令和元年度東北大学サイバーサイエンスセンター講習会

ネットワークとセキュリティ入門

水木敬明

東北大学　サイバーサイエンスセンター
研究開発部　ネットワーク研究部

「ネットワークとセキュリティ入門」

- 日　時：　2019年8月2日(金) 13:30～16:00
- 内　容：　ネットワークを利用する際、危険から自分の身を守るためには、まずネットワークの仕組を理解することが大事です。本講習会では、東北大学のネットワーク TAINS の概要、IP アドレス・ドメイン名、Web や電子メールの仕組みなど、ごく基本的なネットワーク技術について解説します。また、Windows を対象として、セキュリティ上の対策を説明します。
- 受講対象：　初心者

  （本講習会の内容は、**ごく基本的なもの**です。例えば、IP アドレスについてご存知ない方や、電子メールがどのように配送されるのかご存知ない方などが対象となります。昨年度の資料がこちらにあります。申込の前にざっとご覧いただき、全体的な内容がご自身にマッチしていることを確認してからお申し込み下さい。）

おことわり…

以下では、ネットワークの仕組みについて簡単に説明していきます。

なお、本資料は、2003年12月に文学研究科の方々を対象とした講習会ために作成した資料、平成16年度教室系技術職員研修の資料、および平成18年度～30年度東北大学事務情報化講習会「ネットワーク入門」の資料等を一部流用しており、平成16年度～30年度のサイバーサイエンスセンター（旧情報シナジーセンター）講習会「ネットワークとセキュリティ入門」の資料をベースにしてアップデートしたものです。

本講習会の位置付け

ネットワークやセキュリティのことのすべてを2.5時間でお話しすることは無理です。

また、ネットワークやセキュリティに関する情報は、市販されている雑誌やマニュアル本、あるいはインターネットの ウェブサイト上にたくさん存在します。

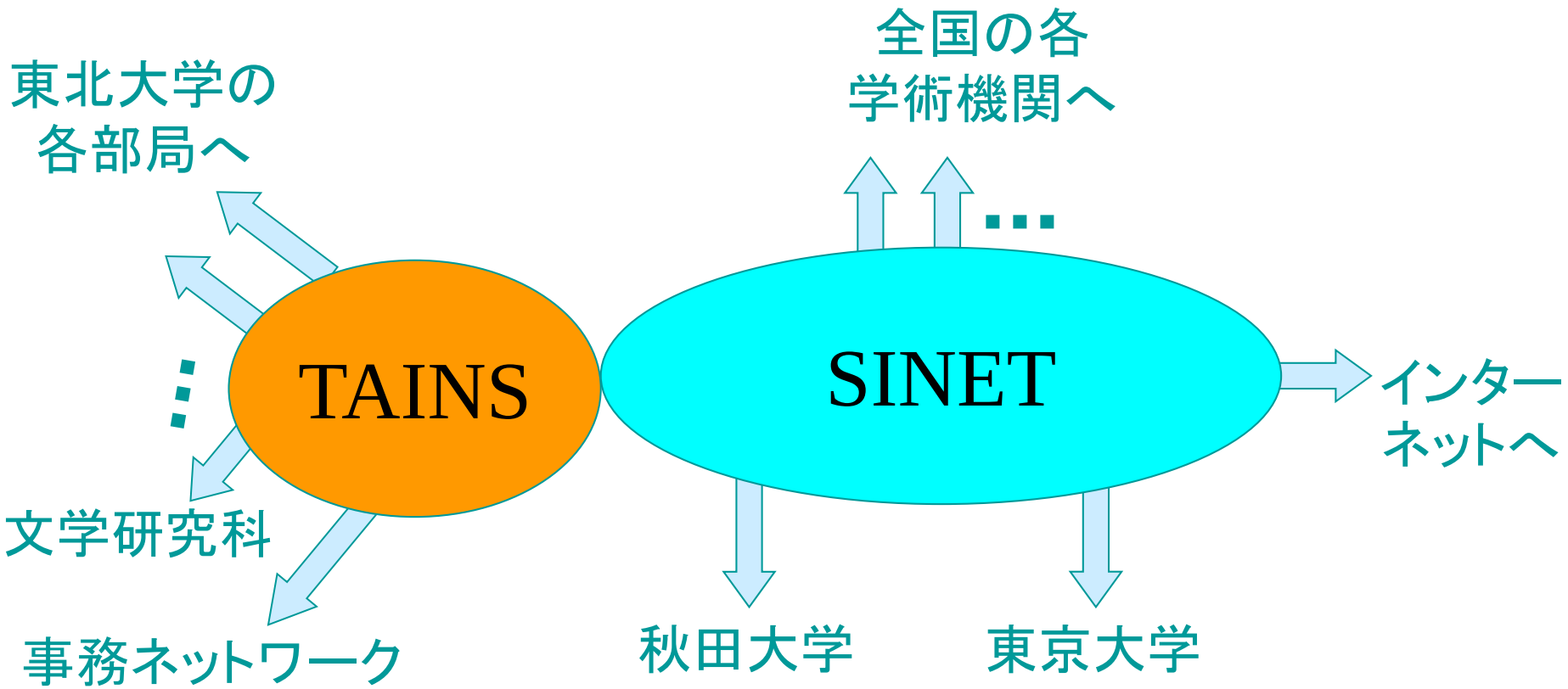
本講習会が、そのような情報にアクセスしようという動機付けになれば幸いです。

（なお、本資料で用いている語句については、正確な定義よりも、わかり易さを優先しています。ご了承下さい。）

目次

1. 東北大学周辺のネットワーク環境

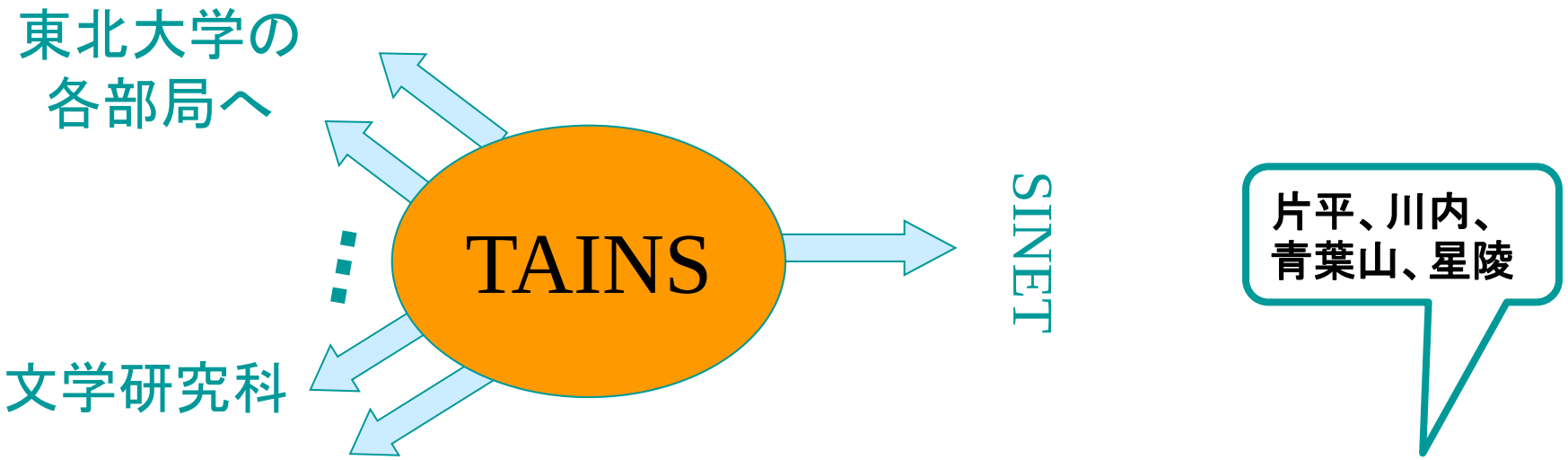
東北大学のネットワーク環境



TAINSとは？

Tohoku University Academic/All-round/Advanced Information Network System

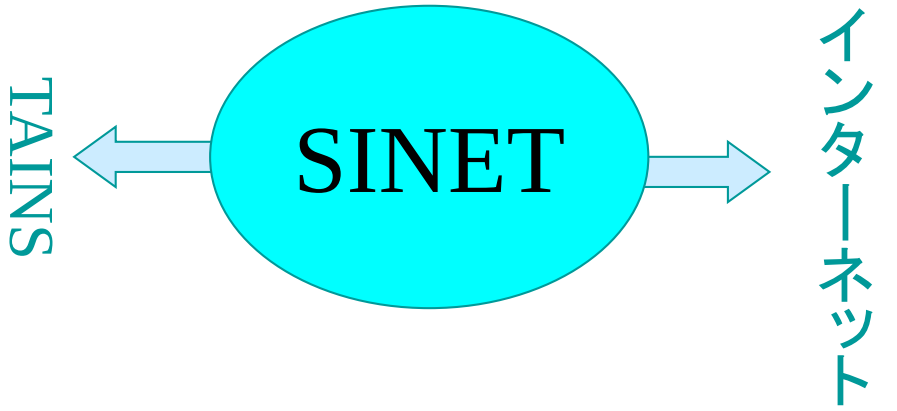
東北大学総合情報ネットワークシステム



仙台市内に分散する各キャンパスを相互に接続（1988年～）

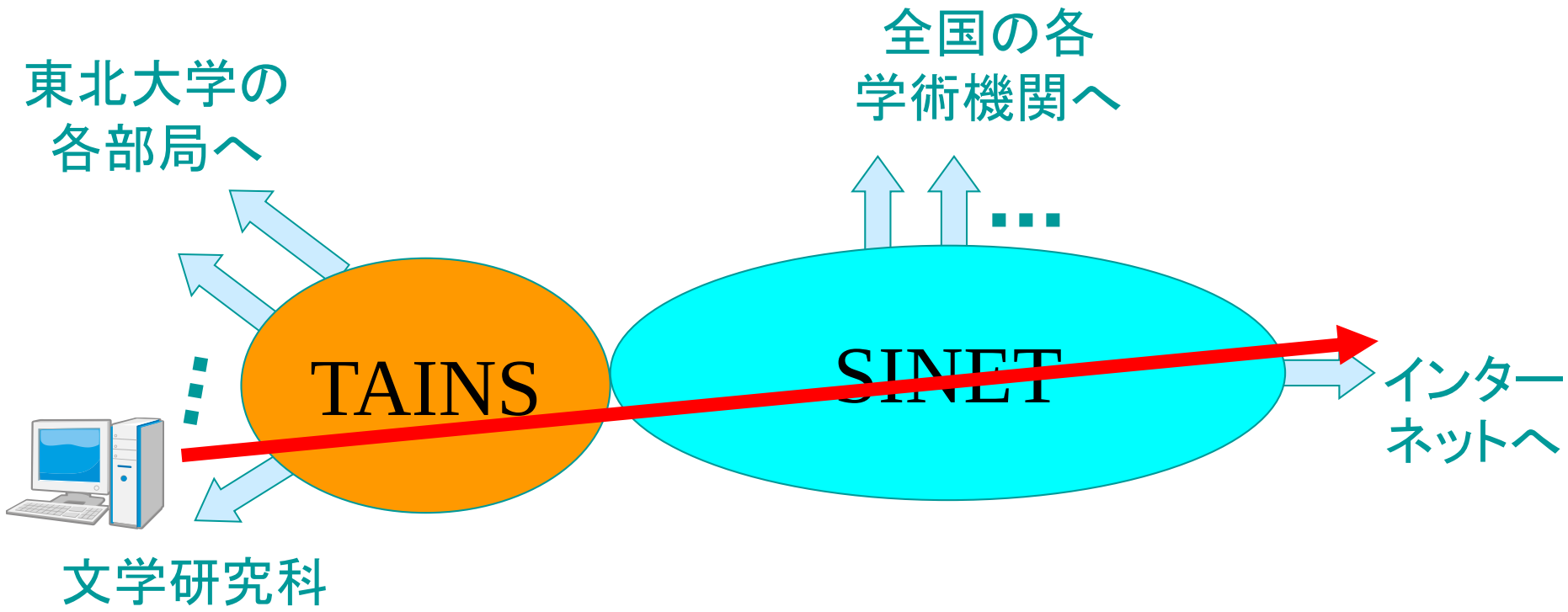
SINET http://www.sinet.ad.jp/

SINET（学術情報ネットワーク）は、情報・システム研究機構国立情報学研究所（NII）が運用する学術研究用のネットワークで、全国の大学や研究機関等を超高速ネットワークで接続している。



