政府機関の動きなども早くなるメリットもある反面、行き過ぎた規制になりがちというデメリットも存在する。そもそも現在のドローンはブレーキが効かないこともある自動車のようなもので、全くもって発展途上だ。現状の法規制などでは、今後見込まれている自律飛行技術や安全性の進歩を考慮できていないとの見方もある。

日本年金機構に対するサイバー攻撃をきっかけにサイバーセキュリティ基本法が改正され、サイバーセキュリティ経営ガイドラインが公開された。現時点では企業や個人を強く縛るものではないが、次に「日本年金機構クラスの事件」が発生した場合、その規制が大きく進む可能性があることに注意したい。いったん強い規制が行われた後は、3 年～ 5 年かけて現実的な落としどころに落ち着くものと思われるが、ガイドラインがガイドラインであるうちに自主的に取り組んでおくことが企業の自衛策となるだろう。

ンター（NISC）」が設置された。NISC は政府機関の情報セキュリティ対策の統一化および水準の底上げのため、「政府機関の情報セキュリティ対策のための統一基準群」[xii] や、重要インフラの分野横断的な対策を促す「重要インフラの情報セキュリティ対策に係る行動計画」を定め、政府機関や重要インフラ事業者が行うべき対策の指針を示した。

さらに、2008 年には政府機関の横断的監視や情報共有を行うため GSOC（Government Security Operation Coordination Team：政府機関情報セキュリティ横断監視・即応調整チーム）、2012 年にはセキュリティ事故発生時の支援を行う情報セキュリティ緊急支援チーム（CYMAT）の運用を開始。NISC は内閣官房の組織として各府省庁の調整を行うだけではなく、実行力を持った組織の運用を行うことで徐々に日本のセキュリティ対策の司令塔としての力を付けてきた。

2014 年には「サイバーセキュリティ基本法」が制定され、その施行に合わせ翌年 2015 年には「情報セキュリティセンター」から「内閣サイバーセキュリティセンター（略称は同じ NISC）」に改組された。この時から NISC は法的根拠を持った組織となり、政府機関における指導力を発揮することができる体制が整った。漢字の名前の法律が多い中、「サイバーセキュリティ」というカタカナ用語を法律の名前に入れたところにこの法案に関する思いを感じることができる。

サイバーセキュリティ基本法は主に政府機関が行うべきセキュリティ対策を盛り込んだものであるが、政府機関に課せられた対策は自然とその監督企業へと課せられていく流れである。

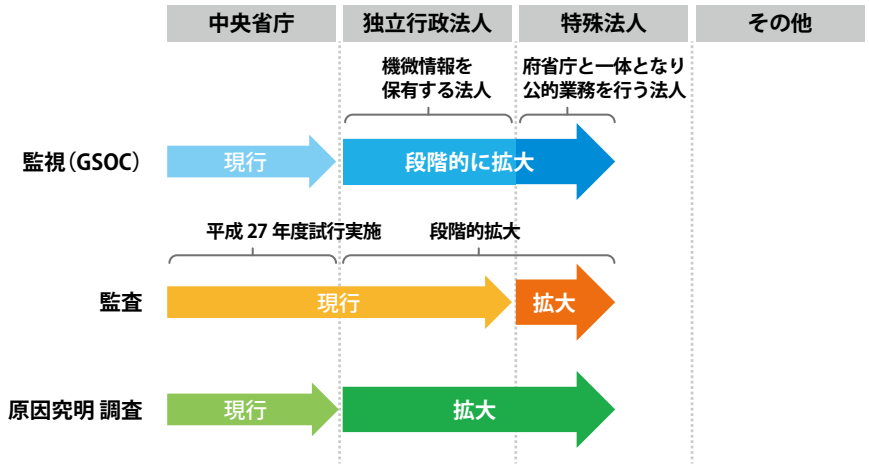
そして 2015 年 5 月に発生した日本年金機構の情報流出事件をきっかけに、セキュリティに関する多くの議論が交わされた。その結果、2016 年 4 月には基本法の改正が公布され、**図 3** のように中央省庁から独立行政法人や特殊法人にまで内閣サイバーセキュリティセンターの指導すべき範囲が広がった[xiii]。

「監視」「監査」「原因究明調査」の 3 つの機能の対象範囲が拡大されていくということは、これらの機能がサイバーセキュリティ確保のためにまず必要であるというメッセージを暗に示している。つまり、今後さまざまな場面において以下のようなことが問われていくことを意味する。

「サイバー攻撃の監視を行っているか ?」
「決められたことを適切に実施しているか ?」
「問題が起こった原因を究明しているか ?」

つまり予防策だけではなく事後対応も含めて求められるということだ。民間企業においても、自組織のサイバーセキュリティ確保のためにこれらの機能が実装されているか確認することをお勧めする。この際参考になるのは、日本年金機構事案に関する事故調査報告書だ。これは 3 つの組織（サイバーセキュリティ戦略本部[xiv]、厚生労働省[xv]、日本年金機構[xvi]）から公開されている。これらの事故調査報告書には実際に行われたサイバー攻撃の手口や組織における問題が詳細に記載されており、サイバー攻撃の実態や課題の現実を学ぶことができる。さらに再発防止策は世の中すべての組織に求められていることであるとされており、多くの組織に適用が可能

3



NISC「新たなサイバーセキュリティ戦略 ~ 政府機関などのサイバーセキュリティ対策の抜本的強化 ~」
http://www.nisc.go.jp/conference/cs/dai04/pdf/04shiryou02.pdf より

図 3　サイバーセキュリティ基本法改正による NISC の機能強化

だ。読者におかれてはぜひこれらの報告書を確認していただきたい。

組織や機能の拡大に伴い、政府機関のセキュリティ対策予算も大きく変化した。日本年金機構の情報漏えい事件が発生した影響もあり、平成 28 年度（2016 年度）のサイバーセキュリティに関する概算要求額[xvii]は 742.8 億円となり、前年度の 325.8 億円から大幅に増加している。NISC の予算 83 億円のうち GSOC の占める割合が 68 億 5000 万円と多く、「実行力」の期待の表れと見ることができる（**図 4**）。

さらに 2015 年末には経済産業省から「サイバーセキュリティ経営ガイドライン」が公開された。このガイドラインは経営者のリーダーシップの下でサイバーセキュリティ対策が推進されることを期待したものであり、経営者が認識する必要がある「3 原則」と CSO や CISO などの情報セキュリティ対策の責任者に指示するべき「重要 10 項目」をまとめたものである。経営者が認識する必要がある「3 原則」は以下のように記載されている。

1. 経営者のリーダーシップによる推進
2. 系列企業や取引先、ビジネスパートナーなどを含めた対策
3. ステークホルダーとの適切なコミュニケーション

いずれも目新しい内容ではないものの、経営者の主導により組織が一体となった対策の実施が期待されていることがわかる。ただしこの「サイバーセキュリティ経営ガイドライン」は現時点ではあくまで「ガイドライン」であり、強制力を持ったものではない。しかし、「ガイドライン」の実行が期待されていることは明白であり、特に経済産業省が所管する企業に関してはこの「ガイドライン」の実行が求められていくだろう。当然のことながら、セキュリティ事故が発生した場合、本ガイドラインへの準拠状況が問われることは想像に難くない。

