BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

サイバーセキュリティの確保に向けた金融機関の取り組みと課題
―アンケート（2019年9月）調査結果―

日本銀行
金融機構局
2020年1月

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

（金融システムレポート別冊シリーズについて）

日本銀行は、マクロ・プルーデンスの視点からわが国金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年 2 回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を不定期に行い、『金融システムレポート』を補完するものである。本別冊では、2019 年 9 月に実施した「サイバーセキュリティに関するアンケート」の結果を紹介する。

（本別冊の要旨）

金融機関によるデジタル技術を活用した新しい顧客サービスや業務改革等が進むにつれ、サイバーセキュリティの確保、すなわち外部などからの攻撃に対するコンピュータシステム・機器・通信ネットワークの安全性や信頼性の確保および情報資産の安全管理が一段と重要性を増している。

日本銀行は、今般、当座預金取引先金融機関等のうち 402 先を対象に、サイバー攻撃の脅威に対する認識、サイバーセキュリティ確保に向けた経営トップの関与、リスク管理体制、サイバーセキュリティ対策の実施状況などについて調査するため、アンケートを実施した。この結果、同様のアンケート調査を実施した 2017 年 4 月時点と比べ、多くの金融機関がサイバーセキュリティの確保を経営上の重要課題と捉え、体制整備や技術対策などの取り組みを進めていることが確認できた。もっとも、サイバーセキュリティの企画に携わる要員が引き続き不足していることや、グループベースでの取り組みには改善の余地があること、コンティンジェンシープランに基づいた訓練の実施など、サイバーセキュリティ対策の実効性向上への取り組みや新たなデジタル技術の導入に対応したサイバーセキュリティ上の体制整備については、十分に進んでいない先も少なくないことが明らかとなった。

デジタライゼーションの動きが急速に拡がる一方、サイバー攻撃の脅威は引き続き高く、金融機関が経営トップの適切な認識・関与のもとで、サイバーセキュリティ対策の強化に向けた取り組みを続けていくことが重要である。日本銀行としては、金融機関が自らのサイバーセキュリティに関する体制面や技術面での取り組みを進めていくうえで、本アンケート結果が活用されることを期待するとともに、考査・モニタリング、各種セミナー等を通じて、そうした取り組みを後押ししていく方針である。

【目　次】

Ⅰ．はじめに　3

Ⅱ．サイバーセキュリティに関するアンケートの結果

１．体制面の取り組み

（１）脅威の認識と自社への攻撃の発生状況　7

（２）組織体制　7

（３）サイバーセキュリティの管理体制強化・実効性の向上　１０

２．技術面の取り組み

（１）守るべき情報資産の特定　１１

（２）端末等への技術的な対策　１２

（３）対策の実効性の向上　１５

（４）攻撃を受けた場合の対応・復旧対策　１６

３．新たなデジタル技術の導入を踏まえた対応　１７

Ⅲ．おわりに　２０

Ⅰ．はじめに

最近のわが国の金融機関を取り巻く環境をみると、スマートフォン・タブレット端末といったモバイル・インターフェースの普及に加え、AI（人工知能）[1]やIoT (Internet of Things)[2]、クラウドサービス[3]などの新たなデジタル技術の活用といった大きな変化が生じている。こうしたデジタル技術の進歩に伴って、金融機関におけるサイバーセキュリティに係るリスクは急速に高まっている。サイバーリスク（サイバー攻撃により影響を被るリスク）は、金融機関の資産・顧客情報の窃取や、金融機関ひいては金融システムの妨害・破壊を企図した、個人や集団によるサイバー攻撃に起因する点が、従来型のリスクと大きく異なる。

こうした点に鑑み、日本銀行の考査やモニタリングでは、経営陣の適切な認識・関与のもとでのサイバーセキュリティ管理体制の整備に向けた取り組み状況や、多様なサイバー攻撃に応じた未然防止策と被害抑止策の有効性を点検している。また、攻撃からの完全な防御は困難であることを踏まえ、サイバーインシデント発生時を想定した体制やコンティンジェンシープランの実効性、訓練・演習の実施状況とその結果を反映した管理体制の見直し状況についても点検している。その際、必要に応じて、金融機関の重要情報にアクセスし得るグループ会社や業務委託先等の管理についての点検も行っている[4]。

金融機関が環境変化に対応し、持続的に付加価値の高いサービスを創出していくうえでは、サイバーセキュリティの確保、すなわち外部などからの攻撃に対するコンピュータシステム・機器・通信ネットワークの安全性や信頼性の確保および情報資産の安全管理が不可欠である[5]。特に、わが国では、本年、東京オリンピック・パラリンピック競技大会を控えていることから、サイバー攻撃が増加する可能性には十分な留意が必要である。

最近のサイバー攻撃の脅威として、被害事象別にみると、情報漏えいに関する脅威については、マルウェア[6]や脆弱性を悪用した事例に加え、何らかの理由で漏えいした多数の個人ログイン ID・パスワードのリストを悪用してシステムへの不正利用を行う事例や、最近では、クラウドサービスを利用する際の設定の不備を突いた攻撃による事例もみられている（図表

---

[1] Artificial Intelligence の略。一義的な定義はないが、人間の知的振舞いの一部を人工的に再現したものに関する総称として使われることが多い。

[2] 様々なモノ（物）をインターネットに接続することにより、対象物の情報収集や制御等を可能とする仕組み。

[3] ネットワーク経由で必要なときに必要なだけコンピュータ資源を利用できるサービス。

[4] サイバーセキュリティの管理体制に関する 2019 年度考査での点検ポイントの詳細については、『2019 年度の考査の実施方針等について』（2019 年 3 月）を参照。

[5] 金融サービスにおける IT の活用とサイバーセキュリティに関する詳細は、『金融システムレポート別冊シリーズ：IT の進歩がもたらす新たな可能性とサイバーセキュリティ』（2016 年 3 月）を参照。

[6] 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コード（コンピュータプログラム）の総称。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が含まれる。

1、2)。システムの機能停止（DoS 攻撃 <DDoS 攻撃を含む>[7]）に関する脅威についても、金融セクターを含む国内外の法人などを対象に数多く確認されており、攻撃規模も拡大傾向を辿っている（図表 3)。

図表 1　金融機関等におけるサイバー攻撃の脅威と攻撃例

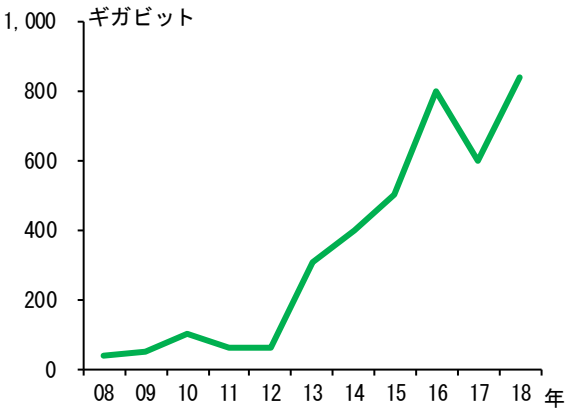
被害事象	攻撃例	内容
情報漏えい	マルウェア	ネットワーク等を通じてマルウェアに感染させ、情報を窃取する攻撃
	脆弱性（設定不備を含む）の悪用	脆弱性を悪用することで、システムに格納されている情報を窃取する攻撃
	パスワードリスト攻撃	漏えいした ID・パスワードのリストを悪用し、情報を窃取する攻撃
システムの機能停止	DoS・DDoS 攻撃	大量の（または不正な）通信により、標的とするコンピュータや通信回線の機能（サービス）を停止（または著しく低下）させる攻撃
	マルウェア	ネットワーク等を通じて不正プログラムに感染させ、システムの機能を停止させる攻撃
システムの破壊・改ざん	マルウェア	ネットワーク等を通じて不正プログラムに感染させ、システムやデータの破壊・改ざん等を行う攻撃
	脆弱性の悪用	脆弱性を悪用することで、システムの破壊・改ざん等を行う攻撃
不正送金・システムの不正利用	マルウェア	ネットワーク等を通じてマルウェアに感染させ、不正な送金指図等を行う攻撃
	フィッシング	偽のサイトにパスワードを入力させることで顧客のパスワードを盗み取り、これを悪用して不正送金等を行う攻撃
	パスワードリスト攻撃	漏えいした ID・パスワードのリストを悪用し、システムを不正利用する攻撃

