金融分野のサイバーセキュリティ強化に向けた取組みについて

2022年5月11日　日本金融監査協会

金融庁総合政策局リスク分析総括課

サイバーセキュリティ対策企画調整室長　齊藤 剛

※本資料は、発表者個人の見解を示すものであり、金融庁の公的な見解を示すものではありません。

アジェンダ

Ⅰ　サイバー攻撃の脅威の動向

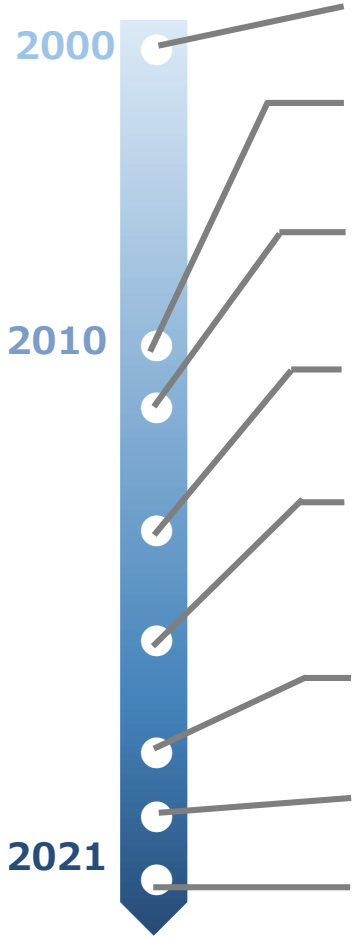
Ⅱ　国際的な議論の動向

Ⅲ　金融分野におけるサイバーセキュリティ強化に向けた取組方針

Ⅰ　サイバー攻撃の脅威の動向

近年の国内外の主要なサイバー攻撃

サイバー攻撃は巧妙化し、その被害は多岐に渡り（業務妨害、重要情報の窃取、金銭の獲得など）、その脅威は増大している。



2000.1　日本官公庁ウェブサイト改ざん事案
科学技術庁（当時）を始め、複数の中央省庁などのウェブサイトが改ざんされた。

2010.1　オーロラ作戦(Operation “Aurora”）の発覚
中国が関与していると疑われるハッキンググループによるInternet Explorerの脆弱性を突いたマルウェア攻撃。
金融、テクノロジ、メディア、化学など様々な分野の大企業から知的財産などを窃取した。

2010.11　イラン マルウェア「Stuxnet」による核関連施設攻撃の発覚
イランのウラン濃縮施設にある閉域ネットワーク内の遠心分離機が、USBストレージ経由にてマルウェア「Stuxnet」に感染。
秘密裏に誤作動し、約1,000台が物理的に破壊された。

2016.2　バングラデシュ中央銀行における不正送金事案
バングラデシュ中央銀行が不正アクセスを受け、SWIFTシステムを通じて不正送金が行われた。
被害額は約8,100万ドル。

2017.5　ランサムウェア「WannaCry」事案
感染端末がネットワークに接続された他の端末にも感染を広げる自己増殖型のマルウェア。
日本を含む約150か国の政府機関、医療機関、企業等がデータを暗号化され身代金を要求された。

2018.1　暗号資産交換業者における不正出金事案
コインチェックが不正アクセスを受け、暗号資産NEM（約580億円相当）が不正送金された。

2020.12 大規模サプライチェーン攻撃
SolarWinds社製IT管理・監視ツール「Orion」の更新プログラムを悪用した大規模な攻撃。

2021.5　コロニアルパイプラインへのランサムウェア攻撃
コロニアルパプラインの業務全体が一時停止（５日間）し、多くのガソリンスタンドでガソリン不足が発生。

※各報道情報をもとに金融庁作成

近年の国内金融分野のサイバー脅威の動向

年月	会社名	概要	
2020/7	証券会社	顧客情報の漏洩 （氏名・生年月日・住所等）	✓ 顧客情報管理システムへの不正アクセス ✓ 個人情報4千名分が漏洩 ※運転免許証、個人番号カード等の画像データも一部流出
2020/8	商品先物業者	顧客情報の漏洩 （氏名・住所・銀行口座情報、パスワード等）	✓ Webサイトへの不正アクセス ✓ オンライントレード口座開設時の入力情報約3千件が漏洩
2020/9	証券会社	不正出金	✓ 何らかの方法で取得したログイン情報を利用してアクセス ✓ 偽装本人確認書類で作成した銀行口座を出金先に変更し、不正に出金 ✓ 被害総額は約１億円
2020/9	資金移動業者	不正出金	✓ キャッシュレス決済サービスにおける本人認証設計の不備によって不正に預貯金が引き出される ✓ 被害総額は約３千万円
2020/10	保険代理店	顧客情報の漏洩 （氏名・生年月日・住所等）	✓ データ管理システムへの不正アクセス ✓ 攻撃を受けた個人データの総数は９万件
2020/11	暗号資産 交換業者	顧客情報の漏洩 （電子メールアドレス、氏名、暗号化されたパスワード等）	✓ ドメイン登録サービスに登録した情報が不正に変更されたことによる、システム・インフラへの不正アクセス ✓ 約17万件の情報が漏洩。（他に身分証明書等の本人確認書類約３万件も漏洩した可能性あり）
2020/12 ～	資金移動業者 銀行等	顧客情報の漏洩 （氏名・住所・電話番号等）	✓ クラウドサービスの設定不備による不正アクセス ✓ 地方自治体及び一般事業者でも発生
2021/4	証券会社	オンライン取引停止	✓ オンライントレードシステムへの不正アクセス ✓ データを暗号化され、現行システムの復旧を断念
2021/11	信用金庫・信用組合	HP改ざん	✓ サイバー攻撃によりHPの閲覧とHP経由のオンラインバンキングが利用不可
2021/11 ～	保険会社	個人情報の漏洩・不正出金	✓ フィッシングサイトへ誘導する不審メールが複数の保険会社で発見 ✓ 偽装口座を使用した不正出金被害も発生

※各報道情報をもとに金融庁作成

IPA「情報セキュリティ10大脅威」（2022年1月）

- **組織に対する情報セキュリティへの脅威として、昨年に引き続き「ランサムウェアによる被害」が1位**
- **サプライチェーンの弱点を悪用した攻撃も昨年4位⇒今年3位と注目度が高い**

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威」 https://www.ipa.go.jp/security/vuln/10threats2022.html

事例紹介①：ランサムウェア攻撃
～コロニアルパイプラインへのランサムウェア攻撃（2021年5月）～

【コロニアルパイプラインとは】

米国最大の石油パイプラインの運営会社。テキサス州ヒューストンからニューヨーク港まで約8,800キロのパイプラインを運営
（東海岸の対象地域で消費される45%の燃料を提供）

【主要な被害】

コロニアルパイプラインの業務全体が一時停止（５日間）し、多くのガソリンスタンドでガソリン不足が発生するなど、国民生活にも影響

【時系列】

5月7日(金)	• ランサムウェアによる影響をうけ業務全体を一時停止すると発表（予防措置としてパイプライン全停止）
5月10日(月)	• FBIがDarkSideと呼称されるランサムウェアギャングが今回の犯行に使われたと声明を発表 • 米大統領が、ロシア政府の関与はないが、ロシア拠点のグループが攻撃したと発言
5月13日(木)	• BloombergがColonial Pipeline社が身代金（500万ドル相当の暗号資産）を支払ったと報道 • セキュリティ研究者らが、DarkSideは米国からの圧力を理由にRaaSプログラムの活動を停止したと報告

