福岡県立大学情報セキュリティマニュアル

平成 31 年 2 月 18 日

福岡県立大学情報セキュリティ委員会

（福岡県立大学情報処理センター）

目次

1. 福岡県立大学の情報セキュリティへの取り組み

福岡県立大学では、情報セキュリティ委員会を設け、学内の情報セキュリティ対策を行っています。

情報セキュリティ委員会構成員	
情報セキュリティ責任者	副理事長
情報セキュリティ管理者	経営管理部長 情報処理センター長
情報セキュリティ技術管理者	理事長が指名する者複数人
情報セキュリティ委員	本学教職員の担当者
その他	理事長が必要と認める者

【情報セキュリティ委員会業務】

①. 情報セキュリティ規則の検討に関すること
②. 理事長に対する情報セキュリティの提言に関すること
③. その他、情報セキュリティの実施推進に関すること

2. 事故や異常に気付いた時の対応

― 事故や異常に気付いたら ―

- **事故の発生や異常の兆候に気づいたら、早急に連絡を**
- **ウイルス感染などでは、二次被害を防ぐため当該情報端末をネットワークから遮断すること**

■ **事故の発生や異常の兆候に気づいたら、早急に連絡を**

情報セキュリティ事故に対する被害を最小限にとどめるためには、速やかな報告が欠かせません。事故が起こった場合、なんらかの異常に気付いた場合は、経営管理部長および情報処理センター長に早急にご連絡ください。事故が自分のミスによるものであっても正直に報告してください。隠蔽したり放置したりすることで被害が拡大する場合があります。

