

## [2013]九州大学情報統括本部年報 : 2013年度

<https://doi.org/10.15017/1559839>

---

出版情報 : 九州大学情報統括本部年報. 2013, pp.1-, 2014. 九州大学情報統括本部  
バージョン :  
権利関係 :



# 第16章 情報セキュリティ対策事業

## 16.1 情報インシデントの事前防止

### (1) 注意喚起等

- 長期休暇中（ゴールデンウィーク、お盆期間中）の著作権侵害等の違法行為について（情報セキュリティ対策室 HP に掲載、部局長等へ通知）
- 「情報セキュリティ安全対策（個人マニュアル）」を九大教職員（新規採用者）へ配布しました。
- 「情報セキュリティガイド」を改訂し、教職員、学生、その他利用者へ配付しました。（平成 25 年 4 月配付）

### (2) 情報セキュリティ関係セミナー

- 部局開催の情報セキュリティ（ファイル交換ソフト、著作権侵害等）セミナー等に係る講師を派遣しました。
- 総務部の依頼に基づき「平成 25 年度個人情報保護研修会」に情報セキュリティに係る講師を派遣しました。

（平成 25 年度）

部局	講演会名等	開催年月日	参加者数	講師
外国人留学生・研究者サポートセンター	新入留学生オリエンテーション	4月 5日	222 名	岡村教授
外国人留学生・研究者サポートセンター	新入留学生オリエンテーション	9月30日	351 名	#
総務部	平成 25 年度個人情報保護研修会	10月28日 10月29日	51 名 22 名	藤村教授 山寄情報企画課長

### (3) 情報インシデント対策に関する広報や文書作成

- 情報インシデント対策に関する注意喚起等に係る文書を作成しました。
  1. 外部サービスを利用した情報発信に関するガイドライン
  2. サポート期間終了ソフトウェアの取扱いについて
  3. 複合機等のネットワークに接続している情報機器のセキュリティについて

4. TV会議システム等の取扱いについて
5. 学外の情報共有サービス等の利用に係る留意点について
6. 日本語文字入力補助ソフトによる情報漏えいの危険性について
7. 九州大学の不特定多数の者に送信されていると思われるメールに対する注意喚起について
8. 動画再生ソフト GOM プレーヤーによる情報漏洩の危険性について
9. 研究者共同利用サーバ不正アクセス等の注意喚起及び被害状況調査
10. Internet Explorer の未修正の脆弱性について
11. 九州大学の不特定多数の者に送信されていると思われるメールに対する注意喚起について
12. 九州大学の不特定多数の者に送信されていると思われるメールに対する注意喚起について
13. 申請されていない学内の VPN 接続をファイアウォールにより制限する注意喚起について
14. Microsoft Word の脆弱性について

## 16.2 情報インシデントの応急対応情報セキュリティインシデント（ウイルス、不正アクセス、不正通信）対応

- セキュリティポリシーに対応したファイアウォールの運用を開始し、P 2 Pソフトウェアの使用による不正な情報通信の遮断を開始しました。
- 情報統括本部から当該支線 LAN 管理者へ IDS による検知通知を行っていますが、通知しても反応がない場合、踏み台による攻撃や著作権侵害などを防止するとともに、利用者に不具合を知らせるために次のような対応を実施しています。
  - － インシデント通知後、翌日正午までに返答がない場合、当該 IP アドレスのフィルタを行う。
  - － ただし、申し出があった場合は速やかに解除を行う。

## 16.3 情報インシデントの調査、事後対策

1. インシデント状況について、情報政策委員会及び部局長会議で報告を行いました。
  - 平成 25 年 4 月～平成 26 年 3 月までにウイルス・ワーム感染系 101 件、セキュリティ被害及び不正利用系 106 件、著作権関連 1 件、PC 等盗難その他 2 件のインシデントの対応を行いました。  
※平成 25 年度 情報セキュリティインシデント管理状況 … [参考資料 1]
2. キャンパス内のセキュリティ状況の把握及び対策について
  - IDS（侵入検知装置）により各支線のセキュリティ侵害の監視を行いました。被害を検知した場合は、各支線 LAN 管理者に対応を行うよう連絡し、その際予防及び対応策についても適時アドバイスをを行いました。
  - 情報セキュリティインシデントが発生した場合の処理フローにしたがって、4 件（平成 26 年 3 月現在）の報告書を処理しました。

### セキュリティインシデント管理状況

(日毎の集計)

項目	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
ウイルス・ワーム感染系	10	6	3	1	7	9	13	7	13	3	20	9	101件
セキュリティ被害不正利用系	5	28	4	2	9	13	5	13	4	4	6	13	106件
著作権関連	0	0	0	0	1	0	0	0	0	0	0	0	1件
PC盗難, その他	0	0	0	0	2	0	0	0	0	0	1	0	3件
計	15	34	7	3	19	22	18	20	17	7	27	22	211件

項目	平成 21 年度	平成 22 年度	平成 23 年度	平成 24 年度	計
ウイルス・ワーム感染系	111	1,050	266	117	1,544件
セキュリティ被害不正利用系	78	192	53	139	462件
著作権関連	16	202	272	53	543件
PC盗難, その他	5	8	11	10	34件
計	210	1,452	602	319	2,583件

※侵入検知装置(IDS)等による検知及び学内外から報告があったインシデントの件数、同一端末インシデントでも別日に再発すれば、再計上。

【主なインシデントの内容】(平成 25 年 4 月～平成 26 年 3 月)

- ・ネットワーク型ワーム(\*)の感染の疑い 101件
  - ・外部より Web サーバに対する不正なファイルアップロードの試みの通信を検知 42件
  - ・学内のホストから外部ホストに対し迷惑メールが送信される 18件
  - ・外部より chargen サービス(19/udp)への多数の通信を検知 10件
  - ・外部からWeb サーバに対するSQL インジェクションを検知 7件
- \*メールではなく、ネットワークを介して感染を広げていくタイプのワームのこと。

(被害件数)

セキュリティ被害状況の推移(平成25年4月～平成26年3月)

