2017年度　コンピュータガイダンス

コンピュータ相談室　日高

本日のテーマ

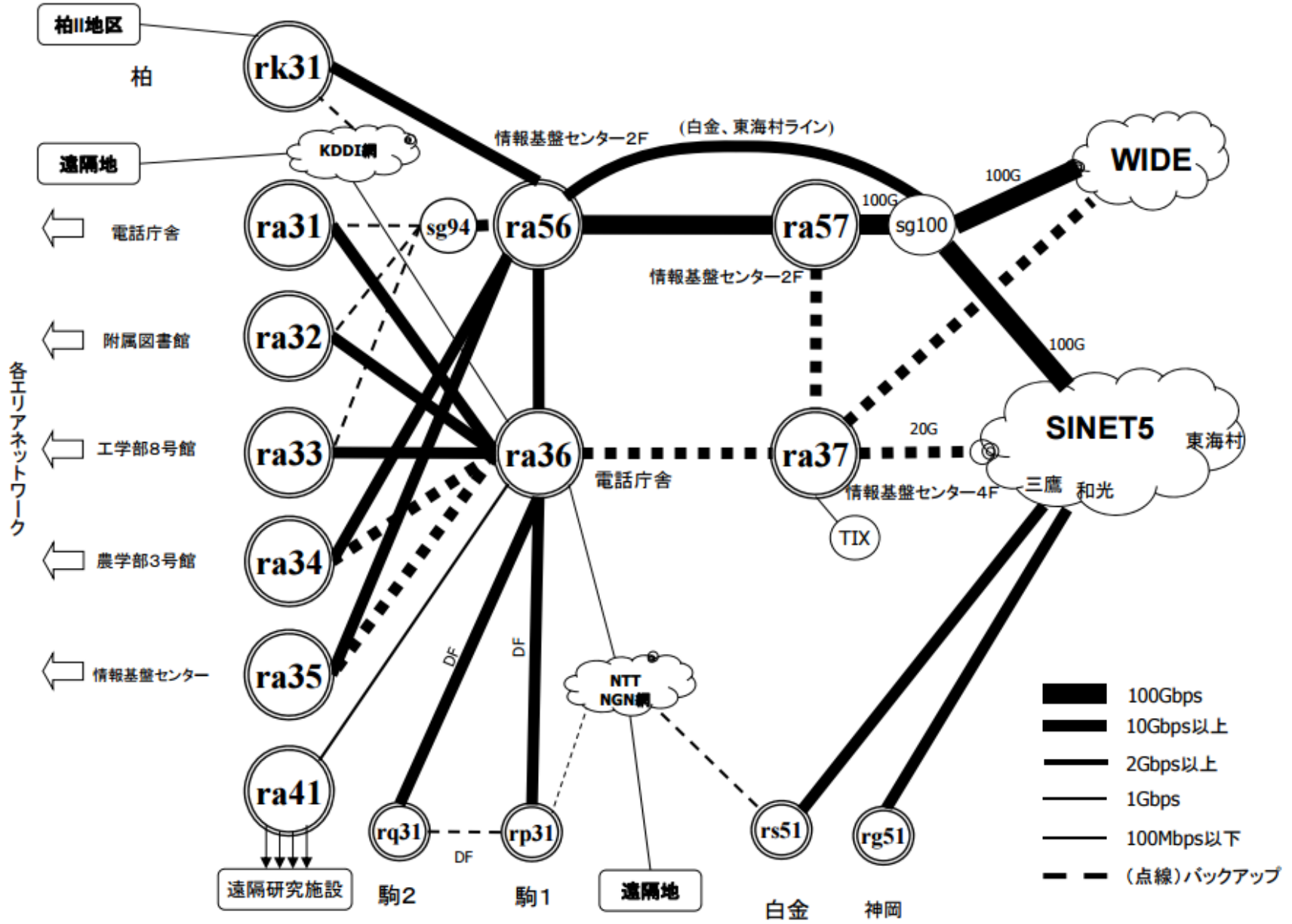
- 1. 教育学部のネットワーク環境／情報倫理・コンピュータ利用ガイドライン／セキュリティ・ポリシー　（学部・大学院）
- 2. コンピュータ／スマホ／タブレットをネットワークに接続する　（学部・大学院）
  - (1) Utokyo WiFi編
  - (2) UTnet編
- 3. UTokyo Microsoft License（個人所有PC／大学所有PC）　（学部・大学院）
- 4. セキュリティ対策　（学部・大学院）
- 5. メールを読む　（大学院）
- 6. サーバにログインする　（大学院）
- 7. メールを転送する　（大学院）
- 8. メーリングリストを開設する　（大学院）
- 9. ホームページを公開する

この資料は「学部内限定ページ」または下記URLからダウンロードできます。
http://www.p.u-tokyo.ac.jp/local/index.html
http://www.p.u-tokyo.ac.jp/~hidaka/guidance/ComputerGuidance2017.pdf (cg2016 / 21235)
http://www.p.u-tokyo.ac.jp/~hidaka/guidance/ComputerGuidance2017.pptx(cg2016 / 21235)

1. 教育学部のネットワーク環境／情報倫理・コンピュータ利用ガイドライン／セキュリティ・ポリシー （学部・大学院）
2. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
   (1) UTokyo WiFI編
   (2) 教育学部LAN編 （学部・大学院）
3. UTokyo Microsoft License（個人所有PC／大学所有PC） （学部・大学院）
4. セキュリティ対策 （大学院）
5. メールを読む （大学院）
6. サーバにログインする （大学院）
7. メールを転送する （大学院）
8. メーリングリストを開設する
9. ホームページを公開する

UTNET4構成図

2017.3.31

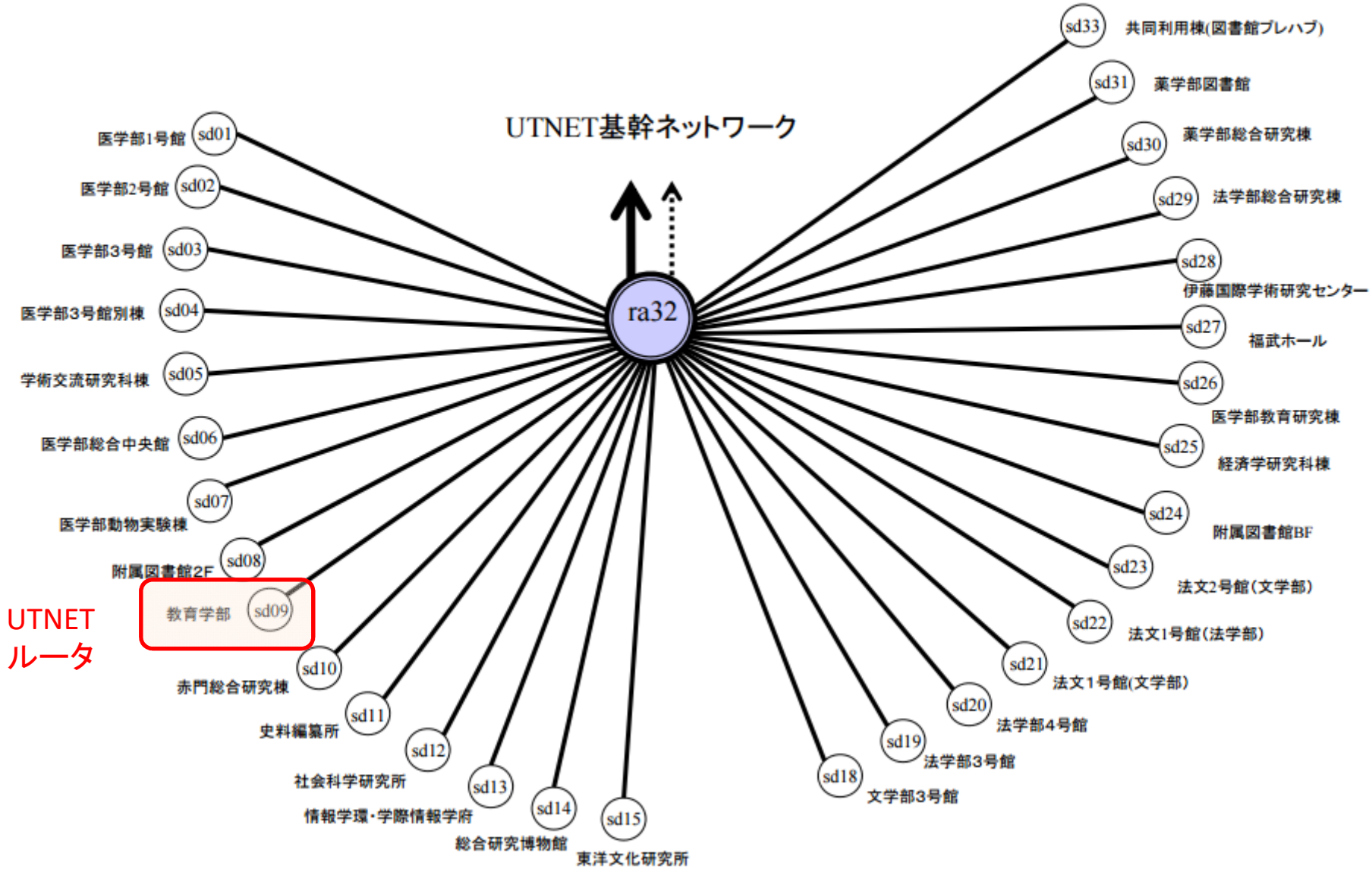


https://www.nc.u-tokyo.ac.jp/guide/topology

附属図書館HUBサイトエリア

2017.2.14

100M以下
1G
10G



教育学部LAN

sd09

UTNETルータ

フロアスイッチ

B1F～4F

各研究室情報コンセント

ハブ

有線

DHCPまたは
固定アドレス

無線AP

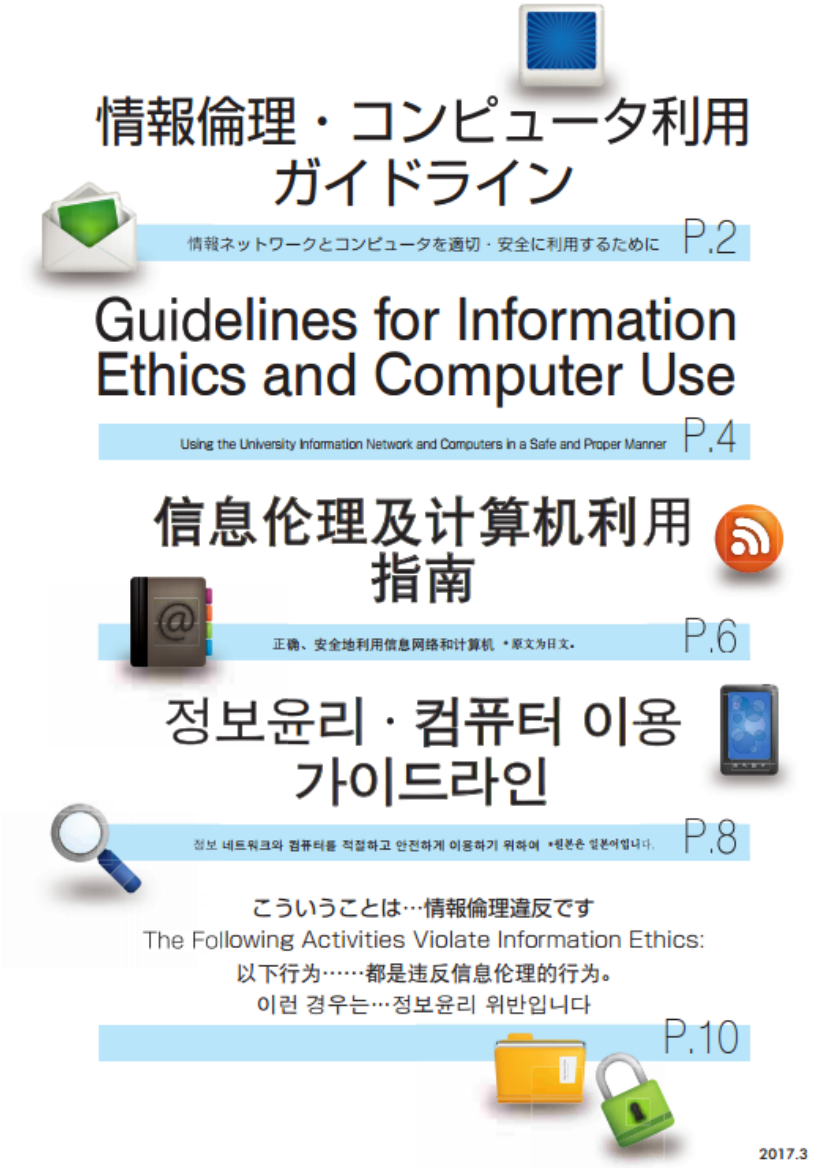
グローバルまたは
ローカルアドレス

各研究室で管理

教育用計算機システム
(ECCS)

UTokyo WiFi

大学のネットに繋ぐ、その前に…



http://www.cie.u-tokyo.ac.jp/guidelinepanf.pdf

本学の計算機資源（情報ネットワークとコンピュータ等）の利用に当たって、以下の点に注意を払い、利用者として自覚と責任を持って行動して下さい。これらに違反した場合、注意や処罰の対象になります。また、学外活動や私生活においても、本学の学生や教職員として良識と節度ある行動をお願いします。

①教育・研究目的に限定

本学の計算機資源の利用は、**教育・研究に関する目的に限定されています。**この目的に沿わない不適切な行為、違法行為、倫理に反する行為を禁じます。

②不適切な情報発信・公開の禁止

本学の計算機資源から、以下のような情報を発信または公開することは禁止されています。

(1) 本名以外（匿名・偽名）による情報
(2) 知的財産権・肖像権を侵害する情報
(3) **差別・誹謗中傷にあたる情報**
(4) プライバシーを侵害する情報
(5) わいせつな情報
(6) 教育・研究を妨害する情報
(7) 他者の業務・作業を妨害する情報
(8) 虚偽の情報
(9) 守秘義務違反にあたる情報

③違法コピーの禁止・違法コンテンツのダウンロード禁止

音楽、映像、本、ソフトウェアなどの著作物を、違法にコピーして配布したり、ライセンス規約を守らずに利用してはいけません。これらを、P2P 型ファイル共有ソフトウェア等を用いて、他人に配布できる状態にすることは違法です。多くの P2P 型ファイル共有ソフトウェアでは、データをダウンロードした端末が**自動的にそのデータの発信者になるため**注意が必要です。また、違法に配信されている音楽・映像コンテンツを、それと知りながらダウンロードすることは違法であり、**刑事罰の対象**となる場合もあります。P2P 型ファイル共有ソフトウェアは教育・研究上どうしても必要である場合以外は使用しないようにしましょう。本学では違法行為や不適切な利用の可能性がある通信を監視しており、疑わしい場合は調査しています。

④大量ダウンロードの禁止

本学から「自由に」使って良いように見えるサービスでも、東京大学とサービス提供元との間で利用条件が定められているのが普通です。例えば、多くの電子ジャーナルやデータベースでは、コンピュータプログラムなどを利用して一度に大量のコンテンツをダウンロードすることは禁じられています。利用条件を守らない者がいると、東京大学全体に対するサービスが停止される可能性がありますので注意して下さい。

⑤アカウントの盗用・貸与の禁止

パスワードを推測するなどして、他人のアカウントを盗用することは犯罪となります。また、全ての利用者には、自分が保持するアカウント、パスワード、情報機器、ソフトウェア等を安全に管理する義務があります。他人に自分のアカウントやコンピュータを悪用されると、所有者自身が困るだけでなく、見知らぬ第三者や大学全体に迷惑がかかります。また、自分の代わりにレポートを提出してもらう、または業務を一時的に代行してもらうなどの目的で、自分のアカウントを他人に貸与することは決してしないで下さい。

