メールとネットワークの基礎

――――初心者対象――――

2012/2/21　第8版

大阪大学レーザーエネルギー学研究センター
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。高校では情報教育が必修化されましたが、まだまだ基礎的なことがよく分からないという方が多数おられ、このようなテキストが必要とされているということを実感してきました。もっと詳細な説明書を作らないといけないのかなと感じていましたが、情報教育シンポジウムに参加して、高校の教科書がよいということを知りました。以下にお勧めする参考文献は、副読本として作成されたものですが、最新の情報が専門家によってまとめられています。

おすすめ参考文献 「キーワードで理解する最新情報リテラシー」
監修：久野靖、辰巳丈夫、佐藤義弘、日経BP社

メールもネットワークも今や、当然知っておかなければならないツールですが、基礎的な知識なしに利用することは、非常に危険なことです。

このテキストを手掛かりに、さらに詳しく勉強していただけるようになっていただけたらと願い、新人目線で大幅に改定して、WEBで公開することにいたしました。2012年2月にはKEKで講習会をする機会をいただいたので、セキュリティマインドも追加いたしました。

自由に再配布していただいてかまいませんが、どのように参考になったかなどの感想やコメント、よい文献などをご連絡いただけたら幸いです。

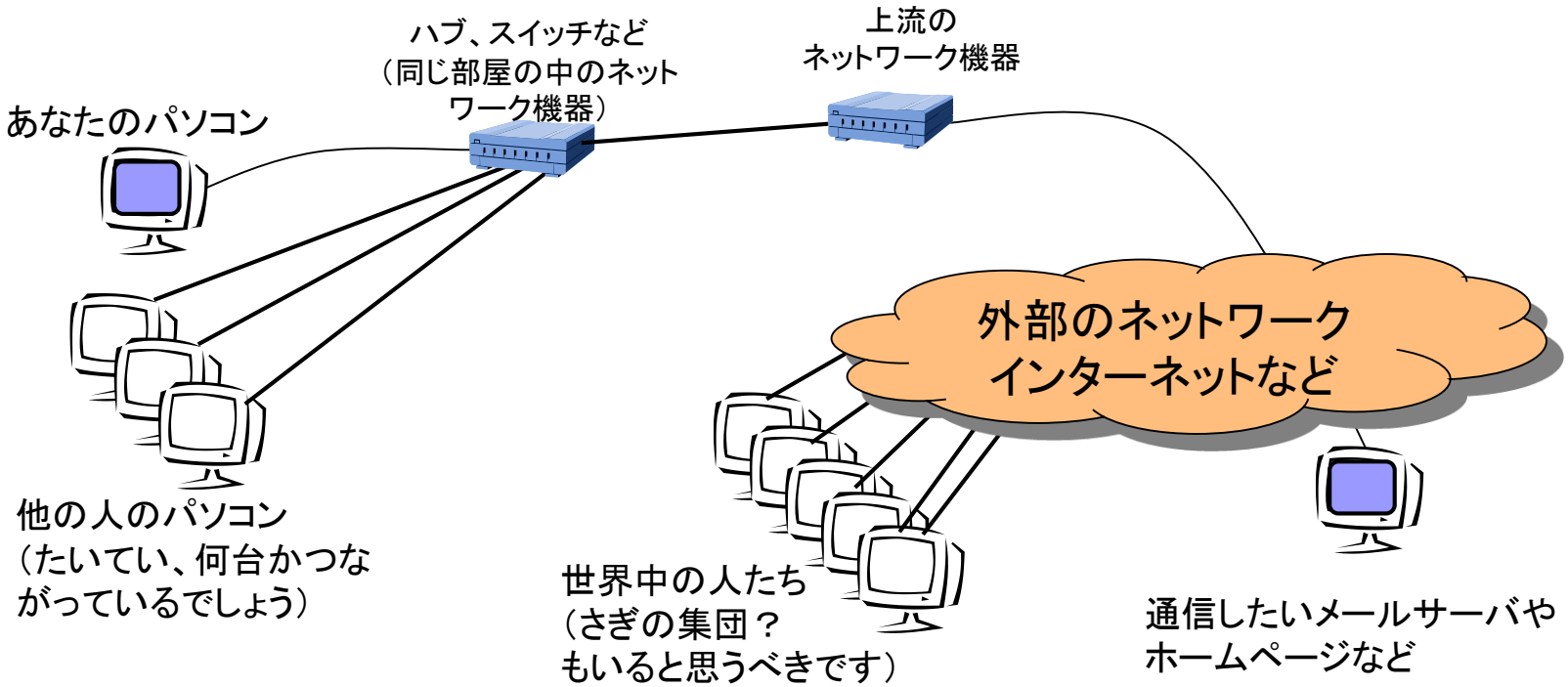
2012年2月21日　福田優子

公開にあたってコメントをいただいたSWS（http://sws.soken.ac.jp/）の皆様に感謝いたします。

1．ネットワークとは

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。
インターネットとは、ホームページだと思われている方もまだまだ世の中には多いようですが、ホームページはインターネットを介して情報発信するツールのひとつであり、インターネットを利用して可能なことは、メール、SNS、ツイッターなども含めていろいろあります。

