諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書

2015年（平成27年）3月31日

pwc プライスウォーターハウスクーパース株式会社

■目次

■ 1. 概要

本調査の概要は次の通りである。

1.1. 調査の背景

近年、世界におけるサイバー攻撃の脅威は急速に増大しており、日本においても、金融機関やその顧客への攻撃をはじめとした種々のサイバー攻撃の被害が拡大している。

日本においては、2014 年（平成 26 年）の一年間における国内のインターネットバンキングの不正送金の被害件数が 1,876 件にも及び、被害総額は約 29 億円を超えた。この数字は、前年比で約 2 倍、前々年比では約 60 倍にまで膨れ上ったことを意味する。金融機関のネットバンキング等の Web サービスを狙った攻撃は、年々その手法（手口）が高度化している。この数年では、従来のマルウェアによる電子証明書や ID・パスワードの不正取得、フィッシングなどの攻撃に加えて、ネットバンキング利用者を偽の入力画面に誘導し、ボット[1]を遠隔操作して不正送金を行う「Gave Over Zeus[2] [3]」と呼ばれるマルウェアや、出荷通知などを装った電子メールに添付する形で個人情報などを収集する「VAWTRAK[4] [5]」と呼ばれるマルウェアが日本でも多く発見された。また、2014 年（平成 26 年）には、JavaScript ファイルを使った「ATS（Automatic Transfer System、自動送金システム）[6]」と呼ばれるマルウェアが確認された。これは、ワンタイムパスワードなどの二要素認証すら破ることのできる新種で、国内でも約 2 万台の PC が感染した[7]。さらに海外では、「CARBANAK（カーバナック）[8] [9]」と呼ばれる多国籍サイバー犯罪集団による金融機関を狙った大規模な標的型サイバー攻撃活動が確認されている。彼らは金融機関の利用者ではなく従業員に狙いを定め、独自に開発したマルウェアを添付ファイルとしてメール送信して金融機関のネットワークに侵入したのち、送金取引の操作記録を盗み見るなど不正送金の手口を探り、金銭の窃取を行う。

---

1 「11.用語の説明」を参照。

2 感染したシステムでインターネットバンキングにログインすると偽画面を表示させ認証情報を攻撃者に転送したり、ボットとして遠隔操作可能にしたりする。また他のシステムと連動してボットネットを形成したり、駆除しづらいという特徴を持つ。

3 http://about-threats.trendmicro.com/Malware.aspx?language=jp&name=ZEUS

4 出荷通知を装った電子メールの添付ファイルとしてマルウェアを感染させ、インターネットバンキングの認証情報の窃取などをおこなうマルウェア。

5 http://about-threats.trendmicro.com/relatedthreats.aspx?language=jp&name=VAWTRAK Plagues Users in Japan

6 閲覧中の Web ページに JavaScript コード（ブラウザで実行されるプログラム）を勝手に挿入して不正送金処理を自動的に行ってしまうように作成されたマルウェア。通常インターネットバンキングの Web サービスは、送金操作に際に二要素認証などで都度の認証が行われるようになっているが、それらも自動的に突破する仕組みを備えている。

7 http://blog.trendmicro.co.jp/archives/9884

8 http://about-threats.trendmicro.com/relatedthreats.aspx?language=jp&name=CARBANAK Targeted Attack Campaign Hits Banks and Financial Institutions

9 この攻撃で使用されるマルウェア自身を CARBANAK と呼ぶ場合もある。

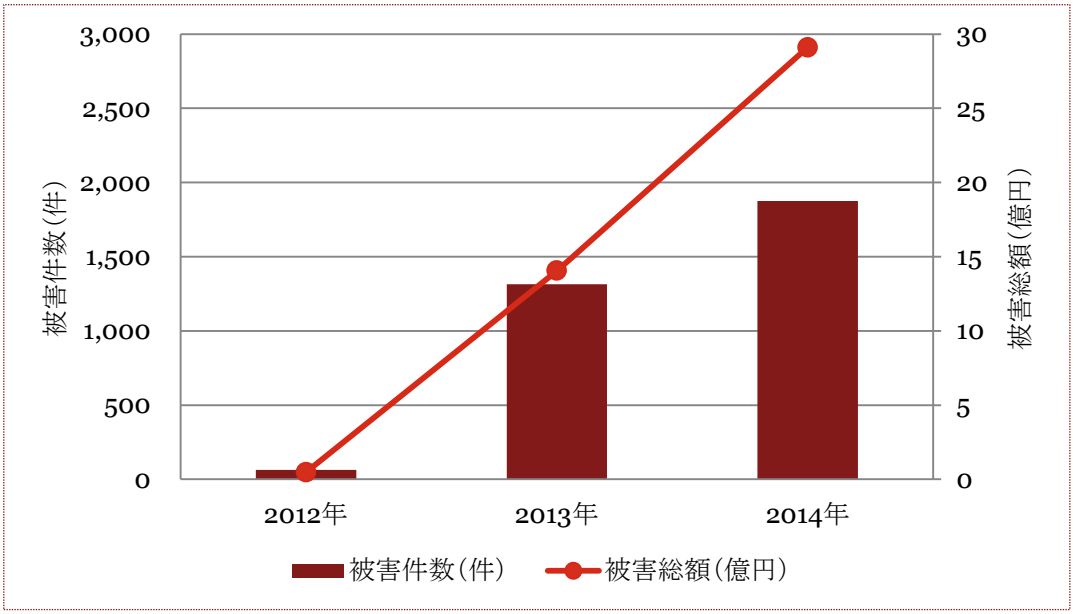

図 1-1 インターネットバンキングの不正被害の件数と総額[10]

このように金融分野を含めて社会全体にサイバー攻撃の脅威が高まる中、2014 年（平成 26 年）11 月 6 日には「サイバーセキュリティ基本法[11]」が成立し、2015 年（平成 27 年）1 月 9 日に全面施行された。今後、内閣に設置された「サイバーセキュリティ戦略本部」の下で、各省庁は監督下の民間企業等におけるサイバーセキュリティ対策を推進していくことになる。

金融庁では、重要インフラである金融分野のサイバーセキュリティ対策に係る取組みを検討していくにあたり諸外国の先行事例について調査研究を行うことが必要であると判断し、本調査の実施を決定した。

1.2. 調査の目的

本調査の目的は、諸外国の政府、監督機関、金融機関におけるサイバーセキュリティの取組みから、今後の日本の金融分野におけるサイバーセキュリティ対策のために参考となる情報を得ることである。中でもサイバーセキュリティに対する積極的な対策が実施されていると思われる米国、英国、韓国、及び欧州連合（EU）を対象として、監督機関におけるサイバーセキュリティへの取組み（サイバーセキュリティに関する法制度に基づいた監督機関の組織、検査監督のガイドラインなど）及び金融機関におけるサイバーセキュリティの取組み（管理体制のガイドライン、金融機関の取組体制、関係組織との連携体制、有事への対応状況や、サイバー保険の動向など）を調査した。

1.3. 調査期間

2015 年（平成 27 年）2 月 2 日（月）~2015 年（平成 27 年）3 月 31 日（火）

10 http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf
11 http://law.e-gov.go.jp/htmldata/H26/H26HO104.html

1.4. 調査対象国・地域

米国、英国、韓国、および欧州連合（EU）

1.5. 調査実施範囲

本調査は、上記の調査対象国および地域におけるサイバーセキュリティへの取組みと対策、国内外関係機関との連携状況、サイバー攻撃やテロに対する演習などの実施状況、金融分野における具体的な攻撃の手口の動向、さらにサイバー保険の利用状況などを対象として実施した。

1.6. 主要調査項目

本調査では、2015 年（平成 27 年）1 月 5 日付けで金融庁より公示された「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究」の入札仕様書に従い、以下の項目を中心に調査を行った。

1） 金融分野における政府及びサイバーセキュリティへの取組みに関する以下の事項の内容

- 政府の中で、金融分野のサイバーセキュリティ対策を担当している組織（以下、「当該組織」という。）
- 当該組織等、政府が公表している金融分野のサイバーセキュリティ対策の取組方針（要人が対外的な発信の中で示したものも含む）
- 当該組織等が定めるサイバーセキュリティの定義、範囲
- 当該組織等が金融機関のサイバーセキュリティ対策の取組み状況を検査・監督する際のガイドライン、ハンドブック等
- 金融機関（又は企業全般）によるサイバーセキュリティ対策に係る安全対策の基準（例：日本における金融情報システムセンター（FISC）による「安全対策基準」のようなもの）とその特徴
- 当該組織等による所管金融機関のサイバーセキュリティ対策の取組状況を評価したもの（実態、課題の抽出、改善策等）
- 当該組織等と海外当局との間での金融分野のサイバーセキュリティ対策についての連携
- 官民・民々間における情報共有の枠組み、情報共有の実態及び共有されている情報の活用状況ならびに情報共有における問題点と対策
- サイバー攻撃やサイバーテロに対する官民における対応態勢
- 政府の主導、または金融業界として取組んでいるサイバー攻撃への対応に係る演習の具体的内容と実施結果に対する評価

2） 現在、調査対象国で特に懸念されている金融に関するサイバー攻撃の手口（金融インフラの機能停止を狙った攻撃、個別金融機関のシステムの機能停止や顧客情報等の窃取を狙った攻撃、金融機関と

その利用者の金銭等を窃取する目的の攻撃それぞれに関して）、攻撃者の特徴ならびに特徴的な攻撃事例、及び我が国において同様の被害が発生する可能性

3） 金融に関するサイバー攻撃の目的や手口のトレンド（変化の状況のほか、英国においては、ロンドン五輪との関連性についても考慮する）

4） 調査対象国（特に米国）におけるサイバー保険の動向（市場規模、補償範囲、保険料算出にあたっての事故率の考え方、日本と比較した顧客ニーズの違いなど）

■ 2. 調査実施方法

本調査の実施にあたり、業務の分担、調査方法等は、次の通りとした。

2.1. 各対象国・地域の調査

各対象国および地域における調査は、プライスウォーターハウスクーパース（PwC）のグローバルネットワークのメンバーファームである PwC 米国（PwC US）、PwC 英国（PwC UK）、PwC 韓国（PwC Korea）に所属する金融サービス部門のサイバーセキュリティ担当者が中心になって行った。

2.2. 調査の方法

調査は、公開情報の収集、分析のほかに、プライスウォーターハウスクーパース（PwC）の社内知見の利用、更に必要に応じて当該機関担当者への聞き取りを実施して行った。

各国および地域で調査した結果を日本に所在するプライスウォーターハウスクーパース株式会社（PwC Japan）が取りまとめ、報告書を作成した。

■ 3. 本調査における前提

本調査における前提として、国や地域に依存しないサイバーセキュリティの定義や攻撃の手口などは、次の通りである。

3.1. サイバーセキュリティの定義

我が国の「サイバーセキュリティ基本法」では、「サイバーセキュリティ」を次のように定義している。

- 「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。」

あらゆるものがコンピュータ・ネットワークに接続され、多種多様な情報がインターネットその他の仮想的なグローバル空間である『サイバー空間』で流通する状況が急速に拡大、浸透する中、サイバー空間を取り巻く不正侵入や、情報の窃取、改竄や破壊、情報システムの機能停止や誤作動誘発、不正プログラムの実行などのサイバー攻撃に対して、情報そのものや、コンピュータやネットワークなどの情報システムを適切に保護する必要性が高まっている。

3.2. 従来の情報セキュリティとの違い

従来の「情報セキュリティ」は、主に組織が保有する情報およびコンピュータ、ネットワーク機器などの情報システムの「機密性」、「完全性」、「可用性」が、その組織において適切に維持管理されていることを示していた。

一方で、「サイバーセキュリティ」は、従来のコンピュータ、ネットワーク機器などの情報システムのみならず、これまで一般的に情報処理に供されていなかった、もしくはコンピュータ・ネットワークとは接続されていなかったあらゆる機器、例えば建物におけるエネルギー制御システムや、照明、監視カメラ、物理セキュリティセンサーなどが、インターネットその他のコンピュータ・ネットワークに接続され、仮想的なグローバル空間である「サイバー空間」上で相互に接続され、そしてサイバー空間に接続される機器及び情報の機密性、完全性、可用性が、サイバー空間上で適切に維持管理されていることと捉えることができる。

リアル空間とサイバー空間における脆弱性を巧みに利用した標的型攻撃（Advanced Persistent Threats attack: APT 攻撃）[12] や、ネットワーク上での重要インフラを対象としたサービス妨害（DoS や DDoS）攻撃[13]、Web ページの改竄などの「コンピュータネットワーク上で行われる不正行為」に対する保護は、サイバーセキュリティに特有な活動と言える。

3.3. 金融機関のサイバー攻撃と対策をめぐる課題

近年、金融機関はサイバーセキュリティへの対策を大幅に改善してきたものの、日々新たに開発されるマルウェアなど攻撃者の最新の手口に対して対応が追い付いているとは言えない。従来のサイバーセキュリティに対する経験則にその多くを頼っているためである。

金融機関の情報システムのインフラの在り方がここ数年で大きく変わったのに対し、サイバーセキュリティへの対策も考え方を大きく転換する事が必要になってきている。

従来の情報システムで多く用いられてきたクライアント・サーバ型の構成では、組織のコンピュータ・ネットワークは外部のネットワークと内部のネットワークが明確に分断され、外部のネットワークに接続する境界の保護と、利用者の操作するエンドポイントの保護が主なものとなっていた。

これに対して、近年はクラウド環境やモバイル機器の普及が急速に進み、情報システムに対して接続する OS の種類や機器の種類、接続形態が増えた。モバイル環境のセキュリティは現在重要性が高まっている領域の一つである。また、国家的な支援を受けた攻撃も重大な懸念事項となってきており、金融機関も攻撃の対象となることが多い。

今日の脅威の増加したコンピュータネットワーク環境を背景に、毎年検出されるインシデント（情報セキュリティ事件・事故）の数は増加している。結果として、インシデントによる経済的損失の合計額は、脅威へ対応するための費用と手間に比例し増加している。

3.4. サイバー攻撃の対象

金融分野におけるサイバー攻撃の対象と成り得るものは、大別すると、「金融機関の情報漏洩を狙った攻撃」、「金融機関の機能停止を狙った攻撃」、「金融機関の利用者に対する攻撃」の三種類が考えられる。

3.4.1. 金融機関の情報漏洩を狙った攻撃

金融分野におけるサイバー攻撃の対象として第一に挙げられるのは、金融機関が保有する情報資産を盗み出す攻撃である。この攻撃の多くは、金融機関の従業員宛てに標的型メールを送信することから始まる。予めソーシャルエンジニアリング[14]などの手口で盗み出した従業員の人事情報やメールアドレスを悪用し、巧妙な成りすましメールを送信する手口である。成りすましメールには攻撃者が構築した悪質な Web サイト

12「11.用語の説明」参照
13「11.用語の説明」参照
14「11.用語の説明」参照

へのリンクや、悪質なプログラムが埋め込まれた添付ファイルが貼られており、それを従業員が不用意にクリックしてしまうことが端緒となり、内部情報の外部流出へと繋がる。金融機関は法人顧客の機密情報や個人顧客の口座情報などを大量に保有しており、これらが外部に流出して悪用された際の財務的損失や評判低下などの影響は甚大である。このようなサイバー攻撃は、グローバルにビジネスを展開している大手金融機関のみならず、中小規模の金融機関も同様に標的となる可能性がある。

3.4.2. 金融機関の機能停止を狙った攻撃

金融分野におけるサイバー攻撃の対象として第二に挙げられるのは、金融機関が保有する情報システムなどの重要機能を停止させる攻撃である。金融機関における ICT[15]は社会基盤そのものであり、金融機関は ICT の活用なくして事業を継続することは不可能である。このため、金融機関の業務、ひいては金融システムの機能停止を狙った、重要な経営資源である情報システムへの攻撃が想定される。攻撃の具体例としては、ATM 網の停止、決済システムの業務の停止、DDoS 攻撃によるインターネットサービスの停止、Web ページなどの外部公開情報の改竄による誤情報掲示などが考えられる。この種の攻撃を受けた場合、個々の金融機関において機会損失や評判の低下が生じるだけでなく、国際社会における日本の金融システムそのものの信頼性が失われる危険性が高く、影響の大きさは計り知れない。

3.4.3. 金融機関の利用者に対する攻撃

金融分野におけるサイバー攻撃の対象として第三に挙げられるのは、金融機関の利用者（顧客）が保有する金融資産を窃取する攻撃である。この種の攻撃は銀行など預金業務を行う金融機関の利用者に対する攻撃であり、次図に示す通り、金融機関の規模や営業地域には関係なく、インターネットバンキングなどのサービス利用者が一様に対象となる可能性があり、フィッシング詐欺や不正プログラム侵入の対象として狙われることが考えられる。

15 Information and Communication Technology の略称で情報通信技術を意味する

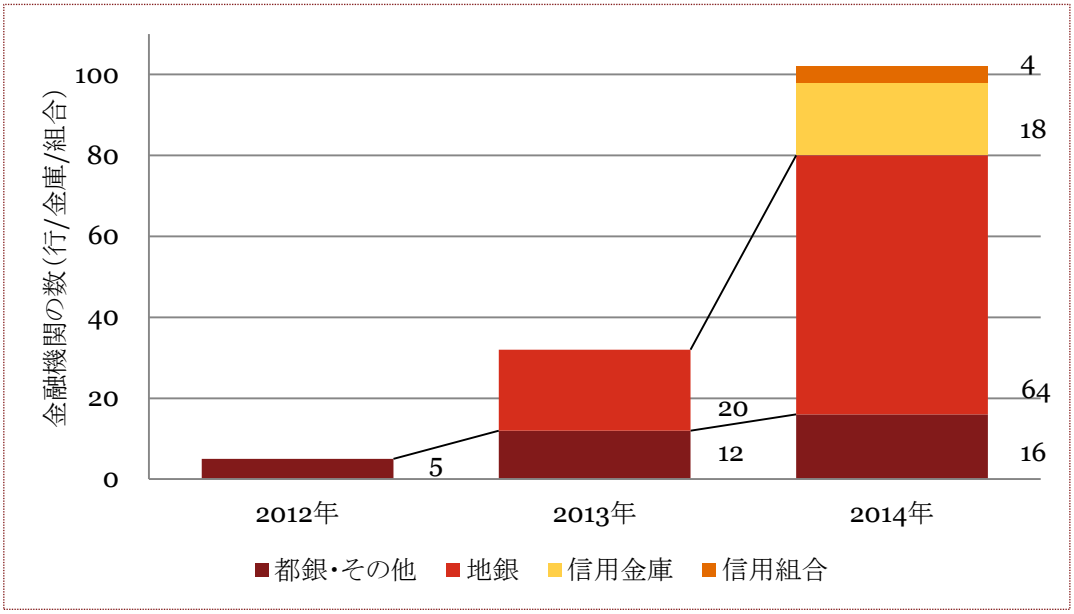

図 3-1 規模ごとの被害にあった金融機関数の推移[16]

一方、証券会社や保険会社など預金業務を行わない金融機関の利用者に対する攻撃は、仮に証券会社のインターネット取引サービスや保険会社のインターネット契約者貸付サービスなどが乗っ取られたとしても、その後、攻撃者の手元に現金が渡るまでに多段階の不正操作が必要となるため、預金口座に比べると発生可能性は低いと考えられる。ただし、不正なオンライントレードによる作為的な相場形成により金融機関利用者が不利益を被るリスクは否定できない。

3.5. サイバー攻撃の手口

サイバー攻撃の手口は、日々新しい技術が出現することに伴い急速に進化し、また地政学的な要素と共にグローバルに拡大している。各金融機関が直面するサイバー攻撃の特性は、事業の本質によって多様である。したがって、各金融機関がとるべき戦略もサイバー攻撃の種類によって異なり、導入される対策も様々である。

ここでは、攻撃の対象ごとに主要な攻撃の手口について整理する。なお、各用語については「11.用語の説明」参照

3.5.1. サイバー攻撃の傾向

近年の金融分野におけるサイバー攻撃において頻繁に見られれる攻撃の傾向は下記の通りである。

- 電子メールまたは電子メール以外によるフィッシング攻撃
- ソーシャルエンジニアリングと ID の組み合わせによるカードデータ不正
- オープンソースのソフトウェアの脆弱性をついた攻撃

16 http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

- 難読化された高度なマルウェアを用いた攻撃
- 最新の修正プログラムが適用されていないソフトウェアや Java の脆弱性をついた攻撃
- ランサムウェアを用いた攻撃

3.5.2. 金融機関の情報漏洩を狙った攻撃の手口

サイバー攻撃のうち金融機関の情報漏洩を狙った攻撃では、Web サーバなどを対象として、次のような手口を駆使して試みられることが多い。一般的には対象システムのソフトウェアの脆弱性を突いた攻撃（エクスプロイト攻撃: Exploit 攻撃）や攻撃相手が使用するコンピュータにその利用者の心理的なすきまを狙ってマルウェアを感染させ遠隔操作を可能にしてさらなる攻撃段階に繋げるなど、いくつかの組み合わせによる手口が多く用いられる。

- 標的型攻撃（APT 攻撃）
  - 特定の攻撃対象に特に狙い定めて執拗なサイバー攻撃を企てるもので、攻撃の過程でマルウェアなども用いる場合が多い。
- Social Engineering（ソーシャルエンジニアリング）
  - 取引先の関係者を成りすまして電話で個人情報を聞き出したり、パスワードのメモを盗み見るなど、技術的ではない人間の心理上の弱点（親近感、油断や勘違いなど）や行動のミスを狙って情報を盗み出す攻撃。
- Phishing（フィッシング）
  - 攻撃対象者を一般的に知られた Web サイトなどに見せかけた偽のサイトに誘導して、個人の認証情報や個人情報を窃取するなどの攻撃。
- SQL Injection（SQL インジェクション）
  - データベースの検索コマンド（SQL）処理の脆弱性を悪用して、データベース内の情報を窃取する攻撃。
- Cross-Site Scripting（クロスサイトスクリプティング）
  - Web ページの中に入力欄がある場合に、本来は文字列などが入力されることを想定している箇所に特定のスクリプトを書くことによって悪意のある動作を引き起こす攻撃。
- Trojan Horse（トロイの木馬）
  - 善良なソフトウェアに見せかけたマルウェアを含むアプリケーションなどを、セキュリティを掻い潜って攻撃対象に感染させてマルウェアを実行する攻撃。外部からの不正アクセスを誘導する事が多い。ターゲットが利用したくなるような有用なソフトウェアを装う場合が多い点が特徴。
- War Driving（ウォードライビング）
  - 無線接続可能な機器に感度の高いアンテナなどを接続して、セキュリティ対策の不十分な接続ポイントなどに接続を行う行為。

上記のほか、近年の動向として特に配慮すべき攻撃の手口として次のようなものがある。

- ゼロデイ攻撃
  - 従来から存在するアンチウィルスソフトウェアでは、既知のマルウェアの特徴情報と検出対象を比較してマルウェアを検出していたが、新しいマルウェアが初めて登場してから、セキュリティソフトウェアベンダーが検出のための特徴情報を更新するまでの間に1日から数日間程度の時間が必要であり、この間は新種のマルウェアを検出できない時間が存在した。この新種のマルウェアが登場してからそのマルウェアを検出することができるようになるまでのシステムが無防備な時間（ゼロデイ）を集中的に狙ったサイバー攻撃である。
- モバイルアプリケーションを対象とした攻撃
  - 従来の PC のみならず、近年モバイル機器が急速に普及したことにより、モバイル機器のアプリケーションを対象としたマルウェアによる攻撃が増えている。
- サービスプロバイダの脆弱性を狙った攻撃
  - クラウドサービスの普及浸透に伴って、金融機関自身によるインフラのみならずサービスプロバイダの脆弱性を狙った攻撃のリスクが高まっている。

3.5.3. 金融機関の機能停止を狙った攻撃の手口

サイバー攻撃のうち金融機関の機能を停止する攻撃は、多くの場合 DDoS 攻撃が用いられる。また、DDoS 攻撃以外にもインフラの機能の停止を引き起こす攻撃の手口はいくつか存在する。

- DDoS（Distributed Denial of Service）攻撃
  - ➢ 攻撃者が Web サーバなどの攻撃対象のシステムに対して同時に大量のリクエストを行い、攻撃対象のシステムに許容外の高負荷をかけることでサービス提供を不能にする攻撃として DoS（Denial of Service）攻撃がある。DDoS 攻撃は、DoS 攻撃元として予め大量のコンピュータにマルウェアを感染させて遠隔操作可能とした一群を用いて、同時多発的に行うことで、非常に効果の高い攻撃を行う手口である。

  - ➢ 一般的な DDoS 攻撃の手順は次の通りである。

    1） インターネットに接続された複数の防御の弱いコンピュータにマルウェアを感染させてボットにする。
    2） マルウェアに感染してボットにされたコンピュータは、処理能力とネットワーク帯域によってランク付けされる。ボットにされた多数のコンピュータはボットネットを構成する。
    3） 追跡不可能 IRC チャネル[17]を使用するか、または他の遠隔で操作できるリモートサーバを C&C サーバ[18]として利用する。
    4） 攻撃対象を特定し、遠隔で IRC チャンネルまたは C&C サーバーを通して DDoS 攻撃を行う指示をボットネットに送る。具体的には休眠状態であったボットネットに対して攻撃対象の URL とプロトコルの詳細を指定し攻撃開始の指示を送る。

---

17 IRC（Internet Relay Chat）は、本来インターネットを使用してチャットを行うしくみであるが、DDoS 攻撃ではボットとなった PC と、このチャットの通信のしくみを使用して、途中経路のファイアウォールなどのセキュリティ保護手段をすり抜けて通信を行うものが多い。IRC チャネルは遠隔で指令を出すための通信経路を指す。
18「11.用語の説明」を参照。

5） 数百万単位など大量の接続リクエストが攻撃対象サーバに対して同時に行われ、サーバはリソースを消費し、正当な利用者がサイトへのアクセスが出来ない状態となる。
6） 攻撃は通常繰り返し処理となり、何らかの外的要因で検出または停止されるまで続く。

➢ このような攻撃の対象とされたサーバでは、ネットワーク帯域とサーバの CPU 処理能力が飽和してしまうため、利用者がサイトにアクセス出来なくなったり、サーバのクラッシュを引き起こしたりする。

➢ DDoS 攻撃による障害は通常数時間、場合によっては数日間に渡って続く。これによる直接的な事業上の機会損失および評判の低下による事業への影響は非常に大きい。

● 修正パッチ配信システムのハッキング

➢ ソフトウェアの修正プログラムの配信システムの脆弱性を悪用した攻撃が 2013 年に韓国で発生している。本来はソフトウェアの修正プログラムを配信するための仕組みに不正に侵入し、システムのデータを破壊するマルウェアを仕込んで一斉に配信することで、大規模なインフラの機能停止を引き起こした攻撃が発生した事例がある（6.5 参照）。

● ランサムウェアによるシステム機能停止

➢ 攻撃対象のシステムに保存されている情報に対して、本来の利用者権限を一時的に無効にしたり、情報自体を暗号化して一時的に読み書きできなくするなどの機能を持ったマルウェアを感染させ、正常なインフラ機能の停止を引き起こしたり、脅迫により金銭を窃取したりする攻撃。

3.5.4. 金融機関の利用者に対する攻撃の手口

金融機関の利用者に対する攻撃の手口は、攻撃対象が金融機関自身のコンピュータではなく、一般顧客のコンピュータであるという点を除いて多くの部分で共通しており、特に 3.5.2 や 3.5.3 に挙げた手口のうち、下記のものを駆使して試みられることが多い。

● 標的型攻撃（APT 攻撃）
● Phishing（フィッシング）
● Social Engineering（ソーシャルエンジニアリング）
● ゼロデイ攻撃
● Trojan Horse（トロイの木馬）
● モバイルアプリケーションを対象とした攻撃
● ATS（Automatic Transfer System、自動送金システム）攻撃
● War Driving（ウォードライビング）
● ランサムウェアによるシステム機能停止や妨害

それ以外にも、利用者に対する攻撃の手口として、下記のものがある。

- マン・イン・ザ・ブラウザ（Man-in-the-Browser: MITB）攻撃
  - マルウェアの感染により Web ブラウザとサーバとの接続を監視して通信内容を改竄したり操作を乗っ取ったりする攻撃手法やそうした機能を有するマルウェアによる攻撃。利用者からみると正規のサービスの画面のように見えるため感染に気付きにくく、また金融機関側も正規の利用者が正常な処理を行っているようにみえるため対策が取りにくい。

3.6. サイバー攻撃への対抗措置

現在、サイバー攻撃に対する技術的な対抗措置としては、一般的に下記の様な施策が用いられている。（用語については「11.用語の説明」参照）

- 二要素による強力な認証
- ダイナミック CAPTCHA
- ソフトウェアキーボード
- アウトオブバンド認証
- エンドユーザ･コンピューティング[19]･ツール
- アンチウィルスソフトウェア
- フィッシング防止のための DNS の DMARC 制御
- クリックストリーム分析

