今日から始める！
ゼロトラスト！

ZTNAとtailscaleの紹介

自己紹介

- ぐすくま(@guskma@abyss.fun) アビス丼 鯖缶やってます
- Linux好きのNWエンジニア、Ubuntu好きだけど仕事ではRHEL
- ふぇでば略歴
  - 2017年4月 第一次マストドンブームに乗って JPに登録
  - 2017年9月ごろ？ Ciscoコンソール風Webクライアント「Tooterminal」開発
  - 2017年11月 メイドインアビス テーマ鯖「Abyss.fun」公開
  - 2018年11月「Mastodon meet-up」運営メンバー
  - 2018年？ 分散SNS鯖缶向けDiscord鯖「鯖缶工場」
- 以降 惰性

※発表長いです※

「よっしゃゼロトラスト発表すっぞ！」

と書き始めたら、想像以上に筆が乗ってしまいました。

スライド30枚以上ある大長編です。

とてもLT時間内で収まるサイズではありません。

（それでも**今回紹介できない内容がまだあります**）

なので、必要なところをピックアップしながら話します。

資料は展開するので、後でゆっくり読んでくださいね！

今回のお話

「従来のVPNとゼロトラスト」
＆
「tailscaleの紹介」

ゼロトラストってなぁに？

- ゼロトラストは**「すべてのアクセスを信頼せず、すべての場所で情報資産を守る」**という概念
- ネットワークだけではなく、アプリケーション、BYOD端末など多岐に渡る技術
  ※私はネット屋さんなのでネットワーク観点で解説をします。
- ざっくりいうと**『ネットワーク、サーバーリソース、端末、アプリケーション、ユーザーデータなど、ネットワーク上でアクセスできるすべての情報資産にリスクがあるから、何も信じません！！ 信じられないから全部制御します！ 全部監視します！ 現代技術なら！ クラウド技術を使えば！ それができます！！！！！』**というもの。

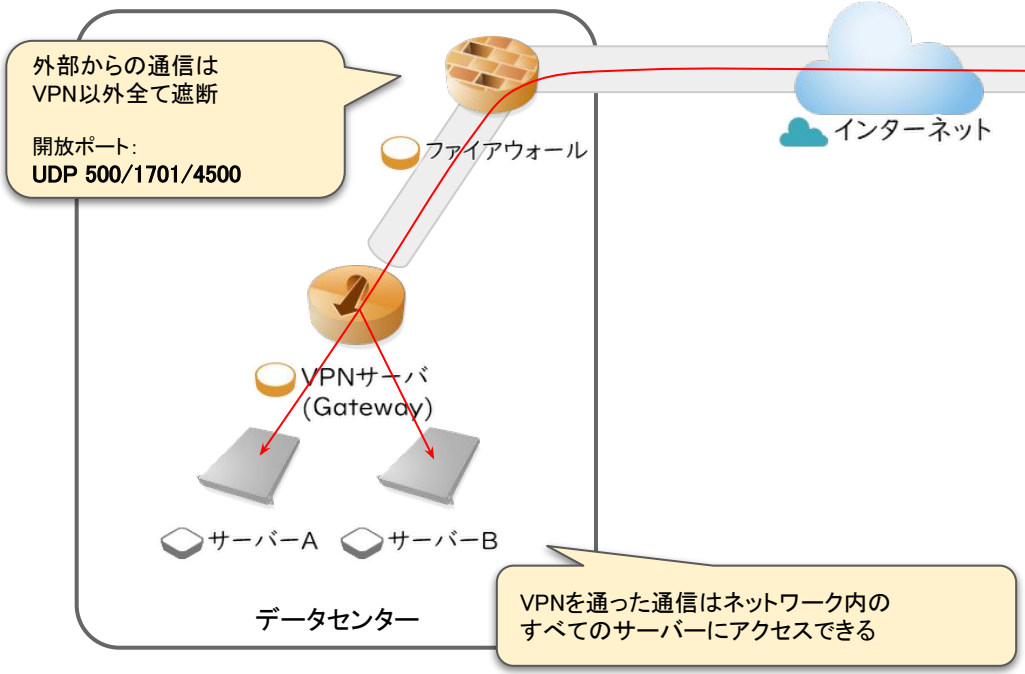
- 今回はFediLUGということで、ゼロトラストの理念に沿っていて、みんなが手軽に利用できるVPNクライアント**「tailscale」**を紹介します。
- 若干付け焼き刃の知識もあるので間違いがあったら指摘お願いします。

