

2018年度 コンピュータガイダンス

コンピュータ相談室／学校教育高度化・効果検証センター 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 (学部・大学院)
利用ガイドライン／セキュリティ・ポリシー
- 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>

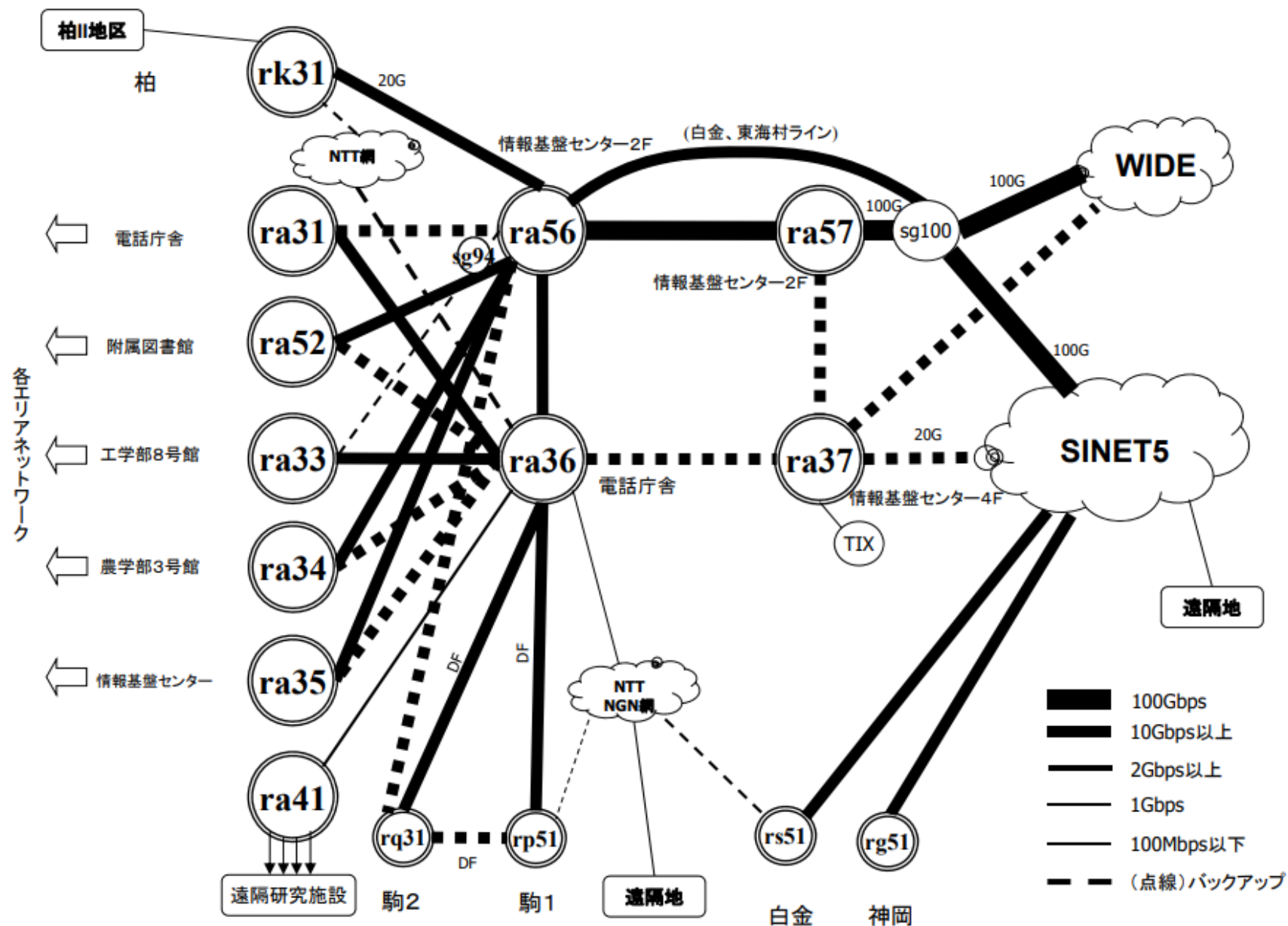
<http://www.p.u-tokyo.ac.jp/~hidaka/guidance/ComputerGuidance2018.pdf> (cg2016 / 21235)

<http://www.p.u-tokyo.ac.jp/~hidaka/guidance/ComputerGuidance2018.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. メール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

