SafeNet Trusted Access
～統合認証・アクセス管理ソリューション～

製品紹介

Canon
キヤノンマーケティングジャパン株式会社

クラウドサービス利用に アクセス管理を

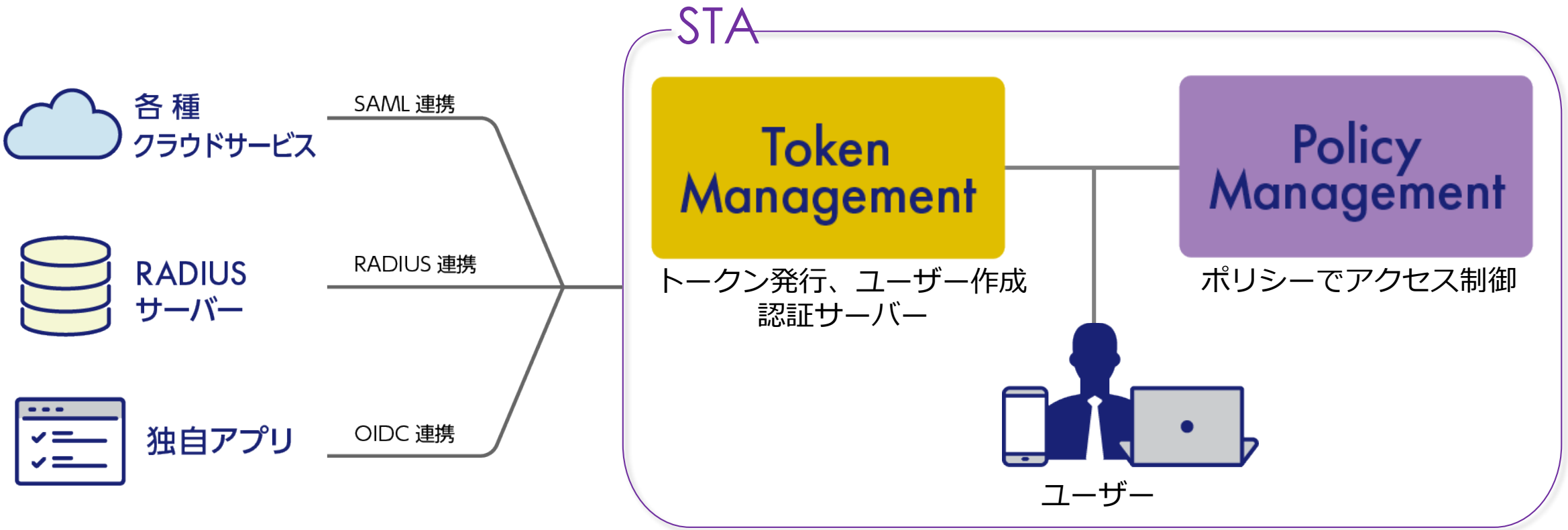
企業における**認証・アクセス管理の重要性**は、近年益々増えてきています。
働き方改革や、クラウドシフトの流れから、Office 365などのクラウドサービスの利用が当たり前となり、
それに伴って社外での利用も増えてきています。利用するクラウドサービスの増加、変化する従業員数など、
従来通りのID/Password管理だけでは、退職者等への対策が疎かになり、社内情報の漏洩リスクを軽減する事は難しくなってきています。弊社は、社内のアクセス管理だけでなく、社外からのアクセスにも対応し、利用しているクラウドサービスのID/パスワード一元管理、SSO対応が可能な**「SafeNet Trusted Access」**をご提供しています。

ThalesGroup 企業紹介

タレスグループはフランスに本社を置く、大手電機企業であり、航空宇宙分野、防衛分野、交通システム分野、セキュリティ分野での情報システムと各種サービスを提供している企業です。

STA製品構成

「SafeNet Trusted Access」は、認証システム機能であるトークンマネジメント、
ポリシーを用いて各種クラウドサービス向けのアクセス制御を加えた、統合認証・アクセス管理ソリューションです。



製品の仕様一覧

「SafeNet Trusted Access」はクラウドサービスへのアクセス制御機能(Policy Management)と、
トークンを管理する機能(Token Management)の二つが存在し、これらを総称してSTAと呼んでいます。
それぞれの機能には以下の役割が存在します。

Token Management

ユーザー作成・管理	● ユーザー登録 ● AD 連携機能
トークン発行	● 豊富な HW・ソフトウェアトークン ● トークン割り当て ● トークン利用方法
認証サーバ	● RADIUS 連携

