（別　紙）

サイバーセキュリティセルフアセスメントの
点検票（2023 年度）

サイバーセキュリティに関する経営層の関与

【問1】　サイバーセキュリティに関する経営方針について、あてはまるものを選択してください。

1. 経営トップ（頭取・社長・理事長等）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ており、ディスクロージャーやHP等で対外公表している 2. 経営トップ（頭取・社長・理事長等）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ている（対外公表はしていない） 3. 今後、経営方針としてサイバーセキュリティの確保を掲げる予定がある 4. 経営方針として、サイバーセキュリティの確保を掲げる予定はない	回答欄 （左記1～4から選択）

【問2】　サイバーセキュリティに関する経営計画について、あてはまるものを選択してください。

1. サイバーセキュリティに関する(単年度に加えて)複数年度の経営計画を策定している 2. サイバーセキュリティに関する単年度の経営計画を策定している 3. 今後、サイバーセキュリティに関する経営計画の策定を予定している 4. サイバーセキュリティに関する経営計画を策定する予定はない	回答欄 （左記1～4から選択）

【問3】　自組織のサイバーセキュリティを統括する責任者について、あてはまるものを選択してください。

1. サイバーセキュリティを専門に担う役員(※)（CISOなど） 2. システムリスク管理部署（サイバーセキュリティを含む）を所掌する役員 3. リスク統括部署を所掌する役員 4. システムリスク管理部署（サイバーセキュリティを含む）、リスク統括部署以外を所掌する役員 5. 複数の役員（それぞれの所掌の範疇でサイバーセキュリティを統括） 6. システムリスク管理部署（サイバーセキュリティを含む）の職員（役員以外） 7. リスク統括部署の職員（役員以外） 8. システムリスク管理部署（サイバーセキュリティを含む）、リスク統括部署以外の部署の職員（役員以外） 9. 責任者がいない	回答欄 （左記1～9から選択）

※ 役員には執行役員などの従業員役職者を含みます

【問4】 サイバーセキュリティに関し、問3で回答した自組織のサイバーセキュリティを統括する責任者に定例報告する内容、経営トップ（頭取・社長・理事長等）に定例報告する内容について、それぞれあてはまるものをすべて選択してください。

定例報告内容	サイバーセキュリティを統括する責任者 （該当するものに○）	経営トップ （頭取・社長・理事長等） （該当するものに○）
1. 自組織におけるサイバーインシデント発生状況等		
2. グループ会社におけるサイバーインシデント発生状況等		
3. 他社におけるサイバーインシデント発生状況(サイバー攻撃に関わる動向を含む)等		
4. 標的型メールや不正通信等の監視結果		
5. 自組織システムに影響が生じ得る脆弱性に関する情報		
6. サイバーセキュリティに関する評価（第三者による評価を含む）		
7. サイバーセキュリティ対策の進捗状況		
8. サイバーインシデント発生時を想定した訓練の実施状況		
9. 役職員向けの教育・啓発活動の状況		
10. その他（自由記入欄に記述してください）		
11. サイバーセキュリティに関する定例報告は行っていない		

「サイバーセキュリティを統括する責任者」の「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

「経営トップ（頭取・社長・理事長等）」の「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問5】 サイバーセキュリティに関し、問3で回答した責任者に随時報告する内容、経営トップ（頭取・社長・理事長等）に随時報告する内容について、あてはまるものをすべて選択してください。

随時報告内容	サイバーセキュリティを統括する責任者 （該当するものに○）	経営トップ （頭取・社長・理事長等） （該当するものに○）
1. 自組織システムで発生した重大インシデント		
2. 自組織に影響が生じ得る、他社で発生した重大インシデント		
3. 自組織システムに影響が生じ得ることが判明した、深刻な脆弱性（不適切な設計・設定を含む）		
4. その他（自由記入欄に記述してください）		
5. 随時報告は行っていない		

「サイバーセキュリティを統括する責任者」の「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

「経営トップ（頭取・社長・理事長等）」の「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

サイバーセキュリティに関するリスクの把握と対応

【問6】　自機関に対するサイバー攻撃による事故等の有無について、あてはまるものをすべて選択してください。
注：本問はFISCアンケートとの共通設問です。

事故等の内容	回答欄 （該当するものに○）
1. コンピュータウイルス等の感染による情報漏洩	
2. 脆弱性の悪用による情報漏洩	
3. DoS・DDoS攻撃によるサービス停止	
4. 自機関Webサイトの不正改ざん	
5. ランサムウェアによるシステムやデータの暗号化・破壊	
6. インターネット取引等における不正送金被害	
7. 自機関を騙る偽サイトや偽SNSアカウントの発生	
8. 外部委託先や外部事業者へのサイバー攻撃による自機関への被害	
9. 上記以外のコンピュータウイルス等の感染による被害	
10. その他	
11. 事故等はない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問7】　サイバーセキュリティに関する情報収集について、あてはまるものをすべて選択してください。
注：本問はFISCアンケートとの共通設問です。

取り組み内容	回答欄 （該当するものに○）
1. FISC『サイバーセキュリティインシデント情報』から収集	
2. 各都道府県警察から収集	
3. 内閣サイバーセキュリティセンター（NISC）から収集	
4. 一般社団法人金融ISACから収集	
5. サイバー攻撃対応のための各種の連携を行う組織体（※１）から収集	
6. 攻撃監視業務の委託先やシステムインテグレーター、セキュリティベンダー等から収集	
7. 脅威インテリジェンスサービス（※２）等を利用して収集	
8. 各種セミナー参加による収集	
9. インターネット(ホームページ、SNS等)、マスコミ情報、新聞報道等から収集	
10. グループ会社から収集	
11. 業界団体及び業界関連組織から収集	
12. その他から収集	
13. 情報収集活動は未実施	

※１　サイバー攻撃対応のための各種の連携を行う組織体とは、一般社団法人JPCERTコーディネーションセンター、一般財団法人日本サイバー犯罪対策センター（JC3）など
※２　ダークウェブも含め、サイバー空間に存在する情報を分析し、各金融機関が早期に認識しておくべき情報を個別に提供するサービス

「その他から収集」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問8】　サイバー攻撃のリスクに対する分析・評価の実施状況について、あてはまるものを選択してください。

注：本問はFISCアンケートとの共通設問です。

	回答欄 （左記1～4から選択）
1. サイバー攻撃をリスクとして認識し、定期的且つ必要に応じてリスク分析・評価を実施している。 2. サイバー攻撃をリスクとして認識し、定期的なリスク分析・評価を実施している。 3. サイバー攻撃をリスクとして認識し、リスク分析・評価を必要に応じて実施している。 4. サイバー攻撃を対象としたリスク分析・評価は実施していない。	

