【特集】サイバー攻撃への対応

システムリスク等に関する監督指針・検査マニュアルの改正

サイバーセキュリティは金融システム全体の信用にかかわる課題

金融庁監督局総務課
監督管理官　稲田　拓司

金融庁は、近年増加している顧客情報の漏洩事案、サイバーセキュリティ事案、不正送金事案等から明らかになった管理態勢の課題をふまえ「主要行等向けの総合的な監督指針」および「金融検査マニュアル」等（以下、「監督指針等」）を改正し、２０１５年４月21日に公表した。本稿では、今回の改正の背景、概要等について解説する。なお、本稿中、意見に係る部分は執筆者の個人的見解であって、必ずしも金融庁の公式見解を表わすものではない。

監督指針等改正の背景・概要

今回の改正は、情報セキュリティ管理、サイバーセキュリティ管理、インターネット・バンキングに係る改正となっており、預金取扱金融機関のほか、保険会社、金融商品取引業者等、貸金業者など、業態を問わず改正を行っている。

(1)情報セキュリティ管理に係る改正

２０１２年11月、システム共同センターの外部委託先社員が顧客の口座情報を不正に取得し、偽造キャッシュカードにより不正出金するという事案が発生した。加えて、14年２月には、地方銀行の外部委託先社員による不正出金事案が明らかになった。また、同年７月には、大手教育会社の外部委託先社員が不正に取得した顧客情報を名簿業者に転売するという事案も発生している。

これらの事案から、専門的な知識を有した者がそのスキルを活用すれば、これまで想定されていない領域から、想定されていない手法で重要な情報をたやすく窃取できることが判明した。前述の事例は、いずれも外部委託先（子会社等を含む）のベテラン社員による犯行であるが、たんに外部委託先管理の問題だけではなく、顧客の重要情報を社内外の不正行為からいかに守るかが問われているととらえる必要がある。

このため、顧客の重要情報の厳格な管理態勢や外部委託先に対する委託元としてのモニタリング態勢の強化について所要の改正を行っている。

(2)サイバーセキュリティ管理に係る改正

12年９月に発生した国内の金融機関等に対する大量アクセス攻撃、翌年３月に韓国で発生した金融機関等に対するサイバー攻撃、さらに昨年８月に発覚し

たアメリカの金融機関におけるサイバー攻撃による顧客情報の大量流出など、サイバーセキュリティに対する脅威は世界的規模で深刻化している。

また、昨年11月にはサイバーセキュリティ基本法が公布・施行され、国や重要社会基盤事業者の責務として、サイバーセキュリティの確保が求められている。とくにサイバーセキュリティは、いちばん弱いところから狙われ、そこから金融システム全体の安全が脅かされる事態へ発展しかねないため、官民一体となって対策水準の底上げを図ることが急務である。

このため、サイバー攻撃に備えた態勢の整備、技術的な対策の実施、人材の育成といった金融機関に求めるサイバーセキュリティ管理態勢を明確化し、所要の改正を行っている。

⑶インターネット・バンキングに係る改正

インターネット・バンキングに係る不正送金事案については、犯罪手口が高度化・巧妙化していることに加え、被害範囲が主要行やインターネット専業銀行だけではなく、中小・地域金融機関に拡大するとともに、法人名義口座の被害が拡大するなど、14年の被害額が前年の2倍を超えたほか、本年も昨年を上回る勢いで被害が急増している。

こうした現状をふまえ、金融機関は利用者利便を確保しつつ、利用者保護の徹底を図る必要があるほか、顧客に対する情報提供、啓発および知識の普及を図ることも重要となっている。

このため、インターネット・バンキングに係る全国銀行協会の申合せや「インターネット・バンキングにおいて留意すべき事項について」の改正等をふまえ、金融機関に求める技術的なセキュリティ対策や顧客への対応について所要の改正を行っている。

主要なコメントの概要と金融庁の考え方

今回の監督指針等の改正に先立ち、本年2月13日から3月16日まで広く意見を募集したところ、15の個人および団体から延べ98件の意見等が寄せられた。寄せられたおもな意見（質問を含む）と金融庁の考え方について、解説を交えて紹介する（文言は一部修正している）。

⑴指針の適用に関するもの（例示部分等）

【意見】システムリスク管理態勢の検証は、従前どおり金融機関の業容に応じてなされるものであり、改正案で記載されている項目すべてを満たすことが求められているわけではないと考えてよいか。

【回答】情報セキュリティ管理およびサイバーセキュリティ管理で示しているそれぞれの着眼点については、取り扱う業務のリスクに見合った態勢整備や対策を講じる必要があると考える。

