メールとネットワークの基礎

～初心者対象～

2025/6/20　第9版

大阪大学レーザー科学研究所
高性能計算機室
http://www.ile.osaka-u.ac.jp/research/cmp/

Contents

はじめに

　このテキストは、ネットワークやメールの基礎がよく分からないという方を対象に、基礎的なことをなるべく分かりやすく、簡潔に説明する講習会資料として2006年に初めて作成しました。

Webなどに情報があふれていますが、セキュリティもスパコン（HPC分野）も変化が著しいので、戸惑う方が多いです。
しかし、基礎のイメージをつかんでいただけば理解も深まり、応用もできるようになると、実感してきました。

セキュリティの最新情報のウォッチ

セキュリティなんて関係ない？

マックやスマホだから大丈夫？

残念ながらそんなことはありません。
状況はどんどん変わり、被害も大きくなっています。

インターネットの基礎

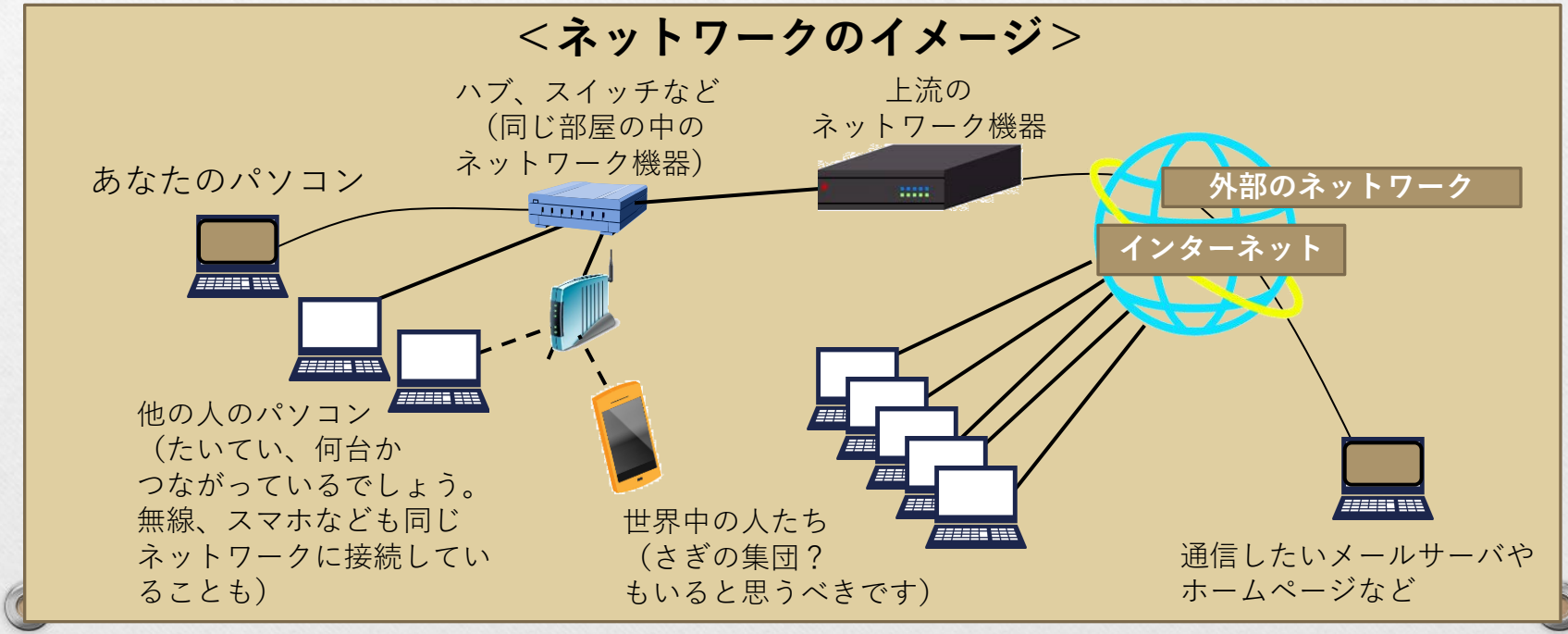
インターネットやネットワークとは、世界中のコンピュータをつなぐ電話線のようなものと思えばよいのでしょうか？

答えはNOだと思います。

コンピュータをネットワークに接続した瞬間、そのコンピュータは世界中から丸見えかもしれません。

家の玄関の扉をあけっぱなしにしていても、前を通った人しか中を見たり、入ってきたりできませんが、ネットワークにつなぐということは、世界中から家（コンピュータ）の中をのぞくだけでなく、入ってくることも可能な状態になるということだという認識が必要です。

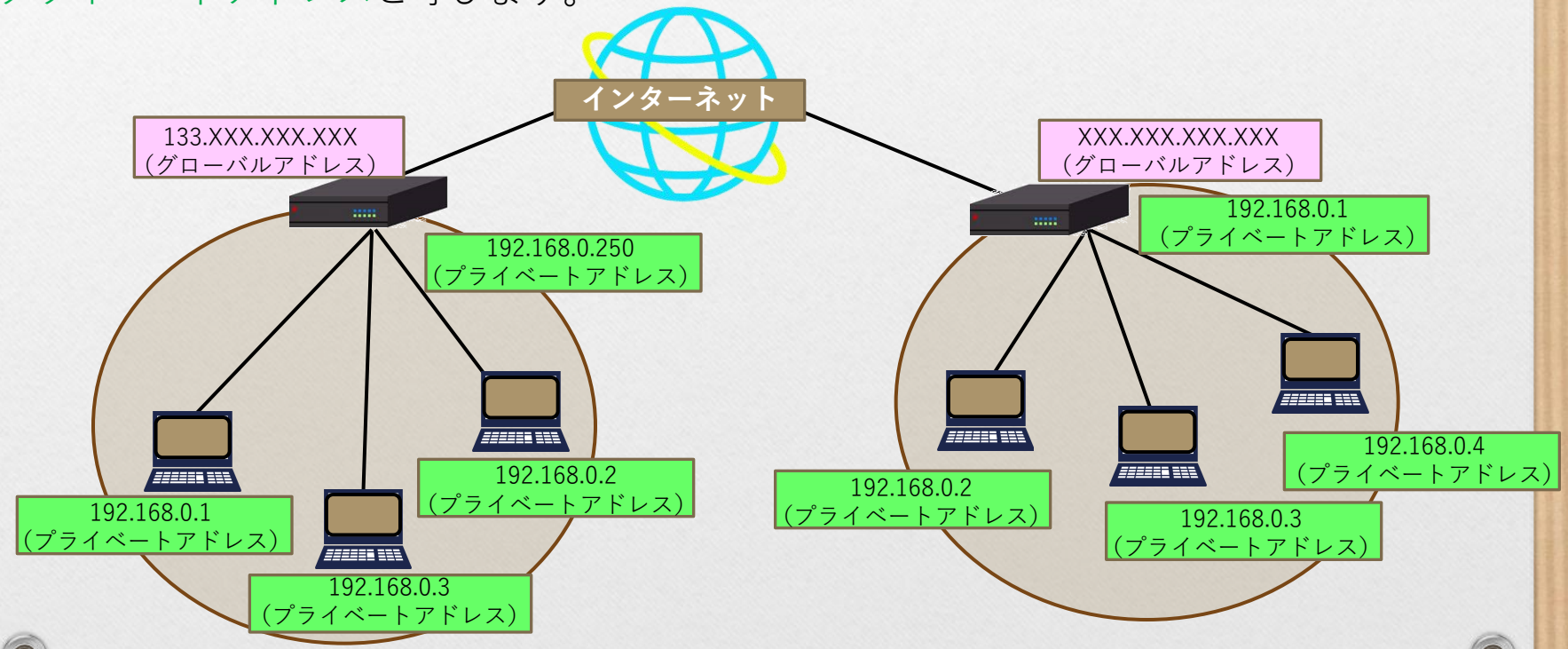
スマホが当たり前の時代になり、ネットを意識せず利用されている方も増えていますが、気をつけて利用する必要があります。



IPアドレス

ＩＰアドレスはネットワーク上の住所を指す情報です。
「192.168.0.1」というように0～２５５までの数字（１０進法表記）を、「.」（ドット）で区切って4つ並べて表します。（IPｖ４）※ＩＰアドレス枯渇問題

インターネット上で利用できる世界中でただ一つのＩＰアドレスをグローバルアドレス、
組織内ＬＡＮや家庭内ＬＡＮなどその組織内でのみ利用できるＩＰアドレスを、
プライベートアドレスと呼びます。



