

情報セキュリティガイド

九州大学情報統括本部九大 CSIRT

第 13 版

令和 5 年 1 月 1 日発行

九州大学では教育、研究、業務のために高速なインターネットや便利な ICT 環境を、全学的に提供するとともにオンライン授業や在宅勤務の支援をしていますが、ルールを守らないことによるトラブルやネットワーク犯罪に発展する案件が発生しています。特に、セキュリティ対策不足によるウイルス感染、不正アクセスによる被害・二次的な加害や、不注意から発生する情報漏洩の後始末にかかる時間や費用は無視できなくなっています。

九州大学のみなさんが安心していつでもどこでも教育、研究、業務に ICT インフラを活用するためには、情報セキュリティ対策の実施や情報セキュリティポリシーに基づく情報の目的外利用、外部からの不正アクセス、情報漏洩などインシデント発生の防止が重要です。また、職員・学生は情報セキュリティに対する意識を高め、インシデント発生の防止に努めるとともに、万一のインシデント発生時には緊急対応や二次的被害の拡大防止に努めることが必要です。インシデント発生時の学内通報ルートや調査・対策・報告の措置については、情報統括本部が定めています。

自分が被害者から二次的な加害者となりインシデントを起こすと、多くの貴重な時間がその処理に費やされ、精神的な苦痛を受けることとなります。これらのコンピューターネットワークの不適切な利用によるインシデントを発生させないよう、大学はもちろん、自宅でも注意してください。

安心して教育、研究、業務活動を持続的に行うためには

セキュリティ対策で重要なことは、遵守すべきことや、注意すべきポイントをよく理解し知っておくことです。本書に書かれている規則やセキュリティ対策のポイントをよく読んで、安心して教育、研究、業務活動を持続的に行うようにしましょう。

○情報倫理規程とセキュリティポリシー

九州大学職員、学生及びその他利用者が安心してネットワークや計算機、情報等の情報資産を利用できるよう、当該情報資産の提供者及び利用者の心得、責務、遵守すべき情報セキュリティに関する基本方針を定めています。情報資産の利用に際して判断に迷われた時は、情報倫理規程及びセキュリティポリシーを参照し、定められた運用ルールを守りましょう。また、自宅で、大学の端末等を利用する際には、必ず大学・部局のルールに従ってください。特に、各種情報の機密性に応じて、大学で定めているルールに従った利用をこころがけてください。

<https://www.sec.kyushu-u.ac.jp>

○法令の遵守

商用ソフトウェアの不正利用、ライセンス違反である非純正の Windows の使用などは絶対にしないでください。また、学内で仮想通貨のマイニングによって報酬を得ることは情報機器や電気使用の不正利用にあたるため禁止されています。インターネット上での著作権遵守を心がけて下さい。インターネットには、著作権がある音楽や映画等の情報コンテンツが違法に流通しています。それらの違法コンテンツをインターネット利用により入手し利用することも違法であり、行ってはいけません。入学前にインストールしていた方は削除してください。さらに、学内から著作権侵害等の違法行為を招くおそれのある Web サイトへのアクセスの制限を行なっています。ただし、教育・研究上必要な場合は、申請によってその制限を解除することができます。外部からのインターネットを通じた様々なサイバー攻撃を未然に防ぐために学外から学内への全ての通信は基本的に全て制限しています。ただし、教育・研究上必要な場合は、申請によってその制限を解除することができます。

