電気技術者試験センターにおける情報セキュリティへの取り組み

― 重要な個人情報・国家試験情報のインターネットからの分離 ―

令和 8 年 11 月 9 日

1. 基本的な考え方

一般財団法人電気技術者試験センター（以下「センター」といいます。）は、電気技術者に関する国家試験を公正かつ確実に実施する機関として、受験申込等を通じてお預かりする個人情報をはじめ、試験の実施に関係する重要な情報を安全に管理することを重要な責務と考えています。

近年、ランサムウェア、不正アクセス、フィッシング、システムの脆弱性を悪用した攻撃、サプライチェーンを経由した攻撃など、サイバーセキュリティを取り巻く脅威は高度化・複雑化しています。特に、AI の悪用により、攻撃対象の調査や侵入が短時間かつ大規模に行われるおそれが高まっています。

センターでは、こうした環境の変化を踏まえ、情報セキュリティの確保を国家試験の公正性と信頼性を支える重要な基盤の一つと位置付け、組織全体で継続的に情報セキュリティ対策に取り組んでいます。

2. 情報セキュリティ管理体制

センターでは、情報セキュリティを組織全体で取り組む重要な課題として位置付け、情報を保護するための管理体制を整備しています。

特に、情報セキュリティ及び情報管理を専門に担当する「情報管理政策室」を設置するとともに、サイバーセキュリティに関する専門的な知識と経験を有する専任の職員を配置し、専門的な知見を活用した情報セキュリティ対策を進めています。

情報管理政策室では、関係部署及び外部の専門家と連携しながら、情報セキュリティ上の脅威やリスクの把握、必要な対策の検討、規程や手順等の整備・見直し、役職員への教育・周知、新たな脅威や脆弱性への対応などに取り組んでいます。

また、情報セキュリティを取り巻く状況、確認されたリスク、対策の実施状況等について、必要に応じて経営層に報告し、組織として必要な判断及び対応につなげています。

3. 個人情報の保護

センターでは、受験申込等を通じてお預かりする個人情報について、利用目的や取扱方法を定め、これに基づいて管理しています。

また、センターは、プライバシーマーク（P マーク）を取得し、個人情報保護マネジメントシステムを整備・運用しています。

受験者の皆様からお預かりする個人情報については、不正アクセス、紛失、漏えい等を防止するための安全管理措置を講じるとともに、その取扱状況を継続的に確認し、必要に応じて管理方法や対策の見直しを行っています。また、保有する個人情報は利用目的に照らして必要な範囲にとどめ、保存期間を定めた上で、不要となったものは適切に消去しています。

4. サイバー攻撃への対策

センターでは、受験者の皆様からお預かりする個人情報や国家試験に関する重要な情報をサイバー攻撃から守るため、技術面と組織面の複数の対策を組み合わせて実施しています。

（1）重要な個人情報・国家試験情報のインターネットからの分離

センターが業務で取り扱う受験者の個人情報（過去の試験の合否に関する情報を含みます。）や、試験問題、解答その他の国家試験の公正な実施に関わる重要な情報は、その性質や取扱方法に応じて、インターネットに接続していない環境で管理し、外部からの不正アクセスによる情報の漏えい、改ざん等のリスクの低減を図っています。

なお、インターネットによる受験申込の受付には外部事業者のシステムを利用しており、当該システムについては、7. に記載のとおり、委託先を含めたセキュリティ対策に取り組んでいます。

(2)不正アクセス・マルウェア等への対策

インターネットへの接続が必要な情報システムについては、不正アクセス、マルウェア、ランサムウェア、フィッシングその他のサイバー攻撃に備え、複数のセキュリティ対策を講じています。

また、認証及びアクセス管理、システムやソフトウェアの更新、バックアップ、ログの確認などを通じて、サイバー攻撃による被害の防止及び影響の低減に取り組んでいます。

(3)脆弱性の検証及びセキュリティ対策の見直し

サイバー攻撃の手法や脅威は絶えず変化していることから、情報管理政策室及び外部の専門家を中心として、情報システムやソフトウェア等の脆弱性に関する情報を継続的に把握し、リスクに応じた対応を行っています。

また、情報システムの脆弱性の検証や、模擬的な攻撃によるセキュリティ対策の検証に取り組み、その結果を対策の見直しや強化に活用します。

さらに、新たな攻撃手法や技術動向等に関する情報を継続的に収集し、センターの情報システムや業務への影響を確認しながら、セキュリティ対策の改善を進めています。

5. 国家試験に関する重要情報の管理

センターでは、国家試験の公正性と信頼性を確保するため、試験問題、解答その他の試験の実施に関係する重要な情報について、その重要性や業務上の必要性に応じた管理を行っています。

これらの情報については、利用できる者や取扱範囲を定めるなど、不正な閲覧、利用、持出し、改ざん、漏えい等を防止するための措置を講じています。

6. 役職員に対する教育・啓発

情報セキュリティを確保するためには、情報システム上の対策だけでなく、役職員一人ひとりが情報セキュリティ上のリスクを認識し、定められたルールに基づいて行動することも重要です。