ドメイン名とホスト名

ネットワークに接続されたコンピュータは、データの送受信をするときには、通信相手をIPアドレスという数字で指定します。
しかし、IPアドレスという数字では、人間にはわかりにくく覚えにくいため、住所にあたる**ドメイン名**と、名前にあたる**ホスト名**を用いて、
メールの送受信やホームページを閲覧などの、ネットワークを介した通信を行います。

＜例＞正式なホスト名

mycomputer.ile.osaka-u.ac.jp

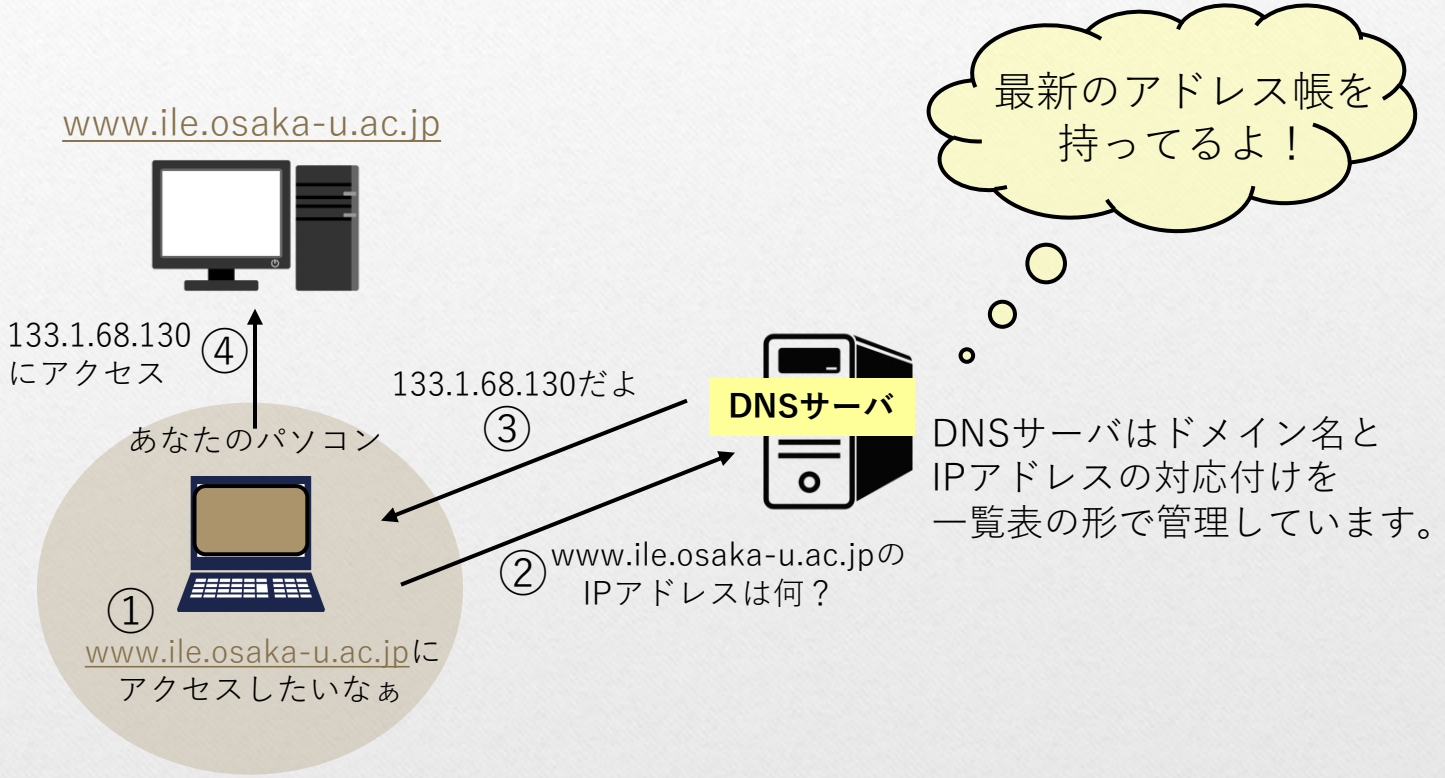
レーザー研．大阪大学．　日本

ドメイン名：
コンピュータの住所を表現したもの。
日本の大阪大学のレーザー研という意味

ホスト名：
コンピュータの名前。
ＩＰアドレスを人間が覚えやすい文字列と対応付け、
人間が文字で相手先コンピュータを指定することを可能にしたもの。

DNS（ドメインネームシステム、名前解決）

DNSとは、コンピュータのホスト名を元に、そのコンピュータのIPアドレスを教えてくれる仕組みです。

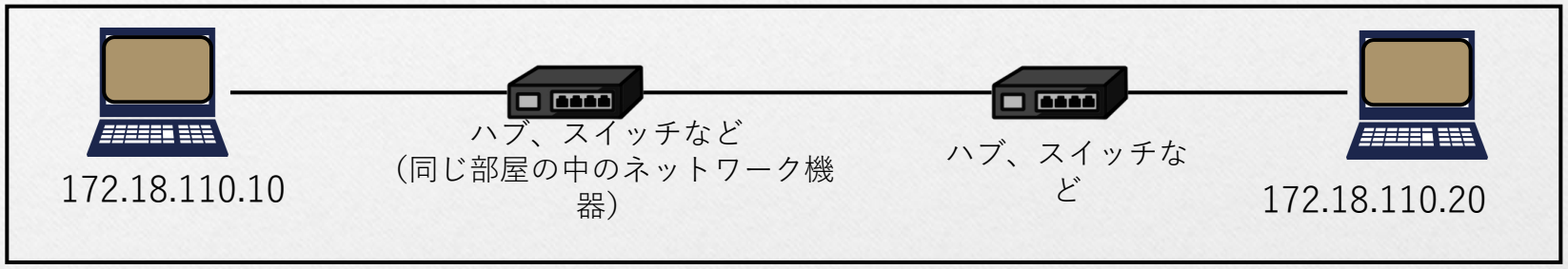


DNSサーバの設定が間違っていると、名前解決に失敗し、メールの送受信ができない、ホームページが見えないなどのネットワークのトラブルの症状が現れます。

セグメント

同じセグメントの中のコンピュータやプリンタとの通信

→ 線さえ**つながって**いれば通信可能



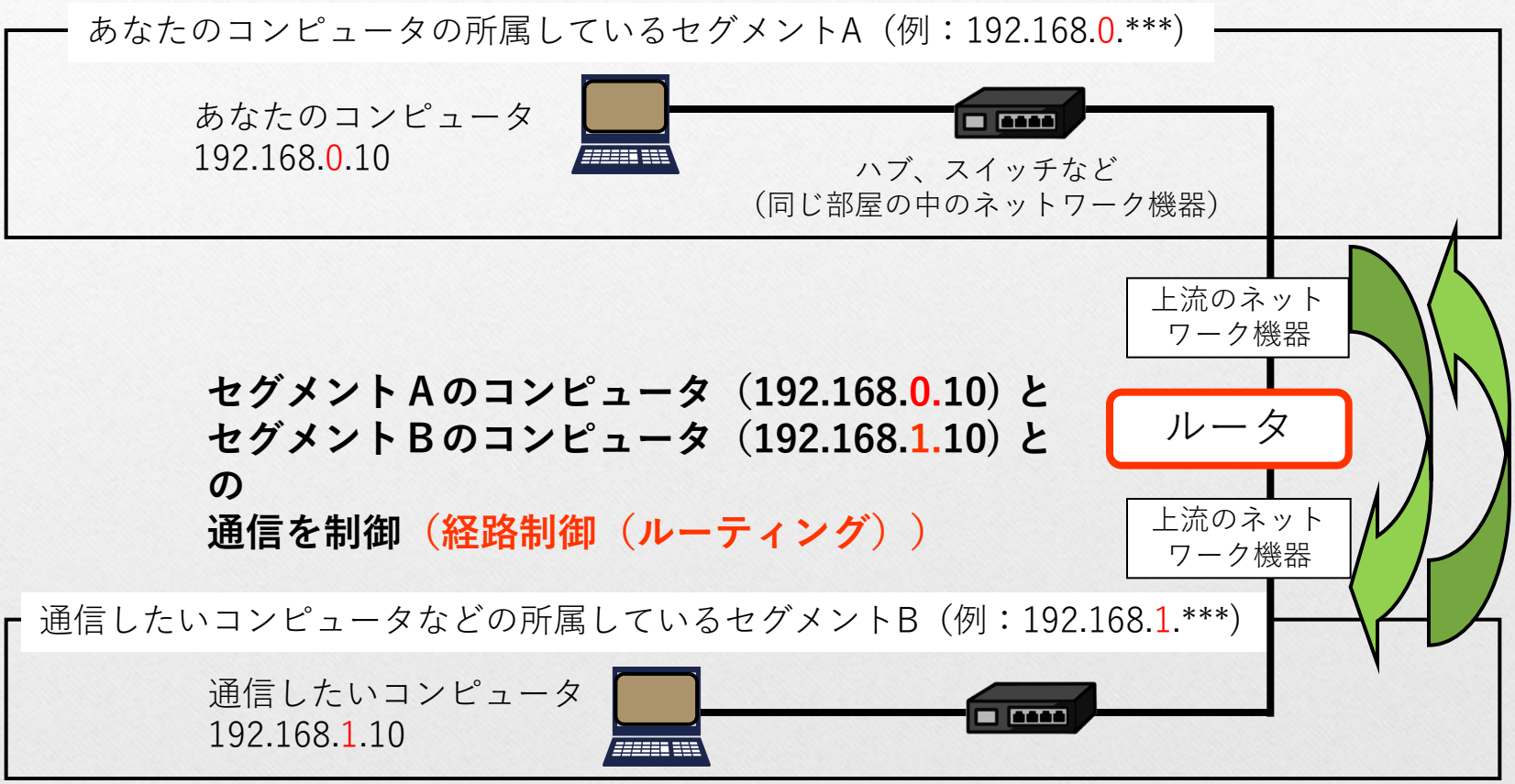
セグメントとは・・・

HUBやスイッチなどで接続された、一つのネットワークのこと。
「サブネット」とも言います。

ルーティング（ゲートウェイ）

異なるセグメントにあるコンピュータやプリンタとの通信には**ルータ**が必要です

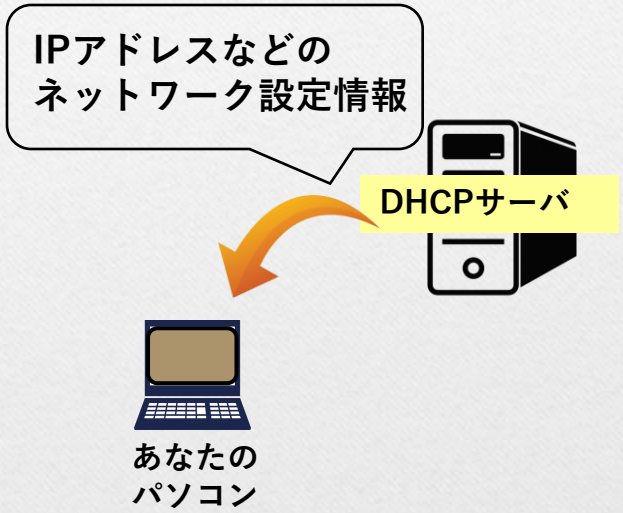
＜例＞　サブネットマスクが　255.255.255.0



DHCP　（Dynamic Host Configuration Protocol ）

DHCPとは、クライアント（パソコン）に対して、動的にIPアドレスを割り振る機能です。

クライアントは、DHCPサーバからIPアドレスをもらいます。
（その他、ゲートウェイアドレスやDNSサーバなど通信に必要な設定も、もらいます）

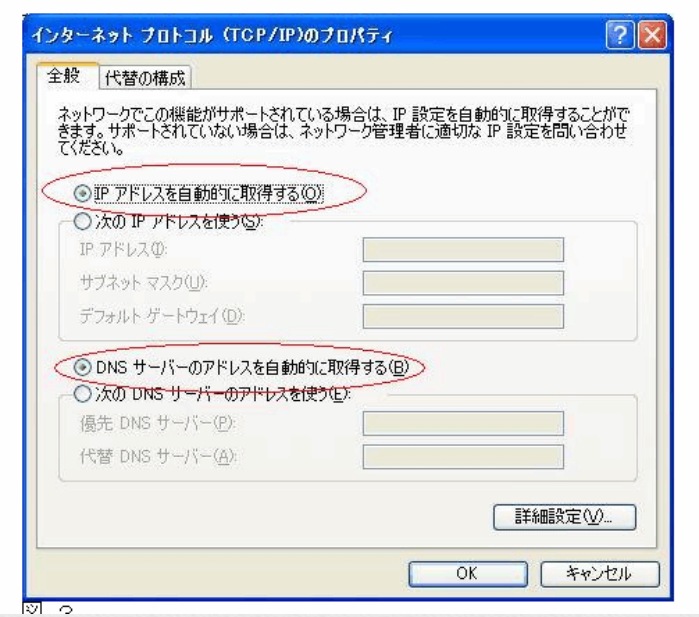


＜DHCPの利点＞
- IPアドレスが有効活用できる
  （起動していないマシンには払いだされない）
- クライアントのネットワーク設定ミスによるトラブルがなくなる。
  （IPアドレス競合など）
- 使用場所を変えても、ネットワーク設定変更が不要のことが多い。

ネットワーク通信のための設定

ネットワークを用いて通信するためには、各パソコンに下記の設定が必要です。

■DHCPサーバから取得する場合