【ランサムウェアの脅迫方法の高度化】

第1段階（従来の攻撃）：**データを暗号化**したうえ、（ビットコインなどでの）**身代金支払いを要求**
（支払わないと復号鍵を渡さない）
第2段階（二重脅迫）：窃取した**機密情報を暴露すると脅す**
第3段階（三重脅迫）：**DDoS攻撃を行うと脅迫する**
第4段階（四重脅迫）：攻撃対象の企業の**顧客に連絡し、（漏洩データを公開するなどと）更に脅す**

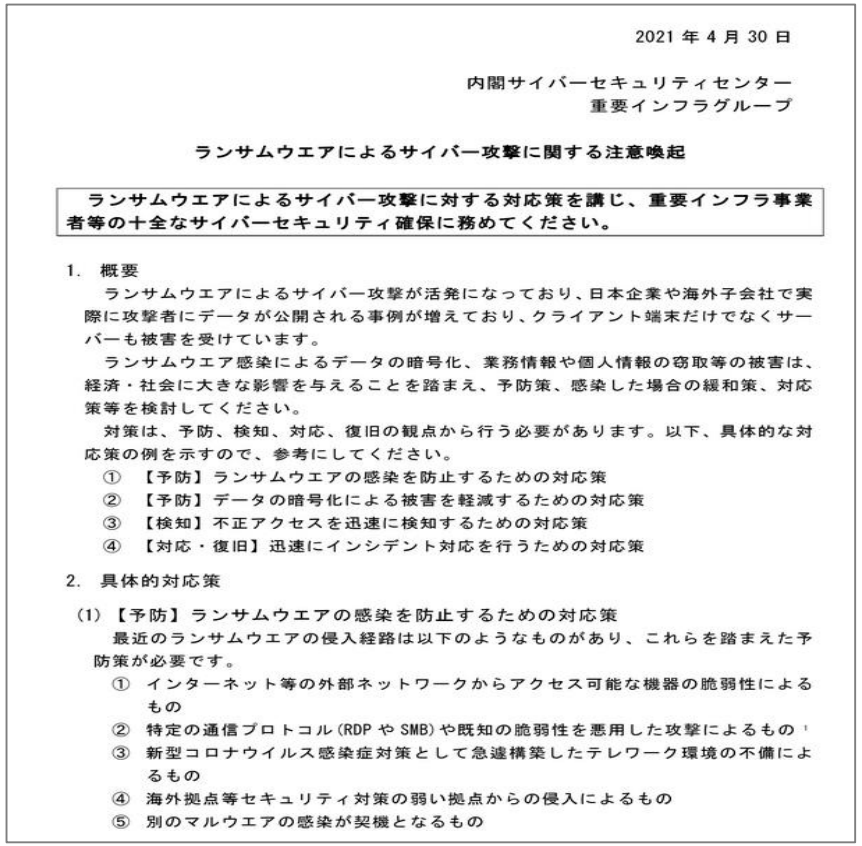
※各報道情報をもとに金融庁作成

NISCによる注意喚起（2021年４月30日）

予　　防：セキュリティパッチのより迅速な適用、バックアップ、機微データの厳格管理（アクセス制御や暗号化）、復旧計画の確認

検　　知：各機器のログ監視の強化、ふるまい検知、EDR（Endpoint Detection and Response）により、PCやサーバ内で不審な挙動や痕跡がないかの常時監視

対応・復旧：データの暗号化、公開、DoS攻撃等を想定した対処態勢、BCPの策定、組織内外（業務委託先、関係省庁を含む）との連絡体制の確認



2021 年 4 月 30 日

内閣サイバーセキュリティセンター
重要インフラグループ

ランサムウエアによるサイバー攻撃に関する注意喚起

ランサムウエアによるサイバー攻撃に対する対応策を講じ、重要インフラ事業者等の十全なサイバーセキュリティ確保に務めてください。

1. 概要

ランサムウエアによるサイバー攻撃が活発になっており、日本企業や海外子会社で実際に攻撃者にデータが公開される事例が増えており、クライアント端末だけでなくサーバーも被害を受けています。

ランサムウエア感染によるデータの暗号化、業務情報や個人情報の窃取等の被害は、経済・社会に大きな影響を与えることを踏まえ、予防策、感染した場合の緩和策、対応策等を検討してください。

対策は、予防、検知、対応、復旧の観点から行う必要があります。以下、具体的な対応策の例を示すので、参考にしてください。

① 【予防】ランサムウエアの感染を防止するための対応策
② 【予防】データの暗号化による被害を軽減するための対応策
③ 【検知】不正アクセスを迅速に検知するための対応策
④ 【対応・復旧】迅速にインシデント対応を行うための対応策

2. 具体的対応策

(1) 【予防】ランサムウエアの感染を防止するための対応策

最近のランサムウエアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル（RDP や SMB）や既知の脆弱性を悪用した攻撃によるもの
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウエアの感染が契機となるもの

（記載例）

【予防】ランサムウェアの感染を防止するための対応策

最近のランサムウェアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル(RDPやSMB)や既知の脆弱性を悪用した攻撃によるもの
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウェアの感染が契機となるもの

【予防】データの暗号化による被害を軽減するための対応策

・・・（略）・・・

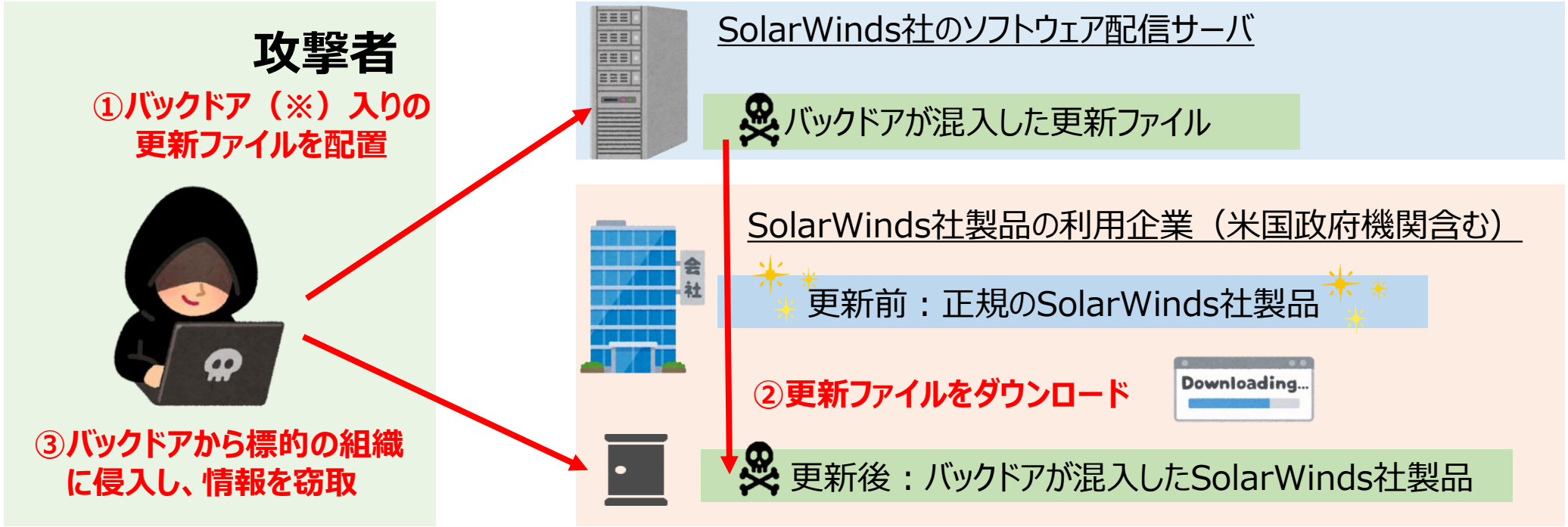
チェックポイント（抜粋）

- 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウェア感染時でもバックアップが保護されるように留意する。例えば、ファイルのコピーを3個取得したうえで、ファイルは異なる2種類の媒体に保存、コピーのうち、1個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管するといった対策等を検討する。
- バックアップデータから実際に復旧できることを確認する

