

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り組み～

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えます。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ならないと



公認社団法人 日本アクチュアリー会
Think the Future, Manage the Risk

Dec 2018

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り組み～

日本銀行 金融機構局
山田 隆人
takahito.yamada@boj.or.jp

本プレゼンテーションの内容と意見は、すべて個人に属するものであり、日本銀行その他の言及された組織の公式見解を示すものではありません。

1

本日のお話

- ・ 近年、金融機関に対するサイバー攻撃の頻度や損害は拡大の一途。
- ・ これまでの事前予防・抑止→事後のインシデント対応力を含む、オペ頑健性全体の底上げへと監督当局の射程が拡大。
- ・ パリゼル委では、昨年10月、傘下にオペ頑健性部会を立ち上げ。
 - 銀行や当局によるサイバー・ガバナンスやその監督に関する、各法域でみられる諸慣行について整理したペーパーを策定。
 - 9月末にロンドンで民間セクターと意見交換会を開催。そこで得られた知見も反映のうえ、パリゼル委での承認を得て公表(12月4日)。
 - 目下、関連する諸原則の整備・改定作業に着手中。
- ・ 本日は、銀行監督の観点からの問題意識や課題を議論させて頂きます。

2

いう方向に、議論がシフトしつつあります。

バーゼル委とは？

- Basel Committee on Banking Supervision
- 国際銀行規制を議論する場として、G10諸国の中央銀行が1974年に設立。
- 中央銀行総裁・銀行監督当局長官グループ(GHOS)を上位機関とする。
- 28法域の45の中央銀行および銀行監督当局で構成。
- Basellにある国際決済銀行(Bank for International Settlements, BIS)が事務局。



3

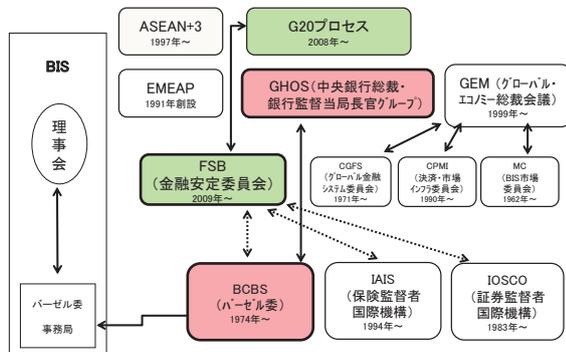
バーゼル委 オペラ健全性作業部会

Policy Development	
Supervision and Implementation	
Chair: Arthur Yuen, Deputy Chief Executive of the Hong Kong Monetary Authority (HKMA)	
SIG working groups / task forces	
Name	Purpose
Working Group on Supervisory Colleges	Develops guidance to enhance the effectiveness of supervisory colleges and assists supervisors in putting the guidance into practice
Pillar 2 Working Group	Acts as a forum for exchanging ideas and good practices related to the implementation of the Pillar 2 of the Basel capital framework
Working Group on Stress Testing	Reviews developments in bank and supervisory stress testing programmes and, as needed, develops further guidance to enhance these programmes
Task Force on Financial Technology	Assesses the risks and supervisory challenges associated with the innovation and technological changes affecting banking
Risk Data Network	Supports the SIG to foster sound and consistent implementation of the Basel Committee's supervisory framework on data access and risk quantification
Operational Resilience Working Group	Assesses issues related to cyber-risk and broader operational resilience. Reports to the PDG and SIG
Credit Risk Group	Assesses issues with the credit risk regulatory framework. Reports to the PDG and SIG
Market Risk Group	Assesses issues with the market risk regulatory framework. Reports to the PDG and SIG
Basel Consultative Group	
Macroprudential Supervision	
Accounting Experts	

(出所) <https://www.bis.org/bcbs/insrc.htm>

4

国際金融規制に関わる主な組織体



5

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

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ラ健全性部会、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。これはオペラ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。

サイバー耐性管理の諸慣行

• バーゼル委では、銀行や当局によるサイバー・ガバナンスやその監督に関する、各法域でみられる下掲の諸慣行について整理したペーパーを策定。

- 銀行のサイバー・ガバナンスの態勢整備
- 事前予防、事後対応の枠組み整備と指標化
- 銀行間、銀行/当局、当局間の情報共有の枠組み
- 金融サプライチェーン全体でのサイバー耐性の確保

• 9月末にロンドンで民間セクターとアウトリーチ会を開催。そこで得られた知見も反映のうえ、バーゼル委での承認を得て公表(12月4日)。

• 目下、関連する諸原則の整備・改定作業に着手中。

6

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、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。

サイバー関連の他の会合での取組

- ・ ほかにも主に以下の取組が存在。

CPMI-IOSCO:
「金融市場インフラのためのサイバー攻撃耐性に係るガイダンス」の公表
(2016年6月)

G7:
「金融セクターのサイバーセキュリティに関するG7の基礎的要素」の公表
(2016年10月)

G7諸国の当局が連携して実施する、大規模なサイバーインシデントに対するクロスボーダーの合同演習(2019年予定)

FSB:
「サイバー用語集」の公表(本年11月)

7

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。

英国における最近の議論 (1)



サイバー攻撃そのものを完全に防ぐことは、難しい。もともと、従来のオペ・リスク管理の枠組みでは適切なサイバー耐性の確保は困難。結果として、金融安定が脅かされるリスクが小さくない？

8

英国における最近の議論 (2)

At its meeting on 19 June 2018, the Financial Policy Committee (FPC):

...