【問9】　（【問8】で1～3を選択した場合に回答してください）
リスク分析・評価にあたり、参考としているガイドライン・フレームワーク等についてあてはまるものをすべて選択してください。

注：本問はFISCアンケートとの共通設問です。

実施状況	回答欄 （該当するものに○）
1. FISC『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』	
2. 経済産業省『サイバーセキュリティ経営ガイドライン』	
3. IPA（独立行政法人情報処理推進機構）『中小企業の情報セキュリティ対策ガイドライン』	
4. NISC（内閣サイバーセキュリティセンター）『重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書』	
5. ISMS（情報セキュリティマネジメントシステム）『ISO/IEC 27001（JIS Q 27001）』	
6. PCI SSC（米国PCIデータセキュリティ基準審議会）『PCI DSS』	
7. NIST（米国商務省国立標準技術研究所）『Cybersecurity Framework』	
8. FFIEC（米国連邦金融機関検査協議会）『Cybersecurity Assessment Tool（CAT）』	
9. CIS(米国インターネット・セキュリティ・センター)『CIS Controls』	
10. Cyber Risk Institute『The Profile』（旧：FSSCC 『Cybersecurity Profile』）	
11. 米国MITRE社『ATT&CK』	
12. 総務省『テレワークセキュリティガイドライン』	
13. その他のガイドライン・フレームワーク（自由記入欄に記載してください）	
14. 参考としているガイドライン・フレームワークはない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問10】　自組織が利用する重要なシステム※のサイバーセキュリティに関するリスク評価の実施状況について、あてはまるものをすべて選択してください。

※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

注：<u>重要なシステムに対するリスク評価</u>の観点で回答してください

取り組み内容	回答欄 （該当するものに○）
1. システムの導入時や大規模更改時にリスク評価を実施している	
2. 定期的にリスク評価を実施している	
3. 随時（サイバーセキュリティに関するリスクの高まりを認識した都度）にリスク評価を実施している	
4. 評価実施時期は定めておらず、不定期でリスク評価を実施している。	
5. リスク評価は実施していない	

【問11】 （【問10】で1～4に「○」を選択した場合に回答してください）
サイバーセキュリティに関するリスク評価を実施する組織について、あてはまるものをすべて選択してください。

リスク評価実施組織	回答欄 （該当するものに○）
1. システムリスク管理部署（サイバーセキュリティを含む）	
2. リスク統括部署	
3. 第三者的な専門組織等（外部ベンダー、コンサル等）	
4. システム所管部署	
5. その他	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問12】 サイバーセキュリティに関するリスクへの対応と優先順位の決定について、あてはまるものを選択してください。

	回答欄 （左記1～5から選択）
1. リスク評価の都度、経営層の判断のもとリスク対応（低減、回避、移転、受容）の要否や優先順位を決定している 2. リスク評価の都度、システムリスク管理部署（サイバーセキュリティを含む）の判断のもとリスク対応（低減、回避、移転、受容）の要否や優先順位を決定している 3. リスク評価の都度、リスク統括部署の判断のもとリスク対応（低減、回避、移転、受容）の要否や優先順位を決定している 4. リスク評価の都度、システム所管部署の判断のもとリスク対応（低減、回避、移転、受容）の要否や優先順位を決定している 5. リスク評価結果を踏まえたリスク対応（低減、回避、移転、受容）は行っていない	

サイバーセキュリティに関する監査

【問13】 サイバーセキュリティに関する監査対象に対する監査の実施状況として、あてはまるものをすべて選択してください。

監査対象	実施状況 (1:対象年度(※１)内に実施している、2:過去に実施したことはあるが、対象年度内には実施していない、3:過去に実施したことはない)	
	1. 自組織職員(※2)(内部監査部門)による検証	2. 外部(第三者)機関(※2)による検証
1. 経営層の関与の適切性		
2. 関連法令や規制遵守の適切性		
3. サイバーセキュリティ関連の組織・予算の適切性		
4. リスク評価の適切性		
5. 重要なシステムに関する技術的対策の適切性		
6. セキュリティ対策に関するルール･手順の遵守状況		

※1　対象年度とは、令和4年4月1日から令和5年3月31日までの1年間を指します
※2　自組織職員(内部監査部門)には、持株会社等を含みます
　　外部(第三者)機関とは、監査法人やコンサルティング会社等を指します

【問14】 被監査部門以外にサイバーセキュリティに関する監査の結果報告を必須とする報告先について、あてはまるものをすべて選択してください。

報告先	回答欄 （該当するものに○）
1. 取締役会、理事会	
2. 監査委員会	
3. 経営会議	
4. 社長、頭取、理事長、CEO等	
5. 監査役会（監査役）、監事会（監事）	
6. その他（自由記入欄に記述してください）	
7. 被監査部門以外に結果報告を行っていない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問15】 被監査部門のサイバーセキュリティの指摘事項に対する改善の実施状況の確認について、監査部門が行っていることとしてあてはまるものを選択してください。

取り組み内容	回答欄 （1:はい、2:いいえ）
1. 監査部門が改善結果の報告を受けている	
2. 重要度の高い改善提案については、その改善結果を監査部門が実査にて確認している	

サイバーセキュリティに関する教育・訓練

【問16】 サイバーセキュリティに関する注意喚起・教育・訓練する内容について、あてはまるものをすべて選択してください。なお、「8. グループ会社・海外拠点を対象としたサイバーセキュリティ教育・研修」「9. 外部委託先における訓練等の実施状況の確認」への回答については「4：対象無し」が選択可能です。

1. 対象年度(※)内に実施している
2. 過去に実施したことはあるが、対象年度内には実施していない
3. 過去に実施したことはない
4. 対象無し

実施状況	回答欄 （上記1～4から選択）
1. 国内外でのインシデント発生時における役職員に対する随時の注意喚起	
2. 脆弱性検知時における役職員、外部委託先に対する随時の注意喚起	
3. 役職員全体を対象とした座学、e-learning（ビデオ、書面を含む）等による定期的な啓発	
4. 役職員全体を対象とした標的型メール訓練	
5. サイバーインシデントシナリオを想定した対応訓練	
6. 役員のみを対象としたサイバーセキュリティ教育・研修	
7. 広報等を対象としたインシデント対応を想定した対外公表に係る訓練	
8. グループ会社・海外拠点を対象としたサイバーセキュリティ教育・研修	
9. 外部委託先における訓練等の実施状況の確認	
10. 外部機関（金融庁、金融ISAC、NISC等）が主催する演習への参加	
11. その他（「1」「2」を選択した場合は自由記入欄に記載してください）	