⑥簡単なパスワードを使用しない

コンピュータが悪用される原因のひとつはパスワードが推測されてしまうことです。特に危険なものは、名称、単語、数、それらの組み合わせ、キーボードの配列、短いものなどです。アルファベット大文字、小文字、数字などを組み合わせた意味のない文字列を利用して下さい。パスワードは記憶するか、それができない場合は他人に盗まれない工夫をして厳重に保管して下さい。また、**パスワードは使い回しをせず**、システムやソフトウェアごとに使い分けて、慎重な管理に努めて下さい。

⑦情報機器の盗難や紛失に注意

ノートパソコン、スマートフォン、タブレット、ハードディスク、USB メモリなど、重要な情報が入った情報機器の紛失と盗難に注意して下さい。盗難による被害は本学でも数多く発生しています。教室や食堂など不特定多数が出入りする場所は特に危険です。本学のシステムのアカウントやパスワードが入った情報機器を失った場合、速やかにその発行元に連絡して下さい。

⑧ウイルス対策の徹底

全てのコンピュータには、最新のウイルス対策ソフトウェアをインストールして下さい。本学では、ウイルス対策ソフトのライセンスが情報基盤センターから各組織（部局や研究室など）に有償配布されています。利用者は自分が所属する組織からライセンスを入手してください。ウイルスのパターンファイルは自動更新して最新版に保ち、定期的にコンピュータ内の全ファイルのウイルスチェックを行って下さい。しかし、ウイルス対策ソフトを導入しても、それだけで全てのウイルスを完全に防げるわけではありません。安心せずに常に感染の危険を避けることを心がけてください。USB メモリなどをコンピュータに接続した際には、最初にウイルスチェックを行って下さい。
学内連絡や取材申し込みなど、**正当な内容を装った悪意のあるウイルスメール**が増えています（標的型攻撃）。メールの添付ファイルやメール本文の外部リンクから、ウイルスに侵入されないよう注意して下さい。

⑨ソフトウェアを最新の状態に

オペレーティングシステムやアプリケーションは常に最新版にアップデートして下さい。自動更新ができるソフトウェアは、その機能をオンにして下さい。最新でないソフトウェアを利用していると、ウイルス感染等のセキュリティ問題が容易に発生します。また、製造者のサポートが切れたソフトウェアは、セキュリティ問題が発見されても修正されないため使用を控えて下さい。

⑩長期間不在にする場合は端末の電源をオフにする

長期休暇や出張などにより数日間以上コンピュータを利用しない場合、セキュリティならびに省エネの観点から、必ず電源をオフにして下さい。再び利用する場合、作業を開始する前にソフトウェアやウイルス対策ソフトウェアのパターンファイルを最新版に更新して下さい。

⑪もしも注意を受けたら

教職員やネットワーク管理者から注意や指示を受けた場合、その内容に速やかに従って下さい。ウイルスに感染したままコンピュータを利用し続けたり、不適切な利用を継続してはいけません。

規則・コンプライアンス

東京大学情報セキュリティ・ポリシー

1 情報セキュリティの基本方針
東京大学が、高度に情報化した21世紀世界において十分な学術研究・教育活動を行い、人類に対するその使命を全うするためには、情報基盤の整備をするのみならず、東京大学保有の情報資産の情報セキュリティを確保することが必要である。東京大学情報セキュリティ・ポリシーは、情報セキュリティを確保するために必要な取り決めを明文化したもので、基本方針と対策基準からなる。さらにこの情報セキュリティ・ポリシーの確実な実施のために、具体的な実施手順を定めることとする。これらは、東京大学の利用者等全てに情報セキュリティの重要性を認識させて、東京大学が保有する全ての情報資産の情報セキュリティを確保するために定めるものである。

2 情報セキュリティ・ポリシーの目標
情報セキュリティ・ポリシーが対象とする利用者等及び対象物は以下の通りである。
利用者等
東京大学の役員・常勤教職員・非常勤教職員、学生・研究生等(聴講生なども含む)、その他東京大学保有の情報資産に対するアクセスを認められている者(共同利用者・来学者等、外部委託先作業者など)。

対象物
東京大学が保有する全ての情報資産。情報資産は「情報」と「情報システム」を含む。「情報」は、それを表現する媒体(磁気的媒体、光学的媒体、紙媒体など)の種類を問わない。磁気ディスク、フラッシュメモリ、手書きメモは対象になる。ただし、当面の間、DNAサンプルのような試料は対象としない。「情報システム」は、「情報」を扱うためのシステムであり、電子的システムだけでなく、紙媒体を扱うための学内便のようなシステムも含む。なお、東京大学以外の情報システムに保管されるものであっても、東京大学保有の情報資産として認められるものは対象となる。
東京大学情報セキュリティ・ポリシーが目指すものは次の通りである。
1. 東京大学保有の情報資産に関する、重要度による分類と相応の管理の徹底
2. 東京大学保有の情報資産に対する侵害からの防衛
3. 東京大学内外の情報資産に対する加害行為の防止
4. 東京大学内におけるセキュリティ侵害等の早期検出と迅速な対応の実現

3 情報セキュリティ・ポリシーの基本方針
3.1 組織・体制
東京大学に大学全体に対する最高情報セキュリティ責任者(CISO:Chief Information Security Officerを置く。最高情報セキュリティ責任者は、本学の情報セキュリティに関する総括的な意思決定を行う。最高情報セキュリティ責任者は、学内及び学外に対する東京大学としての情報セキュリティに関する責任を負う。最高情報セキュリティ責任者は、情報セキュリティに関する施策を定め、それを全学に徹底させるために必要な措置を実施する権限を有するものとする。また、このために必要な組織の設置を命じることができる。

3.2 情報セキュリティ・ポリシー及び実施手順の策定
現状の情報資産の管理状況を把握するために全学的に情報セキュリティ調査を定期的に実施する。情報セキュリティ調査の結果に対してリスク分析を行い、対策基準及び実施手順を作成する。情報セキュリティ・ポリシーと実施手順は定期的に見直す。

3.3 情報の分類と管理
情報の分類を行い、適切な情報管理方法を定める。

（続）

http://www.u-tokyo.ac.jp/gen03/public16_j.html

1. 教育学部の計算機環境 （学部・大学院）
2. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
   (1) UTokyo WiFI編
   (2) 教育学部LAN編
3. UTokyo Microsoft License（個人所有PC／大学所有PC） （学部・大学院）
4. セキュリティ対策 （大学院）
5. メールを読む （大学院）
6. サーバにログインする （大学院）
7. メールを転送する （大学院）
8. メーリングリストを開設する （大学院）
9. ホームページを公開する （大学院）

コンピュータ／スマホ／タブレットをネットワークに接続する（1）
～UTokyo WiFI（学内共通無線LANサービス）を使う～

- UTokyo WiFi 公式ページ
  http://www.u-tokyo.ac.jp/ja/administration/dics/service/wifi.html
  Q&A、問い合わせフォーム等あり

- UTokyo WiFi（無線LAN）ヘルプページ – ECCS相談員（ECCS Tutor's page）
  https://www.sodan.ecc.u-tokyo.ac.jp/?page_id=3996
  アカウント取得から機種別接続まで詳しく解説（オススメ）

【教育学部内の利用可能エリア】
教育学部棟内の講義室、演習室、図書閲覧室、国際交流室

【利用手続きを行う上での注意点】
- UTokyo Accountは持っているか？
- UTokyo Accountにメールアドレスを登録しているか（所要1日）？
- 学内限定の「UTokyo WiFiアカウントメニュー」のページにどうやってアクセスするか？

注意

- UTokyo WiFiのアカウントを使用するにはUTokyo Accountが必要
- 事前にUTask-WebまたはUT-mateで連絡先のメールアドレスが登録されていることが必要です．(学生の場合)
  - UTask-Web あるいは UT-mate での登録は、翌日以降に反映されます．
- アカウント発行の情報は登録してあるメールアドレスに送信されます．
- 2台目以降も同じアカウントで使用できます．
- アカウントは4月末，10月末に失効するので，再取得が必要です．
- その他の注意事項については公式ページを参照してください．

アカウントの取得方法

まず，下記のアドレスにアクセスします．
http://www.u-tokyo.ac.jp/ja/administration/dics/service/wifi.html

ここの中の，「UTokyo WiFi アカウントメニュー」をクリックします．
ただし，このアカウントメニューは学内からのみのアクセスとなっています．

すると，下のようなログイン画面が出てきます

以前はSSID: utroamで仮接続できたが、現在は使えない？

→学内のネットワークにつながっている端末からアクセスする必要がある。

→ブラウザにログイン名とパスワードを記憶させないように！

https://www.sodan.ecc.u-tokyo.ac.jp/?page_id=3996

教育学部LAN

sd09

UTNETルータ

フロアスイッチ

B1F～4F

各研究室情報コンセント

ハブ

有線

DHCPまたは
固定アドレス

無線AP

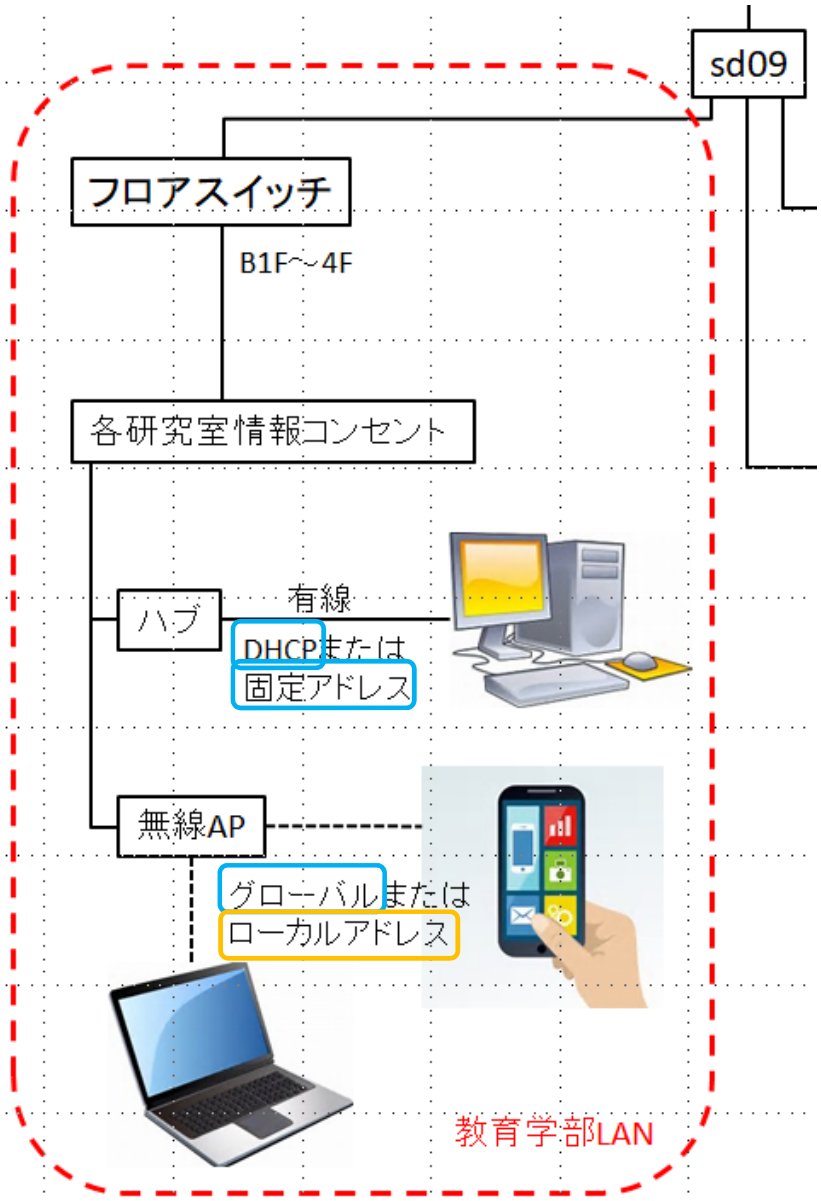
グローバルまたは
ローカルアドレス

各研究室で管理

教育用計算機システム
(ECCS)

UTokyo WiFi

コンピュータ／スマホ／タブレットをネットワークに接続する（2）
～教育学部LAN（UTNET）を使う～



グローバルアドレス（DHCPまたは固定アドレス、133.11….など）で接続する場合は、申請書の提出が必要です。

アドレス変換機能（NAT）のある無線APなどを使ってローカルアドレス（192.168….など）で接続する場合は、各コース・研究室のネットワーク担当の方にご相談ください。

UTnetに接続するには、適切なIPアドレスを設定することが必要

DHCP（Dynamic Host Configuration Protocol）:

ネットワーク設定を自動で行うサービス（繋ぐだけでつながる）。

- 申請無しでも接続できてしまう
  →東大のセキュリティポリシーに違反している可能性
- 将来的には、申請されたMACアドレスに対してのみIPアドレスを割り当てる

割り当てIPアドレスは、時々変わるので、サーバ、ネットワークプリンタには不適。

固定IPアドレス:

IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバを手動設定。
赤門総合研究棟、弥生総合研究棟では固定アドレスのみ。
WWW、ネットワークプリンタ等のサーバ用途。
利用できるリソースが限られる（なので不要になったら返却する）。

※IPアドレス申請書は、「教育学部内限定のページ」（後述）からダウンロード
http://www.p.u-tokyo.ac.jp/local/index.html

固定アドレス／DHCPの接続申請書

学部内限定ページからダウンロード
http://www.p.u-tokyo.ac.jp/local/index.html

UTNet 設置・接続・変更申請書（固定 IP アドレス利用）

		申請年月日	平成　年　月　日
（フリガナ） 設置担当者氏名		役職等	
メールアドレス			
所属	東京大学大学院教育学研究科　　コース		
連絡先		電話番号	内線
設置場所		電話番号	内線
接続機器名			
ＯＳ名			
イーサネット アドレス	－　－　－　－　－		
コンピュータの 名前	（英数 8 文字程度でつけて下さい）		
利用目的	教育学部内で（ Web , Mail , Ftp , その他 ）サーバ用途で使用。 総合研究棟（農学部）でネットワークに接続するため。 赤門総合研究棟でネットワークに接続するため。 その他（IP アドレス返却など　　）		

コンピュータの名前

DNS サーバへの登録のために必要です。英数 8 文字程度の名前を付けてください。

イーサネットアドレスの調べ方

Windows98/Me の場合：

「スタート」－「ファイル名を指定して実行」で winipcfg と入力する。出てきたウインドウの「アダプタアドレス」欄に表示される（「PPP Adapter」となっている場合、他の正しいアダプタを選ぶ）。

Windows 2000/NT/XP の場合：

「コマンドプロンプト」を開き、ipconfig /all と入力する。「Physical Address」というところに表示される。

MacOS の場合：

「アップル」メニューから「コントロールパネル」→「TCP/IP」を選択して、「TCP/IP」設定ウインドウを開く。「経由先」リストで「Ethernet」を選択。ハードウェアアドレスと表示されているのがイーサネットアドレス。

MacOS X の場合

Dock 上の「System Preferences」アイコンをクリックして「システム環境設定」を開き、「システム環境設定」ウインドウから「ネットワーク」をクリックする。タブの上のほうにある「設定」リストより「内蔵 Ethernet」を選択。「TCP/IP」タブをクリックする。「Ethernet アドレス」と表示されている。

