●JAMF NATION LIVE

IT管理者のためのNetwork Relay活用ガイド
～導入から運用まで～



Naoki Hoshiyama

SECURITY SALES MANAGER

Agenda

1. Network Relayとは？
2. 信頼のチェーン（Chain of Trust）
3. Network Relay の設定・活用例

THREAT

MFA バイパス攻撃

- **セッションハイジャック**
  VPNやサーバーの脆弱性を悪用したトークンの奪取
- **AiTM フィッシング**
  リバースプロキシ経由でのトークンを奪取
- **SIM スワップ**
  電話番号を乗っ取り、SMS のコードを取得
- **MFA プロンプト爆撃**
  ユーザーへ大量のプロンプトを送信

THREAT

MFA バイパス攻撃

- **セッションハイジャック**
  VPNやサーバーの脆弱性を悪用したトークンの奪取
- **AiTM フィッシング**
  リバースプロキシ経由でのトークンを奪取
- **SIM スワップ**
  電話番号を乗っ取り、SMS のコードを取得
- **MFA プロンプト爆撃**
  ユーザーへ大量のプロンプトを送信

COUNTERMEASURE

フィッシング耐性 MFA

- ✓ **FIDO2 / WebAuthn（パスキー など）**
  ハードウェア・セキュリティキー
- ✓ **プラットフォーム認証器（Touch ID など）**
  ハードウェア・セキュリティキー
- ✓ **PKIベース認証**

Network Relay とは

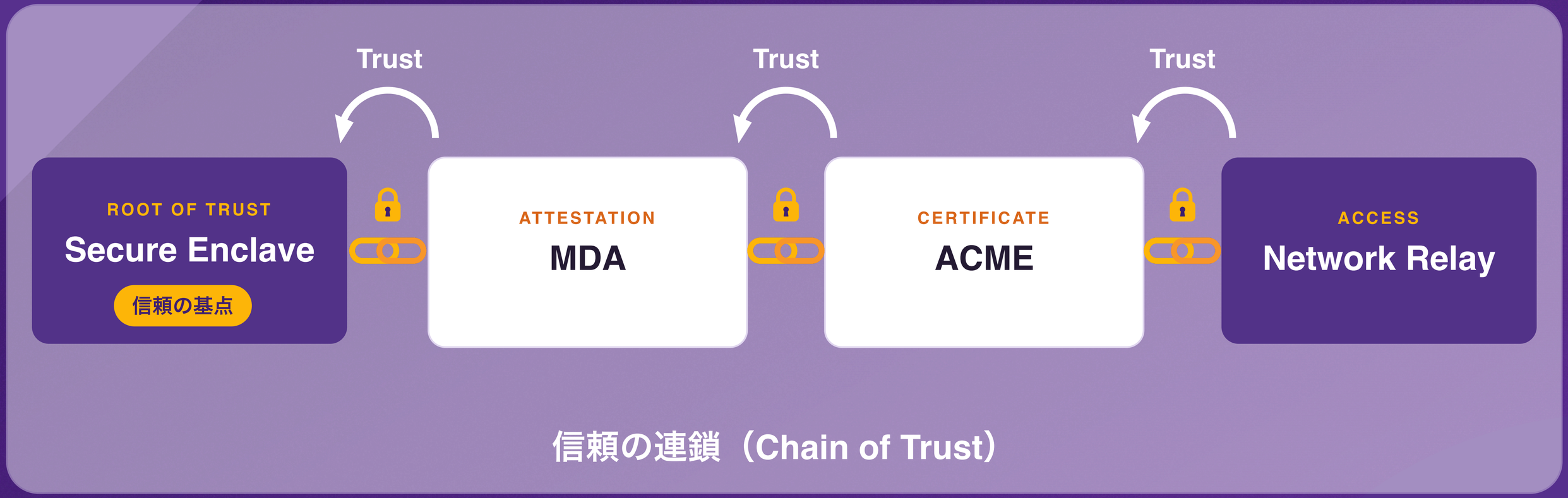
“ Appleデバイス の「強力なデバイス認証」に基づき
特定の通信を「安全に中継」するAppleの技術 ”

「Root of Trust（信頼の起点）」

ROOT OF TRUST

Secure Enclave

信頼の基点



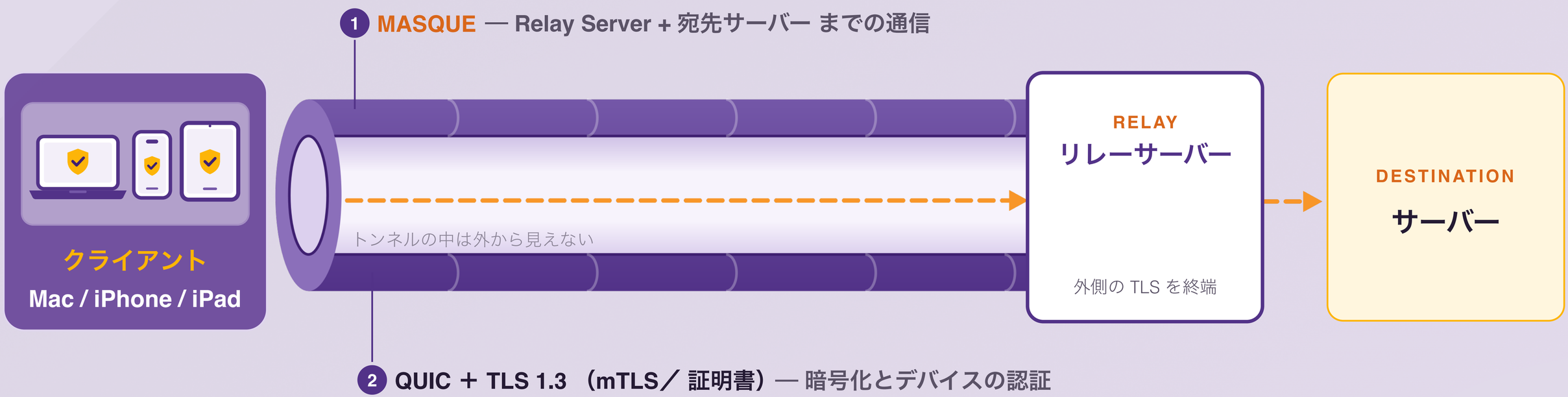
信頼の連鎖（Chain of Trust）


CERTIFICATE
クライアント証明書
ACCESS
Network Relay
相互TLS
安全な通信
SERVER
サーバー
証明書による「デバイス認証」

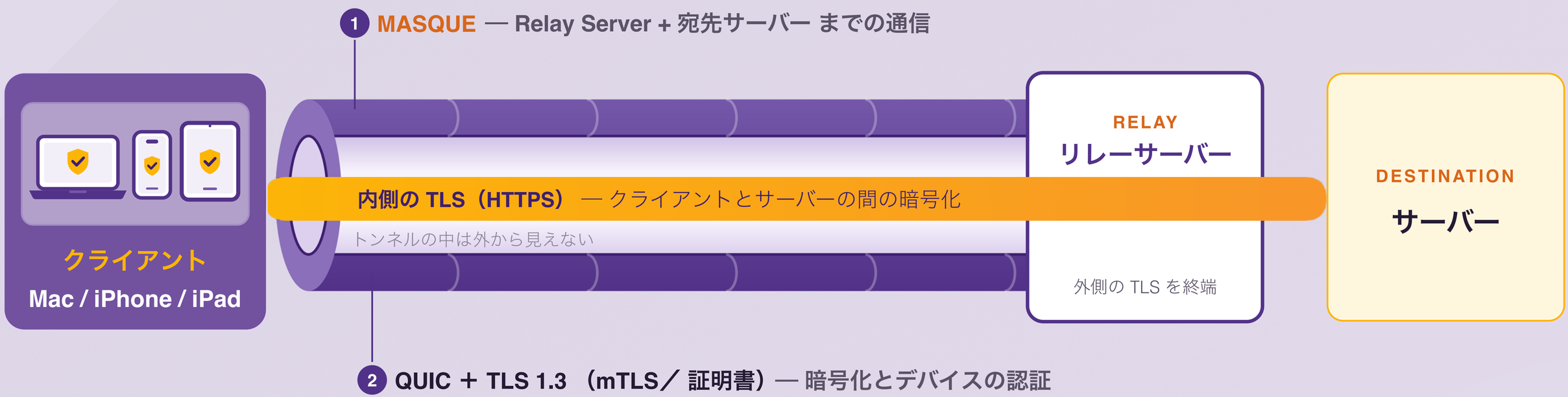
Network Relay とは

“ Appleデバイス の「強力なデバイス認証」に基づき

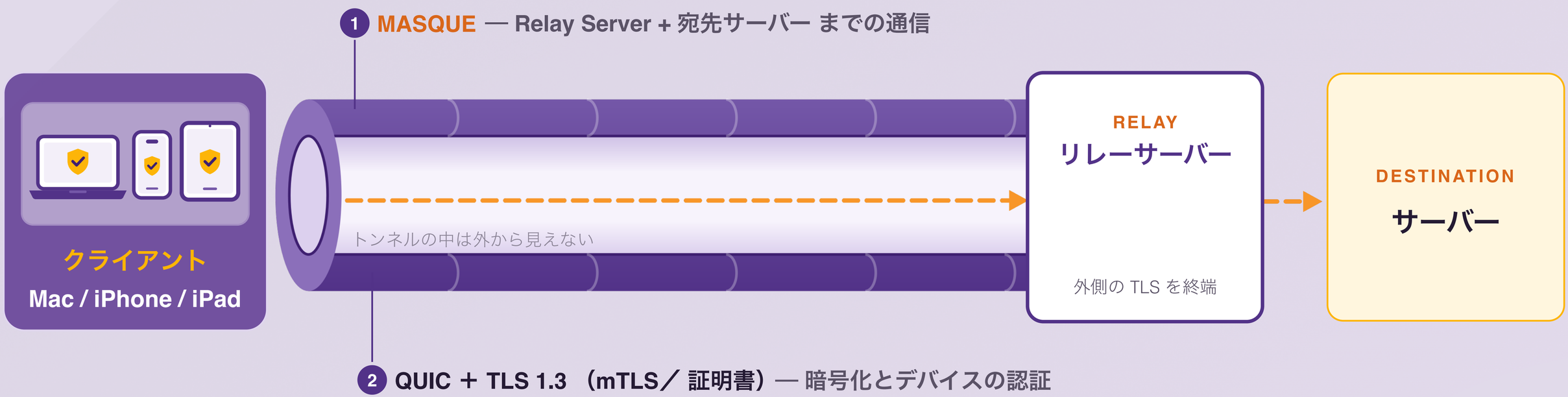
特定の通信を「安全に中継」するAppleの技術 ”