※　対象年度とは、令和4年4月1日から令和5年3月31日までの1年間を指します

「その他」で「1」「2」を選択した場合は以下の自由記入欄に具体的に記入してください。

サイバーセキュリティ人材の確保・育成

【問17】 サイバーセキュリティ人材の確保状況について、あてはまるものを選択してください。

1. 自組織職員のみ(他部署からの配置転換を含む)で人材を十分確保できている
2. 自組織職員に加え、外部人材（親会社等からの人材を含む）の活用により十分な人材を確保できている
3. 外部人材の活用のみで十分な人材を確保できている
4. 人材を十分に確保できていない

人材の確保状況	回答欄 （上記1～4から選択）
1. 新たなデジタル技術の導入に際し、生じ得るサイバーセキュリティに関するリスク評価を行う人材	
2. サイバーセキュリティ戦略・計画の企画・立案を行う人材	
3. サイバーセキュリティに関する研修や人材育成を行う人材	
4. サイバーセキュリティの観点からシステムの設計・開発を行う人材	
5. サイバーセキュリティ脅威、脆弱性に関する情報収集やシステムへの脆弱性対応を行う人材	
6. ログの監視・モニタリングを行う人材	
7. サイバーインシデント発生時に対応を行う人材	
8. サイバーセキュリティ監査を行う人材	

【問18】 自組織内のサイバーセキュリティ人材の確保の取組について、あてはまるものをすべて選択してください。

人材確保の取組	回答欄 （該当するものに○）
1. 新卒採用の強化	
2. ウェブサイトを通した募集による中途採用	
3. エージェントサービスを利用したスカウトや人脈を活用したリファラル採用による中途採用	
4. グループ会社からの移籍	
5. 親密企業等（ベンダー・監査法人等）からの出向受け入れ	
6. その他（自由記入欄に記載してください）	
7. 自組織内のサイバーセキュリティ人材の確保の取組は実施していない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問19】 サイバーセキュリティ人材の育成の取組について、あてはまるものをすべて選択してください。

人材育成の取組	回答欄 （該当するものに○）
1. セキュリティ人材育成計画の策定	
2. サイバーセキュリティ人材の育成を配慮した人事ローテーション（長期的な配置）	
3. セキュリティベンダー、システムベンダー、外部機関等への出向	
4. 社内での講習・勉強会実施	
5. 金融ISACの活動（ワーキンググループや演習等）への参加の奨励	
6. 外部研修・セミナーへの参加の奨励（受講料の会社負担）	
7. セキュリティ資格の取得推奨（受験料・更新料の会社負担）	
8. 計画的なリスキリングの実施	
9. その他（自由記入欄に記載してください）	
10. サイバーセキュリティ人材の育成の取組は実施していない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

デジタル技術の評価

【問20】 デジタル技術の導入の有無および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について、あてはまるものを選択してください。

1. 導入しており、認識した脅威に対して対策を実施している
2. 導入しており、脅威を認識しているが対策は実施していない
3. 導入しているが脅威として認識していない
4. 導入していない

デジタル技術の導入による脅威	回答欄 （上記1～4から選択）
1. パブリッククラウドの設定不備による情報漏洩	
2. パブリッククラウドの高権限アカウントの不正利用	
3. 更新系オープンAPIへの外部からの不正アクセスによる改ざん、停止、情報漏洩	
4. 参照系オープンAPIからの情報漏洩	
5. スマホ・タブレットからの情報漏洩	
6. 在宅勤務のためのシステムに対する外部からの不正アクセスによる改ざん、停止、情報漏洩	

資産管理

【問21】 内部および外部システム※の管理簿等の整備状況について、それぞれあてはまるものを選択してください。
※内部システムとは、自組織が管理・運用しているシステム（外部委託している場合を含む）
外部システムとは、外部組織が管理・運用しているシステム（IaaS、PaaS、SaaSなどのクラウドを含む）

1. 管理簿等を作成し、IT資産管理ツール等によって変更を自動で反映している
2. 管理簿等を作成し、変更の都度更新するとともに定期的に内容を確認している
3. 管理簿等を作成し、変更の都度更新している
4. 管理簿等を作成し、定期的に内容を確認している
5. 管理簿等を作成し、不定期に内容を確認している
6. 管理簿等を作成しているが、更新はしていない
7. 管理簿等を作成していない

①内部システム 回答欄 （左記1～7から選択）

②外部システム 回答欄 （左記1～7から選択）

【問22】 自組織内の①ハードウェア、②ソフトウェアを適切に管理するための、製品名称やバージョンなどを記載している管理簿等の整備状況について、それぞれあてはまるものを選択してください。

1. 管理簿等を作成し、IT資産管理ツール等によって変更を自動で反映している
2. 管理簿等を作成し、変更の都度更新するとともに定期的に内容を確認している
3. 管理簿等を作成し、変更の都度更新している
4. 管理簿等を作成し、定期的に内容を確認している
5. 管理簿等を作成し、不定期に内容を確認している
6. 管理簿等を作成しているが、更新はしていない
7. 管理簿等を作成していない

①ハードウェア 回答欄 （左記1～7から選択）

②ソフトウェア 回答欄 （左記1～7から選択）

【問23】 （問22で1～6を選択した場合にのみ回答してください）
管理簿等で管理している情報について、以下の項目からそれぞれあてはまるものをすべて選択してください。

	回答欄 （該当するものに○）	
管理している情報	①ハードウェア	②ソフトウェア
1. 名称		
2. 製造元		
3. 型番		
4. シリアル番号		
5. ファームウェア		
6. ライセンス番号		
7. バージョン（OSを含む）		
8. インストール先（クラウドを含む）		
9. 保守・サポート期限		
10. 利用部署・利用者名		

【問24】 自組織のネットワーク接続図※の整備状況について、あてはまるものを選択してください。
※自組織内のネットワーク構成および各システム間の接続状況が把握できるもの

1. 接続図を作成し、変更の都度更新するとともに定期的に内容を確認している 2. 接続図を作成し、変更の都度更新している 3. 接続図を作成し、定期的に内容を確認している 4. 接続図を作成し、不定期に内容を確認している 5. 接続図を作成しているが、更新はしていない 6. 接続図を作成していない	回答欄 （左記1～6から選択）

アクセス管理

【問25】 重要なシステムへのアクセス権の付与等についてあてはまるものを選択してください。
※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