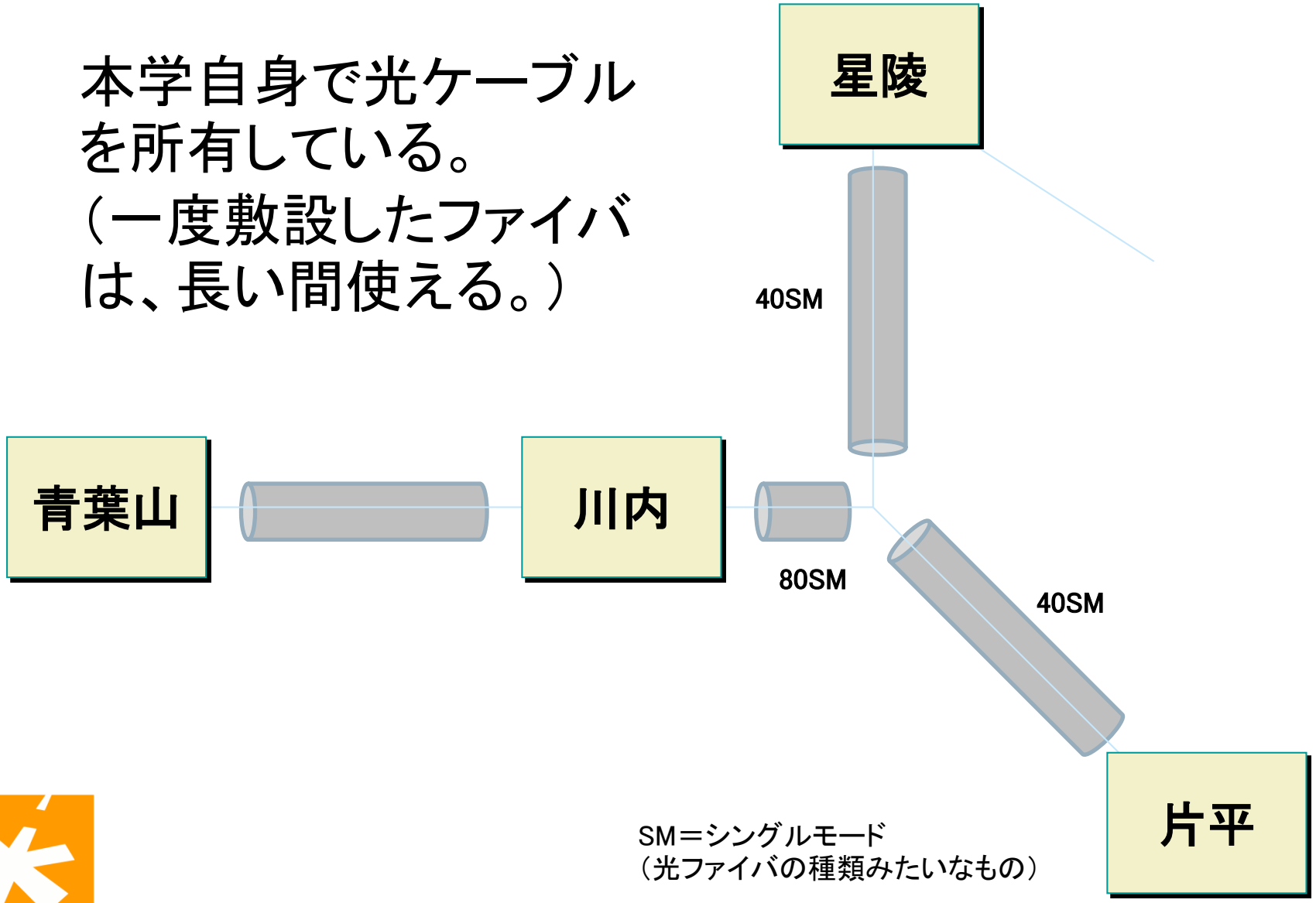
平成28年4月，SINET5の運用開始

TAINSについてもう少し…



TAINSのキャンパス間光ケーブル

本学自身で光ケーブルを所有している。
（一度敷設したファイバは、長い間使える。）



SM＝シングルモード
（光ファイバの種類みたいなもの）

TAINS の歴史

- 第一世代：1988年 ～
  - TAINS88 …FDDI

Fiber-Distributed Data Interface

- 第二世代：1995年～
  - SuperTAINS …ATM

Asynchronous Transfer Mode

- 第三世代：2001年12月～
  - TAINS/G …GbE

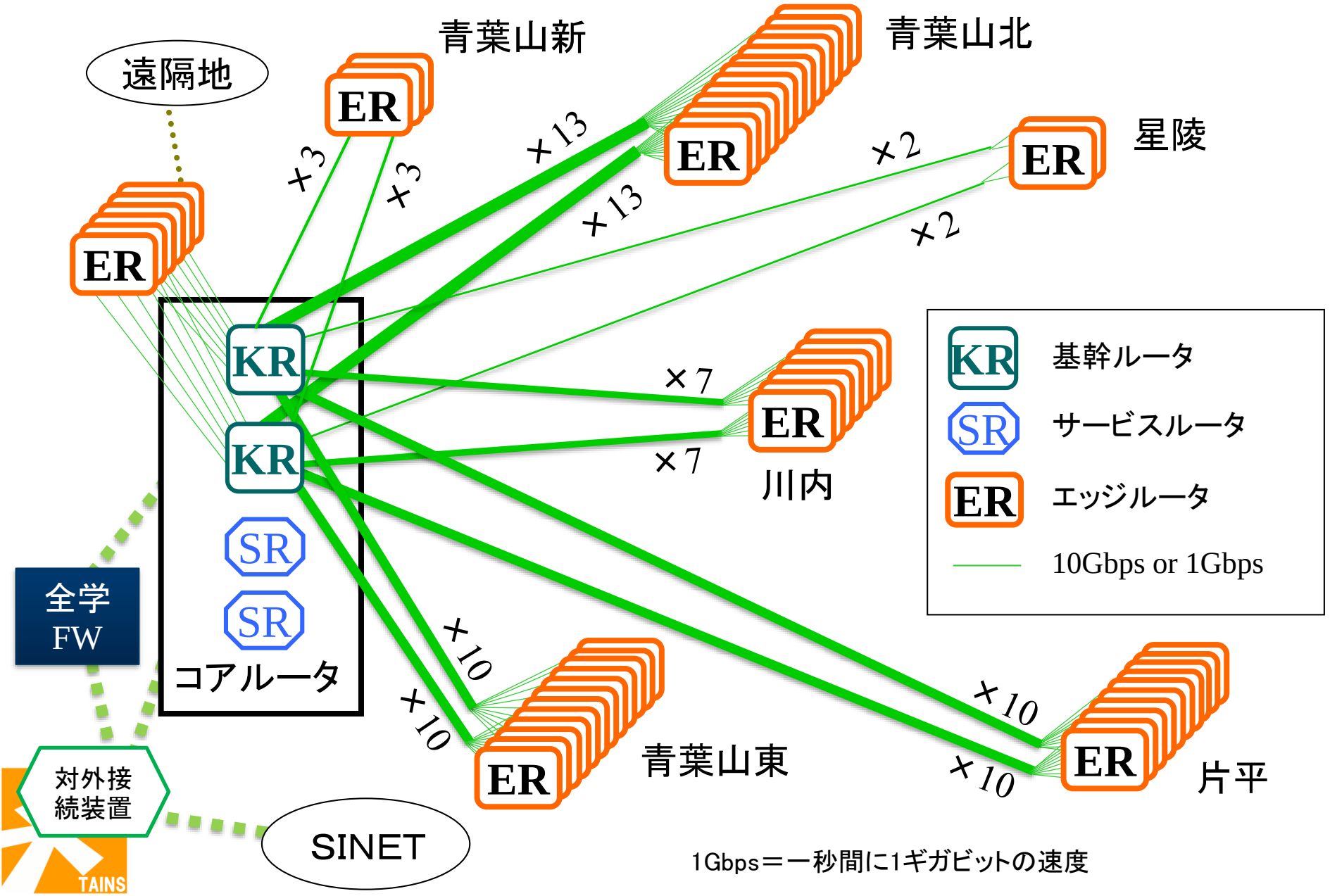
Gigabit Ethernet

- 第四世代：2009年3月～
  - StarTAINS …GbE

2016年3月
設備更新あり

StarTAINSの基幹ネットワーク構成

「ルータ」とは，ネットワーク装置のひとつ。後で写真をお見せします。



1Gbps＝一秒間に1ギガビットの速度

ルータの写真

ER

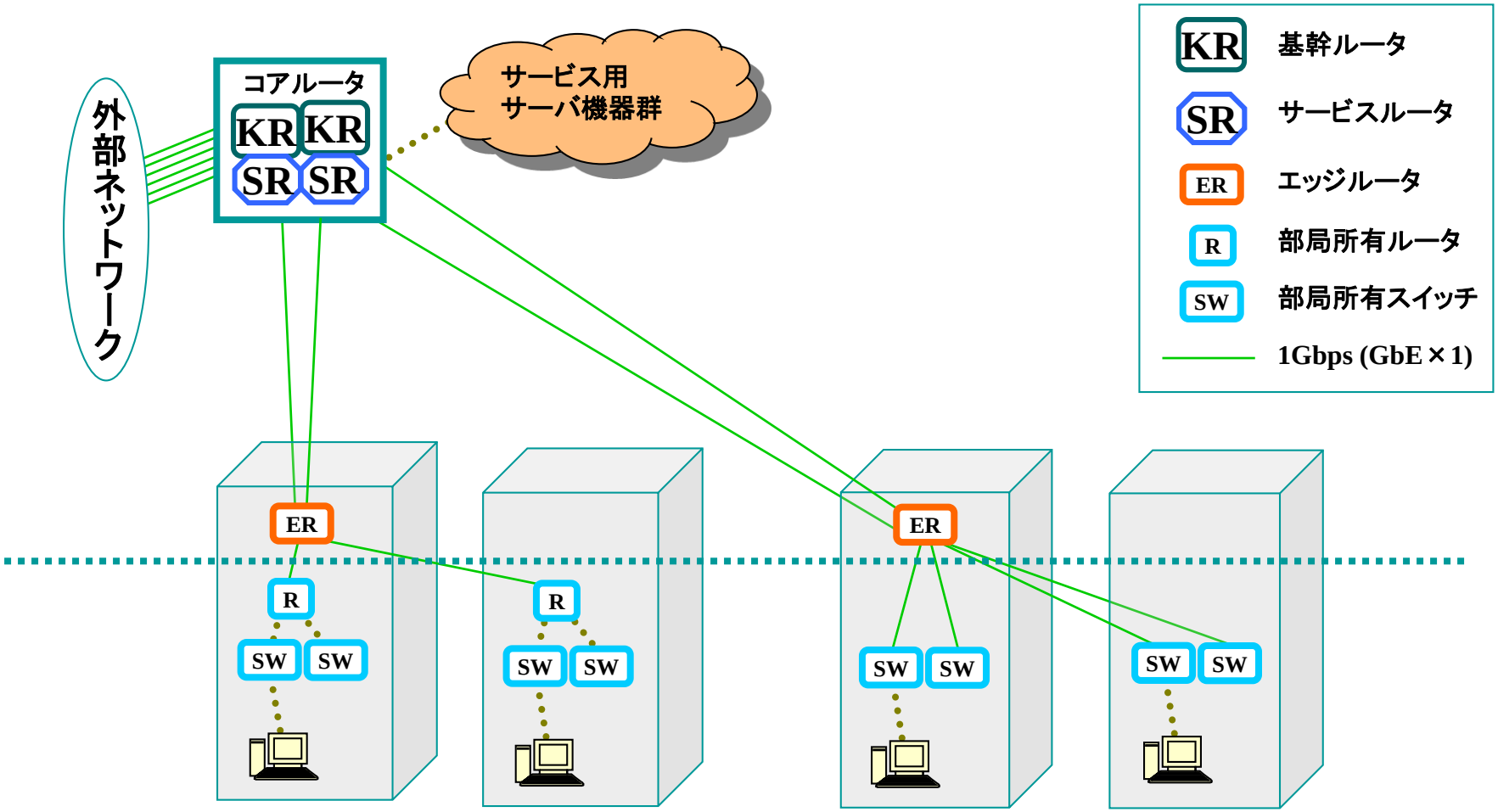
エッジルータ

KR

基幹ルータ

ご覧になりたい方は、お問い合わせください。

StarTAINSへの接続形態



もう少し詳しくは，TAINSウェブサイト
https://www2.tains.tohoku.ac.jp/
の「StarTAINSへの接続について」のページへ

2. IPアドレス関連の基礎

本講習会では，IPアドレスとは，IPv4アドレスのことを指します。

「IPアドレス」って聞いたことありますか？

仙台市青葉区荒巻字青葉6-3

東北大
ウェブサーバ
www.tohoku.ac.jp
130.34.41.135

■文京区〇町?-?

〇大
ウェブサーバ
www.example.ac.jp
xx.yy.zz.aa

MRnet

TAINS

SINET

インターネットへ

130.34.246.81

仙台市青葉区片平2-1-1

これがIPアドレス
インターネットにおける住所

IPアドレスの表示のかたち

東北大
ウェブサーバ
www.tohoku.ac.jp
130.34.41.135

○大
ウェブサーバ
www.example.ac.jp
xx.yy.zz.aa

MRnet

TAINS

SINET

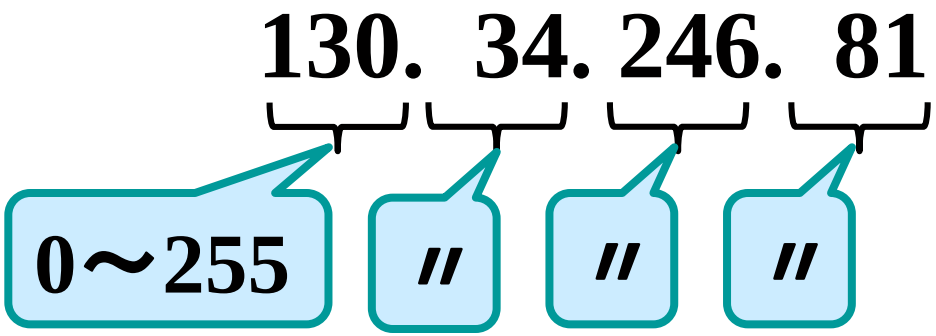
インター
ネットへ

130.34.246.81

130. 34. 246. 81

0～255 〃 〃 〃

IPアドレスの表示のかたち(2)



