ゼロトラストアーキテクチャ
特権ID管理

2024/7/26

プロキューブ 中川路 充

特権ID管理とは

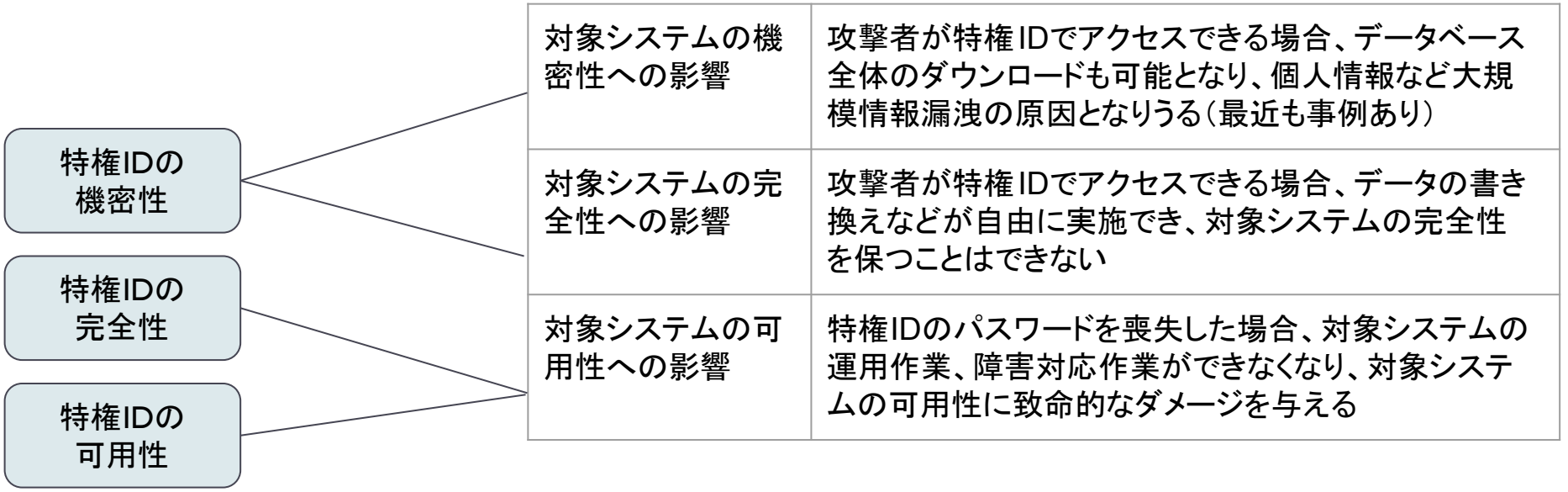
サーバやネットワーク機器の root アカウントや administrator アカウントのことを「特権ID」と呼びます。

サーバやネットワーク機器の保守業者は特権IDを使用して機器にアクセスする必要がありますが、特権IDは全ての情報にアクセスできるため、セキュリティ上の弱点となりやすいという課題があります。

これに対して、近年「特権ID管理」と呼ばれる製品を使用してセキュリティを高める動きがあります。

特権IDのパスワード/鍵の情報資産リスク

ITベンダーの情報セキュリティマネジメントシステムの中では、お客様のシステムの特権IDのパスワード/鍵の情報資産リスクが最も高い。



対象システムの機密性への影響	攻撃者が特権IDでアクセスできる場合、データベース全体のダウンロードも可能となり、個人情報など大規模情報漏洩の原因となりうる（最近も事例あり）
対象システムの完全性への影響	攻撃者が特権IDでアクセスできる場合、データの書き換えなどが自由に実施でき、対象システムの完全性を保つことはできない
対象システムの可用性への影響	特権IDのパスワードを喪失した場合、対象システムの運用作業、障害対応作業ができなくなり、対象システムの可用性に致命的なダメージを与える