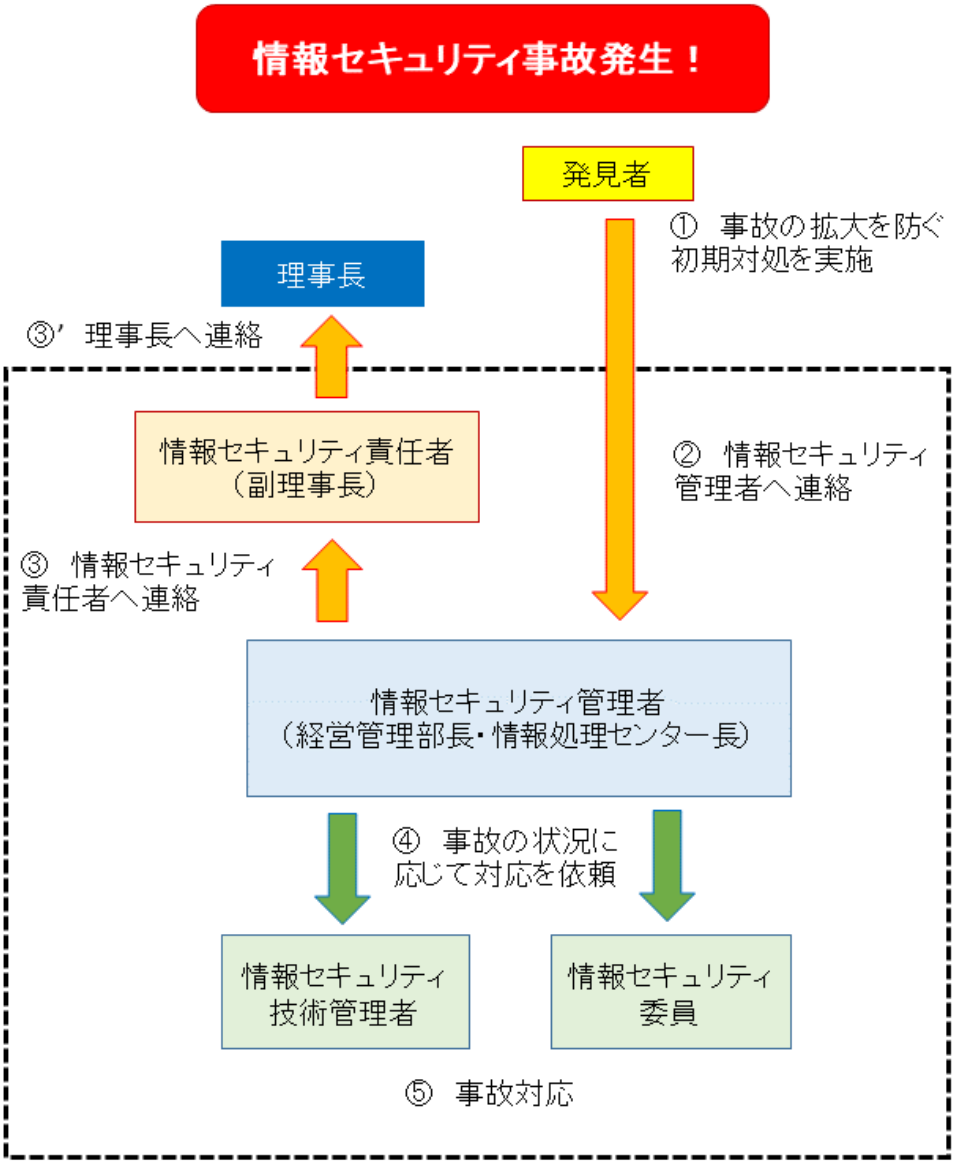
【想定される事故等】

- ウイルスの感染
- 学内情報システムの動作異常
- PC や USB、外付け HDD などの情報記録媒体の紛失、盗難
- 機密データの紛失、盗難
- 個人情報の紛失、盗難
- その他、情報セキュリティ上、重要と思われること

■ **ウイルス感染などでは、二次被害を防ぐため当該情報端末をネットワークから遮断すること**

また、ウイルス感染や情報漏洩などネットワークトラブルに関するものの場合、二次被害を防ぐために当該情報端末の LAN ケーブルを抜く、無線 LAN 接続を解除するなどネットワークを遮断し、隔離を行ってください。

■ 事故が起こったときのワークフロー



3. アカウント管理

― パスワード管理について ―

- 見破られやすいパスワードを使わないように
- パスワードは定期的に変更する

― 各種 Web サービス等のアカウント管理について ―

- いろいろな Web サービスで同一のアカウント名やパスワードを使いまわししない

3.1. パスワード管理

■ **見破られやすいパスワードを使わないように**

入学時や就業開始時にもらったアカウントパスワードはそのまま使わず、必ず変更してください。

文字数の短いパスワード、誕生日、電話番号、辞書に載っている単語など他者から推測されやすいものをパスワードとして使わないようにしてください。パスワードは長いものほど破られにくいですが、自分で覚えられないものもパスワードとして適しません。

また、パスワードを紙に書き留めておく場合も、他人にそのメモ紙を見られないようにしましょう。付箋紙に書いて PC やモニターに貼っておくなどの行為はやめましょう。自分のパスワードを他人に教えてもいけません。

■ **パスワードは定期的に変更する**

同じパスワードを使い続けると、もしアカウントハックなどでパスワードが漏洩した場合に、潜在的なネットワーク攻撃を受け続けることになります。パスワードは定期的に変更してください。

3.2. 各種 Web サービス等のアカウント管理

■ **いろいろな Web サービスで同一のアカウント名やパスワードを使いまわししない**

現在、様々な Web サービスがあり、各 Web サービスに対してアカウントを作成して利用していることと思います。アカウント名やパスワードを忘れないように、すべてのサービスで同じアカウント名、パスワードを使いまわししている人も多いと思われます。しかし、Web サービスの中には、大手のセキュリティ対策のしっかりしたところだけでなく、規模の小さいセキュリティ対策が甘いところも存在し、セキュリティ対策の甘い企業からアカウント情報を盗まれた場合、あなたの利用しているすべてのサイトでアカウント名とパスワードが盗まれたのと同じことになり、アカウント乗っ取りなどのトラブルに巻き込まれる可能性があります。

Web サービスによってアカウント名を変更する、別のパスワードを設定するなどしておいた方がより安全です。すべての Web サービスでパスワードを使い分けるのは大変かもしれません。その場合でも、いつくかのパスワードを用意する、各パスワードをローテーションするなどして定期的に変更する、といった対策を行ってください。

