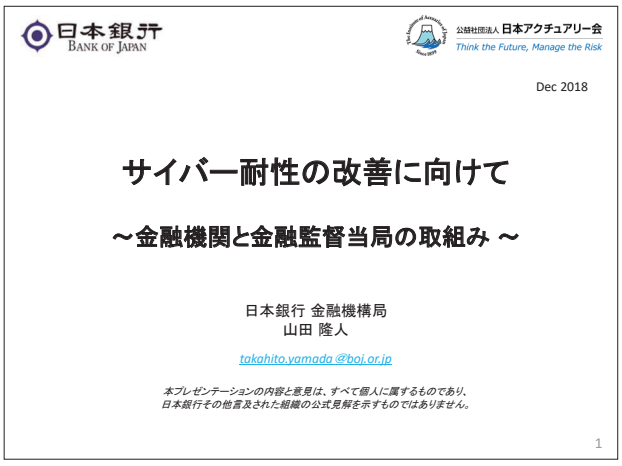
講　演

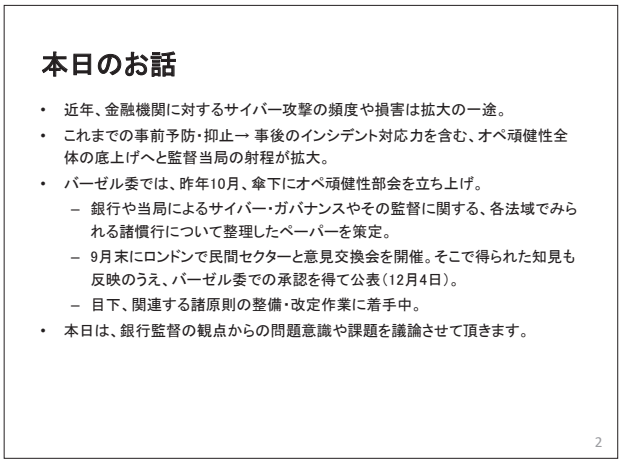
サイバー耐性の改善に向けて
～金融機関と金融監督当局の取組み～

日本銀行　金融機構局　山田　隆人

日本アクチュアリー会 CERA 研修講演 2018 年 12 月 7 日　日本アクチュアリー会大会議室

日本銀行の山田隆人と申します。1995 年の入行以来、海外を含む多くの部署で仕事してきましたが、現在は金融機構局で金融規制監督の枠組み作りをお手伝いさせて頂いております。本日のテーマはサイバーリスクです。お仕事でサイバー保険などを手がけられていらっしゃる方がいらっしゃいましたら、その道のプロとしてのご知見など拝領できれば有り難いです。

