別 紙

# 富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について（概要）

## ◎ 経緯

H28.6/14（火） 外部機関から本学ＰＣのウィルス感染の可能性ありとの情報提供があり，水素同位体科学研究センター非常勤職員が使用する PC がウィルスに感染していたことが判明
直ちに学内調査を開始（通信ログの解析）

6/16（木） 文科省にインシデントの概要，被害状況，外部機関への連携状況等について第 1 報を報告
当該ＰＣ内保有情報の学内調査，分析を開始

6/27（月） 通信ログの解析終了（学内調査）
文科省に今後の再発防止策，当該職員の対応・認識状況，ログの解析状況等について第 2 報として追加報告

7/ 6（水） 外部専門業者による詳細な解析開始

8/ 3（水） 当該ＰＣ内保有情報の学内調査，分析終了

8/31（水） 外部専門業者より調査結果の報告
その後、大学において漏えいした情報の内容を確認・評価

9/27（火） 文科省へ調査状況の報告

10/ 7（金） 関係機関へ連絡開始

## ◎ 調査結果

### ○ 学内調査（通信ログ等）及び外部専門業者の解析結果から判明した事項

①zip 形式のファイルが添付された不審メールを 2 回受信（ファイル展開はなかった）
（受信日：平成 27 年 11 月 5 日，平成 27 年 11 月 17 日）

②標的型メールを受信し，添付ファイル（zip 形式）を展開したことによるウィルス感染
（受信及び感染日：平成 27 年 11 月 24 日）

③外部サーバとの不審な通信（4 件），不審なファイルの作成

（ア） supportservice247.com（平成 27 年 11 月 24 日～平成 28 年 4 月 29 日）

（イ） requestword.com（平成 27 年 11 月 26 日～平成 28 年 2 月 29 日）
不審なファイル（１ファイル 2MB の rar 形式）の作成及び消去の形跡
同様なファイルの 1,000 個以上の作成（総容量は圧縮状態で 2GB 以上と推測）
同時間帯における大量な通信（8GByte 以上）の発生

（ウ） enewsdatabank.com（平成 28 年 2 月 29 日～平成 28 年 6 月 14 日）
不審なファイル（zip 形式）の作成（平成 28 年 3 月 10 日）
同時間帯における大量な通信の発生

（エ） housemarket21.com（平成 28 年 4 月 28 日，平成 28 年 6 月 14 日）

### ○ 当該ＰＣ内保有情報

- 平成 6 年から平成 28 年 6 月 13 日までの電子ファイルを保有
- 全フォルダー数： 7,034 個
- 全ファイル数 ： 59,318 個
- 総容量 ： 40.2GB

◆当該 PC 内保有情報に関する調査結果
全ファイル数のうち展開できたファイル：41,706 個

展開できたファイルのうち，詳細な確認を要するファイルとして内容を精査，確認
ア.個人に関する情報
展開できたファイルのうち，1,492 名分の個人に関する情報が含まれていた
【内訳】

| | | |
|---|---|---|
| ・本学学生 | 15 名分 | |
| ・他大学及び試験研究機関所属 | 1,316 名分 | |
| ・企業（企業の研究所を含む） | 52 名分 | |
| ・官公庁関係 | 3 名分 | |
| ・その他 | 106 名分 | 合計 1,492 名分 |

イ.研究に関する情報
汚染水から放射性物質を分離・除去する技術等をテーマとした外部資金申請関係や学会発表，実験データなどの研究に関する情報（⇒発表等されている公知のもの，公開を前提のものであり、機密情報に該当しない）

## ◎　課題

### ○ 情報セキュリティ実施体制の整備及びログ監視体制の強化
・全学的な情報セキュリティ対策を実施するための組織体制の見直し，整備
・不正アクセス，ウィルス感染等の監視体制の強化

### ○ 関係規則等の整備
・情報の格付けに関する規程，インシデント発生時の対応手順等関係規程の整備

### ○ 教育・研修の実施
・全職員・学生に対する教育の徹底
・非常勤職員を含む職員に対する個人情報保護規則遵守の一層の周知徹底

## ◎　今後の再発防止策

### ○ 全学的な情報セキュリティ実施体制，インシデント対応手順書等の整備
・情報セキュリティポリシーを見直し，CISO，CSIRT の設置を含めた実施体制の整備
・情報セキュリティインシデント対策基準，情報の格付けに関する規程，パスワードの設定に係るガイドライン等の整備

### ○ 情報セキュリティ教育・訓練や啓発活動の実施
・個人情報保護及び情報セキュリティに関する基礎研修（e－learning）の受講を全職員，全学生に義務化
・学内講習会にて，ウィルスに感染しないための教育及び感染した場合の対応に関する教育並びに個人情報の適切な管理に関する教育の実施
・情報管理関係の利用手引の見直しを行い，全職員に改めて配付
・全職員に対し，不正アクセスやウィルス感染等の異常があった際の報告の義務化

### ○ 情報機器の管理状況の把握及び必要な措置の実施
・標的型攻撃検知システムを導入し，ログ監視体制の更なる強化
・情報セキュリティ検査（ポートスキャン）の継続的実施

### ○ 情報セキュリティ対策基本計画の策定等
・情報セキュリティ対策基本計画の策定
・工程表による進捗状況のチェック及び PDCA サイクルの実行

### ○ 危機管理体制の整備
・全学的なリスク管理及び危機事案の情報管理を行う危機管理体制の整備