事例紹介②：サプライチェーン攻撃
～SolarWinds社へのサプライチェーン攻撃（2020年12月）～

米国のサイバーセキュリティ企業SolarWindsは、自社製品に、バックドアが仕込まれていたと公表（2020年12月13日）

- 大手企業（米Intel等）や政府機関（米財務省等）を含め、米国を中心に世界中の組織（最大18,000組織）が情報窃取された可能性がある。
- FBI、NSA（米国家安全保障局）等が、ロシアが関与した可能性が高いと表明。



（※）バックドア：サービス利用者等に知られることなく、秘密裏に設置されたハッキング等のための侵入口のこと

Ⅱ　サイバーセキュリティを巡る国際分野における動向

最近の国際機関での議論の動向

✓金融機関等に対するサイバー攻撃の脅威が増し金融システムの安定等にも影響を与えかねないことを踏まえ、G7、G20・金融安定理事会等でサイバーセキュリティに関する議論が積極的に行われている。

✓近年、IT を活用して新たな金融サービスを提供するフィンテックの台頭や、金融機関と外部の接続の拡大、国際的に活動する大手クラウド事業者への集中リスクの高まりなどを背景に、金融機関における業務継続性の確保について国際的に関心が高まっている。

（参考）G7･G20における関連する文書･活動

G7 - Cyber Expert Group

2016	サイバーセキュリティに関するG7の基礎的要素
2017	サイバーセキュリティの効果的な評価に関するG7の基礎的要素
2018	脅威ベースのペネトレーションテストに関するG7の基礎的要素
2018	サードパーティのサイバーリスクマネジメントに関するG7の基礎的要素
2019	クロスボーダー合同演習
2020	サイバー演習計画に関するG７の基礎的要素
2020	コミュニケーション演習
2021	大臣総裁によるサイバーインシデント討議

G20 – FSB

2017	金融セクターのサイバーセキュリティにおける規制･ガイダンス･監督上の慣行に関する報告書
2018	サイバーセキュリティ用語集（Cyber Lexicon）
2019	クラウドサービス利用における第三者サービスへの依存：金融安定への影響に関する考察
2020	サイバー事象の初動･回復対応の効果的な実務
2020	アウトソーシング･サードパーティに関する規制･監督上の論点（ディスカッション･ペーパー）
2021	アウトソーシング･サードパーティに関する規制･監督上の論点（市中協議に寄せられた意見の概要）
2021	サイバー事象報告－既存のアプローチとより広い範囲での収斂に向けた今後のステップ

Ｇ７の国際的な協調（１）

- 2015年、G7各国の金融当局間で、「G7サイバーエキスパートグループ」が設置。
- 金融分野におけるサイバーセキュリティの促進やＧ７諸国間での協力強化を進めていくことで合意。

（参考１）G7伊勢志摩首脳宣言（抄、平成28年5月27日）

◆ We welcome the work of the G7 Cyber Experts Group in the financial area to foster cyber security and enhance cooperation among G7 countries in this area.

我々は、金融分野におけるサイバーセキュリティを促進し、G7 各国間での協力を強化するための、この分野のG7 サイバーエキスパートグループの作業を歓迎する。

（参考２）サイバーに関するG7の原則と行動（抄、平成28年5月27日）

◆ We commit to enhance cybersecurity threat information sharing and to cooperate for improvement of cybersecurity of critical infrastructure such as finance, energy, transportation, and telecommunication.

我々は、サイバーセキュリティに関する脅威情報の共有を強化すること及び金融、エネルギー、運輸、通信といった重要インフラのサイバーセキュリティ向上のために協力することについてコミットする。

（2016年5月27日外務省HP<http://www.mofa.go.jp/mofaj/ecm/ec/page4_001562.html>より抜粋）

Ｇ７の国際的な協調（２）

（参考３）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（2016年10月11日）

◆ **The G7 Finance Ministers and Central Bank Governors have endorsed the G7 Fundamental Elements of Cybersecurity for the Financial Sector.**

G7財務大臣・中央銀行総裁は、「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」を支持。

◆ **The non-binding elements encapsulate best practices in cybersecurity for public and private financial sector entities of all sizes and are designed to be tailored and proportionate to the particular characteristics of each entity and the cyber risks it faces.**

この要素は拘束力はないが、全ての規模の公的・民間金融セクターの主体にとってのサイバーセキュリティにおけるベスト・プラクティスを包含しており、各主体固有の特質や、直面するサイバーリスクに対応して設計されている。

◆ **The elements serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture.**

本「基礎的要素」は、個々の金融機関が、自らのリスク管理や企業文化に関する認識を踏まえた上で、サイバーセキュリティ・ストラテジーやその運用のためのフレームワークを策定・実施するにあたり、その土台としての役割を果たす。

（2016年10月11日財務省HP<http://www.mof.go.jp/international_policy/convention/g7/g7_161011.htm>より抜粋）

（日本銀行HP <http://www.boj.or.jp/announcements/release_2016/rel161011a.htm/>においても併載）

※「G7サイバーエキスパートグループ」には我が国から金融庁、財務省、日本銀行等が参加

G7の国際的な協調（３）

✓G7財務大臣・中央銀行総裁会議では、2015年に「G7サイバーエキスパートグループ」を設置し、2016年より、順次、サイバーセキュリティに係る国際的な基本原則を示した「基礎的要素」を策定・公表（計5本公表、次頁参照）

✓2019年6月には、G7の関係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を実施

✓2021年11月には、G7財務大臣・中央銀行総裁会議において、サイバーセキュリティに関する討議を実施

（参考）G7財務大臣・中央銀行総裁会議において策定・公表された サイバーセキュリティの「基礎的要素」

	金融セクターのサイバーセキュリティに関する基礎的要素	金融セクターのサイバーセキュリティの効果的な評価に関する基礎的要素	脅威ベースのペネトレーションテスト（TLPT）に関する基礎的要素	金融セクターにおけるサードパーティのサイバーセキュリティリスクマネジメントに関する基礎的要素	サイバー演習計画に関する基礎的要素
公表年月	2016年10月	2017年10月	2018年10月	2018年10月	2020年11月
概要	金融機関がサイバーセキュリティ対策を講ずる上で重要と考えられる基礎的要素	金融機関のサイバーセキュリティに関するプラクティスの適切な実施・評価を行うことに焦点を当てた基礎的要素	脅威動向の分析を踏まえた攻撃シナリオに基づく実践的な侵入テスト（TLPT）を実施する上で重要な基礎的要素	金融機関の外部委託先等、サードパーティとの関係で生じるサイバーリスクに関する基礎的要素	官民金融セクターにおいてサイバー演習計画を立案するための効果的プラクティスの基礎的要素

サイバー事象への初動・回復対応に関する金融安定理事会報告書※（2020年10月19日）

- **主に民間金融機関向けのベストプラクティス集。民間金融機関が自らの組織の規模や複雑性、リスクに基づいて適切なものを選択できるように、広範なプラクティスを7領域計49項目にわたり取り纏めたもの。**