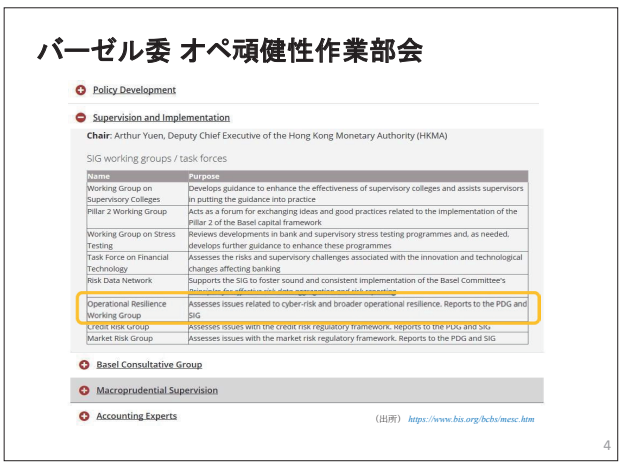


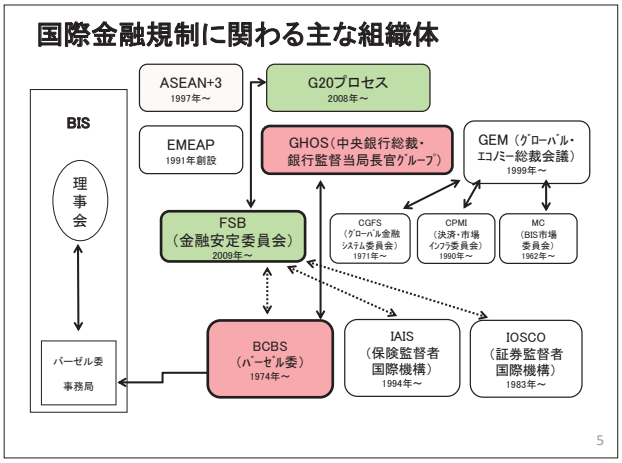


BCP ないし業務継続計画という言葉は、皆さまにも馴染みのあるものと思います。これまで多くの自然災害に見舞われてきた日本では、ある意味で強みのある分野であったりします。ただ、あまりサイバーの世界には活かされてこなかった面もあろうかと思います。むしろ専ら IT の議論に偏重していたといってもよいかもしれません。

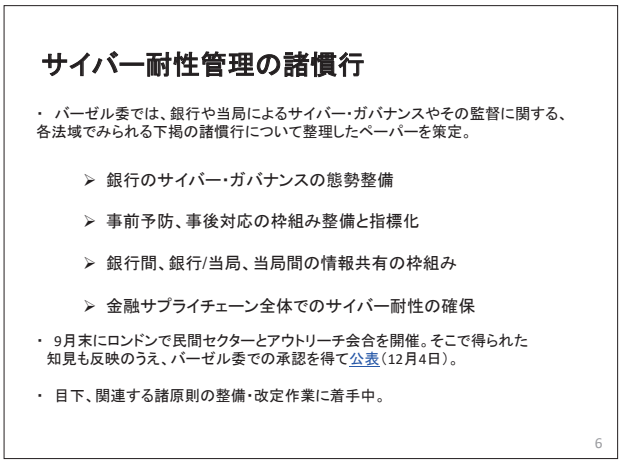
ちょうど昨日（12 月 6 日）も某通信事業者のキャリア網が全国でダウンしていました。もちろん、あのような不具合が発生すると非常に困る訳ですが、一方で極端なリスク回避も全体最適とは言えません。よく金融機関の業務基幹系システムの開発や運行管理などの世界では、99.9999…と安定稼働率の 9 の桁数を競い合う光景に遭遇しますが、私は以前から違和感を覚えていました。この違和感の原因は何か。いくら事前予防、抑止に最善を尽くしても、リスクはゼロにはできませんし、実際に大なり小なりのサイバー事象は常に起こっています。中央銀行の世界でも、バングラデシュ中銀のように不正送金の被害にあうケースも出ています。専ら事前予防に腐心するのではなく、完全な回避、撲滅が不可避な事象、inevitable breach の発生を前提にして、発生してしまった場合の初動対応や影響の緩和、復元に向けた能力、これをひとまとめにサイバー耐性と呼びますが、ひいては金融システム全体としてのオペレーショナルな頑健性を高めなくてはいけないと

いう方向に、議論がシフトしつつあります。





皆さんの業界の中でも、信託銀行の方は、バーゼル委と言えば 2017 年末に最終化した銀行規制、「バーゼルⅢ」を連想される向きも多いと思います。生損保の方は保険規制の国際的な調和を担う IAIS（International Association of Insurance Supervisors）について良くご存知かと思いますが、その銀行版がバーゼル委です。また、本日のテーマ、サイバーについては、決済システムとの関係も重要です。決済システムや取引所等の重要金融インフラ向けのサイバー耐性に対する指針を出している会議体として CPMI（Committee on Payments and Market Infrastructures）が存在します。これらはいずれも同じスイス・バーゼルの中央駅前にある丸い建物に入っています。バーゼル委は世界 28 法域 45 の金融監督当局で構成されます。私は、このバーゼル委がちょうど 1 年前に立ち上げたオペ頑健性部会、Operational Resilience Working Group、ORG に金融庁の方とともに参加しています。ORG はレベル 3 にある部会です。これは、レベル 2 で規制設計を検討する Policy Design Group、PDG と規制の実施を扱う Supervision and Implementation Group、SIG の共管とされています。これはオペレーショナルな頑健性というスコープが新しい課題でありながら、日々の規制・監督の枠組みにも直結することを意味しています。



