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（解答例）

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）

メールヘッダーの確認（メール転送経路やグリニッジ標準時間との差、送信時刻など）、迷惑メール判定、日本語表現の巧拙、PGP、SPF や DKIM の確認、Whois。
留意点として、添付ファイルを開いたり、本文中のリンクをクリックしない、ことが挙げられる。　信頼できる　⇒　（マ）

（マ）

外部機関の連絡先を別途入手し、電話などメール以外の手段で警告の事実を確認する。また、対応窓口（マ）であることを、外部機関に通知する。
信頼できるとし、調査を行うことを判断

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）

学内 LAN のすべてのエリアに接続されている端末やメディア機器は、CIO がレベル２、３のインシデントが疑われ、緊急措置の必要性を判断した場合、その IP アドレスの調査が可能であるよう規定に記載するべき。
また、レベル２、３のインシデントが疑われる場合は、端末管理者は調査に協力しなければならない旨を明記するべき。

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）

F/W、NAT 変換テーブル、IPS/IDS の通信ログ、Proxy（利用していれば）

検索ツール
SIEM(Security Information and Event Management)、F/W のログ検索ツールがあれば望ましい。

※ 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）

学内でログを採取するシステムには時刻同期の必要がある。また、可能なら端末も同様の措置が望ましい。

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）

CIO または情報センター長がレベル２、３のインシデントが疑われると判断し、該当の端末を所有する研究室責任者（教員）に、端末の通信ログ・操作記録の調査の許可を依頼する。また、該当教員に不審なメールの受信が無かったかインタビューする。

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）

IP アドレス、ウイルス対策ソフトのログ、パーソナルファイアウォールのログ
最近開いたファイル、レジストリ、スタートアップ、ウェブ閲覧ログ
※ 研究情報の取り扱いと意味のある情報入手が問題、データ保全（スナップショット）： 委任？ あるいは協働作業

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）

レベル３： 情報漏えい有、またはその可能性大
レベル２： 情報の流失の実態が確認できないが、通信実態有
レベル１： 指摘端末等、その他で通信実態の確認が早急にできない

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）

レベル２のインシデントに対して、該当端末の学内 LAN からの切り離しを指示。
理由： 通信が確認され、二次被害防止のため

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）

該当端末の電源は遮断しないまま、該当の研究室 VLAN の接続されている S/W のポートを無効化する。

⑧ CIO への（一次）報告内容を整理して下さい。

（マ）

外部機関からの通知内容と信憑性
該当する学内端末との通信状況（プロキシ、F/W ログなど）
該当教員のインタビュー結果
想定される脅威（研究データの流出、企業との機密保持契約違反など）
今後の調査方針
その他

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）

調査継続の内容
　該当研究室 VLAN 内のネットワークトラフィックキャプチャ
　該当端末のフォレンジック調査依頼の可否
　侵入・拡散範囲の調査の可否
　複合機（プリンタ）その他のメディア機器と外部通信の有無

これ以外に？

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）

該当の研究室 VLAN 内のみでの内部拡散の調査を行う。
その結果次第で、調査範囲を拡大するか判断する。

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）

要求として、

- ・メモリ、HDD の正確な保全
- ・不審なファイル作成やプロセス起動・通信状況調査、ネットワークログオンや媒体による拡散の有無、トリガーとなったマルウェアの特定
- ・タイムライン解析による侵入・拡散の進行状況調査

★ いつ頃、何処からどのような方法で侵入され、どのような方法でどのようなファイル（情報）が**持ち出されたのか、可能性？**

★ バックドアの有無および種別

★ この行為が外部で**第三者によるものである証拠**

を依頼する。該当端末：100 万円/台程度を CIO 予算から捻出.

③ 攻撃の封じ込めは、どのようにして行いますか？

（テ）

研究データを標的とした攻撃では、他の研究室への拡散は通常少ない。しかし、ポップポイントとして利用が考えられ、外部通信を継続的に監視する。

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）

攻撃調査結果に基づき、原因とされる（可能性含む）事項に対するセキュリティ強化を行う。

・ネットワーク分離、隔離
・通信の監視の機器の強化・更新（外部委託の検討）
・端末セキュリティソフトの強化
・重要データの暗号化

（マ）

・研究者として研究活動の行動規範等に研究として扱う情報の管理について反映あるいは再確認を促し、再認識等の啓蒙を行う。
・研究室内での利用規程策定、適用の推進

② 報告・公示は、誰宛てに行いますか？

（マ）

・外部通報者に対し、大学組織とした（対応策を含め）返答を行う。
・情報流失、漏えいの内容の応じた報告・公示を検討する。なお、漏えい内容に応じては、詳細な情報調査結果を待たず、二次被害防止の観点からの報告（学内関係部局）を検討し、関係者に連絡が必要である。また調査結果に応じ、公示（ガバナンス）を検討する。