第1章　JIU 学内情報関係施設の概要および利用上の注意

この章では、JIU 学内で皆さんが使用できる情報関係施設について紹介します。

1.1　東金キャンパス

1.1.1　PC 教室・情報関係教室

講義、演習、ゼミナールなどで使用する情報機器を備えた教室やセミナー室を紹介します。具体的には以下のとおりです。

・施設名：B206

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	50
Microsoft Windows 7 Microsoft Office 2013	
モノクロ・レーザープリンター	3

・施設名：B207

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	50
Mac OS X v10.8 (Mountain Lion) Adobe Creative Suite 6 Design & Web Premium Canon EDICOLOR 10	
カラー・レーザープリンター	2
スキャナ	25

・施設名：A202

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	20
Mac OS X v10.8 (Mountain Lion) Adobe Creative Suite 6 Master Collection BiND 6 他　サウンド系アプリケーション	

・施設名：A211

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	16
Microsoft Windows 7 Microsoft Office 2013 Canon EDICOLOR 10	
モノクロ・レーザープリンター	1

・施設名：C2-105

ハードおよびソフト名称	台数・個数
電源および情報コンセント、無線 LAN（Wi-Fi）	203
モノクロ・レーザープリンター	3

・施設名：A210

ハードおよびソフト名称	台数・個数
電源および情報コンセント、無線 LAN（Wi-Fi）	16

B303、B310、G1-101、G1-102、G1-302 教室にも情報コンセントを用意しています。LAN への接続は教員の指示に従ってください。

1.1.2　自習コーナー

情報科学研究センターでは、皆さんが自習のために自由に使用できる情報機器を用意しています。具体的には以下のとおりです。

・利用条件：平日および土曜日の 9 時～17 時(ただし、授業期間外は変更されることがあります。)

ハードおよびソフト名称、接続状況	台数・個数
パーソナル・コンピューター	8
Microsoft Windows 8 Microsoft Office 2013	
インターネット	
モノクロ・レーザープリンター	2

1.1.3　印刷

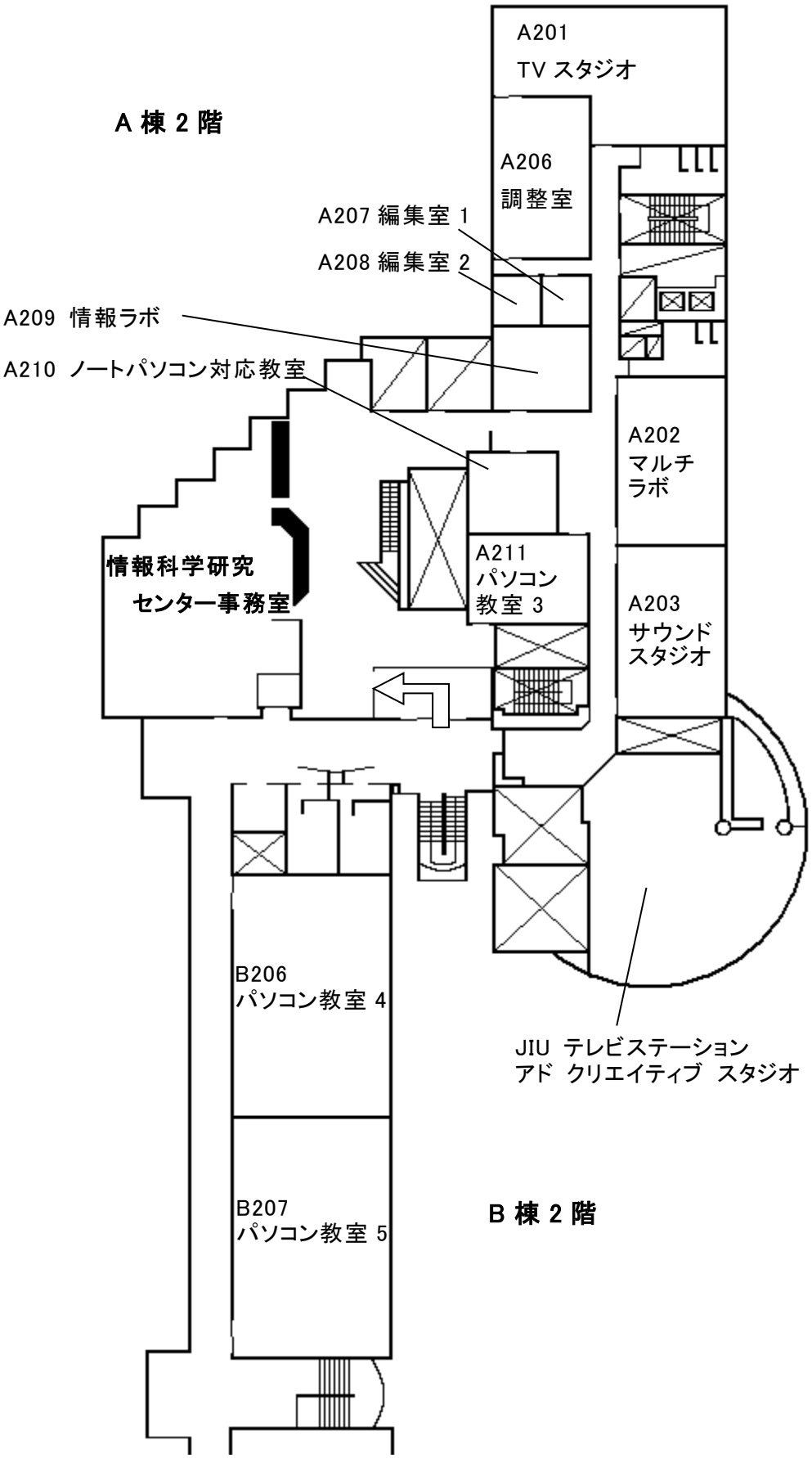
データを保存できるメディアを必ず持参してくだい。

レポート、卒業論文などの印刷は、情報センター内の印刷コーナーを利用してください。スタンド形式で印刷用 PC を設置しています。

なお、入力・編集はデスクトップ PC を利用してください。

また、情報センターカウンターにカラー印刷用 PC も設置しています（有料)。

東金キャンパス　情報科学研究センター



1.1.4　薬学部　医薬品情報実習室(L101 教室)

