データゲートウェイ

近年、インターネット環境は格段に進歩し、大変便利なものとなりましたが、その一方で、ウィルスなどのマルウェアの感染やハッキングなどの危険性も増してきました。
そのため、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。セキュリティ対策を行ったうえで「注意しながら」コンピュータをつかわないと被害をうけたり、知らないうちに加害者になってしまったりする危険性があります。
その一方で、測定器の制御コンピュータなどでは、バージョンアップする事ができない場合もあります。

このようなコンピュータをネットワークからきりはなして、USB メモリや外づけのハードディスクなどでデータを移動しながら作業をすることも可能ですが、十分なチェックをしていないと USB メモリやハードディスクからマルウェア感染してしまう可能性も少なくありません。ところが、データ移動のたびに USB メモリなどのウィルスチェックをするのは大変繁雑な作業となるため、実際上、仕事ができなくなってしまうことになりかねません。
これらの互いに矛盾する要件をみたし、安全性と利便性のバランスをとる必要がでてきました。

「レガシーシステムと通常ネットワーク上のコンピュータの間でのデータの受渡しを容易にする」ためにデータゲートウェイは考案されました。

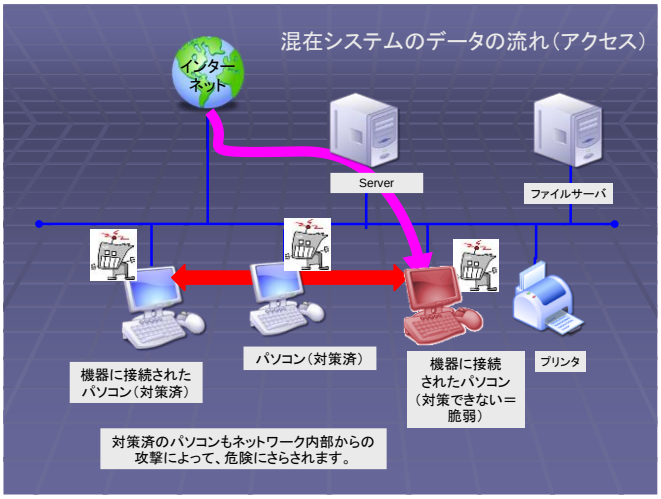
- セキュリティ対策がとれないコンピュータを設置するためのネットワークシステム（レガシーシステム）を構築する。
- 「通常 LAN」と切り離すことによりネットワーク経由でのマルウェア感染を防ぐ。
- チェックが不完全な USB メディア、外づけハードディスク、CD、DVD などからマルウェアが感染することを防ぐ。（データの移動にメディアをつかわない）

価格：128,000 円

財団法人
蛋白質研究奨励会

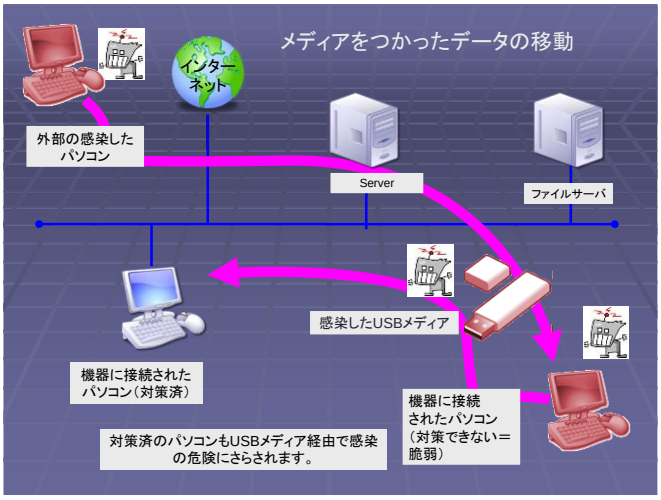
562-8686 大阪府箕面市稲4-1-2
TEL：072-729-4155　　FAX：072-729-4165
ホームページ：http://www.prf.or.jp/
電子メール：misoyama@prf.or.jp

危険なコンピュータの利用形態



インターネットからもローカルエリアネットワーク(LAN)からもマルウェア感染の危険性があります。また、LAN 上の他のコンピュータも内部からの攻撃によるマルウェア感染の危険にさらされます。