「IPアドレスを自動的に取得する」に
チェックをいれる
（DHCPサーバが設定してくれます）



DHCPでの設定例

■手動で設定する場合
1） IPアドレス
（及び、サブネットマスク）
2） ルータアドレス
（ゲートウェイアドレス）
3） DNSサーバアドレス

手動（固定アドレス）の設定例

※現在はほとんどＤＨＣＰです

サブネットマスク

サブネットマスクとは、住所にあたるIPアドレスのうち、
どこまでがネットワークアドレスでどこからがホストアドレスにあたるかを
定義する３２ビットの数値のことです。
１０進法表記の場合は、８ビット毎に「.（ドット）」で区切って表現します。

＜例＞IPアドレスが、192.168.0.1　サブネットマスクが、255.255.255.0/24の場合

11111111 11111111 11111111 00000000

255.255.255.0を
２進法で表現するとこう
なる

192.168.0　が**ネットワークアドレス**

ホストアドレス：
0～255までの256個のIPが利用できるIPアドレスとなる
（最初「0」と最後「255」は実際には使用できない）

同じネットワークアドレスを持ったPCなどの機器　→　同一ネットワークセグメント
線さえつながっていれば、送受信可能

違うネットワークアドレスを持ったPCなどの機器　→　別ネットワークセグメント
ルータなどのネットワーク機器で分割します

ネットワークトラブルの見分け方

Case.　Webが見れない、メールの送受信ができない

メールの送受信ができない、Ｗｅｂページが見えないなどの場合は
まずネットワークの物理的な接続を確認しましょう

たとえば

・ネットワークケーブルはちゃんと接続されていますか？

・リンクアップのランクはついていますか？
（パソコン側、ハブ側）
ネットワークケーブルがささっている所は正常時は何色？

・無線なら無線のポート、無線のアクセスポイントは？

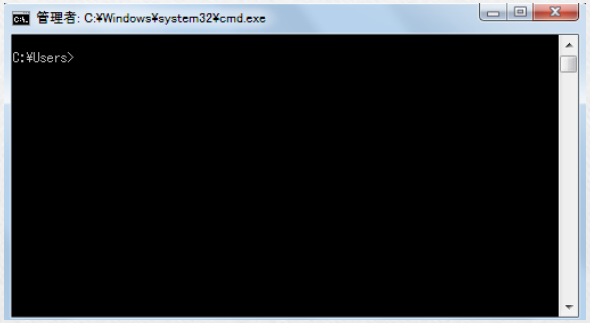
ランプに問題なければ、ローカルは大丈夫そうです
さらに上流も気になりますが、まずは設定確認をしましょう

ネットワークトラブルの見分け方

ネットワークの設定を確認しましょう

・ネットワークの設定はどうなっていますか？
　以下のコマンドを入力してみてください

Windowsの場合	コマンドプロンプトで	------ ipconfig /all
Macintoshの場合	ターミナル画面で	-------- ifconfig
Linuxの場合	ターミナル画面で	--------- /sbin/ifconfig



Windowsのコマンドプロンプトはこんな画面です。
Windowsキー(Windowsの旗のマークが書かれたキー)と
「r」キーを同時に押すと「ファイル名を指定して実行」
ダイアログが表示されますので、
「ｃｍｄ」と入力するとでてきます。