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	106
Microsoft Windows 7 Microsoft Office 2013	
モノクロ・レーザープリンター	6

1.1.5　水田記念図書館

水田記念図書館では、皆さんが自習のために自由に使用できる情報機器を用意しています。具体的には以下のとおりです。

【図書館メディアラウンジ】

・利用条件：平日 9:00～20:00、土曜日 9:00～17:00

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	60
Microsoft Windows 7 Microsoft Office 2010 Adobe Creative Suite Production Premium 5.5	10
パーソナル・コンピューター(印刷用)	1
モノクロ・レーザープリンター	1

また、ノート型 PC 用の情報コンセントも用意しています。具体的には以下のとおりです。

【図書館ネットラウンジ】

・利用時間時間：平日 9:00～20:00、土曜日 9:00～17:00

・電源および情報コンセント：60 個

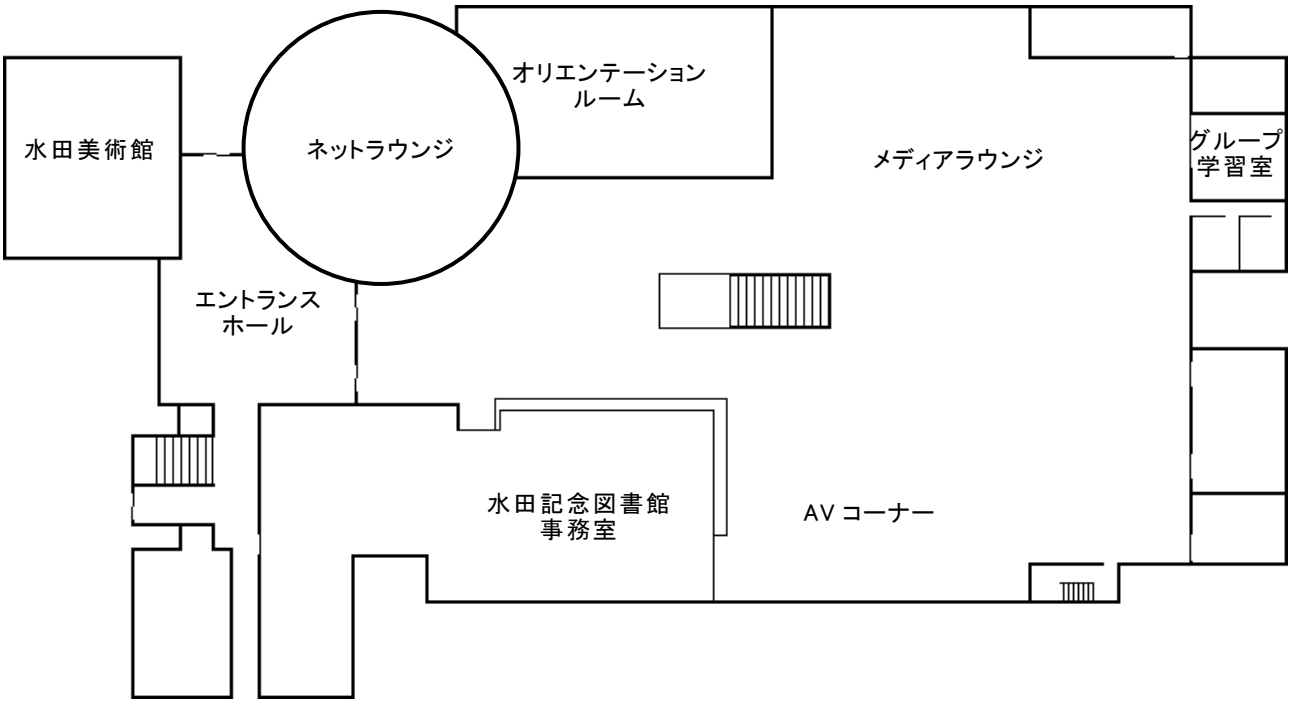
【図書館閲覧室(1～3 階)】

・ 利用時間：平日 9:00～20:00、土曜日 9:00～17:00

・ 電源および情報コンセント(座席)：212 個

・ 電源および情報コンセント(ブース)：16 個

水田記念図書館１階



1.1.6　その他の施設における情報機器の概要

学生ホール(A 棟および F 棟)には、ノート型 PC 用の情報コンセントを用意しています。

【学生ホール(A 棟)】

- 利用時間：7:30～21:00
- 電源および情報コンセント：50 個
- 無線 LAN（Wi-Fi）も使用できます

【学生ホール(F 棟)】

- 利用時間：7:30～21:00
- 電源および情報コンセント：4 個
- 無線 LAN（Wi-Fi）も使用できます

1.2　東京紀尾井町キャンパス

東京紀尾井町キャンパスには、以下の情報関係施設があります。

1 号棟

・施設名：4階　403 教室(PC 教室)

