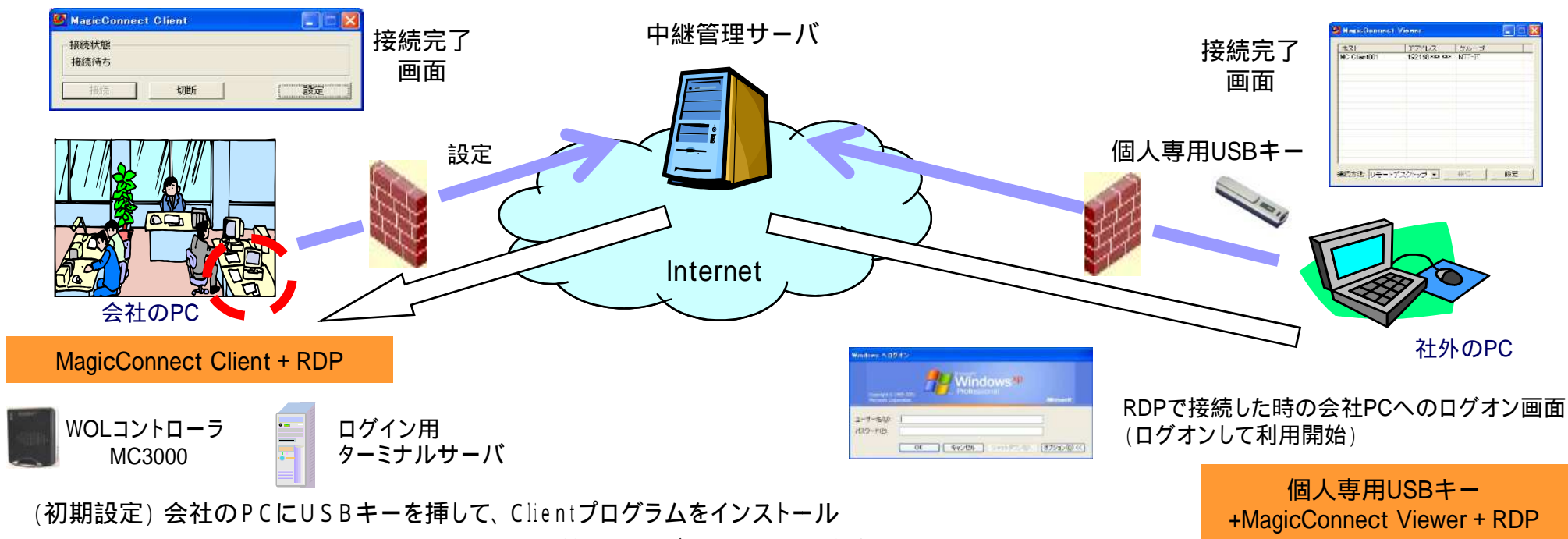


# マジックコネクト(ユビキタスVPN)の概要

個人専用USBキーを1本携帯し、手元のWindowsPCに挿すだけで、世界中どこからでも、会社のPCにVPN接続が可能です。RDPなどで、会社PCの画面を手元PCに表示させ、あたかも手元に会社PCがあるかのように業務の遂行が可能です。

- 簡単:** ・Web閲覧環境があればUSBキーを挿すだけ  
・既設のファイアウォール/ルータの設定変更が不要
- 安全:** ・個人専用USBキーにより、なりすまし利用防止  
・マジックコネクト(ハートID)と利用アプリによる2重の認証と暗号化  
・IPアドレス、MACアドレスによるPCの限定も可能  
・USBキー紛失時は携帯電話で即時ロックが可能

- 便利:** ・ファイルを持ち出すことなく業務が可能  
・メールやファイルを一元的に管理  
・ノートPCの盗難やWinnyなどによる情報流出の不安解消  
・手元のPCには、会社PCのアプリが不要



(初期設定) 会社のPCにUSBキーを挿して、Clientプログラムをインストール

MagicConnect Clientを起動して、中継管理サーバに接続して設定完了

個人専用USBキーを手元PCに挿してMagicConnect Viewerを起動し、中継管理サーバに接続  
接続する会社のPCを選択してRDPを起動し、手元PCから会社PCを操作

# マジックコネクットの技術と接続形態

## 既存リモートアクセスの課題

- ・ RASが低速度
- ・ IPsec VPN  
ファイルの持ち出し必要  
利用環境の制約
- ・ SSL-VPN  
使用可能APの制約  
成りすましの危険