「すべてのプログラム」＞「Windowsツール」＞
「コマンドプロンプト」としても現れます。

ネットワーク設定確認（Windowsの場合）

自分が使っているネットワークの設定情報を確認してください

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 . . . . .:
説明. . . . . .: Realtek PCIe GBE Family Controller
物理アドレス. . . . . .: 12-34-AB-CD-56-78
DHCP 有効 . . . . . .: はい
自動構成有効. . . . . .: はい
IPv6 アドレス . . . . . .: 1111:...:...:...:...:...(優先)
一時 IPv6 アドレス. . . . . .: 1111:...:...:...:...:...:...(優先)
一時 IPv6 アドレス. . . . . .: 1111:...:...:...:...:...:...(使用されていません)
リンクローカル IPv6 アドレス. . . . .:2222 :...:...:...:...:...:... (優先)
IPv4 アドレス . . . . . .: 192.168.0.10(優先)
サブネット マスク . . . . . .: 255.255.255.0
リース取得. . . . . .: 2016年6月3日 9:09:14
リースの有効期限. . . . . .: 2016年6月4日 11:49:55
デフォルト ゲートウェイ . . . . . .: 192.168.0.1
DHCP サーバー . . . . . .: 192.168.0.2
DHCPv6 IAID . . . . . .:
DHCPv6 クライアント DUID. . . . . .: 00-00-00-...
DNS サーバー. . . . . .: 192.168.0.1
NetBIOS over TCP/IP . . . . . .: 有効

有線のイーサーネットアダプターの例
（正常時に確認しておくとよくわかります）

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サーバなどの設定が正しく表示されていますか？

ＤＨＣＰ環境で、この設定がされていればDHCPサーバーまでの通信はＯＫでしょう

OK

複数のネットワークカードが搭載されている場合は、注意！
例）無線LAN用ネットワークカード
有線LAN用ネットワークカード　など・・・
搭載されているネットワークカードそれぞれの情報が表示されます。

通信確認（デフォルトゲートウェイ）

pingコマンドでデフォルトゲートウェイ（ルーター）まで正しく通信できているかを確認してみる

```
C:¥Users>ping 192.168.0.254

192.168.0.254 に ping を送信しています 32 バイトのデータ:
192.168.0.254 からの応答: バイト数 =32 時間 =66ms TTL=62
192.168.0.254 からの応答: バイト数 =32 時間 <1ms TTL=62
192.168.0.254 からの応答: バイト数 =32 時間 <1ms TTL=62
192.168.0.254 からの応答: バイト数 =32 時間 <1ms TTL=62

192.168.0.254 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 0ms、最大 = 66ms、平均 = 16ms
```

応答が返ってきますか？

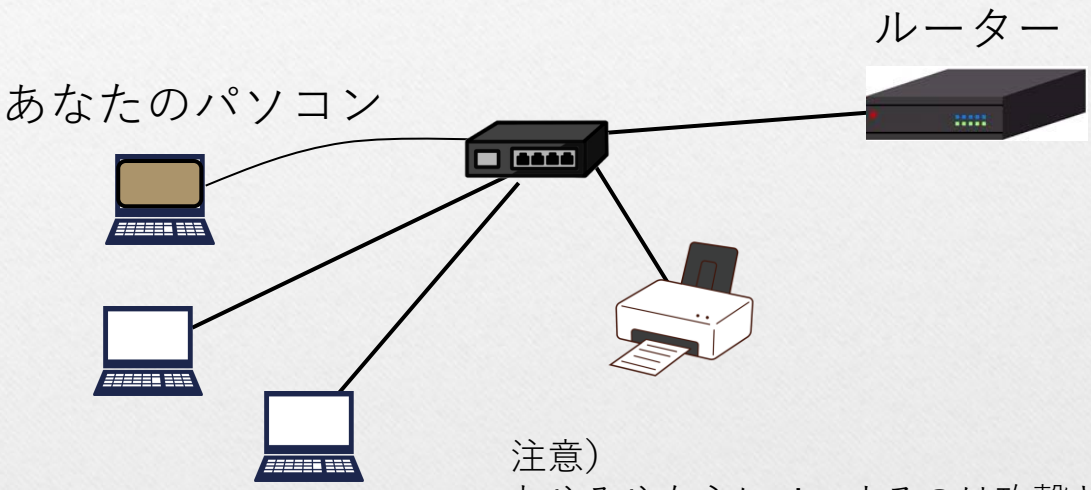
このように応答が返ってきたら
ルーターまでのネットワーク通信はOK

OK

ルータまでの通信確認

ルーターからの応答がなければ、同じセグメントにあるパソコンやプリンタにpingしてみると、どこまで通信できているか分かることがあります。

pingに応答がなければ、そこまでの経路を調べましょう！



注意）
むやみやたらにpingするのは攻撃とみなされる場合がありますし外部からのpingは許可していない場合もあるので、自分が普段使っているルーターやプリンタへの通信を調べましょう。
ルーターや、プリンタなどのIPアドレスは正常時に確認しておきましょう！

通信確認（DNSサーバ）

nslookupコマンドでDNSが機能しているかを確認してみる（名前が引けているか）

```
C:¥Users>nslookup www.ile.osaka-u.ac.jp
サーバー: DNSサーバ
Address:  192.168.0.252

権限のない回答:
名前:    www.ile.osaka-u.ac.jp
Address:  133.1.68.130
```

