金融分野のサイバーセキュリティ強化に向けた金融庁の取組みについて

平成28年11月17日

金融庁　総務企画局　政策課　サイバーセキュリティ対策企画調整室長　　鈴木　　啓嗣

※お断り　：　本稿中、意見に係る部分は担当官個人の見解であって、必ずしも金融庁の公式見解を表わすものではありません。

1．サイバーセキュリティに関する動向等

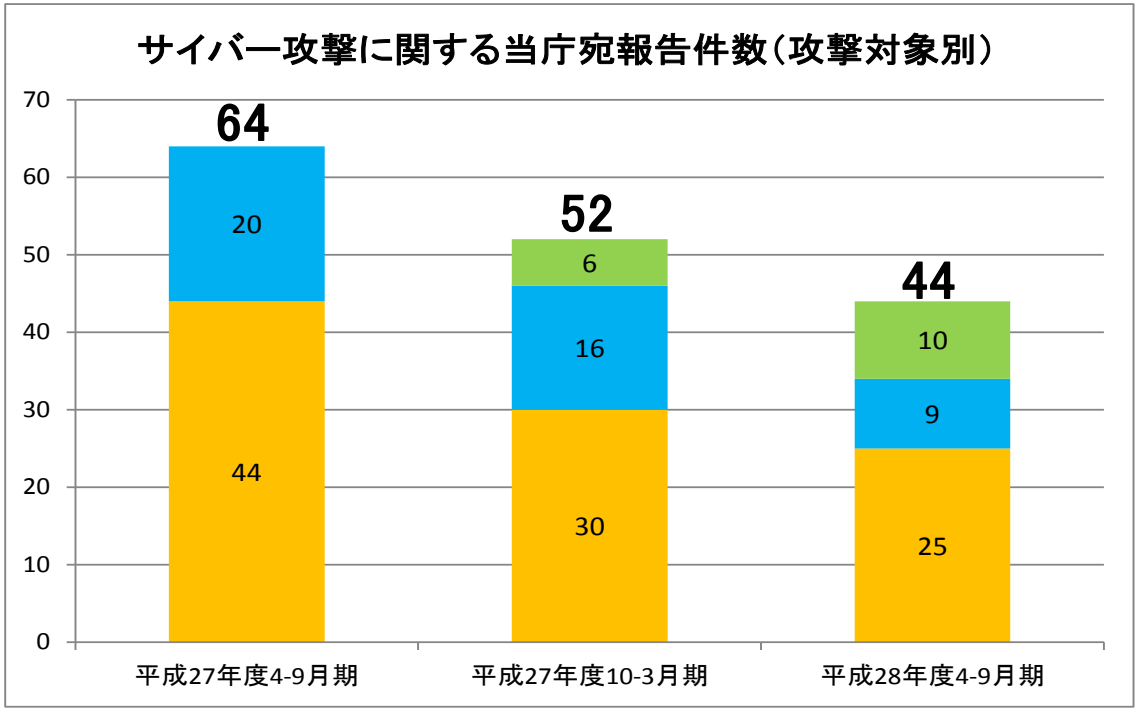
過去のセキュリティインシデント

- ベネッセ（2014/7/9発表）
  社内から顧客情報が外部に持ち出され、確定しているものだけで約760万件の個人情報が流出。
- 日本年金機構（2015/6/1発表）
  標的型メールによるウイルス感染により、年金情報125万件が流出。

最近のセキュリティインシデント

- 日本テレビ（4/21発表）
  HPに対するソフトウェアの脆弱性を利用した不正アクセスにより個人情報約43万件が流出した可能性。
- エイベックス・グループホールディングス（4/28発表）
  公式サイトで使用していたソフトウェアの脆弱性を利用した不正アクセスにより個人情報約35万件が流出した可能性。
- 佐賀県教育情報システム(6/27発表)
  佐賀県の教育情報システム(SEI-NET)、及び校内LANが不正アクセスを受け教員や生徒の個人情報が流出。
- ヤフー(9/22発表)
  2014年に発生した不正アクセスにより少なくとも5億件の個人情報が流出したことを発表。過去最大規模の被害。
- 富山大学(10/10発表)
  富山大学 研究推進機構 水素同位体科学研究センターで標的型攻撃の被害を確認。
  研究成果を含む情報が漏えいした可能性。