企業の変化：業務の IT 依存と深刻化するサイバー脅威

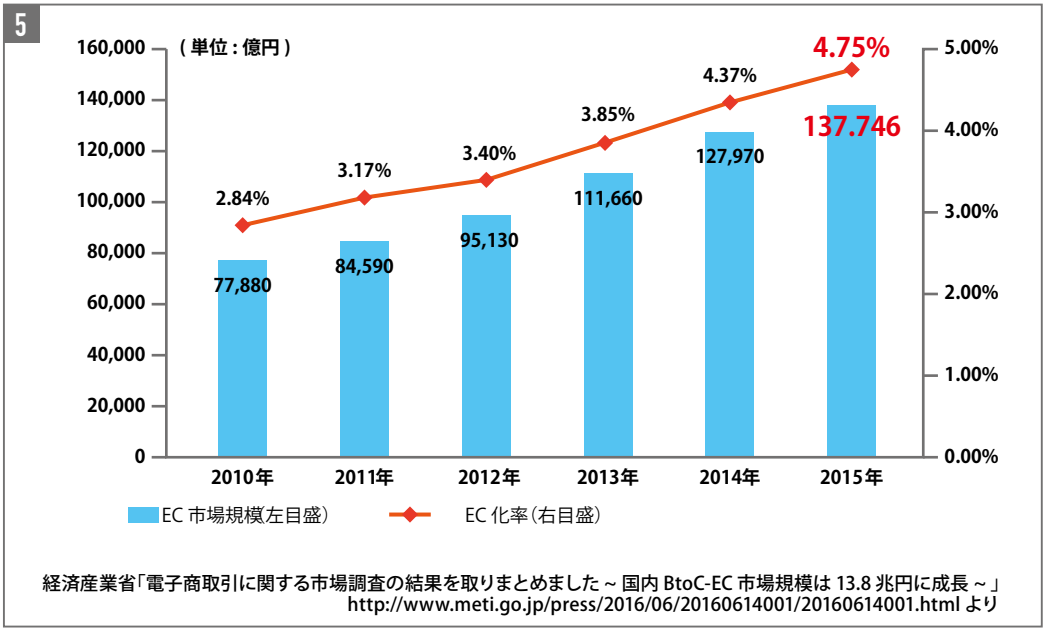
1993 年、日本におけるインターネットの商用利用が始まって以降、企業を取り巻く IT 環境は大きく変化した。多くのインターネットサービスが立ち上がり、それらのサービスが密接に連携した新たなサービスも次々と生まれている。それに伴い、電子商取引の規模は年々増加しており[xviii]、多くの取引がサイバー空間に移行している（**図 5**：次頁）。サイバー空間で多くのお金が動くようになると共に、犯罪者も現実空間からサイバー空間にその活動の領域を移していることは何度も語られているとおりである。

一方、一般のパソコン利用ユーザーの環境も変化している。オフィスには 1 人 1 台のパソコンが用意され、技術者 でなくとも誰もが自席で自分専用のパソコンを使用し、インターネット接続を前提として業務を行っている。特に「業務資料作成」「メール送受信」「インターネット閲覧」の 3 つは企業における主な活用方法であり、これらなくして現在の企業活動は成り立たないと言っても過言ではないだろう。その結果、攻撃者もこれらの業務を狙って攻撃を仕掛けてくる。特に標的型メール攻撃はその典型だ。攻撃者は情報通信技術を悪用し、「業務資料に偽装した不正プログラム」を用意、それらを攻撃対象のユーザーに「業務連絡に偽装したメール」として送り付けることにより実行させ、「インターネット閲覧を偽装した通信」でコントロールを行う。特に、技術者ではないユーザーにはこのような偽装を見破ることは容易ではなく、多くの組織が標的型メール攻撃の被害に遭っている。

サイバー空間における企業の活動が増える一方、サイバー空間の脅威が増大したことで、自然とセキュリティ対策の重要性に対する意識も高まった。株式会社アイ・ティ・アールの「IT 投資動向調査 2016」[xix]によると、最近 5 年間で IT 予算額全体は増加基調にあるが、その中で情報

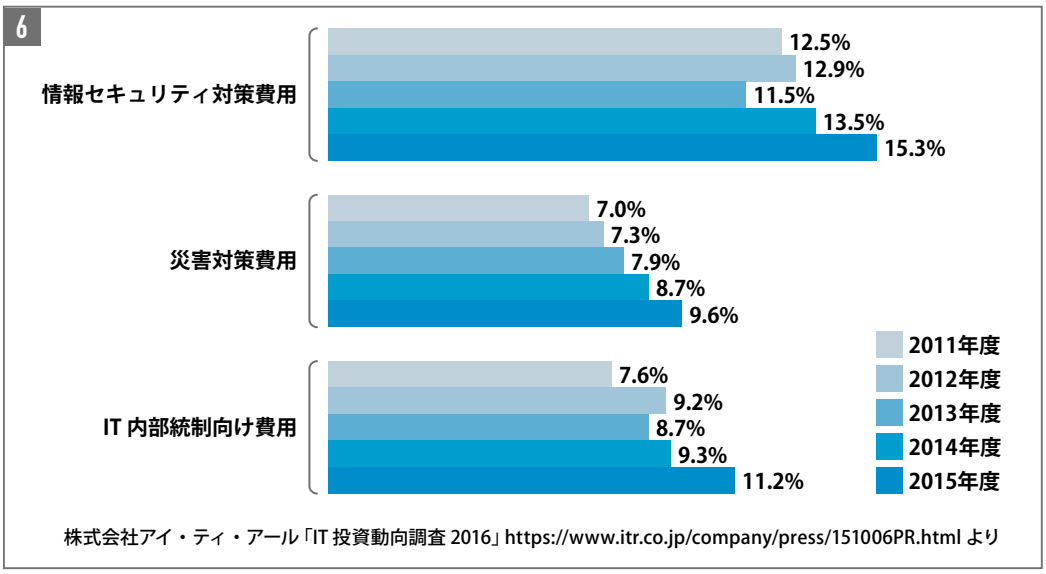
NISC「政府のサイバーセキュリティに関する予算」
http://www.nisc.go.jp/conference/cs/dai05/pdf/05shiryou03.pdf より

図 4　NISC 概算要求額のうち GSOC の予算



経済産業省「電子商取引に関する市場調査の結果を取りまとめました～国内 BtoC-EC 市場規模は 13.8 兆円に成長～」
http://www.meti.go.jp/press/2016/06/20160614001/20160614001.html より

図 5　日本の BtoC-EC 市場規模の推移



株式会社アイ・ティ・アール「IT 投資動向調査 2016」https://www.itr.co.jp/company/press/151006PR.html より

図 6　IT 予算額に対するリスク対策費用割合の経年変化

セキュリティ対策費用が占める割合は年々上昇している（**図 6**）。これには大きなセキュリティ事故に関するニュースやマイナンバー制度の開始も影響していると見られる。だが、企業におけるセキュリティ対策費用は増加傾向にあるものの、ウイルス感染や DDoS 攻撃など何らかの被害を受けた企業が多くあり、世間を騒がすようなニュースになる事件も後を絶たない。

2011 年に日本を襲った東日本大震災を契機に、企業の情報システムに対して災害対策が求められるようになったことも見逃せない。情報システムの可用性 [3] も重要なセキュリティの要素であり、災害発生時に事業が継続できる体制を経営層が重視していると言える。災害対策を考慮した場合、情報システムは分散して稼働させることが望ましいが、機密性 [4] と完全性 [5] の観点からは管理対象が分散することで管理コストが上昇するという頭の痛い事情も存在する。サイバー空間で活動するすべての企業は、管理維持コストをにらみつつ、集中管理と分散管理のバランスを取っていくことが求められる。