Policy Management

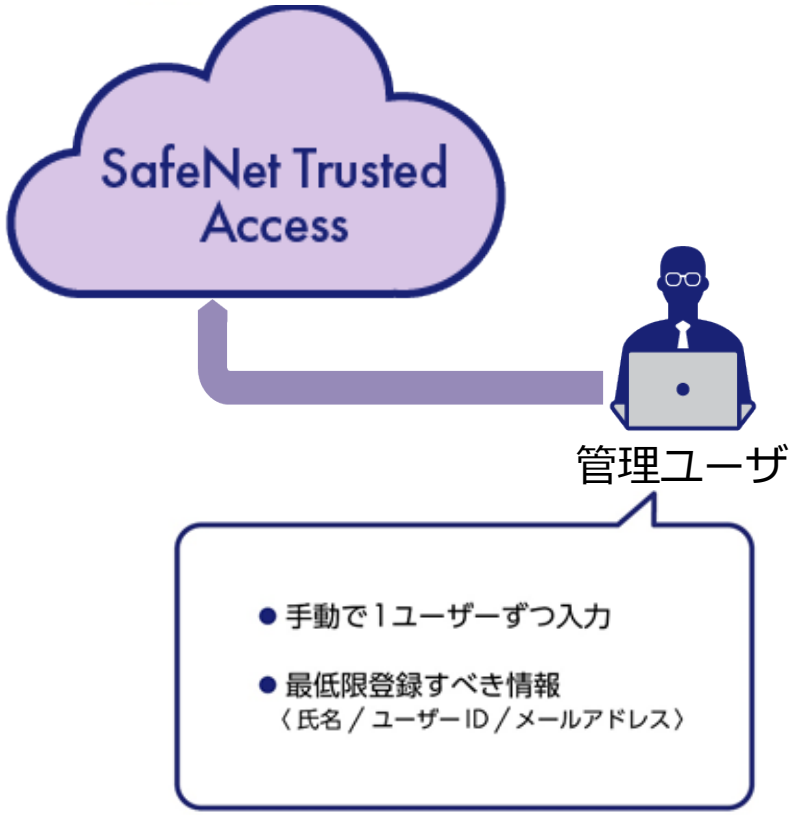
アプリ連携	● クラウドサービスのアクセス制御 ● 外部クラウドサービス連携方法 ● 対応クラウドサービス一覧
SSO	● ユーザーポータル ● SSO 機能
アクセス制御	● シナリオ機能 ● グローバルポリシー ● 通常ポリシー

ユーザー登録

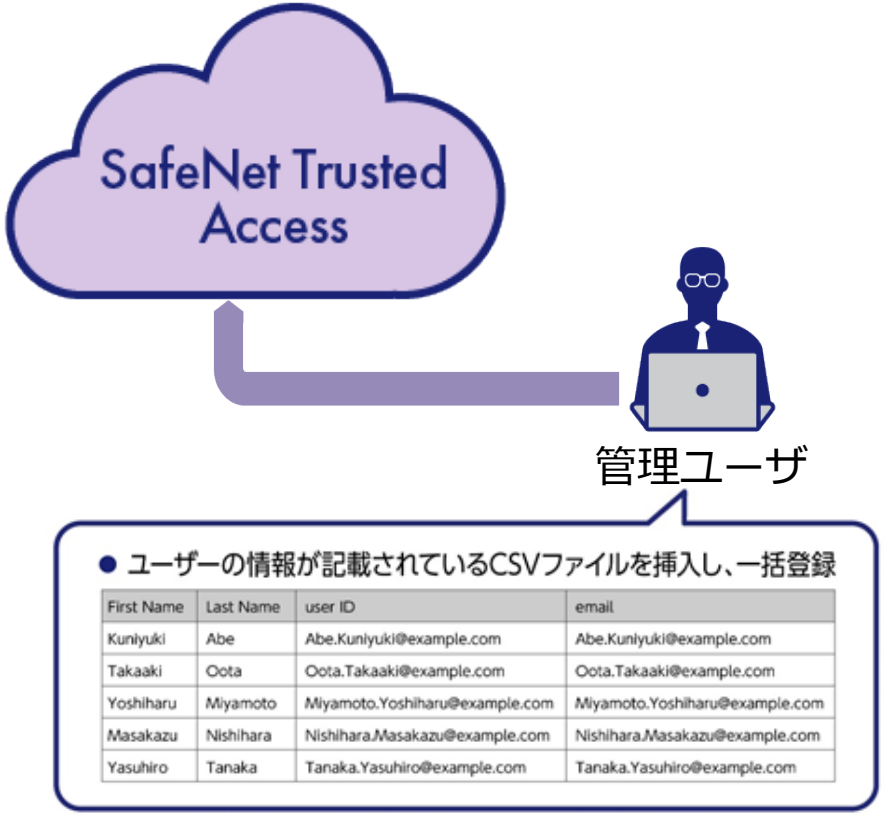
STAにアクセスを一元管理させる為、 ユーザー情報を登録する必要があります。
STAへユーザー登録をする方法は、手動登録、CSV登録、AD連携の三つが存在し、それぞれ登録方法が異なります。