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	30
Microsoft Windows 7 Microsoft Office 2013 Microsoft Windows Vista Microsoft Office 2010 Microsoft Visual Studio Professional 2013	
モノクロ・レーザープリンター	1
カラー・レーザープリンター	1

・施設名：2階　メディアブース

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	16
Microsoft Windows 7 Microsoft Office 2013 Microsoft Windows Vista Microsoft Office 2010 Microsoft Visual Studio Professional 2008 勘定奉行 21 シリーズ Ver.Ⅳ	 2 2
モノクロ・レーザープリンター	1

3 号棟

・施設名：4階　41教室(PC 教室)

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	63
Mac OS X v10.8 (Mountain Lion) Adobe Creative Suite 6 Master Collection (Microsoft Office for Mac 2011)	

1.3　安房キャンパス

安房キャンパスには、以下の情報関係施設があります。

・施設名：A-201(PC 実習室-1)

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	44
Microsoft Windows 7 Microsoft Office 2013 BiND 6	
モノクロ・レーザープリンター	2
カラー・レーザープリンター	1

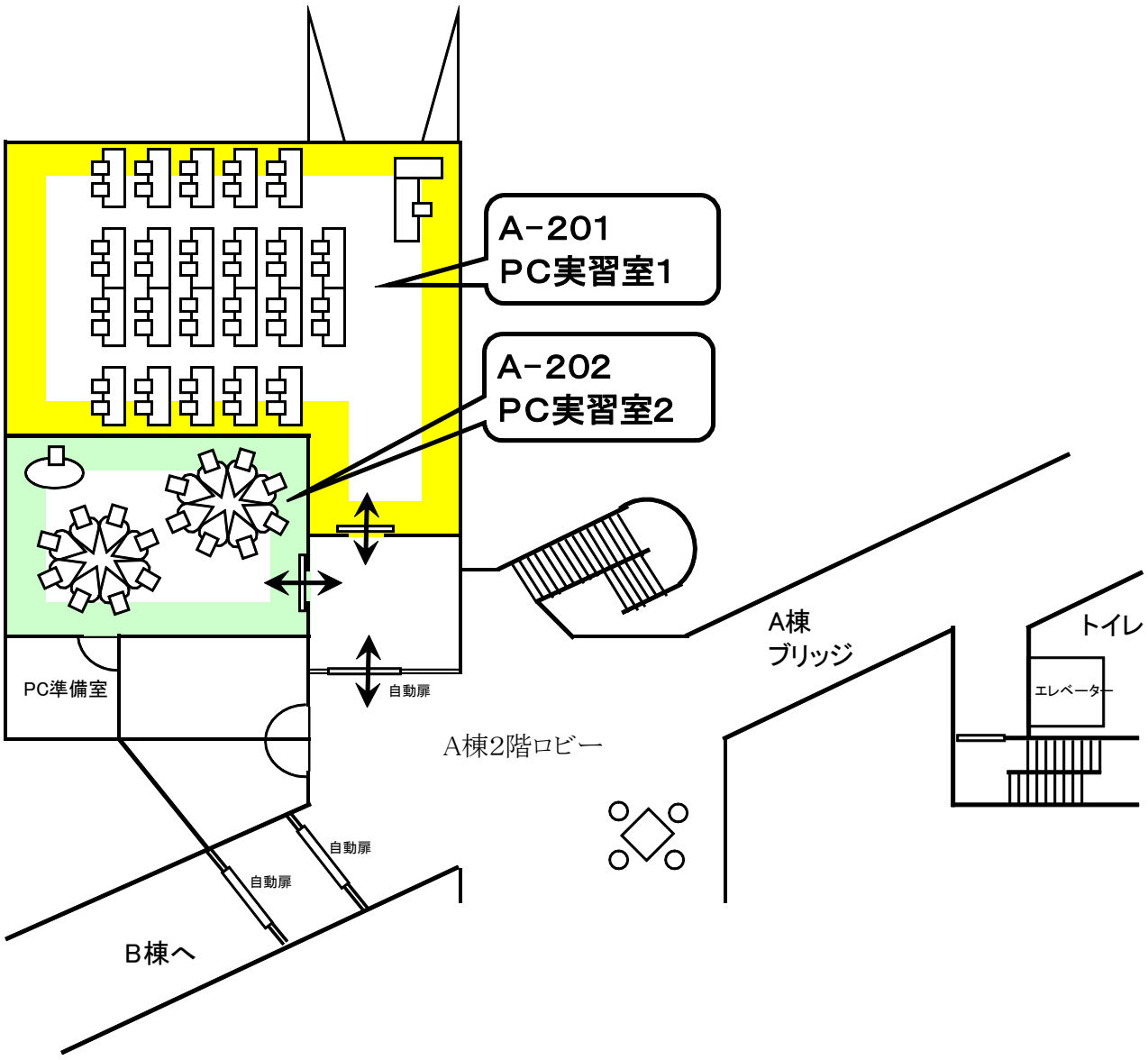
・施設名：A-202(PC 実習室-2)

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	16
Microsoft Windows 7 Microsoft Office 2010	
モノクロ・レーザープリンター	1