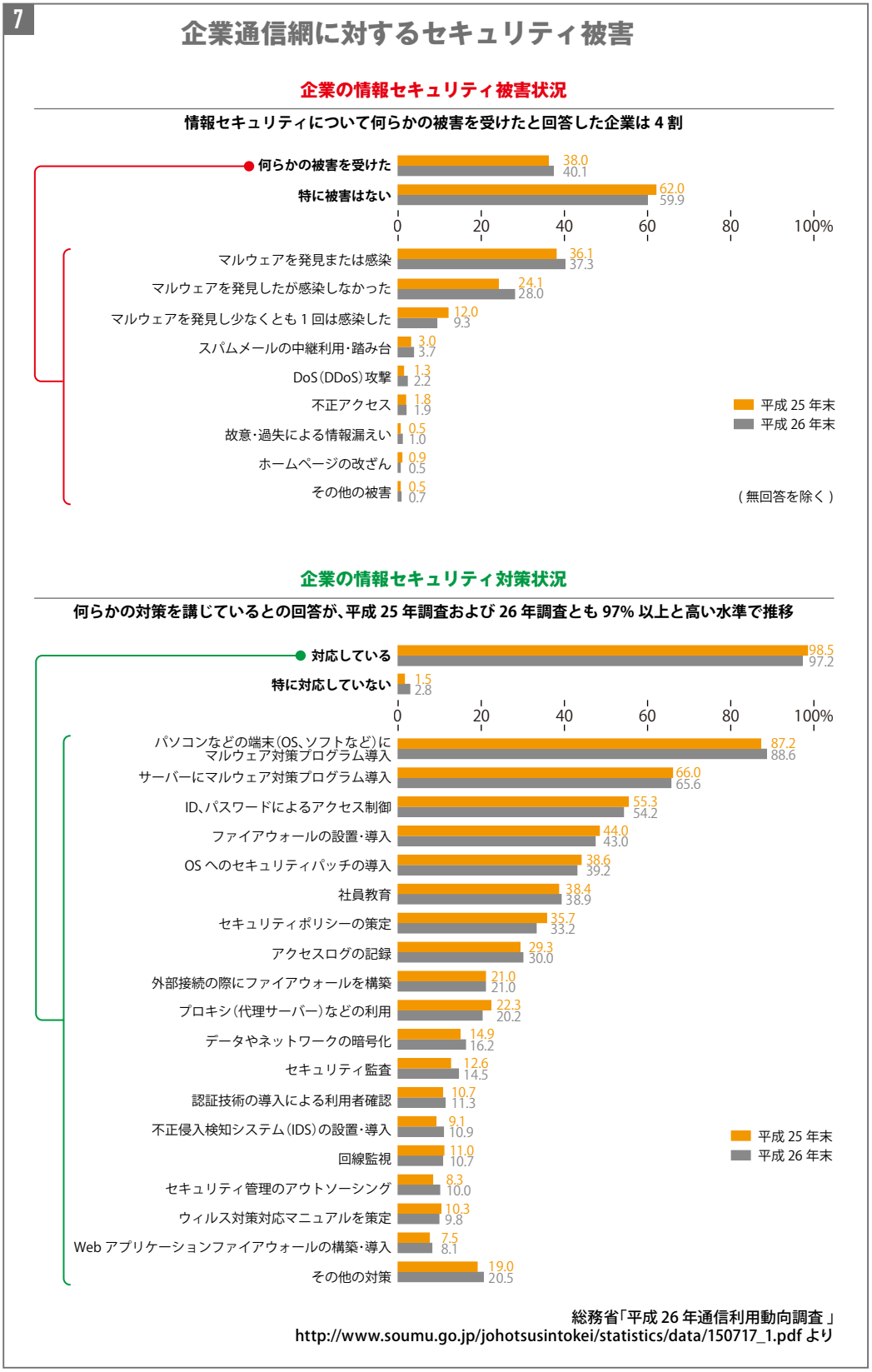
情報セキュリティ対策費用の割合が増加する一方、何らかのサイバー攻撃により被害を受けた企業は 4 割に達している [xx] 。さらにデータから読み取れるのは、アクセスログの記録や不正侵入検知システム（IDS）の導入率が高くないことだ（**図 7**：次頁）。平成 26 年でも、アクセスログを記録しているのは 30%、IDS を導入しているのは 10.9%にすぎない。ここから見て、被害を受けていてもそれに気付いていない企業が多く存在する可能性が高い。実際に、外部からの通報を契機に調査をして被害に気付き、ラックが相談を受ける事例も多く見られる。

[3] Availability に対応する日本語。情報資産を必要な時に使用できるよう、システムを継続して稼働させること。

[4] Confidentiality に対応する日本語。情報資産に正当な権限を持つ者だけが使用できる状態を確保すること。

[5] Integrity に対応する日本語。情報資産が破壊・改ざん・消去されていない状態を確保すること。

図 7　企業の情報セキュリティ対策状況



ビッグイベント開催に向けた課題の整理

2016 年 5 月 27 日に閉幕した伊勢志摩サミットでは、会合の運営に支障をきたすような事象は発生しなかったようだ。これは関係者が事前に連携方法を検討し、緊密に連携した結果と評価していいだろう 。2019 年のラグビーワールドカップ、2020 年の東京オリンピック・パラリンピック競技大会を見据え、ビッグイベント開催に向けての課題の整理をしたい。

多数のステークホルダーとの共同オペレーション

2020 年に開催される東京オリンピック・パラリンピック競技大会（以下、大会）は東京都が主体ではあるものの、日本全体を巻き込んだ一大イベントとなる。少なくとも**図 8** のような 4 つの大きな関係者が存在し、それぞれの関係者が密接に連携して運営が行われる。関連する組織が多くなることで、連絡パスが多くなり、事前の調整が重要となる。組織委員会や NISC もさまざまなワーキンググループやワーキングチームを組織し、事前調整を実施している様子がうかがえる。

図 8 に含まれていない企業にとっても、大会は無関係とは言えない。サイバーセキュリティ経営ガイドラインにも記載があるように、系列企業や取引先企業、ビジネスパートナーまで含めると何らかの関係がある可能性が高いのだ。システムが高度につながり、サービスを提供している時代において、意外なところが「単一障害点」となる可能性もある。システムの関係性を把握するための取り組みは必ず実施しておきたい。

2020 年が近づくにつれ、大会に関係するサービスで発生した事件はささいなものであっても政府機関やメディアの関心を引き、その対応が注目される可能性が高い。長く情報システムの仕事をされている方には、2000 年問題に似ていると言った方がわかりやすいかもしれない。従来は見過ごされていた問題が大きく取り扱われ、企業のイメージ問題に発展することも考えられる。さらに事案発生時には各方面の関係者からの問い合わせが増えることが想定されるため、ステークホルダーの整理と対応方法を事前に整備しておくことが望ましい。

サービス継続への取り組み

大会期間中にはさまざまなサイバー攻撃も想定されるため、大会運営側は入念な準備を行っていることと思う。大会期間中のサービス障害は日本のイメージにも影響するため注目が集まりやすく、小さな事象であっても大きく取り上げられ、経営上の問題としても捉えられる可能性がある。大会成功のためには、サイバー攻撃が行われたとしても関係サービスを継続し続けることが重要だ。そのためにはサイバー攻撃に強い情報システムを作ることに留まらず、サービス全体の対策に抜けや漏れがないかを確認しておかなければならない。情報システム担当者や特定サービスの担当者ではなく、経営者自身がサービス全体を俯瞰し、リスクの分析やリソースの最適化を含め、スピーディな対応を行う必要があるだろう。

サービス継続を妨害する可能性が最も高い脅威は DDoS 攻撃と思われる。監視カメラや家庭用ルーターなど、ネットに接続している多数の機器から攻撃対象に集中的に通信することで、サー