カテゴリ	ベストプラクティス（例）
ガバナンス	✓ CIRR活動における取締役会と経営陣の役割と責任を明確化する。 ✓ 取締役会と経営陣がCIRR活動に十分な予算を配分する。 ✓ インシデントの影響度とCIRR活動の有効性を測る数値指標を定める。
計画と準備	✓ CIRR活動に関する計画や対応手順を定めて更新する。 ✓ 脅威分析を踏まえたストレステストシナリオを定め定期的に評価する。 ✓ サードパーティとの契約情報を管理し、N次受けも含めて合意要項が確保されていることを確認し、そのサービス提供能力を常時評価する。
分析	✓ 関係者間の認識共有等のため、サイバーインシデントを分類するタクソノミや深刻度を評価する枠組みは事前に定めたものを用いる。 ✓ インシデント分析やフォレンジック解析に必要なログを回収する。
被害軽減	✓ サイバーインシデントの種類に応じた封じ込め策を実施する。 ✓ 停止・隔離の判断にあたりコストやビジネスインパクト等を検討する。 ✓ 証跡の回収・保存後に、攻撃に用いられた不正コード等を全て除去する。
復元と回復	✓ オペレーションやシステム、サービスの重要性に基づいて、回復活動に優先順位をつける。 ✓ ドキュメント化されテストされた手順に従ってデータ復元を行う。 ✓ 復元プロセスの間は、異常活動がないか、サードパーティやネットワーク、システムをモニタリングする。
調整とコミュニケーション	✓ 組織内のステークホルダーに対して、事前に合意した深刻度評価枠組みに基づいて、タイムリーにエスカレーションする。 ✓ 予め定めたコミュニケーション戦略に則り、関連部署からなる組織横断的なコミュニケーションチームでメディア対応を行う。
改善	✓ 業界全体の知見やスキルセットの共有を図り、未知の脆弱性等を議論するために、フォーラムなどを通して業界で協力する。 ✓ インシデント対応の完了後、講じた措置の有効性などを検証する。

※「サイバー事象の初動・回復対応の効果的な実務」（原題：”Effective Practices for Cyber Incident Response and Recovery“）

サードパーティ依存の増大

アウトソーシング・サードパーティに関する金融安定理事会報告書(2020年11月9日公表)

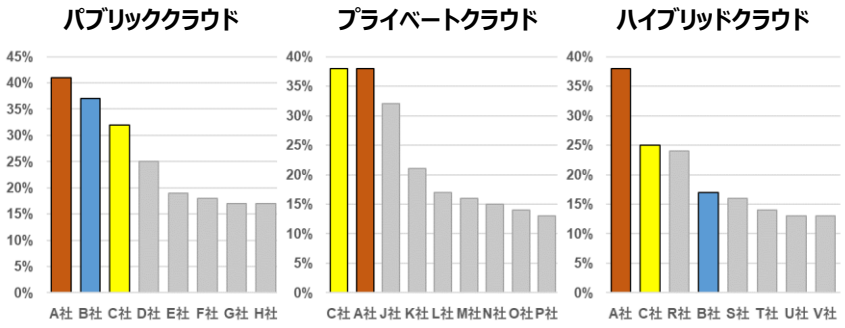
- **金融機関のクラウド利用に関する報告書（クラウドサービス利用における第三者サービスへの依存に関する金融安定理事会報告書：2019年12月公表）に続き、金融機関と外部委託（アウトソーシング）・第三者（サードパーティ）との関係全般における課題を取り纏めた報告書。**
- **規制監督上の課題解決にあたって金融当局、金融機関、サードパーティの間でのグローバルな対話の必要性を指摘。**

✓ 「アウトソーシング」とは金融機関が自社業務を第三者に委託することを指す（BIS 2005年）が、「サードパーティ」とは金融機関と何らかのビジネス関係を持つ先全てを指す。

金融機関にとっての便益

- **スケーラビリティ・迅速性の強化、オペレーショナル・レジリエンスの強化、コスト削減、イノベーション拡大、内部プロセス改善等**

各種クラウド類型における企業シェア（2017年）



FSB, “BigTech in finance: Market developments and potential financial stability implications”, https://www.fsb.org/2019/12/bigtech-in-finance-market-developments-and-potential-financial-stability-implications/, 2021/3/1 より作成

金融機関・当局にとっての課題

- **監査権・アクセス権・情報取得権の不足**
  （例）サードパーティとの力関係で契約文言へ規制監督上の要件を盛り込むことが難しい、各金融機関が個別に同じサードパーティをオンサイト検査するのはサードパーティ側にも多大な負担、問題点を見つけても修正を行わせることが難しい等
- **サプライチェーン管理**
  （例）サプライチェーンにおけるN次受けのリスクを特定し対処するのが難しい（COVID-19の下、グローバルなサプライチェーンの混乱により、リモート作業機器の入手に遅延や物流上の問題が発生）等
- **クロスボーダーに起因する課題**
  （例）監督管轄権が及ばない場合がある、データ守秘義務が異なるため統一的なデータ管理が困難、破綻した際に第三国にある重要なデータやシステムの回収が難しい等
- **システミックリスクの懸念**
  （例）左記の通り、少数のサードパーティの寡占市場となることで単一障害点が生じる等

●左記報告書で指摘された課題は、市中協議でおおむね支持されたことが報告されている
（2021 年 6 月に「アウトソーシング・サードパーティに関する規制・監督上の論点（市中協議に寄せられた意見の概要）」として公表）。

オペレーショナルレジリエンス

✓バーゼル銀行監督委員会（バーゼル委）は、2020年８月６日、オペ・レジリエンス諸原則に係る市中協議文書を公表。

✓オペ・レジリエンスとは、**テロやサイバー攻撃、パンデミック、自然災害等の事象が発生しても、銀行が「重要な業務（critical operations）」を継続できる能力**をいう。

✓「重要な業務」は、途絶すると当該銀行の業務継続、金融システムの中での役割に深刻な影響を及ぼし得る活動やプロセス、サービス、それらを支える資産。各銀行の性質や金融市場における役割によって異なる。

✓重要な業務に対して、各銀行のリスクアペタイト、リスク能力、リスクプロファイルを考慮しつつ、経営陣が「オペ・レジリエンスの期待水準（operational resilience expectations）」を設定するよう求めている。

✓バーゼル委は、オペ・レジリエンスを評価する枠組み（metrics）の開発が今後の課題であるとし、市中協議（2020年11月６日まで）において情報提供を呼びかけた。

（参考）バーゼル委のオペレーショナルレジリエンス諸原則・抄訳

① ガバナンス	銀行は、インシデントが発生した際にも重要な業務の提供に及ぼす影響を最小限に抑えられるよう、既存の体制を活用しつつ、オペ・レジリエンスの確保に向けた有効なガバナンス体制を確立し、監督すること。
② オペリスク管理	銀行は、オペリスク管理における3線防衛態勢を応用することにより、業務プロセス、人的資源、システムに対する組織内外の脅威や潜在的なリスクを常に把握すること。また、自行のオペ・レジリエンスの期待値に沿って、重要な業務の脆弱性を速やかに評価し、リスクを管理すること。
③ BCPとテスト	銀行は、BCPを整備すること。また、深刻であるが起こり得るシナリオを想定した訓練を実施し、インシデント発生時でも重要な業務を継続できるか確認すること。
④ 相互連関性の特定	銀行は、重要な業務の提供に関わる組織内外の相互連関性や相互依存関係を特定および記録し、重要な業務の提供に必要なオペ・レジリエンスの期待値を設定すること。
⑤ サードパーティ依存度の管理	銀行は、重要な業務の提供に関わるサードパーティやグループ内組織への依存を管理すること。
⑥ インシデント管理	銀行は、インシデントが発生した際の初動・回復計画を、自行のリスク許容度（リスクアペタイトやリスク受容力、リスク特性を踏まえて設定）と整合的な形で整備すること。また、実際に発生したインシデントからの教訓を踏まえて、同計画を継続的に更新していくこと。
⑦ サイバーを含むICTセキュリティ対応	銀行は、サイバー関連を含む頑健なICTセキュリティを確保すること。ICT資産について、脅威からの保護を講じるとともに、侵害の検知や初動・回復の訓練を定期的に実施すること。