金融分野においてもサイバー攻撃は現実の脅威。



国内の金融機関、金融市場インフラが機能停止に陥るような重大な事案は発生していないが、個々の金融機関は、標的型攻撃やサービス妨害（DDoS）攻撃、不正ログインの試行等を現実に受けている。

1.3 これまでの金融分野のサイバーセキュリティに関する取組み

① サイバーセキュリティ基本法の制定(26年11月、28年4月改正)

- ◆ インターネット等の活用の進展に伴って世界的規模で生じているサイバーセキュリティ脅威の深刻化等に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題。
- ◆ 政府及び重要インフラ事業者はサイバーセキュリティ確保のための施策を講じることが求められている。

② 監督指針・検査マニュアル改正(27年4月)

- ◆ 金融機関に求めるサイバーセキュリティ管理態勢の整備状況について、監督上の着眼点として明確化する等、改正を実施。

③ サイバーセキュリティ強化に向けた取組方針を公表(27年7月)

金融分野のサイバーセキュリティ強化に向けた5つの方針
1. サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
2. 金融機関同士の情報共有の枠組みの実効性向上
3. 業界横断的演習の継続的な実施
4. 金融分野のサイバーセキュリティ強化に向けた人材育成
5. 金融庁としての態勢構築

④ 金融行政方針にてサイバーセキュリティの強化を重点施策として公表(27年9月、28年10月)

⑤ 経済産業省と(独)情報処理推進機構(IPA)が、「サイバーセキュリティ経営ガイドライン」を公表(27年12月)

⑥ G7伊勢志摩サミット首脳宣言やその付属文書(サイバーに関するG7の原則と行動)を公表(28年5月)

⑦ 「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」を公表(28年10月)

２.「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」と進捗状況

１. サイバーセキュリティに係る金融機関との建設的な対話と一斉把握

２. 金融機関同士の情報共有の枠組みの実効性向上

３. 業界横断的演習の継続的な実施

４. 金融分野のサイバーセキュリティ強化に向けた人材育成

５. 金融庁としての態勢構築

◆ 建設的な対話と一斉把握の実施状況

実態把握の進め方 （昨事務年度は、2段階で実施）

○ 3メガ、大手生損保等は、既に把握済み

○ フェーズ1（H27年10月～12月末まで）

➢ 地銀・第二地銀、証券会社、大手以外の生損保、取引所等、合計82社と対話

○ フェーズ2（H28年5月～6月末まで）

➢ フェーズ1の未実施金融機関の中から、地銀を中心に大手以外の証券会社・生損保など、合計61社と対話

実態把握の手法

○ 金融機関のサイバーセキュリティ対策の状況を深堀りするため、対面でのインタビュー形式で実施。なお、インタビューを効率的に進めるため、事前に「確認項目」への回答を依頼し、その回答を分析した上でインタビューを実施。

○「確認項目」の概要

- ✓ サイバーセキュリティに関する経営陣の取組み
- ✓ リスク管理の枠組み
- ✓ サイバーセキュリティリスクへの対応態勢
- ✓ コンティンジェンシープランの整備と実効性確保
- ✓ サイバーセキュリティに関する監査

ここが疎かな金融機関は、対策に遅れが見られる。

○ サイバー攻撃のいくつかのシナリオに基づく金融機関等の対応の確認（ケーススタディ）

◆ 建設的な対話と一斉把握の結果（概要）①

・経営層の取組が良いところは態勢整備が進んでいる

しかしながら、殆どの金融機関において経営陣の関与が希薄（受動的）。
規程・組織体制の整備に際し、サイバーセキュリティに対する経営陣の役割と責任を文書化する等、経営陣が陣頭指揮を執る態勢を明確にし経営資源を適切に投下していく態勢の確立が必要。