○情報セキュリティ対策に関する学習及び自己点検（教職員のみ）

九州大学全体のセキュリティ対策の向上を図るために九州大学に所属する教職員を対象に情報セキュリティに関する e-ラーニングならびに自己点検を毎年実施しています。

・情報セキュリティ対策に関する学習

情報セキュリティに対する知識・意識の向上を目的にした、全教職員を対象に、e-ラーニングによる学習を全教職員は受講しなく

てはなりません。

・情報セキュリティ対策の自己点検

情報セキュリティポリシー等で利用者として取り組むべき基本的な情報セキュリティ対策について、Web のアンケート形式で全教職員に自己点検を行います。

○情報セキュリティ対策

情報セキュリティ対策で注意すべきことはたくさんありますが、最近のセキュリティインシデントを顧みて特に注意すべき脅威を取りあげています。

・不審なメールへの注意

九州大学の教職員・学生をターゲットにした悪意のあるメールが多数届いており、文章の内容も一見悪意のあるメールとは気がつかないような内容が多くみられます。受け取ったメールに対して、常に不審なメールではないかというセキュリティに対する意識を持っておくことが大切です。不審メールを見分ける際には、様々な観点からメールの内容を注意深く観察し、総合的な判断が必要です。また、メールで Web 会議等の情報を受け取って参加する場合は、自分が参加しようとしている URL が正しいかどうか、十分に確認してください。

不審メールを受け取った方は、情報統括本部に報告してください。また、受信した不審メールを自組織への注意喚起の目的でもそのまま転送することは、被害の拡大に繋がる恐れがあり非常に危険です。実際に学内で転送された不審メールにマルウェアが添付されていた事例が報告されています。不審メールが届いた際には、必ず、まず、情報統括本部にご連絡ください。

・パスワード管理

パスワードは、九州大学のパスワードポリシーに従って設定してください。SSO-KID のパスワードやその他システムのパスワードが、九大のパスワードポリシーに従っていない場合は、今すぐパスワードを変更し直してください。また、パスワードの使い回しは、パスワードリスト型攻撃の対象となる可能性があるため、パスワードの使い回しをしないように、適切に管理するようにしてください。また、パスワードだけでなく、ID (SSO-KID など) も他人に不必要に知らせたりしないようにしましょう。

・ウイルス対策

コンピューターウイルスからパソコンを守るために、セキュリティ対策ソフトウェア (Windows Defender など) をインストールするようにしましょう。現在大学で使用しているパソコンにインストールされているセキュリティ対策ソフトウェアが有効化されているか確認してください。また、セキュリティ対策ソフトウェアのウイルス定義ファイルを常に最新のものに更新してください。

・情報漏洩対策

キャンパス以外の所で大学の端末を利用するときに最も多く発生するインシデントは端末などの紛失・盗難です。教職員の方で、業務用 PC、USB メモリに個人情報や機密情報を保存して持ち出す必要がある場合は、九州大学個人情報管理規程及び部局のルールにしたがって、適切に情報資産を管理するようにしてください。また、業務などに関わらず、研究等で扱う機密情報を学会等でキャンパス外に持ち出す時は注意して下さい。

○その他、注意すべきこと

・他人に自分の ID を貸さない。

学外の友人等に学内ネットワークや、自身の全学共通 ID (SSO-KID、学生 ID) で認証したパソコンやスマートフォンなどを利用させないように注意してください。パソコンを借りた友人が情報インシデントを発生させた場合、貸した側にも責任が問われます。

・SNS や掲示板への不適切な書き込みをしない。

Twitter、Facebook や LINE などの SNS や、Web 掲示板への不適切あるいは過度な書き込みにご留意ください。SNS の匿名性に乗じて普段はしないような発言を行った結果、その反動で大学に問い合わせをされたり、自身のプライバシーが不特定多数に公開されたりする事例もあります。なお、インターネット上での匿名の書き込みも調査すれば、その発言者を特定できます。

