

RemoNavi の現在地は、「開発」が完了し、ここから「事業化」へ です

# RemoNavi SaaS | オンプレ製品のご説明

## アジェンダ

- RemoNavi が実現すること【要約】 (1ページ分)
- **RemoNavi とは【超経済的・脱VPN】** (3ページ分)
- **RemoNavi とは【ゼロトラスの実現】** (3ページ分)  
(以下、企業運用によるもの)
- RemoNavi とは【インシデント 管理とセキュリティ検査】 (3ページ分)

代表取締役 内田高行 (t.uchida@remonavi.com)  
<https://remonavi.com>

株式会社リモナビ は 2024年 5月に設立された会社です (本事業のために新設しました)

# RemoNavi が実現すること 【要約】

セキュリティ担当者不在でも使うだけでセキュリティ対策できてしまう

少人数

専門知識不要

低コスト

セキュリティ能力向上

どこへでも、どこからでも接続できる通信サービス

結果的に脱VPN

必要なのは RemoNavi (ソフトウェア) だけ

手間要らずの SaaS 版も

部署毎の個別導入など自由設計

超・経済化

作業工数削減

専門知識不要

導入設計軽減

VPN機器不要につき、機器保守・運用が不要

30分のレクチャで使いこなせる簡単仕様

RemoNavi を使うだけで実現されるゼロトラスト

結果的にゼロトラスト

RemoNavi での通信は全てゼロトラスト

専門知識不要

人材育成

導入設計軽減

オンプレ版で境界内の高度なゼロトラストの実現

セキュリティ対策を知らなくても RemoNavi が全て教えてくれる

結果的にセキュリティ能力向上

セキュリティ対策に必要な規定一式の提供

インシデント管理、セキュリティ試験の蓄積

作業工数削減

専門知識不要

人材育成

セキュリティ・インシデントの対応フローの提供

全社員へのセキュリティ試験の簡単実施

セキュリティ対策の実現とリソースの経済化

通信に関わる全てのリソースの経済化

# 【超経済的・脱VPN】

## VPN機器なしに境界を超えて Point-to-Pointの接続を実現します

VPN は L2接続ですが、リモナビは L4(tcp|udp)での接続です（中継は TLS通信）

インターネットに接続できればどこへでも接続可能． VPN機器等の購入は一切不要  
接続する利用者環境には、RemoNavi Server ソフト、接続先完了には、RemoNavi Receiver ソフトのインストールが必要です。