8

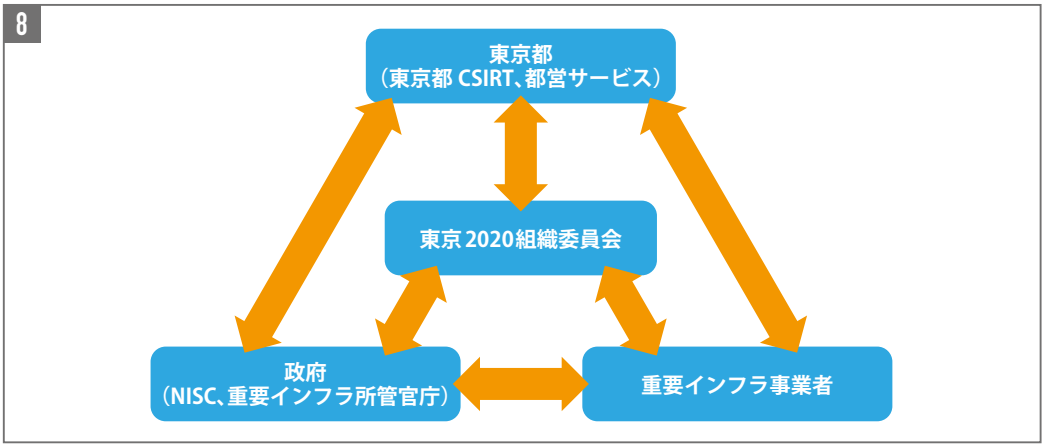


図 8　ラックが想定する東京オリンピック・パラリンピック競技大会運営関係者

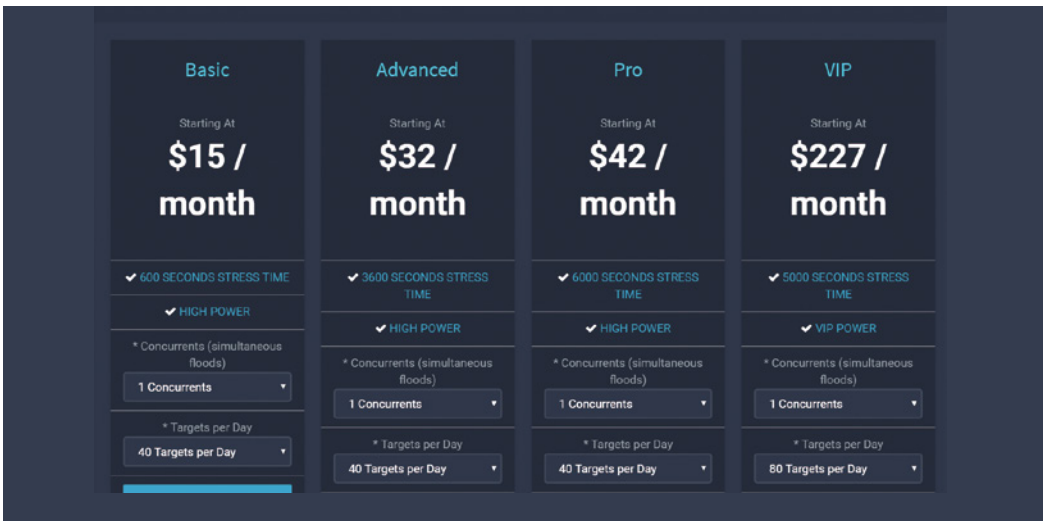


図 9 「DDoS 攻撃用サービス」サイトの例

ビス提供を妨害する攻撃だ。この DDoS 攻撃を行うことができるサービスを「負荷テストサービス」という名目で提供しているサイトが複数存在し、これを悪用した DDoS 攻撃の可能性が想定される。このようなサイトでは月額 15 ドル程度からサービスが提供されており、安価に攻撃を行うことが可能なのだ（**図 9**）。

DDoS 攻撃用サービスのサーバーは海外に存在し、支払いもビットコインなどで行うことができるため、サービス提供者やサービス利用者の追跡が難しい。ラックが調査したある DDoS 攻撃事案では約 38 万もの IP アドレスから攻撃が行われていた。その際の通信量は 200M/bps ～ 250M/bps ほどで、大きなニュースになるほどの威力ではないが、それでも多くのサイトではサービス提供に支障をきたす規模である。

攻撃に使われた IP アドレスの多くでは DNS サービスや NTP サービスを提供しており、設定が不十分なサーバーが攻撃に悪用されていると見られる。さらにアカマイ社のレポート [xxi] によれば、前述の 1000 倍に及ぶ 300Gbps を超えるような攻撃も増加しており、ユーザー側の対策だけでは防ぎきれないほどの規模になっているが、これにも不適切な設定の機器が悪用されている。世界中に散らばるこのような管理が行き届いていない機器への対策を地道に行っていくことが、社会全体の取り組みとして求められる。

認知していないサイバー攻撃への対応

DDoS 攻撃のようなわかりやすい攻撃だけでなく、標的型サイバー攻撃のような認知することが難しい攻撃にも注意する必要がある。海外では変電所、放送局、銀行、製鉄所などが標的型サイバー攻撃を受け、システムの破壊やサービスの停止といった事案が発生している。幸いなことに日本ではそのような重要インフラサービスに大きな支障をきたすような事件は少なくとも表ざたになっていないが、場合によっては、すでに攻撃を受けているのにそれを認知していない可能性も懸念される。

次頁の**図 10** は、ラックが対応したある標的型サイバー攻撃を行うグループの攻撃対象を示したものである。重要インフラ事業者（外側の青枠）およびその事業者に対して機器を提供する会社(外側の橙枠) が狙われていることがわかる。このことは、これまで言われていたような重要インフラ事業者のみが注意すればいいという時代ではなくなっていることを示している。

また、これらの標的型サイバー攻撃の発生日（下段 = 赤字）と対応開始日（上段 = 黒字）の関係を示したものが次頁の**図 11** である。

これを見てのとおり、多くの事案で数カ月から 2 年以上にわたって攻撃の存在を認知することができていない。われわれは、標的型サイバー攻撃によるサービス停止は何年も前から着々と準備が進行していることを認識する必要がある。これら重要インフラ事業者およびインフラ機器事業者を狙った標的型サイバー攻撃の詳細についてはラックのサイバー・グリッド研究所が 2016 年 8 月に公開した CYBER GRID VIEW Vol.2 を参照されたい。

