[2017]九州大学情報統括本部年報 : 2017年度

出版情報：九州大学情報統括本部年報. 2017, pp.1-, 2018-10-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第15章　九大 CSIRT

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、夏季休暇、年末年始）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。（九大 CSIRT 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。
（九大 CSIRT 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。
（九大 CSIRT HP において電子版を配付）（平成 29 年 4、10 月の新入学生に印刷版を配付）

(2) 情報セキュリティ対策についての講演

・比較社会文化研究院ファカルティ・ディベロプメントに講師派遣
（平成 29 年 4 月 28 日　講師：岡村教授）
・平成 29 年度個人情報保護研修会に講師派遣
（平成 30 年 2 月 1 日　講師：嶋吉准教授、　平成 30 年 2 月 8 日　講師：笠原助教）

(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. Windows Vista のサポートについて
2. ゴールデンウィークのインターネット等の利用について
3. Reminder for computer security in this holiday season
4. 世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
5. 全学ファイアウォールシステムのルール追加について
6. 夏季休暇中のインターネット等の利用について
7. Reminder for computer security in this holiday season
8. Apache Struts2 の脆弱性への対策の実施について
9. Apache Struts2 の脆弱性への対策の実施について（その２）
10. Warnings about a vulnerability in Apache Struts2
11. Apache Tomcat の脆弱性について
12. Warnings about a vulnerability in Apache Tomcat
13. Apache Tomcat の脆弱性について（その２）
14. パスワードの強化について
15. Adobe Flash Player の脆弱性が修正されたソフトウェアの公開について
16. Adobe Releases Security Updates for Flash Player
17. 無線 LAN で使用されるセキュリティプロトコル(WPA2)における脆弱性について
18. 実在する企業名を詐称した不審メールについて
19. 感染が拡大中のランサムウェア「Bad Rabbit」の対策について
20. 外務省職員を騙る不審メールについて

21. Mirai 亜種の感染活動に関する注意喚起について
22. 年末年始のインターネット等の利用について
23. Reminder for computer security in this holiday season
24. 九州大学全学基本メールを装った不審メールにご注意ください
25. SNS サイト等におけるアカウント情報の取扱いについて
26. パスワードの漏洩対策について
27. 海洋政策関係者を狙った標的型攻撃について

・10 月入学の留学生オリエンテーションに合わせて、情報セキュリティガイドを第６版に更新した。また、平成 30 年 4 月の入学者に配布するために第７版に更新した。

(4)標的型攻撃メール訓練の実施

・平成 29 年 10 月に、標的型攻撃を体験し、理解を深めることを目的とし、全教職員を対象に、標的型攻撃メール訓練を実施した。また、訓練実施後には、種明かしメールを送付するとともに、情報セキュリティに関する知識を深めるために、Moodle を利用してｅラーニングを実施した。

(5)情報セキュリティ教育ｅラーニングの実施

・平成 30 年 1 月 22 日から 2 月 28 日において、情報セキュリティ意識及び知識の向上を図ることを目的としてｅラーニングによるセキュリティ教育を実施した。

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きたが、7 月 1 日より開始された正式サービスにも加入した。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、5 月 31 日付で日本シーサート協議会へ加盟した。
・日本シーサート協議会主催のシーサート WG に参加した。(6 月 30 日、8 月 23 日～25 日)また、11 月 9 日に九大 CSIRT が共催である NCA ワークショップ in 福岡に参加し、九大 CSIRT の取り組みについて報告した。
・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。
・情報セキュリティ対策基本計画対応タスクフォースにて検討を進めていた脆弱性診断システムについて、九大 CSIRT に業務移管し、導入及び動作検証を行った。

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役員・部局長懇談会で報告を行った。

・平成 29 年 4 月～平成 29 年 9 月までにウイルス・ワーム感染系 89 件、セキュリティ被害及び不正利用系 107 件、著作権関連 10 件、PC 等盗難その他（主に仮想通貨のマイニング行為）24 件のインシデントの対応を行った。

※平成 29 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、82 件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29年度	ウイルス･ワーム感染系	6	5	5	2	2	0	10	11	7	3	17	21	89 件
	セキュリティ被害不正利用系	8	16	9	3	4	13	2	13	16	15	2	6	107 件
	著作権関連	0	0	0	0	0	0	1	1	1	4	3	0	10 件
	PC 盗難、その他	0	1	0	0	0	0	0	1	1	4	16	1	24 件
	計	14	22	14	5	6	13	13	26	25	26	38	28	230 件

	項　目	平成 25 年度	平成 26 年度	平成 27 年度	平成 28 年度	平成 29 年度	計
年度別	ウイルス･ワーム感染系	101	58	74	32	89	354 件
	セキュリティ被害不正利用系	106	96	54	51	107	414 件
	著作権関連	1	1	0	0	10	12 件
	PC 盗難、その他	3	10	12	4	24	53 件
	計	211	165	140	87	230	833 件

※全学ファイアウォール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、

【主なインシデントの内容】(平成 29 年 4 月～平成 30 年 3 月)

- 不審メールの添付ファイルを開封　13件
- 不審メールのリンク先をクリック　47件
- HeartBleed の脆弱性を狙った通信を検知　4件
- 迷惑メールの送信　18件
- SSO-KIDの不正利用による学内サービスへのアクセス　1件
- 情報システムの設定ミスによる情報漏えいの恐れ　1件
- ソフトウェアの不正利用　11件
- 学内における仮想通貨のマイニング行為（その他の１・２月）　20件