・施設名：図書館

ハードおよびソフト名称	台数・個数
パーソナル・コンピューター	14

安房キャンパス　PC 実習室



1.4　PC 教室利用上の諸注意

1. PC 教室での飲食は厳禁とします(持込も厳禁です)。
2. ソフトウェアのインストールは絶対にしないでください。動作不良の原因になります。
3. システムや画面の設定を変更しないでください。大学の PC は個人のものではありません。
4. データは必ず CD-R/RW や USB フラッシュメモリーに保存し、本体のハードディスクには保存しないでください。本体内に保存したデータは消去されます。
5. PC を終了するときは、決められた手順に従ってください。いきなり電源スイッチをオフにすると、故障の原因になります。
6. 印刷に失敗した用紙は放置せず、必ずゴミ箱へ捨ててください。
7. 自習中は、静かに利用してください。
8. PC を終了するときは、CD-R/RW や USB フラッシュメモリーを抜き忘れていないか注意してください。忘れ物は、学生課と PC 周辺機器の一部は情報センターで保管しています(一定期間を過ぎると処分されますのでご注意ください)。
9. 情報センターからの連絡事項は、入口の掲示板に掲示します。
10. PC を使用していて分からないことがあれば、情報センターまでお問い合わせください。
11. 携帯電話の使用は他の学生の迷惑となります。電源を切るか、マナーモードにしたうえで、通話は禁止とします。

1.5　インターネット利用上の諸注意

インターネットは大変便利で私たちの生活に欠かせないものになってきました。しかしその一方でネット犯罪や悪質ないたずらなどのトラブルに巻き込まれる危険性も高くなっています。インターネットとは世界中のネットワークが相互に接続しているもので、全体を管理している者は誰もいません。つまり全体としての管理者はいないのです。自己管理が重要だということを理解しましょう。以下にあげる点に十分注意して、正しくインターネットを利用しましょう。

事例：インターネットで「炎上」された学生

2007 年 9 月に、JIU の学生が mixi に書いた日記の内容がきっかけで、インターネット上での大きな騒動に発展する事件があった。その学生は、友人同士のやりとりのつもりで、mixi 上の日記に、隠語（仲間だけで通用する言葉、他の人が見ると全く別の意味になるものもある）を使って書き込みを行なった。彼の友人達は、その日記が隠語を使った冗談であり、日記の内容に問題はない事を知っていた。ところが、その内容は知らない人が読むと、法的に問題のある反社会的な行為をしたと読めるものであり、その日記を読んだ一般人が、ネット上で取り上げたため、大きな騒ぎとなってしまったのである。

インターネットでの「炎上」はスピードがとても速く、一晩のうちに日記を書いた学生の本名や所属するサークル、アルバイト先、さらには顔写真までネット上で探し集められ、「まとめページ」なるものが作られてさらされてしまった。学生は精神的ショックを受け、またアルバイトも止めることになるなど、実生活にまで重大な影響を受けることになった。

教訓：公共空間と私的空間

この事件から、次のような教訓を学び取ることが出来る。

- **ネット上は、基本的に誰もがアクセス可能な場所であり、仲間だけの世界ではない。**
- **ネットに書き込む情報は、一つ一つは大したものではなくても、つなぎ合わせると個人のさまざまな情報が分かってしまうものとなる。**
- **一度ネットで広まった情報や噂は、それが嘘であったとしても取り消すことは非常に難しい。**

インターネットの世界は公共空間（誰もが参加可能な場所）であり、仲間だけの世界ではない。友人とのいつもの会話の感覚でネット上に書き込みを行なうことは、非常に危険である。事例に挙げた学生以外にも、ネット上での不適切な発言が基で大問題となる例は多発している。**「送信ボタン」をクリックする前に、もう一度自分の書き込みを他人の気持ちで読み直し、問題がないか判断すること**が必要である。

資料：続発する「炎上」(読売新聞 2008 年 2 月 29 日朝刊 1 面)

［ネット社会］深まる闇(2)安易な発信、生活も「炎上」記事

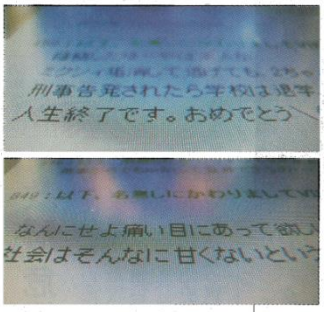
読賣新聞
2008年(平成20年) 2月29日 金曜日

ネット社会

深まる闇 2

安易な発信 生活も「炎上」

ご意見は、internet@yomiuri.comへ



高校生を非難する掲示板への書き込み(田中成浩撮影)

ゴキブリを揚げるなんて」と、「犯人」たちが始まった。ミクシィに公開したプロフィルや日記を手掛かりに、生徒の本名や学校がさらされた。同級生も参加、教室での様子も明らかにされた。

〈暗償金を払わせて、退学に追い込んだ。

〈(バイトしていた)ケン○ッキーでゴキブリ揚げてたムービー撮ればよかった〉

首都圏の私立高校3年の男子生徒が昨年12月上旬、会員同士が交流できる「ミクシィ」の日記にこんな一言を書き込んだ。

この一言は瞬く間にネット上に広がり、「飲食店でいたずらのつもりだったインターネットへの書き込みが、1人の高校生を自主退学に追い込んだ。

〈暗償金を払わせて、退学させよう〉〈そいつの人生をつぶせ〉

ネットの巨大掲示板「2ちゃんねる」には、こんな書き込みがあふれた。日本ケンタッキー・フライド・チキンは、ホームページで「事実無根」と釈明に追われ、高校には約100本もの抗議の電話がかかった。

父親は憔悴しきった生徒を連れ高校を訪れると、電話が鳴り響く事務室の奥で申し出た。「迷惑をかけました。退学させます」

書き込みは、ネット上で牛丼店の従業員が具を大盛りにしてふざけている動画が直前に出回り、騒ぎになった。同級生も参加、教室での様子も明らかにされた。

〈暗償金を払わせて、退学させよう〉〈そいつの人生をつぶせ〉

ネットの巨大掲示板「2ちゃんねる」には、こんな書き込みがあふれた。日本ケンタッキー・フライド・チキンは、ホームページで「事実無根」と釈明に追われ、高校には約100本もの抗議の電話がかかった。