Network Relayによる「通信の中継」



Network Relayによる「通信の中継」



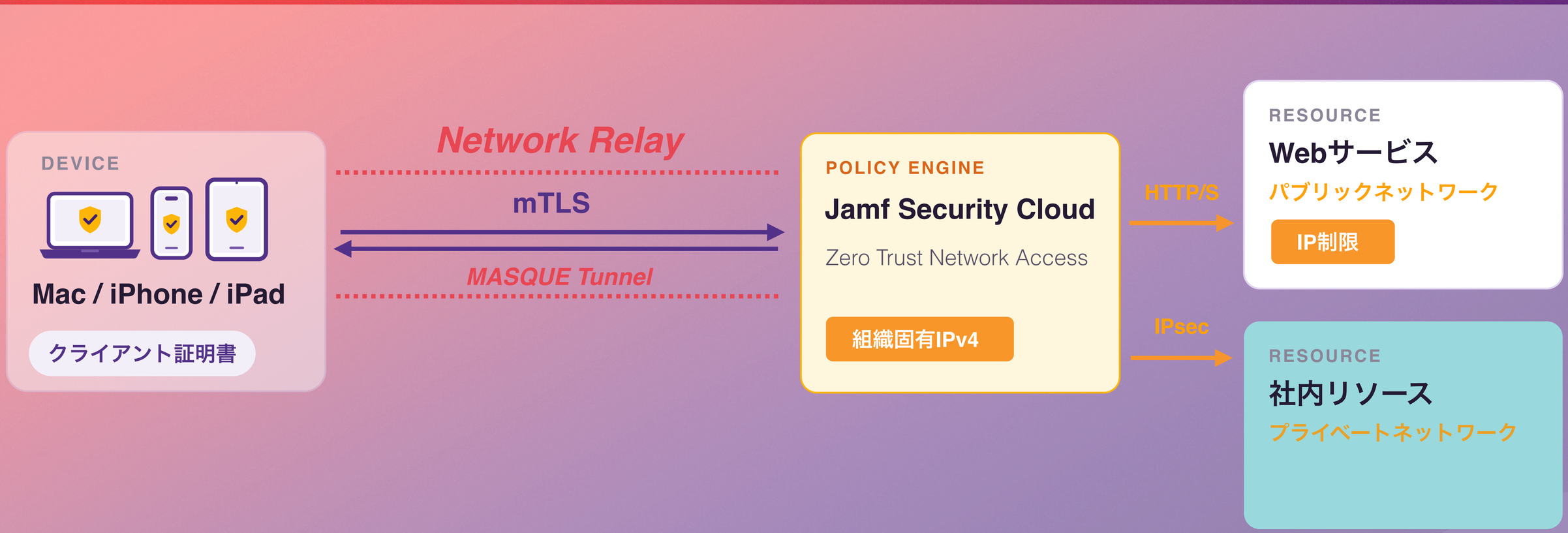
Network Relayによる「通信の中継」

Jamf Security Cloud への実装

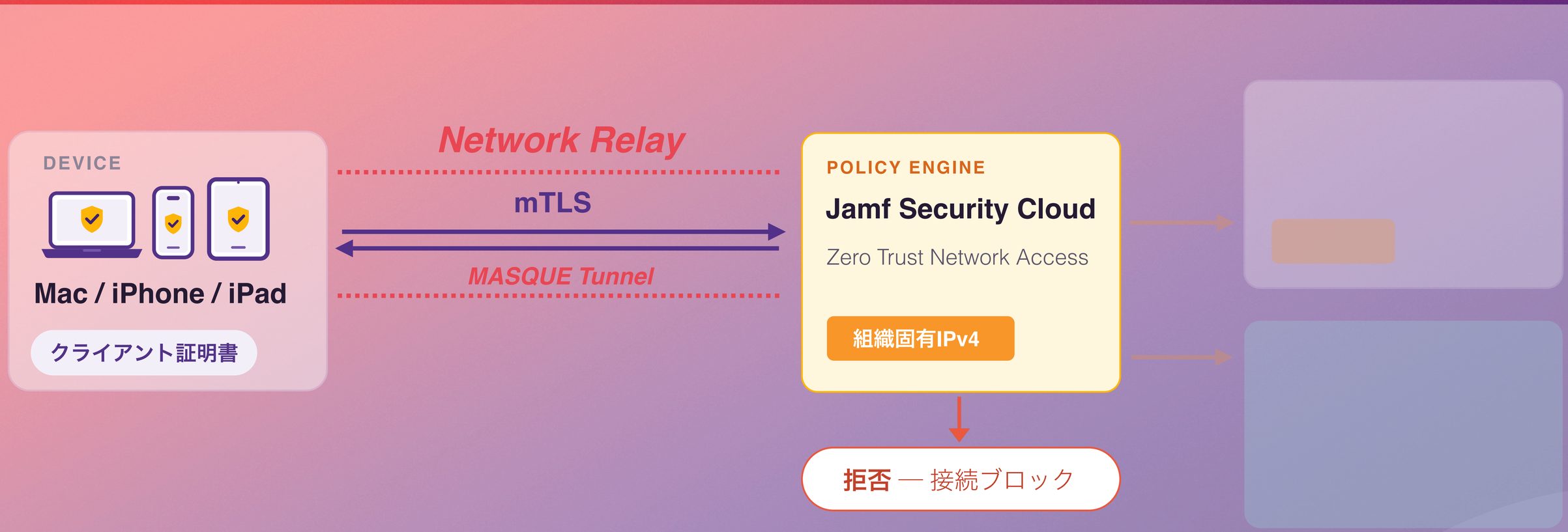
NETWORK RELAY AVAILABILITY

Network Relay の提供状況

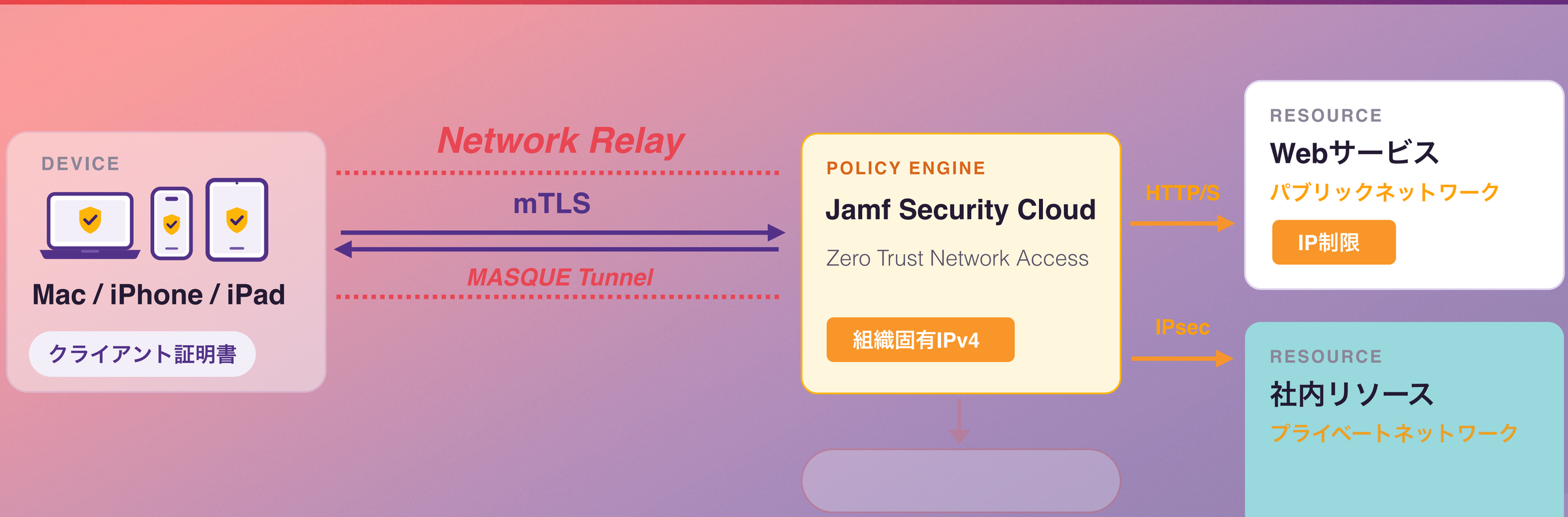
 iOS・iPadOS	***Release Candidate***
 macOS	***Release Candidate***