従来のVPNとゼロトラスト

まずはサーバーに接続する際のセキュリティ対策についてイメージしてみましょう

- Webコンソール
  - ブラウザからサーバを操作できるコンソール画面
  - IaaSやVPSではほぼ標準で提供されている機能
  - コピペができないものも多い
- 直接SSH
  - ユーザー/パスワード入力 →何も対策していない論外
  - 秘密鍵方式 →鍵生成したりユーザー管理したりが面倒
- **インターネットVPN**
  - SSL-VPN、IPSec、SoftEtherなど
  - 今回はこれを採用した場合の話をします。
- その他のVPN
  - IP-VPN、エントリーVPN、広域イーサネット
  - 事業者向けのサービスなので個人利用は現実的じゃない

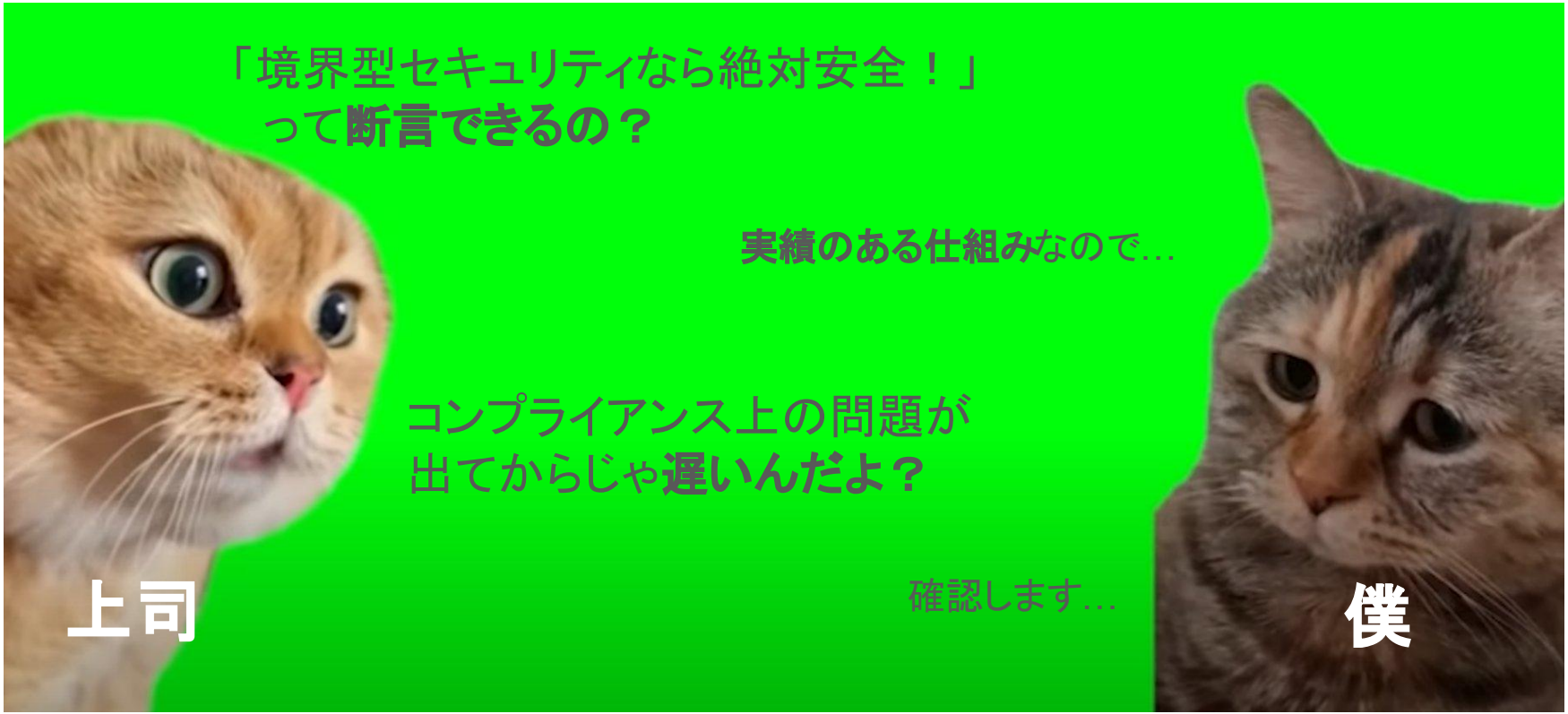
とてもわかりやすい？VPN接続の図



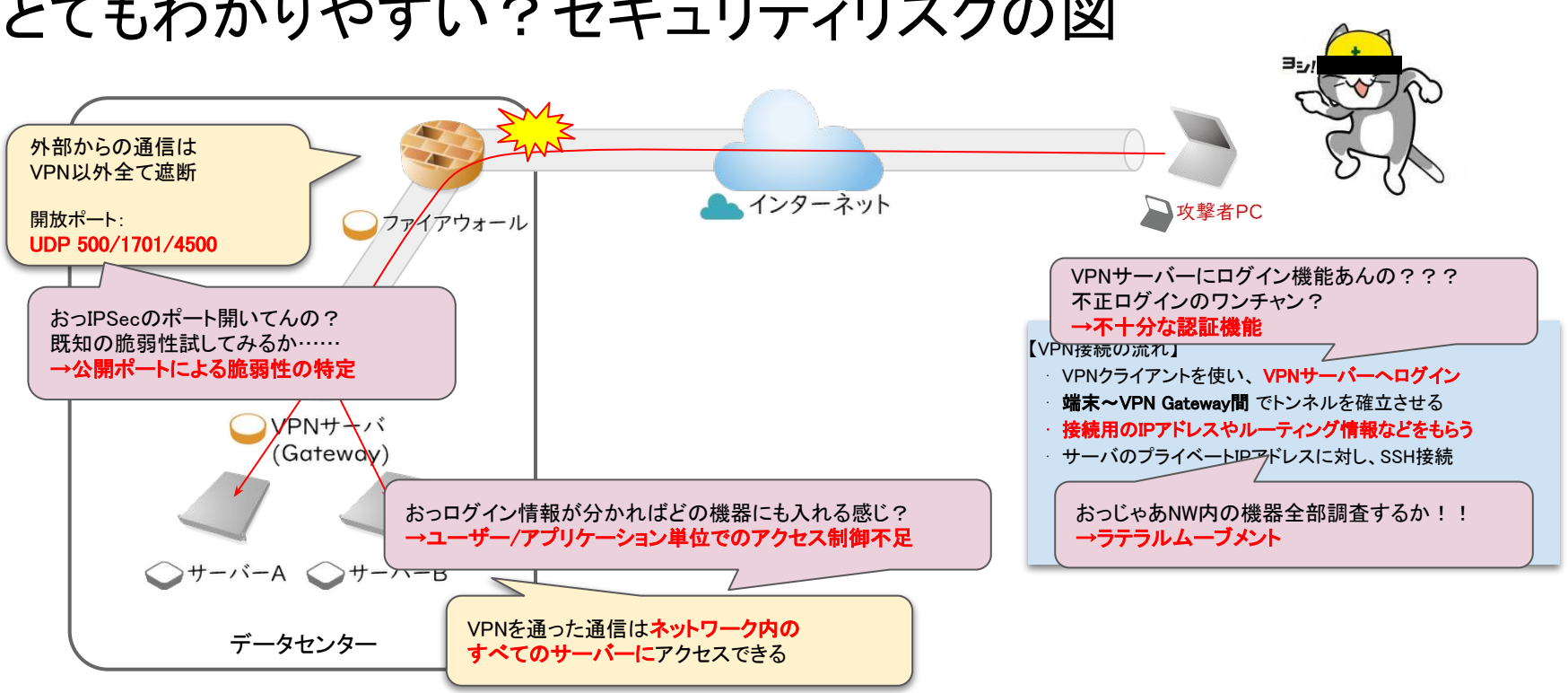
【VPN接続の流れ】
- VPNクライアントを使い、VPNサーバーへログイン
- **端末～VPN Gateway間** でトンネルを確立させる
- 接続用のIPアドレスやルーティング情報などをもらう
- サーバのプライベートIPアドレスに対し、SSH接続

