金融分野におけるサイバーセキュリティ強化に向けた取組方針について

平成２７年７月

金融庁

［目次］

１．金融分野のサイバーセキュリティにおける課題‥‥‥‥‥‥‥‥‥‥‥‥‥‥ P.1

⑴ 取組方針の策定について

⑵ 金融分野のサイバーセキュリティを巡る状況

⑶ 金融分野のサイバーセキュリティとして対処していくスコープ

２．金融分野のサイバーセキュリティ強化に向けた５つの方針‥‥‥‥‥ P.3

⑴ 基本的な考え方

⑵ ５つの方針

① サイバーセキュリティに係る金融機関との建設的な対話と一斉把握

② 金融機関同士の情報共有の枠組みの実効性向上

③ 業界横断的演習の継続的な実施

④ 金融分野のサイバーセキュリティ強化に向けた人材育成

⑤ 金融庁としての態勢構築

１．金融分野のサイバーセキュリティにおける課題

(1) 取組方針の策定について

金融庁では、金融分野におけるサイバーセキュリティ管理態勢について、これまでも金融機関のシステムの安定稼動、業務継続、情報セキュリティ管理、顧客保護といった視点から監督・検査を行ってきた。

他方、日本の金融システムは、現下、総体として健全であり安定しているが、①イノベーションの進展に合わせたインターネットの利用拡大、②サイバー攻撃の高度化（手口の巧妙化、攻撃技術へのアクセスの容易化）、③サイバーテロの脅威の高まり（経済目的ではなく社会秩序を混乱させる目的でのサイバー攻撃）に伴い、サイバー空間からの攻撃が金融システムの安定に影響を及ぼしかねないものとなってきている。

実際海外では、証券会社や医療保険会社において数千万件単位の顧客情報漏えいや銀行ＡＴＭの大規模停止などの事例が発生している。

このため、金融庁の重要目的である「金融システムの健全性確保」の観点に立ち、個々の金融機関がサイバーセキュリティ管理に係る基準を満たしているかの検証に留まらず、業界全体の課題を把握・分析し、サイバーセキュリティ強化を図ることで、金融システム全体の強靭性を高めていくことが必要となっている。

また、昨年 11 月にはサイバーセキュリティ基本法が制定され、金融を含めた重要インフラ事業者のサイバーセキュリティ確保のため、政府一丸となって、施策を講じることとされている。

そこで、今般、金融庁として金融分野へのサイバー攻撃の脅威に対抗するために今後取り組むべき方針を明らかにし、金融機関、金融サービス利用者及び関係機関と問題意識を共有することとした。

(2) 金融分野のサイバーセキュリティを巡る状況

① イノベーションの進展に合わせた金融分野でのインターネットの利用拡大

金融機関の業務では、預金・為替事務の処理はもとより、リスク管理や内部監査に至るまで、様々な場面でコンピュータシステムが活用され、これらの安全性・信頼性の確保は、経営管理上、極めて重要な課題となっている。さらに、情報通信技術の発達と金融機関の業務の多様化・国際化により、金融機関のコンピュータシステムは、インターネット等のオープンな情報通信ネットワーク（以下「インターネット等」という。）との繋がりを強めており、ネットワークを介した外部からの悪意ある接続等に対する堅牢性の確保も新たに重要となってきている。

また、顧客とのチャネルにおいても、インターネットバンキングをはじめとしてインターネットを介して取引が行えるサービスの普及が進んでいる。

（参考）インターネットバンキングの利用状況

（よりよい銀行づくりのためのアンケート（2012 年度）より）

利用している				利用していない
	週１回以上	2～3 ヶ月から 2～3 週間に１回	半年に１回以下	
65.2%	13.0%	38.9%	13.3%	34.8%

（注）全国銀行協会が実施した 3,400 人を対象にしたインターネットによるアンケート結果（回答 3,235 人）

これらのインターネット等を介した業務は、今後も、端末のモバイル化・高性能化や、クラウドサービスの進展、高速通信の利用コストの低減等を背景に、さらに進展していくものと考えられる。

