情報システム　ユーザガイドライン

第４版（学生用）

群馬工業高等専門学校

2023年1月

目次

1. インターネットと 情報セキュリティ対策 5
(1) インターネットに流れる情報は、盗聴の恐れがある 5
(2) 接続記録は把握されている 5
(3) インターネットからの攻撃から、自ら身を守ること 5
2. WWW、ネットワークサービスの利用 6
(1) ウェブブラウザを利用する際の注意事項 6
(2) ネットワークサービスを利用する際の**禁止**事項 6
(3) SNS を利用する際の心構え 7
(4) ウェブを公開する場合 7
3. ユーザ ID とパスワードの管理 11
(1) ユーザ ID とパスワードが第三者に知られると… 11
(2) 高専統一パスワードポリシーを守る 12
4. 多要素認証について 13
(1) 「多要素認証」とは 13
(2) 多要素認証を有効に活用するために 13
5. 校内における端末（PC、タブレット等）の取り扱い 16
(1) 校内で端末（PC、タブレット等）を使う時には 16
(2) 学校管理下の端末を使う時には 17
(3) 管理区域外へパソコンを持ち出す場合 18
(4) 個人で所有する端末を校内で利用（BYOD）する場合に 気を付けること 18
6. 情報セキュリティインシデント 21
(1) 使っている端末がマルウェアに感染してしまったら 21
(2) 教職員または管理者に通報すべき場合 21
(3) 通報先を常に把握しておく 21
7. 電子メール 25
(1) 電子メールを利用する際の禁止事項 25
(2) 電子メール使用時に気を付けること 26
8. 参考情報 27
(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 27
(2) 著作権の侵害 27
(3) 商標の使用 28

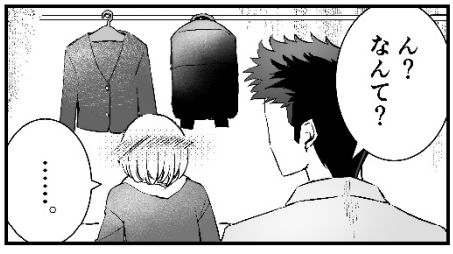
(4)　肖像権の侵害 28
(5)　名誉毀損/偽計業務妨害/電子計算機損壊等業務妨害/ 不正指令電磁的記録作成罪 28
(6)　わいせつな文書や画像の発信 29
(7)　不正アクセス禁止法 30
(8)　電波法および盗聴 30

セキュリティまんが①「インターネット」


そういえばお前、何で今日ここにいるの？
え？
部活の日だろ？


そ…それは、ケンタが初めて…
PCを買ってもらったって聞いて…。


だから…自己防衛しないとね。
●マルウェア対策ソフトウェアを導入する。
●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。
●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。
●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。
●P2Pファイル共有ソフトウェアは使わない。
●懸賞サイト、無料ゲーム、SNSなどのアカウントに授業用のメールアドレスを登録しない。
●授業では利用しないサイトに、学校からもらったメールアドレスやSNSアカウントなどの個人情報を入力しない。


ん？なんて？
……。


カッ
う…うるさいな。
なんでもいいでしょ!?
お、おう…


そ…その…
ちょっと心配だったっていうか…。

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。
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用のメールアドレスを登録しないこと。
- 授業では利用しないサイトに、学校からもらったメールアドレスや SNS アカウントなどの個人情報を入力しないこと。

2. 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。
  ※教員からの指示なしに研究情報等を校外の掲示板やその他ネットワークサービスへ書き込むことは絶対にしないでください。
  (例えば、教員から提示された研究課題等を許可なく Web 掲示板にアップしたり、誰もが見ることのできる設定でクラウドサービスにアップロードしたりしないでください。)
- 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

- 教員からの指示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。

（次ページに続く）

- 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。
- 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。

セキュリティまんが②「パスワード」

高専統一パスワードポリシー

●16文字以上。

●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)

「多要素認証」とは…
認証の3要素である
「知識情報(パスワード等)」
「所持情報(携帯電話・スマートフォン等)」
「生体情報(指紋・声紋等)」
のうち、2つ以上を組み合わせて認証すること。