Jamf Security Cloud への実装



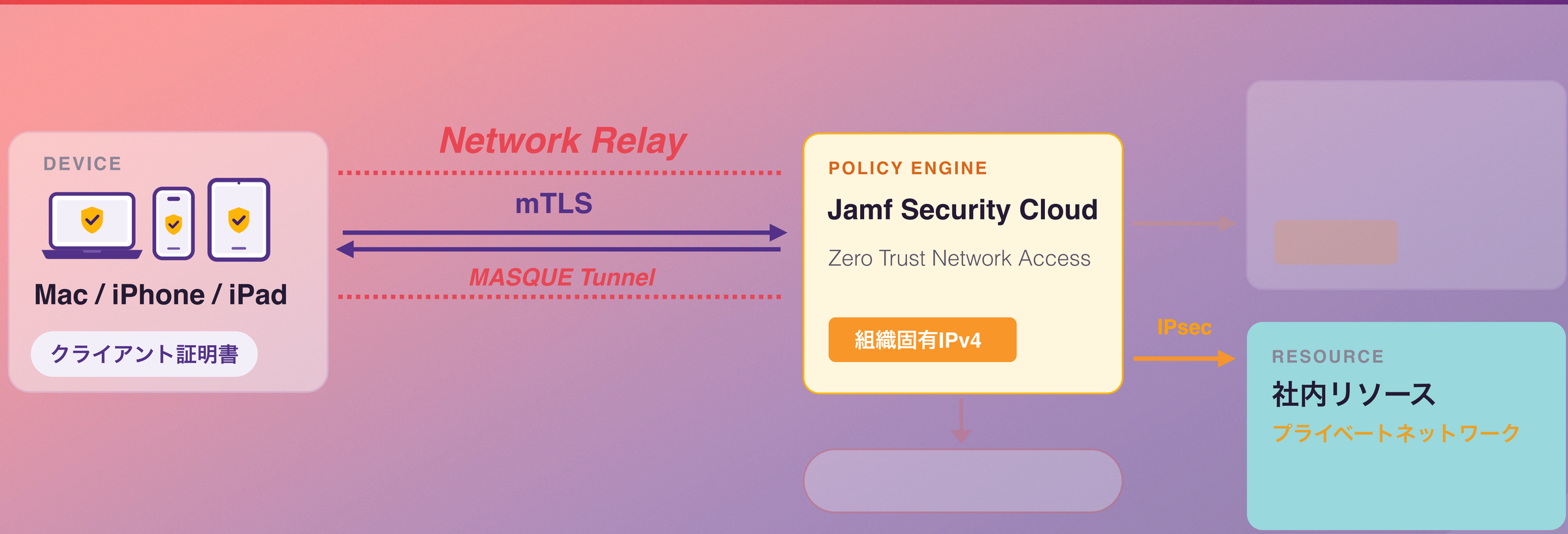
Jamf Security Cloud への実装



Jamf Security Cloud への実装

Network Relay のメリット

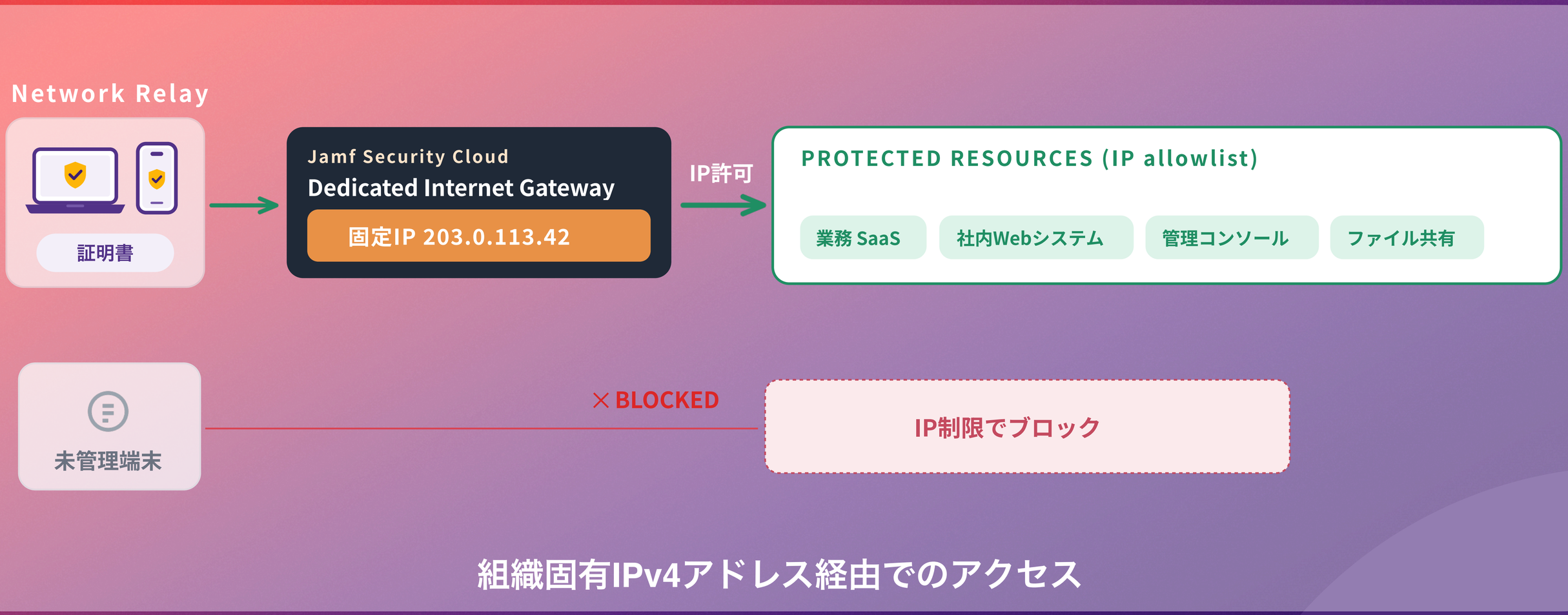
- 強固なデバイス認証を提供
- VPNの代替として利用可能
- 固定IPアドレス経由で接続可能
- ID／PWが不要