セキュリティ施策例

特権IDのパスワードを厳重に管理

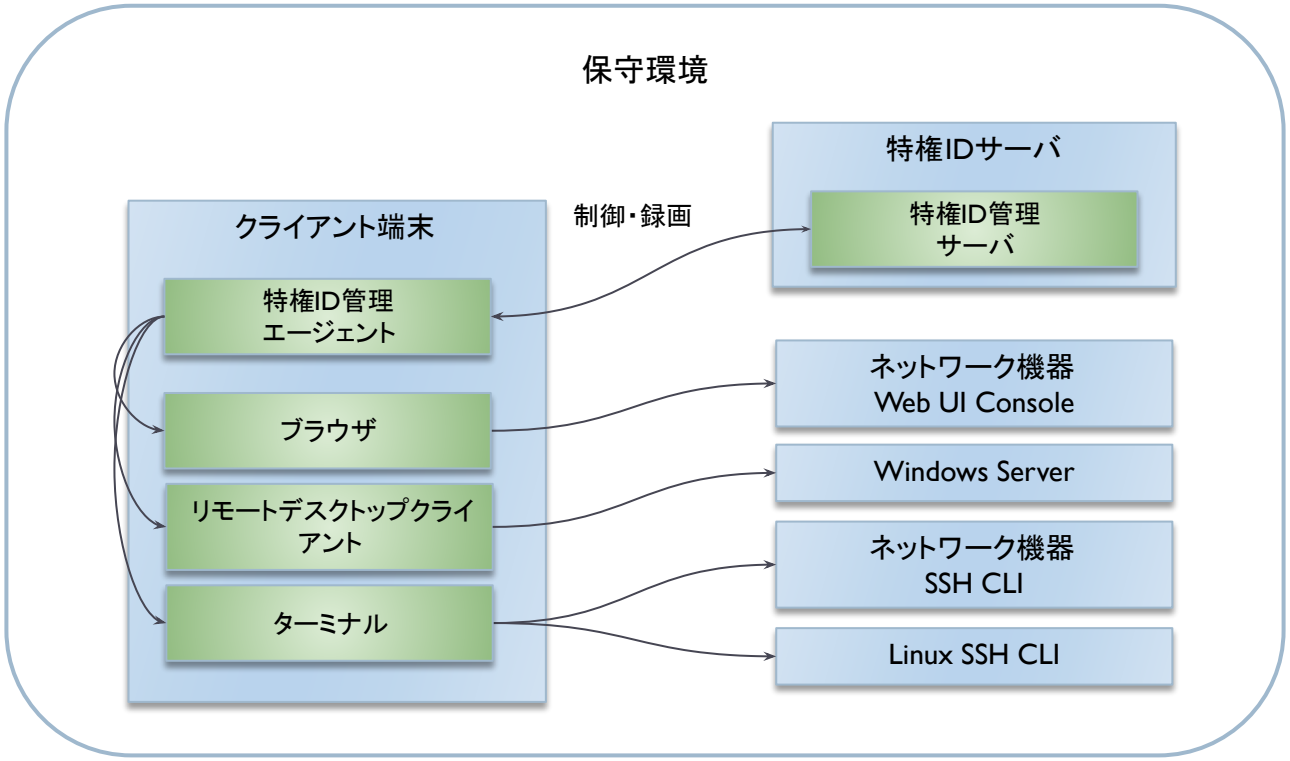
- パスワードをGoogleドライブにおいて、ダウンロードを禁止
- パスワードが書かれているファイルを見ると即時に管理者にメールが飛ぶようにアラートを設定

アクセスをワークフローで管理

- VPNへの接続に対しては接続時に接続申請書を提出
- 作業後に接続報告書を提出
- 管理者は報告書とVPN装置のログを照合して時間帯、ユーザIDが一致しているかを確認