家 → 会社

出先 → 会社

会社 → 家

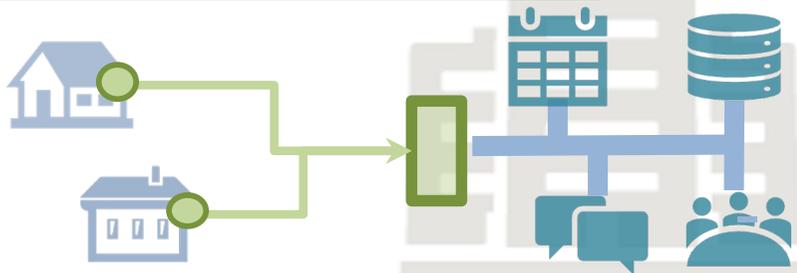
会社 → 出先

出先 → 出先

**カフェの個人PCからに友達のPCにだって接続できます！**

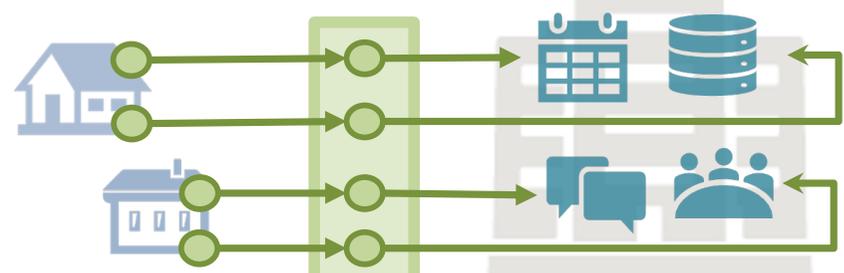
### i VPNとの違い

VPN は社内ネット直接接続します



VPN

リモナビは接続対象と接続します



リモナビ Gateway

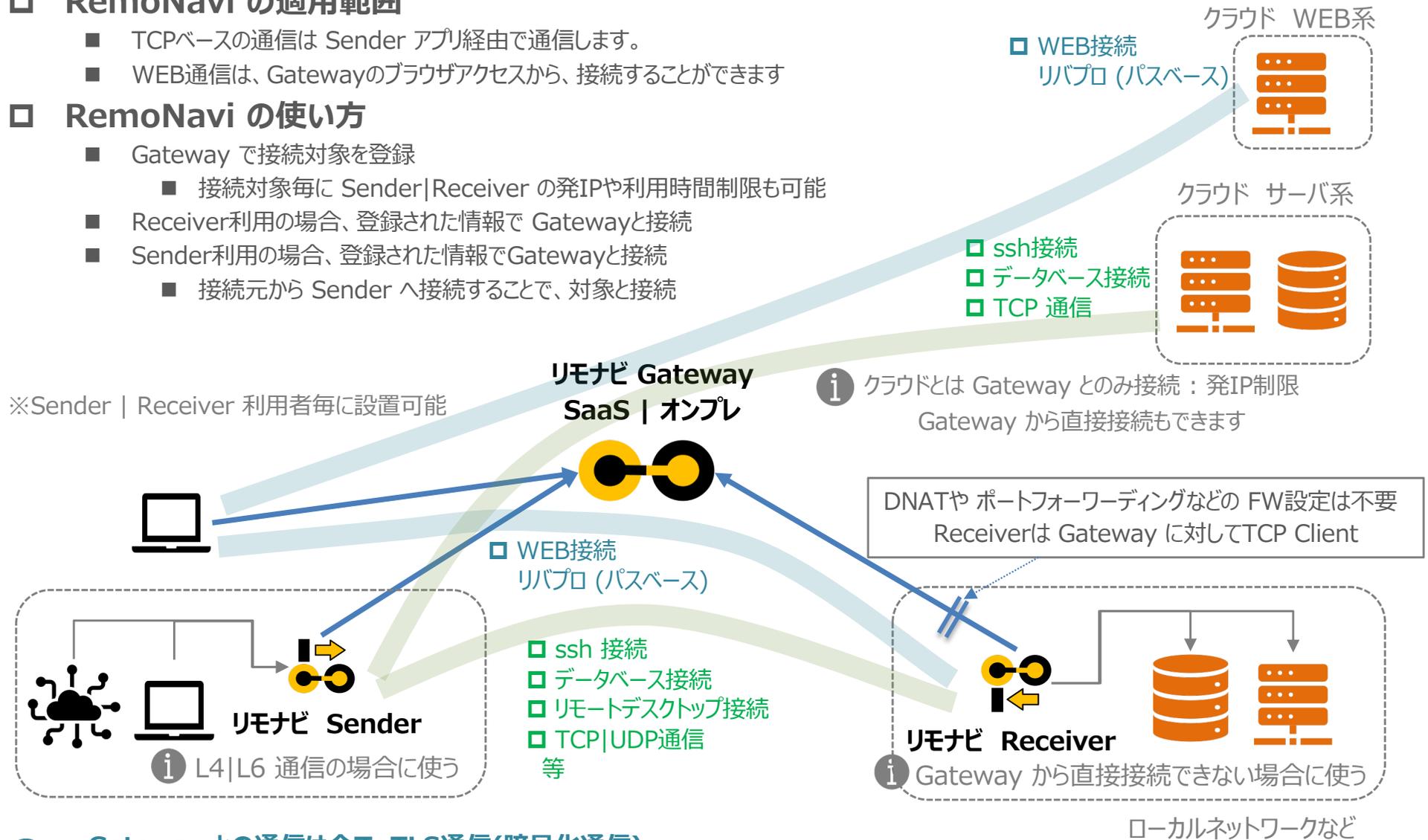
# 【超経済的・脱VPN 続き】

## □ RemoNavi の適用範囲

- TCPベースの通信は Sender アプリ経由で通信します。
- WEB通信は、Gatewayのブラウザアクセスから、接続することができます

## □ RemoNavi の使い方

- Gateway で接続対象を登録
  - 接続対象毎に Sender|Receiver の発IPや利用時間制限も可能
- Receiver利用の場合、登録された情報で Gatewayと接続
- Sender利用の場合、登録された情報でGatewayと接続
  - 接続元から Sender へ接続することで、対象と接続



※Sender | Receiver 利用者毎に設置可能

i クラウドとは Gateway とのみ接続：発IP制限  
Gateway から直接接続もできます

DNATや ポートフォワーディングなどの FW設定は不要  
Receiverは Gateway に対してTCP Client

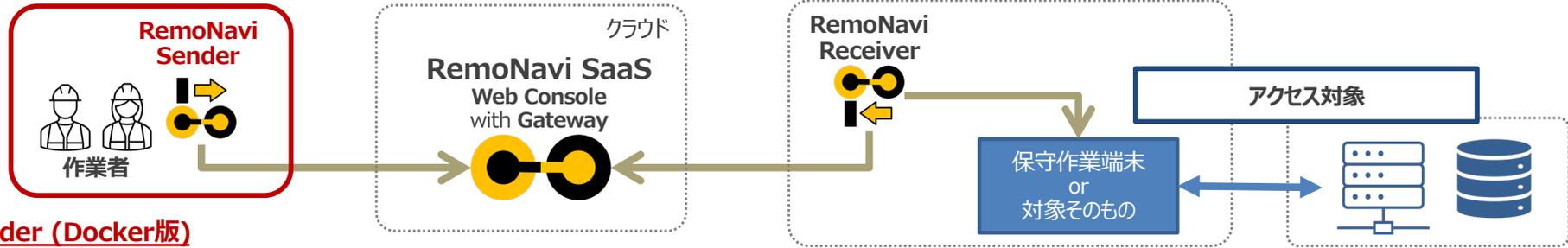
i L4|L6 通信の場合に使う

i Gateway から直接接続できない場合に使う

ローカルネットワークなど

- i ・ Gateway との通信は全て TLS通信(暗号化通信)
- ・ 全ての通信接続と通信量がログされます

# 参考：超経済的・脱VPN RemoNavi Sender (docker版) 利用イメージ



## Sender (Docker版)

RemoNavi Sender アクセスログ JP

Sender設定 (L4|L6 Stream用) 再起動

▶ RemoNavi 接続情報

管理対象	状態	受入IPポート	GatewayID	Gateway名	接続種別	接続方法	備考	ターミナル
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9144	70	local_rdp	L4 (TCP)	Receiver経由	出先でのWindows Note PC へのPDP接続	xterm rdp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9145	65	ssh_secure-ict.com_ssh	L4 (TCP)	Gateway直結	テストサーバへのSSHアクセス試験	xterm rdp

より簡易にアクセスできるよう、Sender(Docker版)ではブラウザからssh terminal や リモートデスクトップアクセスを可能に！

ブラウザ機能は以下のオープンソースを利用

- Terminal : xterm.js
- リモートデスクトップ : mstsc.js , node-rdpjs

## ブラウザ上で ssh terminal操作

```

Type ssh
Server 127.0.0.1 Port 9145
User uchida Password *****
KeyFile ファイルを選択し 選択
Connect

Connected...Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-44-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

System information as of Tue May 6 02:16:32 PM JST 2025
System load: 0.08 Processes: 326
Usage of /: 26.3% of 98.25GB Users logged in: 0
Memory usage: 32% IPv4 address for eth0: 160.251.17.149
Swap usage: 27%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.
191 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Sun May 4 15:27:14 2025 from 122.26.76.139
uchida@secure-ict:~$
uchida@secure-ict:~$
    
```