※Linuxはdigコマンド

DNSサーバの名前とアドレスが表示されますか？

対象物の名前とIPアドレスが表示されますか？

このようにサーバのIPアドレスが表示されれば
DNSサーバまでの通信とDNSサーバの機能に
問題がないことが確認できます

☑ OK

その他試していただきたいこと

・パソコンの再起動

・ハブや無線APの再起動（他の人にも影響ありますので注意！）

・同じ部屋の他のパソコンはいかがですか？

・隣の部屋はどうでしょう？

→ 自分のパソコンだけでなく
他の人のパソコンなども通信できないようなら
他の人と協力して調べましょう

→ ここまで調べて、ネットワーク管理者に相談する場合は
状況をメモして連絡しましょう！

具体的な状況が分かれば管理者の調査もスムーズに始められます

それでも通信できない場合

・他のブラウザ、パソコンなどで試してみる

・しばらく待って試してみる（場合によっては日を改める）

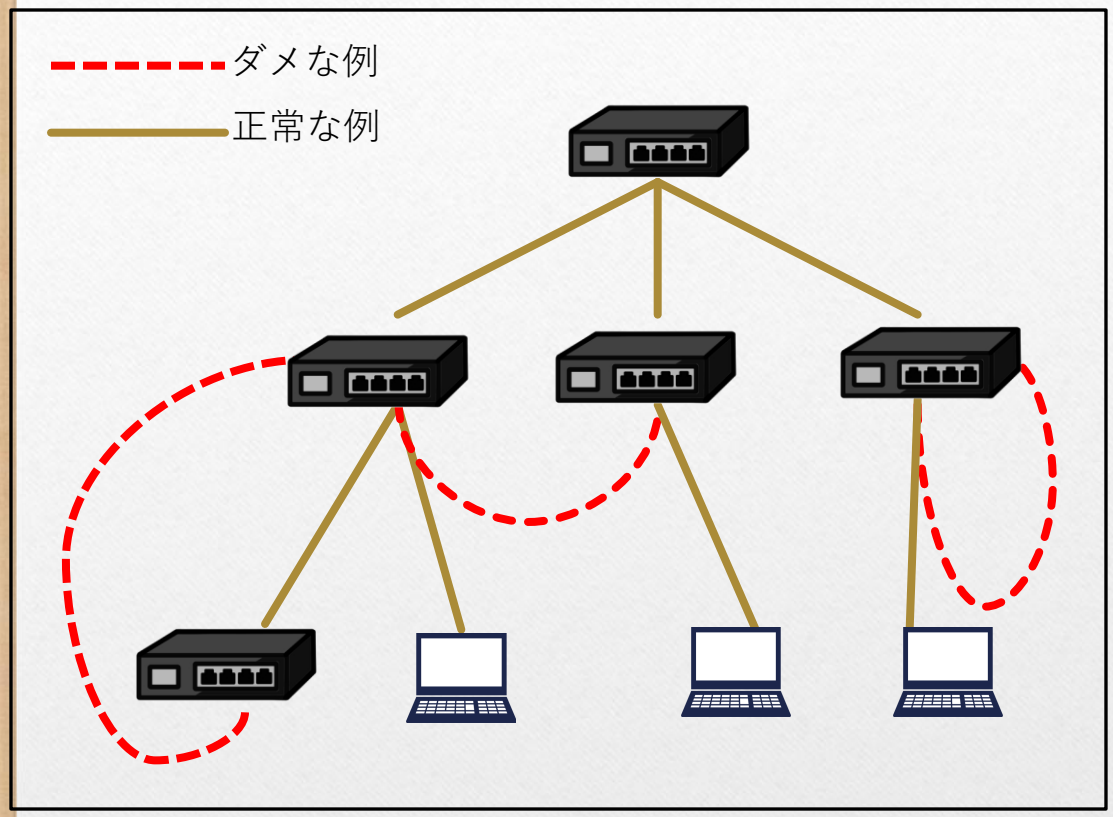
などなど回りの方とも相談してみてください。

特定のサーバに通信できないなら、そのサーバの問題かもしれません。
連絡できるならサーバ管理者に連絡してみてください。

これだけ調べることができればあなたはネットワークの初心者卒業です。

セキュリティにはくれぐれも気をつけて、利用しましょう！

他にも気を付けてほしいこと（ループ）



よくあるトラブルのうち、
原因を調査してみると、
「ループ」を引き起こしている
ケースがよく見られます。

外れているLANケーブルを、
わからないまま適当に
接続すると、ループを
引き起こす可能性があります。

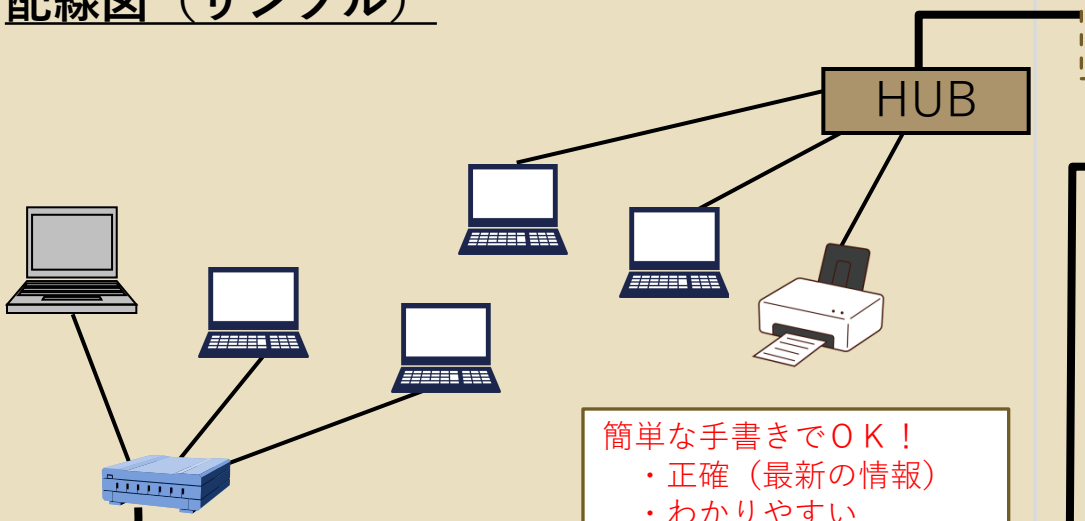
ループを引き起こすと、
ネットワーク全体がダウンする
場合もあります。

不明なケーブルについては、絶対につながないようにしてください。
ケーブルの両端のジャック部分に、ハブ側にはハブ側であることを
わかるようなマークをつけるなどの工夫をすると、便利ですよ！

ネットワーク配線図と環境整備

トラブル時には、パソコンからネットワークケーブル、ハブ、
スイッチ・・・など、物理的に問題が起きていないか、ひとつずつ
動作を確認していきます。
スムーズに原因究明を行えるよう、**部屋内のネットワーク配線図**を
作成するとよいでしょう。
配線図を作成したら、常に最新の状態を保ちましょう。
ハブやケーブルが正しく装着されているか、ハブのランプがついているかなどを
すぐに確認できるよう、周りの環境も整備しましょう。
（本棚などが邪魔をして確認できないというようなことが無いように･･･）