1. ルール・手順を定めており、対策の実施状況をモニタリングしている
2. ルール・手順を定めている
3. ルール・手順を定めていない

対策	回答欄 （上記1～3から選択）
1. 必要最小限の者に限ったアカウントの付与	
2. 利用者ごとに限った、業務上必要最小限の範囲のアクセス権(参照のみ可、更新可等)の付与	
3. 最高権限のアクセス権（特権アカウント）は、有効期限を限った付与	
4. 退職や人事異動、組織体制変更を契機としたアクセス権の都度更新	

【問26】 重要なシステムへのリモートアクセスの管理について、あてはまるものをすべて選択してください。
※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

対策	回答欄 （該当するものに○）
1. 外部からシステムへのリモートアクセス（ログイン）を行う場合の運用管理として、接続元の確認・制限、接続監視等を行っている	
2. 外部からシステムへのリモートアクセス（ログイン）を行う場合、多要素認証の仕組みを導入している	
3. 不正アクセスや情報漏洩防止のため、接続記録を取得している	
4. リモート接続用のモバイル機器および接続時の本人確認に使用する認証デバイス(アクセストークン、ICカード等)を紛失した際の対応手続きを定めている	
5. リモートアクセスで利用できるシステムを制限している	
6. リモートアクセスで利用可能なシステムのアプリケーションを制限している	
7. リモートアクセスを利用しているが、1～6の管理は実施していない	
8. リモートアクセスを利用していない	

データ保護

【問27】 データ保護のための対策としてあてはまるものを選択してください。

1. ルール・手順を定めており、対策の実施状況をモニタリングしている
2. ルール・手順を定めている
3. ルール・手順を定めていない

対策	回答欄 （上記1～3から選択）
1. 重要なデータ※の暗号化	
2. 重要なデータへのアクセス制御	
3. 重要なデータのダウンロード･印刷の制御（ダウンロード･印刷時の作業ログの記録を含む）	
4. データの外部記憶媒体への書出しの制御	
5. 外部の組織等にデータを伝送する場合の、自動的に暗号化される送信手段（オンラインストレージ、ファイル送信サービス等）の利用	

※重要なデータとは、漏洩時に経営上重大な影響を及ぼしうる情報や、破壊等により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、法令等に従った管理が求められている情報など、厳重な管理が必要な情報を含んでいるデータ

【問28】 重要なシステムにおけるランサムウェア感染等によるデータの破壊を想定したバックアップ対策として、あてはまるものを選択してください。
※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

1. ルール・手順を定めており、対策の実施状況をモニタリングしている
2. ルール・手順を定めている
3. ルール・手順を定めていない

対策	回答欄 （上記1～3から選択）
1. 複数世代の保管	
2. オフライン化など、ネットワークから直接にはアクセスできない方法で保管	
3. データの書換･削除不可能な媒体で保管	
4. バックアップからの復旧テストの定期的な実施	

監査証跡(ログ)の管理

【問29】 重要なシステムの監査証跡(ログ)について規定されている事について、あてはまるものをすべて選択してください。
※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

1. ルール・手順を定めており、対策の実施状況をモニタリングしている
2. ルール・手順を定めている
3. ルール・手順を定めていない

対策	回答欄 （上記1～3から選択）
1. 取得すべきログの特定	
2. ログの保管期間	
3. ログの無断改変･削除の禁止	
4. 定期的にログを確認し不正がないかを確認する運用	

システムの脆弱性に関する管理・対応

【問30】 脆弱性診断等により、外部や内部から自組織利用システムへの攻撃対策の実効性を検査（外部にシステム運用を委託している場合、同先での検査の実施状況を確認している場合を含む）する時期について、それぞれあてはまるものを選択してください。
なお、Webサイト(顧客向けの公開Web）やインターネットバンキングを提供していない場合は、「6.提供していない」を選択してください。

1. 定期的、かつシステム導入時や大規模更改時にも検査している
2. 定期的に検査している
3. システム導入または大規模な更改時に検査している
4. 不定期に検査している(検査実施時期についての方針はない)
5. 検査していない
6. 提供していない

実施対象	実施種別（上記1～6から選択） 脆弱性診断（Webアプリケーション）	実施種別（上記1～6から選択） 脆弱性診断（プラットフォーム）
1. OA環境※		
2. Webサイト(顧客向けの公開Web)		
3. インターネットバンキングシステム		

※以下を対象とした診断としてご回答ください
・Web閲覧システム（仮想ブラウザやインターネット用仮想端末を提供するシステム及び、インターネット接続に必要なProxyやDNS等）
・メールシステム、ファイルサーバ
・内部環境のセキュリティ上の根幹となる機器（Active Directoryサーバ等）

【問31】 脆弱性診断等により、モバイルアプリ（※1）への攻撃対策の実効性を検査（外部にシステム運用を委託している場合、同先での検査の実施状況を確認している場合を含む）する時期について、動的脆弱性診断（※2）、静的脆弱性診断（※3）それぞれあてはまるものを選択してください。
なお、モバイルアプリを提供していない場合は、すべて「6.提供していない」を選択してください。

※1　モバイルアプリとは、スマートフォンやタブレット端末上で動作するアプリケーションのこと
※2　動的脆弱性診断とは、プログラムやソフトウェア製品に対して動作状態で行うテスト（DAST）
※3　静的脆弱性診断とは、プログラムのソースコードから検査するテスト（SAST）

1. 定期的、かつシステム導入時や大規模更改時にも検査している
2. 定期的に検査している
3. システム導入または大規模な更改時に検査している
4. 不定期に検査している(検査実施時期についての方針はない)
5. 検査していない
6. 提供していない

実施対象	実施種別（上記1～6から選択） 動的脆弱性診断（モバイルアプリ）	実施種別（上記1～6から選択） 静的脆弱性診断（モバイルアプリ）
1. モバイルアプリ		

【問32】 ペネトレーションテスト（※１）および脅威ベースのペネトレーションテスト等（※２）のこれまでの実施状況について、それぞれあてはまるものを選択してください。（本設問は、令和5年3月31日までの過去の実績（令和4年3月以前を含む）についてご回答ください。）

※１　ペネトレーションテストとは、擬似的なマルウェアを利用したり、脆弱性･設定不備等を悪用したりするなど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･適切性を検証するテスト

※２　脅威ベースのペネトレーションテスト等とは、自組織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、手法を再現し疑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

1. 2回以上実施している
2. 1回実施し、次回の実施を予定している
3. 1回実施し、次回の実施予定はない
4. 実施を検討している（現時点では未実施）
5. 実施する予定はない