FWで外部からの脅威を守る構成を**境界型セキュリティ**と呼びます

しかしこれにも「リスク」は存在します
境界型セキュリティについて考えてみましょう！



とてもわかりやすい？セキュリティリスクの図



今まで**目を背けられていたところのリスクに注目**され始めている

セキュリティリスクの件、上司に話しました。

対策しないと
リリースできんぞ？

途端に泣き崩れる僕

とはいえ、どう対策したらいいんだr……

外部のポート全部閉じろ？？？？
無理やん？？？？？？？

侵入されても被害拡大しないようにしろ？
え、DBのポートも開けちゃダメってこと？？？
なにいってんの？？？？？

VPNサーバの脆弱性？
え、パッチ全部当てろってこと？？
保守コストって知ってる？？？？？？

とはいえ、どう対策したらいいんだ…

!?

今や常識に左右されない

新しいアプローチが

試されるべきと考えます

…境界型防御の欠点…
『脆弱性』
『ラテラルムーブメント』
何とかしたいですよね


ZTNA

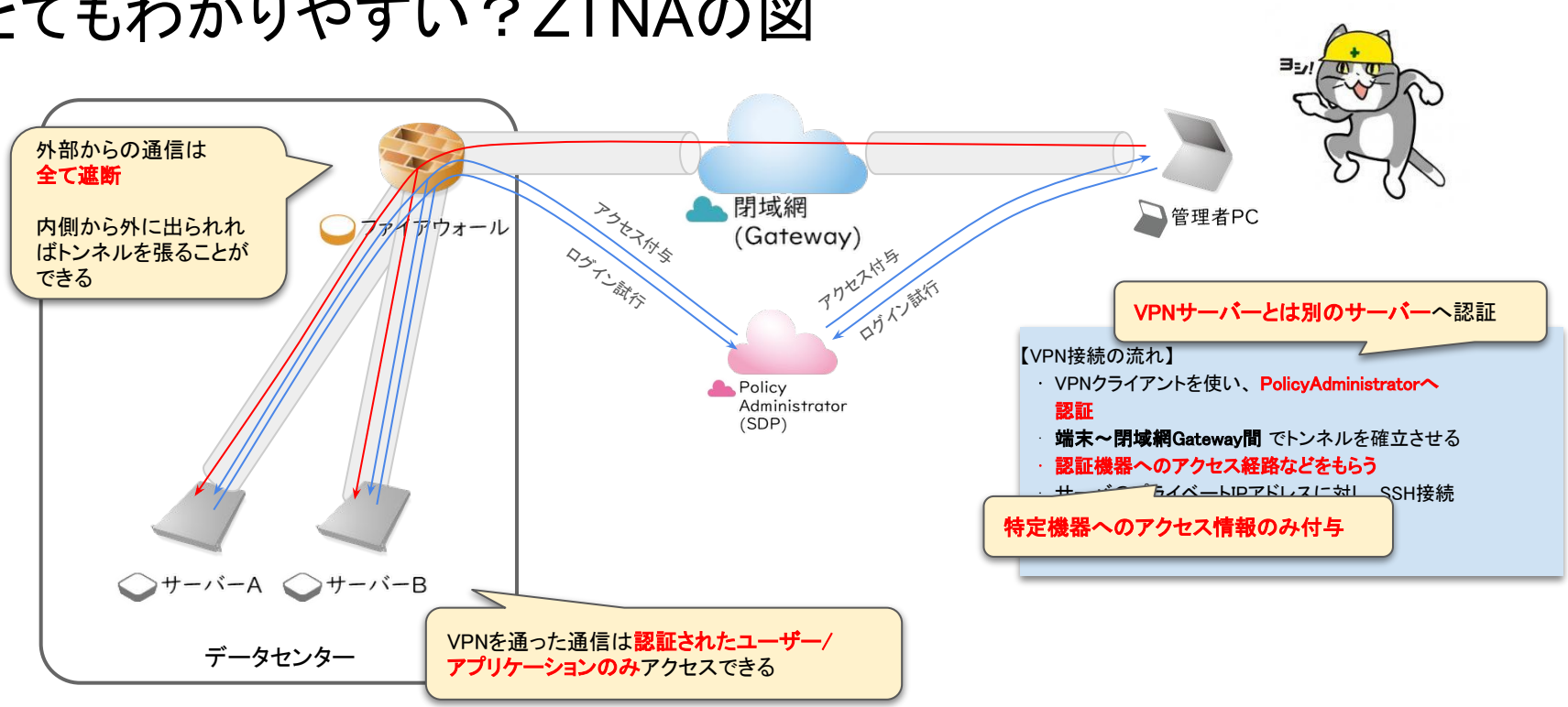
そこでZTNA（Zero Trust Network Access）です

ゼロトラストの概念のうち、ネットワークセキュリティを指すもの

- **リモートアクセス→VPNサーバーで認証。をやめます！**
  - VPN接続先とユーザー認証先はそれぞれ別のサーバとなります。
  - 仮に認証サーバーへの不正ログインでマルウェア感染したとして、VPNサーバーへの影響は抑えられます。
- **ポートは全部閉じます！**
  - FWだけでなくすべての機器は外部からのアクセスを許可しません。
  - どの機器も内側→外側でトンネルを張るだけなのでポートを解放する必要ありません。
  - ネットワークに侵入できてもどんな機器があるかわかりません。
- **細かくアクセス制御します！**
  - VPNで大変だったアプリケーションごとのアクセス制御を容易にします。
  - アクセス制御はクラウド上で管理されます。(**SDP: SoftwareDefinedPerimeter**)
  - 今まで管理しきれなかったアプリケーション間の侵害を抑えられます。
- **エンドツーエンドで暗号化します！**
  - 端末ごとに認証をし、端末間で暗号化するので、途中で盗聴される心配がありません。

