[2020]九州大学情報統括本部年報 : 2020年度

出版情報：九州大学情報統括本部年報. 2020, pp.1-, 2021-12-01. 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、情報政策委員会及び役員・部局長懇談会で報告を行った。

・2020 年 4 月～2021 年 3 月までにウイルス・ワーム感染系 29 件、セキュリティ被害及び不正利用系 209 件、著作権関連 0 件、PC 等盗難その他 18 件のインシデントの対応を行った。

※2020 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、40 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。

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）（2020 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

・2020 年 6 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

・2020 年 10 月 1 日から 12 月 31 日にかけて、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。なお、今年度は在宅勤務におけるセキュリティに関する事項を追加した。

(4) 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。

14.4 ファイアウォールの運用・管理

・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。

14.5 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 21 日）

・学術系 CSIRT 交流会に参加し、情報収集を行った。

14.6 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（オンライン授業や在宅勤務関連を含む）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. オンライン授業での Zoom 利用におけるセキュリティの問題について（注意喚起）
2. Web 会議システム Zoom および Webex への対応あるいは準備について
3. 在宅勤務におけるセキュリティについて（注意喚起）
4. Ensuring security when teleworking
5. 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）
6. Reminder for computer security in this holiday season
7. 夏季休暇中のインターネット等の利用について（通知）
8. Reminder for computer security in this holiday season
9. 文部科学省及び関係機関を騙るメールについて（注意喚起）
10. NetLogon の特権昇格の脆弱性について（注意喚起）
11. Peatix 利用におけるパスワード変更について（注意喚起）
12. 年末年始のインターネット等の利用について（通知）

13. Reminder for computer security in this holiday season
14. 九州大学を装った不審メールにご注意ください（注意喚起）
15. Emotet による不審メール送信事案について（注意喚起）
16. sudo の脆弱性について（注意喚起）

・2021 年 4 月の入学者に配布するため、情報セキュリティガイド第 10 版の更新作業を実施した。

参考資料1

2020度　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
2020年度	ウイルス・ワーム感染系	5 (2)	6 (4)	4 (1)	3 (1)	1 (0)	2 (0)	1 (1)	0 (0)	2 (1)	1 (0)	2 (1)	2 (1)	29 (12)
	セキュリティ被害不正利用系	26 (24)	26 (20)	32 (20)	27 (25)	8 (5)	7 (2)	21 (11)	17 (14)	10 (4)	19 (7)	7 (6)	9 (5)	209 (143)
	著作権関連	0	0	0	0	0	0	0	0	0	0	0	0	0
	PC 盗難、その他			3	3	2		1	4	2			3	18
	計	31 (26)	32 (24)	39 (21)	33 (26)	11 (5)	9 (2)	23 (12)	21 (14)	14 (5)	20 (7)	9 (7)	14 (6)	256 (155)

	項　目	2016 年度	2017年度	2018 年度	2019 年度	2020 年度	計
年度	ウイルス・ワーム感染系	32	89　(47)	165　(119)	104　(66)	29　(12)	419
	セキュリティ被害不正利用系	51	107　(4)	79　(9)	187　(119)	209　(143)	633
	著作権関連	0	10　(1)	23　(11)	13　(7)	0	46
	PC 盗難、その他	4	24　(2)	7	12	18	65
	計	87	230 (54)	274 (139)	317 (192)	256　(155)	1163

※ 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。

【2020 年度　主なインシデントの内容】

- 不審な通信の検知（うち仮想通貨）　26件（4件）
- マルウェアのダウンロード通信の検知　3件
- webサーバ等への不審なアクセスの検知　9件
- XSS等サーバの脆弱性　15件
- パスワード漏洩による大量メール送信　45件
- 不審メールのリンク先、フィッシングサイトへのアクセス　139件
- 学外への攻撃の検知　1件
- メール誤送信、サーバ公開設定ミス　14件
- PC盗難,PC紛失　4件

※　2017年度からNII-SOCS　へ参加し、本学の全学ファイアウォールでは検知できなかったものの検知が可能になったため、件数が増

（被害件数）