・テレワーク、遠隔保守

## 最新技術

- ・ 認証技術
- ・ SSL/httpトンネリング技術
- ・ リモートデスクトップ技術 等

## マジックコネクット

- ・ 高速NW対応
- ・ ファイルの持ち出し禁止
- ・ Web環境で広範囲に利用可能
- ・ 社内PCの全てのAPが使用可能
- ・ 成りすましは不可能

安全、簡単、ユビキタス  
最新のリモートアクセス

テレワーク、遠隔保守  
SBC(サーバベースコンピューティング)  
通勤困難時の事業継続

## 接続形態(マジックコネクット対PC)

### 1対1接続

ユーザが会社の自分のPCにアクセス  
標準アカウントを使用

### 1対N接続

複数の機器を遠隔保守  
操作PC専用、対象機器専用のアカウントを利用し、  
グループ化オプションで接続

### N対1接続

複数のユーザが1台の共用サーバにアクセス  
操作PC専用、対象機器専用のアカウントを利用し、  
グループ化オプションで接続

### N対M接続

ユーザによりアクセスできるPCやサーバが異なる

# マジックコネクトと既存VPNとの比較

## 《マジックコネクト》



安全

仮想的に社内の自席に移動

ABC

社外へデスクトップ画面のみを転送

社内へキーボード、マウス情報を転送

社外からのウイルス感染 **ブロック**

自席PCにアクセス

会社のファイルが  
保存されない

会社のアプリが**不要**

PCの紛失でも安全

443番または80番出側  
ポート以外不要、専用機器  
不要 / 設定不要

社外 ←→ 社内

## 《既存VPN》



不安

社内LANが社外に張り出し

社外へ社内のファイルを転送

社外からのウイルス感染

社内LANへフルアクセス

会社のファイルが  
保存される

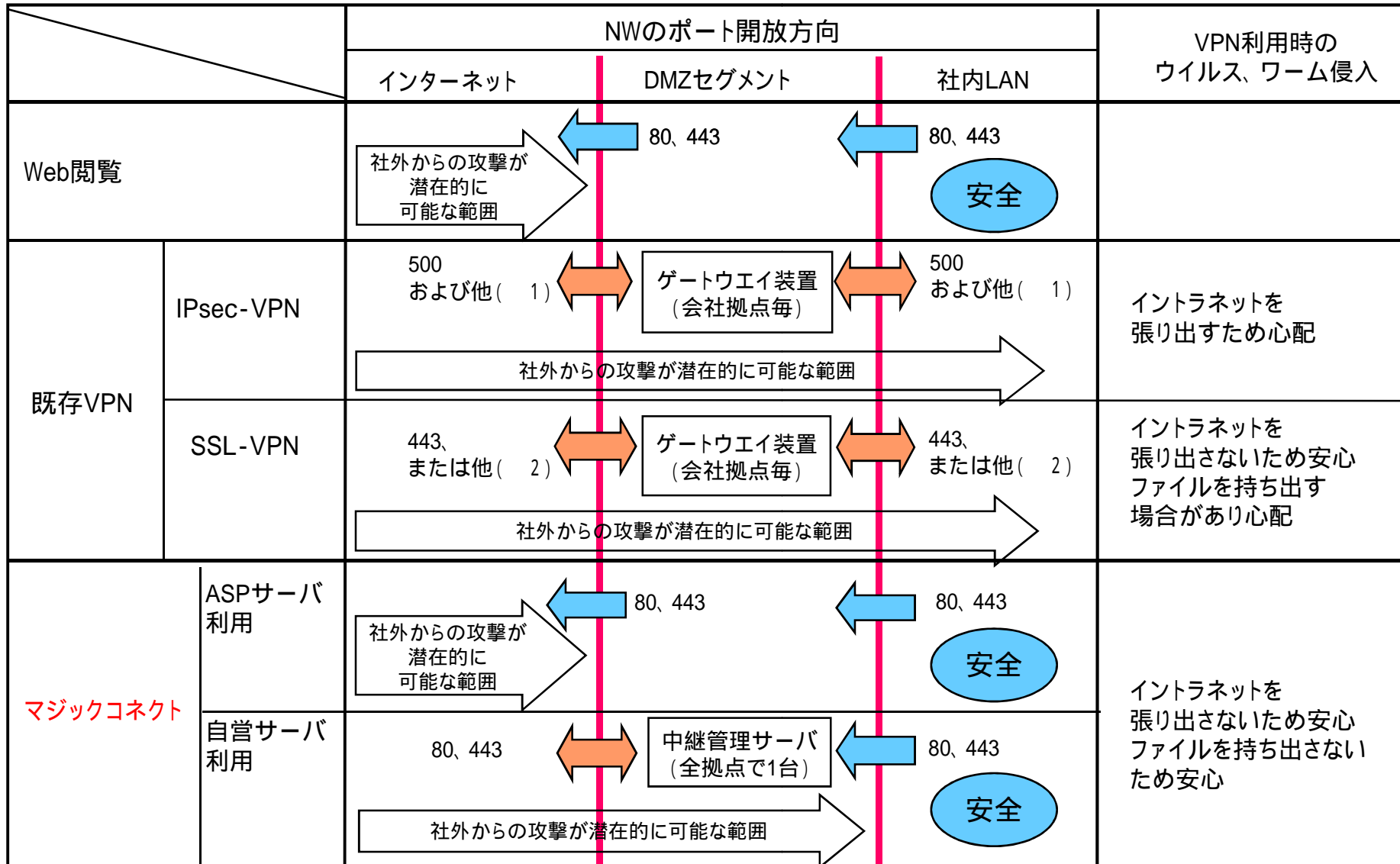
会社のアプリ**必要**

PCの紛失が危険

複数のポート解放が必要、専用機器必要 / 設定必要

# マジックコネクットのNWセキュリティと既存VPNとの比較

マジックコネクットは、社外からのポートを開放せず、イントラネットを張り出さない、もっとも安全なVPN



1) 製品により異なる

2) クライアントソフトが独自の場合