安全なコンピュータ利用のために

インターネットの利用と危険性

一般財団法人蛋白質研究奨励会
情報室
磯山正治

インターネットの脅威

- テクニカルハッキング（クラッキング）
  - コンピュータネットワークに繋がれたシステムにソフトウェアの脆弱性などを利用して不正に侵入したり、コンピュータを破壊・改竄などをしたり、コンピュータを不正に利用すること
    - コンピュータ上のアカウントへの侵入
    - インターネットサービスの乗っ取り
    - データベースへの侵入

従来、ハッキングの主流であった

テクニカルクラッキングを防ぐには

- ウィルスワクチンソフトのインストール
  - 定期的なウィルスデータのアップデート
- システムのアップデートをおこなう
  - Microsoft Update（自動アップデート）
  - MacOS(自動アップデート)
  - 多くのソフトウェアはインターネット経由で自動的にセキュリティアップデートを行うようになっている
- 不要なソフトウェア・サービスをインストールしない
- 推奨ソフト、許可ソフト、禁止ソフトのルールを守る
- データバックアップの励行

ソーシャルハッキング

- ハッキングの目的の変化
  - 愉快犯から経済犯へ
  - 実利をもとめるクラッカー
  - 「相手はお金がかかってるんで本気です」
- テクニカルハッキングの限界
  - 脆弱性のチェックの普及
  - セキュリティアップデートの普及
  - セキュリティ意識の向上

ハッキング手法の組み合わせ

ソーシャルハッキング

- コンピュータ版「振込め詐欺」
- 人間の心理的な隙や、行動のミスにつけ込んで システムクラッキングを行う

- コンピュータシステムは「かなり」安全になってきているが、「人間の命令には従う」
- あの手この手で「クリックさせる」ことをめざす

ソーシャルハッキング事例

- SEOポイズニング
- スピア攻撃（狙い撃ち）
- 電話でたずねる
- メールで引っかける
- 空き巣に入って勝手にインストール

偽サイトへの誘導・有害プログラムの実行

「クリックさせる」

ハッキングされてしまったら・・

- データロガー・キーロガー
  - PCにはいっている重要な個人情報（口座番号、パスワード）が盗まれます。
  - セーブしていない情報でも「入力と同時に」盗まれます。（クレジットカード番号、パスワード）
  - 業務上の秘密情報が盗まれます。

一度出てしまうと取り戻すことはまず不可能です

- ランサムウェア（身代金要求）
  - PCやデータファイルをロック・暗号化して使用できないようにします。
  - PCやデータを「人質」にして「身代金」を要求します。
  - 業務ができなくなってしまいます。

身代金を払ってももとに戻る保証はありません。
ずっと身代金を払い続けないといけないかも・・

社会的責任

- 個人的な被害も甚大ですが、社会的な責任が発生する事もあります。
  - ボットシステムに組み込まれる
  - 知らないうちに加害者になる

アメリカ、韓国に対する大規模攻撃
(2009.07.08-09)

世界中のコンピュータへの大規模攻撃
（2017.05.13～）

ソーシャルハッキング対策

- ウェブを利用するときは
  - リンク先のURLをよく確認する
  - むやみにプログラムを実行しない
  - ダウンロードしたファイルは開く前にウイルスチェックする

ソーシャルハッキング対策

- メールを利用するときは
  - スパムメールはゴミ箱行き
  - 実行形式の添付ファイルはむやみに開かない
  - 必要なときはウィルスチェックをしてから！
  - メール中のリンクをむやみにクリックしない

迷惑メール事例

- 修正パッチ情報に見せかけたメール
- かたりメールやなりすましメール
  - 差出人情報はあてになりません
  - 「なんとなく知ってる人のような気が・・」

おくられてきたメールのリンクをクリックしない！

添付ファイルをダブルクリックなどもってのほか！

修正パッチ情報に見せかけたメール

件名: Security Update for OS Microsoft Windows
差出人: Microsoft Corp. <securityassurance@microsoft.com>
送信日時: 2008/10/14 19:13
宛先: isoyama@prf.or.jp

Dear Microsoft Customer,

Please notice that Microsoft company has recently issued a Security Update for OS Microsoft Windows. The update applies to the following OS versions: Microsoft Windows 98, Microsoft Windows 2000, Microsoft Windows Millenium, Microsoft Windows XP, Microsoft Windows Vista.