テスト内容	回答欄 （上記1～5から選択）
1. ペネトレーションテスト	
2. 脅威ベースのペネトレーションテスト等	

【問33】 自組織システムの深刻な脆弱性が判明した場合のパッチの適用方針について、それぞれあてはまるものを選択してください。

1. 直ちにパッチを適用している
2. 一定の対応期間を定めてパッチを適用している
3. 保守等定期的なタイミングでパッチを適用している
4. システム更改時にパッチを適用している
5. 原則としてパッチを適用しない方針としている
6. パッチ適用に関する方針はない

システム・端末	回答欄 （上記1～6から選択）
1. インターネットとつながっている※システム・端末	
2. インターネットとつながっていないシステム・端末	

※インターネットに接続しているシステムとの通信がある場合を含みます

【問34】 深刻な脆弱性に対してパッチを適用するか否かはどのような判断基準に基づいているか、あてはまるものをすべて選択してください。

判断基準	回答欄 （該当するものに○）
1. CVSSなどの外部の情報提供機関が定めた指標	
2. 当局や金融ISACからの注意喚起	
3. システムベンダーによる推奨情報	
4. システム特性（システムの重要度、取り扱う情報、インターネットにつながっているか否か、など）	
5. 攻撃コードの公開有無	
6. 攻撃情報の有無	
7. 社内有識者による個別判断	
8. その他（自由記入欄に記載してください）	
9. 判断基準はない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問35】 重要なシステムに影響を与える可能性がある深刻な脆弱性に対してパッチを適用しない（脆弱性の影響を受けないための対策＜特定機能の無効化等の脆弱性緩和策＞で済ませる、または脆弱性対応しない）場合の対応についてあてはまるものを選択してください。
なお、深刻な脆弱性に対してすべてパッチ適用をしている組織は、適用しない場合を想定してご回答をお願いします。

※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

	回答欄 （左記1～4から選択）
1. パッチを適用しない場合のリスクが受容できることをシステムリスク（サイバーセキュリティを含む）を所掌する役員が承認している 2. パッチを適用しない場合のリスクが受容できることをシステムリスク管理部署（サイバーセキュリティを含む）が承認している 3. パッチを適用しない場合のリスクが受容できることを当該システム所管部署が承認している 4. 対応しない場合のリスクは考慮していない	

サイバー攻撃に関する技術的な対策

【問36】 OA端末※のサイバー攻撃対策について、あてはまるものをすべて選択してください。
※OA端末とは、職員が文書作成等で標準的に用いる端末を指します

対策	回答欄 （該当するものに○）
1. 端末が属するネットワークとインターネットを分離している （物理的な手法による分離、および仮想ブラウザなど論理的な手法によるものを含む）	
2. 端末のブラウザに表示させるWebコンテンツの実行環境を分離している （無害化ソリューションの導入など）	
3. 端末からアクセス可能なサイトを制限している	
4. 端末のソフトウェアの実行権限を必要最小限に制限している （例えばアドミニストレータ権限をシステム所管部署で管理している）	
5. 端末にパターン検知型マルウェア対策製品を導入している	
6. 端末に振舞検知型マルウェア対策製品(EDRを含む)を導入している	
7. 端末への外部記憶媒体の接続を制限している	
8. 端末が接続するアクセスポイントを予め指定している（不正な無線通信の制限等）	
9. 端末にログインする際、多要素認証の仕組みを導入している	
10. 1～9のOA端末のサイバー攻撃対策はすべて実施していない	

【問37】 自組織外部との境界でのサイバー攻撃対策について、あてはまるものをすべて選択してください。

対策	回答欄 （該当するものに○）
1. ファイアウォールによるアクセス制御を行っている	
2. IDS/IPS※による不正侵入の検知・防止を行っている	
3. 不審なファイルやリンクが記載されたメールのフィルタリングを行っている	
4. 外部からの暗号化されたSSL/TLS通信を復号して、通信の中身を検査している	
5. プロキシサーバを経由しないインターネットとの通信を遮断している	
6. VPN・RDP等の侵入経路となりうる機器の特定と脆弱性対策を行っている	
7. 認証機能によるインターネットとのアクセス制御を行っている	
8. 1～7のサイバー攻撃対策はすべて実施していない	

※IDS（Intrusion Detection System）とは、ネットワーク上の通信を監視し、不正侵入やマルウェアなど不審な通信を検知・通知するシステム
IPS（Intrusion Prevention System）とは、検知した不正な通信を自動的に遮断する機能を備えているシステム

【問38】 Webサイト(顧客向けの公開Web）やインターネットバンキングを提供している場合は、それぞれのサイバー攻撃対策について、あてはまるものをすべて選択してください。

対策	回答欄 （該当するものに○） Webサイト （顧客向けの公開Web）	回答欄 （該当するものに○） インターネットバンキング システム
1. ファイアウォールによるアクセス制御を行っている		
2. IDS/IPSによる不正侵入の検知・防止を行っている		
3. WAF※を用いた不正通信の検知・遮断を行っている		
4. Webサイトの改ざん検知を行っている		
5. システムリソース(ネットワークトラフィック量、メモリ等)を監視している		
6. DoS・DDoS攻撃対策(通信会社等の負荷分散サービス(コンテンツ・デリバリー・サービス等))を導入している		
7. Webサイト(顧客向けの公開Web）/インターネットバンキングを提供しているが、1～6の対策は実施していない		
8. Webサイト(顧客向けの公開Web）/インターネットバンキングを提供していない		

※WAF(Web Application Firewall)とは、Webサイトと利用者の間で交わされるhttp（httpsを含む）通信の内容を解析し、攻撃等の不正な通信を自動的に遮断するソフトウェア、もしくはハードウェアのこと

【問39】 顧客向けにモバイルアプリを提供している場合は、モバイルアプリのセキュリティ対策について、あてはまるものを選択してください。

モバイルアプリのセキュリティ対策	回答欄 (1:はい、2:いいえ、 3:提供していない)
1. 送受信データへの保護対策	
2. 端末保存データへの保護対策	
3. サポート切れＯＳでの動作を制限	
4. 多要素認証方式の採用	
5. リバースエンジニアリング対策の実施	
6. サードパーティ製品（モバイルアプリや同提供基盤等に使用される他社の製品）の脆弱性情報の収集	
7. セキュアな暗号方式の利用	
8. 異常取引の検知	

