我が国のサイバーセキュリティ政策の取組

（第 15 回 FMMC 研究会　2022 年 6 月 22 日実施）

総務省大臣官房審議官（サイバーセキュリティ・国際技術担当）　　山内　智生

本日の話は大きく３つのパートに分かれています。最初が、わが国を取り巻くサイバーセキュリティの脅威の紹介です。次が、わが国の政府機関全体、加えて総務省の取組を紹介します。最後に、私見を交えて、サイバーセキュリティのあり方についてお話しさせていただければと思います。

サイバー空間をめぐる動向

ランサムウエアによる身代金攻撃ですとか、Emotet 等のマルウエアの２つが、日本だけではなく、世界中で猛威を振るっています。

ランサムウエアは、最近は二重の脅迫で、まずサイバー攻撃をかけてデータを奪い、窃盗したデータを公開すると脅す手口があります。それから、感染したパソコンデータの暗号化で、復号化してほしかったらユーザーに金を払えという手口があります。

ランサムウエアでは、少し前に起きていたこととの大きな差異があります。例えば、今まで個人情報が漏れたときに、個人情報１件あたり、QUO カードが１枚、500 円かける漏れた件数を身代金として払うのが、ある意味の２～３年前ぐらいまでの常識でした。現在では、攻撃者側の企業に対する見積もりの精度が増し、ある企業のどの情報は、いくらぐらいの価値であるのかということを、正確に見積もる人たちが増えています。2021 年５月の米国のパイプラインの会社への攻撃では、実際に要求されている額は、数億円の上のほうの位とされています。それぐらいは払えるでしょうと要求され、この会社は、実際に身代金を払ったようです。（FBI 等によって、支払金は、後ほど取り返されています。）別の事例で、2017 年に NotPetya（ノットペチャ）に基幹系のシステムが感染した有名な物流会社では、黒海辺りでの物流が全面的に止まりました。公表はされていませんが、分析にあたったコンサルタントの試算によると、彼らの被害額はおおよそ 200 億～300 億円で、さきほどの個人情報漏洩での試算額では留まりません。そういう問題が発生していることは、覚えておいてください。

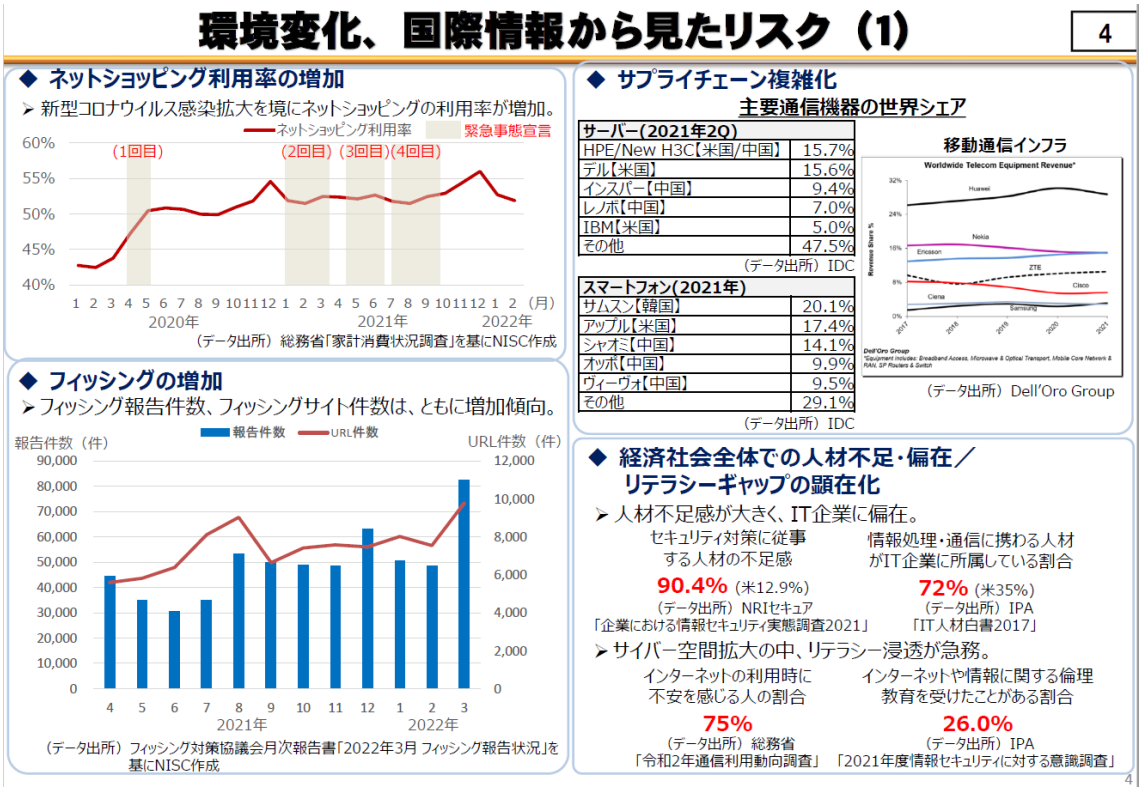
一度、テークダウンをした Emotet が再開されています。Emotet は、一時期、鳴りを潜めていましたが、このマルウエアが改造され、これを使っていた連中も復帰したらしく、2022 年の２月ぐらいから、本格化しています。.jp のアドレスでも、感染して、メール送信に悪用されたという方々が、テークダウンをされる前のピークの 2020 年の５倍以上に増え、手口も、どんどん変わってきています。この手のマルウエアのたちの悪いところは、これで止めたと思うと、止めたものを回避するような手口で広がります。現在、セキュリティ関係機関に多数相談があるものが、ランサムウエアと Emotet の２つです。

パイプラインの事例については、石油価格の一時的な高騰につながるほどの大きな事態になったので、バイデン大統領からのサイバー攻撃に対する注意喚起に派生し、こういうことも含めて、QUAD（自由や民主主義、法の支配といった基本的価値を共有する日米豪印の 4 か国の枠組み）、日米豪印におけるサイバー協議が行われているというのも事実です。2021 年の G7 では、米国の提唱によりランサムウエアに特化した議論をしました。

ランサムウエアをやっている人たちには、Ransomware as a Service を利用している攻撃者の集団が存在します。この集団への対応についても議論されています。セキュリティ機関だけではなく、犯罪捜査機関とも連携して、対応しなくては間に合わないという状況になりつつあります。

