[2025]九州大学情報統括本部年報 : 2025年度

出版情報：九州大学情報統括本部年報. 2025, pp.1-, 2026-09-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 10 章　九大 CSIRT

10.1　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。

10.2　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 17 日、11 月 19 日、2 月 13 日）及び役員・部局長懇談会（12 月 18 日、3 月 13 日）で報告を行った。

- 2025年度に81件のインシデントの対応を行った。内訳は、ウイルス・ワーム感染系34件、セキュリティ被害及び不正利用系35件、その他12件であった。
  ※ 2025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、31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。

10.3　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 HP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 HPにおいて電子版を配布）

（2）標的型攻撃メール訓練の実施

・ 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10月に実施した。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

・ 情報セキュリティ対策基本計画室及び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7月に実施した。

（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。

10.4 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合に参加し、情報収集を行った。（8月29日）

10.5 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 Microsoft 製品の脆弱性対策について（4月～3月）
② macOSのサポート期限及びApple製品のアップデートについて（4月～3月）
③ 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）（4月）
④ パスワードの適切な設定及び管理の徹底について（5月）
⑤ 夏季休暇中のインターネット等の利用について（通知）（7月）
⑥ Windows 10のサポート終了について（注意喚起）［再掲］（9月）
⑦ 多要素認証の活用及びパスワードの適切な管理の徹底について（10月）
⑧ 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月）
⑨ 学内システムアカウントに対する強固なパスワードへの設定変更等について（12月）
⑩ 年末年始のインターネット等の利用について（12月）
⑪ 九州大学総長名等を騙る不審メールについて（注意喚起）（1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 Oracle Java の脆弱性対策について(4月、7月、10月、1月)
② ISC BIND 9における脆弱性について（5月、10月、1月）
③ React Server Componentsの脆弱性について（CVE-2025-55182）（12月）

【参考資料 1】2025 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
2025年度	ウイルス･ワーム感染系	0	4	0	1	1	5	7 (1)	7	4	1	1	3	34 (1)
	セキュリティ被害不正利用系	2 (1)	5 (1)	3	0	3	2	4	2	5	1	5	3	35 (2)
	著作権関連	0	0	0	0	0	0	0	0	0	0	0	0	0
	その他	0	4	1	0	0	0	3	0	2	0	1	1	12
	計	2 (1)	13 (1)	4	1	4	7	14 (1)	9	11	2	7	7	81 (3)

	項　目	2021 年度	2022 年度	2023 年度	2024 年度	2025 年度	計
年度別	ウイルス･ワーム感染系	18　(3)	32　0	14	29　(10)	34　(1)	127 (14)
	セキュリティ被害不正利用系	199　(180)	72　(63)	40　(2)	70　(5)	35　(2)	416 (252)
	著作権関連	0	0	0	2	0	2
	その他	11	4	5	5	12	37
	計	228　(183)	108　(63)	59　(2)	106　(15)	81　(3)	582 (266)

※ 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。

【2025 年度　主なインシデントの内容】

- マルウェア感染（暗号資産）　34件(うち15件)
- SSO-KIDの不正利用　8件
- フィッシングサイトへのアクセス（入力）　7件(うち5件)
- メールの大量送信　3件
- EZproxyへの不正アクセス　2件
- アカウント情報の漏洩　2件
- SSHへの不正アクセス　1件
- ウェブサイトの脆弱性をついた攻撃（XSS）　1件
- ウェブメールRoundcubeの脆弱性　1件
- React Server Componentsの脆弱性　1件
- ｸﾛｽｻｲﾄｽｸﾘﾌﾟﾃｨﾝｸﾞの脆弱性　1件
- .gitフォルダの公開"　4件
- 監視カメラ映像の送信　2件
- ホスティングサーバへのDDos攻撃　1件
- 媒体の盗難、紛失（iPad、PC）　7件
- メールの誤送信　2件
- 作業ミスによる大量の返信メール送信　1件
- サポート詐欺　1件
- 総長名を騙る不審メール　1件