UTNet 設置・接続・変更・停止申請書（DHCP サービス利用）

		申請年月日	平成　年　月　日
（フリガナ） 設置担当者氏名		役職等	
メールアドレス			
所属	東京大学大学院教育学研究科　　コース		
連絡先		電話番号	内線
設置場所		電話番号	内線
接続機器名			
ＯＳ名			
イーサネット アドレス	－　－　－　－　－		
申請理由	1. 新たに購入したパソコンをネットワークに接続するため。 2. 設置場所を変更するため。 3. 固定 IP アドレスからの移行。 4. パソコン廃棄等の理由により DHCP サービス利用の停止		

イーサネットアドレスの調べ方

Windows98/Me の場合：

「スタート」－「ファイル名を指定して実行」で winipcfg と入力する。出てきたウインドウの「アダプタアドレス」欄に表示される（「PPP Adapter」となっている場合、他の正しいアダプタを選ぶ）。

Windows 2000/NT の場合：

「コマンドプロンプト」を開き、ipconfig /all と入力する。「Physical Address」というところに表示される。

Windows XP の場合：

「マイネットワーク」のアイコンを右クリックし「プロパティ」を開く。「ローカルエリア接続」をダブルクリック。「サポート」タブを選び、「詳細」ボタンを押す。「物理アドレス」というところに表示される。

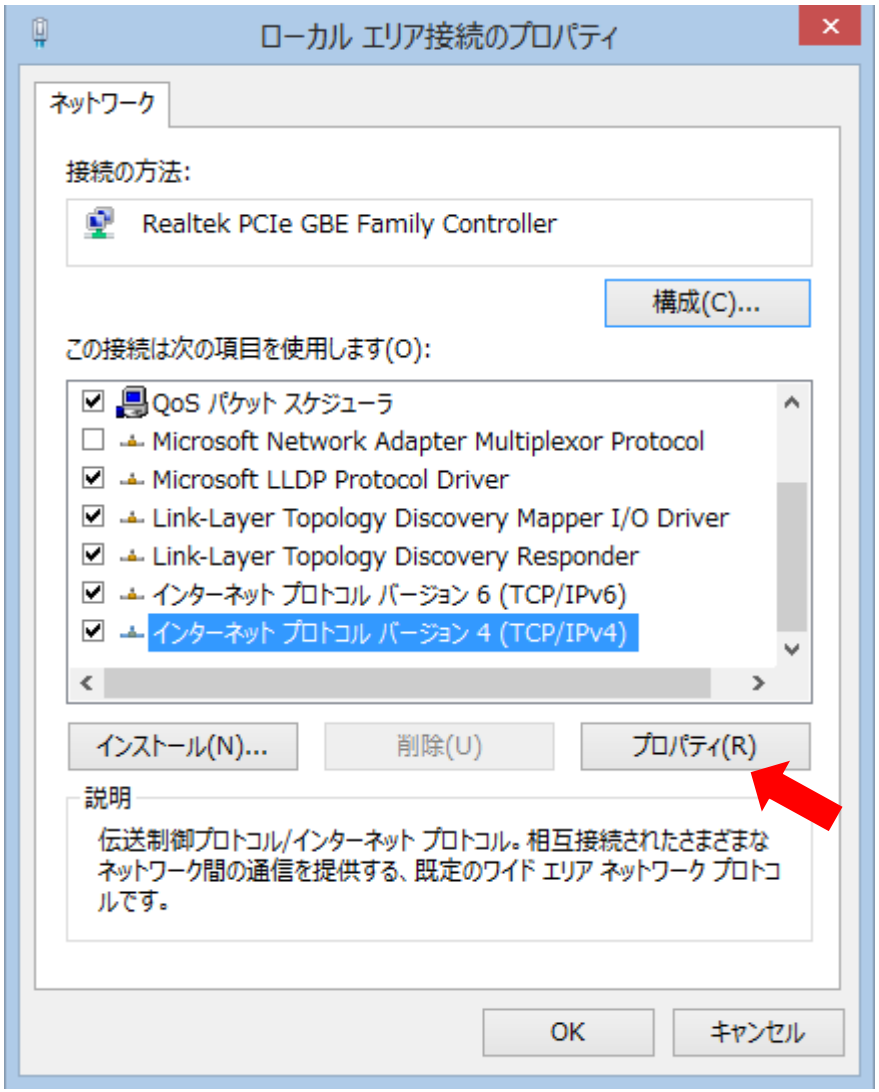
MacOS の場合：

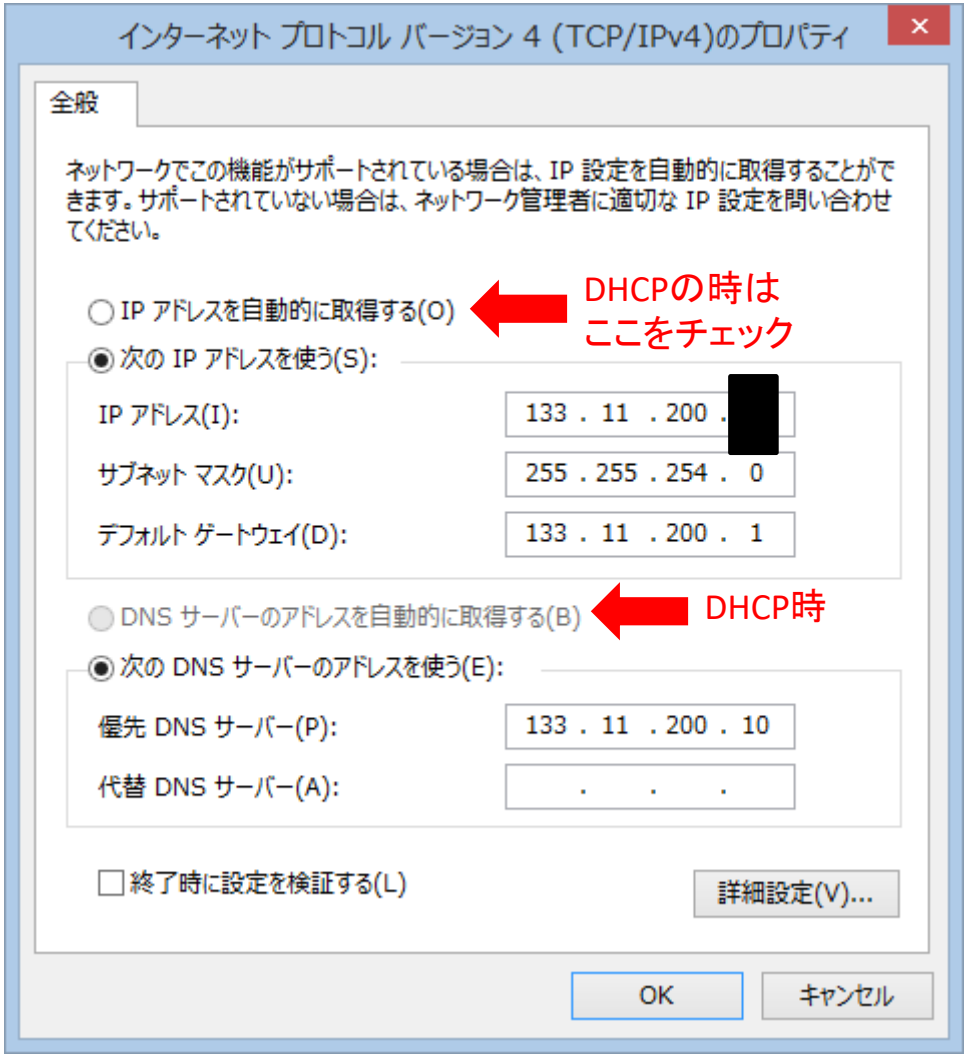
「アップル」メニューから「コントロールパネル」→「TCP/IP」を選択して、「TCP/IP」設定ウインドウを開く。「経由先」リストで「Ethernet」を選択。ハードウェアアドレスと表示されているのがイーサネットアドレス。

MacOS X の場合

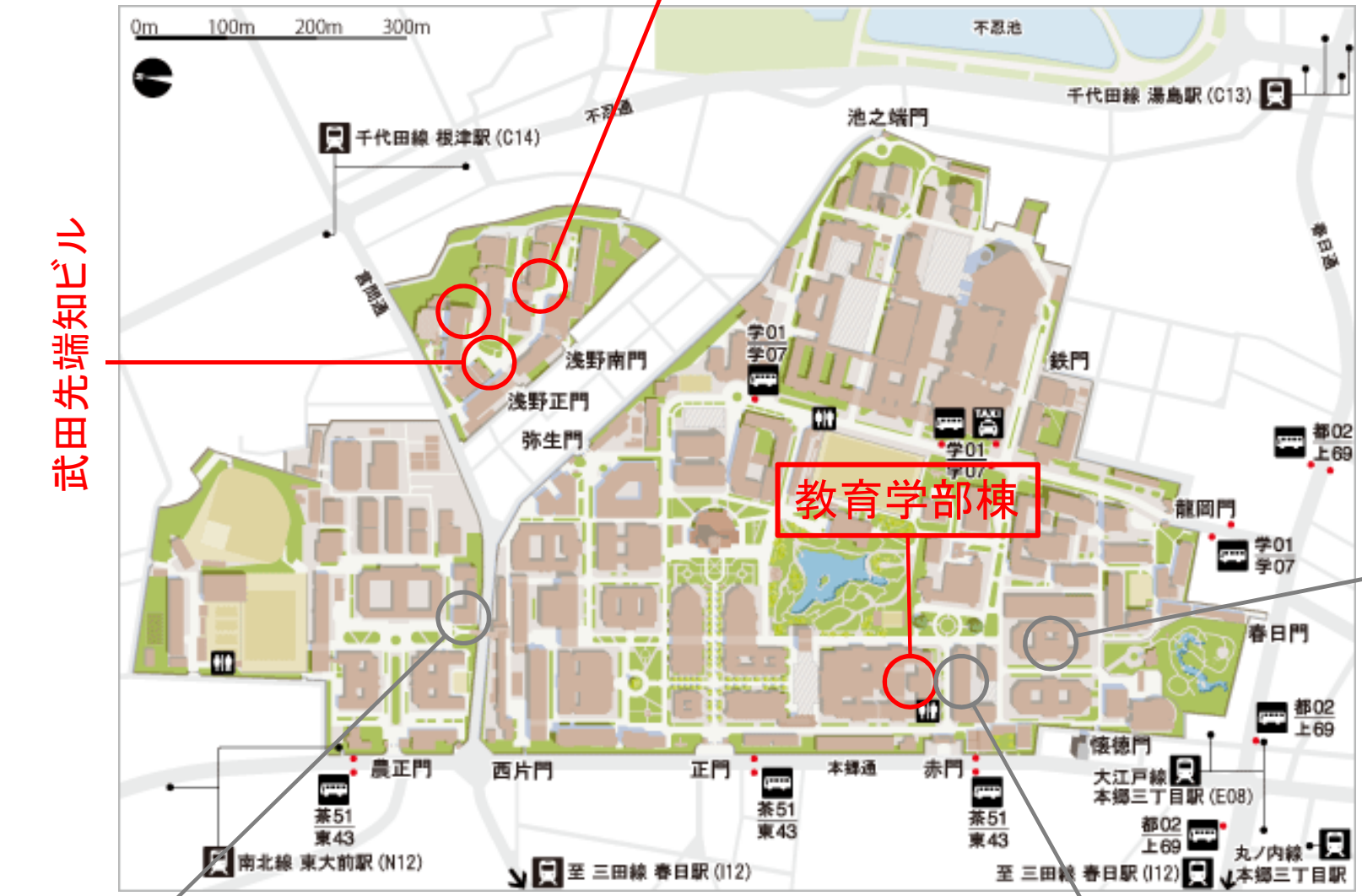
Dock 上の「System Preferences」アイコンをクリックして「システム環境設定」を開き、「システム環境設定」ウインドウから「ネットワーク」をクリックする。タブの上のほうにある「設定」リストより「内蔵 Ethernet」を選択。「TCP/IP」タブをクリックする。「Ethernet アドレス」と表示されている。

ネットワーク設定例（教育学部棟／固定アドレス／Windows 8.1の場合）

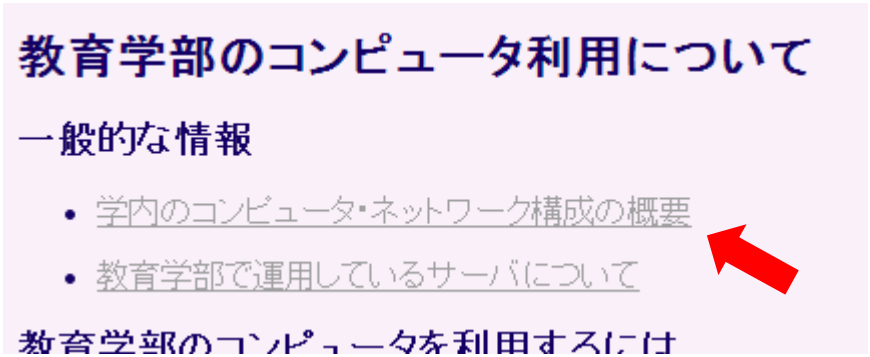




赤字の施設は「建物間VLAN」により
同一セグメントとして取り扱い可能



固定アドレス時のネットワーク設定



「教育学部内限定のページ」
http://www.p.u-tokyo.ac.jp/local/index.html

- コンピュータの設定等を解説。
- 教育学部のネットワーク内でのみ閲覧可能
- ECCS、UTokyo WiFiからは見られない！
  →情報基盤センターのネットワーク配下にあるため。

教育学部のネットワーク構成

場所	教育学部棟	弥生総合研究棟	赤門総合研究棟	医学部1号館
IPアドレス	133.11.200.0/23	130.69.201.64/26	133.11.142.0/26	133.11.142.128/25
サブネットマスク	255.255.254.0	255.255.255.192	255.255.255.192	255.255.255.128
デフォルトゲートウェイ	133.11.200.1	130.69.201.65	133.11.142.1	133.11.142.129
DNSサーバ	133.11.200.10	133.11.200.10	133.11.200.10	133.11.200.10

※教育学部棟と医学部1号館ではDHCPサービスが利用できます。
※工12、工9、武田先端知、図書館西側は教育学部棟と同じ扱いになります

1. 教育学部の計算機環境 （学部・大学院）
2. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
   (1) UTokyo WiFI編
   (2) 教育学部LAN編
3. UTokyo Microsoft License（個人所有PC／大学所有PC） （学部・大学院）
4. セキュリティ対策 （学部・大学院）
5. メールを読む （大学院）
6. サーバにログインする （大学院）
7. メールを転送する （大学院）
8. メーリングリストを開設する （大学院）
9. ホームページを公開する （大学院）

東京大学で（比較的）安価に利用できるソフトウェア（1～3） ※ただし1,2は学生は申請できない

1. Microsoft アカデミックセレクトプラス(ASP) （情報基盤センター）

- 東大教職員のみ
- 要申請
- ダウンロードとインストールは学内で
- 利用負担金が必要

別表　　2017.2.14現在

製品名	負担金額
Office Professional Plus 2016	14,000
Office Standard 2016	12,500
Office fot Mac Standard 2016	12,500
Visio Standard 2016	3,900
Visual Studio Professional 2015	7,600
Windwos Professional (Upgradeライセンス)	6,500
Windows Server Standard 2016 最低（8ライセンス（16コア分））	22,500
Windows Server CAL (UserCAL)	1,000
Windows Server CAL (DeviceCAL)	1,000
Windows Server Datacenter 2016 最低（8ライセンス（16コア分））	156,000
SQL Server Standard 2016	31,000
SQL CAL (UserCAL)	5,500
SQL CAL (DeviceCAL)	5,500