環境変化としては、コロナになってから、いっそう IT を利活用する状況になりました（図表１）。これは、IT に基づくリスクが増えたということにほかなりません。ネットショッピングは、緊急事態宣言の１回目のときから増えて、５割ぐらいの利用率の水準で推移しています。そして、ネット上で、いろいろな活動が増えると、フィッシングも増えています。

図表 1



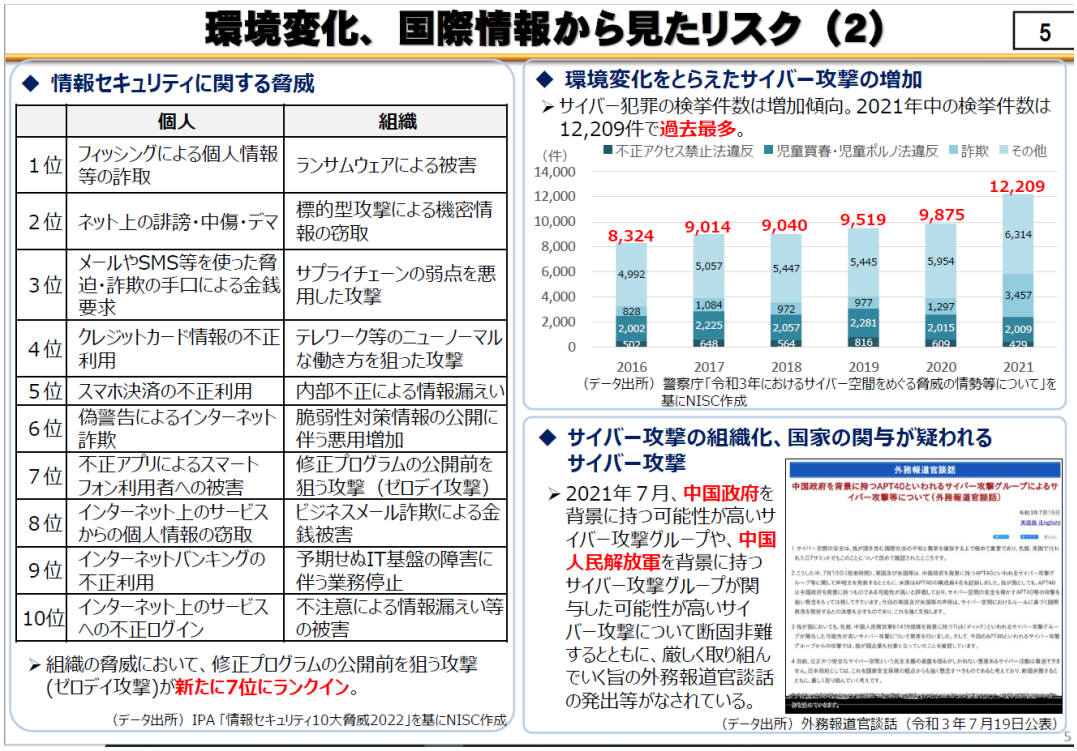
われわれがサーバーとかスマートフォンといった形で見る製品の裏側で、どんな部品が機器を構成しているかを考えると、そこには長いサプライチェーンが存在しています。わかりやすく申しあげると、Wi-Fi の機器がよい例と思います。かなりの数が日本製品として売られていますが、Wi-Fi のルーターのコアになっている送受信機の部分には、かなり

中国製の部品が入っていると言われています。ある製品について、どこの国のものかが一律には言いがたいという状況が起きているのが、このサプライチェーンの複雑化の問題です。

リテラシーギャップの顕在化については、人材が大きく IT 企業に偏在しており、不足感があります。IT の人材が IT 企業に偏在しているというのは、日本特有の事情です。人材の不足感は、グローバルに共通している問題ですが、米国の場合、セキュリティも含めた IT 人材は、IT 側と、いわゆる事業側の両方に、一定数、存在します。日本のように、システムの発注をするときにベンダーに丸投げという構造は、欧米では一般的ではありません。少なくとも、仕様については、一定程度、企業側、事業者側のほうで作成したうえで、ベンダーに要求をするというのが一般的です。よって、社会構造が先にあって人材の不足がうたわれているのか、それとも逆なのかは難しいというのが、人材育成の関係者の共通認識だそうですが、人材が不足しているなかにコロナが起きて、さらに人材不足感が増しているというのは事実のようです。

セキュリティに関する脅威を情報処理推進機構（IPA）が発表している「情報セキュリティ 10 大脅威 2022 」（図表２）で見ると、修正プログラムの公開前を狙うというもの出てきました。ゼロデイ攻撃だけが怖いわけではなく、実際に気をつけなければならないのは、脆弱性が出たあとです。脆弱性を放置していて、その脆弱性を狙った攻撃に無策でいるというのが、一番危険です。

図表２



身近な例ですと、マイクロソフトが月例のアップデートを行っていますが、年間３～４回、脅威度の高い、早く対処する必要のあるアップデートが存在します。このアップデートが告知されたあと、場合によっては数時間、２～３日の内に、政府機関に対して攻撃が始まることがあります。通常でも、２～３週間のうちに、この脆弱性をスキャンしにくるという攻撃が発生します。このスキャンは、皆さまのところにも必ず来ていると思われます。こういう脆弱性に対応していないと、Emotet やランサムウエアは、権限を持っている方のなかへ侵入する行為から始まりますので、こういうものを確実につぶしておくことが重要ですが、その先に、ゼロデイ（情報セキュリティ において、 セキュリティホールが発見された日から、その脆弱性を解消するための対処方法が確立される日までの期間）対策があるということです。

環境変化をとらえるということで、コロナによって大きく様相が変わっています。2020年３月から４月のあいだに、テレワークを狙う、つまり VPN の脆弱性を狙っている攻撃と、テレワーク環境下における脆弱なパソコンを狙っている攻撃が多数、発生しています。

2020 年に、やむを得ずテレワークを例外的に認めていて、その状態が一年間、放置されていました。いきなりの状況だったわけですから、2020 年の措置は、やむを得ないと思います。しかし、これが一年間、放置されているということは、システム管理者が十分な管理下においていないパソコンを使って、テレワークが一年間行われていたことになります。

今からでも遅くないと申しあげておきます。皆さまにとって、テレワークの環境が、どのようなセキュリティポリシーで行われていて、例外措置のまま認めているのであれば、一刻も早い是正と、どのような形で私物の業務利用を認めるかということについてのポリシーの見直しをお勧めいたします。

