

ランサムウェアに備える アイオーデータ NASソリューション

ランサムウェアへの対処

ランサムウェアへの対処は大きく分けて2種類

①発生を未然に防ぐセキュリティ対策



セキュリティアプライアンス



②万が一の被害から守るデータ保全

I-O DATA

NASソリューション

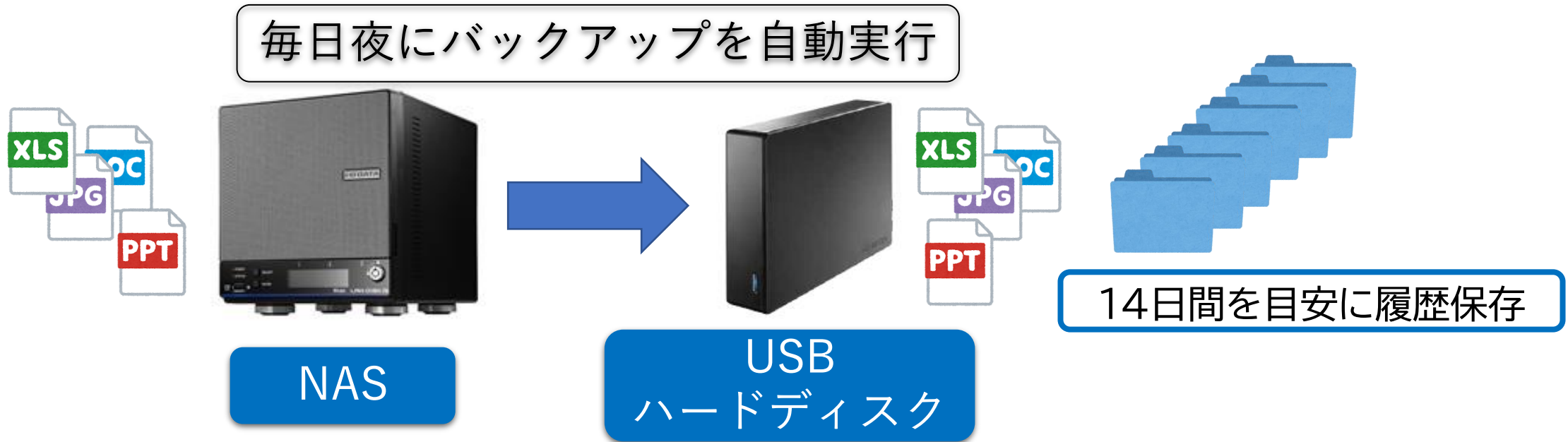


データ保全の条件

1. 被害を受ける前に保存されたデータであること
2. 保存されているデータがランサムウェア被害を受けない(受けていない)状態であること

ランサムウェアからデータを守るバックアップ構成

USBハードディスクへ毎日自動で履歴差分バックアップを行い、世代管理を行うことで、ランサムウェア対策を実現できます。



暗号化からデータを守る①（複数日分データ保存）

履歴差分バックアップで世代管理を行っているため、
万が一の感染時も、バックアップから日付を遡って感染前のデータに復元できます



バックアップは製品故障やファイル誤消去にも有効

暗号化からデータを守る②（ネットワークから隔離）

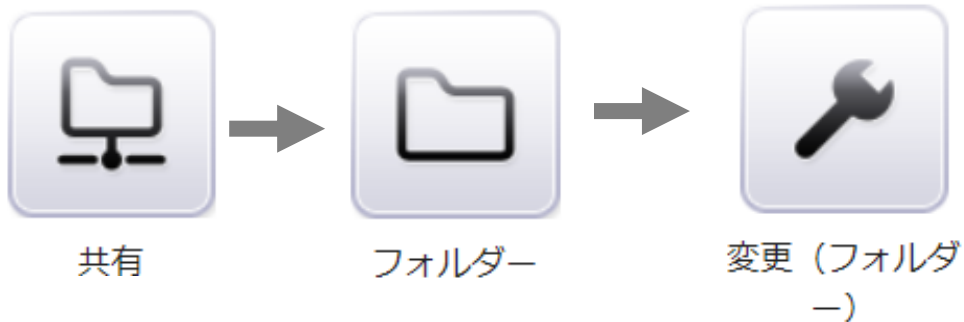
バックアップ先ハードディスクのファイル共有無効化で、
ランサムウェアに感染したPCからのアクセスを防いで安全！