② サイバー攻撃の高度化（手口の巧妙化、攻撃技術へのアクセスの容易化）

サイバー攻撃については、その手口が悪質化するとともに、攻撃技術へのアクセスが容易になり、脅威拡大に繋がっている。

例えば、金融機関の顧客情報や取引データの窃取を狙った攻撃（標的型攻撃[1]）では、ソフトウェアにおける未修正・未発表のセキュリティ上の脆弱性を悪用した「ゼロデイ攻撃」がなされるなど、防御がより難しくなってきている[2]。

また、マルウェア[3]感染により攻撃者の指令で動作させられてしまうコンピュータ群（ボットネット[4]）について指令を行う権利が取引されるなど[5]、攻撃者自身が技術を有していなくとも、攻撃手段へのアクセスが容易になってきている。

③ サイバーテロの脅威（2020 年東京オリンピック・パラリンピック競技大会の開催も見据えて）

サイバー攻撃については、これまでの情報漏えいや不正送金などの経済目的の攻撃だけでなく、近年では、社会不安を引き起こす目的でのサイバー攻撃にも留意する必要が高まってきている。

特に、日本では 2020 年東京オリンピック・パラリンピック競技大会の開催が控えているが、2012 年のロンドンオリンピックでは 2 億件、2014 年のソチオリンピックでは 10 万件のサイバー攻撃が発生したと言われている。

このため、金融を含めた重要インフラでは、政府と事業者が一丸となって取組みを強化していくことが必要となってきている。

(3) 金融分野のサイバーセキュリティとして対処していくスコープ

以上を踏まえ、金融分野のサイバーセキュリティとして対処していくスコープを以下のように整理する。なお、この整理は、現下想定される脅威を類型化したものであり、実際には複数の組合せや新たな脅威の発生も考えられる点に留意する必要がある。

---

1 標的型攻撃とは、情報窃取等を目的に、標的と定めた攻撃対象に対して、マルウェアに感染させること等により、システム内部から有益と思われる情報を窃取するもの。

2 Symantec「2014 年インターネットセキュリティ脅威レポート [第 19 号]」（2014 年 4 月）

3 マルウェアとは、悪意のあるソフトウェアの総称。コンピュータに感染し、不正送金や情報窃取などの遠隔操作を自動的に実行するプログラム。

4 情報窃取のほか、メールの大量送信や DDoS 攻撃等の犯罪行為に利用される。

5 前掲「2014 年インターネットセキュリティ脅威レポート [第 19 号]」において、ボットネットのレンタル市場の存在が指摘されている。

攻撃者の動機	対象	脅威		関連する既存のリスク管理態勢
社会秩序の混乱	金融機関	金融機関・金融インフラの機能停止	金融機関が直接サイバー空間から攻撃されるもの	業務継続（BCM）等
			人的（故意・過失を問わない内部者）に、システムがマルウェアに感染させられ、機能停止に陥るもの	
経済目的		機密漏洩	金融機関が直接サイバー空間から攻撃されるもの	情報セキュリティ管理等
			人的（故意・過失を問わない内部者）に、システムがマルウェアに感染させられ、サイバー空間から機密漏洩	
		不正送金等の不正取引	金融機関のコンピュータがマルウェア(注)に感染して不正送金等の不正な取引がなされるもの	顧客保護 等
	顧客		顧客のコンピュータがマルウェアに感染して、顧客の意志に反した指示が金融機関になされるものや、フィッシング詐欺等	

２．金融分野のサイバーセキュリティ強化に向けた５つの方針

(1) 基本的考え方

金融機関及び金融サービス利用者にとって、インターネット等を活用した業務やサービスは既に経済活動に不可欠なインフラとなっており、サイバー攻撃による被害は個別金融機関の問題に留まらず、日本の金融システムへの信頼を損ないかねないものとなっている。このため、サイバーセキュリティ強化には、官民一体となって取り組むことが必要である。

