情報システム　ユーザガイドライン

第1版(教職員用)

令和3年7月28日制定

独立行政法人　国立高等専門学校機構
岐阜工業高等専門学校

1. インターネットと情報セキュリティ対策

（1）インターネットに流れる情報は、盗聴の恐れがある

インターネットに流れる情報は、その通信路上で容易に盗み見ることが可能です。十分注意していないと、個人情報が流出したり、パスワードや銀行口座の暗証番号が盗まれたりします。

個人情報を Web サイトとやりとりするときは、その Web サイトが https://で暗号化されたやりとりとなっているか、SSL 証明書の有効期限が切れていないかをよく確認しましょう。

（2）接続記録は把握されている

一方、インターネットの最大の特徴は匿名性（誰が利用しているのかわからない、という性質）であると言われていますが、実はサーバ上のアクセス記録を基に、接続したコンピュータを特定することが可能です。

以上のことから、インターネット上の行動は公衆の面前と同じという自覚を持ち、責任を持つようにしましょう。

（3）インターネットからの攻撃から、自ら身を守ること

インターネットに接続するということは、インターネットを介した攻撃を受ける可能性があるということにもなります。

次の自己防衛策を必ず実施しましょう。

【自己防衛に必要なこと】

- マルウェア対策ソフトウェア（アンチマルウェアソフトウェア）を必ず導入すること。
- マルウェア対策ソフトウェアのマルウェア定義ファイルを常に最新にして、定期的にマルウェアチェックをすること。
- オペレーティングシステム（OS）、およびブラウザ、電子メール、Microsoft Office などのソフトウェアの更新（アップデート）を、定期的に実施すること。
- 開発元がはっきりしない怪しいソフトウェアをインストールしないこと。
- P2P ファイル共有ソフトウェアは使わないこと。
- 懸賞サイト、無料ゲーム、SNS などのアカウントに授業や学校業務のメールアドレスを登録しないこと。
- 授業や学校業務以外のサイトに授業や学校業務のメールアドレスや SNS アカウントなどの個人情報を入力しないこと。

2. ユーザIDとパスワードの管理

（1）ユーザ ID とパスワードが第三者に知られると…

ユーザ ID とパスワードが、自分以外の人に知られると、以下のような不利益が起こることが想定されます。

- 自分宛ての電子メールや自分に関するデータが盗み読みされる。
- 自分の知らないうちに、データが追加されたり、改ざん、破壊されたりする。
- 自分になりすました第三者によって不正なアクセスが行われ、「不正アクセス者」として、身に覚えがないのに犯人にされてしまう。

ユーザ ID とパスワードの管理はしっかり行いましょう。

【ID・パスワード管理に関係する一般的注意事項】

・新規登録時に渡された初期パスワードは、速やかに変更すること。

・定期的にパスワードを変更すること。

・他人のユーザIDやパスワードを使用しないこと。

・他人に自分のユーザIDやパスワードを教えないこと。

・メモ、紙、付せんにパスワードを書かないこと。（他人の目に触れるところにパスワードが記入された付せんを貼る行為は、「パスワードを無効にすること」と同じです。）

・パソコンを利用する際にパスワード入力を要求するように設定すること。

・自分のパソコンを他人に使わせる場合でも、他人にパスワードを教えずに自分自身でログインを行うこと。

・高専統一パスワードポリシーにしたがってパスワードを設定すること。

・ネットワーク上で入力を要求されるパスワードは、学校など他で使用しているパスワードと同じパスワードを使わないこと。

(2) 高専統一パスワードポリシーを守る

2019 年 3 月に高専統一パスワードポリシーが変更されたため、教職員および学生は次のポリシーに従ったパスワードを使用してください。

【高専統一パスワードポリシー】

パスワードの最小文字数　:10 文字

パスワードの必須文字種　:以下の文字種を各 1 文字以上必ず含める

英字(大文字／A～Z)、英字(小文字／a～z)、数字(0～9)、記号(!@#$&?_+− 等)

パスワードの有効期限　:600 日以内 (継続利用できる期間)

パスワードの履歴　:3 世代以上 (パスワード再利用禁止の世代数)

(3) 校外のサービスを利用する際に校内の認証を利用する技術

校外のサービスを利用する際に、校内で用いている ID とパスワードで認証できる機能として「学認」があります。学認とは、全国の大学等と国立情報学研究所(NII)が連携して構築・運用する「学術認証フェデレーション」の愛称で、Web アプリケーションへのシングル・サイン・オン(1 つの ID・パスワードであらゆるシステムが利用可能であること)技術を、組織を越えて活用する分散型認証基盤です。認証の連携により、校内でのシングル・サイン・オンを実現可能とし、学習システム Blackboard や CBT システム、および NII が提供するデータベースジャーナル「CiNii」をはじめとした校外のサービスにおいても、1 つのパスワードを利用し、かつ ID・パスワードの再入力を行わずに利用できる環境を実現することができます。

（1）PC ワーキングエリアで端末を使う時には

プログラミングや CAD 演習などで使用される、PC が設置されている部屋・場所を PC ワーキングエリアと呼びます。PC ワーキングエリアでは、次のことに留意しましょう。

