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反する情報の目的外利用、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になります。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。

○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心がけてください。

★もっと詳しく知るには

・九州大学情報倫理規程

https://www1.g-reiki.net/kyushu-u/reiki_honbun/u437RG00000140.html

・九州大学情報セキュリティポリシー

https://www.sec.kyushu-u.ac.jp/sec/policy/policy.html

・九州大学情報セキュリティ対策規程

https://www1.g-reiki.net/kyushu-u/reiki_honbun/u437RG00000131.html

○著作権侵害や情報インシデントへの対策、法令の遵守

コンピューターネットワークの利用に際し、法令の遵守に心がけましょう。著作権侵害やライセンス違反である非純正のWindowsの使用、商用ソフトウェアの不正利用などの違法行為は絶対にしないでください。また、学内で暗号資産のマイニングで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。

九州大学では、著作権侵害等の違法行為や、個人情報等の情報漏洩を招くことに繋がる全てのソフトウェアの利用を規制しています。これらのソフトは大学ではもちろんのこと、自宅でも使用しないようにしましょう。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。

〇情報セキュリティ対策に関する学習及び自己点検

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-ラーニング並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
  情報セキュリティ対策への知識・意識の向上を目的にした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は自己点検を行います。

〇情報セキュリティ対策

情報セキュリティ対策の参考のために、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の例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、九大CSIRT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、九大CSIRT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。（※設定方法に関する詳細は「九州大学SSOポータル」を参照してください。）SSO-KIDのパスワードやその他システムのパスワードが、九州大学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ので、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標準で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最新のものに更新してください。
- ・情報漏洩対策
  職場以外の場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。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。

〇その他、注意するべきこと

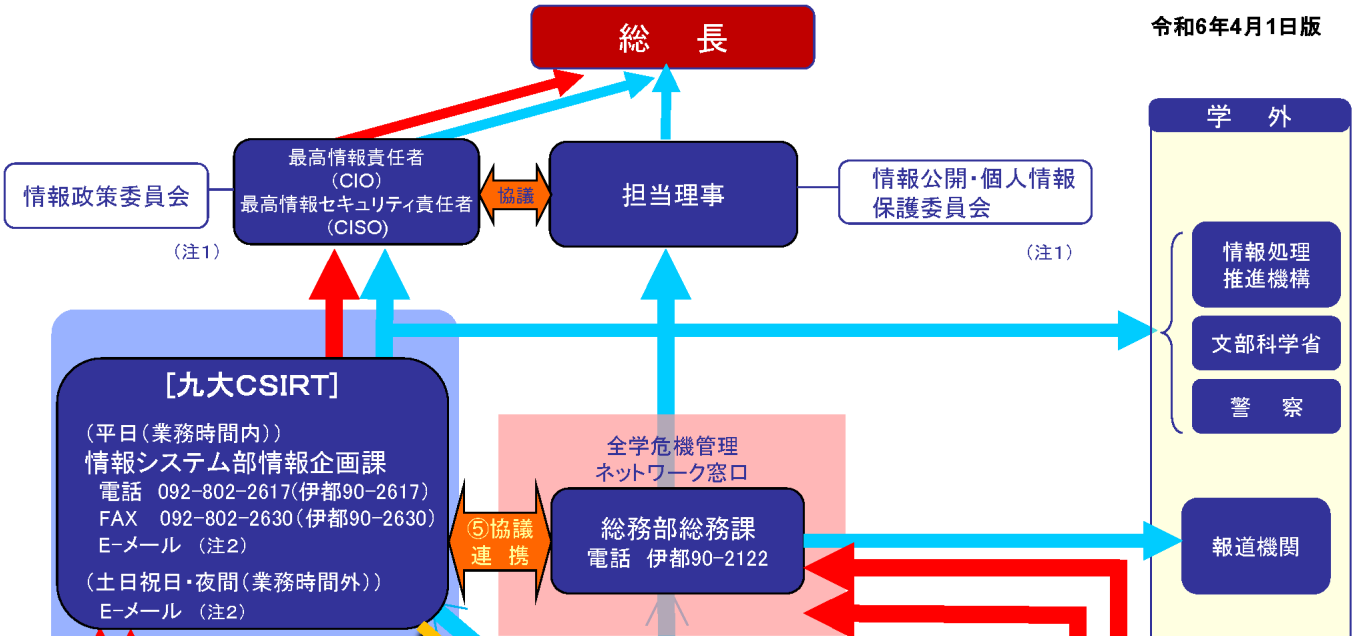
- ＊他人に自分のIDを貸さない
  学外の友人等に学内ネットワークや、自身の全学共通ID（SSO-KID、学生ID）で認証したパソコンやスマートフォンなどを利用させないように注意してください。パソコンを借りた友人が情報インシデントを発生させた場合、貸した側にも責任が問われます。
- ＊SNSや掲示板への不適切な書き込みをしない
  X（旧 Twitter）、FacebookやLINEなどのSNSや、Web掲示板への不適切あるいは過度な書き込みにご留意ください。SNSの匿名性に乗じて普段はしないような発言を行った結果、その反動で大学に問い合わせをされたり、自身のプライバシーが不特定多数に公開さ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。令和７年度に九州大学構成員におけるソーシャルメディア利用ガイドラインが裁定されております。
- ＊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（情報処理推進機構）：https://www.ipa.go.jp/security/security-alert/

〇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、下図「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」に沿った迅速な通報（第一報）を九大CSIRTにお願いします。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ください。

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（改定版）

令和6年4月1日版



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

令和3年12月1日版

平　日（業務時間内）

事務局（総務部、情報統括本部）

電話　092-802-2617（伊都90-2617）
FAX　092-802-2630（伊都90-2630）
E-mail　sec-incident@iii.kyushu-u.ac.jp

土日祝日・夜間（業務時間外）

E-mail　sec-incident@iii.kyushu-u.ac.jp

部　局
上　司
主任教授，学科長，
課長，室長など

②連絡・報告

外部からの通報・連絡

①緊急連絡

外部発見者・通報者

警察
盗難・
紛失届

当事者（発見者）

①緊急連絡

②連絡・報告
PC等盗難・紛失
の場合

インシデント
誤送信等の操作ミス
PC等盗難・紛失
ウィルス感染
不正アクセス
学内・学外ネット
ワークからの漏洩
サイバー詐欺
等

※このフロー図に沿って
メール送信、電話連絡及び
部局への報告を行って下さい。

（注）匿名の個人からの通報等には対応しない。
（参考）報告書等の掲載ホームページ　https://www.sec.kyushu-u.ac.jp/sec/sec-incident.html
（補足）このフローは全学共通版です。これに基づいて別途作成した部局独自フローがある場合はそちらをご利用下さい。

★ もっと詳しく知るには

・情報統括本部Webサイト https://iii.kyushu-u.ac.jp ・九大CSIRT Webサイト https://www.sec.kyushu-u.ac.jp/

◆ お問い合わせ先

・九大CSIRT セキュリティ事故一般に関して E-mail：sec-incident★iii.kyushu-u.ac.jp

メールアドレスは「★」を「@」に置き換えてください 不審メールに関して E-mail：sec-info★iii.kyushu-u.ac.jp

情報システム部情報企画課総務・広報担当 Tel：092-802-2617 内線：90-2617

情報システム部情報基盤課情報セキュリティ担当 Tel：092-802-2685 内線：90-2685