配線図（サンプル）



マシン室エッジスイッチ
上流スイッチ 5番ポートより

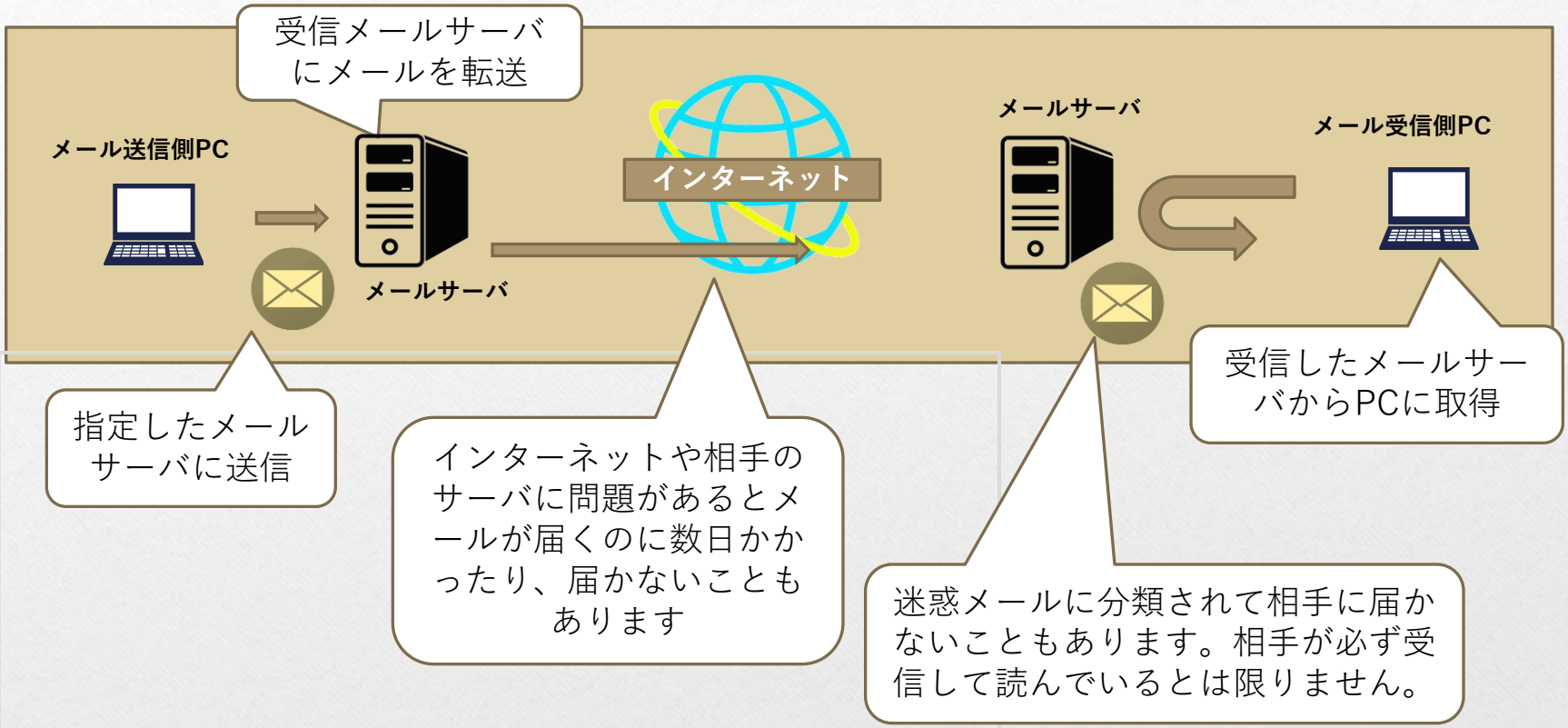
マシン室集約スイッチ
上流スイッチ3番ポートより

簡単な手書きでＯＫ！
・正確（最新の情報）
・わかりやすい
ものであることが重要です

部屋名：△△室
部屋ネット担当者：□□
作成日：〇年〇月〇日

メールの仕組み（メールソフト）

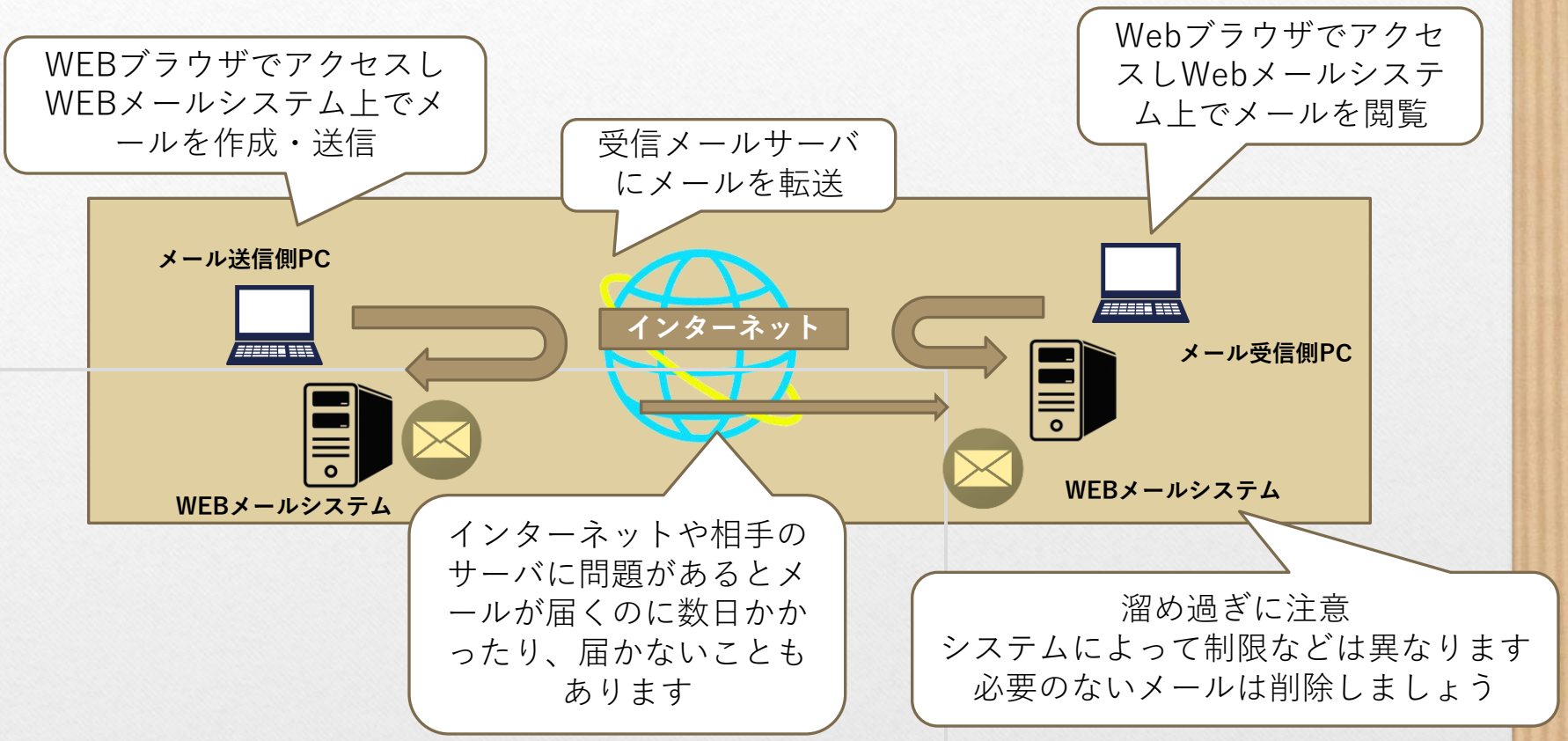
メールソフトでメールを送信すると以下のような経路で送られます



メールサーバやパソコンにメールをためすぎないように注意しましょう

メールの仕組み（WEBメール）

WEBメールを送信すると以下のような経路で送られます



ブラウザがあれば様々な場所からメールのやりとりができるというメリットはあるがネットカフェなどでの利用は危険

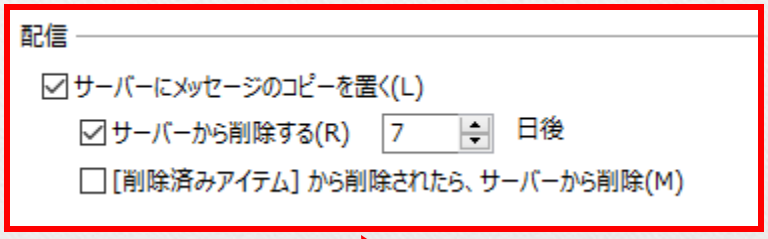
メールの常識

サーバにメールを溜めすぎない

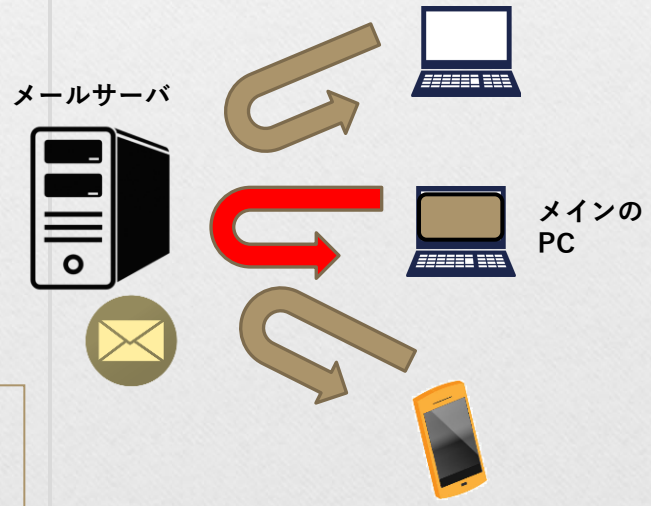
サーバもパソコンも無限ではありません。
どちらもメールをため過ぎるとよくないことがおこります

サーバにメールを残さない、あるいは読んでから一定期間経過したら消す設定にしましょう。パソコンのバックアップも忘れずに！

インターネット電子メール設定の例

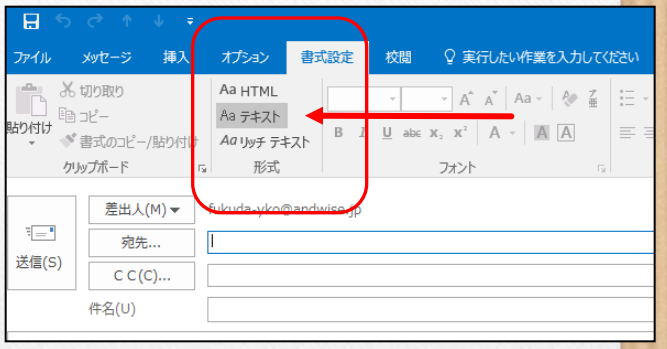


複数のパソコンやスマホでメールを
送受信している場合は、メインのPCの
設定で消すようにしましょう



メールの常識

テキスト形式で送信しましょう



・テキスト形式のメール
テキストだけで作成されていて、裏に情報が隠れたり余計な情報がついたりしない
受信者の環境に依存せず読むことができる

・HTML形式のメール
文字の色や大きさ、装飾、画像なども表示できる。
Javaスクリプトを埋め込むなども可能。
対応していない場合、受信者は判読が難解

通常のやりとりに必要なメールは、HTML形式である必要はありません。
セキュリティ上の理由からHTML形式を読めないようにしているユーザもいます。

設定で**「テキスト形式」で送信するよう**にしましょう。
また、たとえ相手がHTML形式で送信していたとしても、
あなたは「テキスト形式」で返信するようにしましょう。

※業務でやりとりするメールはテキスト形式が常識です！

テキスト形式とHTML形式

■　テキスト形式の場合

これはテキスト形式のメールの例題です

あああああああ
いいいいいいい
ううううううううう
えええええええ
おおおおおおお

HTML形式で
送信すると、
余分な情報まで
付加されます

■　HTML形式の場合

```
------=_NextPart_000_0002_01C47B9C.0376ABC0
Content-Type: text/plain;
        charset="iso-2022-jp"
Content-Transfer-Encoding: 7bit

これはHTML形式のメールの例題です

あああああああ
いいいいいいい
ううううううううう
えええええええ
おおおおおおお

------=_NextPart_000_0002_01C47B9C.0376ABC0
Content-Type: text/html;
        charset="iso-2022-jp"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META HTTP-EQUIV=3D"Content-Type" CONTENT=3D"text/html; =
charset=3Diso-2022-jp">
<TITLE>=1B$B%a%C%;!<%8=1B(J</TITLE>

<META content=3D"MSHTML 6.00.2800.1458" name=3DGENERATOR></HEAD>
<BODY>
<DIV><FONT =
size=3D2>=1B$B$3$l$O=1B(JHTML=1B$B7A<0$N%a!<%k$NNcBj$G$9=1B(J</FO
NT></DIV=>
<DIV><FONT size=3D2></FONT> </DIV>
                        ;
```

メールの常識

プレビューしない設定にする

プレビューとは受信したメッセージを開くことなく自動的に表示させる機能で、
便利ではあるのですが、コンピュータウイルスの中にはこのプレビュー機能を
悪用したものも多く、プレビューするとそのままウイルス感染する可能性が
高いので、プレビュー機能は使わない方が良いでしょう。

メールの件名は簡潔に

メールの件名（タイトル・サブジェクト）は、その内容が一目でわかる
簡潔なものにしましょう。
ただし、スパムメールと間違えられるような件名は避けましょう。
＜例＞ **無題**（件名なし）**, Hello , Hi , Congraturation , Happy birthday** など…