【PC ワーキングエリア内での一般的**禁止**事項】

・PC ワーキングエリア内での飲食。ただし、管理者が許可をした場合を除く。

・大声で騒ぐこと、ゴミを放置すること。

・未使用プリンター用紙の持ち帰り、授業・実験等に関係しない私的なデータの印刷。

【PC ワーキングエリア内に設置されたパソコンに関する**禁止**事項】

・機器のケーブル・コネクタを引き抜いたり、機器を持ち出したりすること。

・無断で機器の接続を変更すること。

・USB メモリを乱雑に引き抜く、キーボードを乱打する、機器の開口部に異物を詰め込むなど、機器の破損につながる行為をすること。

・PC 本体にアプリケーションをインストールすること。ただし、管理者が許可した場合を除く。

・使用後に PC の電源を切らずに放置すること。

・PC をロックせずに長時間離席すること。（トイレなどで離席する場合もロック）

・長時間にわたって PC を占有使用すること。

(2) 学校管理下の端末を使う時には

また、研究室など、PC ワーキングエリア以外で学校管理下の端末を使用する場合は、次のことに留意してください。

【学校が保有するパソコン及び学校のネットワークに接続されたパソコンに関する**禁止**事項】

・授業・実験や学校の業務に必要とされない作業を行うこと。
・私的な電子メールの送受信や、私的に Web サイトを利用すること。
・授業・実験や学校の業務に必要とされないソフトウェアをインストールすること。
・学校が定めたマルウェア対策ソフトウェアを導入せずにパソコンを作動させること。(Linux などの・UNIX 系 OS、MacOS におけるマルウェア対策ソフトウェアのインストールについては、学校の指示に従うこと)
・使用しようとするソフトウェアの利用許諾条件に反する行為を行うこと。(たとえば、購入ライセンス数を超えた数の利用等は厳禁)
・マルウェア等の有害ソフトウェアが含まれていないことを確認せずにソフトウェアをインストールすること、及び開発元が定かでないソフトウェアをインストールすること。
・ネットワーク帯域を占有してしまうような大量データの送受信など、ネットワークや情報システムに過度な負荷をかけて円滑な利用を妨げること。
・著作権侵害を目的として、P2P ファイル共有ソフトウェアをインストールすること、及びそれを利用すること。

【使用する端末についての注意事項】

・利用しているコンピュータの OS のセキュリティアップデート(Windows Update など)を定期的に実行し、セキュリティホールを狙った攻撃(マルウェア感染や侵入)を防止すること。
・マルウェア対策ソフトウェアを導入すること。
・マルウェア対策ソフトウェアのマルウェア定義ファイルを常に最新の状態に保つこと。
・マルウェア対策ソフトウェアによって、定期的に PC 内のファイルや USB メモリのファイルをチェックすること。
・開発元の定かでないソフトウェアをインストール、使用しないこと。新たなソフトウェアが必要になった場合は、必ずマルウェア対策ソフトウェア等により安全性を確認した上でインストールすること。
・実験室や研究室等で管理するパソコンは、必ずログイン認証すること。
・P2P ファイル共有ソフトウェアをインストールしないこと、使用しないこと。
・インターネットカフェ等、不特定多数の人間が使用する PC は使用しないこと。

(3) 管理区域外へパソコンを持ち出す場合には許可が必要です

学校のパソコンを管理区域外に持ち出す場合は、管理者の許可が必要です。持ち出す前に学校で定められた所定の手続きをとってください。

また、次のことを留意してください。

【管理区域内のパソコン等を管理区域外に持ち出して利用する際の注意事項】

・ ⑵で示された禁止事項・注意事項を管理区域外においても遵守すること。ただし、個人や校外団体保有のパソコンを、保有者の活動目的のために使用することは勿論かまいません。

・持ち出した後に、管理区域内に戻す場合には、マルウェア対策ソフトウェアによって、PC 内のファイルをチェックすること。

(4) 個人で所有する端末を校内で利用する場合に気を付けること(BYOD)

個人で所有する PC やスマートフォンなどの端末を、学校に持ち込んで授業などで利用することがあります。これを BYOD(Bring Your Own Device)と呼びます。

BYOD 実施にあたっては、次のことを守りましょう。

【校外から持ち込んだパソコンを学校のネットワークに接続する際の注意事項】

・学校のネットワーク管理者(情報セキュリティ推進責任者)に申し出て許可を受けること。

・ネットワークに接続する前に、マルウェアやスパイウェア等、有害なソフトウェアが含まれていないことを確認すること。

・⑵で示した禁止事項、注意事項を遵守すること。

・無線 LAN は WPA2 などセキュリティが確保された暗号化方式を利用し、盗聴されないようにすること。

5. 情報セキュリティインシデント

(1) 使っている端末がマルウェアに感染してしまったら

使用している端末が、マルウェアに感染した恐れがあるときは、次のように対処してください。
落ち着いて行動することが大切です。

- ネットワークケーブルのコネクターをネットワークから切り離し(無線 LAN の場合は、無線 LAN 用のユニットを取りはずすか、無線 LAN を無効にする。)、管理者に連絡する。
- 電源を切ったり、シャットダウンしない。(被害端末の現状保全のため)
- 管理者の指示に従い、マルウェア対策ソフトウェアの定義ファイルを最新のものに更新する。
- 管理者の指示に従い、マルウェア対策ソフトウェアの駆除機能によってマルウェアの駆除を試みる。
- 駆除が成功したと思われる場合には、その端末と接触のある機器(例えば、 USB メモリ、外付けハードディスク、研究室内の PC など)全てに対して、管理者の指示に従い、処置を施す。
- 以上でマルウェアの駆除ができない場合は、管理者の指示に従って対策方法を調べ実施する。
- 起こったこと、実施したことはしっかり説明できるようにメモをとっておく。