Please notice, that present update applies to high-priority updates category. In order to help protect your computer against security threats and performance problems, we strongly recommend you to install this update.

差出人情報は信用できません

microsoft.comは正しいアドレスです。しかし、このメールはmicrosoft.comから来たものではありません！

修正パッチ情報に見せかけたメール

本物です

Dear Microsoft Customer,

Please notice that Microsoft company has recently issued a Security Update for OS Microsoft Windows. The update applies to the following OS versions: Microsoft Windows 98, Microsoft Windows 2000, Microsoft Windows Millenium, Microsoft Windows XP, Microsoft Windows Vista.

Please notice, that present update applies to high-priority updates category. In order to help protect your computer against security threats and performance problems, we strongly recommend you to install this update.

Since public distribution of this Update through the official website http://www.microsoft.com would have result in efficient creation of a malicious software, we made a decision to issue an experimental private version of an update for all Microsoft Windows OS users.

As your computer is set to receive notifications when new updates are available, you have received this notice.

アドレスは本物なのでクリックするとマイクロソフトのホームページが開きます。

In order to start the update, please follow the step-by-step instruction:

1. Run the file, that you have received along with this message.

2. Carefully follow all the instructions you see on the screen.

If nothing changes after you have run the file, probably in the settings of your OS you have an indication to run all the updates at a background routine. In that case, at this point the upgrade of your OS will be finished.

We apologize for any inconvenience this back order may be causing you.

Thank you,

Steve Lipner

Director of Security Assurance

Microsoft Corp.

-----BEGIN PGP SIGNATURE----- Version: PGP 7.1
8GTP6Z90IT8DES1FLX10EITNOPZU0NH3ZP2G9G3Y1ZHQQWFC6MDJGL3C4Q4L00O0L
8KQQVUXU217HE2CAZE77O2L1P30TITU7KCI79KNZ7I3WN7X335KUKVJSVV3TVURS0
WYE2GT43M4U96INN9KOWDIQ41EUQDX1VUD8KWQDJ1NHY2PV7M56K7R8G7HEF1WYZ5
PZC9HK31QDD9D9SPF7W2L386KUXU2RF10K2B44ZOOXHLAMIOBIOI7MBQVIH2L72IJ
525U4BDQ6EM0NBQIB71BR2U74G3VI94JZP8==

-----END PGP SIGNATURE-----

Steve Lipnerは実在の人物で実際にマイクロソフトのセキュリティ担当者です

それらしいPGP署名もついてます・・にせものですが。

- それでもこのメールは偽物です。
- 添付ファイルはKB601922.exe でした。
- ダブルクリックしたら、ウィルス（トロイの木馬）に感染してしまいます。

- 添付書類のダブルクリックは大変危険な操作です。絶対にしてはいけません。
  - 「名前を付けて保存」し「ウィルスチェック」行う

メールソフトの設定

- 推奨しているメールソフトを使用すること
- 禁止されているメールソフトは使用しないこと
- HTML表示にしない。（プレーンテキストにする
  - 必要に応じてHTML表示に変えるのはよいが、メールの閲覧が終わったら元にもどす

メールソフトの使用習慣

- 受信トレイにメールを保存しない
  - 受信トレイは特殊な意味があります。
  - メールのウィルスチェックや処理に問題が発生することがあります。
  - 「とりあえず」フォルダをつくってそこに移動しておいてください。
  - 「細分化したフォルダをつくれ」と言ってるのではありません。メールの分類は自分の流儀でしてください。

メールソフトの使用習慣

- 迷惑メールの学習をさせましょう
  - 推奨ソフトのサンダーバードには迷惑メールの学習機能があります。
  - 迷惑メールの判断を教えないと適正な動作をしません。
  - 時々は学習を手伝ってあげてください。

メールソフトの使用習慣

- メール判別フィルタを活用しましょう
  - メールフィルタは迷惑メールフィルタより優先されます。
  - 必要なメールが迷惑メールに間違えられることが減ります。
  - 「必要なメール」というフォルダでもかまいません。そこに自動的に移動するようになります。
  - 明らかな迷惑メールを積極的に削除する事にも使えます。