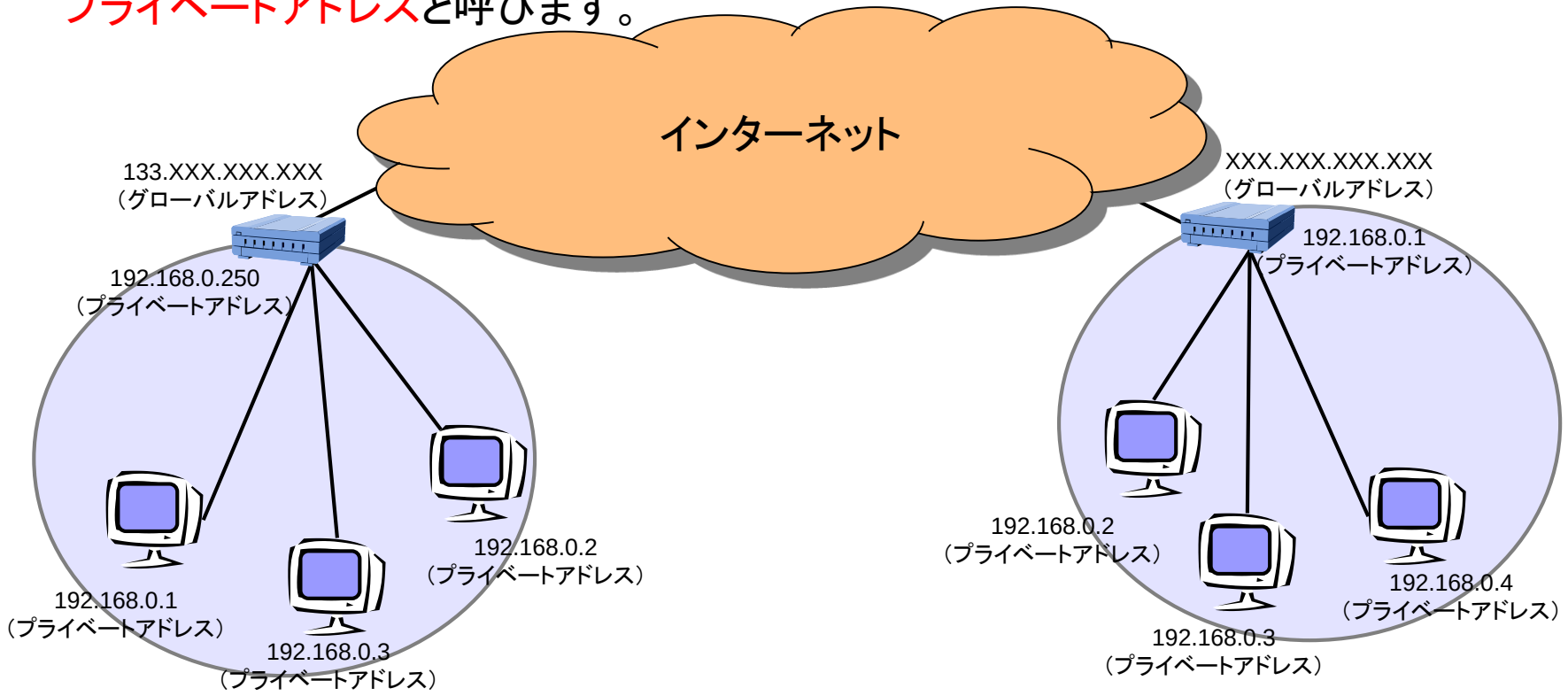
＜ネットワークのイメージ＞



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

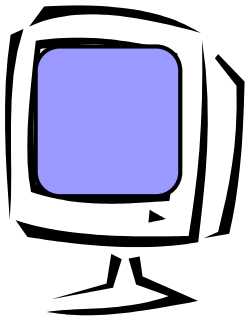
インターネット上で利用できる世界中でただ一つのIPアドレスをグローバルアドレス、
組織内LANや家庭内LANなどその組織内でのみ利用できるIPアドレスを、
プライベートアドレスと呼びます。