3. 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 とパスワードの管理はしっかり行いましょう。

これらが自分以外の人に知られると、以下のような不利益が想定されます。

- 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。

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。
- パスワードの使いまわしはせず、システムごとに異なるパスワードを設定すること。

（2）高専統一パスワードポリシーを守る

2022 年 7 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**「高専統一パスワードポリシー」**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

- パスワードは、**16 文字以上**。
- パスワードには、以下の文字種を、**各 1 文字以上、必ず含める**こと。
  - **英字**（大文字／A～Z）
  - **英字**（小文字／a～z）
  - **数字**（0～9）

4. 多要素認証について

（1）「多要素認証」とは

パスワード認証については、近年、多くの攻撃手法が編み出されており、限界が叫ばれています。よって、高専機構で契約している Microsoft365 をはじめとした多くのクラウドサービスでは、**「多要素認証」**(Multi-Factor Authentication)が導入されています。

「多要素認証」とは、認証の3要素である「知識情報（パスワード等）」、「所持情報（携帯電話・スマートフォン等）」、「生体情報（指紋・声紋等）」のうち、2つ以上を組み合わせて認証することを指します。

（2）多要素認証を有効に活用するために

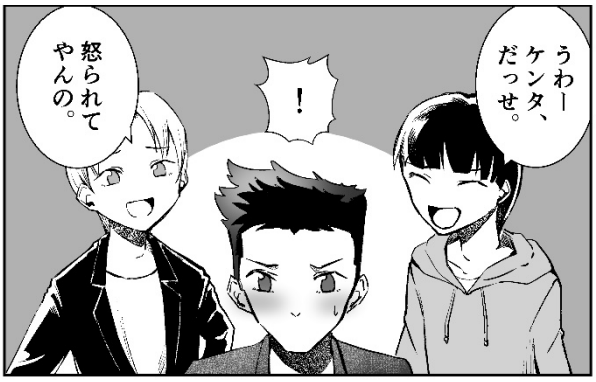
多要素認証はセキュリティ的に信頼性の高い認証方法ですが、攻撃に晒されることで、効力が失われてしまう場合があります。例えば、次に挙げる状態のときは、多要素のうち少なくとも1要素を看破されており、セキュリティ的に脆弱な状態となっています。すぐに対処し、安全な状態を回復しましょう。

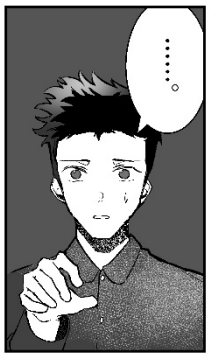
ID、パスワードをどこにも入力していないのに、
２要素目に設定した携帯電話のアプリから、認証を求められた。
パスワードが漏洩している可能性があります。
反射的に「承認」を押すようなことはせず、認証要求は無視し、
すぐにパスワードを変えましょう。

２要素目に設定したデバイス（携帯電話等）を紛失した。
すぐに、高専の担当部署に連絡しましょう。

セキュリティまんが③「校内における端末の取扱」

●授業・実験等で必要とされない作業を行わない。
●私的な電子メールの送受信や、私的にWebサイトを利用しない。
●授業・実験で必要とされないソフトウェアをインストールしない。
●学校が定めたマルウェア対策ソフトウェアを導入する。
●使用するソフトウェアの利用許諾条件に反する行為はしない。
●ソフトウェアをインストールする場合は、有害ソフトウェアが含まれていないことを確認する。
●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ない。
●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しない。(ただし、授業等で教員から指示された場合を除く。)
●OSのセキュリティアップデートを定期的に実行する。
●マルウェア対策ソフトウェアの定義ファイルを常に最新の状態に保つ。
●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。
●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。





5. 校内における端末（PC、タブレット等）の取り扱い

（1）校内で端末（PC、タブレット等）を使う時には

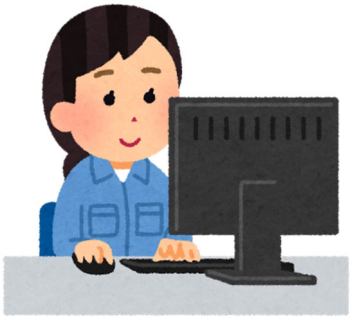
校内に設置された PC、タブレット等を使用する場合は、次のことに留意しましょう。

