

平成25年 9月25日(水)

コンピュータ利用者 各位

情報企画室ネットワークオフィス

## 金研でのコンピュータとネットワークの利用について

### 1. ネットワークの利用について

#### 1. 各種申請書とマニュアル

ネットワークオフィスのホームページ

<http://www.network.imr.tohoku.ac.jp/Jpn/index.html>

より入手できます。なお、申請書、マニュアルについては適宜、追加、修正されますので、できるだけ新しい書式を入手するようにお願いします。

#### 2. アナウンスメールについて

セキュリティ対策、OSのアップデート、ネットワークの利用停止、障害発生などを適宜メールでアナウンスしています。それらには目を通すようにしてください。

#### 3. メールアドレスの取得について

メールアカウント利用申込書に必要事項を記入して提出してください(今後はWebでの申請も行えるようにする予定です)。学生、研究生の方は原則1つになります。教職員については必要があれば複数発行します。

#### 4. コンピュータのOSをアップデートしてください

古いままのOSはセキュリティホールが残ったままの状態で使用されることとなりますので、適宜、OSのアップデートを行うようにしてください。マイクロソフトでは、日本時間の毎月第2水曜に月例のアップデートを公開しています。また、緊急の場合は不定期に公開されることがあります。Appleも不定期ですがアップデートを公開しています。

## 5. セキュリティソフトを必ず利用してください

サーバでもウイルスチェックは行っていますが、タイミングの関係でまれに新種のウイルスが通過することがあります。このような場合にパソコン側のセキュリティソフトが既に対応していると駆除されることがあります。また、ワームに感染したノートパソコンが持ち込まれ、パソコン間で感染が広がる場合があり、パソコン上でセキュリティソフトを使用していることが非常に重要になります。特にノートパソコンを移動して使用する場合は、ウイルスチェック機能だけでなく、ファイアウォール機能のあるセキュリティソフトの利用を推奨します。また、古いままのソフトをインストールしているだけでは意味が無いため、継続使用の手続き、日々のアップデート、定期的なディスクスキャンも実施してください。

## 6. Winny等のP2Pファイル交換ソフトの利用はできません

これについては大学全体で使用禁止と通知されています。関連した記述がありますので、第2章、第3章も参考にしてください。

## 7. 自動ダウンロードソフトの利用は禁止します

過去に、たった1台のパソコンで動かされた自動ダウンロードソフトによって、中継サーバの処理能力をはるかに超えた数の接続が同時に行われ、処理できずに、httpの通信ができなくなる事態が数度起こっています。特にThunder5.0というソフト(中国製)は過去に重大な通信障害を引き起こしましたので、金研内での利用は厳禁とします。

## 8. オンラインジャーナルの不正利用は禁止です

これについては、利用者は図書係から誓約書の提出が求められていますのでそれに従ってください。金研からの不正利用のペナルティとして、東北大学全体が利用禁止に至ることがあります。また、利用禁止中は当該ジャーナルを利用できないことで研究に支障をきたしますし、解除の手続きは、図書本館など所外の職員の協力も必要になるため、多くの方に迷惑をかけることとなります。なお、金研でオンラインジャーナルの不正利用が行われた場合、サーバの記録より研究室は容易に判明します。

## 9. ポスター印刷用B0プリンタ(図書複写室設置)の利用について

利用申請は、各研究室が使用予定の予算(振替可能な公費)毎になります。それに応じてIDとパスワードを配布します。利用者は基本操作(ロール紙の交換、インクの交換、ドライバの設定など)を習得していることを利用条件としていますので、研究室の代表の方に

毎年1～2度行う利用者講習会に参加していただき、研究室内で講習内容を説明し周知していただくことが必要になります。

平成25年度から稼動した新しいプリンタシステムでは、印刷したロール紙の面積で料金が決まり(ロール紙の幅は決まっているので、使用したロール紙の長さが目安になります)、B0サイズで約2200円/1枚として自動集計した金額が研究室毎に請求されます。そのため、前の利用者がPCからログアウトしないまま次の利用者が印刷したような場合は、ログアウトしなかった方の研究室の利用として請求されることとなりますので、**印刷が終了したら印刷用パソコンからログアウトしてください**。また、印刷ミスについては、ユーザーの設定等が原因の場合は請求対象となりますが、**プリンタシステムのトラブル等が原因の場合は、連絡していただければ請求から除外する**処理を行います。

