【作業１】

情報セキュリティ事故発生報告書

インシデント番号/件　　名	Si2016082401　学生個人情報流出インシデント		
報告者 （所属・氏名）	情報処理センタ　〇〇〇〇	報告日	2016 年 8 月 24 日

下記事項のうち判明していることを迅速に報告すること。

事故発見者 （※）	JPCERT/CC，受付　〇〇〇〇 不明	発見日時	2016 年 8 月 23 日 メール受信時時頃
事故発生場所	外部組織からの通報	発生日時	2016 年 8 月 23 日 19 時頃
事故の種類	□システム障害（公開システム・社内共有システム・個人システム）		
	□外部からの攻撃（ウイルス感染・不正アクセス・改ざん・その他）		
	◆情報漏えい		
	（紛失・盗難・誤送信・誤公開・管理ミス・内部犯行・その他） （意図的要因・非意図的要因）（発災当事者判明・発災当事者不明）		
影響範囲	◆学生　□教職員全員　□複数部署　□単一部署 □個人		

（※）情報漏えいの場合は、発災当事者を記載し不明な場合は不明と記載すること。

対象資産 （媒体、範囲、量）		学生の個人情報の流出（デジタルファイル、範囲、量不明）
事故の内容		学生の個人情報が 10.10.19.123 にアップロードされているとの信頼できる組織からの通報があった。ファイルを確認した。なお、8 月 22 日 19:12 に C&C サーバ(10.10.10.2)と通信の追跡の過程で発見をされた。
想定される原因		8 月 22 日 19:12 に C&C サーバ(10.10.10.2)と通信を行った端末（周辺）がマルウェアに感染し、データが搾取されたと思われる。
想定される二次被害等影響		
初期対応	暫定措置	
	現在の状況	
復旧時期の見込み		
対応実施者		