こういうものでも捉えきれないのが、国家の関与が疑われるサイバー攻撃です。APT(Advanced Persistent Threat)と呼ばれる、持続的な、執拗にある人を狙い続ける攻撃は、排除できないものがあるのでしょう。図表２では、APT40 の例を挙げていますが、2021 年の４月に、警察庁が談話として、JAXA を狙った攻撃で実際に動いていた人たちが中国の人民解放軍である可能性が高いことがわかったので、中国に対して、苦言を呈しています。警察が名指しで他国を挙げた例は、初めてです。安全保障の文脈のなかで抑止力として、「われわれは知っているぞ」ということを明らかにして、邪悪な意思を止めるというのは、米国、英国が始めています。われわれも、どこまでできるかということや、技術的な能力の問題もありますが、そういう意図を持ち続けるということについては、2021年９月のサイバーセキュリティ戦略のなかにも書かれています。

ウクライナへの侵攻の前後において、さまざまなかたちでリスク低減措置や、なんらかのインシデントが発生したときに、対処ができるかということを、あらためて確認いただきたいという注意喚起の文書を出しています。幸いにして、侵攻事案において、直接的な

攻撃の対象にはなっていなかったと推察されています。ただ、この時点において、非常にリスクが高いと、政府機関が共通して認識しました。

サイバーセキュリティ戦略のなかでは、DX with Cybersecurity、２つを同時に進めましょうといっています。調査したところ、DX 投資は増やしたいとおっしゃっている方がたくさんいますが、それに対応したセキュリティ対策をつくりましょうといっている方は、あまり増えていないように見えます。セキュリティ対策への経営層の関与が大きく進展しているかどうかは、他国との差異があります。直近１年に実施をしたセキュリティ対策の実施のきっかけは、トップダウンによる指示だったものが、米国では 54.8%、日本は 20%強という状態です。米国で目を引くのは、株主や取引先からの要請があって、ガバナンスの観点、もしくはステークホルダーから注文があって、その一環として、セキュリティ対策が、一般的になっているということです。

米国では、証券取引委員会（SEC）が、セキュリティのインシデントについて、正当な理由なく、報告をしない場合には罰金を科すという勧告を４年前に出しています。また、適時報告のなかに、セキュリティに関する対策、もしくはインシデントが起きたときの報告を、義務づけをしようという動きをしています。まだ、われわれはそこまで至っていませんが、こういうものをどうするのか、ということは、経営層に属する方々にお考えいただきたいと思います。

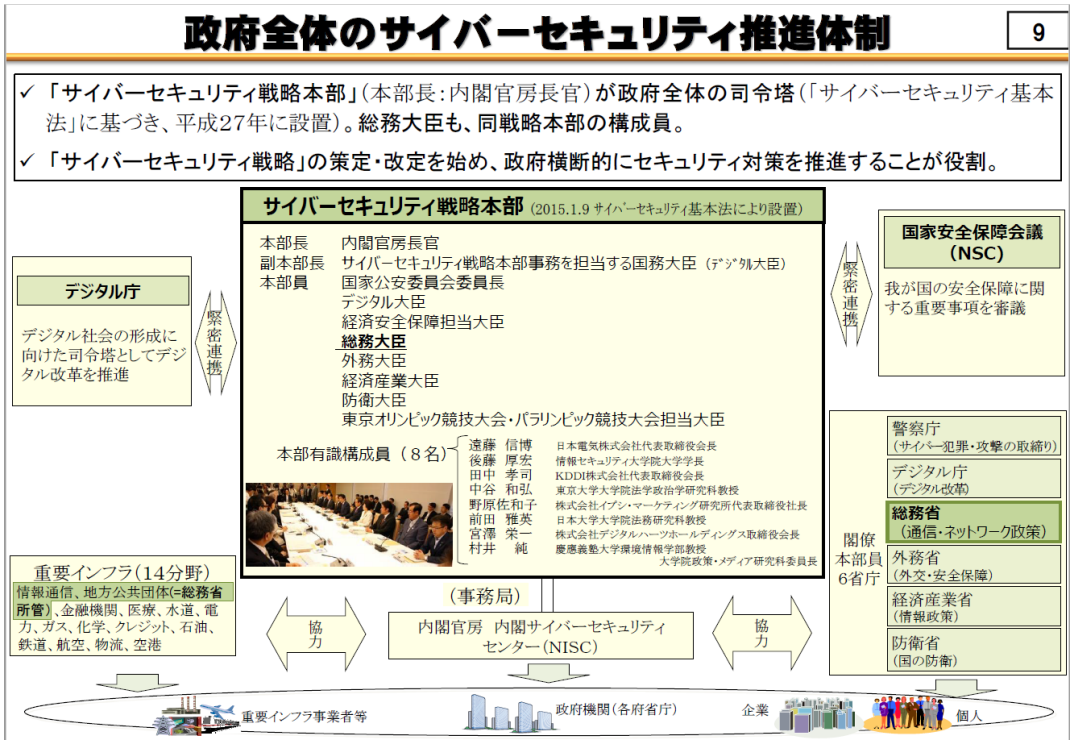
サイバーセキュリティ戦略本部

政府全体では、サイバーセキュリティ基本法に基づいて、サイバーセキュリティ戦略本部が設けられています（図表３）。内閣官房長官が本部長で、総務大臣も含めて本部員がおり、おそらく、オリパラの大臣は、程なく本部員から外れます。経済安全保障担当大臣が 2021 年の時点で追加されました。デジタル庁とは、前身の IT 室時代から当然ながら緊密に連携し、国家安全保障会議とのあいだでも密接な連携をしています。事務局は内閣サイバーセキュリティセンター（NISC）で、閣僚本部員を出している省庁とも連携をし、14 分野の重要インフラと連携をし、総務省は、ここのなかでも情報通信、それから地方公共団体を所管する立場です。