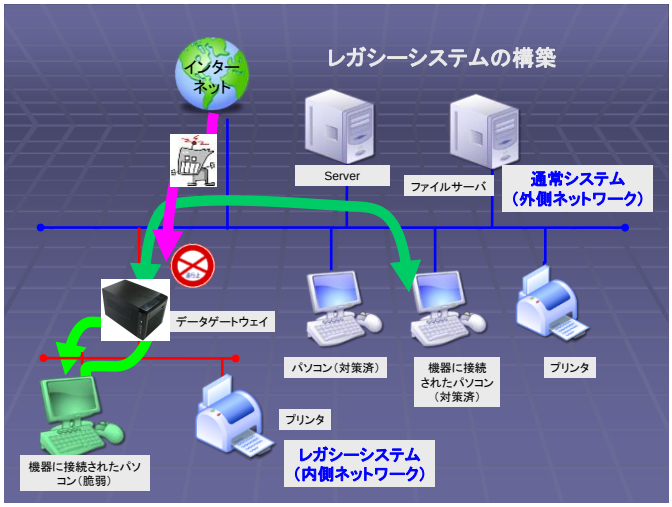
チェックが不完全なメディアは危険



ネットワークに接続していなくても USB メディアなどからマルウェア感染の危険性があります。そのため、コンピュータに接続する前に、USB メディアなどのウィルスチェックをしておく必要があります。

この目的のために「検疫専用のコンピュータ」を準備されることをお薦めします。

データゲートウェイによるネットワークの改善



脆弱なパソコンをインターネット接続ができるネットワーク環境から切り離します。また、データの移動をスムーズに行うことができます。

コンピュータの安全な利用のために

サポートが終了したソフトウェアや OS は危険なものです。

- 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
  - 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

PC 利用に関する「セキュリティポリシー」の制定が推奨されます。

- 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かない。
- USB メモリ、外付け HDD、CD、DVD などのメディアを介したマルウェア感染の危険性を考慮する必要がある。
- セキュリティポリシーを満たすことができない PC からデータのうけわたしなどをする必要がある。

安全性と利便性とコストのバランスをとる必要があります。

○「インターネットに接続する通常 LAN」と切り離したネットワークシステム（レガシーネットワーク）を構築し、ネットワーク経由でのマルウェア感染を防ぐ

○USB メモリなどの外付けメディアを使用しないことで、メディアを経由したマルウェア感染を防ぐ。

万一、マルウェアに感染したら・・・

- PC のデータが破壊されたり、PC が起動しなくなったりすることがあります。
- マルウェアの隔離・除去が完全にはできないことも多く、その時は、HDD の交換や OS や各種ソフトウェアの再インストールが必要となり、業務に多大な悪影響を与えます。
- 重要なデータなどが失われてしまい、回復することができないことも多いです。
- 重要なデータ、個人情報などがインターネットに流出したり、盗まれたりする危険性があります。
- 情報の流出・盗難は訴訟や補償などの「２次被害」を発生させることもあります。