【問40】 その他のサイバー攻撃対策の導入状況や検討状況について、あてはまるものを選択してください。

対策	回答欄 （1:対応済、2:対応中、3:未対応）
1. 組織内に侵入したマルウェア等の活動範囲を限定する仕組み（ネットワークのマイクロセグメンテーションを含む）の導入	
2. 組織内のサーバへの振舞検知型マルウェア対策製品(EDRを含む)の導入	
3. 組織内のユーザによる不審な活動を検出する仕組み（UEBAを含む）の導入	
4. クラウドサービスに導入されたセキュリティポリシーを検証する仕組み（CASBを含む）の導入	
5. 内部システムおよび外部システムの特権IDを一元的に管理する仕組み（PAMを含む）の導入	
6. セキュリティの運用を統合して対応を自動化するソリューション（SOARを含む）の導入	

サイバーインシデントの検知

【問41】 重要なシステムのセキュリティ関連の監視・分析等を行う組織（SOCなど（外部に委託している場合を含む））について、あてはまるものを選択してください。
※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

	回答欄 （左記1～4から選択）
1. 設置している（監視・対応は24時間365日） 2. 設置している（監視・対応は24時間365日ではない） 3. 設置する予定がある・検討している 4. 設置する予定はない	

【問42】 （【問41】で1～3を選択した場合に回答してください）
SOC等サイバーセキュリティの監視・分析等を行う組織でのモニタリング内容について、あてはまるものをすべて選択してください。

サイバーセキュリティの監視内容	回答欄 （該当するものに○）
1. マルウェア検知・感染状況	
2. ファイルが付されたメールの受信状況	
3. 外部サイトの閲覧状況	
4. 外部からの通信状況（Webサイト(顧客向けの公開Web)への通信を含む）	
5. 外部への通信の状況	
6. 内部の通信の状況	
7. USBメモリ等の外部記憶媒体の接続状況	
8. 重要な情報・業務を扱う委託先の自組織システムへの接続状況	
9. 自組織内ネットワークへの端末の接続状況	
10. 自組織内ネットワークにおける不審な活動状況（端末やサーバの不審な動作や、各種ログを関連付けて分析した場合の不整合等の状況）	
11. その他（自由記入欄に記載してください）	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

サイバーインシデント対応・業務復旧の態勢

【問43】 サイバーインシデント発生時の対応要員（親会社等を含む）について、あてはまるものを選択してください。

	回答欄 （左記1～3から選択）
1. サイバーインシデントに対応するための専門組織（CSIRTなど）を常設している 2. 専門組織を常設していないが、サイバーインシデント発生時には、予め任命された要員が対応に当たる 3. サイバーインシデント発生時に対応に当たる要員を定めていない	

【問44】 業界団体や業界関連組織、外部機関（金融ISAC等）の情報共有先への協力（情報提供）方針について、あてはまるものをすべて選択してください。

協力状況	回答欄 （該当するものに○）
1. 自組織で発生したサイバーインシデントの情報を提供することとしている	
2. 自組織で把握した不正な通信先の情報を提供することとしている	
3. 自組織で把握した攻撃の特徴を提供することとしている	
4. 自組織で把握した攻撃予告等の情報を提供することとしている	
5. 自組織で受信した標的型攻撃メールの情報を提供することとしている	
6. 必要に応じて都度判断することとしている	
7. 情報は提供しないこととしている	
8. その他（自由記入欄に記載してください）	
9. 方針は定めていない	

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

【問45】 インシデント発生時の被害拡大防止のためのルール・手順の整備について、あてはまるものを選択してください。

整備状況	回答欄 （該当するものに○）
1. 発生事象への対応の優先順位付け（トリアージ）を行う基準がある	
2. 意思決定や指示を行う責任者および責任者が不在の際の権限移譲のルール・手順がある	
3. マルウェア感染が疑われた段階で、即座にネットワークと切り離すルール・手順がある	
4. 不正アクセスが疑われた段階で、即座にアクセス元の遮断やアクセス経路となり得るネットワークと切り離すルール・手順がある	
5. 不正ログインが疑われた段階で、即座にアカウントの凍結やアクセス経路となり得るネットワークと切り離すルール・手順がある	
6. インシデント発生を背景にシステムを停止するルール・手順がある	
7. インシデントが発生した場合の対外公表に対応するルール・手順がある	
8. システム停止時において代替手段で事業を継続するルール・手順がある	
9. システムの再開判断基準がある	
10. 休日・夜間にインシデントが発生した場合の対応に係るルール・手順がある	
11. 1～10の基準・ルール・手順はない	

【問46】 インシデント対応（訓練・演習を含む）実績を踏まえた態勢の強化状況としてあてはまるものを選択してください。

1. インシデント対応実績を踏まえ、必要に応じて態勢（規程・連絡先・コンティンジェンシープラン・要員数等）や技術的対策の更新を実施 2. インシデント対応実績を踏まえ、必要に応じて態勢の更新のみを実施 3. インシデント対応実績を踏まえ、必要に応じて技術的対策の更新のみを実施 4. インシデント対応実績を踏まえ、態勢や技術的対策の更新は実施していない 5. インシデント対応実績はない	回答欄 （左記1～5から選択）

【問47】 サイバーレジリエンス（被害を受けた場合の対応・復旧力）向上の観点から、サイバー攻撃別のコンティンジェンシープランの取組内容について、それぞれあてはまるものを選択してください。

【攻撃に対応するコンティンジェンシープランの有無等】

1. サイバー攻撃別のコンティンジェンシープランの有無(1:有り、2:無し)
※「2:無し」の場合は、取組内容2～5の回答は不要です
2. 目標復旧時間設定の有無(1:有り、2:無し)
3. コンティンジェンシープランには、外部委託先へのサイバー攻撃を想定した対応が含まれている
(1:はい、2:いいえ)

【コンティンジェンシープランの訓練・演習の実施状況】

4. 攻撃別の訓練・演習実施の有無(1:対象年度(※)内に実施している、2:過去に実施したことはあるが、対象年度内には実施していない、3:過去に実施したことはない)
5. 外部委託先が、コンティンジェンシープランの訓練・演習に参加している(1:はい、2:いいえ、3:対象無し)

サイバー攻撃	攻撃に対応するコンティンジェンシープランの有無等			コンティンジェンシープランの訓練・演習の実施状況	
	1. (1:有り、 2:無し)	2. (1:有り、 2:無し)	3. (1:はい、 2:いいえ)	4. (上記の1～3から選択)	5. (1:はい、 2:いいえ、3:対象無し)
1. Webサイトの改ざん					
2. DDoS攻撃					
3. ランサムウェア攻撃					

