大学セキュリティ運用ベンチマークテスト

情報セキュリティ対策問題研究小委員会
情報セキュリティ研究講習会運営委員会

年金機構からの年金番号流出や大学現場での大規模個人情報流出など今年度は情報セキュリティ基盤の安全性を揺るがす大きな事件が頻発しています。また、国内のインターネットバンキングに係わるアカウント搾取による被害額は昨年度で 1,876 件 29 億 1000 万円となっています。マイナンバー制度は、来年 1 月より利用が開始され、個人情報を守るため大学を含む各事業者には、マイナンバーの管理での安全管理措置などが義務付けられます。

私立大学情報教育協会は、こうした背景から各大学において情報セキュリティ対策の現状を踏まえ、対策について PDCA サイクルの Check（評価）にご活用頂くことを目的にベンチマークテストの作成を検討しております。

第 1 部　情報セキュリティ対策へのガバナンスについて（計 6 問）

問 1 サイバー攻撃による情報資産、金融資産、社会的信頼への脅威やインシデントについて、全学的な危機意識の共有化を推進されていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 2 危機意識の共有化に向けて、担当役員もしくはそれに準ずる法人・大学執行部メンバーが統括責任者としてリーダーシップを発揮して脅威の認識を徹底していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3 貴大学の ICT 予算に対し、セキュリティ対策にかかる費用の割合をお答えください。

① ３%以下、② ４%～６%、③ ７%～９%、④ １０%～１２%、⑤ １３%以上

問 4 上記セキュリティ対策費用の使途優先順位をお答えください。

① ファイヤーウォール更新、② クライアント対策強化、③ セキュリティベンダー契約、
④ 学内体制整備、⑤ 教育・啓蒙、⑥ その他

問 5 個人情報流出対策として、今後どの程度の対策費用を検討されていますか。ICT 予算に対する割合でお答えください。

① ３%以下、② ４%～６%、③ ７%～９%、④ １０%～１２%、⑤ １３%以上

問 6 実際に今年度または来年度にセキュリティ対策を行う際に拠出できる費用を ICT 予算に対する割合でお答えください。

① ３%以下、② ４%～６%、③ ７%～９%、④ １０%～１２%、⑤ １３%以上

第 2 部　情報セキュリティ対策全般について（計 27 問）

注：部門でのご利用に際しては、該当部門の状況を回答して下さい。ただし、例えば、情報セキュリティポリシーなどの規程類は、基本的には、全学を対象とするものがあれば、部門独自のものである必要はありません。

問 1-(1) 情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。

a) 情報セキュリティポリシーの適用範囲は、関係する教職員（非常勤、派遣を含む）すべてとしていますか。

① はい、② いいえ、③ わからない

b) 情報セキュリティポリシーは、自大学組織の事業やリスクを鑑みた内容ですか。

① はい、② いいえ、③ わからない

c) 定めた規程類を関係者に十分に周知させていますか。

① はい、② いいえ、③ わからない

d) 規程類の順守状況を点検し、必要に応じて見直していますか。

① はい、② いいえ、③ わからない

問 1-(2) 情報セキュリティに関する規程や対策を策定する際に、大学組織の重要な資産に関する危険性や脆弱性について評価（リスクアセスメント）していますか。

a) このリスクアセスメントは、年に一度実施していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 1-(3) 大学ガバナンス層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。

a) 最高情報セキュリティ責任者を設置していますか。

① はい、② いいえ、③ わからない

b) 情報セキュリティ委員会を設置していますか。

① はい、② いいえ、③ わからない

c) 部門統括情報セキュリティ責任者・情報セキュリティ責任者等を設置していますか。

① はい、② いいえ、③ わからない

d) 情報セキュリティインシデントに備えた体制の整備を行っていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 1-(4) 重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。

a) 情報について、機密性、完全性及び可用性の 3 つの観点を区別し、それぞれの格付け区分を定義していますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④ 定義できていない。⑤ わからない。

b) 情報資産の格付け区分別に表示や取扱方法などの指針を決めていますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④ 定義できていない。⑤ わからない。

c) 格付け区分別に情報資産の管理責任者を定めていますか。

① はい、② いいえ、③ わからない

d) 格付け区分別に情報資産が漏洩した際のリスクを評価していますか。

① はい、② いいえ、③ わからない

問 1-(5) 重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。

a) 業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などを定めていますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④ 定義できていない。⑤ わからない。