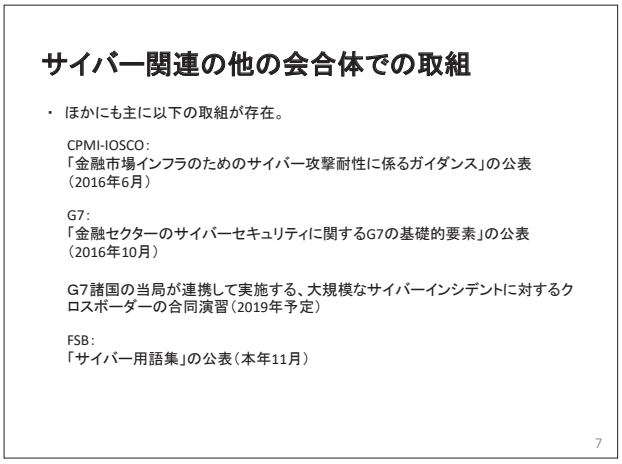
ちょうど今週 12 月 4 日に、バーゼル委から「サイバー耐性管理の諸慣行（“Cyber-resilience：Range of practices”）」が公表されました。本日は主としてこのペーパーに収録した論点、具体的には、サイバー・ガバナンスの一環として、銀行が事前予防だけでなく事後の耐性をどのような形で整備していくのかという観点を中心にお話させていただこうと思います。

2018 年 9 月末に Bank of England で民間の金

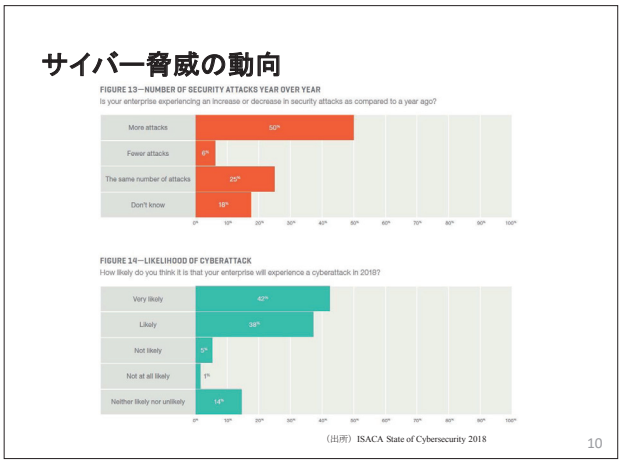
融業界の方々や大学の先生、あと、IT ガバナンスやセキュリティ監査に関する国際的な団体であるISACA などの方もお招きして意見交換会を行いました。その際、侵害訓練なども業界横断的にしっかりやっていて、事前予防の方は割と出来上がっているのですが、事後耐性の方は実は手付かずに近い状態にあり、サイバー耐性について規制監督の枠組みを整備する必要があるとの結論に到達しました。またそうした枠組みを整備するのであれば、効果の比較検証が出来なければいけません。既往の改善状況の評価や将来に向けた目標管理、さらには金融機関間や法域間での比較のために数値指標化することが可能かどうか、併せて検討していくことになりました。

また、情報共有も重要となります。一般に、サイバー脅威やサイバー事象に関する情報交換は銀行間でレシプロな形で行われています。ただ、銀行 - 当局間の情報交換も考えなければなりません。これは従来の規制報告のような一方向ではなく双方向で前広なやりとりをイメージしています。サイバー事象の多くは国家やその支援を受けた組織によるものです。ここでは当局も当事者であり、金融規制監督の局面で一般的なレフリーのような立場ではなくてむしろ一蓮托生な関係になっています。また、当局間の情報共有という観点も重要となります。ただ、先ほど申し上げた 28 法域の中には中国やロシアなども存在するのですから、これはなかなか難しいのですが、すべての法域が共通の枠組みにコミットすることを通して、ある種の抑止効果を狙うことが出来るという面もあります。

