



# Crossway<sup>®</sup>/データブリッジ

## ネットワーク分離環境での 安全なデータ受け渡し



データ持ち出し防止



利用ログの取得



不正利用の防止

インターネット接続環境

機密情報取扱い環境 (閉鎖ネットワーク)

# 機密情報の不正持ち出し、この1台

重要な情報資産を不正利用や漏えいから守るためには、機密情報を扱うネットワークとインターネットにつながるネットワークを分離する方法が有効です。しかし、分離されたネットワーク間でデータを受け渡す場合、USBメモリを利用すると外部に情報を不正に持ち出されてしまうリスクがあります。Crossway/データブリッジは、分離されたネットワーク上の端末間をUSBケーブルでつなぎ、その間だけデータの受け渡しを可能にします。さらに、簡単な操作で利用ができるので、業務の効率化も実現します。

## データ受け渡しの必要性

- ネットワーク分離は、安全性の高い標的型攻撃対策
- ネットワーク分離環境でも、業務上データの受け渡しは必要

## 受け渡し方法の問題点

- USBメモリ：持ち出や紛失による情報漏えいリスクが高く、運用が煩雑
- 中間サーバ：高額で導入に手間がかかる。運用も大変

## なぜデータブリッジが必要？

データブリッジなら、ネットワーク分離環境の高いセキュリティを損なうことなく、手軽で効率的にデータを受け渡します



## データブリッジとは？

- ネットワークが分離された環境で、安全にデータを受け渡す機器
- USBケーブルで端末同士を接続している間だけ、データの受け渡しが可能
- ケーブルを抜く、電源オフなどで、データブリッジからデータは自動消去

## 機密情報保持ネットワーク

送信  
端末



Crossway/データブリッジに  
ファイルを送る

持ち出しや紛失による  
情報漏えいを防ぎ  
安全にデータ流通を制御

Crossway®/データブリッジ



不正利用  
防止



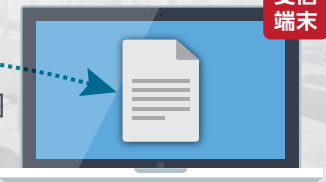
ログ  
取得



利用者  
制限

## インターネット接続系ネットワーク

受信  
端末



Crossway/データブリッジから  
ファイルを受け取る

## 手動転送と自動転送、選べる2つのタイプ

### 手動転送タイプ

USBメモリの代替として、日々の業務の中でスポット的なデータの受け渡しで活用いただけます。

送信端末にて、ファイルを専用アプリケーションにドラッグ&ドロップすることでファイルを転送。受信端末にてリムーバブルディスク領域からファイルを任意の場所にコピーすることで受け取り完了です。



### 自動転送タイプ

ネットワーク間で定期的なデータの受け渡しが必要な場合に有効です。

送信側の任意フォルダに配置されたファイルを、自動的に受信側のフォルダにファイルを転送します。これによりネットワーク間のシームレスな業務連携を実現します。

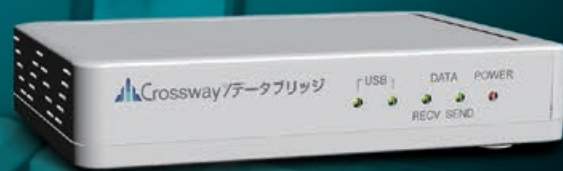


# でしっかり防ぎます。



ネットワーク分離環境のセキュアなデータ受け渡し製品

## Crossway®/データブリッジ



### 充実した機能で情報漏えいリスクを最小化



#### データ持ち出し防止

- USBケーブルの抜き去り、電源オフなどで自動的にデータが消去
- 設定時間によりデータが自動削除

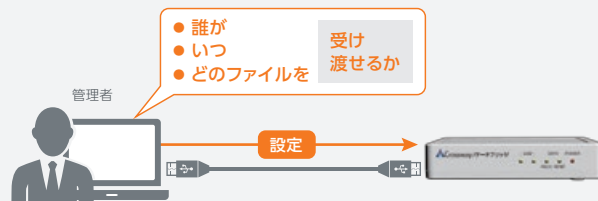
持ち出されたとしても、データが機器に残っていないため、データの不正な持ち出しを防止できます。



#### 不正利用の防止

- 利用できるユーザや端末をあらかじめ設定
- 利用可能な時間や、受け渡し可能なファイルを制御

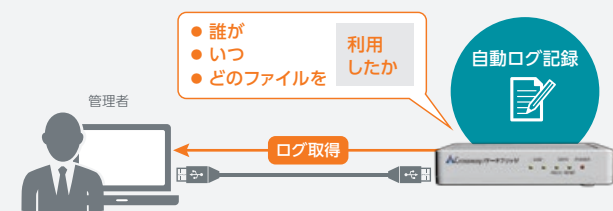
受け渡し可能なファイルの条件を事前に制御できるため、不正利用を防止できます。



#### 利用ログの自動記録

- 誰が、いつ、どのファイルを渡したのか、ファイル送信時に自動でログ記録

ログにより、ファイルを渡した記録が確認できるため、不正利用を抑制し、万が一の際、追跡ができます。



#### ウイルスチェック (オプション)

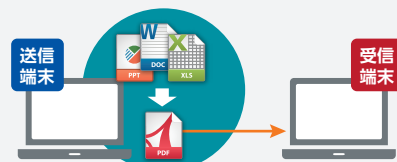
- データブリッジに送信されたファイルをウイルスチェック
- データブリッジ内の「ESET File Security」にてファイルのウイルスチェックを実施。ウイルス検出時は、ファイルは送信せず、ユーザに通知します。