Token Management

1. 手動登録



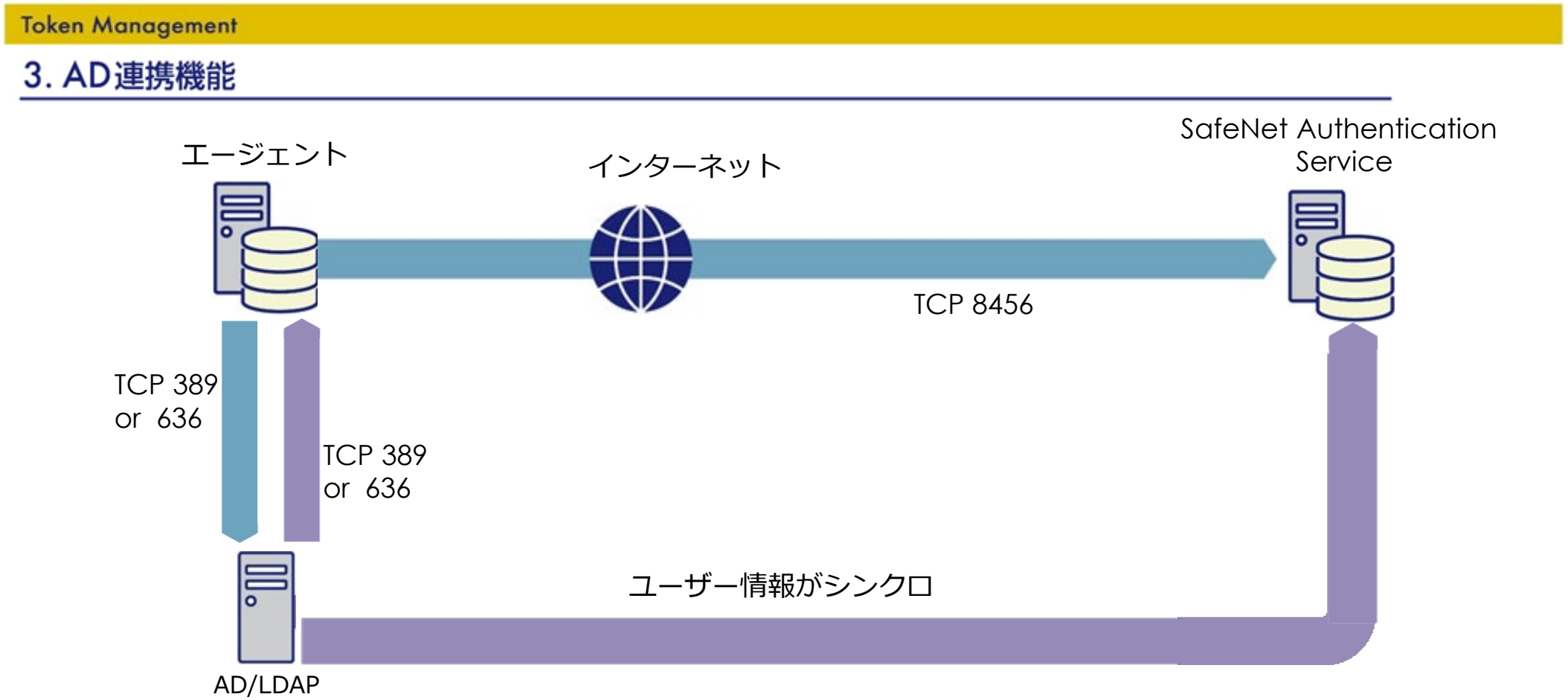
2. CSV登録



First Name	Last Name	user ID	email
Kuniyuki	Abe	Abe.Kuniyuki@example.com	Abe.Kuniyuki@example.com
Takaaki	Oota	Oota.Takaaki@example.com	Oota.Takaaki@example.com
Yoshiharu	Miyamoto	Miyamoto.Yoshiharu@example.com	Miyamoto.Yoshiharu@example.com
Masakazu	Nishihara	Nishihara.Masakazu@example.com	Nishihara.Masakazu@example.com
Yasuhiro	Tanaka	Tanaka.Yasuhiro@example.com	Tanaka.Yasuhiro@example.com

AD連携機能

AD/LDAPでユーザを管理している場合は、STAとADを連携させ、AD上でユーザー変更があった場合STAへ反映させることが可能です。AD連携をさせる為には、ADと同じネットワーク内に連携用エージェントをインストールします。



豊富なHW・ソフトウェアトークン

STAは様々な認証方法を用意しています。iOSアプリ、SMSなどのソフトウェアトークン。
カード型などのデバイスを使用した、ハードウェアトークンなどが利用可能です。

Token Management

H/W トークン

OTP110

Display Card

- 30秒ごとに異なるパスワード生成
- ワンプッシュすれば、異なるパスワードを生成
- PC接続はしない為、ウイルス・マルウェア感染リスク無し
- カードタイプはデザインのカスタマイズも可能
- 50個などの小ロットにも対応
- OAuth準拠