➡ 件名が悪いとスパムメールとして扱われて読まれなくても仕方ありません

メールの常識

個人情報は記載しない

ネットワーク上にデータとして流れていることの危険性を認識しましょう
電子メールのプライバシーは葉書と同じです

宛先を間違える可能性があるだけでなく
送ったメイルが、第3者に転送される可能性もあります

秘密情報、クレジットカード番号、パスワードなどは、電子メールでは
送信しないのが常識です。
そのような情報を要求するメールは無視しましょう

ついでですが
非公開情報をメイルで送るのは要注意
　入札関係、特許関係など
　他人の悪口も

一度送られた情報の削除は事実上不可能です

送信ボタンを押す前に

あて先は間違ってませんか？（特に似た名前は要注意）

メールを送ってしまったら、取り消しすることはできません。
送受信を行う前に、今一度確認する習慣をつけましょう。

ラブレターをうっかり組織全員に配布してしまったり・・・
取引相手に送るメールをうっかり競合他社に送ってしまったり・・・

宛先の種類には「To:（宛先）」　「CC:（カーボンコピー）」「BCC:（ブラインド・カーボンコピー）」があります。それぞれ、以下のように使い分けましょう。

To:　メールの内容を伝えたい人のメールアドレスを書く。複数でもよい。

CC:　確認のため、あるいは参考までにメールの内容を伝えたい人のアドレスを書く。
逆にCCのメールを受け取った場合、必ずしも返事が求められている訳ではない。
また、CCに書かれたアドレスは、メールを受け取った人全員に表示されるため、
必要のない人にまで第三者のメールアドレスを公開してしまわないように注意
すること。空欄でもよい。

BCC:　その人にメールが届けられることを他の人（To、CC:他のBCC:に指定している人）
には知らせたくないときに用いる。
BCC: に入力したアドレスは、受け取った側には表示されない。空欄でもよい。

送信ボタンを押す前に

添付ファイルどうしてますか ➡ 脱PPAPの動き

PPAPはこれまで多くの企業が採用してきたセキュリティ方法の1つです。
しかし、**政府が2020年にPPAP廃止の方針を発表して以来、企業の間では脱PPAPの動きが広がっています。**

PPAPとは
- P：Password付きのZIP暗号化ファイルを送ります
- P：Passwordを送ります
- A：Aん号化（暗号化）
- P：Protocol（プロトコル）

大阪大学では、ファイルはメール添付ではなく、以下方法を推奨しています。
- OneDriveやSharePoint（ICHO）※学内向け
- NII FileSender　※学外向け

以下メリットがあります
- メール送信後でもファイルの挿替や削除が可能
- ファイルの閲覧者や閲覧回数の確認が可能
- 個別にアクセス権を設定することが可能

メールの常識

困ったことにならないために

■　定期的に、メールソフトのバックアップをとる習慣を！

メールソフトの不具合やパソコンの故障などで、メールが消えてしまうこともあります。
普段からバックアップは必ずとるようにしましょう。

■　不審なメールは開かない、変だと思ったら開かず削除

今や不審と思われるメールを送る方が失礼です。
どうしても不安なら、正規のホームページを確認するなどして
相手方に電話か別のメールなどで問い合わせてみましょう。
くれぐれもメール中のURLのクリックや返信はしないで！

銀行や宅配便をかたって誘導するメールもあります。
自分からくることもあります。知り合いでも不審なメールは開かないようにしましょう

■　怪しい添付ファイルは開かない

これも常識です。自分が添付ファイルを送信するときは、
「***のファイルを添付しています」の一言を添えるのが親切です。
拡張子、アイコンの偽装にも注意しましょう。

■　くどいようですが不審なメール、迷惑メール、デマ、チェーンメールなどは返信せずに削除すること。転送もやめましょう！

便利だけど危険もいっぱい

・いろいろな情報があふれています！
・困ったら調べることができます
・すべてが正しい情報とは限りません

SNSや
X（旧twitter）なども注意

・危険もいっぱいあるということを忘れずに！
　見るだけでも危険なページもあります
　怪しいサイトには近づかないようにしたほうがいいでしょう
　ファイルのダウンロードには特に注意しましょう

■業務に関する内容を不用意に発信しない
■業務に関係のないWebページは閲覧しない
■ファイルのダウンロードには特に注意すること
　✓ 拡張子（exe、com、batなど）
　✓ 拡張子を偽造する例もあります
■フィッシング詐欺に注意すること

便利だけど危険もいっぱい

フィッシング詐欺とは？

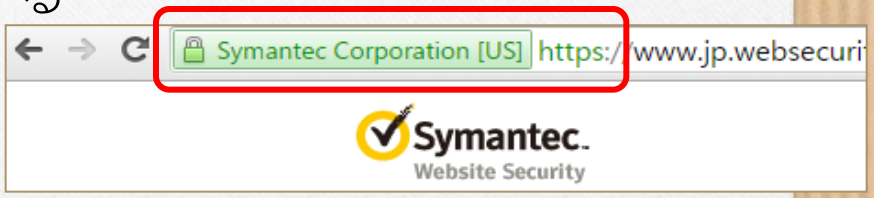
銀行等企業からのメールを装い、メールの受信者に実在する企業の偽ホームページにアクセスさせて、そのページにおいてクレジットカード番号やID、スワード等を入力させるなどして不正に個人情報を入手しようとする行為

被害にあったときは、正規の連絡方法により
サービス会社に連絡を取り、早急にパスワードを変更、
もしくはサービス利用の権限を停止してもらいましょう

セキュアなサイト（https）ですか？

■ Web画面上で個人情報などを入力する際には･･･必ず確認しましょう

- URLが「https://」で始まっているか？
- 錠前マークがついているか？
- 信頼できる証明書を用いているか？



ブラウザによって見え方は異なります

発行先：アクセスしたURLとドメイン名が一致していますか？
発行者：信頼できる認証局が記載されていますか？
有効期限：期限切れになっていませんか？

- ＜サイト例＞
- クレジットカード情報の入力画面
- ネットバンキングのログイン画面
- 人材採用の情報入力画面
- ログイン用のID/パスワード入力画面
- イベントやセミナーの登録フォーム
- ご意見やご相談などお問い合わせフォーム
- ：

パスワード管理の重要性

Ｗｅｂページ閲覧時、会員登録などを行うとパスワードを設定しなければいけない場面に遭遇します。

理想のパスワードとは･･･

- 他人に予想されにくく、自分は覚えやすいもの
- 簡易なパスワードは使用しない
- 英字（大文字、小文字）、数字、記号を混在させる
- 最低**「英大小文字」＋「数字」＋「記号」で10桁**が推奨

パスワード保護の対策

- パスワードは他人に教えない　←　システム管理者でも！
- 紙や付箋に書き留めない
- 定期的に変更する　←　クラック防止のため
- いろんな場面で同じパスワードを設定しない　←　一つクラックされら・・・？

盗まれた時の深刻度に応じたパスワード（長さ、難易度）を設定するのも一つの重要な手段です。

Ｗｅｂサイトからのパスワード漏えいが、あなたの個人情報の漏えいにつながる可能性も？

WEB閲覧の常識

SNS型投資詐欺

投資に「絶対」「確実」はない！
著名人になりすました偽広告急増！

「必ずもうかる」など
甘い言葉にご用心！

1. SNSの広告をタップ
2. 犯人側との接触　グループに招待
3. 儲かっているなどサクラが投稿
4. 投資家やそのアシスタントを名乗るものから振込指示
5. 偽の利益を掲載し、その一部（少額）を被害者口座へ振込
6. 高額の偽利益を表示。全額引出のための手数料などを要求
7. 突然連絡が途絶える

参考WEB：警察庁特殊詐欺対策ページ
https://www.npa.go.jp/bureau/safetylife/sos47/

LINEを悪用した詐欺に注意

近年、LINEを悪用した様々な詐欺事件が増加しています。

参考WEB：LINEヤフー社の注意喚起ページ
https://fraud-alert.landpress.line.me/fraud_alert/

情報発信の常識

■　著作権を意識しましょう

著作権侵害は罰金や民事上の損害賠償の可能性も！

■　必要以上の情報や写真を公開しない

インターネットで公開した情報は、いろいろな人が閲覧できます
ネット上で、氏名、年齢、住所、電話番号、自分の写真などを
公開することは危険があることを認識しておきましょう

■　発信内容は慎重に

一度公開した内容は取り消し不可能です
いろいろな問題になるケースも発生しています
業務に関する内容なども不用意に発信してはいけません

総務省　国民のためのサイバーセキュリティサイト

安心・安全のインターネットライフを

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

最新の情報をチェックしましょう

サイバーセキュリティの三原則

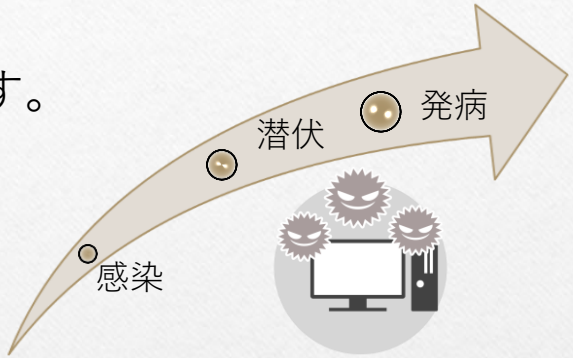
- ソフトウェアを最新に保とう
- 強固なパスワードの設定と多要素認証を活用しよう
- 不用意に開かない・インストールしないようにしよう

