[2021]九州大学情報統括本部年報 : 2021年度

出版情報：九州大学情報統括本部年報. 2021, pp.1-, 2022-10-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第14章　九大 CSIRT

14.1 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。

14.2 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25日、11月5日、2月18日）及び役員・部局長懇談会（4月20日、3月17日）で報告を行った。

・2021年度 4月～3月までにウイルス・ワーム感染系18件、セキュリティ被害及び不正利用系199件、著作権関連0件、その他11件のインシデントの対応を行った。

※2021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、39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。

- 戦略マネジメント層研修（1 名） 9月10日受講　文部科学省主催
- CISO マネジメント研修（1 名） 10月 6日受講　文部科学省主催
- NII-SOCS インシデントマネジメント研修（2 名）12月7日受講 国立情報学研究所主催

14.3 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）の著作権侵害等の違法行為の未然防止や、在宅勤務用に持ち帰った機器の私的利用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）

・「情報セキュリティ安全対策（個人マニュアル）」を九大教職員へ配布した。
（九大 CSIRT HP において電子版を配布）

・「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）（2021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

・2021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1月24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。
（131件）

14.4 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27日）

・学術系CSIRT 交流会に参加し、情報収集を行った。（8月27日）

14.5 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 現行バージョンから３世代以前の macOS の通信制限について（通知）
② Network communication restrictions for macOS(end-of-life)
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 Reminder for computer security in this holiday season
⑤ Windows の印刷スプーラーの脆弱性への対応について（注意喚起）
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 Reminder for computer security in this holiday season
⑧ フィッシング被害によるアカウント窃取の多発について（注意喚起）
⑨ サイバー詐欺や脅迫メールに関する注意喚起
⑩ ソフトウェア（アドビ社製ソフトウェア）の適正な使用について（注意喚起）
⑪ 年末年始のインターネット等の利用について（注意喚起）
⑫ Reminder for computer and networking security in the holiday season
⑬ マルウェア Emotet の急速な感染拡大について（注意喚起）
⑭ マルウェア添付メール（Emotet）の送信事案について（注意喚起）※一斉送信

・2022 年 4 月の入学者向けに、情報セキュリティガイド第 11 版の更新作業を実施した。

参考資料１

２０２１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
２０２１年度	ウイルス･ワーム感染系	2 (0)	1 (1)	0 (0)	2 (1)	1 (0)	2 (0)	2 (0)	1 (0)	2 (0)	2 (0)	1 (0)	2 (1)	18 (3)
	セキュリティ被害不正利用系	9 (9)	6 (3)	5 (4)	13 (13)	9 (7)	6 (4)	19 (18)	40 (35)	32 (31)	21 (21)	24 (20)	15 (15)	199 (180)
	著作権関連	0	0	0	0	0	0	0	0	0	0	0	0	0
	PC 盗難、その他	0	0	0	2	0	1	1	0	2	0	3	2	11
	計	11 (9)	7 (4)	5 (4)	17 (14)	10 (7)	9 (4)	22 (18)	41 (35)	36 (31)	23 (21)	28 (20)	19 (16)	228 (183)

	項　目	2017 年度	2018 年度	2019 年度	2020 年度	2021 年度	計
年度別	ウイルス･ワーム感染系	89 (47)	165 (119)	104 (66)	29 (12)	18 (3)	405
	セキュリティ被害不正利用系	107 (4)	79 (9)	187 (119)	209 (143)	199 (180)	781
	著作権関連	10 (1)	23 (11)	13 (7)	0	0	46
	PC 盗難、その他	24 (2)	7	12	18	11	72
	計	230 (54)	274 (139)	316 (192)	256 (155)	228 (183)	1304

※ 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（2017 年 10 月参加）で検知されたもの。

【2021 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　171件
- 不審な通信の検知（うち仮想通貨）　15件（9件）
- サーバへの不正アクセス　11件
- メール誤送信　9件
- メールアカウントの不正利用、大量メール送信　7件
- サーバの脆弱性　5件
- 偽警告による遠隔操作　3件
- アカウントの漏洩　2件
- マルウェア感染（Emotet）　2件
- マルウェア感染（ランサムウェア）　1件
- 対策不備による情報漏洩　1件
- PC紛失　1件