#### 10. 迷惑メール、1度に多数宛のメールの送信は禁止します

1名の大量送信によって、それ以降、その組織にメールが一切届かなくなる可能性があります。また、一般公開されているブラックリストデータベースに登録されると、複数の組織からメールを拒否される事態になる可能性があります。金研および東北大全体の信用を損なう可能性がありますので、迷惑メールの送信と同等に判断される可能性のある行為は行わないようにしてください。

なお、国際会議や共同研究などで、1度に多数宛のメール連絡が必要な場合は、メーリングリストで送信することを推奨しますので、教職員の方はご相談ください。

#### 11. 金研のサーバは公共物です

個人毎のメール保存量は特に制限を設けていませんが、金研は人数が多いため、合計すると相当量のハードディスクが使用されています。また、この使用量が年々少しずつ増加している状態です。しかし、サーバ全体のハードディスク容量には上限がありますので、バックアップ代わりに長期間にわたってサーバにメールを残すユーザーが増えると、ハードディスクが圧迫されることとなります。そのため、

- 古いメールは定期的に削除する
- 不要なメールは削除する
- バックアップが必要な場合はパソコンに取り込んでからCD-RやDVD-Rに保管する
- すでに公開していないWebコンテンツ(画像など)は削除する

など、公共のスペースであるサーバのディスクを圧迫しないよう、ご注意をお願いします。特にIMAPクライアントやActiveMail!は、サーバにメールを残した状態でメールを管理しながら読んでいますので、そのようなメールソフトを使用している方はご注意ください。

## 公序良俗に反する目的でのネットワークの利用はできません

金研のネットワークの本来の利用目的は「研究活動」にあります。そのため、一部でもモラルの低下が起これば、その影響は利用者全体を制限することにつながります。節度ある利用を続けていただき、規制や制限が増えることがないように、お願いいたします。

## 12. 異動の際のメールの扱いについて

毎年、3月中旬～下旬にかけて、メールの継続利用調査を研究室毎にお願いしています。年度末で異動される方は、その用紙に新年度の廃止あるいは継続(継続期間も)、転送が必要な場合は転送先のメールアドレスを記入して、研究室毎にご回答ください。また、年度途中で金研を離れる方については、年度末の調査時に研究室の方に廃止と記入していただくか、在籍中にメールなどでご連絡いただければ退職、転出後に速やかに廃止の作業を行います。教職員で「研究や論文の問い合わせ等に必要でメールアドレスを残したい」という希望の方については半年を目安に期間を区切って継続利用を認めていますが、異動先で配布される新しいメールアドレスを周知し、早めに切り替えていただけますよう、お願いします。また、卒業学生の猶予期間は2ヶ月程度とと考えてください(大学、研究機関への就職で研究を継続される場合は相談してください)。サーバでのウィルスチェックソフトの経費は利用者数と単価で決まりますが、サーバに登録してあるユーザー数を元に判断しますので、異動された方も利用者として含めることになり、この経費は金研が負担することになります。

また、例年、メールアドレス廃止後でも所外のメーリングリストやメールマガジン等からメールが延々と送られ、エラーメールを発生させる方がいます。メールアドレス廃止予定の方は在籍中にメーリングリスト、メールマガジン等の退会、休止、登録アドレスの変更手続きを確実にを行い、絶対に登録したまま金研を離れることがないようにしてください。平成20年度より、このようなユーザーへの対処は所属研究室の責任で行っていただく方針とします。

## 13. SSH接続の利用申請について

SSHの申請は金研のメールアドレスを利用していることが条件になります。必要な方は公開鍵をメールに添付して送付してください。なお、上記URLから得られるマニュアルで暗号が強固でセキュリティの高い「SSH2プロトコル+DSA暗号の鍵ペア」を作成、使用方法を説明しています。マニュアルは適宜修正されますが、作成方法が不明な場合はご相談ください。