図表 2　サイバー攻撃に起因した国内外の大規模な情報漏えい事例

時期	内容
2017	大学の情報システムで、教員のログインアカウントとパスワードが不正に利用され、関係者の個人情報 7 万件が漏えいした可能性があるとの報道。
2018	電子書籍等をダウンロード販売しているサイトが不正アクセスを受け、50 万件強の顧客情報のほか、このうち 8 千件弱について、同サイトの改ざんにより誘導されたフィッシングサイトからクレジットカード情報が漏えいした可能性があるとの報道。
2019	クラウド環境で運営されているファイル転送サービスのサーバの脆弱性が攻撃され、480 万件強の顧客情報が漏えいしたとの報道。
2019	自動車販売会社グループのネットワークが不正アクセスを受け、傘下の複数企業のサーバから 300 万件以上の顧客情報が漏えいした可能性があるとの報道。
2019	海外大手金融機関が、不正アクセス対策機器の設定不備を攻撃され、クラウド環境に保管していた 1 億人強分の顧客情報が漏えいしたとの報道。

（資料）各種公表情報

図表 3　DoS 攻撃の攻撃規模の拡大

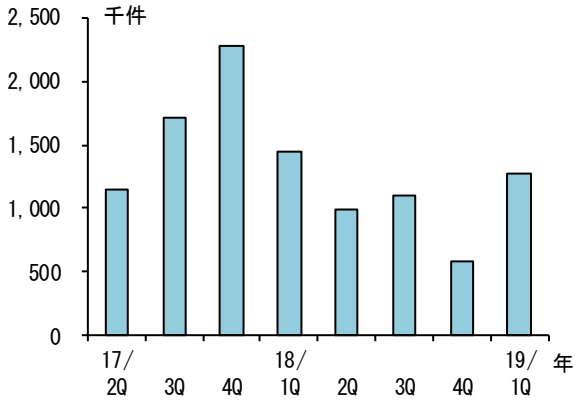


（注）各年で観測された 1 秒当たりの不正通信量の最大値。
（資料）NETSCOUT Systems “Worldwide Infrastructure Security Report”

[7] DoS（Denial of Service）攻撃は、大量の（または不正な）通信により、標的とするコンピュータや通信回線の機能（サービス）を停止（または著しく低下）させる攻撃。このうち、インターネット上に分散する複数の機器から同時に攻撃するものを DDoS（Distributed Denial of Service）攻撃という。

また、システムの破壊・改ざんに関する脅威についてみると、マルウェアの一種で、ファイルを暗号化し暗号の解除の対価として金銭を要求する「ランサムウェア攻撃」が依然として多発している（図表 4）。最近では、自己の複製を作り、ネットワークを介して感染を拡げていく機能を有する感染力の高いランサムウェアが利用されるケースが増加するなど、感染した場合の被害が大きくなる傾向がみられている。

図表 4　新たなランサムウェアの件数

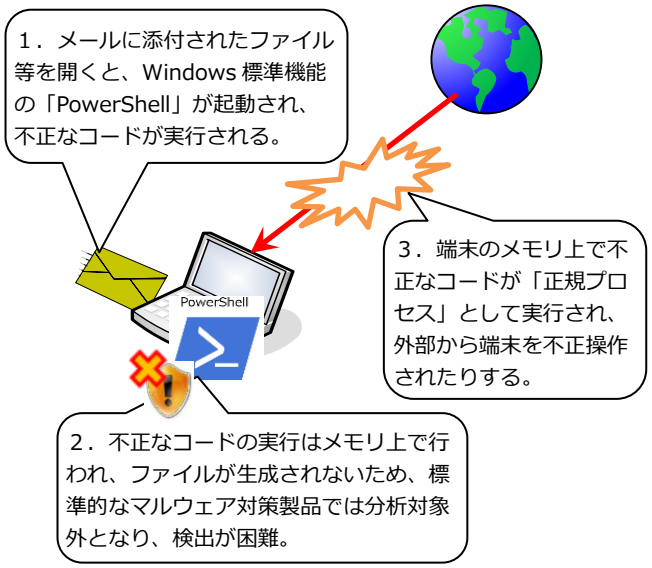


（注）マカフィー社で検知した新たなランサムウェアの件数。全世界ベース。
（資料）マカフィー「McAfee Labs 脅威レポート」

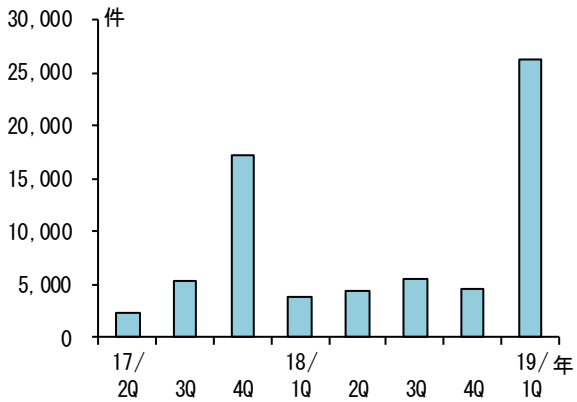
攻撃手法についても、標準的なマルウェア対策製品（ウィルス検知ソフト）では検知が困難な「ファイルレス攻撃」（マルウェアファイルを使用しない攻撃）が多用されるなど、一段と巧妙化しており、攻撃を完全に防御することが困難となってきている（図表 5）。

図表 5　ファイルレス攻撃の例（PowerShell マルウェア）

（イメージ図）



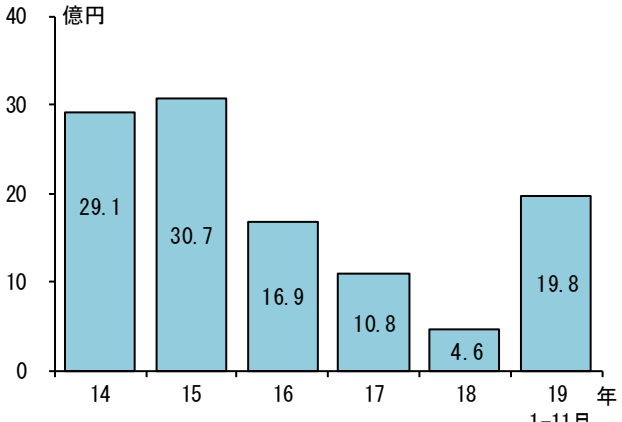
（新たな PowerShell マルウェア件数）



（注）マカフィー社で検知した新たな PowerShell の件数。全世界ベース。
（資料）マカフィー「McAfee Labs 脅威レポート」

こうしたなか、わが国におけるインターネット・バンキング（以下、IB）の顧客を狙った預金などの不正な引出金額の推移をみると、2016 年以降減少傾向を辿ってきたが、足もとは増加している（図表 6）。スマートフォンや携帯電話の SMS（ショート・メッセージ・サービス）を通じて IB のユーザーにフィッシングメールを送り、偽のサイトに入力させたパスワードを盗み取るなど、巧妙な手口を用いた事例が目立つようになっている。

図表 6　IB に係る預金などの不正な引出金額の推移



（注）2019 年は 1～11 月計（暫定値）。
（資料）警察庁

こうした状況のもと、日本銀行は、当座預金取引先金融機関等のうち 402 先[8]を対象に、サイバー攻撃の脅威に対する認識、サイバーセキュリティ確保に向けた経営トップの関与、リスク管理体制、サイバーセキュリティ対策の実施状況と、2017 年 4 月に実施した同様のアンケート調査（以下、「前回」）[9]からの変化を調査することを目的に、サイバーセキュリティに関するアンケート（以下、「アンケート」）を実施した[10]。

以下では、アンケート結果を踏まえつつ、サイバーセキュリティを確保するうえで求められる対応のポイントを紹介する。まず、「体制面の取り組み」として、脅威認識と自社への攻撃の発生状況を確認したうえで、サイバーセキュリティ確保のための組織体制のあり方や、サイバーセキュリティの管理体制強化・実効性の向上への取り組み状況について紹介する。次に、「技術面の取り組み」として、守るべき情報資産の特定状況について触れたうえで、技術的な対策の実施状況や各種対策の実効性向上に向けた取り組み、攻撃を受けた場合の対応・復旧対策の整備状況について紹介する。最後に、「新たなデジタル技術の導入を踏まえた対応」の状況について紹介する。