・サイバーセキュリティに着眼したリスク評価を実施する必要

保護すべき重要情報や重要サービスの網羅的な洗い出しとサイバーセキュリティリスクの把握、自組織に必要な施策の選定と対応の優先付けを行いPDCAを回す。

・侵入されることを前提とした対策を強化する必要

監視、検知能力の向上、攻撃検知時に適切な初動が取れる能力の獲得、コンティンジェンシープランの策定と職員教育・訓練の実施。

・金融ISACをはじめとした情報共有（共助）態勢を確立する必要

加入するだけでなく、活動に参加することが大切。人材育成にも繋がる。

◆ 建設的な対話と一斉把握の結果（概要）②

➢ **態勢整備が進んでいる金融機関に共通してみられたパターン**

① サイバー攻撃状況（自社、他社）の報告を通じ経営陣がリスク認識を深化。

② 取組方針を取締役会レベルで決議し、経営陣が陣頭指揮を執る姿勢を表明。

③ サイバーセキュリティに着眼したリスク評価を行った上で課題を洗い出し、対策や必要な経営資源、取組計画を策定し、取締役会レベルで審議。

④ CSIRT等のサイバーセキュリティ対応部門について、実効性の高い組織体制を確立し、必要に応じ内外からの専門家や予算確保といった経営資源を投下。

⑤ 経営陣が頻繁に取組計画の進捗状況を報告させ把握し、PDCAサイクルを確立。

⑥ 攻撃手法の変化等に応じ速やかにリスクを再評価し、取組計画を見直して技術的対策や追加演習を実施し、不断の対策強化・実効性向上を推進。

業界向けフィードバック

建設的な対話と一斉把握の結果、明らかになった「課題のあった事例」や「良好事例」は、業界団体を通じて金融機関に還元。金融機関に自己点検を通じてサイバーセキュリティ対策の加速を促す。

フィードバックの内容

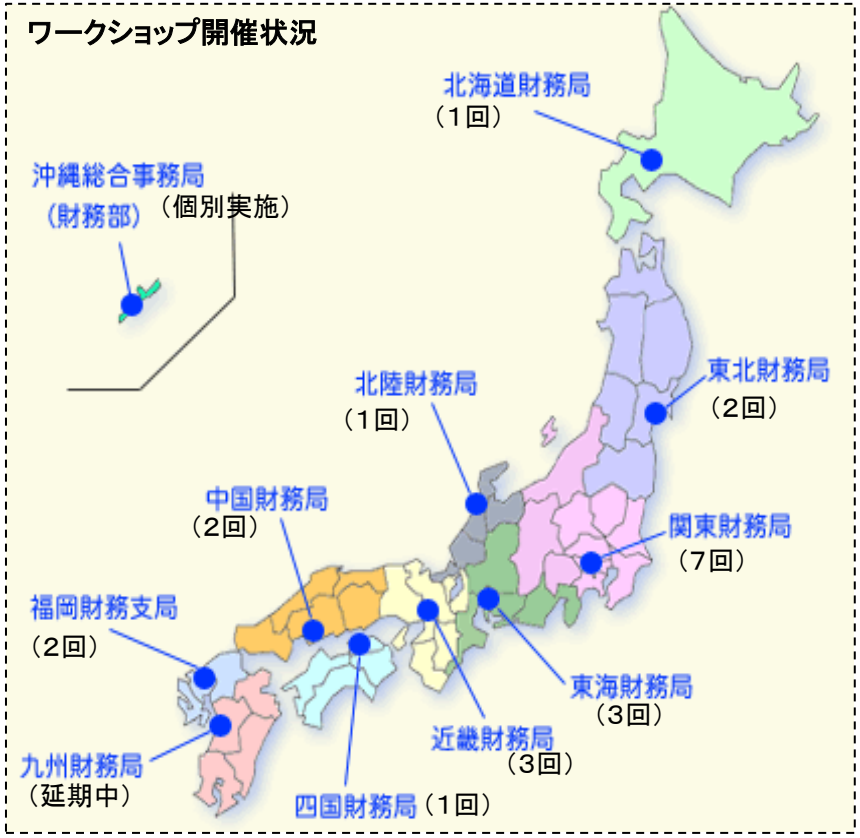
建設的な対話と一斉把握の結果を踏まえて

- ✓ 経営陣の積極的な関与の必要性
- ✓ サイバーセキュリティに着眼したリスク評価の実施
- ✓ 規模・特性に応じたリスクベースアプローチに基づくサイバーセキュリティ対策