ちなみに、「当局」の定義も多義的になってきています。金融システム全体の安定を考える場合、危機が伝播するチャネルともなり得る決済インフラや取引所などの重要金融インフラにも目を配る必要があります。これは日銀では主に決済機構局が所管しておりますが、当局の中で所属部署のサイロに閉じ籠っていては何も出来ない訳です。さらに、金融サービスのサプライチェーンは、随分と延伸しています。アウトソーシングと言えば、以前であればシステム開発や現金輸送などが一般的でした。今では、Microsoft や Amazon 等が提供するクラウドサービス上で勘定系システムを運行する銀行もあり、非金融当局との連携も重要となります。そのような、我々金融当局の手の届かない第三者が多岐に亘り介在する中で、システム全体のサイバー耐性を如何にして確保するかも悩ましい課題です。



なかなか明瞭な解がない中で、バーゼル委としてはまずはファクトを整理するペーパーを作ったというのが現状でしょうか。もちろん、ペーパーだけ出しても世の中が変わる訳ではありません。今、ちょうど取り組んでいるのが G7 の金融当局合同でのクロスボーダーなサイバー演習でして、来年央の実施に向けて準備しているところであります。また、言葉の意味、タクソノミーが曖昧ですと、水掛け論になることも多いことから、Financial Stability Board、FSB の下で、サイバー用語集の第一版を 11 月初に最終化しました。例えば「compromise」という英単語は、サイバーの世界ではサイバー事象により何かしらの被害が出たり、直接的な被害は免れるも何かしらの影響が出た、ストレスを受けた、といった意味があります。そうした用語を収録しています。



さて、我々金融当局の間でも、サイバー耐性の改善という課題にもっとも熱心な先は Bank of England です。イギリスの中央銀行ですが、その他英国の金融当局と一緒にサイバー耐性管理の重要性についてディスカッション・ペーパーを書いたのが 7 月です。そもそも「サイバー耐性が改善する」とはどういうことか。定義は難しいのですが、文脈としては、停止した機能が回復するまでに要する時間が短縮していく展開を念頭においていることが多いです。現状では復旧まで 2 日掛かるところを、予め代替手段を用意したり演習を行うことで機能が停止している期間を 1 営業日に短縮するとか、日付が変わる前には復旧できるようにする、といった具合です。銀行がその日の決済を結了させ、勘定を締められないと、場合によっては当局が支払猶予令を発動する、バンク・ホリデーを宣言する、といった深刻な事態に繋がりかねません。

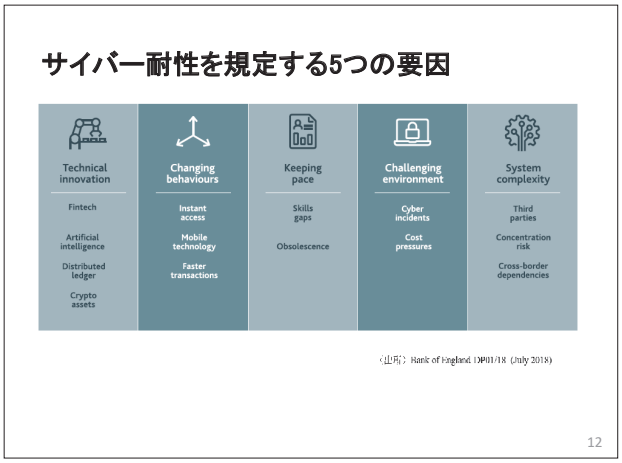
彼らがこの種のペーパーを公表する場合には、何かしらの機関決定を経ていることが多いです。中央銀行は物価の安定と金融システムの安定という、大きく二つの使命を担っており、Bank of England には二つの政策委員会 —— Monetary Policy Committee、MPC と Financial Policy Committee、FPC —— が存在します。いずれも議長は総裁が務めます。6 月 19 日の FPC の議事録には、サイバー事象が発生したときに、重要なサービスをいかに早く復旧できるか、その評価基準を作ることを議決した旨が掲載されています。