※ 対象年度とは、令和4年4月1日から令和5年3月31日までの1年間を指します

【問48】 サイバー攻撃（被害）発生時の関係者への連絡先・伝達ルートの整備状況について、あてはまるものをすべて選択してください。なお、「5. 外部委託先」「６. 自組織のグループ会社」「13. その他」への回答については「4：対象無し」が選択可能です。

連絡対象	回答欄 (1:文書化し、周知している、2:文書化している、3:文書化していない、4:対象無し)
1. 自組織内の緊急連絡網	
2. 所管省庁・日本銀行	
3. 業界団体及び業界関連組織	
4. 顧客	
5. 外部委託先	
6. 自組織のグループ会社	
7. マスコミ・報道機関	
8. 外部機関（金融ISAC、FISC等）	
9. 脆弱性・インシデント情報の届出受付機関（IPA、JPCERT等）	
10. セキュリティ専門の民間企業	
11. 都道府県警察	
12. 個人情報保護委員会	
13. その他（回答欄で「１」「2」を選択した場合は、自由記入欄に記載してください）	

「その他」で「１」「2」を選択した場合は以下の自由記入欄に具体的に記入してください。

サードパーティ等の管理

【問49】 自組織および海外拠点や関連会社、サードパーティ（※１）に対するサイバーセキュリティの管理、モニタリングの状況について、それぞれあてはまるものをすべて選択してください。

対象組織	①対象組織の有無（1:有り、2:無し） 「2:無し」の場合は、②自組織のセキュリティポリシーの遵守状況及び③左記に係るモニタリング等の状況の回答は不要です	②自組織のセキュリティポリシーの遵守状況（択一） 1.自組織のセキュリティポリシーを満たしている（遵守している）ことを確認している（※4） 2.自組織のセキュリティポリシーを満たしていない（遵守できていないものがある）ことを認識している 3.サイバーセキュリティの管理状況を把握していない	③左記に係るモニタリング等の状況	
			対象組織が実施すべきサイバーセキュリティ対策状況（点検、監査等を含む）について、評価している（該当するものに〇）	対象組織のサイバーセキュリティに関するリスクについて評価、分析、格付け等を実施するサービスを利用している（該当するものに〇）
1. 国内拠点（国内に所在する本部・本支店・事務所等）				
2. 自組織の海外拠点				
3. IT関係の子会社・グループ会社				
4. IT関係を除く子会社・グループ会社				
5. 外部委託先（※２）（ただし、クラウド事業者は７に記載してください）				
6. オープンAPI接続先企業				
7. クラウド事業者（※３）				
8. キャッシュレス決済口座等の決済サービスを連携している事業者				

※１　サードパーティとは、自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織を指します。
（例：システム子会社やベンダー等の外部委託先、クラウド等のサービス提供事業者、資金移動業者等の業務提携先）
※２　外部委託先とは、業務を委託している組織（金融機関等が金融サービスを提供するために外部委託するシステム（共同センター等を含む）のベンダーなど。形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む）
ただし、クラウド事業者については「クラウド事業者についての回答欄」に記載してください。
※３　クラウド事業者とは、IaaS、PaaS、SaaSの提供事業者
※４　②1.の選択肢は、自組織のセキュリティポリシーを満たしていない（遵守できていないものがある）が、代替策等を適切に講じていることを確認している場合を含みます

【問50】 重要なサードパーティ（※）のサイバーセキュリティに関するリスクの管理状況について、あてはまるものを選択してください。
※　重要なサードパーティとは、自組織として業務運営上重要と認識しているサードパーティ

	回答欄（左記1～4から選択）
1. 重要なサードパーティ、また、それらが提供するサービス等のサイバーセキュリティに関するリスクを統括部署にて一元的に管理している 2. 重要なサードパーティ、また、それらが提供するサービス等のサイバーセキュリティに関するリスクを各所管部署にて管理している 3. 重要なサードパーティ、また、それらが提供するサービス等のサイバーセキュリティに関するリスクを管理していない 4. 重要なサードパーティは存在しない	

（【問50】で1～3を選択した場合に回答してください）

【問51】 重要なサードパーティ（※1）の選定時および選定後のサイバーセキュリティに関するリスク評価の状況について、あてはまるものをすべて選択してください。
回答に際しては、外部委託先（※2）、クラウド事業者（※3）、外部委託先及びクラウド事業者を除くサードパーティ（※4）のそれぞれの回答欄について選択してください。

なお、上記の問49の 5. 外部委託先において、①対象組織を「2:無し」と回答した先は外部委託先についての回答は不要です。
また、7.クラウド事業者において、①対象組織を「2:無し」と回答した先はクラウド事業者についての回答は不要です。

※1　重要なサードパーティとは、自組織として業務運営上重要と認識しているサードパーティ
※2　外部委託先とは、業務を委託している組織（金融機関等が金融サービスを提供するために外部委託するシステム（共同センター等を含む）のベンダーなど。形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む）
ただし、クラウド事業者については「クラウド事業者についての回答欄」に記載してください。
※3　クラウド事業者とは、IaaS、PaaS、SaaSのサービス提供事業者
※4　外部委託先及びクラウド事業者を除くサードパーティとは、上記※2及び※3以外のサードパーティ
（例：業務提携関係にある電代業者、資金移動業者）

	リスク評価の実施状況	外部委託先についての回答欄（該当するものに○）	クラウド事業者についての回答欄（該当するものに○）	外部委託先及びクラウド事業者を除くサードパーティについての回答欄（該当するものに○）
重要なサードパーティの選定時	1. 書面によるリスク評価を行っている			
	2. ヒアリングによるリスク評価を行っている			
	3. 現地調査などの目視確認によるリスク評価を行っている			
	4. 委託先のリスク評価サービスを提供する外部業者を利用してリスク評価を行っている			
	5. 1～4のリスク評価は行っていない			
	6. 該当なし（重要なサードパーティは存在しない）			
重要なサードパーティの選定後	7. 定期的に書面によるリスク評価を行っている			
	8. 定期的にヒアリングによるリスク評価を行っている			
	9. 定期的に現地調査などの目視確認によるリスク評価を行っている			
	10. 定期的に委託先のリスク評価サービスを提供する外部業者を利用してリスク評価を行っている			
	11. 7～10の定期的なリスク評価は行っていない			
	12. 該当なし（重要なサードパーティは存在しない）			

【問52】 サードパーティとの契約等において、サイバーセキュリティの観点から定められている事柄をすべて選択してください。
回答に際しては、外部委託先との契約等、外部委託先及びクラウド事業者を除くサードパーティとの契約等のそれぞれの回答欄について選択してください。クラウド事業者については問53で回答して下さい。
なお、上記の問49の 5. 外部委託先において、①対象組織を「2:無し」と回答した先は外部委託先についての回答は不要です。