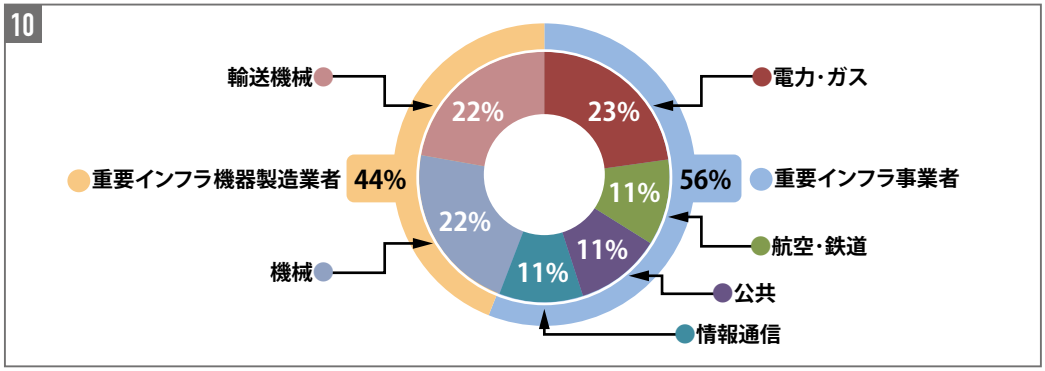


図 10　標的型サイバー攻撃グループの攻撃対象の分類

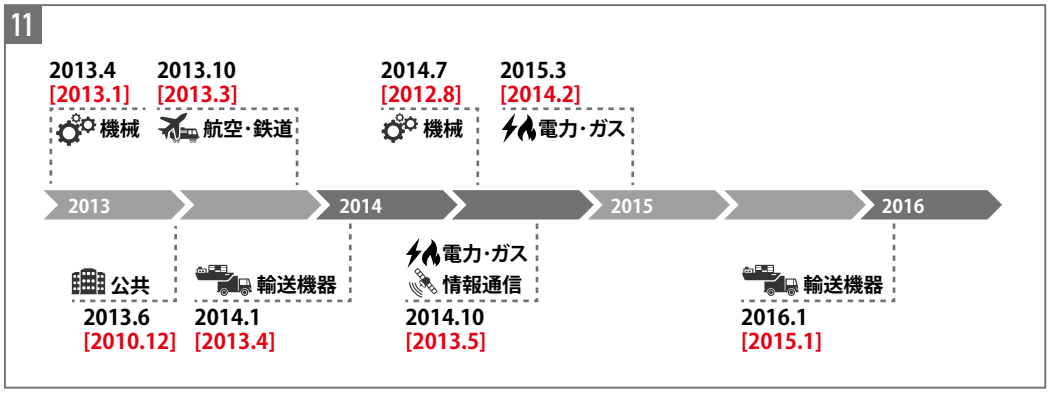


図 11　サイバー攻撃の発生日と対応開始日（下段・赤字が発生日、上段・黒字が対応開始日）

本稿では伊勢志摩サミットの前後の状況を俯瞰し、東京オリンピック・パラリンピック競技大会に向けた課題を整理した。国家の一大イベントに対してさまざまな取り組みが行われており、サイバー空間に関係するすべての事業者は無関係ではいられないだろう。今後も新しい動きがあれば、CYBER GRID JOURNAL やラックの Web サイトを通じて情報を発信していきたい。

出　典

i　http://www.mofa.go.jp/mofaj/ms/is_s/page3_001697.html
ii　http://www.mofa.go.jp/mofaj/gaiko/summit/ko_2000/it1.html
iii　http://law.e-gov.go.jp/htmldata/H12/H12HO144.html
iv　https://tokyo2020.jp/jp/
v　http://law.e-gov.go.jp/htmldata/H26/H26HO104.html
vi　http://www.nisc.go.jp/active/infra/siryou.html
vii　http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html
viii　http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html
ix　http://www.cas.go.jp/jp/siryou/131217anzenhoshou.html
x　http://www.kantei.go.jp/jp/singi/it/index.html
xi　http://www.nisc.go.jp/itso/shoukai/gaiyou.html
xii　http://www.nisc.go.jp/active/general/kijun26.html
xiii　http://www.nisc.go.jp/conference/cs/dai04/pdf/04shiryou02.pdf
xiv　http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf
xv　http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf
xvi　https://www.nenkin.go.jp/oshirase/topics/2015/20150721.files/press0820.pdf
xvii　http://www.nisc.go.jp/conference/cs/dai05/pdf/05shiryou03.pdf
xviii　http://www.meti.go.jp/press/2016/06/20160614001/20160614001.html
xix　https://www.itr.co.jp/company/press/151006PR.html
xx　http://www.soumu.go.jp/johotsusintokei/statistics/data/150717_1.pdf
xxi　https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/state-of-the-internet-report-connectivity-executive-review-q1-2016-akamai.pdf

リサーチャーの眼

《研究・開発の最前線からお届けする技術情報》

第1回

サイバー攻撃最前線

文＝小笠原恒雄（サイバー・グリッド・ジャパン 次世代技術開発センター チーフ リサーチャー）

大規模セキュリティ・インシデント時代における、大量処理可能な調査技術の必要性について

現在、筆者の所属する次世代技術開発センターでは、ラックの緊急対応サービス「サイバー 119」やセキュリティ監視センター「JSOC」が検知したインシデント（事案）の情報を分析し、その傾向などを調査しています。調査・分析した結果については、技術レポート「CYBER GRID VIEW」として公開するなど情報提供していますが、今後増加するであろう大規模なセキュリティ・インシデントに向けて、どのような調査技術が必要かを整理します。

インシデント対応の難しさ

セキュリティ・インシデントの疑いについて調査を進めると高度なコンピューターウイルスが発見され、標的型攻撃による情報漏えい事故であることがわかるケースが多くあります。さらに調査を進めていくと組織内のパソコンが何台もウイルスに感染しており、攻撃者に悪性プログラムを実行されて不正侵入を繰り返されていたことが判明、大規模なセキュリティ・インシデントだと認知するに至ったケースも少なくありません。このような場合、被害がグループ関係組織や取引先に影響が及んでしまうこともあります。

このような状況下において、インシデント対応するメンバーは、侵害されたパソコンの特定と隔離を進めながら調査範囲を絞っていき、徐々に全容を解明していかなくてはなりません。こうしたインシデントの対応途中、被害に遭った組織で対処が進んでいることに攻撃者が気付き、攻撃を仕掛け直すことがあります。つまり現場では、初動対応から正確かつ素早い現状把握と対応方針の意思決定が求められます。

インシデント終息の課題は現場の声にあり

最近の大規模インシデントの対応では、さまざまなツールを駆使してログ（記録）を集約し、総合的に解析を行うのがトレンドです。状況把握から脅威の検知、応急措置や再発防止などについての作業を被害組織の担当者と随時協議をしながら進めていき、一定期間モニタリングを続けながら対応の有効性が確認できるまで支援を継続し、インシデントを終息させていきます。

しかし、実際のインシデント対応では、初期段階から事前に被害組織の担当者と事前に調査対象と想定した全エリア・全パソコンに調査の手があまねく行き渡ることはほとんどありません。なぜなら、ツール配布やインストール後の動作チェックによる手間を要するほか、組織規模が大きくなる

インシデント対応ツールの開発メンバー

表　インシデント対応時に求められる機能の要件

特徴	説明
自動実行プログラムの精査	OS 起動時など、自動的に起動されるプログラムの状況をフォレンジック調査の観点で深い分析を可能にするとともに、コンピューターウイルスと侵害パソコンの迅速かつ正確な特定、事実解明を行うことができる。過去のインシデント対応で得た知見を活用して痕跡チェックや脅威検知を迅速に実現できるようにする
検知後の調査分析	組織全体の包括的な分析をベースとし、特定のパソコンで発見した不正な事象の精査からそのパソコン以外の影響範囲や脅威の関連性について一連での分析ができるようにする。ログを受け取った後でも被害組織から追加でログが届くことを想定し、分析できるようにする
被害組織の環境に合わせたログ取得	ログ取得の際は、被害組織の負担をできるだけ少なくする。それにより、システム環境や突発的な事情によるログ取得漏れの状況を極力なくす仕組みにする
複数パソコンを対象にしたタイムライン解析	ウイルス感染後の組織内の横断的侵害について、手口の解明を従来よりもスムーズにするため、フォレンジック調査の肝とも言えるタイムライン解析を単体のパソコンだけでなく、複数台も対象にして追跡調査が行えるようにする

につれて被害組織担当者の管理外のパソコンが登場し、調査のために調整が必要になるなど、管理責任の問題が発生することや業務がどうしてもすぐ停止できずに対応が遅れてしまう、といったさまざまな要因が出てくるためです。このような突発的な問題によって対応期間が長引き、その影響で侵害されたパソコンが後から見つかることがあります。そうなると、調査手順を再構成しなければならないことがあります。

こうした現実の状況を踏まえると、初動対応から復旧（業務再開）までを、途切れることなく一貫してスピーディーに実行でき、被害を受けた企業が最小のダメージを負うだけで問題解決が可能となる手段が必要と考えられます。

