今日から始める！
ゼロトラスト！２

ZTNAとCloudflareAccess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、仕事ではRHEL、趣味はUbuntu
- 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

※今回のゴメンナサイ※

「よっしゃ今回もゼロトラスト発表すっぞ！」

と書き始めたのが、ここ5日間のことです。。。

直前までこの資料を作ってました。。。

なので**説明不足なところやわかりにくいところが多い**です。

（全部GWとほりほりドリルが悪い）

資料は展開するので、わからないところはFediverseで！

(FediLUGのハッシュタグ追えるだけ追います)

前回のあらすじ：ゼロトラストとは

- 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
- 従来の侵入対策（VPNや境界型セキュリティなど）で放置されていたセキュリティリスクへの対策
- VPNだけでなく、ユーザ認証、クラウドサービス等を組み合わせて端末やサーバ、アプリケーションのすべてのセキュリティを担保する手法
- ネットワークに関するゼロトラスト：ZTNA(ZeroTrustNetworkAccess)
- tailscaleでも似たような技術が使われています。
- tailscaleクライアントはFW越え、NAT越えのためにひと工夫しています。
- レッツゼロトラ！

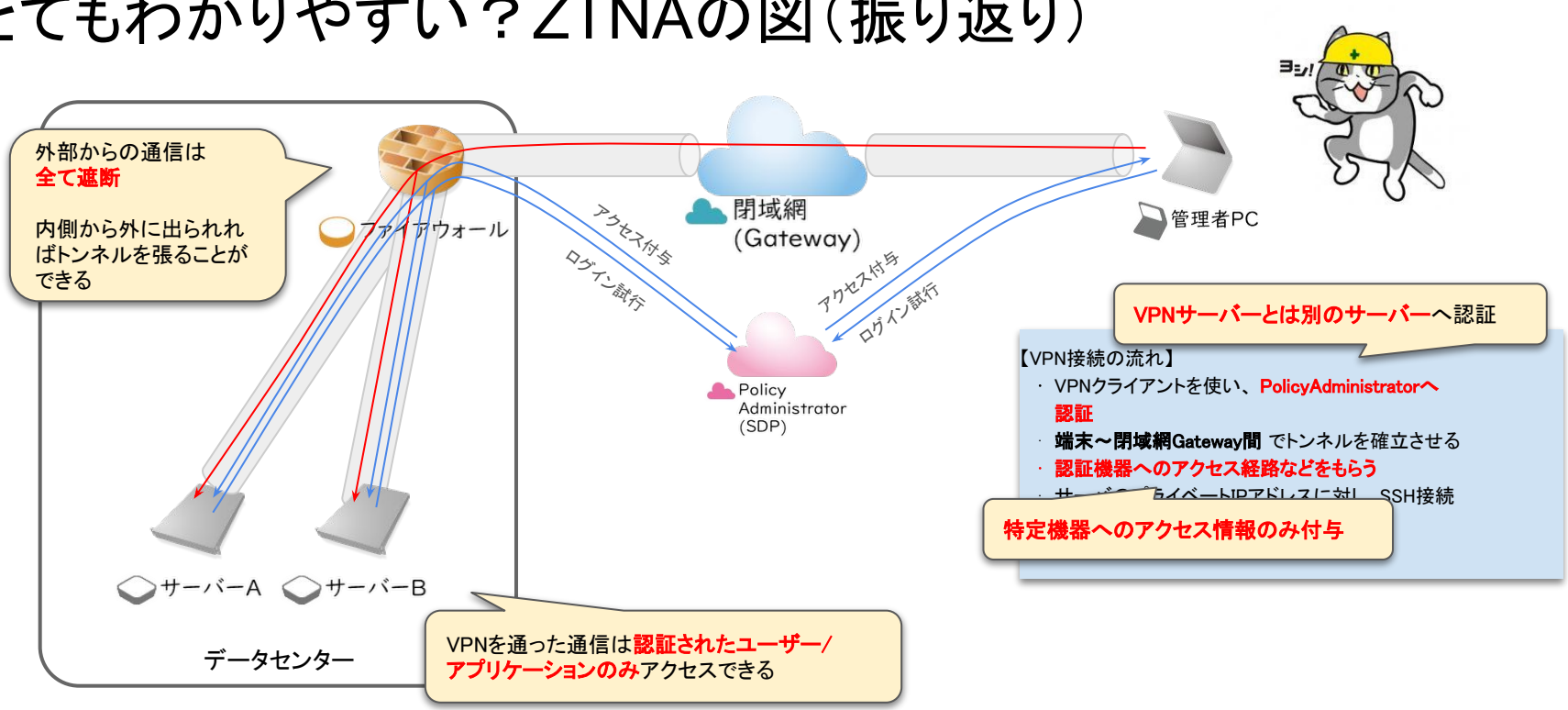
tailscale

前回の発表を聞き逃した方へ

資料は公開しているので良かったら見てね！

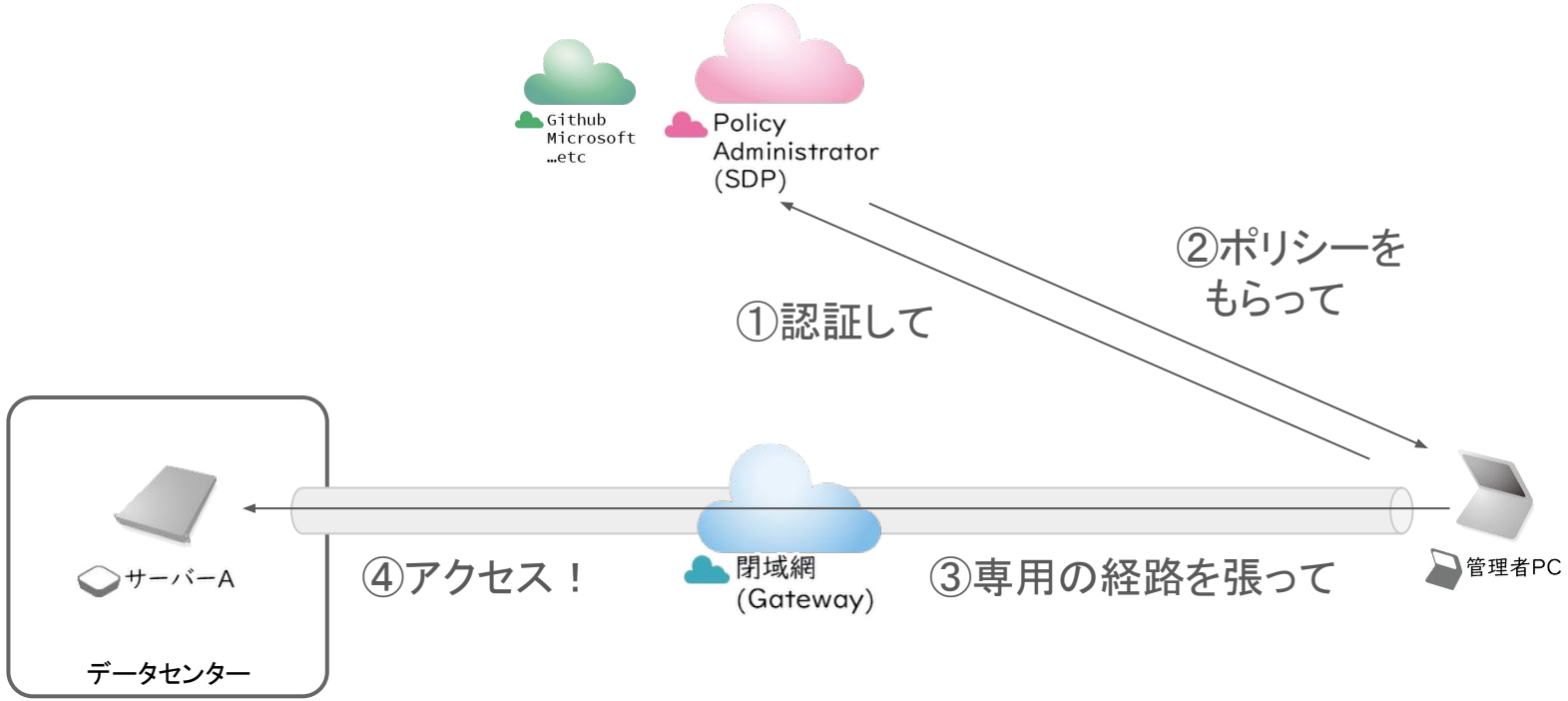
https://github.com/guskma/public_resource/blob/main/20240224_FediLUG%E7%99%BB%E5%A3%87%E8%B3%87%E6%96%99_guskma.pdf