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

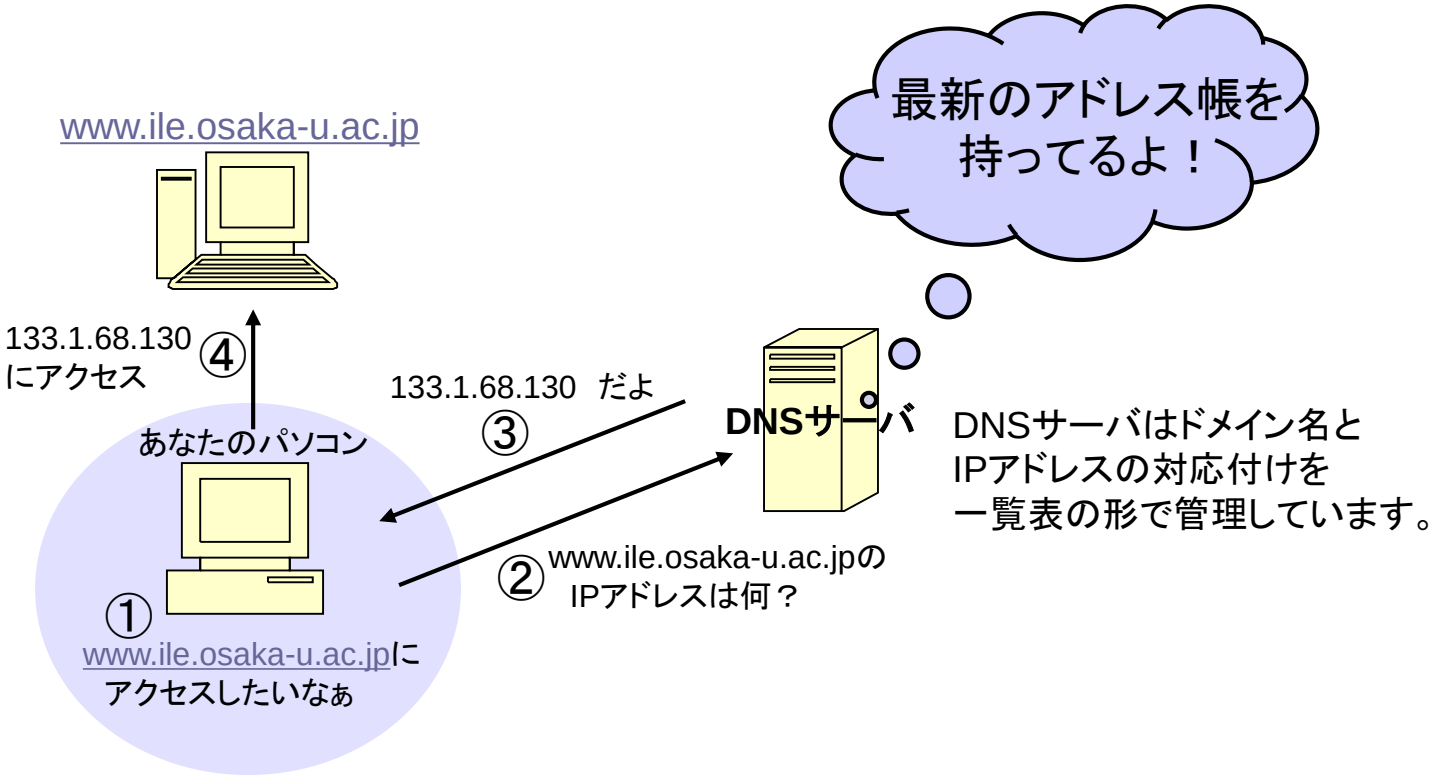
レーザー研．大阪大学．日本

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。

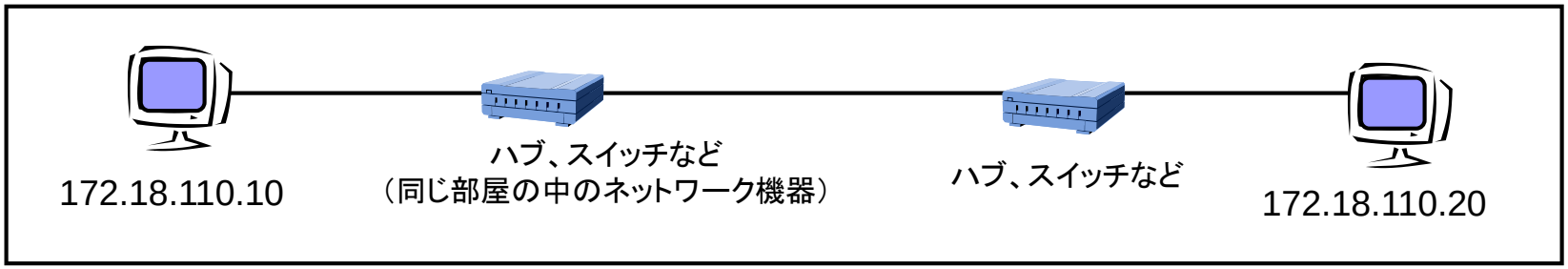


DNSサーバの設定が間違っていると、名前解決に失敗し、メールの送受信ができない、ホームページが見えないなどのネットワークのトラブルの症状が現れます。

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



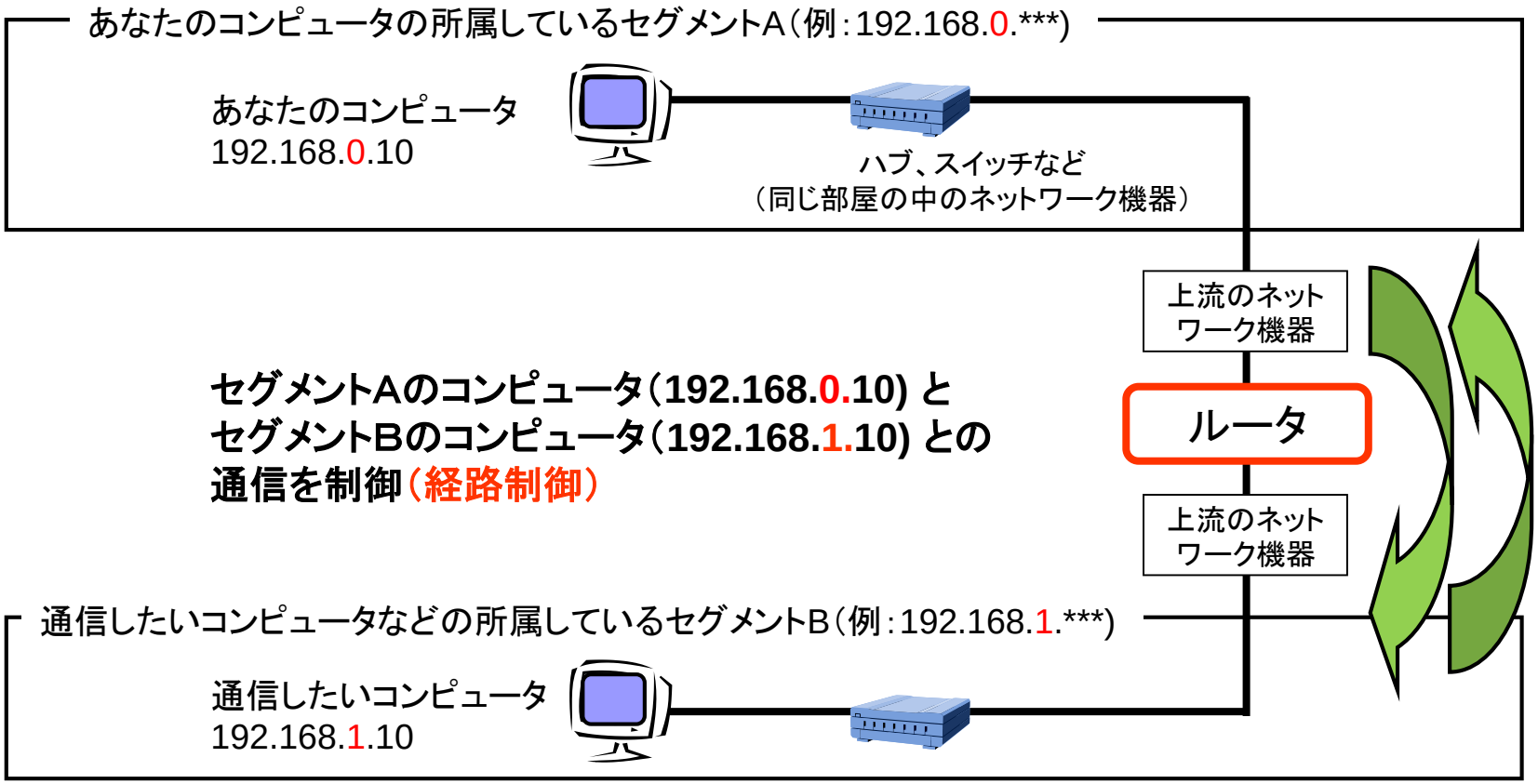
セグメントとは・・・

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。

ルータ（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

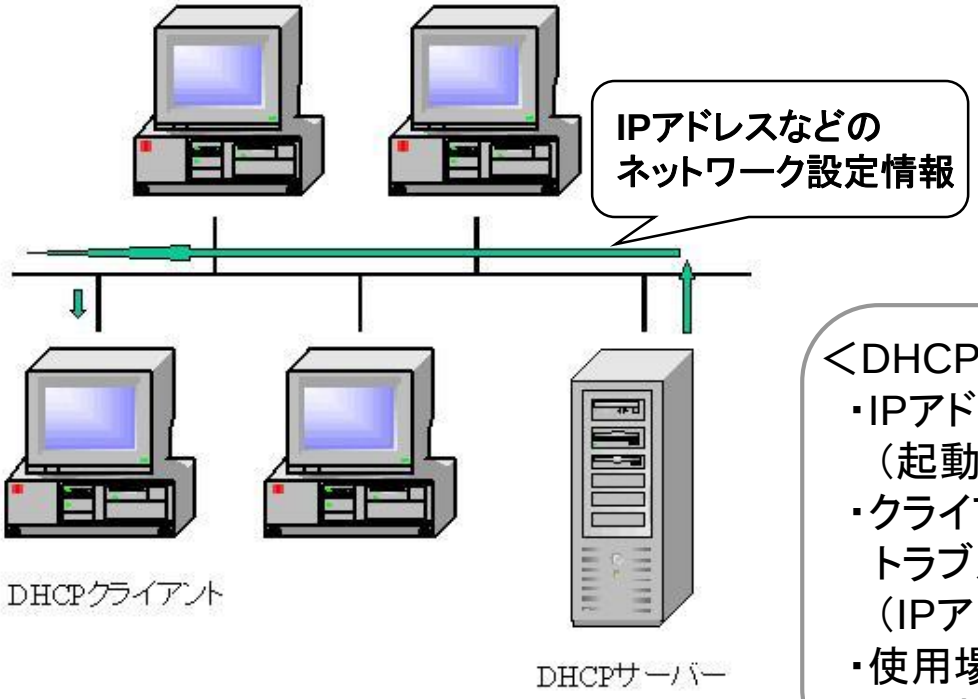
＜例＞　サブネットマスクが　255.255.255.0



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）

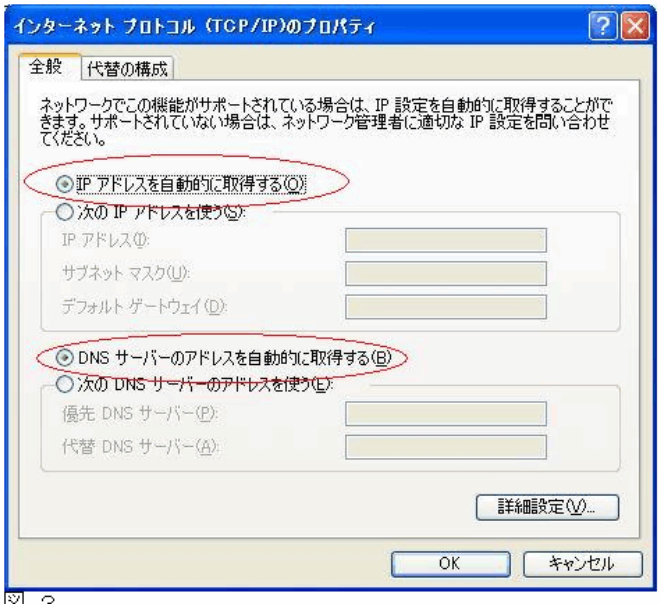


＜DHCPの利点＞
- IPアドレスが有効活用できる
  （起動していないマシンには払いだされない）
- クライアントのネットワーク設定ミスによる
  トラブルがなくなる。
  （IPアドレス競合など）
- 使用場所を変えても、ネットワーク設定変更が不要
  のことが多い。