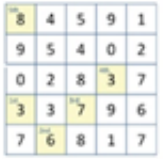
ソフトウェアトークン

MobilePASS+

スマホ、タブレット用アプリ
アプリ上で「承認」ボタンを押して認証完了

S/W トークン

スマホ、タブレット、PC用
SMS/Emailでワンタイムパスワードを発行、
ログイン画面に入力し、認証

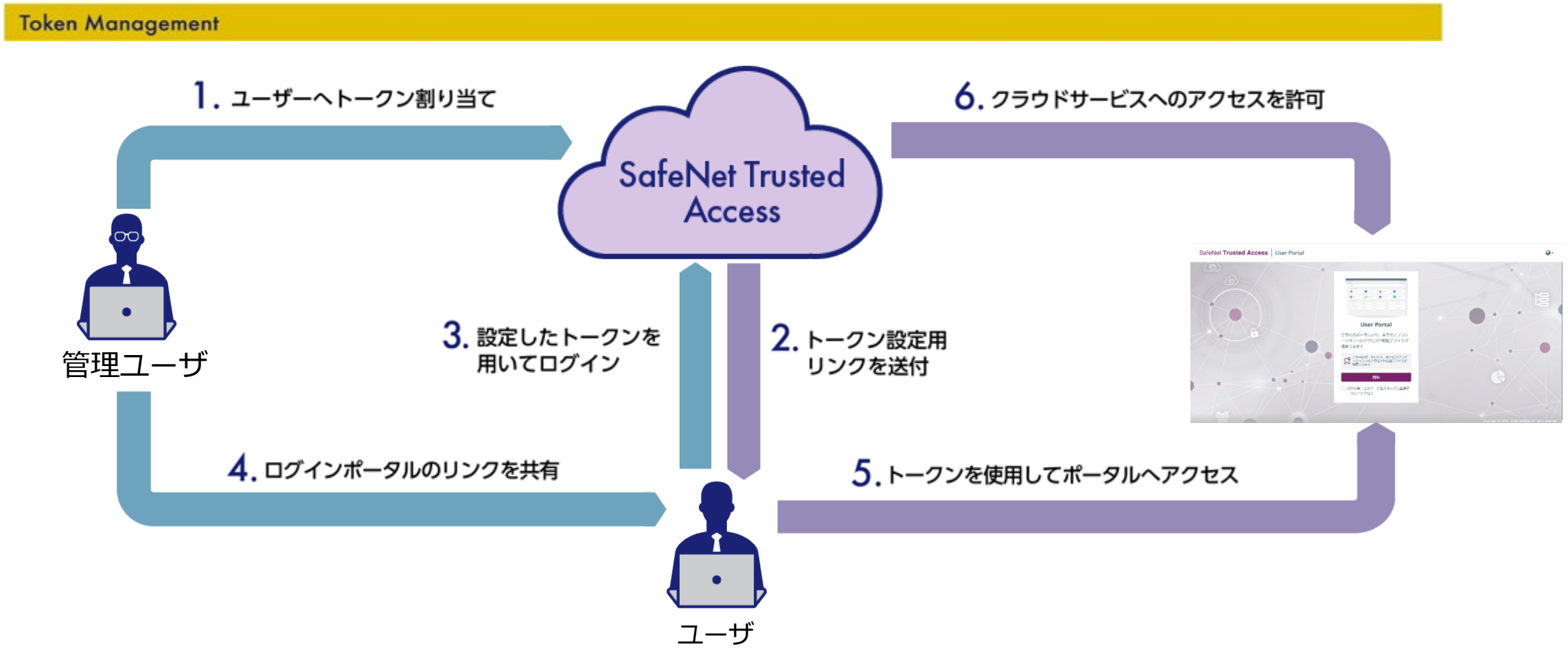


マトリックス認証

スマホ、タブレット、PC用
ブラウザ上で動作し、インストール不要
ユーザーは位置を覚えるだけ

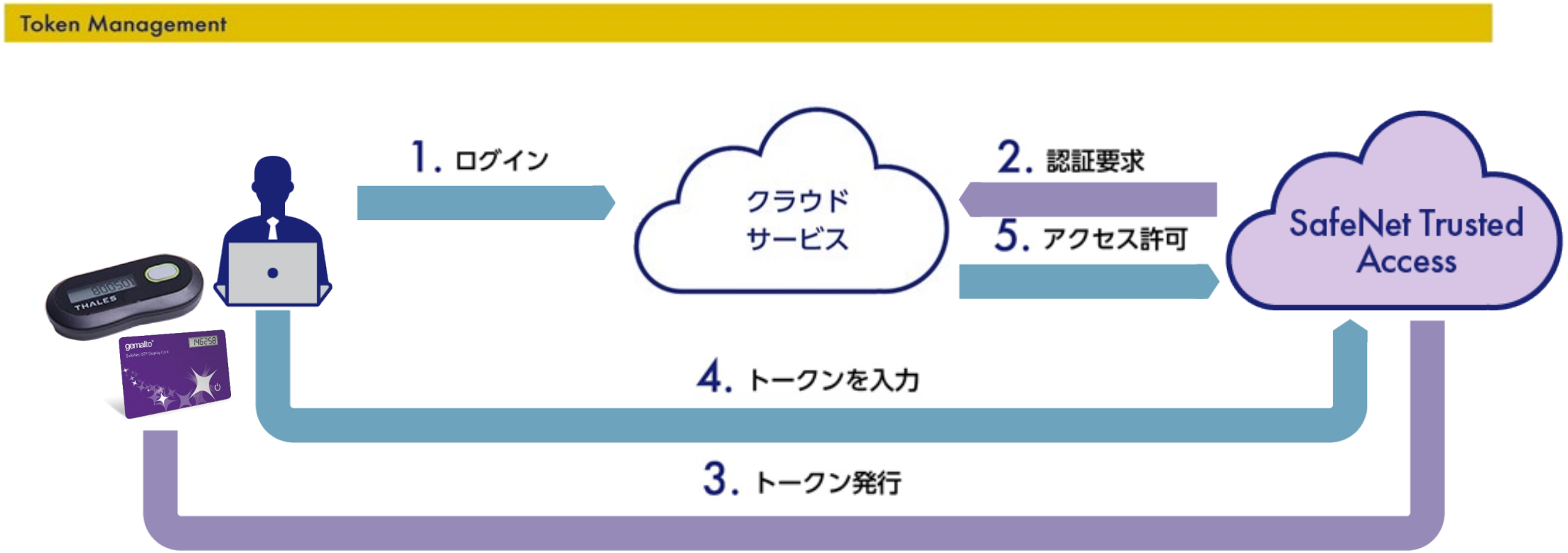
トークン割り当て

トークンの割り当てはSTA管理者が、ユーザーに対して割り当てます。割り当てられたユーザーには、トークンを有効化する手順が記載されたメールが2通が送られます。管理ユーザがトークン割り当て後、ユーザーへポータルサイトへのリンクを連携する事で、各種クラウドサービスへアクセス可能になります。



トークン利用方法

ハードウェア、ソフトウェアトークンを実際に使用し、クラウドサービスへログインする実際の流れは以下になります。
複数の認証方式が選択可能なので、パスワードを忘れた際などはトークンを使用するなどの対処が可能です。