0. 0. 0. 0

～

255. 255. 255. 255

256×256×256×256 個
＝ 4,294,967,296 個

IPアドレスは，32ビット

どういう意味？？

IPアドレス;ビットって？

1ビット:**0**か**1**かで，2 通り
2ビット:**00**か**01**か**10**か**11**かで，$2 \times 2 = 4$ 通り

…
8ビット:**00000000**～**11111111**で，$2^8 = 256$ 通り

0. 0. 0. 0

～

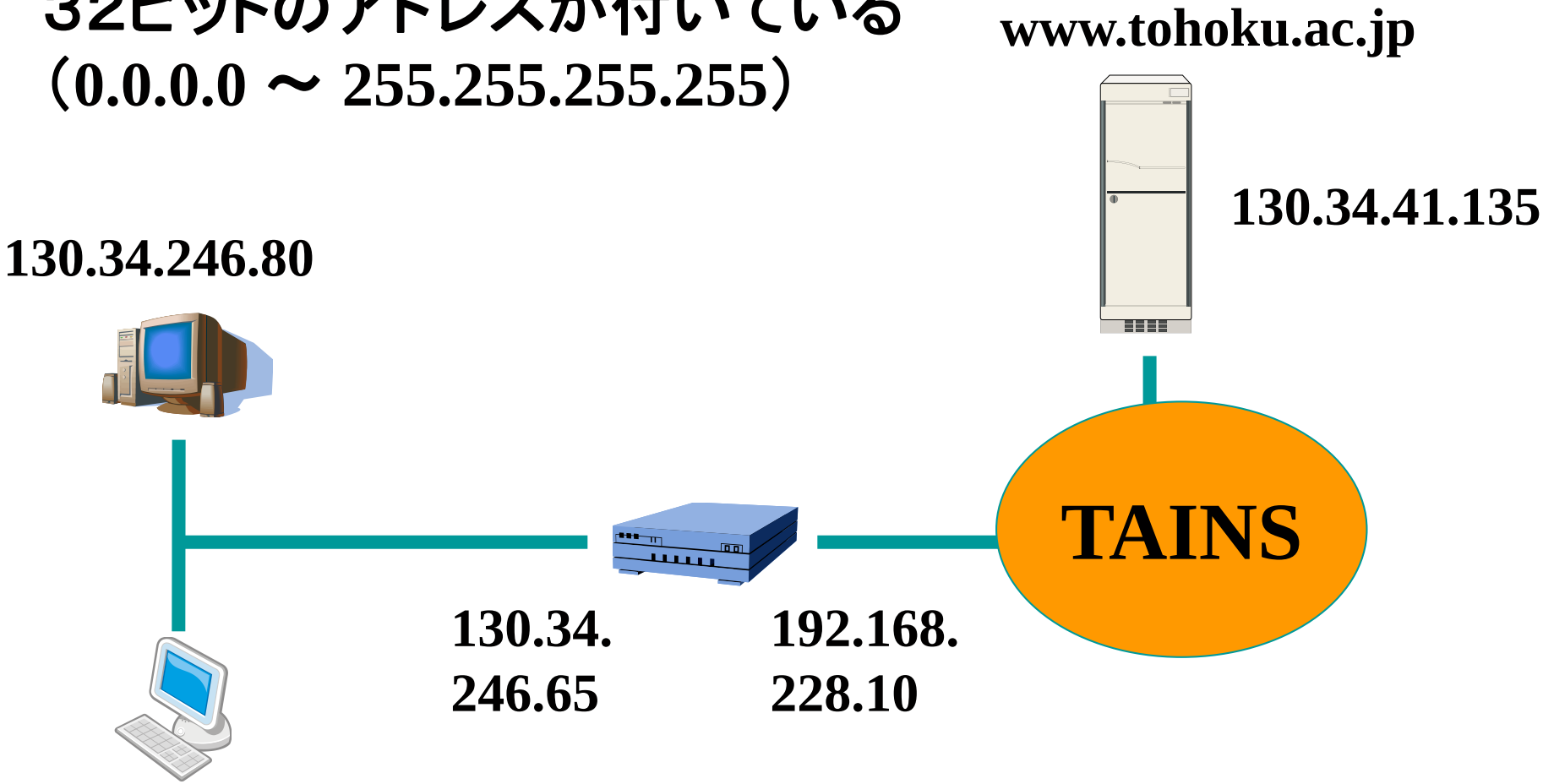
255. 255. 255. 255

8ビット 8ビット 8ビット 8ビット

合計32ビット

IPアドレス

32ビットのアドレスが付いている
（0.0.0.0 ～ 255.255.255.255）



IPアドレスの割り当て

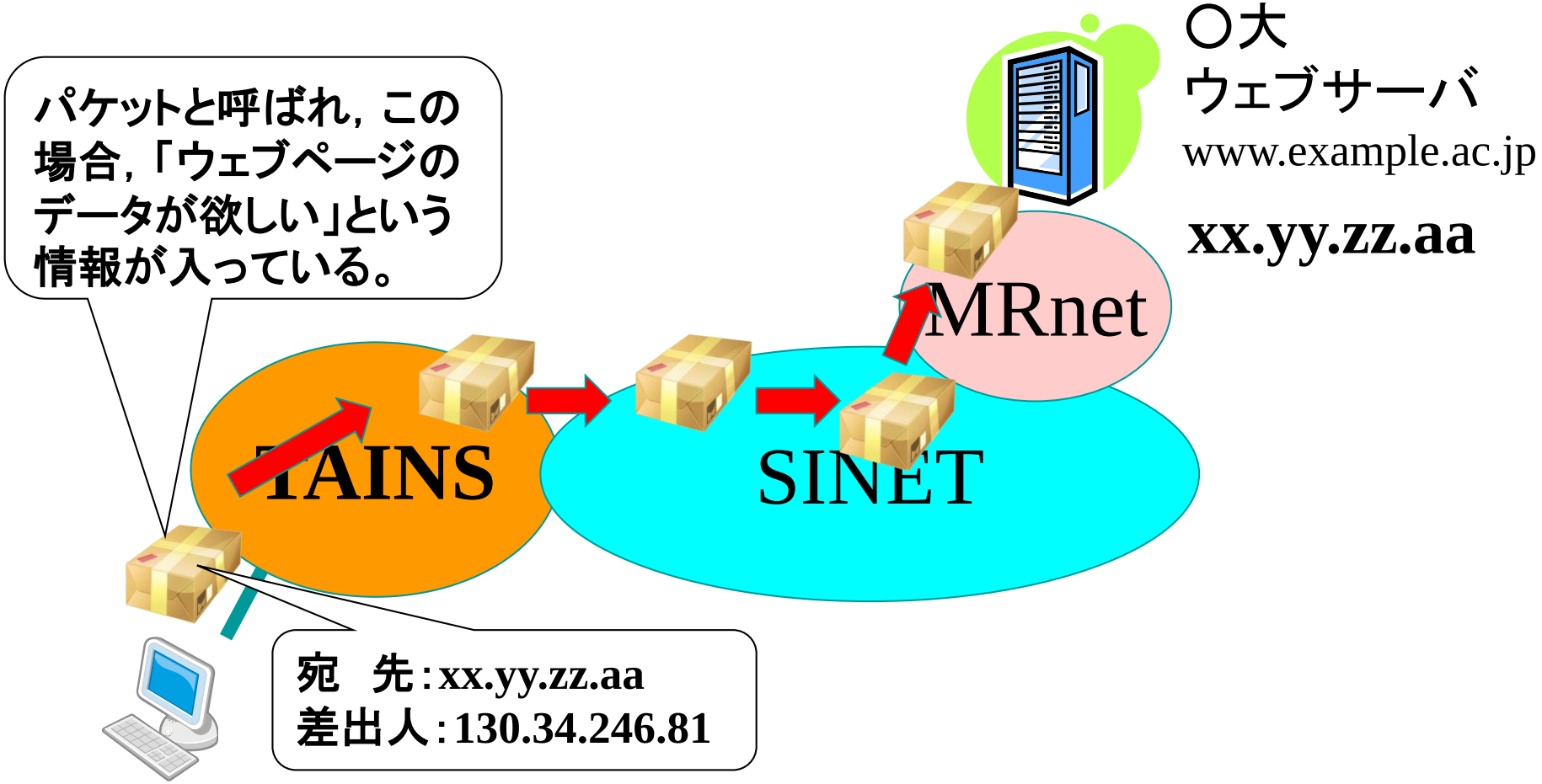
32ビットのアドレス （0.0.0.0 ～ 255.255.255.255）

東北大学　：130.34.0.0 ～ 130.34.255.255

仙台市青葉区片平…

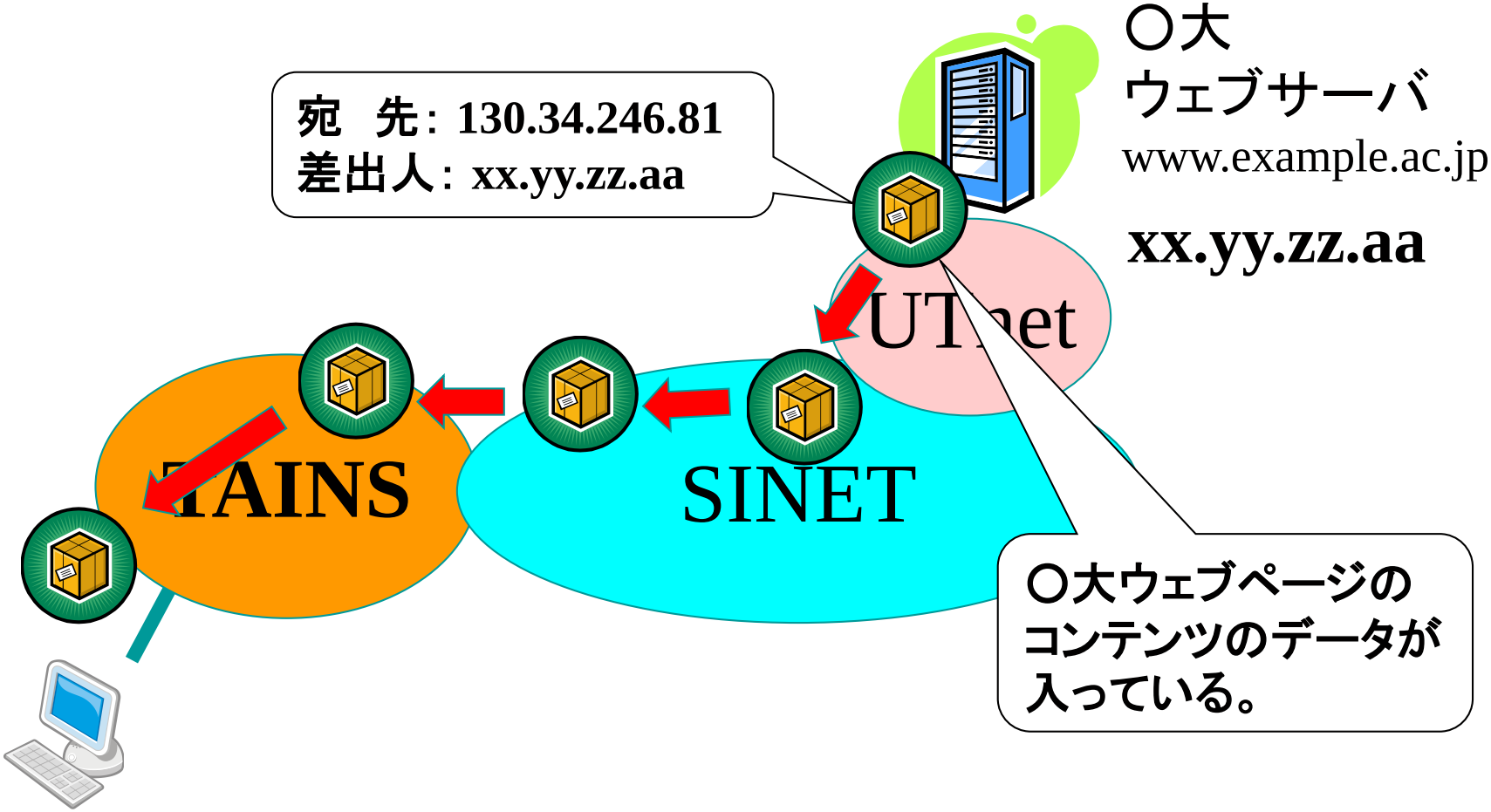
割り当てられるIP アドレスは，世界にひとつしかない。このような一意なIP アドレスは，グローバルアドレスと呼ばれ，階層的に管理されている。その一意性により，インターネットで世界中と通信ができる。

IPアドレスに基づき通信



TCPハンドシェイクとか無視しています。

IPアドレスに基づき通信(2)



IPアドレスの割り当て（学内）

３２ビットのアドレス （0.0.0.0 ～ 255.255.255.255）

東北大学　：130.34.0.0 ～ 130.34.255.255

経済研究科：130.34.140.0 ～ 130.34.141.255
（256×2個）

学内の割り当て状況：
https://www2.tains.tohoku.ac.jp/　のメニューから，
【サブネットアドレス一覧】を選択

自分のIPアドレスを知るには（Windows 10）

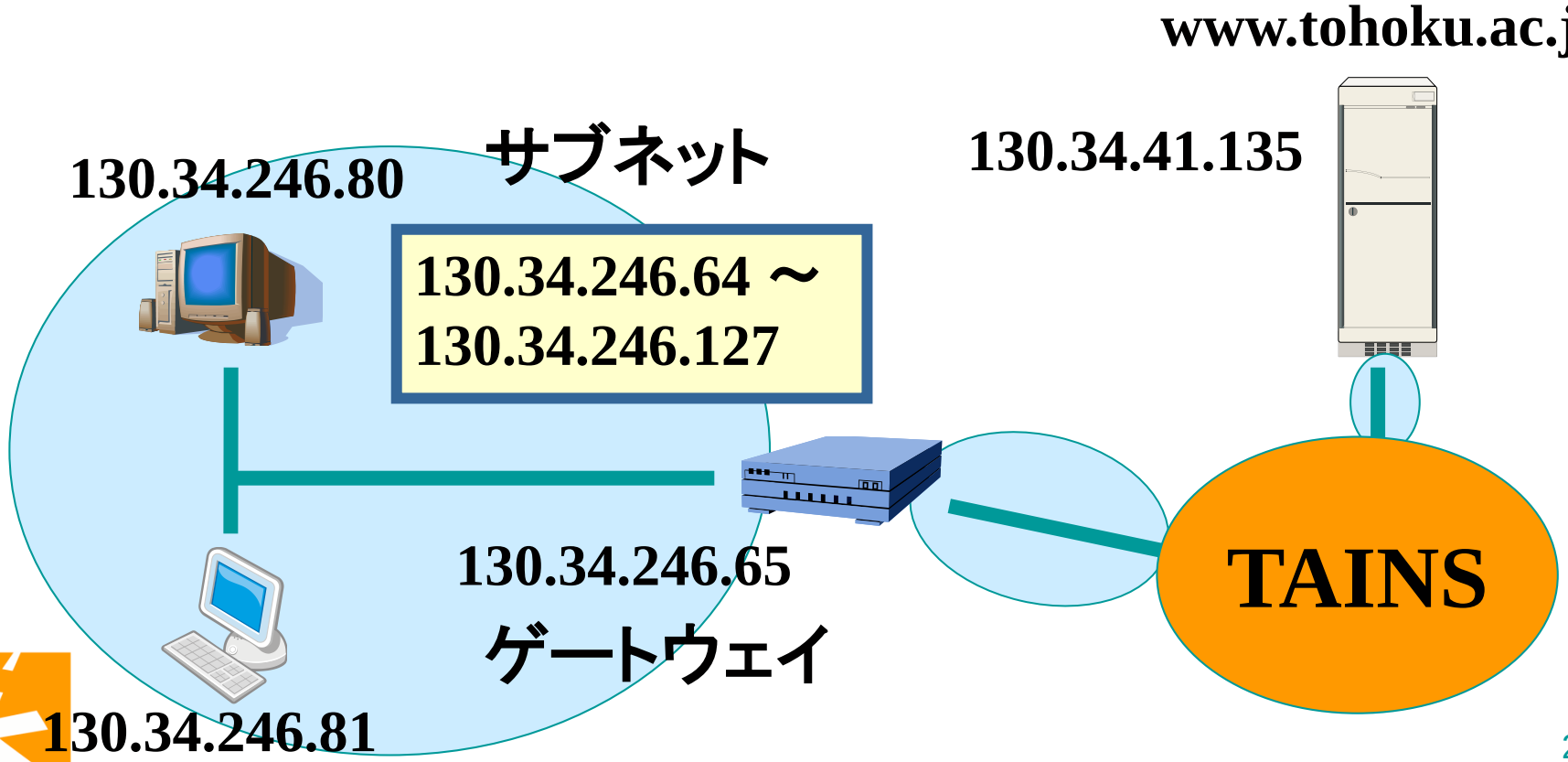
[画面左下のWindowsロゴを左クリック] → [Windowsシステムツール] → [コマンドプロンプト] を選び、ipconfig と打つ。

```
C:¥>ipconfig

Windows IP 構成

イーサネット アダプターイーサネット:
        接続固有の DNS サフィックス . . . :
        IPv4 アドレス. . . . . . . . . . . . : 130.34.246.80
        サブネット マスク. . . . . . . . . . : 255.255.255.192
        デフォルト ゲートウェイ. . . . : 130.34.246.65
```

※IPアドレスを表示する方法には，他にもいろいろあります。

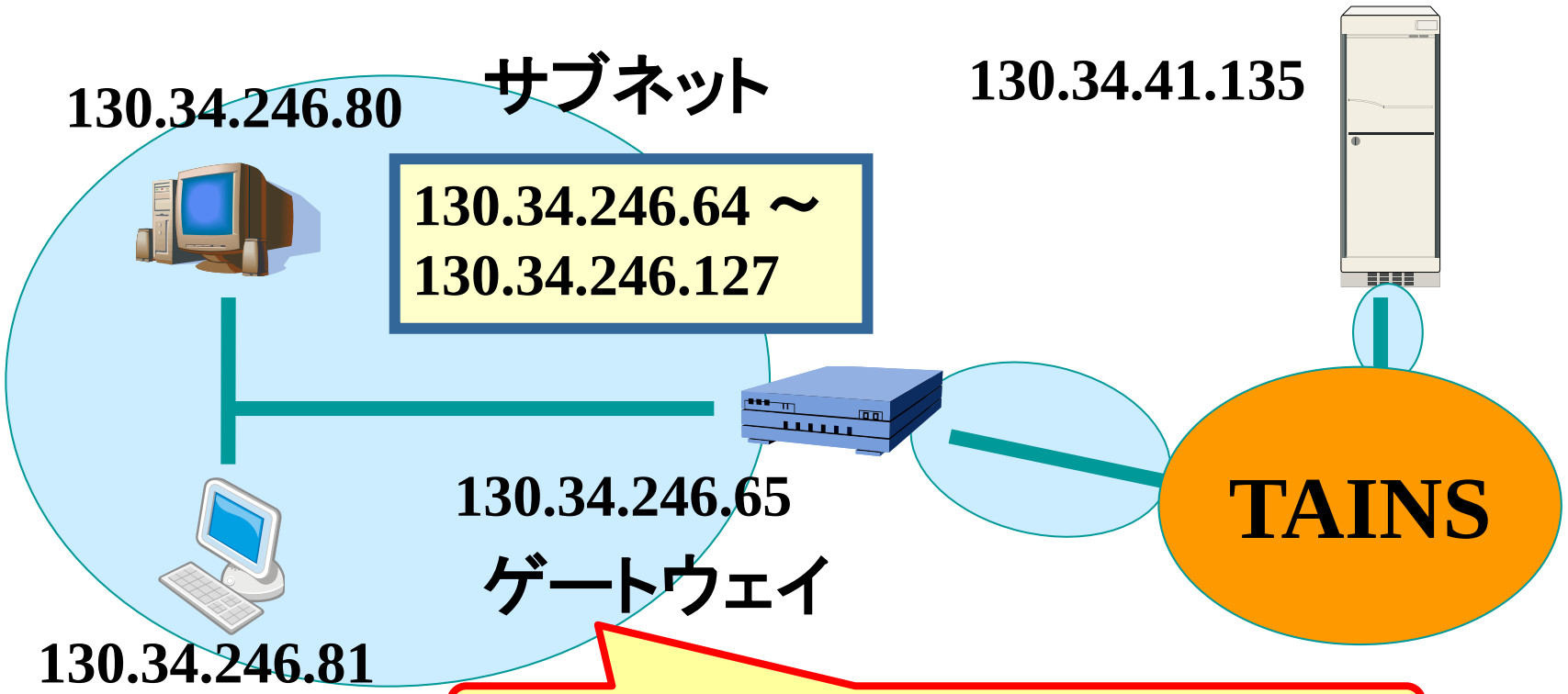
デフォルトゲートウェイとサブネットマスク

```
IPv4 アドレス. . . . . . . . . . . . : 130.34.246.80
サブネット マスク. . . . . . . . . . : 255.255.255.192
デフォルト ゲートウェイ. . . . : 130.34.246.65
```



デフォルトゲートウェイ

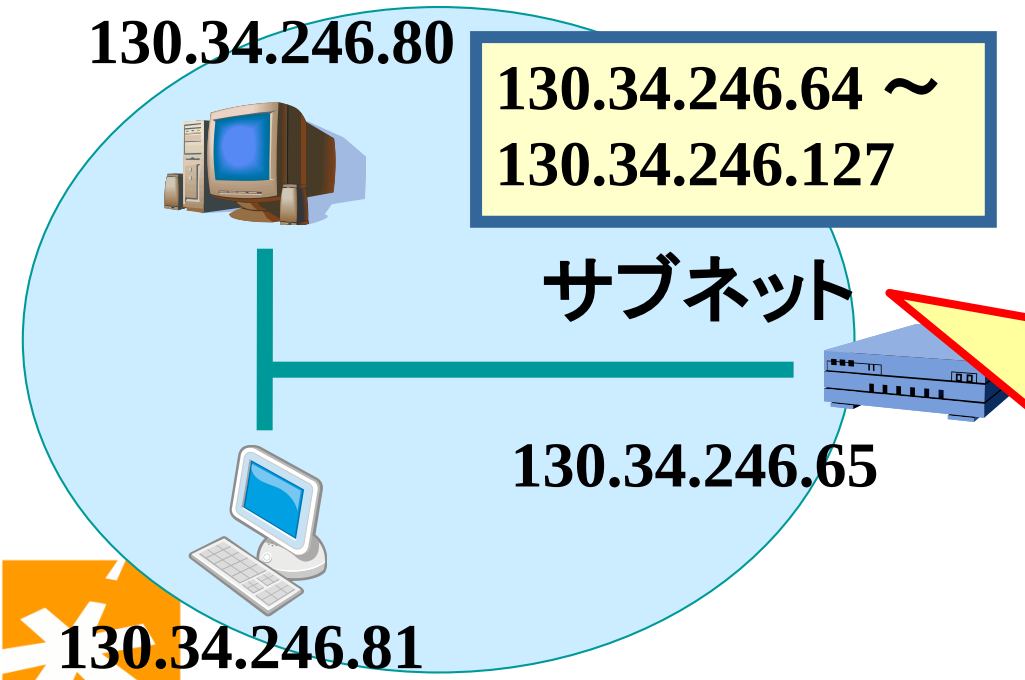
www.tohoku.ac.jp



郵便局の住所みたいなもの（かな？）

サブネットマスク

```
IPv4 アドレス. . . . . . . . . . . . : 130.34.246.80
サブネット マスク. . . . . . . . . . : 255.255.255.192
```



サブネットマスクは，この範囲を定めているものなのだ…ぐらいに思っておいて頂ければ結構かと存じます。

サブネットとは，自分の身内の範囲内の小さなネットワーク，という感じです。研究室とか，家庭内とか，そういう感じ。

TAINS

サブネットマスクの読み方の簡単な例

IPv4 アドレス. . . . . : 130.34.246.80
サブネット マスク. . . . . : 255.255.255.0

IPが256個のサブネット

サブネット　130.34.246.0 ～ 130.34.246.255

サブネット マスク. . . . . : 255.255.255.128

IPが128個のサブネット

サブネット　130.34.246.0 ～ 130.34.246.127

サブネット マスク. . . . . : 255.255.255.192

IPが64個のサブネット

サブネット　130.34.246.64 ～ 130.34.246.127

TAINS

サブネット マスク. . . . . : 255.255.255.0

130.34.246.0 ～ 130.34.246.255
130.34.247.0 ～ 130.34.247.255
. . .

IPが256個；8ビット毎のかたまり

130.34.246.0/24

スラッシュを使った表記（CIDR表示）

サブネット マスク. . . . . : 255.255.255.128

130.34.246.0 ～ 130.34.246.127
130.34.246.128 ～ 130.34.246.255
. . .

