S1-01「SJK 大学研究データの流出疑い（外部通知）」対応フローワークシート

私情協大学セキュリティ研究講習会

Ⅰ．通知者の信憑性確認

① 外部機関から学内の端末と通信している C&C サーバーが発見されたことを、メールで通知されました。そのメールを用いて、通知者の信憑性を確認するにはどのような手段がありますか？また、そのメールを扱う際の注意点には、どのようなものがありますか？

（テ）

（マ）

Ⅱ．一次対応（状況把握とログ保全）

① 通知のあった対象端末は、学内の研究室、事務局、情報教育システム、持ち込みエリアのいずれかに設置されていると推測されます。端末の特定や端末内部の調査を行うにあたって、規定には何が記載されているべきでしょうか？

（マ）

② 対象端末の特定、*関連情報の取集*には、どのようなシステムのログを調査するべきでしょうか？（但し、研究室の端末は除きます。）

（テ）

※ ログを採取するシステムに共通して行うべき重要な設定には、どのようなものがありますか？

（テ）

③ ②の調査によって、指摘を受けた IP アドレスは、学内の研究室に設置された 1 台の端末の IP アドレスと結びついていることが分かりました。この端末の内部を調査するにあたって、組織として、誰が誰にどのような依頼をかけるべきでしょうか？

（マ）

④ ③の依頼が通りました。どのようなログを保全するべきでしょうか？

（テ）

⑤ *②と*④の保全ログを確認したところ、外部通知の内容がほぼ正しいと認められました。インシデントのレベル*（3段階を想定し）*を判定して下さい。

（マ）

⑥ ⑤で判断したインシデントレベルに合せて、緊急措置を発動して下さい。

（マ）→（テ）

⑦ ⑥の緊急措置発令に対し、技術的にはどのような対応をとりますか？

（テ）

⑧ CIO への（一次）報告内容を整理して下さい。

（マ）

⑨二次対応として必要な技術的事項を挙げて下さい。

（テ）→（マ）

Ⅲ．二次対応（詳細な調査と封じ込め）

① 今回の場合*（研究室毎 VLAN で相互通信は不許可）*は、内部拡散の有無については、どの範囲で調査しますか？

（テ）

② 端末のフォレンジック調査は、どの程度の情報を得るようにセキュリティベンダーに依頼しますか？費用の試算はどの位になりますか？また、どの予算からの出費になりますか？

（マ）

③ 攻撃の封じ込めは、どのようにして行いますか？

（テ）

Ⅲ．事後対応計画

① 再発防止策として必要と思われる内容を列挙しなさい。

（テ）

（マ）

② 報告・公示は、誰宛てに行いますか？

（マ）