---

[8] 内訳は、銀行 123 先、信託銀行 11 先、信用金庫 249 先、系統中央機関 4 先、金融商品取引業者 7 先、証券金融会社 1 先、短資会社 3 先、資金清算機関 1 先、金融商品取引清算機関 2 先、その他 1 先。なお、本稿では、これらの先を総称して「金融機関」という。

[9] 『金融システムレポート別冊シリーズ：サイバーセキュリティに関する金融機関の取り組みと改善に向けたポイント―アンケート（2017 年 4 月）調査結果―』（2017 年 10 月）を参照。

[10] アンケート実施期間は、2019 年 9 月 2 日から同 30 日まで。回収率は 100%。

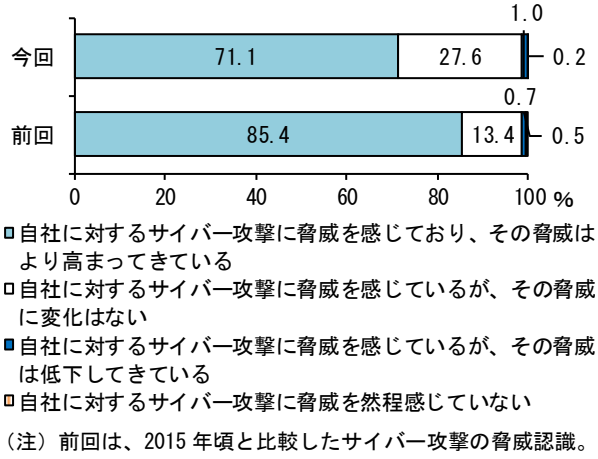
Ⅱ．サイバーセキュリティに関するアンケートの結果

１．体制面の取り組み

（１）脅威の認識と自社への攻撃の発生状況

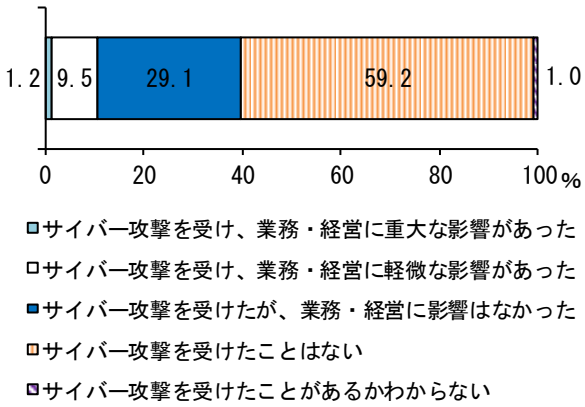
サイバー攻撃への脅威の認識についてみると、ほぼ全先が自社に対するサイバー攻撃に脅威を感じていると回答した。また、2017 年頃と比較して脅威はより高まっていると回答した先がなお 7 割強に上るなど、脅威認識が前回以降も強まる傾向にあることが窺われた（図表 7）。また、この間の自社へのサイバー攻撃事案の発生状況をみると、業務・経営に何らかの影響のある事案が発生した先（1 割強＜前回と同程度＞）と、業務・経営への影響はなかったものの攻撃を受けた先（約 3 割）を合わせた約 4 割の金融機関が、実際にサイバー攻撃を受けたと回答した（図表 8）。詳細をみると、規模の大きな先ほど攻撃を受けた経験があるとの回答割合が高い傾向にあるが、信用金庫などの地域金融機関であっても少なくない先が攻撃を受けていることが確認された。

図表 7　2017 年頃と比較したサイバー攻撃の脅威認識



（注）前回は、2015 年頃と比較したサイバー攻撃の脅威認識。

図表 8　2017 年以降のサイバー攻撃事案の発生状況



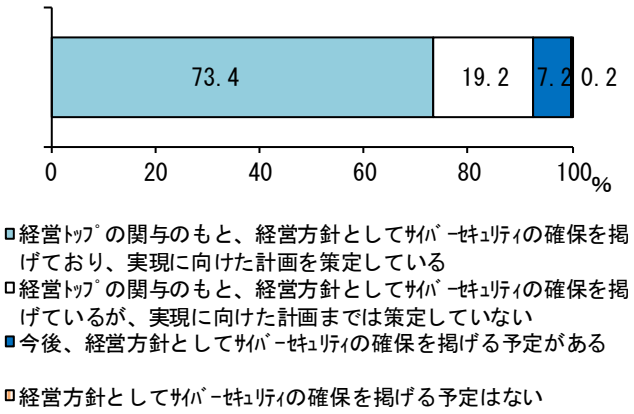
（２）組織体制

サイバー攻撃の脅威が高まるなか、それに応じた対策を講じなければ、サイバーリスクは増加する。サイバーセキュリティ対策を適切に講じていくためには、経営資源の継続的な投入が必要となるため、経営としての取組方針を掲げ、計画的に取り組む必要がある。また、金融機関がデジタル技術を活用した新しい顧客サービスや業務改革等を進めるなかにあっては、サイバーセキュリティの十分性や適切性にかかる検証が、同時並行的に行われていくことが望ましい。この点、7 割強の先では、経営トップの関与のもと、経営方針としてサイバーセキュリティの確保を掲げ、実現に向けた計画を策定していると回答した（図表 9）。前回時

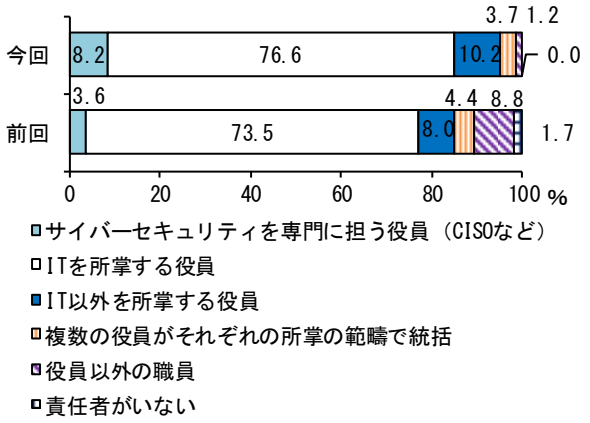
点では、「経営戦略としてサイバーセキュリティの確保を掲げ、その実現に向けロードマップを策定し、対策を講じている」との回答は約 5 割にとどまっていたが、その後、組織的な取り組みが進んでいることが確認された。

高まる脅威に組織的に対応していくうえでは、サイバーセキュリティを統括する責任者の存在は欠かせない。サイバー攻撃対応を強力に進めるためには、強い権限を有する責任者がその任に当たる必要がある。この点、自社のサイバーセキュリティを統括する責任者についてみると、役員（IT を所掌する役員、サイバーセキュリティを専門に担う役員＜CISO[11]など＞）との回答が 8 割強まで増加した。また、役員以外の職員が統括する先や責任者がいない先は、今回は殆どみられず（図表 10）、役員をサイバーセキュリティの統括責任者に据える動きが概ね業界全体に浸透したことがみてとれる。

図表 9 サイバーセキュリティの経営方針・計画



図表 10　サイバーセキュリティの統括責任者



サイバー攻撃の手法が巧妙化しており、完全には防ぎきれない可能性が高まっているため、攻撃を受けた場合に備え、被害が拡大しないように速やかに対応できる専門組織[12]を整備する必要があるほか、インシデント発生時の対応要員や手順を予め定めておく必要がある。また、サイバー攻撃を受けていない平時であっても、脅威動向や攻撃手法等の情報収集や、関係部署や外部機関との連携、経営陣への定期報告、体制整備にかかる各種の企画などを行うことが求められる。こうした点を踏まえると、インシデント対応組織は、常設組織として設置されていることが望ましい。

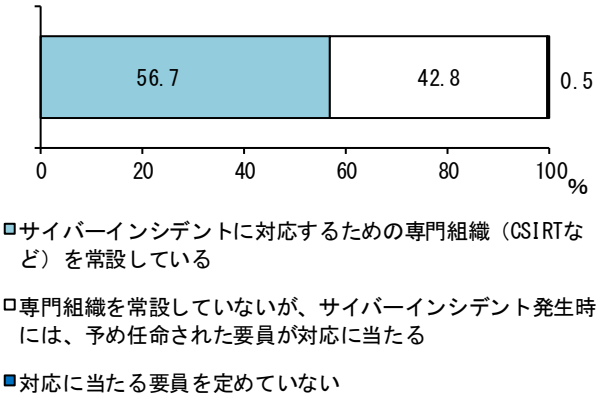
アンケート結果をみると、サイバーインシデントに対応するための専門組織を常設している先は 6 割弱と、前回（約 2 割）対比大幅に増加した（図表 11）。常設していない先でも、予め任命された要員がサイバーインシデント対応に当たる体制となっているとの回答が大部