IPが128個；7ビット毎のかたまり

130.34.246.127/25

サブネット マスク. . . . . : 255.255.255.192

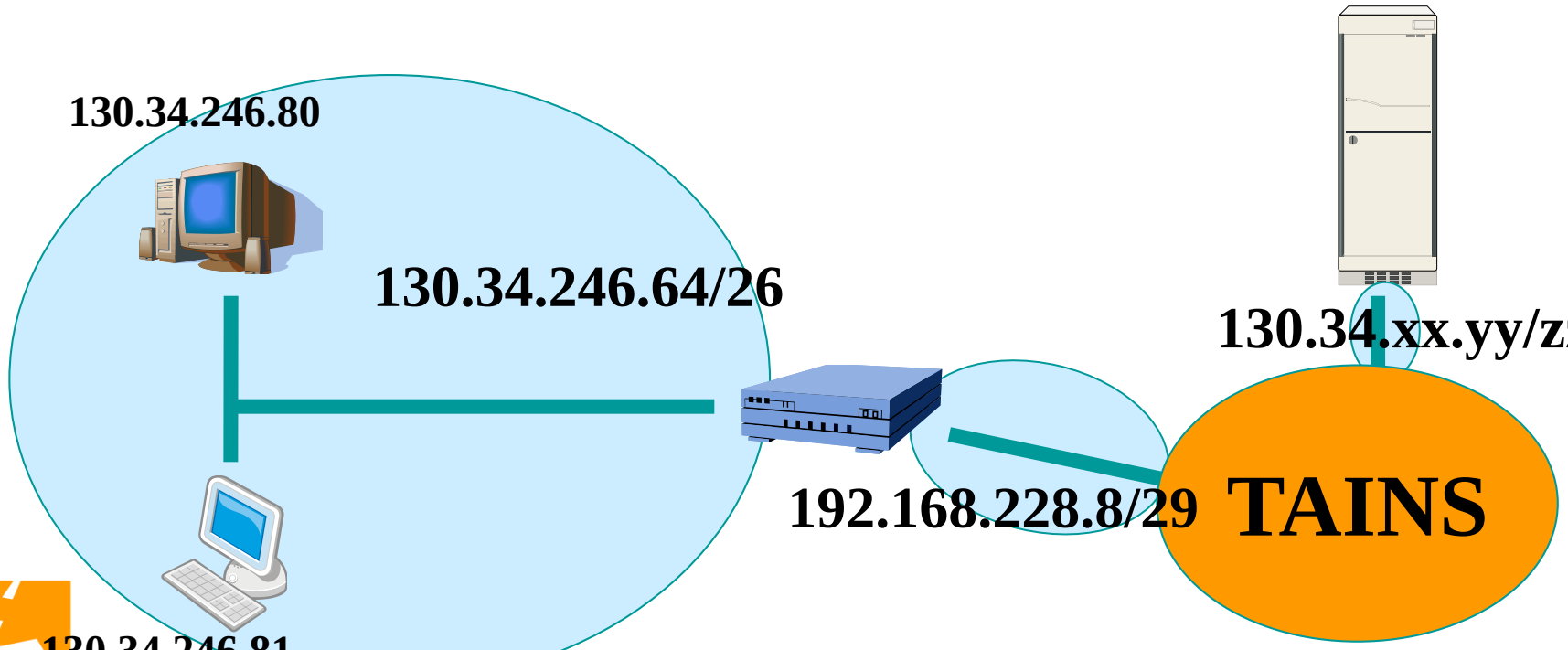
130.34.246.0 ～ 130.34.246.63
130.34.246.64 ～ 130.34.246.127
130.34.246.128 ～ 130.34.246.191
. . .

IPが64個；6ビット毎のかたまり

130.34.246.64/26

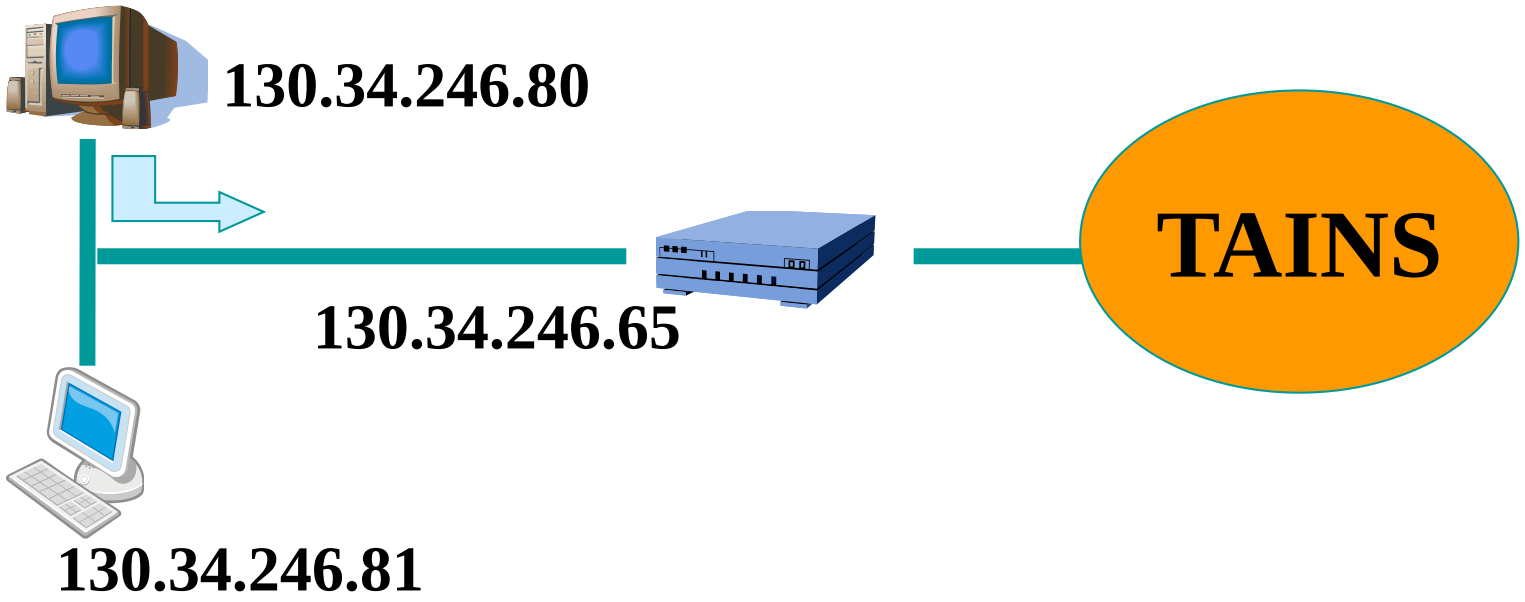
サブネット

各サブネットは，RIPやOSPFなどのルーティングプロトコルにより経路情報を交換したりしている



別なホストの状況の確認方法

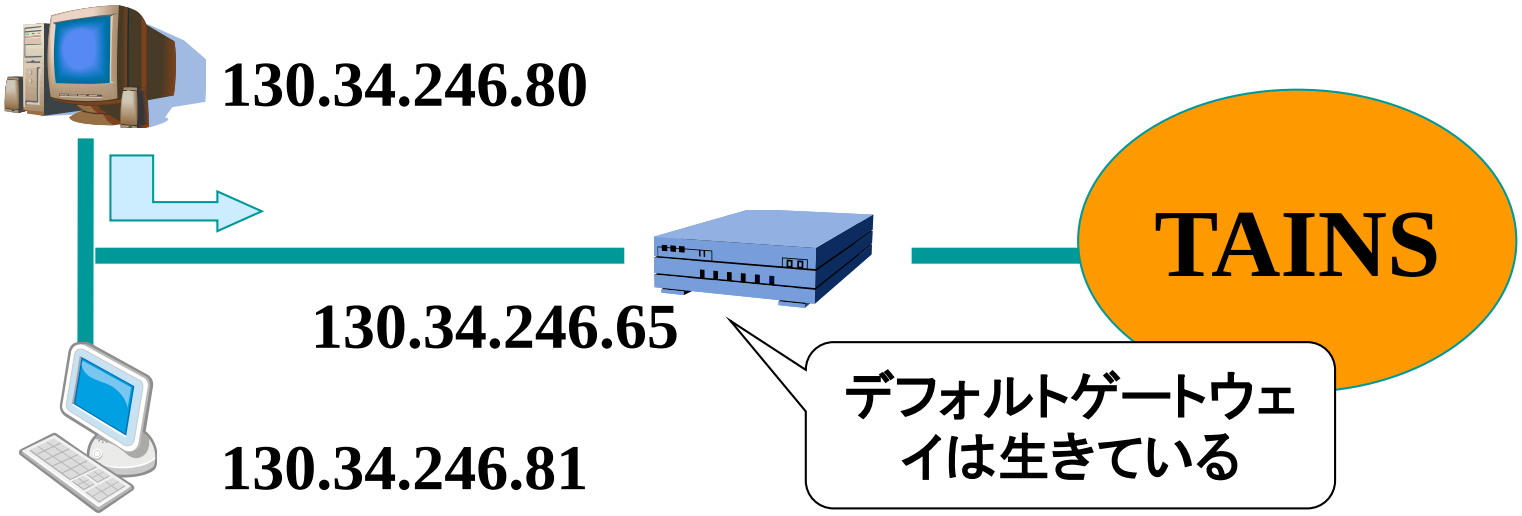
[コマンドプロンプト] を選び、ping コマンドを使うと、相手のホストが「生きている」かどうか確認できる。



pingコマンド

ping のあとに相手のIPアドレスを打つ。

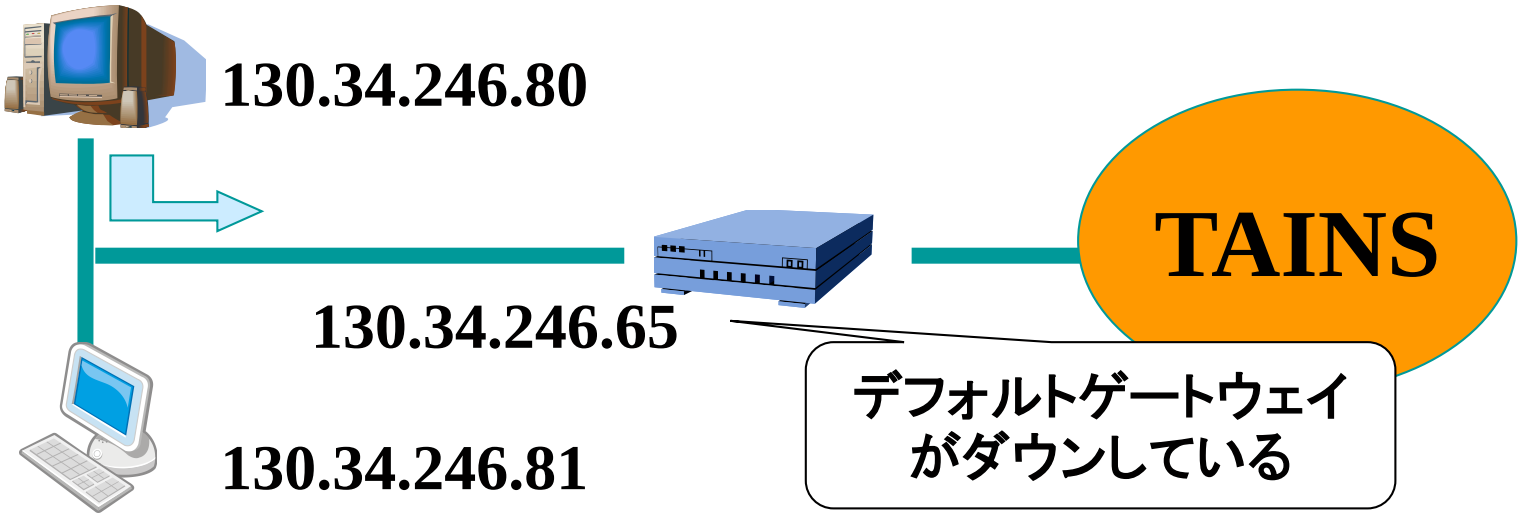
```
C:¥>ping 130.34.246.65

130.34.246.65 に ping を送信しています 32 バイトのデータ:

130.34.246.65 からの応答: バイト数=32 時間=10ms TTL=255
130.34.246.65 からの応答: バイト数=32 時間=4ms TTL=255
```



pingコマンド（不達の例）

130.34.246.65 がない場合　（あるいは答えない場合）

```
C:¥>ping 130.34.246.65

130.34.246.65 に ping を送信しています 32 バイトのデータ:

要求がタイムアウトしました。
要求がタイムアウトしました。
```



Pingコマンドの注意点

ネットワークに接続していても、パソコンなどの設定により、返事が返ってこないこともある（ICMP ECHO に答えないマシンもある）。

なお、（ほとんどの）Windows 7/8.1/10 では、デフォルトでファイアウォールが有効になっており、Ping に答えない。

Ping を打ち過ぎると、攻撃やウィルス（ワーム）と認識されてしまう場合があるので、注意しましょう。身近なところだけにとどめましょう。

プライベートアドレス

130.34.＊.＊ ではなく、192.168.1.10 や 172.16.0.20 のようなアドレスがPCに付いている場合、それはプライベートアドレスです。

130.34.11.111 のようなアドレスはグローバルアドレスと呼ばれ、世界に1つしかありません。
それに対して、プライベートアドレスは、組織内で自由に使ってよいことになっており、また、組織内のネットワークでしか使えず、組織外からプライベートアドレスを持つマシンにアクセスすることはできません。

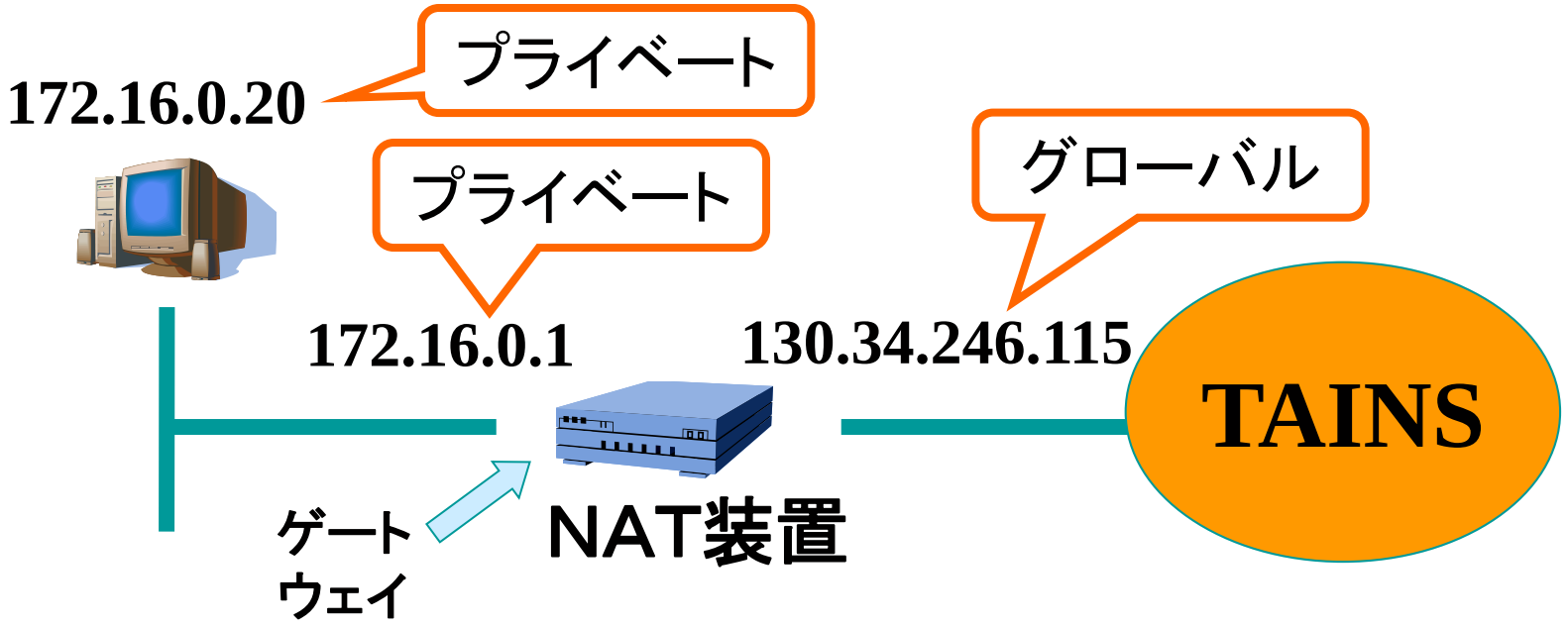
プライベートアドレスの範囲:

10.0.0.0 ～ 10.255.255.255
172.16.0.0 ～ 172.31.255.255　← こちらをお使い下さい
192.168.0.0 ～ 192.168.255.255

もう少し詳しくは、TAINSニュース　34号　9～10ページ
「TAINS 内流通用のプライベートアドレスについて」
http://www.tains.tohoku.ac.jp/news/news-34/0910.html