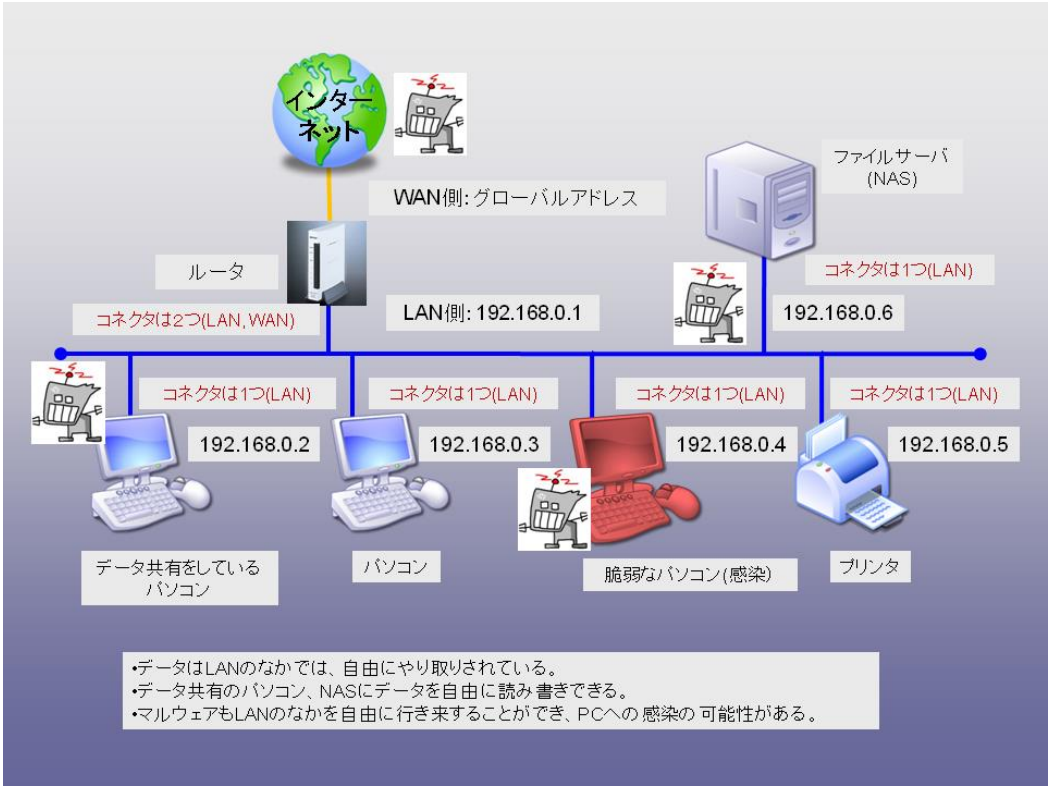
データゲートウェイの動作・仕様について

ネットワーク通信の仕組み

現在、主流となっているネットワーク通信は、インターネットプロトコル(TCP/IP)によって、相互に認識・通信を行ってデータの送受信を行っています。このプロトコルでは、ネットワーク機器に個々独立した番号（IP アドレス）を付与することで、機器の区別と送受信先の認識を行っています。そのため、インターネットやローカルエリアネットワーク(LAN)に機器を接続するためには、機器に固有の番号（アドレス）を付与する必要があります。現在、主流である IPv4 のアドレスでは、機器に 00.00.00.00 から FF.FF.FF.FF までのアドレスから固有の番号を付与します。(実際には使用されない番号もあります。) 全部で約４３億個 (2^{32}) になりますが、このアドレスを全世界で共有しています。アドレスの枯渇を防ぐために、LAN でのみ利用するアドレスとしてプライベートアドレスが準備されています。そのため、LAN に機器を設置・接続する際には、通常、プライベートアドレスを使います。

プライベートアドレスとして定められているアドレスに、192.168.からはじまるものがあります。たとえば、機器に 192.168.0.**のアドレス（**は 1 から 254)を与え、サブネットマスクを 255.255.255.0 とすると、192.168.0.**の機器だけでデータの送受信ができます。たとえば、192.168.100.**のアドレスを持った機器とはデータの送受信ができません。

PC によるファイル共有や NAS（Network Attached Storage）では、ネットワークコネクタは 1 つであり、同一の LAN に接続されているアドレス空間が共通の機器の間でデータのやり取りやデータの読み書きをおこないます。



PC によるファイル共有や NAS のデータ移動の概念図

参考１）Windows PC であれば、コマンドプロンプトから ipconfig [Enter]と入力すると、そのコンピュータのネットワーク設定（アドレス、サブネットマスクなど）を確認することができます。

参考２）192.168 ではじまるアドレスはクラス C と呼ばれており、通常、254 台までの機器を接続できます。IPv4 のアドレスクラスやサブネットマスクについての詳細は他のインターネットに関する成書を参照してください。

ネットワークの隔離

上記の原理により、異なるアドレス空間をもったネットワークはデータの送受信ができません。たとえば、192.168.0.10 と 192.168.0.20 は通信できますが、192.168.0.10 と 192.168.100.10 では、通信ができません。（クラス C では、上位３つの数が一致する必要があります。）ここで両者のネットワークからデータ通信できるようにするためには、ネットワーク接続するコネクタを２つもち、相互に異なるアドレス設定ができるようにした機器が必要です。たとえば、ルーターなどはその代表的な機器の例です。

データゲートウェイの動作原理

隔離されたネットワーク（アドレス空間の異なるネットワーク）間ではデータの送受信ができませんから、ウィルスなどのマルウェアが隔離されたネットワーク経由で直接感染することはありません。

