初期対応協議ワークシート

私立大学情報教育協会
大学情報セキュリティ研究講習会

被害の特定（タイムライン解析の結果を受けて）

1. 被害の期間は
2. 被害の影響範囲は

   学外か、学内か、相手方は更に特定できるのか…　：
3. 被害の対象は

   システムあるいはネットワークの名称　：

   機種　：

   OS　　：

   利用目的　：

   管理される情報の種別　：

   被害の種類（個人情報漏えい、名誉棄損、詐欺etc）　：

   物理的損壊：

発見過程の特定

1. 誰が、いつ、何をしていて発見したのか
   誰：
   いつ：
   何をしていて：

2. 誰が、いつ、どうやって受理したのか
   誰：
   いつ：
   何をしていて：

報告・説明の準備

1. 誰が、誰に報告するのか。
   - □　規程上の学内エスカレーション（上申先）
   - □　広報部門（学外窓口）
   - □　父母
   - □　警察
   - □　法律専門家

2. どういったインシデントと位置づけるか
   - □　セキュリティインシデント
   - □　コンテンツインシデント（不適切なコンテンツの掲出等）
   - □　学内規程違反

原因の特定

1. 感染／攻撃の経路、要因など

□国内　□海外　□経路不明
□電子メール
□ダウンロードファイル
□WEBサイト閲覧
□外部からの媒体
□パスワード盗用
□セキュリティホール悪用・設定不備
(ソフト名・バージョン　　)
□その他
(　　)

システム的被害状況の特定

1. 攻撃手法・ウイルス名称（不明な場合は症状）は？

2. 攻撃の手口は？

□ファイル／データ奪取、改竄、消去、破壊

□不正プログラムの埋め込み（トロイの木馬、ボット、バックドアなど）

□権限取得

□踏み台

□サービス妨害

□資源利用（ファイル、ＣＰＵ使用）

□メールの不正中継

□メールアドレス詐称

３．被害の結果、どのような動作に陥ったか？

応急措置の実施

□パッチ・サービスパック適用

□アンチウイルスソフトで駆除または削除

（社名：　　ソフト名：　　）

□フリーの専用駆除ソフトで駆除

（ソフト名、またはダウンロード先のＵＲＬ等）

□ファイル（メール）の削除

□初期化

□情報発信関連サーバ・BBS等の一時停止

□権利侵害･違法コンテンツ送信の一時停止

□その他（　　）

恒久対処の実施

1. 技術的対処

□パッチ・サービスパック適用 (パッチ・サービスパックの名称は？)

□ソフトウェア・プログラム設定変更 (ソフトウエア・プログラムの名称、設定作業内容は？)

□ソフトウェア・プログラム更新・削除

□機器撤去 (永久使用しない場合のみ)

2. 事務的対処

□利用者の懲罰委員会への報告

□外部機関への連絡・通報・届け出（警察、JPCERT、IPA等）

□民事訴訟他の民事手続きの提起・応訴等

□インシデント終息に向けた学内報告・決裁／記録