2015/8/26
私情協大学セキュリティ研究講習会

S1-03「不可抗力による意図しない情報流失（外部通知)」対応フロー（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

（省略）

ここでは､通知内容をすぐに CIO に報告し､取材対応を行うことを決定したものとします。また、本件はインシデントレベル３と認定され、緊急対応することになりました。

Ⅱ．一次対応（状況把握とログ保全）

① 通知のあった対象複合機（プリンタ）以外にも、複合機（プリンタ）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。複合機（プリンタ）の特定を行うにあたって、規程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３のインシデントが疑われる場合は、端末管理者は、端末の操作・通信記録調査に協力しなければならない旨を明記するべき。

② インターネットからアクセスできる複合機（プリンタ）の特定には、どのような技術あるいは手段を用いて調査するべきでしょうか？

（テ、マ）

ポートスキャン（またはデバイス検索システムなど)。 備品台帳情報による問い合わせ。

③ 緊急対応として、技術的にはどのような対応をとりますか？

（テ）

対象端末のインターネット接続制限 対象端末の管理（パスワード）設定の確認（個別)） 対応端末（複合機）での保存データの内容（公開が好ましくない情報の有無）とその管理調査

Ⅲ．二次対応（詳細な調査と対応の検討）

① 本案件では、あるメーカーの複合機（プリンタ）の仕様として、下記の 3 点に問題がありました。

ｉ）管理画面への接続制限設定手順の説明がない、あるいはその機能がない。

ii）印刷等に不要なサービスがデフォルトで有効：　踏み台？

iii）ジョブ（印刷）履歴の表示制限対応

メーカー：ジョブ履歴表示対応（実習、自習環境）

この問題に対し、メーカー、ネットワーク管理者、複合機（プリンタ）管理責任者に対し、どのような対応を取るべきか、挙げなさい。

テ）

メーカー：複合機、プリンタのサービス範囲を再検討し、端末のアクセスコントロール、ローカル IP 環境への意向、ネットワーク制限等を行う。

ネットワーク・システム管理者：大学としての推奨設定を定め、管理に関する手引きを作成し、不要なサービス（Web, telnet/ssh, ftp, SMB 等）を停止させる。複合機導入時には、メーカーのセキュリティチェック（シート）の活用し、利用者と導入業者が協議し、設定を行い、この情報を利用者が保管すること。

ユーザー：実習、自習環境ではジョブ履歴の表示制限を行う（メーカーによっては、メーカカスタマの設定が必要）。 個別利用は必要時のみに電源を投入する。

② 本件の取材対応は、CIO、事務局責任者、広報部、情報センターで行います。マスコミ側に確認しておくべきことには、どのような事項があるでしょうか？

マ）

取材目的の明確化（情報流出の当事者か？被害者か？） 取材時の資料の準備は必要であるが、要求が無い限り提出は不要。