父親は憔悴しきった生徒を連れ高校を訪れると、電話が鳴り響く事務室の奥で申し出た。「迷惑をかけました。退学させます」

書き込みは、ネット上で牛丼店の従業員が具を大盛り書き込みに批判が集中する「炎上」や「祭り」と呼ばれる現象が相次いでいる。

面白い話を書き込んで、より注目を浴びたい――。そんな思いが、過激な書き込みを生み、炎上や祭りにつながっていく。

「ネタに困り、つい誇張して書いてしまった」

ブログが炎上した経験を持つ首都圏の40歳代の男性は今も悔やむ。ブログを始めたのは2年半前。閲覧数に一喜一憂するようになり、帰宅すると真っ先に確認する習慣がついた。

炎上の原因は、受けを狙って大げさに書いた動物虐待の経験だ。ある日突然告発され、それまで数十件程度だった閲覧数は800件を超えた。すぐに無言電話がかかってくるようになり、掲示板には自宅や車の写真が公開された。「自分がどう書かれているか、見るのが怖い」と炎上後、ネットとは縁を切った。書いた内容は、「もう知られたくない」と話した。

ネットに書いた「ゴキブリ揚げた」といった話は、実生活の会話なら「くだらないこと言うヤツだ」などと軽蔑されるにとどまったかも知れない。

だが、ネットは違う。仲間だけが参加するSNSに書き込んでも、その仲間が別の掲示板に転載すれば、時間や場所を超えて広がっていく。仲間にだけ示したプロフィルも、すぐに見知らぬ人の手に届く。炎上に詳しいウェブコンサルタントの伊地知晋一さん(39)は「ネットは私室ではなく、街角や駅のような空間。不用意な発言や、職場・学校などの個人情報の公開は控えるべきだ」と警告する。

もちろん、言葉尻をとらえられての炎上も多い。確かなのは、誰もが自由に情報発信できる総放送局時代は、いつ自分が集中砲火を浴びるかも知れない危険と隣り合わせということだ。

詳しくは第 5.1 節の「城西国際大学学内ネットワーク利用基準」等を参照してください。

「インターネットの円滑な運用は利用者一人一人のマナーに負っています」

1. 注意深く行動しましょう。

誤った情報を人に送らないようにしましょう。インターネット上の情報はすぐに伝わるため、取り返しのつかないことになります。また、情報発信する際には、きちんと自分の名前をつけましょう。偽名を用いたり、嘘の情報で他人に被害を与えた場合は、当然刑事責任が問われる可能性があるので、このようなことは絶対行ってはいけません。しかしながら、初学者は内容を理解していないため問題を生じさせやすいものです。「知らなかった」では済まされません。利用者は利用資格を取得したときから利用行為について全責任を負うことが原則です。

2. 誤報に気をつけましょう。

誤った情報が提供されている可能性があることに気をつけましょう。いつもその情報が正しいと信じ込んでいては危険です。また、自分が発信する情報が他人に被害を与えるような虚偽や中傷的な内容がないか慎重になる必要があります。

3. 誰かがあなたのプライバシーを侵害するかもしれません。

トラブルに巻き込まれないようにプライベートな情報を提供する際には細心の注意が必要です。自分の住所や電話番号、またクレジットカード等の暗証番号をネットワーク上で打ち込む等の行為は、犯罪に利用される可能性があります。個人情報の提供も自己責任の範囲において行うことが大切です。

4. 善悪の区別をきちんと持ちましょう。

大学の共有施設を使って、社会的に問題のあるホームページへアクセスすることは当然ながら許されていません。猥褻画面等へのアクセスやショッピングなどを目的とした個人本位のネットワーク利用は大学のネットワーク利用規定や学則に抵触し、処罰の対象となります。ネットワークを利用するにあたり、善悪を判断することが個人に求められるので、十分な注意が必要です。

5. 著作権の侵害禁止

他人の文章をコピーして、さも自分の文章のように見せかける行為は禁じられています。これは明らかな著作権法違反です。つまり、事前の同意なしに、他の利用者が保有するファイルまたはデータを削除し、複製し、改変することは法律によって禁じられており許されていません。また、第三者の著作物であるファイルやデータの引用・参照をするときは、著作権法の規定および公正な慣行に従わなければなりません。また、他者の電子メールを許可なく読み、削除、複製、変造又は公開することも決して許されない行為です。パスワード管理はしっかりしましょう。