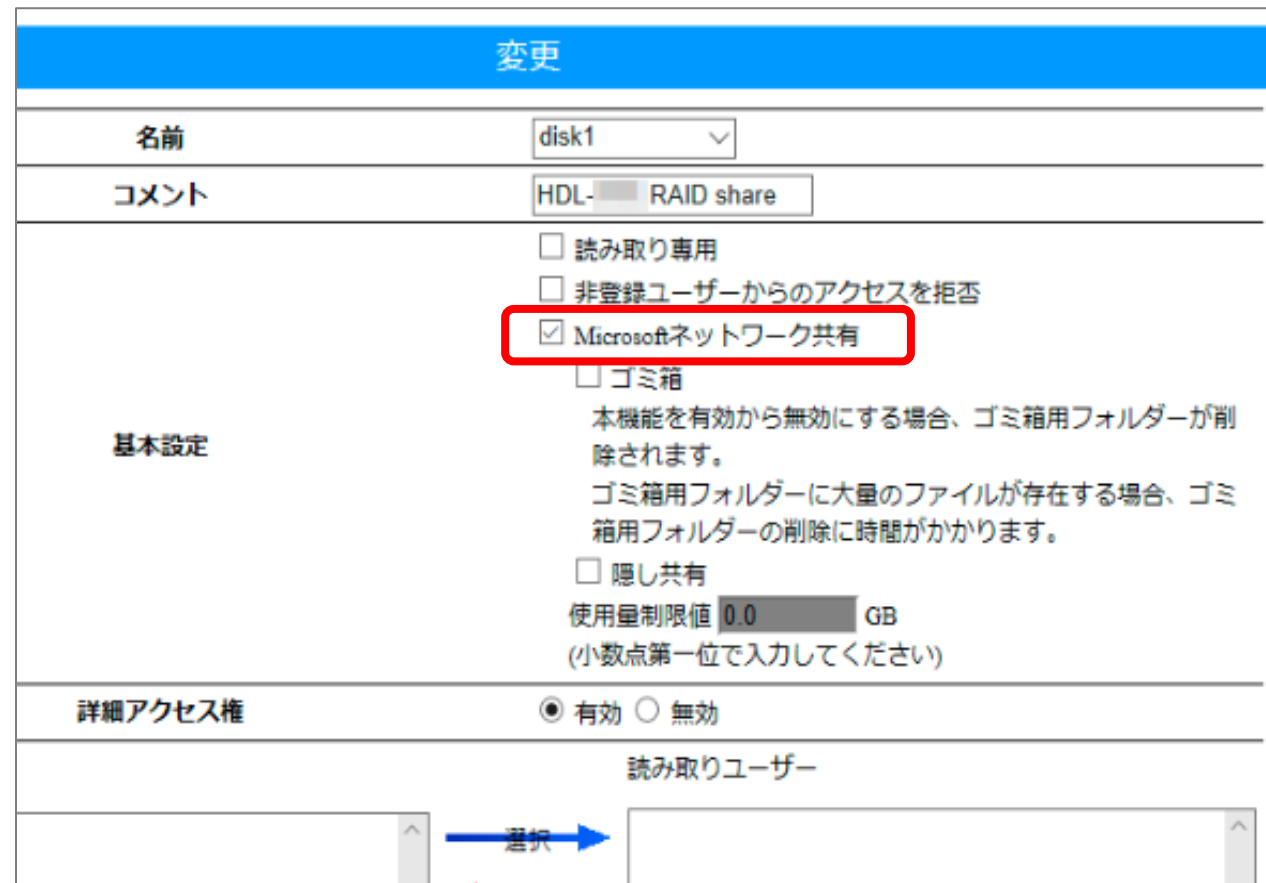
① NASの設定画面にログイン



② 変更するフォルダー(USB HDD)を選択

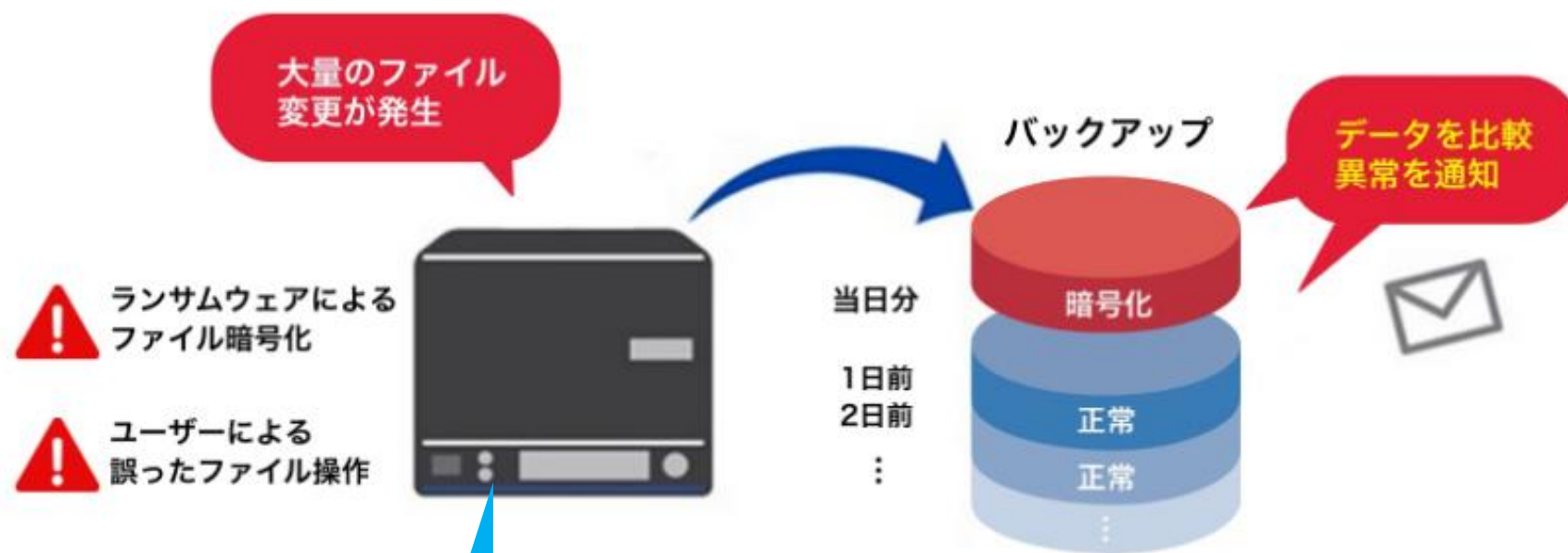


③ ファイル共有を無効化する



暗号化からデータを守る③（不正ファイル操作検知機能）

法人・企業向けNAS（Linuxベース OSモデル）



バックアップジョブ設定

オプション

チェックを入れる

- 実行後にシャットダウンする
- 強制フルコピー
- 多くのファイルに変更があった場合に通知する

アイオーのNASなら安心！

LAN DISK REBORN!

生まれ変わった LAN DISK (ランディスク) の「5つの安心」

安心 01.

業界最高レベル!

5年保証

安心 02.

物理障害を含む
復旧サービス付き

※条件等は以下説明欄を
ご確認ください

安心 03.

**有償保守
サービス**
を用意

安心 04.

5年保証を支える
独自保存技術

**拡張
ボリューム**

安心 05.