社内リソースへのアクセス（VPNの代替）

Network Relay のメリット

- 強固なデバイス認証を提供
- VPNの代替として利用可能
- 固定IPアドレス経由で接続可能
- ID／PWが不要

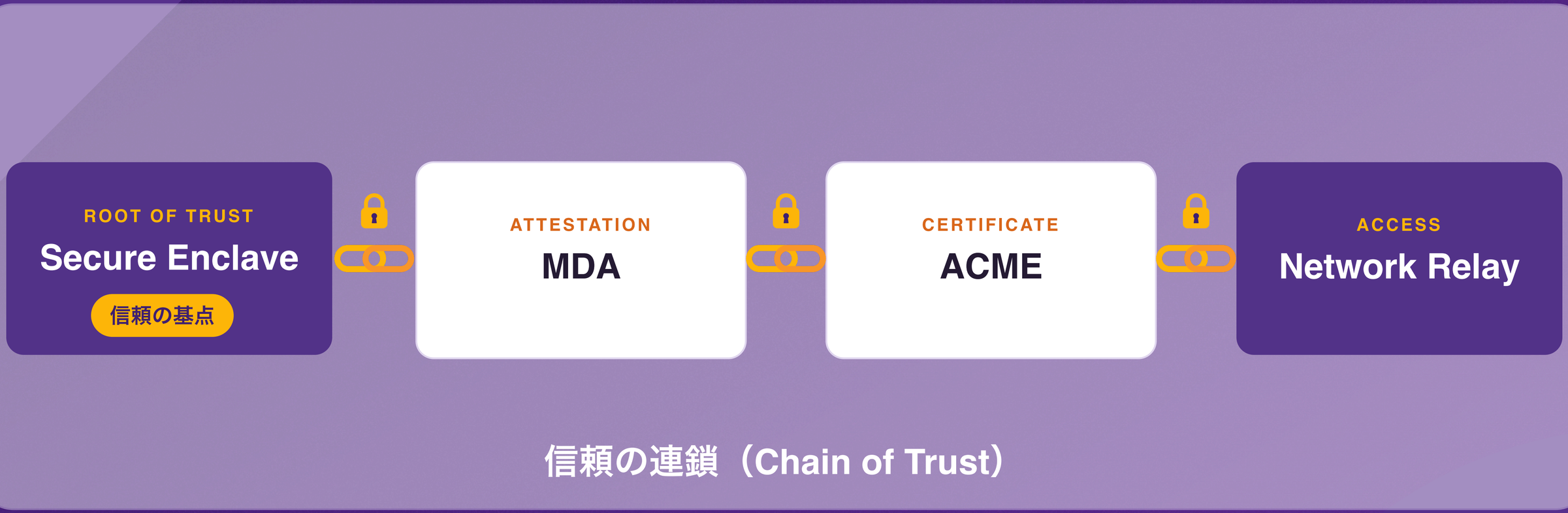


組織固有IPv4アドレス経由でのアクセス

Network Relay のメリット

- 強固なデバイス認証を提供
- VPNの代替として利用可能
- 固定IPアドレス経由で接続可能
- ID／PWが不要

信頼の連鎖（Chain of Trust）



信頼の連鎖（Chain of Trust）

Platform SSO

PASSWORD SYNC

パスワード同期方式



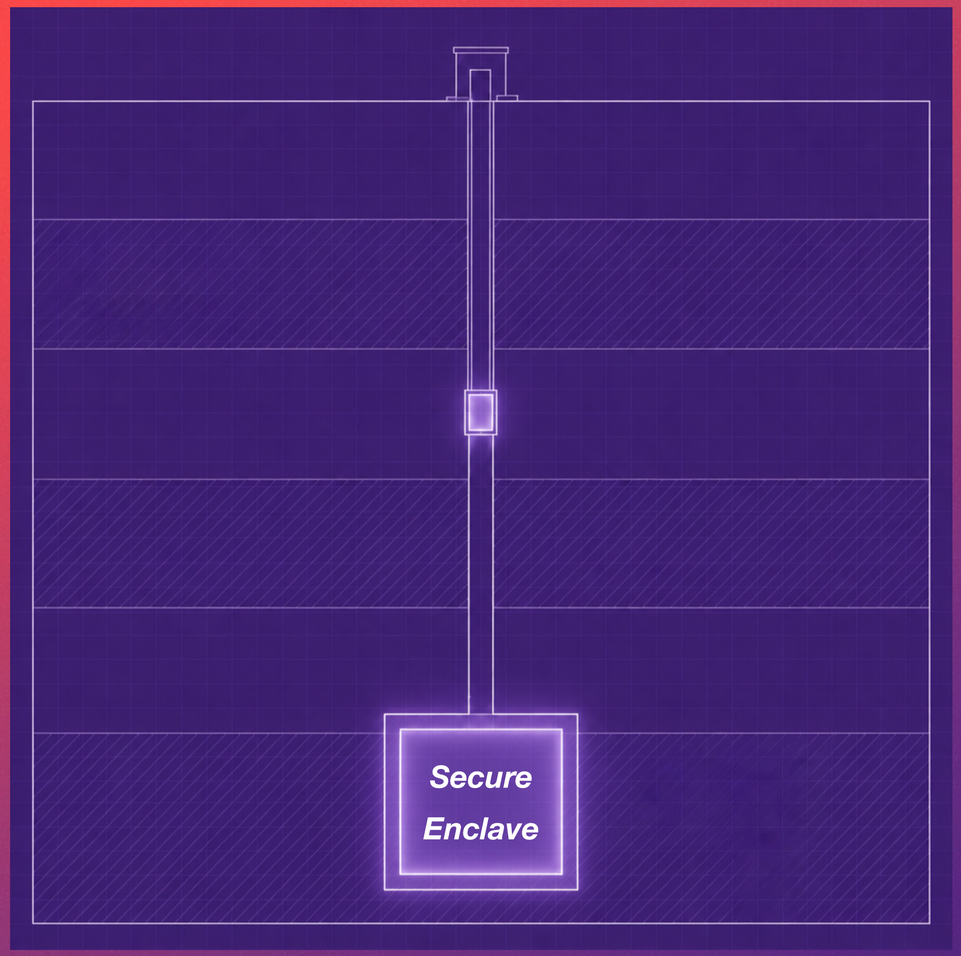
SECURE ENCLAVE

Secure Enclave 方式



Secure Enclaveの活用例

Secure Enclave ——例えるなら核シェルター

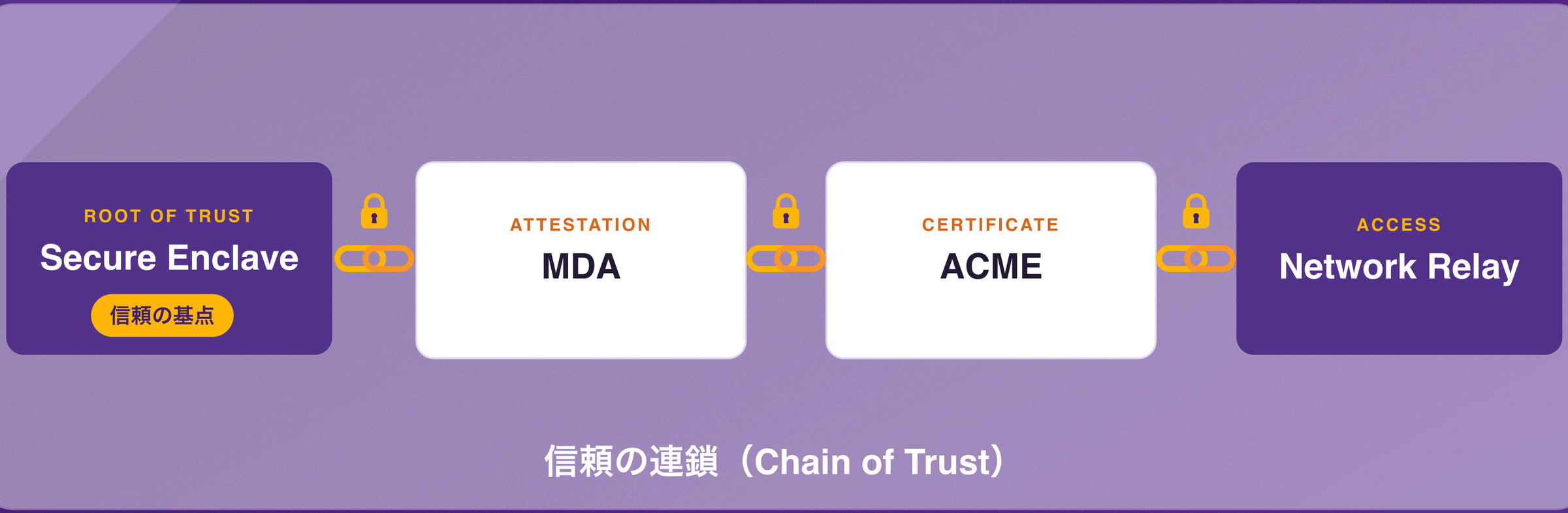


Secure Enclave ——例えるなら核シェルター



Secure Enclave

- 外界の影響を受けない
- 外から中を覗けない
- 保管しているデータが持ち出せない
- 異常検知でシステム停止



信頼の連鎖（Chain of Trust）

私は 01A57Bです！



Secure Enclave

自分の身元を宣言

私も 01A57Bです！



????