## ブラウザ上で リモートデスクトップ

127.0.0.1:9144

Domain

Username

Password

Connect

どこからでも、どこへでも繋ぐ  
VPNとは違う新しいリモート接続  
Raw TCP/UDPがって接続  
SaaS)オンプレ)製品で実現するリモート接続のインフラ

ゼロトラスト実現のために開発されたサービス  
社内データベースを社外からも使える

エンタープライズ版で月額3~10万円

ICTセキュリティ

Terminal 機能の延長で、oracle | sqlserver | postgres | mysql のデータベース・クライアントのターミナル操作もサポート

# 【ゼロトラストの実現】

## ゼロトラストとは

すべてのアクセスを信用せず、アクセスごとに厳格な認証と検証を行うセキュリティの「考え方」

## RemoNavi は

RemoNavi は 登録した管理対象とのみ接続します

RemoNavi では 登録した管理対象へ接続には利用の権限付与が必要です

### 全てを信用せず

「接続対象」を抽出して  
Gatewayに接続情報を登録

### 厳格な権限管理

利用者に「接続対象」の接続権限を与え  
るために Gatewayに権限を登録

### 厳格な運用 (システム+人の ダブルガード)

Sender が稼働しない限り接続不能

Receiver が稼働しない限り接続不能

### 厳格な認証

利用者は 多要素認証でログイン

Sender – Gateway 接続には  
利用者毎発行のアクセストークンが必要

Receiver – Gateway 接続には  
利用者毎発行のアクセストークンが必要

結果的になのですが

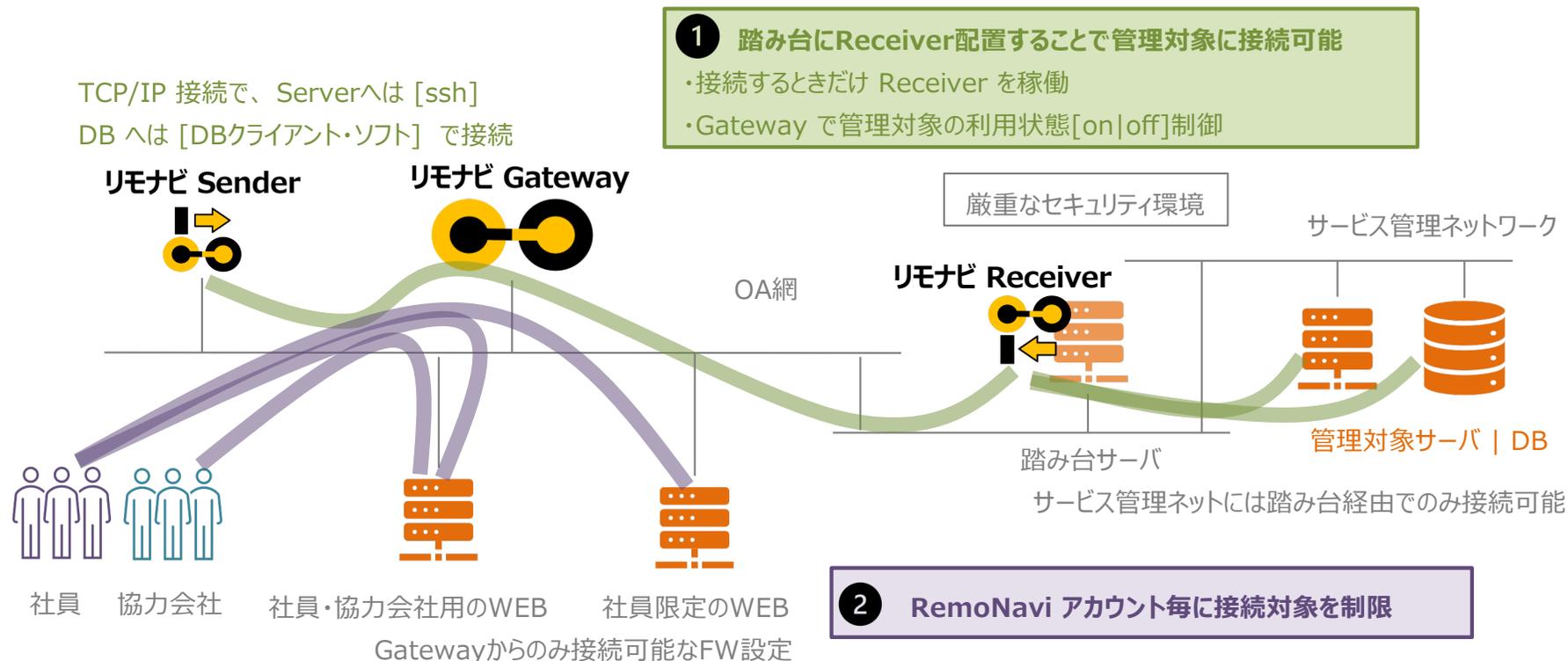
RemoNavi を使えば **ゼロトラスト** になってしまいます

# 【ゼロトラスト 社内こそゼロトラスト】

社内境界のセキュアな横断 や サイロ化の解消など

## □ 境界内 (社内) で実現できる ゼロトラスト

- 1
- 管理対象 : データベース, システム稼働サーバ (関係者しかアクセス不能なネットワーク構成)
  - ゼロトラスト適用 : 抽出された管理対象には、接続を許可された利用者からしか アクセスできない



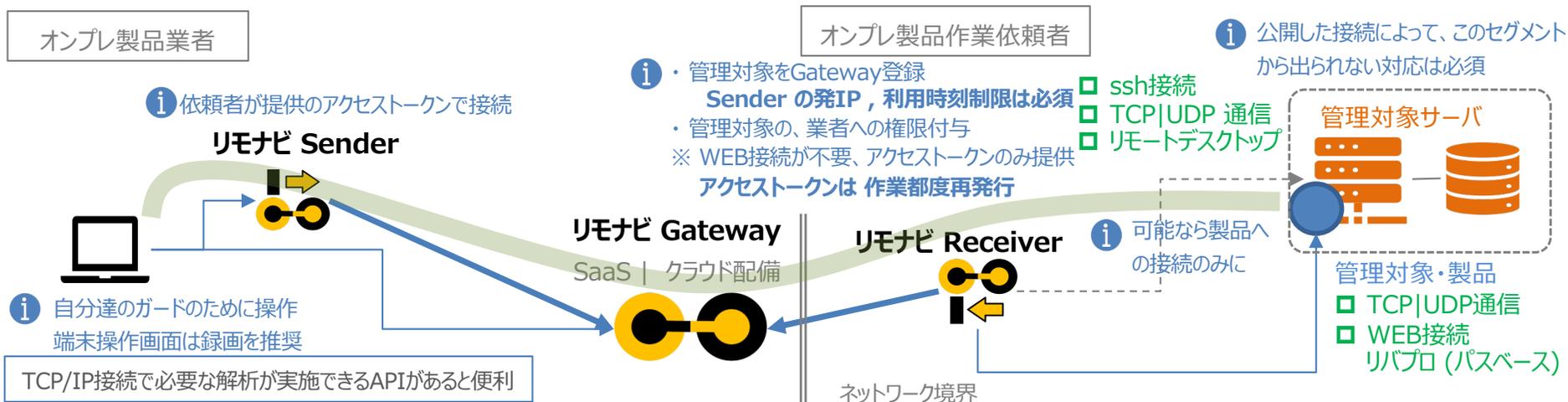
- 2
- 管理対象 : 社員限定のWEBサービス, 社員・協力会社のWEBサービス
  - ゼロトラスト適用 : アカウント毎の利用権限設定による接続先の制限

