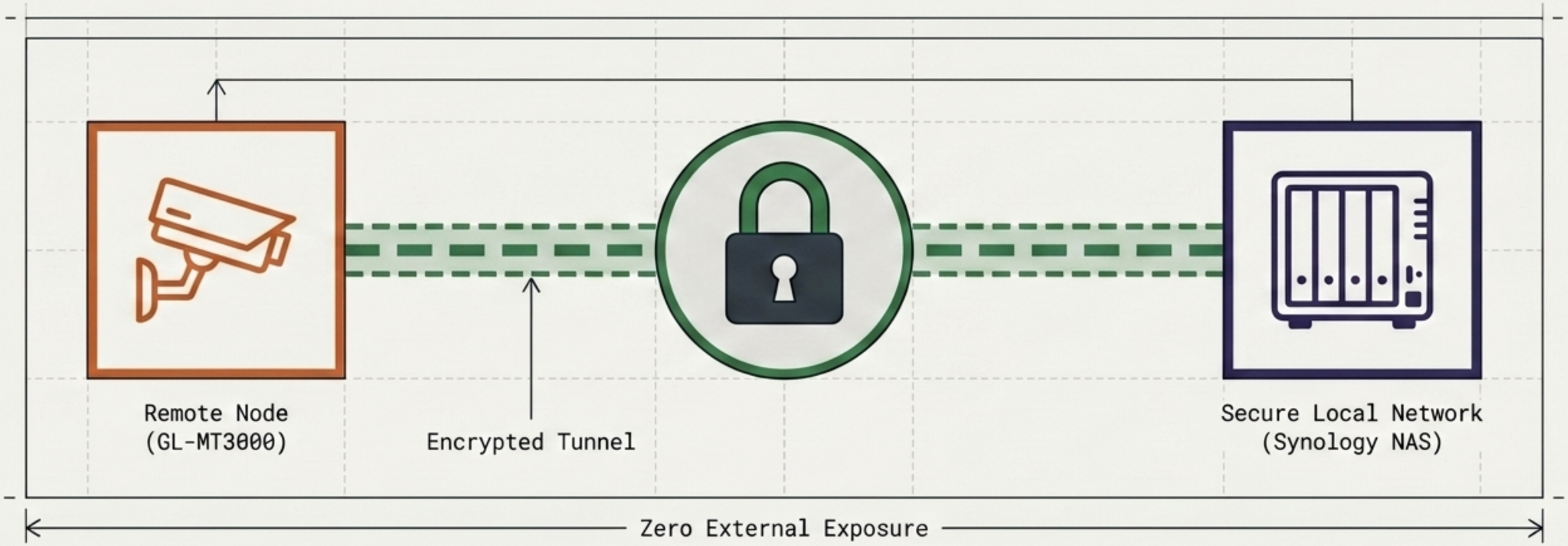
外部公開ゼロの安全な遠隔カメラ監視網

GL-MT3000とSynology NASを活用したリバースSSHトンネル+ローカルプロキシ構築手法



従来のポート開放が直面する3つの壁

キャリアNAT（CGNAT）

グローバルIPが付与されず、外部からの直接通信が不可能。

ルーター設定不可

出先や実家など、管理権限がなくポートフォワード設定ができない。

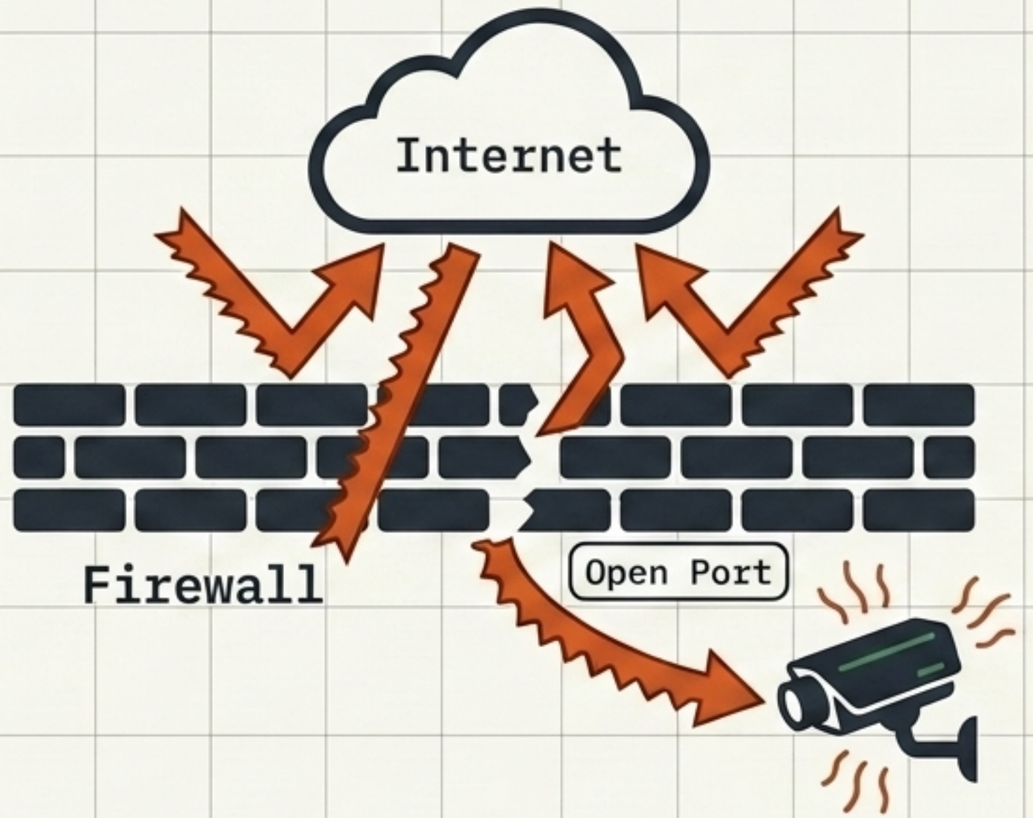
セキュリティリスク