等が重要である旨説明。

開催実績

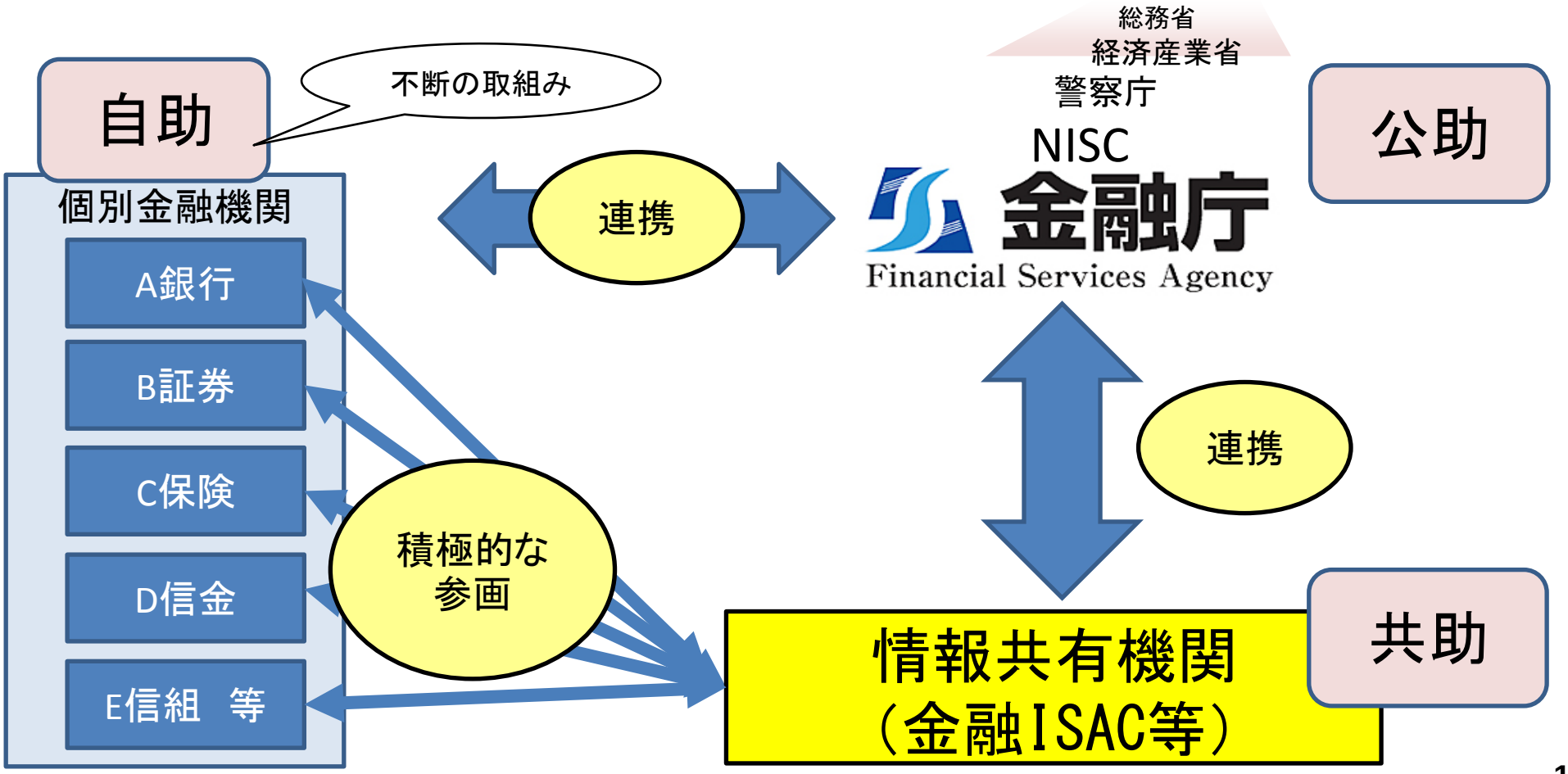
フェーズ2では、ワークショップを併催



- **9財務（支）局で通算22回開催**
  （九州局は熊本地震のため延期中、沖縄は個別実施）
- **参加対象金融機関数（第2地銀、信用金庫、信用組合、証券会社）は456**
  （九州（26）・沖縄（1）を除く）
- **参加金融機関は449（参加率98.5%）**