**安心管理サービス
を無償提供**

進化する明日へ Continue thinking

I-O DATA

安心安全な高セキュリティを実現 リモートアクセスの決定版 『テレワークテル』

株式会社アイ・オー・データ機器



リモートアクセスでの課題

■ リモートアクセスの準備

VPNを構築したいが
準備も設定も難しそう・・・



■ PCのセキュリティ対策

テレワークPCのセキュリティは
どう対策したらいいのか・・・



■ 会社での電話対応

外線電話対応のため
テレワークできない・・・



テレワークテルが解決します！

テレワークテル 特徴

特長1

難解な設定不要、ミスする心配のない簡単セットアップ！

セットアップは画面に従ってクリック・入力だけ。**設置作業者に特別なスキルは不要**です。

特長2

テレワークでも、社内と同じ使い勝手で効率的な仕事ができます！

L2延伸接続なので、NAS、複合機など会社のネットワーク機器が使えます。

特長3

自宅・外出先でも、社内と同じセキュリティポリシー運用ができるので安心！

テレワークでも**全ての通信がオフィスのUTMを経由**する安心設計です。

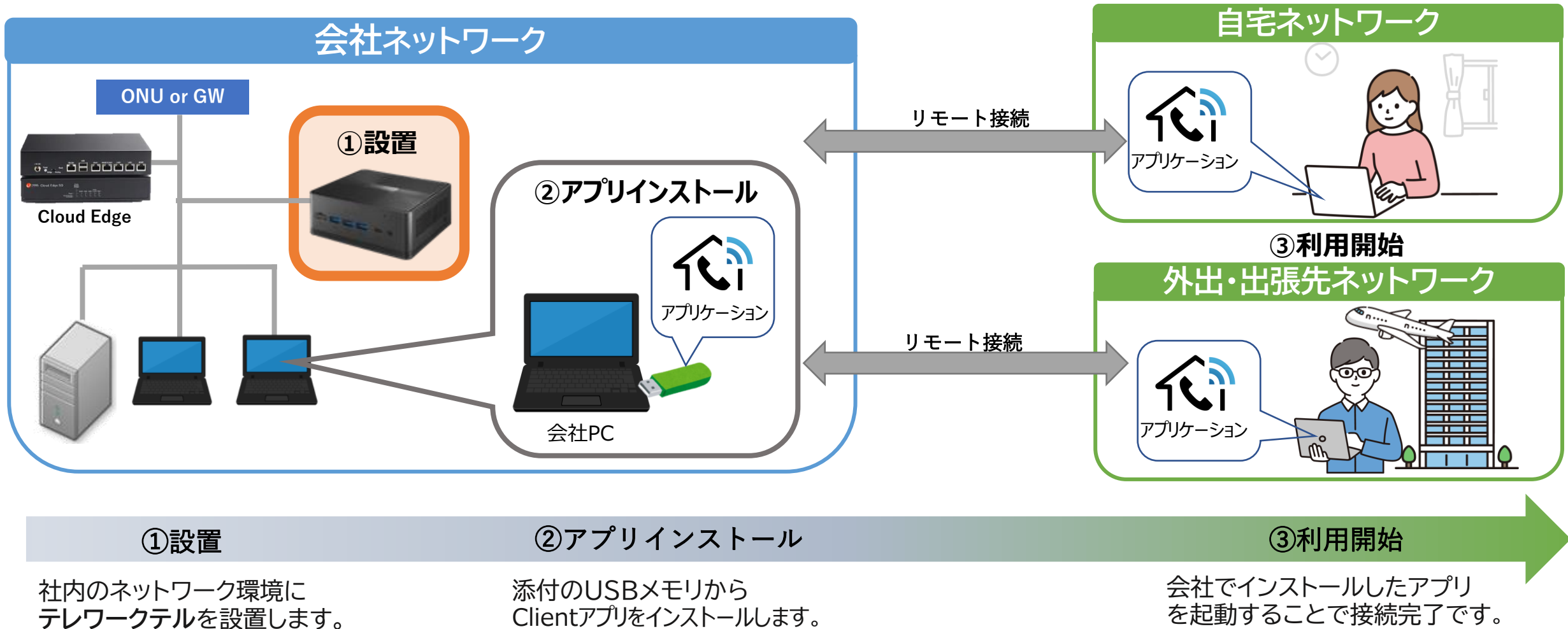
特長4

登録したパソコンしか繋げないので、一般的なVPNよりも高セキュリティ！

アイオー独自の**ZeroIP接続方式**が、悪意のある第三者から社内ネットワークを守ります。

特長1：簡単セットアップ

一般的なVPNのような**難しい設定や専門的なスキルは不要!**



①設置

社内のネットワーク環境に
テレワークテルを設置します。

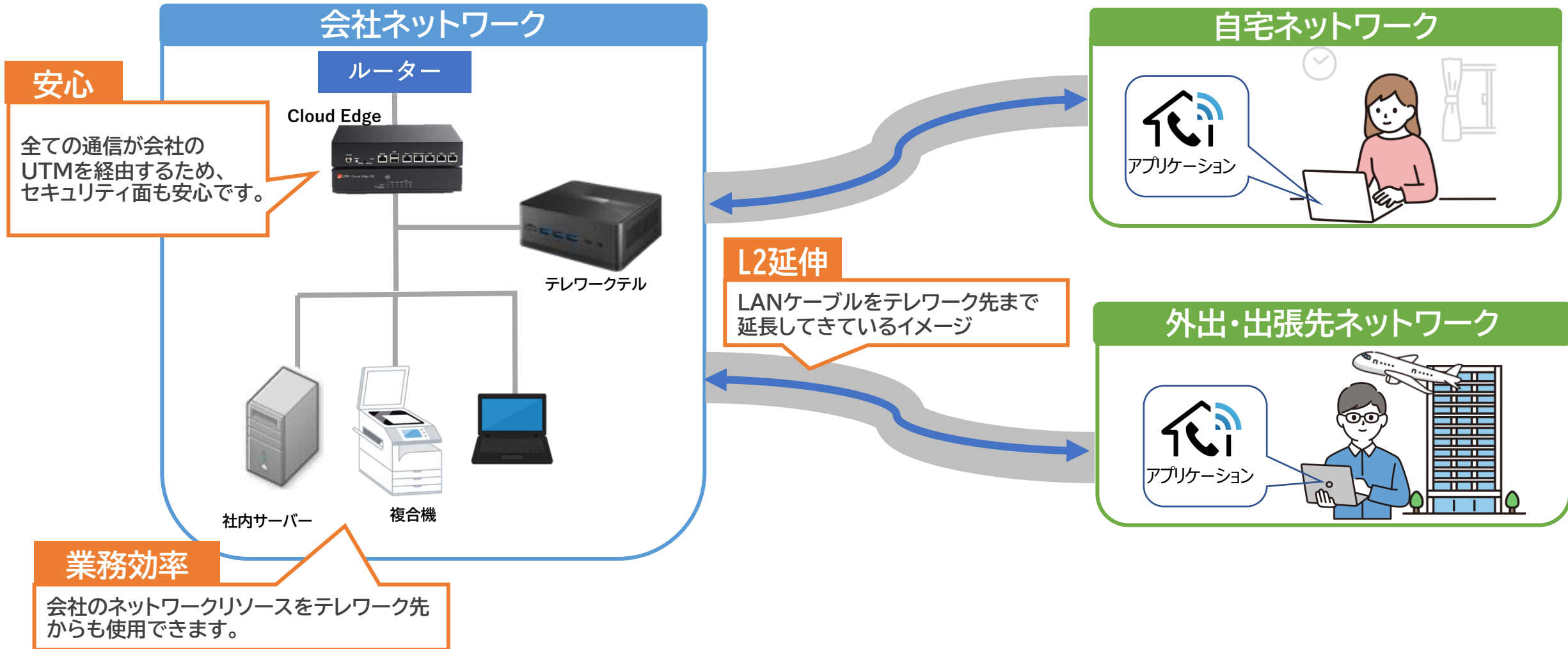
②アプリインストール

添付のUSBメモリから
Clientアプリをインストールします。

③利用開始

会社でインストールしたアプリ
を起動することで接続完了です。

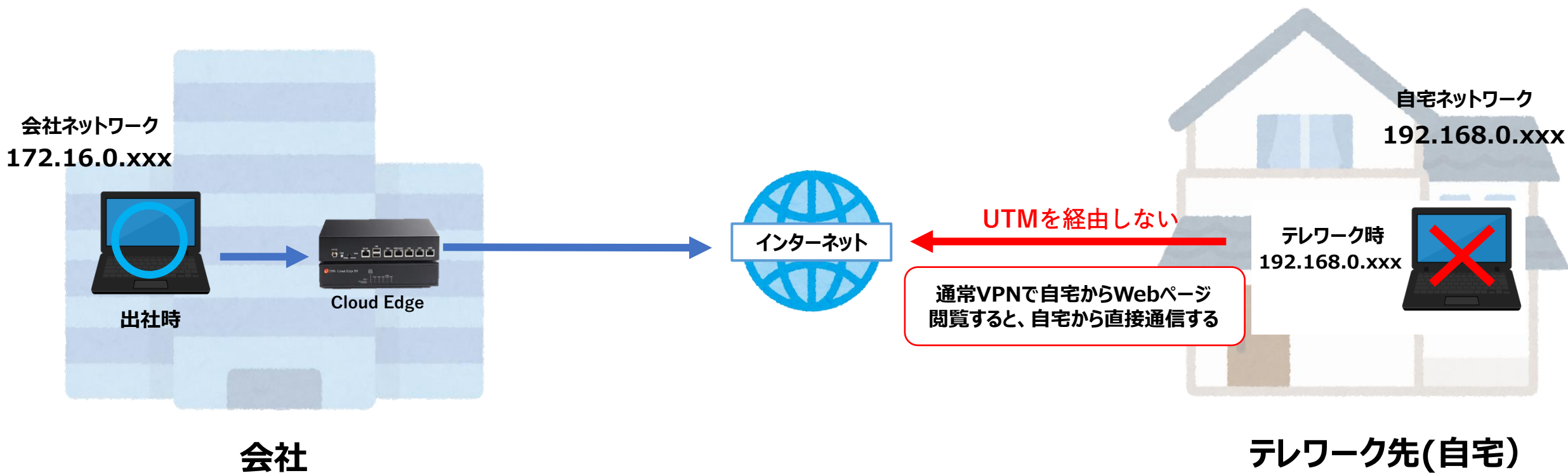
特長 2 : 「L2延伸」 が実現する安心と業務効率



特長3：社内と同じセキュリティポリシーでの運用ができる

課題

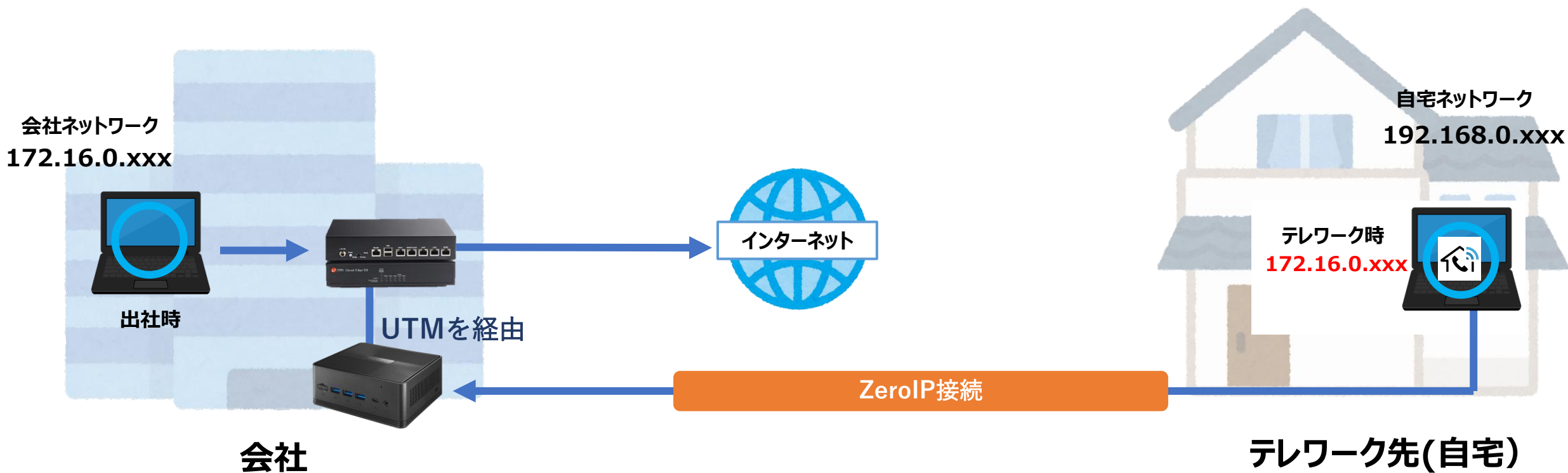
今までのVPNソリューションでは自宅からのインターネットアクセス時に、会社のUTMが使われず、テレワーク中のPCのセキュリティがまもられていなかった。



特長3：社内と同じセキュリティポリシーでの運用ができる

社内にテレワークテルを設置するだけで解決！！！！

自宅からの通信は全て会社のUTMを経由するので、高セキュリティ！



特長4：登録されたPCしか接続できないZeroIP接続

【 ZeroIP 3つの特徴 】

特長2. ハードウェア限定

添付のUSBメモリからのアプリインストール時に、クライアントPCの情報をテレワークテルに送信。当該クライアントPCからしか接続できない。



特長3. ホワイトリスト

クライアントPCから送られてきた情報をホワイトリストに記録。
紛失・盗難時に当該情報を参照し、該当するクライアントPCの接続を無効化できる。

クライアントPC情報



アプリケーション

特長1. 設定用USBキー

添付のUSBメモリを起動したテレワークテル本体に接続して初めて鍵として成立する。
テレワークテル本体に差したUSBメモリからのアプリインストールでないとそのテレワークテルに接続できない。

