[2022]九州大学情報統括本部年報 : 2022年度

出版情報：九州大学情報統括本部年報. 2022, pp.1-, 2023-11-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 9 章　九大 CSIRT

9.1　情報インシデントの応急対応

- 学内外に対する一元的な窓口として、情報セキュリティインシデントに関する通報に対し、通報者への連絡対応や、該当の支線 LAN 管理者へ調査を依頼する等、ハンドリングを行った。
- 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。
- 国立情報学研究所セキュリティ運用サービス（NII-SOCS）からの情報提供に基づき、インシデント対応を実施した。
- 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。

9.2　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（6 月 29 日、11 月 29 日、2 月 22 日）で報告を行った。
- 2022 年度 4 月～ 3 月までにウイルス・ワーム感染系 46 件、セキュリティ被害及び不正利用系 83 件、著作権関連 3 件、その他 12 件のインシデントの対応を行った。
  ※ 2022 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

- 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、46 件の報告書を処理した。
- インシデントの調査結果を基に、全学ファイアウォール、全学基本メール、情報統括本部が管理するサーバー等について、セキュリティ強化を実施した。
- 以下の研修に参加し、情報セキュリティに関する専門的な知識の向上を図った。
  - CISO・戦略マネジメント層研修（2 名）10 月 18 日　文部科学省主催
  - CISRT 研修（基礎編）（1 名）10 月 20 日、21 日　文部科学省主催
  - CISRT 研修（応用編）（1 名）12 月 7 日～ 9 日　文部科学省主催
  - 文部科学省関係機関における VPN 脆弱性対策・セキュリティ対策にかかるセミナー 12 月 27 日　文部科学省主催（ウェビナー）
    ※九大 CSIRT 室員の他、学内管理者に周知し、参加を求めた。
  - 情報セキュリティ監査担当者研修（基礎編）（1 名）1 月 26 日、27 日　文部科学省主催

9.3　情報インシデントの事前防止

(1) 注意喚起等

- マルウェア添付メール（Emotet）に関する注意喚起や、長期休暇中（ゴールデンウィーク、夏季休暇、年末年始）における不審メールやサイバー攻撃に関する注意喚起を行った。（九大 CSIRT HP に掲載、部局長等へ通知）
- 「情報セキュリティガイド」を教職員、学生、その他利用者へ配布した。
  （九大 CSIRT HP において電子版を配布）（2022 年 4 月の新入学生に印刷版を配布）

(2) 標的型攻撃メール訓練の実施

2022 年 9 月に、標的型攻撃を体験し、理解を深めるとともに、インシデントへの対応の手順の確認を目的として、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、今回の訓練内容や、標的型攻撃メールの理解を深めるための説明資料を用意し、事後学習を行った。

(3) 情報セキュリティ教育 eラーニングの実施

2022 年 11 月 10 日から 1 月 31 日にかけて、情報セキュリティ対策基本計画事業室及び ISMS 運用事業室とともに、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。

(4) 脆弱性診断の実施

学外公開の申請があったサーバーに対して脆弱性診断を行い、脆弱性の有無を事前に確認した。また、インシデント対応時やサーバー管理者からの要望に対して適宜脆弱性診断を行った。

9.4　日本シーサート協議会及び学術系 CSIRT 交流会

日本シーサート協議会全体会に参加し、情報収集を行った。（8 月 19 日）

9.5　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に係る文書を作成し、学内に注意喚起を行った。

① 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（通知）
② マルウェア添付メール（Emotet）の送信事案について（注意喚起）
③ 夏季休暇中のインターネット等の利用について（通知）
④ 年末年始のインターネット等の利用について
⑤ 学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について
⑥ ランサムウエア対策および VPN 装置の脆弱性対策について
⑦ ソフトウェアの適正な使用について
⑧ Windows 8.1 のサポート終了について
⑨ macOS のサポート期限について

【参考資料１】　２０２２年度　セキュリティインシデント管理状況

	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
2022年度	ウイルス･ワーム感染系	1 (0)	3 (0)	20 (0)	5 (0)	1 (0)	2 (0)	3 (3)	3 (1)	1 (0)	2 (0)	2 (0)	3 (0)	46 (4)
	セキュリティ被害不正利用系	23 (20)	29 (27)	6 (6)	7 (4)	2 (1)	5 (5)	4 (3)	4 (1)	0 (0)	1 (0)	2 (0)	0 (0)	83 (67)
	著作権関連	0	0	0	0	0	0	0	2	1	0	0	0	3
	PC 盗難、その他	1	1	1	0	1	0	1	1	1	2	3	0	12
	計	25 (20)	33 (27)	27 (6)	12 (4)	4 (1)	7 (5)	8 (3)	10 (1)	3 (1)	5 (1)	7 (0)	3 (2)	144 (71)

	項　目	2018 年度	2019 年度	2020 年度	2021 年度	2022 年度	計
年度別	ウイルス･ワーム感染系	165　(119)	104　(66)	29　(12)	18　(3)	46　(4)	362 (204)
	セキュリティ被害不正利用系	79　(9)	187　(119)	209　(143)	199　(180)	83　(67)	757 (518)
	著作権関連	23　(11)	13　(7)	0	0	3	39 (18)
	PC 盗難、その他	7	12	18	11	12	60 (0)
	計	274　(139)	316　(192)	256　(155)	228　(183)	144　(71)	1218 (740)

※ 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、
ただし、件数欄の（ ）内は NII-SOCS で検知されたもの。

【2022 年度　主なインシデントの内容】

- フィッシングサイトへのアクセス　66件
- マルウェア感染（うち暗号資産）　46件（11件）
  （うちEmotet）　（20件）
- Webサーバへの不正アクセス　8件
- メール誤送信　7件
- アカウントの不正アクセス、大量メール送信　5件
- 脆弱性を狙った攻撃　4件
- 不正ライセンス　3件
- PC、外付けSSDの紛失　2件
- 書類の誤配　1件
- NASのアクセス制限の設定ミス　1件
- サポート詐欺　1件