EUの規制動向

Digital Operational Resilience Act（1）

✓欧州委員会は、2020年9月、DORA（Digital Operational Resilience Act）を提案

✓DORAはEUの幅広い金融機関を対象として、ICTガバナンス、ICTリスクマネジメント、インシデント報告、オペレジに関するテスト、サードパーティリスクマネジメント、重要なサードパーティの監督、情報共有等について規定

✓DORAは、国際的な関心が高いサードパーティの直接監督が規定されているほか、サイバーセキュリティに関する重要な規定が含まれており、今後の国際的な議論に影響を与える可能性

Digital Operational Resilience Act（2）

条項		主な規定
第4条	ICTガバナンス	• リスクマネジメントのフレームワークの策定・承認
第5～14条	ICTリスクマネジメント	• 特定、防御、検知、対応・復旧等に関する要求
第15～20条	インシデント報告	• インシデント管理プロセスの策定、インシデントの分類、共通様式による報告
第21～24条	オペレジに関するテスト	• すべての金融機関は、内部もしくは外部の独立した主体によるテスト（脆弱性評価・診断、ネットワークセキュリティ評価、ソースコードの確認、ペネトレーションテスト等）を実施 • 金融機関はテストで認識された問題を優先順位づけし改善する方針・手続きを確立 • 重要な金融機関についてはTLPTによる高度なテストを実施
第25～39条	ICTサードパーティリスク	• サードパティリスク管理の原則と、重要サードパーティの監視枠組み • サードパーティとの契約に関する情報の目録の作成 • サードパーティとの契約の終了ができることを契約上明示 • 第三国で設立された重要サードパーティの利用禁止 • 重要サードパーティに対する直接監督（資料・報告徴求、調査・検査、勧告）
第40条	情報共有	• 信頼できるコミュニティにおける金融機関同士のサイバー脅威情報の任意の共有（セキュリティ侵害の痕跡、戦術、テクニック及び手順等）

Ⅲ　金融分野における
サイバーセキュリティ強化に向けた取組方針

金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）

～サイバーセキュリティを確保し、安心・安全かつ利便性の高い金融サービスの実現へ～

サイバー空間の変化

- 国家の関与が疑われる**組織化・洗練化されたサイバー攻撃**や、国際的なハッカー集団等による**ランサムウェア攻撃の多発**
- デジタライゼーションの進展による**金融サービスの担い手の多様化**と、キャッシュレス決済などの**連携サービスの進展**
- クラウドサービスをはじめとした**外部委託の拡大、サプライチェーンの複雑化・グローバル化**等による**リスク管理の難度の高まり**

新たな取組方針（以下、５項目）

１．モニタリング・演習の高度化

金融機関の規模・特性やサイバーセキュリティリスクに応じて、検査・モニタリングを実施し、サイバーセキュリティ管理態勢を検証する。
共通の課題や好事例については業界団体を通じて傘下金融機関に還元し、金融業界全体のサイバーセキュリティの高度化を促す。特に

- ✓ 3メガバンクについては、**サイバー攻撃の脅威動向の変化への対応**や**海外大手金融機関における先進事例**を参考にしたサイバーセキュリティの高度化に着目しつつ、モニタリングを実施する
- ✓ 地域金融機関については、**サイバーセキュリティに関する自己評価ツールを整備**し、各金融機関の自己評価結果を収集、分析、還元し、**自律的なサイバーセキュリティの高度化を促す**
- ✓ サイバー演習については、引き続き、**サイバー攻撃の脅威動向**や**他国の演習**等を踏まえて高度化を図る

２．新たなリスクへの備え

- ✓ **キャッシュレス決済サービス**の安全性を確保するため、リスクに見合った**堅牢な認証方式の導入等**を促す**（セキュリティバイデザインの実践）**
- ✓ クラウドサービスの安全な利用に向けて、**利用実態**や**安全対策**の把握を進めるとともに、**クラウドサービス事業者との対話**も実施

３．サイバーセキュリティ確保に向けた組織全体での取組み

- ✓ 経営層の積極的な関与の下、**組織全体でサイバーセキュリティの実効性**の向上を促す（セキュリティ人材の育成も含む）

４．関係機関との連携強化

- ✓ サイバー攻撃等の情報収集・分析、金融犯罪の未然防止と被害拡大防止への対応を強化するため**関係機関（NISC、警察庁、公安調査庁、金融ISAC、海外当局等）との連携を強化**

５．経済安全保障上の対応

- ✓ 政府全体の取組みの中で、機器・システムの利用や業務委託等を通じたリスクについて適切に対応を行う

これまでの経緯

- 金融分野におけるサイバーセキュリティ取組方針（Ver. 1.0）は、サイバーセキュリティ基本法の制定（2014年11月）を踏まえ、2015年7月にサイバーセキュリティ強化に向けた方針を金融機関等と共有するため策定（注1・2）。

  （注1）サイバーセキュリティ基本法では、政府は、金融分野も含めた重要インフラ事業者のサイバーセキュリティ確保のため、政府一丸となって施策を講じることとされている。

  （注2） 取組方針(Ver. 1.0)では、①サイバーセキュリティに係る建設的な対話と一斉把握、②情報共有の実効性向上、③演習の継続的な実施、④サイバーセキュリティ人材の育成、⑤金融庁としての態勢構築を掲げた。

- その後、東京大会に向けたサイバーセキュリティの強化等に対応するため、2018年10月に取組方針をVer. 2.0にアップデート（注3） 。

  （注3） 取組方針(Ver. 2.0)では、①デジタライゼーションの進展を踏まえた対応、②国際的な議論への貢献・対応、③東京大会への対応、④金融機関のサイバーセキュリティ管理態勢の強化、④情報共有の実効性向上、⑤サイバーセキュリティ人材の育成を掲げた。特に、東京大会に向けて中小金融機関のサイバーセキュリティの強化を重要課題として取り組んだ。

- 昨年、取組方針（Ver. 2.0)の重要課題である東京大会が無事終了した一方、国家の関与が疑われる高度なサイバー攻撃や国際的なハッカー集団によるランサムウェア攻撃が多発しているほか、キャッシュレス決済サービスにおける不正出金など新たな金融犯罪も発生するなど、サイバー空間におけるリスクも変化していることを踏まえ、今般、取組方針をVer. 3.0にアップデート。

（１）モニタリング・演習の高度化

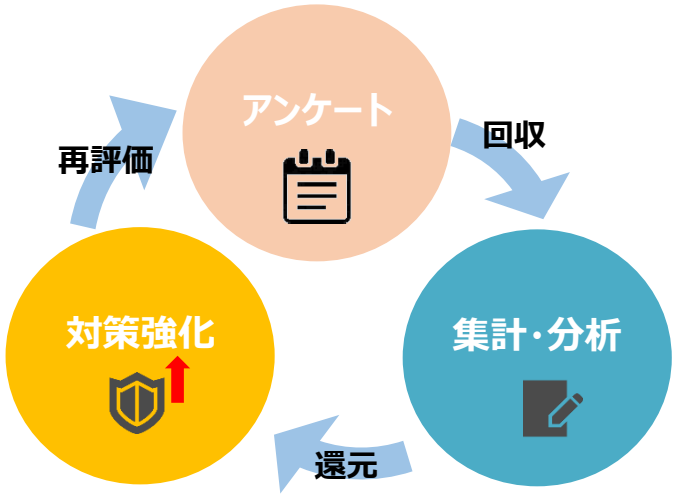
金融機関の規模・特性やサイバーセキュリティリスクに応じたモニタリングを実施

- 大手金融機関
  - ✓ 海外大手金融機関における先進的な取組事例
  - ✓ 国際的な議論の動向

- 地域金融機関
  - ✓ サイバーセキュリティ態勢の実効性の検証
  - ✓ 自己評価ツールの作成

サイバーセキュリティに関する自己評価の促進

課題	地域金融機関（ ①地域銀行、②信用金庫、③信用組合）は、他の金融機関対比での自組織の位置付けや改善すべき領域を特定するツールが必ずしも広く用いられてこなかった
対応策	金融庁、日本銀行、FISCの3者共同で地域金融機関向けのサイバーセキュリティに関する自己評価ツールを整備
目標	地域金融機関の自己評価結果を収集・分析し、その結果を還元することで、地域金融機関のサイバーセキュリティ管理の自律的な高度化を促す