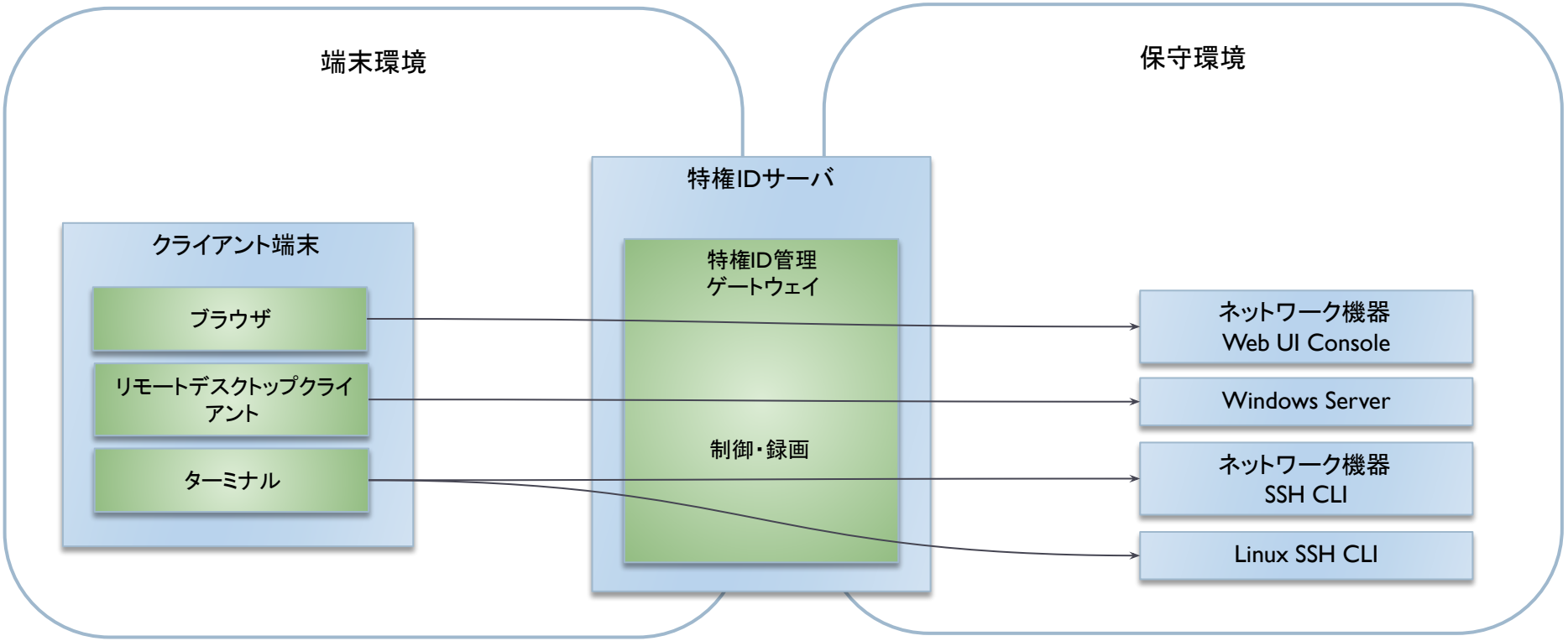
構成：クライアント型

- ネットワーク上はクライアントから機器に直接アクセスする



構成：ゲートウェイ型

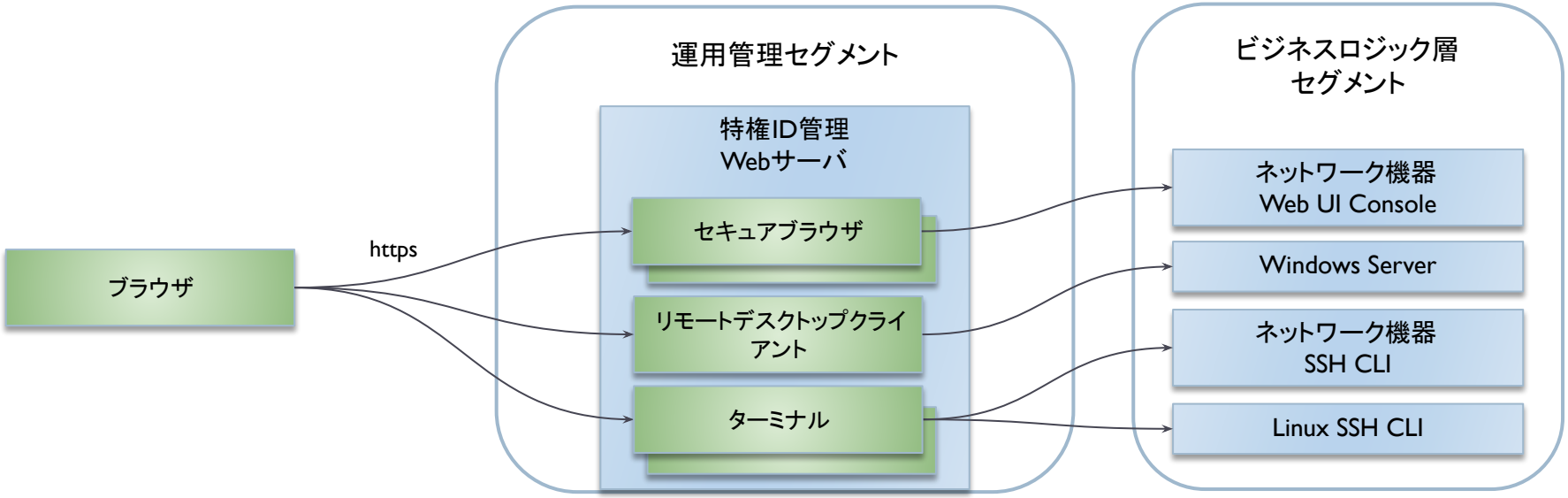
- いわゆるプロキシ的なアクセスとなり、完全分離ではない（=クライアント側で作成したパケットがサーバに到達する）



構成：ゼロトラスト型

ネットワーク完全分離で運用管理層と他の層をマイクロセグメントで分離

- Webサーバ上でブラウザ、リモートデスクトップ、SSH ターミナルを使用可能
- セキュリティリスクの原因となる踏み台端末は不要
- VDIの基盤を必要としないため高性能かつ低価格で構成可能
- IaaS 各社は ssh の画面転送機能は提供しており、多少の機能差はあるが、ワークフローなどの機能はなく、「特権ID管理」と呼ぶのは難しい
  - AWS: ASW Session Manager, AWS System Manager
  - Azure: Bastion
  - GCP: Cloud Identity-Aware Proxy

