3. 情報システムの安全で適正な利用のお願い

3.1. 京都大学のネットワークとセキュリティ

3.1.1. 京都大学のネットワークの作り

京都大学の全学ネットワークKUINS（Kyoto University Integrated Information Network System）は、吉田、宇治、桂などの各キャンパスだけでなく、全国に散らばる小さな研究施設やサテライト・オフィスなど100を超える拠点を繋ぐ大きなネットワークです。KUINSは学内の通信や学内からインターネットへの通信に使われます。インターネットへの接続は100Gの回線でSINETと呼ばれる日本全国の大学や研究機関を結ぶネットワークを経由しています。

3.1.2. 有線LANと無線LAN

学内は全ての建物のほぼ全ての部屋に「情報コンセント」と呼ばれる有線LANへの接続口が設けられていて、LANケーブルを差し込むだけでKUINSに繋がるようになっています。
また、学内の建物は無線LANでもカバーされていて、現在1,600カ所のアクセスポイント（AP）があります。さらに2014年度からの3カ年計画で、古いAPの置き換えと新しいAPの設置を進めていて2016年度末にはほとんどの建物が最新の802.11ac準拠のAPでカバーされることになります。各APからは、場所によって若干の違いはありますが、以下の3種類のSSIDが放出されています。

・KUINS-Air（ECS-IDまたはSPS-IDで認証後、KUINS-IIIへ接続）
・Eduroam（大学関係者に付与されるIDでインターネットに接続）
・通信事業者のWiFiサービス（au、NTTdocomo、Softbankの契約があれば、Wi2_club、0000docomo、mobilepoint2に接続）

3.1.3. ネットワーク・セキュリティの監視

京都大学全体のネットワークであるKUINSには、その出入り口にIDS（Intrusion Detection System）と呼ばれるセキュリティの監視装置が設置されていて、全ての通信を24時間365日監視しています。怪しい通信を発見すると、学内の通信先に安全確認を行うということで、日々インターネットから到来する様々なアタックに対処しています。2013年度は170件あまり、2014年度はHeartbleedなど世界的に大騒ぎになった脆弱性の影響もあり300件あまりと、ほぼ1日～2日に1回の頻度で安全確認を行っていることになります。

3.1.4. 大学全体のセキュリティは、ひとりひとりが守る

上記の監視をしていれば、安全安心なのかというとそうではありません。インターネットはとても便利な道具ですが、セキュリティについては利用者であるあなたが注意していないと、思わぬ事故（セキュリティ・インシデント）に巻き込まれる可能性があります。また、一人の不注意から大学全体が危機的状況に容易に陥ってしまう危険性も高いというのがインターネットのセキュリティ・インシデントの特徴です。従って、大学のセキュリティを守るためには、一人一人の心構えが何よりも大切です。特に、メールの添付ファイル、Webでアクセスするサイトにはマルウェアが隠されている可能性が必ずあります。それに引っ掛からないように特にメールとWebは用心深く使いましょう。また、ウィルス対策ソフトやOS、アプリケーションのアップデートは欠かさず行って下さい。

3.1.5. セキュリティ・ポリシーがあなたを守る

大学では、ネットワークのセキュリティに関して、詳細なセキュリティ・ポリシーを定めています。セキュリティ・ポリシーは、「基本方針・対策規程」「対策基準」「実施手順書」という3階層で定められていて下記のURLから参照する事ができます。

http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/use/regulation.html

セキュリティ・ポリシーは、自由な行動を制限する面倒なものと考える人が多いですが、それは間違った認識です。これらの規則を守って行動すればセキュリティ・インシデントに巻き込まれる可能性が低くなります。また、ポリシーの中には、パスワードのガイドラインや、無線LANアクセスポイントを設置する際のガイドラインなども含まれていますので、ぜひ一度読んでいただきたいです。

セキュリティに関する報告や相談は、先ずは各学部や研究科のセキュリティ連絡窓口にお願いします。あるいは情報環境機構のセキュリティ対策掛までお願いします（お配りしてあるミニガイドもご活用ください）。

3.2. ECS-ID とパスワードの適正な管理

3.2.1. なぜ ECS-ID やパスワードが必要か

教育用コンピュータシステムではその利用を許可された者が、システムを利用する権利や利用者のファイル・情報などを保護することが求められています。そのために利用者を特定する仕組みが ECS-ID とパスワードです。ECS-ID は利用者と 1 対 1 に対応しており、これによってシステムはどの利用者が利用するのかを知ることができます。パスワードは利用しようとする者が、その人のみが知りえる情報としてシステムに伝えることにより、本人であることをシステムに示すためのものです。

教育用コンピュータシステムは ECS-ID とパスワードにより、利用者を特定し利用を許可します。言い換えれば、ECS-ID とパスワードさえ正しければ本人が利用しているものとみなされます。このため ECS-ID とパスワードは適正に管理していただく必要があります。

