[2015]九州大学情報統括本部年報 : 2015年度

出版情報：九州大学情報統括本部年報. 2015, pp.1-. 九州大学情報統括本部
バージョン：published
権利関係：

第15章　情報セキュリティ対策

15.1　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付）
- 「情報セキュリティガイド」を教職員，学生，その他利用者へ配付しました。（平成 27 年 4 月配付）
- 「情報セキュリティポリシー改訂第 4 版」を学内に通知しました。
- 「クラウドサービス利用ガイドライン（クラウド事業者の選定）」を学内に通知しました。
- 情報インシデントが発生した場合の処理・連絡フローを改定し、学内に周知しました。

(2) 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 異動者に係るＩＤやパスワードについて

  ② PC 等を用いてスクリーンに投影を行う際の注意点について

  ③ Windows Server 2003 のサポート期間終了について

  ④ 標的型攻撃メールに関する注意喚起について

  ⑤ 日本学術会議なりすましメール注意喚起について

  ⑥ Adobe Flash Player の未修正の脆弱性について

  ⑦ Adobe Flash ActionScript 3 opaqueBackground Use-After-Free Vulnerability

  ⑧ Adobe Flash Player における修正版ソフトウェアの公開について

  ⑨ Updates Available for Flash AS3 opaqueBackground and BitmapData Use-After-Free Vulnerabilities

  ⑩ 複合機等に対する適切なアクセス制限等の実施について

  ⑪ Adobe Flash Player における修正版ソフトウェアの公開について

  ⑫ Adobe Releases Security Updates for Flash Player

  ⑬ 国立大学法人を狙ったと思われる標的型攻撃について

  ⑭ BIND における修正版ソフトウェアの公開について

  ⑮ BIND Exploitation of the vulnerabilities may allow a remote attacker to cause a denial-of-service condition.

⑯ 不審メールに対する注意喚起について

⑰ サポート期間が終了したソフトウェアの取扱いについて

⑱ サポート終了のマイクロソフト製品について

⑲ Support for older versions of Internet Explorer have ended since January 13th, 2016

⑳ Open SSL における修正版の公開について

㉑ Open SSL Releases Security Advisory

㉒ 本学ユーザ宛ての不審メールについて

㉓ 重要な情報の取扱いに関する留意点について

㉔ サポートが終了した OS を使用している機器の通信制限について

㉕ サポートが終了した OS を使用している機器の通信制限の実施について

㉖ 不審なメールに関する注意喚起および情報提供の依頼について

㉗ Open SSL における修正版の公開について

㉘ Open SSL Releases Security Advisory

15.2　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、P2P 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。

15.3　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 27 年 4 月～平成 28 年 3 月までにウイルス・ワーム感染系 74 件，セキュリティ被害及び不正利用系 54 件，著作権関連 0 件 ,PC 等盗難その他 12 件のインシデントの対応を行いました。

  ※平成 27 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，22 件（平成 28 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27年度	ウイルス･ワーム感染系	1	1	8	12	2	2	1	1	20	19	1	6	74 件
	セキュリティ被害不正利用系	7	4	9	10	2	1	0	3	4	4	4	6	54 件
	著作権関連	0	0	0	0	0	0	0	0	0	0	0	0	0 件
	PC 盗難、その他	1	1	0	2	1	2	0	0	2	1	2	0	12 件
	計	9	6	17	24	5	5	1	4	26	24	7	12	140 件

	項　目	平成 23 年度	平成 24 年度	平成 25 年度	平成 26 年度	平成 27 年度	計
年度別	ウイルス･ワーム感染系	266	117	101	58	74	616 件
	セキュリティ被害不正利用系	53	139	106	96	54	448 件
	著作権関連	272	53	1	1	0	327 件
	PC 盗難、その他	11	10	3	10	12	46 件
	計	602	319	211	165	65	1437 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 27 年 4 月～平成 28 年 3 月)

- ネットワーク型ワーム(*)の感染の疑い　73件
- 外部ホストに対する攻撃（SQLインジェクション攻撃）　15件
- パスワードを破られたユーザーが踏み台となり外部に対し迷惑メールが送信される　19件
- ＰＣ等盗難　9件