監視カメラのポートを直接インターネットに晒す危険性。

解決策：「リバースSSHトンネル」による完全閉鎖網の構築

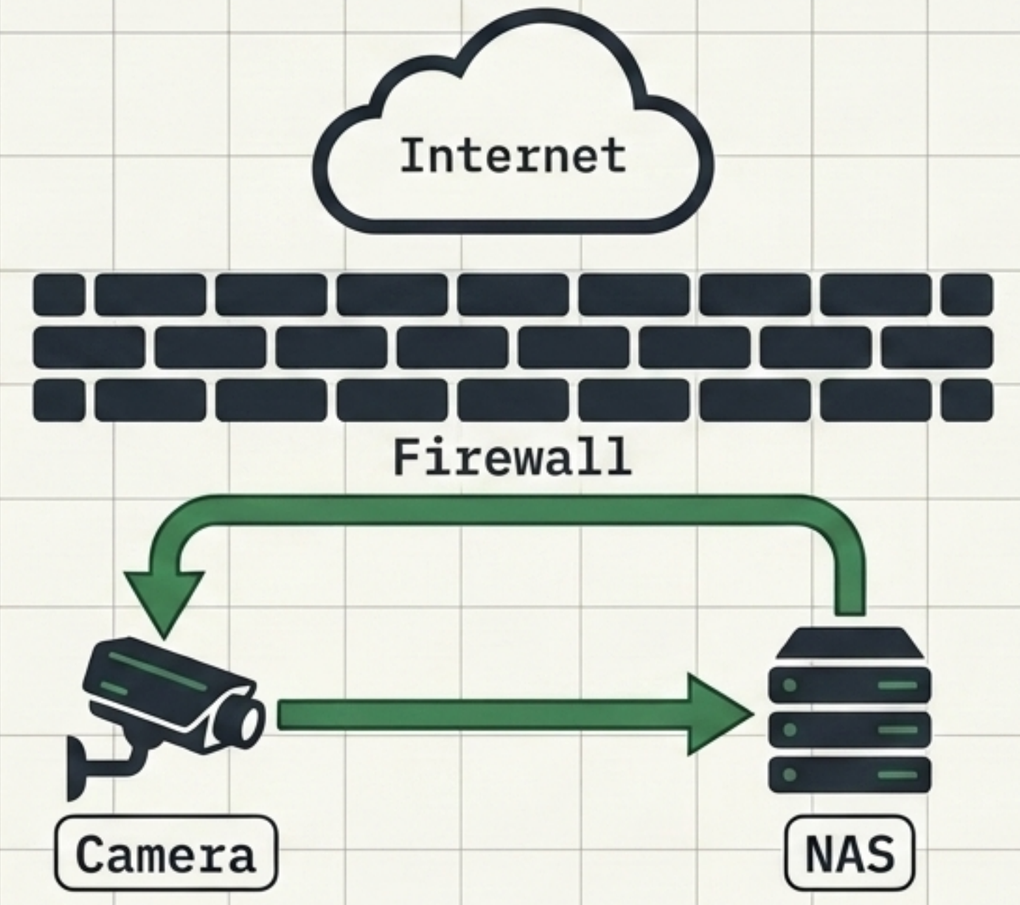
Traditional Method

危険かつ環境依存（ポート開放が必要）

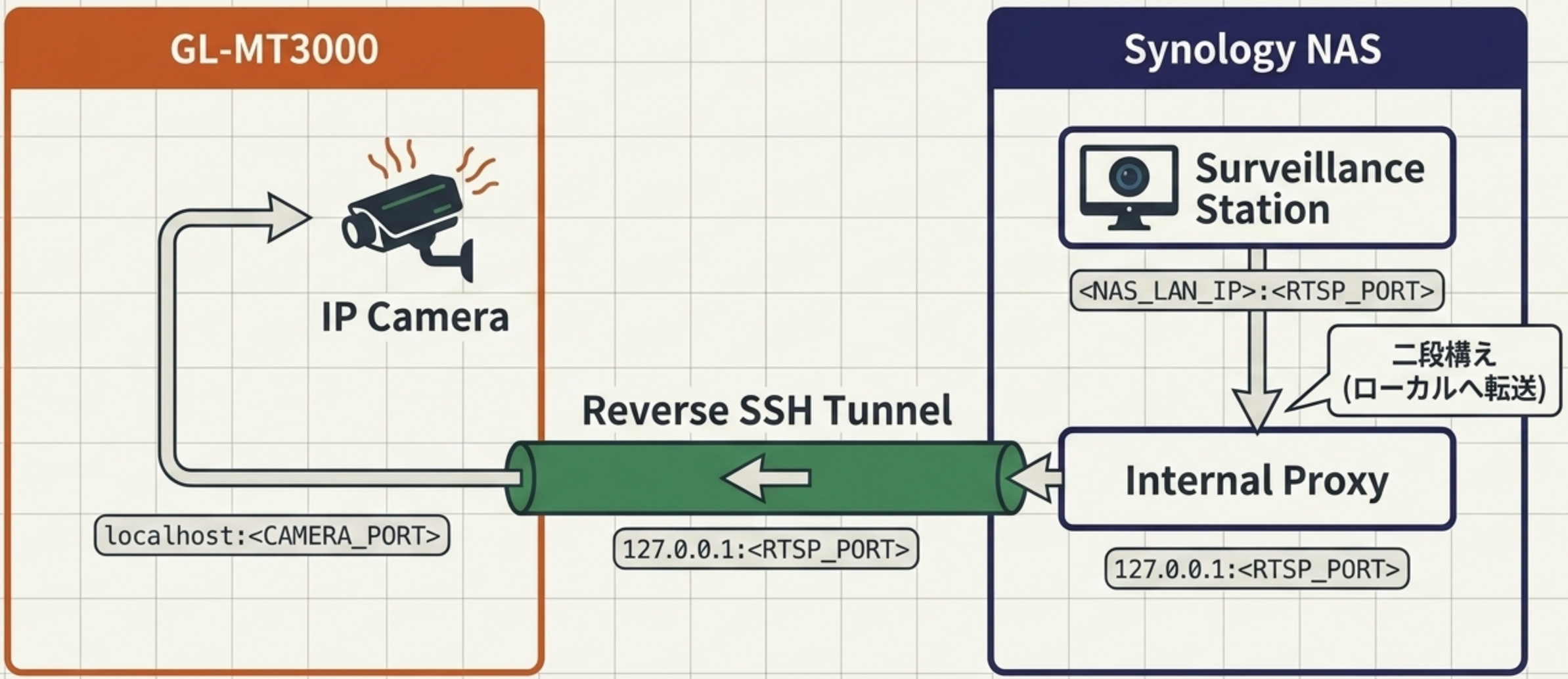


Our Method

外部公開ゼロ（すべてローカルで完結）



システムアーキテクチャ：「二段構え」のプロキシ構成



構築前の前提条件と環境チェック

カメラ側: GL-MT3000

- [ ] カメラがローカル `localhost:<CAMERA_PORT>` で配信中
- [ ] 公開鍵 (`~/.ssh/id_ed25519_mt`) の生成

受け側: Synology NAS

- [ ] SSH設定: `AllowTcpForwarding yes` が有効
  ※最重要
- [ ] SSH設定: `GatewayPorts yes` が有効
- [ ] MT3000の公開鍵を `authorized_keys` に登録済み
- [ ] 制限オプション (`no-port-forwarding` 等) が付与されていないこと

