（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（2022 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や経営計画について、あてはまるものを選択してください。

	回答欄
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、実現に向けた計画を策定している 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が、その実現に向けた計画までは策定していない 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	

【問2】　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。

	回答欄
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（サイバーセキュリティを含む）を所掌する役員 3. システムリスク（サイバーセキュリティを含む）以外を所掌する役員 4. 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） 5. 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） 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）以外の部署の職員（役員以外） 7. 責任者がいない	

【問3】　サイバーセキュリティに関する経営層への定例報告内容について、あてはまるものをすべて選択してください。

定例報告内容	回答欄 （1:はい、2:いいえ）
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. 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. 経営層への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	

「その他」で「1:はい」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4】　サイバーセキュリティに関する経営層への随時報告内容について、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	回答欄 （1:はい、2:いいえ）
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. 自組織システムで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	

「その他」で「1:はい」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5】　自組織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。1頁の【令和4年度FISCアンケートとの共通設問について】をご確認ください

事故等の内容	回答欄 （1:有り、2:無し）
1. コンピュータウィ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. 自組織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. 上記以外のコンピュータウイルス等の感染による被害	
8. その他	
9. 事故等はない	

「その他」で「1:有り」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6】　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。1頁の【令和4年度FISCアンケートとの共通設問について】をご確認ください

取り組み内容	回答欄 (1:はい、2:いいえ)
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. 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	
4. 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	
5. 脅威インテリジェンスサービス（※2）等を利用して収集	
6. 各種セミナー参加による収集	
7. インターネット等、マスコミ情報、新聞報道等から収集	
8. グループ会社から収集	
9. 業界団体から収集	
10. その他から収集	
11. 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、内閣サイバーセキュリティセンター（NISC）、一般社団法人金融ISAC、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「1:はい」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】　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、勘定系や顧客情報を扱うシステムなど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

取り組み内容	回答欄 (1:はい、2:いいえ)
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. 不定期にリスク評価を実施している(評価実施時期についての方針はない)	

【問8】　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
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、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 4. 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9】 サイバーセキュリティに関する監査対象として、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:実施している、2:予定がある、3:予定がない)	
	1. 自組織職員(内部監査部門)による検証	2. 外部(第三者)機関※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. リスク評価の適切性		
4. セキュリティ対策に関するルール･手順の遵守状況		

※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10】 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 (1:はい、2:いいえ)
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. その他（自由記入欄に記述してください）	
6. 被監査部門以外に結果報告を行っていない	

「その他」で「1:はい」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11】 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12】 サイバーセキュリティに関する注意喚起・教育・訓練の実施状況をすべて選択してください。

対象者	随時の注意喚起（1:実施、2:未実施）	e-learning等（ビデオ、書面を含む）による定期的な啓発（1:実施、2:未実施）	標的型メール訓練（1:実施、2:未実施）	マルウェア感染等※を想定した対処訓練（1:実施、2:未実施）
1. 役員				
2. サイバーインシデントに対応するための専門組織（CSIRT等）の職員				
3. システム所管部署の職員				
4. 業務部署の職員（システムのユーザー等）				
5. その他の部署（広報等）の職員				

対象者	随時の注意喚起（1:実施、2:未実施）	訓練等の実施状況の確認（1:実施、2:未実施）
6. 外部委託先		
7. 顧客		

※マルウェア感染時の初動対応の訓練等

新たなデジタル技術の評価

【問13】 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が可能な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。

	回答欄
1. 自組織職員のみ(他部署からの配置転換を含む)で要員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要員を確保できている 3. 外部人材の活用のみで十分な要員を確保できている 4. 要員を十分に確保できていない	

【問14】 新たな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、あてはまるものをすべて選択してください。なお、未導入の場合も「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」にご回答ください。