(2) 教職員または管理者に通報すべき場合

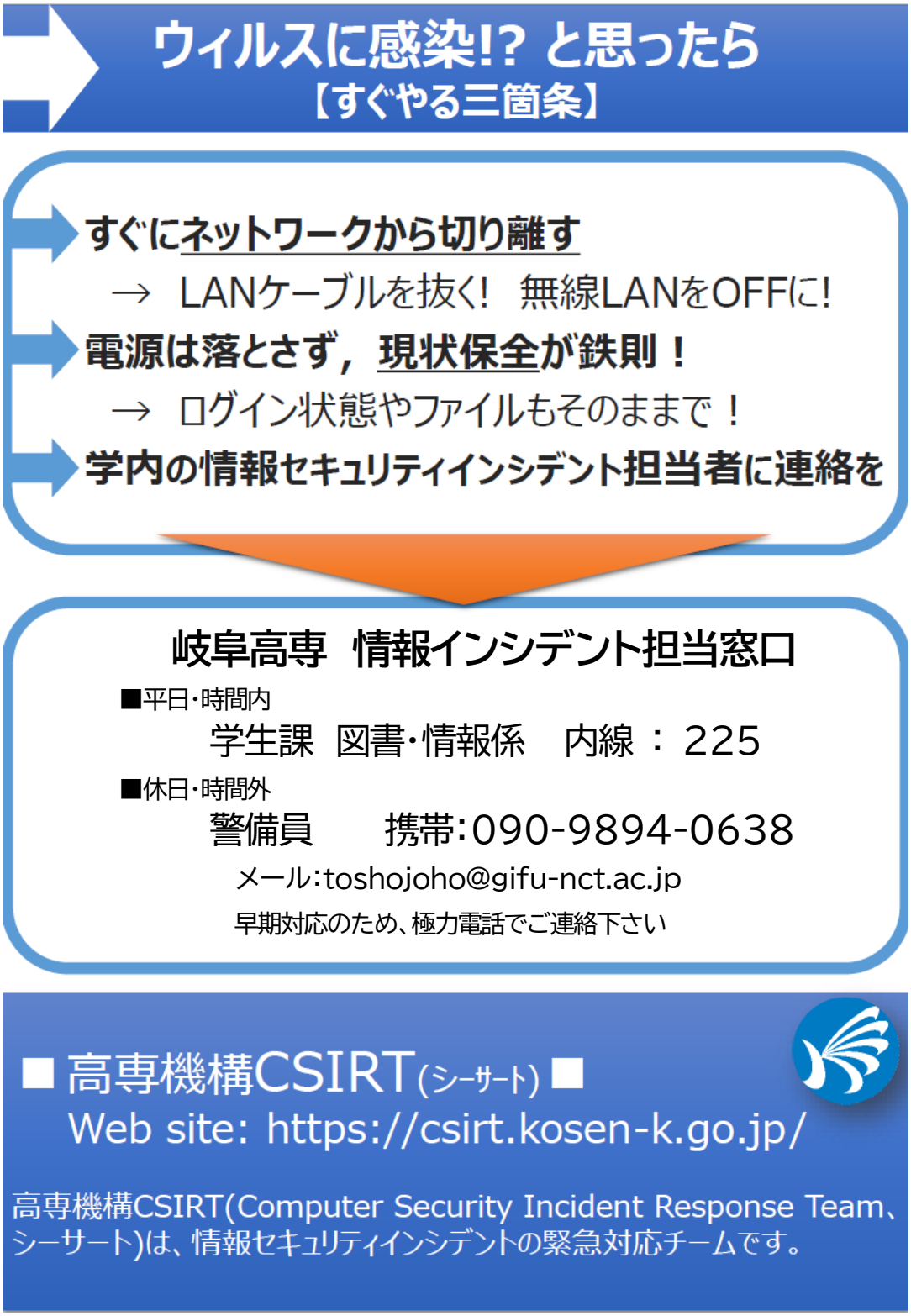
次のことが確認された場合、その端末だけでなく周囲や校内全体に被害を及ぼす可能性がありますので、直ちに通報してください。

- 学校のサーバ上に、著作権を侵害しているおそれのあるコンテンツや、機密情報(機密性 3 又は機密性 2 の情報)が外部に公開されていることを発見した場合。
- 学校のサーバ上にある重要な情報(完全性 2 かつ可用性 2 である情報)に誤りや欠落を見つけた場合。
- インターネット上などで、学校に関する機密情報が公開されている、又は学校が権利を有するコンテンツが無断で使用されていることを発見した場合。
- 自分が管理するユーザ ID やパスワードが漏えいした、またはその可能性がある場合。
- P2P ファイル共有ソフトウェアを利用しているパソコンあるいは学生や教職員を知っている場合。

(3) 通報先を常に把握しておく

インシデントが発生した時は、どこに通報すればよいのか、常に把握しておきましょう。

そのためにも、各校で配布しているインシデント発生時の対処ポスターを、教室や研究室などに掲示しておくようにしてください。(次ページ)



インシデント発生時の対処に関するポスター

6. 電子メール

SNS で連絡を取る例が多い中、汎用的なコミュニケーションツールとして、電子メールはよく使われています。電子メールを使用する際は、次のことに留意してください。

(1) 電子メールを利用する際の禁止事項

・電子メールアカウントを他人に利用させること。つまり、本人以外のメールアカウントを付与あるいは利用許可された場合に、そのアカウントを関係者以外に利用させること。
(例)男子バスケットボール部用として付与されたメールアカウントを、私的なショッピング用のメールアドレスとして EC サイトに登録した。