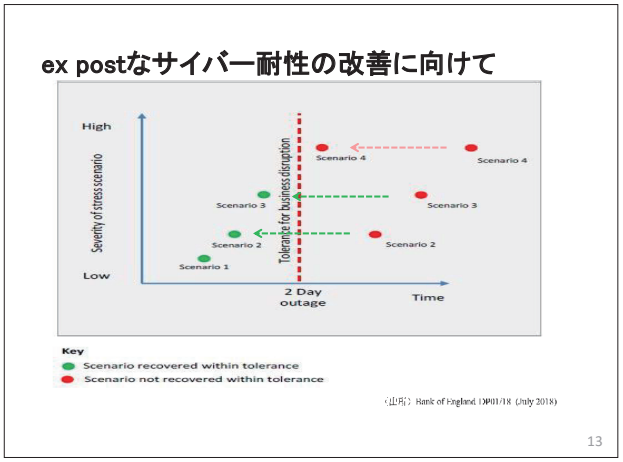
その際、National Cyber Security Centre、NCSC —— これはサイバー・インテリジェンス機関ですが —— そことも連携すると。映画 007 でお馴染みの MI6 にも近い組織です。そのうえで、サイバー耐性の評価基準が出来たら、主要な金融機関をテストしていきますと。

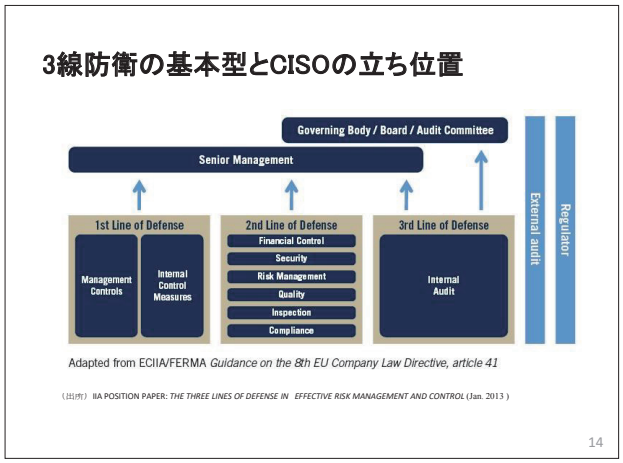
ここで、最近のサイバー攻撃の特徴を少しおさらいしたいと思います。皆さんお察しのとおり、やはり攻撃の数は増える一方です。ISACA のサーベイでは今後も増えていくとみている専門家が圧倒的に多いです。米・欧で盛んに売られているサイバー保険をみますと、従来は専ら個人情報の侵害による賠償債務を補償するための付保が多かったのですが、最近は、サイバー攻撃により送電線を止められたり、原発が暴走しかねないとして、電力会社等のインフ