・新しい脅威を把握する。

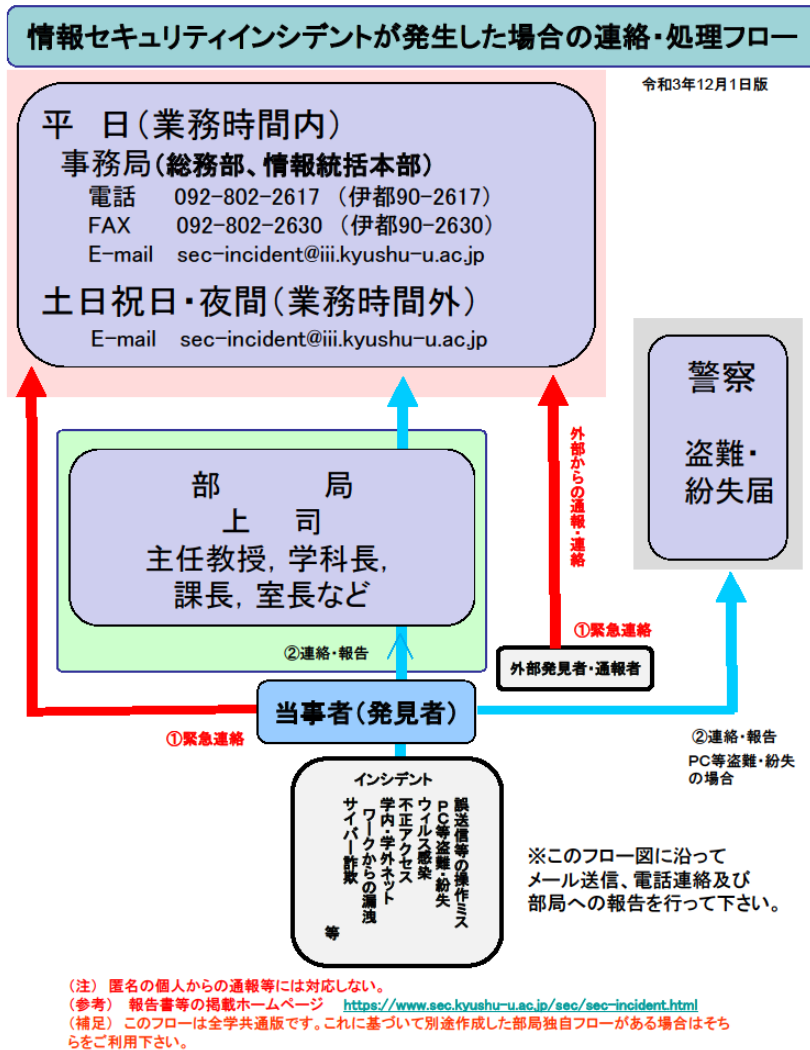
サポート詐欺、ショートメール (SMS) を使った振り込み詐欺など、毎年新しい攻撃手法による攻撃が確認されています。IPA が公開している最新の脅威情報を定期的にチェックしましょう。脅威情報の把握で被害を未然に防ぐことが可能になります。

IPA: <https://www.ipa.go.jp/security/vuln/>

○インシデント発生時の対応フロー

情報セキュリティ上のインシデント（被害及び加害）は早期に発見し、大きな被害に拡大せぬよう対応する必要があります。万一発生した場合は、「情報セキュリティインシデントが発生した場合の連絡・処理フロー図」に沿った迅速な通報（第一報）を情報統括本部九大 CSIRT にお願ひします。その際には、所定の「情報セキュリティインシデント報告書」様式の記載事項に沿った内容をお知らせ下さい。

<https://www.sec.kyushu-u.ac.jp/sec/sec-incident.html>



★参考 URL

・情報統括本部
<https://iii.kyushu-u.ac.jp>



・九大 CSIRT
<https://www.sec.kyushu-u.ac.jp>



◆問合せ先

・情報統括本部九大 CSIRT
 情報セキュリティに関連する問い合わせ

E-mail : sec-incident@iii.kyushu-u.ac.jp
 TEL : 092-802-2617 / 2685 / 2686 / 2687 / 2688

不審メールに関する問い合わせ

E-mail : sec-info@iii.kyushu-u.ac.jp

・情報統括本部「よろず相談窓口」

E-mail : help@iii.kyushu-u.ac.jp