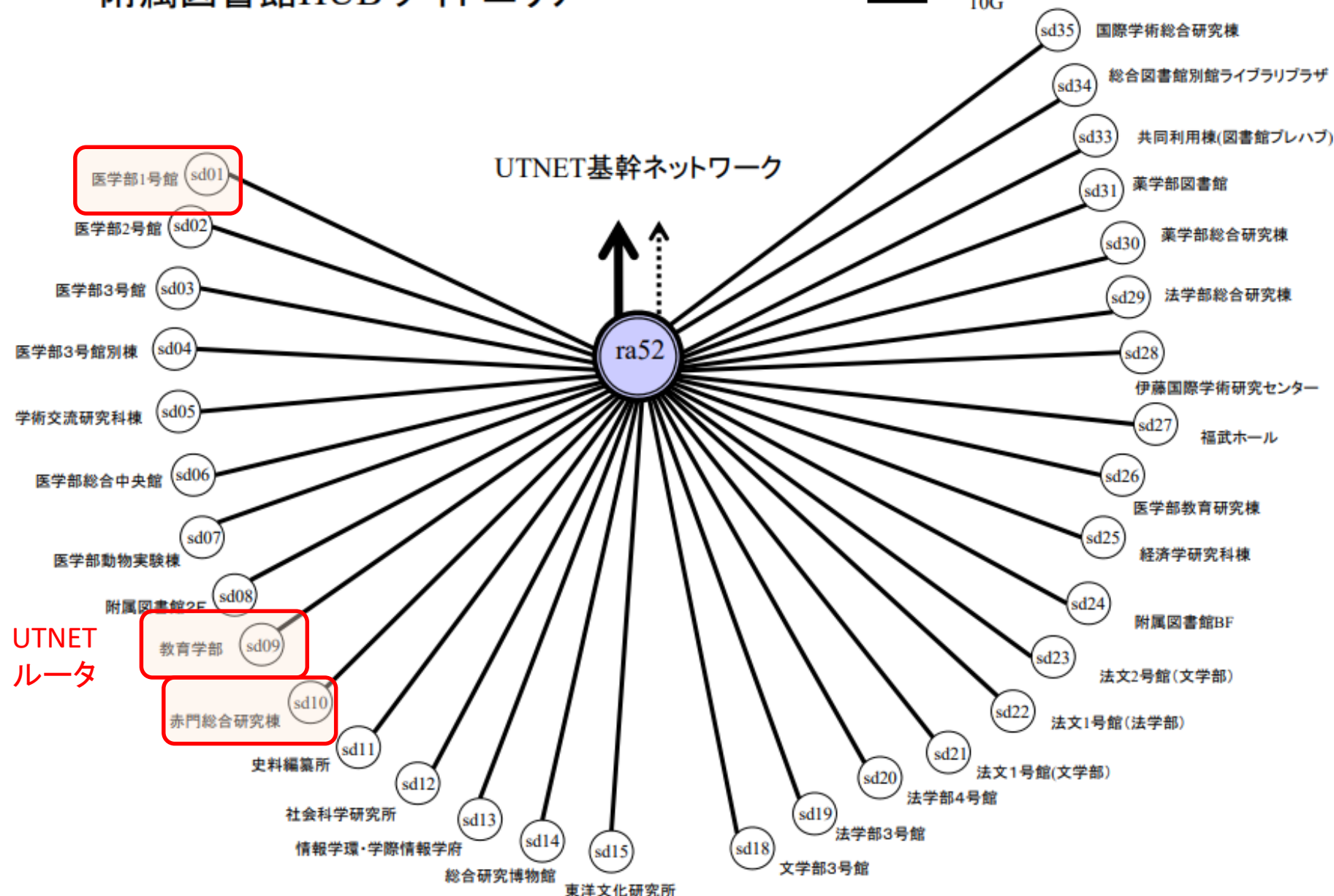
2018.3.29



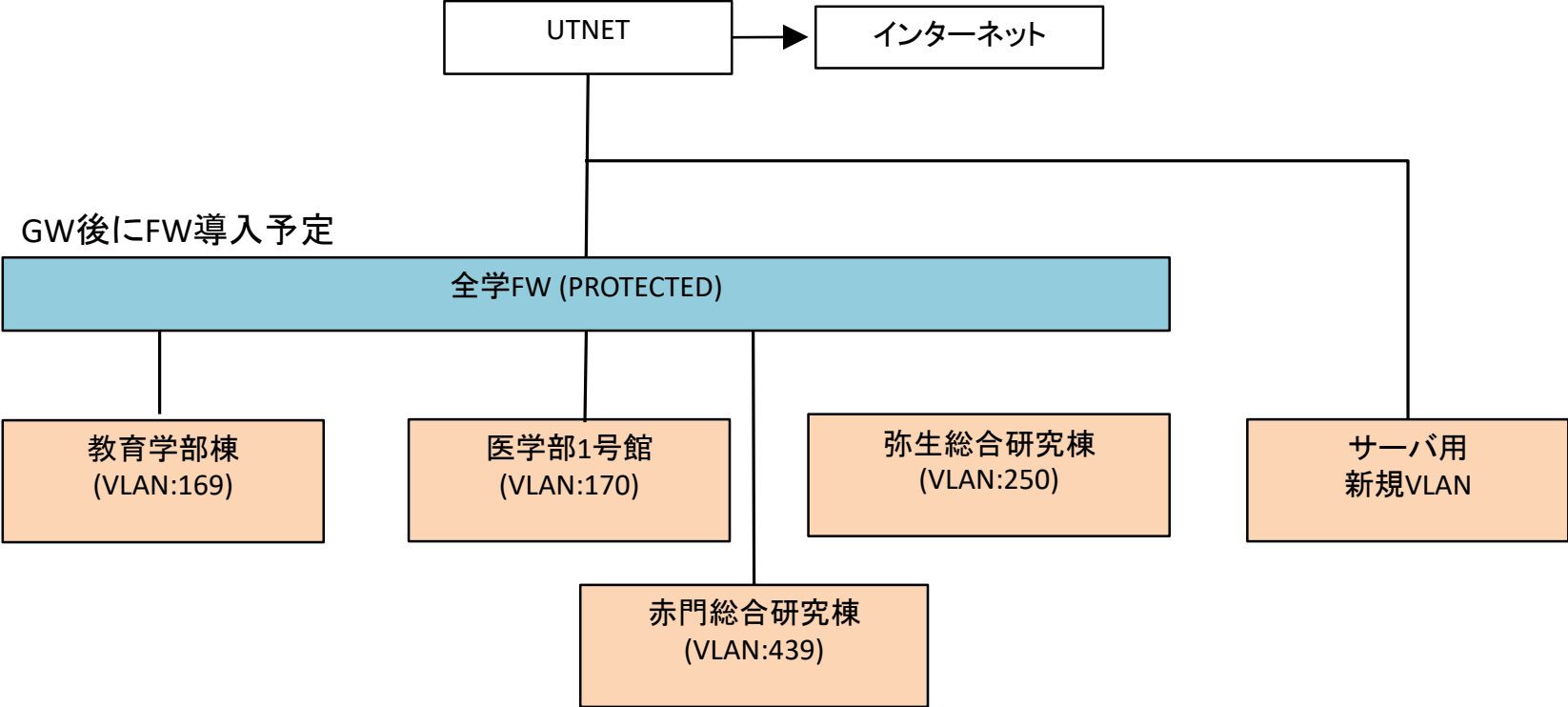
2017.10.26

附属図書館HUBサイトエリア

100M以下
 1G
 10G



研究科ネットワークと全学セキュリティファイアウォール



ネットワーク設定	教育学部棟内部	総合研究棟(農学部)	赤門総合研究棟	医学部1号館
IPアドレス範囲	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
IPアドレス割り当て	固定、DHCP	固定	固定	固定、DHCP

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

教育用計算機システム
(ECCS)



UTokyo WiFi



ハブ

有線

DHCPまたは
固定アドレス

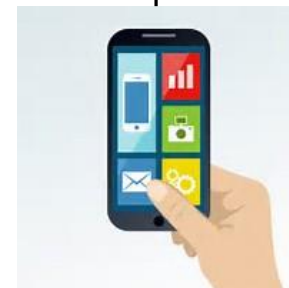


研究室
無線AP

グローバルまたは
ローカルアドレス



各研究室で管理



大学のネットに繋ぐ、その前に...



情報倫理・コンピュータ利用 ガイドライン



情報ネットワークとコンピュータを適切・安全に利用するために

P.2

Guidelines for Information Ethics and Computer Use

Using the University Information Network and Computers in a Safe and Proper Manner

P.4

信息伦理及计算机利用 指南



正确、安全地利用信息网络和计算机 *原文为日文。

P.6

정보윤리·컴퓨터 이용 가이드라인



정보 네트워크와 컴퓨터를 적절하고 안전하게 이용하기 위하여 *원문은 일본어입니다.

P.8

こういうことは…情報倫理違反です

The Following Activities Violate Information Ethics:

以下行為……都是违反信息伦理的行为。

이런 경우는…정보윤리 위반입니다

P.10



2018.3

<http://www.cie.u-tokyo.ac.jp/guidelinepanl.par>

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。

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い、または業務を一時的に代行してもらいなどの目的で、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入り出す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。本学では、通信内容に情報セキュリティ上の問題がないかについて、機械的な検知や遮断を行うことがあります。

大学院教育学研究科・教育学部
部局CERT 各位

C&C サーバとの通信に関する調査依頼

UTokyo-CERT です。貴部局の

133.11.201.XX

について、C&C サーバ (command and control server: 外部から侵入したコンピュータに対して当該コンピュータを制御したり命令を出す役割を持つサーバのこと) と考えられるアドレスに対して通信が行われている可能性があるかと連絡を受けました。

今回連絡を受けた C&C サーバの IPアドレスは、102.83.113.XXX で、(現在は本学からは通信できない状況のようですが)

<https://www.virustotal.com/ja/ip-address/102.83.113.245/information/>

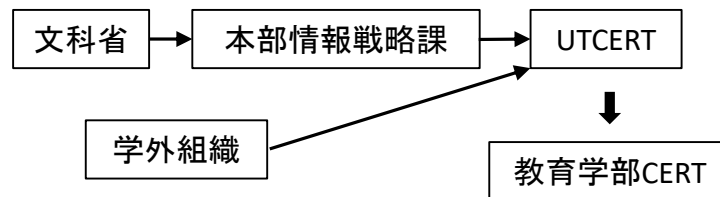
によると、このアドレスの UDP/6711 に向けた通信を行う virus が検知されている様です。

そこで、UTokyo-CERT でも、2016年9月12日と2016年9月20日の学内から学外に向けた通信を調べたところ、以下に示す時間帯に該当するパケットが出ていることが確認されましたので、ご連絡いたします。
上記の機器から、意図しない通信が行われていないかの調査にご協力ください。

インシデントに該当する事態の機器が確認された場合には、インシデントレポートシステムを用いて、貴部局にてインシデントを発行していただき、レポートとして報告していただけますよう、よろしく願いいたします。

不明な点は UTokyo-CERT までご連絡下さい。

UTokyo-CERT
<https://cert.u-tokyo.ac.jp/>



「東京大学情報セキュリティ・ポリシー」も参照
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)？
- 「UTokyo WiFiアカウントメニュー」のページは国内限定

注意 (Notice)

- UTokyo WiFiのアカウントを使用するにはUTokyo Accountが必要
You must be issued "UTokyo Account" to make UTokyo WiFi account.
- 事前に UTAS 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)
You must register your e-mail address on UTAS previously if you are a student.
 - UTAS での登録は、翌日以降に反映されます。
Registrations on UTAS will be applied tomorrow or after.
- 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。
You can get your account information via e-mail you registered on UTAS.
- 2台目以降も同じアカウントで使用できます。
You can use the same account on all of your devices.
- 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。
Your old UTokyo WiFi account will be expired by the end of April or October. You can issue new UTokyo WiFi account since the start of April or October.
- 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。
Please refer [this official web site](#) as well.

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

教育用計算機システム
(ECCS)

UTokyo WiFi

ハブ

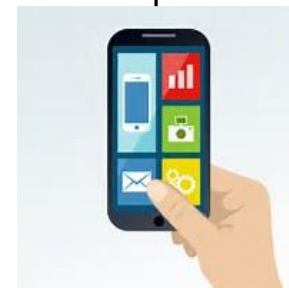
有線

DHCPまたは
固定アドレス

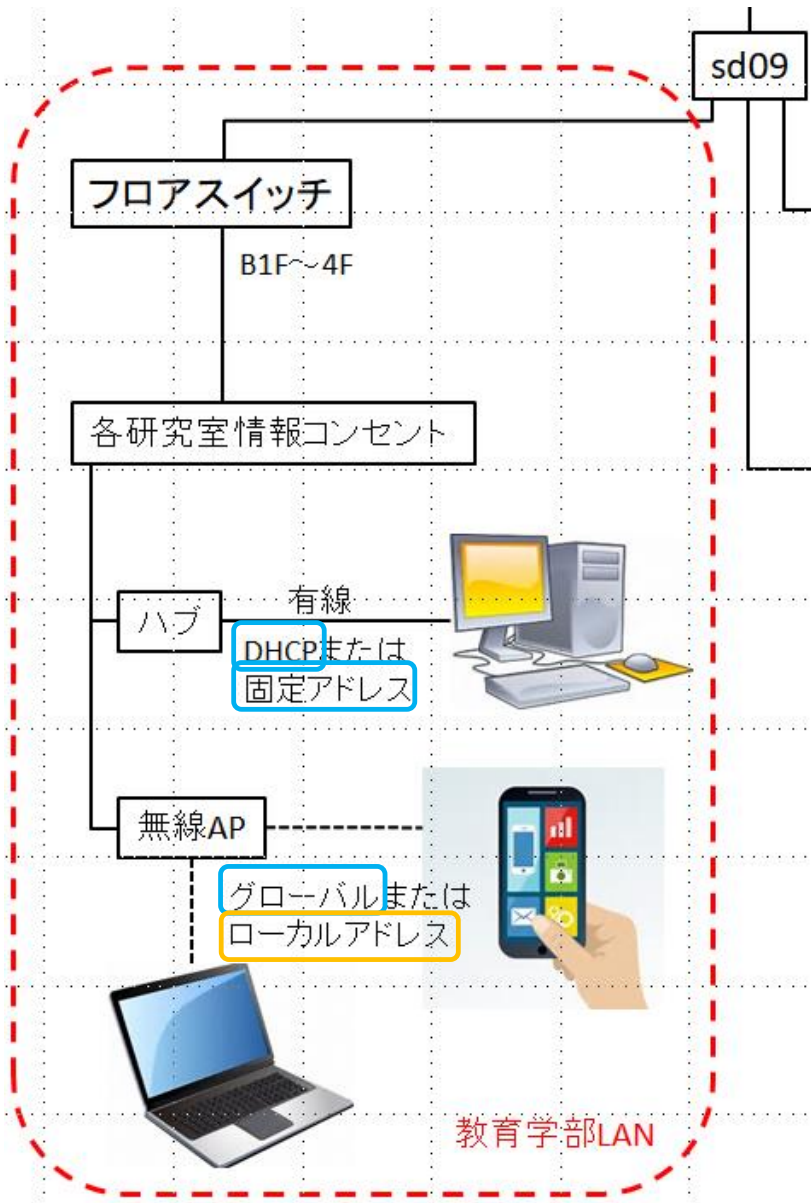
無線AP

グローバルまたは
ローカルアドレス

各研究室で管理



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・研究室的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。