・授業等や学校業務に必要ないメーリングリスト等へ授業や学校業務のメールアドレスを登録すること。

・マルウェア対策ソフトウェアのインストールが確認できないコンピュータで、電子メールを送受信すること。

・迷惑メールやチェーンメールの送信を行うこと。

・メール本文に個人情報や機微情報を記載すること。

・メールで機密情報を漏えいさせること。

・自己解凍形式(.exe 等)の添付ファイルを送受信すること。

・セキュリティ上の安全性が確認できないマクロを含んだファイルを送信すること。

(2) 電子メール使用時に気を付けること

電子メールを使用する際には、次の事項について留意しましょう。

・ 就職等の重要な連絡については、電話などで確認をとるなど慎重な利用を心がけること。

※送信後直ちに届くとは限りません。送信途中のサーバやネットワークの状態によっては時間がかかることも、届かないこともあります。

・ メール送信者やメール受信者以外の第三者がメールの内容を閲覧する可能性があることを理解し、送信するメールの内容は情報流出することがあることを前提に暗号化等の適切な措置を講じること。

※メール配送経路途中に第三者によってメールの内容を盗聴される可能性があることを理解し、システム上のトラブルを解決するためにサーバ管理者が検査する場合がある、最終的には裁判などの証拠とされる場合がある、などの可能性があります。

・ メールに添付ファイルをつけることは極力しないこと。添付ファイルをつける場合は、暗号化を行うこと。

※メールを受信した人にマルウェアを感染させる危険性があります。また、学校によっては添付ファイル付きメールの送受信を禁止していることもあります。各校のルールに従って利用してください。

・ 個人情報、プライバシー情報や機微情報を移送する場合には、電子メール以外の方法を検討すること。

※特に、パスワードや個人情報等のデータをメールで送るのは避けてください。学校のルールの許容範囲内で、どうしても電子メールで送信しなければならない場合は、暗号化などの対策を実施してください。

・ メールを送信する前に、宛先が間違っていないかよく確認すること。

※特に、CC と BCC を間違えて、不必要に他者のメールアドレスを他人に伝えてしまうことなど無いようにし

ましょう。

・ 身に覚えがない電子メールは開かないこと。

・ 迷惑メールは無視して即削除すること。

・ 迷惑メールなどの怪しい電子メールに書いてある URL をクリックしないこと。

※信頼できないサイトへは接続しないようにして下さい。また、送信元が信用できる人でも、送信元が詐称されていることがあります。

・ 「不幸（幸福）の手紙」や、“セキュリティ上の問題点をできるだけ多くの知人に知らせるように”といった、善意を装って不特定多数への配布を目的としたメール(チェーンメール)を他人に転送しないこと。

・ アダルトサービスなどで「利用料金を払わないと法的手段に訴える」などのようなメールには一切返信しないこと。

※このようなメールは詐欺を目的として送られている場合がほとんどです。身に覚えがある場合でも、ばらまき型メールを送付された可能性があります。このようなメールに返信してしまった場合には学校や最寄りの消費生活センター等に相談して下さい。

・ ㈱や①のような環境依存文字を使わないこと。

※受信側で環境依存文字が表示できないことや、文字化けで別の形の文字が表示されることがあります。

・ メーリングリストでは自動返信の機能を用いないこと。

7. WWW、ネットワークサービスの利用

様々な情報を入手するツールとして、WWW (World Wide Web)は非常によく使われています。その他、SNSなどのネットワークサービスも充実し、多くの人が使用しています。

しかし、便利さの一方で危険性もはらんでいます。次の事項に留意して使用してください。

(1) ウェブブラウザを利用する際の注意事項

・ブラウザのセキュリティ対策に気を配ること。ブラウザには修正プログラムを適用し、可能な限り最新の状態にすること。

・パスワード等の保存はしないこと。特に共用コンピュータ上でパスワードを保存しないこと。

作成元が明確でないプラグインを導入しないこと。

(2) ネットワークサービスを利用する際の禁止事項

・授業・演習、学校業務に必要のないサービスを利用すること。

※不正サイトへの接続は厳に慎んで下さい。また、懸賞サイトやゲームサイトへの接続もしないで下さい。なお、コンテンツフィルリングによって、校内から不正サイトへのアクセスを制限していることがあります。

・機密情報 を校外の掲示板、 SNS やブログの書き込みなどで漏えいさせてしまうこと。

※氏名、成績や住所などを公開してしまった例が散見されています。

・共同研究の情報(研究情報等)を契約で締結している範囲外へ漏えいさせてしまうこと。

・誹謗中傷や公序良俗に反する内容、反社会的な内容を SNS やブログなどに書き込むこと。

※発言・書き込みには責任が伴うことを理解して下さい。

・著作権によって保護されているデータの閲覧、ダウンロードを行うこと。

・マルウェア対策ソフトウェアによって、マルウェア感染しているデータかどうかを確認せずに、ダウンロードしたデータやプログラムを開くこと。

(3) SNS を利用する際の心構え

SNS を利用する際には、次の項目に留意しましょう。

・ いたずら書きをしないこと。また、けんか腰での議論をしないこと。

※これは SNS を利用する際に、必ず守らなければならないマナーです。名誉棄損などで訴えられることもあります。なお、書き込みに使われたコンピュータのアドレス情報を基に、学校へ通報されることがあり、思いがけない処分を受けることもあります。

・ SNS 上での発言には責任を持つこと。

※個人として書き込む場合でも、その組織全体の意見として受け取られる可能性があります。立場をわきまえ、発言は責任を持って行って下さい。

・ 他人の意見は寛大に受け取ること。

※感情的になって直ちに返信することは避けて下さい。反論がある場合にも、少し時間を置いて、よく一度考え直してみることが大切です。

・ 犯罪にあたる行動の自慢や、反社会的発言は絶対に行わないこと。

※たとえその事実がなかったとしても、犯罪に当たる行動や反社会的な内容を発言することは厳禁です。事実でなくとも社会的に影響があったという理由で、学生であれば処分や内定取り消しなど、教職員であれば停職や懲戒解雇などが行われる場合があります。