RADIUS連携

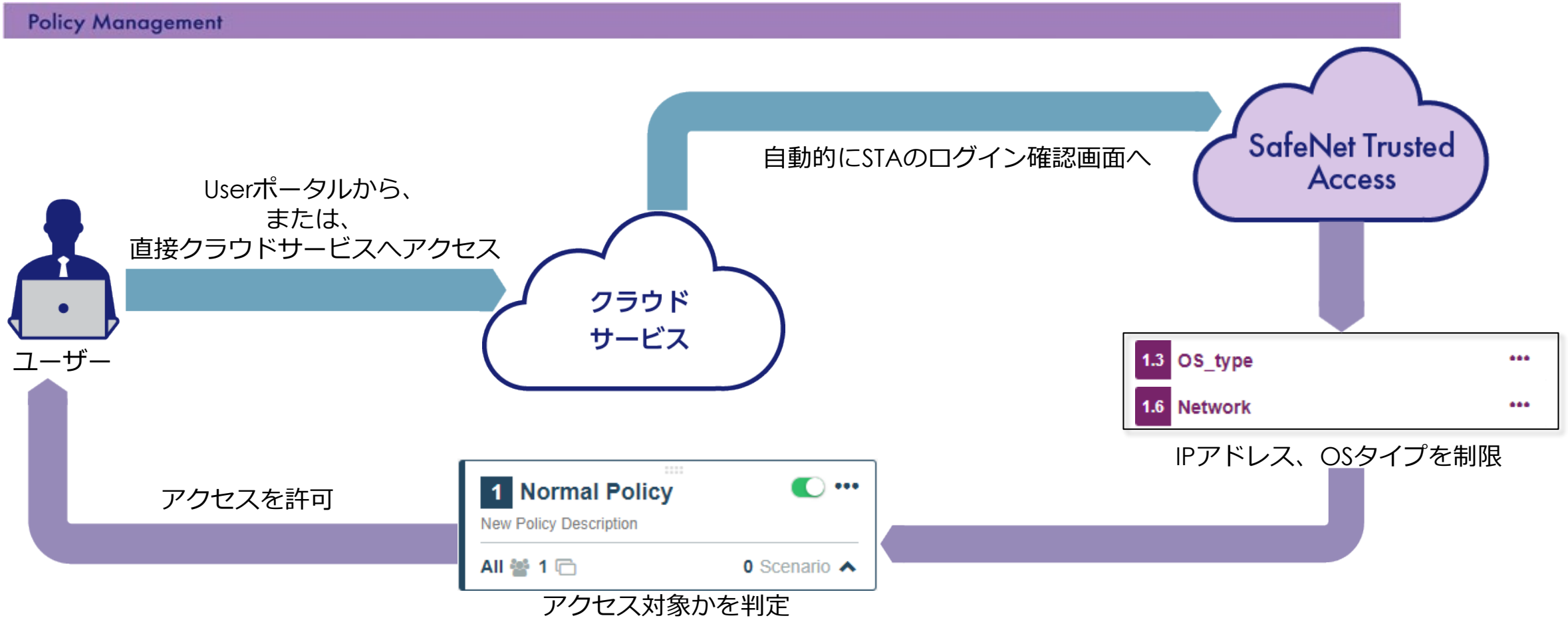
STA側でRADIUSサーバーを用意しているので、簡単にSTAでRADIUS認証が使用可能です。
また既存のRADIUS環境がある場合も、CSVまたは専用エージェントを用いて簡単に移行、連携が可能です。

Token Management

RADIUS ご利用イメージ

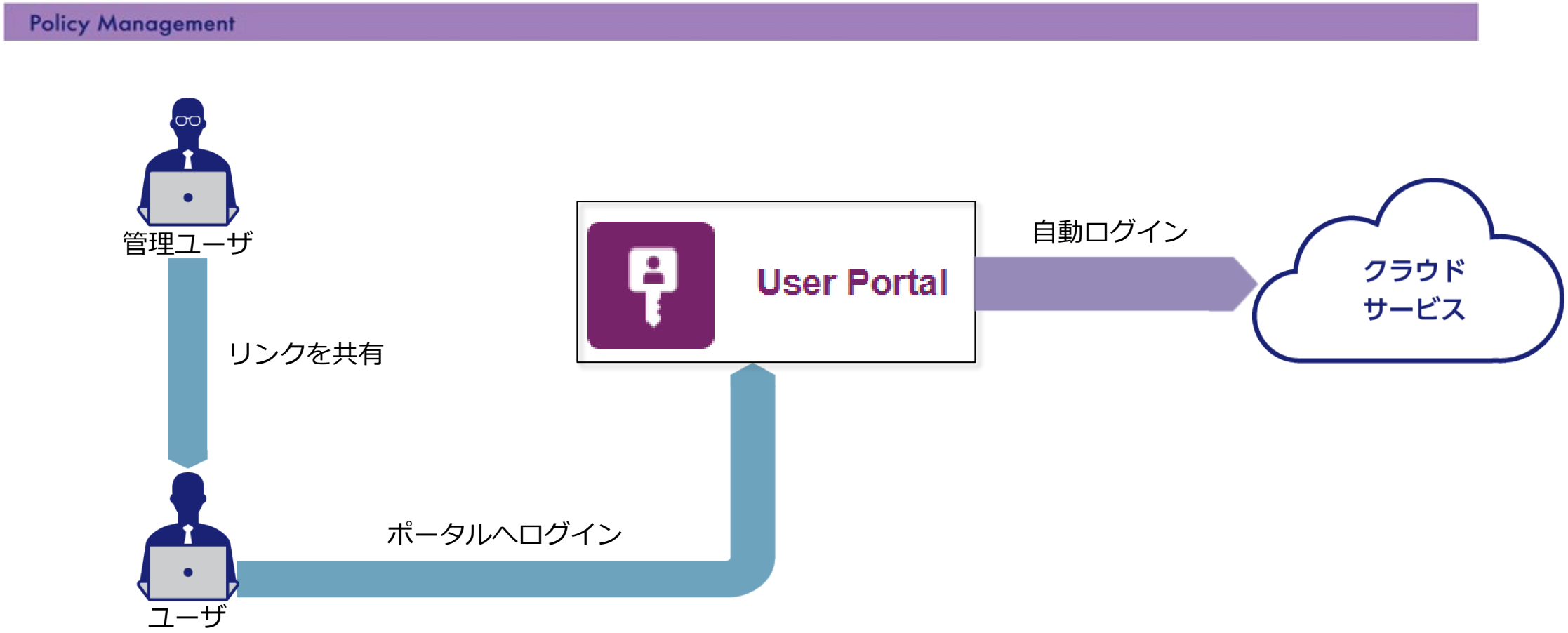
クラウドサービスへのアクセス制御

STAでは、クラウドサービスへアクセス制御を実施する為のポリシーを作成します。
ポリシーではアクセスしてくるIPアドレスや、OSタイプなどを制御するシナリオを作成し、
最終的にアクセス対象のユーザーグループかを判断します。



