

データゲートウェイ

システムの目的

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、マルウェア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

- 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памメール対策が不十分である。
 - スпамメールは「引っかけ」の温床になっている。
 - 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、ウイルスチェックは必須です。

これらの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。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 メモリなどのウイルスチェックをするのは大変複雑な作業となるため、實際上、仕事ができなくなってしまうことになりかねません。

- 十分なセキュリティ対策をしていないコンピュータはインターネット接続環境に置く事はできない。
- しかし、諸般の事情によりセキュリティ対策をすることができないコンピュータが存在する。
- セキュリティ対策をすることはできないが他のコンピュータとデータの共有することが必要である。

これらの互いに矛盾する要件をみだし、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)

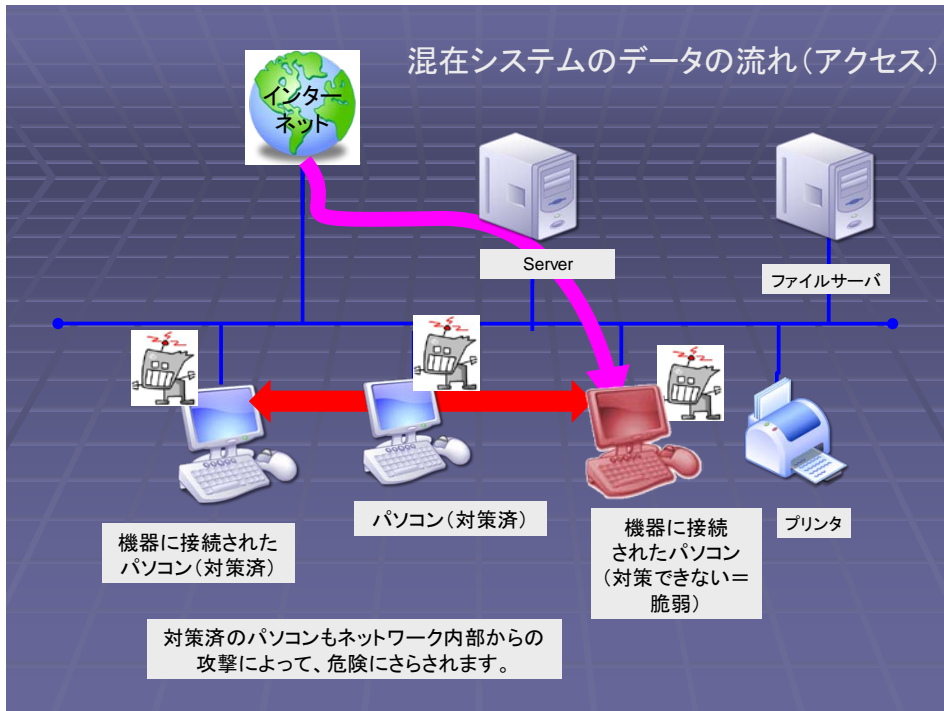
当財団で開発したデータゲートウェイシステムを採用する事で、古い OS (Windows 95, 98 NT など) を搭載した従来からのコンピュータ資源を安全・便利に利用し続ける事ができます。また、アップル・マッキントッシュのクラシック OS (MacOS 9 以前) も、利用する事ができます。

外観



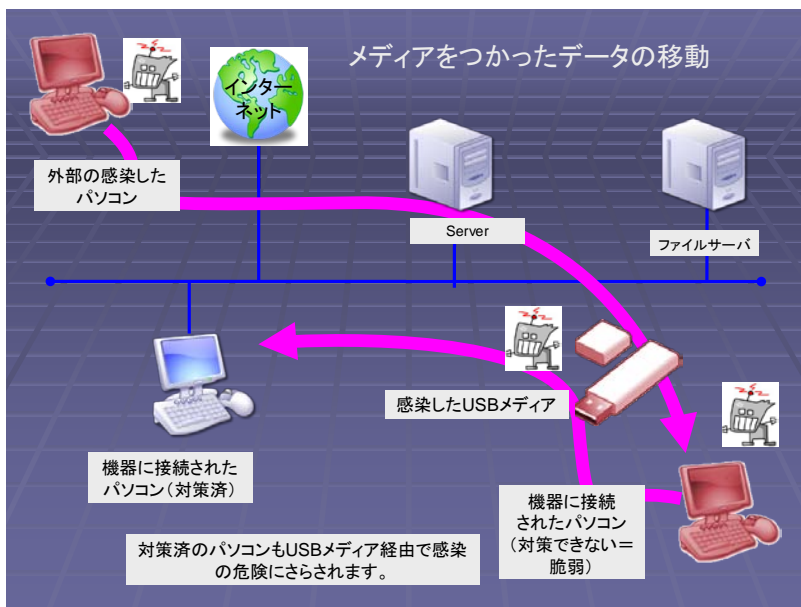
システムの筐体は製品向上のため、予告なく変更することがあります。

危険なコンピュータの利用形態



インターネットからもネットワークからもマルウェア感染の危険性があります。また、ネットワーク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。

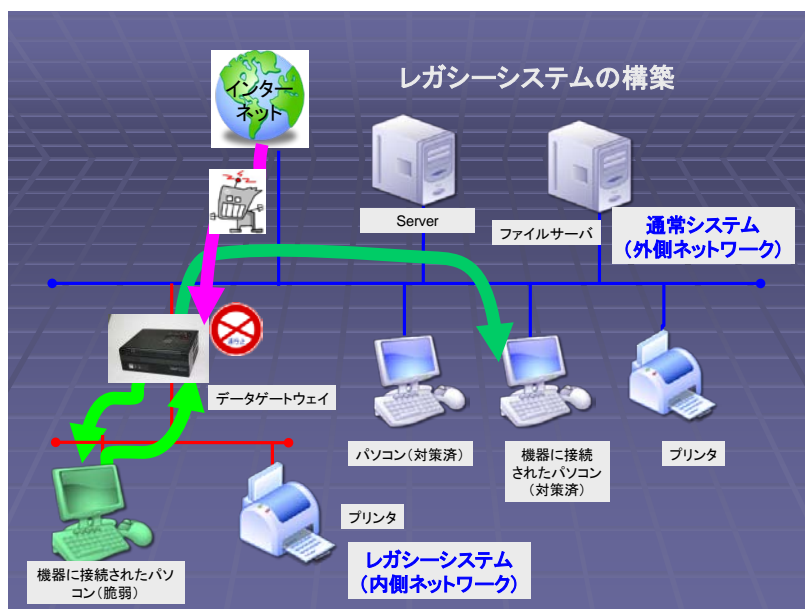
チェックが不完全なメディアは危険



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 メディアなどのウイルスチェックをしておく必要があります。

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。

データゲートウェイシステム 価格:85,000 円

納期:受注後2週間程度

設置について:

本システムには設置のためのマニュアルを添付しておりますが、ネットワークに関する知識が必要とされます。また、誤った設置を行った場合には、十分な安全性が確保できない場合もあります。

当財団から現地に出張しての設置をご希望の場合は別途お問い合わせください。