◆ 官民一体の取組

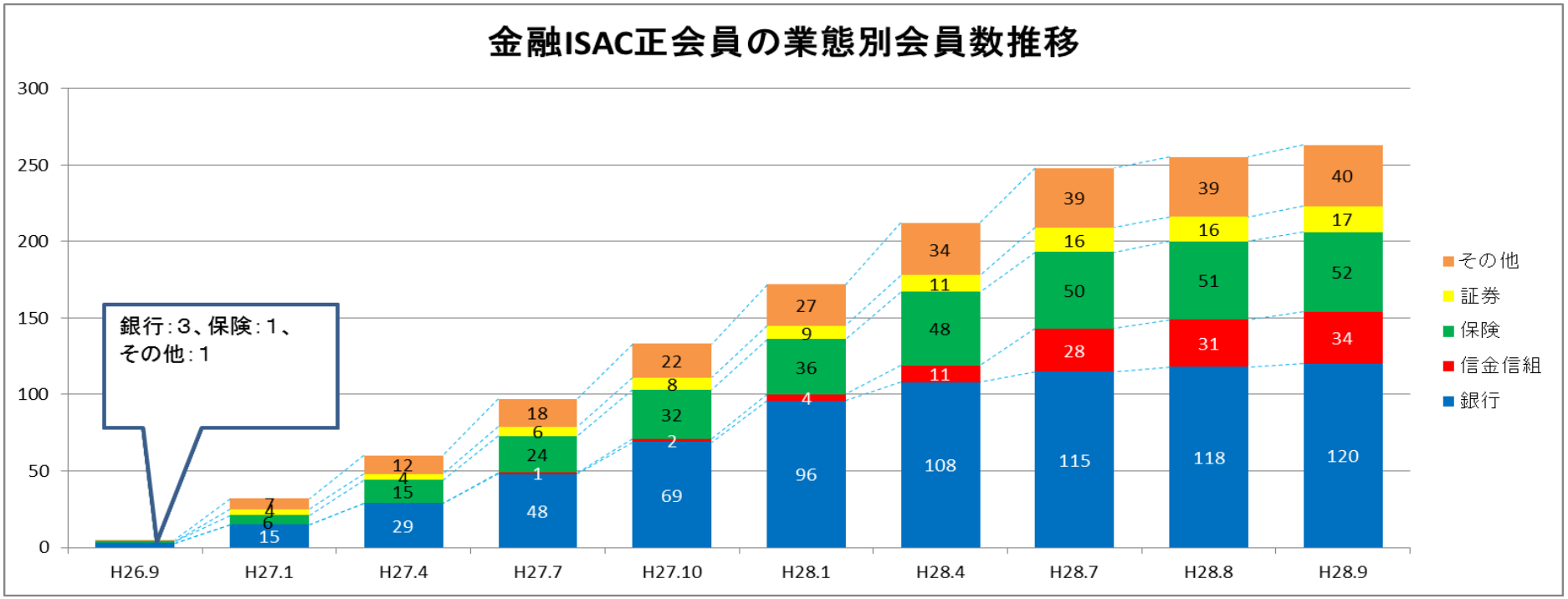
✓ 日々発生しうるサイバー攻撃に対する、個別金融機関のみによる対応には限界がある。金融機関自身による「自助」、金融庁等の当局の支援による「公助」、そして情報共有機関を活用した「共助」の考え方のもと、**官民一体**となってサイバーセキュリティ対策を向上させていく必要がある。



◆ 金融ISACへの加盟状況

参加金融機関279社（正会員：263社、準会員：16社）

地銀・第二地銀、生・損保は加盟が進んでいるが、信金・信組、証券会社の加盟は進んでいない。



出典：金融ISACの情報を基に加工（2016年10月11日時点）

✓ サイバーセキュリティ2016（2016年8月31日サイバーセキュリティ戦略本部）
金融庁において、金融機関に対し、「金融ISAC」を含む情報共有機関等を通じた情報共有網の拡充を進める。

初めての金融業界横断的なサイバーセキュリティ演習（Delta Wall）の実施について

金融分野のサイバーセキュリティを巡る状況

- 金融分野でのインターネットの利用拡大
- サイバー攻撃の高度化
- サイバーテロの脅威（2020年東京オリンピック・パラリンピックも見据えて）

→ サイバーセキュリティの確保は、金融システム全体の安定のため、喫緊の課題

「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」（平成27年７月公表）

➢ 取組方針の5つの柱

1. サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
2. 金融機関同士の情報共有の枠組みの実効性向上
3. 業界横断的演習の継続的な実施
4. 金融分野のサイバーセキュリティ強化に向けた人材育成
5. 金融庁としての態勢構築

（参考）

✓ 米英では、金融分野における業界横断的な演習を実施

国名	実施主体	演習名
米国	米国証券金融市場協会	Quantum Dawn
英国	イングランド銀行等	Waking Shark

金融業界横断的なサイバーセキュリティ演習

◆ **本年10月24～27日**、金融業界全体のサイバーセキュリティの底上げを図ることを目的に、**初めてとなる金融業界横断的な演習（通称：Delta Wall(※)）を実施予定**