また、特に下記のような技術が、サイバー犯罪の防止に積極的に活用され、役立っている例がある。

- リスクベース認証および強力な認証
  - Web サービスへの接続経路が異なる、使用している PC がいつもと異なるなど、利用者の使用場面を想定して、リスクと考えらえる環境の変化などを検出して認証に活用する。

- 不正検出およびリスク低減ツール
  - 人間の挙動に着目して、Web 操作の手順や振る舞いをもとにした不正操作の検出を行うツール。

3.7. 情報共有の意義

サイバー攻撃に関して自組織が把握している攻撃の手口、脅威や脆弱性等の情報を金融機関相互に共有する事で、攻撃に対する対応力を高め、被害を最小化し、インシデント発生時の復旧までの時間を短縮することが可能になる。

19 企業などで情報システムを利用して現場で業務を行う従業員が自らシステムやソフトウェアの開発・構築や運用・管理に携わること。

3.7.1. 情報共有の意義

金融機関において、サイバー攻撃による被害を最小化出来た例を網羅的に特定するのは困難であるが、過去に発生した大きな脆弱性に起因する脅威、例えば、「Shellshock[20]」、「POOLE[21]」、「 Heartbleed[22]」などが露呈した際に、迅速に情報共有を行うことによって、組織内でのリスク評価やシステム回復までの時間が大幅に短縮出来たという事はいくつかの事例として確認されている。

- 例えば英国では、POOLE や Heartbleed が問題となった際に、金融行為規制機構（Financial Conduct Authority: FCA）がこれらの脆弱性によるリスクとリスクの回避策について金融機関に問合せを行い、インシデントの未然防止に貢献した。
- また、このような脆弱性やサイバー脅威に関する情報が広く一般公開され認知度が高まったことにより、サイバー脅威に対する予防や軽減がより効果的になったと言える。

3.7.2. 共有されている情報の内容

サイバー攻撃に関する情報の共有において、金融機関でも近年注目されている技術領域として「セキュリティインテリジェンス（Security Intelligence）」があり、これは広範囲に取得されたサイバーリスク発生までの情報を多面的に分析してインシデントの発生予見や未然の防止に役立てるもので、サイバーセキュリティ対策の戦略的な課題の一つである。この領域に関連した情報の共有が米国や英国では積極的に行われており、関連機関が多数存在している。このような機関では一般的に次のような情報の共有を行っている（但し、共有される情報はこれに限定されない）。

- IP アドレス
- 脅威のタイプと発生元
- マルウェアの詳細
- 攻撃テクニック
- フィッシング攻撃に関する手口

また、企業ごとの要望に合わせてセキュリティインテリジェンスとサイバー犯罪情報を最適化して提供する民間のサービスも存在する。英国等の金融機関では、このような最適化されたサービスが広く利用されている。

3.7.3. 国家を跨いだ情報共有の枠組み

サイバーセキュリティに関する情報共有関しては、国家を跨いだ技術情報や犯罪情報の共有も広く行われている。

---

20 コンピュータに対する指示を解釈するソフトウェアであるコマンドラインインタプリタ（一般的に Shell と呼ばれる）の「Bash (Bourne Again SHell)」に含まれていたバグが原因とする脆弱性、およびこれを悪用した攻撃を指す。
21 暗号化の通信に使用されるソフトウェア SSL 3.0 に内在するソフトウェアの脆弱性、およびこれを悪用した攻撃を指す。
22 暗号化の通信に使用されるソフトウェア OpenSSL に内在するソフトウェアの脆弱性、およびこれを悪用した攻撃を指す。

a) セキュリティ脅威情報など技術情報の共有

- FIRST（Forum of Incident Response and Security Teams）
  - 国を跨いだ CSIRT 組織の連携を図るための組織で、1990 年（平成 2 年）に設立されて以来、25 年に及ぶ活動を続けている。現在 70 の国と地域の CSIRT がメンバーとして登録され、324 団体が参加している。
- FS-ISAC（Financial Services Information Sharing and Analysis Center）
  - 米国を中心とした金融分野でのサイバーセキュリティ情報の共有のための機関。詳細は 4.3.4 参照。

b) 犯罪情報の共有

金融犯罪の実態、脅威の分析、先進的な取組みなどについての情報共有や、組織的犯罪対策についての協議など、国外の規制当局との連携の仕組みとしては、下記のようなものがある。

- 国際刑事警察機構（International Criminal Police Organization: ICPO, INTERPOL）
  - 世界各国の警察機関により組織された国際組織で、2014 年（平成 26 年）時点での加盟国は 190 ヶ国。
- 欧州刑事警察機構（European Police Office: EUROPOL）
  - 欧州連合（EU）の警察専門機関。加盟国間での犯罪に関する情報交換の促進や、情報の収集、加盟国内での捜査の支援などを行う。

■ 4. 米国の金融分野のサイバーセキュリティ対策

4.1. 概要

本章では、米国における金融分野でのサイバーセキュリティ対策への取組みとして、政府よりどのような方針が示されているか、どのような法制度が制定されているか、法制度に基づいてどのような監督機関が規制当局として設置されているか、また、規制当局から金融機関に対してどのような順守要件が示されているか等について示す。さらに、規制当局から求められる要件への適合のみならず、金融機関自身もしくは業界全体としての自主的な取組みとして、どのようなことが実施されているかなどについても示す。

4.2. 監督機関によるサイバーセキュリティ対策への取組み

ここでは、米国の金融機関におけるサイバーセキュリティ強化を目指した政府および監督機関の取組みを説明する。

4.2.1. 法制度や国家戦略

a) 国家戦略

米国においてサイバーセキュリティは、国家が直面する最も深刻な経済的かつ国家安全保障上の課題の一つとされている。「国家安全保障戦略（National Security Strategy, 2010）[23]」において、サイバーセキュリティに関する脅威は国家安全保障および経済発展において重要な課題と位置付けられている。（なお、この戦略はその後改正され現在は「国家安全保障戦略（National Security Strategy, 2015）[24]」となっている。）

国家戦略としては、現在までに、個別の分野ごとに次のようなものが策定されている。

- 「サイバー空間の国際戦略（International Strategy for Cyberspace, 2011）[25]」
  - 2011 年（平成 23 年）5 月、米国政府は、サイバー空間を国際貿易等の場として発展させていくための戦略を発表した。
  - 具体的には、①開放的な、②相互運用可能で、③安全な、④信頼性の高いサイバー空間を将来にわたり維持発展させることを目的として、「包括的な国際連携に向けた方針」を示した。

23 https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
24 https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf
25 https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- 方針では、①基本的自由、②プライバシー、③情報の自由な流通の 3 つを中核的な原則とし、経済やネットワークの保護、インターネットの自由等の領域を優先すべき政策課題として取組むこととした。
- 文書の性格としては、サイバー空間でのセキュリティに関するビジョンや目指す未来の指針が多くを占めている。

●「サイバー空間作戦戦略（Department of Defense Strategy for Operating in Cyberspace）[26]」

- 国防総省（Department of Defense: DOD）が 2011 年（平成 23 年）7 月に軍事的な観点から示した戦略で、インターネットビジネス分野におけるイノベーションを阻害せずに、多大な経済的、社会的価値を守ることを目的としている。これまでの「陸、海、空、宇宙」加えて、「サイバー空間」が第 5 の戦場として追加される等、サイバー戦争に関してはじめて明記された。

b）サイバーセキュリティに関連する法令

米国のサイバーセキュリティに関連する法令としては、2014 年（平成 26 年）12 月 18 日にサイバーセキュリティを監視する連邦政府機関の機構や任務遂行手順に焦点を当てた以下の法案が成立している。

●「国家サイバーセキュリティ保護法 2014（National Cybersecurity Protection Act of 2014）[27]」

- 国土安全保障省（Department of Homeland Security: DHS）に属するサイバーセキュリティ情報運用センターとして「国家サイバーセキュリティ通信統合センター（National Cybersecurity and Communications Integration Center: NCCIC）」を体系的に規定し、同センター（NCCIC）がサイバー脅威に関する情報及び分析を民間部門と共有し、企業や政府機関に対してインシデントの対処手段や技術的支援を提供し、安全対策を勧告するなどの活動が法的に根拠づけられた。（4.3.4 参照）

●「連邦情報セキュリティ近代化法 2014（Federal Information Security Modernization Act of 2014）[28]」

- 「連邦情報セキュリティマネジメント法（FISMA） 2002」を改正し、連邦政府機関の情報セキュリティに関する政策や業務の遂行を管理する権限を国土安全保障省（DHS）に集約するとした。

「連邦情報セキュリティ近代化法 2014（FISMA 2014）」の成立以前までは、2002 年（平成 14 年）12 月に「電子政府法（e-Government Act of 2002）[29]」の一環として成立した「連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002: FISMA 2002）[30]」が主なサイバーセキュリティに関連する法令であった。

行政サービスの電子化と効率化について定めた「電子政府法」は、2001 年（平成 13 年）5 月に連邦議会上院に提出された。その後、同年 9 月の米国同時多発テロ発生により国家安全保障への意識が高まる中で、

26 http://www.defense.gov/news/d20110714cyber.pdf
27 https://www.congress.gov/bill/113th-congress/senate-bill/2519/text
28 https://www.congress.gov/bill/113th-congress/senate-bill/2521/text
29http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
30http://www.dhs.gov/federal-information-security-management-act-fisma

2003 年（平成 15 年）4 月に施行されるまでの間に、特に「情報セキュリティ」に関する法令化が格段に強化され、「連邦情報セキュリティマネジメント法（FISMA）」として制定された経緯がある[31]。

- 連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002: FISMA 2002）
  - 米国の連邦政府機関において、情報セキュリティの強化を行うための取組みを開発、文書化、実践する事を義務付けている。
  - この取組みの一環として、米国商務省国立標準技術研究所（NIST）が具体的なマネジメントシステムの規格やガイドラインを策定することを義務付けている。
  - 規制の対象となるのは、米国の連邦政府機関や連邦政府から業務委託を受けている民間の外部委託先で、一般的な金融機関は対象とならない。

また、オバマ大統領は 2008 年（平成 20 年）の第一期選挙戦の当時からサイバーセキュリティを最優先課題の一つとして位置付けて、サイバーセキュリティへの取組みを積極的に推し進めてきた。ブッシュ政権下で「連邦情報セキュリティマネジメント法 2002（FISMA 2002）」が 2002 年（平成 14 年）12 月に制定されて以降、オバマ政権に移り「連邦情報セキュリティ近代化法 2014（FISMA 2014）」が成立するまでの間に、様々な事情から成立はしなかったものの、いくつかの重要なサイバーセキュリティ法案が審議されてきた。成立しなかった法案として、次のようなものがある。

- 「サイバーセキュリティ法案（CyberSecuirty Act of 2012: CSA2012）[32]」
  - ライフラインや重要インフラに対するサイバーセキュリティの強化を狙ったものであるが、米国商工会議所や産業界の後押しを受けた上院共和党の反対に遭い、廃案となった。
  - 本法案は、上院民主院内総務のハリー・リード（Harry Reid）氏が超党派で包括的な法案を策定しようと試みたものだったが、上院共和党のジョン・マケイン（John McCain）氏は、最低限の基準であっても企業に必要以上の負荷を強いることになるとしてこれに反対し、最終的には、基準を義務ではなく企業の任意とするように変更させた[33]。しかし、この妥協案にもかかわらず、上院の投票では共和党員の議事妨害にあったことで、この法案は採択されなかった[34]。

- 「サイバーインテリジェンスの共有と保護に関する法案（Cyber Intelligence Sharing and Protection Act: CISPA, 2012）[35]」
  - 本法案は 2012 年（平成 24 年）4 月に下院で可決されたが、プライバシー保護を訴える人権団体や多くの Web サービス事業者による大反対キャンペーンが繰り広げられたことで、会期中に成立せず廃案となった。

---

31 http://www.ndl.go.jp/jp/diet/publication/legis/217/21701.pdf
32 https://www.congress.gov/bill/112th-congress/senate-bill/2105
33 http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html?_r=1
34 http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html?_r=0
35 https://www.congress.gov/bill/113th-congress/house-bill/624

- この法案の骨子は、「インテリジェンス・コミュニティと民間部門との脅威情報の共有」であり、民間企業がサイバーテロやセキュリティ脅威に関する情報を発見した場合に、その情報を他の企業および政府と共有できるようにするための法案であった。例えば Web サービス会社（A 社）がショートメッセージサービス会社（B 社）のサービスを脅かす可能性のあるセキュリティ脅威情報を検出した場合、A 社は発信者の ID などの個人情報を、既存の個人情報保護法令等を考慮せずに、B 社および米国政府に対して通知する事が出来るようにすることであった。
  CISPA が成立した場合は、Web サービスなどの民間企業が利用者の通信ログなどプライバシーに関わる情報を政府や情報機関に対して簡単に開示できてしまうことになり、更に、この開示に関する条件が曖昧だったため、プライバシー保護団体や人権擁護団体が猛烈に反対した[36]。その結果、本法案は採択に至らなかった[37]。

こうした背景もあり、米国におけるサイバーセキュリティの法令化では通常の立法を経ずに、大統領令（Executive Order）もいくつか発行されている。

これは、様々な事情により法令化が阻まれた状況の中で、サイバーセキュリティを戦略的課題として重要視しているオバマ政権が、通常の立法の制度を経ずに行政権を行使できる「大統領令」によって、サイバーセキュリティへの取組みの大幅な強化を行ったものとみられる。

米国における大統領令（Executive Order）は、アメリカ合衆国大統領が連邦議会の承認や立法手続きを経ずに、直接連邦政府に対して特権的な行政権を行使出来る命令であり、実質的に法律と同等の効力をもつ。

c）大統領令によるサイバーセキュリティに係る取組みの強化

近年発令された大統領令および大統領令を補完する大統領政策指令には次のようなものがある。

- 大統領令 13636「重要インフラのサイバーセキュリティ強化に関する大統領令（Improving Critical Infrastructure Cybersecurity: Feb 12, 2013）」
- 大統領政策指令 21「重要インフラセキュリティと強靭化に関する大統領政策指令（Critical Infrastructure Security and Resilience: Feb 12, 2013 ）」
  - 2013 年（平成 25 年）2 月に発令された大統領令および大統領政策指令で、重要インフラとして金融をはじめ、通信、エネルギー、運輸、政府施設、原子力等の 16 分野の施設を指定して、各情報インフラを所有する企業や管理者の間での情報の共有の強化、サイバーリスク対応のための標準の開発、その実践のためのパートナーシップの推進、プライバシーの保護などを求めている。
  - 具体的には、下記のような骨子で構成される。

36 http://japan.cnet.com/news/business/35016617/
37 http://www.cnet.com/news/white-house-takes-aim-at-cispa-with-formal-veto-threat/

1) 脅威及び攻撃情報の米国企業への提供
   - 連邦機関はサイバー脅威に関して、米国企業に秘密指定以外の情報を適時提供し、情報共有を図る。
2) サイバーセキュリティフレームワーク(枠組み)の開発
   - 国立標準技術研究所(NIST)が中心となり産業界と協力して既存の国際標準等に依拠しながら、重要インフラのサイバーリスク軽減のためのフレームワークを開発する。
3) プライバシーと市民的自由の確実な保護
   - 連邦機関は、本大統領令実施にあたり、プライバシーと市民的な自由のための保護措置を講じる。
4) サイバーセキュリティフレームワーム(枠組み)の導入の促進
   - 国土安全保障省(DHS)は分野毎の連邦機関と協力し、民間企業によるサイバーセキュリティフレームワークの実践を支援するプログラムの作成、導入の動機付けを明確化する。
5) 現行のサイバーセキュリティ規程の見直し
   - 監督機関はサイバーセキュリティフレームワークに基づきサイバーセキュリティに関する規定を評価し、必要に応じて企業と協力して見直しを行う。
6) 関係法律との一貫性の維持
   - この大統領令は関係法令と一貫性を保ちながら、予算の範囲で実施される。

この大統領令 13636 及び大統領政策指令 21 への対応として、2014 年(平成 26 年)2 月に米国商務省国立標準技術研究所(NIST)が、「重要インフラのサイバーセキュリティを強化するフレームワーク(Framework for Improving Critical Infrastructure Cybersecurity, ver 1.0)[38]」を発表した。同フレームワークは、重要インフラを有する企業や組織に対して、サイバーセキュリティのリスク管理のための指針を提供するものであるが企業における採用は任意で、政府関係者もこれが新たな規制を課すものではないとしている。

- 大統領令(未採番)「政府と民間企業間でサイバー脅威に関する情報の共有を促進するための大統領令(Promoting Private Sector Cybersecurity Information Sharing , Feb 13, 2015)[39]」
  - これは、重要インフラ事業者と政府の間で、サイバーセキュリティに関する脅威情報の共有を進め、共同でリスク対応標準を開発し、実践するためのパートナーシップであり、政府と民間が連携してサイバーセキュリティを強化する事が目的である。民間企業が所有する重要インフラのサイバーセキュリティ強化および政府と民間の相互の情報共有の推進に注目している点が特徴である。

  - 本大統領令の発表に際して 2015 年(平成 27 年)2 月 13 日に米国カリフォルニア州のスタンフォード大学で開催された「サイバーセキュリティと消費者保護に関するホワイトハウス・サミット(White House Summit on Cybersecurity and Consumer Protection)[40]」において、国家安全保障理事会のリサ・モナコ(Lisa Monaco)氏は、本大統領令の発令の背景として次の様に述べた。

38 http://www.nist.gov/cyberframework/
39 http://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform
40 http://news.stanford.edu/news/2015/february/cyber-summit-video-archive-021415.html

背景

- 政府で把握しているサイバーセキュリティに関するインシデントの数は、2009 年（平成 21 年）以来、約 5 倍に膨れ上がっている。
- 急増している攻撃により深刻度は増しており、これらはまた、経済的な損害を益々引き起こしている。
- サイバー空間の脅威は、より多様になり、より高度に、そしてより危険に変わってきている。
- 絶え間なく進化し高度化するサイバー攻撃者と戦うためには、持続的で組織的な取り組みが必要である。
- テロに対する対策と同様に、サイバーセキュリティ対策は、外交力、経済力、諜報力、法的執行力、高い技術力、そして、必要に応じて軍事力など我が国の持てる力の全てを結集して政府全体として取組んでいく必要がある。

本大統領令の概要は次の通りである。

➢ 民間部門における連携の促進
- この大統領令は、民間企業同士および民間企業と政府との間のサイバーセキュリティに関する情報共有と連携の拠点として新しい組織である情報共有分析機関（Information Sharing and Analysis Organizations: ISAO）[41]の設置を強く推奨している。
- 従来から存在する情報共有分析センター（Information Sharing and Analysis Center: ISAC）と情報共有分析機関（ ISAO）との違いは、情報共有分析センター（ISAC）が金融、エネルギー、IT などといった業界ごとの固有のサイバーセキュリティ情報を共有するしくみであったのに対して、情報共有分析機関（ISAO）は、業種、地域、企業規模などの枠に捉われず相互の横断的な情報共有を効果的に行うためのしくみであるという点である。これにより、政府や民間企業からより広範囲な情報が集まり、サイバーセキュリティに対するより精度の高いインテリジェンス（多面的な情報解析）が可能になると考えられている。

➢ より効果的な官民の情報共有の促進
- 大統領令では、非政府系の標準化団体が推進するサイバーセキュリティ関連の技術標準も考慮して標準化を進めることを情報共有分析機関（ISAO）に求めている。また、情報共有分析機関（ISAO）はより円滑な情報共有を実現するための自動化の仕組みの開発の役割も担うことになる。
- 国家サイバーセキュリティ通信統合センター（NCCIC）は、情報共有分析機関（ISAO）との間でサイバー脅威に関する情報共有やセキュリティシステムの強化等に関する継続的かつ包括的な調整を行うことが期待される。

➢ 堅固なプライバシーおよび自由な市民活動の保護
- 情報共有分析機関（ISAO）が遵守すべき共通自主基準には、データ最小化原則等、情報共有分析機関（ISAO）の運営やメンバーシップに関するプライバシー保護策が含まれる。
- 国家レベルで収集されている機密度の高いサイバー攻撃に関する脅威情報を、民間企業が自社のサイバーセキュリティのために入手するには、管理が必要となる。このための承認を行う機関として、国土安全保障省（DHS）に権限を与えることを決定した。

41 https://www.dhs.gov/isao

- 大統領覚書（未採番）「サイバー脅威インテリジェンス統合センター（Cyber Threat Intelligence Integration Center, Feb 25, 2015）[42]」
  - 2015 年（平成 27 年）2 月 25 日に出された大統領覚書では、政府および民間企業の組織間の横断的なサイバーセキュリティ情報の共有を促進するために、国土安全保障省（DHS）の下部組織として「サイバー脅威インテリジェンス統合センター（Cyber Threat Intelligence Integration Center: CTIIC）」の新設が発表された。（4.3.4 参照）
  - サイバー脅威インテリジェンス統合センター（CTIIC）は国家安全上の米国外のサイバー脅威に関する連携の為の国家インテリジェンスセンターとしての機能をもつことになる。

4.2.2. 金融に関わるサイバーセキュリティの関連組織

米国の金融機関に対するサイバーセキュリティの取組みには、以下の二段階のアプローチがある。

第一段階は、国家レベルでのサイバー空間のセキュリティの確保やインテリジェンス（多面的な情報解析）に関連する組織で、主なものは下記の通りである。

- 国土安全保障省（Department of Homeland Security: DHS）
  - 連邦政府のネットワークや重要インフラのサイバーセキュリティに対する責任を持つ政府機関
  - ➢ 国家サイバーセキュリティ部（National Cyber Security Division: NCS）
    - 国土安全保障省（DHS）内の部門で、サイバーセキュリティの戦略目標の設定や総合調整を行う。
  - ➢ 国家サイバーセキュリティ通信統合センター（The National Cybersecurity and Communications Integration Center: NCCIC）
    - 国土安全保障省（DHS）内の部門で、国内のサイバーセキュリティに関する情報を集約するための組織として 2009 年 10 月に設立された。
    - US-CERT（United States Computer Emergency Readiness Team）
      - 国家サイバーセキュリティ通信統合センター（NCCIC）の下部組織として、米国内のネットワークを対象とした攻撃に関する最新のネットワークおよびデジタルメディア解析を行う機関であり、米国における国家的な CSIRT 機関である。米国では代表的な CSIRT 機関として CERT/CC（4.3.4.a）が存在するが、US-CERT は CERT/CC が行っているコンピュータシステムの脆弱性分析などの機能を活用する形で組織の連携を図っている。US-CERT では連邦省庁、州、地方政府、民間組織および国際的に連携する国々へ配信する最新のサイバー攻撃に関する情報を調査し提供している。さらに、連邦省庁に侵入検知および侵入防止の機能を提供する国家サイバーセキュリティ保護システムの運用を行っている。また、US-CERT は国際的なサイバー演習（直近では Cyber Storm III）の主宰なども行うほか、各国の CSIRT との情報連携を行っている。

42 https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center

- 国防総省（Department of Defense: DOD）
  - 米国の国防、軍事を統合する機関
  - ➢ 国家安全保障局（National Security Agency: NSA）
    - 国防総省内の組織で国外情報の分析を行う機関
- 中央情報局（Central Intelligence Agency: CIA）
  - 国外での諜報活動を行う情報機関

第二段階は、金融機関に特化した金融政策を決定する機関であり、次のものがある。各々は、監督する対象の機関の種類によって分かれている。

- 連邦準備制度理事会（Board of Government of the Federal Reserve System: FRB）
  - 米国の中央銀行である連邦準備制度（FRS）の最高機関で、市中銀行の検査監督を行う。
  - ➢ 消費者金融保護局（Consumer Financial Protection Bureau: CFPB）
    - 消費者が金融機関に騙されたり不公正な契約をさせられたりすることを防止することを目的として消費者金融商品およびサービスの提供に関する規制監督を行う。
- 連邦預金保険公社（Federal Deposit Insurance Corporation: FDIC）
  - 連邦政府の独立機関で、預金保険加入機関の検査監督を行う。
- 通貨監督庁（Office of the Comptroller of the Currency: OCC）
  - 財務省（Department of the Treasury: DOT）の内部機関で、国法銀行と連邦貯蓄金融機関の検査監督を行う。
- 信用組合監督庁（National Credit Union Association: NCUA）
  - 連邦政府の独立機関で、信用組合の検査監督を行う。
- 証券取引委員会（Securities Exchange Commission: SEC）
  - 連邦政府の独立機関で、証券会社、投資顧問会社、自主規制機関等の検査監督を行う。
  - ◆ コンプライアンス検査局（the Office of Compliance Inspections and Examinations: OCIE）
    - コンプライアンスに関する検査の実施部門。

また、サイバーセキュリティに関する具体的な方針、標準、要件等を策定する機関として下記がある。

- 国立標準技術研究所（National Institute of Standards and Technology: NIST）
  - ◆ 商務省（Department of Commerce: DOC）傘下の主要機関で、情報セキュリティに関する様々な規格、標準、ガイドラインを策定している。
- 連邦金融機関検査協議会（Federal Financial Institutions Examination Council: FFIEC）
  - ◆ 米国政府の主要機関で、連邦準備制度理事会（FRB）、連邦預金保険公社（FDIC）、信用組合監督庁（NCUA）、通貨監督庁（OCC）、消費者金融保護局（CFPB）の理事会により組織された金融機関の政府調査のための基本方針、標準、報告形式を規定する機関である。
  - ◆ 金融監督行政には連邦と州とで重複している点が多い現状を踏まえ、上記の各監督機関が金融機関に対する統一した一貫性のある検査・監督指針を規定し各監督機関の方針の整合性を図っている。

なお、生命保険会社や損害保険会社などの保険会社は各州法によって規制されている。

その他に、金融に関する関係組織としては、下記のような部門がある。

- 金融業規制機構（Financial Industry Regulatory Authority: FINRA）
  - 米国最大の自主規制機関で投資家保護と米国市場における公平性維持を主要な役割とし、2007 年 7 月に全米証券業協会（NASD）とニューヨーク証券取引所（NYSE）の規制機関の一部を統合して設立された。
  - 現在 5,000 近くの証券会社およびその支店約 172,000 店と約 665,000 人の NASD 資格保有者を監督する。
- 金融サービス分野調整協議会（Financial Services Sector Coordinating Council: FSSCC）
  - 金融業界の重要インフラの保護を目的として 2002 年に設立された業界団体の機関で、FS-ISAC も金融サービス分野調整協議会（FSSCC）の加盟機関の一つになっている。
  - FS-ISAC と同様に財務省（DOT）と連携しながら、米国金融セクターの安全保障強化に取り組んでいる。

4.2.3. 検査監督のガイドライン

a）金融機関向けの検査監督のガイドライン

金融機関向けのサイバーセキュリティに関連する検査監督のガイドラインとしては、次のようなものがある。

- 連邦金融機関検査協議会（FFIEC）

  サイバーセキュリティに関する主なガイドラインとして、次のようなものがある。

  - 「FFIEC IT 検査ハンドブック（Information Technology （IT） Examination Handbook）[43]」
    - 監督機関が金融機関に対して情報システムおよびその管理体制に関する監督指針、検査のガイドラインとして示している文書である。監査、事業継続計画、情報セキュリティ、管理、運営などの広範囲にわたる検査のガイドラインが具体的な要件と共に記載されている。
    - このガイドラインは、連邦準備制度理事会（FRB）、連邦預金保険公社（FDIC）、信用組合監督庁（NCUA）、通貨監督庁（OCC）、消費者金融保護局（CFPB）の検査官が金融機関の情報システムを検査する際の手引きとなる。
  - IT 検査ハンドブックの構成
    - 監査（Audit）
    - 事業継続計画（Business Cotinuity Planning）
    - 開発と調達（Development and Acquisition）
    - 電子バンキング（e-Banking）
    - 情報セキュリティ（Information Security）
    - 管理（Management）

43 http://ithandbook.ffiec.gov/it-booklets/

- 運用（Operations）
- 外部調達技術サービス（Outsourcing Technology Services）
- リテール支払システム（Retail Payment Systems）
- 技術サービス提供者の監督（Supervision of Technology Service Providers）
- ホールセール支払システム（Wholesale Payment Systems）

その他に、以下は連邦金融機関検査協議会（FFIEC）が公表している主な個別の要件に関する文書である。

- 「インターネットバンキング環境における認証（Authentication in an Internet Banking Environment）[44]」
  - IT 検査ハンドブックに対する補足ガイドラインとして、インターネットバンキング環境における認証の具体的な要件について定義している文書である。
- 「事業継続計画ブックレット 付録:アウトソース技術サービスの回復力を強化（Business Continuity Planning Booklet Appendix: Strengthening the Resilience of Outsourced Technology Services）[45]」
  - 事業継続性の観点からサイバーセキュリティにおける情報システムの回復力について定義している文書である。