とてもわかりやすい？ZTNAの図（振り返り）

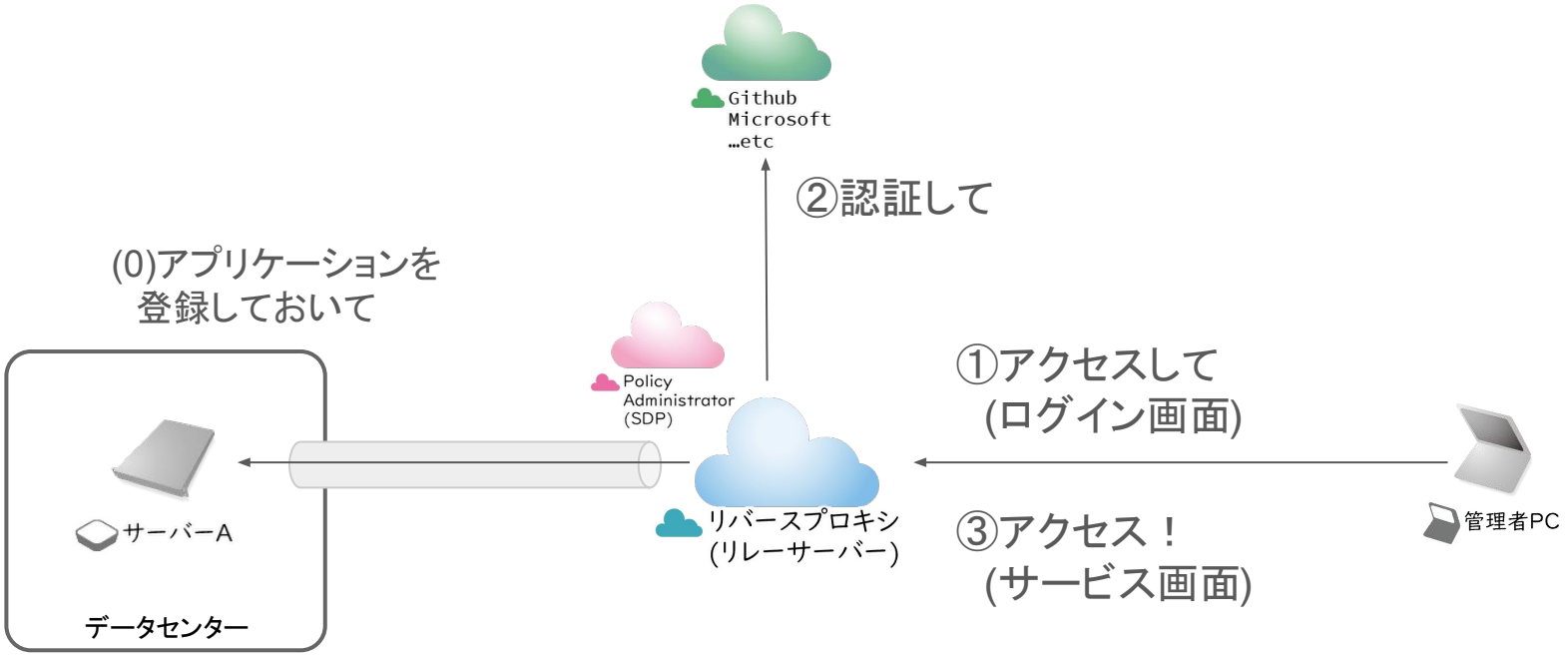


境界型セキュリティの欠点を解決。すべての機器に対して同一の対策が可能

前回紹介したのは、「SDPベース」のZTNA



今回紹介するのが、「プロキシベース」のZTNA



SDPベース vs プロキシベース

- SDPが **VPNの発展版** だとしたら プロキシは **BASIC認証の発展版**
  ※あくまで雰囲気
- SDPは**認証して初めて**接続を確立するが、プロキシは**認証前から**リレーサーバに接続を確立する。
- SDPは専用クライアント(VPNクライアント)が**必要になる場合が多い**が、プロキシは専用クライアントが**必要になる場合が少ない**。
- SDPは**特定のTCP/UDPポートを通す場合がある**が、プロキシは**汎用のHTTPSポートを利用する場合が多い**