[11] Chief Information Security Officer の略。

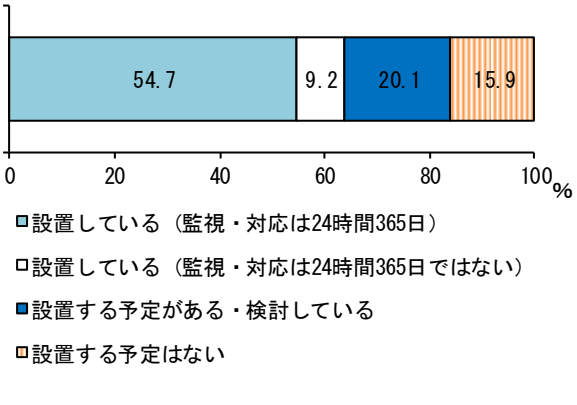
[12] 例えば、CSIRT（Computer Security Incident Response Team）がこれに該当する。

分を占めた。セキュリティ関連の監視・分析等を行う組織を設置（SOC[13]など＜外部委託含む＞）している先についても、6 割強と、前回（4 割強）対比増加した（図表 12）。

図表 11 サイバーインシデントに対応するための組織の整備状況

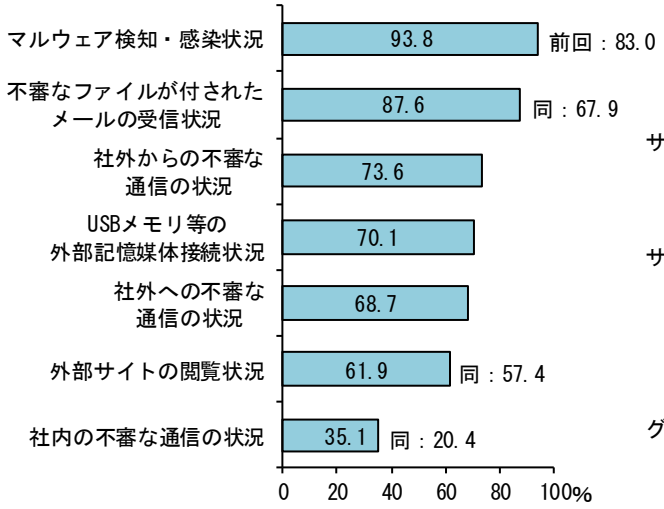


図表 12 セキュリティ関連の監視・分析等を行う組織の設置状況

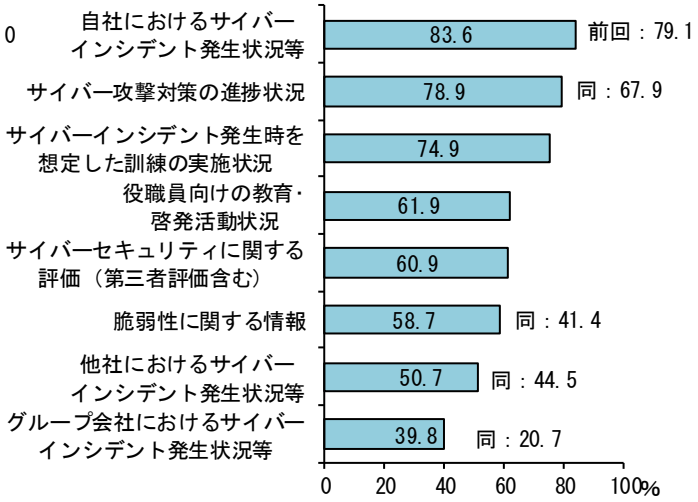


セキュリティに関する監視対象では、マルウェア検知・感染や、感染につながり得る不審なファイルが付されたメール受信状況は 9 割前後、外部記憶媒体の接続や外部サイトの閲覧状況についても 6 割以上の先が監視している。また、社外との通信状況については 7 割前後が監視している。社内での通信については、3 割台半ばではあるが、前回（約 2 割）対比では増加した（図表 13）。また、経営陣へ定例報告している内容については、前回から拡充されている状況が窺われた（図表 14）。

図表 13 セキュリティに関する監視



図表 14 経営陣への定例報告内容



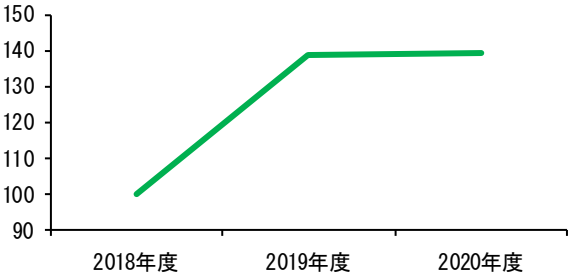
（注）グループ会社を持たない先も分母に含めている。

脅威の高まりに応じて、必要な予算や人材といった経営資源の確保に計画的に努める必要がある。サイバーセキュリティ関連の経費の実績と計画をみると、増加傾向にあり、経費を

[13] Security Operation Center の略。ネットワークやサーバ、ファイアウォール等の機器への攻撃状況など、セキュリティ関連の監視・分析等を行う組織。

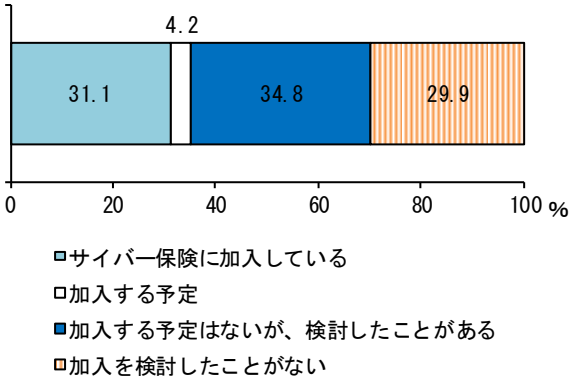
かけて対策に取り組んでいる状況が窺われた（図表 15）。また、サイバー攻撃を受け、マルウェア感染等が生じてしまった場合、原因や被害状況の調査、機器交換等のため、相応の金銭的・人的な負担が発生することとなる。そうした負担に備えて、3 割強の先ではサイバー保険を活用している（図表 16）。

図表 15 サイバーセキュリティ関連の経費



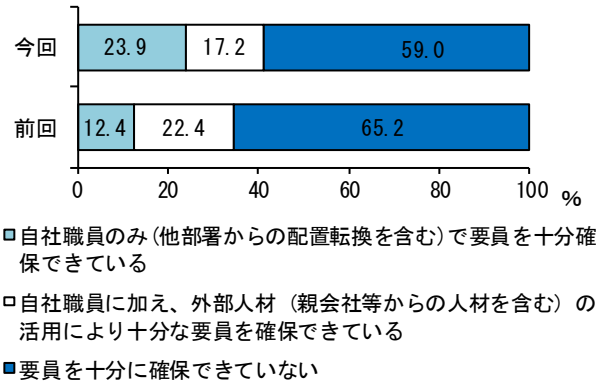
（注）2018 年度実績、2019 年度見込み、2020 年度計画の全てに回答があった先について集計。個別金融機関の 2018 年度実績を 100 としてその後の推移を指数化したものを単純平均。キャッシュアウトベース。

図表 16 サイバー保険の活用状況

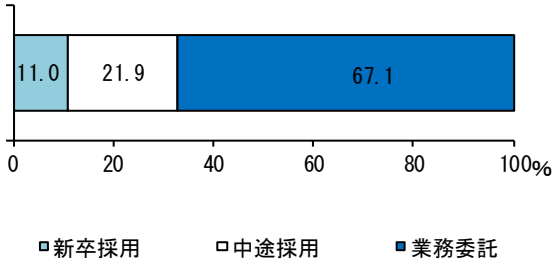


一方で、サイバーセキュリティに係る企画要員の確保状況をみると、十分に確保できていないとする先が 6 割弱に達しており、前回に引き続き、人材の不足感が強いことが確認された（図表 17）。なお、企画要員を十分に確保できていない先が想定している主な人材確保策としては、業務委託を想定する先が 7 割弱を占めた（図表 18）。