参考: ゼロトラスト ネットワーク アクセス(ZTNA)とは？ | Zscaler

とてもわかりやすい？ZTNAの図



境界型セキュリティの欠点を解決。すべての機器に対して同一の対策が可能

対策できました！！！！！！！！

はっぴー はっぴー はっぴー

はぴはぴはっぴー はっぴー

僕

上司

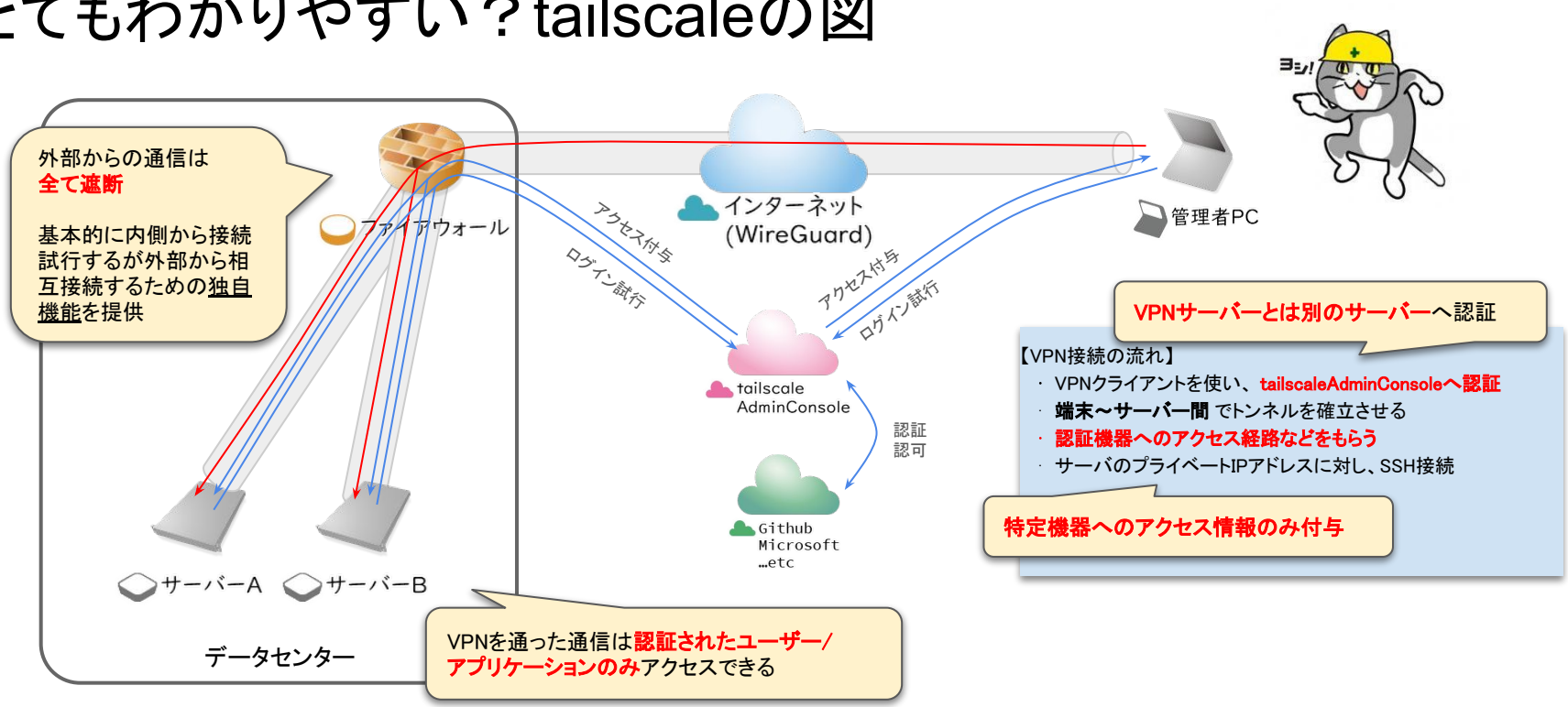
ボンさん

tailscaleから始めるZTNA生活

tailscaleとは？

- 無償で利用できる**WireGuard** VPNクライアント、および関連サービス
- ZTNAの思想に沿っていて、**完全に暗号化されたエンドツーエンド通信**を実現している。
- **NAT越え、FW越えをするため**にVoIPで使われるSTUNサーバの技術を利用するなどの**工夫が盛り込まれている。**