緊急対応に当たるサイバー 119 のエンジニアと問題解決の手段をブレーンストーミングしたところ、「インストールに手間取るようなツールは避けたい」、「複数種類のログ解析を複数台のパソコンに対してまとめて一気に解析できるようにはならないか」、「被害組織から後日、調査ログを受け取った場合でも、分析のやり直しをせずに全容が容易に把握できるようにならないか」など、現場ならではの意見が集まりました。

ブレーンストーミングで集まったインシデント対応時に求められる機能の要件を上の表にまとめました。要件としては最小限ですが、最も実効的なものだと言えます。脅威の検知からインシデントの終息に向けた包括的な分析とチェックを実現するため、これらの要件を重要な研究開発テーマとして捉えてツールの開発を進めました。このツールを使い、調査分析のプロがインシデントレスポンスを効率的に実施すれば、被害組織の業務復旧スピードやインシデント管理能力、事業継続性の向上が期待できると考えています。

サイバー攻撃は今後、ますます複雑化することが予想されており、検知・防御はさらに難しくなるかもしれません。脅威を完璧に防御でき、インシデントを未然に防ぐことができればそれが理想ですが、現実的にはインシデントが発生する前提での取り組みがまだ必要不可欠です。今回挙がった機能要件をもとに、調査分析の工程について研究開発を通じた改良を重ねることが必要であり、「総合的な脅威分析の視点を持った調査分析や脅威検知」を軸にした対策ソリューションがより重要性を持つと考えています。

脅威の検知・分析が可能な総合的なソリューションへ

今回のプロジェクトには、次世代技術開発センターのほかに、現場のプロとしてサイバー救急センターも参画しています。本稿の執筆時点では、ツールのコア部分の開発を終えており、現在は解析部の機能強化に取り組んでいるところです。

また今後は、顧客自身が迅速かつ容易に総合的な分析結果を見て対処できるように、さらにツールの改良と研究開発を進めていきたいと考えています。また今回紹介した研究開発とは別に、並行して進めている他の研究活動も存在します。各研究の成果の融合し、新しい視点を持った脅威検知や分析技術の実現についても考えていますので、今後の研究開発にご期待ください。

ラックの顔　様々な場所で活躍する社員をご紹介

“サイバー空間の安心・安全に貢献したい”

第1回 大塚慎太郎　シンガポール・IGCI（The INTERPOL Global Complex for Innovation）

アジア屈指の国際都市といわれるシンガポール。東京 23 区ほどの大きさの島に、中華系・マレー系・インド系などの民族が暮らす。近年では外国企業の進出も進み、金融や情報分野などにおいてハブとしての役割を担っている。

インターポール（国際刑事警察機構）がこの地に IGCI（The INTERPOL Global Complex for Innovation）を設立したのは 2015 年のこと。そして、この組織の一員として活躍しているのが今回紹介する大塚慎太郎さんだ。

インタビュー＝斉藤健一（株式会社 HTP）

水産学部からセキュリティの世界へ

大塚さんの出身校は北海道大学大学院水産学研究科。学部時代には海洋実習もあったという。一風変わった経歴に思えるが話を聞いてみると、専攻は物理海洋学で、海流や水の流れを研究しており、研究室では解析用コンピューターを使う機会も多かったという。

その流れから就職活動でもコンピューター関連の企業に的を絞る。中でも情報セキュリティに力を入れているラックに興味を持ち、2001 年に入社。

当時は 24 時間 365 日体制の有人監視サービスを提供する国内企業は存在しなかったという。このセキュリティ監視センターは 2002 年にお台場から神谷町へ移転され、JSOC（Japan Security Operation Center）という名称となる（その後、現在地へ本社と共に移転）。

JSOC では、顧客ネットワークのファイアウォールや IPS の監視・保守を行うオペレーターや、ログの分析を担当するアナリスト、さらに JSOC 自体のインフラを管理・運用するメンバーなど、いくつかのチームで構成されている。

大塚さんも 2002 年の JSOC 設立に携わっており、2005 年にはデバイス運用グループのリーダーに任命される。

手前にはマーライオン、奥にはマリーナベイサンズ。シンガポールを代表する観光名所だ

2000 年代前半といえば、マイクロソフト社の IIS Web サーバーを狙った Code Red（2001 年）や、Windows シリーズの OS にさまざまな手段で感染するように作られた Nimda（2001 年）など、大規模に拡散するワームが次々と登場して世間を騒がせた時代だが、大塚さんも SQL Slammer（2003 年）による混乱は今でも記憶に残っていると話す。

「ワームの爆発的な拡散が起きた時、日本ではちょうど週末にかかっていました。JSOC 業務の一環としてファイアウォールのログを監視しています。各ポートの平常時のトラフィック量はだいたい把握していましたが、この日は違っていました。突然 SQL ポートへのトラフィックが見る見るうちに増加していったのです。いったい何が起こっているのか全くわかりませんでした。ニュースなどで報じられる前のことですから、SQL Slammer という名前すらありません。JSOC のメンバーで必死にパケット解析などを行ったのを覚えています」

このワームはマイクロソフト社製 SQL サーバーの既知の脆弱性を攻撃する。感染後に自身のコピーを大量に送信することからネズミ算的にトラフィックが増大し、ネットワーク遅延やダウンを引き起こした。このワームの感染を増やす攻撃はセキュリティパッチの適用で比較的簡単に防げるが、ファイアウォールの設定ミスやパッチの適用ミスなどにより、しばらくの間、突然新たな感染コンピューターが現れる事象が続いたという。

2010 年、大塚さんは JSOC のセンター長に就任する。前述のとおりセキュリティの世界では、いつ・どんなインシデントが発生するのか予測はできない。24 時間 365 日の体制で顧客ネットワークの監視を行っていれば、ましてやセンター長という立場であれば、昼夜を問わず呼び出されることとなるが、この点に関して気忙しさはなかったかと聞いてみた。

すると「もちろん心が落ち着かない時もありますが、JSOC は 24 時間 365 日にわたりストップすることのない業務ですから、覚悟はできていました」と力強い答えが返ってきた。

シンガポールで新たな挑戦を開始

大塚さんには常々考えていることがあった。それは SOC という世界から外に出て、新たな活躍の場でキャリアを積んでいくというものだ。日ごろから JSOC のメンバーにも話しており、自らが挑戦し後進へ道を作っていくことが自分の役割の 1 つだとも考えていた。そして、インターポール勤務の打診を受けたのは、ちょうどそのような折だった。

インターポールは、官民連携などによるサイバー犯罪撲滅を目的とし、世界各国の法執行機関と民間企業などが連携できるようコーディネーションを行う施設として The INTERPOL Global Complex for Innovation（IGCI） を 2015 年 4 月にシンガポールに設立。

余談だが、全世界で 77 万台以上の PC が感染していたと見られるボットネット「Simda」のテイクダウン作戦が同時期に実施されたが、この作戦を統括したのが IGCI だ。

インターポールは NEC とサイバーセキュリティ対策で提携しており、ラックは NEC のサイバーセキュリティソリューションのパートナーであったことから IGCI へ参画することとなった。

ラックは、IGCI の活動を支援するため、自社開発のサイバー攻撃相関分析エンジン「LAC Falcon（ラック ファルコン）」を提供するとともに、JSOC の運営経験がある人材として大塚さんを派遣することとなった。

大塚さんは「多少の不安はありましたが、迷いはありませんでした」と、その時の心境をこのように語った。

IGCI のネットワークに監視の目を光らせる

大塚さんが所属するのは IGCI 内の「Cyber Fusion Centre」という組織。世界各国の法執行機関や民間企業からスペシャリストが集まり、協力しながら犯罪捜査に有効な情報を発信しているという。

この中で大塚さんは、LAC Falcon を用いて IGCI のネットワークのセキュリティ監視を行っている。IGCI の持つ重要な情報や職員が利用するネットワークの状況に目を光らせ、セキュリティインシデントが起こらないよう注意を払っているのだそうだ。