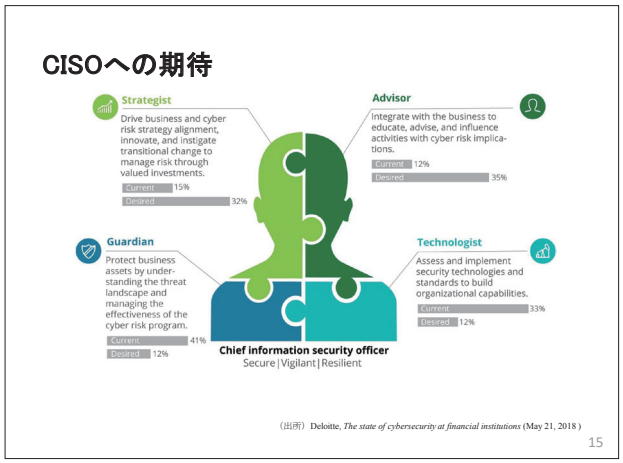
ラ事業者からの引き合いも高まっているようです。

先日、米国出張中に書店を訪れた際「パーフェクト・ウェポン」という本が平積みされていました。David E. Sanger というニューヨーク・タイムズの記者が書いた本です。この記者は、サイバー問題を追い掛けていて、特にここ３年ぐらいの動向を非常に克明にルポルタージュしています。サイバー攻撃には核の専門家もロケット・サイエンティストも要らない。最小限の投資で非常に大きな効果が得られるので、費用対効果としてはパーフェクトなウェポンであると。これは、サイバー攻撃に固有の特性を上手く捉えた表現であると言えましょう。地政学的な動向を映じて、サイバー攻撃にも地域性があります。やはりアジアでは北朝鮮、中国からのものが目立ちます。他方、中南米では、麻薬マフィア等の広域犯罪組織によるものが多かったりします。



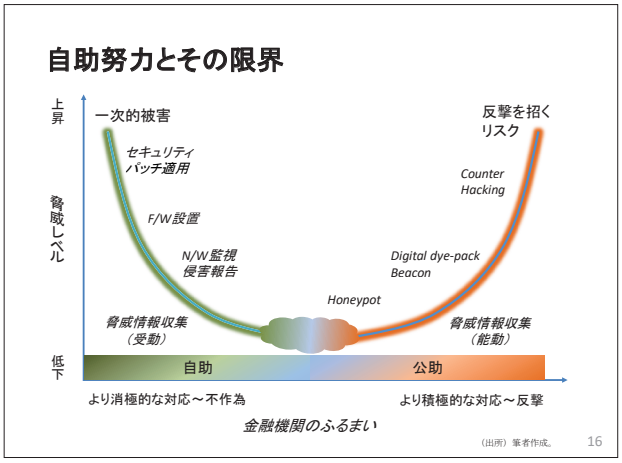






さて、金融監督の世界に話を戻しましょう。３線防衛、これはコーポレート・ガバナンスの世界でお馴染みのお話かと思いますが、ここでの Chief Information Security Officer、CISO の位置付けは各金融機関によって区々です。一般的には、Chief Risk Officer、CRO と同じ第２線に設置されることが多い。ただ、オペ・リスクも含めて通常の事前予防に主眼を置いたマンデートであればそれでよい

のですが、サイバー耐性を扱う場合は、受け身でガードしていればよいのではなく、ハッカーや攻撃者とのある種の「競争」の中で、先例に囚われず、思い切った技術革新を採用する創造性や先見性も必要となります。どちらかと言えば、第１線の Chief Technology Officer、CTO に近いマインドセットを要求されるとも言えましょう。また、影響緩和や回復過程には手作業による人海戦術を含む代替手段を採らなければならず、Chief Operation Officer、COO との連携も大切になります。かといって、CTO や COO に寄せて第１線に置けばよいという訳ではありません。収益プレッシャーの中で他の事業案件に優先順位が劣後してしまってはいけないことは、先の巨額窃取事件に見舞われた仮想通貨の取引所などをみても明らかです。



ここで、金融機関の経営者や金融当局にとっての他のリスクカテゴリーと比べたサイバーリスクの特殊性が、対応をさらに難しくします。ハッカーが古典的な銀行強盗と同じであれば、ある意味、処方箋は簡単で「自行で有効な対策を立て、十分な財務バッファーを確保してください」で済みます。また、ファイアーウォールなどのセキュリティ実装にきちんと投資して、それでも防げなかった場合はカネで解決…というお話なのかもしれません。もっとも、攻撃者が国家やその支援を受けた組織であったりすると話は別です。この対応を民間の自助努力だけに依存することはミッション・インポッシブルなのです。バックファイアが発生した場合の金融機関経営者の株主や債権者、預金者や従業員への責任を考えれば、軽々しく反撃できないし、してはいけない場合も多いのです。