3.2.2. パスワードを知られると

他人にパスワードを知られると、他人があなたの ECS-ID を使って教育用コンピュータシステムや提携するサービスにアクセスし、あなたの名をかたって、以下のような行為を行うことが可能になります。

- あなたが受け取ったメールやあなたのファイルを覗き見したり、変更したり、消去したりする。
- あなたの信用をおとしめるようなメールの送信や、掲示板への書き込みを行う。
- 他のコンピュータへの侵入など、迷惑行為・犯罪行為をする。

コンピュータを介した行動では顔が見えないので、行為者の特定は ECS-ID によってしかできません。このため、あなたの ECS-ID を使って行われた行為はすべてあなたの行為とみなされ、あなたが責任を負うことになります。

3.2.3. ECS-ID とパスワードの管理

パスワードは、ECS-ID の保持者本人だけが知っている秘密の文字列です。パスワードは、他の誰にも知られてはいけません。そのため、次の点に注意して厳重に管理してください。

当然ながら、誰にも教えてはいけません。TA、職員がパスワードを尋ねることもありません。

- 紙などにメモをとってはいけません。頭の中でしっかりと覚えておきましょう。
- パスワードは必ず、定期的に変更してください。同じパスワードを長期間利用すると、誰かに知られてしまう可能性が高くなります。また、知られていることに気がつきにくくなります。詳しくは「3.2. パスワードの変更」をご覧ください。
- パスワードを推測するツールは誰でも簡単に入手可能です。ツールによって簡単なパスワードは容易に推測されてしまいます。推測されない安全なパスワードを作成してください。
- 他人にあなたの ECS-ID を使用させることは禁止されています。また、他人の ECS-ID を使用することも禁止されています。
- ログオンしたまま PC 端末を離れることは非常に危険です。一時的に端末を離れるときはロックしてください。
- ログオンしたまま放置されている PC 端末を見つけた場合は、触れずにメディアセンター南館 OSL の TA までご連絡ください。
- 利用を承認されていない学内外の計算機に対して利用を試みてはいけません。

注意

ECS-ID では、8 文字以上のパスワードのみ認めています。

3.2.4. 誰かにあなたの ECS-ID が使われていると感じたら

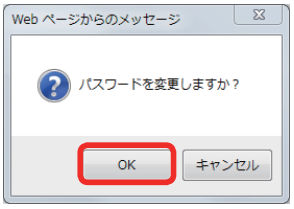
「付録-3. 困ったときには」の連絡先にすぐに相談してください。

3.3. パスワードの変更

パスワード変更は Web ページを通して行います。

1. ブラウザから https://ecs.iimc.kyoto-u.ac.jp/ にアクセスしてください。
2.「設定変更へ進む」をクリックし、ECS-ID と現在のパスワードを入力してログインしてください。

3. 左にある [パスワード変更] をクリックしてください。



4. 現在のパスワードと、新しいパスワードを２回入力し、実行をクリックします。

5.「OK」をクリックし、「パスワードの変更を依頼しました。」と出たら完了です。

3.4. ネットワーク利用上の注意

インターネットにより世界中のコンピュータが相互に接続され、さまざまな情報サービスが提供されています。一方で、ネットワークなどの利用については様々な社会的問題も生じています。問題点を理解し、適切な利用をお願いします。

3.4.1. 情報セキュリティ面の注意

◆ ECS-ID とパスワードの適切な管理

教育用コンピュータシステムや学生用メールでは ECS-ID とパスワードで利用者を特定し、PC 端末や電子メールなどのサービスを提供しています。他人に ECS-ID とパスワードが知られると、「3.1.2. パスワードを知られると」で述べたような問題を招きますので、ECS-ID とパスワードは適切に管理してください。

◆コンピュータウィルスへの注意

コンピュータウィルスとは、電子メールの添付ファイルや Web サイトの閲覧、フラッシュメモリ等の外部記憶メディアなどから感染する悪意のあるコンピュータプログラムです。ネットワークや USB フラッシュメモリなどの外部記憶メディアを介して感染が広がります。

利用者の皆様には次の点の注意をお願いします。

- 不審なメール（添付ファイル）を開かない。
- 怪しい Web サイトには行かない。
- 出所のはっきりしないファイルを開かない。

◆利用者ご自身のパソコンのセキュリティ対策

利用者の皆様がお持ちのパソコンについても以下のようなセキュリティ対策をお願いします。

- ウィルス対策ソフトを導入し 、常に最新のウィルス定義ファイル（パターンファイル）に更新する。
- Windows や Office などソフトウェアは常に最新の修正プログラムを適用する。
- 自宅等でのネットワークへの接続では、ファイアウォールの設定などにより安全性の高い接続を確保する。