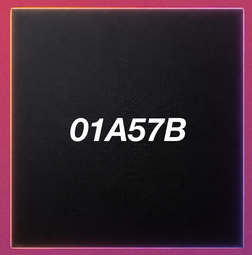
私は 01A57Bです！

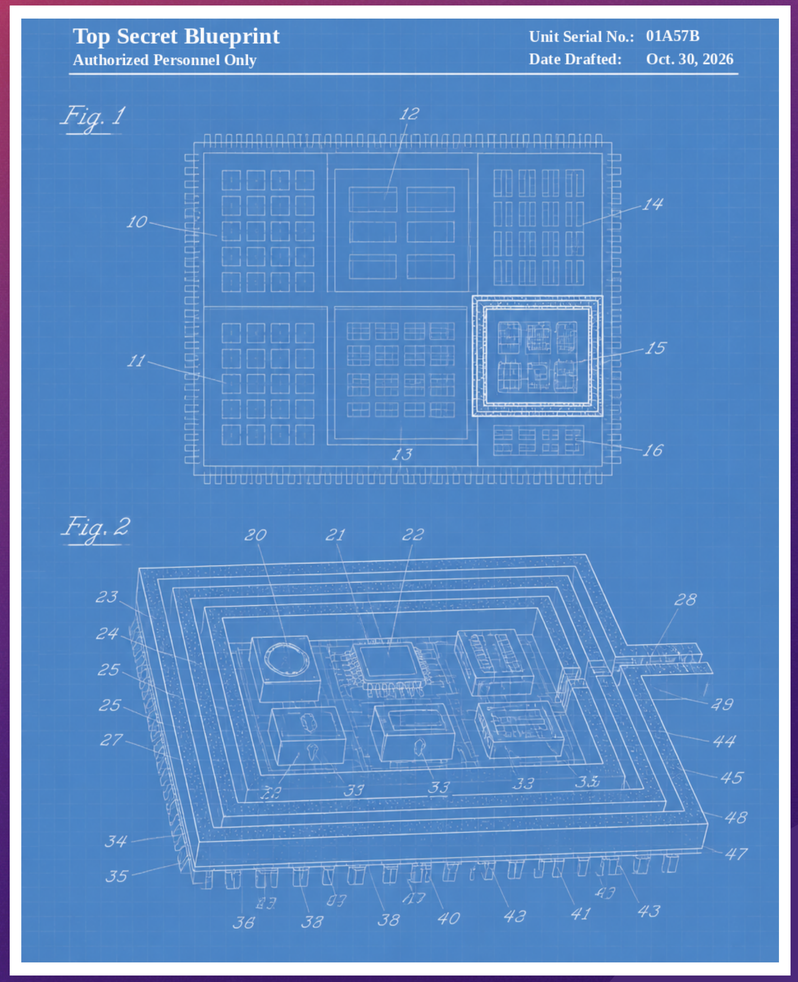


Secure Enclave

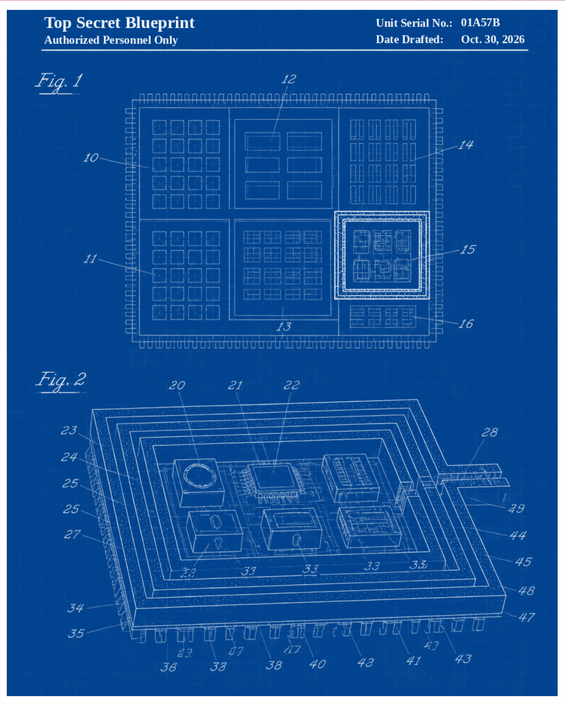
どのように証明する？

私は 01A57B です！
＋私の設計図 です！

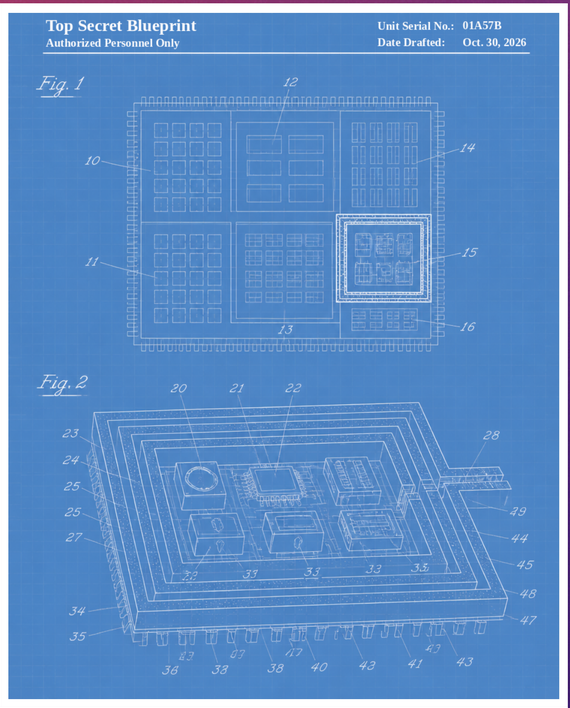




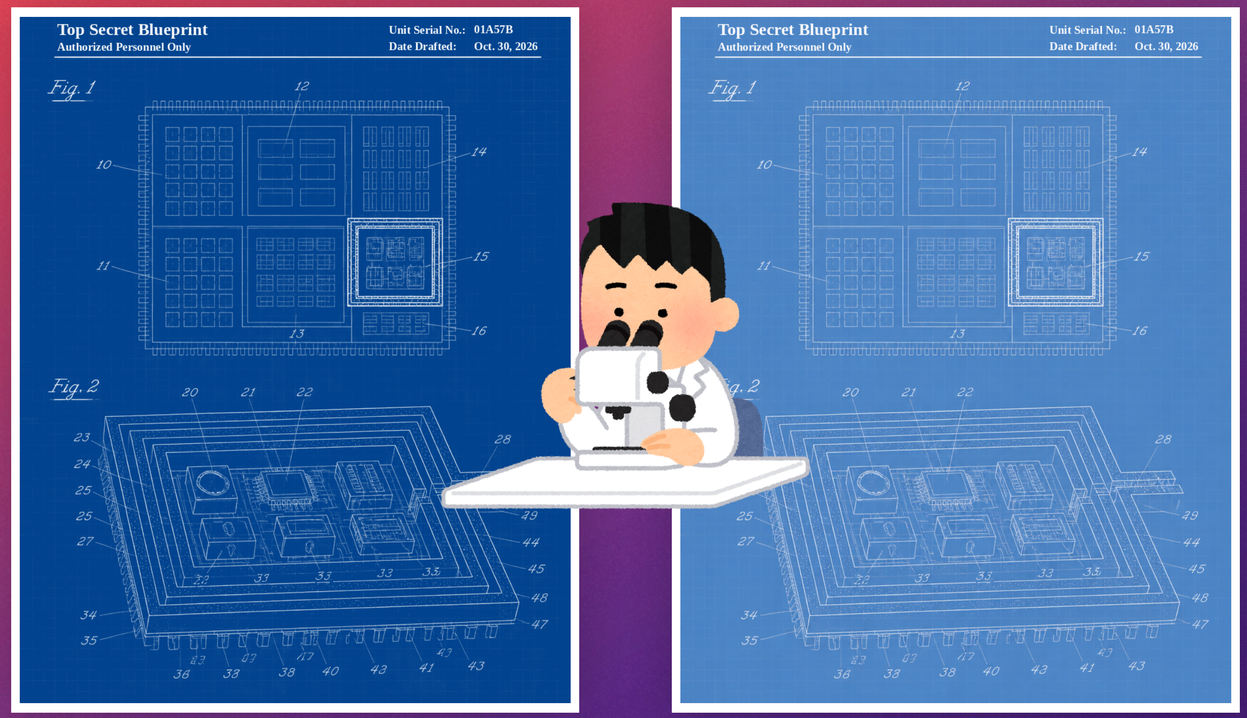
Appleが保持している情報



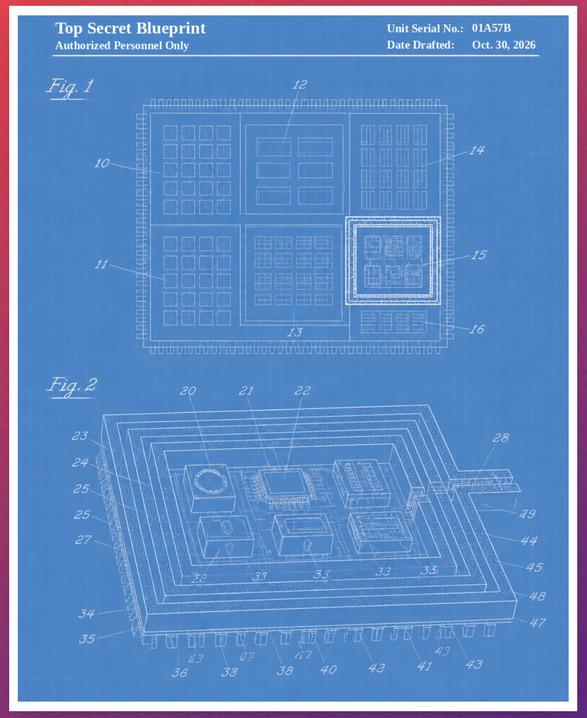
提出されたもの



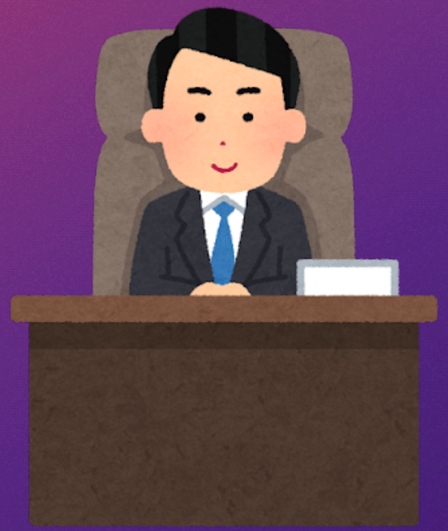
Appleが保持している情報　　提出されたもの



提出されたもの


Top Secret Blueprint
Authorized Personnel Only
Unit Serial No.: 01A57B
Date Drafted: Oct. 30, 2026
Fig. 1
Fig. 2