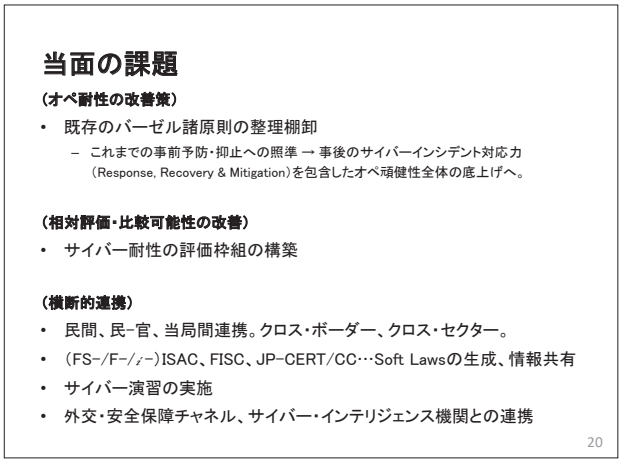
金融はもとより電力、エネルギー、交通、通信といったセクターごとに Information Sharing and Analysis Center、ISAC という組織を作って「共助」の精神で連携しています。もっとも「皆さんの『自助』ないし『共助』で対応して下さい」と突き離すことができないようなサイバー事象が増えていることも事実です。

例えば日本銀行であれば、万一、金融危機に繋がりかねない事態が発生した際に影響を最低限に留め、ないし拡がりを一定範囲に留めるべく、必要な市場流動性を供給するといった手段も用意しております。実際、1990 年代には日本でも金融危機はありましたし、アジアでは通貨危機もありました。その都度、当局間で連携して乗り越えてきたのですが、サイバー事象の場合、その先の対応は政府、それも外務や警察、防衛等の非経済省庁による措置との連携も重要になります。こうした当局間の連携の対象も大きく拡がりをみせているのが、我々当局に突き付けられた課題であったりします。

国家やその支援を受けたサイバー攻撃者が狙うとすれば民間金融セクターです。不正送金のトラップ

を仕掛けたりと、いろいろやる訳ですが、彼らは決して当局などは狙いません。米国の FS-ISAC という組織は、世界中の約 7,000 の金融機関が加盟している「共助」のための組織ですが、米国の 8 つの大手行、G-SIB がこの FS-ISAC の姉妹組織として Financial Systemic Analysis and Resilience Center、FSARC という組織を立ち上げています。これは FRB や OCC や FDIC といった米国の金融当局だけでなく、FBI や国土安全保障省などとも連携しています。あくまで民間の組織なのですが、民間側からサイバー脅威やサイバー事象に関する「ダッシュボード」を共有して、非金融当局を含む幅広い当局と連携して事に当たっているのですね。

2016 年には G7 伊勢志摩サミットがありました。ここでの一つの画期的なイベントが伊勢志摩サイバー・グループによる初めての会合開催でした。首脳レベルがサイバー問題について集まって議論したのは初めてでした。来年（2019 年）は G20 を日本がホストします。福岡で財務大臣・中央銀行総裁会合が、大阪でサミットが開催されます。2 年前の G7 とはまた異なる成果が期待されています。



さて、皆さんご存知のとおり、金融庁の検査マニュアルが廃止されます。むしろ自律的なガバナンスにお任せした方が効果的という判断かと思われますが、目線が揃わないと色々と混乱するかもしれないとの懸念の声も耳にします。もっとも、IT やサイバーの世界に関しては、あまりそうした懸念はないかもしれません。わが国には、例えば FISC のような金融機関や IT ベンダー、更に我々のような当局者もいる半官半民の場において、安全対策要綱などのソフトロー、デファクトな規範が整備されてきた長い歴史があります。今後も、法律や施行令・規則、告示などのハードローを補完する形で、こうしたソフトローをうまく活用していきながら、例えば、自然災害と闘う中で我々が整備してきた BCP を、サイバー事象に固有の特性を踏まえてファイン・チューンする形でサイバー BCP へと発展させることも可能ではないかと期待する次第であります。

以　上