シンガポールでの仕事について尋ねてみると「サイバー空間では、国境を越えた犯罪が頻繁に発生し、各国で足並みを揃えた法整備や抑止策などさまざまな対策を講じる必要があります。官民連携はもちろんのこと、各国間の連携もこれまでの犯罪にはないレベルで必要になってきているのではないかと思います。これまでも、お客様の資産とビジネスを守ることを目標に仕事をしてきましたが、もう一歩踏み込んだ、サイバー犯罪捜査支援の取り組みに関われることができ、非常にうれしく思っています。それと同時に、サイバー空間をより安全で安心できる環境にするための取り組みに、少しでも貢献できるようこれからも努力していきます」と語ってくれた。

大塚慎太郎（40 歳）：群馬県前橋市出身。北海道大学大学院水産学研究科を 2001 年に修了しラックに入社。セキュリティ製品の構築業務を経て、2002 年から JSOC の業務に携わる。2005 年にデバイス運用グループのリーダーに任命。2010 年からセンター長を務める。2014 年 10 月よりインターポール勤務を開始。写真は IGCI のエントランスで撮影した一葉

一方、初の海外赴任で、当初は不安に感じていたプライベート面についても、住み始めてみるとシンガポールには 3 万 5000 人ほどの日本人がいることがわかり、海外初心者にとっても住みやすい環境だということがわかったという。

また、シンガポールは観光地として人気があり、アジア諸国への玄関口としても利用されている。大塚さんも「ありがたいことに、日本でお世話になった多くの方々が、出張や乗り継ぎの際にシンガポールを訪れ、この地で日本の近況を伺うことも珍しくありません。皆さんも機会があればホットなシンガポールにぜひともお越しください」と生活に慣れたことを感じさせる発言もあった。

多様な文化や価値観に触れて

大塚さんは IGCI での任期満了後は、後進へ席を譲りたいと考えている。シンガポールで多様な文化に触れ、IGCI で国籍の異なるスタッフと共に働くことで、価値観を超えた経験ができたそうだ。また、サイバーセキュリティは国境にとらわれない情報収集と多くの人たちの協力の上に成り立っていることを改めて感じることができたともいう。

インタビューの最後では「本任務完了後は、こういった経験を活かしてラックのビジネスを広げていくような仕事に取り組んでいきたい」と今後の抱負を語ってくれた。

Cheer Up! ラックの対外活動

安心・安全な ICT 利用環境を目指して

～ ICT 利用環境啓発支援室の活動～

文=吉岡良平（サイバー・グリッド・ジャパン ICT 利用環境啓発支援室 室長）

インターネットの負の側面を見つめて

総務省の「情報通信白書平成 28 年版」によると、平成 27 年末の 13 歳から 59 歳までの年齢層のインターネット利用率はいずれも 9 割を超えており、年少の 13 歳未満では 74.8%、80 歳以上の高齢者でも実に 20.2% で、平成 14 年当時と比較してもそれぞれ約 20 ポイントも上昇しています。特にスマートフォンの登場により、誰もがネットを持ち歩き、いつでもどこでも利用できる環境が整いました。

その反面、コミュニティサイトを通じて性犯罪などに巻き込まれた児童数は、警察庁の発表によると平成 27 年中には 1652 人に上り、年々増加しています。また不正アクセスなどのサイバー犯罪も毎日のように報道され、その手口もますます複雑で狡猾（こうかつ）になっています。さらに平成 27 年度に全国の消費者センターに寄せられた相談では、アダルト情報サイトや何らかのインターネットサイトに関連する「デジタルコンテンツ」に関するものが 18 万 1000 件にのぼり、他の商品・サービスを大きく引き離しています。

ネットやスマホの普及によって私たちの生活は飛躍的に便利になりました。ネットは善良な利用者ばかりでなく、悪意のある者にとっても便利なため、容易にサイバー犯罪に手を染めることも可能になりました。また悪意はなくとも、意識下にある感情をむき出しにした文章や悪ふざけの写真を SNS に投稿することでいわゆる「炎上」を巻き起こし、社会問題化することも多くなりました。

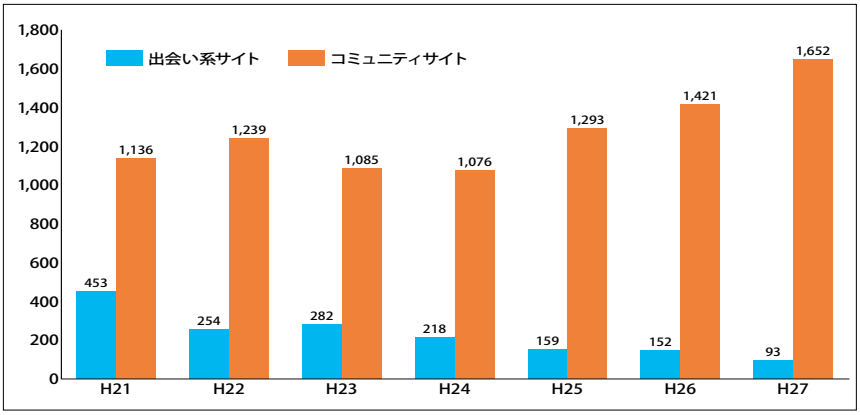
インターネットが私たちにとって身近な存在になって約 20 年が経ちましたが、新聞やテレビに比べればまだまだ新しいメディアです。またネットは私たちが自ら簡単に情報発信をすることができる初めてのメディアでもあります。こうした新しいメディアを活用する上では、それに応じた規範意識やモラルの醸成、危機回避能力を身に付けることが必要です。今や各地でセキュリティの勉強会が開催され、学校では情報モラル教室が催されるなど、情報リテラシー（活用能力）の向上のための取り組みが盛んに行われるようになりました。にもかかわらず未だトラブルは後を絶ちません。利用者が安心して安全にネットを利用し、豊かな生活を実現するためにも、あらゆる世代がインターネットの負の側面を正しく理解し、継続的にリテラシー向上に努めることができる社会環境の整備が必要な時代になったといえます。

ICT 利用環境啓発支援室が目指すもの

ラックは情報セキュリティ企業として、豊富な経験と技術力により業界での認知も高い企業です。監視や診断、解析などセキュリティ関連のサービスにより、技術的な側面から安心・安全なインターネット環境の維持・発展に貢献しています。またラックの中の研究組織であるサイバー・グリッド・ジャパンでは、進化を続ける技術に歩調を合わせ、今後予測されるリスクにも対応できるように、さまざまな研究開発や情報収集に取り組むことで社会に貢献することを任務としています。

こうした動きは単にラックのようなセキュリティ企業だけでなく、行政や大学、研究機関を含め世界中の技術者が安定かつ安全なネット環境の維持に努めています。しかし、誰もが手軽に情報発信ができるというインターネットの特性がゆえに、利用者にはリスクがいつ、どこに生じるか、容易には想像がつきません。特に利用者のレベルで生じるトラブルやインシデントは、操作上の不注意によるコンピューターウイ

図　出会い系サイト及びコミュニティサイトに起因する事犯の被害児童数



出典：平成 27 年中の出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について
警察庁・平成 28 年 4 月 14 日

ルスの侵入などのセキュリティリスクだけでなく、SNS への安易な投稿による炎上騒ぎなども含まれます。こうしたトラブルの影響は個人にとどまらず、家族や所属する会社、学校にまで及びます。企業がイメージの向上やセキュリティ確保のために多額の投資をして対策を行っていても、社員のミスや不注意な投稿ひとつでせっかくの努力が水泡に帰してしまうことがあります。