署名



Appleの正式な証明書

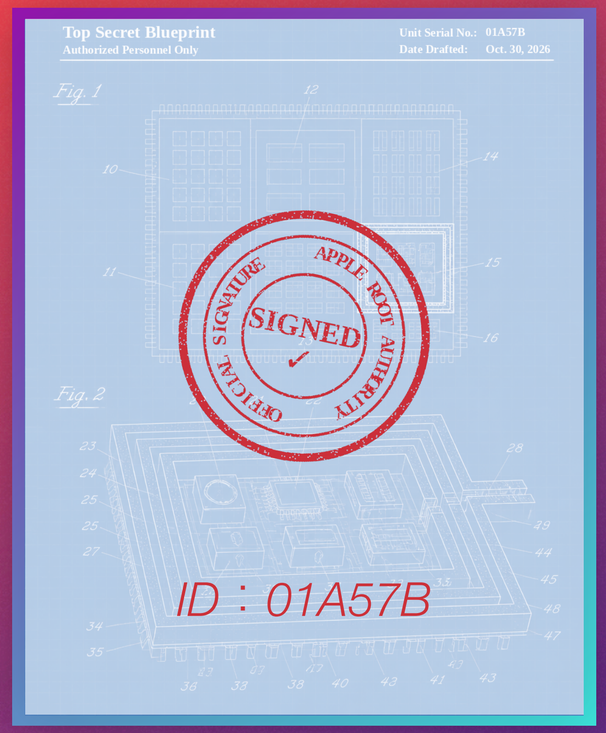


署名



Appleの偉い人

Apple が発行する Attestation 証明書
（X.509 形式の証明書チェーン）



署名



Apple Enterprise Attestation CA

私も 01A57Bです！



私は 01A57Bです！



私は 01A57Bです！



Appleの正式な証明書



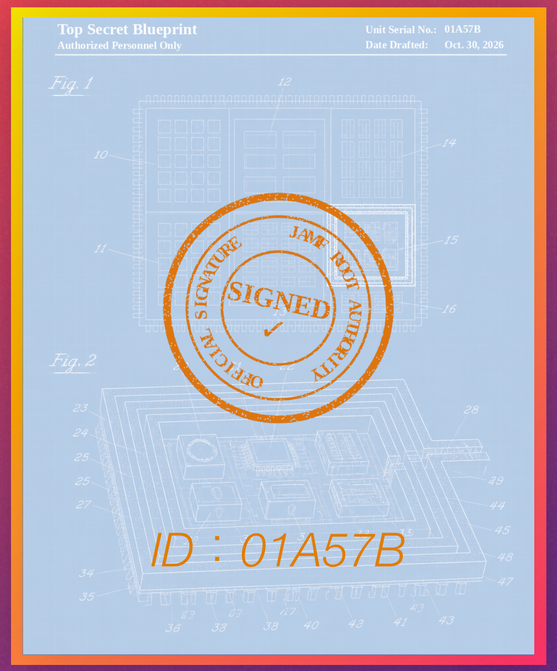
Managed Device Attestation（MDA）

Appleの正式な証明書



例えるなら「パスポート」

自社が発行する証明書



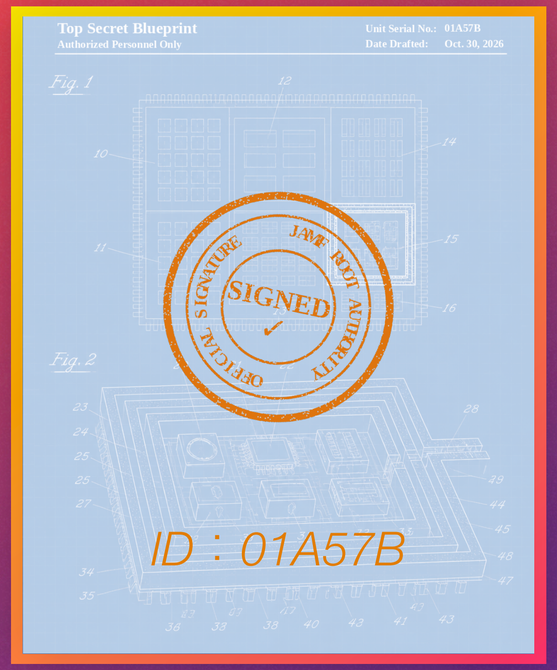
例えるなら「社員証」

Appleの正式な証明書



例えるなら「パスポート」

自社が発行する証明書



Appleの正式な証明書



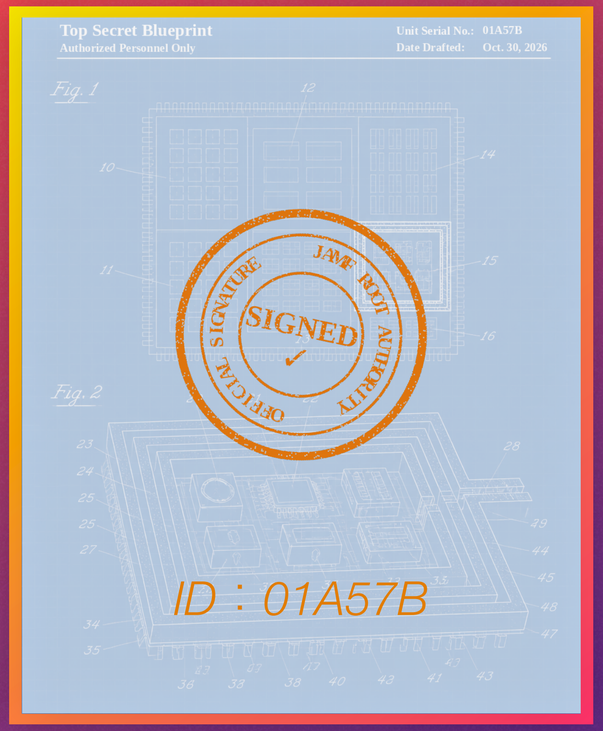
ACME Device Attestation

Appleが発行した証明書

Appleのサイン



社員証

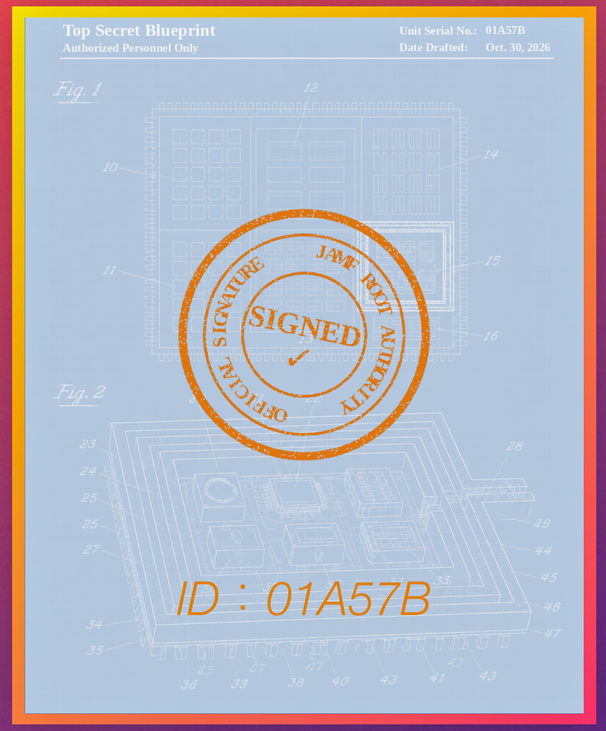

Top Secret Blueprint
Authorized Personnel Only
Unit Serial No.: 01A57B
Date Drafted: Oct. 30, 2026
Fig. 1
Fig. 2
SIGNED
OFFICIAL SIGNATURE
JAMF ROOT AUTHORITY
ID：01A57B