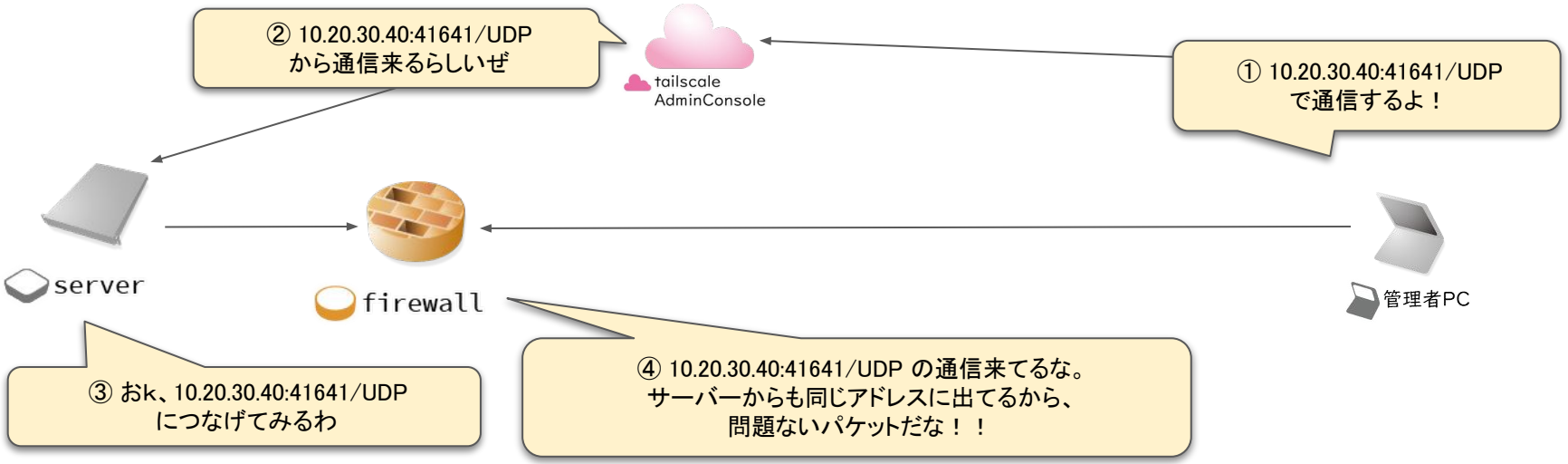
とてもわかりやすい？tailscaleの図



ZTNAの思想に沿ったシステム構成をとっている。

FW越えのために用いている技術

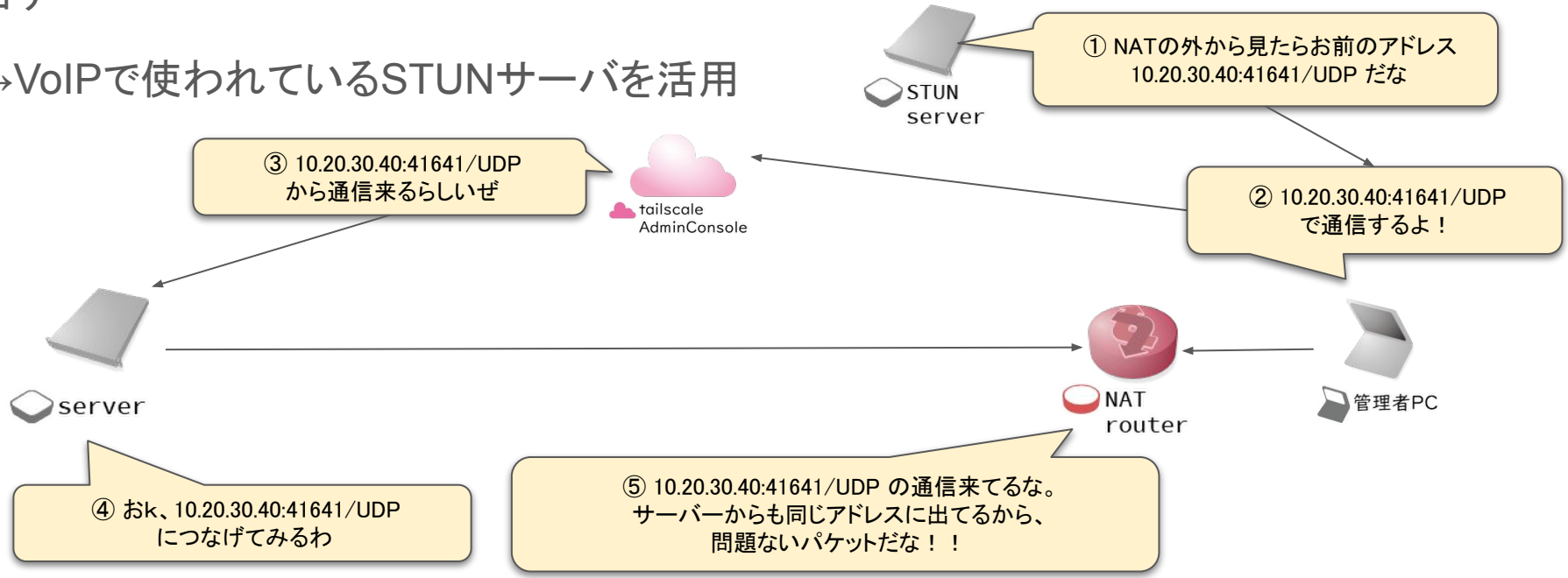
「送信元/宛先のIPアドレス:ポートが一致していれば双方向通信ができる」NW機器の仕様を利用



