ファイナルウォールって何？

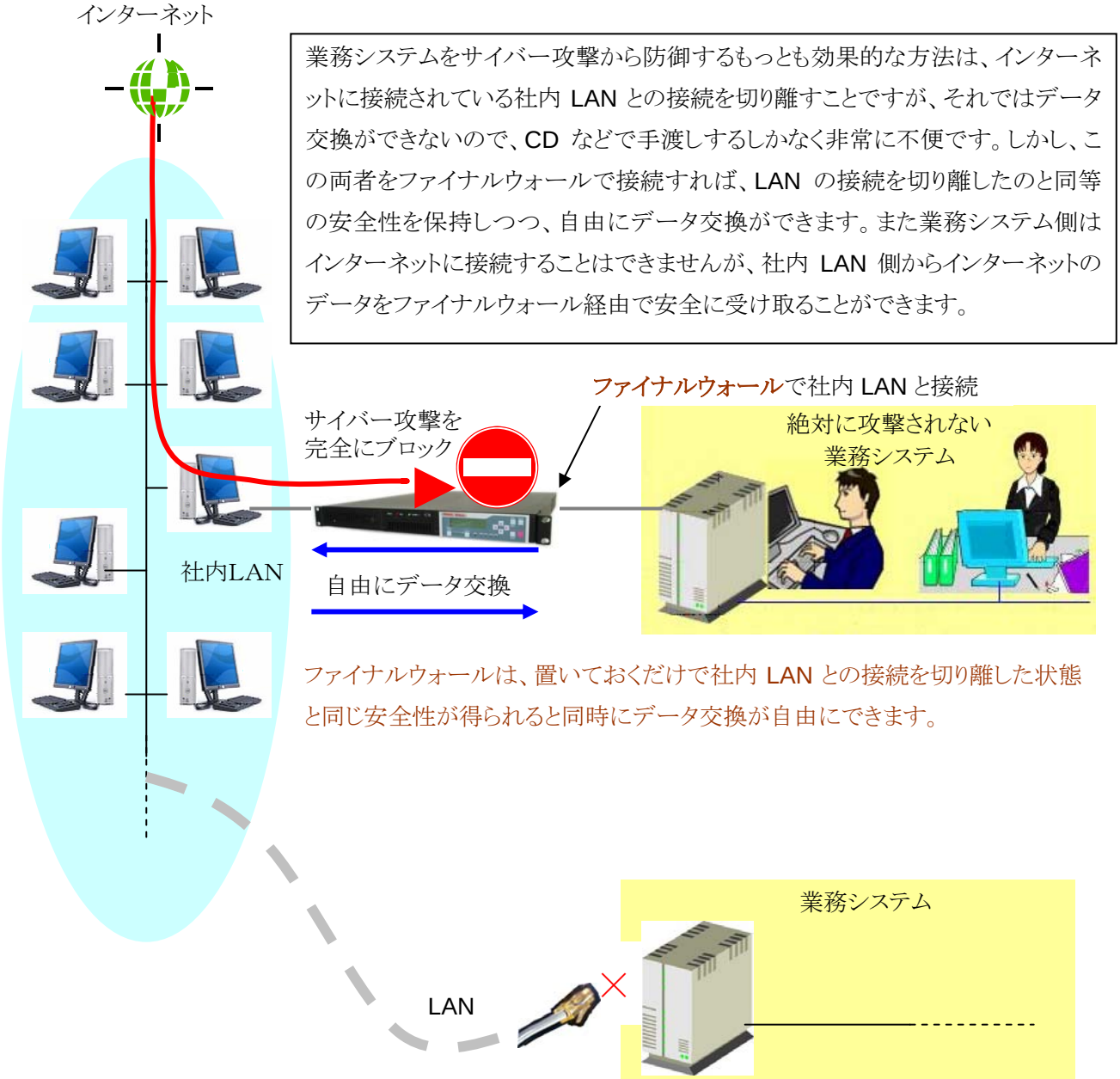
… ファイナルウォールは置いておくだけで安全、安心です …

… 特別な知識は必要ないのでどなたでも導入できます …

ファイナルウォールは、絶対に外部からの攻撃や不正アクセス（サイバー攻撃）をされてはならない、という使命を果たすためにNHKと共同で開発した、最も堅固なネットワーク防御装置です。