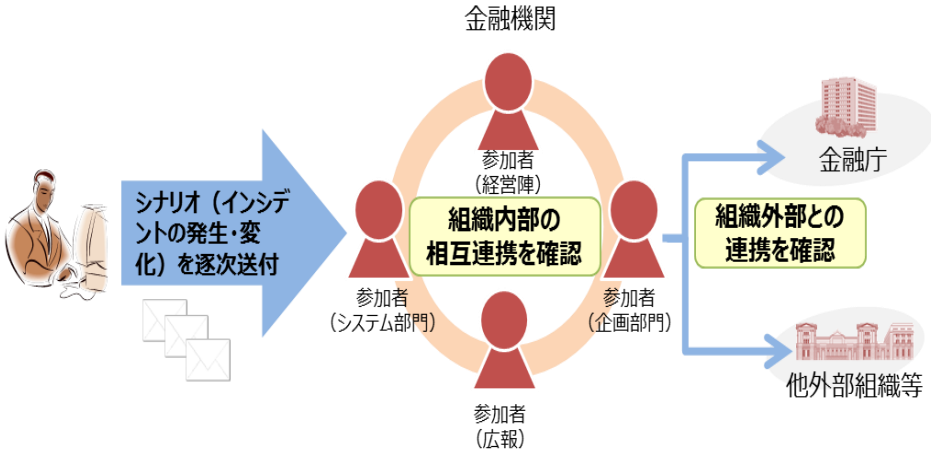
金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅵ）

- 金融庁主催による６回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅵ）を実施し、150先が参加。
- インシデント発生時の顧客対応や部門間及び組織外部との連携の実効性を確認し、業界全体のインシデント対応能力の底上げを図る。

演習の特徴

- ✓ インシデント発生時における**初動対応、攻撃内容の調査等の技術的対応、情報連携、業務継続**等を確認
- ✓ 銀行では、インシデント対応時における**議論の内容や意思決定過程**を検証
- ✓ 経営層や多くの関係部署（システム部門、広報、企画部門等）が参加できるよう、**自職場参加方式**で実施
- ✓ 参加金融機関がPDCAサイクルを回しつつ、対応能力の向上を図れるよう、具体的な改善策や優良事例を示すなど、**事後評価に力点**
- ✓ 本演習の結果は、参加金融機関以外にも**業界全体にフィードバック**

演習スキーム

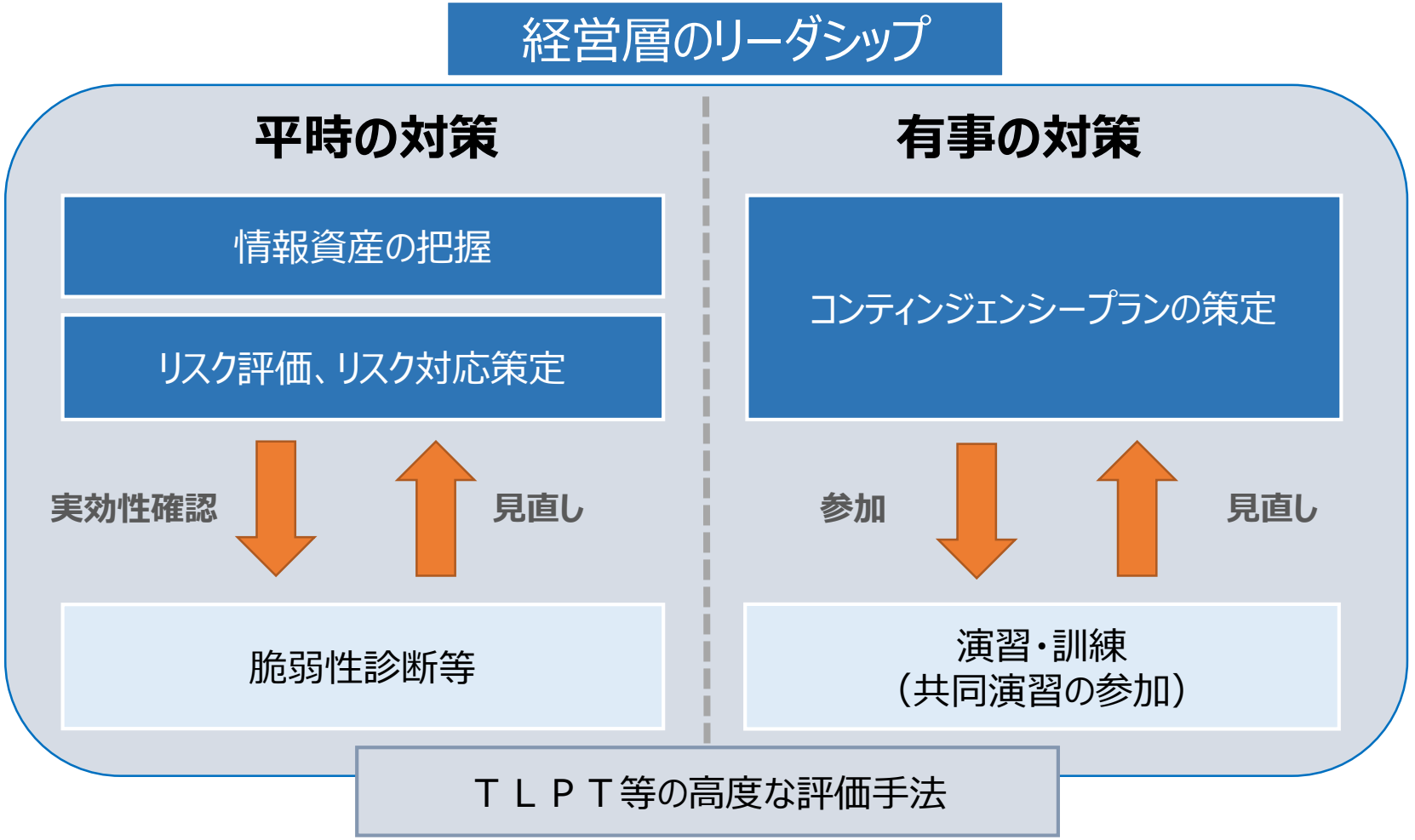


【演習シナリオの概要】

- ●**銀行等**
  - ✓（ブラインド方式のため非開示）
- ●**信金・信組**
  - ✓重要システムの異常による顧客影響が発生
- ●**証券・FX・資金移動業者・暗号資産交換業者等**
  - ✓取引システムへの不正アクセスにより、顧客資産の流出が発生
- ●**生命保険・損害保険・保険代理店・監査法人**
  - ✓顧客情報の漏えいが発生