# 【ゼロトラスト 社外リソースの高度な活用】

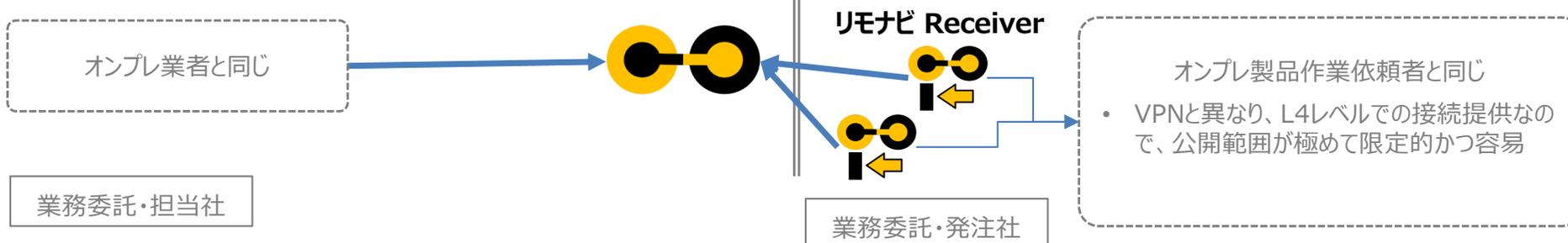
少数・情シスだからこそその高度な利用

## □ 境界を跨いだ ゼロトラスト で実現できること

- 管理対象 : 購入したオンプレ製品
  - ゼロトラスト適用 : 提供しているオンプレ製品の保守や解析等で、許可された管理リソースにピンポイントで接続



## 社外事業者向けの VPN や 境界FWに DNAT, ポートフォワード等の穴あけ なしに管理対象にピンポイントに接続を提供できる



- 管理対象 : 業務委託したシステム等
  - ゼロトラスト適用 : 業務委託したシステム等、許可された管理リソースにピンポイントで接続して委託業務の実施

# インシデント管理とセキュリティ検査

## 少数・情シス あるある

- 多くの情シスでの仕事は、「業務系」と「ネットワーク系・セキュリティ系」の2つに大別できます。
- 2つの業務は全く異なるもので、少数・情シスにとって両方に精通した人材は皆無。2つの業務に優劣はありませんが、どちらか一方に比重を求められるのなら、経営層の関係性も強い「業務系」に傾くことがしばしば。それでもリモートワーク時代。ネットワーク系の比重は削減できない。そこで、生産性のないセキュリティが犠牲に。

## RemoNavi は

具体的な取り組みスキルがなくても、システムをなぞればセキュリティ運営ができる仕組みを提供しています

セキュリティ運営で最初に策定する「**セキュリティ規定書**」と「**セキュリティ対策基準**」を提供  
提供書類を自社向けにカスタマイズすればいいだけ。規定書、対策基準を満たした**インシデント対応の備え**も提供。

「**セキュリティ・インシデント**」が発生した際にすべき対応をワークフローとして提供  
インシデントの備えと、システムが提供するワークフロー通りに処理すれば、インシデント対応できます。

セキュリティ規定、対策基準で定めた「**セキュリティ検査**」もワークフローとして提供  
システムが提供するワークフローを実施すれば、セキュリティ検査を容易に実施できます。