ICT 利用環境啓発支援室は、ネットの利用者に最も近い地域社会が住民のセキュリティ意識や情報モラルの向上に務める体制作りの支援をしています。実際に多くの地域では、自治体や警察、NPO、有識者などが中心となって、地域住民に対してセキュリティやスマホの取り扱いや子供や高齢者によるネット利用にまつわるトラブルについて啓発活動を行っています。ICT 利用環境啓発支援室では、地域で啓発活動を行っている方々への情報提供や相談対応に加え、各地で開催される講演会や研修会の講師なども引き受け、地域での取り組みを積極的に促進しています。また、取り組みが活発でない地域には、他の地域などでの好事例を紹介し、活動の活性化にも取り組んでいます。さらに今後必要とされる情報セキュリティに関わる技術者を目指す層を拡大するために、児童、生徒や学生に、情報セキュリティの重要性とそれに携わることの意義について、周知することも大切な役割のひとつと考えています。

ICT 利用環境啓発室の取り組み

ICT利用環境啓発室では、“Evidence based Encouragement（根拠に基づく支援）”をキーワードに活動しています。啓発の目的、内容や手法などについて手探りではなく、明確な指針を定めて検証しながら活動することで、根拠をより明確にし、効果的な活動を行うためです。特に以下3つの指針を作成し、精度の高い啓発活動を行う上での根拠にしています。

1. 情報モラル　啓発教育シラバス

近年のスマートフォンの急速な普及により、発生するトラブルも多様で複雑になりました。SNS やメッセージアプリによる誹謗・中傷、炎上やソーシャルゲームにおける高額課金にとどまらず、面識のない者との出会いによる性犯罪や児童ポルノ、リベンジポルノの被害など枚挙にいとまがありません。こうした問題はこれまで「青少年インターネット環境整備法」に基づき、官民が一体となって、主に青少年対策として取り組んできましたが、最近では高齢者や成人も含めた社会問題となりました。トラブルを未然に防止しつつ、情報化社会の中でネットの利便性を享受するためにも、情報モラルの啓発は年齢を問わず行っていく必要がありますが、啓発に対する理解度やその実践力は人によってまちまちです。「情報モラル　啓発教育シラバス」では、啓発対象者の学齢や年齢、立場などに応じて必要となる項目やその伝え方などを精査しています。そして、日々の啓発活動の中で実践、検証しながら、地域の啓発活動にとって、一定の指針となるガイドラインを作成しています。

2. セキュリティ・エンカレッジメント成熟度指標

利用者が安心してネットを利用するためには、利用者のモラル向上だけでは対処できず、ネットの機器や仕組みなどの技術面に関する知識や経験が必要となります。さらに社会全体としては、専門的にセキュリティに従事する人材の育成も必要です。ネットと接する際に技術をどの程度必要とするかは、立場や職業、担当している業務、所属する集団の目的などによっても異なり、その水準も段階的で、それに応じた啓発が必要となります。対象者がどのような水準にあるかを測るための指標として「セキュリティ・エンカレッジメント成熟度指標」を作成し、この指標を用いて、セキュリティの勉強会や啓発活動への参加者が、現状よりも高い成熟度を達成できるように支援を行っています。

3. 地域情報の整理・分析

啓発活動は、各地で行われていますが、ネットやスマホの普及度合いを考えると決して充足しているとはいえません。時間や距離を超越するインターネットの特性を考えれば、ネットのトラブルはいつでも、どこでも、誰にでも起こる可能性があります。ネットの安心・安全な利用環境を構築するためには、全国的に地域に密着した啓発が必要とされます。ICT 利用環境啓発支援室では、啓発活動を通じて地域の実情を把握し、情報リテラシー向上のために必要なデータを整理・分析することで、地域が自発的かつ継続的な啓発が実施できる体制作りに努めています。

最後に

情報化社会は、技術の進歩とともに立ち止まることなく、日々進化を続けています。IoT（さまざまなものがインターネットに接続され情報のやりとりがされる仕組み）や Fintech（新たな金融サービスを生み出す IT 技術）といった新しい概念も生まれ、私たちの生活はますます便利になっていきます。同時にインターネットという便利なメディアが、必要不可欠なインフラとなった社会では、常にそれに起因するインシデントやトラブルに対して心構えが必要です。ICT 利用環境啓発室では、ネットを使う一人ひとりが啓発活動を通じてリスク回避と対応能力を磨き、新しい時代の生活をより豊かなものにできることを祈って、日々の活動を推進しています。

サイバー・グリッド・ジャパン活動のご紹介

昨今、サイバーセキュリティは企業の経営課題となっています。企業の経営者には、リスク管理・品質管理・CSR といったさまざまな観点から、セキュリティへの取り組みが求められています。その取り組みは自社のみにとどまらず、グループ企業やサプライチェーンのセキュリティについても責任が問われます。日本が健全な発展を遂げるために、今こそ企業に「強さ」と「しなやかさ」が求められているのです。

サイバー・グリッド・ジャパンは、高度に巧妙化するサイバー攻撃とそれによる被害発生を防ぐため、2014 年に発足しました。サイバー・グリッド・ジャパンの主な活動は、以下のとおりです。

情報分析・動向調査

高度な知見を有するリサーチャーが、サイバー攻撃の動向や各種公開情報などを集積・分析することにより、防御に資する知見を見出して活用するとともに、積極的に発信していきます。また、国レベルのセキュリティを支援すべく、サイバー戦・国際情勢・法制度の動向などの調査・研究を行います。

注意喚起情報・脆弱性情報の発信

ラックは全社的な取り組みとして、コンピューターの OS やソフトウェアにおいて、不正アクセスやコンピューターウイルスなどのサイバー攻撃を受けやすくなるセキュリティ上の欠陥（脆弱性）の発見を推進しており、サイバー・グリッド・ジャパンでその取りまとめを行っています。広く一般に周知を図るべき脆弱性などを把握したときは、注意喚起情報や脆弱性情報を発信し、確認・対策を呼び掛けます。

研究開発

急速に進化する ICT（情報通信技術）や関連業界の動向を踏まえ、攻撃検知／防御技術、インシデント対応技術、IoT セキュリティ技術、データ分析技術など、来るべき「超サイバー社会」に求められる技術の研究開発を行います。

啓発活動

日本の ICT リテラシーを向上させ、安心・安全なインターネット環境の利用を促進するために、各種団体での活動や講演を通して、専門家や技術者以外の方々にも、セキュリティをはじめとした ICT の適切な利用を促す活動を行います。また、若年層や地域住民への積極的な活動を通し、日本全体の ICT リテラシーの底上げを図ります。

若手技術者支援

次世代を担う ICT 人材の育成と裾野拡大のために、IT スーパーエンジニア・サポートプログラム「すごうで」を主催し、卓越した技術力を持つ若者の才能の芽を発掘し・支援します。また「セキュリティ・キャンプ」の支援など、若手 IT 人材の発掘、育成に積極的に取り組みます。

2016 年度は、啓発活動を体系化・加速化すべく、「ICT 利用環境啓発支援室」を新設しました。さらに、次世代技術の統合的な研究開発と実用化を見据え、「次世代技術開発センター」を新設しました。その他の活動も、外部環境や社会の要請に応じて迅速・柔軟に見直し、最適な組織体制を構築して、効果的・効率的に推進していきます。

また、これらの活動はラック単独の取り組みにとどまらず、他企業・機関と連携して推進いたします。各種業界団体・コミュニティにおける活動や、研究開発におけるオープンイノベーションを通して、技術と情報のシナジーを生み出し、日本のセキュリティレベルを向上させます。

サイバー・グリッド・ジャパンは、ラックの長年の経験・技術力を結集し、産官学連携を通して、ICT 環境を強く、安全に進化させ、日本の発展に寄与すべく邁進いたします。

株式会社ラック
サイバー・グリッド・ジャパン