※ 本表に記載のないものは、個別にお問い合わせください。
情報システム部 情報戦略課 情報戦略チーム
E-mail：asp@nc.u-tokyo.ac.jp

2. ソフトウェアライセンス（情報基盤センター）

※要申請／一般学生の利用は困難

ソフトウェア（利用内規等）（学内向け制限）		メーカ（リンク）	利用申込み	契約期間（ライセンス期限）	経費	問い合わせ先
ウイルス対策ソフトウェア	ウイルスバスター(Windows 日本語版) ウイルスバスター(Windows 英語版) Server Protect for Windows(Windowsサーバ専用) Server Protect for Linux(Linux環境) nterScan Messaging Security Virtual Appliance（仮想化OS用) InterScan Messaging Security Suite Plus（物理サーバ用 WindowsServer Linux)	トレンドマイクロ社	年度毎※	単年度	有料	anti-virus@itc.u-tokyo.ac.jp
	Sophos Anti-Virus	Sophos	年度毎※	2007.4.1から	1,000円/年（1台）	
	ESET Endpoint Security	Canon IT ソリューションズ	年度毎※	2009.11.1から	1,000円/年（1台）	
	Symantec Endpoint Protection	株式会社Symantec	年度毎※	2011.11.29から	1,000円/年（1台）	
Creo		Parametric Technology Corporation/PTCジャパン	年度毎※	2005.4.1から	20,000円/年（1申請）	proengineer@itc.u-tokyo.ac.jp
JMP		SAS Institute Japan株式会社 JMPジャパン事業部	年度毎※	2007.9.5から	10,000円/年（1申請）	jmp@itc.u-tokyo.ac.jp
SAS9		SAS Institute Japan株式会社	年度毎※	2013.2.28	50,000円/年（1台）	sas@itc.u-tokyo.ac.jp
MATHEMATICA		Wolfram Research	年度毎※	2016.2.29	50,000円/年（1申請）	mathematica@itc.u-tokyo.ac.jp
CHEMOFFICE		Perkin Elmer社(旧CambridgeSoft社)	年度毎※	2007.9.5から	40,000円/年（1申請5台まで）	chemoffice@itc.u-tokyo.ac.jp
LabVIEW ※ LabVIEW Academy 提供開始		ナショナルインスツルメンツ株式会社	年度毎※	2008.4.1から	50,000円/年（1申請）	labview@itc.u-tokyo.ac.jp 工学系研究科 伴野講師

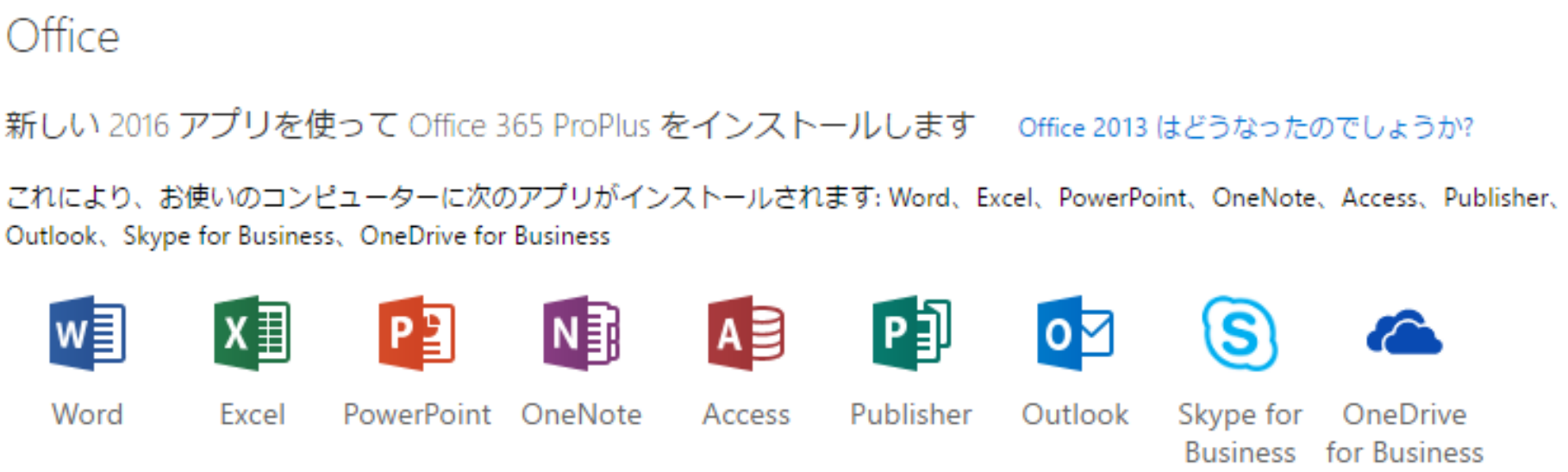
3. UTokyo Microsoft License（Microsoft Office 包括ライセンス、個人所有PC向け）

公式ページ
http://www.u-tokyo.ac.jp/ja/administration/dics/service/mslicense.html

Microsoft Office 包括ライセンスについて – FAQ（ECCS Tutor's page） オススメ
https://www.sodan.ecc.u-tokyo.ac.jp/?page_id=4446

【対象】学生・教職員

【ソフトウェア】Office 365 ProPlus



【参考】大学所有のコンピュータ向けライセンス UTokyo Microsoft License for University PC

公式ページ（学内のみ）:
http://www.ut-portal.u-tokyo.ac.jp/wiki/index.php/UTokyo_Microsoft_License_for_University_PC

大学所有PCとは:
「大学が購入し保有し、大学の教職員が管理するPC」

ダウンロードおよびインストールが出来る身分:
管理者である教職員（学生不可）

ソフトウェアの利用者:
上記教職員、当該PCの利用を許された者（学生、受け入れ研究者、一時的な利用者）も

利用できるソフト:
Windows 10 Education（日本語版/英語版）Upgrade版
Office Professional Plus 2016（Windows版）(32bit/64bit)（日本語版/英語版）
Office for Mac Standard 2016（macOS版）（日本語版/英語版）
System Center Endpoint Protection （Windows版/macOS版）（日本語版/英語版

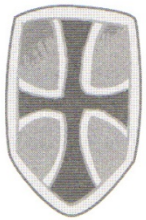
1. 教育学部の計算機環境 （学部・大学院）
2. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
   (1) UTokyo WiFI編
   (2) 教育学部LAN編
3. UTokyo Microsoft License（個人所有PC／大学所有PC） （学部・大学院）
4. セキュリティ対策 （学部・大学院）
5. メールを読む （大学院）
6. サーバにログインする （大学院）
7. メールを転送する （大学院）
8. メーリングリストを開設する （大学院）
9. ホームページを公開する （大学院）

セキュリティ対策

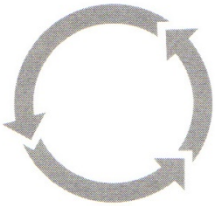
セキュリティ対策は「多層防御」で

図3-3　エンドポイントで取れる対策とその注意点　単独では万全な防御にならないため、複数を組み合わせる必要がある。

(1)ウイルス対策ソフトを導入
→定義ファイルを最新に保つ

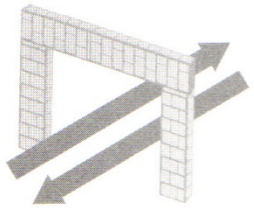


(2)セキュリティ更新プログラムを適用
→計画的に適用、更新する

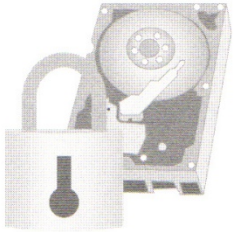


(3)不正プログラムの起動を防止
→起動できるソフトを選別する
ホワイトリスト方式がより安全

(4)不正通信を禁止
→受信制限に加え、端末からの
送信制限も活用する



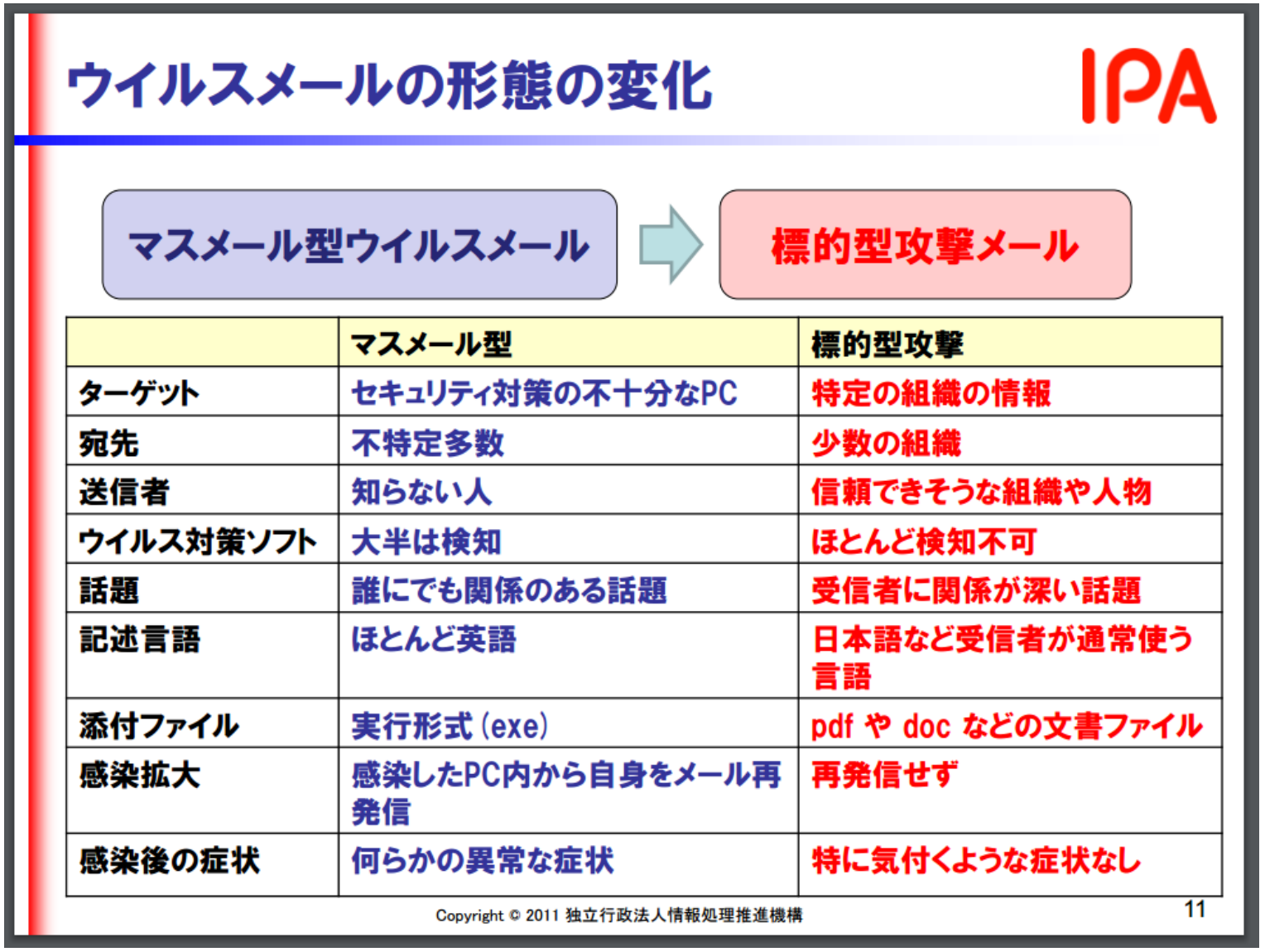
(5)盗難・紛失による情報漏洩を防止
→ディスク全体を暗号化する



具体的な対策：

- パスワードを定期的に変更する
- OS、アプリのセキュリティアップデートを常に適用する
- OSやセキュリティ対策ソフトのファイアウォール機能を有効にする
- 最新のウイルス対策ソフト・定義ファイルを使用する
- メールの添付ファイルはウイルス検査後に開く
- ダウンロード／USBメモリからコピーしたファイルはウイルス検査後に開く
- ウイルス検査をまめに行う
- フィッシング詐欺・標的型攻撃メールを見抜く
- 不用意に他人にコンピュータを触らせない
- 万一の被害に備えるためにデータのバックアップをまめに行う
- ファイルを暗号化する

標的型攻撃（スピアフィッシング）



ウイルスメールの形態の変化

IPA

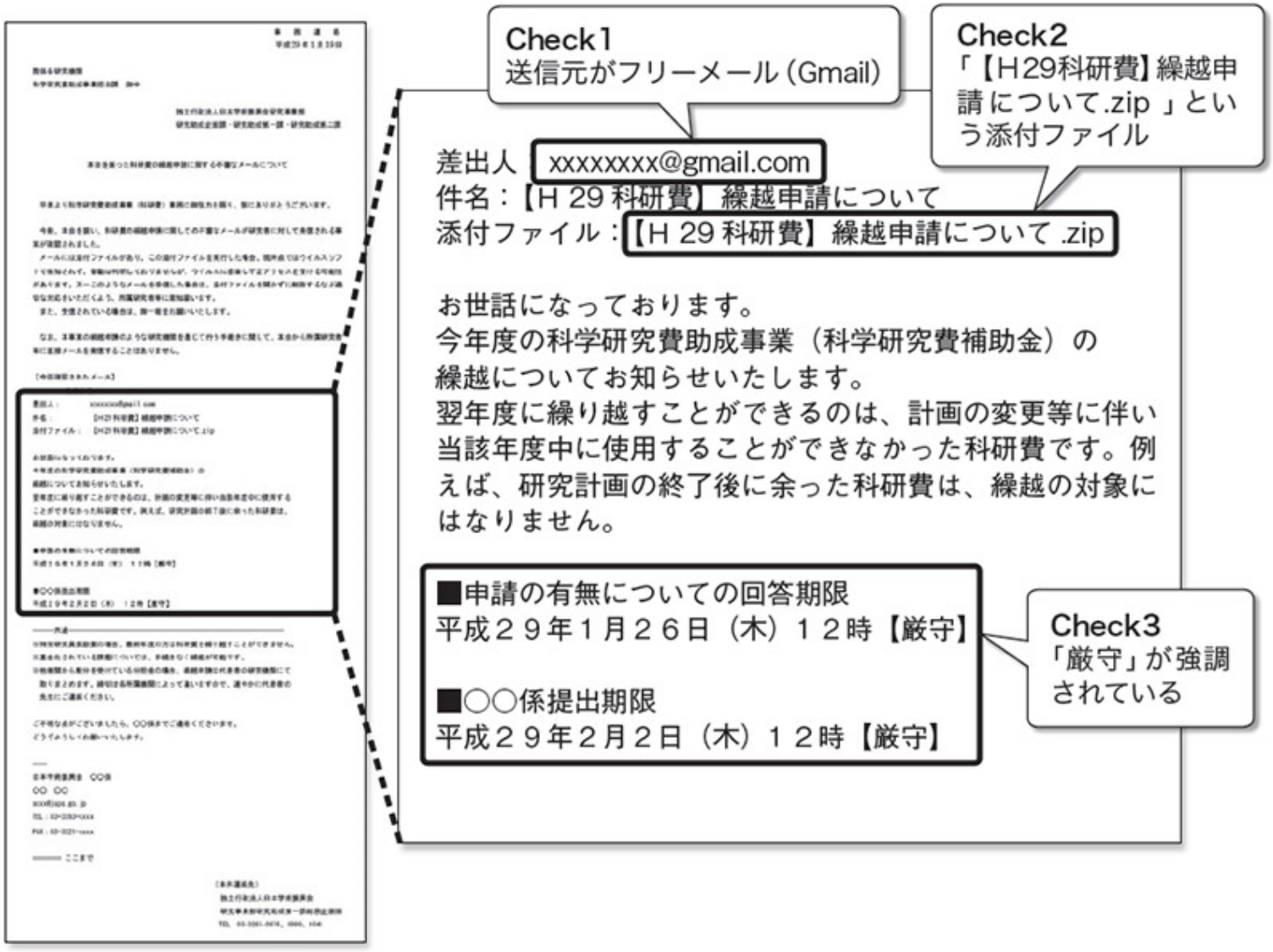
マスメール型ウイルスメール ⇒ 標的型攻撃メール

	マスメール型	標的型攻撃
ターゲット	セキュリティ対策の不十分なPC	特定の組織の情報
宛先	不特定多数	少数の組織
送信者	知らない人	信頼できそうな組織や人物
ウイルス対策ソフト	大半は検知	ほとんど検知不可
話題	誰にでも関係のある話題	受信者に関係が深い話題
記述言語	ほとんど英語	日本語など受信者が通常使う言語
添付ファイル	実行形式（exe）	pdf や doc などの文書ファイル
感染拡大	感染したPC内から自身をメール再発信	再発信せず
感染後の症状	何らかの異常な症状	特に気付くような症状なし

https://www.ipa.go.jp/files/000024542.pdf

標的型攻撃の例:「大学関係者をだます攻撃の調査で見つかった、複数の外交文書」

http://itpro.nikkeibp.co.jp/atcl/column/16/012900025/042100039/?n_cid=nbpitp_mled_itp&rt=nocnt （要登録）