4. ウイルス対策ソフトのインストール

― ウイルス対策ソフトのインストール ―

- **パソコン等の情報端末にはウイルス対策ソフトをインストールする**
- **ウイルス対策ソフトの定義ファイルの更新を忘れない**

■ パソコン等の情報端末にはウイルス対策ソフトをインストールする

コンピュータウイルスの発見・駆除に最も有効的な対抗手段はウイルス対策ソフトの導入です。外部から PC に持ち込まれたファイルやアプリケーションについて、コンピュータウイルスが潜伏していないかチェックをしたり、すでに PC がコンピュータウイルスに感染していた場合にそれを発見・駆除したりすることができます。ウイルスに感染していた PC を放置しておくと、その PC から別の PC へウイルス感染が広まります。学内に持ち込む PC については、必ずウイルス対策ソフトをインストールしておいてください。

■ ウイルス対策ソフトの定義ファイルの更新を忘れない

また、日々新たなコンピュータウイルスが生み出されているため、ウイルスの定義ファイルは定期的に更新し、最新のものにしておいてください。自動更新にしておくことをお勧めします。

― 学内ウイルス対策ソフトの提供について（専任教員対象） ―

本学教員については、学内で使用するパソコンについて、ウイルス対策ソフト（ノートンインターネットセキュリティ）を提供しています。

1 台目については各教員にメールでインストールの案内を送っていますので、そちらのメールの URL からライセンスサーバーにアクセスしてインストールしてください。2 台以上のパソコンにウイルス対策ソフトをインストールしたい場合には、PC ヘルプデスクに申請をお願いします。申請した台数分のライセンスを発行いたします。

5. アプリケーションのインストール

― パソコン等にインストールするアプリケーションについて ―

- **正規のライセンスで利用する**
- **ダウンロードサイトに注意する**
- **インストール時に抱き合わせアプリケーションに注意**

■ 正規のライセンスで利用する

パソコンなどにソフトをインストールする際には正規のライセンスを取得して利用するようにしてください。海賊版の有償ソフトなど非合法な手段で取得したものを利用することは、知的財産権の侵害にあたるだけでなく、ウイルスなどの温床となっている場合があります。

■ ダウンロードサイトに注意する

Adobe Reader など無料で使用できるフリーソフトをダウンロード・インストールして使うこともできます。Microsoft Store，App Store，Google Play ストアなどのストアアプリを利用するのが比較的安全ですが、パソコンの場合 Web 検索をかけて Web サイトからダウンロードすることもできます。ただし、この際はできるだけ公式のサイトからダウンロードしてください。いろんなフリーソフトをまとめているダウンロードサイトなどもありますが、悪質なサイトからダウンロードするとウイルスに感染する場合があります。ダウンロードするサイトの URL を確認することも重要です。インストールするソフトやダウンロード元のサイトが安全かどうかを、Web 検索などで評判を調べるとよいでしょう。

インストーラーを用いてインストールする場合に、さまざまな確認処理を要求されることがありますが、よく読まずに［OK］や［Yes］などのボタンを押さないでください。インストールの際に別の“お勧めソフト”をインストールしていいかと聞かれている場合があり、確認せずに［OK］を押し続けると、自分の意図していないソフトが抱き合わせでインストールされてしまうことがあります。最悪それがウイルスやマルウェアである場合も考えられます。

6. 不審なメールへの対応

― 不審なメールが届いた場合 ―

- 怪しいメールはそのまま削除する
- アカウントや個人情報を確認しろというメールには要注意！
- 確認もせず添付ファイルをいきなり開かない
- 送り元のメールアドレスや、メール内リンクの URL についても確認する

■ **怪しいメールはそのまま削除する**

世の中には、アダルト情報、マルチ商法、架空請求などのスパムメールを大量かつ無差別に送り付けるスパム業者がいます。近年は、相手の個人情報（らしきもの）が書かれていたり、アカウント情報が流出したなど相手の不安を煽ったりといった巧妙なものも増えています。スパムメールからウイルスに感染したり個人情報流出したりする場合もありますので、知らない相手からのメールや身に覚えのないメールなど、不審なメールが届いた場合には、そのまま削除してください。

その際ですが、メールを読んだだけではウイルス等に感染することはありません。添付ファイルを開いたり、メールに載っている URL のリンクを開いたりすることでウイルス感染や情報流出にいたる場合がありますので、無闇に触らずそのまま削除してください。