校内での一般的禁止事項

- PC が置いてある演習室での飲食。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。
- 空調コントローラの操作。ただし、管理者が許可した場合を除く。

校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（トイレ等で離席する場合も該当する）。
- 長時間にわたって PC を占有使用すること。
  ただし、授業等で教員から指示された場合を除く。



（2）学校管理下の端末を使う時には

研究室など、演習室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・実験等で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・実験で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、
  パソコンを使用すること。
  （Linux などの UNIX 系 OS や、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。
  ただし、授業等で教員から指示された場合を除く。

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。

（次ページへ続く）

- 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。

（3）管理区域外へパソコンを持ち出す場合

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。持ち出す前に本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

- (2)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（BYOD）する場合に気を付けること

学校によっては、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。
- (2)で示した禁止事項、注意事項を遵守すること。

セキュリティまんが④「情報セキュリティインシデント」


いい？　もし情報セキュリティインシデントに遭遇したら…
落ち着いて「すぐやる三箇条」を行うのよ。
すぐやる三箇条
1. すぐにネットワークから切り離す
2. 電源は落とさず、現状保全
3. 学内の
情報セキュリティインシデント担当者に連絡
とにかく現状維持が鉄則！
電源を落とすと、検証作業が難しくなるわ。
ケンタはパニックになったアツシの代わりに…
まずはLANを抜く
「すぐやる三箇条」を実施し、情報処理センターに報告した。
ほどなくしてアツシのPCは復旧したが…
消えたデータは二度と戻って来なかった。
アツシはマルウェア対策ソフトをインストールしてなかったし…
どんなソフトも警戒せずにインストールしてたらしい。
マルウェア対策ソフト入れなさい
あいつがいなかったら…。
今日、データを消されたのは僕だったかも…。

6. 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、**「すぐやる三箇条」**に従い、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。

「すぐやる三箇条」

- すぐにネットワークから切り離す。
- 電源を落とさず、現状保全する。（ログイン状態や、ファイルもそのまま）
- 学内の情報セキュリティインシデント担当者に連絡する。
  （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）教職員または情報システム担当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、**直ちにインシデント対応窓口へ通報**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、機密情報が外部に公開されていることを発見した場合。
- 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、また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

情報セキュリティインシデント（（1）や（2）に該当する場合）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、すぐやる三箇条の画像をスマートフォンに保存するなど、何かあった時にすぐ対応できるような措置をとってください。

「すぐやる三箇条」の画像


ウィルスに感染!? と思ったら
【すぐやる三箇条】
すぐにネットワークから切り離す
→ LANケーブルを抜く! 無線LANをOFFに!
電源は落とさず，現状保全が鉄則！
→ ログイン状態やファイルもそのままで！
学内の情報セキュリティインシデント担当者に連絡を
■群馬高専 情報ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄ通報窓口
総務課 電話： 027-254-9012
土日祝：027-254-9000
メール：incident@gunma-ct.ac.jp
■高専機構CSIRT(シーサート)■
Web site: https://csirt.kosen-k.go.jp/
高専機構CSIRT(Computer Security Incident Response Team、シーサート)は、情報セキュリティインシデントの緊急対応チームです。
2016.10.24ver

セキュリティまんが⑤「電子メール」


k
kenta@guide.kosen-ac.jp
宛先: ハナ
きついこと言ってごめん
いつもありがとう
ブブ
…なにこれ。
はは。
直接言えよ。
いくじなしじゃん。
インターネットに感謝しろよ！
ばし
おしまい

7. 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。）
- 授業等に必要ないメーリングリスト等へ授業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

- 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。

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。

8. 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、等。
- 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。)

独立行政法人 国立高等専門学校機構
Institute of National Colleges of Technology, Japan

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
令和　４年７月 第４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

群馬工業高等専門学校

発行日：平成２８年１２月　７日制定
令和　元年１０月１８日改正
令和　３年　１月　６日改正
令和　５年　１月２０日改正
編　集：群馬高専情報セキュリティ管理委員会