一般的に、連邦準備制度理事会（FRB）、連邦預金保険公社（FDIC）、信用組合監督庁（NCUA）、通貨監督庁（OCC）、消費者金融保護局（CFPB）の 5 つの組織の内の一つが、対象の金融機関の評価者として、年次で検査を行い、想定されるリスクに応じた異なった切り口の検査が実施される。

b）ガイドラインでの具体的なサイバーセキュリティ対策要件

「FFIEC IT 検査ハンドブック」で求められている具体的なセキュリティ対策要件は次の通りである。

- セキュリティプロセス
  - ガバナンス
- セキュリティリスク評価
  - リスク評価手順
- 情報セキュリティ戦略
  - アーキテクチャの検討
- セキュリティ制御の実装
  - アクセス制御
  - 物理的および環境的保護
  - 暗号化
  - マルウェア検知と分析

44 http://www.ffiec.gov/pdf/authentication_guidance.pdf
45 http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

- ◆ システム開発/調達/維持
- ◆ 人材セキュリティ
- ◆ データセキュリティ
- ◆ サービス提供者の管理
- ◆ 事業継続の検討
- ◆ 保険

➢ セキュリティ監視

- ◆ アーキテクチャの課題
- ◆ 活動監視
- ◆ 条件監視
- ◆ インシデント分析と対応
- ◆ 外注システム

➢ セキュリティプロセスの監視と更新

- ◆ 監視
- ◆ 更新

c) 金融サービスを含むすべての事業向けの管理体制のガイドライン

● 国立標準技術研究所(NIST)

➢「重要インフラのサイバーセキュリティ改善のためのフレームワーク(NIST Framework for Improving Critical Infrastructure Cybersecurity, 2014)[46]」

- ◆ 2013 年(平成 25 年)2 月 12 日の大統領令 13636「Improving Critical Infrastructure Cybersecurity」を契機に策定された技術標準で、重要インフラサービスの提供に関わるプロセス、情報、システムに対するサイバーセキュリティリスクの管理にあたってのガイダンスである。
- ◆ 優先順位付けができて柔軟性があり、繰り返し適用することで費用対効果の高いアプローチを実現するための自主参加型のフレームワークであることが特徴である。

➢「Special Publications 800-xxx シリーズ(例 800-61, 800-86 など、4.4.1 参照)[47]」

- ◆ 米国政府がセキュリティ対策を実施する際に利用することを前提として作成された技術標準で、米国政府機関はもとより、民間企業でも広く活用されている。セキュリティ管理、リスク管理、セキュリティ技術、セキュリティの対策状況の評価指標、セキュリティ教育、インシデント対応など、セキュリティに関して広く網羅されている。

● 国際標準化機構(International Organization for Standardization: ISO)

➢ ISO 27000 シリーズ- 情報セキュリティマネージメントシステム(ISO 27000 Series – Information Security Management System)

- ◆ 国際標準である ISO で規定されている情報セキュリティ管理システムの規格で多くの組織で情報セキュリティの管理体制のフレームワークとして活用されている。国際標準であるため、各国の事情に柔軟に適用できるような構成となっているのが特徴である。

46 http://www.nist.gov/cyberframework/
47 http://csrc.nist.gov/publications/PubsSPs.html

- ISF（Information Security Forum）
  - Standard of Good Practice for Information Security
    - セキュリティ標準の開発、脅威の予測、リスク分析ツールなどの開発を行っており、世界の情報セキュリティ分野に大きな影響力を持つ ISF が公表している技術文書で、世界的にも最も包括的な情報セキュリティ標準として情報システムに関する事業リスクを許容範囲内に収めるための施策やベストプラクティスが収められている。
- SANS Institute（SANS）
  - 20 Critical Security Controls [48]
    - サイバーセキュリティの専門家に対する教育機関として世界的に権威ある団体 SANS Institute が公開している技術情報で、現在までに認識されている攻撃と、近い将来に発生が懸念される攻撃を阻む上で、有効であると考えられる 20 の技術的なセキュリティ防御策（コントロール）が記載されている。
    - それぞれの防御策には、組織が防御の手段を改善するためにとり得る措置を定めた複数の個別実施項目が含まれ、また、組織が各実施項目を評価するテスト基準に関する記述も付随している。

4.2.4. 金融機関向けの検査監督のガイドラインに関する最近の動向

最近の金融機関向けのガイドラインに関する動向としては次のようなものがある。

- 連邦金融機関検査協議会（FFIEC）
  - 2013 年（平成 25 年）6 月、連邦金融機関検査協議会（FFIEC）は、サイバーセキュリティと重要インフラのための「サイバーセキュリティ・重要インフラ・ワーキンググループ（Cybersecurity and Critical Infrastructure Working Group: CCWIG）[49]」を設立し、近年重要となっているこれらの問題について諜報機関、法執行機関、国土安全保障省（DHS）、および金融機関の関係団体と連携を図っている。

  - サイバーセキュリティ・重要インフラ・ワーキンググループ（CCWIG）は、連邦および州銀行の規制当局が地方金融機関のサイバー脅威の耐性を評価するための制度（サイバーセキュリティ評価）を設立した。この制度を用いて、連邦および州銀行の規制当局は地方金融機関のサイバーセキュリティ対策状況を評価し、地方金融機関のサイバーリスク低減のための改善事項を指摘することとしている[50]。当制度は、サイバーセキュリティの知見が不足しがちな地方金融機関に対して評価結果を提供する事によって、地方金融機関のサイバーセキュリティ対策の向上に寄与している。

  - 2014 年（平成 26 年）5 月に連邦金融機関検査協議会（FFIEC）は、金融機関のおよそ 5,000 名の金融機関の経営層が視聴するオンラインセミナーでサイバーセキュリティの強化について強調した。この中で、自己評価による規制への遵守状況の把握のみならず、脆弱性やリスク軽減策についての評価の実施を発表した。2014 年（平成 26 年）度に実施する評価は、求める基準に対する現状とのギャップ分

48 https://www.sans.org/critical-security-controls/
49 https://www.ffiec.gov/press/pr060613.htm
50 http://www.ffiec.gov/pdf/cybersecurity/2014_June_FFIEC-Cybersecurity-Assessment-Overview.pdf

析を行い、サイバーセキュリティ対策に多くのリソースを費やすことが難しい地方銀行への支援を強化すると述べた[51]。

- 2014 年（平成 26 年）11 月に連邦金融機関検査協議会（FFIEC）は、管轄下にある金融機関に対して、「試験的に実施したサイバーセキュリティの評価結果の発表と、全ての規模の金融機関に対して、FS-ISAC への加入を求める発表[52]をした。
  - この中で金融機関に問われた具体的な内容は次の通りである。
    - 自社では、どのような種類のネットワーク接続を使用しているか？
    - 急速に進化変貌するサイバー脅威と脆弱性に対して、そのネットワーク接続をどのように管理しているか？
    - 現在使用しているネットワーク接続は、本当に全て必要なものか？管理を容易にするために、ネットワークの種類や接続の頻度は減らせないのか？
    - 現在使用している技術や製品と利用しているサービスに対するリスクアセスメントのプロセスの中で、急速に進化変貌するサイバー脅威や脆弱性をどのように評価しているのか？
    - 自社の抱えるサイバーリスクに対して、現在使用しているネットワーク接続、製品、サービス、および技術は、本当に最適な組み合わせで効果的に機能しているのか？

● ニューヨーク州金融サービス局（NYDFS）

- 2013 年（平成 25 年）、ニューヨーク州金融サービス局（NYDFS）は、増加するサイバーセキュリティのリスクに対する銀行の対応状況を把握するため、「銀行におけるサイバーセキュリティの対応状況の調査（an industry survey on cyber security）」を実施し、報告書を発表した[53] 。この調査では、154 の銀行に対してアンケートが用意され、各行におけるサイバーセキュリティ対策の取組状況、費用、および今後の計画などについて質問が行われた。主な目的は金融サービス業界全体の横断的なサイバー対策の状況や態勢などについて把握する事であった。
- 当アンケートの結果として、銀行の情報システムの管理が自組織で行われているか、外注されているか、情報セキュリティに関して既に規程が定められているか、情報セキュリティに対する予算がどの程度確保されているかなど、企業規模毎の状況が明らかになった。情報セキュリティ予算は調査対象の銀行のうち 77%がこの 3 年間増加していると答えている。

- 2013 年（平成 25 年）から 2014 年（平成 26 年）にかけて、ニューヨーク州金融サービス局（NYDFS）は、「規制管轄下の保険会社におけるサイバーセキュリティに関する調査（a survey with respect to cyber security at a significant cross-section of regulated insurance companies）」を実施し、報告書を発表した[54] 。この調査では合計資本総額がおよそ 3.2 兆米ドル（384 兆円[55]）にのぼる 43 の保険会社が対象とされ、各保険会社のサイバーセキュリティへの取組み、予算、および将来計画が調査された。

---

51 https://www.ffiec.gov/press/pr050714.htm
52 http://www.ffiec.gov/press/pr110314.htm
53 http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf
54 http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf
55 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 米ドル=120 円として換算。

- 当アンケートの結果として、保険会社の情報システムの管理が自組織で行われているか、外注されているか、情報セキュリティに関して既に規程が定められているか、情報セキュリティに対する予算がどの程度確保されているかなど、企業規模毎の状況が明らかとなった。保険会社における情報システム予算に占める情報セキュリティの予算の割合は概ね 1~3%程度であることが分かった。

- ニューヨーク州知事のアンドリュー・クオモ氏は、2014 年(平成 26 年)5 月、ニューヨーク州金融サービス局(NYDFS)が金融機関のサイバーセキュリティへの対応状況の検査を開始すると発表した[56]。

- 2014 年(平成 26 年)6 月から 8 月にかけて、米国最大級の銀行 JP モルガン・チェースがサイバー攻撃を受け、8,300 万件もの膨大な顧客情報の漏洩が同年 8 月に発覚した[57]。この事件をきっかけとして、ニューヨーク州金融サービス局(NYDFS)は、「サイバーセキュリティを単なる情報技術の一部としてではなく、組織全体のリスク管理の戦略の中で不可欠な要素として見直すように求める」との通達を金融機関向けに行った[58]。

- 2014 年(平成 26 年)10 月に、ニューヨーク州金融サービス局(NYDFS)は、管轄下にある銀行に対する「標的型攻撃への耐性評価の実施の通告と、銀行評価プロセスへの耐性評価試験の追加計画(NYDFS issues examination guidance to banks outlining new targeted cyber security preparedness assessments)[59] [60]」を発表した。

  - 具体的な評価項目は次の通りである。
    - 情報セキュリティと事業機能の相互連携、セキュリティ方針などの文書化などを含めたサイバーセキュリティ課題の管理状況
    - 情報セキュリティやリスク管理全般に対するリソースの充当具合
    - 共有インフラ環境の利用による想定リスク
    - 多要素認証や動的認証などの不正侵入保護
    - ペネトレーションテストを含めた情報セキュリティテストおよび監視
    - ネットワーク監視を含めたイベントの検出とインシデント対応の体制
    - 情報セキュリティ専門家の教育
    - 外部サービス提供者の管理
    - 事業継続性計画への情報セキュリティ管理体制の組み込み
    - サイバーセキュリティ保険の補償範囲

56 http://www.governor.ny.gov/news/governor-cuomo-announces-new-cyber-security-assessments-banks
57 http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm
58 http://www.reuters.com/article/2014/10/22/us-regulator-cybersecurity-lawsky-idUSKCN0IB03220141022
59 http://www.dfs.ny.gov/about/press2014/pr1412101.htm
60 http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf

● 証券取引委員会（SEC）

➢ 2014 年（平成 26 年）4 月 15 日、証券取引委員会（SEC）は、委員会に登録されているブローカー・ディーラーと投資アドバイザーの 50 団体以上に対して、委員会内のコンプライアンス検査局（OCIE）によるサイバーセキュリティ保護の対応状況の監査を行うと発表した[61]。

➢ 2015 年（平成 27 年）2 月 3 日には、証券取引委員会（SEC）内に設置されているコンプライアンス検査局（OCIE）が上記のサイバーセキュリティ保護の監査において発見された見解事項をまとめたリスク警告文書を発表した[62]。

◆ コンプライアンス検査局（OCIE）の担当者らは、登録されたブローカー・ディーラー57 団体、投資アドバイザー49 団体に対して、サイバーセキュリティに関連した法律、規制、コンプライアンスの課題について、どのように取り組んでいるかを検査する。

◆ 検査対象の団体は、金融サービス業界から横断的な分析結果が得られるよう、またサイバー攻撃に対して様々な団体の脆弱性が浮き彫りになるよう選択された。

◆ コンプライアンス検査局（OCIE）の検査で使用される証券取引委員会（SEC）の新しいガイドラインの主な点は次の通りである。

▫ 金融機関向けの証券取引委員会（SEC）のセキュリティガイドラインは、長い間、業界の先進的な経験則や連邦金融機関検査協議会（FFIEC）などの機関から出されるものが標準だった。

▫ このガイダンスでは、金融機関がサイバー保険に加入する事を推奨しており、証券取引委員会（SEC）は必須の要件として加えた。

▫ 他の多くのサイバーセキュリティガイドラインと同様に、このガイダンスはリスクと事前精査に加えて、リスク評価プロセスを求めている。

▫ 文書では、金融機関におけるもっとも深刻なサイバーセキュリティのリスク 3 つを理由と共に挙げる事を求めている。

▫ また文書では、DDoS 攻撃の防止について着目している。

▫ この文書では、金融機関における多層での不正防止や認証の強化などについても言及している。

● 金融業規制機構（FINRA）

➢ 2014 年（平成 26 年）1 月、サイバーセキュリティが 2014 年（平成 26 年）の優先課題であり、証券会社（ブローカー）におけるサイバーセキュリティ対策の調査を行うと通達した[63]。

◆ この調査は4つの目的にために実施された。

▫ 証券会社における脅威の種類を理解する

▫ 証券会社の情報システムにおけるサイバーリスクの容認度、影響度、および脆弱性の領域について理解を高める

61 http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf
62 http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf
63 http://www.finra.org/industry/sweeps-letter-cybersecurity

- これらの脅威を管理する手法についてのより良い理解を高める
- 発見事項等について証券会社と共有する

➢ 2014 年（平成 26 年）に金融機関に対して行った検査の結果をまとめた報告書を、2015 年（平成 27 年）2 月に発表した[64]。

◆ この中で、効果的なサイバーセキュリティ対策のためには、経営陣主導の強いリーダーシップによるセキュリティガバナンスが有効であること、各金融機関が取り組むべきサイバーセキュリティ対策を導きだすには、リスク評価が重要であることなどが、改めて確認された。

4.3. 金融機関によるサイバーセキュリティ対策への取組み

4.3.1. 経営陣の発表

プライスウォーターハウスクーパース（PwC）が、毎年、世界の主要企業の最高情報責任者（CIO）らに対して実施しているグローバル情報セキュリティ調査（Global State of Information Security Survey: GSISS）2014[65]によると、近年、世界の主要な企業におけるサイバーセキュリティ対策に対する予算が拡大されていることが示されている。収益 10 億米ドル以上の大企業における情報セキュリティ予算は 2013 年（平成 25 年）1,030 万米ドルから 2014 年（平成 26 年）1,080 万米ドルに、収益 10 億米ドル未満の中堅企業でも 2013 年（平成 25 年）280 万米ドルから 2014 年（平成 26 年）300 万米ドルへと増加している。また金融機関の経営陣による公式発表では、サイバーセキュリティに対する積極的な対策の実施が述べられている。具体的には、サイバーセキュリティ専任の組織の設置や、最高情報セキュリティ責任者（Chief Information Security Officer, CISO）の配置、意識向上プログラムの実施と優先事項への対応などが、活発に行われるようになってきている。

64 http://www.finra.org/sites/default/files/p602363%20Report%200n%20Cybersecurity%20Practices_0.pdf
65 http://www.pwc.com/jp/ja/advisory/press-room/news-release/2014/information-security-survey140205.jhtml

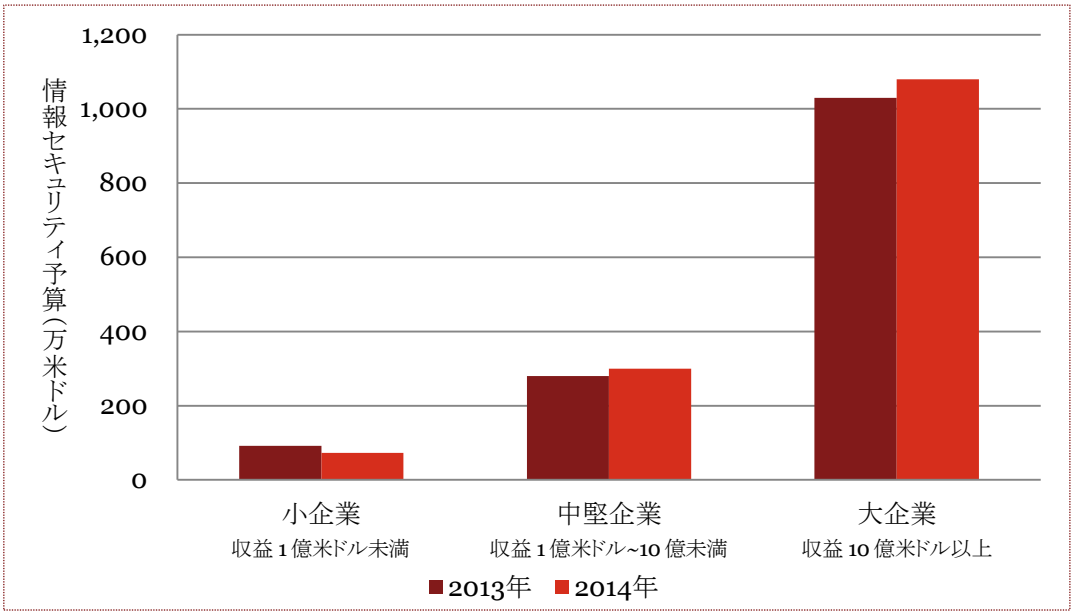

図 4-1　企業規模（収益）別の情報セキュリティ予算

一例として、米国の代表的な銀行である、JP モルガン・チェース銀行の会長であり最高経営責任者（CEO）であるジェイミー・ダイモン氏は、2014 年（平成 26 年）8 月の株主総会において、2014 年（平成 26 年）度だけで実に 2 億 5,000 万米ドル（299 億円[66]）、または、全利益の 0.1%もの費用をサイバーセキュリティ対策に投じ、1,000 名を超えるサイバーセキュリティの人材を新たに雇用する予定であると発表した[67]。

また、同氏は、金融機関におけるサイバーセキュリティ対策の優先順位は、第一に売上総利益に対するセキュリティ投資比率の拡大、第二に最高情報セキュリティ責任者（CISO）と最高経営責任者（CEO）の間の情報連携の強化であると述べた。

4.3.2. 金融機関による取組体制

プライスウォーターハウスクーパース（PwC）が実施したグローバル情報セキュリティ調査（GSISS）2014[68]によると、米国の大規模金融機関（21 行）のうち、77%の金融機関がすでに最高情報セキュリティ責任者（CISO）を任命し、5%が今後 1 年間に任命することを検討するとしている。最高情報セキュリティ責任者（CISO）は、これまで最高情報責任者（CIO）の配下で情報システムの運用に関わる業務を兼任するケースが多かった。しかし、昨今では、最高情報セキュリティ責任者（CISO）は最高リスク責任者（CRO）の配下に設置され、リスク管理やガバナンスの一環として情報セキュリティ管理を推進するケースが増えてきた。

専任の最高情報セキュリティ責任者（CISO）を任命し、最高リスク責任者（CRO）の下に配置することの利点は、情報システムにおけるセキュリティ対策の十分性や妥当性を客観的な立場からレビューし、牽制出来ることにある。

---

66 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 米ドル=120 円として換算。
67 http://www.cbsnews.com/news/why-250m-didnt-protect-jp-morgan-from-hackers/
68 http://www.pwc.com/jp/ja/advisory/press-room/news-release/2014/information-security-survey140205.jhtml

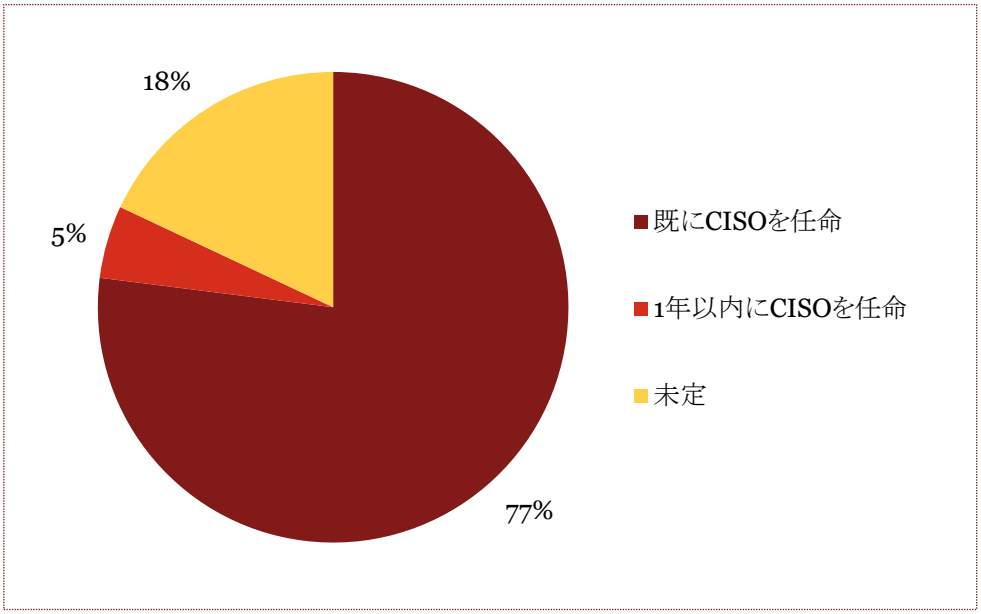

図 4-2　米国の大規模金融機関 21 行の CISO 任命状況

4.3.3. 人材の育成

金融機関に限定したものではないが、下記のような人材育成の取り組みが実施されている。

- アメリカ国家科学財団（National Science Foundation, NSF）[69]という科学技術の振興機関では、サイバーセキュリティに特化した人材の育成のためのプログラムに対する資金提供、資金援助の取組みがなされている。
- 国家安全保障局（NSA）とカーネギーメロン大学が高校生を対象としたコンペを開催（2013 年（平成 25 年）3 月）[70]
- 国家安全保障局（NSA）が大学でのサイバー運用の人材奨学制度を実施（2013 年（平成 25 年）9 月）[71]
- 国家安全保障局（NSA）がサイバーセキュリティ教育を推進（National Initiative for Cybersecurity Education）[72]
- 国土安全保障省（DHS）が大学生向けサイバー防衛競技会を後援（National Collegiate Cyber Defense Competition）[73]

69 http://www.nsf.gov/
70 http://www.washingtontimes.com/news/2013/mar/15/carnegie-mellon-nsa-seek-high-school-hackers/#!
71 http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/11/the-nsa-sponsors-cyber-operations-training-at-universities-heres-what-students-learn/
72 http://csrc.nist.gov/nice/
73 http://www.nationalccdc.org/

4.3.4. 金融機関のセキュリティ関係組織との連携体制

政府機関と民間企業、金融機関同士、金融機関を含む民間企業相互の情報共有フレームワークには、次の様なものがある。

a) 情報共有のための組織

- FS-ISAC（Financial Services Information Sharing and Analysis Center: FS-ISAC）
  - 金融分野におけるサイバーおよび物理的な脅威に関する情報収集と解析および加盟団体間での共有を行うためのグローバルな業界団体による非営利の機関である。
  - 米国で 1999 年に設立され、政府の関係機関ではない非営利団体として銀行、証券会社および保険会社等 4,600 社を超える金融機関が会員として加入しており、幹部および役員は各金融機関の役員等で構成されている。
  - 公表されている任務は、財務省（DOT）および金融サービス分野調整協議会（FSSCC）と連携し、金融分野のサイバー情報の脅威、脆弱性および攻撃に対する準備と対応能力を高め、分野内の主要な情報交換拠点（コミュニケーションチャネル）として機能することである。
  - 金融分野の重要インフラに関するセキュリティ情報の共有や、公表することが難しい標的型攻撃、フィッシング詐欺、不正送金、DDoS 攻撃、ゼロデイ攻撃などの最新の攻撃手法や被害に関する情報などを会員に対してポータルサイト等で共有している。
  - サイバーに関する情報源として、脅威レベルの情報やベンダーのセキュリティアラート、脆弱性アラート、サイバーセキュリティ関連ニュース、脆弱性公開情報の他に、リアルタイムで発生している事象など広範囲に情報収集している。
  - 具体的な業務の内容は次の通りである。
    - 金融サービス分野に有用な情報共有の場を提供すると同時に、重要インフラ及び重要資産に係わる組織及び政府と連携する
    - 脅威、脆弱性及びインシデントに関する分析や分野に与える影響評価結果を、金融サービス分野調整協議会（FSSCC）などにフィードバックする
    - 金融サービス分野におけるオペレーションに関わる課題、要求事項を整理し、財務省（DOT）及び国土安全保障省（DHS）に対して報告する
    - サイバー/物理上の脅威、脆弱性インシデント情報を、リアルタイムで正確に会員に発信し、分野のコミュニケーションハブとして機能する
    - 緊急時の分野内のコミュニケーションハブとして機能し、会員及び金融サービス分野調整協議会（FSSCC）に対して迅速な情報提供を行う
    - 財務省（DOT）及び金融サービス分野調整協議会（FSSCC）と連携し、以下の目的を果たす
      - 分野内、他重要インフラ/重要資産に関わる組織、及び政府と情報共有を行うことの有効性を説明する
      - 重要インフラ/重要資産防護、脆弱性、脅威、リスクマネジメント及びコンプライアンス等に関して金融サービス分野内の教育活動を行う

- 他重要インフラ/重要資産分野との調整の中で、分野内の意識及び危機準備体制を向上させる

◆ FS-ISAC における情報共有の手法は次の通りである。

▫ 国土安全保障省（DHS）の国土安全情報ネットワーク（Homeland Security Information Network: HSIN）システム[74]及び US-CERT（4.2.2 参照）のセキュアポータル（政府機関や各業界の ISAC に対してサイバーインシデントの情報提供をしている）を通じての情報共有

▫ 国土安全保障省（DHS） 及び米国の研究開発企業で政府や民間向けに情報技術およびシステム統合のための製品とサービスを提供するサイエンスアプリケーションインターナショナルコーポレーション（Science Applications International Corporation: SAIC）[75]との脅威情報に関する隔週の電話会議

▫ 緊急時の電話会議

▫ 対面ミーティング

▫ 会員のアニュアルミーティング（毎年春頃、2～3 日間の日程で開催、金融サービス分野における脅威や、新規技術に関する講演や会員間の交流のためのイベントが開催される。）

▫ 会員向け調査の実施（2013 年の調査テーマ[76]を以下に示す。）

- 可搬媒体のアクセス方針の調査
- DDoS に関する認識と技術の調査
- Java 脆弱性の提言に関する調査
- HTML 形式電子メールの埋め込み画像周辺の制御に関する調査

➢ Soltra Edge[77]

◆ 従来より FS-ISAC によってサイバー脅威情報（疑わしい Web サイトアドレス、悪意ある email アドレス、ウィルスソフトの定義情報、フィッシング攻撃に使われる文言など）の共有は行われていたが、脅威情報の入手から自組織のセキュリティソフトへの適用には 7 時間程度もかかっていたため、同時多発的な攻撃に対しては無防備であることが大きな課題であった。これを解決するため、サイバー脅威情報を各金融機関で導入しているセキュリティソフトに自動的に適用することで、同時多発的な金融機関に対するサイバー攻撃にいち早く防御態勢が整えられるようにしたソフトウェアであり、FS-ISAC と米国証券保管振替機関（DTCC）が共同出資したソルトラ（Soltra）社が開発し、2014 年 12 月より本格稼働している。このソフトウェアの開発には、125 団体にもおよぶ FS-ISAC 加盟団体および金融以外の部門の政府および民間団体が参加し、脅威情報構造化記述形式 STIX やインジケータ情報の信頼済み自動交換 TAXII（4.3.4 参照）といったオープンスタンダードを活用してあらゆる規模の組織での効果的な脅威情報の交換に適用できるように設計されている。

● ISF（Information Security Forum）

◆ 英国で設立された団体であるが、米国の金融機関も多数加盟している。5.3.3 参照

● 情報共有分析機関（Information Sharing and Analysis Organizations: ISAO）

◆ 4.2.1 参照

---

74 http://www.dhs.gov/what-hsin
75 http://www.saic.com/about/about-saic/
76 http://www.fsisac.com/news/surveys/
77 http://www.soltra.com/