セキュリティと取り回しのしやすさによって採用する方式を選択すること

SDPベース vs プロキシベース

	SDP	プロキシ
接続の確立	認証後	認証前
クライアント	VPNクライアント等	ブラウザ等
プロトコル	特定のTCP/UDPポート	HTTPS等

で、こういうのはCloudflareの得意分野です。

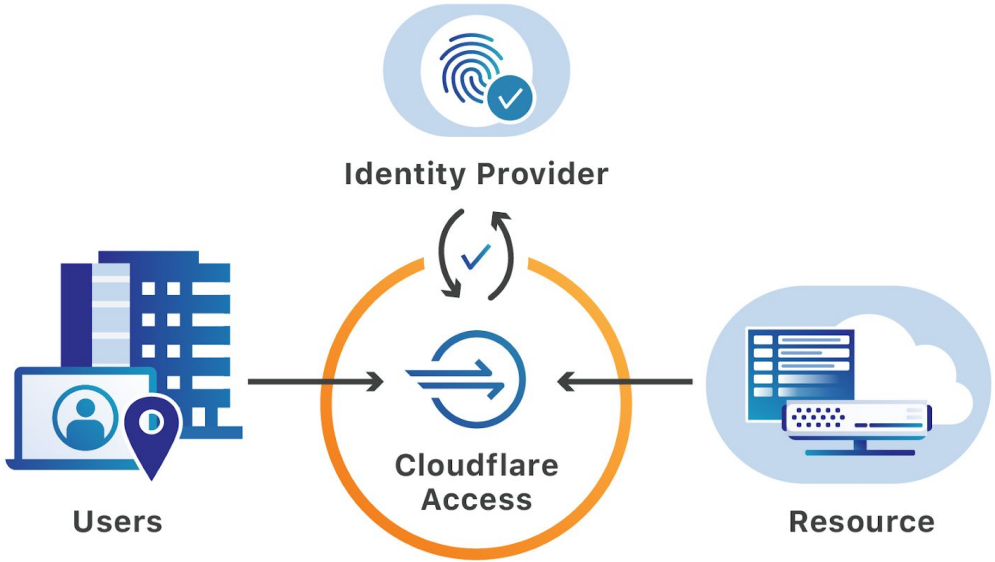
CDNやDNSなどでおなじみの米国のIT企業Cloudflare。
負荷分散、オリジンサーバ隠蔽などでCloudflareを利用している人も多いのではないでしょうか。

Cloudflare者が提供するゼロトラストサービス→その名もCloudflare ZeroTrust

→今回はその中でもCloudflareAccessについて説明

とてもわかりやすい？CloudflareAccessの図

公式ブログの紹介記事にそれっぽい図があったからもうこれでいいや（投）
https://blog.cloudflare.com/ja-jp/cloudflare-for-teams-products-ja-jp



まちめ

- 前回の発表と合わせ、2回に分けてゼロトラストについて紹介しました。
- いかがだったでしょうか？
- ゼロトラストを通して現在トレンドとなっているセキュリティ対策の一端を知り、サーバーを運用するうえで必要な安全性と信頼のあるシステムを構築することで、楽しいインターネット生活を送ることができるようになるという私の思いはになった