図表 17 サイバーセキュリティに係る企画要員の確保状況



図表 18 「十分に確保できていない」先が想定している主な人材確保策

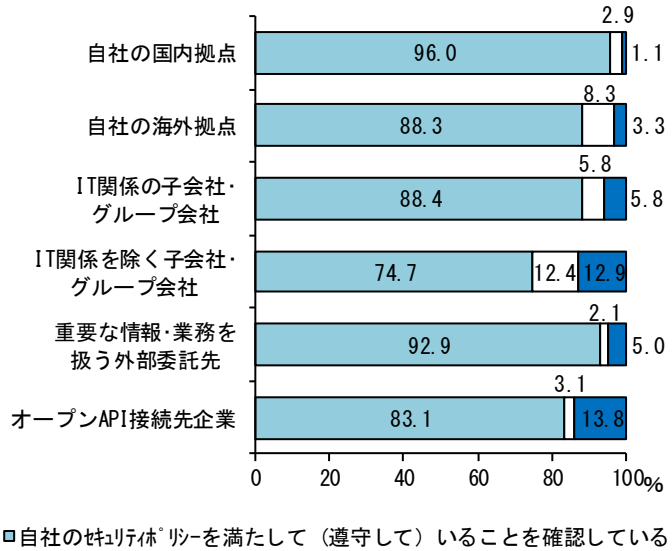


（3）サイバーセキュリティの管理体制強化・実効性の向上

サイバーセキュリティを確保するうえでは、自社のセキュリティポリシーを整備するとともに、自社の各拠点、重要な情報資産・業務を扱う外部委託先等におけるセキュリティポリシーの遵守状況を把握し必要な対策を施す必要がある。アンケート結果をみると、自社の国内外拠点、IT 関係の子会社・グループ会社、重要な情報資産・業務を扱う委託先については、

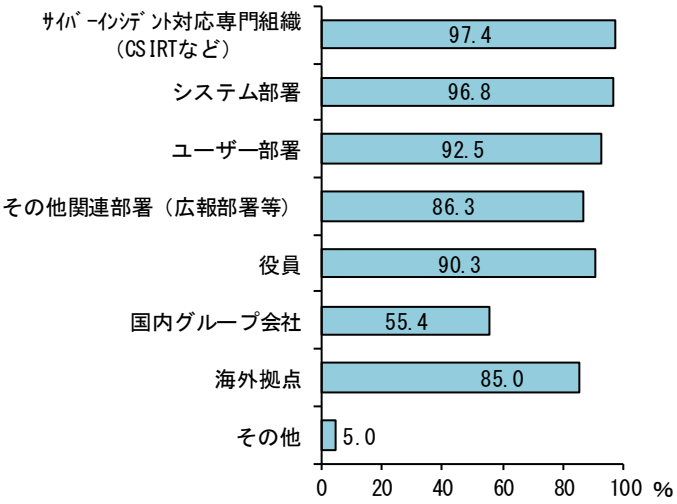
自社のセキュリティポリシーを満たしていることを確認している先が大部分を占めた。一方、オープン API 接続先企業については、1 割強の先ではサイバーセキュリティの管理状況を把握しておらず、改善の余地があることが明らかとなった（図表 19）。

図表 19　自社のセキュリティポリシーの遵守状況の把握



（注）分母は、対象組織があると回答した先。

図表 20　2017 年度以降、サイバー攻撃を想定した啓発・教育・訓練の実施対象者



（注）分母は、「専門組織」については図表 11 の設問にて「常設している」と回答した先、「国内グループ会社」、「海外拠点」については図表 19 の設問にてそれぞれ「子会社・グループ会社がある」、「海外拠点がある」とした先が対象。それ以外は全先が対象。

サイバー攻撃を受けた場合に適切に対応するためには、平時より、随時の注意喚起や定期的な啓発・教育、標的型メール訓練等を、海外拠点を含む自社の役職員や子会社・グループ会社向けに広く実施することが効果的である。アンケート結果をみると、2017 年度以降、インシデント対応組織やシステム部署の職員（9 割台半ば）のみならず、ユーザー部署や役員（約 9 割）を含む幅広い役職員を対象に啓発・教育・訓練を実施する動きが業界全体に浸透してきている。もっとも、国内グループ会社では 5 割台半ばにとどまるなど、グループベースでの取り組みについては改善の余地がある（図表 20）。

2．技術面の取り組み

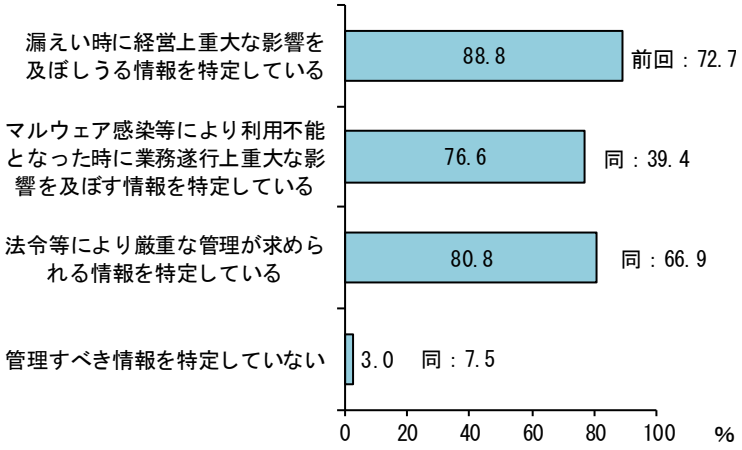
（1）守るべき情報資産の特定

サイバー攻撃の手法が巧妙化していることを踏まえると、攻撃被害を受けることを前提に、自社が守るべき重要な情報資産を予め特定し、その重要度に応じて対応策を講じることが必要である。アンケート結果をみると、「漏えい時に経営上重大な影響を及ぼしうる情報」、「利用不能となった時に業務遂行上重大な影響を及ぼす情報」、「法令等により厳重な管理が求め

られる情報」を特定している先の割合が 8 割弱～9 割弱に達した。ただし、ごく一部ながら、管理すべき情報資産を特定していない先もみられた（図表 21）。

前回対比では、上記いずれの情報資産についても、管理すべき情報資産として特定する先の割合が上昇した。特に、情報資産が利用不能となるリスクが強く認識され、「利用不能になった時に業務遂行上重大な影響を及ぼす情報を特定している」先の増加（前回：約 4 割→今回：8 割弱）が目立った。

図表 21 重要な情報資産の特定



（２）端末等への技術的な対策

コンピュータシステム・機器・通信ネットワークへの攻撃に対し、外部との接続を遮断すること、すなわち、外部記憶媒体の端末等への接続を不可とするとともに、社内の業務ネットワークとインターネットを分離することによりインターネットとの接続も断つ措置は、最も有力な対策の 1 つと考えられる。もっとも、外部との接続を遮断したとしても、設定ミスやルール違反等により、感染が生じるケースは想定し得る。また、そもそもデジタル技術活用の取り組みを強化するなかにおいては、外部との接続を遮断するとむしろ業務上支障を来すなど、業務効率性との兼ね合いから、こうした対策を完全なかたちで実施することが困難なケースも想定される。このため、外部との接続遮断以外の対策を含めて対応を検討することが求められる。