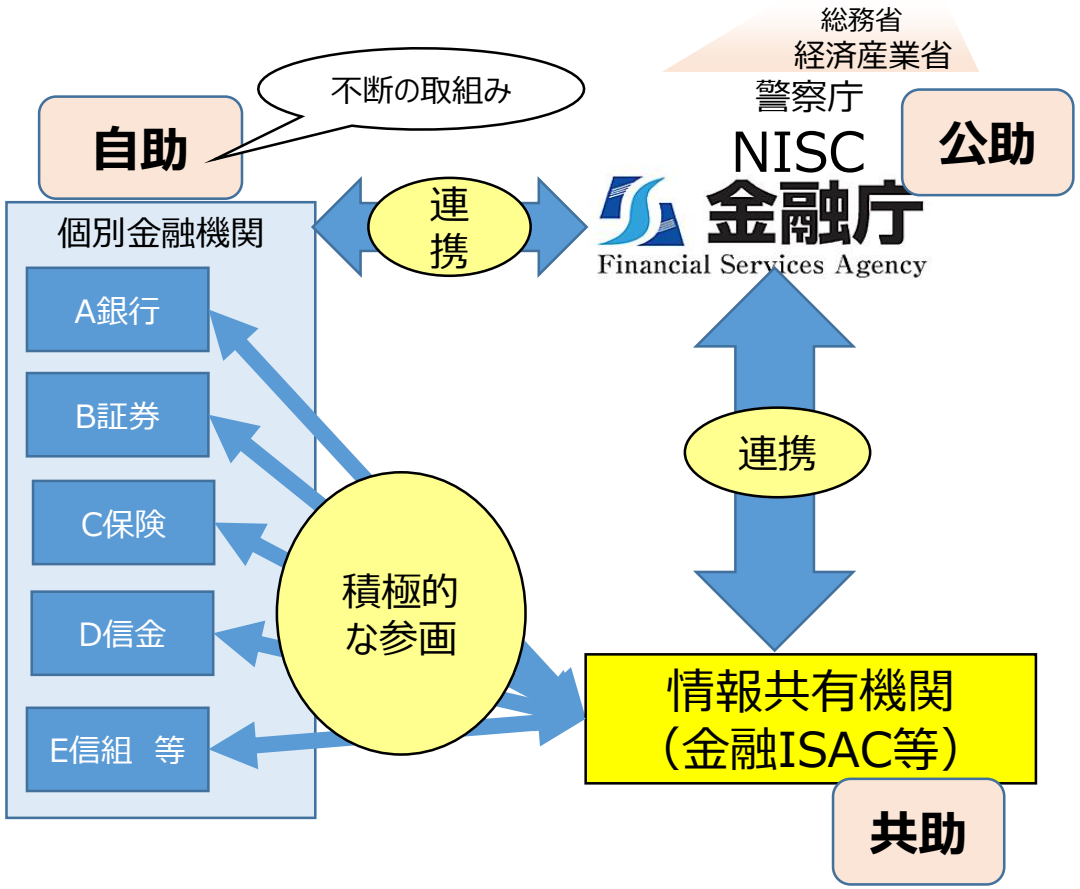
サイバーセキュリティの確保に向けて

サイバーセキュリティ攻撃は経営層の積極的なリーダーシップの下、①平時の対策と②有事の対策を両輪として進めていくことが重要



COLUMN:
サイバーセキュリティに関する「自助」、「共助」、「公助」について

日々巧妙化するサイバー攻撃に対し、個別金融機関のみでの対応には限界。 金融機関自身による「自助」、情報共有機関等を活用した「共助」、そして金融庁等の当局の支援による「公助」の考え方のもと、官民一体となってサイバーセキュリティ対策を向上させていく必要



（２）新たなリスクへの備え①

金融ビジネスを取り巻くIT環境が変容。新たなリスクに対してセキュリティを確保する。

- **金融ビジネスの担い手の多様化（フィンテック企業等の参入）と、それぞれの強みを連携したサービスの展開（キャッシュレス決済等の普及）**
- **クラウドサービスの利用浸透のほか、外部委託の拡大、サプライチェーンのグローバル化・複雑化**

①　キャッシュレス決済サービスにおける安全性の確保

金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティバイデザイン」を実践し、サービス全体の流れの中で、連携先も含めて脆弱性を洗い出し 、リスクに見合った堅牢な認証方式を導入することが重要。

②　クラウドサービスの普及等への対応

✓ クラウドの利点を活用しつつ、仕様・特性に伴うリスクも適切に評価し、システム稼働の安定性と顧客情報の適切な管理を確保することが重要（コンティンジェンシープランの整備や演習の実施）。

✓ インシデント発生時における金融機関や金融機関の顧客に対する情報発信の強化等についてクラウド事業者との対話を行う。

（２）新たなリスクへの備え②

③　サイバーハイジーンの徹底（サイバー公衆衛生）

✓ 外部委託の拡大などにより、IT資産管理の範囲が拡大・複雑化する中、安全性の高いIT環境を維持するには、境界型セキュリティ等や特定のセキュリティ製品だけに依存することなく、サイバーハイジーンの推進が重要。

④　サイバーレジリエンスの強化

✓ サイバーセキュリティ管理の範囲は、インシデントの未然防止から、インシデント発生時の検知、特定、対応、業務の早期復旧や顧客影響の軽減といったレジリエンス（いわゆる復元力）の強化へと拡大。

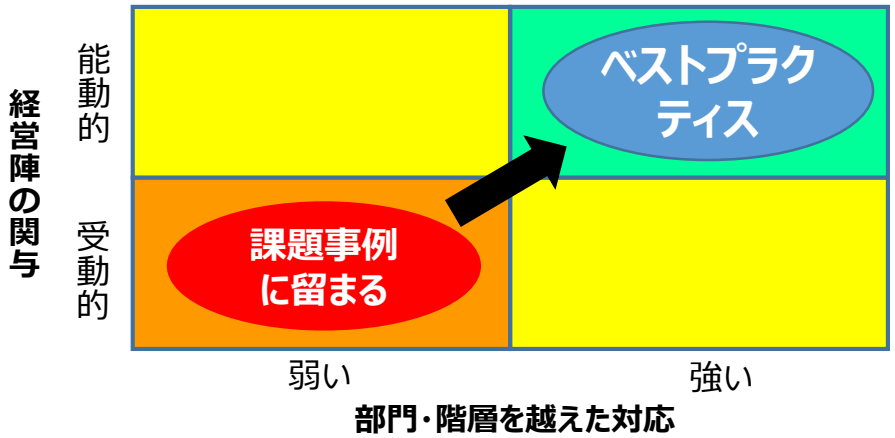
✓ インシデントによって業務が中断した場合も、業務や顧客への影響を許容水準内に収めるよう、訓練・テスト等を通じて、業務やサービスの強靭性・頑健性・冗長性を高めることを促す。

（３）サイバーセキュリティ確保に向けた組織全体での取組み

セキュリティ確保のため、引き続き、経営層の積極的な関与とセキュリティ人材の育成を促す

①　経営層の関与

- ✓ サイバーセキュリティはIT・システム部門のみの問題ではなく、あらゆる部門、階層での対応が求められる。
- ✓ 組織全体でのサイバーセキュリティ管理の実効性を高めるため、経営層の積極的な関与、リーダーシップの発揮を促す。



②　セキュリティ人材の育成

- ✓ 人事ローテーションを前提としたうえで、各部署に必要なセキュリティ人材を育成、配置することが必要。
- ✓ 例えば、自組織で知見が不足しているセキュリティ分野を洗い出し、人材育成計画を作成、実行するほか、内部の研修だけではなく、金融ISAC等の外部の活動にも参加しやすい職場環境を整備するなど、計画的に組織全体でのセキュリティ人材の育成を図る。
- ✓ 特に、経営層の方針を踏まえ、具体的なサイバーセキュリティの立案と指揮を担う戦略マネジメント層や、研修や人材育成を担うセキュリティトレーナー、システムの開発・運用担当者については、育成に時間を要するため、計画的に取り組むことが重要である。