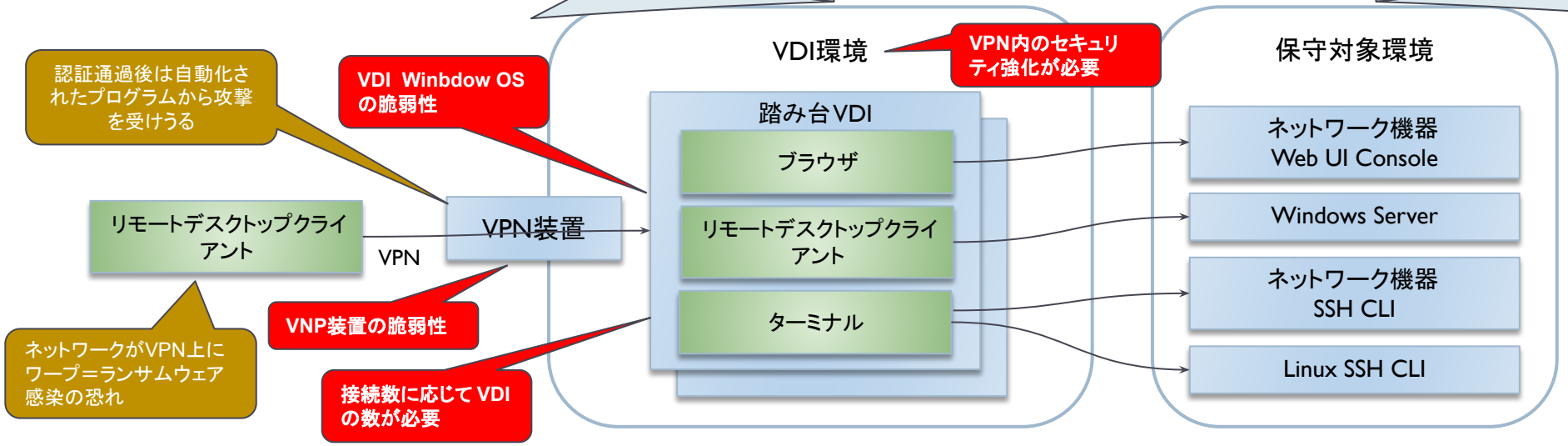


ゼロトラスト型の特長

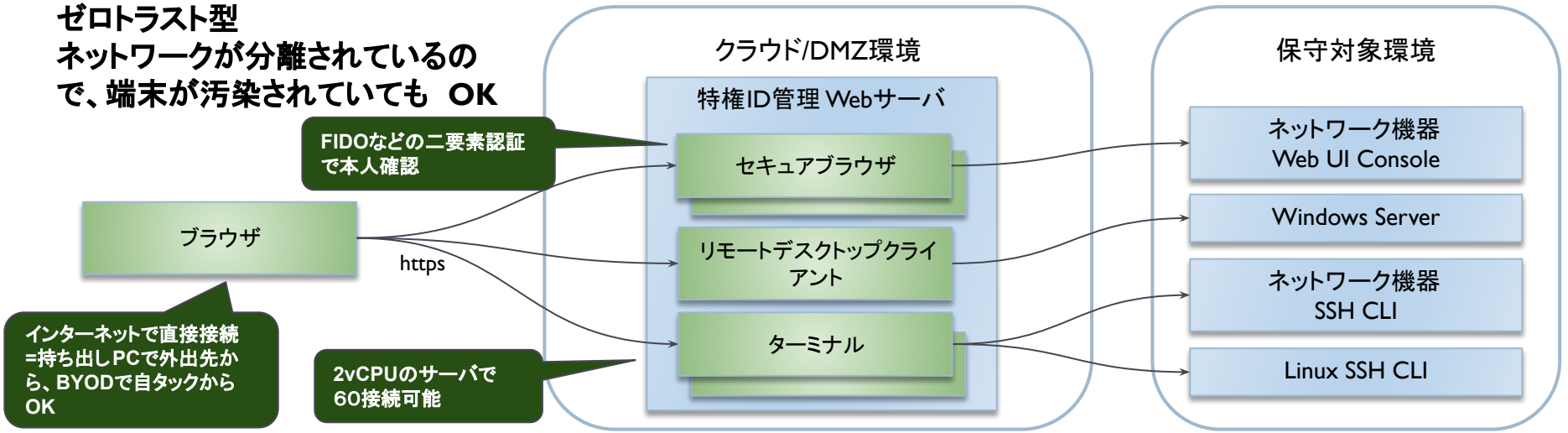
ZTA

保守対象はインターネットに接続されているように扱い、マイクロセグメンテーションと通信の暗号化を施す。
(M-22-09: 3. Network/4. Applications and Workloads)

クライアント型 /ゲートウェイ型＋端末が信用



ゼロトラスト型
ネットワークが分離されているので、端末が汚染されていても　OK



株式会社プロキューブ

要件：保守対象機器への代行ログイン

ZTA

PEP/PDP実現のために、まず、ユーザが直接保守対象にログインできないようにする。

~~root のパスワードはみんなが知っている~~

- ユーザの代わりに保守対象機器に保守用のユーザIDでログインすることを代行ログインという
- 代行ログインに使用するパスワードや秘密鍵がユーザにもれないようにすることで特権でのアクセスを特権ID管理サービス経由でないとできないようにする
- SSH：パスワード、秘密鍵による代行ログイン
- リモートデスクトップ：パスワードによる代行ログイン
- ブラウザ：ログインフォームをHTML内に発見するとIDとパスワードを自動的に入力して代行ログイン
- ブラウザの代行ログインはログイン時の挙動をブラウザのデバッグツールで解析し、自動ログインの設定を行う必要がある

要件：作業管理、ID管理、インベントリ管理

ZTA

Subject/Resourceを管理し、厳格な特権利用を申請・承認ワークフローで
Policy Defineする。
(M-22-09: 2. Devices)