コンピュータウィルス

ウイルスの侵入経路は様々なパターンがあります。

- 電子メール
- USBメモリや外付けHDDなどの媒体
- 悪意あるWebページ
- Webサイトよりダウンロードしたファイル
- ファイル交換ソフト（P2P）

など・・・



ウイルス感染時の症状例

最近のウイルスは派手な活動をしないことが多いので、注意が必要です。
下記のような症状がない（気付かない）うちに、データを転送されたりするケースも！！

- コンピュータが自動的にシャットダウンしてしまう
- 勝手にインターネットへ接続しようとする
- ハードディスクのアクセスランプの点滅が継続的に行われる
- ウイルスに感染しているメールが他のコンピュータに転送される
- Windows Updateなどの更新プログラムの提供サイトへアクセスできなくなる
- コンピュータの動作速度が遅くなる

次々新種のウイルスが発生するなど、種類も数多くあり発病した際の症状も様々です。
常に**最新情報に注意**し、ウイルスに対する警戒心を持ちましょう。

ウイルス感染時の対処法

もしもウィルスに感染してしまったら・・・

・ネットワークケーブルをパソコンから外しましょう

⇨ さらなる感染による、被害拡大を防ぐため

・グループリーダーやシステム管理者へ連絡し指示に従いましょう

⇨ もしかしたら、周りにも同じような症状の人がいるかもしれません
被害を掌握すべき責任者に必ず報告しましょう

・自分の判断で回復しようと試みない！！

⇨ 誤った対応をすれば、被害の拡大を促す可能性があります
法的措置が必要な場合に、証拠収集が必要かもしれません

個人（プライベート）のコンピュータなど、頼れるべき管理者がいない時には、OSの再インストールをするのが、安心です。
日ごろから重要なデータはバックアップを取っておきましょう。

ウイルス対策ソフトの活用のすすめ

ウイルス対策ソフトは、コンピュータがウイルスに感染していないかをチェックして、
感染している場合には、駆除してくれます。が、完全ではありません。
新種のウイルス（ゼロデイアタック）や、ZIPファイルなど中身を解析できない
ファイルは解凍後、ウイルススキャンする必要があります。

ウイルスパターンファイルの更新

- ◆ウイルスは日々、新しい種類が作成されているため、ウイルスパターンファイルは、常に最新の状態を保つようにしましょう。
- ◆ウイルスパターンファイルの更新は、インターネットを利用して更新するのが一般的であり、インターネットに接続をしないパソコンは更新が停滞しやすいので注意しましょう。

ウイルススキャンの実行

- ◆メール添付や、外部媒体を介して情報をやり取りする場合は、「渡すとき」「受け取るとき」を合わせて、ウイルスチェックを忘れないようにしましょう。
- ◆ドライブ内全体へのウイルススキャンをできるだけ毎日実行しましょう。
- ◆パスワード付きZIPファイルや暗号化機能付きUSBメモリなど、中身を解析できないファイルは、解凍後、ウイルススキャンをする必要があるので注意しましょう。

ソフトがなければ、
OS標準装備のセキュリティ対策を！
（例）Windows Defender など

自分のパソコンは自分で守りましょう

OS、ウイルス対策をはじめとするソフトウェアは最新のものですか？

OSやソフトウェアにセキュリティ上の欠陥が見つかった場合、
それに対する修正が出る場合がありますので、定期的にチェックし、
常に最新の修正が適用されている状態にしましょう。

■　**Windows Update（Windowsの場合）**

マイクロソフト社から定期的に出される修正を適応させ、
常に最新のものにしてください。

■　**導入ソフトウェア、プラグインの更新**

PC内の導入ソフトウェアやプラグインの更新（Adobe ReaderやFlash Playerなど）も、チェックし、常に最新のものにしましょう。

■　**ウイルス対策ソフトの更新**

ウイルス対策ソフトの中には、１年間〇〇円といった料金体系のものもあります。
更新手続きを忘れないようにしましょう。

定期的にバックアップしていますか？

万一のマシントラブル時に備え、定期的にバックアップを取りましょう。

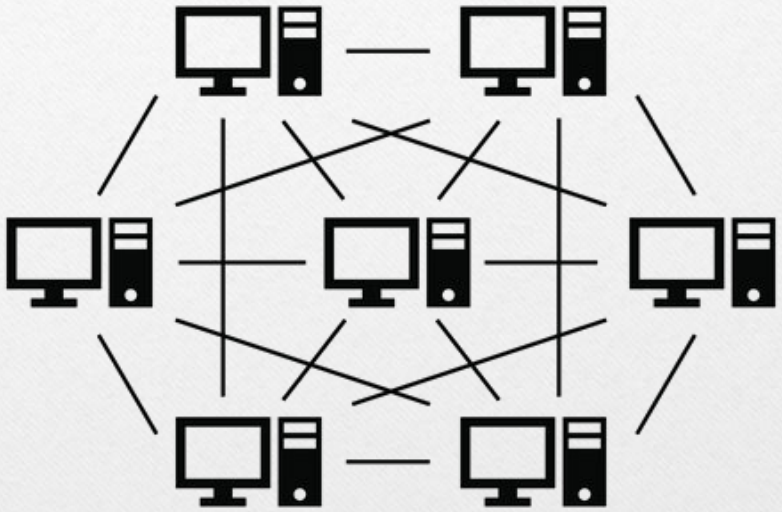
ある日、突然パソコンが、故障してしまうこともあります。うっかり削除してしまうこともあるかもしれません。忘れがちなのがメールのバックアップです。バックアップ項目を一覧にして管理するのもいいかもしれません。

USB-HDDなどの外部メディアなど、２箇所以上にバックアップすれば、心配ないでしょう。汎用性の高い方法で取ることをお勧めします。

ウイルスに感染してしまった場合、大阪大学ではOSの再インストールを命じられることもあります。
バックアップを日ごろからとっておけば、
最小限の被害ですむかもしれません。

ファイル交換ソフト（P2P　Peer to Peer）の危険性

ファイル交換ソフトは、著作権侵害やコンピュータウイルスの温床にもなっています。
著作権侵害行為には、3年以下の懲役、又は300万円以下の罰金という刑事処罰や
民事上の損害賠償という制裁が科されます。
組織内違法コピーや、海賊版の使用は絶対にしてはいけません。



P2P(peer-to-peer)とは、コンピュータ同士が直接接続してデータやサービスをやり取りする分散型の通信形態のこと

＜代表事例：＞
コンピュータウイルス「W32/Antiny」

症状：ファイル交換ソフトWinnyを利用し
不正に情報を流出させる

不特定多数の人が接続している
ネットワークに流出した情報を、
取り返すことはまず不可能です。

付録： IP v 4　IPアドレス枯渇問題とは

現在広く普及している「IP v 4」(Internet Protocol version 4)では、
IPアドレスに8ビットずつ4つに区切られた32ビットの数値が使われ、
「192.168.0.1」といったように、0から255までの10進法の数字を
4つ並べて表現します。

現在のIPv4では、32ビットの数値で識別できる上限である約42億台(2の32乗)までしか
一つのネットワークに接続することができず(実際の運用ではこれより少なくなる)、
インターネットで利用するIPアドレスが足りなくなることが懸念されています。
このため、企業など多くの機器を利用するところでは、組織内ネットワークでは
自由にいくらでも使えるプライベートアドレスを使い、インターネットとの境界に
グローバルアドレスとのアドレス変換（NAT変換）を行う機器を設置するといった
運用方法が普及しています。

次世代のIPv6では128ビットのIPアドレスが使われ、単純計算で2の128乗、
約340澗(かん)、約3.40×10^{38}個のIPアドレスが利用可能になるため、
IPv6に移行すれば当分はIPアドレスが不足する心配はなくなると言われています。

ただし、IP v 6とIP v 4は互換性が無いため、移行は簡単なものではありません。
相応のコストがかかると言われています。

2011/9/30　記

メールとネットワークの基礎

初版	2006.4.6	福田　優子
第2版	2007.4.3	谷口　麻梨香
第3版	2008.5.8	谷口　麻梨香
第4版	2010.3.30	宇佐美　賢子
第5版	2011.10.17	林　麗美
第6版	2011.11.30	林　麗美
第7版	2011.12.22	宇佐美　賢子
第8版	2012.2.21	林　麗美
第9版	2025.6.20	橋本　賢子

大阪大学レーザー科学研究所
高性能計算機室
http://www.ile.osaka-u.ac.jp/research/cmp/