サイバーセキュリティ（ＦＡＱ）

・「安全対策基準・解説書（第12版）」を2024年3月に公表。
・英訳版については、「安全対策基準・解説書（第11版）」を2024年1月に公表。
・「コンティンジェンシープラン策定のための手引書（第4版）」を2024年1月に公表。

2024/8/9時点

No.	質問	回答	ガイドライン記載箇所（参考）			追加／修正
			規定種別	項目	項番	
「サイバーセキュリティ」に対するＦＡＱ						
1	サイバー攻撃に対応するために、事前の情報収集並びに攻撃発生時の相談先として、どのようなセキュリティ対応機関が利用できるか。	事前の情報収集先においては、例えば、金融ISAC、IPA、JPCERT/CCなどが考えられます。 また、攻撃発生時の相談先においては、例えば、都道府県警察JPCERT/CC等が考えられます。	コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	2.(2)	－
2	サイバー攻撃を受けた場合に、FISCへの届出や連絡が必要か。	サイバー攻撃を受けた場合に、FISCに対して届出や連絡をいただく必要はございません。 なお、インシデント対応時の連携先については、例えば、金融庁、都道府県警察、個人データ等の漏えい等事案が発覚した際には個人情報保護委員会への報告などが考えられます。	コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	2.(2)	－
3	国内・海外の技術動向、及び具体的な「対応策」「対策事例」を知りたい。	・サイバー攻撃に伴うシステムの停止及び不正な資金移動に対応するために、未然防止策・事前対策、検知策及び対応策を検討し、態勢を整備することが必要となります。なお、あらゆるサイバー攻撃を事前に防御することは難しいため、侵入されることを前提とした対応策について事前に検討しておくことが必要となります。 ・サイバー攻撃に対応するためには、国内外のサイバー攻撃動向・事例、脆弱性などに関する事前の情報収集並びに攻撃発生時の相談先として、セキュリティ対応機関を利用することや業界団体と情報共有することが推奨されます。情報共有を行うことで同様の被害を未然に防止し、企業における対応コストを低減することができます。	安全対策基準・解説書	第2編　統5　サイバー攻撃対応態勢を整備すること。	1.～2.	－
4	既存のBCP（事業継続計画）にサイバー攻撃対応をどのように盛り込んでいくか検討したい。	サイバー攻撃対応については、「コンティンジェンシープラン策定のための手引書（第4版）」の「Ⅳ　サイバー攻撃・情報漏えいの考慮事項」に関連する記載がございますのでご参照ください。	コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	－	－
5	サイバー攻撃を想定した対応訓練のシナリオや訓練実施事例を知りたい。訓練や初動の演習について実効性をどのように確保すべきか。	サイバー攻撃を想定した対応訓練のシナリオにおいては、「コンティンジェンシープラン策定のための手引書（第4版）」の「⑦教育・訓練」に記載している図表5にて例示を挙げておりますのでご参照ください。なお、シナリオの作成に当たっては、必要に応じて、外部のセキュリティ対応機関等を活用することが考えられます。 また、訓練実施事例においては、例えば、役職員向けのセキュリティ意識の啓発教育、外部機関が主催する共同演習などが考えられます。	コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	2.(1)	－
					3	－