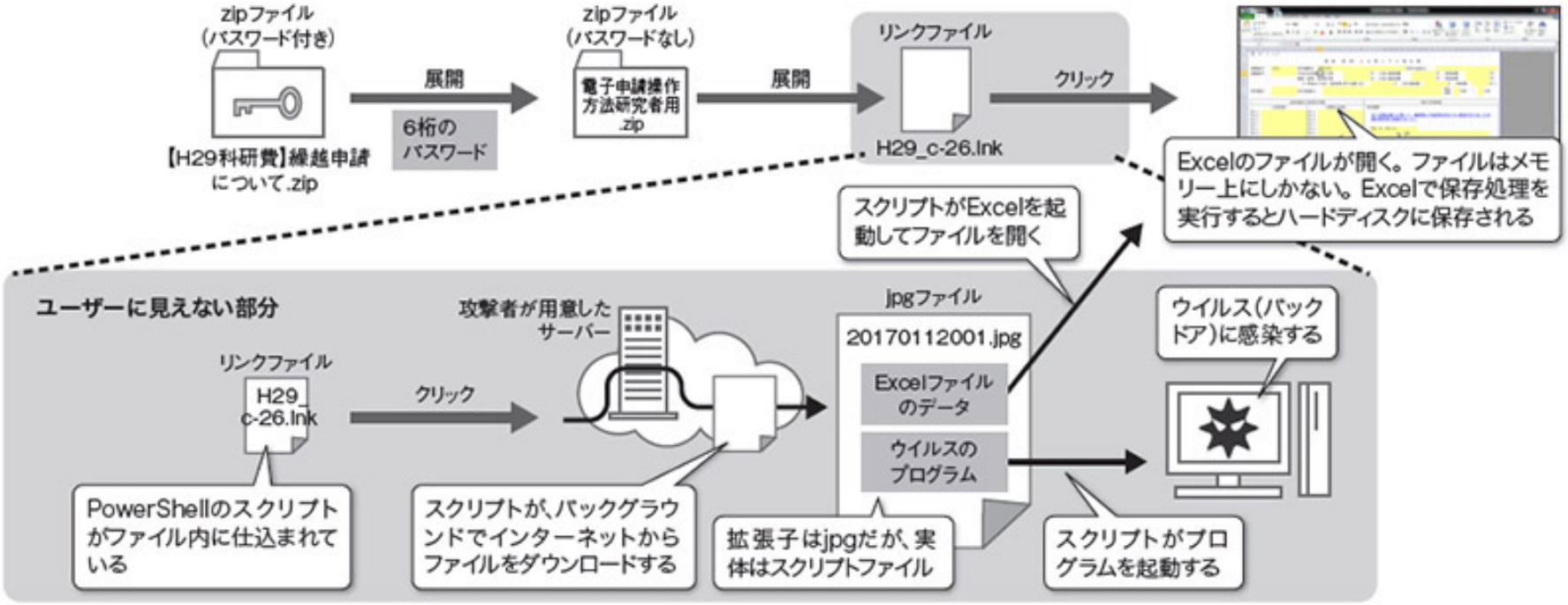


図3●添付ファイルをクリックするとExcelファイルが表示、バックグラウンドでウイルス感染

メールに添付されたzipファイルを展開するとリンクファイルが生成される。リンクファイルには悪質なスクリプトが仕込まれているため、クリックするとバックグラウンドでウイルスがダウンロードされて、ウイルスに感染する。パソコンの画面には、ユーザーを欺くためのExcelファイルが表示される。

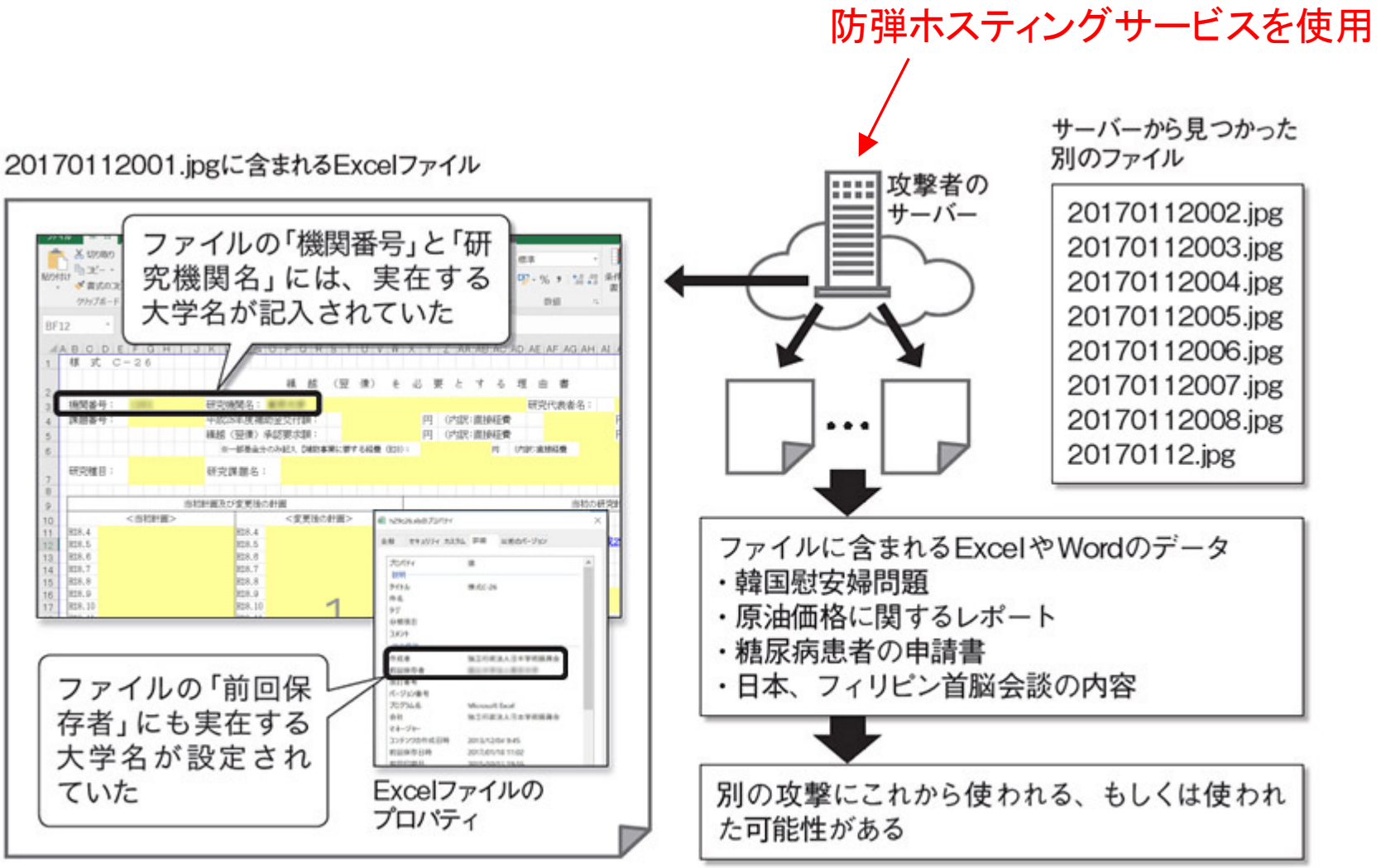


図4●ダミーの申請書を表示してユーザーを信用させる

リンクファイルをクリックすると、ユーザーを安心させるために攻撃者が用意したダミーの申請書が表示される。実在する大学名が、ファイルのデータとしてだけでなく、ファイルのプロパティの前回保存者にも含まれていた。また、攻撃者のサーバーを調べると別のダミーデータを含むスクリプトファイルを見つけた。これらのダミーは今後、別の攻撃で使われる可能性がある。担当者を欺こうとするとダミーデータを「デコイ」と呼ぶこともある。

2.1. 標的型攻撃メールと注意する時の着眼点

表 2-1 は、IPA に情報提供があった標的型攻撃メールや公開情報から得た知見を基に標的型攻撃メールの特徴をまとめたものである。

これらの特徴に複数合致するメールを受信した場合は、標的型攻撃メールの可能性があるため、注意して対応する必要がある。対応方法については、「3. 標的型攻撃メールへの対応」を参照いただきたい。

表 2-1　標的型攻撃メールの着眼点

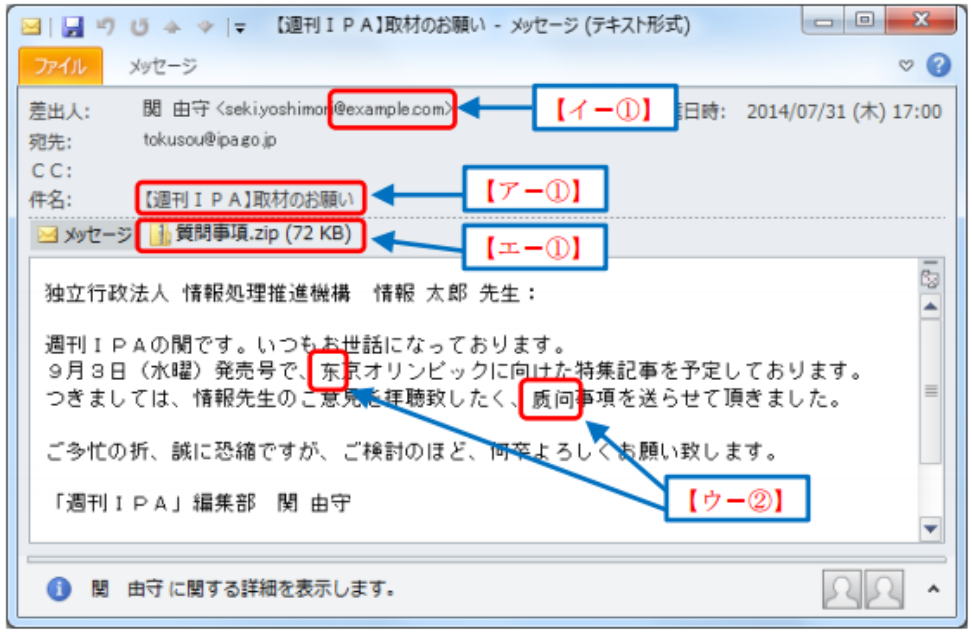
(ア)メールのテーマ	① 知らない人からのメールだが、メール本文の URL や添付ファイルを開かざるを得ない内容 (例 1) 新聞社や出版社からの取材申込や講演依頼 (例 2) 就職活動に関する問い合わせや履歴書送付 (例 3) 製品やサービスに関する問い合わせ、クレーム (例 4) アンケート調査
	② 心当たりのないメールだが、興味をそそられる内容 (例 1) 議事録、演説原稿などの内部文書送付 (例 2) VIP 訪問に関する情報
	③ これまで届いたことがない公的機関からのお知らせ (例 1) 情報セキュリティに関する注意喚起 (例 2) インフルエンザ等の感染症流行情報 (例 3) 災害情報
	④ 組織全体への案内

IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」
https://www.ipa.go.jp/files/000043331.pdf

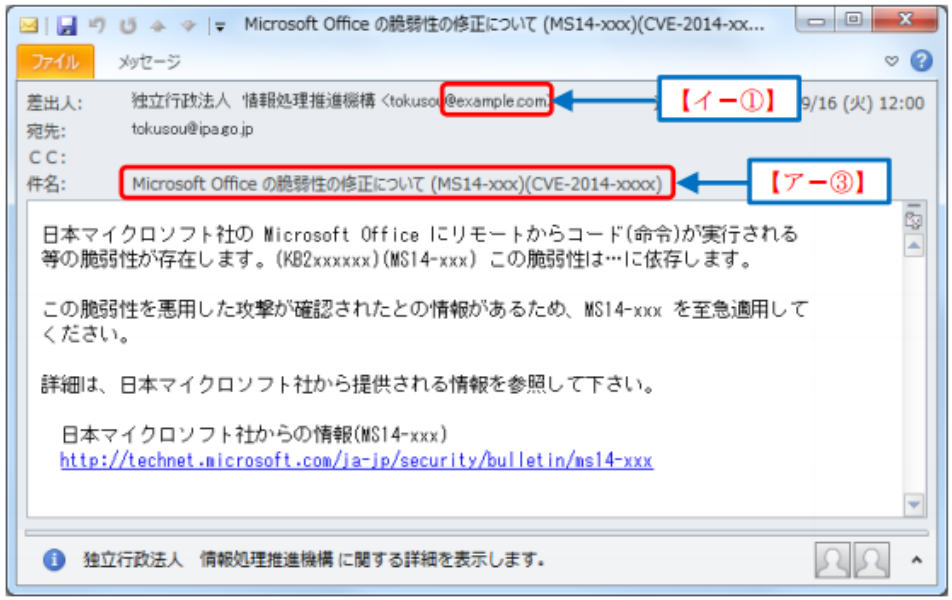
	(例 1) 人事情報 (例 2) 新年度の事業方針 (例 3) 資料の再送、差替え
	⑤ 心当たりのない、決裁や配送通知（英文の場合が多い） (例 1) 航空券の予約確認 (例 2) 荷物の配達通知
	⑥ ID やパスワードなどの入力を要求するメール (例 1) メールボックスの容量オーバーの警告 (例 2) 銀行からの登録情報確認
(イ)差出人のメールアドレス	① フリーメールアドレスから送信されている
	② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
(ウ)メールの本文	① 日本語の言い回しが不自然である
	② 日本語では使用されない漢字（繁体字、簡体字）が使われている
	③ 実在する名称を一部に含む URL が記載されている
	④ 表示されている URL（アンカーテキスト）と実際のリンク先の URL が異なる（HTML メールの場合）
	⑤ 署名の内容が誤っている (例 1) 組織名や電話番号が実在しない (例 2) 電話番号が FAX 番号として記載されている
(エ)添付ファイル	① ファイルが添付されている
	② 実行形式ファイル(exe / scr / cpl など)が添付されている
	③ ショートカットファイル(lnk など)が添付されている
	④ アイコンが偽装されている (例 1) 実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
	⑤ ファイル拡張子が偽装されている (例 1) 二重拡張子となっている (例 2) ファイル拡張子の前に大量の空白文字が挿入されている (例 3) ファイル名に RLO[4]が使用されている

https://www.ipa.go.jp/files/000043331.pdf

2.2.1. 新聞社や出版社からの取材申込のメール



2.2.4. セキュリティに係る注意喚起のメール



※差出人情報はメールソフトによっては表示されない。より正確に判断するには、ソーステキストのヘッダ情報を見て判断する。

https://www.ipa.go.jp/files/000043331.pdf

IPA Better Life with IT

第 15-09-334 号
2015 年 6 月 1 日
独立行政法人情報処理推進機構

ランサムウェア
（ransom：身代金）

今月の呼びかけ

「 パソコン内のファイルを人質にとるランサムウェアに注意！ 」
～ メッセージが流暢な日本語になるなど国内流行の懸念 ～

2015 年 4 月に、IPA の情報セキュリティ安心相談窓口に「パソコンに『暗号化しました』というメッセージが表示されて、ファイルが開けなくなった」という相談の件数が増えました。相談内容からランサムウェアの被害と推測されます。