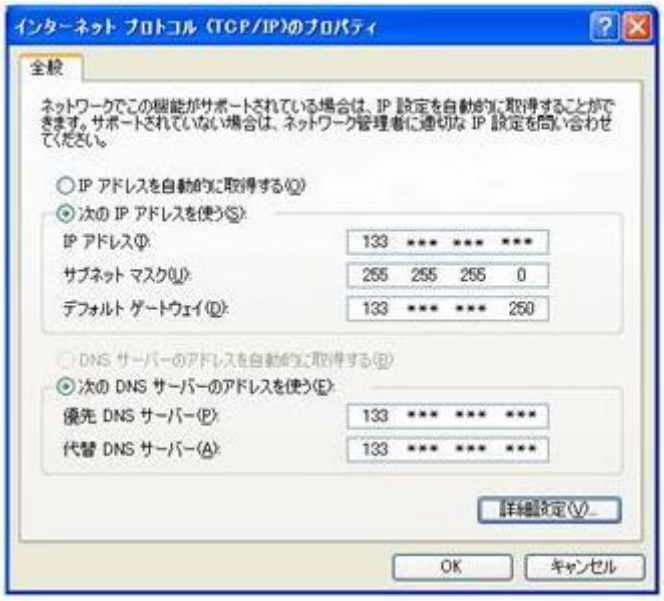
2.ネットワーク通信のための設定

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）
■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

DHCPでの設定例



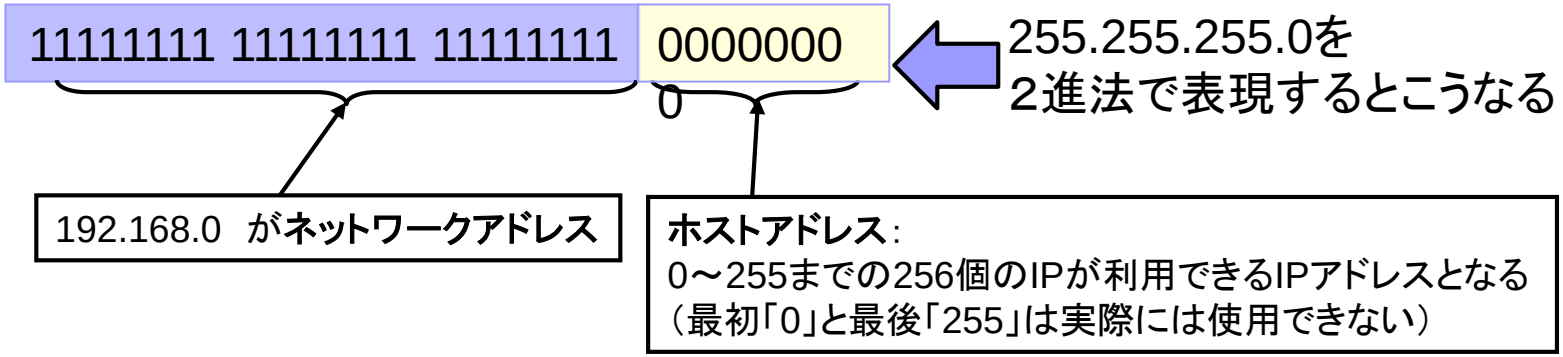
固定アドレスの設定例



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



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

3.うまくつながらない時は･･･？1（ネットワークの設定を確認してみる）

```
C:¥Users>ipconfig /all
Windows IP 構成
   ホスト名 . . . . . . . . . . . . : XXXX
   プライマリ DNS サフィックス . . . . . . . :
   ノード タイプ . . . . . . . . . . . . : ハイブリッド
   IP ルーティング有効 . . . . . . . . : いいえ
   WINS プロキシ有効 . . . . . . . . : いいえ
イーサネット アダプター ローカル エリア接続:
   メディアの状態. . . . . . . . . . . : メディアは接続されていません
   接続固有の DNS サフィックス . . . :
   説明. . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   物理アドレス. . . . . . . . . . . : 00- - - - -1C
   DHCP 有効 . . . . . . . . . . . . : はい