（※）Delta Wall：サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の3つの視点（Delta）＋防御（Wall）

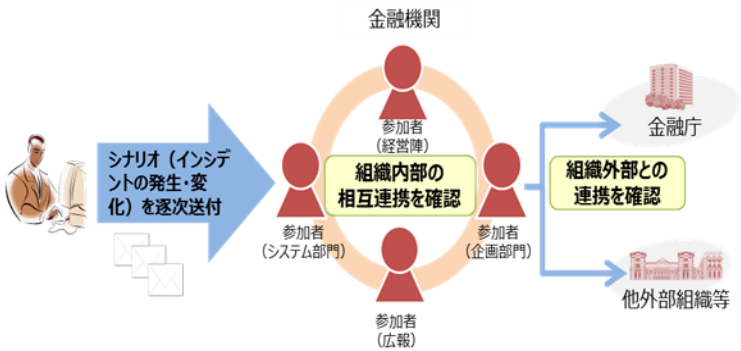
◆ **約80の金融機関（銀行、信金・信組、証券会社及び保険会社）が参加。**今後も継続的に実施予定（注）

（注）29年度は演習実施経費等として約78百万円を予算要求（28年度予算：約45百万円）。また、本演習に係る費用は金融庁と参加金融機関の双方で負担

演習の特徴

- 民間コンサル等の演習を利用しにくい**中小地域金融機関が多数参加**
- 多くの関係部署（経営層、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（⇔会場集合方式）
- 民間の**専門家の知見や攻撃の実例分析等を参考**にしつつ、金融機関が陥りやすい弱点が浮き彫りとなり、**参加者に「気づき」を与える**ことが可能な内容
- 参加金融機関が「つつがなく演習をクリア」したことで良しとしないよう、「とり得た他の選択肢」等を提示するなど**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



【シナリオの一例】

✓ 自社ウェブサイトを閲覧した者からウイルスに感染したとの苦情
  ➢ 組織内部の情報共有、初動対応の確認

✓ 自社ウェブサイトに、ウイルスが仕込まれていることが発覚
  ➢ 対処方法の確認・実施、当局等外部関係者への連絡

✓ 顧客・マスコミからの問合せ
  ➢ オンラインサービス停止等の経営判断、顧客等への周知

✓ ウェブサイトの復旧の準備が完了
  ➢ 外部関係者への連絡、顧客等への周知

（参考）
- 本演習では、上記のほか、サイバー攻撃予告、ウイルス感染による情報流出のシナリオを用意

３．金融行政方針（平成28事務年度）

抄、平成28事務年度金融行政方針

Ⅰ．金融行政運営の基本方針

Ⅱ．金融当局・金融行政運営の変革

Ⅲ．活力ある資本市場と安定的な資産形成の実現、市場の公正性・透明性の確保

Ⅳ．金融仲介機能の十分な発揮と健全な金融システムの確保等

Ⅴ．IT技術の進展による金融業・市場の変革への戦略的な対応

Ⅵ．国際的な課題への対応

Ⅶ．顧客の信頼・安心感の確保

Ⅷ．その他の重点施策

（1）FinTechへの対応
＜略＞
（2）サイバーセキュリティの強化
- **高度化するサイバー攻撃の脅威に対し**、金融分野のサイバーセキュリティの底上げを図るため、金融機関のサイバーセキュリティ管理態勢の向上や情報共有を推進
- 初の**金融業界横断的なサイバーセキュリティ演習**を2016年10月末に実施

（3）アルゴリズム取引等への対応
＜略＞

抄、平成28事務年度金融行政方針

Ⅴ．IT技術の進展による金融業・市場の変革への戦略的な対応

（2）サイバーセキュリティの強化

金融分野におけるサイバー攻撃の高度化が進む中、サイバーセキュリティの確保は、金融システム全体の安定のため喫緊の課題となっている。金融庁としては、「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」（2015 年7月）に沿って、**引き続き、実態把握を通じた金融機関のサイバーセキュリティ管理態勢の向上、金融ISAC等を通じた情報共有の推進等に取り組んでいく**。

さらに、**初の金融業界横断的なサイバーセキュリティ演習を2016 年10 月末に実施し、金融業界全体のサイバーセキュリティの底上げを図る**。

また、G7各国の金融監督当局・財務省・中央銀行の間で、**「G7サイバーエキスパートグループ」が設置され、金融分野におけるサイバーセキュリティの促進やG7各国間での連携強化等に向けた議論が開始されており、各国当局とともにこうした議論に貢献**していく。