#### **14. 固定IPアドレス、グローバルIPアドレス機器の設置について**

教職員名でのネットワーク利用申込書の提出が必要です(学生の申請は不可)。特にグローバルIPアドレス機器については、管理にセキュリティやサーバ管理の知識が必要になり、申請者よる管理が適切になされることが前提になります。なお、グローバルIPアドレス機器の設定不備が原因で、第三者による不正侵入や外部への攻撃などが発生した場合、利用を停止していただくことになります。

#### **15. 無線LAN機器(アクセスポイント、ルーター)の設置について**

教職員名での無線LANアクセスポイント接続申請書の提出が必要です(学生の申請は不可)。無届設置と暗号化の無い状態での運用は禁止します。なお、情報漏えい防止、盗聴防止のため、接続申請書に記載されている内容を逐一確認しながら、無線LAN機器を適切に設定していただく必要があります。

#### **16. ファイアウォール(F/W)装置の調整依頼について**

業務上、所外と所内のパソコンを直接通信させる必要がある場合は、当該研究室から必要な通信ができるようにF/W装置の調整を行うことも可能です。ただし、設定に際してヒアリングが必要になりますので、先にご相談をお願いします。その際に依頼書及び同意書をお渡しますが、作業にあたっては、部門担当教員名での依頼書と実際の利用者名での同意書の提出が必要になります。実際の利用者が学生、研究生の場合は指導教員名での提出をお願いします。なお、金研のネットワーク全体に危険を及ぼす可能性があるため検討のうえ許可されない場合や接続先の運用ポリシーのため金研側の調整だけでは接続できないということも考えられます。この点をご理解ください。

## 2. ソフトウェア使用条件の遵守に関する点検のお願い

これまでにいくつかの国立大学法人において不正コピーソフトウェアの利用が発覚し問題になってきました。このような行為が所内で行われた場合、知的活動を担う金属材料研究所および東北大学の信用が失墜するのはもちろんのこと、多額の損害賠償等、非常に厳しい処分が下されることが予想されます。そのためにも、ソフトウェア使用条件やライセンスに関しては、十分に注意のうえ、使用可能な範囲内で利用するようにお願いいたします。

### 1. ライセンス番号とパソコンの対応表を作成して管理する

公費で購入したパソコン、ソフトウェアについては、以下のような対応表を作成し、1つのソフトウェアが2台にインストールされ、不正に使用されていないかを管理、確認できるようにしておく利用状況を把握しやすいと思います。

	パソコン1	ノートパソコン2	パソコン3	パソコン4
ソフト1	111AAAA	未インストール	未インストール	未インストール
ソフト2 注1	S333333	S333333	未インストール	未インストール
ソフト3	未インストール	未インストール	D123456	未インストール
ソフト4	未インストール	未インストール	未インストール	G444444

注1 同一人が使う場合にかぎりデスクトップとノートパソコンに入れられるソフトウェア (MS Officeなど)

記号数字はシリアル番号、ライセンス番号等を示す

### 2. ライセンス条項を確認する

ライセンスの形態は様々ですので、使用する場合は必ず条件を確認してください。以下のような場合があります。

- (1) パソコン1台につき1ライセンスが必要なもの
- (2) 1つのパッケージで同一人物に限りデスクトップとノートPCの2台で利用できるもの
- (3) (2)と同様だが「同時使用を認めない」と明記のものや逆に「インストール可能な台数が明記されていないもの」もありますが、基本的に一人で1ライセンスが必要なもの
- (4) 自宅、職場、ノートパソコンと同時に使わなければ3台まで利用できるもの

### 3. パソコン単位の管理か人単位の管理かを考える

2でも述べましたが、使用者単位でライセンスを管理する場合、特定の1名だけが使用する限り複数のパソコンにインストールすることが可能なソフトウェアでも、研究室の共有パソコンにインストールして複数ユーザーが共用して使用する場合、研究室共通のデスクトップとノートパソコンに1つのライセンスでインストールすることはできないことがあります。この二つの管理を混同しないように、共有パソコンに関しては1台に1ライセンスとすることが必要です。