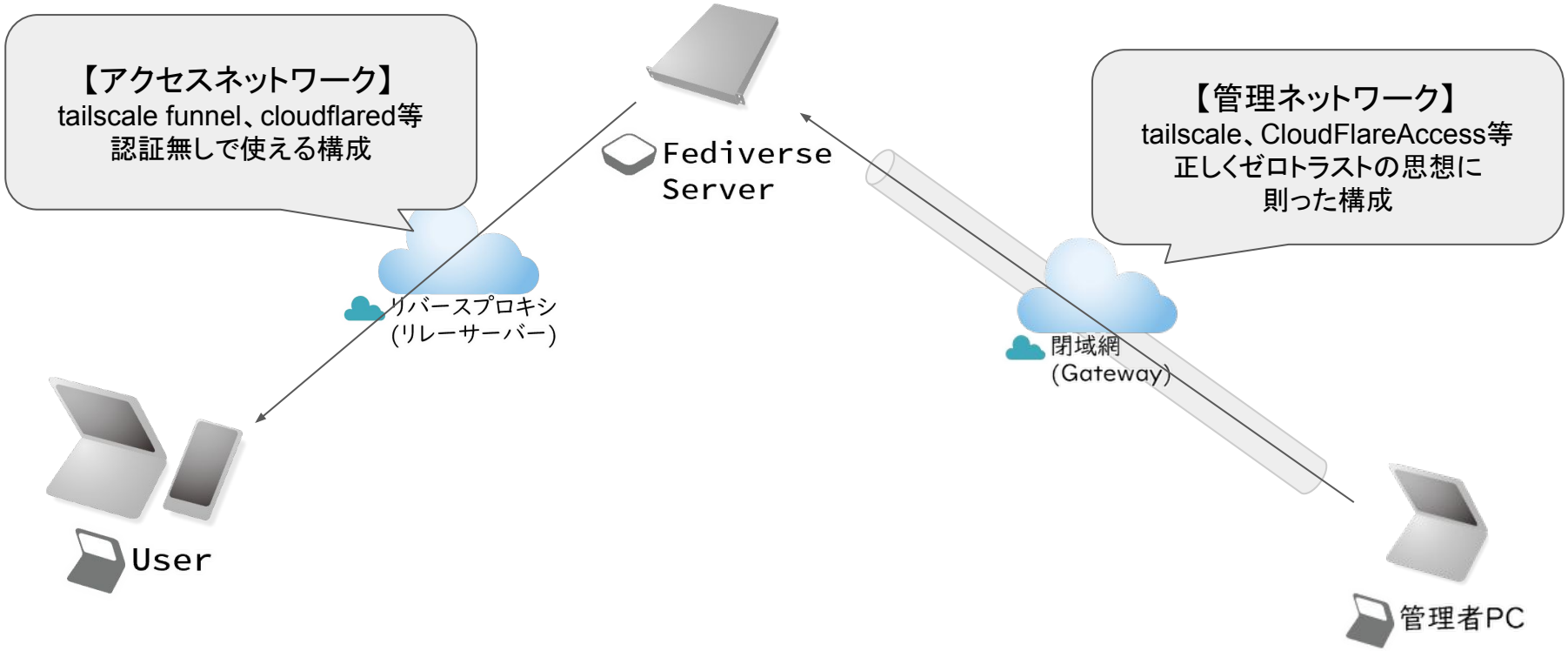
この発表（ゼロトラスト）って。。。

Fediverseをゼロトラスト化できるのか

限定的に対応することは可能

- ゼロトラストではすべてのデータや通信に対し、**所有者を明確**にし、**保護**しなければならない。
- **ActivityPubでは認証/認可の必要なく**不特定多数の人がみたり、他のサーバへフェデレーションできたりする。(他のプロトコルは未調査)
- 相容れない思想で設計されているため、Fediverseサービス（というか公開サービス全般）はゼロトラスト化することはできない。
- ただし、リバースプロキシやリレーサーバによるオリジンサーバの隠蔽、侵入対策やログ監査をすることにより、部分的にゼロトラスト化することは可能。
- 完全対応でなくても、概念を理解して適切にセキュリティ対策を取ることが大事

ざっくりこんな感じにすればいいんじゃね？の図



補足：tailscale funnelについて

そもそも今回の発表をしようとした根拠が「ウチのサーバーで使ってるcloudflaredとかtailscale funnelってゼロトラストなのでは？？？？」というのが発端だった。

ただ調べていくと、「これらはクライアント端末側からの認証がなくてもパブリックアクセスができ、ログの監査等もしていないので、厳密にはゼロトラストではない」というのが結論だった

→ただし、おそらくポリシーの設定しだいではクライアント端末側の認証も入れられるのではないか(未検証)

なので、これらはあくまで「ゼロトラストっぽい何か」として扱う程度が良さげ

ただし、Webサービスを一般公開するにはつよつよのつよなので入れておいてもいいかもしれない

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！