インターネットとPCの利用

- バージョンアップが終わったソフトウェアやOSはどんどん危険なものになります
  - 脆弱性が解消されない
    - テクニカルハッキングをうける
  - スパムメール対策が不十分
    - スパムメールは「引っかけ」の温床です
    - ソーシャルハッキングを受ける
  - 「安全なOS」など存在しません。
    - バージョンアップ、アップデート、ウィルスチェックは必須です。
- 「その上」で「注意しながら」PCをつかう

レガシーネットワークの意義

- セキュリティポリシーを満たさないPCはインターネット接続環境に置く事はできない
- セキュリティポリシーを満たすことができないPCは存在する
- セキュリティポリシーを満たすことはできないがネットワークをつかってデータの共有などの機能が必要

「レガシーネットワーク」として「通常LAN」と切り離したネットワークシステムの構築

ネットワーク経由でのマルウェア感染を防ぐ

ネットワークの再構築（案）

- 「ネットワークのクリーンベンチ」
- セキュリティポリシーを満たさないPCをレガシーネットワークに設置する。
- インターネット接続環境から隔離する。
- データの受渡し方法が問題になる。
  - USBメモリなどは大変不便であり、危険性もともなう

- データゲートウェイで受渡しとネット隔離をおこなう

ネットワークの相違点

- 通常ネットワーク
  - 現在考えられ得る最善のセキュリティ対策を施されたPCのみが接続できる安全なネットワーク
    - ウィルスチェック、OS・ソフトウェアの自動アップデート
    - ソフトウェアの使用制限