(4) ウェブを公開する場合

研究室情報など、WWW 上に情報を公開する場合には、次のことに留意してください。

【ウェブ公開における全般的注意事項】

・学校の業務目的以外のウェブ公開は行わないこと。

・営利を目的とした利用を行わないこと。

・盗聴など、通信の秘密を侵害しないこと

・過度な負荷をかけるなど、ネットワークの運用に支障を及ぼすような利用をしないこと。

・ネットワーク及び接続するコンピュータに対する不正行為等が発生しないように最善の努力を払うこと。

【ウェブ公開において不正行為を防止するための注意事項】

・公開を行うデータの安全性(マルウェアに感染していないこと)を確認すること。

・圧縮形式のデータを提供する場合、.exe などの自己解凍形式のデータを提供しないこと。

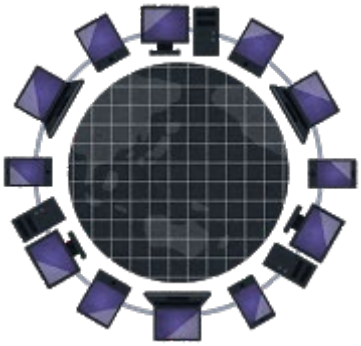
・電子署名されていない実行モジュール(Java アプレット、ActiveX コントロールなど)を使用しないこと。

・電子署名は、可能な限り第三者が保証したものを利用すること。

・ウェブコンテンツを参照する際に、ブラウザのセキュリティ設定を変更するような要求を行わないこと。

・ウェブコンテンツを参照する際に、安全性が保証されないソフトウェアのインストールを要求しないこと。

・セキュリティ上の安全性が確認できないマクロを含んだファイルを提供しないこと。



8. 端末の保全・管理対策

PC、タブレット、スマートフォンなどの各種端末の管理に当たっては、次の点に留意してください。

(1) 端末の保全・管理における注意事項

・ IDとパスワードの管理を徹底すること。

・ 必要に応じて、盗難防止策と UEFI・BIOS レベルでのパスワード設定を行なうこと。

※UEFI・BIOS レベルでのパスワードを設定しておくことで、パスワードを入力しないとパソコンの起動さえ不可能にすることができます。

・ 重要なデータが入っているパソコンは、持ち出しができないように専用のチェーン等でロックするなどの対策をとること。

・ 資産管理を徹底させること。

※資産管理が不十分だと、最悪の場合、盗難に遭ったことさえわからなくなります。パソコンの備品番号、利用者、設置場所、利用内容など、必要な情報を管理して下さい。

・ 端末の内部には重要なデータが残されているかもしれないので、端末の廃棄時には、その端末のハードディスク内容を消去すること。

※ディスクを物理的に破壊する、あるいは完全にデータを消去する、又は別のデータで上書きするなどの対策をとってください。通常の操作でファイルを消しただけでは不十分です。専用のソフトウェアを使用することでファイルを復元できます。

・ パソコンの修理を業者に依頼する場合は、機密情報、個人情報の漏えい防止策を講じた上で行うこと。

※情報セキュリティ推進委員に相談の上、修理を依頼するのも一考です。

9. 在宅勤務における情報の取扱いに係る注意事項

(1) 基本事項

・ 在宅勤務は、本人以外に業務の内容が見られないよう、周りに人がいない環境で行うこと。また、離席する場合は PC にスクリーンロックをかけること。
・ 在宅勤務中においても守秘義務があることを留意して業務を実施すること。
・ 在宅勤務中に情報セキュリティインシデントが発生した場合の対応手順について確認しておくこと。
・ 在宅勤務に使用する PC は、公衆無線 LAN などの安全性の確保できないネットワークには接続しないこと。

(2) 情報の持ち出しについて

・ 在宅勤務を実施する場合、原則として情報は Microsoft365 等の高専が契約しているクラウド上でのみで取扱い、USB フラッシュメモリ等での情報の持ち出しは禁止する。また、在宅勤務に使用する PC 上に情報を保存しないこと。
・ 本校の管理区域外への情報を持ち出しが必要となった場合は、情報セキュリティ管理規程等に基づき、適切に取扱うこと。情報の機密性についての格付けは別表を参照し、機密性3情報の場合は、別紙様式により情報セキュリティ責任者への申請を行うこと。機密性2甲情報の場合は別紙様式により届け出を行うか、本校情報処理センターホームページ内の「要機密情報の持出し届け出フォーム」より届け出をすること。USB フラッシュメモリ等を使用する場合は、暗号化されたものを用いること。
・ 情報の持ち出しに該当しない場合であっても、情報セキュリティ責任者が特に機密性が高いと判断した情報は、原則として在宅勤務では取り扱わず、管理区域内で取り扱うこと。

(3) 在宅勤務時に高専の PC を使用する場合

・ 本校の PC を持ち出す場合は、物品管理規則(機構規則第39号)に基づき、適切に取扱うこと。
・ 本校の PC を在宅勤務で使用する場合は、業務以外の用途には使用しないこと。

(4) 在宅勤務時に個人用 PC を使用する場合

・ OS 及びマルウェア(ウイルス)対策ソフトを最新状態に更新すること。また、マルウェア対策ソフトは情報セキュリティ責任者が信頼できると判断したソフトを使用すること。
・ PC のユーザーアカウントを新規で作成し、業務はそのユーザーアカウントで行うこと。また、在宅勤務が終了した場合は、速やかに当該ユーザーアカウントを削除すること。