ファイナルウォールは、その名の通り『**最後の防御壁**』として一般の防御装置（ファイアウォール）では防ぎきれないサイバー攻撃を、根本的なレベルで（物理的に）強固にブロックしてくれます。

○ 社内LAN側からのサイバー攻撃を完全にブロックします。



業務システムをサイバー攻撃から防御するもっとも効果的な方法は、インターネットに接続されている社内 LAN との接続を切り離すことですが、それではデータ交換ができないので、CD などで手渡しするしかなく非常に不便です。しかし、この両者をファイナルウォールで接続すれば、LAN の接続を切り離したのと同等の安全性を保持しつつ、自由にデータ交換ができます。また業務システム側はインターネットに接続することはできませんが、社内 LAN 側からインターネットのデータをファイナルウォール経由で安全に受け取ることができます。

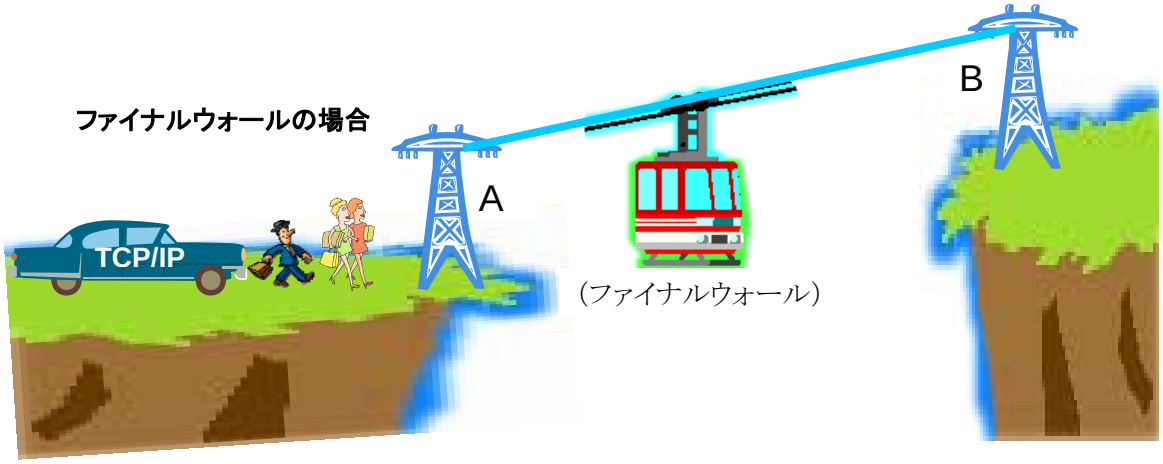
ファイナルウォールは、置いておくだけで社内 LAN との接続を切り離した状態と同じ安全性が得られると同時にデータ交換が自由にできます。

社内 LAN と業務システムを LAN で接続している場合、サイバー攻撃を完全に防ぐには LAN 接続を切り離すしかありませんが、それではデータ交換ができません。

ファイナルウォールはなぜ安全なの？

…　TCP/IPが通る道路がないので安全なのです　…

ファイナルウォールの最大の特長は、サイバー攻撃の常套手段であるTCP/IPが全く通じないということです。下の図に例えて説明すると、A地点からB地点に渡るにはファイナルウォールというケーブルカーに乗る以外に方法がない、ということです。つまり通信経路である道路がないのでTCP/IPという車では絶対に渡れません。このことは、一般のファイアウォールでは受けるおそれのあるB地点に対するTCP/IPによる侵入、攻撃がファイナルウォールの場合は根本的に不可能であることを意味します。なおこの図からもおわかりの通り、乗り換えの中に不審者（ウイルス、ワームなど）が混じっているおそれがありますが、その場合でもB地点からは何も持ち出すことはできません（一方通行）。このようにB地点に運ばれた不審者対策（ウイルス駆除など）は別途必要としますが、まずここではTCP/IPによる攻撃がまったく無効であるということと、Bからの持ち出し（漏洩）が不可能であることが保証されます。