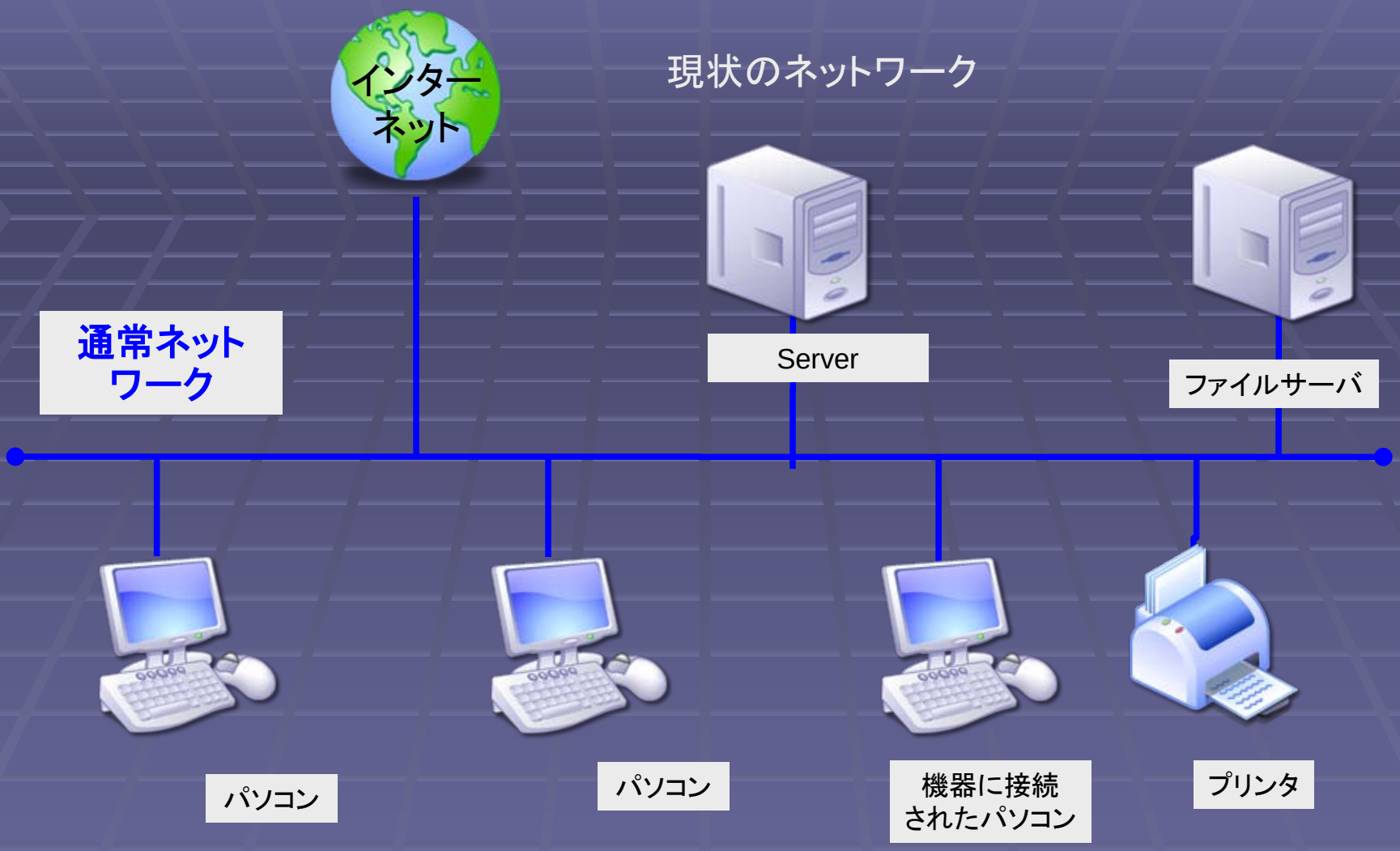
インターネットに接続可能

ネットワークの相違点

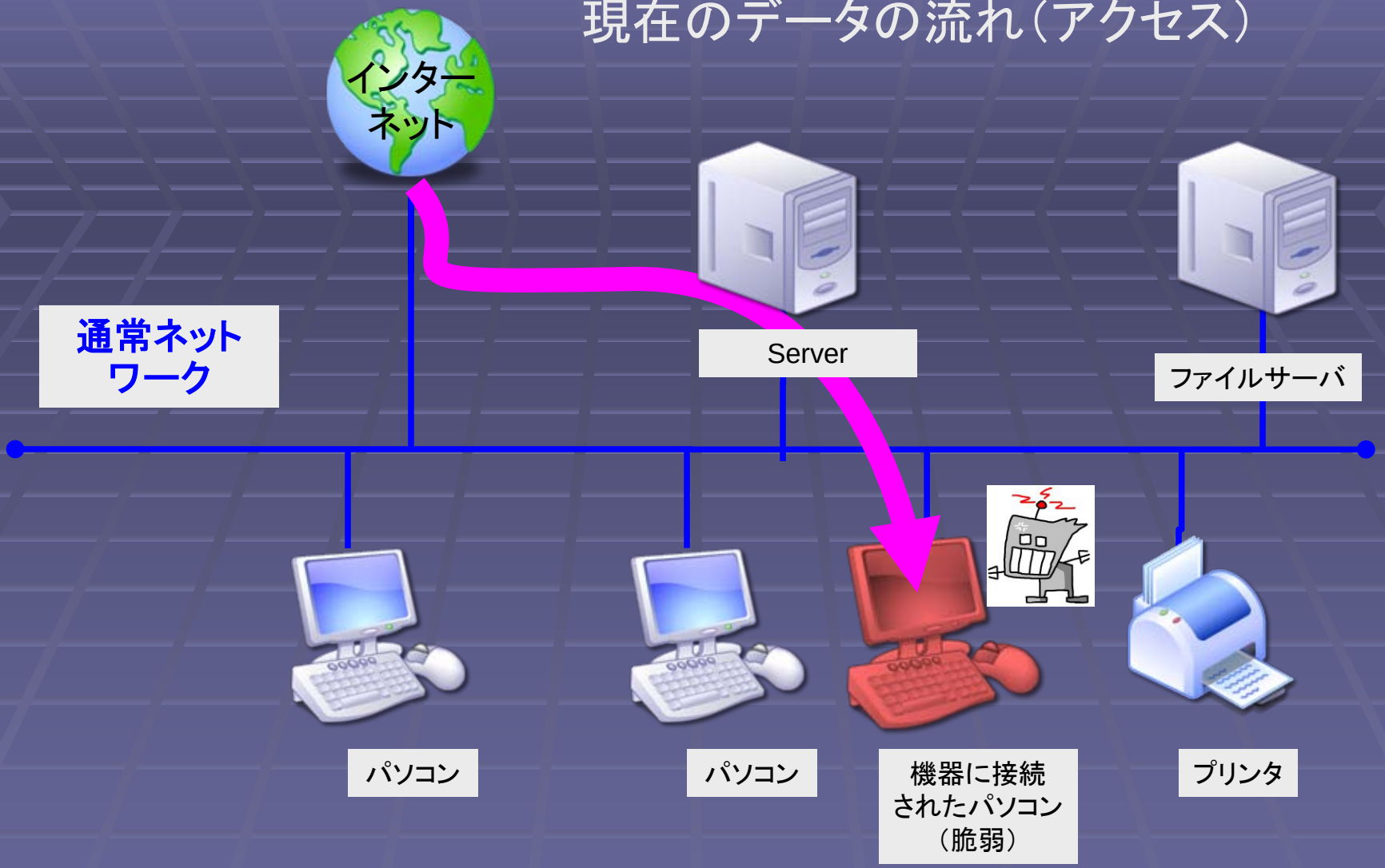
- レガシーシステムのためのネットワーク
  - セキュリティレベルは必ずしも高くないが、特定の機器との互換性から必要不可欠なサーバやPCを接続するためのネットワーク
    - OS・ソフトウェアの自動アップデートは不要
    - ウィルスチェックなどインターネット接続が必要なシステムはインストールできない
    - ソフトウェアの使用制限なし