そこで、金融庁は、金融機関・金融市場インフラ（以下「金融機関等」という。）との間で、金融分野のサイバーセキュリティ確保という共通目的を有しているとの理解の下、建設的な対話を日常的に重ねていくことに努めるとともに、行政当局の立場から金融分野のサイバーセキュリティ強化に貢献すべく、以下の５項目に取り組む。なお、これらの項目については、今後の情勢の変化等を踏まえて、適時に見直しを行う。

(2) ５つの方針

① サイバーセキュリティに係る金融機関との建設的な対話と一斉把握

サイバー攻撃に対処するには、金融機関等との間で最近の攻撃の動向や取組みについて日常的に情報交換を行い、金融庁として新たな脅威をフォワードルッキングに把握するとともに、金融機関等のサイバーセキュリティ管理態勢がより実効性のある優れた取組みとなるよう建設的な対話を重ねていくことが重要となる。

特に、サイバーセキュリティ管理態勢は、日本の金融システムへの信頼確保のためには、規模やビジネスモデルに応じて必要となる取組みの内容や深度に違いはあるものの、すべての金融機関等において実効性のある態勢整備が求められる。

そこで、金融機関等ごとのサイバーセキュリティ管理態勢の取組状況やその実効性について実態把握を行い、各業態の課題について分析を行うため、全ての金融業態等に対してアンケートも活用した実態把握を今年中に実施する。調査の結果は、金融機関等にフィードバックすることで自己点検を促すとともに、モニタリング（監督・検査）に活用し、より良い業務運営に向けた対話に繋げていく。

調査の際は、サイバー攻撃への対処を行う各ステップ、すなわち、以下の項目ごとにいかなる対応が取られているか確認する。

ア．特定
・サイバー攻撃から保護すべき対象（情報資産等）の把握
・経営陣によるサイバーセキュリティ管理の重要性の認識
・セキュリティ水準の定期的評価
・システム開発におけるセキュリティ管理の視点の導入　等
イ．防御
・組織内の緊急時対応・早期警戒体制の整備
・情報共有機関等を通じた情報収集・共有体制の整備
・多層防御（入口対策・内部対策・出口対策）
・システムの脆弱性についての適時の対応
・コンティンジェンシープランの策定・業界横断的演習への参加　等
ウ．検知
・通信記録（ログ）等の取得・分析を含むサイバー攻撃に対する監視　等
エ．対応、復旧
・コンティンジェンシープランに沿った適切な対応　等

また、顧客への攻撃による不正送金等への対処について、以下につき確認を行う。
ア．サービス提供の状況
・より安全な認証手段をはじめとする不正防止策の組合せ状況　等
イ．顧客への働きかけ
・顧客の利用環境のセキュリティ強化の取組み
・異常な取引等の検知・連絡　等

② 金融機関同士の情報共有の枠組みの実効性向上

金融機関等の取組みを向上させ、金融業界全体のサイバーセキュリティを強化していくためには、内閣サイバーセキュリティセンター（以下「NISC」という。）からの情報提供（「公助」）だけではなく、金融機関同士で情報共有・分析を行う「共助」が非常に有効となる。具体的には、活発な情報提供・活用により、ある金融機関が攻撃を受けた際、他の金融機関が同種の攻撃手法への備えを予め講じられるようになるほか、参加金融機関間の交流を通じて、先進的な金融機関の積極的貢献によるスキルやノウハウの共有が進み、全体としての底上げ効果などが期待できる。

このため、金融機関に対して、昨年11月に活動を開始した一般社団法人　金融ISACをはじめとする情報共有機関等を活用した情報収集・提供及びこれを踏まえた取組みの高度化（脆弱性情報の迅速な把握・防御技術の導入等）の意義について、引き続き、機会を捉えて周知していく。

また、業界団体等（CEPTOAR）を通じた情報提供についても、NISCから発信されたものに限らず、金融庁から金融分野向けに提供すべき情報があれば、積極的に発信していく。