- 国家サイバーセキュリティ統合センター（The National Cybersecurity and Communications Integration Center: NCCIC）
  - 国土安全保障省（DHS）内の部門で、24 時間 365 日稼働でサイバー空間の監視や情報共有、分析、インシデント対応などサイバーリスクに関する国家的な統合管理センターとして機能し、さらに情報共有分析機関（ISAO）との間でサイバー脅威に関する情報共有やセキュリティシステムの強化等に関する継続的で包括的な調整に携わる。これによって、官民両部門間の堅固かつ自主的な情報共有の維持・拡充が保証されることとなる。
- サイバー脅威インテリジェンス統合センター（Cyber Threat Intelligence Integration Center : CTIIC）
  - 2015 年（平成 27 年）2 月 13 日付の大統領覚書（未採番）「サイバー脅威インテリジェンス統合センター」に基づいて、国土安全保障省（DHS）の下部組織として新設されることになった機関で、国家安全上の米国外のサイバー脅威に関する連携の為の国家インテリジェンスセンターとしての機能をもつ。
  - 類似の既存機関である国家サイバーセキュリティ統合センター（NCCIC）が国土安全保障省（DHS）配下で情報共有分析センター（ISAC）や情報共有分析機関（ISAO）と連携してサイバーセキュリティ情報の共有を行うのに対して、サイバー脅威インテリジェンス統合センター（CTIIC）は、国土安全保障省（DHS）の上位に位置づけられ、国土安全保障に関する情報の他に国防総省（DOD）と軍事情報を交換したり中央情報局（CIA）と海外情報の交換を含めて行う。
- CERT/CC（CERT Coordination Center）
  - 米国のインターネットセキュリティを扱う研究開発センターで、CSIRT の草分けであり、同分野で最も権威ある組織の一つである。ペンシルベニア州ピッツバーグのカーネギーメロン大学（Carnegie Mellon University）ソフトウェア工学研究所（Software Engineering Institute: SEI）[78]で運営されている。脆弱性の分析などを行っている。
- US-CERT（United States Computer Emergency Readiness Team）
  - 4.2.2 参照。
- InfraGard [79]
  - 米国の民間企業と連邦捜査局（Federal Bureau of Investigation: FBI）のパートナーシップのための非営利団体であり、金融をはじめエネルギーや交通、ヘルスケアなど国家の重要インフラの物理的セキュリティおよびサイバーセキュリティの保護を目的とした信頼ある知識や経験などの共有を行う組織である。

b）情報共有の関連技術

- 脅威情報構造化記述形式 STIX（Structured Threat Information eXpression）[80]
  - サイバー攻撃の活動を俯瞰的に把握するには、攻撃者、攻撃者の行動や手口、狙っているシステムの脆弱性などの攻撃者側からの状況や、サイバー攻撃を検知するための兆候、攻撃によって引き起こされる問題、対処するために取るべき措置などの防衛側からの状況などをまとめる必要がある。STIX は、こうしたサイバー攻撃に関する情報や対応に関する知識の交換を共通形式によって

78 http://www.sei.cmu.edu/
79 https://www.infragard.org/
80 http://www.ipa.go.jp/security/vuln/STIX.html

効果的に行うために、攻撃活動の内容を記述するために開発された技術仕様で、標準化されたXML形式で記述するように設計されている。

- サイバー攻撃活動の記述に関する取組みは2010年にUS-CERTとCERT/CCが脅威情報の交換や脅威情報を構造化したアーキテクチャの検討を行ったことをきっかけとなっており、この脅威情報を構造化したアーキテクチャでは、検知に有効なサイバー攻撃を特徴付ける指標(Indicator)という概念が導入され、また脅威情報に含まれる情報のスコープや種類が整理された。米国政府の支援を受けた非営利団体MITRE Corporation[81]が中心となって仕様策定が行われている。
- 具体的には、攻撃の意図や攻撃に関与している人・組織、攻撃者の行動や手口などといった一連の攻撃の要素を繋がりとして記述できる形式となっている。

● 検知指標情報自動交換手順TAXII(Trusted Automated eXchange of Indicator Information)[82]

- サイバー攻撃活動の情報や対応に関する知識を自動的に交換するための規格で、STIXなどの標準化された形式で記述された攻撃に関する情報を信頼性高く交換することを目的とした技術仕様である。
- 国土安全保障省(DHS)の主導により安全で迅速にサイバー脅威情報を交換することを目的に開発され非営利団体MITRE Corporationが中心となって仕様策定が行われている。

4.4. 有事における対応

4.4.1. サイバー攻撃やテロに対する官民の対応態勢

米国の多くの金融機関では、国立標準技術研究所(NIST)の技術仕様である「Special Publication 800-61」や「Special Publication 800-86」、更に「Framework for Improving Critical Infrastructure Cybersecurity」を基にして、サイバーセキュリティの態勢を整備している。

● 国立標準技術研究所(NIST) (4.2.3参照)

➢「Special Publication 800-61 - Computer Security Incident Handling Guide[83]」

▫ 情報セキュリティのインシデントの対応を行うCSIRT組織、システムやネットワークの管理者、セキュリティ担当者、CISOやCIO、コンピュータセキュリティのプログラム管理者を対象として書かれており、インシデント対応ための組織構成や、インシデント対応の手順、インシデント情報の効果的な共有方法などについて標準化されたもの。

➢「Special Publication 800-86 - Guide to Integrating Forensic Techniques into Incident Response[84]」

▫ インシデント対応に対するフォレンジック技術の活用に関して標準化されたもの。ファイル、OS、ネットワーク通信およびアプリケーションといった4つの主要な情報ソースにおけるフォレンジック調査の解析プロセスに対しての推奨方法などが記載されている。

81 http://www.mitre.org/
82 http://taxiiproject.github.io/getting-started/intro/
83 http://csrc.nist.gov/publications/PubsSPs.html
84 http://csrc.nist.gov/publications/PubsSPs.html

- 「Framework for Improving Critical Infrastructure Cybersecurity[85]」
  - 金融やエネルギー、運輸をはじめとする政府機関の重要な社会インフラにおける情報システムのサイバーセキュリティ対策について標準化されたもの。政府機関向けでは遵守が求められているが、体系的に整理されたモデルであるため民間の金融機関等での情報システムのサイバーセキュリティ対策への利活用も多い。

4.4.2. 政府または業界として取組んでいるサイバー攻撃の対応演習

米国において、サイバー攻撃の有事の際への備えとして過去に実施された主な演習は次の通りである。

- FS-ISAC CAPP（Cyber Attack against Payment Processes）Exercise（2010）[86]
  - 主催
    - FS-ISAC
  - 開催日時
    - 2010 年（平成 22 年）2 月 9 日から 11 日の 3 日間
  - 対象者
    - 金融機関（FS-ISAC への加盟は必要なし）
  - 目的
    - 支払システムに対する大規模なサイバー攻撃への関係機関の対応力のテスト
    - サイバー脅威に対する認知度の向上と金融機関への教育
    - インシデント対応の手順の改善のための推奨事例の作成
    - リスク低減の推奨事例の評価と開発
    - 将来の脅威や脆弱性およびインシデント情報の共有のための参加企業の参画推進
    - 事後のワークショップや Web セミナー等に活用する教育素材の開発
  - 攻撃シナリオ
    - データベースへの SQL インジェクション
    - Web サービスへの DDoS 攻撃
    - スピアフィッシング
- FS-ISAC CAPP（Cyber Attack against Payment Processes）Exercise（2014）[87]
  - 主催
    - FS-ISAC
  - 開催日時
    - 2014 年（平成 26 年）9 月 9 日から 10 日と 16 日から 17 日の 4 日間
  - 対象者
    - 金融機関（FS-ISAC への加盟は必要なし）
  - 目的

85 http://www.nist.gov/cyberframework/
86 https://www.fdic.gov/news/conferences/2010_fraud/Simmons.pdf
87 https://www.fsisac.com/sites/default/files/2014CAPP_Outreach1_PDF_0.pdf

- サイバーリスクやコンプライアンス、風評脅威などに関する現状とのギャップ特定のためのプロセスを通してインシデント対応チームを主導
- サイバー攻撃での実世界におけるリスクの理解を深める
- 技術的なインフラを強化する
- サイバー攻撃に際しての危機対応連携態勢が適切かの立証
- リスク低減、コンプライアンス遵守体制、風評脅威の保護などにおけるベストプラクティスを用いたサイバー攻撃に対する持続のための計画

● Quantum Dawn（2011）
  - ➢ 主催
    - 金融サービス分野調整協議会（FSSCC）
  - ➢ 開催時期
    - 2011 年（平成 23 年）11 月 2 日
  - ➢ 目的
    - 金融サービス部門における州ごとのサイバーインシデント対応の連携を円滑にすること
    - 金融サービス分野調整協議会（FSSCC）が用意したインシデントシナリオに則った演習の検証結果を収集すること。

● Quantum Dawn 2（2013）
  - ➢ 主催
    - 米国証券業金融市場協会（SIFMA）
  - ➢ 開催日時
    - 2013 年（平成 25 年）7 月 18 日
  - ➢ 対象者
    - 金融機関、証券取引所、財務省（DOT）、国土安全保障省（DHS）、FBI、証券取引委員会（SEC）等、50 以上の組織、500 人以上
  - ➢ 目的
    - サイバー攻撃シナリオに対応した危機管理計画と危機低減戦略の演習および金融業界としての事業継続と情報セキュリティ実践の演習
    - サイバー攻撃時の市場反応の委員会での意思決定の演習
    - 金融サービス分野の重要インフラの損害のシミュレーション
    - Quantum Dawn の結果を踏まえたインシデント対応手順の再検証
    - 攻撃後の業界の運用復旧のための手順の検証
  - ➢ 攻撃シナリオ
    - 株式市場に対する同時多発的なサイバー攻撃が行われ、市場取引に連鎖的に影響が及び、株式市場がシャットダウンという想定。

● 国土安全保障省（DHS） Cyber Storm I (2006)[88]
  - ➢ 主催
    - 国土安全保障省（DHS）
  - ➢ 開催日時

88 http://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20I%20After%20Action%20Final%20Report.pdf

- 2006 年（平成 18 年）2 月

➢ 対象者

- 115 以上の連邦政府、州政府、地方政府および金融機関を含む民間企業

➢ 内容

- 内容政府主導による最初の本格的なサイバー演習として実施された。

➢ 攻撃シナリオ

- エネルギーと輸送機関の寸断を引き起こすサイバー攻撃および政府機関の業務の寸断や国民の信頼の失墜に繋がるサイバー攻撃がおこなわれたという想定。

● 国土安全保障省（DHS） Cyber Storm II (2008)[89]

➢ 主催

- 国土安全保障省（DHS）

➢ 開催日時

- 2008 年（平成 20 年）3 月

➢ 対象者

- 5 ヶ国（オーストラリア、カナダ、ニュージーランド、英国、米国）の政府機関、18 の省庁（防衛省、法務省など）と 9 つの州（ペンシルベニア、コロラド、カリフォルニア、デラウェア、テキサス、イリノイ、ミシガン、ノースキャロライナ、バージニア）、および 40 以上の民間企業

➢ 攻撃シナリオ

- 明確な政治的かつ経済的な目的を持つ架空の持続的な敵が、洗練された攻撃の手口で大規模な影響を引き起こすという想定。

● 国土安全保障省（DHS） Cyber Storm III (2010)[90]

➢ 主催

- 国土安全保障省（DHS）

➢ 開催日時

- 2010 年（平成 22 年）9 月

➢ 対象者

- 12 ヶ国（オーストラリア、カナダ、フランス、ドイツ、ハンガリー、日本、イタリア、オランダ、ニュージーランド、スウェーデン、英国、米国）の政府機関、8 の省庁、11 の州、および 60 の民間企業

➢ 目的

- Cyber Storm II を継承する内容で実施され、国家のサイバーセキュリティ態勢の増強や絶え間なく高度化するサイバー脅威に対する対応の拡充、政府機関と民間企業との連携のしくみなどを反映して、さらに下記を加えて、新たに組み直された。
- 新たに開発された国家サイバーインシデント対応計画（National Cyber Incident Response Plan: NCIRP）の検証。
- 2009 年（平成 21 年）10 月に新設された国家サイバーセキュリティ通信統合センター（NCCIC）の機能の検証。

89 http://www.dhs.gov/sites/default/files/publications/Cyber%20Storm%20II%20Final%20Report.pdf
90 http://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf

- 国土安全保障省（DHS） Cyber Storm IV (2011-2)[91]
  - 主催
    - 国土安全保障省（DHS）
  - 開催日時
    - 2011 年（平成 23 年）から 2012 年（平成 24 年）にかけて
  - 対象者
    - 11 ヶ国（オーストラリア、カナダ、フランス、ドイツ、ハンガリー、日本、オランダ、ノルウェー、スウェーデン、スイス、米国）の政府機関、7 の州政府機関など。
  - 目的
    - 国家サイバーインシデント対応計画（National Cyber Incident Response Plan: NCIRP）に基づいたサイバー脅威の特定、インシデント対応プロセスの改善、情報の共有などの検証
    - グローバルなサイバーインシデントの際の国土安全保障省（DHS）の役割の検証
    - 組織連携や情報共有、意思決定の手順などの各組織間での役割の検証

4.5. サイバー保険の動向

4.5.1. サイバー保険の市場規模

米国保険関連サービス大手のマーシュ・アンド・マクレナンの試算によると、2013 年（平成 25 年）度の米国でのサイバー保険市場全体の規模は、正味収入保険料で 10 億米ドル（1,200 億円[92]）であり、2014 年（平成 26 年）度では、20 億米ドル（2,400 億円[93]）まで拡大すると述べられている[94]。

これまでのところ、保険の請求件数が少ないことから、保険会社はまだサイバー保険の料率やリスク評価方法について検討段階にある。

4.5.2. サイバー保険の補償範囲

米国で提供されているサイバー保険の補償内容の一例は下記の通りである[95]。

- 特徴
  - 情報漏洩リスクにつき、グローバルでの補償を提供。
  - 事故発生時にはグローバルなネットワークを活用し、各国の危機管理コンサルタントを紹介。
  - サイバー攻撃等のセキュリティ事故によってコンピュータ・ネットワークが中断した結果発生した自社の逸失利益を補償（オプション契約）。

---

91 http://www.dhs.gov/cyber-storm-securing-cyber-space
92 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 米ドル=120 円として換算。
93 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 米ドル=120 円として換算。
94 http://jp.reuters.com/article/companyNews/idJPL4N0PQ19O20140715
95 http://www.aiu.co.jp/business/product/liability/cyberedge/index.htm

- ◆ 不正アクセスがなされた場合に、原因調査などを行うためのフォレンジック費用を補償。
- ◆ 情報漏洩に関する賠償責任だけでなく、コンピュータシステムに対する不正アクセス、ウィルス感染などによって第三者にも同様の被害を与えた場合の損害賠償責任について補償。（被保険者の web サイトを経由してのウィルス感染など）

➢ 補償内容

- ◆ 賠償責任に対する補償
  - ▫ 個人情報漏洩賠償責任
  - ▫ 企業情報漏洩賠償責任
  - ▫ 外部委託による賠償責任
  - ▫ 情報セキュリティ賠償責任
- ◆ 行政手続きに対する補償
  - ▫ 調査対象費用
  - ▫ 課徴金補償
- ◆ 危機管理対応のための費用に対する補償
  - ▫ 危機管理 PR 費用
  - ▫ 通知・モニタリング費用
  - ▫ 復元費用
  - ▫ フォレンジック費用
  - ▫ 危機管理実行費用
- ◆ コンピュータ・ネットワーク中断に対する補償

4.5.3. サイバー保険の採用状況

現在、サイバーセキュリティのガイドライン等でサイバー保険への加入を強く求めているものは見られないが、米国の企業の多くが企業規模に関係なくサイバー保険に積極的に加入している。

なお、2012 年（平成 24 年）に否決されたサイバーセキュリティに関する法案、「サイバーインテリジェンスの共有と保護に関する法案（CISPA）」（4.2.1 参照）では、金融機関のサイバー損害賠償保険への加入を推奨とする要件が盛り込まれていた。近い将来、金融分野でのサイバー保険の加入の必要性の議論が再燃する可能性は否定できない。

■ 5. 英国の金融分野のサイバーセキュリティ対策

5.1. 概要

本章では、英国における金融分野でのサイバーセキュリティ対策への取組みとして、英国政府よりどのような方針が示されているか、どのような法制度が制定されているか、法制度に基づいてどのような監督機関が規制当局として設置されているか、また、規制当局から金融機関に対してどのような遵守要件が示されているか等について示す。 さらに、規制当局から求められる要件に対する金融機関による適合の取組みのみならず、金融機関自身もしくは金融業界全体としての自主的な取組みとして、どのようなことが実施されているかなどについても示す。

5.2. 監督機関によるサイバーセキュリティ対策への取組み

ここでは、英国の金融機関におけるサイバーセキュリティ強化を目指した政府および監督機関の取組みを説明する。

5.2.1. 法制度や国家戦略

a) 国家戦略

英国においては、インターネットによる経済成長の促進と同時に重要なデータやシステムのサイバー空間への依存が高まることにより、検知や防御が困難な新たなリスクが国家安全保障への脅威として現実的なものとして認識されるようになり、2010 年(平成 22 年)に「サイバーセキュリティ」を最優先に取り組むべきリスクとした「国家安全保障戦略(A Strong Britain in an Age of Uncertainty: The National Security Strategy, 2010)[96]」が策定された。

更に、翌年の 2011 年(平成 23 年)11 月には、サイバー攻撃に対抗して国家安全保障や国民生活を守ることを国家の指針とした「英国サイバーセキュリティ戦略(The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011)[97]」が策定された。この中で、サイバーセキュリティに関わる二つの政府機関の新設と 4 年間に及ぶ「国家サイバーセキュリティ計画(National Cyber Security Programme)[98]」の実行に対して、6.5 億ポンド(約 1,170 億円)[99]に及ぶ予算の確保を決定している。

---

96 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf
97https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
98 http://www.parliament.uk/briefing-papers/SN05832/cyber-security-a-new-national-programme
99 平成 27 年(2015 年)3 月時点でのおよその為替レート1 ポンド=180 円として換算。

こうした政策に先立ち、英国情報局秘密情報部（通称 MI6）長官は、2009 年（平成 21 年）の議会において、「サイバーセキュリティの問題は、近年急速に国家の課題として重要性を増してきた。」と証言している。（Intelligence & Security Committee: 2010）

さらに、英国政府は 2011 年（平成 23 年）にサイバー空間に関するロンドン会議を主催し、これには日本をはじめとする主要国の政府関係者が参加した。

「英国サイバーセキュリティ戦略」には、2015 年（平成 27 年）までに達成することを目指した次の 4 つの目標が掲げられている。

目標 1	英国を、サイバー犯罪に立ち向かいサイバー空間において事業を行う際の世界で最も安全な場所の一つとする。
目標 2	英国をサイバー攻撃に対してよりレジリエントな（回復力の高い）ものとし、サイバー空間における英国の利益をより防御出来るようにする。
目標 3	英国民が安全に利用出来る、より開かれて安定した活発なサイバー空間の形成を助け、開かれた社会を支持する。
目標 4	英国のすべてのサイバーセキュリティの目的を支持するために、さまざまな分野における横断的な知識や技術、能力を確保する。

これらの目標は金融サービスに限定したものではないが、「目標 1」および「目標 2」については、金融サービス業に対してより直接的な関与や影響が考えられる。

また、「英国サイバーセキュリティ戦略」には、戦略をより広く普及させる事を目的に、具体的な達成課題と課題の解決に必要な実行計画を期限付きで示した細目が含まれている。また、これらの実行計画の一部として、サイバーセキュリティ対策のための規格やガイドラインを策定する事が含まれており、実際に英国政府は、2011 年（平成 23 年）以降の数年間で、政府通信本部（Government Communications Headquarters: GCHQ）、英国知的財産庁（Department for Business, Innovation and Skills: BIS）、およびイングランド銀行（Bank of England: BoE）の協力を得て、CBEST 脆弱性テストフレームワーク（CBEST Vulnerability Testing Framework: CBEST）、Cyber essentials scheme[100]、CESG 10 guidelines[101]などの幾つかの規格やガイドラインを策定した。

b）人材の育成

2011 年（平成 23 年）の「英国サイバーセキュリティ戦略」には、その目的の一つとして、「英国内の関連する業界での技能や能力の向上」が含まれており、これらの実現のため、具体的な実施計画が次のように定められている。

100 https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
101 https://www.cesg.gov.uk/News/Pages/10-Steps-to-Cyber-Security.aspx

- 英国が保有する世界最先端の技術力は国家における安全保障上の利益およびより高い経済発展をもたらす一方、革新的なサイバーセキュリティソリューションを構築するために、その技術力を活用し、科学技術機関ならびにその他の政府機関と連携し研究応用を進める。
- 英国内においてより強固なネットワークを構築し確実に維持するため、高いスキルや能力を持つ人材を把握し、英国内におけるエシカルハッカー[102]のコミュニティ創設を支援する。
- 政府通信本部（GCHQ）における世界水準の技術的スキルを強化する。
- 英国が持つ強みを明確にするためサイバーセキュリティの中核研究拠点に集中的な投資を行う。まずは、2012 年（平成 24 年）3 月に集中的な投資を実施する。
- 脅威ならびに脅威に対する自衛のための行動について、公共機関および民間企業において、認識の向上を働きかける。

上記の行動計画の成果として、2015 年（平成 27 年）の時点で、既に以下が達成された。

- 政府通信本部（GCHQ）は、非営利企業である CREST（GB）Limited（CREST）[103]と共同で、サイバーセキュリティに関する一連の演習や認証プログラムの開発に取り組んできた。CREST は、また、セキュリティサービス提供事業者向けの認定プログラムを提供している。5.2.3 参照。

● 英国政府は 2011 年（平成 23 年）に策定した英国サイバーセキュリティ戦略の下、サイバーセキュリティに関わる人材の育成を積極的に行っており、次の様な取り組みに資金援助を含めて推進してきている[104]。

- サイバーセキュリティの教育コンテンツの作成
- サイバーセキュリティに関する修士学位の創設
- サイバーセキュリティの公開講座開設
- 政府機関におけるサイバーセキュリティの教育

5.2.2. 金融に関わるサイバーセキュリティの関連組織

英国の金融機関に対するサイバーセキュリティ向上のための取組みには、以下の二段階のアプローチがある。

● 国家レベルでの取組み

第一段階は、英国政府が広範囲な国家安全保障戦略の一環として 2011 年（平成 23 年）に策定したサイバーセキュリティ戦略である。このサイバーセキュリティ戦略を支援するため、政府に関係するいくつかの機関、中央銀行、および防衛機関を含む組織が一丸となって協力し国家サイバーセキュリティの計画の導入にあたっている。5.2.1 参照。

102「11.用語の説明」参照

103 http://www.crest-approved.org/

104 https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

国家レベルでのサイバーセキュリティに対する取組みに関係する機関として次のようなものがある。

- 政府通信本部（Government Communications Headquarters: GCHQ）
  - 英国の外務英連邦大臣（Her Majesty's Principal Secretary of State for Foreign and Commonwealth Aggairs）直轄の情報機関の一つで、政府のサイバーセキュリティ対策を推進する中心的な役割を担っている。
  - ➢ 通信機器セキュリティグループ（Communications-Electronics Security Group Information: CESG）
    - 英国における情報保証のために政府通信本部（GCHQ）の内部に設置された情報セキュリティ部門である。産業界および学術界と連携して通信のセキュリティに関する助言や指導を英国政府に提供する。
- 知的財産庁（Department for Business: Innovation and Skills: BIS）
  - 英国の経済成長の促進を担当する政府機関で、貿易、技術革新、および経済成長の推進をする人材の支援を推進している。知的財産庁（BIS）は、ロンドン証券取引所に登録されているトップ350社に対して、年次でサイバーセキュリティ・レビューを実施している。また、「サイバーエッセンシャルズ（5.2.3参照）」の主要スポンサーの一つである。
- 国家インフラ保護センター（Centre for the Protection of National Infrastructure: CPNI）
  - 2007年（平成19年）2月に、それまで国家の重要なインフラに対するリスクを最小化するための機関であった国家インフラセキュリティ調整センター（National Infrastructure Security Co-ordination Centre: NISCC）と英国保安局（Militrary Intelligence Sction 5: MI5）の内部の組織として英国の政府機関に対してセキュリティのアドバイスを行う機関であった国家セキュリティアドバイスセンター（National Security Advice Centre: NSAC）を統合して設立された。政府機関および民間企業に対して、物理的なセキュリティ、個人情報、サイバーセキュリティ、情報保証などの重要なインフラの保護に関する助言を提供する組織である。

第二段階は、英国の金融業界に特化したサイバーセキュリティ向上の枠組みであり、大蔵省（HM Treasury）の協力の下でイングランド銀行（BOE）と金融行為規制機構（FCA）が中心となり推進をしている。

金融機関レベルでのサイバーセキュリティに対する取組みに関係する機関として次のようなものがある。

- 大蔵省（HM Treasury）
  - 英国の国家財政を担当する政府機関であり、後述のイングランド銀行（BOE）と連携してサイバーセキュリティに関する英国の金融分野の指導と監督を行っている。
- イングランド銀行（Bank of England: BOE）
  - 通貨および金融の安定を維持管理するための独立した国営組織であり、金融サービス業界のサイバーセキュリティに関するテストフレームワークである「CBESTフレームワーク」（5.2.3参照）のメインスポンサーである。
- 健全性監督機構（Prudential Regulatory Authority: PRA）
  - イングランド銀行（BOE）の傘下で銀行、住宅組合、信用組合、保険会社や大手投資会社の規制や監督を担当している政府機関で、これらの企業の安全性と健全性を促進し、特に保険会社に関

しては保険契約者の保護に関する適切なレベルを確保するための規制当局としての機能をもっている。

- 金融行為規制機構（Financial Conduct Authority: FCA）
  - 政府から独立した組織で、監督機関として健全性監督機構（PRA）の監督を受けない金融機関（小売商品の仲介業者、小規模な投資会社、電子マネー機関、決済サービス機関など）の健全性規制、監督、全ての認可業者の業務行為規制、市場規制を担当する。

英国の金融業界におけるサイバーセキュリティに対する取組みは、イングランド銀行（BOE）と金融行為規制機構（FCA）とが中心となって推進している。イングランド銀行（BOE）は、英国政府および業界の主要な団体と協力して金融分野の指導と監督を行い、英国政府のサイバーセキュリティ戦略の動向を反映した金融機関のための施策を定期的に策定している。また、CBEST のような脆弱性検査などのプログラムのスポンサーとして先導的な役割を担っている。金融行為規制機構（FCA）は、主要な金融機関と連携し、定期的にサイバーセキュリティに関する複数のプログラムを実施している。また、イングランド銀行（BOE）傘下の組織である健全性監督機構（PRA）もイングランド銀行（BOE）が主導する監督検査に対して金融の安定性の観点で調整する責任を持つ。

政府通信本部（GCHQ）、知的財産庁（BIS）および国家インフラ保護センター（CPNI）は英国政府内のあらゆる部門に対してサイバー脅威の調査解析と防衛指導の支援を提供しているが、その中でも金融分野はこれらの機関の助言に基づく戦略的なセキュリティ対策が必要な領域として積極的に連携が行われている。

その他民間のサイバーセキュリティに関係する機関としてつぎのようなものがある。

- CREST（GB）Limited,（The Council for Registered Ethical Security Testers）
  - 英国の情報セキュリティ技術者、特にセキュリティテストの専門家向けのトレーニングおよび認定資格試験実施機関であり、ペネトレーションテスト等の提供も行う民間非営利団体。2008 年（平成 22 年）に監査法人等により設立された。
  - CREST の各種プログラムに対しては、政府通信本部（GCHQ）の通信機器セキュリティグループ（CESG）および国家インフラ保護センター（CPNI）が承認を行っている。
  - 英国には、政府が公認するサイバーセキュリティ専門家のための認定資格として、「CESG Certified Professional（CCP）scheme[105]」と呼ばれるものがあり、情報セキュリティ分野に従事する専門家向けの独立した評価検証プロセスを提供している。CREST は、この CCP 試験の運営を行っている共同事業体（IISP[106]と Royal Holloway College[107]と共同の運営）である。

105 http://certifications.bcs.org/category/15865
106 https://www.iisp.org/imis15
107 https://www.royalholloway.ac.uk/home.aspx

