S-6 構造化質問一覧

※「M」:政策・運営コース受講者、「T」:インシデント分析コース受講者。

サイバー経営ガイドラインV2.0（付録A サイバーセキュリティ経営チェックシート）より抜粋ー部修正

No.	質問No.	M→T	T→M	指示No.	指示項目	細目No.	指示細目
1		理事長・学長にサイバーセキュリティリスクが大学運営リスクになり得ると説得するための具体例を挙げて下さい。	理事長・学長にサイバーセキュリティリスクが大学運営リスクになり得ると説得する機会を作っていますか？	1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	1.1	理事長・学長がサイバーセキュリティリスクを大学運営リスクの1つとして認識している
2	0		理事長・学長名でセキュリティポリシーを策定・宣言していますか？			1.2	理事長・学長が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言している
3	8	個人情報保護やGDPRに対応した技術的対策は取っていますか？	個人情報保護やGDPRの法的リスクは学内のどの部署と共有していますか？			1.3	法律や業界のガイドライン等の要求事項を把握している
4	1	CISOは設置されていますか？ 設置されている・いないにかかわらず、技術的な対応は、誰に報告するのかあらかじめ決まっていますか？	CISOは設置されていますか？設置されている場合、その経緯は？また、設置されていない場合の今後の計画は？	2	サイバーセキュリティリスク管理体制の構築	2.1	組織の対応方針（セキュリティポリシー）に基づき、CISO等からなるサイバーセキュリティリスク管理体制を構築している
5		セキュリティ対策費用を予算として計上していますか？その費用を誰に提出していますか？	セキュリティ予算は、IT予算の中でどの位を想定していますか？臨時支出は可能ですか？	3	サイバーセキュリティ対策のための資源（予算、人材等）確保	3.1	必要なサイバーセキュリティ対策を明確にし、理事会・執行部会議などで対策の内容に見合った適切な費用かどうかを評価し、必要な予算を確保している
6		セキュリティ関係の講習会には、ご自身以外の方は参加していますか？セキュリティ担当の分担はありますか？	セキュリティ関係の講習会は、年間で何人を何回派遣していますか？それは、毎年ですか？			3.3	組織内でサイバーセキュリティ人材を育成している
7		学内での一般ユーザー向けのセキュリティ講習会の企画や外部講師の紹介などを提案していますか？	学内での一般ユーザー向けセキュリティ講習会のための予算措置は継続して行っていますか？			3.5	セキュリティ担当者以外も含めた構成員向けセキュリティ研修等を継続的に実施している
8	4	学生個人情報、成績データ、入試データは、どこに保存されているか把握していますか？ 誰がアクセスできるのか、どのPCからアクセスできるのか把握できていますか？ アクセスログは取れていますか？	情報資産台帳は作っていますか？ 各情報資産の保管先システムの概要は把握していますか？	4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	4.1	守るべき情報を特定し、当該情報の保管場所や重要度等に基づいて優先順位付けを行っている
9		上記のシステムの脆弱性情報はどのように取得していますか？	上記の保管先システムの脅威（CIAの観点）についてはリストアップされていますか？			4.2	特定した守るべき情報に対するサイバー攻撃の脅威、脆弱性を識別し、事業継続性を踏まえたサイバーセキュリティリスクとして把握している
10	7	今後の再発防止策を考えなければなりません。 どのような技術的な改善点がありますか？ （ヒント） ・多層防御の観点　・セキュリティ監視の観点　・利用者教育の観点	侵入防止のためのシステム設計や運用（重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネットワークセグメントの分離、アクセス制御、暗号化等の実施）を指示していますか？または、報告を受けていますか？定期的に見直しを図っていますか？	5	サイバーセキュリティリスクに対応するための仕組みの構築	5.1	重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネットワークセグメントの分離、アクセス制御、暗号化等の多層防御を実施している。
11		検知すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築していますか？	検知すべきイベントに対して、それぞれ手順書作成の指示を行っていますか？定期的な見直しを行っていますか？			5.3	検知すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築している。
12		意図していない通信の一例を挙げて、その対応計画例を挙げて下さい。	意図していない通信やアクセスに対して、それぞれ手順書作成の指示を行っていますか？定期的な見直しをはかっていますか？			5.4	意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、対応者などの責任分担等）を策定している