また、架空請求などが送られてきても、相手がこちらを把握しているわけではありません。確認メールを出したり確認の電話を入れたりすると、逆に相手にこちらの個人情報を教えることになりトラブルの元となりますので、無視してください。

■ **アカウントや個人情報を確認しろというメールには要注意！**

最近の手口としてアカウント情報が流出した、不正なクレジット使用が見つかったなど、こちらの不安を煽るスパムメールが出回っています。メールに「こちらのサイトで確認をお願いします」のようなリンクを貼り、悪徳業者の偽サイト（銀行やクレジットカード会社そっくりに作っているので一見して分からないように作っています）に誘導、アカウントやパスワードを入力させ、データを盗み出すという手口です。銀行やクレジットカード会社がメールでこのような個人情報確認を促すということはありませんので相手にしないでください。不安ならば、電話等でこちらから銀行やクレジットカード会社に連絡・確認を行ってください。もちろん、メールに直接返信しないでください。

■ **確認もせず添付ファイルをいきなり開かない**

上記の通り、スパムメールに添付されているファイルにウイルスやマルウェアが仕込まれている可能性があります。実行ファイル（.exe）には特に注意し、いきなり「開く」などで実行しないでください。また、画像ファイルや Word ファイルなどに偽造したものや画像ファイルなどに埋め込まれているマルウェアもありますので充分注意してください。

ただし、こちらはダウンロードしただけではウイルス感染しません。あくまで「実行する」「閲覧する」などファイルを開いた時点で感染しますので、そのまま削除してしまえば大丈夫です。

■ **送り元のメールアドレスや、メール内リンクの URL についても確認する**

不審なメールが来たときは、メールアドレスを確認してください。アカウント名（@より前の部分）がでたらめなアルファベットや数字の羅列であったり、ドメイン（@より後ろの部分）がフリーメールアドレスであったりする場合は要注意です。ほかにも、アドレスを偽造している場合もありますので、差出人のアドレスをきちんと確認してください。同様に、リンク先の URL についてもドメインを確認して偽サイトではないかどうかをチェックしてください。たとえば、本学からの注意喚起メールでアカウント確認を要求されたのに、そのリンク先のドメインが“fukuoka-pu.ac.jp”でないというのは普通考えられません。

7. 情報機器の管理

― ノート PC、タブレット等の管理 ―

- 学外に持ち出す情報機器に機密データを入れておかない
- 紛失、盗難、破損等に十分な注意を払う
- ログインパスワードを設定し、他人が操作できないようにする
- 定期的にデータのバックアップを取っておく

― USB メモリの使用について ―

- 機密データを外部に持ち出さない
- 紛失、盗難、破損等に十分な注意を払う
- USB メモリは消耗品で経年劣化することを知っておく
- ウイルス感染に十分注意する
- 暗号化できるものを使用する

7.1. ノート PC、タブレットの管理

■ **学外に持ち出す情報機器に機密データを入れておかない**

出張等で学外にノート PC やタブレットなどの情報端末を持ち出す場合、その中に学生の個人情報や成績情報など機密となるデータを入れたままにしないよう十分に気を付けてください。学外へ持ち出しするべきでない機密データについては、別途外付けハードディスクなどに保存し、PC 内に保存しない方が安全性は高まります。また、研究発表のために研究データを出張に持っていく必要がある場合にも、データにパスワードをかけ、外部の人間が簡単にアクセスでき

ないようにしてください。また、学外でパソコン作業をする場合、他人から画面を覗かれる可能性もありますので、特に機密ファイルを開くときには十分注意をしてください。

■ **紛失、盗難、破損等に十分な注意を払う**

学外にノート PC やタブレットなどの情報端末を持ち出した場合、電車やタクシーに置き忘れる、置き引き等で盗難にあうなど、紛失する可能性があります。情報端末には前述したように機密データや個人情報が残っている場合があり、情報端末の紛失から学内機密情報の漏洩につながるかもしれません。紛失には十分注意してください。また情報端末が他者の手に渡った際のことを考え、機密ファイルにはパスワードをかける、パソコン等にはログインパスワードの設定をするなど安全対策をしておいてください。