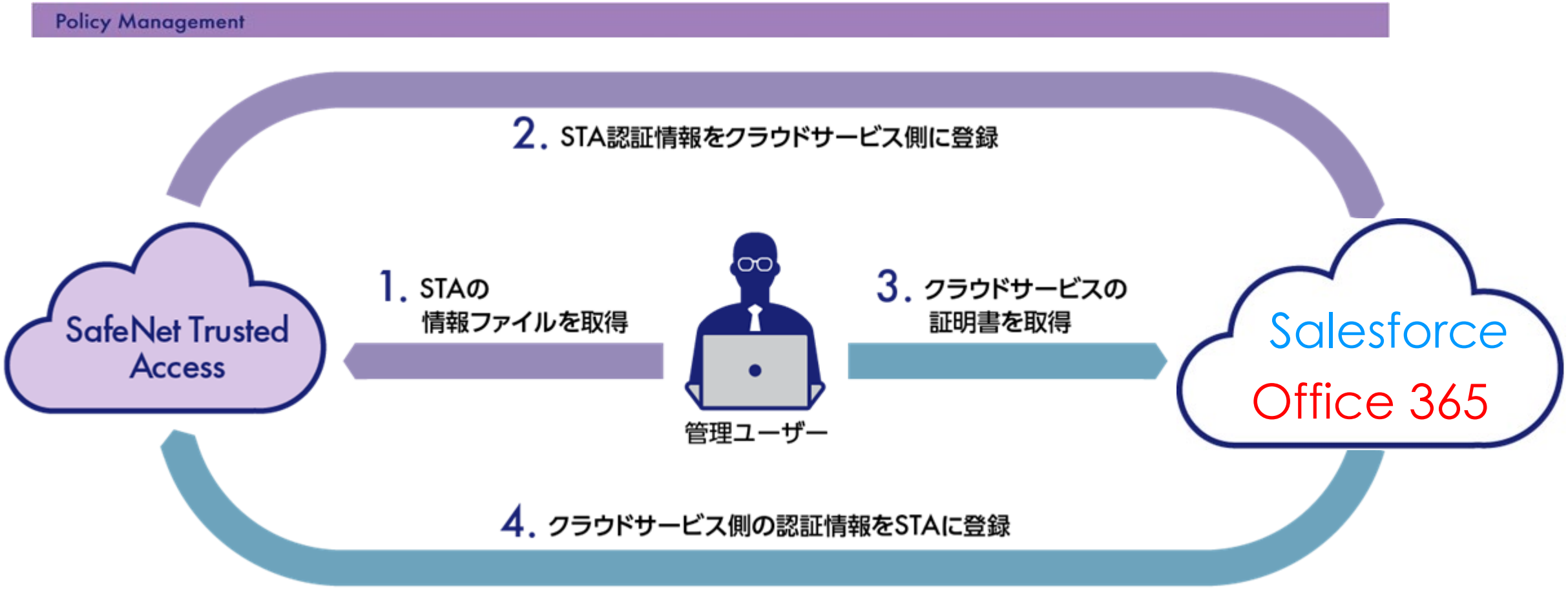
ユーザーポータル

STAには、ユーザーが簡単にクラウドサービスへアクセスする為のポータルが用意されています。
このポータルはクラウドサービスを一元管理し、アクセスする際にはパスワードを入力せずにログイン可能です。
また、ポータルでは個人のアクセス履歴を確認することも可能です。



外部クラウドサービス連携方法

STAはデフォルトで連携可能なクラウドサービスが多数用意されています。
連携させるクラウドサービスを管理者が選択し、STAに追加します。
その際、クラウドサービス側も含めた操作ドキュメントに従って、クラウドサービスを連携させることが可能です。



対応クラウドサービス一覧

STAではデフォルトで多数の連携可能なクラウドサービスが用意されており、OIDCが使用可能な場合は独自アプリケーションも連携可能です。STAで連携できる主なクラウドサービスは以下の通りです。