発行

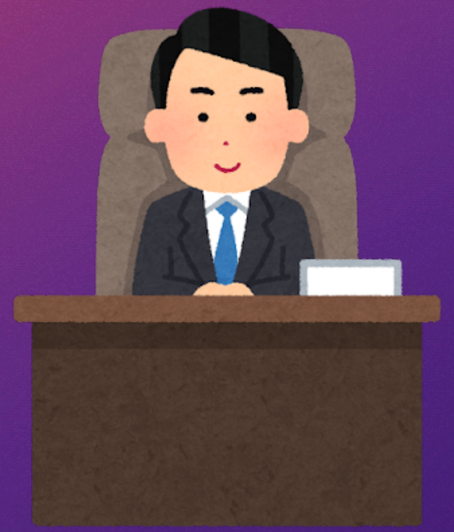


○○社の偉い人

Jamf が発行するクライアント証明書



発行

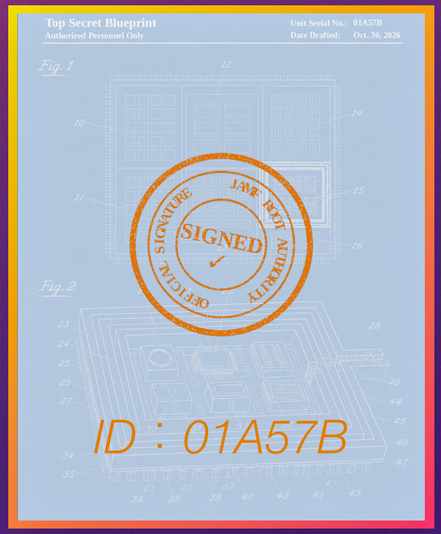


Jamf ACME サーバー



Mac / iPhone / iPad

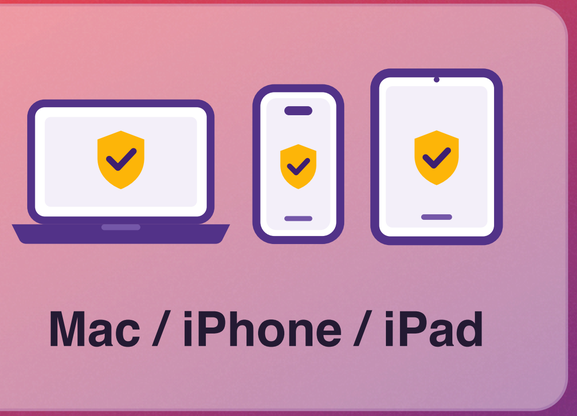
クライアント証明書



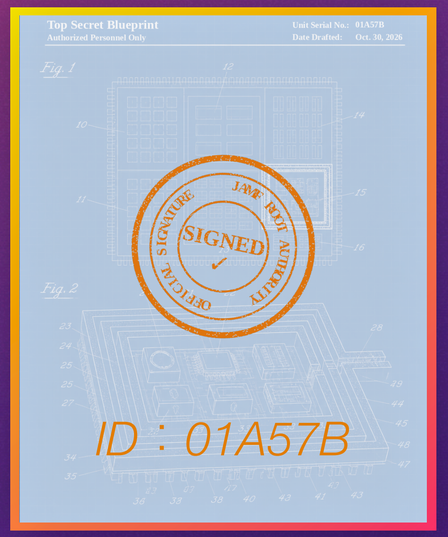
JAMF NATION LIVE

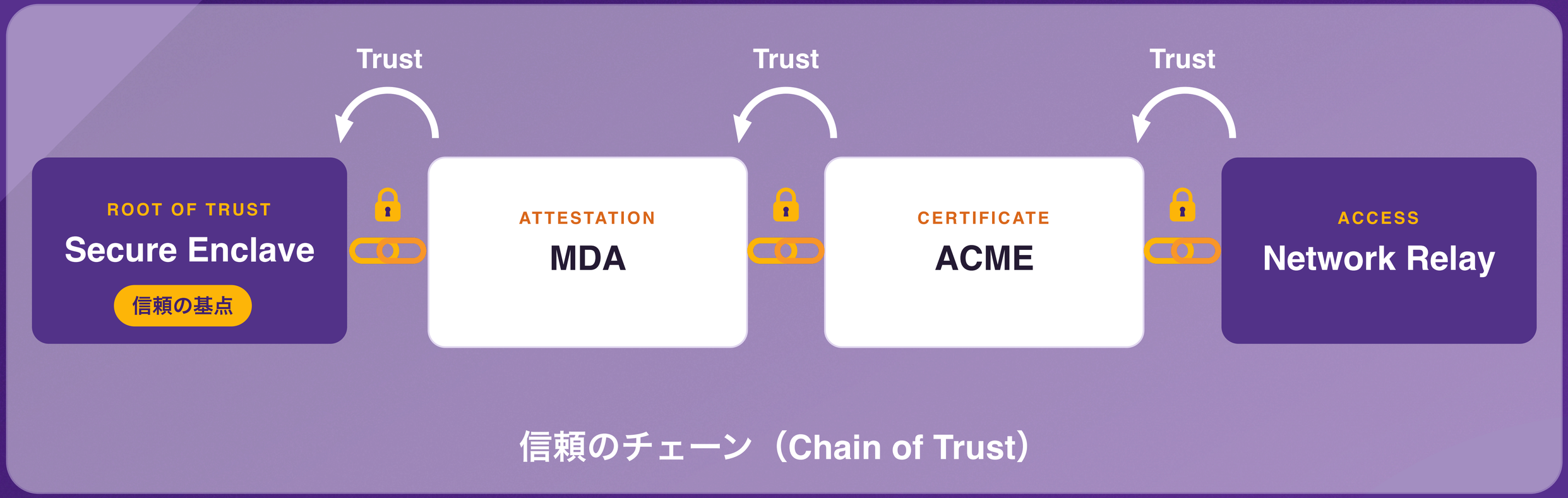
クライアント証明書

Jamf Pro から
自動配布

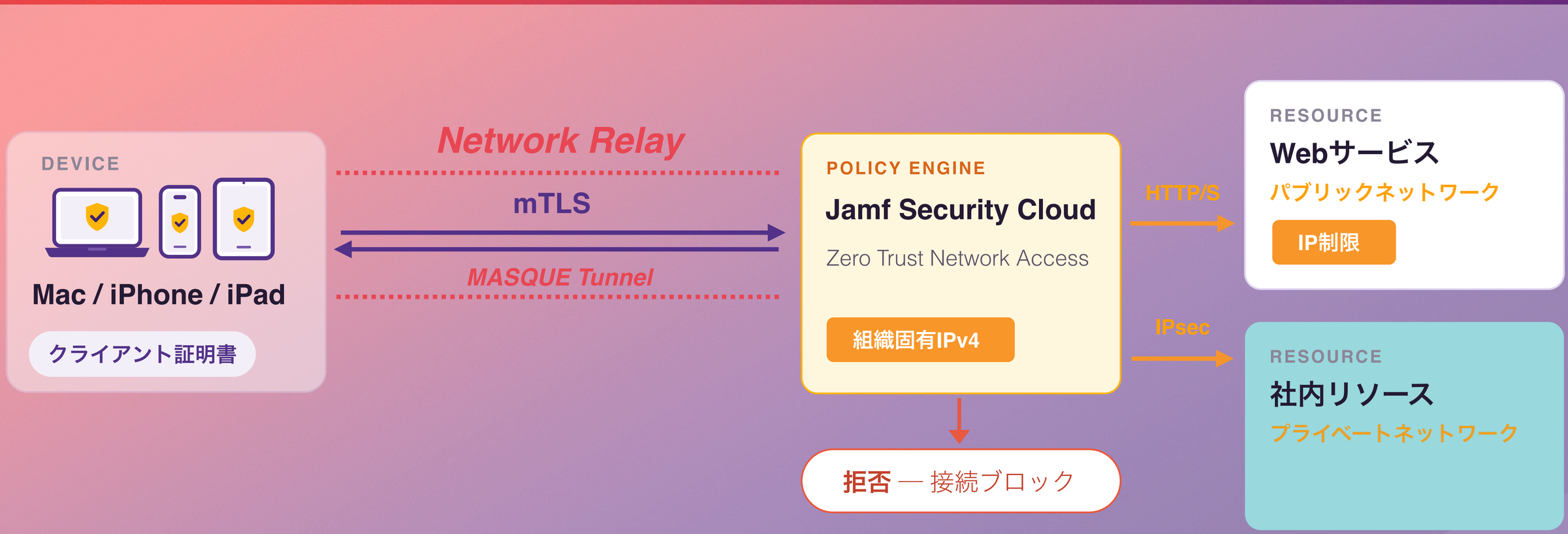


Mac / iPhone / iPad





信頼のチェーン（Chain of Trust）



Jamf Security Cloud への実装

DEVICE



Mac / iPhone / iPad

クライアント証明書

ゼロタッチ

Network Relay

mTLS

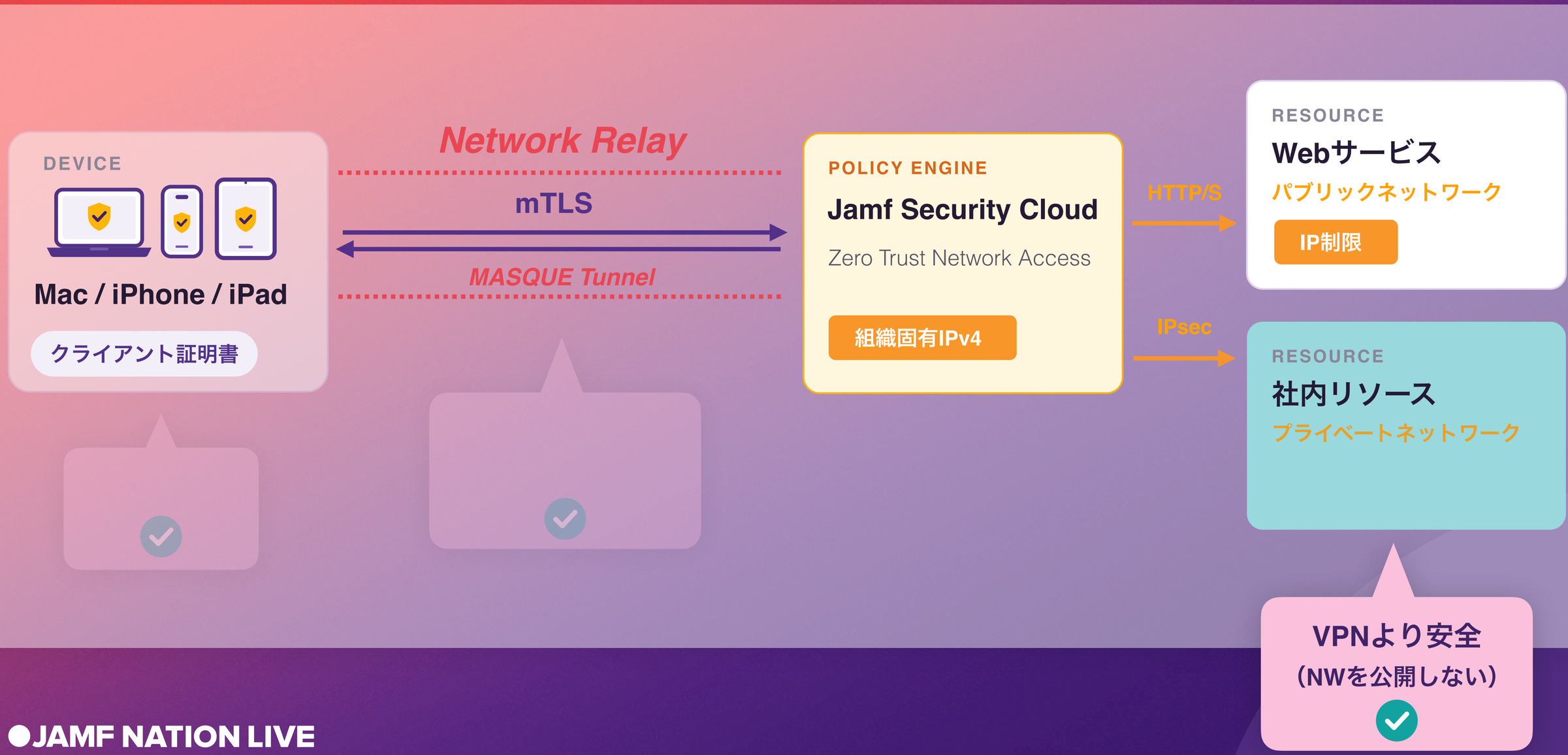
MASQUE Tunnel

OSネイティブ動作
（ブラウザ・アプリ）

POLICY ENGINE

Jamf Security Cloud

Zero Trust Network Access


DEVICE
Mac / iPhone / iPad
クライアント証明書
Network Relay
mTLS
MASQUE Tunnel
POLICY ENGINE
Jamf Security Cloud
Zero Trust Network Access
組織固有IPv4
HTTP/S
IPsec
RESOURCE
Webサービス
パブリックネットワーク
IP制限
RESOURCE
社内リソース
プライベートネットワーク
VPNより安全
（NWを公開しない）

Network Relay の設定・活用例

GETTING STARTED

Network Relay を始めるには

	01 Jamf Pro	02 Jamf Security Cloud	03 Network Relay
Jamf Pro をお使いの方	✓ 導入済み	導入が必要	有効化が必要
Jamf for Mac もしくは **Jamf for Mobile** もお使いの方	✓ 導入済み	✓ 導入済み	有効化が必要