   自動構成有効. . . . . . . . . . . : はい
Wireless LAN adapter ワイヤレス ネットワーク接続:
   接続固有の DNS サフィックス . . . :
   説明. . . . . . . . . . . . . . . : Atheros AR9285 Wireless Network Adapter
   物理アドレス. . . . . . . . . . . : 00- - - - -E1
   DHCP 有効 . . . . . . . . . . . . : はい
   自動構成有効. . . . . . . . . . . : はい
   リンクローカル IPv6 アドレス. . . . : fe80::   :   :   :d7f1%11(優先)
   IPv4 アドレス . . . . . . . . . . : 192.168.0.1(優先)
   サブネット マスク . . . . . . . . : 255.255.255.0
   リース取得. . . . . . . . . . . . : 2011年X月XX日 9:35:55
   リースの有効期限. . . . . . . . . : 2011年X月XX日 10:05:55
   デフォルト ゲートウェイ . . . . . : 192.168.0.254
   DHCP サーバー . . . . . . . . . . : 192.168.0.251
   DHCPv6 IAID . . . . . . . . . . . :
   DHCPv6 クライアント DUID. . . . . . . . :
   DNS サーバー. . . . . . . . . . . : 192.168.0.252
   NetBIOS over TCP/IP . . . . . . . : 有効
```