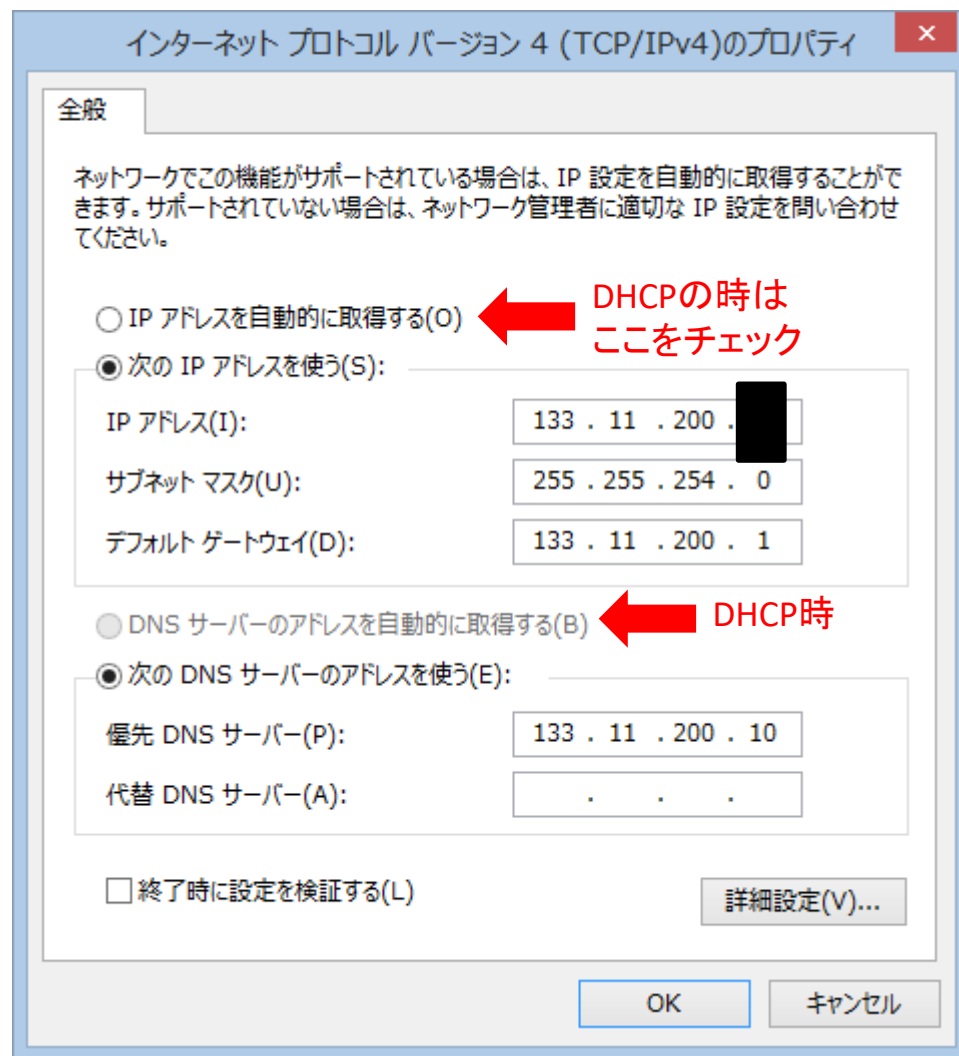
MacOS の場合：

「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)



固定アドレス時のネットワーク設定

教育学部のコンピュータ利用について

一般的な情報

- 学内のコンピュータ・ネットワーク構成の概要
- 教育学部で運用しているサーバについて



教育学部のコンピュータを利用するには

「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。

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)

- 東大教職員対象。学生の場合は指導教員からの申し込みが必要
- 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 for Mac Standard 2016	12,500
Visio Standard 2016	3,900
Visual Studio Professional 2015	7,600
Windows 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

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

ウイルス対策ソフトウェア

ソフトウェア	メーカー(リンク)	経費	問い合わせ先
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)	トレンドマイクロ社	1,000円/年 (1台) *	anti-virus@itc.u-tokyo.ac.jp
Server Protect for Windows(Windowsサーバ)		5,000円/年 (1台)	
Server Protect for Linux(Linux環境)		10,000円/年 (1台)	
Sophos Anti-Virus(Windows版、Mac版)	Sophos	1,000円/年 (1台) *	
ESET Endpoint Security(Windows版、Mac版)	Canon IT ソリューションズ	1,000円/年 (1台) *	
Symantec Endpoint Protection(Windows版、Mac版)	株式会社Symantec	1,000円/年 (1台) *	

研究用ソフトウェア

ソフトウェア	メーカー(リンク)	経費	問い合わせ先
三次元CADソフト Creo	PTCジャパン	20,000円/年 (1申請)	proengineer@itc.u-tokyo.ac.jp
統計解析ソフト JMP Pro	SAS Institute Japan株式会社	10,000円/年 (1申請)	jmp@itc.u-tokyo.ac.jp
統計解析ソフト SAS	SAS Institute Japan 株式会社	50,000円/年 (1台)	sas@itc.u-tokyo.ac.jp
数式処理システム Mathematica	Wolfram Research	50,000円/年 (1申請)	mathematica@itc.u-tokyo.ac.jp
統合化学ソフト Chem Office	Perkin Elmer社	40,000円/年 (1申請 5台まで)	chemoffice@itc.u-tokyo.ac.jp
システム開発ソフト LabVIEW	ナショナルインスツルメンツ株式会社	50,000円/年 工学部は 新規年額2万円 継続年額1万円 (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

Office

新しい 2016 アプリを使って Office 365 ProPlus をインストールします [Office 2013 はどうなったのでしょうか?](#)

これにより、お使いのコンピューターに次のアプリがインストールされます: Word、Excel、PowerPoint、OneNote、Access、Publisher、Outlook、Skype for Business、OneDrive for Business



Word



Excel



PowerPoint



OneNote



Access



Publisher



Outlook



Skype for
Business



OneDrive
for Business

【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. メール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(全学FW)

PROTECTED 内で利用者端末にて「出来ないこと」(例)

- 学内(当該部局 PROTECTED を除く)・学外への公開を目的としたサーバの設置

例: Web サーバ、ファイル共有サーバ、プリンタサーバなど

- 学内(当該部局 PROTECTED を除く)・学外から PROTECTED 内の機器に対する通信(こうした通信を必要とする機器は、第1段階の時点で PROTECTED に含めず、現行の構成と運用を継続)

例: Polycom など学内(当該部局 PROTECTED を除く)・学外からの着信が必要なオンライン会議システムは利用できない

例: SSH を用いて学内(当該部局 PROTECTED を除く)・学外から PROTECTED 内に設置された機器へ接続できない(ただし、部局 PROTECTED 内の機器間では可能)

- 違法コンテンツの共有に利用されている主要な P2P アプリケーションの利用(BitTorrent などの P2P ファイル共有など)

ただし、Skype、QQ、WeChat 等の主要なメッセージング用 P2P アプリケーションは対象外とする。P2P アプリケーションの判定は Palo Alto Networks 社の NGFW である PA-5060 にて自動で行われる。

- 外部の悪性サイト等への通信

フィッシング、マルウェア配布サイトといった悪性サイト(C&Cを含む)に対する通信は遮断される。悪性サイトの判定は P2P アプリケーションと同じくファイアウォール装置 PA-5060 にて、データベースに基づき自動で行われる。

全学ファイアウォールに関する情報

<http://www.ut-portal.u-tokyo.ac.jp/wiki/index.php/全学ファイアウォール整備>
(東大ポータル > 便利帳 > 情報システム本部)

セキュリティ対策(続き)

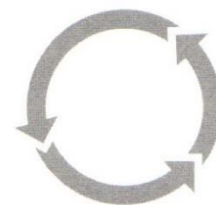
セキュリティ対策は「多層防御」で

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



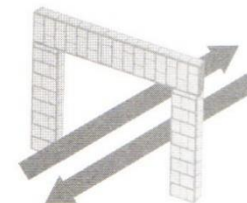
(2) セキュリティ更新プログラムを適用
→ 計画的に適用、更新する



(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



もしも社長が
セキュリティ対策を
聞いてきたら

Yuichi Kuramoto
蔵本 雄一
日経コミュニケーション 監

「なるほど分かった!」と
言わせる
秘訣

「小難しい専門技術の話は
極力避ける」
「マーケティング手法の
考え方を取り入れる」
「ビジネスインパクトを明確に伝える」

セキュリティをもっと知りたい
非エンジニアの方にもおすすめ!