Policy Management

以下のメジャーなクラウドサービスに加えて、その他150以上の外部クラウドサービスと連携可能です

メジャーなクラウドサービス

Salesforce

Office 365

Amazon Web Service

その他150以上の外部クラウドサービス

Google Cloud Platform

Dropbox

Evernote

Asana

Apache HTTP Server

WordPress

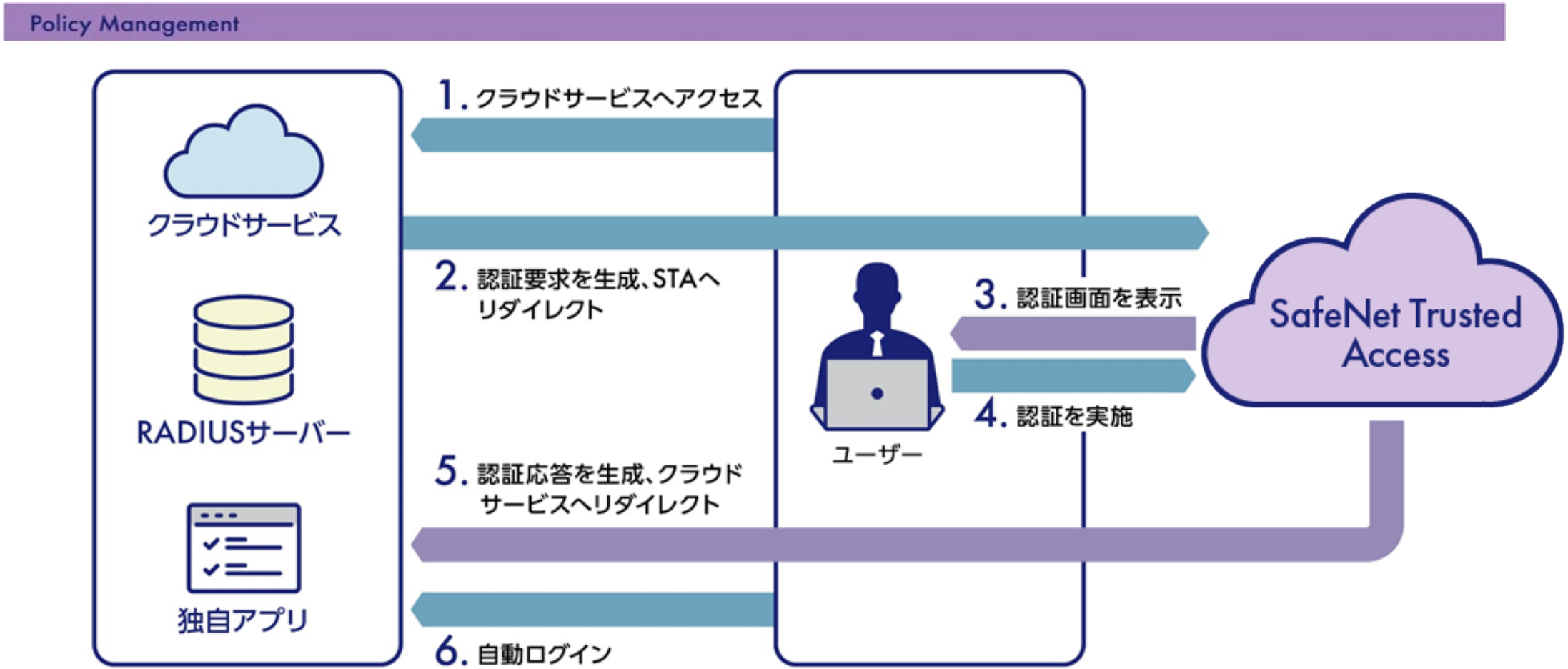
GitLab

Slack

Splunk Enterprise

SSO機能

STAと対象のクラウドサービス連携させると下記の様なSSOの仕組みがご利用頂けます。
ユーザーが従来の煩雑なパスワード管理をする必要はもうありません。



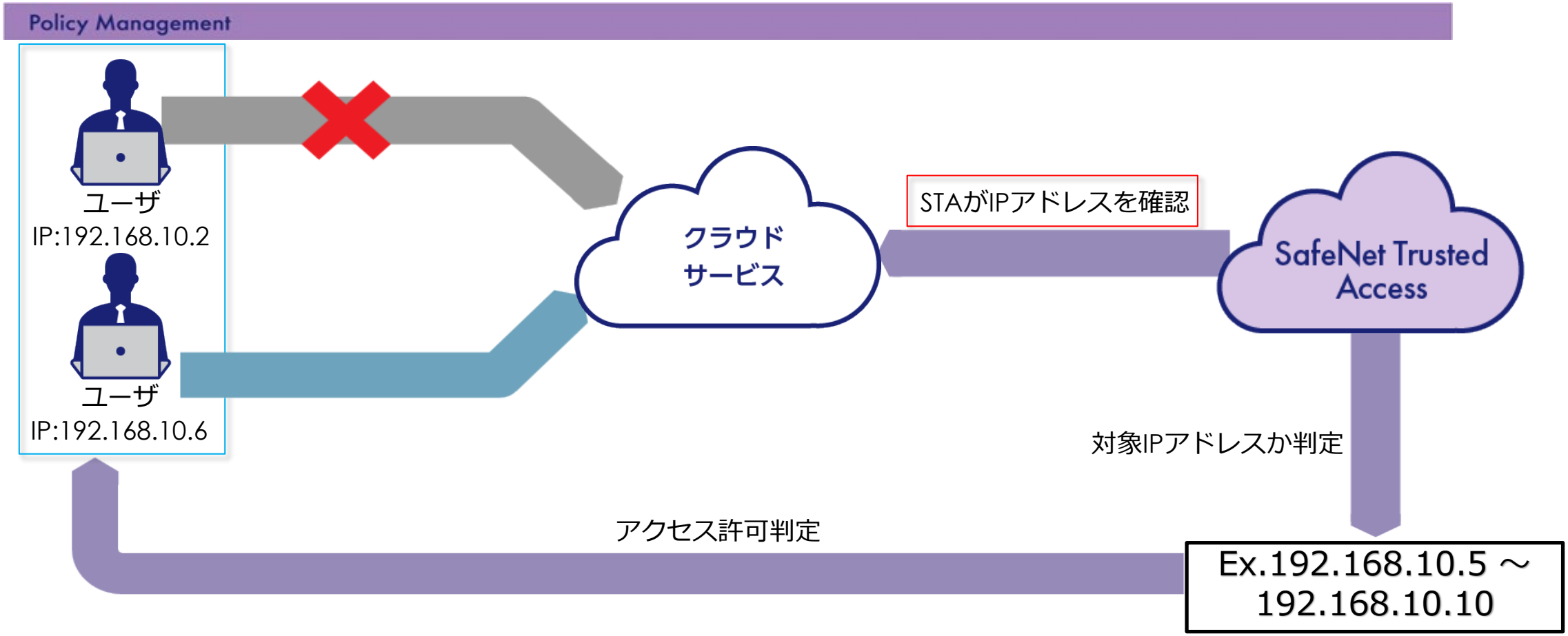
シナリオ機能

STAには、利用用途に応じた細かいアクセスを制御を実施する為の機能である、シナリオ機能が存在します。

このシナリオ機能は、ポリシーに付与する形で設定します。シナリオ機能は、全6つ用意されており、特定のシナリオ機能に該当する場合にアクセスを「許可する」「許可しない」といった使い方が可能です。