注意

お持ちのパソコンがウィルスに感染すると知らない間に多くの人に迷惑をかけます。管理責任を問われることもありますので、必ず十分なセキュリティ対策をしてください。

3.4.2. 個人情報の保護への注意

ネットワーク上での利用者ご自身や他人の個人情報、プライバシーに関わる情報の取り扱いには十分注意してください。

Web サイトなどで個人情報を入力する際には、十分に信頼できるサービス提供者であり、情報が安全に取り扱われることを確認してください。クレジットカード番号等の重要な情報をやりとりする際には、通信を暗号化する方式や、他人になりすましていないことを証明する機構を用いた安全な手段が取られているかどうかなどの確認をしてください。

電子メールアドレスを安易に人に教えたり、Web で公開したりすると、大量の迷惑メールやウィルスメールなどが送りつけられる可能性があります。一度迷惑メールが送りつけられるようになると振り分け以外に対処法はありませんので、不特定多数の人にメールアドレスを知られることのないよう、くれぐれもご注意ください。

教育用コンピュータシステムでは利用心得で「利用者は利用に際して、利用者本人の氏名を用いなければならず、他人の氏名または架空の人物の氏名を用いてはならない。利用者は、電子メールアドレスなど連絡方法を明示して利用しなければならない。」ということをお願いしていますので、サービスの提供者は慎重に選択してください。また、教育用コンピュータシステムにおける個人情報保護については「付録 -4.4.」を参照してください。

3.4.3. 著作物の適正な利用

コンピュータソフトウェア、音楽、映像、文章などは多くの場合、著作物として著作権法で保護されています。これらを利用する際には著作権についてよく理解し、適切な利用をお願いします。

- コンピュータソフトウェアなどの利用に関しては、利用者にどのような権利が許諾されているかを確認し、その範囲で利用してください。
- 著作物を著作権法での特例範囲を超えて複製することや、ネットワークからアクセスできる状態にするには、著作権者の許諾を得る必要があります。
- 論文などで他人の文章を著作権者の許諾を得ることなく引用することは、著作権法で一定の条件を満たす場合に限って認められています。定められた制限について十分に理解したうえで文章を作成してください。
- 他人の写真などの使用については、肖像権という考え方でその人の権利が保護されています。ご本人の了解を得るなど権利に注意した取り扱いをお願いします。

3.4.4. 犯罪や迷惑行為、性的嫌がらせなど

電子メールや Web を用いた詐欺などの犯罪や迷惑行為も多発するようになってきています。

- 日頃から危険性の認識に心がけてください。
- 犯罪や迷惑行為に巻き込まれたかもしれない、と思ったときには慌てず落ち着いて対応してください。
- 困ったことが生じた場合は自分だけで解決しようとせず、専門家などのアドバイスを受けるようにしてください。
- 性的嫌がらせなどについては、情報環境機構や各学部のハラスメント相談窓口に相談してください。

3.4.5. P2P 型ファイル交換ソフトの使用禁止

P2P 型ファイル交換ソフトは、P2P システムの一種として、接続されたパソコン間でファイルを互いに交換し、共有するシステムとして利用されていますが、著作権者に無断で著作物を広く共有する目的でも使われているため重大な社会問題となっています。

またP2P型ファイル交換ソフトウェアを狙ったウィルスによって、大量の情報漏洩の原因になっていることでも知られています。

そこで、学内ネットワークを管理する KUINS では P2P 型ファイル交換システムの使用に際し届出を行うよう求めています。教育用コンピュータシステムではこの届出を行いませんので、教育用コンピュータシステム内で P2P 型ファイル交換ソフトの使用はできません。

使用できないプログラムには以下のようなものがあります。

- Winny
- Share
- WinMX
- KaZaa
- eDonkey 及びその互換ソフトウェア (eMule など)
- Gnutella 及びその互換ソフトウェア
  (BareShare, LimeWire など)
- BitTorrent 及びその互換ソフトウェア
  (BitComet, cTorrent など , Opera の BitTorrent 機能や FireFox の AllPeers プラグインも含む)

また、これらに限らず、ファイルを広く公開する機能のあるソフトウェアを一般に禁止します。これらは現時点では教育用コンピュータシステムの PC 端末にはインストールできないようになっているものがほとんどですが、一部動作することがあるので注意してください。

3.4.6. ファイル交換ソフト以外の P2P システムの原則使用禁止

KUINS の規定では、ファイル交換目的以外の P2P システムは使用可能ですが、 教育用コンピュータシステムではその構成上、インターネットとの通信が全て中継サーバ (proxy) を介して行われるため、P2P システムを動作させると中継サーバが過負荷に陥り他の利用者に迷惑がかかる可能性があります。

そこで、Skype などファイル交換ソフト以外の P2P システムについても教育用コンピュータシステムでは使用を原則禁止します。

3.5. 情報セキュリティ e-Learning の受講

本学の全構成員には、情報セキュリティ e-Learning の受講が義務付けられています。次の URL を参照して受講してください。

http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/

詳しい受講方法は 51 ページの付録 -4.1. を参照してください。