[2023]九州大学情報統括本部年報 : 2023年度

出版情報：九州大学情報統括本部年報. 2023, pp.1-, 2024-09-01. 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

インシデント状況について、情報政策委員会（6 月 30 日、11 月 24 日、2 月 27 日）、及び役員・部局長懇談会（10 月 19 日、3 月 19 日）で報告を行った。

- 2023 年度 4 月～ 3 月までにウイルス・ワーム感染系 26 件、セキュリティ被害及び不正利用系 116 件、著作権関連 1 件、その他 31 件、合計 174 件のインシデントの対応を行った。
  ※ 2023 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、55 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。

9.3　情報インシデントの事前防止

（1）注意喚起等

- 不審なメール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）の著作権侵害等の違法行為の未然防止に関する注意喚起を行った。（九大 CSIRT ホームページに掲載、部局長等へ通知）
- 脆弱性の対策情報を収集し、サーバ等の管理者向けに情報提供を行った。（九大 CSIRT HP に掲載）
- 「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 ホームページにおいて電子版を配布）

(2) 標的型攻撃メール訓練の実施

・ 2023 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

・ 2023 年 10 月 16 日から 3 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 25 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等を作成し、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 Apple 製品のアップデートについて（2023 年 6 月）
③ 本学ドメインを装った不審メールにご注意ください（注意喚起）
④ Apple 製品のアップデートおよび緊急セキュリティ対応について（2023 年 7 月）
⑤ Microsoft 製品の脆弱性対策について（2023 年 7 月）
⑥ 夏季休暇中のインターネット等の利用について（通知）
⑦ Windows Server 2012 及び 2012 R2 のサポート終了について（注意喚起）
⑧ Microsoft 製品の脆弱性対策について（2023 年 8 月）
⑨ 指導教員になりすました詐欺メールについて（注意喚起）
⑩ Apple 製品のアップデートについて（2023 年 9 月）
⑪ Microsoft 製品の脆弱性対策について（2023 年 9 月）
⑫ Apple 製品のアップデートについて（2023 年 9 月 第 2 号）
⑬ Apple 製品のアップデートについて（2023 年 10 月）
⑭ Microsoft 製品の脆弱性対策について（2023 年 10 月）
⑮ macOS のサポート期限について
⑯ ドメイン名の適正な管理について
⑰ Microsoft 製品の脆弱性対策について（2023 年 11 月）
⑱ Microsoft 製品の脆弱性対策について（2023 年 12 月）

⑲【更新】Apple 製品のアップデートについて（2023 年 12 月）

⑳ 年末年始のインターネット等の利用について（2023 年 12 月）

㉑ CentOS 7 のサポート終了について（注意喚起）（2023 年 12 月）

㉒ Microsoft 製品の脆弱性対策について（2024 年 1 月）

㉓ 【更新】指導教員になりすました詐欺メールについて（注意喚起）（2024 年 1 月）

㉔ WordPress など CMS への不正アクセスについて（注意喚起）（2024 年 1 月）

㉕ Microsoft 製品の脆弱性対策について（2024 年 2 月）

㉖ Apple 製品のアップデートについて（2024 年 3 月）

㉗ Microsoft 製品の脆弱性対策について（2024 年 3 月）

・ 脆弱性対策情報を収集し、管理者向けに情報提供を行った。

① Fortinet 製 FortiOS および FortiProxy の脆弱性対策について (CVE-2023-27997)

② ISC BIND 9 における複数の脆弱性について（2023 年 6 月）

③ Oracle Java の脆弱性対策について (CVE-2023-22043 等)

④ Cisco IOS XE の Web UI における権限昇格の脆弱性（CVE-2023-20198）について

⑤ Fortinet 製 FortiOS SSL VPN の脆弱性対策について (CVE-2024-21762)

⑥ ISC BIND 9 における複数の脆弱性について（2024 年 2 月）

【参考資料】 2023 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
2023年度	ウイルス･ワーム感染系	4	5	0	2	3	0	4	5	1	1	0	1 (1)	26 (1)
	セキュリティ被害不正利用系	2 (1)	5	5	9	11 (1)	8	3 (3)	7 (3)	2 (1)	26	33	5	116 (9)
	著作権関連	0	0	0	0	0	0	0	1	0	0	0	0	1
	その他	0	1	1	1	1	1	0	0	0	24	2	0	31
	計	6 (1)	11	6	12	15 (1)	9	7 (3)	13 (3)	3 (1)	51	35	6 (1)	174 (10)

	項　目	2019 年度	2020 年度	2021 年度	2022 年度	2023 年度	計
年度別	ウイルス･ワーム感染系	104　(66)	29　(12)	18　(3)	32	26　(1)	209 (82)
	セキュリティ被害不正利用系	187　(119)	209　(143)	199　(180)	72　(63)	116　(9)	783 (514)
	著作権関連	13　(7)	0	0	0	1	14 (7
	その他	12	18	11	4	31	76 (0)
	計	316　(192)	256　(155)	228　(183)	108　(63)	174　(10)	1082 (603)

※ 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。

【2023 年度　主なインシデントの内容】

- マルウェア感染（うち暗号資産）　26件（5件）
- Webサイトへの不正アクセス　60件
- フィッシングサイトへのアクセス　18件
- SSO-KIDへの不正アクセス　18件
- メールアカウントの不正利用　5件
- 意図しないサーバ情報の公開　5件
- 意図しないサーバ機能の設定　2件
- 外部ホストに対する不審な通信　3件
- 不審なソフトのインストール　1件
- 検索エンジン最適化（SEO）の悪用　1件
- 大量のメール送信　1件
- Fortinet製品の脆弱性　1件
- サプライチェーン攻撃の可能性があるサービスの利用　1件
- 購入していないソフトのインストール　1件
- 指導教員になりすました詐欺メール　26件
- サポート詐欺　2件
- ビジネスメール詐欺　1件
- 設定ミスによる情報漏洩　2件