ホワイトリスト

teleworktel - リモートデスクトップ接続

http://127.0.0.1/TBuserManage

ユーザー一覧

仮想HUB選択 VPN

ユーザー一覧

チェック	ユーザ名	ログイン回数	最終ログイン日時	転送バイト数	転送バケット数
<input type="checkbox"/>	hase	3	2021年12月11日(土) 10時 0分 0秒	57,592,307	819,666
<input type="checkbox"/>	iyoshida	1	2021年12月10日(金) 11時 1分 9秒	39,089,125	2,128,008
<input type="checkbox"/>	Nakajima	2	2021年12月10日(金) 18時45分15秒	2,944,399	918,856
<input type="checkbox"/>	sasaki	1	2021年12月10日(金) 18時25分21秒	4,135,087	1,576,754
<input type="checkbox"/>	teraryu2	1	2021年12月10日(金) 10時24分13秒	9,100,340	907,920
<input type="checkbox"/>	tsuburaya	8	2021年12月10日(金) 18時31分12秒	91,757,403	1,091,707

削除対象ユーザをチェックしてください

削除実行

MACアドレス一覧

状態	MACアドレス1	MACアドレス2	ユーザ名
有効			Nakajima
有効			tsuburaya
有効			iyoshida
有効			hase
有効			teraryu2
有効			sasaki