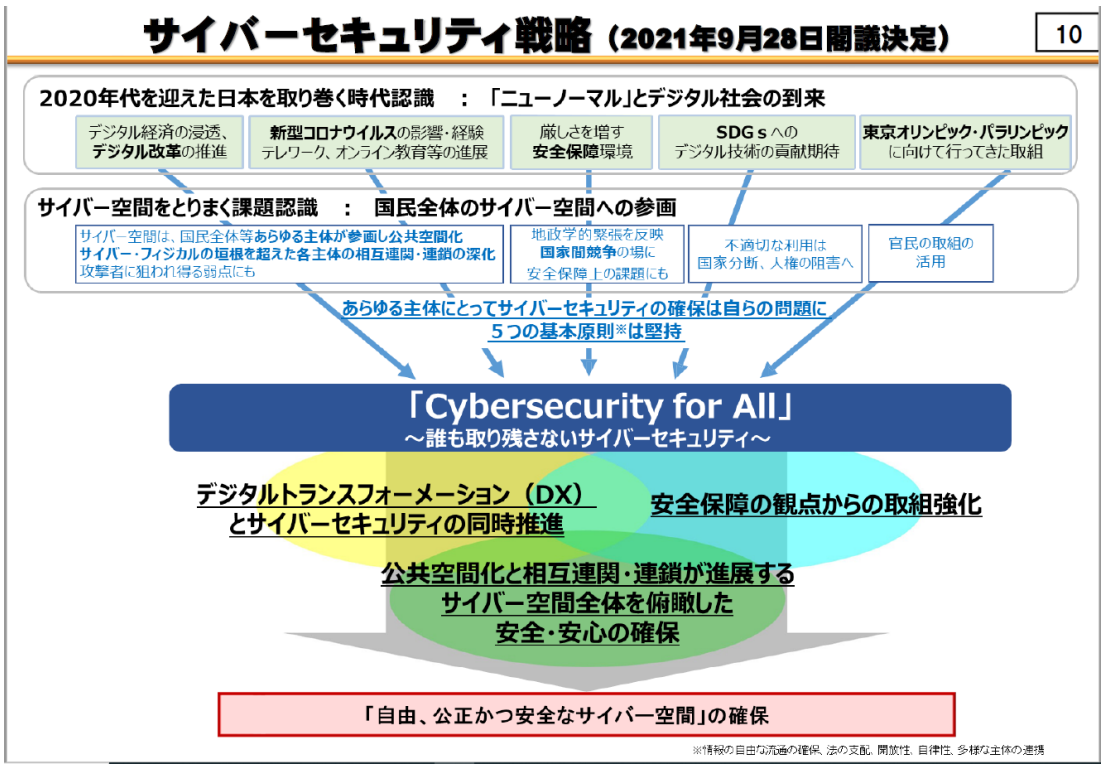
サイバーセキュリティ戦略

サイバーセキュリティ戦略について（図表４）、標語は、「Cybersecurity for All」、IT 化は誰も取り残さないということを標榜している以上、サイバーセキュリティでも誰も取り残さないということを目指します。「自由、公正、かつ、安全なサイバー空間」については、戦略には明確には書いていませんが、中国、ロシアに対するアンチテーゼとして、自由で公正で、かつ安全なサイバー空間を有志国、同志国とともに目指しましょうというのが、われわれの立場です。

図表３


政府全体のサイバーセキュリティ推進体制
9
✓「サイバーセキュリティ戦略本部」（本部長：内閣官房長官）が政府全体の司令塔（「サイバーセキュリティ基本法」に基づき、平成27年に設置）。総務大臣も、同戦略本部の構成員。
✓「サイバーセキュリティ戦略」の策定・改定を始め、政府横断的にセキュリティ対策を推進することが役割。
サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）
本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部事務を担当する国務大臣（デジタル大臣）
本部員　国家公安委員会委員長
デジタル大臣
経済安全保障担当大臣
総務大臣
外務大臣
経済産業大臣
防衛大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣
本部有識構成員（８名）
遠藤　信博　日本電気株式会社代表取締役会長
後藤　厚宏　情報セキュリティ大学院大学学長
田中　孝司　KDDI株式会社代表取締役会長
中谷　和弘　東京大学大学院法学政治学研究科教授
野原佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英　日本大学大学院法務研究科教授
宮澤　栄一　株式会社デジタルハーツホールディングス取締役会長
村井　純　慶應義塾大学環境情報学部教授 大学院政策・メディア研究科委員長
デジタル庁
デジタル社会の形成に向けた司令塔としてデジタル改革を推進
緊密連携
国家安全保障会議（NSC）
我が国の安全保障に関する重要事項を審議
緊密連携
閣僚本部員６省庁
警察庁（サイバー犯罪・攻撃の取締り）
デジタル庁（デジタル改革）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）
重要インフラ（14分野）
情報通信、地方公共団体(=総務省所管)、金融機関、医療、水道、電力、ガス、化学、クレジット、石油、鉄道、航空、物流、空港
協力
（事務局）
内閣官房　内閣サイバーセキュリティセンター（NISC）
協力
重要インフラ事業者等
政府機関（各府省庁）
企業
個人

図表４


サイバーセキュリティ戦略（2021年9月28日閣議決定）
10
2020年代を迎えた日本を取り巻く時代認識　：「ニューノーマル」とデジタル社会の到来
デジタル経済の浸透、デジタル改革の推進
新型コロナウイルスの影響・経験 テレワーク、オンライン教育等の進展
厳しさを増す安全保障環境
SDGｓへのデジタル技術の貢献期待
東京オリンピック・パラリンピックに向けて行ってきた取組
サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画
サイバー空間は、国民全体等あらゆる主体が参画し公共空間化
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
地政学的緊張を反映 国家間競争の場に 安全保障上の課題にも
不適切な利用は国家分断、人権の阻害へ
官民の取組の活用
あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持
「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～
デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進
安全保障の観点からの取組強化
公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
「自由、公正かつ安全なサイバー空間」の確保
※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

まず、先ほどの DX とサイバーセキュリティの同時推進、があります。また、安全保障は切っても切り離せません。この観点からも取組を強化します。さらに、サイバー空間、ICT が公共空間化をしており、すでにサイバーの空間のなかに、みんなが生活しています。また、サプライチェーンのことを考えると、どこかで起きたことが、サイバー空間のなかで、隅々まで、連鎖して影響しかねないという状況が起きています。そうすると、サイバー空間全体を俯瞰して、どのように安全、安心を確保するか、ということを考えなくてはならなくなっています。

戦略の構成について、いくつかのポイントに絞って、紹介します。５つの基本原則には、順番に意味があり、情報の自由な流通の確保が、法の支配の前にあります。自由な流通の確保が、一番前にあるというのが、非常に大きなポイントです。

2021 年の戦略を 2018 年の戦略と比較してみると、まず、リテラシー対策について、高齢者を新たに追加しています。Cybersecurity for All といったときに、取り残されかねないのは、セキュリティについて十分に理解ができないままに、スマホを使わざるを得ない高齢者の方、こういう方にも、一定のリテラシーが必要と追加したのが、大きなポイントです。