結果的になのですが

RemoNavi を使えばセキュリティ運用が実現できるだけでなく、  
セキュリティ管理者に必要なスキル一式を習得してしまいます。

# 【インシデント管理とセキュリティ検査】

セキュリティ・インシデント対応はシステムの通りに！

インシデント発生前の事前準備

セキュリティ管理者  
全員

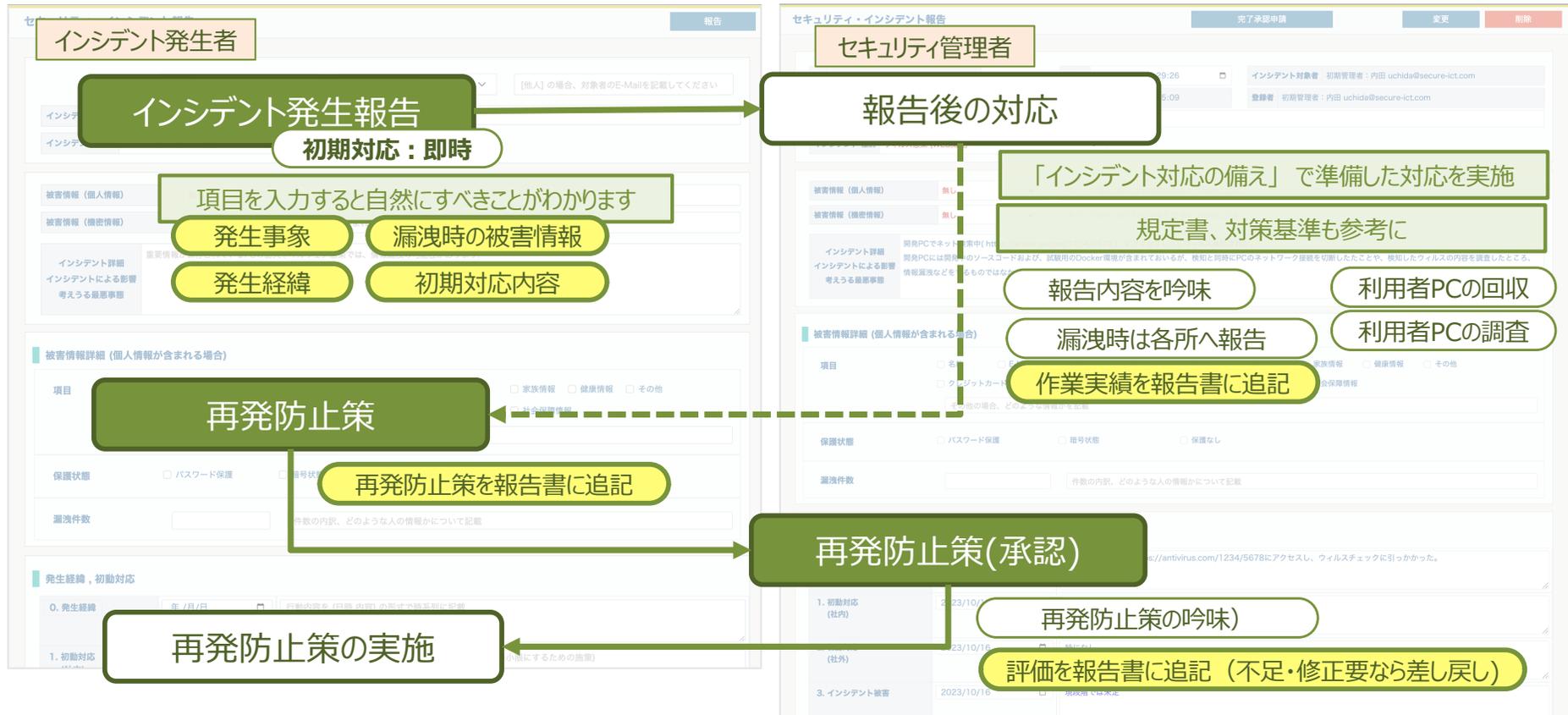
「規定書」、「対策基準」の確立

「セキュリティ検査」の計画・実施

「インシデント対応の備え」を習得

準備万端！

発生時は  
システムの通りに



# 【インシデント管理とセキュリティ検査】

RemoNavi で提供するセキュリティ検査は、**全社員参加のセキュリティ試験** です！

試験問題は「セキュリティ管理者」が作成します（サンプル問題あり）

問題を作成することでセキュリティ技術が向上

※情報セキュリティ試験の問題・回答はネットで収集可能

試験未実施・試験未完了 社員の検索なども容易

強制ではなく、無理なくセキュリティ技術の向上

セキュリティ管理者

全社員（試験対象者）

検査情報作成（試験作成）

ネットなどから選択式の試験問題を検索・作成

実施日の決定

合格条件の決定

試験問題の作成

回答形式/問題/回答 + 備考に回答解説

検査の結果集計

試験完了者、未完了者の検索

未完了者への必要に応じた対応実施

ID	アカウント	E-Mail	部	課	グループ	期限
2	内田真行	uchida@v-software.co.jp				2025-06-06 13:31:38

検査の実施（回答の提出）

試験実施期間になると表示される

合格条件に達するまで完了できません

問[1] 2023年最も多く発生した「個人情報漏えい事故」は次のうちどれで  
 ウイルス感染・不正アクセス  
 誤表示・誤操作  
 紛失・盗難  
 その他

問[2] 近年「ランサムウェア」被害が増加している。ランサムウェアとは、どのような意味でしょうか？  
 強盗  
 誘拐  
 身代金  
 なりすまし

問[3] 次のうち「標的型攻撃メール」の特徴として当てはまらないものは？  
 攻撃対象を管理職や情報担当者に向けている  
 知り合いや関係者を偽ってメールを送る  
 添付ファイルからウイルスに感染させる  
 メール内のリンクから不正なサイトへ誘導する

