2015/8/26
私情協大学セキュリティ研究講習会

S1-02「SJK 大学事務局マルウェア感染の疑い（内部通知）」対応フロー

私情協大学セキュリティ研究講習会

Ⅰ．通知者の確認

① 内部の者から、「2 日ほど前に、メールに添付されたファイルを開いて、マルウェアに感染したかもしれない」、との電話連絡がありました。連絡を受け付ける際には、どのような情報を収集しますか？

（マ）

Ⅱ．一次対応（状況把握とログ保全）

① 通知のあった標的型サイバー攻撃メールの調査を行うにあたって、該当のメールからはどのような情報を収集するべきでしょうか？また、注意点を挙げなさい。

（テ）

② 同様の被害（同様のメール受信）が発生していないか調べるには、どのようなシステムのログを調査するべきでしょうか？

（テ）

③ 通知者から該当のメールおよび添付ファイルを、どのような方法で入手しますか？また、その添付ファイルがマルウェアとしての挙動を示すか調査するためには、どのような作業を行いますか？

最終的に、このメールと添付ファイルは、どのように処分しますか？

（テ）

④ ③の調査で、該当の添付ファイルはマルウェアであると確認されました。（テ）は（マ）への報告を行ってください。

（テ）→（マ）

⑤ インシデントのレベルを判定して下さい。

（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 二次対応として技術的に必要な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、何を証明するため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 ②の要求を技術的な要求仕様にすると、どのような項目になりますか？

（テ）

④ 攻撃の封じ込めは、どのようにして行いますか？

（テ）

Ⅳ．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）