インシデント情報共有の仕組みづくり提案に向けて
−調査項目中間報告−

立命館大学　情報システム部
岡　潤也

平成26年度　大学情報セキュリティ研究講習会

検討項目

1. 目的・成果物への賛否
2. 収集/公開対象のインシデント情報
3. 共有情報の範囲
4. 情報共有の対象
5. 想定される学内手続
6. 約款・申し合わせ事項に含むべき項目

1. 目的・成果物への賛否

1) 目的
ITインフラの複雑化、SNSの普及、標的型攻撃など、インシデント発生の可能性が高まっている。
また、学生や研究者を擁する大学という特殊な性質上、発生したインシデントの情報を大学間で共有し、今後の対策に相互に役立てていく仕組みが有効ではないかと考える。

2) 成果
事例シートの公開（半期ごとのレビュー）
メーリングリストによる攻撃手法告知

※ 原則となる考え方
共有する情報は、情報提供元や関係者の特定に繋がる内容や、機微な内容を極力マスク（匿名化）したものとする。

2. 収集/公開対象のインシデント情報

1) 2つのカテゴリー

「教育インフラとしての安全性」カテゴリー⇒アーカイブの必要性

「研究機関としての機密性」カテゴリー　⇒リアルタイム性の要求

2) 具体例

Web改竄、なりすましメール送信、踏み台、フィッシング、情報漏洩、情報消失、SNSトラブル、ITを使った悪戯、未然に防いだインシデント

3.共有情報の範囲

1) インシデント自体に係る情報
- ・発見者（学外者からの通報）
- ・発見日時（2014.6.30）
- ・被害者（XX学部学生）
- ・被害内容
  （氏名・住所のリスト流失）
- ・被害額（不明）
- ・発生日時
  （2014.4月頃と推定）
- ・一次原因
  （研究室で管理PCより流失）

2) 原因・要因に係る情報
- ・根本原因 （XXウィルス感染）
- ・失敗要因
  （ウイルス対策ソフトの
  未インストール）

3) 対策に係る情報
- ・暫定対策（PCをLANから解除、
  学内全PCにスキャン実施）
- ・事態収束日時 （2014.5月頃と推定）
- ・恒久対策
  （情報部門がFW内にファイルサーバを設置、今後利用規則を整備予定）
- ・回復費用（ベンダーSE人件費）
- ・対策費用
  （約2千万円サーバー機器設置費用）
- ・公表範囲
  （理事会報告および貴社発表）

4) その他
- ・公開出来ない理由
  （被害関係者との協定）

4. 情報共有の対象

- *・私情協加盟校のうち協定のある学校*
- *・私情協加盟校*
- *・特に対象は問わない（IPA等通じて公開可能）*

5. 想定される学内手続

例　理事会での承認が必要

情報センター長の決裁で対応可能

6. 約款・申し合わせ事項に含むべき項目

1. 私情協側
   - ・責任者リスト
   - ・情報アクセス者のリスト
   - ・情報記載ファイルの保管体制
   - ・情報の削除要求方法

2. 情報提供側
   - ・公開項目・公開時期
   - ・情報共有対象者
   - ・漏洩時の対処方法

3. 情報受理側
   - ・情報共有対象者
     - ・情報システム部門
     - ・教職員
     - ・学生
   - ・共有期間