常に自分は城西国際大学の一員としてインターネットにアクセスしているという公共の責任をしっかり自覚して有意義にインターネットを利用してください。

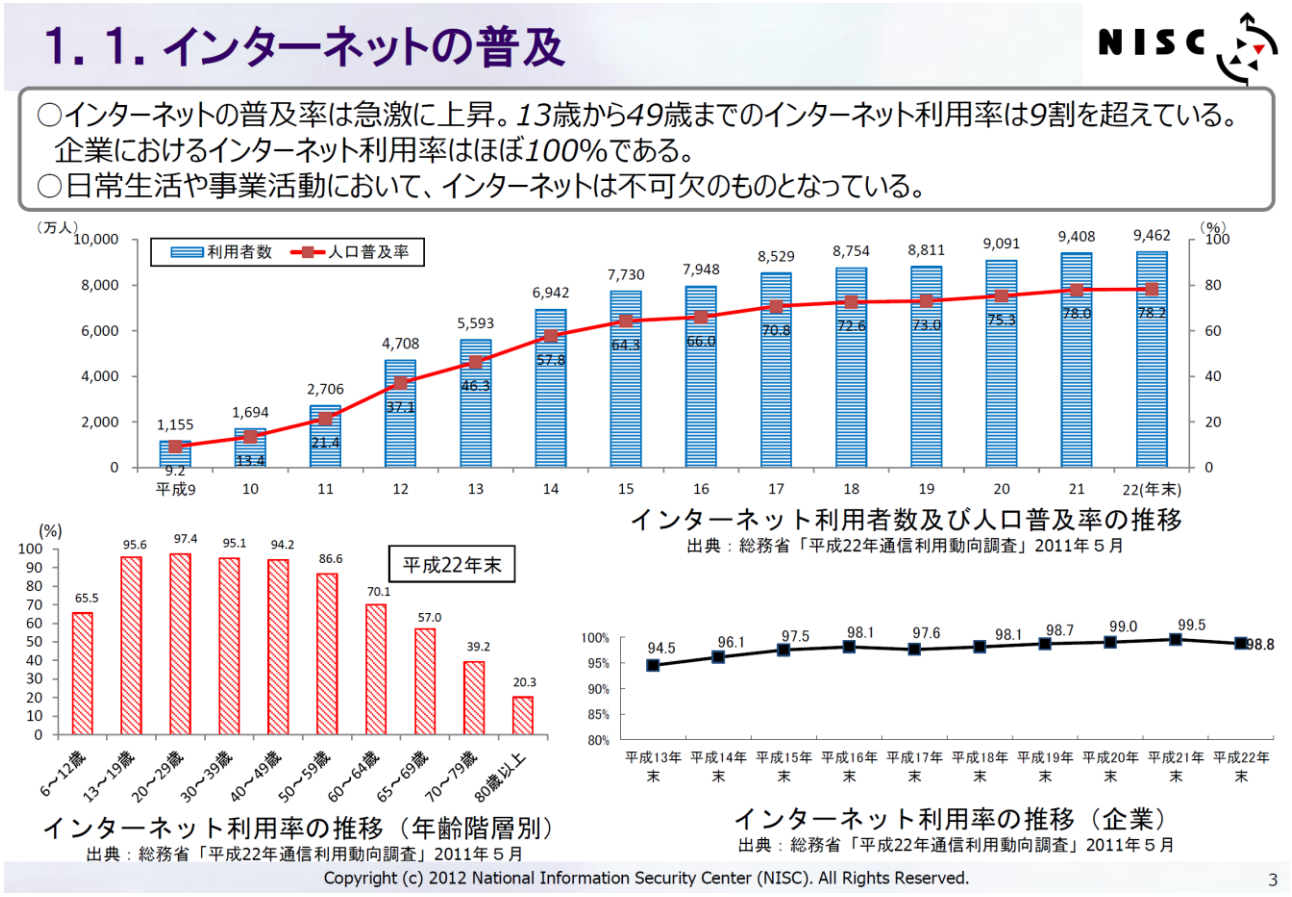
1.6　情報セキュリティを巡る状況

情報セキュリティとは、「パソコンやスマートフォン自身やそこにある様々な情報を守ることによって、その情報がだれかに勝手に使われてしまったり、その情報がだれかに勝手に変更されてしまうことを無くすとともに、あなたがその情報を利用したい時に利用できるようにすること」です。

パソコンやスマートフォンは生活を快適で便利にすることができます。ところが、ちょっとした不注意で、あなた自身やあなたのお友達などが辛い思いをすることがあります。そのような思いをしないよう、各自で必要な情報セキュリティ対策を講じましょう。

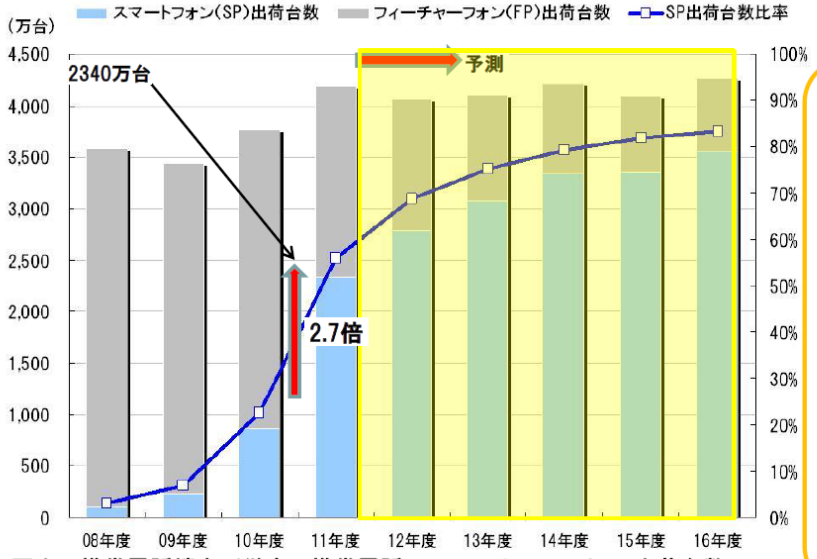
以下に内閣官房情報セキュリティセンター（NISC）がまとめた最近の情報セキュリティを巡る状況についてのレポートを引用して掲載しますので、情報セキュリティ対策の参考にしてください。

内閣官房情報セキュリティセンター（NISC）．“情報セキュリティ人材の必要性について”．
http://www.nisc.go.jp/security-site/glossary/nisc.pdf，（参照 2013-03-01）．