重点領域については、サイバー関連事業者と呼んでいますが、クラウドの事業者や CDN（コンテンツ配信ネットワーク）の方も、どのように一緒にカバーをしていくのかということを考える必要があります。また、いわゆる情報窃取のリスクを考えると、知的財産や個人情報を扱っている方々をどう守るかについても考えることとしました。

防御態勢については、これは今、内閣サイバーセキュリティセンター（NISC）を中心に、ナショナルサート機能を強化しています。縦割りで、いろいろな情報が集まらないという課題を解消すべく、NISC の内部を含め、2022 年の 6 月に体制変更をしています。

警察庁でも、2022 年 4 月から、今まで複数の局に分かれていたサイバー関係というのを集め、サイバー警察局を設置しました。また、複数の都道府県にまたがる事案を担当するサイバー特捜隊を警察庁直下の管区警察局の下に同時に設置しました。目的は、各都道府県警を連携させて、どのようなかたちで、どういう基準なのかということを合わせるという作業をし、複数の県にまたがる犯罪の捜査を一元的することです。

経済安全保障については、IT インフラの信頼性を高めるために、2022 年 5 月に、経済安全保障推進法が成立しました。基盤インフラの防護のために、特定の事業者の基幹的な設備については、サプライチェーンまで含めて、安全性を確保することが規定されています。

安全保障では、外交安保上の優先度や、「妨げる能力」の活用がポイントです。「妨げる能力」とは、具体的に国の名前を挙げて、その国における、何か脅威であるということを名指しして、われわれは知っているぞということに始まり、外交当局下の直接的な会話を含めて、抑止力を活用したいということです。

事業会社等において、専門家ではなくてもセキュリティの概要を知っている方々が持っている知識をプラスセキュリティといっています。人材育成については、ある程度、セキュリティを知っているこの方々を増やすために、プラスセキュリティ知識を補完しようとしています。また、近い将来にリスクとして見える AI、それから量子コンピュータによる暗号の危殆化といったものに対し、対応の具体化をしていかなくてはいけないということを、戦略に書いています。

2022 年 6 月 17 日に戦略本部が開催されて、重要インフラのサイバーセキュリティ行動計画が決定されました。これまでの計画は、「重要インフラの情報セキュリティに係る行動計画」と書いてありました。「情報セキュリティに係る行動計画」という文字を経営層の方が読むと、それはシステム屋の話ですねというところにいくので、訴求のポイントとして、いわゆる経営リスクの一環に、サイバーセキュリティがあるということをぜひ知っていただきたいということで、タイトルを、「サイバーセキュリティに係る行動計画」という名前に変えています。

この行動計画では、組織統治の一部としてサイバーセキュリティを組み入れます。障害が起きたとしましょう。送金システムに LAN が組み込まれている場合、LAN のシステムが落ちた場合には、取引が止まります。企業行動の一部が阻害されるので、そこで損失が発生するということを、ぜひ、経営層の方にご認識をいただきたいと考えています。まして、それがサイバー攻撃を受けてということであれば、それにどう対応したかということを報告する必要が出てくるのではないかと考えました。

この障害対応体制の強化について、経営層、それに直接的な責任を持つ最高情報セキュリティ責任者（CISO)、それを支える戦略マネジメント層の方、現場にいるシステム担当の方が、組織統治の一部としてサイバーセキュリティを認知し、経営層が、障害が起きたときに何をすればいいかを知っていただくということが重要です。障害対応体制の強化は、今までの行動計画では、３番目に入れていました。これまでは、安全基準等の整備、浸透が前でしたが、インシデントが起きた、もっとひどい事故が起きたというときに、どう対応するかということこそが経営層に求められているとしました。もちろん、それを起こさないための事前の努力が必要です。そのための資源配分をどうするかということを含めて、組織統治の一部として、サイバーセキュリティをお考えいただきたいというのが、今回のこの行動計画の一番のポイントになっています。

経済安全保障推進法

経済安全保障推進法の大きなポイントは、まず、基幹インフラ役務について、14 分野[1]において役務の安定的な提供をするために、実施すべきことが書いてあります。特定重要

[1] 情報通信、金融、航空、 空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む)、 医療、水道、物流、化学、クレジット及び石油

物資、半導体等が例になりますが、その安定的な供給を確保するために、さまざまな取組をします。また、デュアルユース等が念頭にある先端的な重要技術の研究開発支援や、国とし保全したい特許があった場合に、秘密特許をどうするかといったことを含む、法律が成立しています。

法律の成立だけでは終わりでなく、経済安全保障のなかで、まだ手だてが尽くされていないものもあるので、今回が始まりの始まりで、こういうものを積みあげていくことによって、経済安全保障を全うしようという議論が、これからも続きます。

総務省の取組

これまで説明した全体像のなかで、総務省は何ができるかということを少し話します。昨年までの当面の目的であった、オリンピック・パラリンピックに向けての体制整備が終わりましたので、あらためて、何をすることが必要なのかという話です（図表５）。

図表５

まず、情報通信ネットワークをどのように守っていくかという議論で、特に注目しているのが、通信の秘密に係る新たな法的整理を前提とした電気通信事業者におけるフロー情報です。総務省に対する誤解を招く要因として、電気通信事業者、ISP がエンドユーザーのトラフィックの情報のすべてを記録していると思っている方がたくさんいらっしゃるようです。そのため、事業者のログを見ると、普通の方が保存できていない情報があると思っている方がいるわけです。ISP が、「いや、そんなものはありません」というと、「総務

省が通信事業者と結託して、通信の秘密の名の下に、いろいろな情報を隠している」という誤解が生まれているのが現状です。

そのため、通信事業者は何ができるのかということを、しっかり考えなければいけません。フロー情報については、あるサイバー攻撃があったと認められる状況において、どこの IP から来ているのか、どのポートが使われているのかということを、しっかり分析することによって、その攻撃はどこから来たのか、どこに向かって攻撃が行われていたのかということを類推ができる可能性があります。しっかりした調査によって、その攻撃の二次被害等、攻撃の被害の拡大の防止ができるのではないかと考えます。