また同様に、歩行中に落として破損したりしないよう、精密機械であることを認識して気を付けて使ってください。

■ **ログインパスワードを設定し、他人が操作できないようにする**

前述のように、情報端末が紛失した場合、他人が自分の情報端末に簡単にアクセスできると、情報漏洩のリスクが高まります。また、いたずら等で自分のアカウントを使って悪いことをされてしまうかもしれません。パソコンなどの情報端末にはログインパスワードを設定し、他人が勝手に使用できないようにしておきましょう。またパスワード管理については 3.1 で述べた通り、定期的に変更する習慣をつけましょう。

■ **定期的にデータのバックアップを取っておく**

情報端末紛失、ウイルス感染、ハードウェア破損など、重要データが使えなくなる場合は十分考えられます。データ破損や紛失に対しては、定期的なデータバクアップが重要となります。それなりに予算をかければ RAID などデータ破損に強いハードディスク構成もありますので、絶対にデータ破損してはいけない重要データを取り扱う場合は、そちらの検討もいいかと思います。

7.2. USB メモリの使用

■ **機密データを外部に持ち出さない**

USB メモリの取り扱いに関しても、情報端末と同様です。機密データを不用意に学外に持ち出さないでください。

■ **紛失、盗難、破損等に十分な注意を払う**

こちらも情報端末の取り扱いと同様です。特に USB メモリは小さく、紛失しやすいため特に注意してください。また、パソコンなどに挿したまま抜き忘れてしまうこともよくありますので、抜き忘れにも注意してください。

■ **USB メモリは消耗品で経年劣化することを知っておく**

USB メモリや SD カードのようなフラッシュメモリには寿命があります。通常使用でも数万回の書き込みで壊れると言われており、利用期間についても 5～10 年程度でデータ欠損が起こります。また頻繁に抜き挿しするとコネクタ部分が劣化し認識しなくなることもあります。USB メモリはあくまでも消耗品として扱った方がよいかと思います。

■ **ウイルス感染に十分注意する**

USB メモリ内のファイルがウイルスに感染していると、USB メモリを介して他の情報端末にウイルスが感染拡大する可能性がありますので注意して下さい。

■ **暗号化できるものを使用する**

USB メモリの中には、USB メモリそのものにパスワードをかけ暗号化できるものもあります。安全のため暗号化できるタイプの USB メモリを使用してください。特に、機密データを格納する場合は必ず暗号化できる USB メモリを使ってください。

8. ネットワーク利用

― 学内でのルーターの設置 ―

- 研究室などでルーターなどネットワーク機器を設置する場合は、PC ヘルプデスクに連絡すること

― 無線 LAN のセキュリティ ―

- 出所不明の野良無線 LAN を使用しない
- 無線 LAN ルーター設置の際は暗号化等のセキュリティ設定を行う
- 公衆無線 LAN の使用にも注意

― オンラインストレージの利用 ―

- セキュリティに十分注意して利用する
- 利用規約をきちんと確認してから利用すること
- 機密データの保管にはオンラインストレージを利用しない

― SNS の利用 ―

- 写真のアップなどでは個人情報、機密データの流出に十分注意
- 他者への誹謗中傷など行わない
- ネットの拡散は急速で広範囲に渡る可能性がある
- 一度拡散した情報をインターネットから完全に消すことは難しい

※「福岡県立大学ソーシャルメディア利用ガイドライン」に従い適切な運用を

8.1. 学内でのルーターの設置

■ **研究室などでルーターなどネットワーク機器を設置する場合は、PC ヘルプデスクに連絡すること**

教員が研究室等でルーターなどのネットワーク機器を設置する場合、設定を間違うと学内全体がネットワークトラブルに見舞われ、多大な影響を及ぼす可能性があります。また、その際にトラブルの原因を突き止めることも困難となり、トラブル解消までの時間も長くなります。2.で示した通り、トラブルの際は早急に連絡をお願いします。また、そのようなトラブルをできるだけ回避するために、ネットワーク機器やネットワークプリンタの設置については、あらかじめ PC ヘルプデスクへご連絡、ご相談を宜しくお願いいたします。