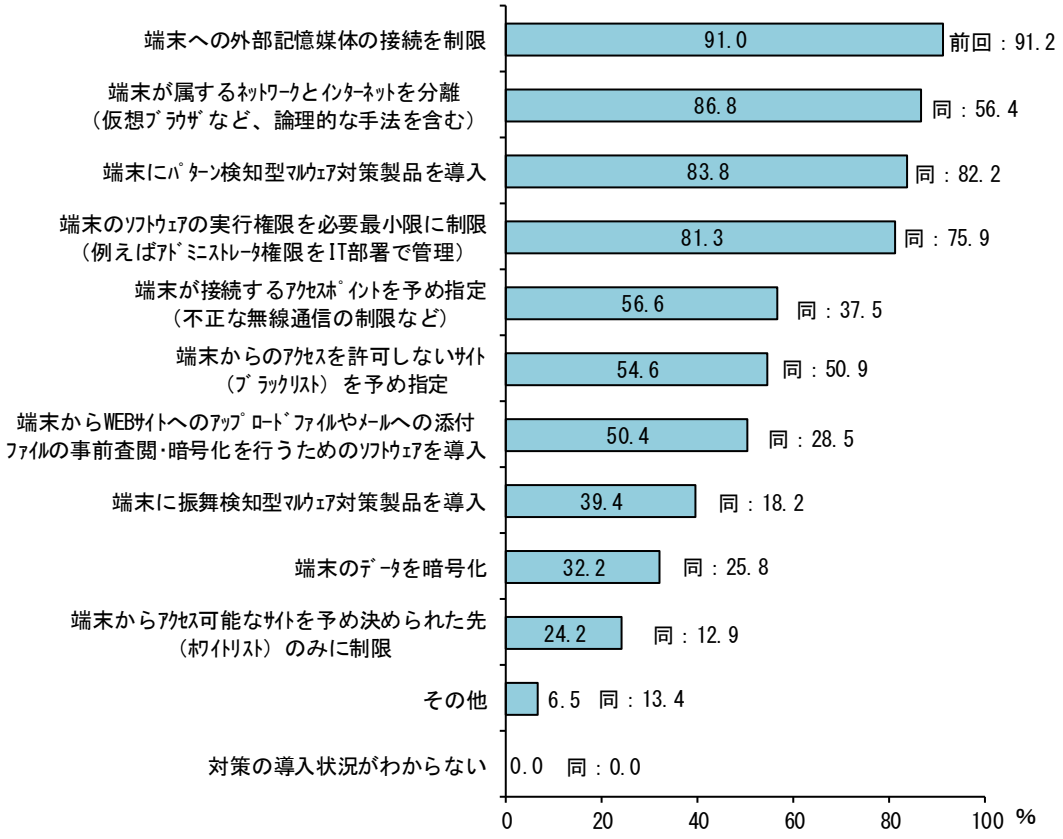
アンケート結果をみると、OA 端末（役職員が文書作成等で標準的に用いる端末）への対策としては、外部記憶媒体の接続を制限（9 割強）、ネットワークをインターネットと分離（論理的な手法[14]によるものを含む）（9 割弱）との回答が最も多かった。加えて、これら以外の

[14] 例えば、端末からインターネットにアクセスする際に経由するサーバを用意したうえで、サーバから端末への通信は画面転送のみとし、インターネットを通じたファイルの授受や外部からの遠隔操作をできないようにする手法。

様々な対策も講じている先が多いことが確認された（図表 22）。

前回との比較では、ネットワークをインターネットと分離しているとの回答割合の上昇（前回：6 割弱→今回：9 割弱）が目立った。また、振舞検知型マルウェア対策製品を導入（前回：2 割弱→今回：4 割弱）、Web へのアップロードファイルやメールへの添付ファイルの事前査閲・暗号化を行うソフトを導入（前回：3 割弱→今回：約 5 割）といった対策についても、進んでいることが明らかとなった。

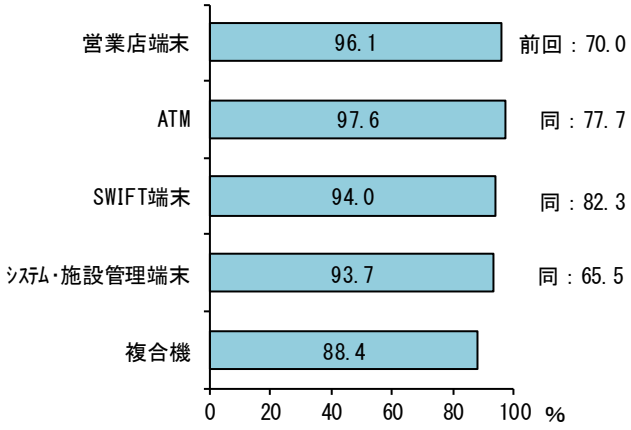
図表 22　OA 端末のサイバー攻撃対策



また、OA 端末以外では、営業店端末、ATM、SWIFT 端末についても、インターネットとの分離の動きが拡がっている。このほか、今回初めて調査を実施した複合機[15]についても、多くの先でインターネットとの分離が行われていることが確認できた（図表 23）。

[15] 複合機がインターネットと接続されている場合で、外部からの不正なアクセスを遮断するための適切な設定を怠ると、複合機上に保存された情報が流出したり、ウィルス感染や攻撃の道具として利用されたりするといった問題が発生し得る。

図表 23　OA 端末以外のインターネットとの分離状況

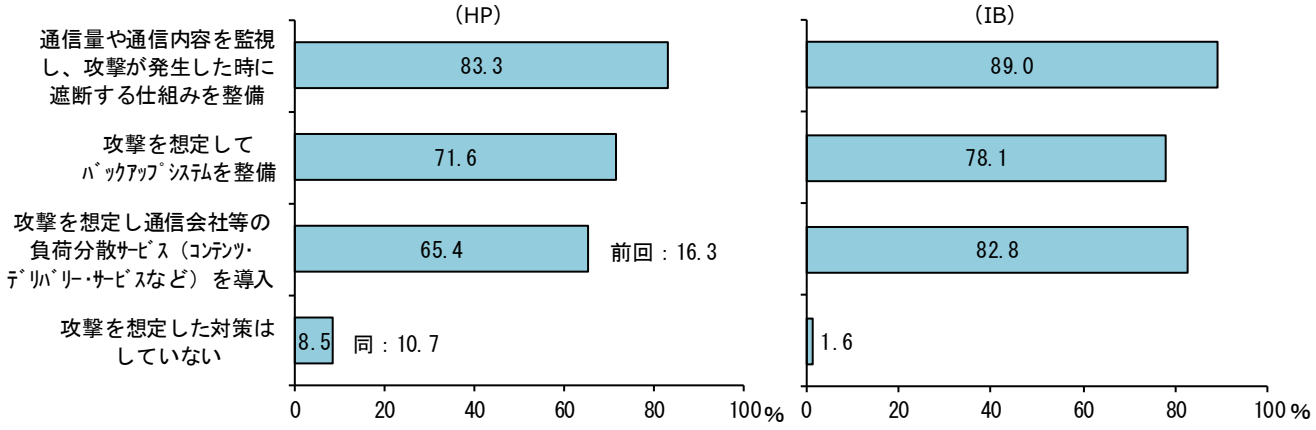


（注）分母は、各端末・機器を導入している先。

インターネットとの接続が前提となる金融機関のシステムとして、顧客向けサービスとして提供しているホームページ（以下、HP）や IB があげられる。これらについては、DoS 攻撃（DDoS 攻撃を含む）を受ける可能性があるため、予め自社が受ける可能性のある攻撃の規模を想定したうえで、対策を講じる必要がある。もっとも、DoS 攻撃の規模や手法は様々であり、十分な対策を行っているつもりでも必ず防ぎきれるとは限らないため、こうした事態に備えたコンティンジェンシープランを併せて策定しておく必要がある。

アンケート結果をみると、HP については、通信の監視と攻撃発生時の通信遮断の仕組みを導入している先が 8 割台半ばで最多となり、バックアップシステムを整備（7 割強）、負荷分散サービスを導入（7 割弱）がそれに続いた。前回対比、HP に負荷分散サービスを導入する先が大幅に増加するなど（前回：2 割弱→今回：7 割弱）、対策が進展している。また、IB については、通信の監視と攻撃発生時の通信遮断の仕組みを導入（9 割弱）、負荷分散サービスを導入（8 割強）、バックアップシステムを整備（8 割弱）の順となった（図表 24）。