Windowsの場合
コマンドプロンプト(cmd.exe)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」

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サーバーなどの設定が正しくされていますか？

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。

うまくつながらない時は･･･？2（ネットワークの設定に問題がなかったら）

pingコマンドでデフォルトゲートウェイ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？（このように表示されたらネットワークはつながっている）

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
```

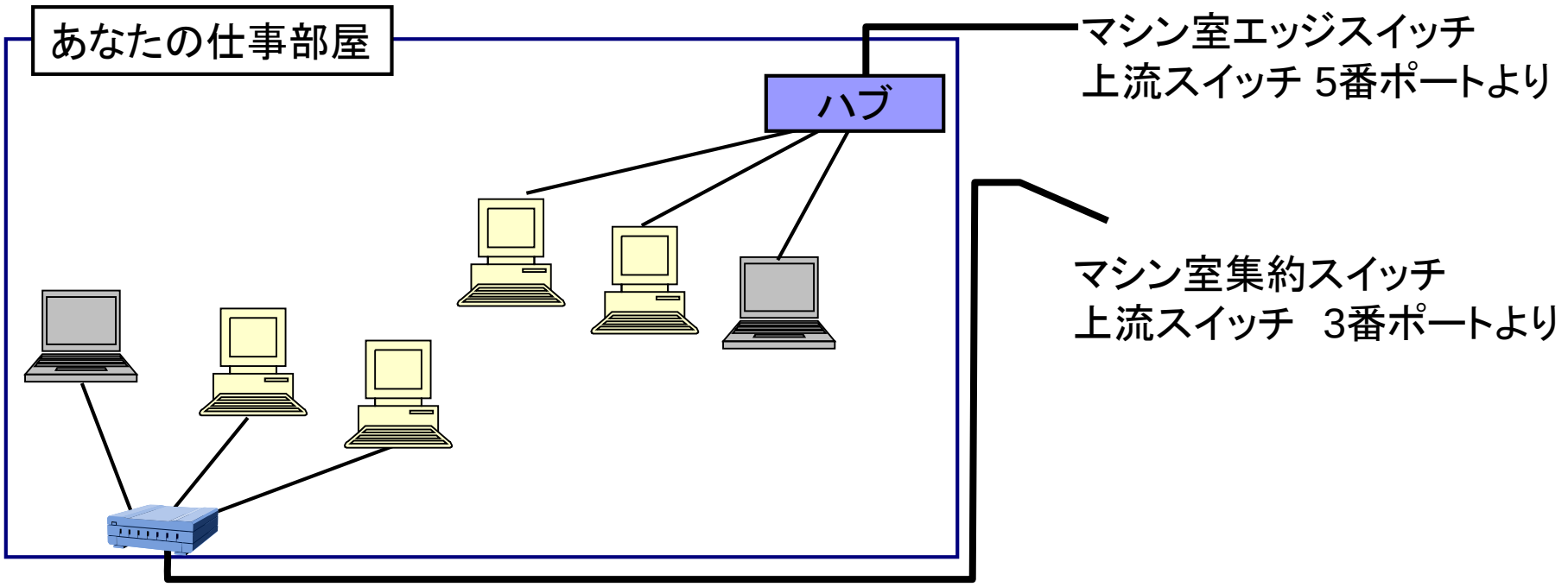
DNSサーバの名前とアドレスが表示されますか？

対象物の名前とアドレスが表示されますか？

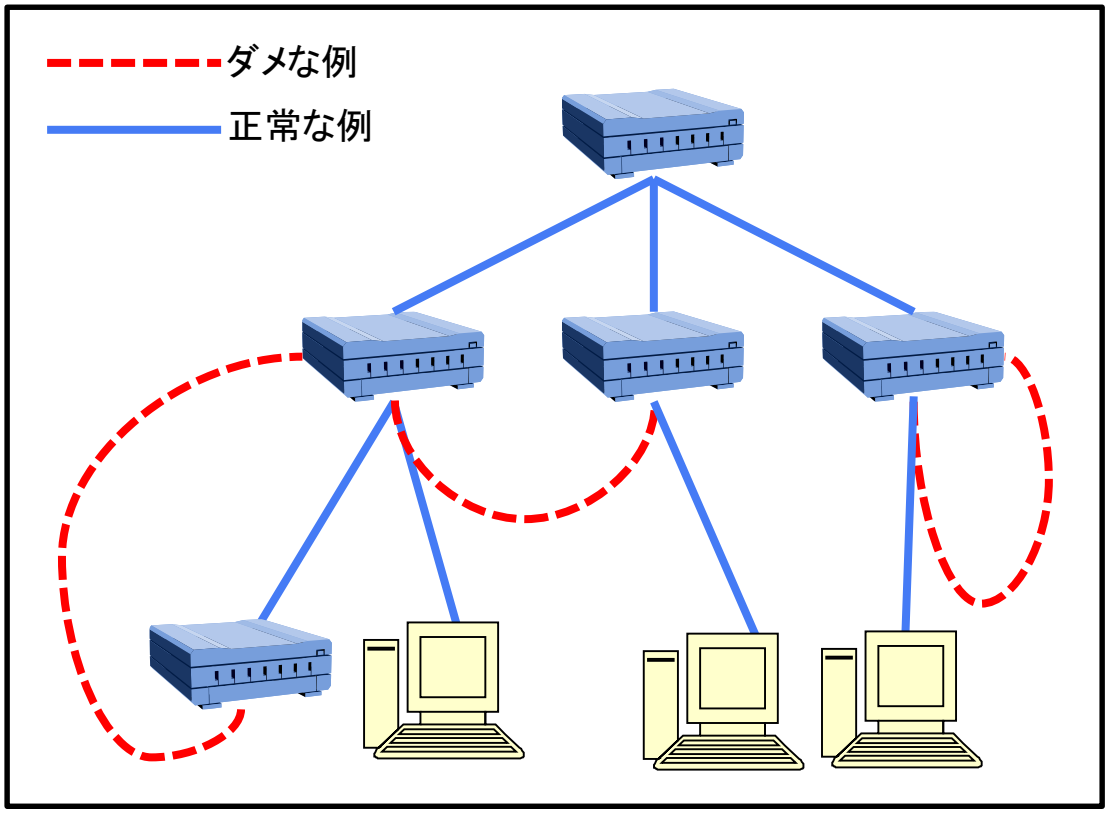
※Linuxはdigコマンド

4.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・・・）



ループに注意！



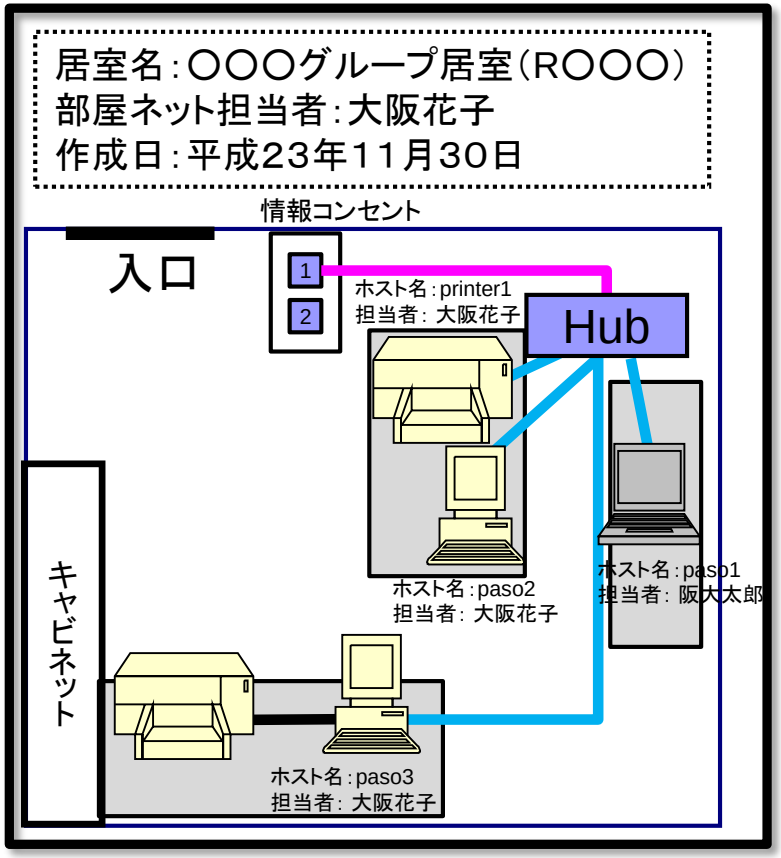
よくあるトラブルのうち、
原因を調査してみると、
「ループ」を引き起こしている
ケースがよく見られます。

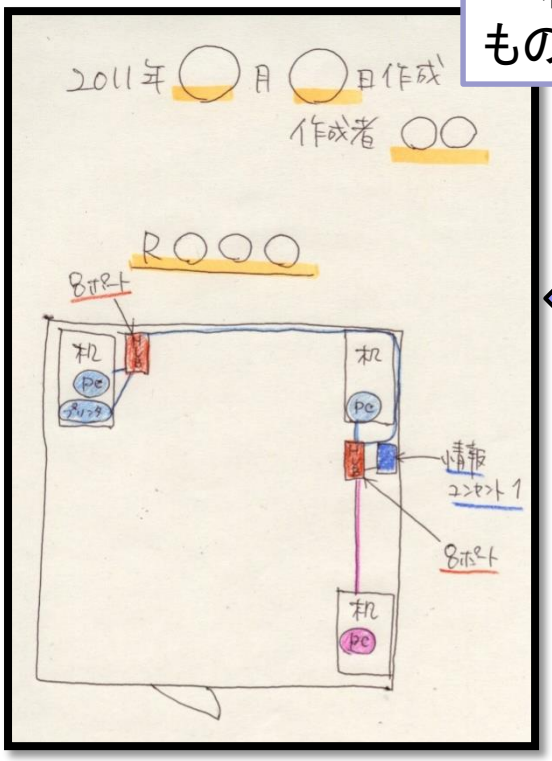
外れているLANケーブルを、
わからないまま適当に
接続すると、ループを
引き起こす可能性があります。

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！

トラブル対処とネットワーク配線図（サンプル）

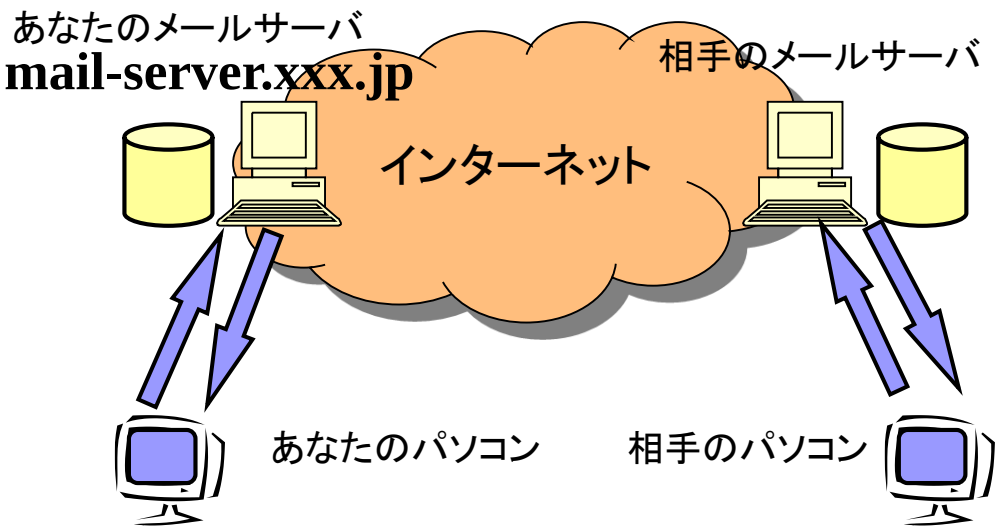




簡単な手書きでOK！
・正確（最新の情報）
・わかりやすい
ものであることが重要です

大阪大学レーザーエネルギー学研究センターでは、各部屋にネットワーク担当者を決めていただき、
各部屋の配線図の提出をお願いしています。
配線図は、「正確」「わかりやすい」ものであれば、手書きでもかまいません。
各部屋で内容を周知徹底できれば、トラブルもスムーズに対処できるでしょう。

5.電子メールとは（電子メールの仕組みとメールソフト）



パソコンで電子メールの送受信の操作をすると
設定されたメールサーバとの間で送信または