実行手順：安全なトンネルを開通させる4ステップ

1

Synologyプロキシの一時停止（ポート占有を解除）

2

MT3000からリバースSSHトンネルを張る

code

```
ssh -R 127.0.0.1:<RTSP_PORT>:localhost:<CAMERA_PORT>
```

3

Synologyプロキシを `127.0.0.1` 向けに再起動

4

RTSPの動作確認（OPTIONSリクエスト）

output

```
✅ RTSP/1.0 200 OK
```

トラブルシューティング：ポート衝突の罠と回避

エラー (Error)

ログ:
`Error: remote port forwarding failed for listen port <RTSP_PORT>`

原因 (Cause)

原因:
Synology側で既存のプロキシが `<RTSP_PORT>` を既に占有している。

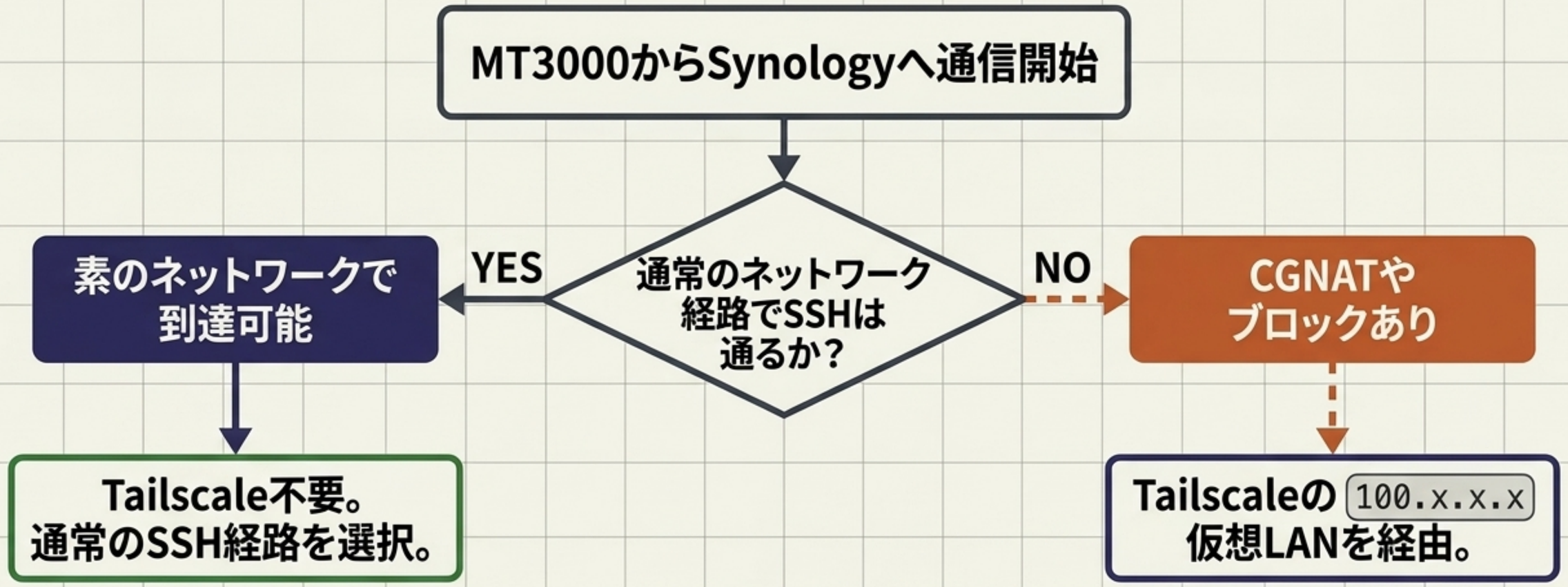
解決策 (Action)

解決策:
`pkill` **コマンドで既存プロセスを強制停止。**

結果 (Success)