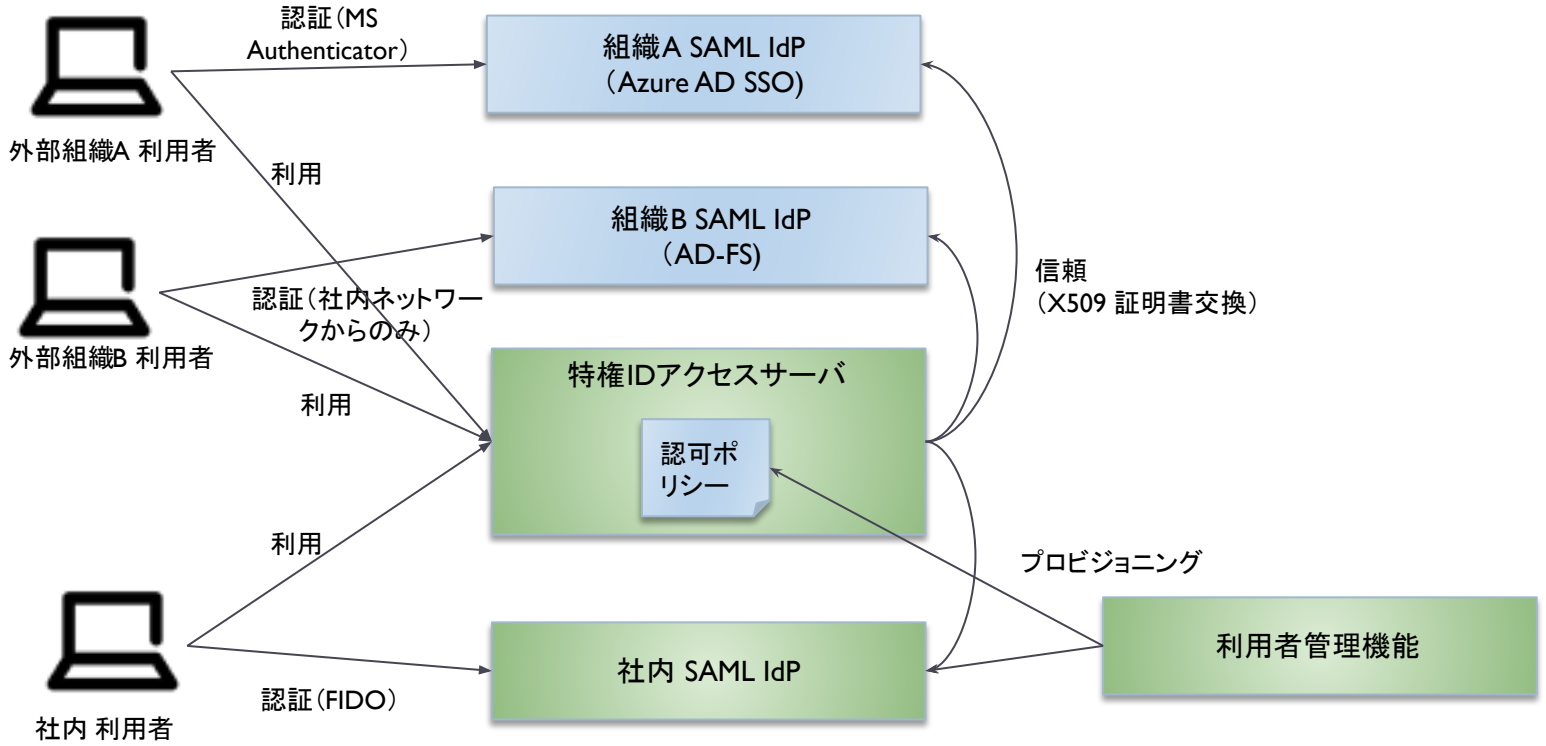
機能	ユースケース	説明
申請・承認ワークフロー	起票	許可グループ、接続先機器、特権IDの権限、ファイルのアップロード/ダウンロードの有無を指定して接続を申請できます
	承認	接続申請を承認/却下できます
	確認・取り消し	申請状況の確認ができます。申請の取り消し、承認の取り消しができます
利用者管理	認証連携設定	認証サーバとの連携内容を設定できます
	利用者管理	利用者の登録・変更・削除を行えます
	グループ管理	グループの登録・変更・削除を行えます
対象機器管理	接続設定登録	IPアドレス、ポート番号、プロトコル、特権ユーザID、パスワード、秘密鍵などを指定して対象機器を登録できます
	確認・変更・削除	登録されている接続設定のリストを確認し、変更/削除できます
	パスワード自動変更	登録されている接続設定に対して、パスワードやペア鍵を生成し、対象機器側のパスワード/公開鍵の変更を行えます

要件：利用者のWeb認証

ZTA

組織が管理するIDの利用、MFAの利用 (M-22-09: 1. Identity)

- SAMLによる認証連携により利用者の認証を所属組織に委譲
  - 他のアプリケーション(ex. Office 365, Google workspace, Box)とシングルサインオンが可能
  - MS Authenticator, FIDO など組織固有の認証を利用可能
  - 退職者のID無効化、所属・役職の変更などの管理を所属組織に委譲することで認証の品質を担保



株式会社プロキューブ

特権ID管理製品の機能

ワークフロー機能

作業者がシステムに特権 IDでアクセスするためにはワークフローで作業申請しシステムのオーナーの許可を得る必要があります。

- 作業者が勝手にアクセスしてシステムに意図しない変更が加えられるのを防ぐ
- システムの秘密情報が知らない間に抜き取られるのを防ぐ

パスワード管理機能

特権IDのパスワードは特権 ID管理システムが自動的に設定し、作業者がアクセスする場合は代行ログインを行うため、作業者はパスワードを知らなくても特権IDでの作業を実施できます。