問[4] パソコンがウイルスに感染した疑いがある場合、最優先で行うべき行動は次のうちどれでしょうか？  
 パソコンを強制シャットダウンする  
 ウイルス対策ソフトでウイルスチェックを行う  
 重要なデータをUSBメモリにコピーする  
 パソコンをネットワークから切り離す

問[5] 安全なパスワード管理について正しいものはどれでしょうか？  
 名前などの個人情報からは推測できない  
 英単語などをそのまま使用しない  
 アルファベットと数字が混在している  
 類推しやすい並び方やその変形を組み合わせない  
 できる限り複数のサービスで使い回さない  
 入力時、ショルダーハックに注意する

# 資料の補足

## RemoNavi 通信の補足

RemoNavi は L4(tcp|udp)レベルで境界に関係なくセキュアな接続を実現し、それによって以下が実現されます。

- 脱VPNの実現
- ゼロトラストの実現
- オンプレ回帰、クラウド・ハイブリッド環境の実現 (境界を超えて、社内リソースが可能)

L4レベルの接続は、全ての接続対象の抽出が必要になります。ゼロトラストではそれ必須になりますが、大量の接続対象を持つ企業運営にとって全てにゼロトラストを適用するコストはデメリットになります。

言い換えると、RemoNavi は VPN を置き換えるものではなく、共存関係にあると言えます。一方で接続対象が多い中小企業にとっては、VPN機器導入・運用のコスト／スキルを削減できる最適なサービス | 製品であると言えます。

大企業においても、部署毎の導入なども可能であり、かつ境界内の高度なゼロトラストの実現などに貢献することができます。( [https://remonavi.com/?pos=saas\\_doc](https://remonavi.com/?pos=saas_doc) \*1 : リモナビを利用した高度なゼロトラストの実現)

\*1) RemoNavi に関わる資料を公開しています。

## RemoNavi セキュリティ対策の補足

RemoNavi がセキュリティ対策として提供する以下は、セキュリティ対策の重要な助けになりますですが、それを実現するのは人です。そしてセキュリティ対策は日々の蓄積と進化を必要とします。

- セキュリティ規定、セキュリティ対策基準、インシデント発生の備え
- インシデント管理
- セキュリティ検査