セキュリティインシデント対応支援サービス

仕様書

１．件名

セキュリティインシデント対応支援サービス

２．概要

本学におけるセキュリティインシデント発生時に、迅速にフォレンジック調査等の支援、情報セキュリティに関する専門的な知識をもった外部サポートの提供等を受ける為に、事前に対応支援サービスを契約するもの。

３．契約期間

2025年10月1日から2026年９月30日まで

４．要件

インシデント対応や支援内容には、以下の項目を含むこと。

(1) リモートまたは対面によるインシデントに関する相談を受け入れること。

(2) マルウェアなどの不審なプログラムについて、逆アセンブルによる静的解析をすること。

(3) PC、またはサーバのシステムログ、ネットワーク（Proxy、Firewall、その他NW機器など）の調査およびログ解析をすること。

(4) IPアドレスやURLなどの悪性調査をすること。

(5) インシデント発生時の初動対応や封じ込めに伴う技術支援や対応方針の助言を行うこと。
なお初回打合せは、8営業時間内を目標に実施すること。

(6) インシデント概要の整理に向けての後方支援を行うこと。

(7) インシデントの調査方針に関する助言を行うこと。

(8) インシデント対応に関する打合せに同席と助言を行うこと。

(9) 関係各所への技術的な説明を実施する際に、対面またはオンラインで同行・同席すること。

(10) 不正アクセスによる侵入痕跡の事実確認と原因調査をすること。

(11) 不正ログイン、ファイル・コマンド操作履歴等の確認による影響範囲を調査すること。

(12) 情報漏洩の痕跡や他システムへの影響範囲を調査すること。

(13) マルウェア検体の抽出・解析を試行し、動作原理・機能および痕跡より影響を推定すること。

(14) 調査結果などに基づいた被害拡大防止に資する助言を行うこと

(15) 再発防止策や復旧に関する助言を通じて事態収束に向けた支援を行うこと。

(16) 進捗報告（実施内容、調査結果、今後の計画を含む）を行うこと。

(17) 支援結果の報告を行うこと。

(18) (1)～(17)のサービスはチケット制による提供で、受けるサービスに対し保有しているチケット内で自由に選択できること。

なおチケットは、(1)～(17)のサービスについて実施時間20時間以上を保証すること。

(19) 本サービスを提供する従業員の中に、以下の資格保有者が含まれていること。

CISSP, 情報処理安全確保支援士

5.機密情報の取扱

本サービスが終了したとき、調査・解析したすべての秘密情報について、返還、消去または廃棄すること。ただし、本サービスの取引記録、または、紛争解決等合理的な目的により保管する必要がある秘密情報は除く。

6.その他

その他業務の実施にあたり、この仕様書に定めのない事項について疑義が生じた場合は、協議のうえこれを解決するものとする。