- 作業者は特権 IDのパスワードを管理する必要がなく、漏洩、紛失などのセキュリティリスクを軽減できる

ネットワーク完全分離機能

作業者が対象機器の SSH、RDP、WebUIにアクセスする際にそのプロトコルに 直接アクセスするのではなくブラウザ内に画像としてレンダリングされた端末を操作します。

- 各プロトコルを使用した攻撃を一切受け付けない
- VPNに頼らないゼロトラストアーキテクチャを構成できる

ファイルサーバ

対象機器とのファイル交換は専用のファイルサーバを経由します。外からは Web UI でしかアクセスできず、ウィルススキャンも行います。対象機器には WinSCP に似た UI でファイルを転送できます。すべてのアクセス履歴が残ります。作業ごとにファイルサーバの利用を制限できます。

- ウィルスの混入を防ぐ
- サーバから勝手に秘密情報がダウンロードされるのを抑止

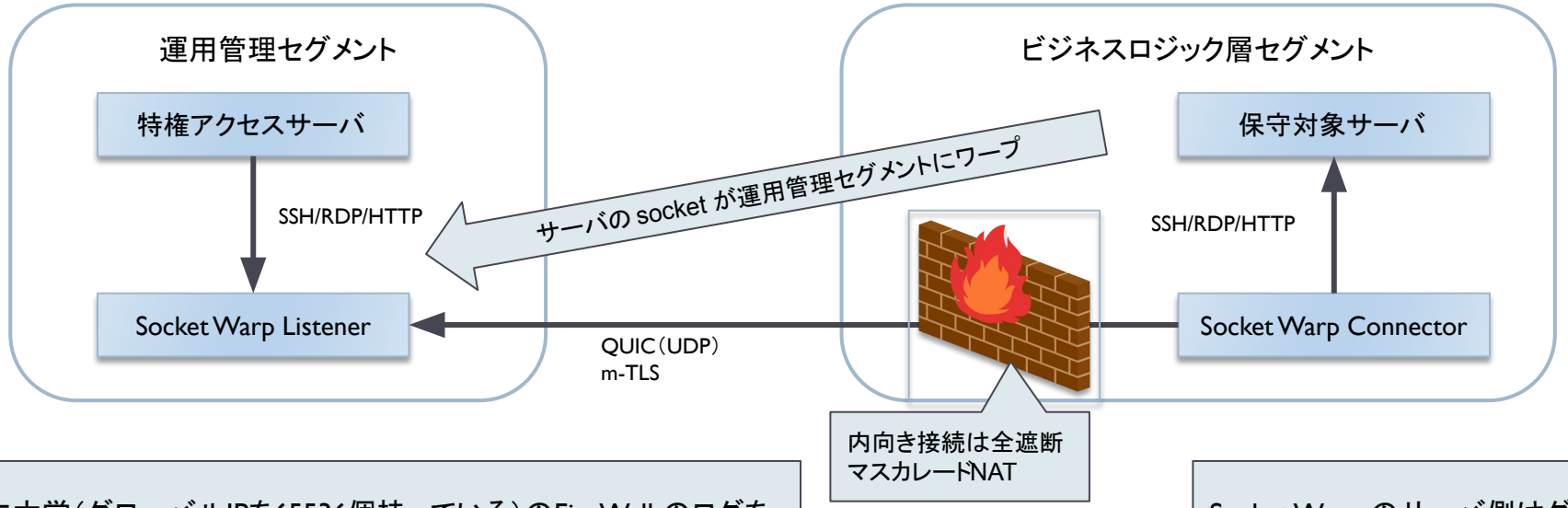
録画機能

作業中のレンダリング内容は録画されて、後で再生することが可能です。

- 作業ミス発生時に再発防止策の策定に利用可能

実装例：Socket Warp 接続

- クラウド上の特権ID管理サービスから保守対象環境のネットワークに安全に接続
- 保守対象機器のネットワークはインターネットとのファイアウォールで内向き全遮断＆マスカレードでも接続可能
- インターネット上は m-TLS で暗号化し、サーバ証明書とクライアント証明書で相互認証
- サーバからIPとポートを指定してワープするため、追加のアクセス制御は不要
- Socket Warp Connector は保守対象環境のサーバにインストールするか、Raspberry Pi を設置することで利用可能
- Socket Warp Connector を複数台設置することで冗長負荷分散が可能
- ワープ後はVPC内のIPアドレスとなるためクラウド上 VPCSocketと保守対象環境でネットワークアドレスがかぶっていてもワープ可能



- 国立大学（グローバルIPを65536個持っている）のFireWall のログを見ていると一回スキャンが来ると40億回のアクセスがある
- AWS の WAF で見ていると1時間に1件くらい攻撃を検出する
- サーバ証明書を取るとそのFQDNの存在が公開される