別表　　岐阜高専 情報の格付一覧

情報資産の分類					情報資産の項目	情報資産例	運用方法	情報資産の保管
重要度分類	定　義	機密性	完全性	可用性				
Ⅰ	セキュリティ侵害が教職員又は学生の生命、財産、プライバシー等へ重大な影響を及ぼす。	3	2	2	○ 成績関係	指導要録原本(紙ベース) 等	**[電子記録媒体での保管時]** 外部のネットワークから直接学内のネットワークに接続できない環境下にある機器(暗号化による保護による保存) **[紙媒体での保管時]** 施錠可能な場所へ保管し、盗難及び不正な持ち出し等の物理的な脅威から保護をすること **[複製・配布]** 必要以上の複製及び配布禁止 **[情報の持ち出し]** 特別な事由を除いて禁止(真にやむを得ない場合に限り、情報セキュリティ責任者の許可で持ち出し可)	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管 ・情報資産を格納するサーバのバックアップ ・1年以上のログ保管 ・サーバの冗長化(推奨事項) ・インターネット接続されるネットワークにサーバーを置く場合は、情報資産にファイル暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止
					○入試関係	入学者選抜問題(実施前) 等		
					○その他、高度な機密性があると認められる情報			
Ⅱ	セキュリティ侵害が学校事務及び教育活動の実務に重大な影響を及ぼす。	2甲	2	2	○学校関係	出席簿、卒業証書授与台帳、転学・退学受付簿、学生異動報告書(住所変更、名前変更等)、各種委員会等会議関連情報、その他 就学援助関係書類 等	**[電子記録媒体での保管時]** 本校で業務上許可されたファイルサーバー **[紙媒体での保管時]** 施錠可能な場所へ保管し、盗難及び不正な持ち出し等の物理的な脅威から保護をすること **[複製・配布]** 必要以上の複製及び配布禁止 **[情報の持ち出し]** 都度情報セキュリティ責任者への届出が必要 ただし、記録媒体による移送は特別な事由を除いて禁止(真にやむを得ない場合に限り、情報セキュリティ責任者の許可で持ち出し可)	同上
					○成績関係	評定一覧表、指導要録原本(電子媒体)成績関係資料、通知書、定期考査・テスト等の答案用紙(学生が記入済みのもの) 等		
					○指導関係	事故報告書・記録簿、学生指導・特別指導等記録簿、学生写真・集合写真、個別指導計画、個別面談記録、教務手帳、週ごとの指導計画(個人情報が含まれるもの) 等		
					○進路関係	卒業生連絡先一覧等、進路希望調査、進路判定会議資料、進路希望記録簿、入学者選抜に関する表簿(願書等)、調査書、推薦書 等		
					○健康関係	健康診断に関する表簿、健康診断票、心臓管理等医療情報、学校生活管理指導票、健康調査票、健康保険等被保険者証の写 等		
					○学生に関する個人情報	生活歴、心身の状況、財産状況等の情報、その他学生の基本情報を含むもの 等		
					○学校教職員に関する個人情報	人事情報、病歴、心身の状況、収入等の情報 等		
					○名簿等	学生名簿、住所録、後援会会員名簿、職員緊急連絡網、職員住所録、委員会名簿 等		
					○教職員に割り当てた機密性の高い情報	情報システムログイン、情報端末ログイン情報 等		
					○学生の学習系情報(学生の学習記録	学生の学習記録(ワークシート、レポート、作品等)、学習活動の記録(動画・写真等) 等 ※学習後のもの		
					○学校運営システム関連情報	開発ソフトウェア関連情報、情報システム関連情報 等		
					○研究関連情報	知財関連情報、共同研究等関連情報、学会等発表前研究論文関連情報、学会誌掲載審査研究論文関連情報 等		
					○寄宿舎寮関係資料	寮生名簿その他個人情報が含まれている情報 等		
					○監査情報	内部監査、外部監査、情報セキュリティ監査における情報 等		
					○その他、機密性があると認められる情報			
Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす	2乙	2	2	○学生の学習系情報(学習中)	学生の学習記録(ワークシート、レポート、作品等)、学習活動の記録(動画・写真等) 等 ※学習中のもの	**[電子記録媒体での保管時]** 本校で業務上許可されたファイルサーバー **[紙媒体での保管時]** 施錠可能な場所へ保管し、盗難及び不正な持ち出し等の物理的な脅威から保護をすること **[複製・配布]** 必要以上の複製及び配布禁止 **[情報の持ち出し]** 情報セキュリティ責任者の包括的承認が必要	・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管 ・情報資産を格納するサーバのバックアップ(推奨事項) ・1年以上のログ保管 ・サーバーハードディスクの冗長化(推奨事項) ・保管場所への必要以上の電磁記録媒体の持ち込み禁止
					○学校運営関係	卒業アルバム、学校行事等の学生の写真 等		
					○その他、機密性があると認められる情報			
Ⅳ	影響をほとんど及ぼさない。	1	2	2	○学校運営関係	学校要覧、学校紹介パンフレット、使用教科書一覧、教育課程編成表、学校設定科目の届け出、特色紹介冊子原稿、学校徴収金会計簿(学年費・教育振興費等)、学校行事実施計画、保護者等への配布文書文例、各種届雛形、公務分担表、後援会資料、学校だより、学校ホームページ掲載情報、学校行事のしおり、授業用教材、教材研究資料、学生用配布プリント(校務分掌名等で出すもの)　その他公表を前提とした資料 等	特になし	特になし

