基本的な情報セキュリティ対策（大学生編）

慶應義塾情報セキュリティインシデント対応チーム (CSIRT) 2025年3月

★の部分は次ページ以降の
補足資料をご参照ください。

多要素認証

多要素認証★[1]を利用することで、認証情報やフィッシング対策に失敗しパスワードが漏洩した場合でも、第三者のログインを防ぐ一定の効果がある。

情報セキュリティ対策	対策なしで起こる可能性のある結果
認証情報対策 1. 十分に複雑なパスワード★[2]を設定 2. 同じパスワードを使いまわさない 3. パスワードを他人に教えない 4. 他人のアカウントでログインしない	1. 簡単に推測、または力づくでパスワードを知られる 2. 一件のパスワード漏洩が他サービスにも波及★[3] 3. 不正ログインや犯罪★[4]に利用される可能性がある 4. 正当な理由がなければ不正アクセス禁止法違反
ソフトウェア対策 1. OS、アプリは最新に保つ 2. サポート終了したOS、アプリを使わない 3. PCはアンチウイルスソフト★[6]を必ず使う 4. 不正コピー、チートツール等を使わない 5. インフォスティーラー★[7]に特に注意	1. 脆弱性を利用してマルウェア★[5]に感染する 2. OS、アプリの脆弱性修正がなされない 3. マルウェアへの感染確率が非常に上がる 4. その種のソフトはマルウェアの巣窟のため危険 5. ブラウザに保存したパスワード等が全て盗まれる
フィッシング対策 1. 偽ログイン画面に誘導するメールに注意 2. ログイン画面以外のフィッシングに注意 3. メールの差出人のアドレス★[8]に注意 4. リンク付きメールのリンク先URL ★[9]に注意 5. 不自然に対応を急かす文面に注意	1. 攻撃者にID・パスワードを提供してしまう 2. インフォスティーラー ★[7]感染の可能性もある 3. 差出人の名前だけ偽造したメールを信用してしまう 4. 偽ログイン画面やマルウェアにアクセスしてしまう 5. 冷静でない状態で対応を誤ってしまう

ユーザへの連絡

これらの事態の発生をCSIRTやKICが認識した場合、必要であればユーザに対して個別に連絡します。問題解決に向けた支援も可能です。

○ keio.jpなどのサービスでの多要素認証の利用をご検討ください。

○ KICやCSIRTから個人宛に情報セキュリティに関する連絡が来た場合は、早急にご対応ください！

○ フィッシングでパスワードを入力してしまったら、すぐにパスワードを変更し、KICにご連絡ください！

★[10]

基本的な情報セキュリティ対策（大学生編） 補足情報（1）

慶應義塾情報セキュリティインシデント対応チーム (CSIRT) 2025年3月

★1 多要素認証とは？

パスワードと併用の場合、「所持情報」「生体情報」のいずれかを同時に用いる認証のこと。仮にパスワードが盗まれても、第三者がすぐに不正ログインすることはできません。
keio.jpや、学外の多くのWebサービスで利用可能となっているため、積極的に利用することを推奨します。
keio.jpの多要素認証については
https://www.itc.keio.ac.jp/ja/keiojp_mfa2.html
をご参照ください。

★2 十分に複雑なパスワードとは？

従来は複数の文字種を用いて長いパスワードを設定し、定期的に変更することが望ましいとされてきましたが、現在は複雑性に関してはより総合的な判断がなされる傾向があり、定期的な変更は重視されなくなっています。
現在のkeio.jpにおけるパスワードポリシーは、
https://www.itc.keio.ac.jp/ja/keiojp_manual_activation.html
中の「B」の項目をご参照ください。

★3 パスワードの使い回しの問題とは？

塾外のWebサービスから、IDとパスワードの情報が漏洩しますが、パスワードを使い回していると、他サイト（keio.jpなども含む）の不正ログインに利用できてしまいます。
パスワードマネージャーのようなアプリの利用も、このような使い回しを避ける1つの手段です。