### 4. OpenOffice.orgなどフリーソフトウェアやStudentソフトなどの活用

学生さんが多数いる場合はソフトウェア代金もかかります。そのような場合、凝ったドキュメントの作成でなければ、MS Officeの代わりにフリーのOpenOffice.orgを使用することもできると思います。また学生が個人で購入するStudentソフトウェアは格安ですので、研究のための必須の道具として購入させる事も良い方法です。ただしStudentソフトウェアはアカデミックディスカウントのように研究室で購入して他の学生に受け継ぐ事は出来ない点に注意が必要です。

### 5. 古いソフトウェアに関しても注意する

アップグレードライセンスで新バージョンアップした場合、通常は旧バージョンを他の人に使わせるといった事は禁止されています。またネットワークでの登録など不正防止策が施されていない古いソフトウェアに関しては十分に注意しないと、意図しない不正使用になっていることがあります。

### 6. ソフトウェアの持ち出しに関して注意する

訪問者や短期滞在者、学生などの転出や卒業に当たっては、研究室の公費で購入したソフトウェアを様々な事情で個人のパソコン等で使用していた場合、インストールメディアの複製の所持やパソコンからのアンインストールを確実に確認する事が必要です。知的財産権に関する重要性が十分に理解されていない場合もありますので、折に触れて啓蒙することが求められます。

## 7. ネットワークライセンスやマルチユーザーライセンス利用を導入する

最近ではパソコンも安価になったので一人で複数所有することや、装置に接続したパソコンが増える等、研究室の教職員、学生の数よりパソコンの数の方が多い場合もあります。そのようなときに1台に1ライセンスを導入するのは実態に合わない事になります。このようにとき、同時使用数の制限がついたネットワークライセンスやマルチユーザーライセンスを用いれば実質的に使う人間の数だけライセンスを買うことになり結果として得になることがあります。

## 8. Winny等のファイル交換ソフトウェアの排除

Winny等のファイル交換ソフトウェアに関しては、情報流失やウイルス蔓延あるいは不正利用対策の面から問題があります。法的には議論があるところもありますが、研究室の公的な活動では用いない、所内のネットワークでは使用しないとといった点に関して注意を徹底してください。

## 9. 音楽ソフト、映像ソフトの不正コピーも犯罪行為です

不正にファイルをアップロードする行為は著作権法に触れます(公衆送信権侵害)が、不正なファイルをダウンロードする行為は、**大学という公共の場所で認められる行為ではありません**。また、金研のサーバを利用して不正なファイルと公序良俗に反するファイルを不特定多数にダウンロードできるようにすること、および、サーバを利用して金銭の授受を伴う行為は、大学のサーバ利用という点からは認められません。もし、このような行為を発見した場合はペナルティが課されることになりますので行わないように注意してください。



### 3. 情報の管理のためのチェックリスト

ネットワークを通じた情報の流失が最近問題になっています。それを防ぐため、チェックすべき内容をリストにまとめました。各自の点検をお願いします。

#### 1. “管理すべき情報とは何か”を意識し、考えていますか？

成績、試験問題、人事や評価など個人情報を含む書類、名簿、メールアドレスのリストなど“管理すべき情報とは何か”を考えて、一般の情報と区別する事がまず必要です。特に業務を行う部門では管理すべき情報に関するガイドラインを作ることが必要です。

#### 2. 公私の区別をきちんとしていますか？

出張や仕事で外部にパソコンを持ち出すことは避けられません。そのため、パソコン使用時は公私についてきちんと線を引いておかないと情報流失のリスクは高くなります。漏洩して困る情報は自宅や私有のパソコンで扱わないようにしましょう。

#### 3. 重要な情報をハードディスクに入れっぱなしにしていませんか？

日頃きちんと管理していても思わぬ事故や盗難で重要な情報が流失することもあります。本当に重要な情報は不用意に持ち歩かない事が大切です。例えば CD-R 等に保存し鍵をかけて管理する、所内の安全なサーバに入れておくなどしてください。また不要になった情報はこまめに消去する事も大切です。