インターネットに接続不可

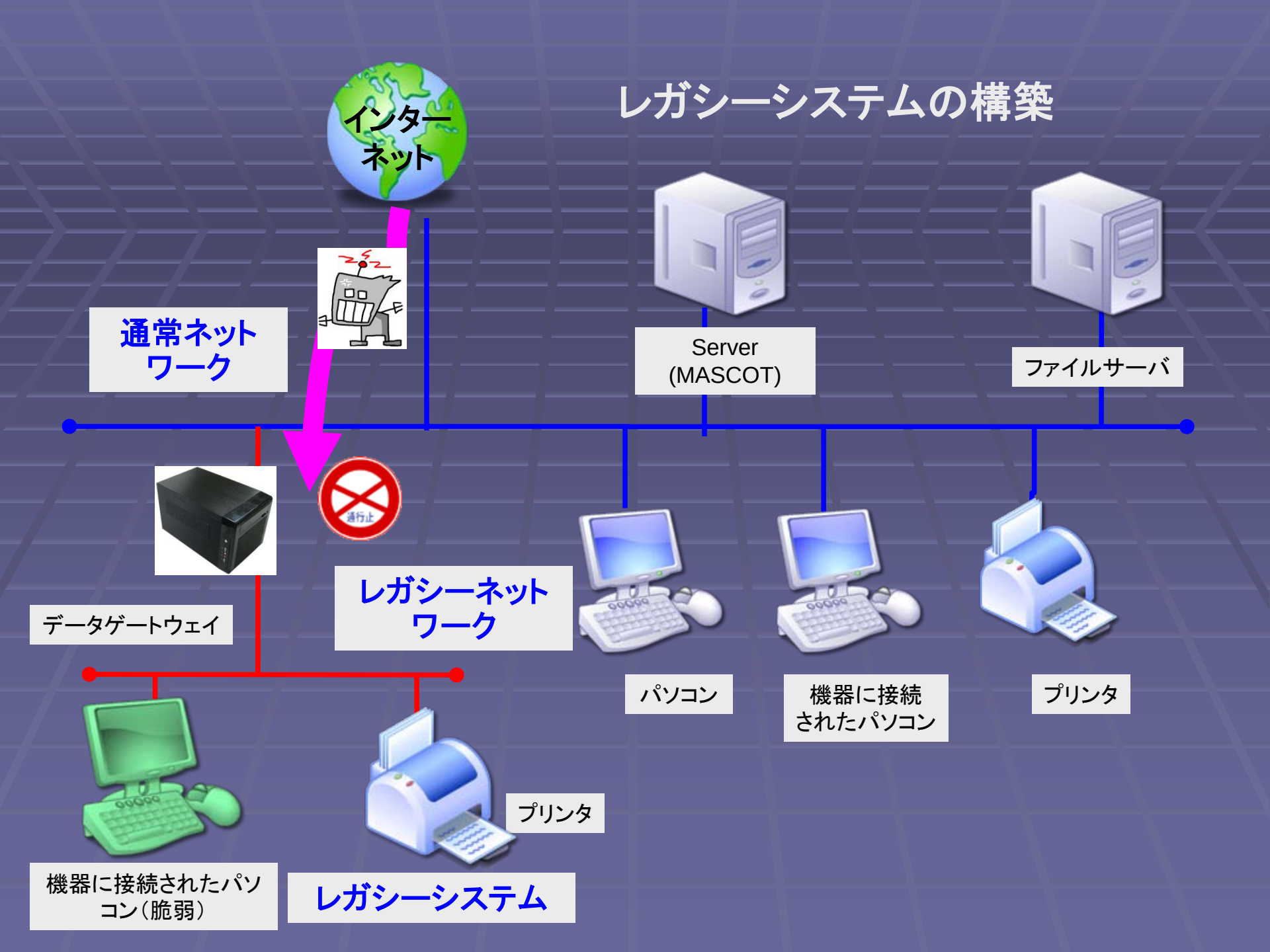
現状のネットワーク


インター
ネット
通常ネット
ワーク
Server
ファイルサーバ
パソコン
パソコン
機器に接続
されたパソコン
プリンタ

現在のデータの流れ（アクセス）



レガシーシステムの構築



古典的な危険

- インターネット以外の危険性は今も残っています。
- 最近はメディア経由の危険は特に増してきています。
  - インターネットの危険性が強調されすぎて盲点となってしまった。
  - USBメディア、CD、DVD、外づけHDDなど
  - 感染したコンピュータの接続
  - 共有コンピュータ、写真プリンターなど

感染事例

警視庁の感染もUSBか

警視庁のオンラインシステムに接続している端末のパソコンが、「W32・Do

wnadup・B」と呼ばれる新種のネットワーク感染型ウイルスに感染した問題で、同庁は、USBメモリーなどをパソコンで使った際に感染した可能性があるとして感染経路を調べている。完全復旧は週明けの26日になる見込み。

2009年(平成21年)1月24日(土曜日) 夕刊 讀賣新聞

USB感染 大学で500件超

共有PC、管理甘く

本社調査

パソコンのデータを保存する外部記憶媒体「USBメモリー」経由で感染するコンピューターウイルスが全国の大学で猛威を振るっている。読売新聞が主な30大学に聞き取り調査したところ、半数近い13大学で500件以上の感染が確認された。大勢の学生がUSBメモリーを持ち込み、共有のパソコンを使うことが多い大学は、管理の甘さもネックとなって感染の温床になっている。重要な研究成果が流出する恐れもあり、文部科学省は昨年末、全国の国立大学に文書で注意を呼びかけた。

学生数や知名度などから大学を選び、調査。回答のあった27大学のうち13大学でUSBメモリーによる感染があり、被害件数は確認できただけで527件にのぼった。筑波大、九州大、中央大は回答しなかった。

多くは「オートラン」と呼ばれるウイルスで、感染したUSBメモリーをパソコンに挿入すると、自己増殖。表面上はパソコンの動作が遅くなる程度の変化だが、パソコン内部の情報を第三者にメールで送ったり、別のウイルスを誘導したりすることもある。

東京外国語大では昨年11月、学生から「論文を書いていたら勝手にメール送信が始まった」と届け出があり、80台以上のパソコンで感染を確認した。パソコンからは大量のメールが送られた形跡があったが、どんな内容で、どこに送信されたかは記録がなく、「情報を抜き取られたのかもしれないが、さっぱり分からない。検証しようもない」と担当者は困惑する。

京都大では昨年7月に感染が判明。12月末までに168台の感染がわかった。感染源は研究者や学生、業者などが持ち込んだUSBメモリーが大半だった。ただ、現時点で実害は報告されていないという。

