[2016]九州大学情報統括本部年報 : 2016年度

出版情報：九州大学情報統括本部年報. 2016, pp.1-. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第15章　九大CSIRT（情報セキュリティ対策）

九州大学の情報セキュリティの保全のさらなる強化を目的に、平成 28 年 9 月 30 日付けで情報セキュリティ対策室を発展的に改組し、これまで同室が行ってきた情報セキュリティインシデント等が発生した際の応急対応、調査等の事後対策ならびに日々の情報セキュリティ状況の把握と情報セキュリティインシデントの事前防止など安全な九州大学サイバー空間の維持・強化に取り組んだ。

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った。（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た。（情報セキュリティ対策室 HP において電子版を配付）（平成 28 年 4 月配付）
- 「九州大学情報セキュリティ対策基本計画」の策定により，他の事業室やタスクフォースと連携しながら「九州大学情報セキュリティポリシー」を第 5 版へ改定した。また，関連した制度の変更や規程等の制定を行った。
- 伊都地区への移転及び九大 CSIRT の設置に伴い，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た。

(2) 情報セキュリティ対策についての講演

- 平成 28 年度個人情報保護研修会（総務部総務課主催）へ講師派遣
  （平成 29 年 2 月 9 日　講師：嶋吉准教授、　平成 29 年 2 月 10 日　講師：笠原助教）
- 薬学研究院ファカルティ・ディベロプメントへ講師派遣
  （平成 29 年 3 月 8 日　講師：岡村教授）

(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った。
  1. 人事異動に係るＩＤやパスワードの適正な管理について
  2. 複合機に対する適切なアクセス制限等の実施について
  3. 九大図書館を名乗る不審メールについて
  4. Warnings about Suspicious e-Mails
  5. Apache Struts2 の脆弱性を狙った攻撃について
  6. Warnings about a vulnerability in Apache Struts2
  7. 文部科学省が送信したメールが標的型メール攻撃に悪用された事案について
  8. 九州大学を騙る不審メールについて
  9. 九州大学を標的にした不審メールについて

10. メール容量超過を偽った不審メールについて
11. NAS やネットワークカメラ等の管理画面の学外における公開制限について
12. ヤマト運輸を装った添付ファイル付きの不審メールについて
13. 九州大学を騙る不審メールについて
14. DNS サーバ BIND の脆弱性対策について
15. BIND Exploitation of the vulnerabilities may allow a remote attacker to cause a denial-of-service condition.
16. 年末年始のインターネット等の利用について
17. Reminder for computer security in this holiday season
18. PHPMailer における修正版ソフトウェアの公開について
19. 日本マイクロソフトを装った不審メールについて
20. 九州大学を騙りメール容量超過を装った不審メールについて
21. 日本マイクロソフトを装った不審メールについて（その 2）
22. WordPress のセキュリティ対策の実施について
23. Apache Struts 2 の脆弱性への対策の実施について

(4) 九大 CSIRT の訓練を開始

「九州大学情報セキュリティ対策基本計画」の取組として，平成 29 年 3 月 30 日にラックによる研修会を計画し、受講した。

(5)「九州大学情報セキュリティ対策基本計画」に基づき，「事業継続のために重要な ICT 機器」について学内に照会した。また，情報機器の管理状況の把握及び必要な措置について検討した。

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た。
- 国立情報学研究所の「大学間連携に基づく情報セキュリティ体制の基盤構築」の試行運用に協力している。また，「九州大学情報セキュリティ対策基本計画」の取組として，日本シーサート協議会への加盟申請を検討した。
- 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る。
  - ・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。

15.3　情報インシデントの調査，事後対策

(1) 情インシデント状況について，情報政策委員会及び役員・部局長懇談会で報告を行った。

- 平成 28 年 4 月～平成 29 年 3 月までにウイルス・ワーム感染系 32 件，セキュリティ被害及び不正利用系 51 件，著作権関連 0 件,PC 等盗難その他 4 件のインシデントの対応を行った。

  ※平成 28 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］

また，該当部署の情報セキュリティ責任者への口頭注意や，福岡県警との情報共有を行った。

（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った。
- 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 29 年 3 月現在）の報告書を処理した。

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２８年度	ウイルス･ワーム感染系	3	2	3	0	1	1	0	11	5	3	0	3	32 件
	セキュリティ被害不正利用系	3	1	1	2	5	2	4	8	8	4	4	9	51 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	3	0	0	0	0	1	0	0	0	0	0	0	4 件
	計	9	3	4	2	6	4	4	19	13	7	4	12	87 件

	項　目	平成 24 年度	平成 25 年度	平成 26 年度	平成 27 年度	平成 28 年度	計
年度別	ウイルス･ワーム感染系	117	101	58	74	32	382 件
	セキュリティ被害不正利用系	139	106	96	54	51	446 件
	著作権関連	53	1	1	0	0	55 件
	PC 盗難、その他	10	3	10	12	4	39 件
	計	319	211	165	65	87	847 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 28 年 4 月～平成 29 年 3 月)

- ネットワーク型ワームの感染の疑い　32件
- 内部ホストに対する攻撃（SQLインジェクション攻撃等）　25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　16件
- 不審メールの添付ファイルを開封　3件
- webサイトの改竄　1件