日経BP社

将来はAI型のセキュリティ対策に移行するかも
(例) Cylance PROTECTなど

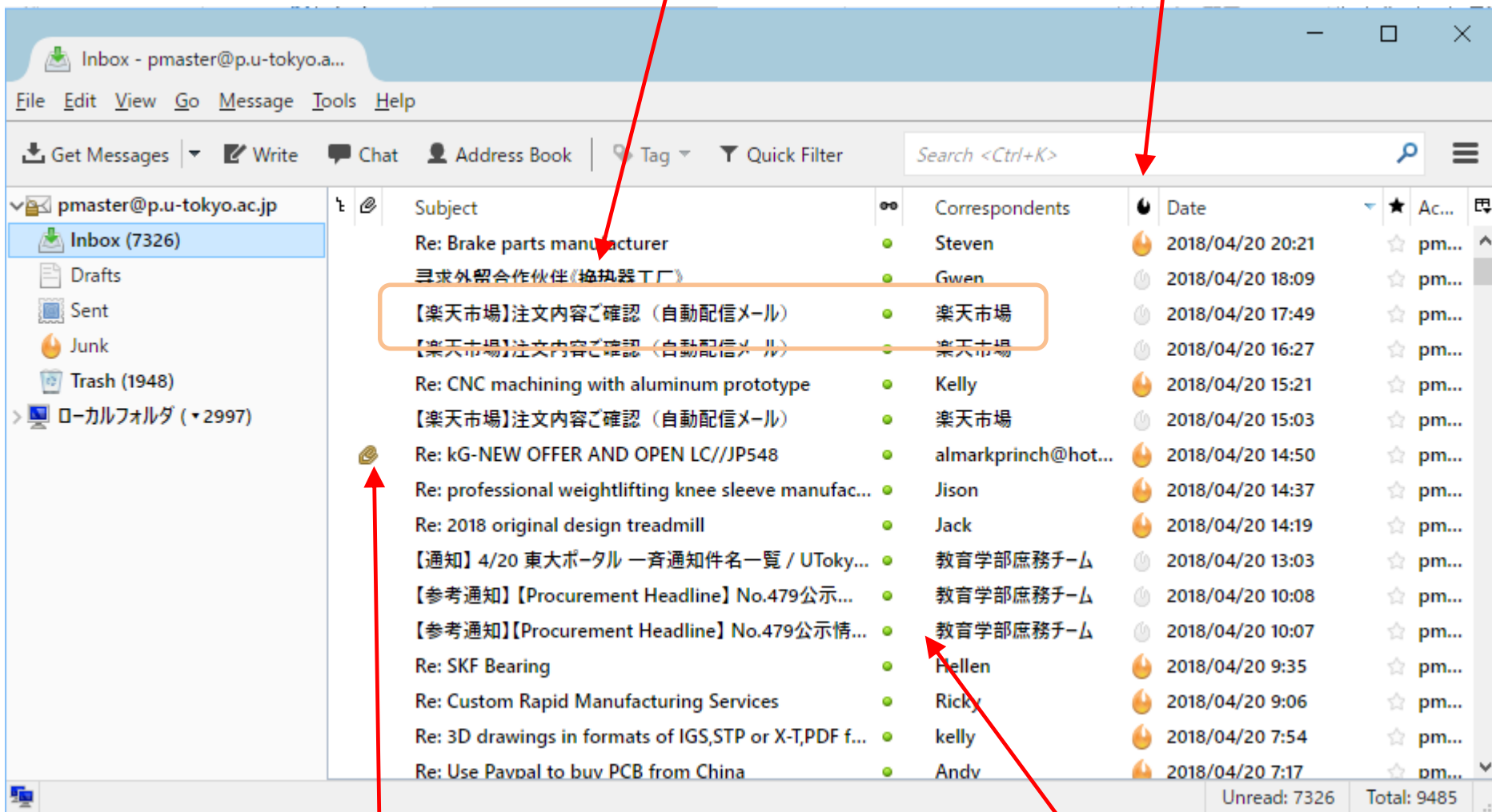
具体的な対策:

- 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

不審(?)なメールが届いたら...