図表 24　HP および IB への DoS 攻撃対策



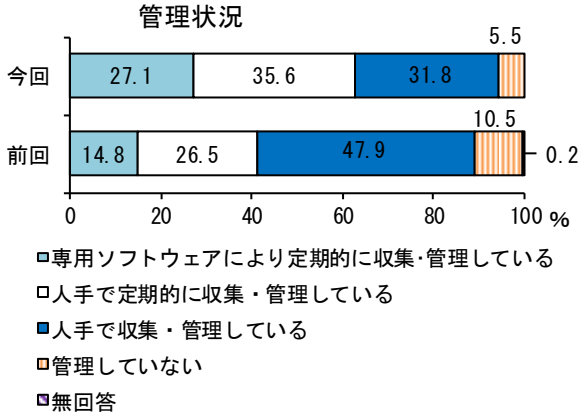
（注）分母は、上記 4 つのいずれかに相当する回答があった先。

（３）対策の実効性の向上

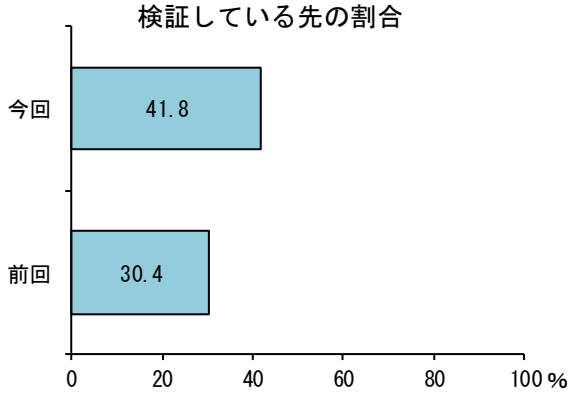
セキュリティ対策を適切に行っていると認識していても、日々発見される脆弱性のうち自社に影響するものを見逃し、重要なセキュリティパッチ[16]の適用を行わずに放置してしまう、また、メンテナンス時に認識不足から適切でない設定を行ってしまうといったリスクは常に存在する。対策の実効性を高めるうえでは、サイバーセキュリティが通常の金融機関業務とは異なる専門性を要することに鑑み、その妥当性について、第三者の専門家等による検証を行っていることが望ましい。

この点、まず、脆弱性に関するリスクを効率的に管理するうえでは、自社のシステム構成や仕様にかかる情報を定期的に収集・管理する必要がある。重要なシステムについて、OS・ソフトウェアのバージョンやセキュリティパッチの適用状況等の収集・管理体制をみると、専用ソフトウェアまたは人手により定期的に収集・管理している先は、前回から大幅に上昇（前回：4 割強→今回：6 割強）していることが確認された（図表 25）。また、技術対策の実効性を外部の専門家を活用して検証している先についても、前回から増加（前回：約 3 割→今回：4 割強）した（図表 26）。

図表 25　重要なシステムの構成情報の管理状況



図表 26　技術対策の実効性を外部の専門家が検証している先の割合

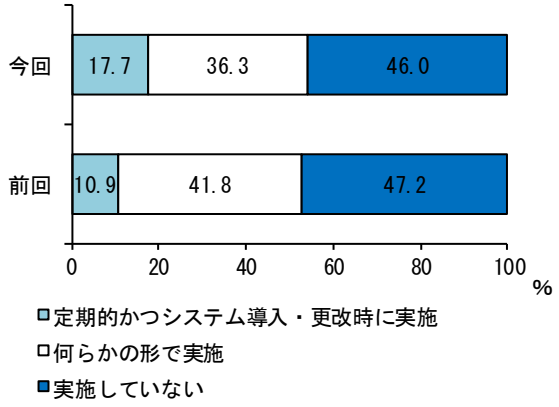


もっとも、脆弱性診断やシステムへの攻撃（侵入・破壊・サービス停止等）の試行などにより自社利用システムに対する外部からの攻撃可能性を検査する体制についてみると、「定期的かつシステム導入・更改時に検査を実施している先」は 2 割弱、それ以外の何らかの形で実施している先を含めても 5 割強にとどまり、前回から目立った体制強化はみられなかった（図表 27）。なお、脅威ベースのペネトレーションテスト（TLPT <Threat-Led Penetration Test >）やレッドチームテストと呼ばれる、自社が抱えるリスクを個別具体的に分析したうえで、攻撃者が採用する戦術、手法を再現し擬似的な攻撃を仕掛けることで、侵入・改ざんの可否や検知の可否、対応の迅速性・適切性を検証する、より実践的なテストを実施したことのある先は、上記の検査を実施している先の 2 割程度（全体の 1 割程度）にとどまっている（図

[16] 発見された OS・ソフトウェアの脆弱性を修正するプログラム。

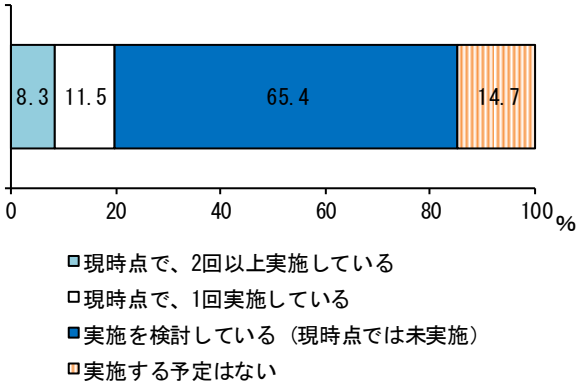
表 28)。

図表 27　脆弱性診断やシステムへの攻撃試行等による検査体制



（注）選択肢は、今回は「攻撃可能性」、前回は「侵入可能性」。

図表 28　TLPT の実施状況



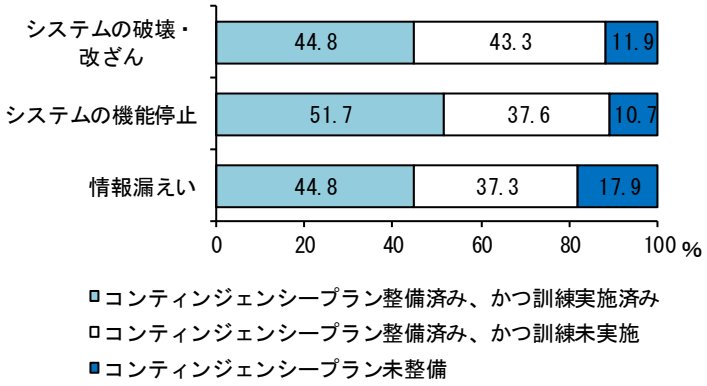
（注）分母は、図表 27 の設問で検査を実施している先。

（4）攻撃を受けた場合の対応・復旧対策

対策を施していても、攻撃手法が巧妙化するなかにあっては、攻撃の被害を防ぎきることはより困難となっている。このため、攻撃を受けた場合の効率的な対応・復旧のために、予め被害事象別のコンティンジェンシープランを整備する必要がある。加えて、同プランの実効性を検証するための訓練を実施する必要がある。

アンケート結果をみると、しばしば被害が報じられている「システムの破壊・改ざん（ランサムウェアや HP 改ざん等の被害）」、「システムの機能停止（DoS 攻撃やランサムウェア等の被害）」、「情報漏えい（マルウェアを通じた情報窃取等の被害）」については、8 割以上の先がコンティンジェンシープランを整備している。一方、同プランに基づいた訓練の実施については、システムの破壊・改ざんおよび情報漏えいで 4 割強、機能停止で 5 割強にとどまっている（図表 29）。

図表 29　サイバー攻撃（被害）別のコンティンジェンシープランの整備状況



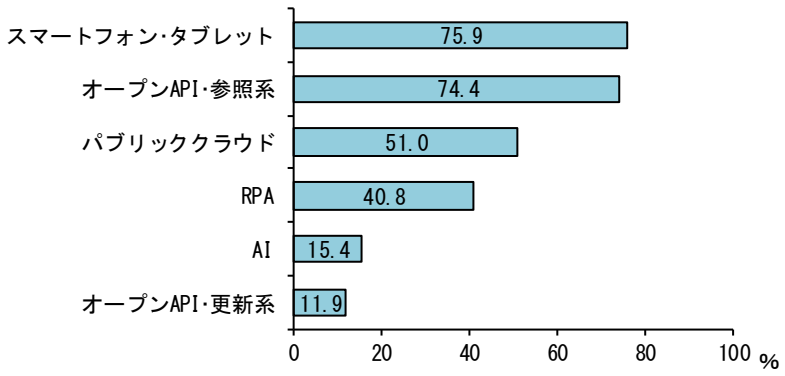
３．新たなデジタル技術の導入を踏まえた対応

昨今の金融機関を取り巻く環境をみると、スマートフォン・タブレット端末といったモバイル・インターフェースの普及に加え、AI、RPA（ロボティクス・プロセス・オートメーション）[17]やIoT、クラウドサービスなど新たなデジタル技術を活用した大きな変化が生じている。金融機関がこうした環境変化に対応し、持続的に付加価値の高いサービスを創出していくうえでは、新たなデジタル技術について、導入に伴う脅威や人為的な設定ミスによる情報漏えい等のリスクを認識し、生じ得るサイバー攻撃への体制整備や技術面の対応を検討することが必須である。

アンケート結果のうち、新たなデジタル技術の導入状況をみると、スマートフォン・タブレットは 8 割弱と高い。また、パブリッククラウド[18]の導入割合も過半に達している。この間、オープン API については、更新系（1 割強）と参照系（7 割強）[19]で大きな差がみられている（図表 30）。