「福岡県立大学ソーシャルメディア利用ガイドライン」に基づき適切に運用してください。

8.2. 無線 LAN のセキュリティ

■ **出所不明の野良無線 LAN を使用しない**

無線 LAN は局所的範囲内で特定の利用者に対して利用を許すのが基本です。ただし、後述のセキュリティ設定を正しく行わないと、誰でも自由に利用できる状態になります。パソコンやスマートフォン、タブレットなどで利用可能な無線 LAN を検索すると時折このようなセキュリティ設定のできていない無線 LAN（SSID）を拾う場合があります。そのような場合でも、出自不明の無線 LAN を利用しないようにしてください。きちんとセキュリティ設定ができていないため、通信内容が盗聴されてしまうリスクが高いです。また悪意のある者が野良無線 LAN にアクセスした情報端末に対して、逆に不正アクセスを仕掛けたりすることも考えられます。無線 LAN 利用の際は出自の分かっているものを利用してください。

学内であれば、FPUNETWORK（学生用）、FPUNETWORK-STAFF（教職員用）の二つの SSID を用意していますので、そちらをお使いください。

■ **無線 LAN ルーター設置の際は暗号化等のセキュリティ設定を行う**

無線 LAN ルーターを購入して利用する場合には、説明書等をしっかり読んで暗号化などセキュリティの設定を適切に行ってください。セキュリティ設定を正しく行わないと、前述のように知らない他人が勝手に自分の無線 LAN ネットワークにアクセスしたり、そこから不正アクセスに利用されたりする可能性が

あります。また容易に通信盗聴されてしまう危険性もあります。

セキュリティ設定として行うべきことは、主に SSID（ネットワークの名前）の設定、暗号化方式の設定（今なら WPA2-AES または WPA2-PSK(AES)にすればよい)、暗号化キー（パスワード）の設定です。これを行うことにより、SSID を検索して無線 LAN に初回アクセスするときに暗号化キーを入力しなければアクセスできないようになります。

そのほか、学内の無線 LAN では、最初に Web 上で学内アカウント（メールアドレスの@より前の部分）を入力させる Web 認証システムを使用しています。

■ **公衆無線 LAN の使用にも注意**

現在、駅、空港、コンビニ、カフェなどで公衆無線 LAN が設置され、誰でも自由に利用できるものもあります。またキャリア 3 社（DoCoMo、au、Softbank）なども各所でユーザが自由に無線 LAN を使えるようにしています。非常に便利ですが、利用の際には注意も必要です。

誰でも使えるように無線 LAN を利用できるようにするために、無線 LAN のセキュリティ設定を落としている場合があり、その場合には前述のように通信盗聴の危険性があります。アクセスする無線 LAN についてセキュリティ設定がされているか確認してください。（SSID 検索したときに暗号化されているものは錠前マークがつきます。）Web ページを見る程度なら問題ないかと思いますが、個人情報のような機密性の高いデータを通信しない、メール送受信など外部漏洩されては困るものの通信は控えるなど、利用する Web サービスについて配慮することが大事です。

8.3. オンラインストレージの利用

■ **セキュリティに十分注意して利用する**

GoogleDrive、Dropbox、OneDrive などネットワーク上にデータ保存場所を貸してもらい、ネットワーク上にファイルを保存することのできるオンラインストレージサービスも広まっています。情報端末間のデータの共有、グループワークなどでのデータ共有のために利用でき、非常に便利ですが、データを外部に出すことになりますので、利用には注意が必要です。

■ **利用規約をきちんと確認してから利用すること**

サービス利用について利用規約をきちんと確認してください。万が一オンラインストレージ上のデータが消えた場合の免責事項、保存したデータの取り扱

い（著作権等）に関してもきちんと確認し、問題のない範囲で利用してください。

■ **機密データの保管にはオンラインストレージを利用しない**

通信盗聴の危険性なども考え、なんでもかんでもオンラインストレージに置くのではなく、機密性の高いデータに関してはオンラインストレージに保存しないといった配慮をしてください。

8.4. SNS の利用

■ **写真のアップなどでは個人情報、機密データの流出に十分注意**

SNS などに写真をアップロードする際には問題のあるものが写り込んでいないか注意してください。たとえば海外の空港は撮影禁止である場合もあり、最悪逮捕されてしまう可能性もあります。また個人情報を不用意に公開することは大きなトラブルになる可能性があります。自分の個人情報あるいは他人の個人情報の管理には十分注意してください。またスマートフォンやデジタルカメラで撮影した写真にはジオタグという撮影した場所（緯度と経度）の情報が含まれている場合があります。その場合、たとえば自宅で撮影した写真から自宅が特定されてしまう可能性があります。スマートフォンやデジタルカメラのジオタグの設定を確認しておいてください。