5.2.3. 検査監督のガイドライン

金融分野における検査監督の規制やガイドラインとしては、現在のところ、金融サービス業界特有のガイドラインが 2 種類と、金融サービス事業者を含む英国すべての事業向けのガイドラインが 3 種類存在する。ただし、2015 年（平成 27 年）3 月時点で義務付けはない。

a）金融機関向けの検査監督のガイドライン：

- CREST「CBEST 脆弱性テストフレームワーク（CBEST Vulnerability Testing Framework: CBEST）[108] [109]」
  - 2014 年（平成 26 年）6 月に発表された新たなサイバーセキュリティテストのフレームワークである。既存のペネトレーションテストではセキュリティ確保の保証をする事が難しくなってきたため、最新の攻撃手法に対応したテストを提供する事を目的としている。
  - CBEST は、イングランド銀行（BOE）および CREST[110]が開発し、サイバー攻撃の脅威源となる人物やシステムの挙動を再現した脅威インテリジェンスベース[111]のペネトレーションテストを行うフレームワークである。政府が提供する情報と、民間の機関から得られた情報を元に精度の高いテストが行うことができる。
  - 金融機関やインフラ事業者、および規制当局の経営層が、金融システムの安定を脅かすサイバー攻撃の種類と金融機関がそれらの攻撃に対してどの程度脆弱であるかについて、理解を促進するための情報を提供する。

- 金融行為規制機構（FCA）「金融犯罪ガイドライン（Financial Crime Guideline）[112]」
  - 金融機関における金融犯罪リスクの軽減のためのガイドラインとして提供されている。このガイドラインでは、規模の大きな金融機関のみならず、あらゆる規模の金融行為規制機構（FCA）の監督下の機関や個人が顧客の信用情報を安全に取り扱うために、金融犯罪の仕組みと防御策の評価する事を目的としている。
  - 金融犯罪のリスクに対抗するために、実践的な方法の構築を支援する事を目的としており、金融犯罪を発見、防止、または抑止するための効果的なシステムや防御策、金融行為規制機構（FCA）の過去知見に基づく様々な金融犯罪のリスクに関する対策のよい例や悪い例に関する情報などが含まれている。

b）金融機関向けのガイドラインに関する最近の動向

- 2013 年 6 月、金融方針委員会（Financial Policy Committee: FPC）は、英国の金融分野の情報インフラのレジリエンス（回復力）を向上させるために、規制当局である大蔵省（HM Treasury）、健全性監督機構（PRA）、金融行為規制機構（FCA）およびその他の政府機関が相互に連携するよう勧告を発令した[113]。

---

108 http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
109 http://www.crest-approved.org/industry-government/cbest/index.html
110 http://www.crest-approved.org/news/crestcon-iisp-congress-2014-registration-goes-live/index.html
111 脅威に関して蓄積された膨大な情報から特定の切り口での特徴情報を多面的分析によって抽出し判断を行うしくみ
112 http://fshandbook.info/FS/html/FCA/FC/link/PDF

➢ イングランド銀行（BOE）「金融インフラの監督に関する年次報告書（The bank of England's supervision of financial market infrastructures – Annual Report, March 2014）[114]」

- 金融行為規制機構（FCA）と健全性監督機構（PRA）は、2014 年（平成 26 年）に、主要な英国の金融機関に対して対面でアンケート調査を実施した。このアンケートは、サイバー攻撃に対する態勢についてより理解を深めてもらうことを目的して、「350 社サイバーガバナンスヘルスチェック」の事後指導という位置付けで行われた。
  - こうした継続的な働きかけの結果によって、金融分野におけるサイバーセキュリティ対策が改善され、CBEST のような対策基準を制定する事に繋がった。

c）金融サービスを含むすべての事業向けの管理体制のガイドライン

- 通信機器セキュリティグループ CESG「サイバーセキュリティに対する 10 ステップ（CESG 10 steps to Cyber Security）[115]」
  - この文書は、サイバー脅威から自らを守ろうとする英国の事業者のためのサイバーセキュリティ・ガイダンスである。企業が留意すべきサイバー攻撃から身を守るための効果的な防御策や、組織が最低限度導入を検討しなければならない仕組みについて、10 項目に整理して示されている。本ガイダンスは、2012 年（平成 24 年）に初版が発行され、現在では FTSE350[116]社の内の 3 分の 2 の企業において活用されている。
  - 具体的な「10 ステップ」の概要は次の通りである。
    1） 情報リスクとマネジメントの領域
    2） 安全な構成
    3） ネットワークセキュリティ
    4） ユーザー権限の管理
    5） ユーザー教育と認知度
    6） インシデント管理
    7） マルウェアの予防
    8） 監視（モニタリング）
    9） 可搬媒体の制御
    10） ホーム・モバイルワーキング

- サイバーエッセンシャルズ（Cyber Essentials[117] [118]）
- サイバーエッセンシャルプラス（Cyber Essentials Plus）
  - 英国政府が推進する情報セキュリティに関する制度で、機密データや個人データを取り扱う組織や法人が、適切にこれらのデータを取り扱うための仕組みを備える事を目的としている。この中には、情報保証の枠組みと、IT を守る簡単なセキュリティ防御施策が含まれる。

---

113 イングランド銀行の 2014 年 3 月発行の年次報告書（10 ページ参照）
114 http://www.bankofengland.co.uk/publications/Documents/fmi/fmiap1403.pdf
115 https://www.cesg.gov.uk/News/Pages/10-Steps-to-Cyber-Security.aspx
116 ロンドン証券取引所に上場する企業のうち、時価総額上位 350 社の企業。
117 https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
118 http://www.crest-approved.org/industry-government/cyber-essentials/index.html

- Cybersecurity Essentials は、対象組織自身が自組織のシステムを評価するためのフレームワークで、個別に評価するものである。
- Cybersecurity Essentials Plus は、システムが個別にテストされ、組織の情報リスク管理の体制の中に組み込んで評価するものである。
- CREST が開発し、2004 年（平成 16 年）6 月からサービスの提供が開始されている。現在、特定の機密情報を取り扱う政府調達企業には、Cyber Essentials 認証が求められる場合がある。
- 本フレームワークは、金融サービスを含め、英国において事業を行っているあらゆる組織、およびこのフレームワークに則り、認証を活用する組織に広く公開されている。

● 英国知的財産庁（BIS）「サイバーガバナンスヘルスチェック（Cyber Governance Health Check）[119]」
- FTSE 上場 350 社を対象としたガバナンスに関する現状調査として年次で行われており、毎年報告書が出されている[120]。

英国知的財産庁（BIS）「サイバーガバナンスヘルスチェック」は、元来「主要な資産に対する経営幹部による理解の促進」、「現在の警戒態勢のレビュー」などを主眼においていた。これに加えて、金融行為規制機構（FCA）と健全性監督機構（PRA）によるアンケートは、主に「主要なサイバーリスクの理解促進」、「事業への影響低減と金融機関の回復力強化」、「セキュリティ対策のあるべき姿とのギャップを軽減するための計画策定や復旧施策の実行促進」を狙ったものである。

具体的には、サイバー脅威への理解度、サイバーセキュリティ対策に対する組織体制、リスク管理の状況、各種のガイドラインなどセキュリティ対策促進策の認識度、インシデントの発生状況などについて調査を行い結果を整理している。

こうした継続的な取組みは、金融機関での全般的なサイバーセキュリティの課題解決の推進に繋がっており、公開された「CBEST」や「サイバーエッセンシャル」などのガイドラインは金融機関がサイバーセキュリティの対策において、一定の努力を行っている事を示すための基準としても機能している。

「CBEST」や「サイバーエッセンシャル」などのガイドラインや規格は、2015 年（平成 27 年）3 月現在、英国の金融機関に対して適合が義務付けられているわけではない。しかし、クレジットカードに関するセキュリティ規格である「PCI DSS」[121]のように、CBEST についても金融分野における業界特有のセキュリティ規格として、近い将来、適合が義務付けられる可能性がある[122]。

---

119 https://www.gov.uk/government/publications/cyber-governance-health-check-2014
120 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/399260/bis-15-37-ftse-350-cyber-governance-health-check-tracker-report-2014.pdf
121 PCI-DSS は、主要なクレジットカードのペイメントブランド会社らによって設立された、セキュリティ規格で、クレジットカード決済を取り扱う企業での遵守が求められている。
122 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf

5.3. 金融機関によるサイバーセキュリティ対策への取組み

ここでは、銀行、証券、保険といった各種金融機関によるサイバーセキュリティへの取組みについて説明する。

5.3.1. 金融機関による取組体制

各金融機関におけるサイバーセキュリティ分野の人的資源の配置状況などは、通常は非公開情報であるため明示的なデータを入手するのは困難である。しかし、英国知的財産庁（BIS）の 350 社サイバーガバナンスヘルスチェックレポート（5.2.3 参照）によると、多くの企業ではサイバーセキュリティをより重要な経営課題ととらえており、サイバーセキュリティに取組む人材の増員と、人材に対する積極的な演習の実施に関して、現状よりも更に投資を増やす計画であることが示されている。

現在、多くの金融機関では、以下の領域で人材の増強計画があるか、または実施途中だと考えられる[123]。

1) セキュリティオペレーションセンター（Security Operation Center: SOC）
2) 重大インシデント対応センター（Critical Incident Response Center: CIRC）
3) セキュリティ・アーキテクチャ
4) アプリケーションのセキュリティ
5) フォレンジックス
6) セキュリティ技術の評価

5.3.2. 人材の育成

現在の金融機関におけるサイバーセキュリティ要員の育成計画や採用計画は次の通りである。

- 人材に関する課題は業界や個々の金融機関によって様々である。しかし、全般的にサイバーセキュリティに従事する専門家は不足しており、またそのスキルには共通性があり、これが金融業界全体とサイバーセキュリティを強化する際の主なギャップ要因になっている。また、これらのサイバーセキュリティ人材の育成は、金融機関にとっても投資の領域として考えらえている。
- 英国を中心としてグローバルに事業展開する大規模な金融機関では、情報セキュリティの維持管理に携わる要員の規模は、おおむね 100 人以上である。

123 PwC の過去事例に基づく知見による。

5.3.3. 金融機関のセキュリティ関係組織との連携体制

政府と民間企業、金融機関同士、金融機関をふくむ民間企業間の情報共有フレームワークには、次の様なものがある。

- FS-ISAC（Financial Services – Information Sharing and Analysis Center）（4.3.4 参照）
  - 米国で設立されたグローバルな金融機関の情報共有のための組織で 4,600 社を超える金融機関が会員として加入している。英国の多くの金融機関もこの組織に加盟している。
- CERT-UK（Computer Emergency Response Team – United Kingdom）
  - CERT は、国家サイバーセキュリティ戦略の制定に対応して、2014 年（平成 26 年）3 月に設立された英国政府配下のコンピュータ緊急対応チームでサイバー空間における不正アクセス、不正プログラム、システムの脆弱性などに関して、情報を収集し、迅速に分析を行い、分析結果を公表共有する専門の組織である。CERT-UK は、英国内を対象とした組織であり、金融機関を含むあらゆる産業分野と連携し、また民間および政府の両方からの情報を共有するための体制を構築している。

➢ CiSP（The Cyber Security Information Sharing Partnership）

- CERT-UK の一部門として、政府と産業界がサイバー空間における現在の脅威と安全な環境でのインシデントの管理に関する情報を共有するパートナーシッププログラムで、2014 年（平成 26 年）12 月までに 750 以上の企業が加盟しており、加盟者でサイバー脅威と脆弱性に関する情報をオンラインで共有できるようになっている。またこの共有される情報には守秘義務が課せられている。
- CiSP には産業界のアナリストに加えて英国政府の保安局（Security Service）と国家犯罪対策庁（National Crime Agency）の支援を受けたアナリストのチーム「Fusion Cell」があり、英国が全体で直面しているサイバー脅威の最新情報や事業への影響を分析している。
- 英国で行われたサイバー演習ウェイキングシャーク II（Waking Shark II）でもサイバー攻撃に対する金融部門のリアルタイムでの情報共有態勢がテストされ、その効果が実証された。

- WARP（Warning, Advice and Reporting Point） Programme
  - 2002 年（平成 12 年）に国家サイバーセキュリティ通信統合センター（NISCC）によって設立され、現在国家インフラ保護センター（CPNI）の配下で利用者参加型のメンバー間におけるサイバー脅威やその対策のための情報の共有を行っているサービスプログラムで、大規模資本ではない企業などが低コストでサイバー攻撃に対する防御情報を効果的に共有するために開発されたしくみである。
  - これまでの長年の運用実績による情報の集約を活用したより横断的な連携を目指して 2015 年（平成 27 年）1 月には英国内で WARP と CiSP および CERT-UK の情報共有の体制（Cybersecurity Information Partnership）が構築されることとなった。
- ISF（Information Security Forum）
  - 1989 年（平成元年）に設立され、Fortune 500 社や Forbes 2000 社の登録企業などを中心とした 300 余りの国際的な企業・団体を会員とする非営利団体で、加盟企業が効果的に活用できる情報セキュリティやリスクマネジメントに関する概念モデルやソリューション等の開発、資金提供などを行っている。

- 加盟企業における情報セキュリティ対策に対する実践的な事例として「The Standard of Good Practice for Information Security」を年次で発表しており、金融機関でのサイバーセキュリティ対策にも活用がされている。

● CMBCG（Cross-Market Business Continuity Group）

- 2005 年（平成 17 年）11 月に金融業界における事業継続（Business Continuity）の業界横断的な協議のために、当時の（旧）金融サービス機構（FSA）と財務省（HM Treasury）および各銀行により設立された協議会で、金融当局の他にインフラ提供者および主要な金融システムの組織で構成されている。。
- 本来は事業継続に関わる影響の大きな途絶情報などの集約を行う組織であるが、後述のサイバー攻撃の対応演習「ウェイキングシャーク, 2011」（5.4.1 参照）での発見事項として有事の際の金融機関の間の横断的な連携組織として当組織が適格という評価により、近年は事業継続に影響する情報としてサイバーセキュリティに関する情報共有の役割も担っている。

5.4. 有事における対応

5.4.1. サイバー攻撃やテロに対する官民の対応態勢

a）金融機関におけるインシデント対応態勢の整備状況

英国企業におけるインシデント対応の態勢は、各組織に依存する部分が多く、業界全体を見ても様々である。

金融業界においては、前述の通り、顧客情報を大量に扱うことの多いリテールバンクや投資銀行、保険会社などが先駆的な対策をとっており、インシデント対応についても体制の整備が進んでいる[124]。

それ以外の金融機関については、中小の金融機関がインシデントの監視の体制構築やサードパーティ企業のサービスを活用した監視体制の実現を検討している状況である。

b）過去のインシデント対応の評価と発見事項

英国において、金融行為規制機構（FCA）、健全性監督機構（PRA）などの監督機関は、金融機関においてインシデントが発生した際の回復のための作業には関与はしない。

回復策は当事者である金融機関が策定する。実際にインシデントが発生した状況では、CESG や CERT-UK などの政府系団体から支援を受ける場合がある。

但し、CBEST のテスト実施が必須の要件になった場合には、規制当局と政府関係機関は、対象機関のギャップや CBEST の結果に関してより積極的な関与をする可能性がある。

5.4.2. 政府または業界として取組んでいるサイバー攻撃の対応演習

124 PwC UK の調査知見による。

英国で行われている金融機関を中心としたサイバー演習は次の通りである。財務省（HM Treasury）はイングランド銀行（BOE）と共に、大手金融機関のサイバー攻撃への耐性をテストするため、下記のような演習を行っている。

●「ウェイキングシャーク（Waking Shark）, 2011 [125]」
- ➢ 主催
  - ◆ 証券業界の事業継続マネジメントグループ（the Securities Industry Business Continuity Management Group: SIBCMG ）
  - ◆ イングランド銀行（BOE）
  - ◆ 財務省（HM Treasury）
  - ◆ 金融行為規制機構（FCA）
- ➢ 開催日時
  - ◆ 2011 年（平成 23 年）3 月 11 日
- ➢ 対象者
  - ◆ 英国の金融機関、インフラ事業者、および金融当局など 33 団体から 100 名を超える関係者に加えて国家インフラ保護センター（CPNI）、SOCA（the Serious Organised Crime Agency）、CSOC（the Cyber Security Operations Centre）、Payment Council、更にブリティッシュテレコムや O2 といった通信事業者などから代表者が参加し、専門者委員会が組織された
- ➢ 内容
  - ◆ 金融機関横断的な連携の仕組みを円滑かしてサイバー攻撃への態勢を整えるため。
  - ◆ 当演習は、下記のような課題を設定して行われた。
    - ▫ 大規模サイバー攻撃に際して業界間の連携における課題を見つける。
    - ▫ 既知のサイバー攻撃における対応上の課題に対する解決策を導き出す。
    - ▫ サイバー攻撃の際の金融機関の間での連携のルールを導き出す。
  - ◆ その他の目的として、同年 11 月に予定されていた「Market-wide Exercise（MWE）」（後述）のシナリオ検討の材料としても活用を想定していた。
- ➢ 背景
  - ◆ 当時、英国の様々な金融機関においては、インターネットの利用で電子化が進んだ金融情報システム上で頻繁にサイバー攻撃が発生しその手口が巧妙化することに直面していた。そこで当時の英国の（旧）金融サービス機構（FSA）との間で様々な議論をする中で、この机上サイバー演習へと繋がった。
- ➢ 発見事項
  - ◆ 有事の際における金融機関の間の横断的な連携組織として、当時既に存在していた CMBCG が適格ではないかとの意見が出た。
  - ◆ 一方で、既存の情報共有の組織が多数存在する一方で、具体的に機能や役割分担などが周知されていないため、既存の主要な組織についても周知と連携がなされるべきだとの意見もあった。

●「ウェイキングシャーク II（Waking Shark II）, 2013 [126] [127]」

125 http://www.bankofengland.co.uk/financialstability/fsc/Documents/DesktopCyberExercise(WakingShark).pdf

- ➢ 主催
  - ◆ 証券業界の事業継続マネジメントグループ（the Securities Industry Business Continuity Management Group: SIBCMG ）
  - ◆ イングランド銀行（BOE）
  - ◆ 財務省（HM Treasury）
  - ◆ 金融行為規制機構（FCA）
- ➢ 開催日
  - ◆ 2013 年（平成 25 年）11 月 12 日
- ➢ 対象者
  - ◆ 英国の銀行、決済機関、証券取引機関など、数十の機関から 220 名程度
- ➢ 内容
  - ◆ 証券市場を対象とした DDoS 攻撃や PC ワイプ攻撃など、様々な攻撃を想定した演習
  - ◆ 個別の金融機関のサイバーインシデントの耐性ではなく、投資銀行や証券市場を含む大口金融機関のシステムのサイバー攻撃に対する影響の最小化や耐性の見極めを目的に実施
  - ◆ 金融機関の組織内部のサイバーインシデント対応手順の検証
  - ◆ 国家インフラ保護センター（CPNI）や既存の危機や情報セキュリティの情報共有機関との連携の体制の検証
- ➢ 発見事項
  - ◆ 演習を通して、CMBCG を通した部門間の連携の有効性や、CiSP プラットフォームを使用した部門間の連携の有効性が実証された。

● 「Market-wide Exercise （MWE）[128]」

- ◆ 主催
  - ▫ 大蔵省（HM Treasury）
  - ▫ イングランド銀行（BOE）
- ◆ 開催日
  - ▫ 2003 年（平成 15 年）から継続的に実施
- ◆ 対象者
  - ▫ 英国の金融機関
- ◆ 内容
  - ▫ 英国の金融機関全体の事業継続力向上を目的として演習（マーケットワイド演習）である。
  - ▫ インターネットと通信に関わる主要な機器やサービス間の相互互換性や依存性をテストする（提供者が異なる機器やサービスでの相互の連携に支障がないかテストする）。
  - ▫ 参加者と市場が混乱した後、通常状態への復帰までどのように優先順位を付け、管理するかを決定する。
  - ▫ 上級スタッフ不在の際に、特に大きな混乱が生じた場合の影響について、参加者に機会を提供する（オリンピック計画の準備体制の評価をするため）。

---

126 http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf
127 http://www.bankofengland.co.uk/financialstability/fsc/Documents/mwe11report.pdf
128 http://www.bankofengland.co.uk/financialstability/fsc/Documents/mwe11report.pdf

- 戦略的な意思決定に注力して、経営陣をより効果的に関与させるために経済的な損失の要素を加味して評価する。
- 演習後、該当グループによるさらなる検討のための課題を特定する。
- イングランド銀行（BOE）による、機器提供者の参加の義務付けが予定である。

➢ 演習シナリオ

◆ 卸売や小売での支払やオンラインサービスなどに大きな混乱を生じさせるような金融分野における具体的な攻撃を想定して実施されている。また、部門規模で大きな混乱が発生している間、対象組織が他の組織とどのように連絡し調整するかをテストする。また、通信やインターネットに障害が発生した場合に、遠隔での作業ができなくなる事への影響を確認している。

5.5. 国際イベントとサイバー攻撃の関係

昨今、不正や詐欺などの攻撃者が、グローバルなイベントや著名人のニュースなどを機密情報取得の機会に利用することは、十分に想定しなければならない事態である。

例えば、2012 年（平成 24 年）のロンドンオリンピック開催中においては、次の様なインシデントが確認されている。

➢ ロンドンオリンピックのプロモーションを語った不正な電子メールによる詐欺が発生し、被害者はロンドンオリンピックの資金担当責任者を名乗る人物から不正な電子メールを受けとり、165 万ドル（2 億 9700 万円[129]）の賞金を準備するためとして個人の銀行口座へ入金を要求される事件が確認された。

➢ 清涼飲料水のロンドンオリンピック専用プロモーションサイトを装った不正な電子メールによるフィッシングが発生し、偽のサイトに誘導され、利用者がフォームに個人情報の記入を求められる事件[130]が確認された。

➢ オリンピック会場建設委員会で、コンピュータシステムにウィルスが感染し、逼迫した建設日程の中で業務が半日中断した。

➢ 他にもチケット、宿泊施設、商品販売の問題、Web サイトのスプーフィング（なりすまし）、電子メール詐欺、スピアフィッシングなどのオンライン詐欺が多数発生した。オリンピックの開催に際して、警察機関では 200 件の逮捕があり、そのうちの約 100 件がオンライン犯罪や詐欺に関わるものであった[131]。

5.6. サイバー保険の動向

5.6.1. サイバー保険の市場規模

英国におけるサイバー保険に年間の市場規模は、2016 年（平成 28 年）末の時点における正味収入保険料で、およそ 5,000 万~1 億ポンド（90~180 億円[132]）と予想される。

---

129 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 英ポンド=180 円として換算。
130 http://www.coca-cola.co.uk/faq/rumours/i-recently-got-an-email-from-coca-cola-saying-i-had-won-a-lot-of-money-is-this-a-scam.html
131 http://www.ipa.go.jp/files/000039004.pdf

5.6.2. サイバー保険の補償範囲

英国で提供されている主なサイバー保険の補償内容はグローバルで提供されているものと同様のため、4.5を参照。

5.6.3. サイバー保険の採用状況

インターネットビジネスを営む小売事業者は事業の中断に非常に高い関心を持っており、また PCI-DSS[133]に対する罰金についても補償されるサイバー保険の活用に比較的積極的である。その一方で、銀行や保険会社の一部は、サイバー保険に加入はしているものの、金融業界に広く普及している状態までには至っていない。

---

132 2015 年(平成 27 年)3 月時点でのおよその為替レート1 英ポンド=180 円として換算。

133 PCI-DSS (Payment Card Industry–Data Security Standard)は、ペイメントカードの業界団体が定めたセキュリティ基準で、法的な拘束力はないものの、ペイメントカードの加盟店や決済代行業者におけるセキュリティ対策に対する遵守基準として広く導入されている。加盟店等からの情報の漏洩などが発生しても、その加盟店が PCI－DSS 基準への準拠している場合に損害補償の一部に対して免責が認められる一方で、基準への非適合が発見された場合には罰金が科せられるという管理体制の特徴をもつ。

■ 6. 韓国の金融分野のサイバーセキュリティ対策

6.1. 概要

本章では、韓国における金融分野でのサイバーセキュリティ対策への取組みとして、政府よりどのような方針が示されているか、どのような法制度が制定されているか、法制度に基づいてどのような監督機関が規制当局として設置されているか、また、規制当局から金融機関に対してどのような順守要件が示されているか等について示す。さらに、規制当局から求められる要件への適合のみならず、金融機関自身もしくは業界全体としての自主的な取組みとして、どのようなことが実施されているかなどについても示す。

6.2. 監督機関によるサイバーセキュリティ対策への取組み

ここでは、銀行、証券、保険といった金融に関わる各種事業に対する監督機関によるサイバーセキュリティへの取組みについて説明する。

6.2.1. 法制度や国家戦略

韓国においては、過去に政府機関を含んだ大規模なサイバー攻撃を経験していることからも、サイバー攻撃が国民の財産や国家安全保障を脅かす状況にまで至っているという認識がある。

a) サイバーセキュリティに関する政策や関連法令

韓国において、国家安全保障としてのサイバーセキュリティに関する法令としては、下記のものがある。

2009 年（平成 21 年）7 月には韓国の政府や銀行、報道機関をはじめ、各種ポータルサイトが断続的に分散型サービス妨害（DDoS）攻撃を受け、横断的なサイバーテロ対策の不備が顕在化した[134]。これを契機として、下記の法令が制定された。

- 「国家サイバー危機総合対策（2009）」
  - DDoS などのサイバー攻撃に対して、先制防御および攻撃時の被害の最小化のため、策定された対策法令である。この「国家サイバー危機総合対策」では平時の各省庁の役割分担を定め、国家情報院（National Intelligence Service: NIS）は危機対応で総括的役割を、放送通信委員会

134 http://internet.watch.impress.co.jp/docs/column/security/20090804_306868.html

（Korea Communications Commission : KCC）[135]はマルウェアの感染した PC の削除及びサイバー安全関連広報および啓蒙関連業務を担当、国防部（Ministry of National Defense: MND）はサイバー部隊を新設して軍事分野を補強することとされた。（6.2.2 参照）

●「国家サイバーセキュリティマスタープラン（National Cybersecurity Masterplan – Protecting national cyber space from cyber attacks）[136]」

- ➢ ますます高度化する国家レベルのサイバー脅威に対応するために、関係する 15 省庁が合同で然るべき体制を整備し、各行政機関の役割の明確化を図ること等を定めた「国家サイバーセキュリティマスタープランを 2011 年（平成 23 年）8 月に策定した。
- ➢ この「国家サイバーセキュリティマスタープラン」では、 重点的な推進課題として以下の5つを掲げている。
  1） 脅威の早期検知及び対応体制の整備
  2） 重要な情報およびインフラにおけるセキュリティの強化
  3） サイバーセキュリティの一層の強化のためのインフラ整備
  4） サイバー空間における挑発の抑止と国際協調の強化
  5） 重要な情報およびインフラにおけるセキュリティマネジメントレベルの向上

●「国家サイバー安保総合対策（2013）」

- ➢ サイバーセキュリティの司令塔を青瓦台（大統領官邸）が担い、実務統括を国家情報院（NIS）が担当する事を決定した。これにより、未来創造科学部（Ministry of Science, ICT and Future Planning: MSIP）や国防部（MND）等の関係機関は管轄分野をそれぞれ担当し、青瓦台（大統領官邸）、国家情報院（NIS）、未来創造科学部（MSIP）等がサイバーの状況を即時に把握して対処できるよう情報連絡網を構築する事が定められた。
- ➢ 一方でこのサイバーセキュリティ体制構築に当たっては、情報収集、諜略、秘密工作活動をしている国家情報院（NIS）が情報共有や透明性といったサイバーセキュリティの基本哲学を遵守できるのかという点で懸念が示されている。

また、金融取引に関する法令としてサイバーセキュリティに関する法令としては、下記のものがある。

●「電子金融取引法（Electronic Financial Transaction Act: EFTA）[137]」

- ◆ 情報セキュリティで保護する情報、および情報に関連する金融資産等の安全性の確保（端末の保護、ネットワークの保護、電算資料漏洩の防止、情報処理システムの保護、ハッキングなどの防止対策、ウィルス対策等）、CISO（最高情報セキュリティ責任者）任命義務、セキュリティ関連の人材、組織、予算規制、施設部門などが規定されている。

135 当時の組織名称で2013 年（平成 25 年）に改組により現在は未来創造科学部（MSIP）に変更。6.2.3 参照。
136 http://service1.nis.go.kr/safe/120802_masterplan_kr.pdf
137 http://www.fsc.go.kr/downManager?bbsid=BBS0054&no=21201

その他、金融分野での法制度として、金融委員会（Financial Services Commission : FSC）と金融監督院（Financial Supervisory Service: FSS）が発行する「金融電算セキュリティ強化総合対策[138]」により、次のような推進課題への取組みがなされている。

1） 金融情報システム、電子金融安全性確保のための IT 部門の監督強化
2） 電子金融取引事故とサイバーテロに対する先制的対応
3） 電子金融取引の利便性向上と消費者保護の強化
4） IT 検査を強化し、検査品質の向上

加えて、金融委員会（FSC）と金融監督院（FSS）が発行する「金融電算セキュリティ強化総合対策」には、次のような推進計画が策定されている。

1） 金融情報システムの危機対応の強化
2） 金融機関の電子金融インフラのセキュリティ強化
3） 金融機関のセキュリティ組織人材力の強化
4） 利用者（顧客）の保護と監督を強化
5） 金融機関の自律的なセキュリティ推進活動を支援