導入しているデジタル技術について認識しているサイバーセキュリティ上の脅威についてみると、パブリッククラウドおよびオープン API（更新系）については、導入している殆どの先が、破壊・改ざん、停止、情報漏えいの全てに関するセキュリティ上の脅威を認識している。また、オープン API（参照系）およびスマートフォン・タブレットについても、導入先のうち 9 割強の先が情報漏えいに関する脅威を認識している（図表 31）。

図表 30　導入しているデジタル技術

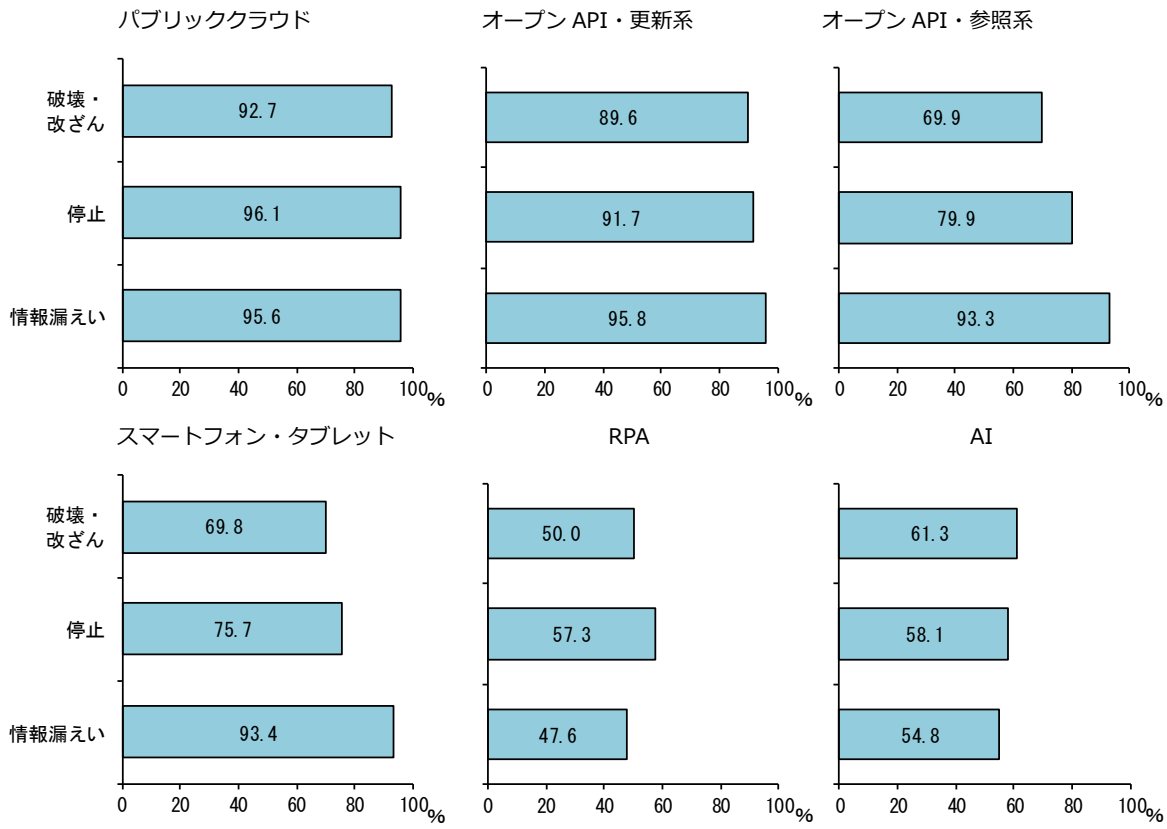


[17] 定型的な事務処理等の自動化を目的とした、端末等で動作するソフトウェア。

[18] クラウドサービスのうち、利用者が限定されず不特定多数が利用可能なサービス。

[19] 「更新系」は振込などにより口座残高などを更新することを、「参照系」は口座残高などの参照のみ行うことを指す。

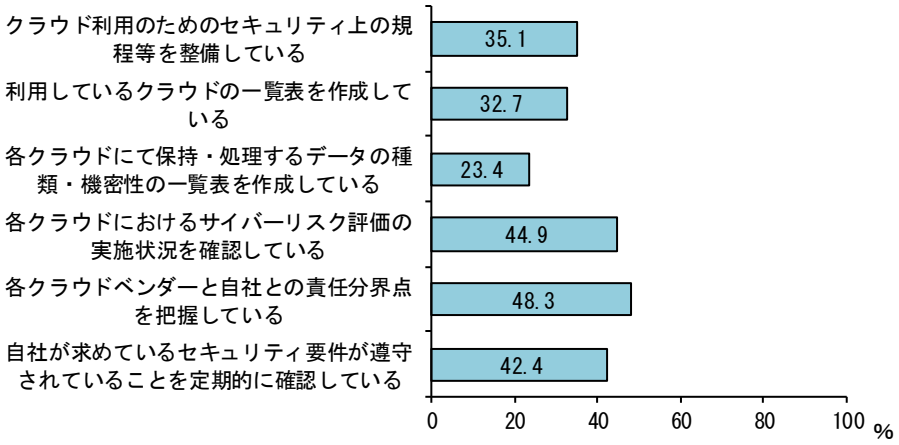
図表 31　デジタル技術の導入に伴うサイバーセキュリティ上の脅威として認識しているもの



（注）分母は、各デジタル技術を導入している先。

しかしながら、これらのうち、パブリッククラウドに関するサイバーセキュリティ管理体制をみると、十分には進んでいない（図表 32）。パブリッククラウドはインターネット空間上にあるがゆえに、設定ミス等を狙ったサイバー攻撃の標的となり易いため、経営上重要なシステムを構築する場合や重要な情報資産を扱う場合には追加的な管理体制が必要といえる。アンケート結果をみると、クラウド利用のためのセキュリティ上の規程等を整備している先は 3 割台半ば、利用しているクラウドの一覧表を作成している先は 3 割強、クラウドに保持・処理するデータの種類・機密性の一覧表を作成している先は 2 割強にとどまっている。また、各クラウドベンダーと自社との責任分界点の把握、サイバーリスク評価の実施状況の確認、自社のセキュリティ要件が遵守されていることの定期的な確認についての実施割合も 5 割に満たなかった。

図表 32　パブリッククラウド利用におけるサイバーセキュリティ体制の状況



（注）分母は、パブリッククラウド導入「有」の先。

Ⅲ．おわりに

アンケート結果から、金融機関のサイバーセキュリティ対策の状況をみると、脅威認識が前回以降も強まる傾向にあるなかで、前回時点よりも多くの金融機関がサイバーセキュリティの確保を経営上の課題と捉え、体制整備や技術対策などの取り組みを進めていることが確認できた。もっとも、体制面では、サイバーセキュリティの企画に携わる要員が引き続き不足していることや、サイバーセキュリティに関する啓発・教育・訓練のグループベースでの取り組みに改善の余地があることが確認された。また、技術面では、脆弱性診断やシステムへの攻撃試行等による検査、コンティンジェンシープランに基づいた訓練の実施について、十分には進んでいない先が少なくないことが明らかとなった。加えて、新たなデジタル技術の導入に伴う対応についても、オープン API 接続先企業におけるサイバーセキュリティの管理状況の把握や、パブリッククラウドの利用のためのサイバーセキュリティ管理体制の整備が、一部の先では十分に進んでおらず、今後の課題であることが確認された。

各金融機関のビジネスの内容やインターネットの業務上の利用状況、システム構成によって、直面するサイバー攻撃の脅威に違いがあることを踏まえれば、サイバーセキュリティの確保のために求められる取り組みも一律ではない。しかしながら、デジタル技術の進歩の動きが急速に拡がるもとで、サイバー攻撃の脅威は高まり続けることが予想されるため、金融機関が経営トップの適切な認識・関与のもとで、対策強化に向けた取り組みを続けていくことが重要である。特に、東京オリンピック・パラリンピック競技大会の開催が迫るなかで、サイバー攻撃による被害を受けることを前提とした訓練の実施など、対応が急がれる項目については、優先的な経営課題として対応していく必要がある。

日本銀行としては、今後も、考査・モニタリングやセミナーなどを通じて、金融機関の取り組みを後押ししていく方針である。