13		大学構成員それぞれに必要な防御対策（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）のリストアップとその講習会の提案を行っていますか？	大学構成員それぞれに必要な防御対策（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）について、適切な時期に講習会を実施し、参加を組織として促していますか？			5.6	構成員に対して、サイバーセキュリティに関する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）の周知、標的型攻撃メール訓練など）を実施している。
14		理事長・学長に定期的な報告を行うべき項目を挙げて下さい。	理事長・学長に定期的な報告を行う機会を作っていますか？	6	サイバーセキュリティ対策におけるPDCAサイクルの実施	6.1	理事長・学長が定期的に、サイバーセキュリティ対策状況の報告を受け、把握している
15		サイバーセキュリティにかかる外部監査を実施していますか？	サイバーセキュリティにかかる外部監査を実施していますか？			6.2	サイバーセキュリティにかかる外部監査を実施している
16	5	標的型攻撃によって学内の重要情報が流出した可能性があります。 被害拡大防止のため、緊急停止をするシステムやネットワークの遮断箇所はすぐに列挙できますか？	標的型攻撃によって学内の重要情報が流出した可能性があります。 システムの緊急停止、パソコンの回収やネットワーク遮断に関する権限は、どのように決めていますか？ 学内外の緊急連絡先はリストにしていますか？ （ヒント） 学長・CISO・ベンダー・警察・JPCERT/CC・IPA・文部科学省・個人情報保護委員会	7	インシデント発生時の緊急対応体制の整備	7.1	組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、システム運用、Webサイト保守・運用、契約しているセキュリティベンダの連絡先含む）
17	3	標的型攻撃によって学内の重要情報が流出した可能性があります。 初動対応マニュアルはありますか？	学内の重要情報が流出した場合の初動対応マニュアル作成を指示していますか？ その他、どんなインシデントに対する初動対応マニュアルの作成を指示していますか？			7.2	サイバー攻撃の初動対応マニュアルを整備している
18	2	インシデント対応の専門チーム（CSIRT等）は設置していますか？	インシデント対応の専門チーム（CSIRT等）を設置していますか？			7.3	インシデント対応の専門チーム（CSIRT等）を設置している
19	6	理事長・学長にインシデントや被害状況の説明を行うために、どのような痕跡や証拠となるデータが提示できますか？	総務・広報部門と情報セキュリティリスクについて話し合う機会を作っていますか？			7.4	理事長・学長が責任を持って組織の内外へ説明ができるように、総務・広報部門への報告ルート、公表すべき内容やタイミング等を定めている
20		インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っていますか？	インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行うよう指示していますか？			7.6	インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている
21		緊急停止したシステムの代替手段は用意していますか？ 緊急停止するシステムの再稼働に必要な条件は何ですか？	代替手段や再稼働に関する判断や情報提供の権限・方法等について検討していますか？	8	インシデントによる被害に備えた復旧体制の整備	8.1	被害が発生した場合に備えた業務の復旧計画を策定している
22		定期的に復旧対応訓練や演習を行っていますか？	復旧対応訓練や演習を定期的に年次計画に組み込んでいますか？			8.4	定期的に復旧対応訓練や演習を行っている
23		システム管理・セキュリティ監視に関して、外注すべき内容を挙げて下さい。	システム管理・セキュリティ監視に関して、外注していますか？外注時のリスクは何ですか？	9	委託先等を含めた全体の対策及び状況把握	9.1	システム管理などについて、自組織のスキルや各種機能の重要性等を考慮して、自組織で対応できる部分と外部に委託する部分を適切に切り分けている
24		業務委託先にセキュリティ保護のための技術的な相談窓口がありますか？	業務委託先にセキュリティ対策を指示・契約していますか？			9.2	委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にしている
25		IPAやJPCERT/CCへの情報提供の経験はありますか？	IPAやJPCERT/CCへの情報提供を指示したことがありますか？	10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	10.2	マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPAへの届出や一般社団法人JPCERTコーディネーションセンターへの情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している