6.2.2. 金融に関わるサイバーセキュリティの関連組織

a） 担当組織と位置付け

国家レベルでのサイバーセキュリティに対する取組みに関係する機関として次のようなものがある。

- 国家情報院（National Intelligence Service: NIS）
  - 国家安全保障に関わる情報、保安及び犯罪捜査などに関する業務を担当するために大統領直属で設置されている情報機関である。国家サイバー安保総合対策では国家のサイバーセキュリティに関する司令塔としての機能を大統領官邸である「青瓦台」が、青瓦台の下で実務統括を国家情報院（NIS）が担当するとされている。
- 未来創造科学部（Ministry of Science, ICT and Future Planning: MSIP）[139]
  - 2013 年（平成 25 年）に朴槿恵政権のもとで省庁再編により設置された省で、科学技術と産業、文化と産業の融合を進める「創造経済」を主導する省庁の中で科学技術分野と情報通信分野を所掌する学部（省に相当）である。
- 韓国インターネット振興院（Korea Internet and Security Agency: KISA） [140] [141]

---

138 Enhanced Security Integrated Financial Management Measures, 金融委員会（FSC）および金融監督院（FSS）
139 放送通信委員会（Korea Communications Commission: KCC）が 2013 年に改組して未来創造科学部（MSIP）となった。
140http://www.kisa.or.kr/main.jsp
141 2009 年 7 月 23 日に Korea Information Security Agency と Korea Internet Security Agency 、Korea IT International Cooperation Agency の 3 団体が合併して、現在の KISA となる。在籍職員数は約 500 名

- 未来創造科学部（MSIP）の関連組織で、サイバーセキュリティ対策の規制やシステム障害の回復のための研究やインシデント対応センターの運営を行っている。金融業界に限らず公共および民間の両方を対象としている。

金融業界に特化した取組みに関係する機関としては次のようなものがある。

- 金融委員会（Financial Service Committee: FSC）[142]
  - 政府機関であり、金融分野におけるサイバーセキュリティに関する規制やガイドラインを制定している。
- 金融監督院（Financial Supervisory Service : FSS）[143]
  - 政府から独立した非営利法人であり、金融機関に対する情報セキュリティの監督、およびアセスメントの実施を行っている。
- 金融セキュリティ機関（Financial Security Agency: FSA）[144]
  - 政府から独立した組織で、金融機関によって設立された業界団体のための非営利団体である。金融に関わる方法論の研究や、脆弱性解析、DDoS を想定したトレーニングなどのサービスを実施している。
  - 2015 年（平成 27 年）初頭に総合的な金融コンピュータセキュリティの専門機関として、金融保安院（Financial Security Institute: FSI）として改組され、サイバー攻撃対応、政策研究などの業務を統合する予定である。金融セキュリティ研究者と管轄捜査機関は常時協力関係を構築している。
- 韓国金融決済院（Korea Financial Telecommunications and Clearing Institute: KFTC）[145]
  - 金融委員会（FSC）の関連組織で、金融機関の情報ネットワークの監督及び Koscom と共同で「（韓国）金融 ISAC」としての業務を行っている。
- Koscom（Korea Securities Computing Corporation）
  - 企画財政部（Ministry of Strategy and Finance: MOSF）[146]と韓国証券取引所（Korea Exchange: KRX）[147]によって 1977 年（昭和 52 年）に設立された会社で、「（韓国）金融 ISAC」関連の業務を韓国金融決済院（KFTC）と共同で行う。

b）体制

金融委員会（FSC）は法律に基づいて設立された組織であり、金融監督院（FSS）は金融委員会（FSC）の傘下に位置付けられる。金融委員会（FSC）は、金融監督院（FSS）に対して金融機関の IT や情報管理の検査を行うためのガイドラインを提供する。

142 http://www.fsc.go.kr/
143 http://www.fss.or.kr/fss/kr/main.html
144 http://www.fsa.or.kr/Eng/Main.do
145 http://www.kftc.or.kr/indexEn.jsp
146 http://english.mosf.go.kr/
147 http://eng.krx.co.kr/

金融監督院（FSS）は、金融分野のサイバーセキュリティを実質的に監督する機関であり、金融機関の情報システムの障害の防止とサイバーテロの脅威に対する IT セキュリティ向上を目的としている。また、金融監督院（FSS）の中には、IT の監督、検査および情報管理機能を統合した「IT 金融情報保護委員会」が設立されている。当委員会は、韓国インターネット振興院（KISA）と金融セキュリティ機関（FSA）からセキュリティポリシーと技術動向についての報告を受け、また韓国金融決済院（KFTC）からセキュリティインシデントの傾向に関する報告を受ける形で連携している。IT 金融情報保護委員会は、IT セキュリティと個人情報の保護をより強化するため、2014 年（平成 26 年）に関連機能を統合して、検査を担当する部署として「IT 金融情報保護部門」と監督を担当する部署である「IT 監督室」の二つに再編した。IT 金融情報保護部門は約 50 人で構成されており、IT セキュリティや情報の保護などの業務経験を 3 年以上持つセキュリティ関連の学位保持者や資格保持者、金融分野のセキュリティ研究者らを優先的に採用している。

金融機関に対する監査の実施の際には、金融監督院（FSS）が金融機関の総合的な検査や部門単位での検査を実施することがある。検査は、現場調査や社内規程等の書面の査閲などの方法で実施する。ほとんどの場合、金融監督院（FSS）は金融機関に対して事前に検査スケジュールを通知して検査を実施する。金融監督院（FSS）は金融機関に対して資料の提出等を求めることができ、必要に応じて関係者へのヒアリングや業務の観察などを行うことが出来る。金融監督院（FSS）は検査の結果を金融委員会（FSC）に報告し金融委員会（FSC）は、その結果に応じて、金融機関に対して改善措置を要求することがある。

c）関連部署との連携

韓国国内での金融分野のサイバーセキュリティ情報の連携体制としては、金融委員会（FSC）が金融機関のサイバーセキュリティのための政策的な指針を示し、金融監督院（FSS）がこれに伴う金融機関のための監督、検査を実施し、報告する。金融監督院は、韓国インターネット振興院（KISA）と金融セキュリティ機関（FSA）からセキュリティポリシーと技術動向についての報告を受け、韓国金融決済院（KFTC）からセキュリティインシデントの動向についての報告を受けている。

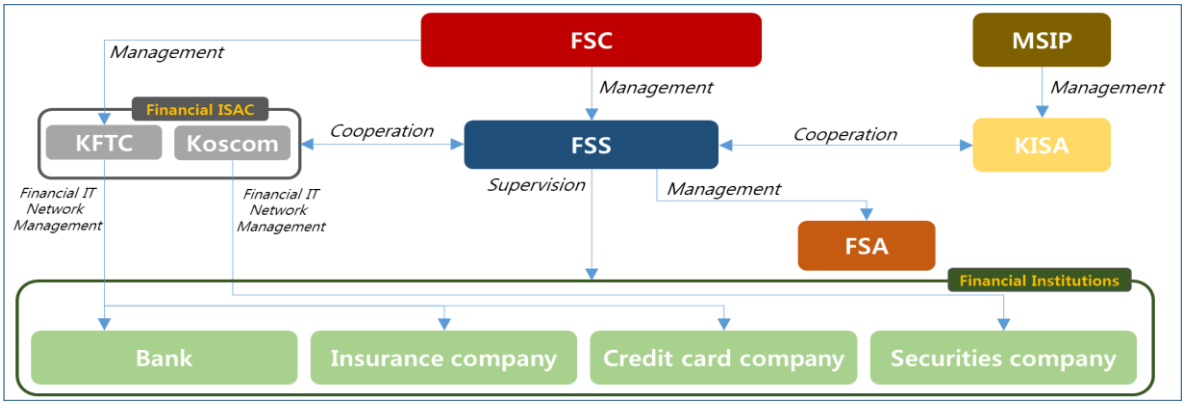

図 6-1 関連部署の連携体制[148]

148 MSIP – 未来創造科学（Ministry of Science, ICT and Future Planning）、教育、科学技術、情報通信を担当する政府機関。

6.2.3. 検査監督のガイドライン

a) 金融機関向けの検査監督のガイドライン

金融機関の検査や行政指導に関する規定、ガイドライン、安全対策の基準（例えば、日本における金融情報システムセンター（FISC）による「安全対策基準」のようなもの）としては、以下のようなものがある。

- 電子金融取引の監督規制（Regulations on Supervision of Electronic Financial Transactions [FSC Public Notification No. 2013-39, Dec 3, 2013]）
  - 金融機関の電子金融取引に関する監督の基準に関して規定されている。「人材と組織」、「施設」、「情報技術」、「安全性確保のために必要な事項」で構成されており、金融機関の情報システムにおけるネットワークの分離の義務付け、脆弱性の分析と評価、情報保護委員会の設置義務などが含まれる。
- 金融機関のサイバーセキュリティ強化計画（Security Enhancement Plan for Cybersecurity in financial institutions）
  - 金融機関のサイバーセキュリティ対策の強化のための取組み計画について規定されている。
- 電算機器を使用した関連内部統制模範規準
  - 電算機器のセキュリティ管理とシステムの構築などが規定されている。
- 金融電算セキュリティ標準のガイドライン
  - 外注請負契約時のデータ保護措置、パスワードの暗号化などの義務が規定されている。

b) 情報の管理体制

金融委員会（FSC）による電子金融取引の監督規制 では、次の通り金融機関における情報の管理体制を求めている。

- 金融機関やネット系金融機関は、重要な情報の保護に関する事項を審議、議決する情報保護委員会を設置、運営しなければならない。
- 情報保護委員会の代表者は、情報保護の最高責任者として、情報保護委員会の審議･議決を最高経営責任者（CEO）に報告しなければならない。
- 情報保護委員会は、次の各号の事項を審議･議決する。
  - 情報技術部門計画書に関する事項
  - 電子金融取引の安全性の確保と利用者保護のための戦略と計画の策定に関する事項
  - 脆弱性の分析･評価の結果と補完措置の実施計画に関する事項
  - コンピュータセキュリティインシデントと情報セキュリティ関連規定違反の処理に関する事項
  - その他の情報保護委員会の情報セキュリティ業務の遂行に必要と定めた事項
- 最高経営責任者（CEO）は、特別な事情がない限り、情報保護委員会の審議･議決事項を遵守しなければならない。

金融委員会（FSC）は 2013 年（平成 25 年）7 月に、金融機関のサイバーセキュリティ保護のための取組み強化策として、「金融電算セキュリティ強化総合対策」、同年 10 月には、「個人情報流出再発防止総合対策」を発表した。金融機関には、これらの強化策として次の様な事が求められている。

1) 金融サービスに関わる情報システムは、インターネットなど外部と通信を行うネットワークと物理的に分離する
2) 資産 10 兆ウォン以上または従業員 1,500 人以上の金融機関は、専任の最高情報セキュリティ責任者（CISO）を設置する（兼職 CISO の禁止）
3) データバックアップ専用に使用するデータセンターなどの施設を設置する
4) （韓国）金融 ISAC（6.3.2 参照）の中でセキュリティインシデントへの対応と分析のためのチームを設置する
5) 全ての金融機関にリアルタイム監視の体制を構築する
6) 不正取引検知システム（FDS）[149]の導入を推進する

c) サイバーセキュリティ取組態勢

金融機関のとるべき態勢として、電子金融取引の監督規制 において次のように規定されている。

- 金融機関における IT 担当者数は、全従業員総数の 5%以上、そのうち情報保護担当者数は、IT 担当者数の 5%以上で編成すること
- IT セキュリティ予算は、IT 予算総額のうち 7%以上を投下すること。

実際には、金融機関における IT 人材はアウトソーシング要員も含んでおり、大多数の IT 担当者および情報保護担当者がアウトソーシングの形で雇用されている場合も見受けられる。

IT 担当者の従業員比率規制は、銀行では 100%、証券では 89%、保険では 96%が遵守している。

d) 人材の育成

電子金融取引法（Electronic Financial Transaction Act: EFTA）、および電子金融監督規定により、金融機関は、電子金融取引の監督規制に基づいた従業員の雇用と教育を実施しなければならない。

e) ガイドラインでの具体的なサイバーセキュリティ対策

金融機関で発生したセキュリティインシデントの中には、従業員やアウトソーシング人材など内部関係者が介在した情報漏洩が非常に多く含まれている。金融機関では、これを防止するために、内部統制と従業員への教育を義務化する検討がなされている。

近年、FinTech[150]が急速に発達してきており、金融取引を行う際に支払い方法を簡素化出来るなどの利点があるが、一方でセキュリティの確保が懸念されている。

個人情報の保護に関して以下のような一般的な要求事項がほとんどの金融機関に適用されている。

1) 必要最低限の個人情報のみを収集する
2) 重要な個人情報（固有の識別情報、パスワードなど）は暗号化する
3) データベースのアクセス制御を強化する（権限分掌など）

149「11.用語の説明」参照
150 Financial Technology の意味の造語で IT を活用した金融サービスを提供する事業領域および産業分野。

4） 不必要な個人情報を迅速に破棄する
5） インターネット回線など外部のネットワークと金融機関のシステムを分離する

また、電子金融取引の監督規制においては、DDoS 攻撃のような機能停止に対する総合的な防衛策として、金融機関において以下のような施策を講じることが目標とされている。

- DDoS 攻撃対応システムを導入し、24 時間 365 日サイバー攻撃を監視する。
- 年 1 回以上、サイバー攻撃の模擬演習を実施する。
- 韓国金融決済院（KFTC）と Koscom による共同事業である（韓国）金融 ISAC と連携し、サイバー攻撃への対応とセキュリティ監視、情報共有･分析機能の実施を迅速に行う。

同規制において、金融機関は顧客向けサービスの保護策として、デジタル証明書の再発行時または 300 万ウォン（32 万 7,000 円）[151]以上の資金調達時に本人確認の手続きをより強化するために不正検知サービスの導入や乱数表、またはワンタイムパスワード、携帯電話のテキストメッセージや電話による認証などのセキュリティ強化を実施することが求められている。

また、電子金融取引の監督規制 では、金融機関やネット系金融機関が情報システムへのマルウェア感染を防ぐために以下のような対策を講じることを求めている。

1） アプリケーションを使用する場合は、事前にマルウェアの検出プログラムなどでシステムを診断および修復する
2） マルウェアの検出および修復用プログラムにおいては、パターンファイルを最新の状態に維持する
3） マルウェア感染に備えて回復手順を用意する
4） 重要な端末は、マルウェアに感染していないか毎日チェックする
5） 金融機関またはネット系金融機関は、マルウェア感染が発見された場合、拡散と被害を最小限に抑えるために必要な措置を迅速にとる

金融機関向けの参考情報として、以下のガイドラインを公開されている。

- 「スマートフォンによる金融取引のセキュリティガイドライン」
  - アプリケーションの設計からシステム管理まで、業務手順ごとにセキュリティ保護の具体策を提示
- 「金融機関でのクラウドコンピューティング環境でのセキュリティガイド」
  - クラウドコンピューティング環境を使用した場合のセキュリティ保護のためのガイドラインを提示
- 「金融機関におけるスマートワークのための情報保護のガイドライン」
  - スマートワーク[152]環境の構築の際の機密保護策を提示
- 「金融機関における無線 LAN に関するセキュリティガイド」

---

151 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 韓国ウォン=0.109 円として換算。
152 韓国政府が推進している、IT を活用したして勤務場所や時間に囚われない柔軟な勤務形態。勤務時間は場所の柔軟性によって、自宅で働く在宅勤務、自宅近くの遠隔事務所に出勤するスマートワークセンター勤務、スマートフォン等を利用した移動勤務の 3 つに分けられる。

- ◆ 金融機関が無線 LAN を利用したシステムを構築する際に考慮すべき事項を提示

● 「電子金融取引の認証方法の安全性ガイドライン」

- ◆ デジタル証明書以外の安全な認証手続きを設計する方法

6.3. 金融機関によるサイバーセキュリティ対策への取組み

ここでは、銀行、証券、保険といった金融に関わる各種事業の運営体である金融機関によるサイバーセキュリティへの取組みについて説明する。

6.3.1. 人材の育成

金融監督院（FSS）および金融セキュリティ機関（FSA）（2015 年初頭に金融保安院（FSI）として改組、6.2.2 参照）は、金融分野におけるセキュリティ専門人材の養成と教育のため、セキュリティ研究者らが私設で民間の金融情報の保護に関する専門のアカデミーを運営しており、情報保護の修士課程を開設している大学院とも教育プログラムの連携などの協力体制を構築している。

また、金融機関の役員は 3 時間以上、IT 担当者は 9 時間以上、情報セキュリティ担当者は 12 時間以上の情報セキュリティの教育を毎年履修するよう規定されている[153]。

2012 年（平成 23 年）以降、毎年 7 月を「情報保護の月」として指定し、金融委員会（FSC）と金融監督院（FSS）によって金融セキュリティセミナーが開催され、大学生 100 人を対象として、2 泊 3 日の金融情報セキュリティ・キャンプが実施されている。

6.3.2. 金融機関のセキュリティ関係組織との連携体制

a) 情報共有のための組織

● （韓国）金融 ISAC（Financial ISAC）

- ◆ 韓国金融決済院（KFTC）と Koscom が共同で業務を行っており、韓国の金融業界における情報共有のための組織として、最新の攻撃手法などに関する機密の情報などの共有を行っている。
- ◆ 2001 年に施行された「情報通信基盤保護法」に基づき、2002 年に当時の財政経済部と金融監督委員会により、①証券系 IT 企業である Koscom、②金融決済機能やインターネットバンキングの電子認証業務を行っている韓国金融決済院（KFTC）、の2つの組織が（韓国）金融 ISAC として指定されており、会員企業や政府機関から収集した最新のサイバー脅威の情報を共有している機関。
- ◆ すべての金融機関は、（韓国）金融 ISAC と連携して情報の共有等を行うことが義務付けられている[154]。

---

153 "Regulation on Supervision of Electronic Financial Transactions, FSC Public Notification No. 2013-39, Dec 3, 2013" – Article 37-4 (Designation of Scope of Work of Computer Security Incident Response Teams. etc.)

154 "Regulation on Supervision of Electronic Financial Transactions, FSC Public Notification No. 2013-39, Dec 3, 2013" – Article 37-4 (Designation of Scope of Work of Computer Security Incident Response Teams. etc.)

● 韓国インターネット振興院（KISA）

◆ 6.2.2 参照

➢ KrCERT/CC（Korea National Computer Emergency Response Team）

◆ 韓国国内における情報セキュリティ対策のための専門組織として、韓国インターネット振興院（KISA）配下に設置されている国家的な CSIRT である。韓国国内のサイバー攻撃の防止や情報システムの保護、インターネットにおけるサイバー攻撃への対応を行うほか、各国の CSIRT との情報連携を行っている。

b）情報共有のための体制

政府と民間企業、民間企業同士の間では、既にサイバーセキュリティに関する情報の共有や組織連携は活発に行われている。

また、金融業界内での国内のセキュリティ情報の共有や脅威の解析、セキュリティインシデント対応などについては、（韓国）金融 ISAC が行っている。

政府と民間企業におけるサイバーセキュリティ対策に対する情報共有の仕組みとして、金融監督院（FSS）と韓国インターネット振興院（KISA）などが金融情報の保護セミナーを定期的に開催しており、このセミナーには金融機関の CISO やセキュリティの専門家 200 人余りが参加し、セキュリティ対策の課題などについて情報を共有している。また規制当局側からも関係者が参加し、解決策を模索するワーキンググループが開催されており、効果的な情報共有の機会となっている。

更に、金融監督院（FSS）は、サイバー攻撃を受けるなど有事の際のトリアージのポリシーについて、金融機関の点検やレポートを受け付け、情報収集を行っている。また、セミナーを通じて金融機関の意見を集約、議論をしながら、最適解の検討を行っている。これらの情報は関係者内で分類され、金融機関向けガイドラインの形で情報の提供に活用される。

金融分野におけるサイバー攻撃対策や金融犯罪対策のための国際的な情報連携については、いくつかの試験的な取組みがなされているが、共同連携のフレームワークが確立しているという状況には至っていない。

韓国国内の連携に関しては、国家サイバー安全センター（NCSC）と韓国インターネット振興院（KISA）、金融監督院（FSS）とその関係機関が、技術研究、人材教育、人材交流に関する協力体制を備えている。

その他、韓国インターネット振興院（KISA）と行政自治部は、民間/公共機関を対象にしたセミナーやレポートなどによる情報の収集を行っている。この情報共有の仕組みを活用してサイバー被害を最小化した実例はまだ無いものの、今後のさらなる活用には官民から期待が寄せられている。

このほかに各金融機関は、独自の正常セキュリティ監視体制を構築することが義務付けられており[155]、その結果を定期的に経営陣に報告しなければならない。

サイバー攻撃の手法などに関する情報は、主にセミナーなどの機会を利用して共有されている。

6.3.3. 関係組織との国際連携

韓国国外の組織との連携に関しては、韓国インターネット振興院（KISA）がセミナーやワークショップを開催したり、国外機関との国際協力体系を備えたりしており、多数の外国侵害事故対応チームと協力体制を構築している。一般的に金融機関は、韓国インターネット振興院（KISA）を介して国外のセキュリティインシデントと脅威の動向について予防対策などの情報を得ている。

韓国では、近年、不正なコードの実行や、フィッシング、モバイルアプリケーションの改竄などによる個人情報や認証情報の窃取の事例が急増したため、金融監督院（FSS）は、金融犯罪の実態、脅威の分析、先進的な取組みなどについて、国外の機関と連携してガイドライン（**エラー！参照元が見つかりません。**参照）を発表した。また、これらの不正取引の検知システム（Fraud Detection System: FDS）を構築し、独自に検出された検出情報を金融機関と共有するシステムを備えている。

金融犯罪への対抗措置や対抗事例（犯罪の特定や検挙）としてよく知られているものとして、2011 年（平成 23 年）に発生した中央選挙管理委員会への DDoS 攻撃が挙げられる。2011 年（平成 23 年）の補欠選挙当時、中央選挙管理委員会の Web サイトが DDoS 攻撃を受け 2 時間利用出来なくなった。この時は、韓国インターネット振興院（KISA）が中央選挙管理委員会の Web サイトにおける DDoS 攻撃の兆候を検知した。サイバー警察捜査隊と協力して攻撃元 IP アドレスを分析し、マルウェアに感染した PC を一早く発見した後、IP のトレースバック技術を用いて犯罪者を識別し、拘束するに至った。

6.4. 有事における対応

6.4.1. サイバー攻撃やテロに対する官民の対応態勢

金融分野におけるセキュリティインシデント発生時の対応態勢として、韓国金融決済院（KFTC）、Koscom または金融委員会（FSC）が指名する機関は、金融分野横断的な CSIRT としての機能を提供しなければならない。さらに（韓国）金融 ISAC（韓国金融決済院（KFTC）と Koscom で構成される機関）と金融分野のセキュリティ研究者はサイバー脅威に対するインシデントを分析し、報告することが求められている。（前出の電子金融取引の監督規制 37-4、6.2.3 参照）

155 “Regulation on Supervision of Electronic Financial Transactions, FSC Public Notification No. 2013-39, Dec 3, 2013” – Article 37-4 (Designation of Scope of Work of Computer Security Incident Response Teams. etc.)

上記の金融分野横断的な CSIRT は、次の業務を行う事が求められている。

1) サイバー攻撃に関する情報の収集･伝達のための情報共有システムの構築
2) サイバー攻撃の予報･警報発令の内容の伝達
3) サイバー攻撃の原因分析と迅速な対応と被害拡散防止のために必要な措置の実施

また、全ての金融機関は、金融委員会（FSC）の「金融およびコンピュータ部門の緊急対応マニュアル」に準拠しなければならず、セキュリティインシデントが発生した金融機関は、約 2 週間程度の金融監督院（FSS）による特別監査を受けなければならない。そして、金融監督院（FSS）は、特別監査の結果をまとめて、金融委員会（FSC）に報告した後、金融委員会（FSC）は当該金融機関に対して改善勧告を行う。（6.2.2 参照）

実際に 2013 年（平成 25 年）3 月 20 日に発生したパッチプログラム更新システムの乗っ取りによる ATM などの大規模なシステム停止を招いたサイバー攻撃[156]の後、金融監督院（FSS）は、セキュリティの専門家で構成されるタスクフォースを構成し、金融機関に対する総合点検を実施した。

金融委員会（FSC）および関連機関は、金融分野のセキュリティのコントロールタワーの役割をする金融コンピュータセキュリティ協議会（Financial IT Security Council）を設置した。金融コンピュータセキュリティ協議会には、多数の金融機関が参加して、セキュリティ関連の問題を共有している。

6.4.2. 政府または業界として取組んでいるサイバー攻撃への対応演習

金融機関やネット系金融機関は、最低年 1 回の緊急時対応演習を実施し、その結果を金融委員会（FSC）に報告しなければならない。

金融委員会（FSC）は、金融分野の緊急対応能力を強化するために、金融機関またはネット系金融機関を選別して、金融分野合同の緊急時対応演習を実施することがある。

金融委員会（FSC）は、合同演習を実施する際に、次の機関に支援を要請することがある。

1) 国家情報院（国家サイバー安全センター）
2) 警察庁（サイバーテロ対応センター）
3) 侵害事故対応機関
4) 他に緊急時の対応演習の実効性確保のために、金融委員会（FSC）が必要と認めた機関

合同演習は、実際に発生する可能性が高い攻撃を想定して行われており、独自に開発した攻撃のシナリオに基づいて演習が行われる。Web 脆弱性攻撃、サーバとネットワークへの攻撃、マルウェアやフィッシングメール、DDoS 攻撃などで構成されている。

156「10.資料」参照

6.5. 最近のサイバー攻撃の動向

現在、韓国において特に懸念されている金融に関するサイバー攻撃の手口、攻撃者の特徴、攻撃事例や日本において同様の被害が発生しうる可能性は次の通りである。

2013 年（平成 25 年）3 月に、システム運用会社のセキュリティパッチ配信システム（Patch Management system: PMS）が乗っ取られた。その結果、このシステムからセキュリティパッチの配信を受けている多数の企業のシステムが一斉にダウンし、合計で約 48,700 台の PC やサーバが再起動出来ないという被害の報告を受けた[157]。このマルウェアはハードディスクのブートレコード（システムを起動するプログラムの領域）を破壊するなどの攻撃を行い、システムが起動できない状態を引き起こすものだった。結果的に、金融機関、報道機関などの主要なコンピュータ・ネットワークネットワークが麻痺する大惨事を招いた。ある金融機関では、PC 2 万台と ATM、PC など数百台が機能不全となり、約 5.45 億ウォン（5940 万円）[158]の損害につながった。

インターネットバンキング利用者（顧客）の PC、モバイル機器などにマルウェアを感染させた後、金融機関の Web サイトに似せたフィッシングサイトに誘導し、顧客の口座番号やパスワードなどの重要な情報を窃取して不正に送金するなどの事案が発生している。このような事案ではいくつかの巧妙なソーシャルエンジニアリングが使われており、1 人当たり数千万ウォンに達する被害が発生した。

最近の韓国国内でのサイバー攻撃では、大部分が個人情報の漏洩を目的としている。金融機関が保有するサーバやコンピュータにマルウェアを感染させ、そこから情報を盗み出す事案が多く発生しており、数百件から数千万件の個人情報が漏洩した事案が報告されている。

最近では、マルウェアを使用して、PC と Web サーバの間で行き来する Cookie[159]などの情報を窃取して通信プログラムを改竄し特定のページに利用者を誘導する事案が発生しており、合計 1,200 万人の個人情報が漏洩した例がある。このような事案では、送信区間の暗号化など基本的な措置が行われていない場合もある。

規制当局として認識しているサイバー攻撃の脅威に関わる優先順位は、攻撃の種類に応じて分類しているわけではない。国家サイバー安全センター（NCSC）がリアルタイムにサイバー脅威を分析し、その都度、必要なレベルの警報を発令している。

サイバー脅威の警告段階は、次の 5 つに分類される

1) 正常:低リスク。ワーム、ウィルスウィルスの発生など。

157 http://itpro.nikkeibp.co.jp/article/COLUMN/20130328/466648/
158 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 韓国ウォン=0.109 円として換算
159 Web サーバと Web ブラウザ間で状態の管理をするために Web ブラウザに保存される情報のことを指す。ユーザの識別やセッションの管理のために使用される。

2) 注目:国外のサイバー攻撃の被害の拡散またはハッキング等による被害発生の可能性の増加。検出活動の強化が必要。
3) 注意:一部のネットワークと情報システムにおいて障害が発生。セキュリティ体制の強化が必要。
4) 警告:多数の情報通信サービス提供者(ISP)のネットワーク障害の発生。いくつかの機関との協力対応が必要。
5) 深刻:国家レベルでのネットワークや情報システムの利用不可。大規模な被害が発生。国家レベルの共同対応が必要。