取締役会の役割

経済産業省：グループ・ガバナンス・システムに関する実務指針（19年6月）

- サイバーセキュリティについては、内部統制システム上の重要なリスク項目として認識し、サイバー攻撃を受けた場合のダメージの甚大さに鑑み、親会社の取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れたセキュリティ対策の在り方について検討されるべきである。

経団連：サイバーリスクハンドブック　取締役向けハンドブック　日本版（19年10月）

【５原則】

1. 取締役会は、サイバーセキュリティを、単なるITの問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要がある。
   - （米国の事例）取締役会全体が、サイバーセキュリティに関する事項の概要について、少なくとも半年ごとに、また具体的なインシデントや状況によって必要となった場合はその都度、報告を受けるべきである。リスク監督（とくにサイバー関連リスクの監督）の責任を負う委員会は、少なくとも四半期ごとに報告を受けるべきである。
2. 取締役は、自社固有の状況と関連付けて、サイバーリスクの法的意味を理解すべきである。
3. 取締役会は、サイバーセキュリティに関する十分な専門知識を利用できるようにしておくとともに、取締役会の議題としてサイバーリスク管理を定期的に取り挙げ、十分な時間をかけて議論を行うべきである。
   - 取締役はサイバーセキュリティ担当取締役または担当部門の説明に疑問を投げかけ、建設的に異議を唱えるなど、積極的な役割を果たす必要がある。
4. 取締役は、十分な人員と予算を投じて、全社的なサイバーリスク管理の枠組みを確立すべきである。
5. サイバーリスクに関する取締役会における議論の内容として、回避すべきリスク、許容すべきリスク、保険等によって軽減・移転すべきリスクの特定や、それぞれのリスクへの対処方法に関する具体的な計画等を含めるべきである。

実務者層と経営層の相互理解が鍵

サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集　悩みの分類　セキュリティ意識の向上

悩み (10)　IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている

O社は役員も対象に全従業員向けのセキュリティ教育を実施している。しかしながら、年1回の標的型メール訓練では経営層のメール開封率が他の従業員と比較して高い傾向にあった。

基本情報

O社の状況

- ✓ 役員を含めて、全社員向けのセキュリティ教育を設計、運営している。
- ✓ セキュリティ教育や訓練の結果を部署ごとに分析している。
- ✓ 経営層に対するセキュリティ教育はどのような内容を行えばよいかわからない。

O社のプロフィール

業種		製造業
規模		6,000人
管理体制	CISOの有無	有（CIOと兼務）
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	IT部門

セキュリティ担当者の問題・悩み

O社では、製造部門でIoTの利用が進んでいる等、経営としてセキュリティに取り組む必要性とともに以下のような悩みを持っていた。

- **経営層はセキュリティリスクを認識してはいるが、ITリテラシーが十分でない**
- **経営層もサイバーセキュリティのトレンド等を理解していなければ、適切な経営判断が下せない**

一方、部下の立場から経営層に研修を実施することに否定的な意見もあり、経営層のためのセキュリティ教育の実施について悩んでいた。

67

サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集　対応する指示項目　2　対象読者　経営者　CISO等　セキュリティ担当者

取組 (8)　社内の関連部門と連携して外部サービスの選定を行う

解決に向けたアプローチ

システム部門・法務部門の早めの確認によるメリット

システム部門
- ✓ サービス事業者の信頼性・セキュリティ管理体制の確認
- ✓ サービス自体のセキュリティ対策の確認　等

法務部門
- ✓ 利用契約の精査
- ✓ サービス事業者との責任範囲の確認　等

外部サービス利用の検討段階から関与することで、ベンダー選定の判断がより適切になる

そこでN社のCISOは、外部サービス選定の判断に、**システム部門だけでなく法務部門にも参画してもらうことにした。**

当初はシステム部門で判断が難しい場合に適宜法務部門へ問い合わせていたが、問い合わせ件数の増加を踏まえ、定例会を開催することにした。

また、法務部門と協力しながら、チェックシートへ法務的な確認事項も追加し、事業部門で包括的な観点から確認ができるようにした。

得られた知見

N社のCISOは、クラウドサービス等の場合であっても、外部委託と同様、サービス選定に際しては、**サイバーセキュリティリスクの管理部門のみならず、法務部門等、複数の部門の関与が必要不可欠**であると考えている。

これまでは、システム部門・法務部門が定期的に連携することがなかったため、用語の使い方や認識の齟齬が発生することもあったが、次第に**互いに同じ方向で議論でき、建設的なコミュニケーション**ができるようになっていると感じている。

■「サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集」（独立行政法人情報処理推進機構（IPA））
（https://www.ipa.go.jp/security/fy30/reports/ciso/index.html）

（４）関係機関との連携強化

① NISC、金融ISAC等との連携

② 捜査当局等との連携
（金融犯罪の未然防止と被害拡大防止）

③ 国際連携の深化

サイバーセキュリティ対策の強化について（注意喚起）
（2022年2月23日、3月1日、３月24日、4月25日）

- 昨今のサイバー攻撃のリスクの高まりを踏まえ、累次の注意喚起を発出。

➢ 経営層のリーダーシップの下、取引先などのサプライチェーンや国外拠点も含めて、セキュリティ対策の徹底を要請。

①リスク低減のための措置

- ✓ 本人認証の強化（パスワードが単純でないかの確認、多要素認証の利用）・アクセス権限の確認等
- ✓ 情報資産の保有状況の把握・セキュリティパッチの迅速な適用
- ✓ 不用意に添付ファイル・URLを開かないこと等の組織内の周知

②インシデントの早期検知

- ✓ 各種ログの確認
- ✓ 通信の監視・分析等

③インシデント発生時の対処・回復

- ✓ データのバックアップの実施・復旧手順の確認
- ✓ インシデント発生時の対処手順の確認、対外応答・連絡体制等の準備

➢ 金融機関に対し、サイバーインシデント発生時の詳細が判明していない段階であっても、速やかに当局に報告するよう再周知した。

（５）経済安全保障上の対応

- 安全保障の裾野が経済・技術分野に急速に拡大する中、経済安全保障への対応がより重要性を増しており、政府では、その重要分野の一つとして、基幹インフラの安全性・信頼性の確保について検討を進めている。

- 金融業については、国民生活や経済活動の基盤となる基幹インフラの一つであるとともに、大量の個人・企業の情報を保有する産業である。このため、経済安全保障の観点からは、金融業の保有するデータの適切な管理やサイバーセキュリティの強化に加えて、その機器・システムの利用や業務委託等を通じたリスクへの対処などに取り組む必要がある。

- 金融庁としては、関係機関とも連携しつつ、引き続き適切に対応を行う。

最後に

- 金融機関においては、サイバーセキュリティに関する規程・マニュアルや、部署・役職の整備などの体制面での整備に止まらず、その運用が実効的に行われる必要。

（例）・脆弱性管理の基礎となるIT資産台帳（ソフトウェア含む）が適切に整備されていない、セキュリティパッチの適用やOSの更新が適切に行われていない、特権ID管理（パスワード管理、ログ監視を含む）が適切に行われていない、ログの監視・分析を行っていない、といった事例が認められる。

・また、定期的な脆弱性診断、脅威動向を踏まえた演習・訓練の実施といった点についても継続的な取組みが必要。

- サイバーセキュリティ対策を実効的なものとするためには、経営陣が主体的に関与する必要。経営陣のリーダーシップの下で、1線・2線・3線による牽制を働かせるほか、経営陣から現場担当者までセキュリティを実践することが重要。

(例) ・サイバーセキュリティが監査対象に含まれているか。監査の指摘事項に対して適切に改善策が講じられているか。

・経営層は、サイバーセキュリティに関する今後の計画の妥当性を検討しているか。

・ 監査部門と外部専門家による共同監査（コソース）、システム監査人による内部監査を実施しているか。

ご清聴ありがとうございました