ファイアウォールとはどうちがうの？

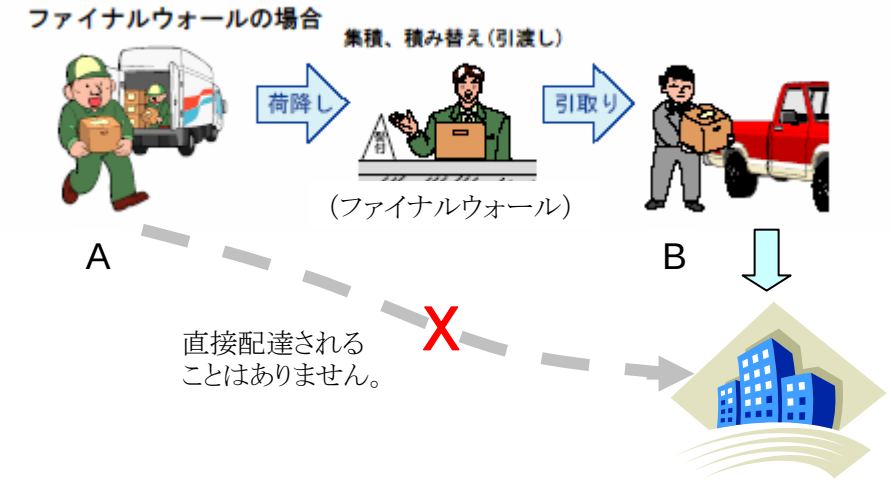
…　ファイナルウォールは通知なし郵便局止めなので配達されません（何が送りつけられても引き取りしない限り安全です）　…

【ファイアウォールの場合】

緊張関係にある国境の検問所を想定してください。検問所がファイアウォールです。ここを通過するにはパスポートや通行許可証が必要ですが、これらを偽造したり、さらには強行突破と検問所をすりぬけて侵入する手口は様々存在します。しかし「ファイナルウォール」に対しては、前項の図で理解していただいた通り、ファイアウォールと同じ手段（TCP/IP）で突破することは不可能です。

【ファイナルウォールの場合】

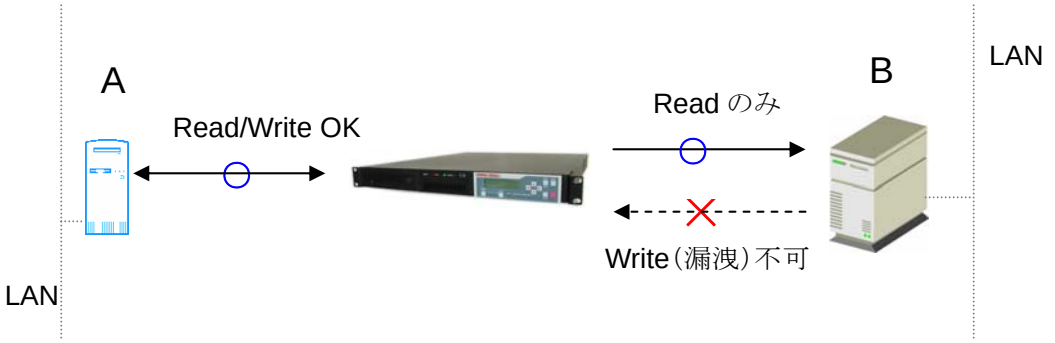
こちらは「通知なし郵便局止め」の子包み(荷物)を想像してください。郵便局がファイナルウォールです。Aから配送（書込み）された子包み（データ）は、郵便局（ファイナルウォール）に留め置かれ、Bから引取り（読み出し）があるまで決して配達されることはありません。つまり受け取り側の意思に反して不審な荷物(ウイルス、ワームなど)が送りつけられたとしても、引取りしない限り危険はありません。こうした仕組みは、この郵便子包みの例に限定されることなくユーザ側で自由に構築できます。