Socket Warp のサーバ側はグローバルIPもサーバ証明書もない→ポートスキャンで攻撃される可能性を0に

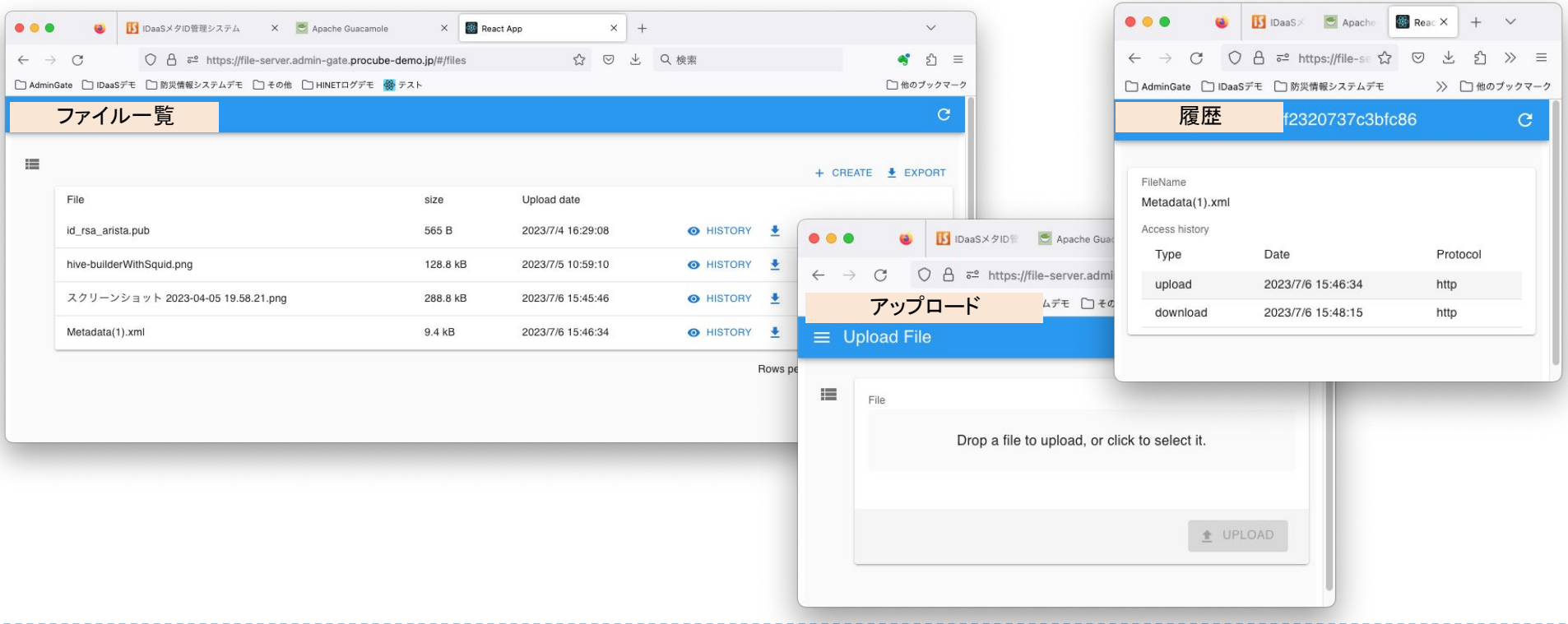
実装例:パスワード自動変更

特権ID管理システムは対象機器のパスワードを自動的に変更します。

対象機器のOSの機能	実装方法	設定数	設定作業内容	難易度
Junos, IOS など ansible のユーザ管理モジュールが提供されているもの	ansible の専用モジュールでパスワードを書き換える	OS毎	playbook を作成し、テストする	C
SSH/Telnet のCLIでパスワード変更が可能なもの	ansilble の expect/telnet モジュールでCLIを呼び出してパスワードを変更する	対話パターン毎	対話内容を採取し、対話をシミュレートする playbook を作成し、テストする	B
REST API でパスワード変更が可能なもの	ansilble の uri/get_url モジュールでREST APIを呼び出してパスワードを変更する	OS毎	API仕様を調査し、APIを呼び出す playbook を作成し、テストする	B
Web UI でしかパスワードが変更できないもの	Selenium により、自動ログイン後、パスワード変更画面に遷移し、パスワード変更フィールドを検出して、パスワードを自動的に入力する	OS毎	入力手順を採取し、手順をシミュレートするseleniumuのPythonスクリプトを作成し、テストする	S

実装例:ファイルサーバ

- 保守対象機器内のファイルをファイルサーバにアップロード後、手元にダウンロード
- 手元のファイルをアップロード後、保守対象機器にダウンロード
- どちらからアップロードされたものに対してもウィルススキャンを実行(最初のバージョンでは ClamAV のみ対応、将来的にはメジャーなアンチウイルスソフトに対応)
- 以下のような制限が可能
  - ワークフローで許可を得ないとダウンロード/アップロードできない
  - ダウンロード/アップロードすると管理者に通知メールが出る
  - ダウンロード/アップロードにサイズ制限がある