日頃使わない
言語・文字

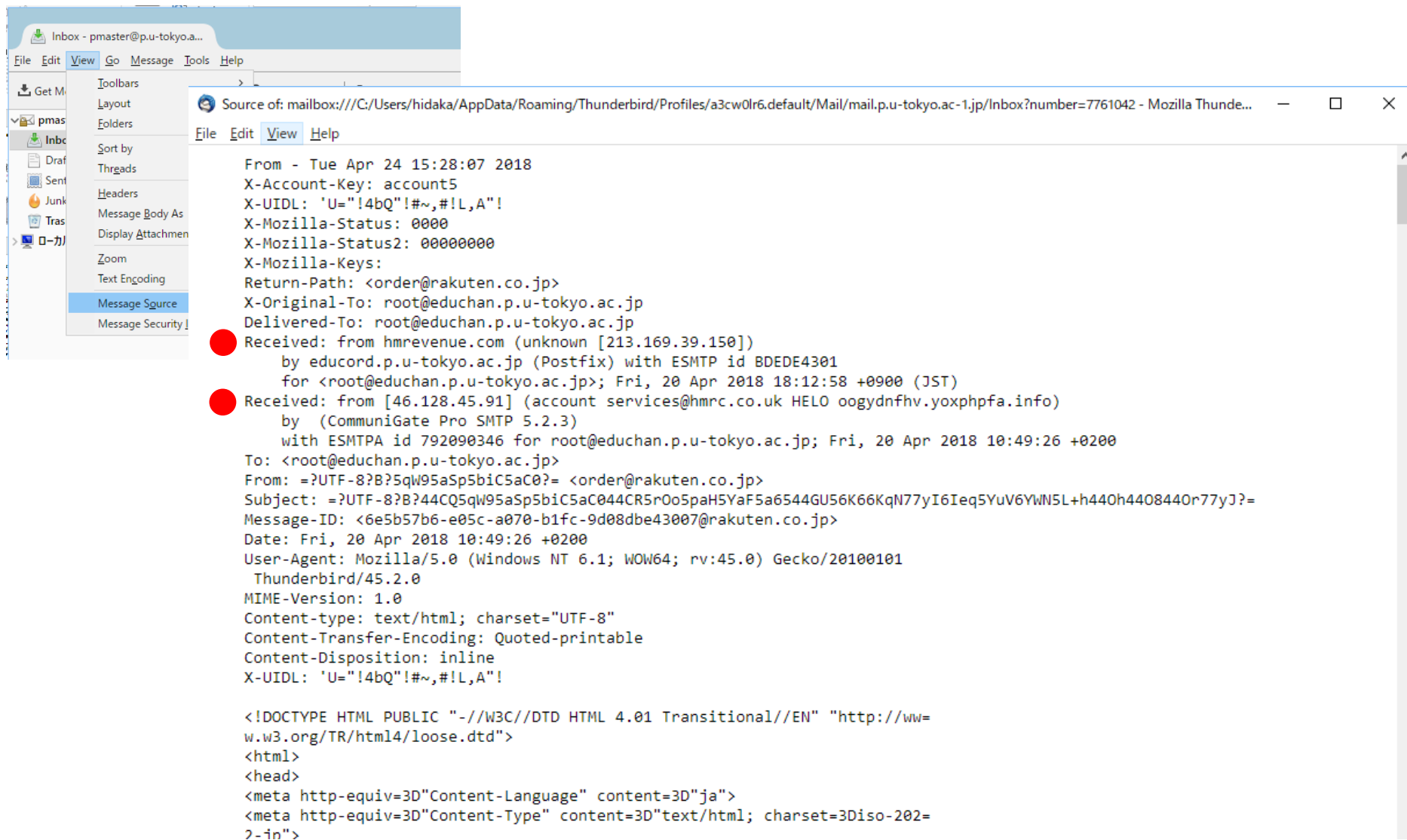
参考程度に



マルウェア添付の可能性
添付ファイルがなくてもリンクがあるかも

アカウント偽装
の可能性

メッセージを開くと、メールソフトの設定によっては画像から感染することがある。
開かずに、ソース(特にヘッダ)をしてみる。



ヘッダ部分は偽装可能だが、信頼できる情報はあ

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

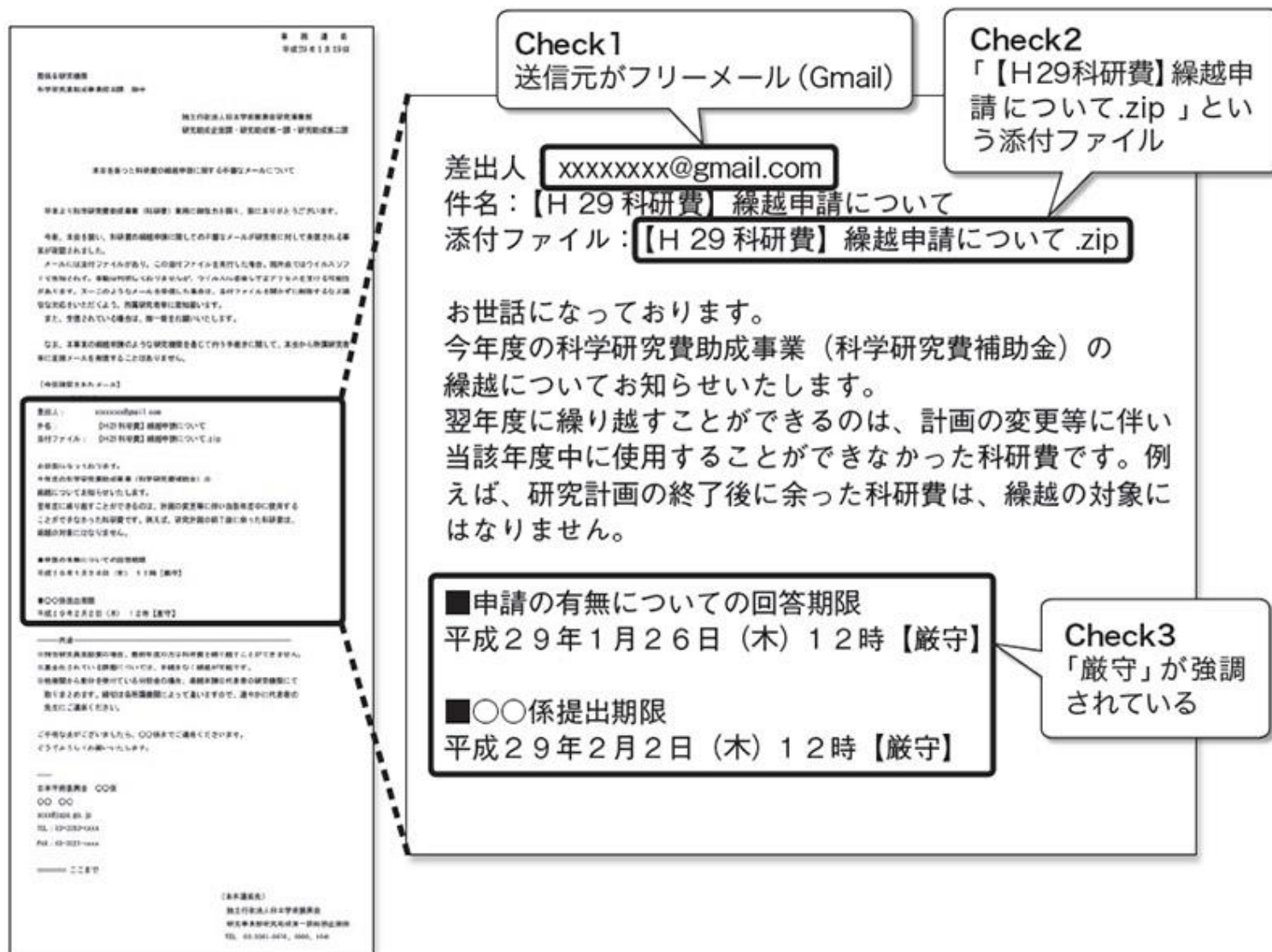


標的型攻撃メール

	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

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

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



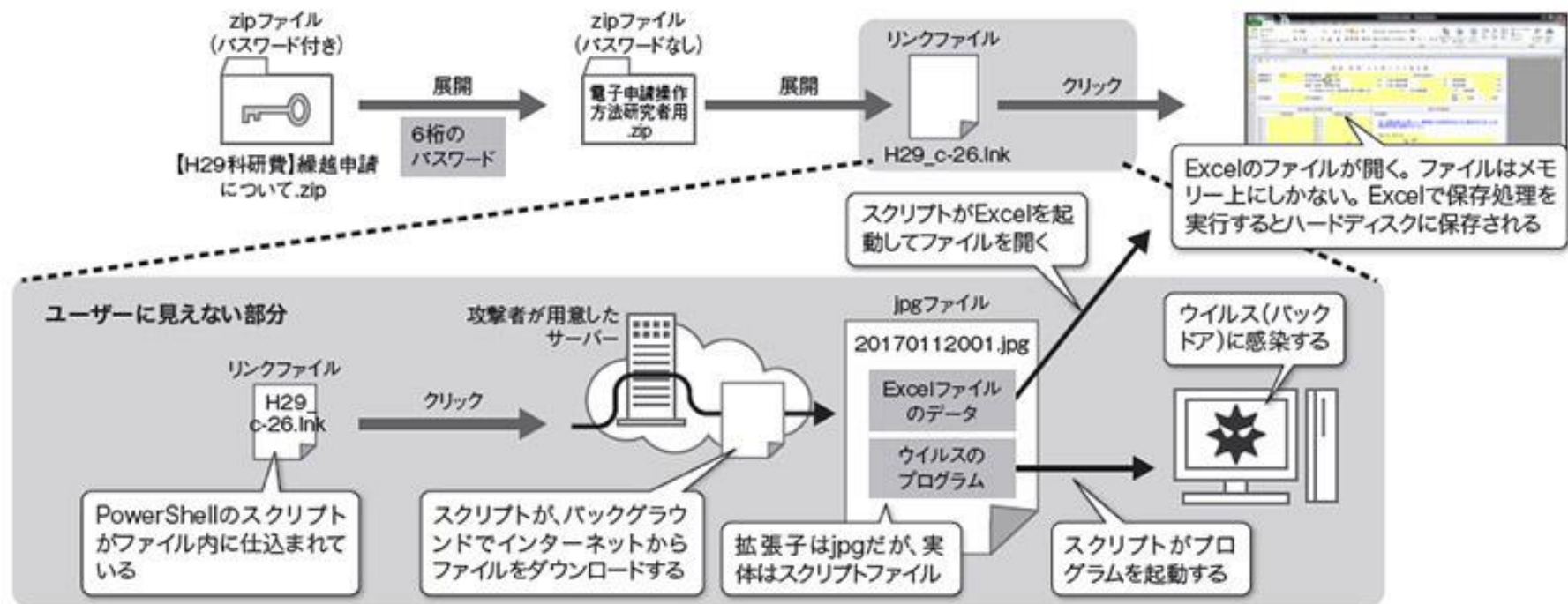


図3●添付ファイルをクリックするとExcelファイルが表示、バックグラウンドでウイルス感染

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。

防弾ホスティングサービスを使用

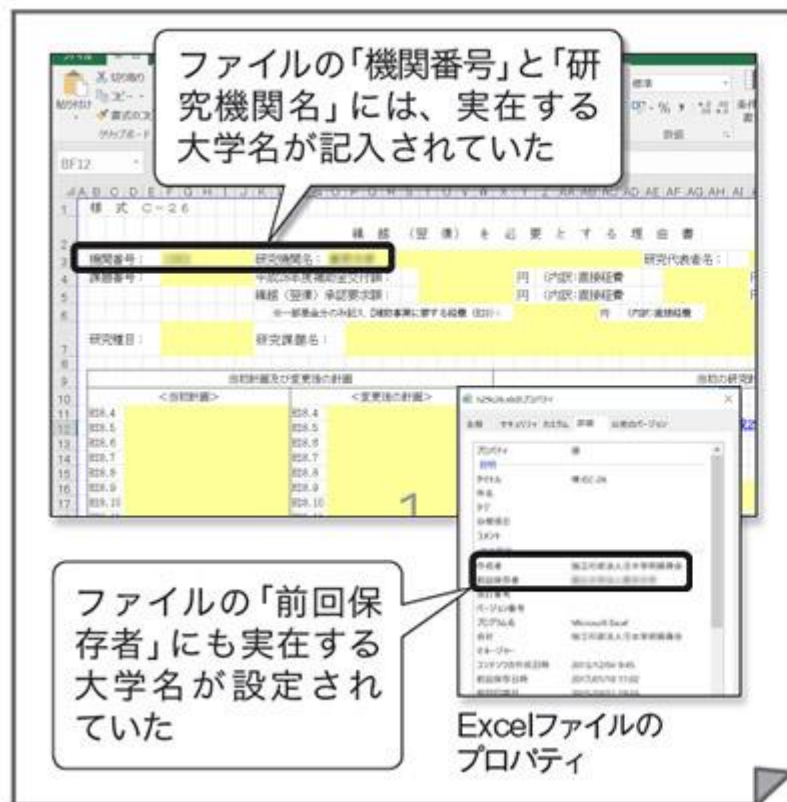
<https://gigazine.net/news/20170511-most-dangerous-town-on-the-internet/>

20170112001.jpgに含まれるExcelファイル

ファイルの「機関番号」と「研究機関名」には、実在する大学名が記入されていた

ファイルの「前回保存者」にも実在する大学名が設定されていた

Excelファイルのプロパティ



サーバーから見つかった別のファイル



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。

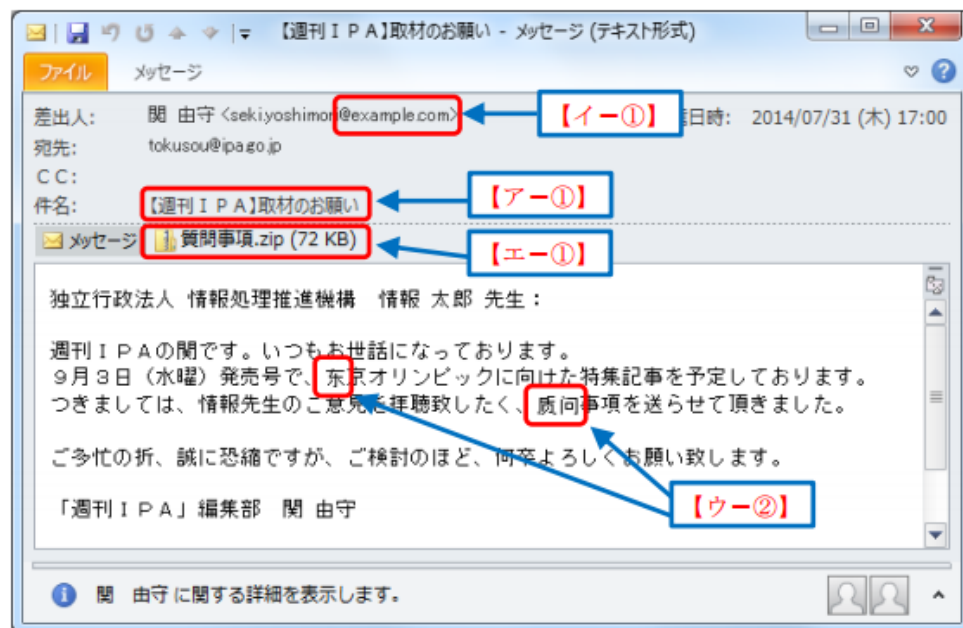
これらの特徴に複数合致するメールを受信した場合は、標的型攻撃メールの可能性があるので、注意して対応する必要がある。対応方法については、「3. 標的型攻撃メールへの対応」を参照いただきたい。

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

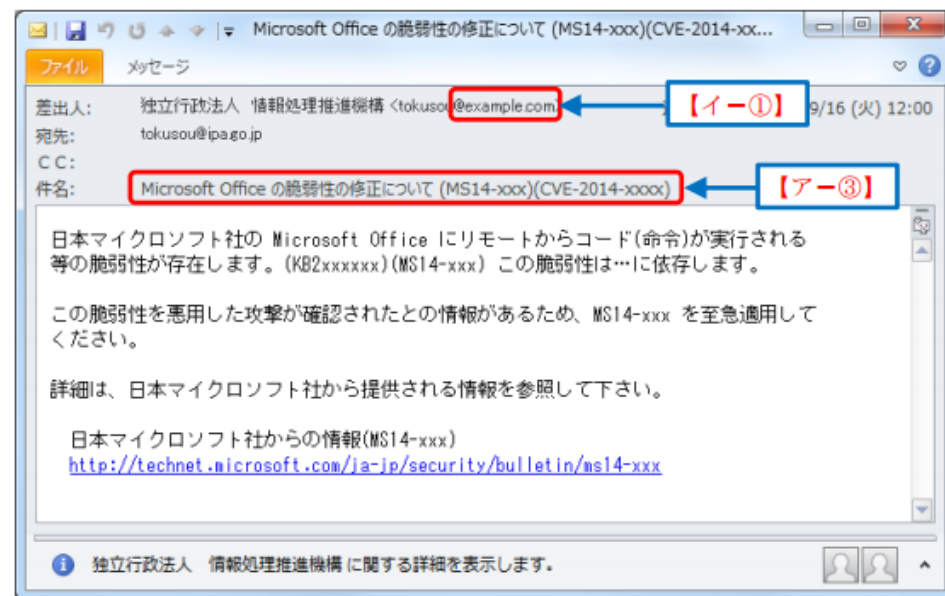
	(例 1) 人事情報 (例 2) 新年度の事業方針 (例 3) 資料の再送、差替え
	⑤ 心当たりのない、決裁や配送通知（英文の場合が多い） (例 1) 航空券の予約確認 (例 2) 荷物の配達通知
	⑥ ID やパスワードなどの入力进行要求するメール (例 1) メールボックスの容量オーバーの警告 (例 2) 銀行からの登録情報確認
(イ)差出人のメールアドレス	① フリーメールアドレスから送信されている ② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
(ウ)メールの本文	① 日本語の言い回しが不自然である ② 日本語では使用されない漢字（繁体字、簡体字）が使われている 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