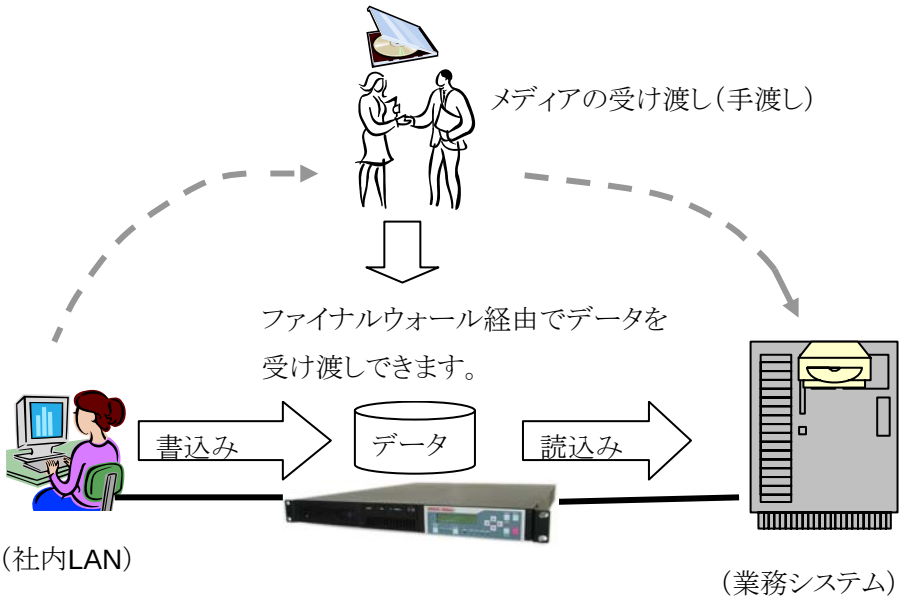
ファイナルウォールはなぜ安心なの？

…　ファイナルウォールは一方通行なので反対側から通過される（データが漏洩する）心配はありません　…

ファイナルウォールにおいて、データの転送方向は随時切り替えが可能ですが、指定した転送方向以外（逆方向）の転送ができない一方通行です。ですから必要に合わせて転送方向を指定して一方通行（たとえばA→B）にすることで、逆の転送（A←B）を完全に防止することができ、これを利用するとデータの漏洩を完全に防止することができます。



代表的な例として、業務システムと社内 LAN とのデータ交換において、安全のためこれまで CD などのメディアで手渡ししていた作業が、ファイナルウォールにより、手渡しの場合と同等の安全性と、LAN で接続した場合と同等の利便性が得られます。ファイナルウォールは一方通行なので、たとえば下の図の場合、業務システムのデータが社内 LAN 側に持ち出される（漏洩する）危険はありません。もちろん業務システムのデータを社内 LAN に受け渡す場合も、業務システム内にスパイがいない限り安心です。



ファイナルウォールはどう操作するの？

… 電源を入れるだけで2台のPCからアクセスできます …

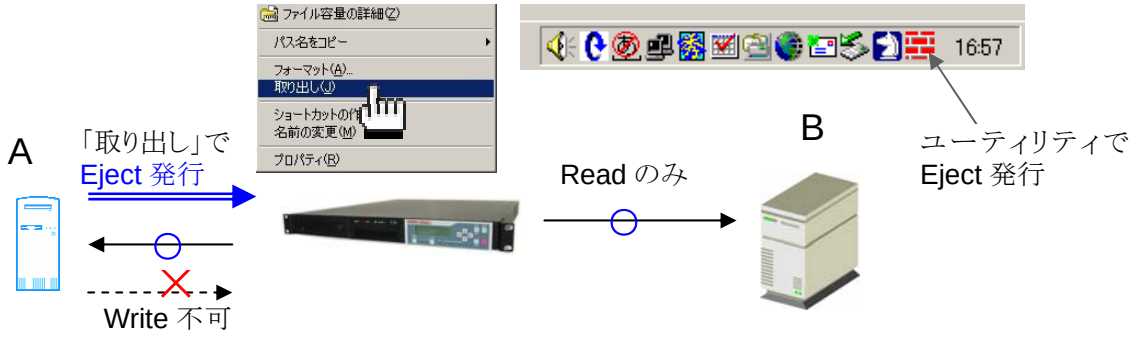
… イジェクト（Eject）操作で転送方向が切り替わります …

【起動時の状態】

A 側が読み書き（Read/Write）可能で B 側は読み取りのみ可能（Read のみ Write 不可）です。

【転送方向を切り替える場合】

ファイナルウォールは CD などと同じ大容量リムーバブルメディアとして認識されます。まず A 側でファイナルウォールに対して「Eject」を発行して書き込みの権利を放棄します。Eject はマイコンピュータの「取り出し」、もしくは付属のユーティリティプログラムから手動で、またはバッチプログラムなどから付属の専用サービスプログラムを呼び出すことにより発行できます（自動化できます）。