受信を行います。

次に自分のメールサーバと、相手の
メールサーバ間で、送受信を行います。

サーバ間のインターネットや、相手のサーバに
問題があるとメールが届くのに数日かかることや、
届かないこともあります。

あるいは、迷惑メールとして分類されてしまい、
相手に届かないということもあるかもしれません。

■メールソフトの選択

メールソフトには多くの種類がありますので、ここではそのごく一部を紹介します。

- WindowsLiveメール
- Windowsメール
- Outlook
- Opera
- Apple Mail
- Thunderbird
- Becky! Internet mail

市販されているものや無償配布のもの
OSに付属されているもの
ブラウザと一体型のもの　　などなど・・・

ここで紹介した以外にも多くのメールソフトがありますので、
機能や使い勝手を考慮し自分にあったものを、
使用するとよいでしょう。

6.メールソフト設定時に注意すること

■ 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。

■ メールサーバにメールを残さない設定にする

サーバに保存できるとはいえ、溜め過ぎるとメールの送受信ができなくなるなどのトラブルが起こりやすくなります。トラブルの例としては、同じメールが何度も届いたり、受信そのものができなくなったりします。
メールソフト上で「メールサーバに残さない」、あるいは「受信後数日で削除する設定」にしておきましょう。
同様にパソコン内にメールを溜め過ぎるとトラブルの原因になることがあります。
サーバーもパソコンも無限ではありません、不要なメールは削除しましょう。

■ テキスト形式で送信する設定にする

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。
最近のスパムメールの多くはHTML形式であったり、Javaスクリプトを埋め込まれる危険性もあるなど、
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。
そのようなユーザにHTML形式のメールを送ると、非常に見づらい状態に表示されてしまいます。
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！

詳しくは次のページへ・・・

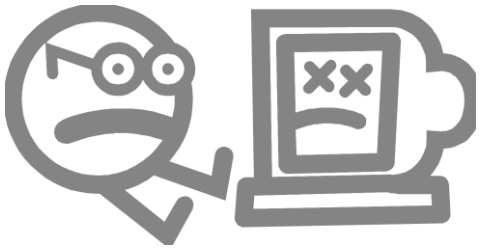
テキスト形式とHTML形式

■ 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



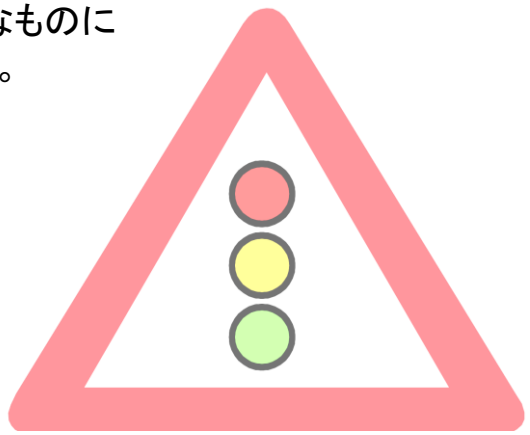
■ HTML形式の場合