※：情報資産の持ち出しとは、学校の管理区域外に情報資産を持ち出すことを示す。

※：「情報資産の項目」内の「その他」については、情報セキュリティ責任者に相談をすること。

別紙様式

情報ｾｷｭﾘﾃｨ責任者	情報ｾｷｭﾘﾃｨ副責任者	情報ｾｷｭﾘﾃｨ推進責任者	事務部長	総務課長	学生課長	図書・情報係

要機密情報の持出し　許可申請書　・　届出書

情報セキュリティ責任者
物品管理役　　殿

申請・届出日：令和　　年　　月　　日
申請・届出者：所属
氏名（自署）

下記の通り、（物品・個人情報）を学外へ持ち出したいので（申請・届出）します。
なお、持出し期間中は、要機密情報を厳重に管理し、当該情報漏洩しないよう注意します。

記

要機密情報の区分	□機密性３情報　　□機密性２甲情報
持　出　先	
持 出 期 間	令和　　年　　月　　日　～　令和　　年　　月　　日
持 出 理 由	
情報資産名 (出席簿・テスト答案用紙等)	
持 出 方 法	□紙　　□記録媒体（USB ﾒﾓﾘ・ﾒﾓﾘｰｶｰﾄﾞ等） □情報機器（ﾊﾟｿｺﾝ・ﾀﾌﾞﾚｯﾄ・ｽﾏﾎ等）　□その他　（　　）
情　報　量 (クラス・人数等)	
持出物品名	（本校に属する物品を持ち出す際にご記入ください） 物　品　名： 規　　格： 管 理 番 号：

保 護 対 策	はい	いいえ	該当無し
パスワードによる保護又は暗号化を行う	□	□	□
情報端末にパスワードによる保護又は暗号化を行う	□	□	□
運搬する際の紛失・盗難対策を講じる	□	□	□

上記申請書について許可します。
令和　　年　　月　　日

情報セキュリティ責任者
校　　長
物品管理役
総 務 課 長

10. 参考情報

(1) 電子決済・インターネットバンキング・オンラインショッピング等

オンラインショッピングなど、インターネット上で金銭的決済を行うことが多くなっています。電子決済等においては、下記の項目について留意してください。

・ショップの信頼性を確認すること。

※ショップの Web サイトでフリーメールではない電子メールアドレスが公開されているか、一般加入・電話のように契約者が特定できる電話番号が公開されているか、など

・決済方法を確認すること。

※前払い方式の決済の場合だと、商品が送られてこない危険性があります。高額な商品の購入は避ける、代金引換方式のショップを利用する、などを検討して下さい。

・セキュリティ対策が実施されているか確認すること。

※クレジットカード番号、個人の情報などを暗号化して送る仕組みが提供されているかを確認して下さい。少なくともクレジットカード決済の場合は SSL などによる暗号化の対策が実施されているショップを選んで下さい。Web サイトのアドレス(URL)の先頭が http://ではなく https://になっていれば SSL による暗号化対策が実施されています。

・クレジットカード利用状況を確認すること。

※自分が利用しているクレジットカードの利用状況を常に把握し、自分の知らないところで不明な引落し等が発生していないか日頃からチェックして下さい。

(2) 著作権の侵害

著作権侵害はエンジニアとして恥ずべき行為です。

2010 年の著作権法の改正(データを提供するだけでなく、ダウンロードして入手することそのものが摘発の対象となった。)もあり、コンピュータを利用した著作権侵害行為について、警察や著作権保護団体による監視、摘発が強化されようとしています。エンジニアは知的財産権を産みだし、守るのが仕事です。そのエンジニアの卵を輩出する組織が「著作権侵害」では、学校そのものの存在意義が問われます。

【著作権侵害を行った場合のペナルティ】

・著作権で保護されたデータを提供(アップロード)した場合

懲役 10 年以下あるいは 1000 万円以下の罰金

民事訴訟による損害賠償金・・・購入代金の 3 倍 ×想定コピー数

・著作権で保護されたデータを入手(ダウンロード)した場合

懲役 2 年以下あるいは 200 万円以下の罰金、またはその両方

民事訴訟による損害賠償金・・・購入代金の 3 倍 ×想定コピー数

「1000 万円以下の罰金」は、万引きなどの窃盗による刑罰(懲役 10 年以下、50 万円以下の罰金)よりも重いことに注意して下さい。なお、民事訴訟による損害賠償金は、億単位の額になった判例があります。

(3) 商標の使用

「**商標**」は主に商売と密接な関係があり、商品名、サービス名、商品の形状、ロゴやマークなどが対象となります。他人の商標を、自分の商品やサービスに使用すると**商標権の侵害**となります。

同じでなくても、混同されるような名称を使うのは不正競争防止法違反となる場合がありますので注意して下さい。

(4) 肖像権/プライバシーの侵害

自分で撮った写真を、SNS や Web サイトに掲載する場合、著作権は自分にあるので一般的には問題ありません。ただし、他の人物が写っている写真などについては、肖像権やプライバシー権に気を付ける必要があります。

プライバシー権は、個人情報をみだりに公開されないという権利です。肖像権はプライバシー権のひとつとなります。さらに、有名人の場合は、肖像自体に経済的な価値があるため、パブリシティ権（財産的に利用する権利）が認められます。

個人が有名人の写真を許可なく使うと、肖像権の侵害となるほか、自分で撮影した写真でない場合は著作権の侵害にもなります。さらに、有名人の写真を使うことで結果的に利益を生み出すような場合は、パブリシティ権も侵害することになります。