1. 2. スマートフォンの普及

○2011年度の国内のスマートフォン出荷台数は、*2340*万台であり、携帯電話端末総出荷台数の*55.8*%を占めている。今後さらにその比率は増加すると予想されている。
○スマートフォンはパソコンに近い機能を有しており、危険性は従来の携帯電話に比べて高く、より一層のセキュリティ対策が必要である。



国内の携帯電話端末（従来の携帯電話＋スマートフォン）の出荷台数

（出典）(株)MM総研ニュースリリース(平成24年3月13日)

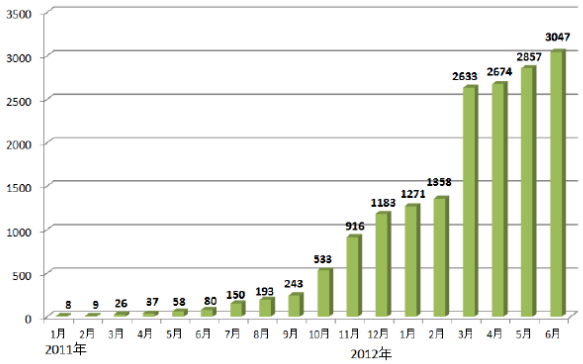
スマートフォンの特徴

- 携帯電話に比べて高機能で操作性が高い。
- パソコンのように様々なアプリケーションを利用したり、パソコンと同じウェブサイトを閲覧できる。
- 携帯電話に比べて利用者の個人情報等が集約される傾向にある。
- 多くの利用者が携帯電話と同レベルで安全であると認識しており、パソコン利用者と比較して情報セキュリティに対する意識が低い傾向にある。
- 全世界的に利用者が多い。
- セキュリティ対策ソフトの技術が発展途上である。
- マルウェア等の作成が容易なOSの利用が進んでいること等により、マルウェア等の開発者にとって、ローコスト・ハイリターンな攻撃対象である。

1. 3. スマートフォンを狙った攻撃

○スマートフォンを対象としたマルウエアが出現しており、その種類は増加傾向にある。現在、発見されているものは*Android*を対象としたものが大半であり、平成*23*年度後半に大幅な増加を示している。
○不正課金、管理者権限奪取、無断で電話を発呼、遠隔操作による通話の盗聴及びデータの窃取、利用者の電話帳に登録された個人情報の外部への送信、位置情報を無断で第三者に知らせるなどのマルウエアが確認されている。

Android端末に感染するマルウェアを検出するパターンファイル数



（出典）トレンドマイクロ(株)
「インターネット脅威マンスリーレポート - 2012年上半期・6月度」

マルウエアの最近の事例

発見年月	名称	OS	概　要	備　考
平成２１年１１月	ikee	iOS	Jailbreakしたiphoneに感染し、勝手に壁紙を変更するワーム。	
平成２２年８月	FakePlayer	Android	Androidを狙った初めてのマルウェア。ロシアのプレミアムSMSに勝手に送信する。	当該ＳＭＳには、ロシア国外からは送信できない。
平成２２年１２月	Geinimi	Android	Androidを狙った初めてのボットウイルス。インストール後、端末内の情報を収集し、サーバからの指令を待つ。	有料アプリケーションの海賊版に、このマルウェアを埋め込み配付。日本語版アプリケーションも存在。
平成２３年２月	DroidDream	Android	ＯＳのぜい弱性を突き、管理者権限を奪取するボットウイルス。起動時に、定期的にサーバと通信し、コマンドやアップデートを実行する。	有料アプリケーションに埋め込み、無料アプリケーションとして配付。Android Market（現Google Play）で提供するアプリケーションの中からも検出。
平成２３年５月	Lightdd	Android	アプリケーション起動なしに端末を監視し、着信や受信、通話の終了などの際に悪性コードを実行し、外部に情報を送信する。	Android Market（現Google Play）で提供するアプリケーションの中からも検出。
平成２４年１月	FakeTimer	Android	電話番号やメールアドレス等を外部に送信するとともに、これらの情報とともに架空の利用料金を請求するポップアップを画面に表示させる。	日本のワンクリック詐欺サイトで用いられ、アクセスすると動画を再生するアプリケーションと称して、端末内にインストールを促す。

（出典）総務省：スマートフォン・クラウドセキュリティ研究会　最終報告

1. 4. SNSの利用の本格化

○SNSの利用率は2012年末には50%を超えた。これに伴い、いままで想定されなかった問題も発生している。

2011年１月11日　都内ホテル

ホテルのアルバイト店員が、有名選手が女性タレントと来店したことを個人のtwitterで書き込み。総支配人が謝罪することとなった。

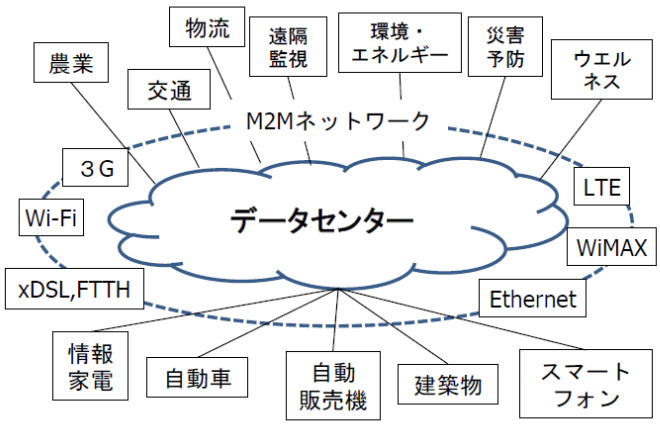
2011年５月19日　スポーツ用品メーカー

スポーツ用品メーカー新入社員が、直営店に来店したプロサッカー選手とその妻に対する中傷をFacebookに書き込み。本名や勤務店舗、顔写真も特定される。メーカーはホームページにて謝罪、本人は退職となった。