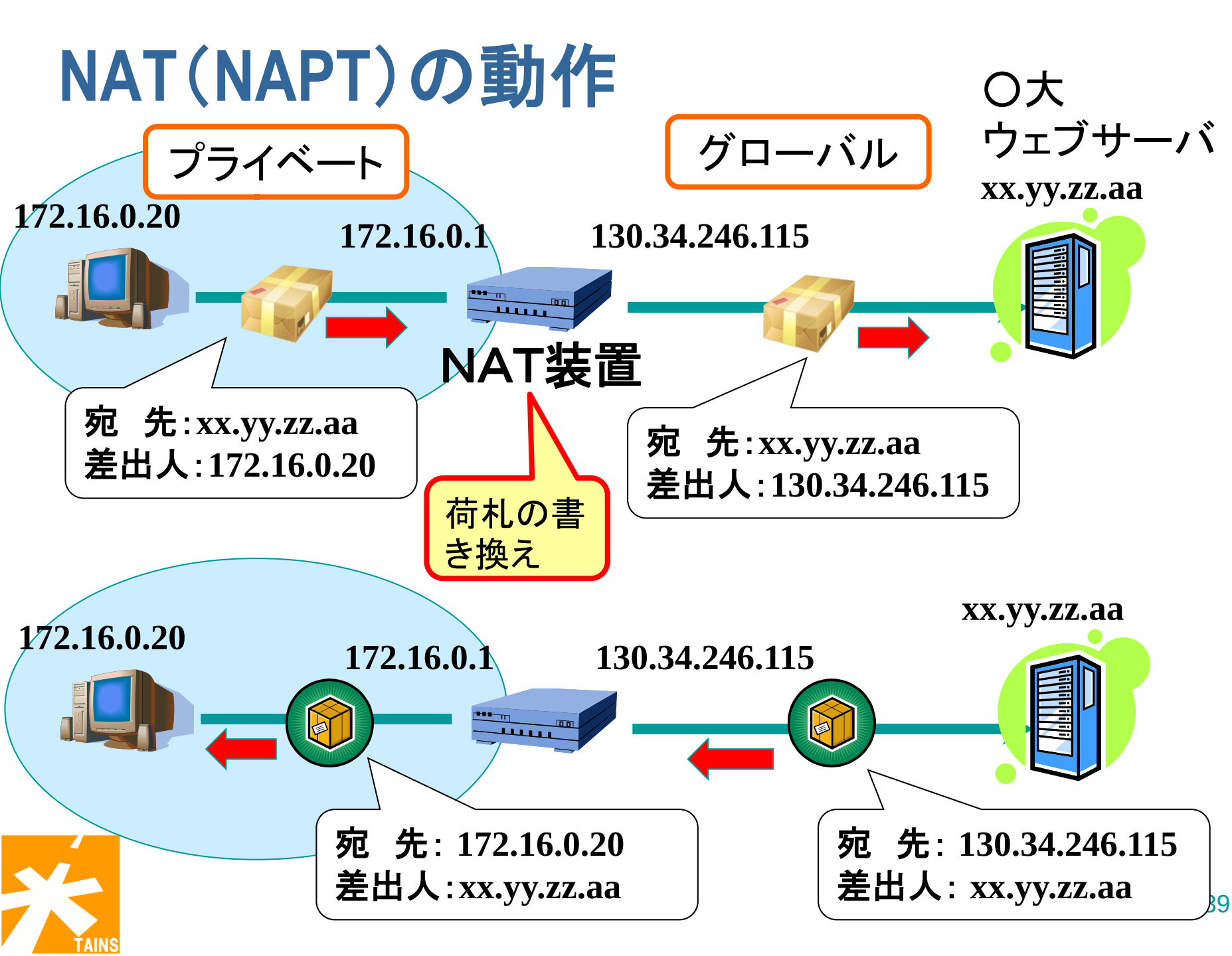
プライベートアドレスの変換

プライベートアドレスとグローバルアドレスを変換してくれるのが、「NAT」です。
ファイヤーウォールやブロードバンドルータは、NATの機能を持つものが多いです。



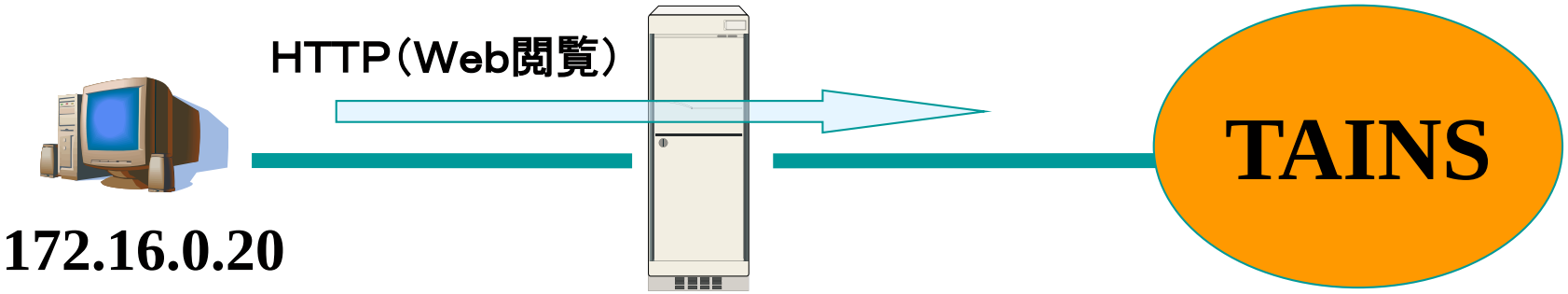
もう少し詳しくは、TAINSニュース　31号　2～10ページ
「いわゆるブロードバンドルータによる NAT の利用」
http://www.tains.tohoku.ac.jp/news/news-31/0210.html

NAT（NAPT）の動作


プライベート
グローバル
○大
ウェブサーバ
xx.yy.zz.aa
172.16.0.20
172.16.0.1
130.34.246.115
NAT装置
宛　先：xx.yy.zz.aa
差出人：172.16.0.20
宛　先：xx.yy.zz.aa
差出人：130.34.246.115
荷札の書き換え
172.16.0.20
172.16.0.1
130.34.246.115
xx.yy.zz.aa
宛　先：172.16.0.20
差出人：xx.yy.zz.aa
宛　先：130.34.246.115
差出人：xx.yy.zz.aa

プロキシサーバ

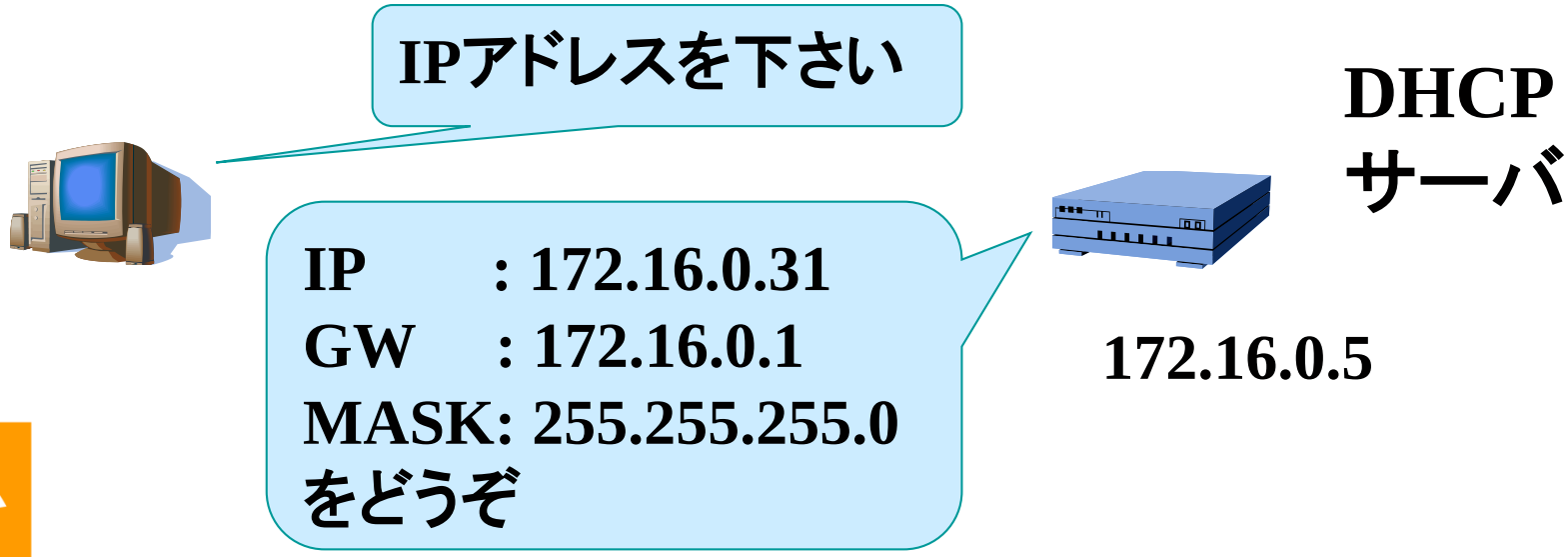
プライベートアドレスを持つパソコンが、インターネットと通信するために、プロキシサーバ（代理サーバ）が用いられることもあります。プロキシサーバは、Web などの特定のアプリケーションに対して、橋渡しをしてくれます。



プロキシサーバ

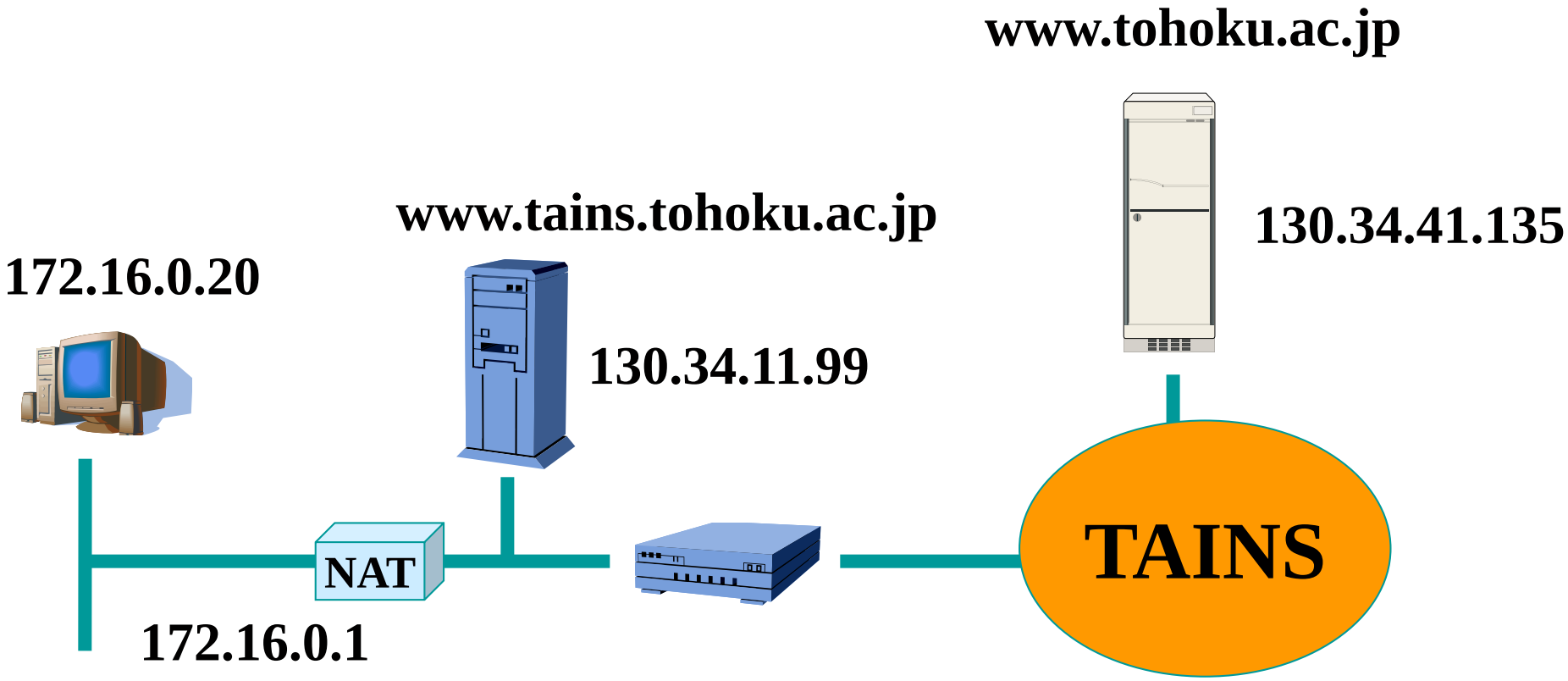
DHCP （Dynamic Host Configuration Protocol）

DHCP というプロトコルにより、ユーザは特別何もせずに、IP アドレスやデフォルトゲートウェイを貰うことができる。
Windows 7/8.1/10の場合、「IPアドレスを自動的に取得」という設定（ほぼデフォルト）になっているとき、アドレスを DHCP サーバから貰おうとする。



3. ドメイン名関連の基礎

ドメイン名と IP アドレス



ドメイン名

IPアドレスを憶えるのは大変なので、ドメイン名が利用されている。
たとえば、東北大のホームページは、
http://130.34.41.135/ でも開くことができる。
でも、普通は http://www.tohoku.ac.jp/ を使う。

東北大学　：tohoku.ac.jp
東北医科薬科大学：tohoku-mpu.ac.jp
文学研究科：sal.tohoku.ac.jp

学内の割り当て状況：
https://www2.tains.tohoku.ac.jp/　のメニューから，
【サブドメイン名一覧】を選択

JPドメイン

.JPというccTLD（国別ドメイン名）は，株式会社日本レジストリサービス（JPRS）により運用されている。

属性型JPドメイン名：
tohoku.ac.jp, example.co.jp, …

1つの組織が登録出来るドメイン名は1つだけ

汎用JPドメイン名：
tohoku-university.jp, …

日本に住所があれば誰でも登録できる

＜参考＞

Internet Week　ショーケース in 仙台（2019.5.31）

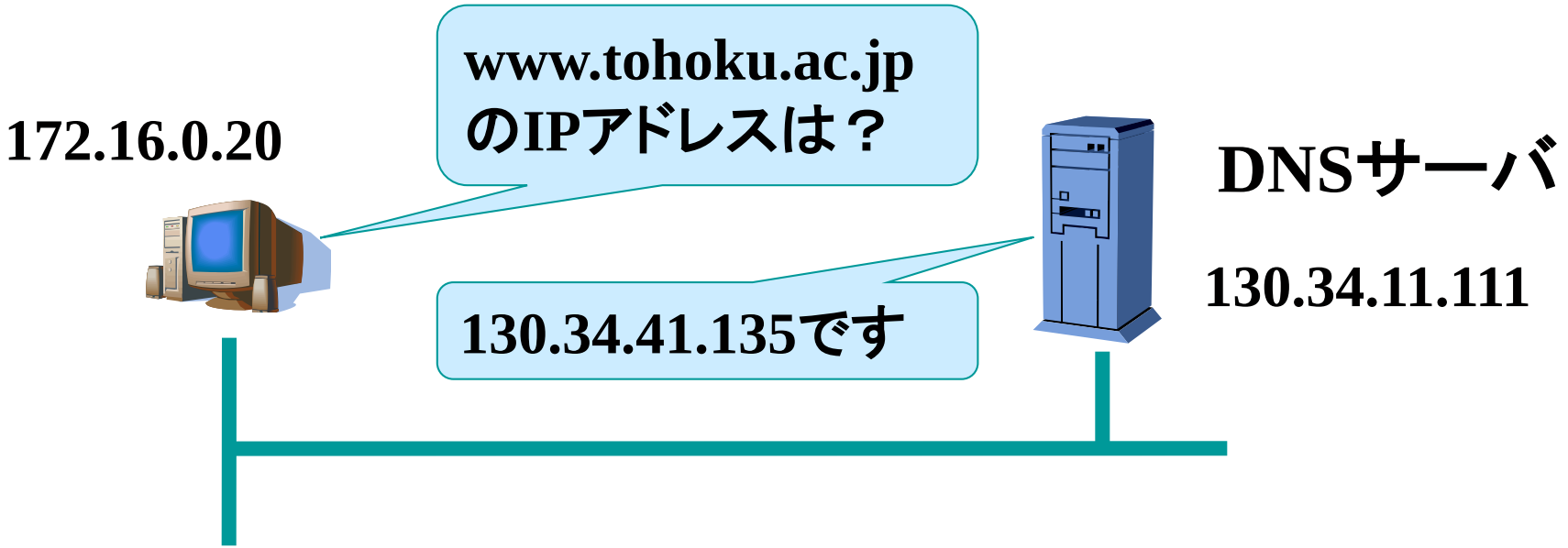
DNS Day mini - 大切なドメイン名を守る –

其田学(株式会社インターネットイニシアティブ)

https://www.nic.ad.jp/sc-sendai/program/iwsc-sendai-d2-4.pdf

キャッシュDNSサーバ

ドメイン名とIPアドレスの変換をしてくれるのが、
キャッシュDNSサーバ。



DNSのより詳しい正確な情報は、TAINSニュース　35号　17～22ページ
「DNS 設定ガイド（一般利用者向け）」
http://www.tains.tohoku.ac.jp/news/news-35/1722.html