また、試験問題の写真、実習先リストの写真などを SNS にアップロードして公開することも大きなトラブルを招くことになりかねませんので、お止めください。

■ **他者への誹謗中傷など行わない**

SNS などの文字でのやりとりは、文次第で誤解を招きやすいものです。また、匿名性が高く個人の特定がされにくいため、必要以上に他人に厳しい書き方をしてしまいヒートアップしてしまう場合があります。最悪、そこから火がついて炎上状態になってしまう可能性もあります。SNS 等で意見を言う場合には、一度冷静になって自分の文章を読みなおし、他者への誹謗中傷になっていないか、誤解を生むような表現ではないかを確認してください。また、意見の食い違い以上の他者への個人攻撃や人格否定はヘイトスピーチになる可能性もあります。お気を付けください。

■ **ネットの拡散は急速で広範囲に渡る可能性がある**

インターネットや SNS での拡散スピードは非常に速く、また広範囲に広がる可能性があります。特に最近はスマートフォンでいつでも気楽に情報発信が行

えるため、Twitter のリツイートなどであっという間に拡散してしまうこともしばしばあります。たとえば友達同士の内輪でのウケを狙うためにしたいたずらが拡散し、一晩で大炎上してしまうといったことも起こっています。公開範囲を設定する、不用意に問題となるような投稿を行わないなど注意をしてください。

■ **一度拡散した情報をインターネットから完全に消すことは難しい**

インターネットでは情報が簡単にコピーできてしまうため、一度広まった情報に対しては大量のコピーが出回り、そのコピーを見た人がさらにそのコピーを広めるといった具合に情報が拡散していきます。その場合、元々のオリジナルのデータを削除しても、コピーはインターネット上に残ってしまいます。拡散した大量のコピーをすべて削除することは至難の業です。高校時代に行った飲酒の写真が、就職面接時に人事担当に発見されてしまうといったこともあり得ます。注意してください。

※ SNS の利用に関しては、添付の「福岡県立大学ソーシャルメディア利用ガイドライン」（P20）を熟読の上、適切に運用してください。

9. 個人情報の取り扱い

― 個人情報の取り扱い ―

- **不用意に個人情報を他人に教えない**
- **他者の個人情報の扱いにも注意**
- **スマートフォンのアプリでの「アクセス許可」にも注意**

■ **不用意に個人情報を他人に教えない**

個人情報の取り扱いには十分注意をしてください。不用意に自分の個人情報を他人に教えたりインターネットで書き込んだりすると、いたずら電話やストーカー被害などのトラブルに巻き込まれる可能性があります。自分の個人情報を SNS 等でどこまで公開するか十分考慮してください。

■ **他者の個人情報の扱いにも注意**

自分の個人情報だけでなく、他者の個人情報にも配慮してください。友人と行った旅行の写真を SNS などにアップロードする際、一緒に写っている友人にも許可をもらってからにしてください。また、たまたま映り込んだ歩行者や車のナンバーなどについても、勝手にアップロードすると問題になる場合があります。写真加工でぼかしを入れる等の配慮をしてください。

もちろん、名簿など個人情報が含まれるファイルの取り扱いについても、パスワードをかける、紛失盗難等に気を付けるなど十分以上の注意が必要です。

■ **スマートフォンのアプリでの「アクセス許可」にも注意**

スマートフォンのアプリを実行するとき GPS 情報や写真情報、電話帳情報などにアクセスしていいかと聞かれる場合があります。地図アプリで GPS にアクセスする必要がある、写真加工アプリで写真情報にアクセスする必要がある、などアプリのサービスを受けるために必要な場合もありますが、悪意のあるアプリの場合、不必要と思われる情報のアクセス許可を求めている可能性もあります。たとえばゲームをするのに電話帳へのアクセスを求められる場合、電話帳の個人情報を集めることが目的の怪しいアプリである可能性もあります。