	導入有無（1:導入済、2:未導入）	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（1:脅威として認識※、2:脅威として認識していない）			
		破壊・改ざん	停止	情報漏洩	その他
1. パブリッククラウド					
2. オープンAPI(更新系)					
3. オープンAPI(参照系)					
4. スマホ・タブレット					
5. 在宅勤務のためのシステム					

※対策の有無にかかわらず、脅威として認識している場合に「1：脅威として認識」を選択してください

「その他」で「1:脅威として認識」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。

資産管理

【問15】 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、自組織内で運用しているシステム
外部システムとは、自組織の外部で運用しているシステム（クラウドを含む）

1. 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
2. 管理簿等を作成し、変更の都度更新している
3. 管理簿等を作成し、定期的に内容を確認している
4. 管理簿等を作成し、不定期に内容を確認している
5. 管理簿等を作成しているが、更新はしていない
6. 管理簿等を作成していない

①内部システム 回答欄

②外部システム 回答欄

【問16】 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、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. 管理簿等を作成し、変更の都度更新している
3. 管理簿等を作成し、定期的に内容を確認している
4. 管理簿等を作成し、不定期に内容を確認している
5. 管理簿等を作成しているが、更新はしていない
6. 管理簿等を作成していない

①ハードウェア 回答欄

②ソフトウェア 回答欄

【問17】 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

アクセス管理

【問18】 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すべて選択してください。

取り組み内容	回答欄 (1:はい、2:いいえ)
1. アカウントは、必要最小限の者に限って付与している	
2. 利用者ごとに、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)を付与している	
3. アクセス権は有効期限を限って付与している	
4. アクセス権は、退職や人事異動、組織体制変更の都度更新している	
5. アクセス権の設定を定期的に確認している	

【問19】 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。

取り組み内容	回答欄 (1:はい、2:いいえ)
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. 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)を本人が紛失した際の対応策を定めている	
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. リモートアクセスを利用していない	

データ保護

【問20】 データ保護のための対策としてあてはまるものをすべて選択してください。

取り組み内容	回答欄 (1:はい、2:いいえ)
1. 重要なデータ※を暗号化している	
2. 重要なデータへのアクセスを制御している	
3. 重要なデータのダウンロード・印刷を制御(ダウンロード・印刷時の作業ログの記録を含む)している	
4. データの外部記憶媒体への書出しを制御している	
5. 外部の組織等にデータを伝送する場合、自動的に暗号化される仕組みを導入している	

※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21】 ランサムウェア等による重要なシステムのバックアップデータの破壊・改ざんを想定した対策として、あてはまるものをすべて選択してください。

取り組み内容	回答欄 (1:はい、2:いいえ)
1. 複数世代保管している	
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. その他(自由記入欄に記述してください)	
5. あてはまる取り組みはない	

「その他」で「1:はい」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。

監査証跡(ログ)の管理

【問22】 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。

取り組み内容	回答欄 (1:はい、2:いいえ)
1. 取得すべきログについての定めがある	
2. ログの保管期間についての定めがある	
3. ログの無断改変・削除を禁止する定めがある	
4. 定期的にログを確認し不正がないかを確認する定めがある	
5. システムの監査証跡(ログ)について規定されている事はない	

システムの脆弱性に関する管理・対応

【問23】 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

	実施種別	
実施対象	脆弱性診断 （Webアプリケーション）	脆弱性診断 （プラットフォーム）
OA環境※		
Webサイト(顧客向けの公開Web)		
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24】 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。

※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
ペネトレーションテスト	
脅威ベースのペネトレーションテスト等	

【問25】 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. 可及的速やかにパッチを適用している
2. 保守等定期的なタイミングでパッチを適用している
3. システム更改時にパッチを適用している
4. 原則としてパッチを適用しない

システム・端末	回答欄
インターネットとつながっている※システム・端末	
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26】 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。

	回答欄
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27】 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