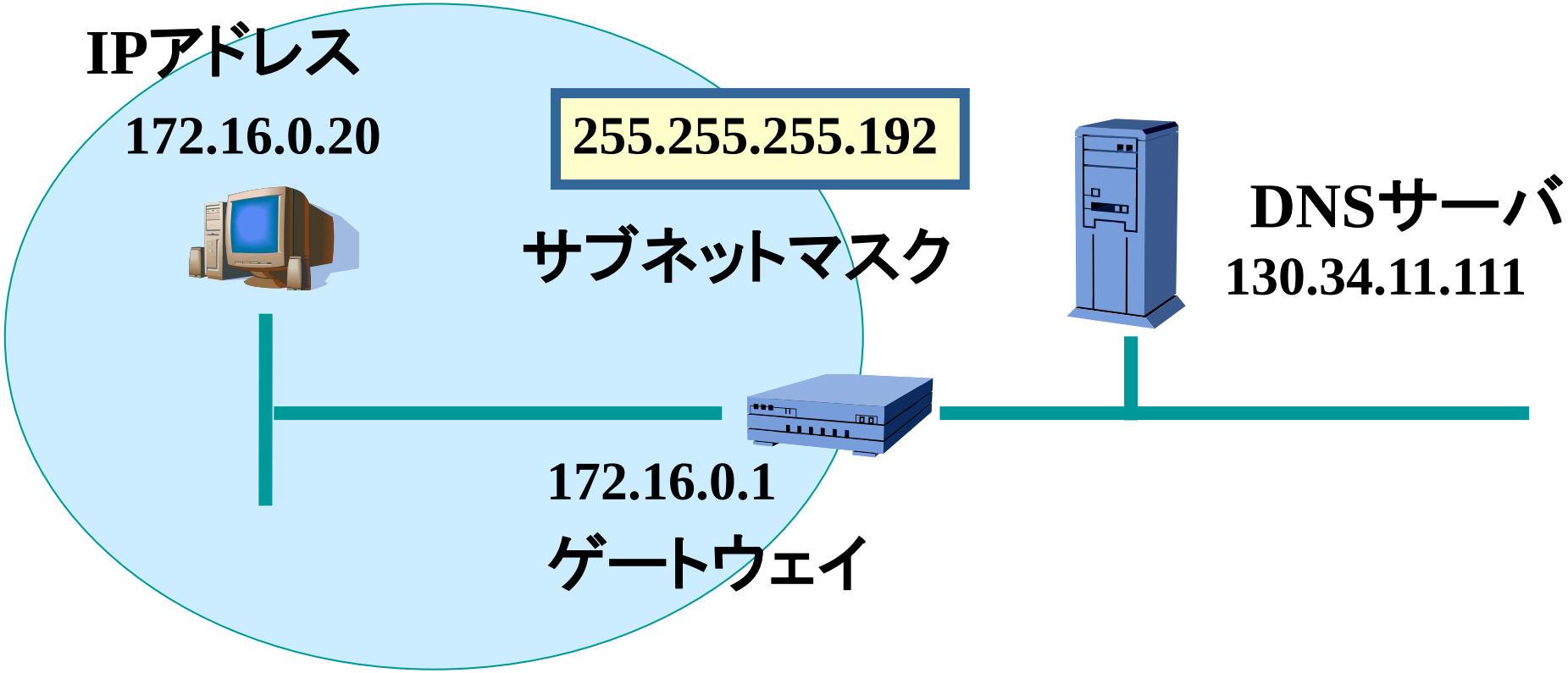
自分のDNSサーバを知るには（Windows 10）

[画面左下のWindowsロゴを左クリック] → [Windowsシステムツール] → [コマンドプロンプト] を選び、ipconfig /all と打つ。

```
C:¥>ipconfig /all

Windows IP 構成

イーサネット アダプターイーサネット:
        接続固有の DNS サフィックス . . . :
        IPv4 アドレス. . . . . . . . . . . . : 172.16.0.20
        サブネット マスク. . . . . . . . . . : 255.255.255.192
        デフォルト ゲートウェイ. . . . : 172.16.0.1
        DHCP サーバー . . . . . . . . . . : 172.16.0.1
        DNS サーバー .. . . . . . . . . . : 130.34.11.111
```

※一部の行だけ抜粋しています。

まとめ：4つの基本情報



その他の便利なコマンド： tracert, nslookup

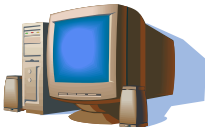
使い方を十分に理解してからお使い下さい。
（場合によっては、攻撃と間違われる可能性あり）

MAC アドレス(1)

MAC(Media Access Control)アドレスとは，ネットワークでホストを識別するために使うアドレスです。

Ethernetでは，すべてのネットワークカードに 48 ビットのアドレスが付いています。

MAC アドレスは，それぞれのカードに固有のもので，基本的に，同じ番号を持つカードは世界に1つしかありません。

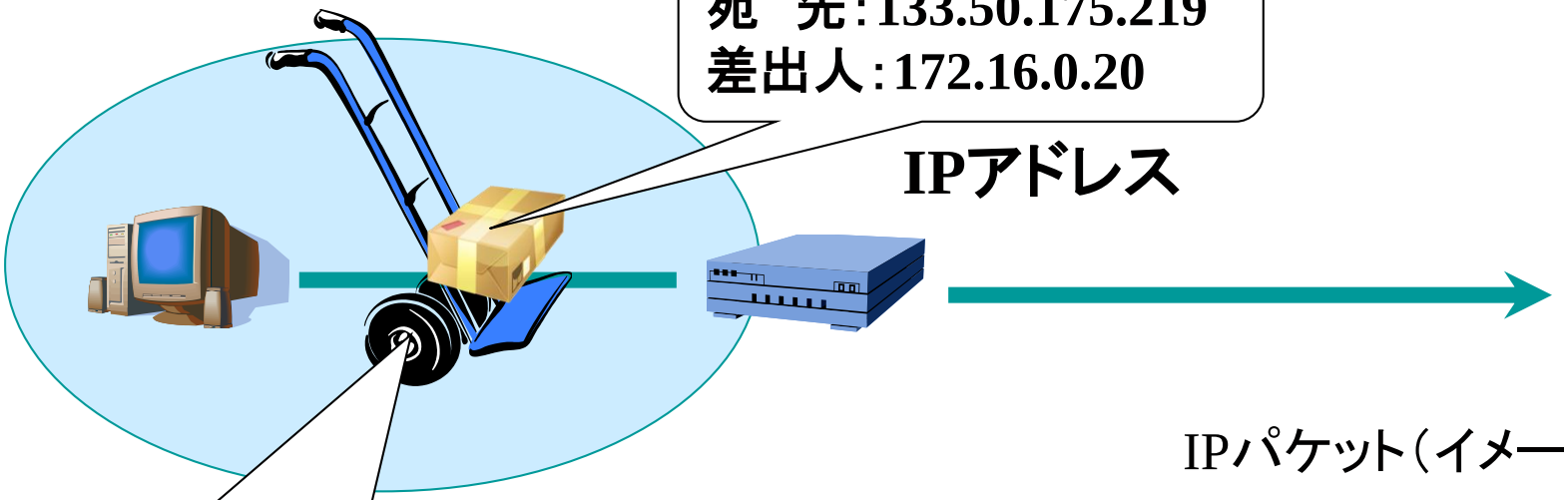


00 00 48 9F 1C 64

00 00 48 9F 1C 64

ベンダー

MAC アドレス(2)



IPパケット(イメージ)

イーサフレーム(イメージ)

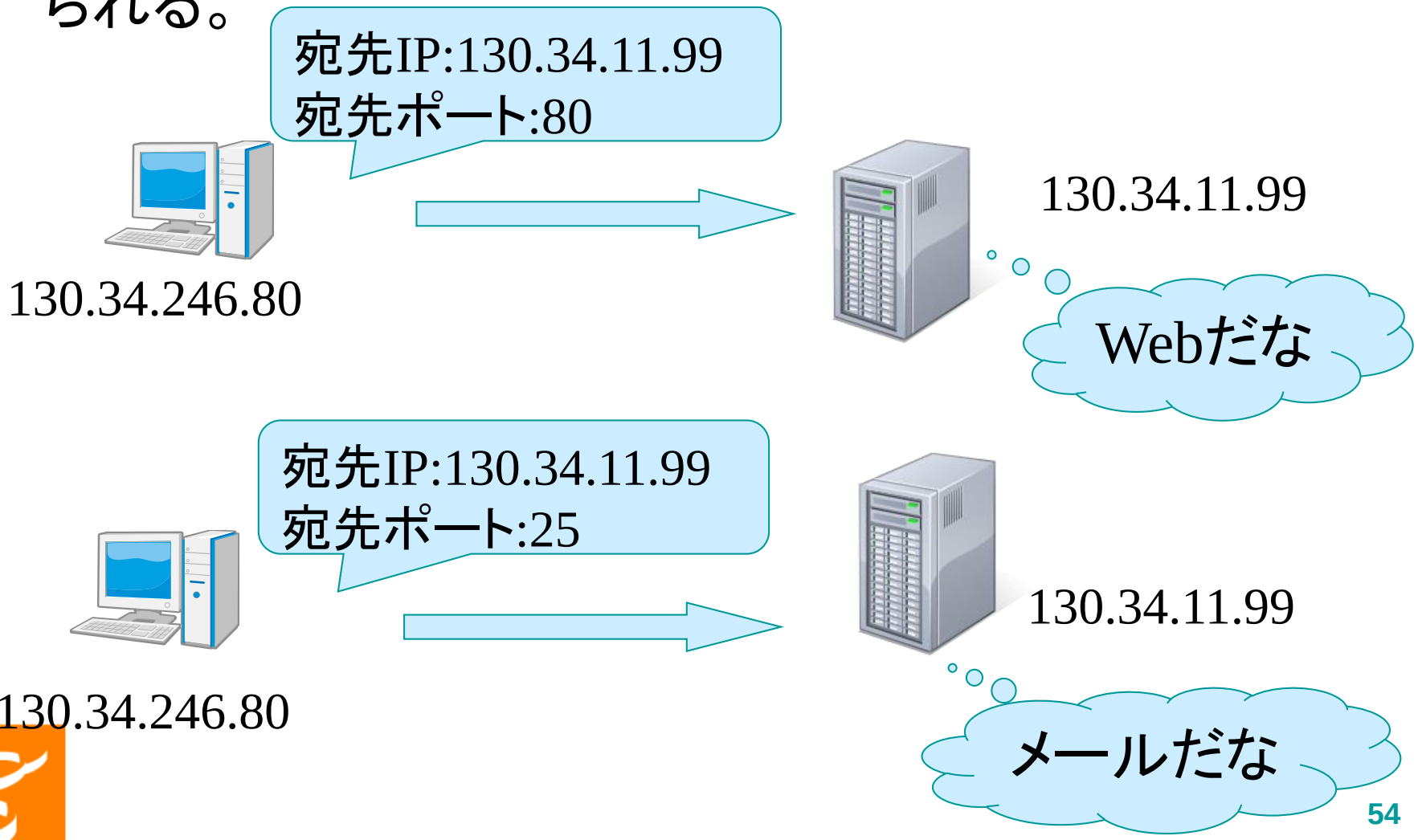
復習に…

Internet Week **ショーケース in 名古屋（2017.6.1）**
今さら聞けないIPアドレスとドメイン名
～ 見抜く力の基礎知識 ～
角倉 教義 (JPNIC)
https://www.nic.ad.jp/sc-nagoya/sc-program/day1-kadokura.pdf

4. ポート番号と ファイアウォール

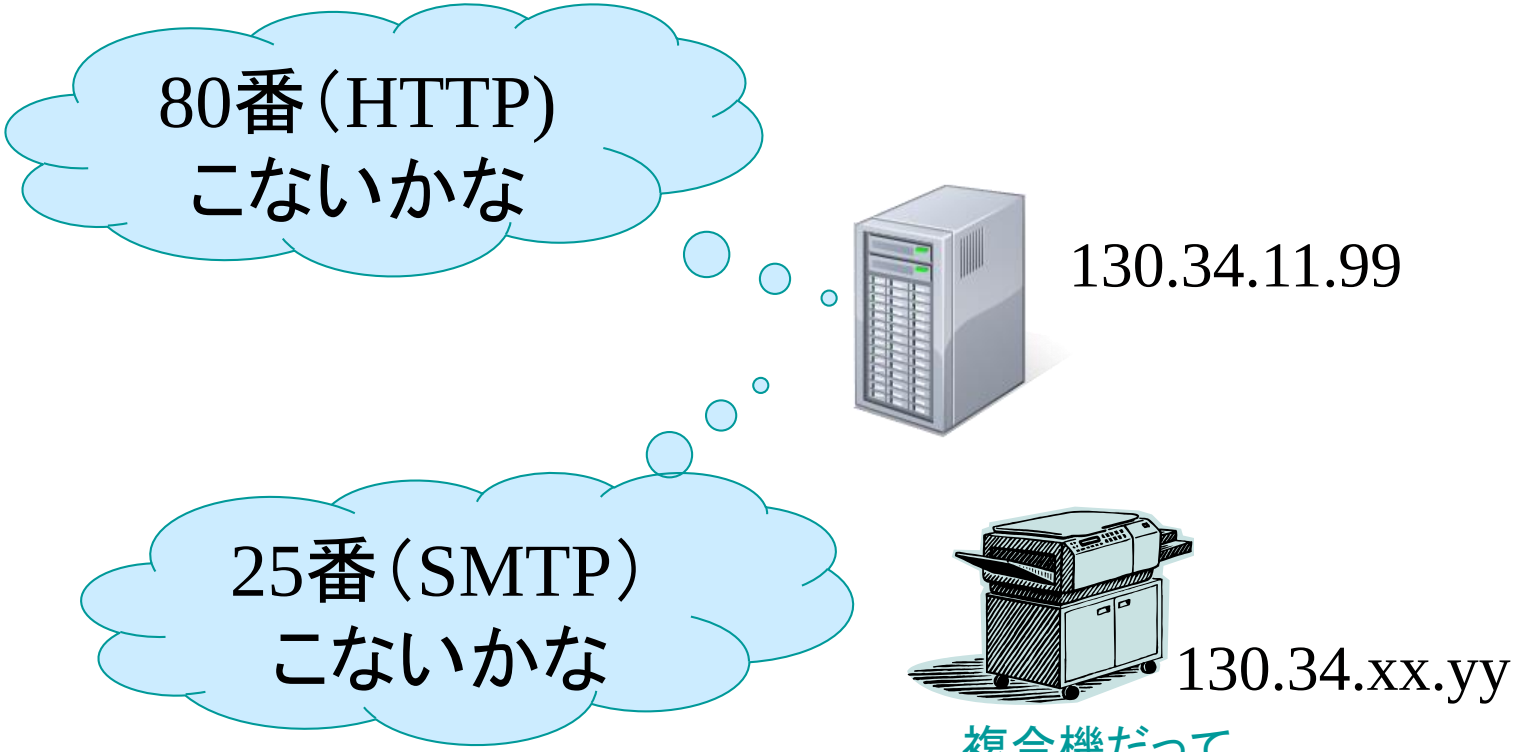
ポート番号

ポート番号は、アプリケーションを識別するのに用いられる。



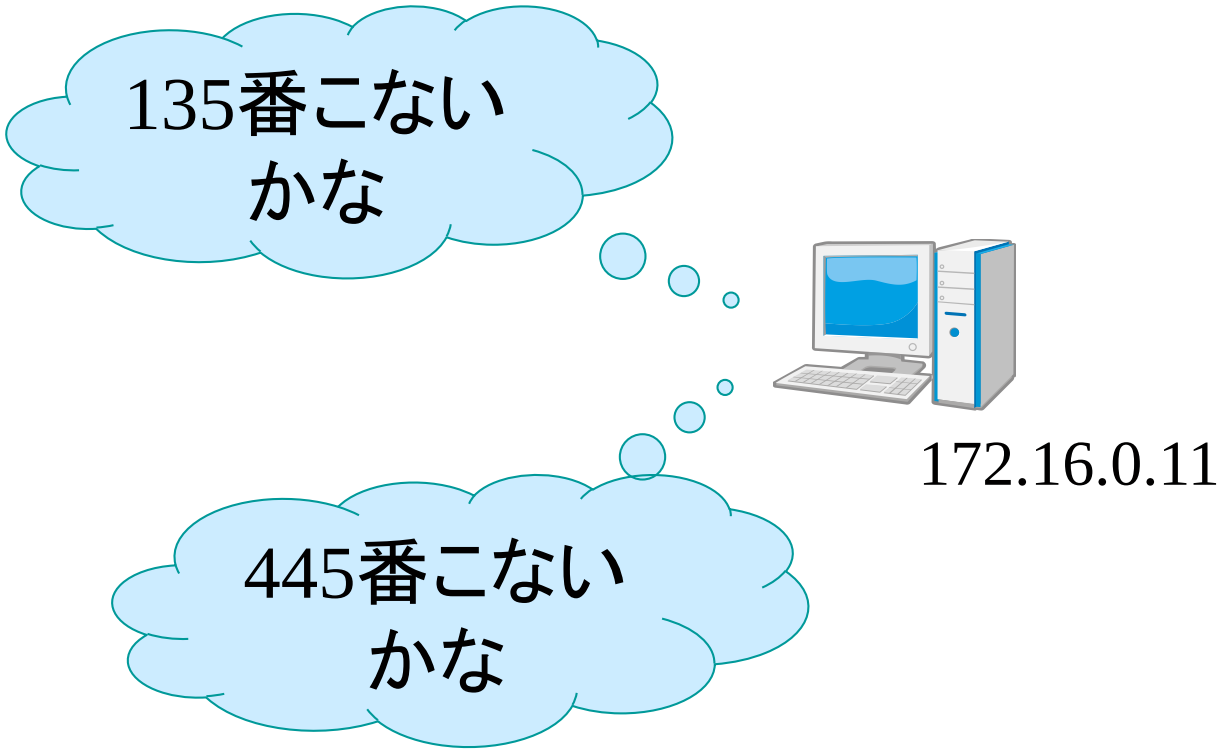
ポート番号（リッスン）

サーバは常に利用されるポートを開いて待っている。
つまり、「リッスン」している。



Windows もリッスン

Windows も、ファイル共有などに使うため、いくつかのポートをリッスンしている。



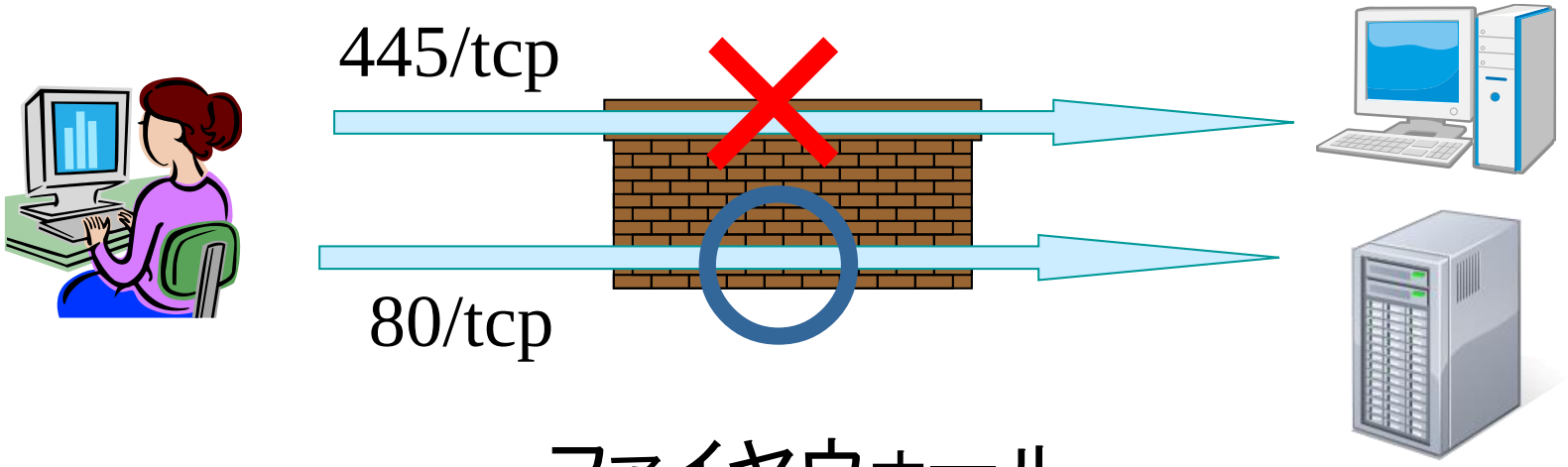
リッスンの確認

コマンドプロンプトで、netstat –an と打つ。

```
C:¥>netstat -an
アクティブな接続

  プロトコル  ローカル アドレス         外部アドレス         状態
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
…
```