NAT越えのために用いている技術

SNATをしていたら送信元機器がわからない→外から見えるIPアドレス:ポートを見つけ出す

→VoIPで使われているSTUNサーバを活用



tailscaleの導入方法(Linux)

- ブラウザからtailscaleサイトへ行きGitHubアカウントなどで**サインアップ**
- 各サーバーから操作

クライアントのダウンロード＆インストール

```
# curl -fsSL https://tailscale.com/install.sh | sh
```

tailscaleアカウントと端末を紐づけ

```
# tailscale login
```

- 以上！

→従来のようにVPNを構築したりSSHで秘密鍵作ったりするよりも圧倒的に楽ちん！

アカウントに紐づいている機器の確認

```
root@server01:~# tailscale status
100.126.xx.xx  vm-server01          guskma@      linux   -
100.118.xx.xx  n8n                  guskma@      linux   -
100.124.xx.xx  desktop-pc           guskma@      windows active; relay "tok", tx 22284 rx 23556
100.77.xx.xx   macbook              guskma@      macOS   offline
```

みんなもtailscaleでレッツゼロトラ！

今回話したことのまとめです

- ゼロトラスト(ZTNA)の説明
  - 従来の境界型セキュリティには様々なセキュリティリスクがある
  - ZTNAではそれらの問題を解決。「誰も信用しない NW」を実現
- 誰でも簡単に始められるゼロトラスト「tailscale」
  - WireGuardで実現しているエンドツーエンド通信
  - FW越え、NAT越えのために用いられている様々な技術
  - 導入はわずか数ステップのお手軽導入

最後に:メイドインアビスの紹介

メイドインアビスは世界の果てにある孤島に存在する大穴「アビス」を探検する少年少女たちを描いた冒険ファンタジーだよ！

Amazonプライムビデオで アニメ1期、劇場版、2期 と配信されているから良かったら見てね！

補足資料

ゼロトラストの全体像

- ZTNAはあくまでゼロトラストにおけるネットワーク領域のはなし
  - アプリケーションやBYOD端末の対策もゼロトラストに含まれる。
- ゼロトラストの概念は「7つの大原則」をベースとしている
  - https://jp.ext.hp.com/techdevice/wolf/security_sc40_09/
- 今回は詳しく取り上げなかったが、「認証」「監視」「通信の保護」といったものを「すべて」行うことでゼロトラスト環境が実現できる。
- しかしすべてを既存システムに組み込むのは現実的に難しいものも多い。
- できるところから少しずつ取り組んでいくことが大事。

ありがちな質問：VPNとゼロトラストの違いって何？

- ほんとありがちな質問（僕もした）
- ぶっちゃけゼロトラストにおいてもVPN技術は使っているので「全く違う！」と言うわけではない。
- 言い換えるなら「VPN 2.0」または「シン・VPN」
- 今回の発表でなんとなくでも雰囲気が伝われば幸いです。

ちょっとした小ネタ：VPNの種類について

VPNについて、普段特に区別なく「VPN」と言われがちですが、実は4種類あります。
※VPNの種類を調べると、エントリーVPNとIP-VPNの順番が入れ替わっているものが多いですが、歴史的経緯からするとIP-VPNの方が先らしいので、順番を入れ替えて紹介します。

- インターネットVPN
  - SSL-VPN、IPSec、SoftEtherなど、特定のアプリケーションやプロトコルを使いインターネット上に仮想閉域網を作る方式
  - 普段使ってるVPNは大抵これを指す
- IP-VPN
  - NTTなどの通信事業者が提供している閉域網サービス
- エントリーVPN
  - NTTなどの通信事業者が提供している、ブロードバンド回線を介して閉域網に接続するサービス
- 広域イーサネット
  - IP-VPNの欠点であった、MPLSを利用した閉域網（L3レイヤでのIP通信網）を改善し、L2レイヤで閉域網を提供できるようになったサービス

参考：

- VPNと専用線の違いを分かりやすく解説
- エントリーVPN | 日経クロステック（xTECH）