ランサムウェアとは、ファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに金銭を要求する不正プログラムの総称です。IPA に寄せられたランサムウェアに感染したという相談は、2011 年 7 月が初めてでした。その後もランサムウェアに関する相談はありましたが、2014 年 12 月に初めて日本語でメッセージが表示される種類のランサムウェアの相談が 1 件※1寄せられました。2015 年 4 月にはさらに異なる種類のランサムウェアの相談が 6 件※2あり、すべてが日本語でメッセージが表示される種類のものでした（図 1）。また、そのうち 1 件は初めて企業から寄せられた感染被害の相談でした。

直近で確認されているランサムウェアは支払い方法がビットコインのみのため、現状日本国内で金銭面での被害は大きくないと考えられますが、今後は支払い方法を日本向けに工夫するなどの可能性は否定できません。

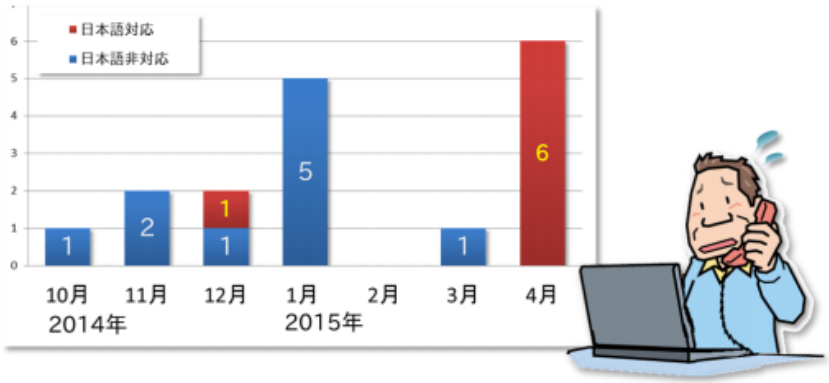


図 1：ランサムウェアに関する相談件数の推移

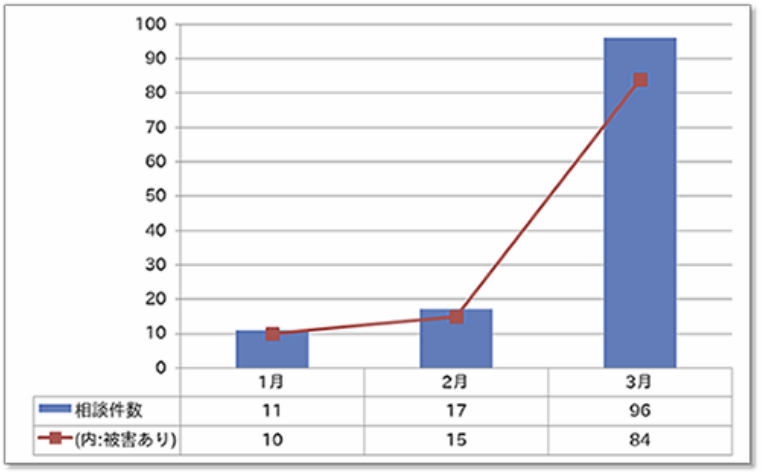


図.ランサムウェアに関する相談の月別推移（2016年1月～3月）

https://www.ipa.go.jp/files/000046075.pdf

IPA が 2014 年 10 月に実施した意識調査[※3]において、ランサムウェアを知っている人は約 2 割という結果が出ています。被害防止の観点から早急に周知を図りたいと考え、今月の呼びかけではこのランサムウェアについて、その手口と対策を紹介します。

（1） ランサムウェアとは

ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。パソコンに保存されている特定のファイル（オフィスドキュメントや圧縮ファイル、音楽、画像など）に**勝手に暗号化処理を行い、読みとれない状態にしてしまう不正プログラムで、ファイルを暗号化した後にそのファイルの復元と引き換えに金銭を要求する**ような文面が表示されます。この現象が、あたかもファイルが身代金を要求するための人質の様であることからランサムウェアと呼ばれます（図 2）。

要求される金額は様々ですが、数万円程度の額に相当するビットコインの支払いを要求されるケースが多いようです。なお、ファイルを暗号化されてしまった後は、ランサムウェア自体を駆除してもファイルを復元することはできません。また、要求された金額を支払ったところで元に戻せる保証もありませんので、感染してしまうとパソコン内の重要なファイルを失ってしまうことになり、影響度の大きい不正プログラムと言えます。

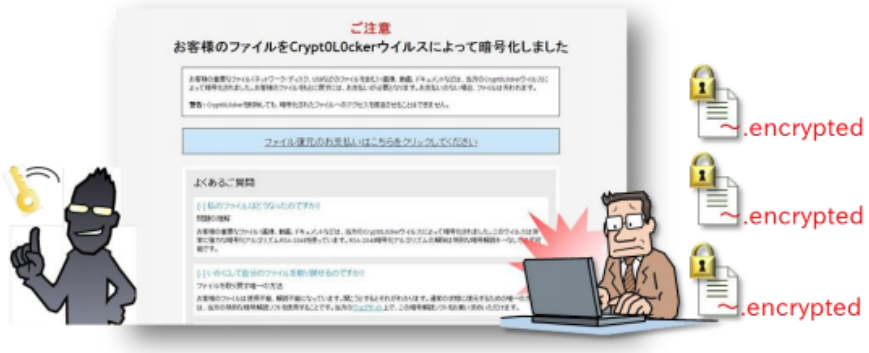


図 2：ファイルを暗号化した後に表示されるメッセージ

ランサムウェアの感染経路は、一般的なウイルスの感染経路と同様です。メール内の URL をクリックしたり、攻撃者が用意したウェブサイトを閲覧したりすることで感染[※4]します。

冒頭の相談の事例では、特にメールの添付ファイルを開いたり、URL をクリックしたりという自覚が利用者になく、怪しいとは思えないブログを閲覧した後で金銭を要求するメッセージが表示されたとのことでした。このことから、パソコンにインストールされているソフトウェアの脆弱性を

悪用し、**ウェブサイトにアクセスしただけでウイルスに感染するドライブ・バイ・ダウンロード**[※5]による被害と、IPA では推測しています。

（2） ランサムウェアへの対策

ランサムウェアによって暗号化されてしまったファイルの復元は困難なことから、予防がとても重要です。ランサムウェアの感染対策として、以下を実施してください。

■セキュリティソフトを導入する
セキュリティソフトを導入し、定義ファイルを最新に保つことで、ランサムウェアの感染リスクを低減させることができます。

■OS および利用ソフトウェアを最新の状態にする
OS およびソフトウェアのバージョンを常に最新の状態に保ち、脆弱性をなくすことでドライブ・バイ・ダウンロードによる感染リスクを低減します。

■重要なファイルを定期的にバックアップする
基本的にはランサムウェアによって暗号化されたファイルは復元できません。そのため、重要なファイルについては、定期的にバックアップする必要があります。

IPA ではパソコンにインストールされているソフトウェアが最新の状態であるか、どのようにアップデートを行えば良いのかが確認できるツール「MyJVN バージョンチェッカ[※6]」を提供しています。これを活用して使用しているソフトウェアのバージョン管理の実施を推奨しています。

また、冒頭で紹介した意識調査では、“定期的にバックアップをしている人は約５割”で、半数の人は定期的にバックアップを取っていない、という結果が出ています。バックアップはランサムウェアへの対策としてだけでなく、パソコンが突然故障してしまった場合の備えにもなります。

バックアップの方法には、Windows のバックアップ機能を利用する、同一フォルダで管理して定期的に外部媒体やクラウドサービスへコピーするなどがあります。万が一の場合に備えて定期的にバックアップをとることを推奨します。

もしランサムウェアと疑われる症状が確認されたなど、パソコンのウイルス感染に関しての相談は安心相談窓口[※7]に連絡してください。

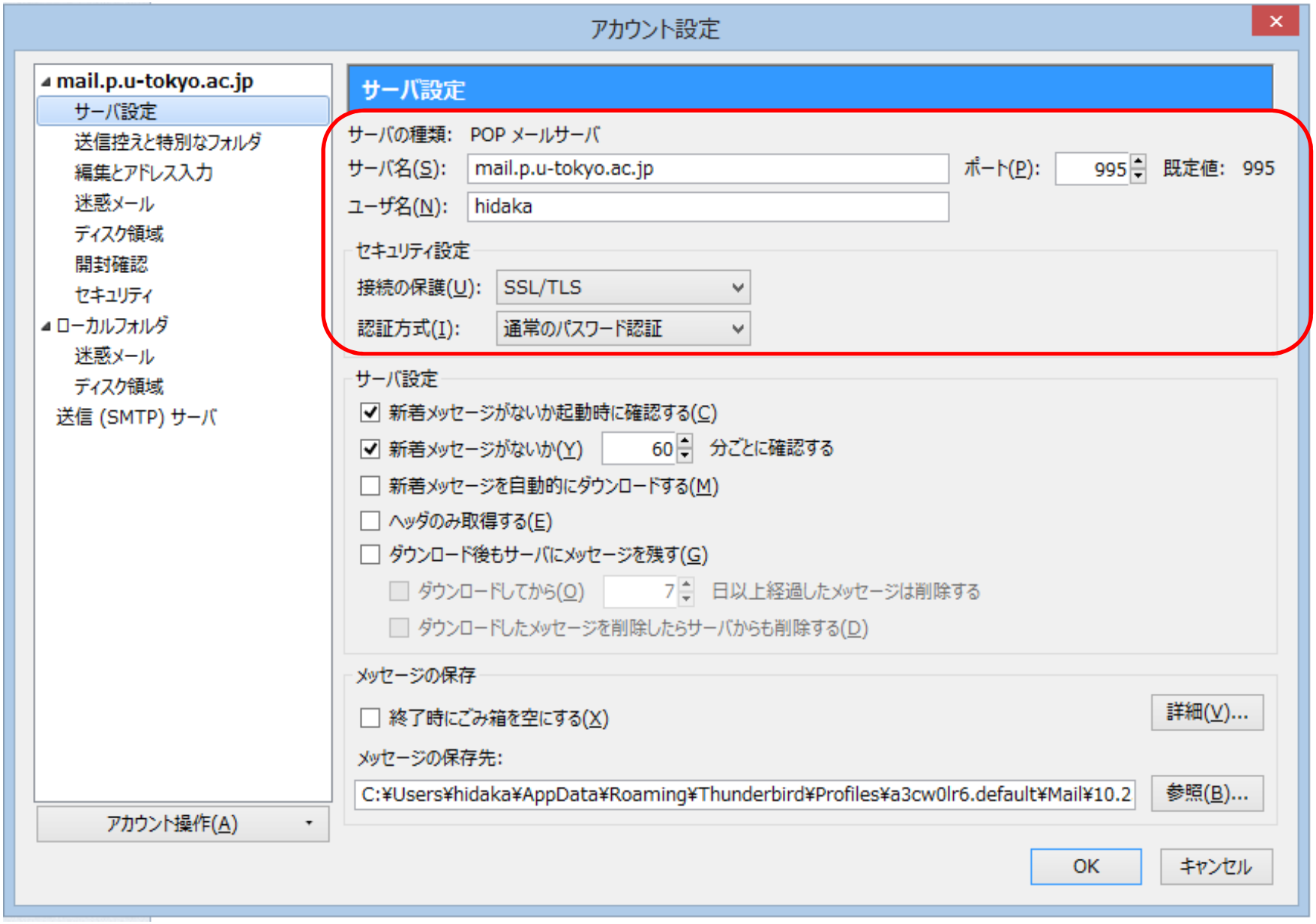
1. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
2. セキュリティ対策 （学部・大学院）
3. メールを読む （大学院）
4. サーバにログインする （大学院）
5. メールを転送する （大学院）
6. メーリングリストを開設する （大学院）
7. ホームページを公開する （大学院）

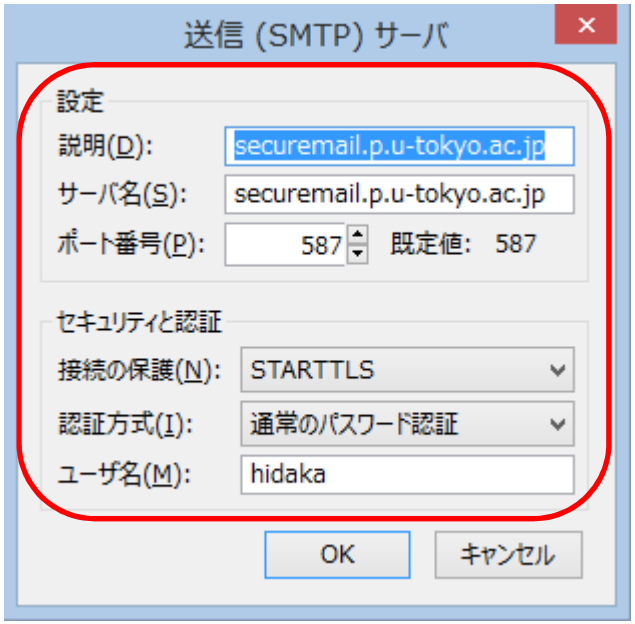
教育学研究科のサーバ群

サーバ名（別名）	IPアドレス	用途
edusan	133.11.200.10	DNS, DHCP, LDAP
complex (securemail)	133.11.200.	WWW, SMTP（メール送信）
educord (mail)	133.11.200.34	ファイルサーバ, POP3（メール受信）
edcom	133.11.200.2	ファイルサーバ、アプリケーションサーバ

アカウント申請書は1F事務室前にある（大学院生、大学院研究生、教職員のみ）。
ログイン名／パスワードは全サーバ共通
ユーザのホームディレクトリは全サーバで共有（どれにログインしてもよい）
※通常の作業はeducordで。学外からはアクセスできないサーバもある。