ファイアウォール

ポート番号やアドレスにより、パケットを破棄したり、通過させたり設定できる。



ファイヤウォール

Windows 10付属のファイアウォール：

[スタート] → [設定] → [更新とセキュリティ] → [Windows Defender セキュリティセンター] → [ファイアウォールとネットワーク保護]

全学ファイヤーウォール(1)

略

全学ファイヤーウォール(2)

略

全学ファイヤーウォール(3)

略

全学ファイヤーウォール(4)

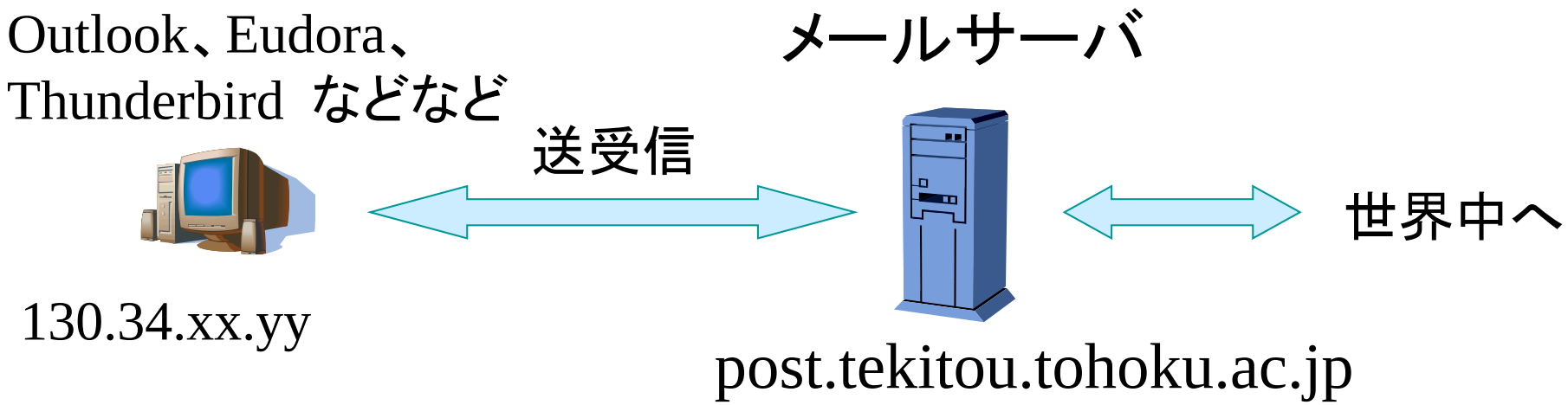
略

5. 電子メールの仕組み

電子メールについて

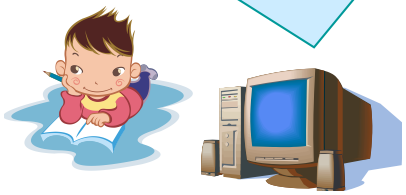
メールは、サーバに一時的に保存され、
バケツリレー式に中継されていく。

nanashidesu@tekitou.tohoku.ac.jp



電子メール（送信）

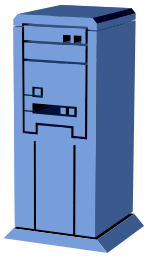
To: taro@bou.tohoku.ac.jp
From: hanako@tekitou.tohoku.ac.jp



130.34.xx.yy

送信（SMTP)

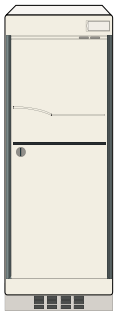
post.tekitou.tohoku.ac.jp



適当研究科
SMTPサーバ

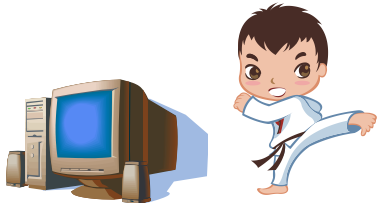
中継

mail.bou.tohoku.ac.jp



某センター
メールサーバ

受信（POP, IMAP）



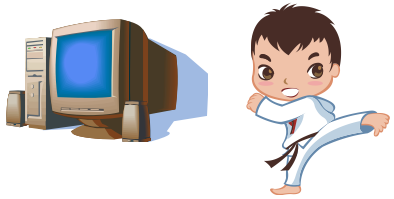
130.34.zz.aa

電子メール（受信）

某センター
メールサーバ

mail.bou.tohoku.ac.jp

ユーザ名　：　taro
パスワード：himitsu99



130.34.zz.aa

メール受信（POP, IMAP）

*****@bou.tohoku.ac.jp
宛てのメールがたくさん溜まっている。

spamメール（迷惑メール）

Web に自分のメールアドレスを掲載すると、あっという間に spam メールが届き始めます。
スパム業者が、ロボットにより、メールアドレスを収集しているためです。

アドレスを拾われないようにする対策：
（１）画像ファイルにする
（２）一部置き換え
taro＊bou.tohoku.ac.jp（＊を@に置き換えて下さい）

電子メールと安全

電子メールの差出人（From:フィールド）などは、簡単に偽造ができます。

変なメールやウイルスメールがきて、「差出人」に苦情を言っても、偽装のために、濡れ衣である場合も少なくありません。

苦情を言う場合には、ヘッダ（本文の上にあるもの）などをよく確認するとよいでしょう。

Received フィールドの読み方（1）

メールメッセージは一般に次のような形をしています。

```
Received: from mx.rei.topic.ad.jp ([202.211.0.xx])
        by mail.ex.tohoku.ac.jp; Wed, 9 Mar 2005 16:29:14 +0900
Received: from pc1.rei.topic.ad.jp ([202.211.0.yy])
        by mx.rei.topic.ad.jp; Wed, 9 Mar 2005 16:29:02 +0900
X-Mailer: Michinoku Message Reader 0.49
Message-Id:
<200503090729.j227SNHK090219.taro@rei.topic.ad.jp>
Subject: tomorrow's meeting
From: taro@rei.topic.ad.jp
To: hanako@ex.tohoku.ac.jp
Date: Wed, 9 Mar 2005 16:28:23 +0900

明日の研究打ち合わせは何時から始めましょう？
太郎より
```

Received フィールドの読み方（2）

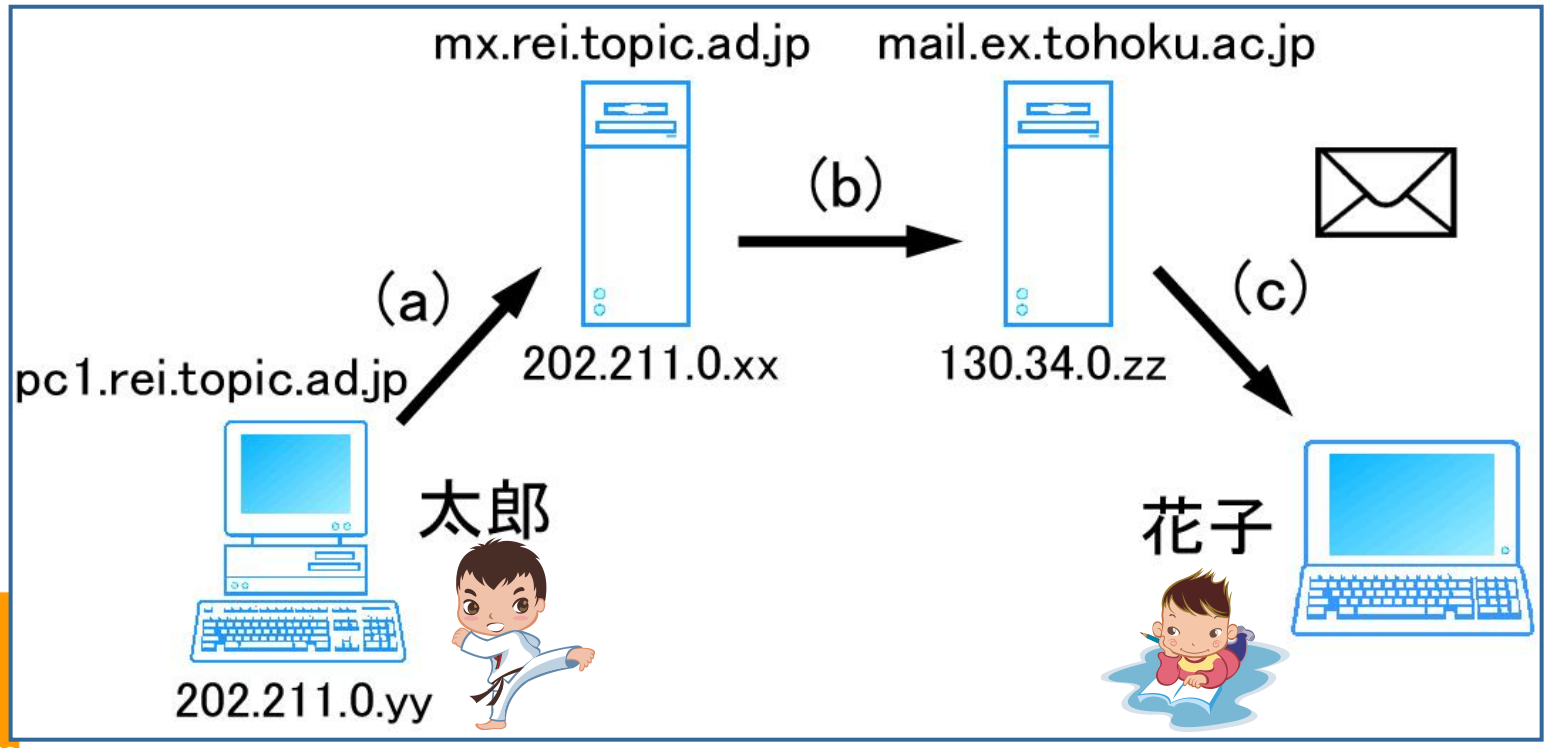
Received フィールド，From フィールドおよび To フィールドだけを抜き出してみます。

```
Received: from mx.rei.topic.ad.jp ([202.211.0.xx])
        by mail.ex.tohoku.ac.jp; Wed, 9 Mar 2005 16:29:14 +0900
Received: from pc1.rei.topic.ad.jp ([202.211.0.yy])
        by mx.rei.topic.ad.jp; Wed, 9 Mar 2005 16:29:02 +0900
From: taro@rei.topic.ad.jp
To: hanako@ex.tohoku.ac.jp
```

Received フィールドの読み方（3）

（b）
（a）

```
Received: from mx.rei.topic.ad.jp ([202.211.0.xx])
        by mail.ex.tohoku.ac.jp; Wed, 9 Mar 2005 16:29:14 +0900
Received: from pc1.rei.topic.ad.jp ([202.211.0.yy])
        by mx.rei.topic.ad.jp; Wed, 9 Mar 2005 16:29:02 +0900
From: taro@rei.topic.ad.jp
To: hanako@ex.tohoku.ac.jp
```



Received フィールドの読み方(4)

Subject: Mail Delivery System (hanako@ex.tohoku.ac.jp)
From: taro@rei.topic.ad.jp
To: hanako@ex.tohoku.ac.jp
Date: Tue, 8 Mar 2005 17:32:54 +0900

Mail Delivery Failure - This mail couldn't be shown.

---------- failed message ----------
2,mnqxZk,jgsdf:YE#0yB.+sgH| -JNqMd9n#OC,SQ-V-8&6W0KtK|LGB06c2Y,9.Zutqn0pIoG..gBB5Lmga+WnKrGhk+F|hS2aY'3i44+asdfLj_6nd4LXQtyt.USYfP

Note: Received message has been sent as a binary file

太郎君を疑う前に …

Received フィールドの読み方（5）

注目！

```
Received: from ex.tohoku.ac.jp (pasokon.example.jp [192.42.103.xx])
        by mail.ex.tohoku.ac.jp; Tue, 8 Mar 2005 17:35:12 +0900
From: taro@rei.topic.ad.jp
To: hanako@ex.tohoku.ac.jp
```

このウイルスメール（Netsky.Q）は，192.42.103.xx という IP アドレスを持ち，その逆引きドメイン名が pasokon.example.jp であるパソコンから発信されたもの。「from …」の直後の「ex.tohoku.ac.jp」は，その感染パソコンが自己申告した情報をそのまま記しただけで，正確なものであるとは限らない。
それに対し，その後ろの括弧内は，サーバ mail が自分で接続元を調べて記したもの。つまり，サーバ mail が正常であれば，括弧内のコメントは正確なものになる。

Received フィールドの読み方（6）

Received: from ex.tohoku.ac.jp (pasokon.example.jp [192.42.103.xx])
by mail.ex.tohoku.ac.jp; Tue, 8 Mar 2005 17:35:12 +0900
From: taro@rei.topic.ad.jp
To: hanako@ex.tohoku.ac.jp

192.42.103.xx

詐称メール（SMTP）

某部局
メールサーバ

mail.ex.tohoku.ac.jp

受信（POP）

hanako@ex.tohoku.ac.jp

詳しくは、TAINSニュース　32号　5～10ページ
「メールヘッダの Received フィールドの読み方」
http://www.tains.tohoku.ac.jp/news/news-32/0510.html

実例(1)

略

実例(2)

略

IPA テクニカルウォッチより

「標的型攻撃メールの例と見分け方」
独立行政法人情報処理推進機構

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

【以下引用】
標的型攻撃メールは、不特定多数に大量に送られるウイルスメールとは異なり、特定の組織や人にしか送られないため、セキュリティソフトの定義ファイルに登録される前に標的とするメール受信者まで届いてしまう。そのため、受信者がセキュリティソフトを利用していても、被害を防ぐことが難しい。