10. 機密データの取り扱い

― 機密データの取り扱い ―

- 機密データを学外に持ち出さない
- 機密データを取り扱うファイルにはパスワードを設定する
- 機密データの受け渡しにメールなどを使わない

■ **機密データを学外に持ち出さない**

前述したように機密データの入った情報端末や外部ストレージを学外に持ち出さないようにしてください。

■ **機密データを取り扱うファイルにはパスワードを設定する**

こちらも既に説明した通り、機密データを取り扱うファイルについてはパスワードを設定し、他者が簡単に開けないようにしてください。

■ **機密データの受け渡しにメールなどを使わない**

機密データに対してメールやオンラインストレージを使っての受け渡しはセキュリティ上問題があります。学内であればできるだけ直接手渡しで行う方が安全です。どうしてもメール等で機密データをやり取りする場合には、メールに平文で機密情報を書かず添付ファイル等にして送る、添付ファイルにはパスワードをかけるといった配慮をしてください。

（参考）

○福岡県立大学ソーシャルメディア利用ガイドライン

平成３１年２月１８日
情報セキュリティ委員会

１　目　的

本ガイドラインは、本学の学生・教職員が公私を問わず、ソーシャルメディアを利用するにあたりトラブル等の被害者や加害者にならず、ソーシャルメディアを適切に利用してもらうための指針を定めたものです。

２　定　義

(1) ソーシャルメディアとは利用者が情報を発信してコミュニケーションを可能とする Twitter、Facebook、Line、Instagram などに代表される電子的なメディアをいいます。

(2) 本学の学生とは、学部生、院生、科目等履修生、研究生、留学生、認定教育課程の研修生などの本学に在籍しながら学ぶ者を、本学の教職員とは、職位や職種などに関係なく、本学の教育研究や大学運営の業務を行っている者すべてをいいます。

３　利用の基本原則

(1) 法律等を守りましょう

他者の基本的人権を尊重すること。プライバシー権、肖像権、著作権、商標権などを侵害しないよう注意しましょう。また、海外旅行や留学中は外国の法令を遵守するとともに、その国の慣習等も尊重しましょう。

(2) 守秘義務を守りましょう

学生は授業、実習、アルバイトをはじめ、学生生活などで得た個人情報、企業情報、実習施設情報などを発信してはいけません。教職員は職務上知り得た守秘義務のある情報を発信してはいけません。

(3) 正確な情報を適切な表現で発信しましょう

自分が掲載する内容には責任をもち、正しい情報を発信するようにしてください。虚偽はもちろんのこと、不確かな情報を発信してはいけません。また、誤解を招かないような適切な表現をするよう努めましょう。他人の悪口やわいせつな内容など、他者を不快にさせる表現は止めましょう。

(4) 慎重に行動し、誠実に対応しましょう

ソーシャルメディアへの発信にあたっては、インターネット上で不特定

多数の者に公開された情報は、直ちに誰もが閲覧できるようになるとともに、完全に削除することが難しくなります。このことを念頭において、自らの安全と大切な関係者の安全、他者の権利等を侵害しないか等十分検討し、慎重に行動しましょう。

また、万が一自ら発信した情報により他者を傷つけたり、誤解を与えた場合は、誠実に対応しましょう。

(5) 安全性の確保

自らの個人情報を発信する場合でも、その必要性や自らの身の安全を良く考えてから行いましょう。不用意な発信は思わぬ形で悪用され、事件・事故につながる恐れがあります。

4　禁止事項

次に掲げる情報を発信してはいけません。

① 反社会的行為や不法行為をあおる情報
② 発信することについて許可を得ていない他者の個人情報
③ 人種、思想、信条、宗教等に関する差別的内容の情報
④ 誹謗中傷、事実の歪曲など、他者の正当な権利や名誉などを損なう恐れのある情報
⑤ その他法令違反や公序良俗に反する内容を含む情報

※　非違行為等により、本学または第三者に損害を与えた場合、懲戒処分等の対象となったり、損害賠償を請求される場合があります。

5　学内の相談窓口

ソーシャルメディアを利用してトラブルが起きた（起きそうな）時、トラブルにつながりそうな情報を見つけたときの相談窓口は次のとおりです。

○情報セキュリティ管理者（経営管理部長）