さらに進んで、ある種のビッグデータの解析ができるようになると、振る舞い検知を行うことによって、似たようなトラフィックが走ったときに、サイバー攻撃の蓋然性を捉えることによって、攻撃が成立する前の時点で、なんらかの措置ができないのかと考える時期に来ているというのが、今の時点での推察です。2021 年度の補正で、この実証実験の予算化をしています。ICT 対策の方々と連携をして、どの程度、私が申しあげた仮説が実際に有効なのかということを示し、そのデータを元に、このサイバー攻撃に対する対応を進めていることを掲げています。

IoT におけるサイバーセキュリティについては、2019 年 2 月から「NOTICE 注意喚起」を始めています。監視カメラ、それからルーターにおいて、ID、パスワードが不備である方々について、情報通信研究機構（NICT）に調査をしてもらって、通信事業者、ISP に対して通知をして、そこから注意喚起をします。実施にあたって、ID、パスワードの調査をすること自体が、不正アクセス禁止法に触れるため、この除外規定を NICT 法においているのですが、これは時限になっており、2024 年 3 月には終わります。しかし、ID、パスワードの不備は枚挙に暇がありません。

また、ID、パスワードに不備がある人だけが脆弱性を持っているわけではなく、最近の例では、ルーターに脆弱性が見つかりました。倒産や年数が経っているためのサポートの中止、古いメカニズムの変更ができない等の理由から、ハードウエアに脆弱性が発生をしているが、有効な手段がとれない例があります。こういうものを是正する手段について、われわれも対応の仕方を少し考え直さないといけないと思っています。こういうものに対応ができないと、IoT 機器の脆弱性の調査の有効性を訴求することは難しいです。

通信事業者が注意喚起をすることが、現時点の最終手段だというのも課題です。注意喚起をするだけにとどまって、それ以上の強硬手段はとれません。現状では、端末設備は、技術的に合致をしていると認められれば、あとから認められた脆弱性を、今の技術基準に合致しないといえない状態にあります。脆弱性が明らかになっているのにもかかわらず、技術基準に合致しているのかについて、議論は行うべきことと思っています。

サプライチェーンリスクについては、５G のオープン化に後ろ向きな勢力が混じっている欧州から持ちかけられている議論があります。５G のオープン化には賛成だが、実際の基地局設備、例えば、いわゆる CU（集約ノード）とか DU（分散ノード）といわれてい

るユニットもオープン化され、仮想的に一体化していて、ネットワークを介してつながっていることによって、ネットワーク上の脆弱性を増やしているということになるのではないかという議論です。いろいろなソフトウエアによって構成されるということは、それらのソフトウエアの正当性をどうやって検証するのかということについて疑義がある。これについてリスクが増えていくということを、ヨーロッパでは主張しています。一定程度、リスク源としての主張は合理性がありますが、疑問は残ります。オープン化しない場合、ネットワークとしてはクローズドかもしれませんが、ネットワークがつながっているということには変わりがありません。そうであれば、どこに本当にリスクがあるということを、吟味する必要があると思っています。

現時点、設計の指針としての５G のセキュリティガイドラインの策定をして、これを事業者の方々と共有していますが、もう少し進めて、Software Bill Of Material（SBOM）、わかりやすくいうとソフトウエアの血統書、これをどのようにつくるかという議論を進めながら、オープンソフトウエアになったときに、トレーサビリティの確保やアップデートの確認について、実施可能な手段について議論をしていきたいと思っています。

SBOM の議論は、NISC を中心に政府機関に導入する情報システムのなかでも、同様に検討しています。米国では政府機関に導入することをすでに宣言して、SBOM のあり方の検討を開始しています。米国での導入の動きを見ながら、検討を進めていきたいと考えています。

人材育成は、地方公共団体向けの実践的サイバー防御演習（CYDER）と、オリパラ向けにやっていて 2021 年に終わったコロッセオがありました。コロッセオがわりと好評だったもので、2025 年大阪万博向けに研修プログラムを実施したいと思っています。

国際連携についてのポイントは、ISAC（Information Sharing and Analysis Center）を通じて民ー民間でもやっていますというお話と、QUAD のなかで議論をして、東南アジア向けに日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）を通じ、国際協力機構（JICA）と連携をしながら東南アジア諸国のセキュリティリテラシーの向上、キャパシティービルディングの研修をやっている、という２つが主なものです。また、太平洋地域については、オーストラリアに前に立ってセンターを設立してもらって、仲間を増やす作業に出ていきたいと思っています。太平洋地域では中国側になびいている国が出てきているので、キャパシティービルディングを実際に進めていくことによって、少なくとも、一方的な見方にならないという取組を進めていきたいと思っています。

普及啓発のポイントは、サイバー攻撃被害に係る情報の共有です。被害組織において、どんな攻撃を受けたか、どこから、どこの IP が見えているかとか、どういう手段かについて情報を共有していただくと、被害の防止につながると思っています。被害情報の公開については、２つ大きな壁があります。１つは経営層の無理解で、２つめが、コンプライアンス上、企業情報を出せないとして、法務部門がストップするパターンや報道部門に、なんでうちの恥をさらすんだといって止められるというパターンです。そのため、企業の

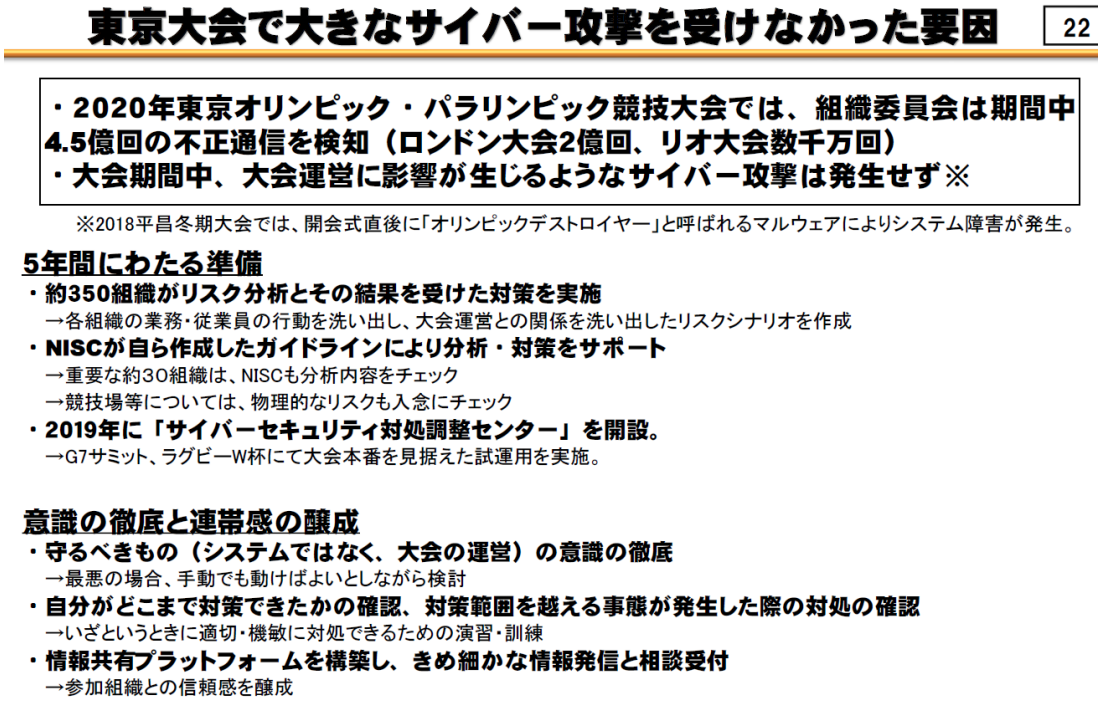
コンプライアンスなり統治の観点を含めて、どんな情報を、どういうポイントを踏まえて、どういうタイミングで、どういうふうに共有、公開されるのが適切なのか、例示としてのガイダンスを 2022 年内に行いたいと思っています。