ウイルス付メールの注意喚起情報

日本サイバー犯罪対策センター

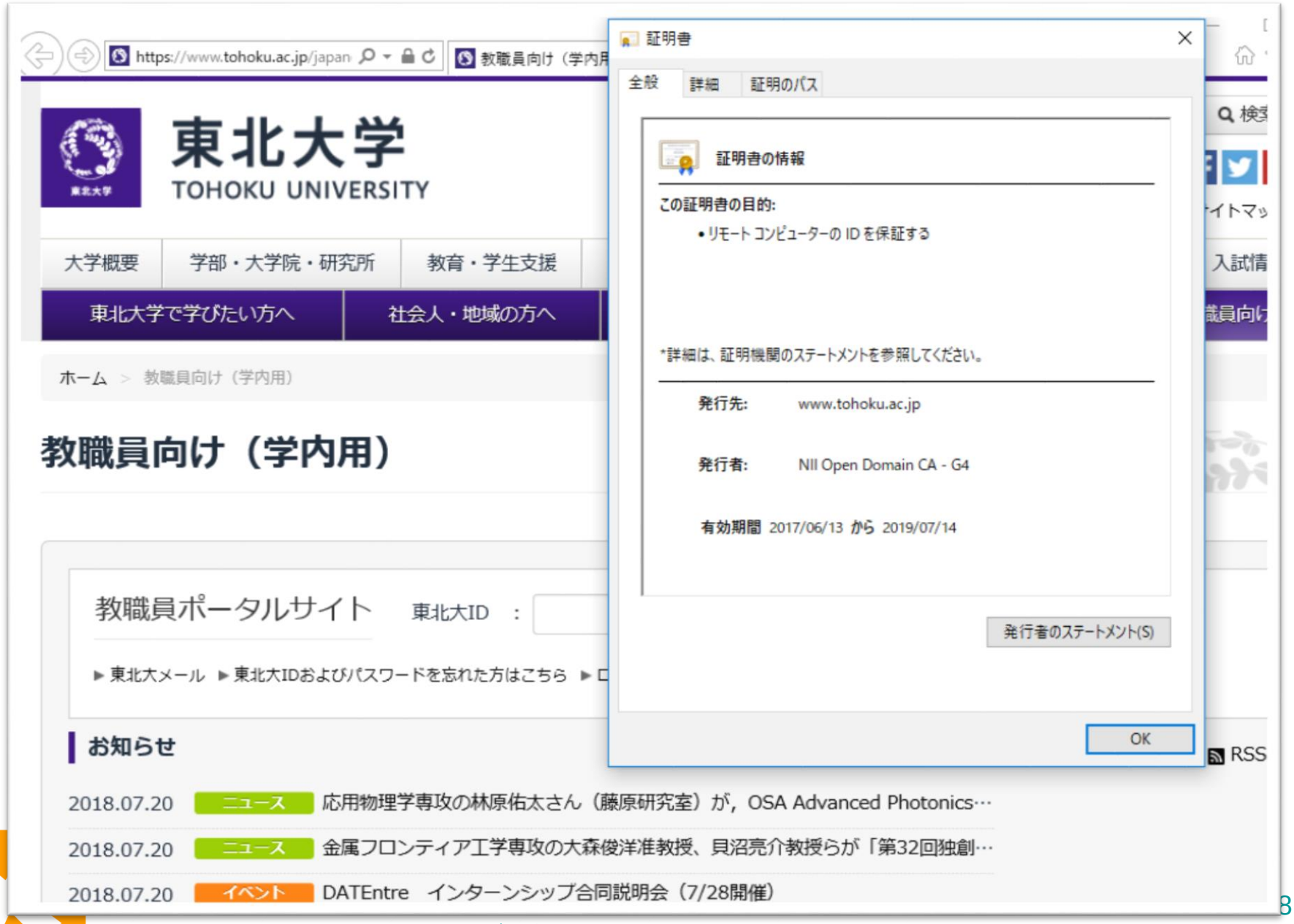
https://www.jc3.or.jp/topics/virusmail.html

6. Web の安全な利用

HTTPS

HTTPSでは，HTTP over SSL/TLS により，サーバの認証やメッセージの暗号化等が行われ，Webの利用の安全性を向上させている。

具体例:ブラウザで接続(○)

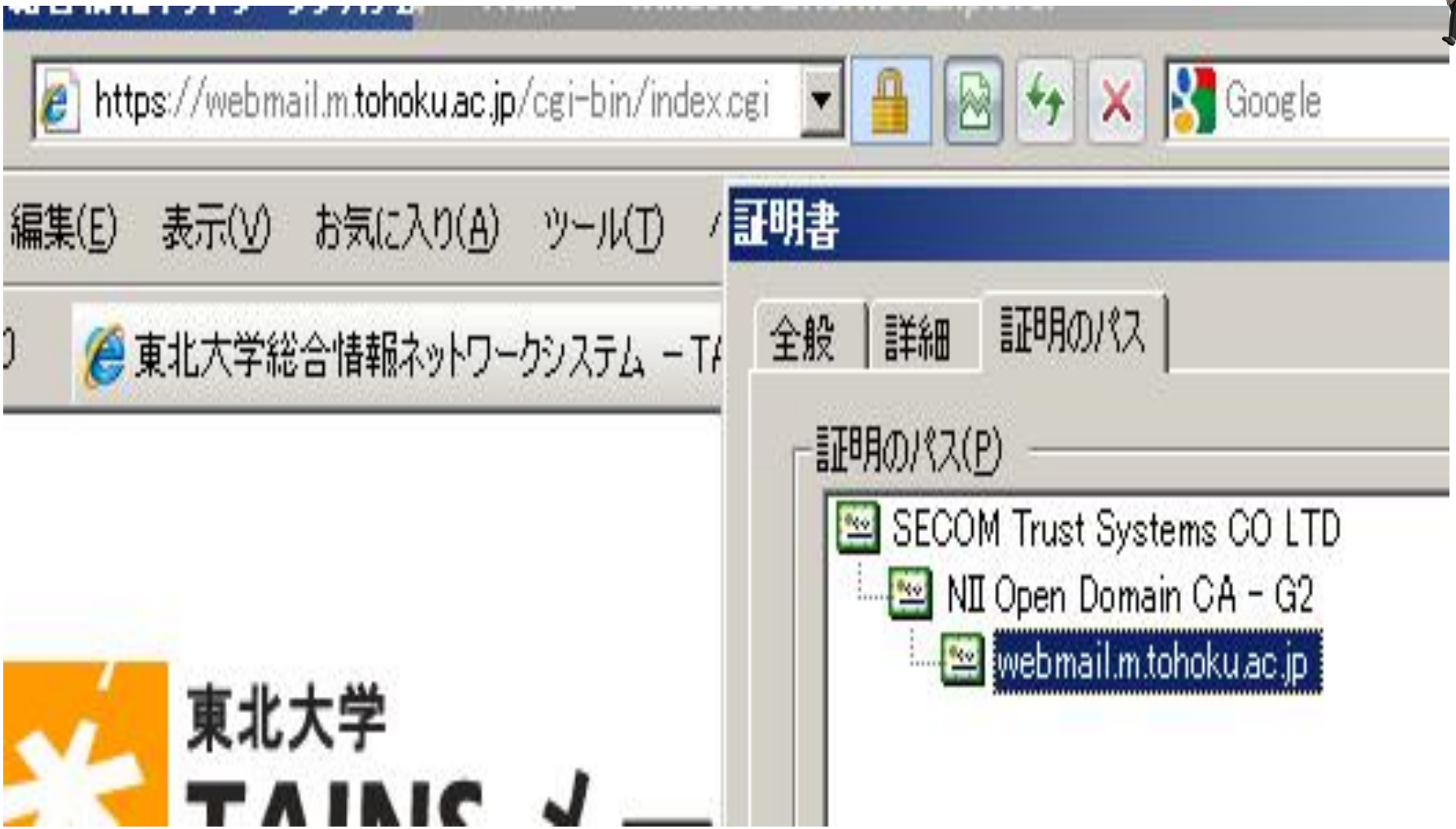


Microsoft Corporation のガイドラインに従って画面写真を使用しています。

具体例:ブラウザで接続(×)

略

サーバ証明書のチェイン

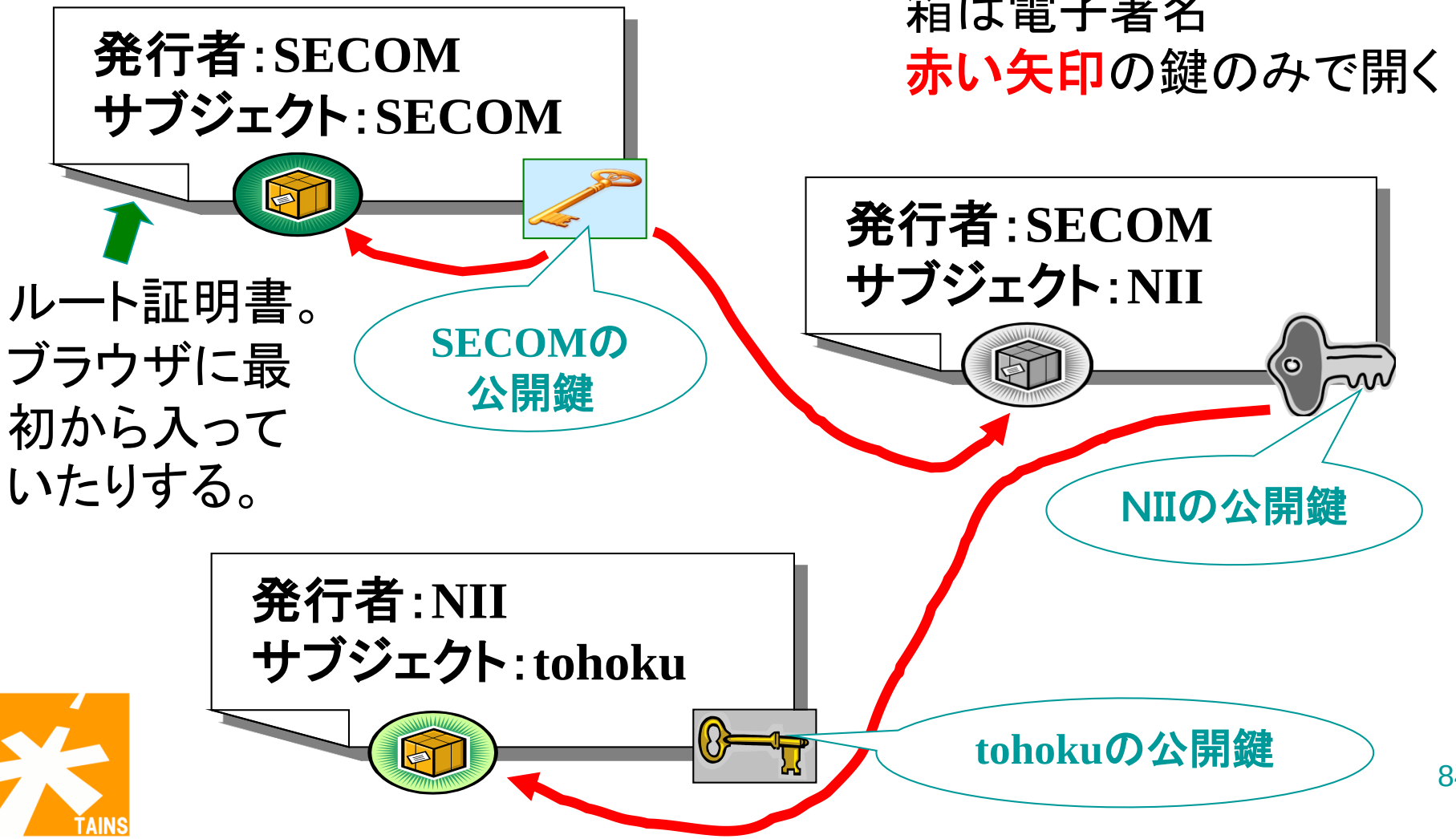


SECOM → NII → tohoku.ac.jp

TAINS

サーバ証明書のチェイン;3つの証明書

SECOM → NII → tohoku.ac.jp



サーバ証明書のチェイン;通信の流れ

webmail.m.
tohoku.ac.jp

証明書を送る

発行者:SECOM
サブジェクト:SECOM

設定依存

発行者:SECOM
サブジェクト:NII

発行者:NII
サブジェクト:tohoku

ブラウザの中

発行者:SECOM
サブジェクト:SECOM

サーバ証明書;オレオレの場合(一例)

oreore.
example.jp

1枚の証明書を送る

発行者:OREORE
サブジェクト:OREORE

ブラウザの中

???

7. セキュリティ情報

情報シナジー機構のページより(1)

学内限定:

略

情報シナジー機構のページより(2)

セキュリティ対策ソフト

略

セキュリティ対策ソフトウェア

情報シナジー機構では，以下を配布しています。

略

情報シナジー機構のページより(3)

パスワードの取り扱い

略

STOP! パスワード使い回し!（JPCERT/CCより）

STOP! パスワード使い回し! ～知っておきたい、パスワードの危険な落とし穴とその対策～

http://www.jpcert.or.jp/pr/2018/stop-password2018.html

情報シナジー機構のページより(4)

持ち出し時の対策

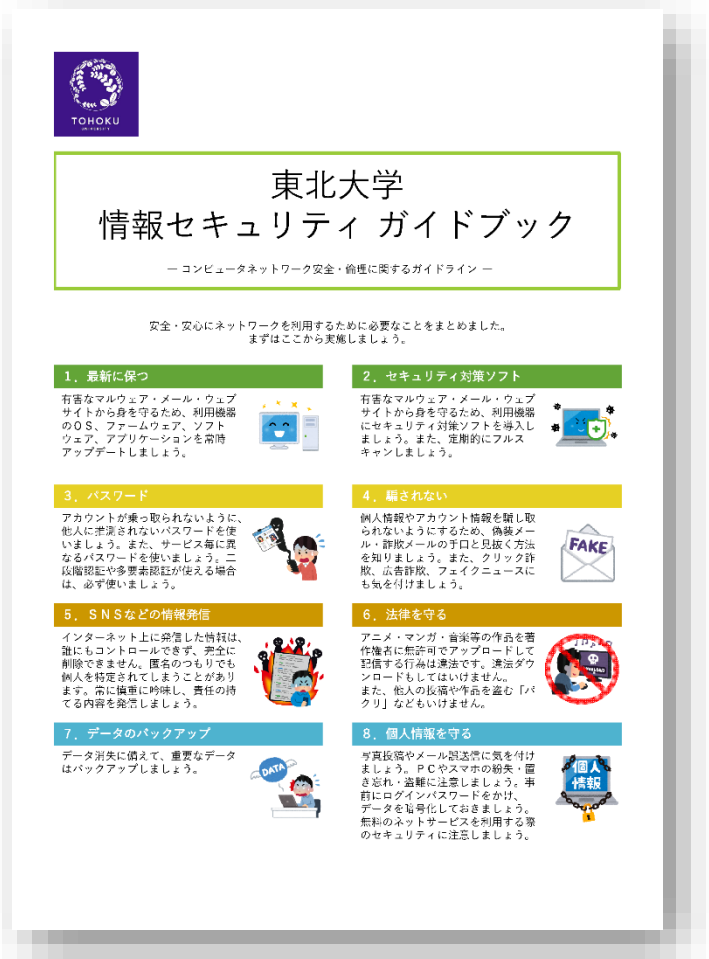
略

情報シナジー機構のページより(5)

利用開始時・終了時の対策

略

コンピュータネットワーク安全・倫理に関するガイドライン


東北大学
情報セキュリティ ガイドブック

― コンピュータネットワーク安全・倫理に関するガイドライン ―

安全・安心にネットワークを利用するために必要なことをまとめました。
まずはここから実施しましょう。

1．最新に保つ
有害なマルウェア・メール・ウェブサイトから身を守るため、利用機器のＯＳ、ファームウェア、ソフトウェア、アプリケーションを常時アップデートしましょう。

2．セキュリティ対策ソフト
有害なマルウェア・メール・ウェブサイトから身を守るため、利用機器にセキュリティ対策ソフトを導入しましょう。また、定期的にフルスキャンしましょう。

3．パスワード
アカウントが乗っ取られないように、他人に推測されないパスワードを使いましょう。また、サービス毎に異なるパスワードを使いましょう。二段階認証や多要素認証が使える場合は、必ず使いましょう。

4．騙されない
個人情報やアカウント情報を騙し取られないようにするため、偽装メール・詐欺メールの手口と見抜く方法を知りましょう。また、クリック詐欺、広告詐欺、フェイクニュースにも気を付けましょう。

5．ＳＮＳなどの情報発信
インターネット上に発信した情報は、誰にもコントロールできず、完全に削除できません。匿名のつもりでも個人を特定されてしまうことがあります。常に倫理に吟味し、責任の持てる内容を発信しましょう。

6．法律を守る
アニメ・マンガ・音楽等の作品を著作権者に無許可でアップロードして配信する行為は違法です。違法ダウンロードもしてはいけません。また、他人の投稿や作品を盗む「パクリ」などもいけません。

7．データのバックアップ
データ消失に備えて、重要なデータはバックアップしましょう。

8．個人情報を守る
写真投稿やメール誤送信に気を付けましょう。ＰＣやスマホの紛失・置き忘れ・盗難に注意しましょう。事前にログインパスワードをかけ、データを暗号化しておきましょう。無料のネットサービスを利用する際のセキュリティに注意しましょう。

このガイドラインは、コンピュータネットワークを利用する際に守るべき、安全・倫理に関する注意事項を示したものです。
携帯電話やスマートフォンなどからインターネットを利用する際も参考にしてください。

情報シナジー機構ウェブページ
http://www.bureau.tohoku.ac.jp/i-synergy/index.html
→刊行物をみたい（学内限定）

情報セキュリティハンドブック

内閣サイバーセキュリティセンター（NISC）の「ネットワークビギナーのための情報セキュリティハンドブック」は読み応えがあります。電子書籍無料です。一読をお勧めします。

http://www.nisc.go.jp/security-site/handbook/index.html

Ver.4.03（平成31年6月18日）

8. おわりに

おわりに

コンピュータネットワークの仕組みを理解しましょう。

- 自分のIPアドレス、ゲートウェイなどを知る
- ドメイン名（DNS）、メール、ポート、ウイルス等
- トラブルがあったとき、原因を自分で調べてみる

もし被害にあったら…

加害者になってしまった場合：早急に対処しましょう

攻撃を受けた場合：慌てず、落ち着いて、暖かい目で

まとまりのないお話しでした。

ネットワークやセキュリティに関する情報は、市販されている雑誌やマニュアル本、あるいはインターネットの Web 上にたくさん存在します。

本講習会が、そのような情報にアクセスしようという動機付けになれば幸いです。

どうもありがとうございました