2.2.1. 新聞社や出版社からの取材申込のメール



※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。

2.2.4. セキュリティに係る注意喚起のメール



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为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て「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。

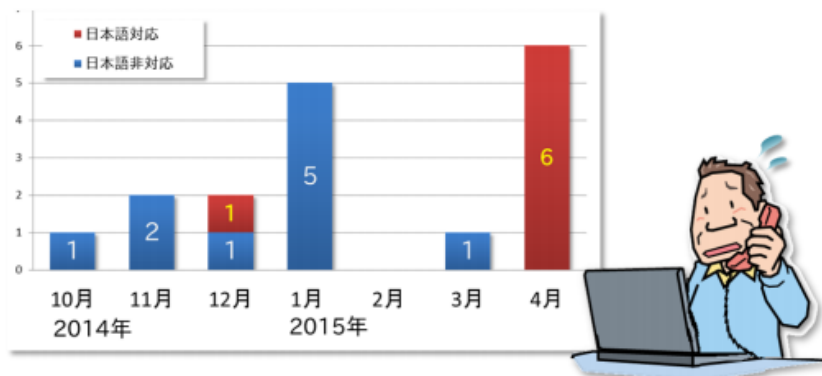


図 1：ランサムウェアに関する相談件数の推移

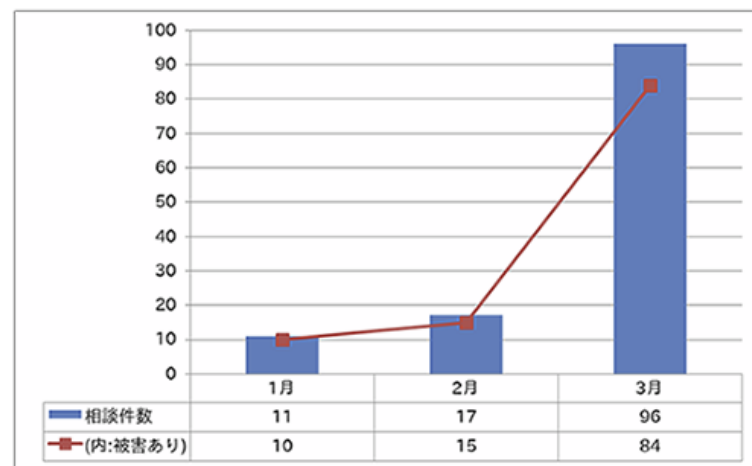


図.ランサムウェアに関する相談の月別推移（2016年1月～3月）

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. メール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

アカウント設定

mail.p.u-tokyo.ac.jp

- サーバ設定
- 送信控えと特別なフォルダ
- 編集とアドレス入力
- 迷惑メール
- ディスク領域
- 開封確認
- セキュリティ
- ローカルフォルダ
 - 迷惑メール
 - ディスク領域
 - 送信 (SMTP) サーバ

アカウント操作(A)

サーバ設定

サーバの種類: POP メールサーバ

サーバ名(S): mail.p.u-tokyo.ac.jp ポート(P): 995 既定値: 995

ユーザ名(N): hidaka

セキュリティ設定

接続の保護(U): SSL/TLS

認証方式(I): 通常のパスワード認証

サーバ設定

☒ 新着メッセージがないか起動時に確認する(C)

☒ 新着メッセージがないか(Y) 60 分ごとに確認する

☐ 新着メッセージを自動的にダウンロードする(M)

☐ ヘッダのみ取得する(E)

☐ ダウンロード後もサーバにメッセージを残す(G)

☐ ダウンロードしてから(Q) 7 日以上経過したメッセージは削除する

☐ ダウンロードしたメッセージを削除したらサーバからも削除する(D)

メッセージの保存

☐ 終了時にゴミ箱を空にする(X) 詳細(V)...

メッセージの保存先:

C:\Users\hidaka\AppData\Roaming\Thunderbird\Profiles\{a3cw0lr6.default}\Mail\10.2 参照(B)...

OK キャンセル

詳しい設定は、こちら:

送信 (SMTP) サーバ

設定

説明(D): securemail.p.u-tokyo.ac.jp

サーバ名(S): securemail.p.u-tokyo.ac.jp

ポート番号(P): 587 既定値: 587

セキュリティと認証

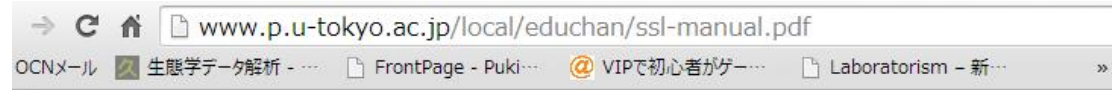
接続の保護(N): STARTTLS

認証方式(I): 通常のパスワード認証

ユーザ名(M): hidaka

OK キャンセル

- 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？



メールクライアントの SSL 対応設定マニュアル

1. 設定に必要な項目と設定値

教育学部サーバでのメールの送受信を SSL 対応させるには、使用するメールクライアントで、メール受信・メール送信それぞれ以下の値が設定されている必要があります。

メール受信

サーバ名: mail.p.u-tokyo.ac.jp ポート: 995

セキュリティ設定

接続の保護: SSL

認証方式: パスワード認証

メール送信

サーバ名: securemail.p.u-tokyo.ac.jp ポート: 587

セキュリティ設定

接続の保護: STARTTLS

認証方式: パスワード認証

以下、主なメールクライアントでこれらの値を設定する方法について説明します。

Outlook Express, Windows Mail, Windows Live Mail の場合 ⇒ p.2

Office Outlook の場合 ⇒ p.6

Thunderbird の場合 ⇒ p.11

AL-Mail の場合 ⇒ p.16

Mail (Mac OS X) の場合 ⇒ p.21

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. メール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

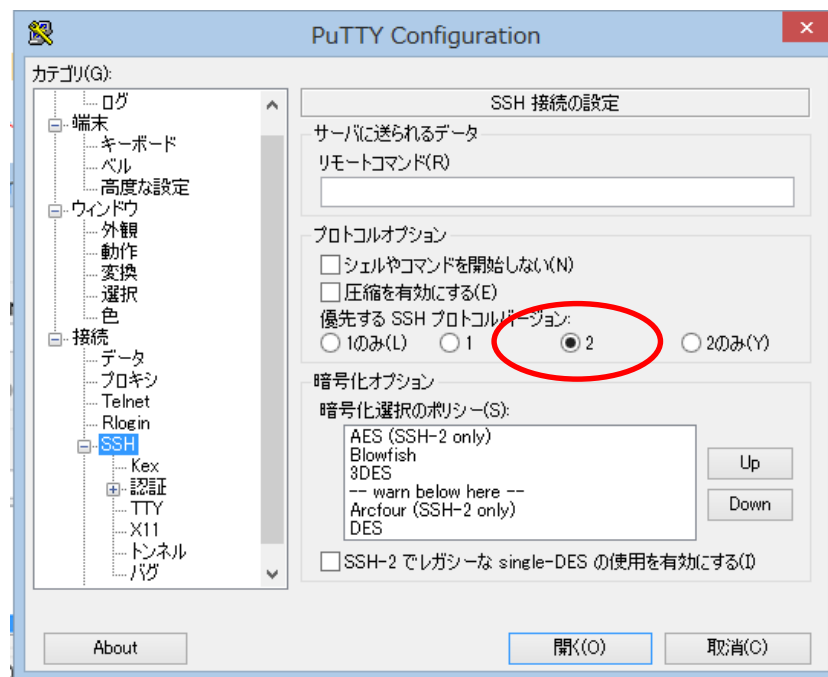
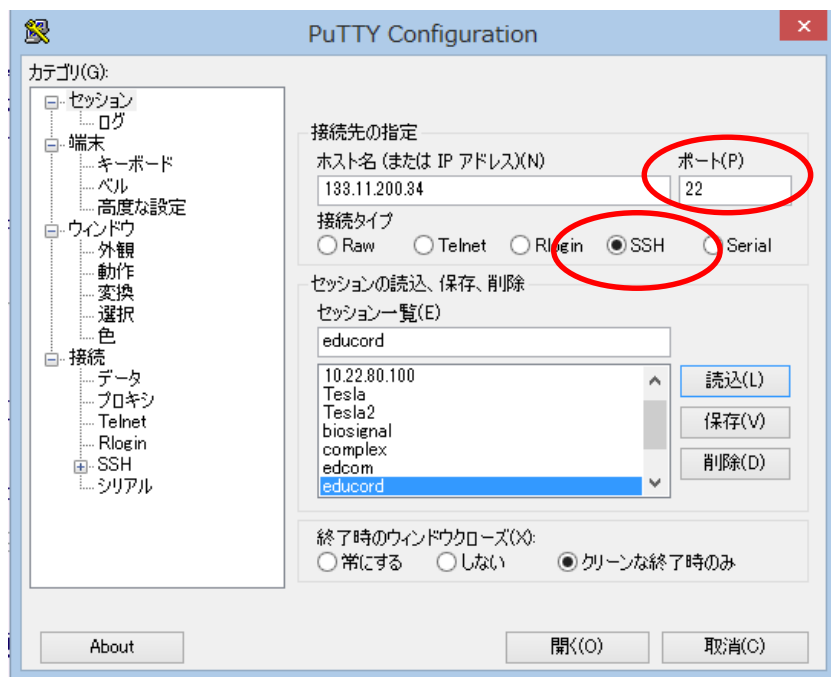
こんな時は、サーバへログインして作業する。