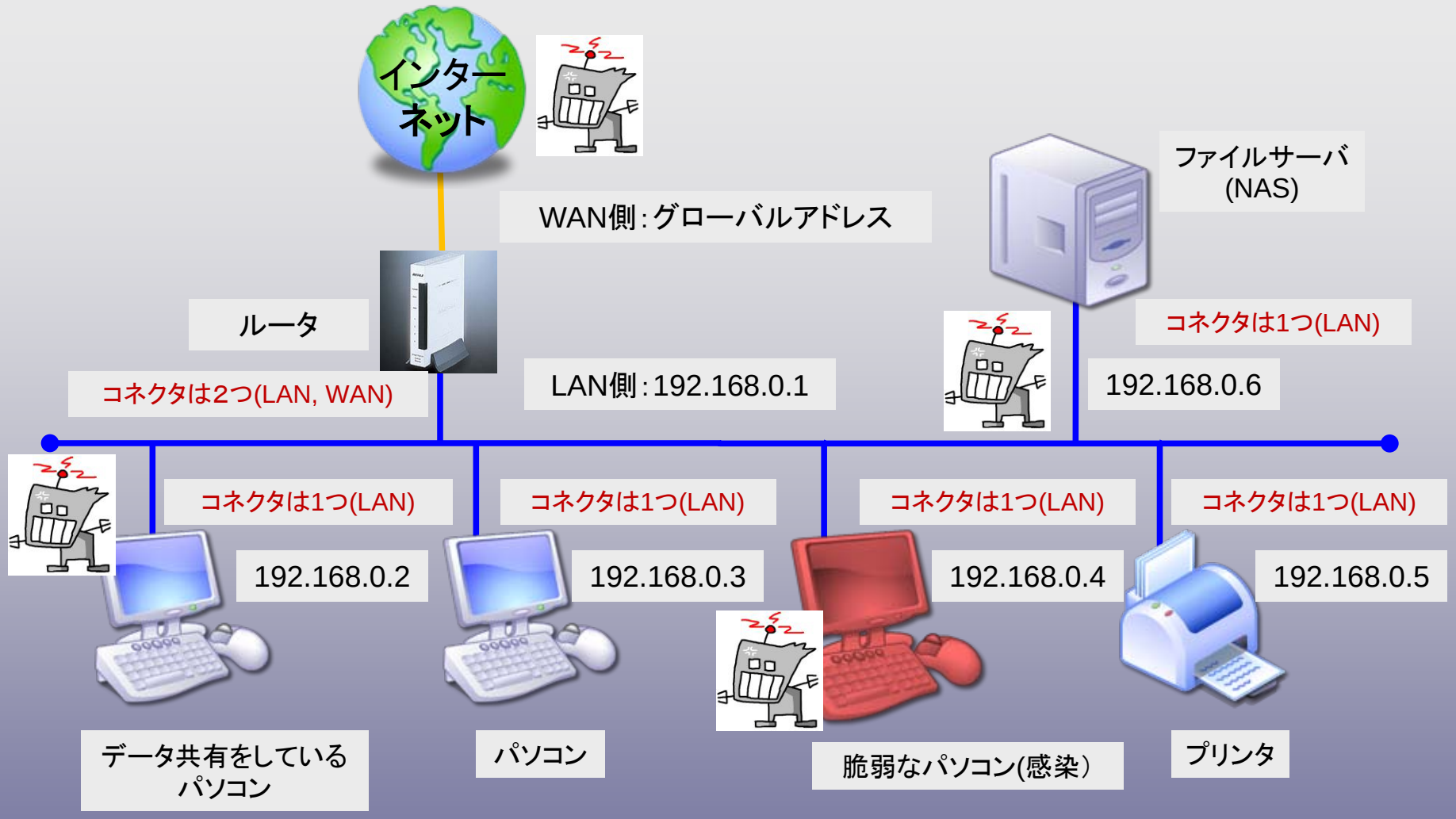
九州歯科大では、サークル活動棟の共有パソコンの3分の1にあたる20台が昨年5月に感染。1台で60種類のウイルスに感染したパソコンもあったほか、一部の学生は感染したパソコンで作成したリポートを提出し、教員らのパソコンに二次感染した事例もあった。