なお、それぞれの着眼点で「たとえば」と記載されているような具体的な対策例については、例示に限定されるものではなく、例示以外の方法も含め検討し、適切な対策を講じる必要がある。

【解説】監督指針等の適用にあたっては、引き続き金融機関の規模や特性を十分にふまえ、機械的・画一的な運用に陥らないよう配慮される。

一方で、情報セキュリティ、サイバーセキュリティの観点でみれば、対策の弱いところから攻撃者に狙われ、そこから金融システム全体に被害が波及するようなケースも考えられるため、着眼点として示した項目については、取り扱う業務のリスクに応じて、態勢整備や技術的対策を講じる必要がある。

⑵顧客の重要情報の定義に関するもの

【意見】「顧客の重要情報」とは具体的にどのようなものか。

【回答】金融機関が責任を負うべき顧客の重要情報については、たとえば、個人情報、認証情報、電子的価値情報等が考えられるが、個々の金融機関が業務やリスクに応じて適切に定義を行う必要があると考える。一般的には、各社のセキュリティポリシーにおいて規定されているものと考える。

【解説】金融機関が責任を負うべき顧客の重要情報については、個々の金融機関が取り扱う業務やリスクに応じて適切に定義を行う必要があり、前述のほか、顧客の営業秘密や融資先に関す

る社内格付等も考えられる。

（参考）金融情報システムセンター（ＦＩＳＣ）の「金融機関等におけるセキュリティポリシー策定のための手引書」

⑶顧客の重要情報の洗出しに関するもの

【意見】「通常の業務では使用しないシステム領域に格納されたデータ」とは、具体的にどのようなデータをさすのか。

【回答】重要情報の洗出しでは、業務プログラム等で呼び出されるデータベース内の情報のみを対象にするだけではなく、たとえば、ＯＳが取得しているシステムログやメモリ領域等の一次的に保管されるデータ等も含め、洗い出す必要があると考える。

【解説】前述の不正出金事案では、情報システムの設計仕様では想定されていない領域に顧客の重要情報が暗号化されていない状態で保存されており、それを知る者が不正行為を働いている。クラウドサービス等の外部サービスを利用する場合においても漏れのないように網羅的に洗い出し、把握しておくことが望ましい。

⑷組織内ＣＳＩＲＴの体制整備に関するもの

【意見】「組織内ＣＳＩＲＴ」（Computer Security Incident Response Team）等の緊急時対応および早期警戒のための体制」について、関係会社でそのような組織が備わっている、もしくは自社において独立した組織でなくても機能が備わっておれば足りるという理解でよいか。

【回答】ご認識のとおり。「組織内ＣＳＩＲＴ等の緊急時対応および早期警戒のための体制」の整備は、態勢整備の一例であり、物理的な組織体制や組織名称にかかわらず同等以上の機能が備わった態勢を整備していただくことが必要と考える。

【解説】「ＣＳＩＲＴ」（シーサート）という名称の部署を社内に設けなければいけないのかという誤解もみられたが、名称にかかわらず「機能」を有することが必要である。設置形態についても金融機関の規模・特性に応じてさまざまな形態が考えられ、単独で設けることが困難な場合は、外部委託や共同で整備する等の工夫が考えられる。

⑸情報共有機関に関するもの

【意見】「情報共有機関等」とは、具体的にどのような機関を想定しているのか。

【回答】たとえば、金融セプターや業界団体、ＩＰＡ、ＪＰＣＥＲＴ／ＣＣのほか、金融ＩＳＡＣ、日本シーサート協議会などが考えられる。

【解説】サイバー攻撃の被害拡大を防止するためにも情報共有機関等を積極的に活用し、金融機関相互でタイムリーな情報共有を行うことが有益である。情報共有機関としては、前述のほか、日本サイバー犯罪対策センター（ＪＣ３）、フィッシング対策協議会等が考えられる。

⑹業界横断的な演習に関するもの

【意見】「業界横断的な演習に参加」とは、具体的にどのような演習を想定しているのか。

【回答】個別金融機関単独の訓練ではなく、業界内の演習や銀行、保険、証券、貸金等の垣根を越えた演習を想定している。また、すでにＮＩＳＣが毎年実施している演習のように金融分野以外の重要インフラ事業者との演習も考えられる。