結果:
障害物がなくなり、トンネルのバインドが成功。

なぜ今回は Tailscale を使わなかったのか？



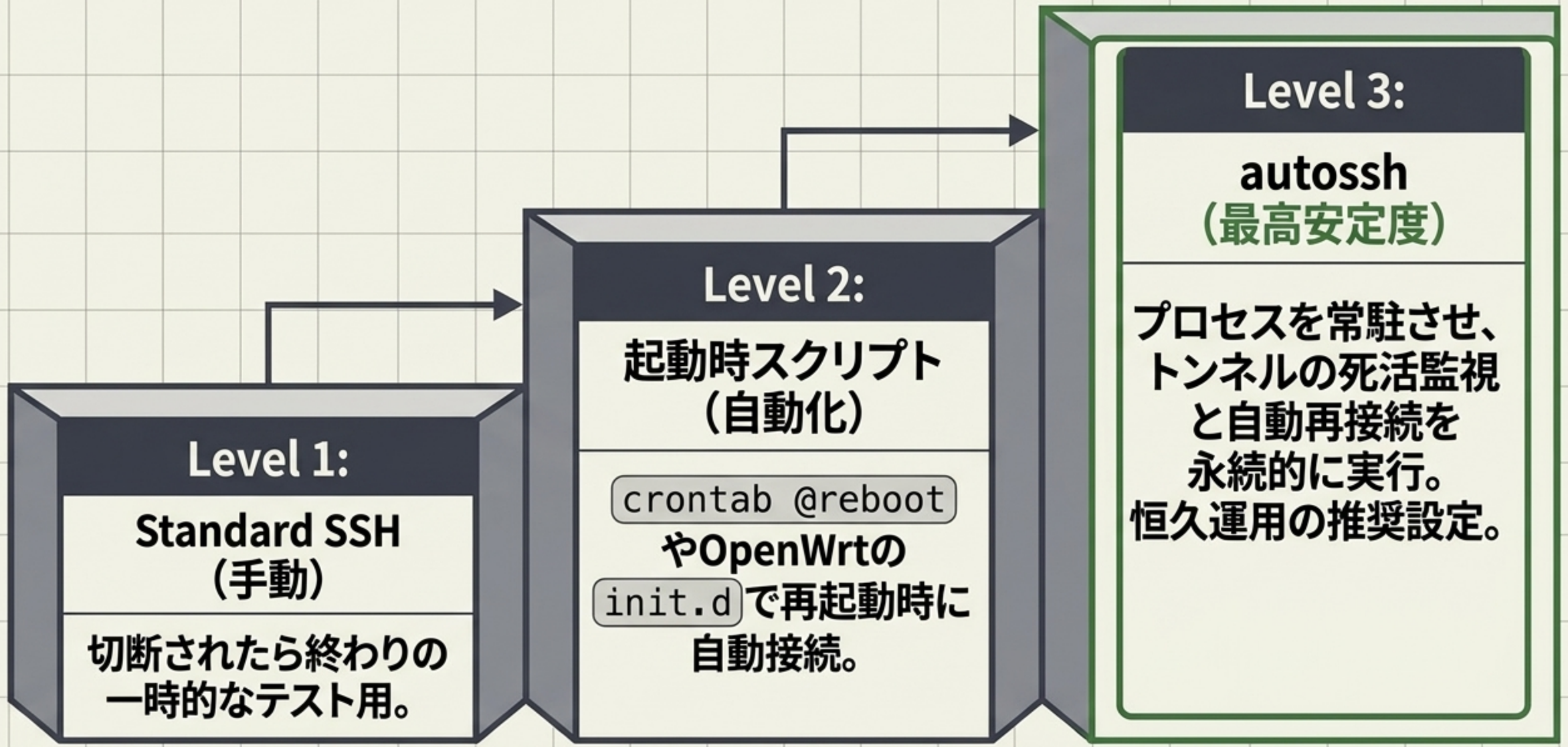
Tailscaleは「使える状態」であっても、通常経路が通ればSSHには登場しない。
優先経路ではなく「強力な補助経路」である。

導入判断マトリクス：Direct SSH vs Tailscale併用

	Direct SSH	Tailscale + SSH
MT3000が外出先・モバイル回線	✗	✓
Synology側がCGNAT (IPv6 only)	✗	✓
ルーター設定が一切触れない	✗	✓
ネットワーク環境が頻繁に変わる	✗	✓

Tailscaleが仮想LANを構築し、「常に同じネットワークにいる状態」を偽装するため、環境変動に極めて強くなる。

運用フェーズ：トンネルの恒久化と自動復旧



プロダクション環境のためのセキュリティ・ベストプラクティス

秘密鍵のパーミッションは必ず `chmod 600` に設定する。

authorized_keys 内で `from="192.168.0.0/24"` 等を指定し、接続元IPを制限する。

運用モードの選択：基本は `127.0.0.1:<RTSP_PORT>` の閉じた運用を推奨。
LAN内他機器からのアクセスが不要なら外部に公開しない。

外部に一切のポートを開かず、強固なプライベート監視網をコントロールする。