★4 パスワードを他人に教える危険性とは？

パスワードを他人に教えることで、そのアカウントで可能な処理や手続きは、犯罪を含め、全てその他人が自由に行うことができるようになります。
特に金融系、決済系（電子マネー等含む）のパスワードを他人に渡して犯罪に使用された場合、容易に回復できない信用情報の毀損につながる可能性があるだけではなく、自身も幇助犯となる可能性があります。
それ以外のサービスでも、発覚時には該当サービスを二度と使えない様に処置される可能性もあります。

★5 マルウェアに感染すると何が起こるのか？

マルウェアとは「ウイルス」や「ワーム」「トロイの木馬」など、悪意のあるソフトウェア（Malicious Software）の総称です。
感染した場合に発生する事象は、負荷上昇、他のシステムへの感染、遠隔制御、情報漏洩、システム妨害・破壊、脅迫のための暗号化等、マルウェアの種類によってまちまちです。
KICやCSIRTではマルウェア特有の動作などをネットワーク上の記録から発見した場合、該当ユーザに対して連絡する場合がありますので、その場合は早急にご対応ください。

基本的な情報セキュリティ対策（大学生編） 補足情報（2）

慶應義塾情報セキュリティインシデント対応チーム (CSIRT) 2025年3月

★6 PCで利用するアンチウイルスソフトとは？

慶應義塾では、個人向けにESET Internet Securityのライセンスを提供していますが、Windows 10以降に標準で付属しているWindows Defenderでも問題ありません。
ESET Internet Securityのライセンス利用に関しては
https://secure.itc.keio.ac.jp/c/a/itc/ja/software_license_esets.html
をご覧ください。
ただし、アンチウイルスソフトをすり抜けるマルウェアは昨今増加しています。

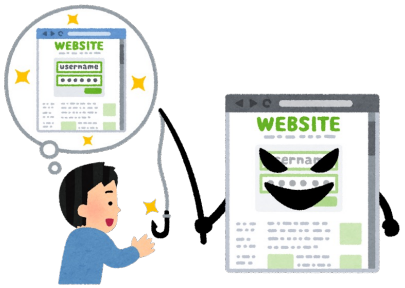
★7 インフォスティーラーとは？

インフォスティーラーは、感染した端末から「ブラウザに記録されたパスワード情報」などを盗む危険なマルウェアの総称です。
アンチウイルスソフトがStealer, RedLine, Raccoon, Lummaなどの単語を含むマルウェアを検知した場合、インフォスティーラーへの感染が考えられます。KICまでご相談ください。
インフォスティーラーは、ゲームのチートツール、不正利用アプリ、非公式の場所から入手したアプリ、そしてフィッシングメールなどから感染しがちです。これらのリスクを避けるようにしましょう。

★8 フィッシングメールの差出人とは？

メールにおいて差出人の表記は一般的に、
「慶應太郎 <keio-taro@keio.ac.jp>」
のように名前とメールアドレスで構成されていますが、昨今のフィッシングメールでは、名前の方だけを偽造してメールアドレスの方は偽造していないものが多くなっています。

★9 フィッシングメールのURLとは？



フィッシングメール上のURLは多くの場合、無関係なWebサイトの一部を改ざんして作られているため、本来のサービスとは無関係なサーバ名であることが多くなっています。
この様な場合、URL中のサーバ名をきちんとチェックすることで偽サイトへの移動を防ぐことが可能です。

★10 連絡と対応は迅速に！

ID・パスワードをフィッシングサイトに入力してしまった場合、まずは直ちにそのID・パスワードを使用しているサイト全て（重要なもの優先）でパスワードを変更し、それからKICにご連絡ください。
マルウェアを含む可能性のある不審なファイルを開いてしまった場合なども同様に、早急にKICまでご連絡ください。
また、KICやCSIRTからセキュリティ関係の連絡を差し上げる場合がありますが、残念ながらその連絡への対応が非常に遅れてしまう場合が散見されます。
連絡をためらっている間に、あるいはKICやCSIRTからの連絡を無視している間に、取り返しのつかない被害に進展する可能性があります。早急な連絡と対応が、被害を最小限に食い止めるために必要です。

質問・相談などの問い合わせ先
csirt@info.keio.ac.jp