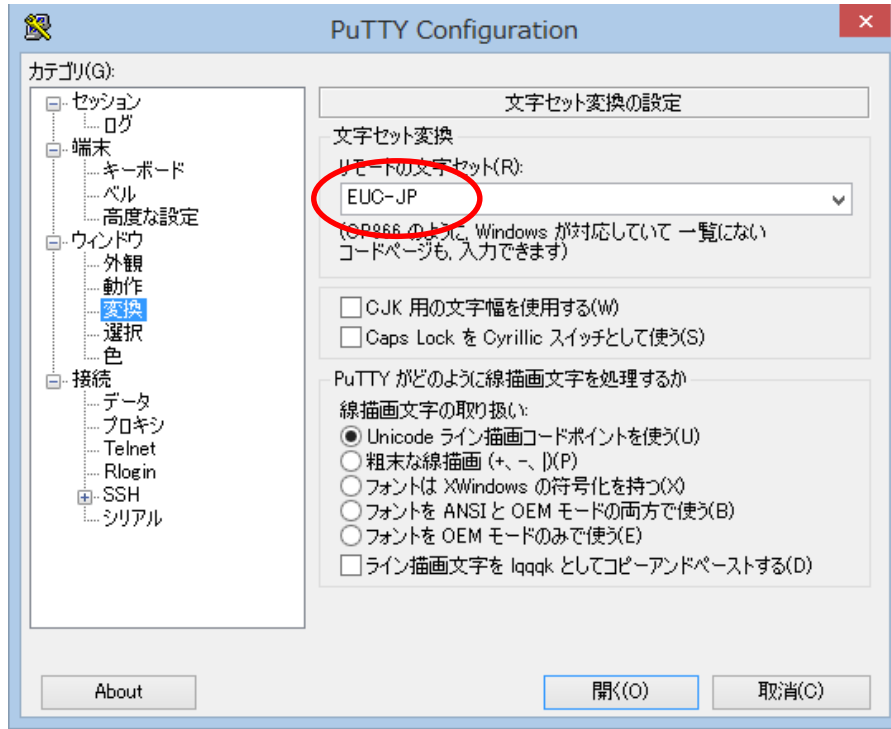
ログイン方法	用途	アプリ名
SSH (Ver.2)	各種コマンドを実行	PuTTY, TeraTerm+TTSSH, sshなど
SFTP	ファイル転送	WinSCP, FFFTPなど

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>





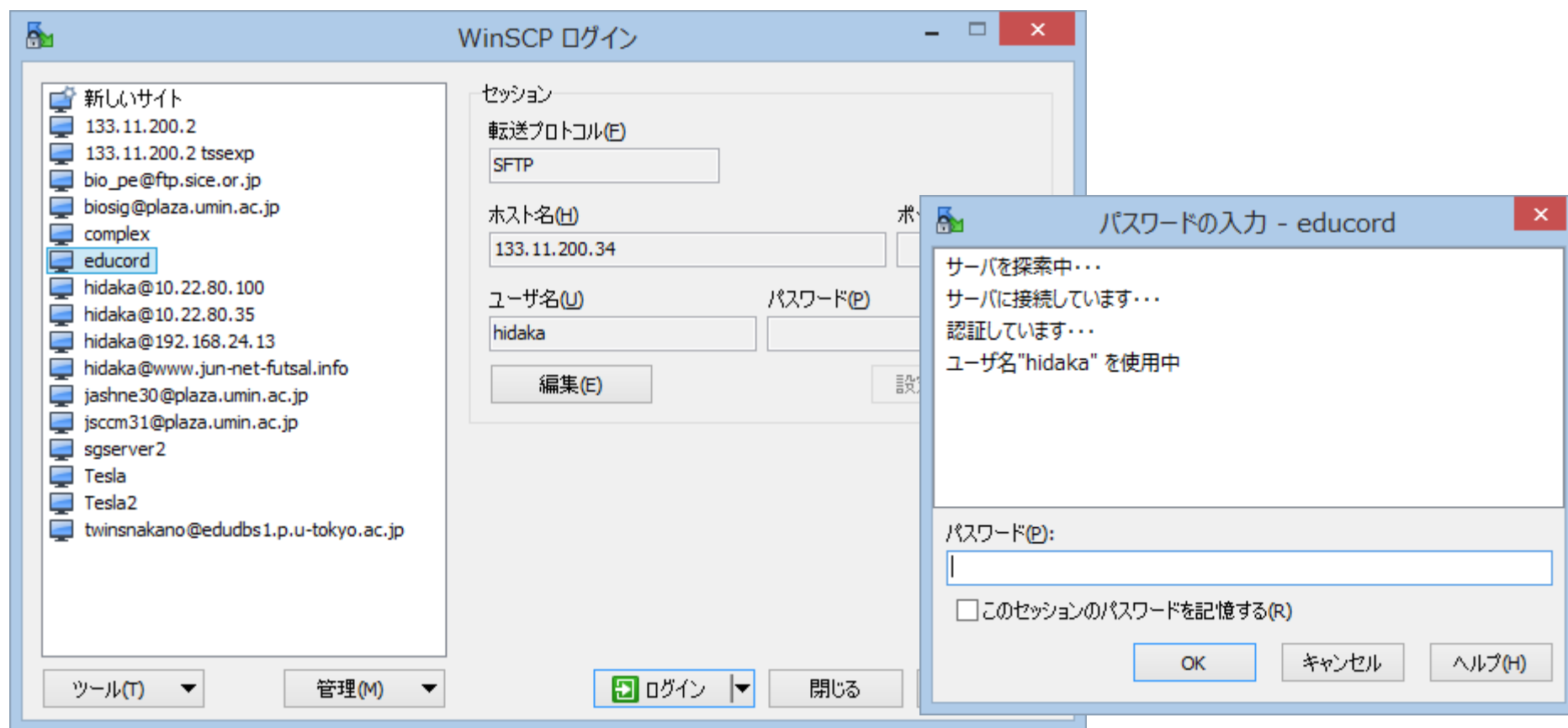
パスワードの変更

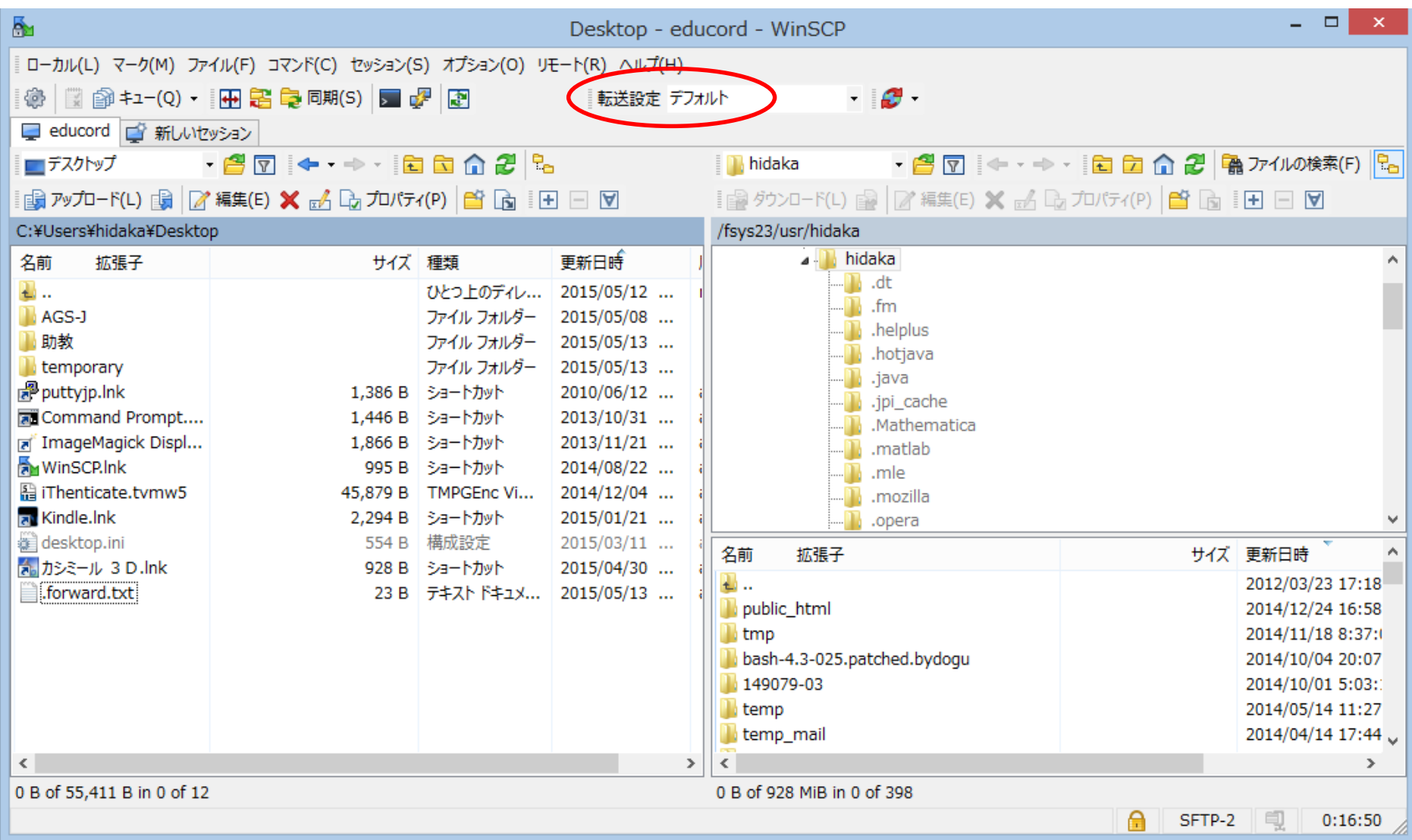
- ログイン後、passwdコマンドを実行する。
- ターミナルでの操作は、Linuxのシェルと各コマンドの知識が必要