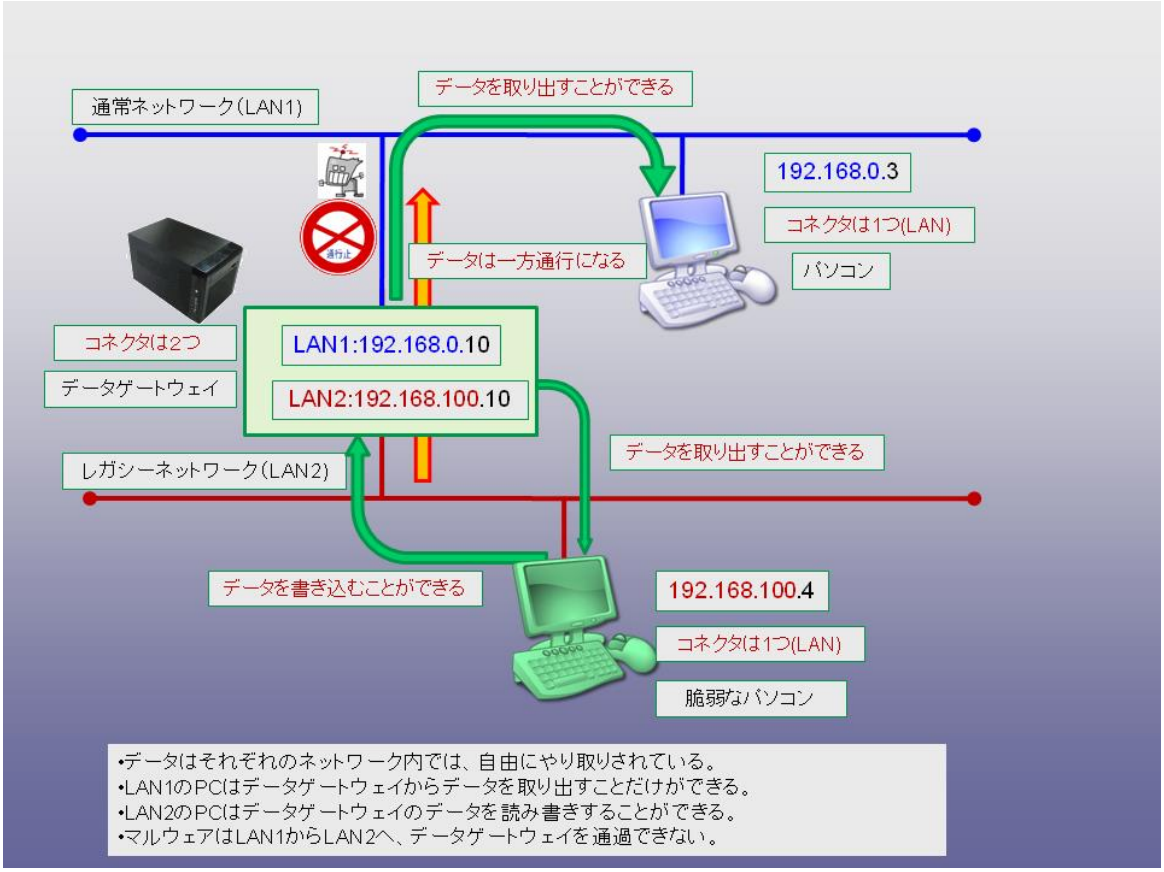
データゲートウェイはネットワーク接続のコネクタを２つそなえて、それぞれのネットワークからアクセス可能となるように作成されています。ただし、データの書き込みと読みだしの権限設定が一般ネットワーク側とレガシーネットワーク側では異なっています。

レガシーネットワーク側からは、「書き込み」「読み出し」「変更」ができますが、通常ネットワーク側からは、「読み出し」のみ可能となっています。この設定により、データゲートウェイを経由するデータはレガシーネットワーク側から一般ネットワーク側への一方通行になります。従って、万一、通常ネットワーク側にマルウェアが存在しても、データゲートウェイのデータフォルダを経由して、レガシーネットワーク側へ感染することはありません。

データゲートウェイはネットワークコネクタを２つもっており、通常ネットワークとレガシーネットワークにそれぞれ接続することで、ネットワーク間のデータ移動を可能としています。

データゲートウェイのネットワーク結線

*ネットワークコネクタなどのハードウェア仕様は、性能向上のため変更することがあります。



データゲートウェイによるデータ移動の概念図

データゲートウェイの仕様

通常仕様のデータゲートウェイは、異なるアドレス空間をもつネットワーク間で一方向でのみデータを受け渡すために設計されています。従って、「データの一時保管」を行うことを主たる目的として、主要部品の選定やシステムの設計をしております。レガシーネットワークのデータの保管場所として NAS のように利用することも可能ですが、データを長期保管する目的で使用するには、データ保管システムの機能（安全性、冗長性、可用性）が不十分です。

データをより安全に長期保管するための機能として、データゲートウェイに RAID システムを導入することも可能です。（別途、お見積もりいたします。）