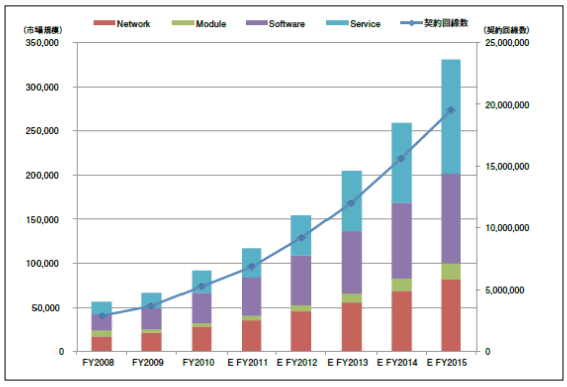
1. 5. M2M（Machine-to-Machine）環境の出現

○ネットワークに繋がれた機械同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるM2M（Machine-to-Machine）が出現。
○各種センサー・デバイス（情報家電、自動車、建築物、スマートフォン等）を、ネットワークを通じて協調させ、エネルギー管理、施設管理、防災、福祉等のサービスを実現するものが例として挙げられる。
○これらのシステムに繋がれる機器は、ネットワークに接続しないことを前提として設計されたものが多く、これらのセキュリティ対策が重要。

M2Mの概念図



カテゴリー別M2M市場規模予測（2008年～2015年）（単位 million yen）



（出典）株式会社ROA Holdings：日本国内M2Mマーケット市場展望2012

社会の幅広い分野でICTサービスの介在を意識せずその恩恵を享受できる環境の構築
○　従前はネットワークに未接続、クローズド前提のネットワーク構成　○　暗号化や認証機能が不十分

1. 6. 最近のサイバー攻撃等①（主な攻撃事例）

NISC

○最近の情報セキュリティに係る脅威は、ますます大規模化・高度化・複雑化してきている。
○最近の事例にみられるように、政府機関や民間企業に対するサイバー攻撃の脅威が現実化している。

最近の事例

2007.4	エストニア政府機関等への大規模なサイバー攻撃（DDoS攻撃(注1)）。 政府機関、報道機関、銀行等のウェブサイトが利用不能に。
2008.8	グルジア政府機関への大規模なサイバー攻撃（DDoS攻撃）。 政府機関、報道機関、銀行等のウェブサイトが利用不能に。
2009.7	米国、韓国政府機関等への大規模なサイバー攻撃（DDoS攻撃）。 米国のホワイトハウス、国務省等14サイト、韓国の大統領府、国会等21サイトが攻撃の対象に。
2009末	「ガンブラー攻撃(注2)」によるウェブサイト改ざん被害等が増加。
2010.7	イランの原子力発電所へのスタックスネットによる攻撃が判明。 その後、ウラン濃縮施設への攻撃も判明し、遠心分離機が全て停止。
2010.9	我が国政府機関等へのDDoS攻撃等
2011.3	韓国政府機関等への大規模なDDoS攻撃
2011.4	ソニー米国子会社のネットワークへの不正侵入。最大で7700万人分の顧客情報が流出。
2011.9~	三菱重工業、衆議院等への標的型攻撃によるウィルス感染発覚。
2012.4~	スマートフォンのアプリから、100万件を超える個人情報流出。
2012.6~	我が国政府機関等に対するウェブサイト改ざん及びDDoS攻撃。

（注1）Distributed Denial of Service（分散サービス妨害）

（注2）コンピュータウイルスによる攻撃の一種であり、一般企業のホームページに潜り込むことで、利用者に感染を広めていく攻撃手段を特徴とする。

※ 本資料は報道ベースで作成

1. 6. 最近のサイバー攻撃等②（直近の事例）

NISC

○サイバー攻撃や情報漏えい事件等は日々発生しており、不正アクセス、管理ミス、従業員の不注意などによる事故が報道されている。
○多くの事故は日頃の情報セキュリティ対策により防げると考えられる。

5月15日　英会話サービス

オンライン英会話サービスのネットワークシステムから受講生ら約11万人分の個人情報が流出した可能性があることが分かった。ウイルスが侵入し、名前やメールアドレス、英会話レベルなどを記録したサーバーにアクセスできる状態だった。

7月13日　飲料メーカー

飲料メーカーのキャンペーンに応募した顧客の個人情報が流出した可能性があると発表。約95000件の氏名や性別、メールアドレス、住所などが２月３日から７月５日まで、インターネットで閲覧できる状態だった。
個人情報の管理の委託先の担当者が個人情報のデータを個人使用パソコンに複製して保有。レンタルサーバへ移したことからインターネット検索でアクセス可能な状態になっていた。

7月20日　病院

都内の病院が、患者の個人情報を記録したパソコンなどを紛失したと発表。
病院の研修医が医局に個人所有のノートパソコンとＵＳＢメモリーを残したまま診療業務に出向き、医局に戻ったところ無くなっていた。

10月３日　大学

国内の５大学のサーバーがハッキングされ、教職員らの個人情報や研究リストなどが流出した。
大学は「サーバーの弱点を突かれた。甘い管理で申し訳ない。現在、再発防止策を検討している」とした。

⋮

※ 本資料は報道ベースで作成