Security Cloud

読み取り専用

レポート

アクセス

アプリケーション

ユーザアクティビティ

イベントログ

インターネット

使用量

サイトと App

ブロック

カテゴリ

ローミング

テザリング

上限

セキュリティ

脅威ビュー

デバイスビュー

脆弱性管理

App インサイト

MI:RIAM 解析

リクエスト数

アクセス

148K

合計

24,982

過去24時間

14,323

拒否されました

直近 7 日間 アプリケーション >

ユーザ接続済み

アクセス

23

合計

28

先月

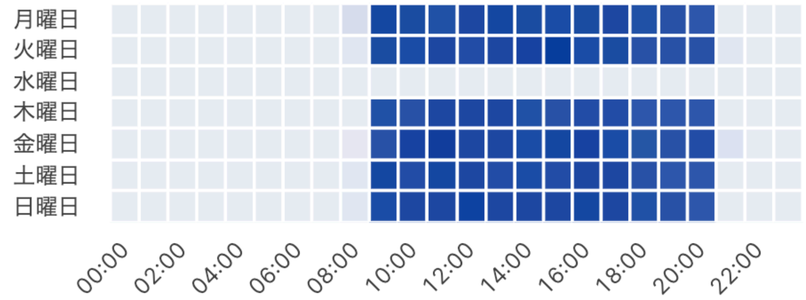
22

過去24時間

直近 7 日間 ユーザアクティビティ >

毎日の使用量

アクセス



直近 7 日間

アプリケーション >

セキュリティ評価

セキュリティ

23%

デバイスビュー >

デバイスリスク

セキュリティ

70

高リスクデバイス

24 保護されています

12 低

0 中

デバイスビュー >

平均 CVSS スコア

セキュリティ



脆弱性管理 >

脆弱なデバイス

セキュリティ



脆弱性管理 >

上位サイトと App のトランザクション

データ

グローバルデータ使用量

データ

ローミングが利用されている上位5ヵ国

データ



レポート

アクセス
アプリケーション
ユーザアクティビティ
イベントログ

インターネット
使用量
サイトと App
ブロック
カテゴリ
ローミング
テザリング
上限

セキュリティ
脅威ビュー
デバイスビュー
脆弱性管理
App インサイト
MI:RIAM 解析

App の内訳

アプリケーション	タイプ	カテゴリ	許可されました	拒否されました	接続共有
Workday	SaaS	テクノロジー	0	16,342	9.00%
Trello	Enterprise	生産性	17,127	0	9.00%
Snowflake	SaaS	テクノロジー	14,668	0	8.00%
Slack	SaaS	未分類	16,674	0	9.00%
Okta	SaaS	テクノロジー	16,432	0	9.00%
Monday.com	Enterprise	生産性	443	0	0%
Microsoft Teams	SaaS	テクノロジー	16,610	0	9.00%
Microsoft Authentication	SaaS	生産性	16,062	0	9.00%
Microsoft 365	SaaS	生産性	40,486	0	23.0%
IP Location Tool	Enterprise	テクノロジー	620	0	0%
Google Cloud	Enterprise	テクノロジー	0	50	0%
GitHub	SaaS	テクノロジー	111	202	0%
Atlassian Cloud	SaaS	生産性	16,660	0	9.00%

DEPLOYMENT

Network Relay ── 配布手順

1 Jamf Security Cloud

設定ファイル作成

ZTNAのアクティベーション
プロファイルを作成

2 Jamf Pro

配布

対象の端末にスコープ

- ACME証明書
- Network Relay

3 Device

自動アクティベーション

端末が証明書を自動取得、
即座にNetwork Relay が有効化

INTEGRATION

Jamf Pro と Jamf Security Cloud

Jamf Security Cloud

役割

- 設定ファイルの作成
- アクセスポリシーの設定

作成したプロファイル→



←端末情報・グループ情報

Jamf Pro

役割

- 構成プロファイルの配布

プライベート

jamf.com

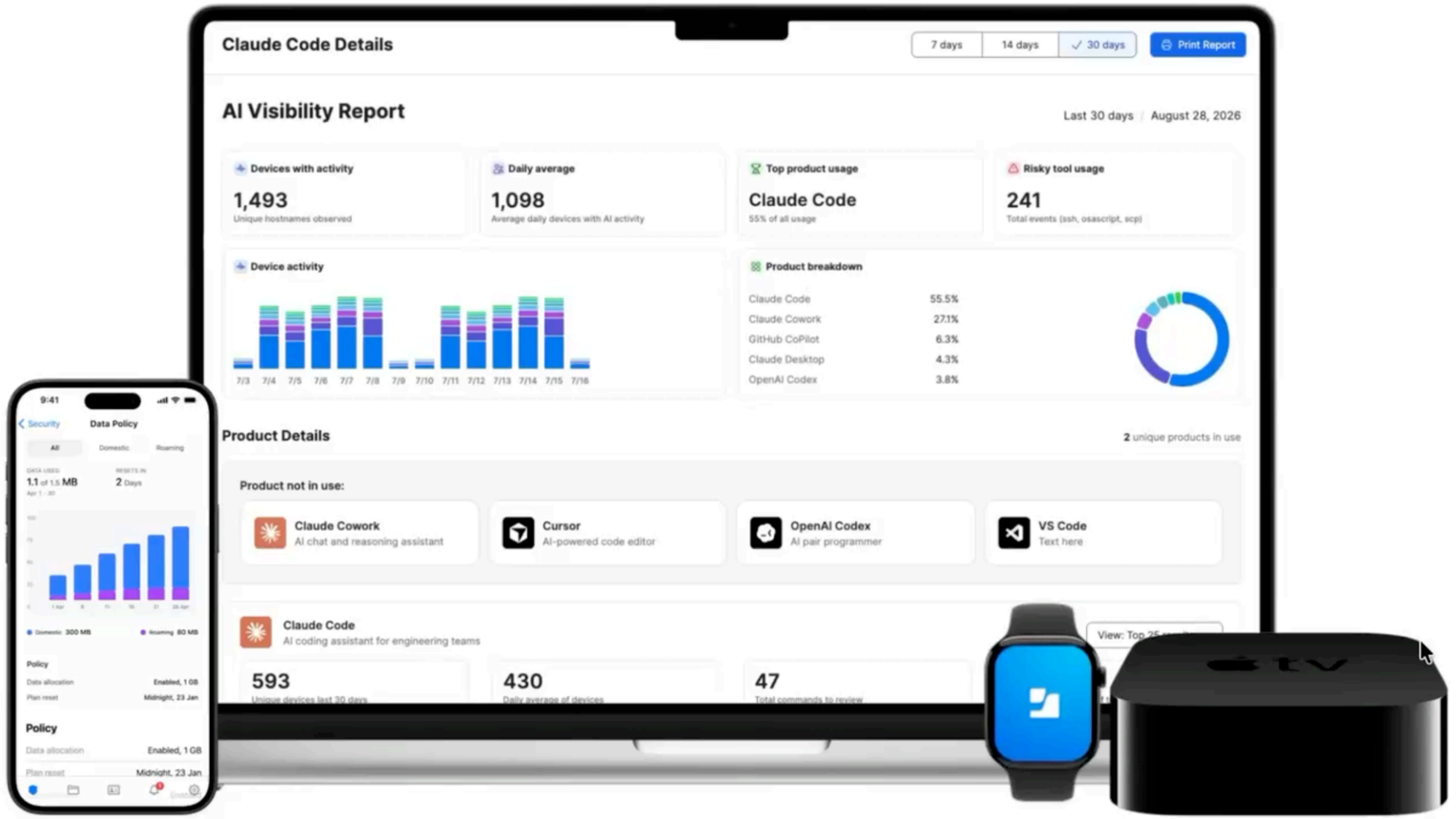
1

ログイン 日本語

jamf

Jamfが選ばれる理由 製品 価格 リソース パートナー

無料トライアル 連絡先



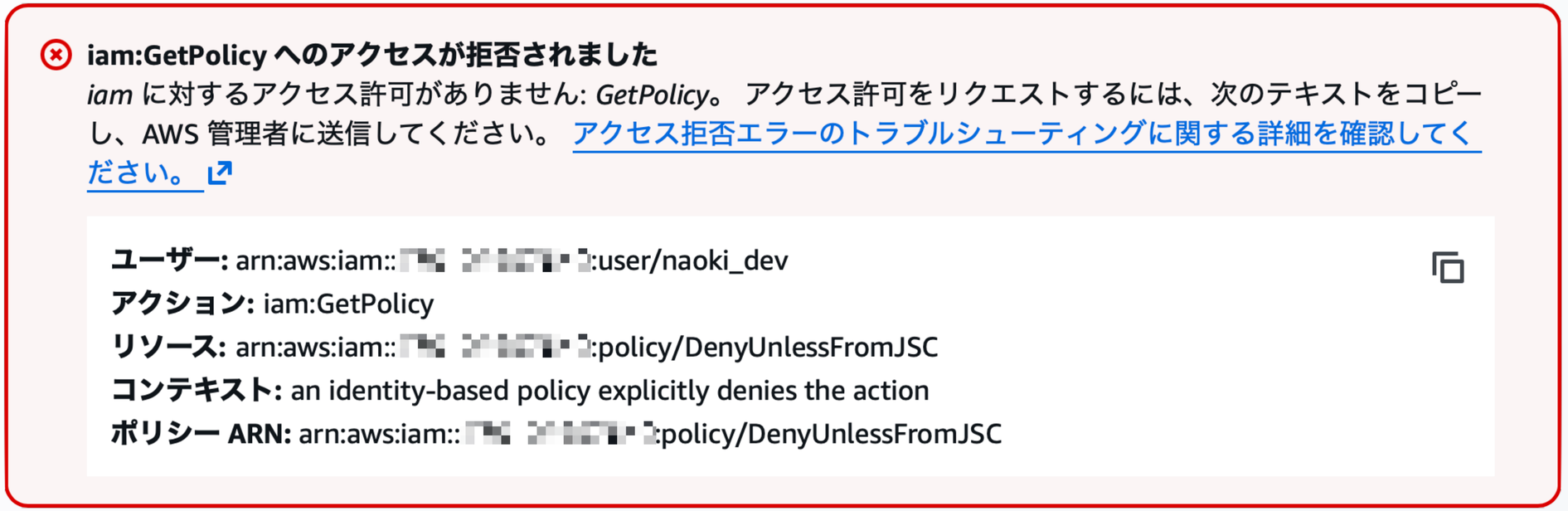
NETWORK RELAY × AWS MANAGEMENT CONSOLE

例：AWS へのアクセス制御





IAM（IAM Identity Center）のIP アドレス制限ポリシー



AWSサービスへのアクセス拒否（例：IAM）

NETWORK RELAY × AWS MANAGEMENT CONSOLE

例：AWS へのアクセス制御



既存のVPN・SASEと共存可能

Network Relay

“ Appleデバイス の「強力なデバイス認証」に基づき
特定の通信を「安全に中継」するAppleの技術 ”