問 1-(6) 外部の大学組織に業務や情報システムの運用管理を委託する際の契約書には、セ情報漏洩や情報消失の点から相手方に求めるべき事項（SLA）を記載していますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④ 定義できていない。⑤ わからない。

問 1-(7) 教職員（非常勤・派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④ 定義できていない。⑤ わからない。

問 1-(8) 大学ガバナンス層や非常勤・派遣を含む全ての教職員に対し、情報セキュリティに関する自大学組織の取組や関連規程類について、計画的な教育や指導を定期的に実施していますか。

a) セキュリティ対策上の順守事項、禁止事項の徹底および、情報セキュリティの脅威と対策についても教育していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。

③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 2-(1) 特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。

a) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策がなされていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

b) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策がなされていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 2-(2) 学生、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 2-(3) 重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。

a) 重要なシステムは安全な場所へ設置されていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 2-(4) 重要な書類、モバイル PC、記憶媒体などについて適切な管理を行っていますか。

a) 重要書類の保管場所の施錠や印刷物の放置禁止などの規則がありますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④定義できていない。⑤ わからない。

b) USB メモリや CD などの廃棄の際の消磁・破砕規則がありますか。

① 定義されており、定期的な確認も行っている。② 定義されているが、定期的な確認はできていない。
③ 一部の定義に留まっている。④ 定義できていない。⑤ わからない。

問 3-(1) 情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。

a) テスト環境と運用環境を分離していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

b) 運用データの変更管理を行っていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3-(2) 情報システムの運用に際して、必要なセキュリティ対策を実施していますか。

a) システム運用に必要な手順書を作成していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

b) システムログを取得し、不正アクセスの監視などを行っていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3-(3) 重要なデータや関連するシステムのバックアップに関する手順を文書化し、実施していますか。

a) 情報の格付に応じて、適切な方法で情報のバックアップを実施していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

b) 取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定めて管理していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

c) 保存期間を過ぎた情報のバックアップについては、適切な方法で消去、抹消又は廃棄していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3-(4) 不正プログラム（ウイルス、ワーム、ボット、スパイウェアなど）への対策を実施していますか。

a) サーバ及び端末に不正プログラム対策ソフトウェア等を導入していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3-(5) 導入している情報システムに対して、適切なぜい弱性対策を実施していますか。

a) セキュリティを考慮した設定を行っていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

b) パッチ（修正プログラム）の適用、を行っていますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3-(6) 通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。
（適切な保護策には、VPN の使用や重要な情報の SSL などによる暗号化があります。）
① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 3-(7) モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。
（モバイル PC や USB メモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部のセキュリティの脅威は内部よりも高いことを考慮して対策を行う必要があります。）
① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 4-(1) 情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証を適切に実施していますか。
（適切な利用者 ID の管理には、利用者 ID の定期的な見直しによる不要な ID の削除や共用 ID の利用制限、単純なパスワードの設定禁止などがあります。）
① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 4-(2) 情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。
（適切なアクセス権の管理には、アクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。）
① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 4-(3) ネットワークのアクセス制御を適切に実施していますか。
（適切なネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。）
① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 4-(4) 業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。
（自大学組織での開発、外部委託による開発を問わず、開発の際に必要なセキュリティ対

策としては、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開 発に際してぜい弱性を作りこまないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどがあります。）

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 4-(5) ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 5-(1) 万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。

（適切な対策には、たとえばシステムの二重化、バックアップと運用記録の取得、障害対応手順の明確化、外部委託先とのサービスレベルの合意などがあります。）

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

問 5-(2) 情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。

（事件や事故への備えには、そうした万が一の場合にとるべき行動をあらかじめ検討しておくこと、検討した結果を文書にまとめて関係者に周知しておくこと、緊急の連絡網を整備すると共に、必要な要員や資機材を揃えられるようにあらかじめ手配しておくことなどがあります。）

①実施されており、定期的な確認も行っている。③実施されているが、定期的な確認はできていない。
③一部の実施に留まっている。④実施できていない。⑤わからない。

問 5-(3) 何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。

（万が一、情報システムが停止してしまった場合に備えて、普段は情報システムで行っている業務をたとえば手作業で代替できるように、そうした業務の手順書 や様式類をあらかじめ用意しておくこと、またそうした手作業を実施できる場所や資機材を確保しておくこと、さらに手作業で代替できるように要員を訓練して おくことなどが重要です。）