ここ数年のサイバー攻撃では主に金融機関、通信事業者、政府機関を対象とした個人情報の窃取を目的とする攻撃が多く発生している。また、APT、マルウェア、およびゼロデイ攻撃だけでなく、内部者による情報漏洩事例も頻繁に生じている。その他、メディア、金融機関を対象とした計画的な機能停止などのマルウェア攻撃なども発生している。

6.6. サイバー保険の動向

サイバー攻撃による組織での損害を補償するサイバー保険の市場規模、補償の対象となる範囲、採用状況は、次の通りである。

6.6.1. サイバー保険の市場規模

韓国におけるサイバー賠償責任保険(Cyber Liability Insurance, CLI)の市場規模は、正味収入保険料で、おおよそ 78.8 億ウォン(日本円で 8 億 6,000 万円[160])程度と見込まれる。

金融機関においては、強制保険への加入が求められている。

- 強制保険
  - 電子金融取引: 54.5 億ウォン
  - 公認電子文書保管所: 1.8 億ウォン
- 任意保険(強制なし)
  - 個人情報の漏洩: 4.3 億ウォン
  - e-Biz: 8.3 億ウォン

CLI 保険料の総額は、損害保険全体の保険料 51.4 兆ウォンの 0.015%の水準に過ぎなかった

2013 年度(平成 25 年)に 53 の金融機関が納付した電子金融取引賠償責任保険料は約 43 億ウォン程度減少した。

6.6.2. サイバー保険の補償範囲

160 2015 年(平成 27 年)3 月時点でのおよその為替レート1 韓国ウォン=0.109 円として換算。

韓国で一般的に活用されている CLI 保険は、以下のような範囲を補償している。主に第三者と利用者保護のための損害賠償を補償したものである。

1) データの復旧および代償費用
2) 個人情報の漏洩による損害賠償費用
3) ネットワークの安全性確保の障害による損害賠償費用
4) 盗まれた情報が公的に漏洩した場合の損害賠償費用
5) ハッキング、ウィルス関連の損害賠償費用
6) 技術的な誤りや不注意で起こった損害賠償費用

6.6.3. サイバー保険の採用状況

個人情報漏洩事故の増加や個人情報保護法の施行に伴い、個人情報の漏洩に伴う賠償責任保険を中心として、サイバー保険の市場が形成されている。

証券会社および損害保険会社の個人情報の漏洩賠償責任保険への加入率は 100%であるが、その他の金融機関での加入率は約半分程度である。

最近の保険研究機関による報告では、今後の非金融事業者の加入を想定すると、最大 820 万の事業者が賠償責任保険に加入する見込みであるとの見方がある。しかし、「利用規約に様々な免責事由を含む」、「損害発生の事例が不足している」、「損害賠償は低額なものが多い」、「補償の対象とするリスクの多様性が不足している」など CLI の普及を阻害する要因もある。

■ 7. 欧州連合の金融分野のサイバーセキュリティ対策

7.1. 概要

本章では、欧州連合（EU）における金融分野でのサイバーセキュリティ対策への取組みとして、欧州連合より、どのような方針が示されているか、どのような法制度が制定されているか、法制度に基づいてどのような監督機関が規制当局として設置されているか、また、規制当局から金融機関に対してどのような順守要件が示されているか等について示す。さらに、規制当局から求められる要件への適合のみならず、金融機関自身もしくは業界全体としての自主的な取組みとして、どのようなことが実施されているかなどについても示す。

7.2. 監督機関によるサイバーセキュリティ対策への取組み

ここでは、銀行、証券、保険といった金融に関わる各種事業に対する監督機関によるサイバーセキュリティへの取組みについて説明する。

7.2.1. 法制度や国家戦略

a）地域戦略

欧州連合（EU）においては、自然災害やテロ等に加え、経済スパイや国家支援によるサイバー攻撃という国境を越えた新たな脅威により、サイバーセキュリティインシデントの頻度・規模が増大し、ヘルスケア、電力や自動車等の重要サービスの供給が破壊されるなど国家の安全や経済に多大な損害を及ぼし得るという認識の下、2013 年（平成 25 年）2 月に、サイバー攻撃等の予防や対応に関する包括的な将来像を示した「EU サイバーセキュリティ戦略（Cybersecurity Strategy of the European Union）[161]」が公表された。

これに先立って、2004 年（平成 16 年）には、サイバーセキュリティ対策の専門機関として、欧州 ネットワーク情報セキュリティ庁（European Network and Information Security Agency: ENISA）が設立され、それ以来、情報システム、サービス、ネットワークを含む ICT インフラの保護に関する政策や法整備が、欧州 ネットワーク情報セキュリティ庁（ENISA）によって大規模に進められている[162]。

サイバーセキュリティに対する一貫したアプローチをとるために、全体的な戦略は欧州連合（EU）と各加盟国の組み合わせで取り組んでいる。戦略の一環として欧州連合（EU）の議会は欧州 ネットワーク情報セキュリ

161 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
162 http://www.enisa.europa.eu/about-enisa

ティ庁（ENISA）を強化するための法案を提案し、ネットワークおよび情報セキュリティ（NIS）に関連する方針を開発している。

また、2012 年（平成 24 年）には、コンピュータ緊急対応チームとして、CERT-EU を設立し、また、サイバー犯罪と闘うために、欧州サイバー犯罪センター（EC3, 後述）を設立した。

欧州連合（EU）の全体的な戦略では、サイバー攻撃に対して法執行機関や防衛機関と共に活動するための官民のパートナーシップに特化した機関の設立が求められている。

b）サイバーセキュリティ戦略の実施項目[163]

EU サイバーセキュリティ戦略の中では、基本的権利、民主主義、法の支配という欧州連合（EU）の原則がサイバー空間でも守られるように、加盟国政府とデジタル市場の担い手である民間企業の双方が果たすべき役割があるとしている。

サイバー妨害や攻撃に対して防御し対処するために、欧州連合（EU）が優先的に取り組むのは次の 5 つの分野である。

1） サイバー態勢を構築する

攻撃の影響をできる限り抑えるために、攻撃に対する耐性、回復力を備えておくことが重要である。そこで欧州委員会は、「ネットワークと情報セキュリティ（Network and Information Security: NIS）指令[164]」を作成した。また、2004 年（平成 16 年）には欧州 ネットワーク情報セキュリティ庁（ENISA）を設立した。2012 年（平成 24 年）には、欧州委員会をはじめとする EU の各関係機関の IT セキュリティ専門家で構成される、「コンピュータ緊急対応チーム（Computer Emergency Response Team: CERT-EU）」が発足している。各業務の階層ごとに、サイバー攻撃時の協力体制のシミュレーション演習や、利用者の意識を高める啓発活動を行っている。

2） サイバー犯罪を激減させる

サイバー犯罪は世界で最も急速に拡大している犯罪の形態で、1 日に世界で 100 万人以上が被害にあっていると言われている。法体制を整えることも重要な対策の一つであり、「サイバー犯罪に関する条約」（2004 年（平成 16 年）7 月 1 日発効）が各国での法制定に拘束力のある国際的な取り決めとして締結されている。日本もこの条約に署名し、2012 年（平成 24 年）11 月 1 日より有効となっている。

欧州連合（EU）では、最新技術を使って行われるサイバー犯罪に対応する手段として、2013 年（平成 25 年）1 月、オランダのハーグにある欧州警察機関（ユーロポール）内に、「欧州サイバー犯罪センター（European Cybercrime Centre）」を開所した。同センターは分析や諜報、調査、資料作成、加盟国の警察組織や民間部門、その他関係者との情報共有や捜査支援などを行う欧州の中心機関として機能している。

163「駐日欧州連合代表部」Web ページを元に作成
164 http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=1666
http://qed.eu/files/Jakub_Boratyn%CC%81ski.pdf
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015639%202014%20INIT

3)　共通安全保障・防衛政策に関するサイバー防衛政策・能力を確立する

防衛の分野では、検知および高度なサイバー脅威に対する対応と復旧に焦点を当てる。脅威は多面的であるため、民間と軍部双方の対策の相乗効果が期待される。欧州連合（EU）は、北大西洋条約機構（NATO）と共に重複を避けて相互補完し、EU および NATO のそれぞれの加盟国の防衛能力と情報インフラの強化に努めている。また、EU 外務・安全保障政策に関する上級代表が、加盟国と欧州防衛機関に対し、演習や情報共有などでの協力を呼びかけている。

4)　サイバーセキュリティに向けた産業・技術資源を確保する

革新的な ICT 製品は欧州連合（EU）域外で製造されていることが多く、欧州連合（EU）では、域内製のまたは第三国製のものについてはどちらであっても、信頼性が高く安全で個人情報の保護が保障されるハードウェアやソフトウェア、インフラ、モバイル端末を調達する方針である。また欧州連合（EU）は、単一の市場で一貫したアプローチをとり、地域差が開かないようにしている。そのために、セキュリティの標準化やクラウドコンピューティングの認証制度などに対する支援を行っている。信頼のおける欧州の ICT 産業を育成し、外国技術依存を減らすべく、「ホライズン 2020[165]」という研究資金の助成の枠組みなどを最大限に利用して研究開発を進めている。

5)　首尾一貫した EU の国際サイバー空間政策を確立し、EU の価値を促進する

欧州連合（EU）の対外関係や共通外交・安全保障政策の中心にサイバーセキュリティを組み入れ、サイバー空間においても自由と基本的権利が守られるようにしている。EU 加盟国政府のほか、民間企業、市民、第三国、国際機関など、あらゆるパートナーと対話・協力を行っていっている。また、第三国のサイバーセキュリティの能力強化や耐久力のある情報インフラ構築も行っている。

c）人材の育成

サイバーセキュリティに関して、規制当局および金融機関における人材の育成計画や教育機関との連携体制として、EU サイバーセキュリティ戦略の中で実施されている活動の一つとして、「ネットワーク情報セキュリティ（Network and Information Security: NIS）の教育と演習」がある。この活動の一部として、欧州 ネットワーク情報セキュリティ庁（ENISA）は Web サイトの管理者などの能力向上を促進し、高いネットワーク情報セキュリティに関するスキルと専門性をもった IT 専門家を認定する、ネットワーク情報セキュリティ認定プログラム[166]の設立を計画している。

金融機関におけるサイバーセキュリティ要員の育成計画や採用計画：

- EU 圏内の金融機関におけるサイバーセキュリティ要員の育成計画や採用計画は各組織に依存し、業種によってその内容は様々である。しかしながら、求められているスキルの不足が業界の主要なギャップの一つであり、重要な焦点として今後の投資の領域として認識されている。

165 http://ec.europa.eu/programmes/horizon2020/

166 https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe/at_download/fullReport

d) サイバーセキュリティに関する政策や関連法令[167]

サイバーセキュリティに関連する法令や戦略として次のようなものがある。

- 情報社会政策「欧州デジタル・アジェンダ（Digital Agenda for Europe）[168]」 2010 年（平成 22 年）制定
  - 欧州連合（EU）の成長戦略「欧州 2020（Europe 2020）[169]」（2010 年（平成 22 年）3 月策定）に掲げた 7 つの主要事業のうちの 1 つである。
  - 同事業は、2020 年（平成 32 年）までにインターネットを基盤とする経済活動（デジタル経済）を繁栄させ、デジタル革命の恩恵を全ての人に広めることを目的とするもので、①デジタル分野の市場統合、②標準規格及び相互運用性の改善、③インターネットの信頼性及び安全性の向上、④インターネットアクセス確保と高速化、⑤最新技術の研究開発、⑥デジタルデバイドの解消、⑦多目的な技術開発の 7 つの目標を掲げている。
  - 欧州委員会によれば、デジタル経済はそれ以外の分野に比較して 7 倍の速度で成長しているものの、加盟国全体の政策について枠組みが統合されていないために成長の潜在能力が発揮出来ていない。また、情報通信技術の利用の爆発的な伸びは、生産やサービスの在り方を大きく変えてきているが、一方で、サイバー犯罪等の脅威も増してきているとしている。

- 「EU サイバーセキュリティ戦略（Cybersecurity Strategy of the European Union）[170]」 2013 年（平成 25 年）
  - ネットワーク情報セキュリティ（Network and Information Security: NIS）関連の指令提案を含む

- 「EU におけるクラウドコンピューティングの潜在力の解放（Unleashing the Potential of Cloud Computing in Europe: 欧州クラウド戦略）」 2012 年（平成 24 年）

- サイバーセキュリティに関する EU 指令
  - ➢ サイバーセキュリティに関する EU 指令（EU Directive）[171]の提案が 2014 年（平成 26 年）3 月に欧州委員会によって承認され、現在具体化に向けた審議中である。なお、独国等は本指令の導入を先行して進めている。

7.2.2. 金融に関わるサイバーセキュリティの関連組織

167 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/n4b00000.pdf
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc132120.html
168 http://ec.europa.eu/digital-agenda/
169 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF
170 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
171 http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and

a) 組織と位置付け

欧州連合（EU）において地域レベルでのサイバー空間のセキュリティの確保やインテリジェンス（多面的な情報解析）に関連する組織として、主なものは下記の通りである。

- 欧州 ネットワーク情報セキュリティ庁（European Network and Information Security Agency: ENISA）
  - 欧州 ネットワーク情報セキュリティ庁（ENISA）の役割は、次の通りである。
    - 各加盟国が、強固な国家サイバーセキュリティ回復力を開発することを支援する
    - 定期的な欧州全体のサイバーインシデント演習を実施する際に、各加盟国および EU 機関を支援する。
    - CERT-EU を一括管理する。
  - 欧州 ネットワーク情報セキュリティ庁（ENISA）は、欧州連合（EU）域内において、EU 加盟国に対する牽引役であり、サイバーセキュリティ対策の中央拠点としてとして機能している。
- 欧州サイバー犯罪センター（European Cyber Crime Center: EC3）
  - 2013 年（平成 25 年）にオランダ・ハーグにある欧州警察機関（Europole）内に設置された。
  - 専門知識と情報を持ち寄り、犯罪捜査を支援し、EU 全体としての解決策を推進して、欧州連合（EU）内のサイバー犯罪への対処法を大きく転換させるための機能として位置付けられている。
- 欧州刑事警察機構（Europol）
  - 国際犯罪やテロのために加盟国を支援する組織であり、欧州の法執行機関である。
- 欧州防衛機関（European Defence Agency: EDA）
  - サイバーセキュリティに関する防衛力を改善するための新しい取り組みやソリューションの推進、開発等を行う。
- コンピュータ緊急対応チーム（Computer Emergency Response Team EU: CERT-EU）
  - EU の各組織における IT システムのセキュリティインシデントに対する緊急対応を行う組織。

b) 関連部署との連携

欧州 ネットワーク情報セキュリティ庁（ENISA）は、サイバーセキュリティに関する専門性を向上し維持するため、Europol、EDA、CERT-EU のような他の EU の関係機関と共に、極めて密に連携しており、定期的な情報交換のほか、大規模なサイバー攻撃に際には各国のネットワークおよび情報セキュリティ（NIS）機関や各国 CERT とも連携する。

欧州 ネットワーク情報セキュリティ庁（ENISA）は、また、特定の国において国を跨ぐ大きなサイバー攻撃が発生した場合には脅威を評価し、攻撃の影響を緩和するための支援を行う。

欧州連合（EU）は欧州議会と連携して、欧州 ネットワーク情報セキュリティ庁（ENISA）が上記を実現するための具体的な規制を定めている。

また、欧州連合（EU）の加盟国は、加盟国間で大きなサイバー攻撃と闘う為に、「テロや人的もしくは自然災害」などの際の加盟国間の相互援助を約束した、連帯条項（Solidarity Clause）[172]を行使することができる。

172 http://eumag.jp/question/f1013/

7.2.3. 検査監督のガイドライン

- 金融機関向けのサイバーセキュリティに関連するガイドラインとしては、次のようなものがある。ヨーロッパ中央銀行（ECB）のガイドライン
  - ➢「インターネット決済のセキュリティ勧告（Recommendations for the Security of Internet Payment）[173]」
    - インターネット決済におけるセキュリティ強化の為の要件が勧告として提供されている。

7.3. 金融機関によるサイバーセキュリティ対策への取組み

7.3.1. 経営陣の発表

金融機関におけるサイバーセキュリティ戦略と経営陣のコミットメントとして、欧州連合（EU）における金融機関の経営陣によるサイバーセキュリティに関する公式なコミットメントは発表されていない。

一方で、ドイツなど一部の EU 加盟国では、金融機関の経営陣がサイバーセキュリティ対策にコミットすることが義務化されることになっている。

欧州連合（EU）域内では、金融機関が参加する公式または非公式のフォーラム（評議会）が数多く開催されており、こういった業界の情報交換の場において、他の EU 加盟国における、より積極的なサイバーセキュリティ対策の事例の紹介や、サイバーセキュリティ対する知見の共有などが行われている。

EU 加盟国における主要な金融機関の多くでは、サイバーセキュリティ対策の取組みについて既に対応力の向上を図る専門部門を配し、戦略的取り組みを実施しているか、もしくは、そのような積極的な取り組みを計画している。

7.3.2. 金融機関による取組体制

金融機関によるサイバーセキュリティ対策の取り組みの体制として、欧州連合（EU）の加盟国の主要な金融機関のほとんどは、以下の分野に対して投資する計画を表明している。

1) セキュリティオペレーションセンター（Security Operation Center: SOC）
2) 重大インシデント対応センター（Critical Incident Response Center: CIRC）
3) セキュリティ・アーキテクチャ
4) フォレンジックス
5) セキュリティ技術の評価
6) トレーニング

---

173 https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

また、欧州連合（EU）の加盟国の主要な金融機関のほとんどは、サイバーインシデントが発生した場合に、国家レベルまたは EU 全体レベルでの積極的な連携をサイバーセキュリティ対策の実施内容に組み込んでいるか、または組み込む計画が既にあるという状況である。

7.3.3. 金融機関のセキュリティ関係組織との連携体制

a）情報共有のための組織

政府機関と民間企業相互の取組み、金融機関同士の取組み、もしくは、金融機関をふくむ民間企業間相互の情報共有フレームワークとして、次の様なものがある。

- FI-ISAC[174]
  - Financial Institutions – Information Sharing and Analysis Centre
  - 主に民間の金融機関が多数参加する評議会組織で、金融機関への情報共有のための業界団体である。金融分野の政府関係機関、国家 CSIRT 機関および法執行機関で構成される。また、欧州ネットワーク情報セキュリティ庁（ENISA）、Europol、ヨーロッパ中央銀行（ECB）、欧州決済協議会（EPC: European Payments Council）[175]および欧州委員会が参加している。
- CERT-EU
  - Computer Emergency Response Team – Europe Union
  - CERT は、サイバー空間に関する不正アクセス、不正プログラム、システムの脆弱性などに関して、情報を収集し迅速に分析を行い、分析結果について公表共有する専門の組織で、CERT-EU は、EU 加盟国内を対象とした組織。金融機関を含むあらゆる産業分野と連携し、また民間および政府の両方からの情報の共有のための体制を構築している。

EU 加盟国に拠点を置く多くの金融機関は、FI-ISAC に加盟している。

- FI-ISAC は業界団体のフォーラムで、グローバル金融サービス部門に対する重要セキュリティ脅威の協力を行っている。
- EU 全体としては、CERT-EU がサイバーセキュリティインシデントに関して、金融機関などの重要機関との調整や手助けを行っている。

b）相互共有される内容

サイバー脅威を多面的に分析する「脅威インテリジェンス」は、金融機関の組織において注力されている技術分野であり、サイバーセキュリティ対策の戦略の一部である。EU 圏内には、情報共有のための公開フォーラムやコミュニティが多数存在する。

174 https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership
175 http://www.europeanpaymentscouncil.eu/

7.4. 有事における対応

7.4.1. サイバー攻撃やテロに対する官民の対応態勢

a) 過去のインシデント対応の評価と発見事項

EU 圏内の金融機関にとって、欧州 ネットワーク情報セキュリティ庁（ENISA）のサイバーセキュリティガイドラインについては現在のところ遵守義務があるわけではない。しかし、ドイツなどいくつかの EU 加盟国では、サイバーおよび IT セキュリティの関連法令で、金融機関のサイバー攻撃への回復力とサイバーインシデントの管理体制の成熟度合いを検査する仕組みの導入が予定されている。また、フランスやオランダでは、これらのフレームワークを含めた国家サイバーセキュリティ戦略の策定を計画している。

b) 当該組織、金融機関、捜査当局との相互連携のしくみ

- 欧州 ネットワーク情報セキュリティ庁（ENISA）
  - 2004 年（平成 16 年）に設立され、2013 年（平成 25 年）のサイバーセキュリティ戦略制定以降の役割は、次の通りである。
    - 各加盟国が、強固な国家サイバーセキュリティ回復力を開発することを支援する
    - 定期的な欧州全体のサイバーインシデント演習を実施する際に、各加盟国および EU 機関を支援する。
    - CERT-EU を一括管理する。
    - 欧州 ネットワーク情報セキュリティ庁（ENISA）は、EU 域内において EU 加盟国に対する牽引役であり、中央ハブとして機能している。
    - また、欧州 ネットワーク情報セキュリティ庁（ENISA）は、サイバーセキュリティに関する専門性を向上し維持するため、Europol、EDA、CERT-EU のような EU の機関と定期的に情報交換をし、大規模なサイバー攻撃に際には各国の NIS や各国 CERT と連携する。
    - 欧州 ネットワーク情報セキュリティ庁（ENISA）は、また、特定の国において国を跨ぐ大きなサイバー攻撃が発生した場合には、脅威を評価し、攻撃の影響を緩和するための支援を行う。
    - 欧州連合（EU）は、欧州議会と連携して、欧州 ネットワーク情報セキュリティ庁（ENISA）のための上記を実現するための具体的な規制を定めている。
    - また、欧州連合（EU）の加盟国は、加盟国間で大きなサイバー攻撃と闘う為に、「テロや人的もしくは自然災害」などの際の加盟国間の相互援助を約束した、連帯条項（Solidarity Clause）[176]を行使することができる。
- 欧州サイバー犯罪センター（EC3）
  - 2013 年（平成 25 年）にオランダ・ハーグにある欧州警察機関（Europol）内に設置された。
  - 専門知識と情報を持ち寄り、犯罪捜査を支援し、EU 全体としての解決策を推進して、欧州連合（EU）内のサイバー犯罪への対処法を大きく転換させる。

176 連帯条項 - EU 条約における「テロや人的もしくは自然災害」などの際の加盟国間の相互援助を約束したもの。

- 欧州刑事警察機構（Europol）
  - ➢ 国際犯罪やテロのために加盟国を支援する組織であり、欧州の法執行機関である。
- 欧州防衛機関（EDA）
  - ➢ サイバーセキュリティに関する防衛力を改善するための新しい取り組みやソリューションの推進、開発等を行う。

7.4.2. 欧州連合または業界として取組んでいるサイバー攻撃への対応演習

欧州連合（EU）としてサイバー攻撃への対応演習としては、金融機関が単独で参加する形式ではなく、業界横断的に、より広範囲なテーマを掲げ、いくつかのサイバー攻撃対応演習を行っている。

具体的に欧州連合（EU）が行った演習は次のようなものがある。

- Cyber Atlantic 2011 exercise [177]
  - ◆ 主催
    - ▫ 欧州連合（EU）のネットワーク情報セキュリティ庁（ENISA）
    - ▫ 米国の国土安全保障省（DHS）
  - ◆ 開催日時
    - ▫ 2011 年（平成 23 年）11 月 3 日
  - ◆ 対象者
    - ▫ 16 の欧州連合（EU）加盟国と米国から 60 名以上の政府関係者
  - ◆ 目的
    - ▫ 国家間レベルでのサイバー危機発生時の欧州連合（EU）加盟国と米国の連携体制の模索と改善
    - ▫ 米国での危機対応手順を活用したサイバー危機発生時の欧州連合（EU）と米国の連携体制の模索と課題の発見
    - ▫ サイバー危機発生時における欧州連合（EU）各加盟国および米国それぞれの国内ベストプラクティスの意見交換
- Cyber Europe 2010/2012/2014 exercise
  - ◆ 主催
    - ▫ 欧州連合（EU）
    - ▫ 協賛として、欧州ネットワーク情報セキュリティ庁（ENISA）および連合研究センター（JRC）
  - ◆ 開催日時
    - ▫ 2010 年（平成 22 年）11 月 4 日
    - ▫ 2012 年（平成 24 年）10 月 4 日
    - ▫ 2014 年（平成 26 年）10 月 24 日
  - ◆ 対象者
    - ▫ 欧州連合（EU）の政府機関
  - ◆ 目的

177 Cyber Atlantic 2011 - http://www.bic-trust.eu/files/2011/12/slides15.pdf

- 重要情報インフラ保護に関する全欧州規模の演習として 2010 年から開催
- 大規模なサイバー攻撃に対する対応するため欧州の各国間における連携体制を構築する
- 演習開催中、欧州各国政府機関からの参加した専門家らはインターネットや重要オンラインサービスを麻痺させようとするハッカーの攻撃に対して相互に連携して取り組んだ

これらの主な目的は、サイバー犯罪の防止に対する実践的な研究であった。

7.5. サイバー保険の動向

7.5.1. サイバー保険の市場規模

サイバー保険の世界全体での市場規模は、正味収入保険料で、およそ 25 億ポンド（4,500 億円）[178]程度と予想される。このうち、EU 全体としての市場規模は、2016 年（平成 28 年）末までに 4 億ポンド（720 億円）程度に拡大すると予測されている。現時点では、8,000 万 ~2 億ポンド（144 億円から 360 億円）と見込まれる。

178 2015 年（平成 27 年）3 月時点でのおよその為替レート 1 英ポンド=180 円として換算。

■ 8. 各国・地域の制度比較

各国・地域における「サイバーセキュリティ対策」の制度を法令、組織、ガイドライン、組織連携、演習の観点で比較する。各項目については、該当する要素が含まれている内容を網羅的に示した。

分野	具体策	米国	英国	韓国	欧州連合	日本
組織	監督機関およびガイドライン策定に関する主な担当組織	連邦準備制度（FRB）、連邦預金保険公社（FDIC）、通貨監督庁（OCC）、証券取引委員会（SEC）、連邦金融機関検査協議会（FFIEC）	金融行為規制機構（FCA）とイングランド銀行（BOE）	金融委員会（FSC）、金融監督院（FSS）	ヨーロッパ中央銀行（ECB）	日本銀行、金融庁（FSA）、金融情報システムセンター（FISC）
金融分野の法令・ガイドライン	金融分野における法令指針等	金融サービス近代化法、FFIEC IT Handbook、OCIE のガイドライン、NIST Cybersecurity Framework（現時点で義務付けではない）	CBEST 脆弱性テストフレームワーク、金融犯罪ガイドラインサイバーセキュリティに対する 10 ステップ、サイバーエッセンシャルズ、サイバーガバナンスチェック	電子金融取引法、電子金融取引の監督規制 、金融機関のサイバーセキュリティ強化計画、電算機器を使用した関連内部統制模範基準、金融電算セキュリティ標準のガイドライン（義務付け）	ヨーロッパ中央銀行（EOB）のガイドライン EU 指令を現在審議中	銀行法、金融商品取引法、保険業法、金融庁監督指針、金融検査マニュアルなど、FISC 金融機関等コンピュータシステムの安全対策基準、金融機関等のシステム監査指針など
連携組織	国外・地域外との連携	FIRST、国際刑事警察機構（Interpol）				
	国内・地域内の連携	CERT/CC、US-CERT、国家サイバーセキュリティ通信統合センター（NCCIC）、情報共有分析機関（ISAO）、サイバー脅威インテリジェンス統合センター（CTIIC）	CERT-UK、CiSP、ISF、欧州刑事警察機構（Europol）	KrCERT/CC、国家情報院（NIS）、未来創造科学部（MSIP）	CERT-EU、欧州サイバー犯罪センター（EC3）、ISF 欧州防衛機関（EDA）	JPCERT/CC、官民ボード
	情報共有機関	FS-ISAC、Anti-Phishing Working Group	FS-ISAC	（韓国）金融 ISAC	FI-ISAC	（日本）金融 ISAC[179]、フィッシング対策協議会
演習	国家・地域的な演習	Cyber Storm	Cyber Europe	原発サイバー演習	Cyber Atlantic、Cyber Europe	CYDER、CEPTOAR、CIIREX

179 日本における「金融 ISAC」は 2014 年 8 月に設立

金融業界での横断的な演習	CAPP（金融業界団体による実践的な演習）、Quantum Dawn（政府機関による金融事業継続演習）	Waiking Shark（イングランド銀行による金融機関相互連携演習）、Market-wide Exercise（業界横断的な事業継続力向上演習）	Emergency Response Training（業界横断的な危機対応演習）	---	Marunouchi Dawn 1（金融業界団体による実践的な演習）