センターでは、フィッシング、不審なメールやファイル、認証情報や個人情報の不適切な取扱い等による事故を防止するため、役職員に対する情報セキュリティ及び個人情報保護に関する教育、周知、注意喚起等を継続して行っています。

7. 委託先等を含めたセキュリティ対策

センターの業務では、外部事業者が提供するシステムやサービス等も利用しています。

そのため、センター内部の対策だけでなく、委託先等を含めたサプライチェーン全体のセキュリティリスクを考慮することが重要であると認識しています。

業務を外部に委託する場合には、取り扱う情報や業務の重要性に応じて、委託先に求める情報セキュリティ上の事項を定めるとともに、契約、委託先における取扱状況の確認、事故発生時の報告等を通じて、委託業務に伴うセキュリティリスクの低減に取り組んでいます。

8. インシデント発生時の対応

センターでは、サイバー攻撃、不正アクセス、情報漏えいその他の情報セキュリティ上の事案が発生した場合に備え、被害の拡大防止、状況の把握、原因の調査、システム及び業務の復旧並びに再発防止等を行うための体制を整備しています。

重大な事案が発生した場合には、その内容や影響に応じて、関係機関や外部の専門機関等とも連携し、必要な対応を行います。

また、関係法令等に基づき、報告、本人への通知、公表等が必要となる場合には、法令や定められた手順等に基づいて対応します。

情報セキュリティに関する情報については、その内容や影響に応じて、受験者、関係機関、役職員その他の関係者など、情報を必要とする対象を明確にした上で、必要な情報を分かりやすく発信します。

特に、情報漏えい等による二次被害のおそれがある場合には、被害の拡大防止の観点から、対象となる方への通知、注意喚起、公表その他の情報発信を行います。

9. 事業継続及び早期復旧への取組

サイバーセキュリティ対策では、サイバー攻撃を未然に防止することに加え、万一の事態が発生した場合にも、重要な業務への影響をできるだけ抑え、早期に復旧することが重要です。

センターでは、サイバー攻撃や情報システム障害等によって国家試験の実施や受験者サービスに重大な影響が生じることがないよう、事業継続及び早期復旧の観点から必要な対策に取り組んでいます。

また、重要なシステム及びデータについては、業務への影響や情報の重要性を踏まえたバックアップ及び復旧手順を整備し、必要に応じて見直しや確認を行っています。

10. 継続的なセキュリティ対策の強化

サイバー攻撃の手法や情報セキュリティを取り巻く環境は絶えず変化しています。

センターでは、こうした変化に対応するため、情報管理政策室及び外部の専門家を中心として、関係部署と連携しながら、次の取組を継続して進めてまいります。

- 重要な個人情報・国家試験情報の分離・管理
- 情報セキュリティ管理体制の継続的な改善
- 個人情報保護マネジメントシステムに基づく管理の継続
- 不正アクセスやマルウェア等への対策
- 情報システム等の脆弱性の把握・検証及び対応
- 模擬的な攻撃等によるセキュリティ対策の検証
- 認証及びアクセス管理の強化
- 国家試験に関する重要情報の管理
- インシデントへの対応能力の向上
- 事業継続及び早期復旧に向けた取組
- 委託先等を含めたサプライチェーンリスクへの対応
- 役職員に対する継続的な教育・啓発
- 情報を必要とする対象を明確にした情報発信の強化

これらの取組について、新たな脅威、攻撃手法、技術動向等を踏まえて継続的に見直し、センター全体のサイバーセキュリティ対策の強化につなげてまいります。

おわりに

センターは、国家試験を実施する機関として、試験の公正性と信頼性を確保するとともに、受験者の皆様からお預かりする個人情報や国家試験に関する重要な情報を安全に管理することが、社会からの信頼を維持するための重要な責務であると考えています。

今後も、重要な個人情報・国家試験情報の管理、プライバシーマーク制度に基づく個人情報保護、情報管理政策室及び外部の専門家を中心とした情報セキュリティ管理体制の充実を図るとともに、脆弱性の検証や模擬的な攻撃による検証等を取り入れながら、情報セキュリティ対策を継続的に強化してまいります。

また、情報セキュリティ上の事案が発生した場合には、その内容や影響を踏まえ、情報を必要とする対象に応じた情報発信を行い、被害の拡大や二次被害の防止に取り組みます。

センターは、内閣官房国家サイバー統括室（※）が令和 8 年 11 月 5 日に公表した「個人情報の漏えい等につながる不正アクセスへの対策について」、及び同月 6 日にサイバーセキュリティに関する関係閣僚会議で決定された「サイバーセキュリティ緊急対策パッケージ」の内容も踏まえ、これらの取組を通じて、安全かつ安定した国家試験の実施に努めてまいります。

※ https://www.cyber.go.jp/

受験者の皆様へのお願い

センターを装った不審なメールや SMS、電話等にご注意ください。お心当たりのない連絡を受け取った場合は、記載されたリンクを開いたり、個人情報を入力したりせず、センターの公式ホームページに掲載している連絡先にお問い合わせください。