① 実施されており、定期的な確認も行っている。② 実施されているが、定期的な確認はできていない。
③ 一部の実施に留まっている。④ 実施できていない。⑤ わからない。

第 3 部　貴大学の規模等について（計 13 問）

問１　大学の規模を番号でお答えください。

①大規模大学　入学定員 3,000 人以上　複数学部有り

②中規模大学　入学定員 2,000 人以上　3,000 人未満　複数学部有り

③中小規模大学　入学定員 2,000 人未満　複数学部有り　自然科学系学部有り

④中小規模大学　入学定員 2,000 人未満　複数学部有り　自然科学系学部無し

⑤自然科学系　単科大学

⑥社会科学系　単科大学

⑦人文科学系　単科大学

⑧医・歯・薬系　単科大学

⑨その他　単科大学

⑩大学併設短期大学

⑪短期大学法人

問２　教職員数(非常勤、派遣、アルバイトを含む)をお答え下さい。(部門単位で利用する場合も、全学の単位で回答して下さい。)

① 100 人未満　② 500 人未満　③ 1,000 人未満　④ 2,000 人未満　⑤ 2,000 人以上

問３ 教職員数のうちの専任教職員の割合をお答えください(部門単位で利用する場合も、全学の単位で回答して下さい。)

① 10%以下　② 30%以下　③ 50%以下　④ 70%以下　⑤ 70%を超える

問４ 国内の拠点数をお答えください。(部門単位で利用する場合も、全学の単位で回答して下さい。)

① １箇所　② ２箇所　③ ３箇所　④ ５箇所未満　⑤ ５箇所以上

問５ 海外の拠点数をお答えください。(部門単位で利用する場合も、全学の単位で回答して下さい。)

① ０箇所　② １箇所　③ ２箇所　④ ５箇所未満　⑤ ５箇所以上

問６ 主要な業務に関わるプロセスのうち、情報システム(外部のシステム含む)に依存している割合はどの程度ですか。

① 一部にとどまる（25%以下）　② 若干依存している（50%以下）

③ 多くの部分が依存している（75%以下）④ ほとんどの部分が依存している（75%を超える）

問７ 主要な業務に関わるプロセスのうち、インターネットに依存している割合はどの程度ですか。

① 一部にとどまる（25%以下）　② 若干依存している（50%以下）
③ 多くの部分が依存している（75%以下）④ ほとんどの部分が依存している（75%を超える）

問８ 主要な情報システムについて、教育業務に影響を及ぼさないで済む、許容停止時間はどれくらいですか。
① 1時間以内　② 半日以内　③ 1日以内　④ 数３日以内　⑤ それ以上

問９ 主要な情報システムが授業期間に「24時間」停止した場合、その日の教育業務にどの程度の影響を及ぼしますか。
① ほとんど影響を受けない（25%減以下）　② 影響はあるが、部分的にとどまる（50%減以下）
③ 大きな影響を受ける（75%減以下）　④ 深刻な影響を受ける（75%減を超える）

問 10 個人情報漏洩等、情報セキュリティ関連の事故が発生した場合、貴学のイメージにどの程度の影響がありますか。
① ほとんどない ② 部分的に影響がある　③ 大きな影響がある ④ 存続に関わる影響がある

問 11 外部に漏洩すると事業に極めて深刻な影響が生じる重要情報(プライバシー情報等)をどの程度保有、管理または使用していますか。
① ほとんどない　② 少ない　③ 全体の半分程度　④ ほとんどがその種の情報である

問 12 何名分程度の個人情報を取り扱っていますか。(データの述べ数の概要でお答え下さい。)
① 1000 件以下 ② 5000 件以下 ③ 1 万件以下 ④ 10 万件以下 ⑤ 10 万件を超える

問 13 過去に教育活動に影響を与えるような IT 事故が発生したことがありますか。
① はい ② いいえ

「①はい」と答えた方は、あてはまるもの全てにチェックしてください。

① 主要な教育業務に関わる情報システムのウイルス感染
② 全学的な PC のウイルス感染
③ 社内システムへの（ネットワーク経由での）不正侵入
④ ホームページの改ざん
⑤ 学生情報等、機密情報や個人情報の学外への漏洩
⑥ 学外のホームページ等に対する意図しない攻撃や、ウイルスメールの送信
⑦ 許容停止時間を超えるシステムダウン
⑧ その他

以上