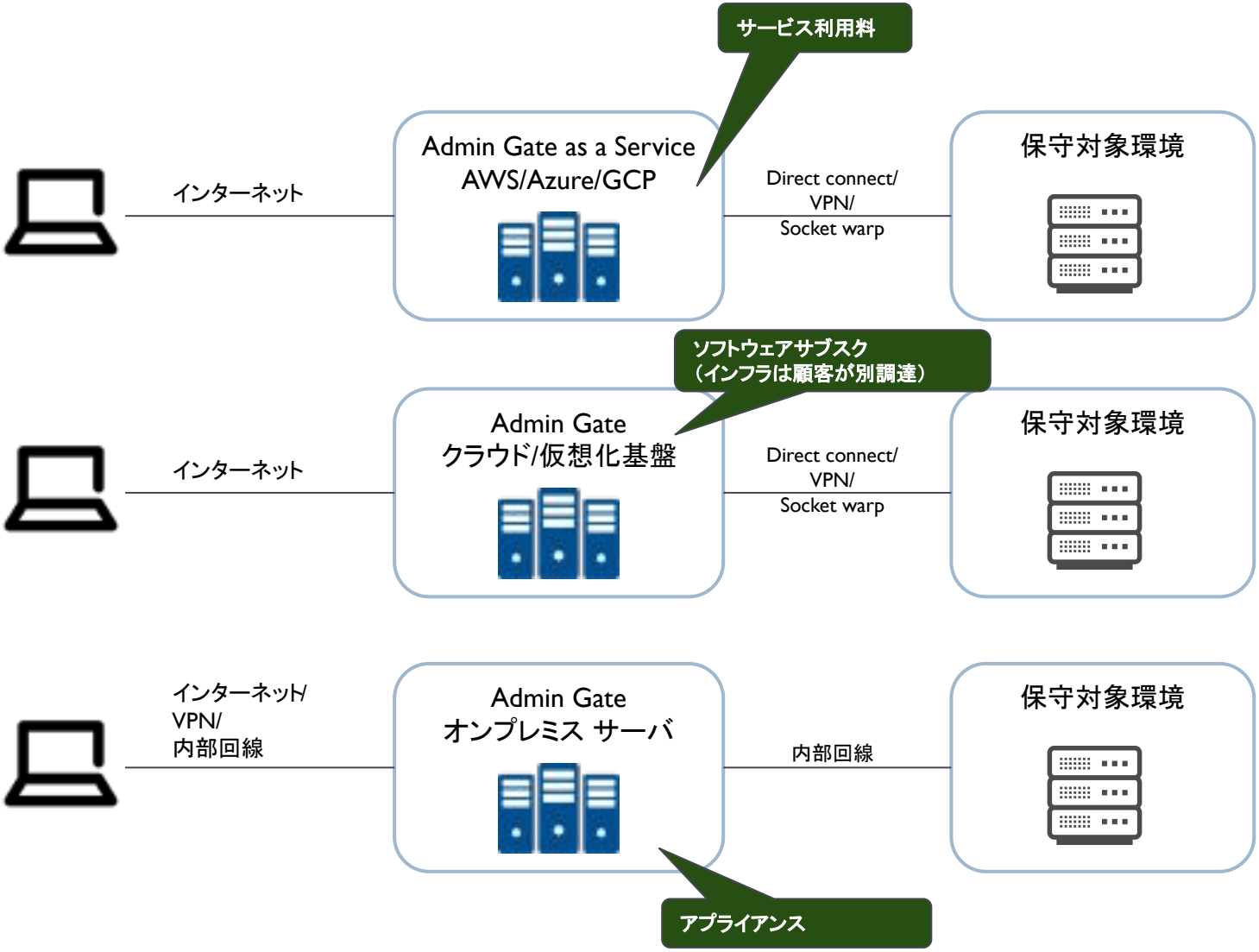
株式会社プロキューブ

実装例:性能

- 踏み台サーバを必要としないため少ないリソースで多数の接続を処理可能
- セキュアブラウザが最もリソースを消費し、1接続ごとにvCPU1個と1Gのめもりを必要とします

アプリケーション	プロトコル	1vCPUあたりの最大同時接続数	メモリ1 Gあたりの最大同時接続数
リモートデスクトップ	RDP	5.5	27
ターミナル	SSH/Telnet	30	50
セキュアブラウザ	HTTP/HTTPS	2.3	2.5

実装例：設置パターン


サービス利用料
Admin Gate as a Service
AWS/Azure/GCP
インターネット
Direct connect/
VPN/
Socket warp
保守対象環境
ソフトウェアサブスク
（インフラは顧客が別調達）
Admin Gate
クラウド/仮想化基盤
インターネット
Direct connect/
VPN/
Socket warp
保守対象環境
インターネット/
VPN/
内部回線
Admin Gate
オンプレミス サーバ
内部回線
保守対象環境
アプライアンス

特権ID管理システムの弱点

特権ID管理システム自身が攻撃されたり、障害で落ちたりすると業務システムの保守ができなくなる。

↓

ビジネスロジック層セグメントへの接続を完全に塞いでしまうことはできない？踏み台残す？

特権ID管理自身のインフラ（ex. AWSコンソール/API, VSphere Client, iLO/IDRAC）が取られると、対抗できない

↓

インフラをマイクロセグメント化し、認証を強化 or 物理的遮断（何かあったらデータセンタに行く）