```
------=_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>
                        ;
```

7.電子メール利用時の注意　ー送信時ー　その１

■　メールの件名

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 , Hello , Hi , Congraturation , Happy birthday** など…
→ このような件名のメールは、読まれなくても仕方ないでしょう



■　個人情報は記載しない

メール本文は容易に内容を読めるため、宛先の誤りの他、
盗聴などの手口で漏えいの可能性が高いので、
必要以上に情報を開示しないように注意しましょう。

また、電子メールはネットワークを経由するため、100%他人に見られない保証はありません。
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ようにしましょう。
（郵便でいうハガキと思えばよい）

電子メールの情報が、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しっかりと認識しましょう。

電子メール利用時の注意　ー送信時ー　その2

■　宛先のメールアドレスの確認

宛先のメールアドレスをよく確認しましょう。
また、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。

また、返信するときはTo、CC:などをよく確認し、メールを送る必要がない人に
送信することのないように注意しましょう。

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・・・

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。

電子メール利用時の注意　ー送信時ー　その3

■　添付ファイル送信時の注意

◆互換性に注意！

相手も同じアプリケーションソフトを持っているとは限りません。お互いのメール・パソコン環境が異なっているかもしれない、ということを考えて送信しましょう。
自分が参照できるファイルだからといって、相手もそうだとは限りません。
ファイルサイズ（容量）にも気をつけましょう。

◆機密情報にはパスワードを付ける

機密情報を記載した添付ファイルを送信するときには、必ずパスワードをつけるようにしましょう。
パスワードを設定した場合には、パスワードをメール本文には記載せず、
別メールとして通知するなどの工夫が必要です。

◆再確認！

送ってはいけないファイルと誤って送信することがないよう、送信ボタンを押す前に、
再度、送るべき添付ファイルが正しいか確認するようにしましょう。

添付ファイルを含む誤送信は情報漏えいにつながる危険性があります。
場面によっては取り返しのつかないことになり、うっかりミスでは済まされないケースもあります。
十分注意しましょう。

電子メール利用時の注意　－その他－

■　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

発信元が不明なメールは開かずに削除しましょう。
見覚えのないアドレスや怪しげな件名のメールは開かないのが常識です。
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。
悪質な犯罪に巻き込まれる恐れもあります。注意しましょう。

■　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。

■　迷惑メール（デマ、チェーンメール、スパムなど）は、返信せずに削除すること

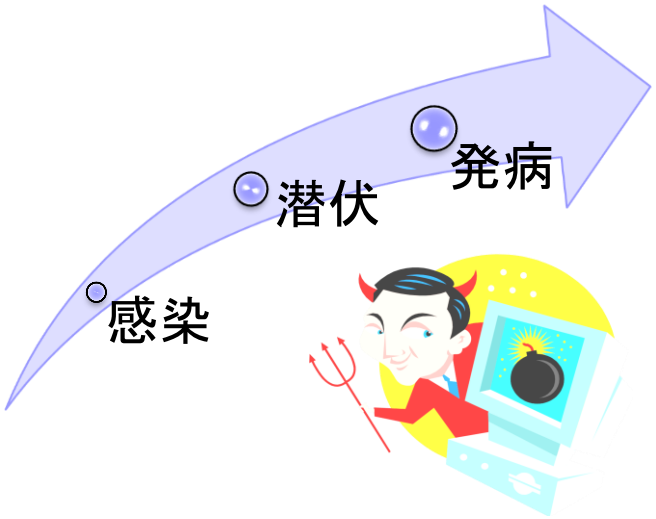
発信者へ問合せをしたり、メール本文に記載されているURLへアクセスしてしまうと、
大量の迷惑メールを受信するようになったり、身に覚えのない料金の請求などの
トラブルを招くきっかけとなってしまう恐れがあります。

8.パソコンのセキュリティ

― 8．1 コンピュータウイルス ―

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

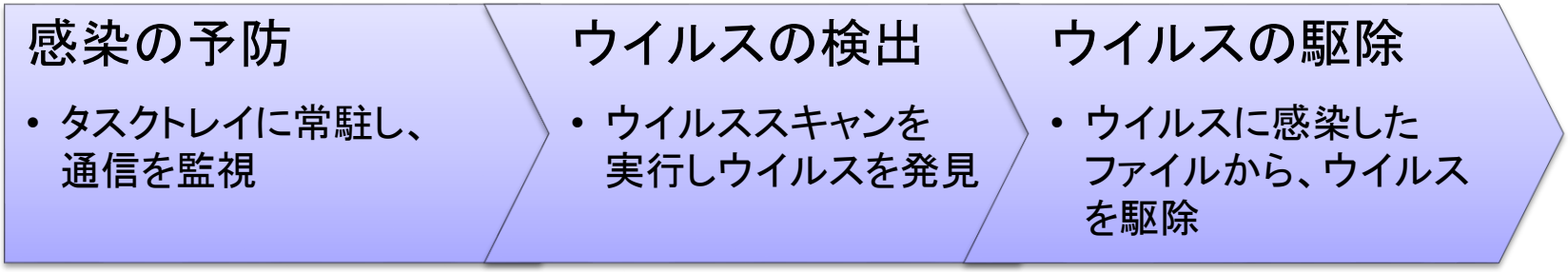
最近のウイルスは派手な活動をしないことが多いので、注意が必要です。
下記のような症状がない（気付かない）うちに、データを転送されたりするケースも！！

- 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。

― 8．2 ウイルス対策ソフト ―

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。

もしもウイ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・・・
- 上司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。（P.30でも記載しています）

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。

個人情報（個人を特定できるような情報）やパスワードを守ってますか？

個人情報や、あなたのパスワードが漏えいしたために、多大なる被害を被ることがあるかもしれません。信頼できないサイトでは絶対に入力しないのはもちろん、パソコン内にそういったファイルを保存したまま、そのパソコンを廃棄したり、他人に容易に知られてしまうようなことは絶対にしてはいけません。

常に最新情報に注意しましょう。

新聞やニュースなどにも注意し、サイバー犯罪に巻き込まれないよう、最新情報にも注意しましょう。
そういった情報を発信しているサイトもあります。定期的に確認するなど、情報収集も怠らないようにしましょう。

■ IPA（独立行政法人情報処理推進機構）
http://www.ipa.go.jp/ セキュリティ情報や情報セキュリティポスターなど
■ 警視庁 情報セキュリティ広場
http://www.keishicho.metro.tokyo.jp/haiteku/ ネット犯罪対策やサイバー事件簿など

― 8．6 バックアップの重要性 ―

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。

DVD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。

9.Web閲覧時の注意　その1

SNSやtwitter
なども注意

- 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

フィッシング詐欺：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、パ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

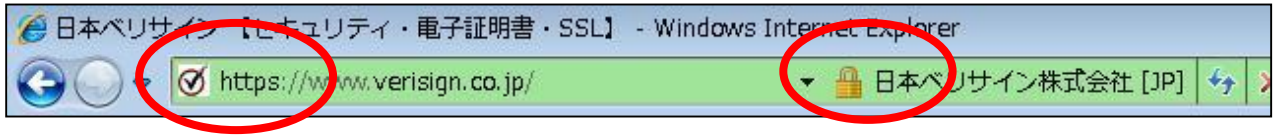
被害にあったときは、正規の連絡方法によりサービス会社に連絡を取り、
早急にパスワードを変更、もしくはサービス利用の権限を停止してもらいましょう

Web閲覧時の注意　その2

SSL通信（暗号化）

SSLはセキュリティを高める暗号化通信の規約（プロトコル）です。

- Web画面上で個人情報などを入力する際には･･･
  - URLが「https://」で始まっていますか？



  - ブラウザに錠前のマークが表示されていますか？
    - ✓ 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ること
    - ✓ 有効期限：期限切れになっていないこと

•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
•アンケート画面
•ご意見やご相談などお問い合わせフォーム　など…

Web閲覧時の注意　その3

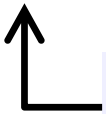
Webページ閲覧時、会員登録などを行うとパスワードを設定しなければいけない場面に遭遇します。
パスワードクラックされないように、以下のようなことに気をつけなければいけません。

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

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　←　一つクラックされたら･･･？

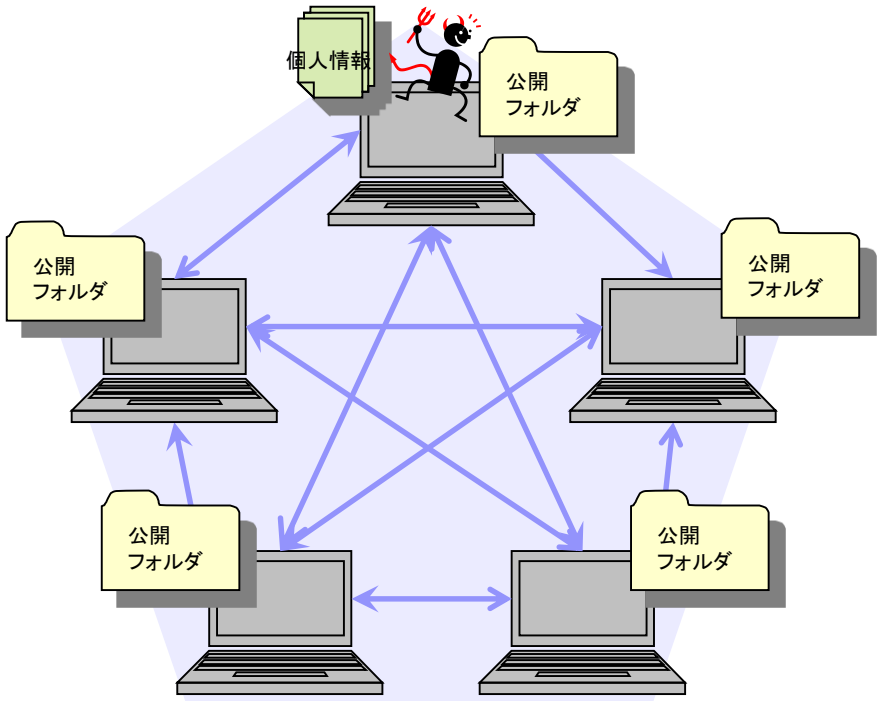


盗まれた時の深刻度に応じたパスワード（長さ、難易度）を設定するのも一つの重要な手段です。

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？

10. ファイル交換ソフト(P2P)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。



＜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：IPv4　IPアドレス枯渇問題とは

現在広く普及している「IPv4」(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、IPv6とIPv4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

大阪大学レーザーエネルギー学研究センター
高性能計算機室
http://www.ile.osaka-u.ac.jp/research/cmp/