４．国際的な金融分野のサイバーセキュリティに関する取組み

○昨年、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）

「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」

（G7議長国 プレスリリース（仮訳）抄　2016年10月11日）

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。この作業は、金融セクターのサイバーセキュリティを改善するために、「G7伊勢志摩首脳宣言」や「サイバーに関するG7の原則と行動」で求められたコミットメントを果たす上での重要な進捗を示している。

○ 基礎的要素は、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なポイントを示したものであり、以下の8項目が示されている。

- ◆ 要素1：サイバーセキュリティ・ストラテジーとフレームワーク（Cybersecurity Strategy and Framework）
- ◆ 要素2：ガバナンス（Governance）
- ◆ 要素3：リスク管理の評価（Risk and Control Assessment）
- ◆ 要素4：モニタリング（Monitoring）
- ◆ 要素5：インシデント発生時の対応（Response）
- ◆ 要素6：復旧（Recovery）
- ◆ 要素7：情報共有（Information Sharing）
- ◆ 要素8：継続的な学習（Continuous Learning）

要素1：サイバーセキュリティ・ストラテジーとフレームワーク（Cybersecurity Strategy and Framework）

◆ 国内外及び業界における標準やガイドラインを適切に踏まえ、自らが対峙するサイバーリスクに対応したサイバーセキュリティ・ストラテジーとフレームワークを構築・維持すること。

要素2：ガバナンス（Governance）

◆ サイバーセキュリティ・ストラテジーとフレームワークを実施し、管理し、有効性を確認する役職員の役割・責任を明確化し、これらの手順を促進することにより、アカウンタビリティを確保すること。また、当該役職員に対し、十分なリソース、適切な権限、経営陣等（例えば、企業にあっては取締役会、当局にあっては幹部）へのアクセスを付与すること。

要素3：リスク管理の評価（Risk and Control Assessment）

◆ 相互接続関係や依存度、外部委託の状況も踏まえ、機能・業務・製品・サービスを特定し、それらの重要性に優先順位を付した上で、それぞれのサイバーリスクを評価すること。経営陣によって設定された許容度の範囲内で、こうしたリスクを統御・管理するため、システム、方針、手順そして訓練を含めた管理手法を確定・実施すること。

要素4：モニタリング（Monitoring）

◆ サイバーインシデントを速やかに検知し、ネットワークのモニタリング、テスト、監査、演習等を通じて種々の管理手段の有効性を定期的に評価する、体系的なモニタリングプロセスを構築すること。

要素5：インシデント発生時の対応（Response）

◆ インシデント発生時に、以下のような対応をタイムリーにとること。

(a) サイバーインシデントの特性、範囲、影響を評価すること。
(b) インシデントを封じ込め、その影響を軽減すること。
(c) 内外の関係者（司法当局、規制当局、その他の当局に加え、必要に応じ、株主、外部委託先サービスプロバイダー、顧客）へ通知すること。
(d) 必要に応じて、共同でインシデント対応を図ること。

要素6：復旧（Recovery）

◆ 脆弱性等の改善作業を継続しつつ、速やかに業務を再開すること。具体的には、以下のような対応をとること。

(a) インシデントによる有害な痕跡を除去すること。
(b) システムやデータを正常に復旧し、平常状態を確保すること。
(c) 悪用された脆弱性をすべて特定し、軽減すること。
(d) 同様のインシデントから防御するため、脆弱性を改善すること。
(e) 内外との適切なコミュニケーションを確保すること。

要素7：情報共有（Information Sharing）

◆ 防御の強化や被害の最小化、状況認識の向上や広汎な知識の習得のため、脅威、脆弱性、インシデントの発生、発生時の対応に関する、信頼性の高い実践的なサイバーセキュリティ情報を、内外の関係者（金融セクター内外の金融機関及び当局を含む）とタイムリーに共有すること。

要素8：継続的な学習（Continuous Learning）

◆ サイバーリスクの変化に対処し、資源を割当て、ギャップを特定・改善し、教訓を活かすため、サイバーセキュリティ・ストラテジーとフレームワークを定期的かつ必要に応じて見直すこと（見直しに際しては、ガバナンス、リスク管理の評価、モニタリング、インシデント対応、復旧、情報共有の要素を含むこと）。

本日はお忙しい中、ご出席くださいまして
ありがとうございました。