### その他の機能

#### ファイルの簡易無害化

送信端末の印刷機能を利用し、送信したいデータをPDFファイルに変換。無害化して送信できます。



#### 一方通行

送信端末から受信端末へデータの流れを制限し、セキュリティポリシーの異なるデータの混在やウイルスの逆流を防ぎます。



#### IPパケット遮断

IPパケットを通さないため完全なネットワーク分離を実現します。これによりIPによるウイルス侵入を防ぐ効果もあります。



## 主な利用シーン

### CASE 1

#### 自治体

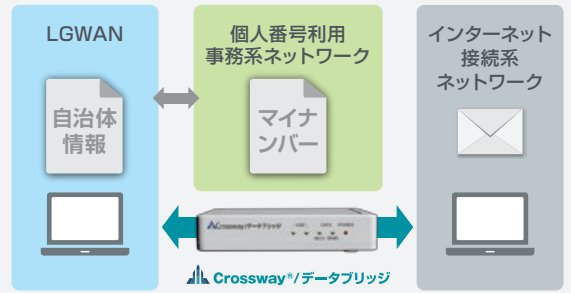


#### 課題

- 三層のネットワーク分離をしたが、ネットワークを越えてデータの受け渡しが必要
- USBメモリはリスクが高く、中間サーバは高額

#### 解決

- 利用後自動消去などで、セキュリティ高く分離ネットワークのデータ受け渡しを実現
- 高いセキュリティのまま、簡単に導入、利用ができる



### CASE 2

#### 金融機関



#### 課題

- 金融ネットワーク系と自行業務系でネットワークの完全分離が必要
- 取引情報の流出を防ぐため、USBメモリなどによるデータ受け渡しは禁止されている

#### 解決

- 利用者を制御してデータを受け渡し
- 紙やCDの利用をなくし、データ受け渡しの事務負担を軽減・効率化



### CASE 3

#### 機密情報 取り扱い 部署

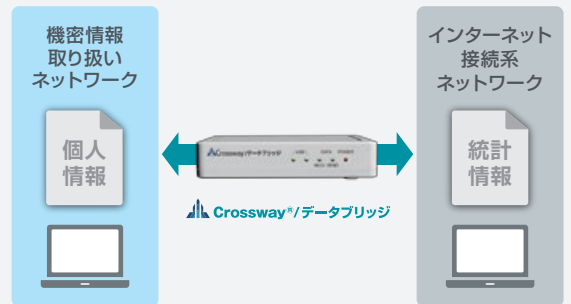


#### 課題

- 顧客情報システムや基幹システムはネットワーク分離をしているが、統計データ作成のためデータの受け渡しが必要
- USBメモリを利用しているが、顧客情報の持ち出しが心配

#### 解決

- 機器の持ち出しができないため、情報流出を最低限に抑止
- 難しい設定もなく、すぐに導入できる。人手を介さず自動でデータの流通もできる



## 製品仕様 / 動作環境

製品名		データブリッジ (手動転送タイプ)	データブリッジ AT (自動転送タイプ)
ハードウェア仕様	重量	275g	
	寸法	155×105×30 (mm)	
性能	データ転送速度	～8MB/Sec	
	データ保存容量	6.85GB	
	ログ容量	3GB	
端末条件	OS	Windows XP SP3、Windows 7 SP1、Windows 8.1、Windows 10、Windows Server 2012 R2	
	端末ハードウェア条件	<ul style="list-style-type: none"> <li>● CPU： 1GHz以上</li> <li>● HDD： 1GB以上空き容量があること</li> <li>● メモリ： 1GB以上</li> <li>● I/O： USB2.0以上に対応していること</li> </ul>	



本製品は、NTTアクセスサービスシステム研究所の技術を用いることでクライアント端末間の安全かつ簡易なデータ流通を実現します。このマークはNTTの研究所技術を活用していることを表しています。

日本電信電話株式会社



NTTテクノクロス株式会社  
ビジネスソリューション事業部

TEL.03-5347-8026

E-mail : databridge@cs.ntt-tx.co.jp

製品URL : <https://www.ntt-tx.co.jp/products/crossway/databridge/>

URL : <https://www.ntt-tx.co.jp/>

※お問い合わせは、販売代理店またはNTTテクノクロスの営業まで。