[2014]九州大学情報統括本部年報 : 2014年度

https://doi.org/10.15017/1560528

出版情報：九州大学情報統括本部年報. 2014, pp.1-, 2015. 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，未然に防ぐための注意喚起を行いました。（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）」を九大教職員へ配付しました。（情報セキュリティ対策室 HP において電子版を配布）

●「情報セキュリティガイド」を教職員，学生，その他利用者へ配布しました。（平成 26 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。

●総務部が主催する「平成 26 年度個人情報保護研修会」に、情報セキュリティ担当として講師を派遣しました。

（平成 26 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 4日	208 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	450 名	〃
総務部	平成 26 年度個人情報保護研修会	11月4日 11月6日 11月7日	27 名 30 名 12 名	山嵜情報企画課長 岡村教授 柳場専門職員

(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，学内に注意喚起を行いました。
  ① OpenSSL における修正版ソフトウェアの公開について
  ② Internet Explorer の未修正の脆弱性ついて
  ③ Internet Explorer の未修正の脆弱性ついて（追加情報）
  ④ マイクロソフトワードの脆弱性について：修正プログラム公開
  ⑤ Adobe Flash Player の脆弱性に関する注意喚起

⑥ Security updates available for Adobe Flash Player (APSB14-13)
⑦ Adobe Flash Player の脆弱性に関する注意喚起（追加情報）
⑧ OpenSSL の脆弱性（6 月 5 日公開）に対するお願いと対策方法
⑨ New vulnerabilities of OpenSSL had been disclosed on 5th June,2014.
⑩ Java 実行環境における修正版ソフトウェアの公開について
⑪ Oracle Releases July 2014 Security Advisory
⑫ 夏季休暇中のインターネット等の利用について
⑬ EmEditor の更新機能を悪用したウイルス感染に関する注意喚起
⑭ 情報セキュリティに係る秘密情報及びその取扱いについて
⑮ GNU bash の脆弱性に関する注意喚起 (CVE-2014-6271, CVE-2014-7169)
⑯ Bourne Again Shell (Bash) Remote Code Execution Vulnerability (CVE-2014-6271, CVE-2014-7169)
⑰ GNU bash の脆弱性に関する注意喚起 (CVE-2014-7186, CVE-2014-7187)
⑱ Bourne Again Shell (Bash) Remote Code Execution Vulnerability (CVE-2014-7186, CVE-2014- 7187)
⑲ Kerberos KDC の脆弱性に関する注意喚起
⑳ Vulnerability in Kerberos could allow elevation of privilege
㉑教育、研究、事務等で使用しているスマートフォンの取扱いについて
㉒ GNU C Library (glibc) における修正版ソフトウェアの公開について
㉓ Linux "Ghost" Remote Code Execution Vulnerability
㉔ オンライン翻訳サービスにおける情報漏洩について
㉕ Translated texts leaked onto the Internet
㉖ Lenovo 製 PC の SUPERFISH による不正なデジタル証明書の危険性について
㉗ Lenovo Computers Vulnerable to HTTPS Spoofing
㉘ 米国輸出規制に起因する TLS/SSL ソフトウェアの脆弱性について
㉙ FREAK (Factoring Attack on RSA-EXPORT Keys) SSL/TLS Vulnerability
㉚ サポートの終了したウェブサイト用ソフトウェアへの対応について

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（ウィルス，不正アクセス，不正通信）対応

●セキュリティーポリシーに対応したファイアウォールの運用を実施し、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実施しました。

●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るが，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います。
・ただし，申し出があった場合は速やかに解除を行います。

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 26 年 4 月～平成 27 年 3 月までにウイルス・ワーム感染系 58 件，セキュリティ被害及び不正利用系 96 件，著作権関連 1 件 ,PC 等盗難その他 10 件のインシデントの対応を行いました。

※平成 26 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った。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，15 件（平成 27 年 3 月現在）の報告書を処理しました。

参考資料 1

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
平成26年度	ウイルス･ワーム感染系	7	0	1	5	2	2	1	4	13	1	1	21	58 件
	セキュリティ被害不正利用系	9	9	3	4	9	7	19	6	13	7	7	3	96 件
	著作権関連	0	0	0	1	0	0	0	0	0	0	0	0	1 件
	PC 盗難、その他	0	0	0	0	2	3	0	0	4	0	0	1	10 件
	計	16	9	4	10	13	12	20	10	30	8	8	25	165 件

	項　目	平成 22 年度	平成 23 年度	平成 24 年度	平成 25 年度	平成 26 年度	計
年度別	ウイルス･ワーム感染系	1,050	266	117	101	58	1,592 件
	セキュリティ被害不正利用系	192	53	139	106	96	586 件
	著作権関連	202	272	53	1	1	529 件
	PC 盗難、その他	8	11	10	3	10	42 件
	計	1,452	602	319	211	165	2,749 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 26 年 4 月～平成 27 年 3 月)

- ネットワーク型ワーム(*)の感染の疑い　58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　36件
- Webサーバに対する不正なファイルのアップロードの試みを検知　25件
- PC盗難　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　6件
- Webサーバに対するコマンド実行の試みを検知　6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。