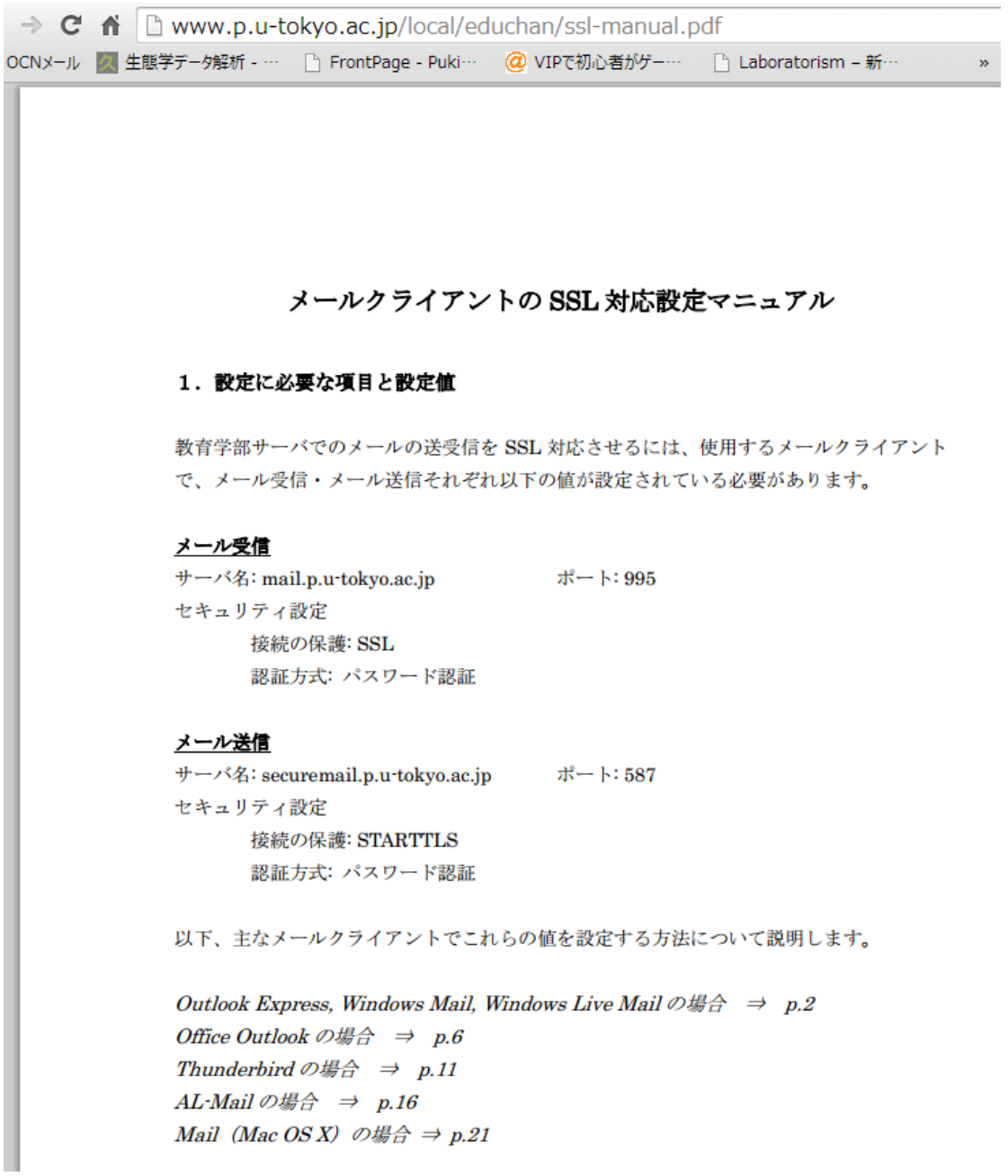
メーラー（Tunderbird、Windowsメール等）の設定





- 受信サーバ(mail)、送信サーバ(securemail)は教育学部サーバアカウントを申請して使う。
- ECCSのアカウントは使えない。
- パスワードは長いもの、辞書攻撃に耐えるものにする。
- パスワードが破られると、どうなるか？

詳しい設定は、こちら:



1. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
2. セキュリティ対策 （学部・大学院）
3. メールを読む （大学院）
4. サーバにログインする （大学院）
5. メールを転送する （大学院）
6. メーリングリストを開設する （大学院）
7. ホームページを公開する （大学院）

- パスワードを変えたい
- サーバにファイルをアップロードしたい
- ホームページを開設したい
- UNIX / Linuxのプログラムを使いたい／作りたい

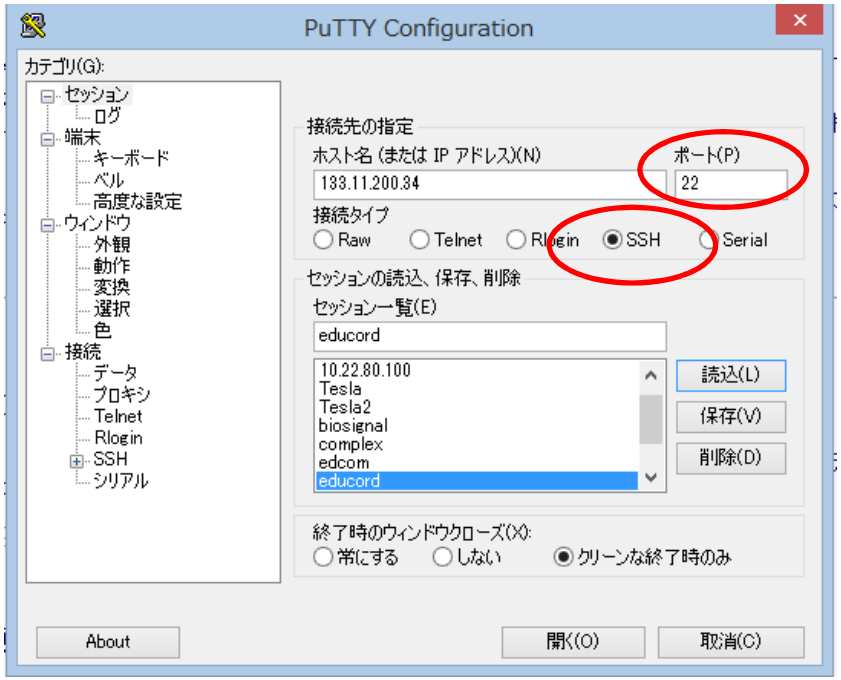
こんな時は、サーバへログインして作業する。

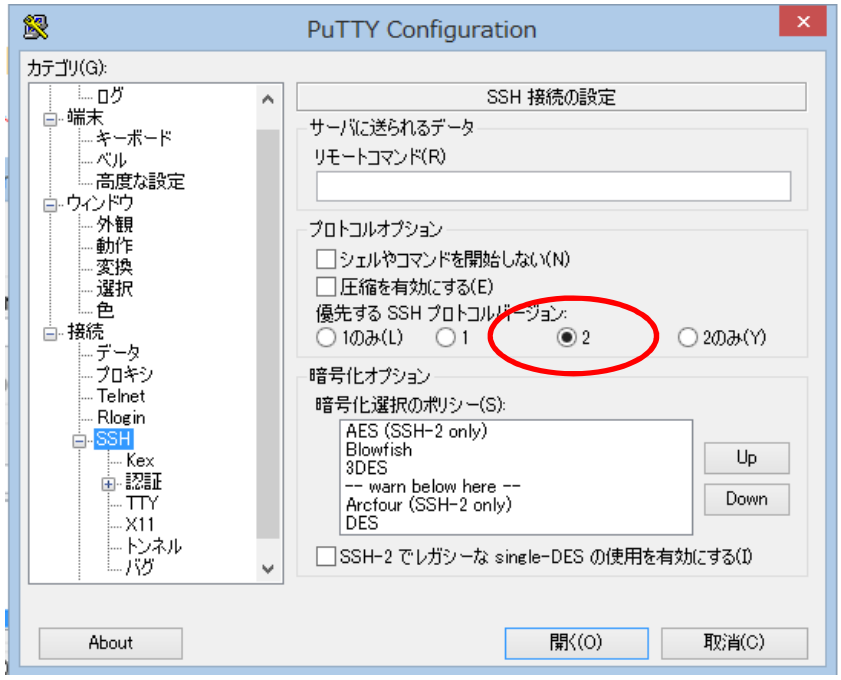
ログイン方法	用途	アプリ名
SSH (Ver.2)	各種コマンドを実行	PuTTY, TeraTerm+TTSSH, sshなど
SFTP	ファイル転送	WinSCP, FFFTPなど

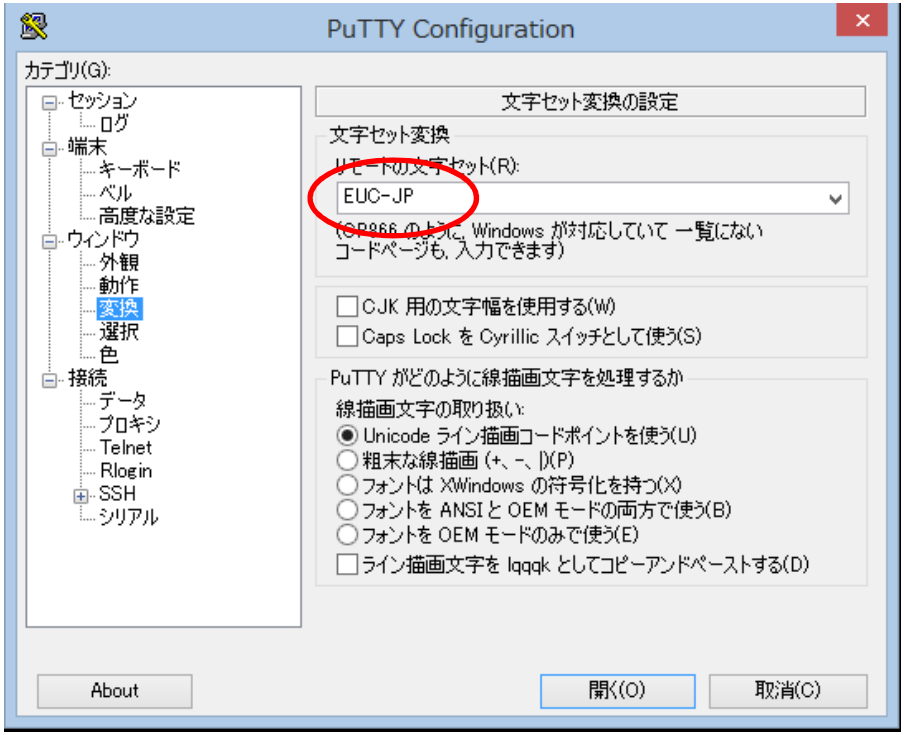
ログイン時にはログイン名とパスワードをネット越しに入力するが、
SSH、SFTPとも通信経路を暗号化するので（比較的）安全