Agreed to set standards for how quickly critical financial companies must be able to restore vital services following a cyber attack. Working with others, especially the National Cyber Security Centre, the Bank would test that firms would be able to meet the FPC's standard for recovering services.

(出所) Record of the Financial Policy Committee meeting held on 19 June 2018

サイバー攻撃を受けてサービスを停止した主要行がこれを復旧するまでの所要時間に関する基準を作ることに合意。英国中銀は、National Cyber Security Centreを中心に他の当局とも連携のうえ、金融政策委員会としての基準に照らし、各行の事後復旧力をテストしていく。

9

サイバー脅威の動向

FIGURE 13—NUMBER OF SECURITY ATTACKS YEAR OVER YEAR
Is your enterprise experiencing an increase or decrease in security attacks as compared to a year ago?

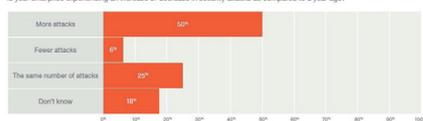
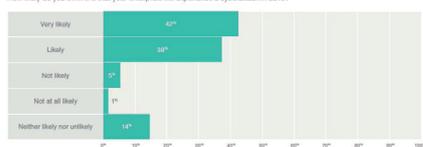


FIGURE 14—LIKELIHOOD OF CYBERATTACK
How likely do you think it is that your enterprise will experience a cyberattack in 2018?



(出所) ISACA State of Cybersecurity 2018

10

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にかえりません。

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、最近では、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。



Paramount Pictures "The Perfect Weapon" (1991)

David E. Sanger, "The Perfect Weapon: war, sabotage, and fear in the cyber age" (2018/6/21)

11

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す。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です。

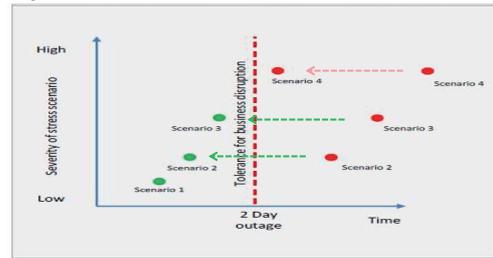
サイバー耐性を規定する5つの要因



(出所) Bank of England (M01)18 (July 2018)

12

ex postなサイバー耐性の改善に向けて



Key
● Scenario recovered within tolerance
● Scenario not recovered within tolerance

(出所) Bank of England (M01)18 (July 2018)

13

3線防衛の基本型とCISOの立ち位置

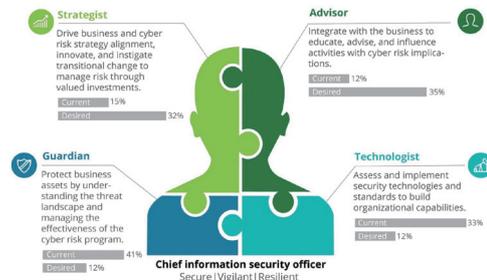


Adapted from ECIA/FERMA Guidance on the 8th EU Company Law Directive, article 41

(出所) IIA POSITION PAPER: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL (Jan. 2013)

14

CISOへの期待

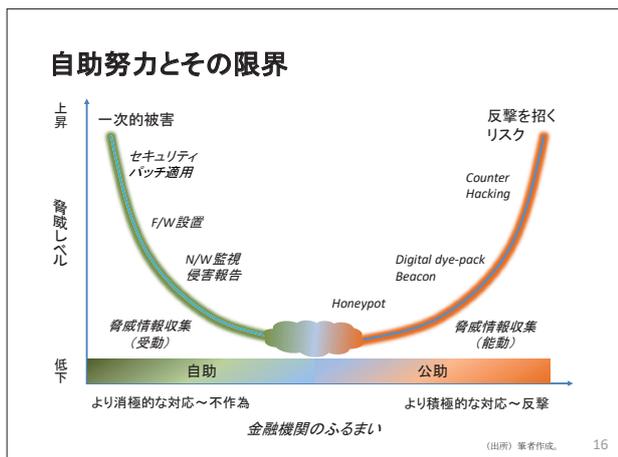


(出所) Deloitte, The state of cybersecurity at financial institutions (May 21, 2018)

15

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ニフェス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ただけとはいえないことは、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、金融危機に繋がりがねない事態が発生した際に影響を最低限に留め、ないし拡がりをも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もせているのが、我々当局に突き付けられた課題であつたりします。

民と官の連携 米国のケース

About FSARC

In 2016, the CEOs of **eight banks** – Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street and Wells Fargo – came together to proactively identify ways to **enhance the resilience of the critical infrastructure** underpinning much of the US financial system. The result is the creation of a long-term strategic initiative that performs deep analyses of systemic risk across financial products and practices, known as the **Financial Systemic Analysis and Resilience Center (FSARC)**. The FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the US financial system from current and emerging cybersecurity threats through focused operations and **enhanced collaboration between participating firms, industry partners and the US Government**.

出所：FS-ISAC

17

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