(5) 名誉毀損/偽計業務妨害/電子計算機損壊等業務妨害/不正指令電磁的記録作成罪

SNS や Web サイトに記載または掲載された情報は、「公開」されたことになります。公開された場において、他者の社会的評価を低下させるような表現を行なうと、「名誉毀損」となる場合があります。「名誉毀損」には刑事罰が適用されます。

また、虚偽の風説などを流して業務を妨害する行為、威力を用いて業務を妨害する行為は、それぞれ「偽計業務妨害」「威力業務妨害」と呼ばれます。さらに、コンピュータに虚偽のデータや不正な実行を行わせて業務を妨害する行為は「電子計算機損壊等業務妨害」と呼ばれます。

例えば、あなたの PC に感染したマルウェアが、あなたの知らないうちにある企業のサーバを攻撃して、そのサーバの機能をマヒさせてしまった場合、威力業務妨害ないし電子計算機損壊等業務妨害に問われることがあります。

また、マルウェアを作成、配布する行為は「不正指令電磁的記録作成罪」に相当します。

【名誉毀損、偽計業務妨害、電子計算機損壊等業務妨害に関する法律】

[名誉毀損(民法 710、723 条)]

品性、徳行、名声、信用その他の人格的価値について社会から受ける客観的評価(社会的評価)を低下させる行為の禁止。損害賠償責任が肯定されています。

[信用および業務に対する罪(刑法第 168、233、234 条)]

虚偽の風説を流し、または偽計を用いて人の業務を妨害すること(偽計業務妨害罪)。または威力を用いて人の業務を妨害すること(威力業務妨害罪)。他人のコンピュータやその電磁的記録の損壊、不正な指令などで業務を妨害する行為(電子計算機損壊等業務妨害罪)については、5 年以下の懲役または 100 万円以下の罰金に処せられます。

また、コンピュータウィルスを作成、または提供する行為 (不正指令電磁的記録作成罪)については、3 年以下の懲役または 50 万円以下の罰金に処せられます。

(6) わいせつな文書や画像の発信

Web サイトに掲載、または SNS に投稿した情報が「わいせつ」であると判断されると次のような法律によって処罰されます。

【わいせつな情報発信に対する罰則】

[刑法(明治 40 年法律第 45 号) 第 175 条]

わいせつな文書、図画その他の物を頒布し、販売し、又は公然と陳列した者は、 2 年以下の懲役又は 250 万円以下の罰金若しくは科料に処する。販売の目的でこれらの物を所持した者も、同様とする。

[児童買春・児童ポルノに係る行為等の処罰及び児童の保護に関する法律(平成 11 年法律第 52 号)第 7 条第 4 項]

児童ポルノを不特定若しくは多数の者に提供し、又は公然と陳列した者は、5 年以下の懲役若しくは 500 万円以下の罰金に処し、又はこれを併科する。電気通信回線を通じて第二条第三項各号のいずれかに掲げる児童の姿態を視覚により認識することができる方法により描写した情報を記録した電磁的記録その他の記録を不特定又は多数の者に提供した者も、同様とする。

(7) 不正アクセス禁止法

2000 年 2 月 13 日に「不正アクセス行為の禁止等に関する法律」いわゆる不正アクセス禁止法が施行されました。不正アクセス禁止法では、次の行為が禁止されていて、何の実害を与えなくても処罰の対象になります。

【 不正アクセス行為 】

アクセスが制限されたコンピュータに対し、他人のユーザID／パスワードを使ってログイン（コンピュータが使える状態に）すること。

アクセスが制限されたコンピュータに対し、セキュリティホールをついて侵入し、コンピュータが使える状態にすること。

【 不正アクセス行為を助長する行為 】

偽サイト（フィッシングサイト）を作成して閲覧可能にすること。

偽サイト（フィッシングサイト）に誘導するメールを送信すること。

他人のユーザID／パスワードを当該コンピュータの管理者、当該ユーザID／パスワードの利用者以外に提供すること。

ただし、次のような場合は不正アクセス行為に該当しないものと考えられています。

・パソコン初心者に頼まれて接続操作を行なってあげた。

・コンピュータの管理者自ら、もしくは管理者の承諾を得た者が行なった。

(8) 電波法および盗聴

ネットワーク上の情報の盗聴は法律で禁止されています。また、盗聴した内容を第三者に漏らす行為についても電波法、電気通信事業法違反となり罰せられます。

【 電波法、電気通信事業法による規制 】

[有線通信における秘密の保護(有線電気通信法第 9 条)]

電話や FAX、インターネットなど有線でつながれた方法で得た秘密や情報は他人に話してはならない。（違反した者は 1 年以下の懲役または 20 万円以下の罰金に処せられます。）

[無線通信における秘密の保護(電波法第 59 条)]

特定の相手に対して行われる無線通信を傍受してその存在もしくは内容を漏らし、盗用してはならない。（違反した者は 1 年以下の懲役または 20 万円以下の罰金に処せられます。）

[電気通信事業者の守秘義務(電気通信事業法第 4 条)]

電気通信事業者は業務の取扱中にかかる通信の秘密を侵してはならない。（違反した者は 1 年以下の懲役または 50 万円以下の罰金に処せられます。）

付　記

このガイドラインは令和3年7月1日から適用する。

（参照元）
情報システムユーザガイドライン
発行日：平成２３年６月 初版
平成２５月９月 第２版
令和２年９月　 第３版

編　集：・情報戦略推進本部
情報セキュリティ部門
・高専機構 CSIRT