No.	質問	回答	ガイドライン記載箇所（参考）			追加／修正
			規定種別	項目	項番	
6	インターネットバンキングの利用者保護の指針や対策事例を教えて欲しい。	・不正使用防止策として、サービス内容及びリスク特性に応じて多要素認証の併用を検討する等、厳正な本人確認を実施することが必要となります。特に資金移動及び注文等の取引に関しては、より厳正な本人確認を実施することが必要となります。 ・ユーザーID等が不正使用されていないか、利用者自身で確認可能にすることが必要となります。特に資金移動及び注文等の取引に関しては、不正使用の早期発見のため、処理結果が確認できる機能を提供することが必要となります。なお、不正に使用されていないかの確認を利用者自身が行うことを注意喚起することが推奨されます。 ・利用者との取引を安全に実施するため、インターネット、モバイル等を用いた金融サービスにおいて、注意喚起、受付対応等の顧客対応方法を明確にすることが必要となります。顧客に周知すべき事項として、例えば、サービス内容・規約、金融機関等が実施している安全対策の概要等があります。 ・インターネット・モバイルサービスにおいては、利用者を保護し、安全性を確保し円滑に稼働させるため、運用管理方法を明確にすることが必要となります。不正な取引を防止する対策として、例えば、伝送データの漏えい防止策、本人確認機能、アクセス履歴の管理などがあります。	安全対策基準・解説書	第2編 実112　インターネット・モバイルサービスの不正使用を防止すること。 第2編 実113　インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること。 第2編 実115　インターネット・モバイルサービスの顧客対応方法を明確にすること。 第2編 実116　インターネット・モバイルサービスの運用管理方法を明確にすること。	1.～5.	－
7	組織内CSIRTはどのように整備すればよいか。どこから何をすればよいのか定まらない。	・インシデント発生時における部署間の連携及び外部との連絡窓口の機能を担い、経営層への報告並びに経営層からの指示を実施することができる組織としてCSIRT（Computer Security Incident Response Team）を整備する必要があります。 ・金融機関等は自社のサイバー攻撃対応に必要な機能を検討したうえで、それらの機能を担うインシデント対応組織としてCSIRTを整備する必要があります。インシデント対応組織は、インシデントの検知及び対応等のインシデント発生時の役割のみならず、経営層や社内関係部門、セキュリティ対応機関や情報共有機関、業界団体等との連携・調整、サイバー攻撃に関する情報収集や、システムの監視・ログの分析等、平時の役割を担うことにより、サイバー攻撃対応態勢の実効性を高めることができます。	安全対策基準・解説書	第2編 統5　サイバー攻撃対応態勢を整備すること。	1.～2.	－
			コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	2.(1)	
8	経営陣の危機感が少ない。経営陣への啓発活動を期待している。サイバー攻撃のリスク評価材料や、サイバーセキュリティ強化の投資判断材料等を提供して欲しい。	経営陣への啓発活動においては、当センターが主催する「経営層向けサイバーセキュリティセミナー」のほか、「FISC エグゼクティブセミナー」「FISC セミナー」等においてもサイバーセキュリティ対応に関するテーマを取り上げて参りますので、経営者の方々にも是非ご参加頂ければと存じます。 また、サイバー攻撃のリスク評価材料や投資判断材料においては、以下の参考文献をご参照ください。 ・「企業経営のためのサイバーセキュリティの考え方」（内閣サイバーセキュリティセンター（NISC））、「サイバーセキュリティ経営ガイドラインVer3.0」（経済産業省、独立行政法人情報処理推進機構（IPA））	コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	2.(1)	－
9	サイバーセキュリティの人材不足で困っている。人材はどこまでのレベルのどのような知識・経験が必要なのか。専門知識の習得には難しい面がある。人材はどのように確保・育成すればよいのか。	教育に当たっては、以下の重要性を明確にすることが必要となります。 (1) コンピュータシステムが果たす役割 (2) 機密保護、顧客データの保護 (3) システムの安全運用等についての対策 なお、IT人材の確保・育成にあたっては、当センター発刊の「金融機関等におけるIT人材の確保・育成計画の策定のための手引書」、独立行政法人情報処理推進機構IT人材育成本部 HRDイニシアティブセンターの「ITのスキル指標を活用した情報セキュリティ人材育成ガイド」等をご参照ください。	安全対策基準・解説書	第2編 統14　セキュリティ教育を行うこと。	3.	－
10	サイバーセキュリティについて、どのような事から態勢整備すればよいか、基本となるマニュアルが提供されるとよい。	サイバー攻撃対応態勢の整備については、「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書（第4版）」の「④組織体制の整備」に関連する記載がございますのでご参照ください。	コンティンジェンシープラン策定のための手引書	第４編　Ⅳ　サイバー攻撃・情報漏えいの考慮事項	2.(1)	－
11	様々な対策がある中で、サイバーセキュリティにかけられる資源に限りがあるため、何からどこまでやればよいか。	サイバーセキュリティに対する安全対策への資源配分については、各金融機関等の経営層が、あらかじめ保有する経営資源を踏まえた達成目標を検討するとともに、リスク特性に応じた資源配分を決定するものであると考えております。この際、必ずしもリスクゼロを追求しないといった「リスクベースアプローチ」の考え方を取り入れることが有益となります。	安全対策基準・解説書	第2編 (2) リスクベースアプローチ	－	－

No.	質問	回答	ガイドライン記載箇所（参考）			追加／修正
			規定種別	項目	項番	
12	監視機能へのサイバー攻撃への対策を検討するにあたり、監視機能がサイバー攻撃を受けた事例を教えてほしい。	金融機関、その他業種において報道情報等からは具体的な事例はございませんが、NISCが発行する「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」別紙において、サイバー攻撃リスクの特性⑦が事例として紹介されていますのでご参照ください。 https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf	安全対策基準・解説書	第2編　統5　サイバー攻撃対応態勢を整備すること。	1.(2)	追加
13	【統5】1.(2)にある、「監視手段を複数用意する」方法について、具体例を教えてほしい。	運用管理システムに加えて、各サーバの状態監視を重要度に応じて能動的に定点で確認するという方法が考えられます。	安全対策基準・解説書	第2編　統5　サイバー攻撃対応態勢を整備すること。	1.(2)	追加
14	【実115】5.(3)において「フィッシングサイトが検知された場合には、当該フィッシングサイトの閉鎖等の対応を行う」という記載があるが、フィッシングサイトが発生していないかを金融機関が能動的に監視すべきということか。	「不正取引の発生」後では遅いことから、「フィッシングサイトの検知」時点で対策を講じるべきという趣旨で記載しております。金融機関が能動的にフィッシングサイトを監視する日常的な対応が必要、という意図ではありません。 なお、外部サービスを活用し、能動的にフィッシングサイトの発生を確認している金融機関の事例はあります。	安全対策基準・解説書	第2編　実115　インターネット・モバイルサービスの顧客対応方法を明確にすること。	5.(3)	追加
15	【統5】 1.(2)⑥において 「サイバーセキュリティ関係機関等が公開している情報」という記載があるが、これは脆弱性などの情報のことか、もしくは、ログ情報のことを指しているのか。	「サイバーセキュリティ関係機関等が公開しているサイバーセキュリティに係る取組みの事例や動向」を指しております。 これらの情報を確認いただき、自組織で取得対象ログと保存期間の見直しを行う必要があります。	安全対策基準・解説書	第2編　統5　サイバー攻撃対応態勢を整備すること。	1.(2)	追加