東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策

東京オリンピック・パラリンピックについては、大会の運営に影響を与えるようなサイバー攻撃はありませんでした。4.5 億回ぐらいのサイバー攻撃、正確にいうと、怪しげな通信が組織委員会で確認されていますが、重要サービス事業者を含めて、幸いにして、影響は出ませんでした。日本のなかではあまり話題になりませんが、外国では、東京大会はサイバーについては成功していると、高い評価だったと思っています。

成功の要因を、NISC に設置されたサイバーセキュリティ対処調整センターの副センター長として振り返ってみました（図表 6）。2016 年ぐらいから、実際の対応を始め、準備期間が 5 年間です。350 ぐらいの組織に協力をいただいてリスク分析をして、その結果の対応についても検討することを計 6 回行いました。この間に挫折をした組織が多数あって、これは、うちの担当じゃないだとか、これは IT の話じゃないから、ここまでやらなきゃいけないのかという議論がありました。

図表 6



実際のリスクとして、IT サービスが止まる原因は様々です。コンピュータが壊れることもリスクの一因です。第一は、しっかりした管理体制のなかでシステムを動かしていないと、セキュリティ対策にもならないことをおわかりいただくことです。国際放送センター

（IBC）のリスクを実際に見たときに、われわれが指摘したうちのひとつに、避けられないこととして、ジャーナリストが持ち込んでくるマルウエアつきの PC がありました。これは、検知を一生懸命やるしかありません。もうひとつが下水道です。下水道のシステムには水冷の機能もあり、下水道が止まると、上水道も止まるのですが放送センターには、大量のサーバーが入っているので、下水道が止まると、水冷機能が効かなくなって、おそらくコンピュータの稼働が止まります。つまり、IBC が動かなくなる。「下水道が止まったらどうするのですか」と聞いたら、みんなから驚いた顔をされたそうです。対応としては、大規模なイベントのときには、実際にポンプ車を持ってきて強制排水することを、ビッグサイトの運営者に提言するところまでやっています。

申しあげたいことは、IT のリスクは必ずしも IT の中だけにとどまっていない、リスク分析を行うなら、そういうところまでやらなければならないことです。これが、大きな気づきですが、今回参加いただいた方々にも、物理的なリスクを入念にチェックするというのが、一番大きな資産だと言っていただいています。

それから、G7 のサミットとか、ラグビーのワールドカップのときに、対処調整センターはすでに稼働していましたので、トライアルをやっていました。24 時間はりついて、実際、何かあったときにどうするということもやりました。ワールドカップのときに、競技会場で照明が 1 度消えています。これについては、最初から予定している容量を超えたときには観客席の照明は消えてもいいということになっているらしくて、予定行動だから大丈夫と組織委員会から連絡がきたので、大騒ぎにならず「そうですか」と留まったのですが、そういう情報まで全部共有をするということをやっていました。

何かなかったという報告だけじゃなくて、リスクにつながる情報を集めたうえで、それが問題ないのかを判断するということが必要だとこのときによくわかりました。そのため、本番のときには、組織委員会と密接に連携をして、サイバーセキュリティの担当でない部署とも連携をしていました。

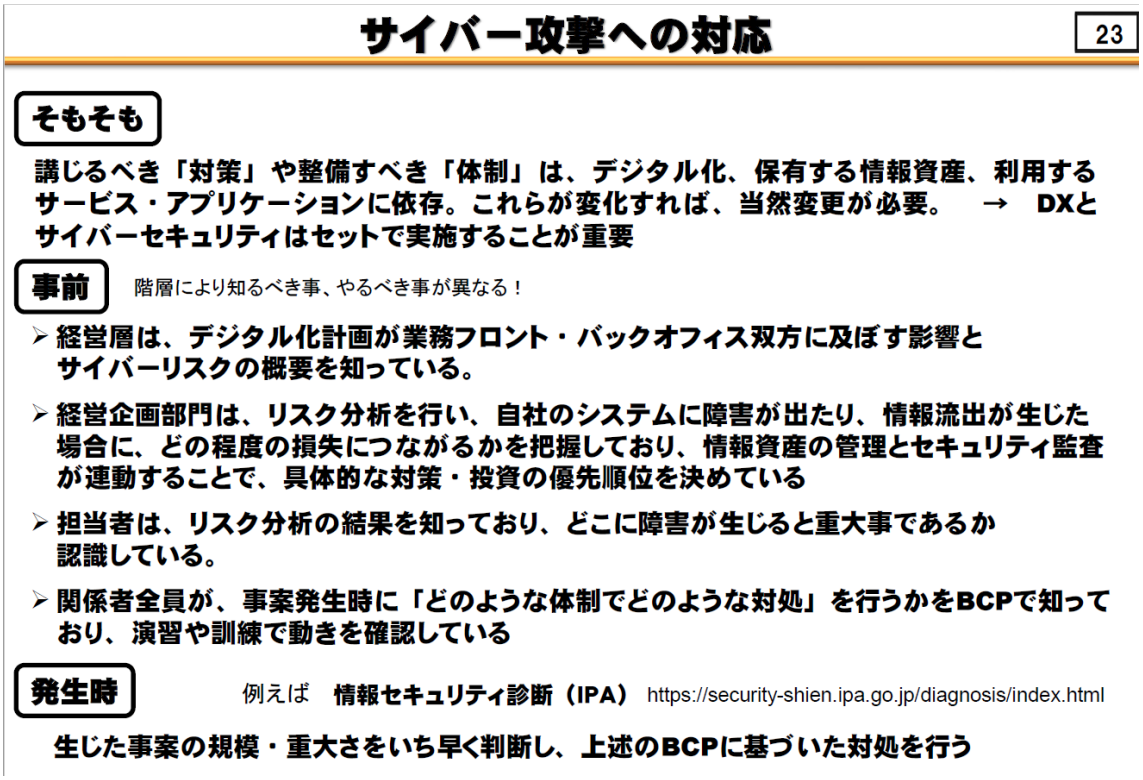
「意識の徹底」と表現しましたが、オリンピックの場合は、大会を円滑に運営することが目的です。システムを守ることではありません。すなわち、場合によっては、サービスを提供できるときに不完全でもいいということを念頭において、対処のシナリオを考えていただくということです。また、本当に、そういうことが起きたときに、どうしようかということを適切機敏に判断できるということが必要です。自分たちだけで悩む必要はなく、秘密を守れる人という条件はつきますが、参加組織と信頼感を醸成しながら、きめ細かな情報発信と相談を受ける、そういうことが非常に大切です。