取り組み内容	回答欄（1:はい、2:いいえ、3:わからない）
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（仮想ブラウザなど、論理的な手法によるものを含む）	
2. 端末からアクセス可能なサイトを制限している	
3. 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）	
4. 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	
5. 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	
6. 端末への外部記憶媒体の接続を制限している	
7. 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）	
8. 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	

【問28】 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。

取り組み内容	回答欄（1:はい、2:いいえ、3:わからない）
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通信を遮断している	
6. 認証機能によるアクセス制御を行っている	

※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29】 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。
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、「4:提供していない」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、3:わからない、4:提供していない)	Webサイト (顧客向けの公開Web)	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		

※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

サイバーインシデントの検知

【問30】 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。

	回答欄
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31】 SOC等サイバーセキュリティの監視部署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 (1:はい、2:いいえ)
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. 各種ログを関連付けて分析した場合の不整合等の状況(不審な活動状況)	

サイバーインシデント対応・業務復旧の態勢

【問32】 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
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33】 外部機関（金融ISAC等）への協力（情報提供）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。

協力状況	回答欄 （1:はい、2:いいえ）
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. 情報は提供しないこととしている	

【問34】 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、あてはまるものをすべて選択してください。

整備状況	回答欄 （1:はい、2:いいえ）
1. 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	
2. 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	
3. 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	
4. 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	
5. 被害拡大防止のルール・手順はない	

【問35】 インシデント対応（訓練・演習を含む）実績を踏まえた体制の強化状況としてあてはまるものを選択してください。

	回答欄
1. インシデント対応実績を踏まえ、必要に応じて体制（規程・情報連絡体制・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、必要に応じて体制の更新のみを実施 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、体制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	

【問36】 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（被害）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（被害）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:有り、2:無し)
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)

サイバー攻撃（被害）	コンティンジェンシープランの取組内容				
	1	2	3	4	5
1. システムの破壊・改ざん					
2. システムの機能停止					
3. 情報漏洩					

【問37】 サイバー攻撃（被害）発生時の関係者への連絡手順（マニュアル等）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。なお、「4. 自組織のグループ会社」への回答のみ「3：対象無し」が選択可能です。

連絡対象	回答欄 (1:有り、2:無し 3：対象無し)
1. 所管省庁・日本銀行	
2. 顧客	
3. 外部委託先	
4. 自組織のグループ会社	
5. 外部一般（マスコミ含む）	

サードパーティ等の管理

【問38】 サードパーティ（※1）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、あてはまるものを選択してください。
なお、回答に際しては、外部委託先、外部委託先を除くサードパーティ（※2）のそれぞれの回答欄について選択してください。

※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 等）
※2 外部委託先を除くサードパーティとは、委託契約を締結していないサードパーティ

手続等の状況	外部委託先についての回答欄 (1:はい、2:いいえ)	外部委託先を除くサードパーティについての回答欄 (1:はい、2:いいえ)
1. サードパーティの選定時に、サイバーセキュリティに関するリスク評価を行っている		
2. サードパーティの選定後も、定期的にサイバーセキュリティに関するリスク評価を行っている		

【問39】 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
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	

【問40】 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。
なお、回答に際しては、外部委託先との契約等、外部委託先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。

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（1:はい、2:いいえ）	外部委託先を除くサードパーティとの契約等についての回答欄（1:はい、2:いいえ）
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		
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. 自組織の立入調査の受け入れ		
6. 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		

【問41】 自組織および海外拠点や関連会社、外部委託先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）	③左記に係るモニタリング等の状況	
		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※ 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	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（1:はい、2:いいえ）	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（1:はい、2:いいえ）
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（クラウド事業者を除く）				
6. オープンAPI接続先企業				
7. クラウド事業者				
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				

※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42】 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41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。1頁の【令和4年度FISCアンケートとの共通設問について】をご確認ください

安全対策	回答欄 （1:はい、2:いいえ）
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	
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（※5））の構築	
14. その他	

※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 CCoE(Cloud Center of Excellence)

「その他」で「1:はい」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。

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】