[2019]九州大学情報統括本部年報 : 2019年度

出版情報：九州大学情報統括本部年報. 2019, pp.1-, 2020-12-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 15 章　九大 CSIRT

15.1 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。

・外部から連絡を受けて、文部科学省、セキュリティベンダとインシデント対応を行った。

・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。

15.2 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。

・2019 年 4 月～2020 年 3 月までにウイルス・ワーム感染系 104 件、セキュリティ被害及び不正利用系 187 件、著作権関連 13 件、PC 等盗難その他 12 件のインシデントの対応を行った。
※2019 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、38 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。

15.3 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、年末年始）の著作権侵害等の違法行為について、未然に防ぐための注意喚起を行った。（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、その他利用者へ配付した。

（九大 CSIRT HP において電子版を配付）（2019 年 4、10 月の新入学生に印刷版を配付）

(2) 標的型攻撃メール訓練の実施

・2019 年 5 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

・2019 年 9 月 10 日から 11 月 30 日において、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。

(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。

15.4 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。

・最近のネットワークの高速化やそれに伴いデータ量が増加している環境においても、本学全体に、より安全で安心なネットワーク環境の提供を実現するため、ファイアウォールのバージョンアップを行った。（3 月）

15.5 日本シーサート協議会、学術系 CSIRT 情報交流会へのイベントへの参加、情報収集

・日本シーサート協議会主催のシーサート WG に参加し、情報収集を行った（8 月 23 日）。また、11 月 1 日には NCA ワークショップ in 北九州に参加し、九州地区の企業や他大学と情報交換を行った。

・学術系 CSIRT 交流会に参加し、私学を含めた他大学の取組等の情報収集・意見交換を行った。（6 月 11 日、10 月 7 日、1 月 29 日）

15.6 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に関する注意喚起等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
2. Reminder for computer security in this holiday season
3. 九州大学関係者を装った不審メールにご注意ください
4. リモートデスクトップサービスのリモートでコードが実行される脆弱性について
5. Windows 7、Windows Server 2008、Windows Server 2008 R2 の計画的な更新について
6. 夏季休暇中のインターネット等の利用について
7. Reminder for computer security in this holiday season
8. 現行バージョンから３世代以前の Mac OS の通信制限について
9. リモートデスクトップサービスの公開ポリシーの変更について
10. Emotet による最近の不審メール送信事案について
11. 年末年始のインターネット等の利用について

12. Reminder for computer security in this holiday season
13. Windows 7、Windows Server 2008、Windows Server 2008 R2 の通信制限について
14. Network communication restrictions for Windows 7, Windows Server 2008, and Windows Server 2008 R2
15. ソフトウェアの適正な使用について
16. Use software under copyright laws and license agreements
17. 九州大学を装った不審メールにご注意ください
18. 九州大学情報統括本部を装った不審サイト（Google フォーム）にご注意ください

・10 月入学の留学生オリエンテーション開催時に情報セキュリティガイドの第８版を配布した。また、2020 年 4 月の入学者に配布するため、第９版に更新作業を実施した。