■ 9. 考察

本調査を通して得られた米国、英国、韓国および欧州連合でのサイバーセキュリティの取組みから、我が国での今後の金融分野におけるサイバーセキュリティ対策として、特に重要と考えられる施策について、ここで考察する。

a) 組織の壁を越えた情報連携の必要性

日本の企業では、組織の壁を越えてサイバー攻撃やサイバーセキュリティに関する情報の連携を強化することが重要と考えられる。

昨今のサイバー攻撃は、単純な愉快犯のようなものから、金融機関のセキュリティ防御策を熟知し極めて高度な専門知識を持つ組織的な攻撃へ、さらには国家の支援を得ていると思われる高次元の攻撃へと移行している[180]。現状においては、攻撃の手口の高度化の速度に対して、防御側の企業のセキュリティ対策が追い付いていない場合が多い。このような状況では、企業がサイバー攻撃を防ごうとしても、単体の組織で太刀打ちできないことは明白である。

米国では、1999 年（平成 11 年）の FS-ISAC 設立以来、既に 16 年もの間、金融業界内で情報が連携されてきた。我が国では、2014 年（平成 26 年）8 月に金融分野におけるサイバーセキュリティの情報共有のための組織として、「金融 ISAC」[181]が設立され業界内の情報連携が始まったところである。運用期間はまだ短いが、会員となった金融機関からは、「自社の人員だけではすぐに解決できない課題でも、金融 ISAC の仲間同士で助け合い、短期間で解決できた。」、「今、自社が受けている攻撃が、自社だけが受けているのか他社も同様に受けているのかを知るだけでも、有効な対策を見出す近道となる。」といった前向きな声が聞かれ、概ね満足度は高いようだ。金融 ISAC の会員となった金融機関は 2015 年（平成 27 年）3 月末時点で 38 社となり、今後も増加する見込みである。

日本人が得意とする「自助・共助・公助」の概念は、サイバーセキュリティの分野においても有効だと考えられる。将来的には情報連携の輪をさらに広げ、同業種の企業だけではなく、官民や異業種間での連携を強化することによって、より早く、より効果的な情報を入手し提供できるようになるはずだ。国際的な情報連携フレームワークの構築も大きな課題となる。

---

180 ベライゾンデータ漏洩/侵害調査報告書(サイバースパイ活動の外部実行者のタイプ)-
http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_ja_xg.pdf
181 http://www.f-isac.jp/index.html

b) サイバーセキュリティ人材の育成の必要性

日本企業では、サイバーセキュリティ対策を適切に推進するため、専門的な能力を有したサイバーセキュリティ人材を確保することが重要と考えられる。

日に日に増大するサイバー攻撃の脅威に対して、防御する側である企業のサイバーセキュリティ人材が不足しているのは世界共通の課題である。米国ではコンピュータ・サイエンスを専攻する学生や受け皿となる研究室などに、政府が奨学金や助成金を拠出するなどして、サイバーセキュリティ人材の裾野を計画的に広げる動きがある。成果が出るまでに数年かかるアプローチではあるが、確実に成果を出しやすい。

日本でも、東京電機大学、会津大学、九州大学などがセキュリティ専攻のコースを設けるなど人材育成の動きがあるが、企業が自社のセキュリティ人材を確保するためにはこれまで以上に人材育成に投資し、産学官の連携を強めることが必要なのではないだろうか。

人材難が深刻なのは技術者だけではない。経営陣の一員として組織のサイバーセキュリティ対策を先導する最高情報セキュリティ責任者（CISO）の適任者を見つけるのが難しいという問題がある。

日本企業が取りうる選択肢は二種類である。時間をかけて社内の人材を CISO として育成するか、外部から CISO に適した経験・スキルを持った人材を採用するかである。社内の人材を CISO として育成する場合、日本企業の役員の大多数は内部からの昇格者であるため、社風と親和性が高いなどの利点があるが、人材の育成には時間がかかる。一方で、外部から CISO に適した経験・スキルを持った人材を採用する場合、素早く対応できるが、絶対数は少なく適任者を見つけるのは難しい。即戦力という意味では、近い将来日本企業の CISO に外国人の専門家が就任するケースも十分考えられる。

c) サイバー攻撃を想定したインシデント対応の演習を繰り返し実施する必要性

日本の金融機関では、来たるべき大規模サイバー攻撃に備えて、インシデント対応の演習を繰り返し実施することが重要と考えられる。

国内でも、既にサイバー攻撃を想定したインシデント対応時の手順書などを整備した金融機関はある。しかし、実際のサイバー攻撃が事前に想定したシナリオと全く同じ手順で発生する可能性は極めて低い。インシデント対応の演習を実施する意義はここにある。演習を繰り返し実施することにより、その都度、手順の不備に気付き、手直しすることができる。また、演習に参加した人には、その経験を基に応用力が養われる。演習を繰り返し実施するうちに、未経験のシナリオにも対応できるようになる。

我が国においていは、2014 年（平成 26 年）10 月には、金融機関 6 社が参加して初回となるサイバー演習「Marunouchi Dawn 1」が開催された。これは日本の金融業界にとって大きな一歩であるが、今後は、演習

の効果を高めるため、より多くの組織が参加することが望まれる。例えば、過去に韓国で実際に発生したようなATM網の大規模停止を想定する場合には、金融機関だけでなく、システム運用会社、ハードウェアベンダー、現金輸送会社、コンビニエンスストア、情報通信会社、規制当局、中央銀行など、より多くの関係機関を巻き込んだ実践的な演習が効果的だろう。

万が一、複数の金融機関が同時にサイバー攻撃を受け、業務機能が停止したり、大量の情報が漏洩したりすれば、単体の企業としてだけでなく、日本の金融システム全体の信頼性を損なうことになる。英国の「Waking Shark」をはじめ、既に数年前から業界横断型のサイバー演習を繰り返し実施している海外の先進事例から学ぶべきことは多い。

我が国では、2020年（平成32年）の東京オリンピック・パラリンピックの開催を控え、関連組織、関連施設、スポンサー企業などがサイバー攻撃の標的になる可能性がある。5年後の2020年（平成32年）には、過去のオリンピック・パラリンピックが開催された時に比べて、サイバー攻撃の手口は確実に進化し複雑化する。まさに未知の領域であり、国家が一丸となって取り組むべきチャレンジとなる。

■ 10. 資料

近年の金融に関する主なサイバー攻撃による事件事故は次の通りである。なお、既に公表されている政府機関のサイバーセキュリティに関する報告書や主要紙等の報道記事を元に作成した。

時期	地域	攻撃の概要	影響
2009 年 7 月	韓国	韓国政府機関の Web サイトへの分散型サービス拒否（DDoS）攻撃が引き起こされた。韓国全土のインターネットが麻痺。	大統領府のサイトを含む、政府機関、銀行、メディアのサイトが 4 時間に渡ってアクセス出来ない状態が発生した。
2010 年 1 月	米国	米国ニューヨーク州の銀行 Suffolk Country National Bank（SCNB）において、オンラインバンキングシステムにハッカーによる侵入があった。SQL インジェクションにより、ID やパスワードの窃取が発生した。	8,300 人分のオンラインバンキング用 ID とパスワードが窃取された。
2010 年 2 月	ラトビア	ラトビア国税庁の電子納税システムがハッキングされた。SQL インジェクションによって、ID、パスワードが抜き取られ、不正侵入された。	個人や企業の情報、納税情報が漏洩した。
2010 年 3 月	米国	運輸保安局（TSA）でテロリストの情報を管理している同局のサーバに対して、元職員が使用を禁止されているソフトウェアを持ち込んでインストールした。ソフトウェアの資産管理は行われていなかった。	実害はなかった。
2010 年 7 月	米国	インディアナ州において、クレジットカードの中央処理装置システムがハッキングされた。SQL インジェクションによって、ID、パスワードが、窃取され、システムに不正侵入された。	クレジットカード情報が窃取された。
2010 年 7 月	米国	米国内の 2 種の ATM 端末がハッキング可能であるとセキュリティのカンファレンスで発表された。インターネットで販売されている ATM の保守用の鍵を入手し、物理的に扉を開け、銀行等が ATM 専用の制御ソフトウェアの脆弱性を利用してシステムに侵入し、スタンドアロン並びにローカル LAN 経由で操作が可能であるとした。	パスワードの入手、預金の引き出し、送金が可能であるとし、ATM メーカーが改善を行った。
2011 年 3 月	韓国	韓国の大統領府などの政府機関やネイバーなどの主要なサービス 40 サイトに対して、分散型サービス拒否（DDoS）攻撃が発生。ゾンビ化したパソコン台数は 11 万 6,000 台に及んだ。	大統領府などの政府機関やネイバーなどの主要なサービスのサービス不能化。マルウェアによって、攻撃終了後ゾンビパソコンのデータ破壊。
2011 年 4 月	韓国	ハッカーが韓国農協の金融システムの管理保守を担当している協力会社社員のラップトップパソコンをハッキングし、ラップトップパソコン経由でマルウェアを金融システム自体に感染させ、金融システムを外部から遠隔操作して攻撃を行った。	韓国農協銀行（韓国最大規模の金融機関）の電算ネットワークのデータが大量に破壊（バックアップデータも同時に削除）され、数日にわたってサービス停止した。3,000 万名の大規模利用者が被害。金融ネットワーク史上初の麻痺状態に陥った。
2011 年 4 月	韓国	韓国最大手の消費者金融業者である現在キャピタルのデータベースが Web サーバの脆弱性を利用して侵入され、顧客の個人情報が漏洩した。	42 万人におよぶ顧客の氏名、住民番号、ローン商品のパスワードが窃取された。

2011 年後半	米国	米国の大手金融機関（Bank of America, JP Morgan Chase, Citi Group など）の Web サイトに対して DoS 攻撃が頻発した。	各種金融機関のサービス機能の停止が生じた。
2012 年 1 月	欧州、中南米、米国	金融機関の預金者にフィッシングメールを送り、コンピュータに MITB マルウェアを感染させ、ブラウザとオンラインバンキングのサーバ間の通信を乗っ取り金融詐欺を行った。いわゆる Operation High Roller 手法による攻撃。	総額で 7,800 万米ドルもの預金が不正に移動し搾取された。
2012 年 7 月	英国	ロンドンオリンピック開催中に、清涼飲料水のオリンピックのプロモーションサイトを語った不正電子メールが送信され個人情報の記入を求める詐欺行為が確認された。また、オリンピックの資金担当責任者を名乗る不正な電子メールにより賞金の準備金のための送金を求める詐欺行為も確認された。	被害の実態は不明。
2013 年 3 月	韓国	ハッカーによる対象ネットワークへの侵入の後、韓国のセキュリティソフト最大手アンラボ（AhnLab）のパッチプログラム更新システム（PMS）の管理者権限が乗っ取られ、ハードディスクの完全削除を含むデータ破壊可能なマルウェアを感染されられた。	同 PMS を導入していた新韓銀行、農協銀行や主要放送局数社のコンピュータシステム合計 4 万 8,700 台が被害を受け、ATMがシステム停止するなどの、大規模な障害が発生した。
2014 年 1 月	日本	警視庁が、2013 年中にインターネットバンキングの ID やパスワードが窃取され、銀行口座から不正に預金が引き出される等の事犯の状況を発表[182]。	不正送金等の発生件数が 1,315 件、被害総額が 14 億円を超えた。
2014 年 6 月～8 月	米国	米国大手銀行（JP Morgan）にサイバー攻撃を受けたことが 8 月に発覚。捜査は現在も継続中。	8,300 万件の個人情報が流出した。
2015 年 2 月	ロシア、米国、ドイツなど	国際的な犯罪者集団「カーバナック（Carbanak）」が 2013 年から世界 30 ヶ国 100 もの銀行、電子決済システム、そのほかの金融機関に標的型の攻撃を行っていたことが判明した。	2 年間に渡るサイバー攻撃により世界 100 の金融機関から 10 億ドルが不正に送金や引き出しが行われた。
2015 年 2 月	日本	警視庁が、2014 年中にインターネットバンキングの ID やパスワードが窃取され、銀行口座から不正に預金が引き出される等の事犯の状況を発表[183]。	不正送金等の発生件数が 1,876 件、被害総額が 29 億円を超えた。

182 http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf
183 http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

■ 11. 用語の説明

本文中で取り上げた主なサイバーセキュリティに関する用語について、ここで説明する。

- BGP（Border Gateway Protocol）
  - インターネット接続サービスを提供している通信事業者間、または大規模なネットワーク接続網を自身で持つ組織では、通信事業者と組織間でのネットワークパケットの通信に用いられる通信プロトコル。
- C&C サーバ（Command and Control Server）
  - バックドアを仕掛けたシステムに対して攻撃指令を出すサーバ。DDoS 攻撃ではボットネットに対して C&C サーバから攻撃対象への攻撃指令を出し一斉に攻撃を開始する。
- CAPTCHA（Completely Automated Public Turing ₸test to tell Computers and Humans Apart）
  - 自動化されたログイン試行プログラムなどによる不正なログインを防止するため、ログインを試みている相手が人間なのかどうかを識別するための画像を表示して読み取った文字を入力させる認証のしくみ。読みはキャプチャ。
- CSIRT（Computer Security Incident Response Team）/CERT（Computer Emergency Respones Team）/CERT（Computer Emergency Readiness Team ）
  - 企業や組織におけるコンピュータシステムやネットワークの保安上の事件事故（インシデント）に緊急対応する組織を意味する。
  - サイバー攻撃が発覚した直後の影響範囲の把握やシステムの正常復旧までの回復業務を専門的に取り扱う。
  - 一般名称は、「CSIRT」であるが、組織の成り立ちの経緯から、CERT 等の名称を用いているものがある。なお、CERT（Computer Emergency Response Team）は、米国 CERT/CC（http://www.cert.org/）の登録商標である。
  - また一般的に各企業や組織単位の CSIRT は国家単位で運営されている CSIRT と連携し、さらに国家単位の CSIRT は国際的な連携がある。
- DLP（Data Loss Prevention）
  - 企業や組織のコンピュータ・ネットワークシステムで運用されている機密の電子ファイルが、企業や組織のネットワークの境界を越えて、外部に漏洩するのを阻止するためのシステム。
- DMARC（Domain-based Message Authentication, Reporting & Conformance）
  - 従前の電子メールの仕様の課題であった送信者成りすましを防止するための仕組みで新しいプロトコル SPF と DKIM を使用する。
- DNS（Domain Name System）
  - インターネットの通信で個々のコンピュータに割り振られたアドレス番号の数値とドメイン名の文字列を変換するための仕組み。
- FDS（Fraud Detection System/Service）
  - 金融決済取引における不正使用などを蓄積したブラックリストや疑わしい利用者特性等の情報から検知し、不正取引を未然に防止するためのシステムやサービス。
- HA インフラ（High Availability Infrastructure）
  - コンピュータシステム等を機器故障や障害でのシステム停止に備えて、予め二組以上の同一システムを並行して稼働させ、故障や障害発生時にはいずれかのシステムが稼働し続けられるようにした構成のシステム。

- IDS（Intrusion Detection System）
  - 企業や組織のネットワークの外部との境界において、不正な侵入をネットワーク上のパケットから検知するシステム。
- IPS（Intrusion Prevention System）
  - 企業や組織のネットワークの外部との境界において、不正な侵入を阻止するシステム。
- Logic Bomb（ロジックボム）
  - ソフトウェア内に意図的に仕込まれたマルウェアで、ソフトウェアを利用中に、ある条件を満たした場合にコンピュータを誤動作させる攻撃。
- SQL Injection（SQL インジェクション）
  - データベースの検索コマンド（SQL）処理の脆弱性を悪用して、データベース内の情報を窃取する攻撃。
- Passive Wiretapping（パッシブワイヤタッピング）
  - ネットワーク上のパケットを盗聴したり、不正にモニタリングしたりするなどして、パケット内の意味のある情報を盗み出す攻撃。
- WAF（Web Application Firewall）
  - Web アプリケーションへの外部からの攻撃や侵入を検知し阻止するためのシステム。ハードウェアとソフトウェアの両方の形態がある。
- War Driving（ウォードライビング）
  - 無線接続可能な機器に感度の高いアンテナなどを接続して、市中のセキュリティ対策の不十分な接続ポイントなどに接続を行う行為。
- アウトオブバンド認証
  - 携帯電話や SMS など、Web ブラウザ以外の通信経路を組み合わせて利用者の認証を行うしくみで、二要素認証を強化した認証方式である。
- アンチウィルスソフトウェア（Anti-virus Software）
  - マルウェアを検出し駆除を行う防御のためのソフトウェア。一般的にはウィルスのみならず、マルウェアを広範囲に対応しているものもアンチウィルスソフトウェアと呼ぶ。
- インシデント（Incident）
  - 情報セキュリティに関する事件・事故を意味する。
- ウィルス（Virus）
  - 利用者の操作などにより攻撃対象のシステムに感染し、悪意ある操作を行うソフトウェアのことで、データの削除や電子メールの送信、ファイルの漏洩など、有害な操作を行う。「ワーム」と類似するが、不正なプログラムの実行など、利用者の操作等をきかっけとして、感染が生じる点で、異なる。
- エシカルハッカー（Ethical Hacker）
  - サイバーセキュリティに関する高度な専門知識や技術をもちながら、高い倫理観と道徳心を兼ね備えた、善良的なハッカーを示す。別名、ホワイトハッカー。
- エンドポイント（Endpoint）
  - 企業や組織が Web サービスを提供するために稼働しているサーバ、および組織内外の利用者が利用しているコンピュータ（PC）を含めて、ネットワークに接続させる機器類に対する呼称。
- キーロガー（Key Logger）
  - 利用者のキーボードの入力を記録し ID やパスワードを含む認証情報などを自動的にネットワーク送信し情報を漏洩させるマルウェア。
- クリックストリーム（Click Stream）
  - Web サイトの利用者が操作閲覧する際の画面の遷移履歴をクリックストリームといい、Web サイトの使い勝手の評価に活用するほか、利用者の不審な操作流れがないかセキュリティ目的でも活用される。
- クロスサイトスクリプティング（Cross Site Scripting: XSS）
  - Web サイトを介した攻撃手法で、攻撃者が攻撃対象となる Web サイトとは異なるサイトから攻撃対象のブラウザや Web アプリケーションにスクリプトを送り込み、スクリプトを実行させることで、更なる攻撃に繋げる攻撃。

- サービス妨害（Denial of Service: DoS）
  - 攻撃者が攻撃対象のシステムに対して、同時に大量の接続リクエストを行い、攻撃対象のシステムに許容外の高負荷をかけることで、サービス提供を不能にする攻撃の手法。
- スパイウェア（Spyware）
  - 利用者に関する情報を収集し、外部に自動的にネットワーク送信し情報を漏洩させるマルウェア。
- セッションハイジャック（Session Hijack）
  - ネットワークにおいて原則的に一対一で行われている通信（セッション）を途中で乗っ取り、片方に成りすまして、不正にデータの窃取や改竄などを行う手法。
- ソーシャルエンジニアリング（Social Engineering）
  - 取引先の関係者を成りすました電子メールや本来の Web サイトに酷似させた不正な Web サイトを作成し誘導するなど、技術的ではない人間の心理上の弱点（親近感や油断など）を狙って利用者が使用しているコンピュータにマルウェアを感染させるなどの攻撃。
- ソフトウェアキーボード
  - 物理的なキーボードの代わりに画面上に表示されたキーボードをマウスで操作して入力をおこなうキーボード。
  - キーの操作内容を盗み出すマルウェアに対する対策として利用されることが多い。
- チョークポイント監視（Choke Point Monitoring）
  - コンピュータ・ネットワーク上の要所の通信等の挙動を監視し、時間的な変化などの相関分析を行い、マルウェアの感染によって引き起こされる不正な通信、主には遠隔での操作や不正なデータ送信を監視する手法。チョークポイントは、軍事用語の水路上の要衝から。
- トロイの木馬（Trojan Horse）
  - 善良なソフトウェアに見せかけたマルウェアを含むアプリケーションなどを、セキュリティを掻い潜り、攻撃対象に配置し、マルウェアを実行する攻撃。外部からの不正アクセスを誘導する事が多い。ターゲットが利用したくなるような有用な機能を装う場合が多い点が特徴。
- ハクティビスト（Hacktivist）
  - 社会的または政治的な主張を目的としたハッキング活動を行う者のこと。「Anonymous」「LulzSec」などがこれに当てはまる。
- バックドア（Back Door）
  - 攻撃対象のシステムに攻撃者がネットワーク接続を介して指示を与え遠隔操作できるようにするソフトウェア上の受け口または受け口をつけるマルウェア。
- ヒューリスティックマルウェア解析（Heuristic Malware Analysis）
  - マルウェアの解析の比較的新しい方法で、従前のアンチウィルスソフトウェアの多くがマルウェアのコードの特徴点（シグネチャー, signature）をブラックリストとして登録したものと一対一で比較して検出を行うのに対して、ヒューリスティック解析ではブラックリスト化されたマルウェアの特徴の傾向と比較することで、より柔軟性をもって検出できるのが特徴。日々新しいマルウェアが登場し、また多くの派生種が生成されるため、従前のシグネチャー解析では、最新のマルウェアの検出が適時に出来ないという課題に対応する。
- 標的型攻撃（Advanced Persistent Threats attack: APT 攻撃）
  - 特定の組織や個人を狙って様々な手法を組み合わせて持続的に行われるサイバー攻撃。
  - 特定の企業や国家など組織のコンピュータシステムへの不正侵入、機密情報の窃取、システムやデータの破壊などを目的とした組織性、計画性があるものが多い。
- フィッシング（Phishing）
  - 金融機関などからの正規のメールや金融機関の正規の Web サイトを精巧に模倣し、ID やパスワード、クレジットカード番号などを入力させて不正に窃取する攻撃の手法。

- フォレンジクス（Forensics）
  - 不正アクセスや機密情報の漏洩などのサイバーインシデント（事件事故）等に際して、コンピュータおよびネットワークに蓄積または通信された電子的な情報を元に、詳細な分析をおこない、電子的な証跡を導き出す技術的な専門領域。法的な係争の際には、証拠として利用されることがある。
- 分散型サービス妨害（Distributed Denaial of Service: DDoS）
  - 「サービス妨害（DoS）」を複数から同時に行う手法で、より致命的な被害を与えることができる手法。場合によっては数十万単位などの膨大な数のコンピュータから攻撃対象のシステムへの接続リクエストが行われ、その被害は甚大となる。DDoS の場合、多くの場合、事前に大量の「ボット」を用意しておき、攻撃者（人間）自身は遠隔から操作して、一斉に DoS 攻撃をしかける手法がとられる。
- ペネトレーションテスト（Penetration Test）
  - 組織のネットワークシステムの外部ネットワークとの境界の堅牢性を評価するためのテストで、ネットワーク境界の外部から内部へ侵入をあらゆる側面から試みるテスト。
- ボット（Bot）/インターネットボット（Internet bot）/Web ボット（Web bot）
  - 「ロボット（Robot）」の略称に由来し、「バックドア」を感染させてネットワーク接続を介して、外部から遠隔制御が可能になったシステム。
  - DDoS 攻撃では一般的にボットを多数束ねて（これをボットネット（Botnet）と呼ぶ）操作することで攻撃を行い、最近の DDoS 攻撃では数万単位、時として数十万を超えるボット化されたシステムを束ねて遠隔操作での攻撃が行われる場合がある。
- マルウェア（Malware）
  - 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪意のあるコード（コンピュータプログラム）の総称。マルウェアには、次の様なものが含まれる： ウィルス、ワーム、トロイの木馬、スパイウェア、キーロガー、バックドア、ランサムウェアなど
- マン・イン・ザ・ブラウザ攻撃（Man-in-the-Browser）
  - マルウェアの感染により Web ブラウザとサーバとの接続を監視して通信内容を改竄したり操作を乗っ取ったりする攻撃手法やそうした機能を有するマルウェアによる攻撃。利用者からみると正規のサービスの画面のようみ見えるため感染に気付きにくく、また金融機関側も正規の利用者が正常な処理を行っているようにみえるため対策が取りにくい。
- ワーム（Worm）
  - 悪意ある操作を行うソフトウェアという点で、ウィルスに類似するが、ワームはネットワークの構成を利用して自動的に増殖を行う。
- ランサムウェア（Ransomware）
  - マルウェアの一種で、攻撃対象システムの本来の利用者の利用を一時的に制限したり、対象データへのアクセスを不能にしてしまう動作をする。一時的な利用制限やアクセス不能の状態に対する身代金要求の手段として使用される場合が多い。

■ 12. 参考文献

本報告書の作成にあたって、下記の文献を参照または引用した。その他各ページの脚注に記載している文献を参照または引用した。

Bank of England. Resilience Information. (オンライン)
http://www.bankofengland.co.uk/financialstability/fsc/Pages/bcinformation.aspx.
Department of Financial Services (DFS). (オンライン) http://www.dfs.ny.gov/.
European Commission. Digital Agenda for Eupope. (オンライン) https://ec.europa.eu/digital-agenda/en.
Federal Financial Institutions Examination Council (FFIEC). (オンライン) https://www.ffiec.gov/.
HM Government. FTSE 350 Cyber Governance Health Check. (オンライン)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/399260/bis-15-37-ftse-350-cyber-governance-health-check-tracker-report-2014.pdf.
National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. (オンライン) http://www.nist.gov/cyberframework/.
—. Special Publications (800 Series). (オンライン) http://csrc.nist.gov/publications/PubsSPs.html.
NHK 放送文化研究所. 調査研究成果 海外放送事情. (オンライン)
http://www.nhk.or.jp/bunken/summary/research/oversea/126.html.
プライスウォーターハウスクーパース株式会社. グローバル情報セキュリティ調査®2015. (オンライン)
http://www.pwc.com/jp/ja/advisory/research-insights-report/information-security-survey.jhtml.
金融情報システムセンター. H22 年度 金融機関におけるサイバー攻撃対応に関する有識者検討会報告書. (オンライン) http://www.nisc.go.jp/inquiry/pdf/ken_honbun.pdf.
金融庁. 諸外国における金融制度の概要に関する調査. (オンライン)
http://www.fsa.go.jp/common/about/research/20140603.html.
国際公共政策研究センター. 解説: 英国「サイバーセキュリティ政策」. (オンライン)
http://www.cipps.org/group/cyber_memo/002_121128.pdf.
国際社会経済研究所. 個人情報保護の国内外動向と日本企業から見た課題. (オンライン) http://www.i-ise.com/jp/information/report/20150212_koizumi.html.
国立国会図書館調査及び立法考査局. アメリカ サイバーセキュリティに関する大統領令. (オンライン)
http://dl.ndl.go.jp/view/download/digidepo_8205972_po_02550201.pdf?contentNo=1&alternativeNo=.
—. アメリカ サイバーセキュリティ情報の共有を促す大統領令. (オンライン)
http://dl.ndl.go.jp/view/download/digidepo_9218613_po_02630101.pdf?contentNo=1.
消費者庁 消費者制度課. 個人情報の保護. (オンライン) http://www.caa.go.jp/planning/kojin/.
情報セキュリティ政策会議. サイバーセキュリティ戦略. (オンライン)
http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf.
情報処理推進機構 (IPA). (オンライン) https://www.ipa.go.jp/.
—. IPA ニューヨークだより. (オンライン) https://www.ipa.go.jp/about/NYreport/.

情報通信政策研究所 . 政策レビュー. (オンライン)
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/06/review06.html.
総務省. 情報通信統計データベース. (オンライン)
http://www.soumu.go.jp/johotsusintokei/whitepaper/h25.html.
―. 情報通信白書. (オンライン) http://www.soumu.go.jp/johotsusintokei/whitepaper/h25.html.
―. 世界情報通信事情. (オンライン) http://www.soumu.go.jp/g-ict/country/korea/index.html.
駐日欧州連合代表部. 駐日欧州連合代表部 公式ウェブマガジン. (オンライン) http://eumag.jp/.
内閣サイバーセキュリティセンター（NISC）. (オンライン) http://www.nisc.go.jp/index.html.
―. 各国の情報セキュリティ政策における情報連携モデルに関する調査. (オンライン)
http://www.nisc.go.jp/inquiry/.
―. 2011. 平成 22 年度 サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化に関する調査. (オンライン) 2011 年 3 月. http://www.nisc.go.jp/inquiry/.
日本国際問題研究所. (オンライン) http://www2.jiia.or.jp/.

ご注意

本書において各国金融監督機関、各技術機関、各銀行などが開示しているインターネット上の Web ページの情報を掲載した URL は 2015 年（平成 27 年）3 月現在のものであり、URL およびその内容は、変更、移動、削除される場合がある。

2014 年（平成 26 年）度　金融庁委託調査

諸外国の金融分野のサイバーセキュリティ対策に関する調査研究
報告書

プライスウォーターハウスクーパース株式会社
2015 年（平成 27 年）3 月 31 日　発行

<Intentionally left blank>