取り決め事項または報告事項	外部委託先との契約等についての回答欄（該当するものに○）	外部委託先及びクラウド事業者を除くサードパーティとの契約等についての回答欄（該当するものに○）
1. 委託業務や提供サービス等におけるサイバーセキュリティ対策についての責任分界点		
2. サイバーセキュリティのリスク管理責任者		
3. 実施すべきサイバーセキュリティ対策		
4. インシデント発生時の対応		
5. 委託業務を取扱うシステム環境に係る脆弱性診断等の実施および報告		
6. 委託業務を取扱うシステム環境に深刻な脆弱性が判明した場合の対応および報告		
7. 自組織の立入調査の受け入れ		
8. 自組織のサイバーセキュリティに影響が生じる委託業務を再委託する場合の、自組織への連絡		
9. 1～8の取り決め事項または報告事項は定めていない		

【問53】 クラウドサービスに対する安全対策について、あてはまるもの（※１）をすべて選択してください。
なお、上記の問49の 7. クラウド事業者において、①対象組織を「2:無し」と回答した先は回答不要です。

注：本問はFISCアンケートとの共通設問です。

安全対策	回答欄 （該当するものに○）
1. サービス導入検討時の評価プロセス確立	
2. 契約書上、責任分界点やクラウドサービス終了時の取扱いを明確化	
3. 特定システム（※２）に係るクラウドサービス利用において、契約書上、統制対象クラウド拠点（※３）を明確化	
4. 特定システムに係るクラウドサービス利用において、契約書上、業務データの所在を明確化	
5. クラウドサービスの設定ミスを検出するためのチェックツール等の利用	
6. クラウドサービスの仕様変更にかかる確認体制を整備	
7. クラウドサービス事業者との間で、障害時の連絡体制を整備	
8. 政府情報システムのためのセキュリティ評価制度(ISMAP（※４）)のクラウドサービスリストの登録の有無の確認	
9. ISO認証(ISO27001、ISO27017等)等の取得状況の確認	
10. 第三者保証報告書（SOC２、第７号保証等）の利用	
11. クラウドサービス事業者への立入監査(*5)	
12. 専門知識を有する人材の配置	
13. 社内横断的な組織体制（CCoE（※6））の構築	
14. その他	
15. 1～14の安全対策は実施していない	

※１　複数のクラウドサービスを利用している場合は、１つでも当てはまるクラウドサービスがあれば、該当項目を選択してください
※２　金融情報システムのうち、重大な外部性を有するシステム（システム障害等が発生した場合の社会的な影響が大きく、個別金融機関等では影響をコントロールできない可能性があるシステム）や、機微情報（要配慮個人情報を含む）を有するシステム（機微情報（要配慮個人情報を含む）の漏えい等により顧客に広範な損失を与える可能性があるシステム）
※３　データに対する実行的なアクセスを行う拠点
※４　ISMAP(Information system Security Management and Assessment Program)
※５　事業者の制約により立入監査を実施出来ない場合は空欄にしてください。
※６　CCoE(Cloud Center of Excellence)

「その他」で「○」を選択した場合は以下の自由記入欄に具体的に記入してください。

不正送金・フィッシングの脅威への対応

【問54】 不正送金、フィッシング攻撃に対する以下の対策の実施状況として、あてはまるものを選択してください。
なお、インターネットバンキングやモバイルアプリは提供していない場合は、すべて「4:提供していない」を選択してください。

不正送金、フィッシング対策	インターネットバンキング 回答欄 （1:対策を実施している、 2:対策を検討している、 3:対策は検討していない、 4:提供していない）	モバイルアプリ 回答欄 （1:対策を実施している、 2:対策を検討している、 3:対策は検討していない、 4:提供していない）
1. 利用者（契約者）に対する注意喚起		
2. ログイン時の多要素認証		
3. 資金移動実行時の多要素認証		
4. 利用者に対して取引状況（ログイン、パスワード変更、送金等）を通知		
5. セキュリティ対策ソフトの提供		
6. 送信ドメイン認証（DMARC）の導入		
7. フィッシングサイトの検知とテイクダウン手順の整備		
8. 緊急連絡窓口の設置		

ゼロトラスト化

【問55】 ゼロトラスト・アーキテクチャの導入状況として、あてはまるものを選択してください。

※ ゼロトラストとは、「企業のネットワークやデバイスからのアクセスを暗黙に信頼せず、常にアクセスの信頼性を検証することで企業の情報資産や IT資産を保護すること」に焦点をあてたセキュリティの考え方

※ 本設問の回答にあたっては、以下も参考にしてください。
「ゼロトラストの現状調査と事例分析に関する調査報告書」
https://www.fsa.go.jp/common/about/research/20210630/zerotrust.pdf

1. ゼロトラスト・アーキテクチャを運用している 2. ゼロトラスト・アーキテクチャの実装・導入を進めている 3. ゼロトラスト・アーキテクチャ導入に向けたリスクアセスメントと方針策定を進めている 4. ゼロトラスト・アーキテクチャ導入に向けた現状把握・特定を進めている 5. ゼロトラスト・アーキテクチャ導入を検討している 6. ゼロトラスト・アーキテクチャ導入を検討した結果、行わないことと判断した 7. ゼロトラスト・アーキテクチャ導入は検討していない	回答欄 （左記1～7から選択）

本セルフアセスメントによる設問は以上になります。ほか、サイバーセキュリティ対策を整備・推進するうえで認識している課題があれば、以下の自由記入欄に記入してください。

（記入例）
・サイバーセキュリティ上の最新の問題点について、十分に理解することができていない。
・インシデント認識時に即座の対応ができるよう、社内にインシデント分析等が行える職員を配置したいが、その人材がいない。
・リスク対策製品を導入してはいるが、その仕様等を理解できる人材がいないため、同製品では守りきれない脅威について理解できていない。
・リスク対策（製品等）を検討するにあたり、費用対効果の評価が難しく、導入が進まない。
・ゼロデイマルウェアを脅威と考えており、これに対応すべくより強固な仕組みを導入したいと考えているが、そのための予算が確保できない。
・パブリッククラウドへの移行を進めたいと考えているが、リスク評価が難しく、なかなか進めることができていない。
・サイバーセキュリティ対策を進めているが、現時点では〇〇についての対策が弱いと認識している。このため、今後強化していく方針。

【自由記入欄】