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

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）

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）

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）

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）

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）