なお、公益財団法人　金融情報システムセンターでは、本年 6 月に「金融機関等コンピュータシステムの安全対策基準・解説書」のサイバーセキュリティに関する

記述を改訂の上、当該記述の解釈に関する金融機関向けの問合せ窓口を開設し、広く周知すべき質問・回答を「FISC サイバーセキュリティ参考情報」として公表する取組みを行っており、金融機関による活用が期待される。

③　業界横断的演習の継続的な実施

サイバー攻撃への対応能力の向上に当たっては、演習の実施を通じて、経営層から担当者に至る関係者の実戦能力を向上させるとともに、現在想定している対応体制・手順の有効性を確認し、PDCA サイクルを回していくことが有用である。

特に、規模が大きくない金融機関等、十分な対策を講じることが困難な組織では、国・関係機関等の関係者が連携し、実戦的な演習の実施等を通じた取組み強化の支援が有用である。

また、先進的な金融機関では、自らの取組状況を評価・分析するため、金融機関単位での演習を実施している。しかし、現実の事案への対応において必要となる、関係機関（金融庁・情報共有機関・他の金融機関その他）との連携のあり方について、予め確認しておくことは必要となる。

そこで、海外でも行われているような当局を含む業界横断的な演習事例も参考にしつつ、関係者を含めた業界横断的な演習を速やかに実施することとし、早急にその具体的方法（実施主体（他省庁・関係機関との連携を含む）、演習の目的、シナリオの内容等）を検討する。

④　金融分野のサイバーセキュリティ強化に向けた人材育成

金融分野のサイバーセキュリティ強化を進めていく上では、実際に各種サイバーセキュリティ対策を行う技術担当者だけではなく、サイバーセキュリティ管理態勢の整備に関する意思決定・組織内への指示を行う経営層やこれを支える管理部門の職員も、意識の向上や必要な知見の習得が求められる。また、これに合わせて、監督当局の担当者の質の向上も不可欠となる。

そこで、これら関係者の質の向上に向けて、平成 27 事務年度より、以下について取り組んでいく。

ア．金融機関等の経営層の意識向上を目的としたセミナー等の開催

イ．金融機関等でサイバーセキュリティに関与する職員として求められる人材及びその育成方法（キャリアパス、バックグラウンド等を含む）等について関係者との議論・検討

ウ．金融庁担当者の様々な専門性確保（外部登用・内部育成）

⑤　金融庁としての態勢構築

金融庁では、サイバーセキュリティに関して、金融機関等を検査する部署（検査局・証券取引等監視委員会）・監督する部署（監督局・総務企画局市場課）、NISC との連携を行う部署（総務企画局政策課）、政府の一員である金融庁自身のセキュリティ対策を行う部署（総務企画局総務課情報化統括室）等が、それぞれの業務を遂行している。

しかし、①～④の実施を含め、金融分野におけるサイバーセキュリティ向上に強力に取り組んでいくには、金融庁内部において情報・知見を一元的に集約し、組織横断的に企画・調整を行うことが必要となる。

そこで、外部の専門家を活用しつつ、

ア．有識者等からの情報収集、国内外の事例の収集・分析、各部局からの情報集約を通じた知見の集積と幹部及び各部局への還元

イ．知見を活かした金融機関等へのモニタリングの企画・立案支援

ウ．その他金融機関等のサイバーセキュリティ強化に必要な施策の企画立案

といった業務を行う部署を、総括審議官の下、総務企画局政策課に直ちに設置する。

合わせて、金融機関等に対するサイバー攻撃事案が発生した際の金融庁としての対応手順の整理（コンティンジェンシープランの策定）も行う。

さらには、サイバー攻撃の手口の高度化・巧妙化が進み、どれだけ予め対策を講じたとしても被害を受けてしまうことは生じ得るとの状況を踏まえて、金融庁の立場から、金融システム全体での強靭性を高めるべく、①～④の他にも金融機関等のサイバーセキュリティ強化を支援していく方策がないか、不断に検討していく。