【解説】欧米諸国においては、当局が関与した業界横断的な演習が実施されている。これをふまえ、当庁としても関係団体等と緊密に連携していく所存である。

金融機関は、たとえば下記のように目的に応じて演習を重ね、整備した態勢についての実効性を確保することが重要である。

- 経営層の意識改革およびトリアージ能力の向上
- 連絡・報告、情報共有等、初動態勢の検証
- 証拠保全、ログ解析等、技術スキルの向上　等

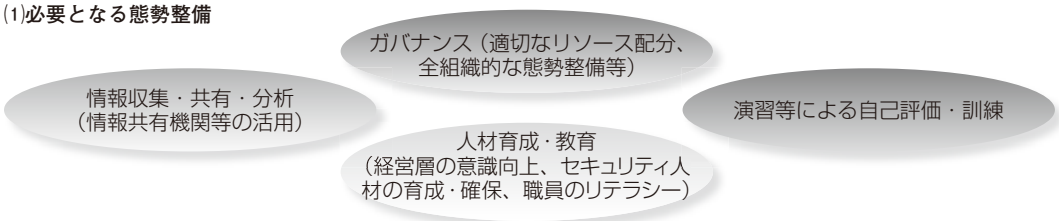
金融機関に求められる対応や留意点

サイバーセキュリティは、個別金融機関としての信用問題にとどまらず、日本の金融システム全体への信用問題となりかねない課題であり、官民一体となった取組みが不可欠である。そのため、一つでも対応が疎かな金融機関があっては、脅威を低減させることはできない。

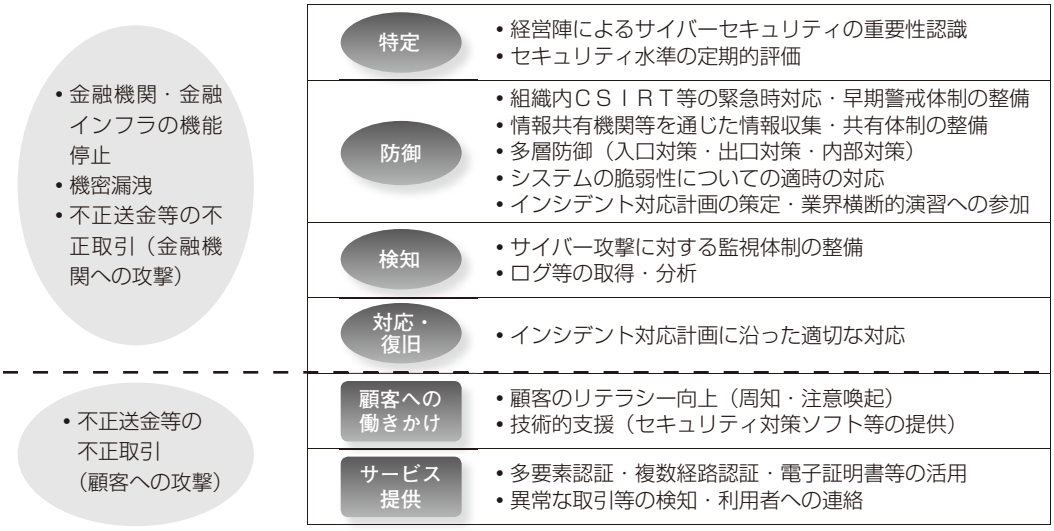
⑴サイバーセキュリティは、ＩＴ部門に任せておけばよいとい

〔図表〕　サイバーセキュリティ管理で求められる態勢整備

⑴必要となる態勢整備



⑵具体的な対応



うことではなく、経営陣が先頭に立って重要性を認識し、態勢整備を図っていくことが不可欠である（図表参照）。

⑵今回の監督指針等の改正においては、着眼点を理解しやすいように、できるだけ例示を入れている。これは、例示されている事項を実施すれば、それでよいということではなく、また、たんなる機器の導入や組織の設置にとどまることなく、個別の着眼点の背景・趣旨を十分に理解したうえで、個別金融機関の業務やリスクに応じて、組織全体の取組みとして適切な対応を図っていくことが必要である。

⑶サイバーセキュリティへの対応は、喫緊の課題であることから、改正した監督指針等については、即日施行としており、経過期間は設けていない。金融機関は、着眼点に基づいて自己点検を行い、対応の優先付けを行ったうえで対応計画（ロードマップ）を策定するなど、経営陣の積極的な関与のもと、ＰＤＣＡサイクルを回していくことが大切である。

金融庁における今後の取組み

金融庁では、改正された監督指針等をふまえて、金融機関のサイバーセキュリティ対策の取組み状況を継続的に把握し、よりよい業務運営に向けた対話を実施していくこととしているほか、把握結果をふまえながら、監督指針等についても適宜見直しを図っていく予定である。

また、サイバーセキュリティ基本法などもふまえながら、演習や人材育成の促進など、モニタリング以外の取組みについても検討していきたい。

いなだ　たくじ
民間のＩＴ企業、金融機関等での勤務を経て、08年6月金融庁に入庁。総務企画局にて庁内の情報システム、情報セキュリティを担当。14年7月に監督局に異動し、15年4月から現職。