サイバー攻撃の対応として目指したい姿

最後にサイバー攻撃の対応について考えますが、よく聞かれる質問で答えに困る話を先にします。それは、「わが社のサイバーセキュリティ対策はどうしたらいいですか」という質問です。「御社のシステムを知らないので答えられません」というのが、私の率直な

答えです。保有している情報資産がどうなっていて、どんなサービスを守りたいのか、どんなアプリケーションを使っているのかということに、完全に依存します。さらにいうと、それが変化をしているのであれば、必要な変更をしなければいけないということです。今の状況にあてはめると、各社は、DX を進めていると思うので、それと一緒にセキュリティをやらなきゃいけないというのが、そもそも論です（図表７）。

図表７



私が願う姿ですが、経営層の方は細かく知っている必要はなく、DX を進めるときに、その DX が、業務フロント、バックオフィスに、よい面でどういう変化が出るかを掴むことです。何が止まるとまずいのかということも知っていただくということだと思います。それを支える方々は、システムの障害、情報流失が出たときに、それがログオーダーでどれくらいなのか、どういう損失につながるかということがわかる必要があります。実務的にいうと、止まったときに、「どうなっているんだ」って聞く担当者が特定できているということだと思いますが、システム担当者と連動して、情報資産、つまり IT 資産管理ができていて、対策投資の優先順位が決められているということを、経営企画の方には知っていただきたい。担当の人はリスク分析の結果を知っていて、何が起こるとまずいのかということを知っているということが重要だと思います。上司に相談しないといけない、報告しないといけないことに優先順位づけができているということが必要です。この状態に至ったときに、どういう体制でどういう対処をする、誰が意思決定をする、ということを、BCP に落とし込むことを、ぜひやっていただき、それを演習・訓練で確認をしていた

だきたい。IT 資産って何っていうところから始まる方は、IPA が情報セキュリティ診断をしていますので、一回実施していただくことをお勧めいたします。

IT 資産管理は、もともとは資産管理の一環です。デジタル化を進めるときに、効率化・重複排除ということでやっていますが、最近はコンプライアンスだとか内部統制の強化、セキュリティの強化という観点で使われているといえます。たとえば、サブスクモデルが増えてきているので、ID とかアカウントの発行数と実態が異なっていると損害賠償になり、企業レピュテーション上、まずいことになります。セキュリティ側では、適切にアップデートされていないというのはまずいです。自身の経験でも管理下にあるパソコンのうちの５％くらいはアップデートが成功していないことがありました。管理者が実施したと思っていることが、実際にそうなっているという保証がないことを、痛感したことがあります。

IT 資産管理ソフトは、高価です。当面は手動でも、後々の人件費、抜け漏れがない、継続的に動かせるという観点で、私としては、若干高くても、IT 資産管理は自動的なソフトウエアでやることをお勧めいたします。例えば、セキュリティポリシーで禁止されている USB を接続したことがログで残ります。普通は禁止されていることを、検知できないとことに問題があります。

サイバー攻撃への具体的な対応例として（図表８）、今、申しあげた、情報資産の適切な管理をしっかりやっていただきたいと思います。規模の小さい方にとってはクラウドへの移行は、メリットがあります。任せられるということだけでなくて、セキュリティのレベルの向上が期待できます。一方で、クラウドベンダーで気をつけるのは、いろいろな契約条件において、責任分解点が違います。そうすると、自分に任されているところがどこかということを、正確に知っておかないといけないということです。また、契約条件によって、よくも悪くも機動的に内容を変えられるので、変えた結果がどうなっているかも、知っておかないといけないということです。

職員の自覚も必要です。お気をつけいただきたいのが、標的型攻撃メール訓練を実施したときによくあるのが、開けちゃった人を怒ると、その人は次の時は隠して報告しなくなるので、報告に対しては怒らないということをぜひ徹底していただきたい。これは、けっこう重要です。怒ったことで担当者が隠すようになり、大きな事故が発生した事例が実際にあります。

リスクゼロ、サイバー攻撃リスクは絶対ゼロにならないので、それを前提にすべきというのもポイントです。そういうことが起きたときにどうしようかということを、決めていただくということですし、バックアップ、システム復旧の手順が決まっていないと、そのときに考えても間に合いません。ぜひ、そういう手順を BCP、コンテンジェンシープランと、コンティニュイティプランのなかに収めていただきたいと思います。

最後に、セキュリティ対策を実施するのは人です。ぜひ、内部で育成、確保していただきたいと思いますし、いなかったら、頼れる相談先を確保して、単独で無理なら共同で囲

い込みましょう。「ISAC から誰か供給してもらえないの」、そういう話でもいいと思います。それから、適切な処遇とキャリアパスの設定も必要です。最近まで、例えば銀行では、いわゆるシステム担当の「上がりポスト」がシステム部長でしたが、これだとやる気が起きません。今では改善されて、適切なキャリアパスが設定されています。担当者のやる気につながるかたちで、人材育成をしていただければ、セキュリティの人材は増えるのではないかと、期待しております。

最後の部分には、私見を交え、今までの経験からお話をさせていただきました。

図表 8