（例）puTTY（パティ）でeducordにログインする

puTTYjp　http://hp.vector.co.jp/authors/VA024651/PuTTYkj.html





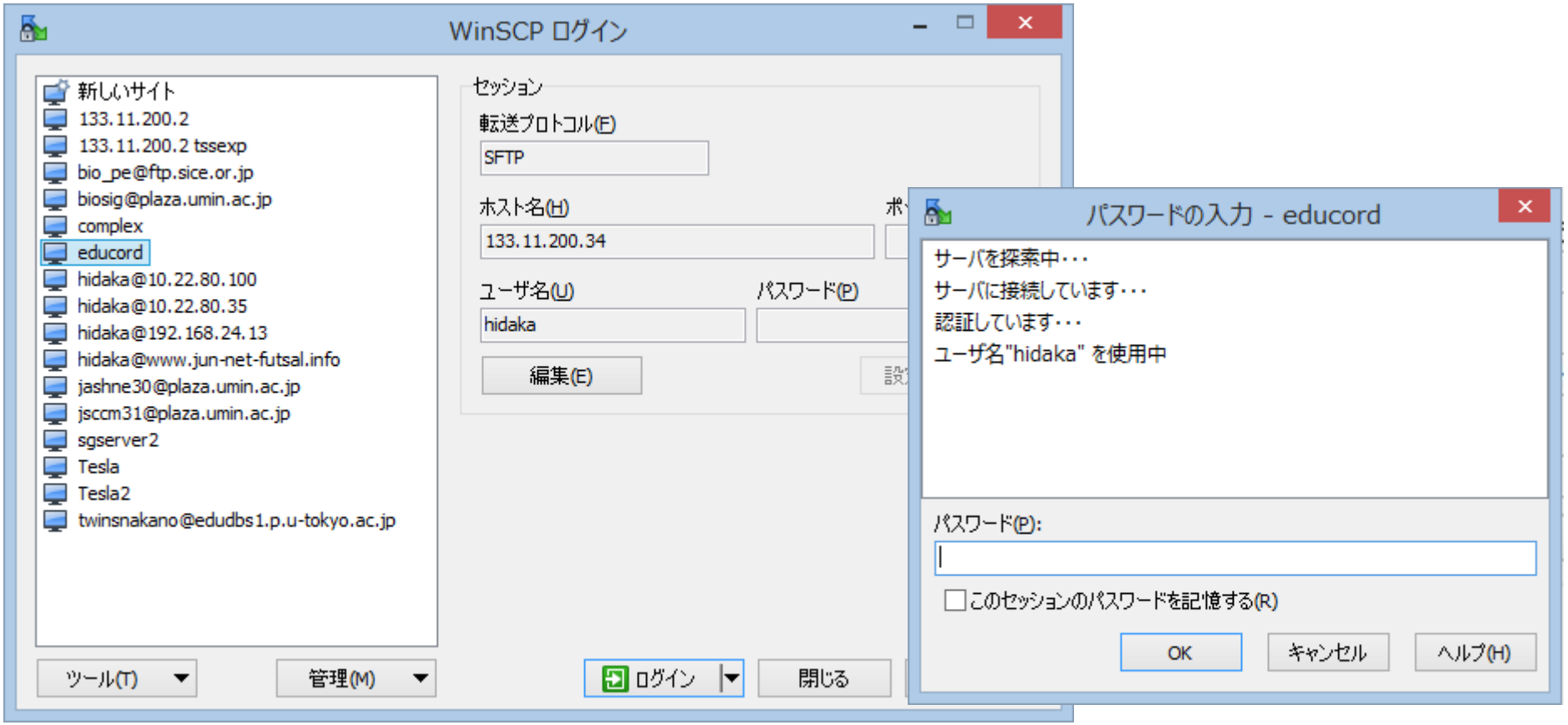


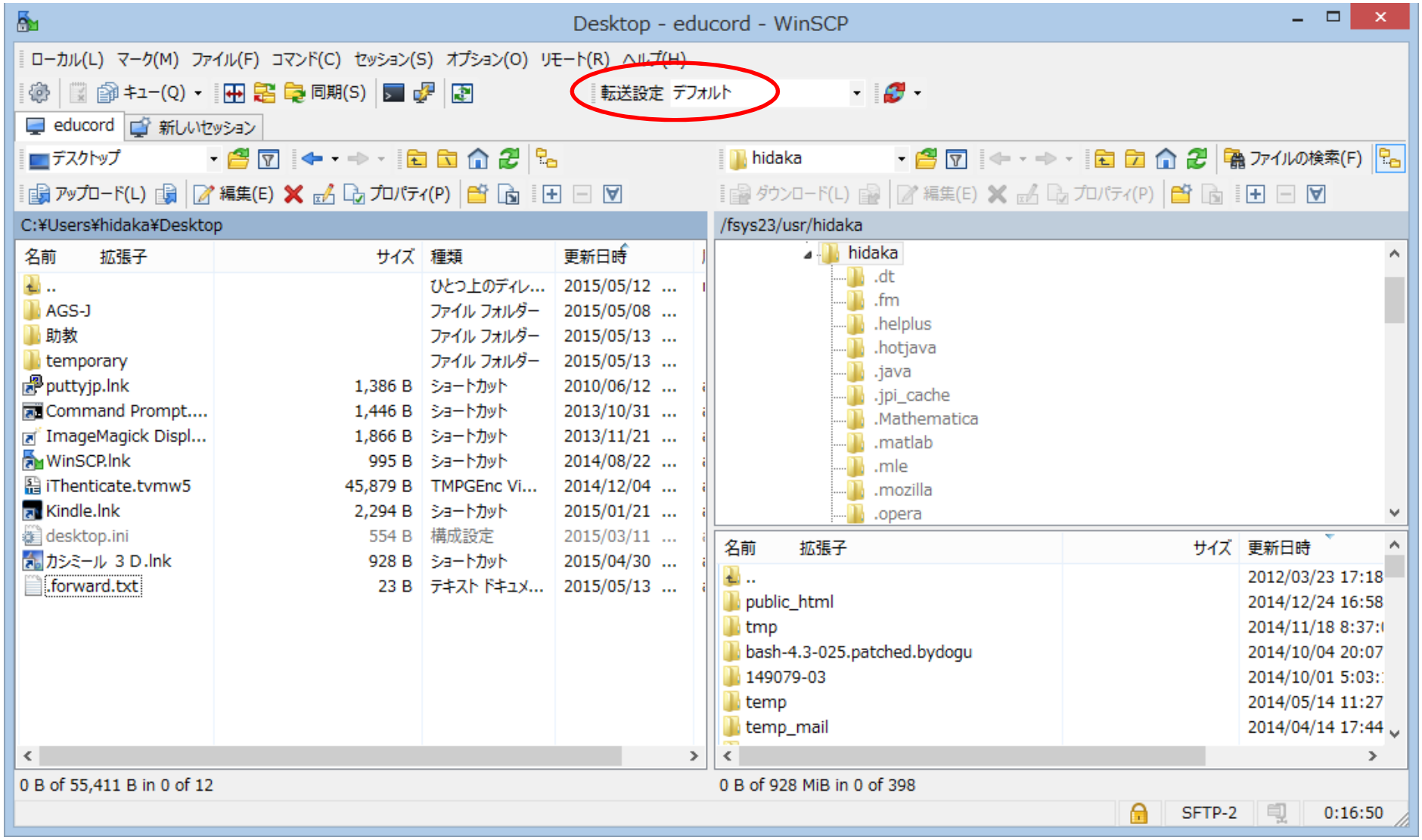
パスワードの変更

- ログイン後、passwdコマンドを実行する。
- ターミナルでの操作は、Linuxのシェルと各コマンドの知識が必要

（例）WinSCPでファイルサーバにログインし、ファイルを転送する

WinSCP http://winscp.net/eng/docs/lang:jp



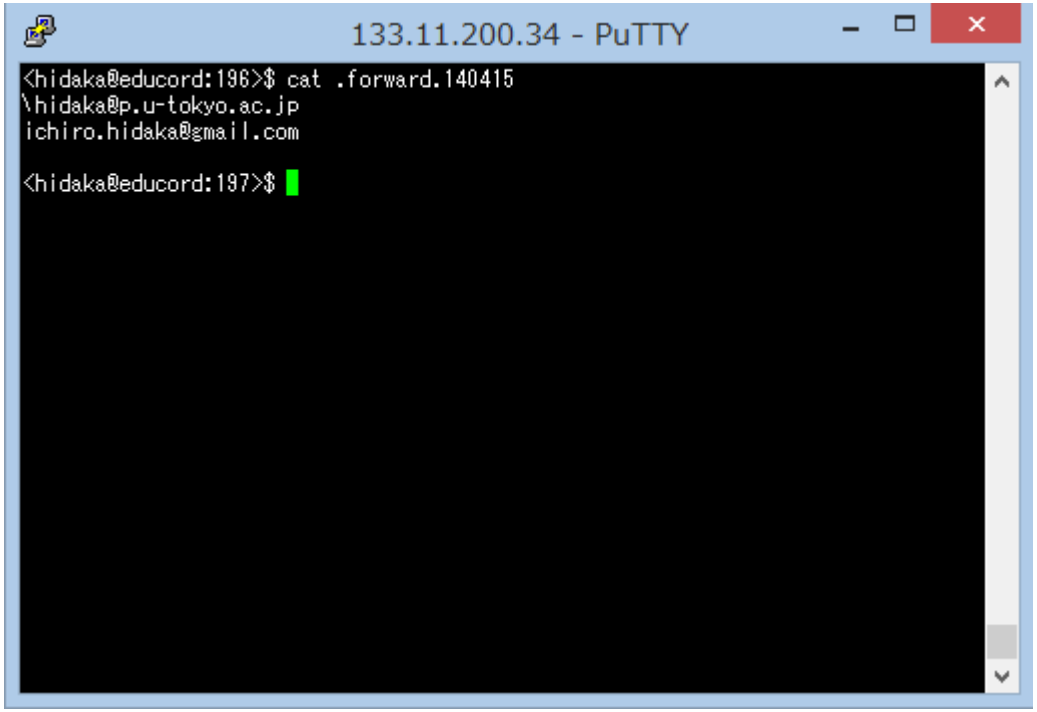


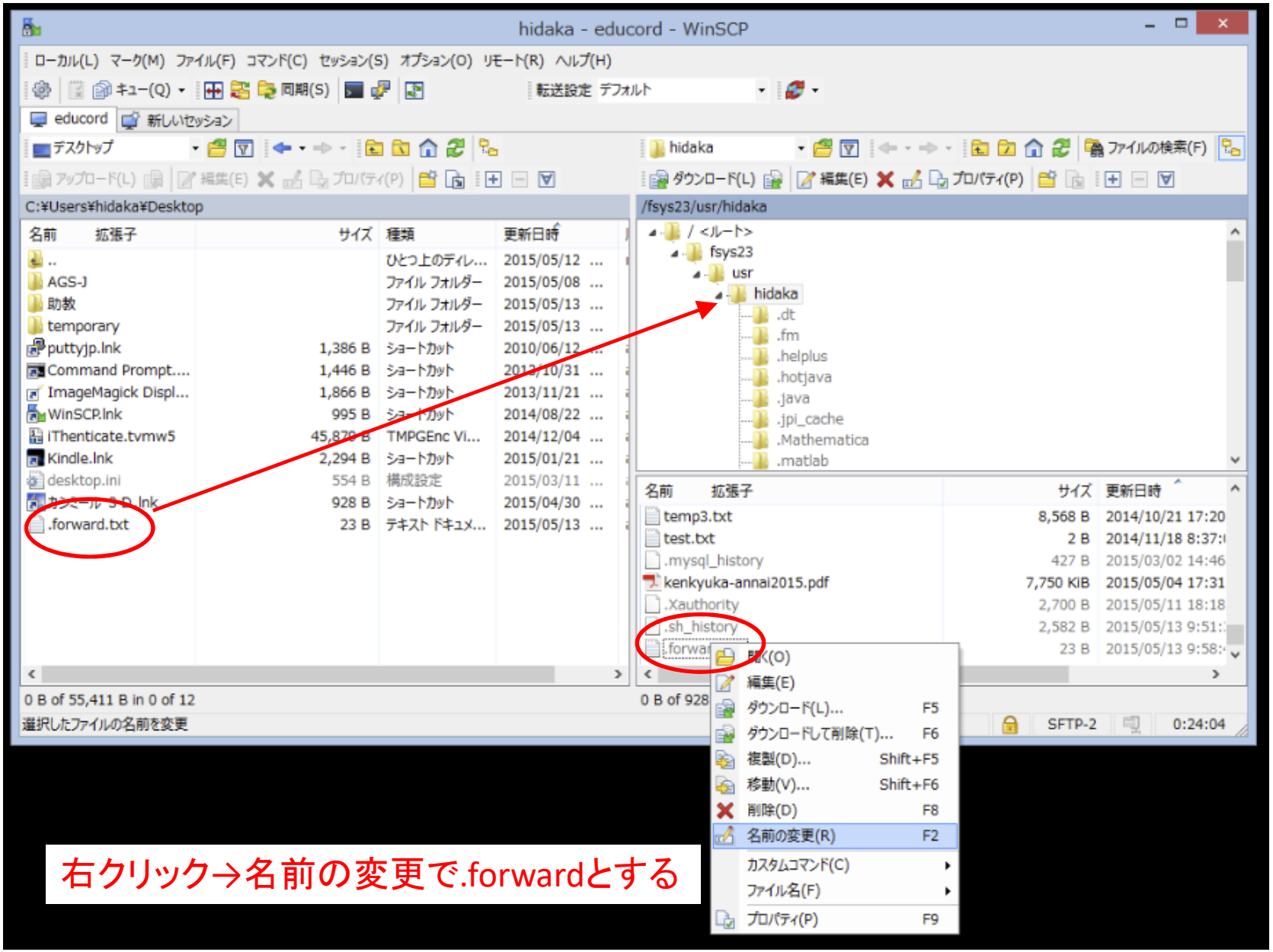
- エクスプローラのような操作感
- 「転送設定」は大抵はデフォルトでよいが、テキスト／バイナリを明示した方がよいこともある。

1. コンピュータ／スマホ／タブレットをネットワークに接続する（学部・大学院）
2. セキュリティ対策（学部・大学院）
3. メールを読む（大学院）
4. サーバにログインする（大学院）
5. メールを転送する（大学院）
6. メーリングリストを開設する（大学院）
7. ホームページを公開する（大学院）

.forwardファイルでメール転送設定

- 各自のホームディレクトリに.forwardという名前のテキストファイルを置く。
  →Windowsでは.forwardという名前のファイルは作れないので、別名（例えば.forward.txt）でファイルを作成してWinSCPでファイル転送し、名前を変更。
- ファイルの中身は、転送先アドレス。
- サーバにメールを残す場合は、バックスラッシュ（¥）に続いて自分のメールアドレスを記入。




hidaka - educord - WinSCP
ローカル(L) マーク(M) ファイル(F) コマンド(C) セッション(S) オプション(O) リモート(R) ヘルプ(H)
キュー(Q) 同期(S) 転送設定 デフォルト
educord 新しいセッション
デスクトップ
hidaka
ファイルの検索(F)
アップロード(L) 編集(E) プロパティ(P)
ダウンロード(L) 編集(E) プロパティ(P)
C:¥Users¥hidaka¥Desktop
/fsys23/usr/hidaka
名前 拡張子 サイズ 種類 更新日時
AGS-J
助教
temporary
puttyjp.lnk 1,386 B
Command Prompt.... 1,446 B
ImageMagick Displ... 1,866 B
WinSCP.lnk 995 B
iThenticate.tvmw5 45,870 B
Kindle.lnk 2,294 B
desktop.ini 554 B
.forward.txt 23 B
/ <ルート>
fsys23
usr
hidaka
.dt
.fm
.helplus
.hotjava
.java
.jpi_cache
.Mathematica
.matlab
temp3.txt 8,568 B 2014/10/21 17:20
test.txt 2 B
.mysql_history 427 B 2015/03/02 14:46
kenkyuka-annai2015.pdf 7,750 KiB 2015/05/04 17:31
.Xauthority 2,700 B 2015/05/11 18:18
.sh_history 2,582 B 2015/05/13 9:51
0 B of 55,411 B in 0 of 12
0 B of 928
選択したファイルの名前を変更
SFTP-2
0:24:04
開く(O)
編集(E)
ダウンロード(L)... F5
ダウンロードして削除(T)... F6
複製(D)... Shift+F5
移動(V)... Shift+F6
削除(D) F8
名前の変更(R) F2
カスタムコマンド(C)
ファイル名(F)
プロパティ(P) F9
右クリック→名前の変更で.forwardとする

1. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
2. セキュリティ対策 （学部・大学院）
3. メールを読む （大学院）
4. サーバにログインする （大学院）
5. メールを転送する （大学院）
6. メーリングリストを開設する （大学院）
7. ホームページを公開する （大学院）

メーリングリストを作る

- メーリングリスト名を決める
- 参加メンバーのメールアドレスを記入したテキストファイルをサーバにアップロードする
- メーリングリスト名、リストファイル名、アップロード場所をコンピュータ相談室に連絡

※リストファイルの例

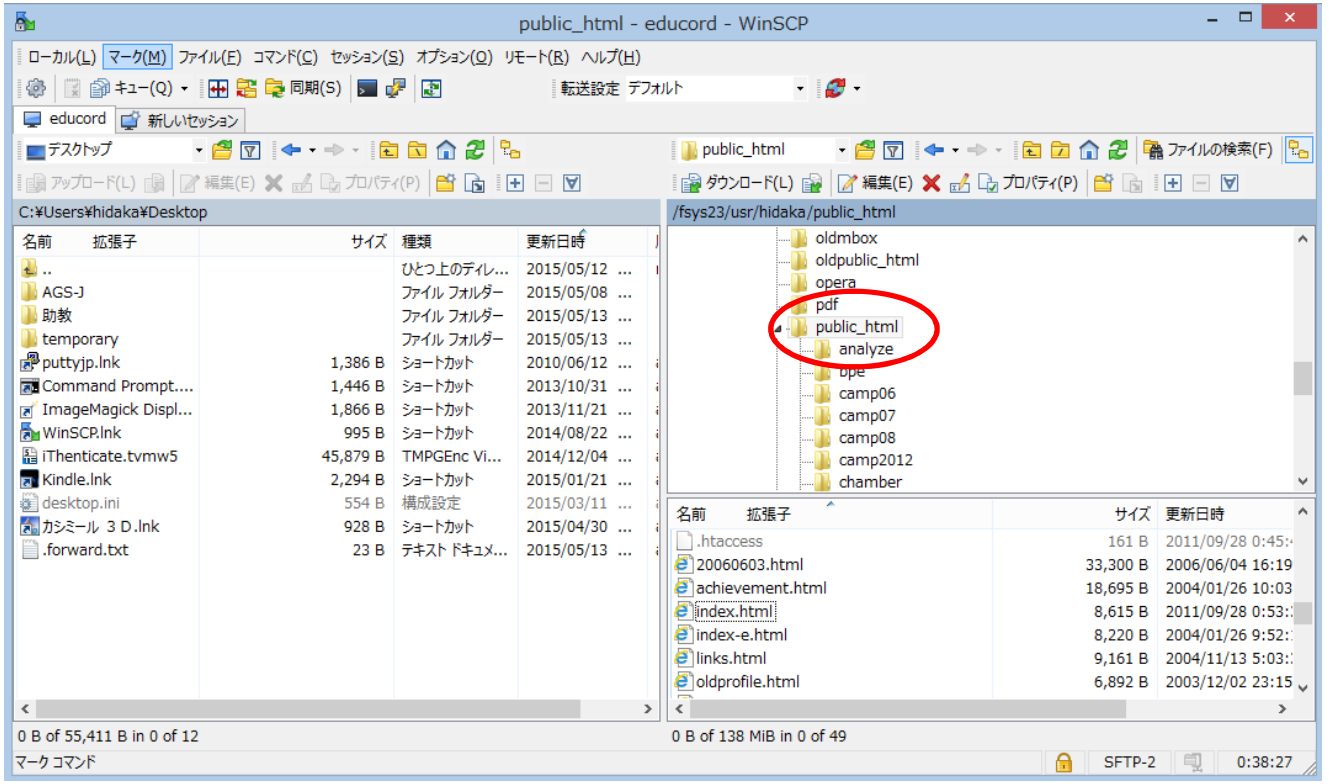
```
member1@p.u-tokyo.ac.jp
member2@mail.ecc.u-tokyo.ac.jp
member3@gmail.com
member4@yahoo.com
```

- 携帯アドレス宛のメールは、キャリア／端末の設定によっては届かないことがある
- MLに送信した場合、自分自身には届かない（対策を調査中）

1. コンピュータ／スマホ／タブレットをネットワークに接続する （学部・大学院）
2. セキュリティ対策 （学部・大学院）
3. メールを読む （大学院）
4. サーバにログインする （大学院）
5. メールを転送する （大学院）
6. メーリングリストを開設する （大学院）
7. ホームページを公開する （大学院）

ホームページの作成

- 各自のホームディレクトリの直下にpublic_htmlというディレクトリを作り、index.htmlを置く（これがトップページとなる）。
- URLはhttp://www.p.u-tokyo.ac.jp/~xxxx
- CGIスクリプト等も使える。WordPress等のCMSについては、一般ユーザも使えるように環境を整備中。



※コンピュータ相談室について

コンピュータ、ネットワークに関する相談事を受け付けます

担当教員（特任助教）：　日高 一郎

部屋：武田先端知ビル314（移転期間中）／教育学部棟459A（移転終了後）
　　メールでアポイントを取ってから来てください（技術的な準備のため）
連絡先：
　pmaster@p.u-tokyo.ac.jp　03-5841-1235　内線21235