A 側が読み書き（Read/Write）可能状態で Eject を発行すると、書き込みの権利を放棄したことになり、A 側は Read のみ可能な状態（Write 不可）になります。B 側はそのまま。

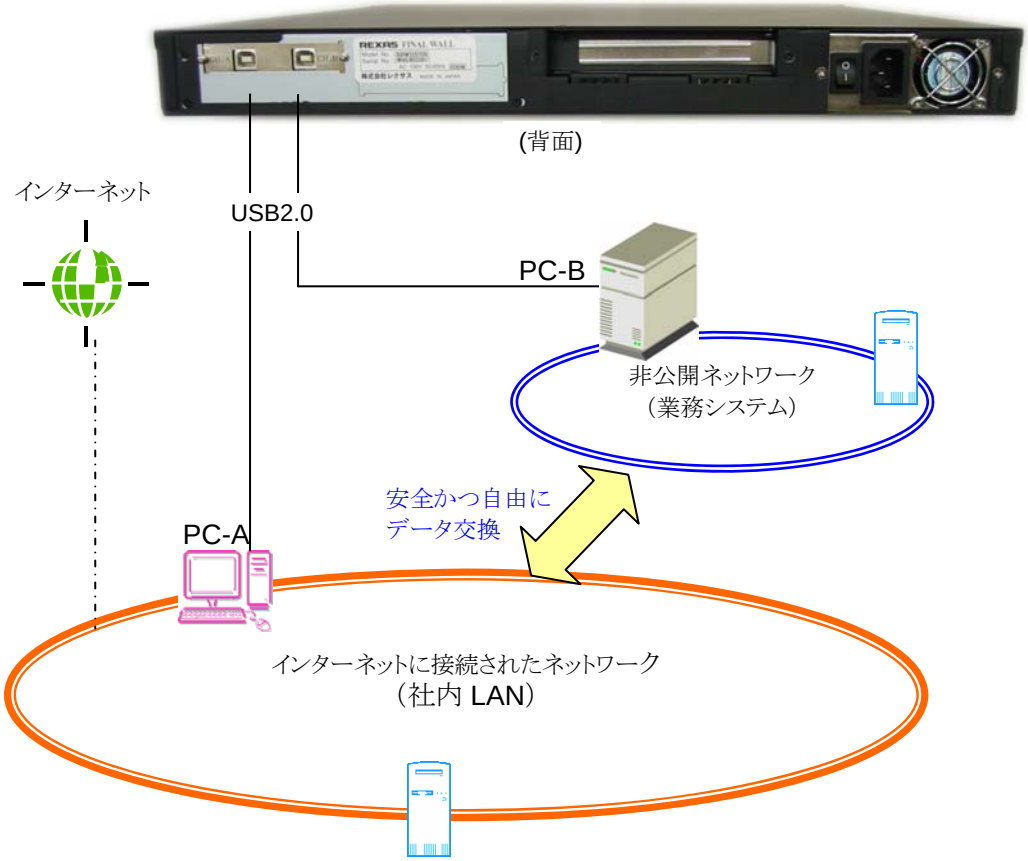
A 側が書き込みの権利を放棄した状態（Read のみ可能な状態）で B 側が Eject を発行すると、発行した側（B 側）が書き込みの権利を獲得することができます。以後この繰り返しで随時転送方向を切り替えることができます。

相手（A 側）が Read のみ可能な状態で B 側が Eject を発行すると B 側は読み書き（Read/Write）可能になります。

ファイナルウォールはどうつなぐの？

… 2 つのシステム間を USB で接続するだけで特別なスキルは必要ないので
どなたでも導入できます …

絶対に攻撃されてはならない業務システムと、社内 LAN それぞれの PC1 台（PC-B と PC-A）をファイナルウォールに USB で接続するだけで OK です。



☆ ファイナルウォールは NHK が認めた世界的にも類のない
究極のサイバー攻撃防御装置です。

ファイナルウォールはNHKのためだけのものではなく、みんなの財産です。
あなたの会社に役立てていただくために無償で導入指導、コンサルティングいたします。
どんなことでも気軽にお問い合わせください。

株式会社 レクサス
〒213-0012
神奈川県川崎市高津区坂戸3-2-1
かながわサイエンスパーク西棟6F
TEL：044-844-2255　FAX：044-844-7720
Home Page: http://www.rexas.co.jp/
e-mail: info@rexas.co.jp

REXAS