#### 4. パソコンの OS は最新の状態になっていますか？

どんな OS でも、日々手法が進化する外部からの攻撃に耐えるためには日常的なメンテナンスが必要です。常に最新の状態にアップデートすることで、セキュリティの穴を作らないようにしましょう。

#### 5. ウィルス対策をしていますか？

所内ではメールに添付されたウィルスが侵入しないように常にサーバが監視をしていますが、所外のネットワークに繋いだ時に感染したノートパソコンを経由して所内にワーム、ウィルスを持ち込まれた事があります。そのようなことを防止するため、ウィルス対策ソフトで常にチェックを怠らないようにしてください。高機能のセキュリティソフトを購入して使用

するのが最善の方法ですが、ウイルスチェックのみならば、学内での利用という制限はありませんが、情報シナジーセンターがウイルス対策ソフトを提供しています。

<http://www.tains.tohoku.ac.jp/index-j.html>

#### **6. セキュリティを安全教育の一環として教育啓蒙をしていますか？**

事故を防ぐために安全教育が必要なと同様、セキュリティの欠陥による情報流失を防ぐには、セキュリティに対する教育を研究室や部署で行いましょう。

#### **7. パソコンにパスワードを設定していますか？**

パソコンにパスワードを設定していなければ、席を離れた際に他人が情報を見ることが可能になります。パスワードは必ず設定しましょう。外のパソコンで Web メールを読んだ時にパスワード等が記憶されている事があります。必ず消去するように気をつけましょう。特にインターネットカフェなど不特定多数の人が利用するパソコンで Web メールを利用することはやめましょう。キーロガー等による ID、パスワードの流出の危険があります。(キーロガー:パスワードや ID、カード番号等を盗むソフト)

#### **8. そのパソコンは LAN に接続する必要はありますか？**

計測に使用するパソコンなどは OS を変えられないものもあります。LAN に繋がなければ情報流失の危険性はかなり減少します。LAN に接続する必要性をよく考えましょう。

#### **9. メールで大事な情報を送っていませんか？**

メールは大変有用ですが、ちょっとした間違いで無関係な相手に送信する事が起こります。また、返信の際にそのまま送ると、内容によっては送るべきではない相手を含んでいることもありますので”全員に返信をする”のような返信方法を標準設定にすることは避けられた方が無難です。メールを送る前にもう一度宛先をチェックしましょう。メールを使うべきでない情報は電話、FAX 等の手段で伝えることも検討しましょう。

#### **10. ファイル共有を意識していますか？**

ファイル共有は大変便利ですが、意識して管理しないと、誰もがあなたのパソコンの中を覗き見できるようになっているかもしれません。ファイル共有は必要性和範囲をよく考えましょう。どうしても必要なときはパスワードが必要になるように設定しましょう。

### 11. 使用している無線 LAN は安全ですか？

無線 LAN は盗聴されるおそれがあります。最低限でも WEP キーを使った暗号化を行いましょう。また、使用者や使用するパソコンが決まっている場合、MAC アドレスによる接続制限を行いましょう。なお、WEP はそれほど暗号が強くないため、より暗号強度が高い方式が選択できる場合はそちらを使う方がさらに安全です。

なお、金研では、無線アクセスポイントと無線ルーターについては、WEP キー等の入力無しに利用可能な運用と届出無しの設置は禁止しています。

### 12. 携帯できるメディアの管理は万全ですか？

携帯に便利な USB メモリや CD-R 等は紛失による情報流失の危険性が高いので、管理は適切に行いましょう。また、重要な情報の入った FD、CD-R、DVD-R、MO、ハードディスクを廃棄する場合は、第三者に情報が読み取れないように完全に破壊しましょう。ハードディスクについては、内容を完全に削除するソフトを金研全体で利用可能なライセンスで購入していますので、ご連絡いただければ貸し出します。

### 13. Winny のようなファイル共有ソフトを使っていませんか？

独立行政法人 情報処理推進機構セキュリティセンターの解説が詳しいのでよく読んでください。

[http://www.ipa.go.jp/security/topics/20060310\\_winny.html](http://www.ipa.go.jp/security/topics/20060310_winny.html)

なお、東北大学では本部より通達があり、Winny 等のファイル交換ソフトの利用は認められていません。