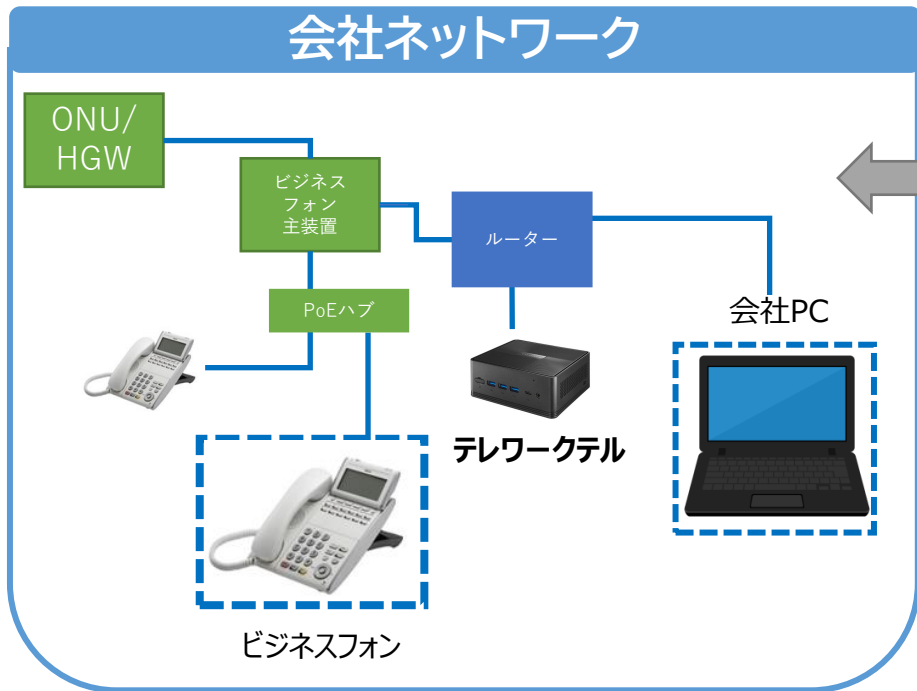
対象MACアドレスの状態を選択してください

状態切替実行

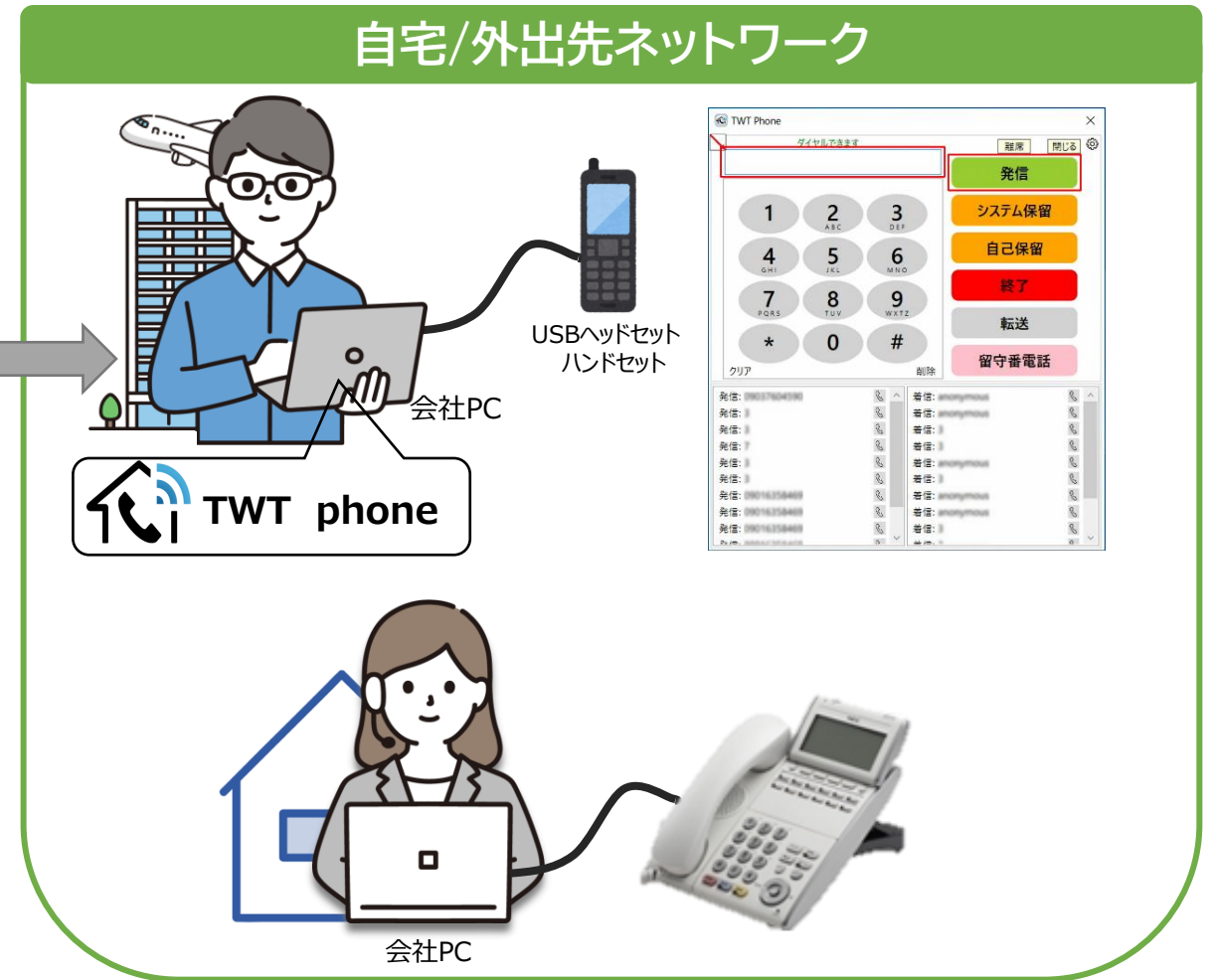
ビジネスフォンに対応 (テレワークテルのみ)

＜社内でビジネスフォンを既にご利用の環境の場合＞

- ・会社にかかってきた電話を自宅で受ける
- ・会社の代表番号で自宅から外部に電話する
- ・自宅で受け取った電話を社内の人に転送



※音声とデータは同一セグメントである必要があります。



テレワークテル

リモート初回設定

添付モデル (-TWTS1, -TWTS5)

5年間先出し交換保証

添付モデル (-TWTS5)

ソフトライセンスや保守費用など
年次の追加費用一切不要

同時接続台数 **5台**
(ビジネスフォン利用が無ければ10台)



テレワークテル
(MPC-LVZ2/TWT, TWTS1、TWTS5)

進化する明日へ Continue thinking

I-O DATA