(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>



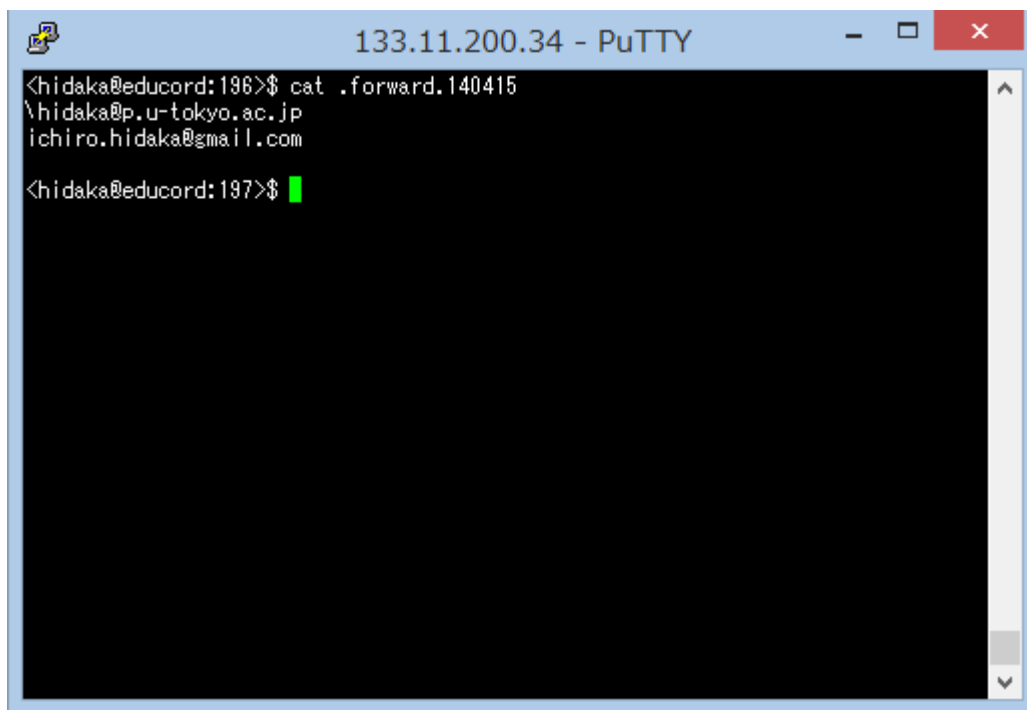


- エクスプローラのような操作感
- 「転送設定」は大抵はデフォルトでよいが、テキスト／バイナリを明示した方がよいこともある。

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。

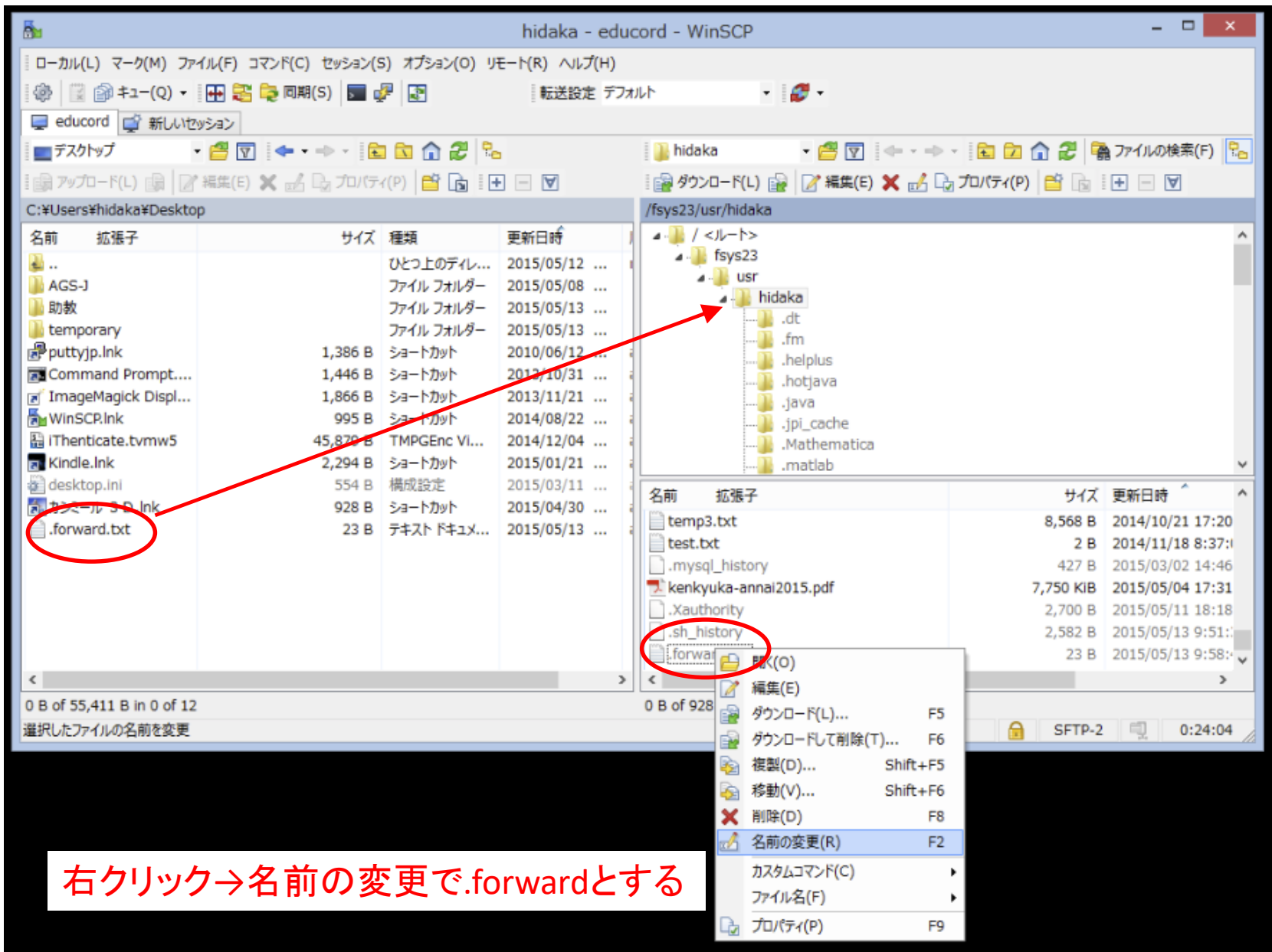


The screenshot shows a PuTTY terminal window titled "133.11.200.34 - PuTTY". The terminal displays the command `cat .forward.140415` and its output, which lists two email addresses: `\hidaka@p.u-tokyo.ac.jp` and `ichiro.hidaka@gmail.com`. The prompt `<hidaka@educord:197>$` is visible at the bottom.

```
<hidaka@educord:196>$ cat .forward.140415
\hidaka@p.u-tokyo.ac.jp
ichiro.hidaka@gmail.com
<hidaka@educord:197>$
```

【注】

「¥」マークは、サーバでは「\」と表記されることがある。



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)

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

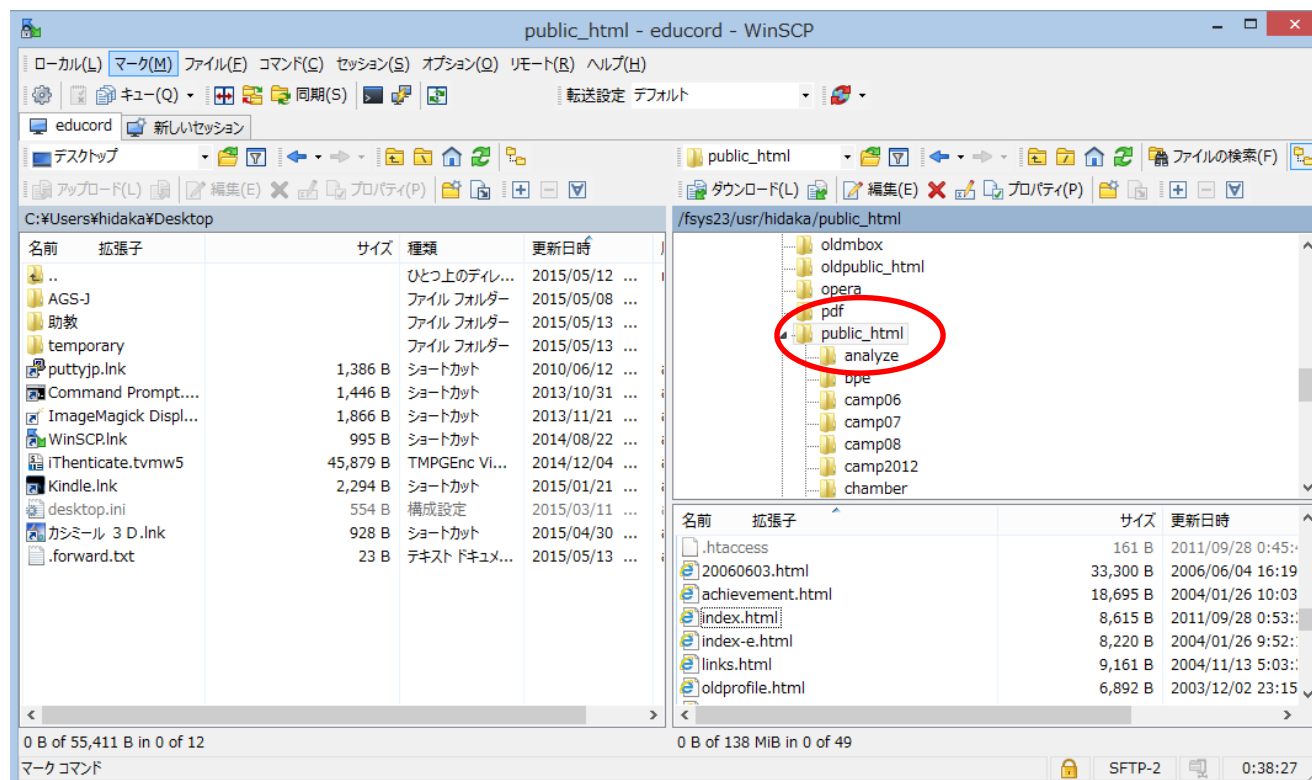
```
member1@p.u-tokyo.ac.jp  
member2@mail.ecc.u-tokyo.ac.jp  
member3@gmail.com  
member4@yahoo.com
```

- 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. メールिंग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:教育学部棟459A

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