ほかにも、日本大文理学部で約200件、近畿大で20件、それぞれ感染報告があった。

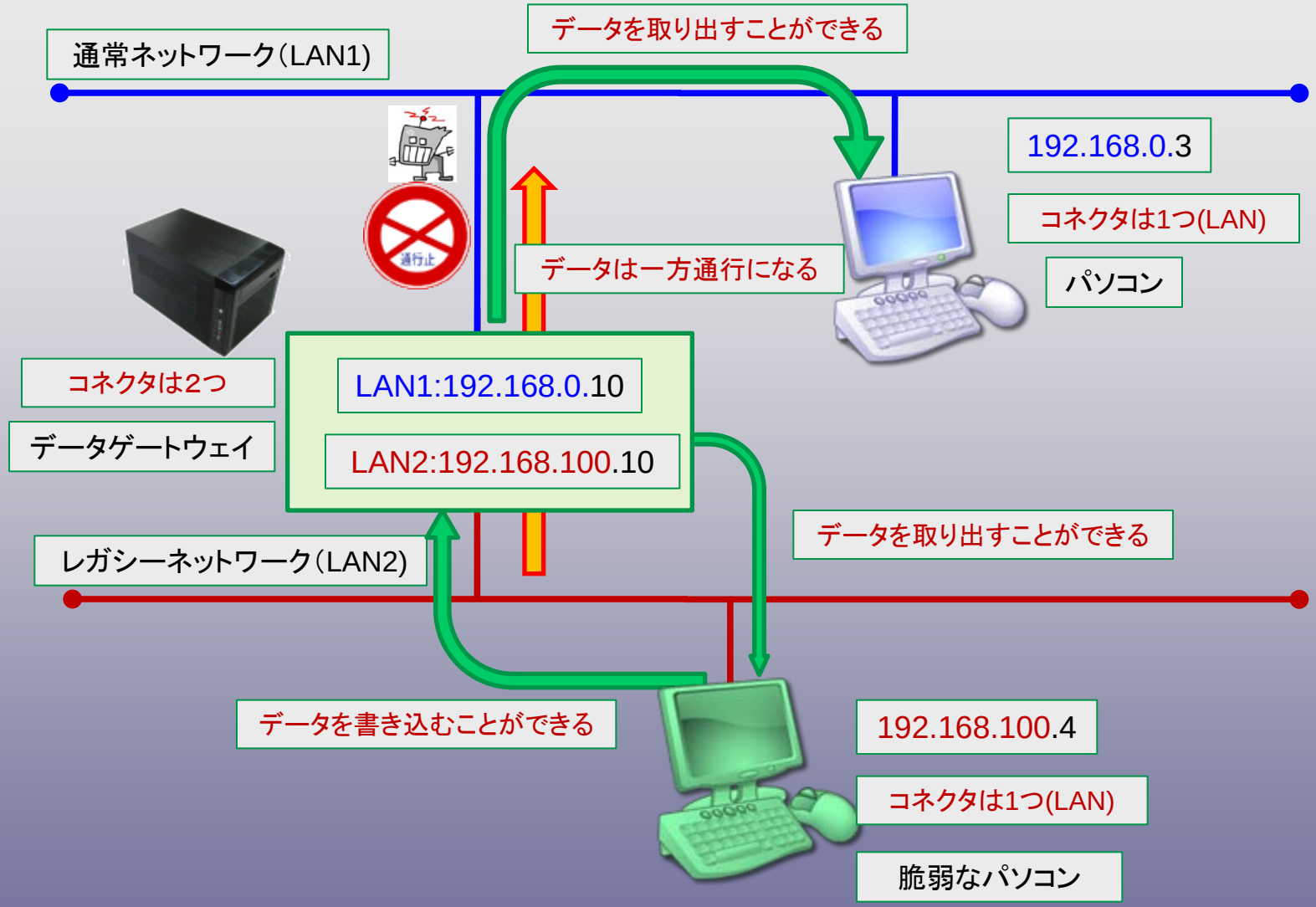
USBメモリー　パソコンのUSB端子に差し込んで使う外部記憶媒体。2㌢ほどの大きさで、一昔前のパソコン並みの容量があるものも。これを介してパソコンがウイルスに感染する被害が昨年急増。独立行政法人「情報処理推進機構」によると、昨年11月に届け出のあった全ウイルス検出数の4割の10万1000個がUSBメモリー経由だった。

ヒト経由の感染を防ぐ

- USBメモリ、CD、外づけHDDでレガシーシステムにデータを持ち込むときは十分に注意をしてください。
  - 万一、メディアなどが感染していたら、レガシーシステムでは大災害が発生します。
  - 自分のPCでチェックする事も可能です。
  - 感染が見つかると安全が確認されるまでPCが使えません。場合によっては、PCのデータなどに被害がでます。



•データはLANのなかでは、自由にやり取りされている。
•データ共有のパソコン、NASにデータを自由に読み書きできる。
•マルウェアもLANのなかを自由に行き来することができ、PCへの感染の可能性がある。



- データはそれぞれのネットワーク内では、自由にやり取りされている。
- LAN1のPCはデータゲートウェイからデータを取り出すことだけができる。
- LAN2のPCはデータゲートウェイのデータを読み書きすることができる。
- マルウェアはLAN1からLAN2へ、データゲートウェイを通過できない。