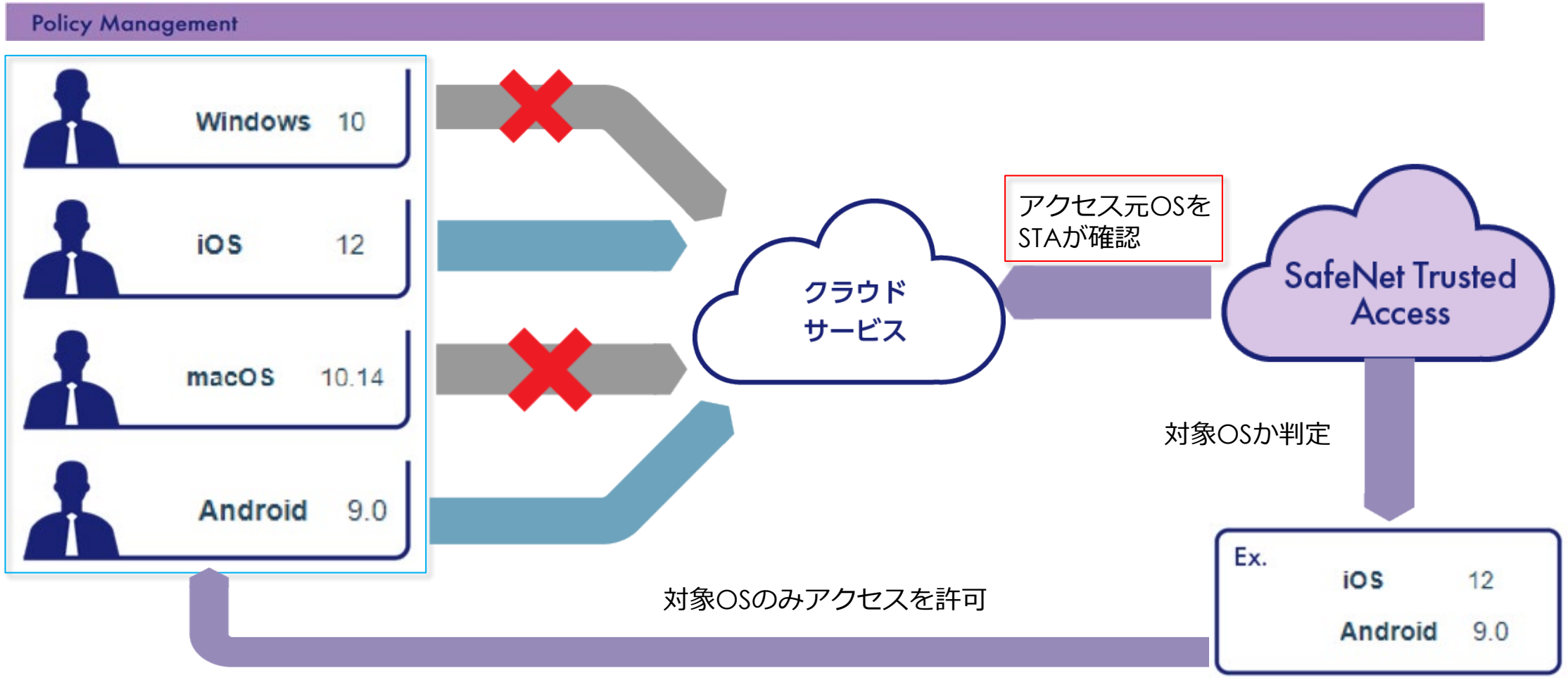
シナリオ機能「Network」

ここではシナリオ機能の具体的な機能1つ「Network」を紹介します。
「Network」は、指定したIPレンジ内外からのアクセスを制御する機能です。



シナリオ機能「Operating System」

シナリオ機能にはOS別にアクセスを制御する機能の1つ「Operating System」があります。
Windows, macOS, iOS, Androidからのアクセスを制御できます。
STAでサポートされている範囲内であれば、OSのバージョンも指定可能です。



グローバルポリシー

クラウドサービスをアクセス制御するポリシーは「グローバルポリシー」「通常ポリシー」 の2種類が存在し、
この二つの組み合わせでクラウドサービスへのアクセスを制御します。
グローバルポリシーは、デフォルトかつ、全てのユーザーグループ、クラウドサービスに対してルールを設定します。

通常ポリシー

「グローバルポリシー」で全社向けにポリシーを作成したのち、ある特定のユーザーグループ、またはクラウドサービスに対してのポリシーが「通常ポリシー」です。「通常ポリシー」は「グローバルポリシー」と異なり、削除が可能です。
部署や事業所別にアクセス管理をしたい場合は、「通常ポリシー」を使用します。

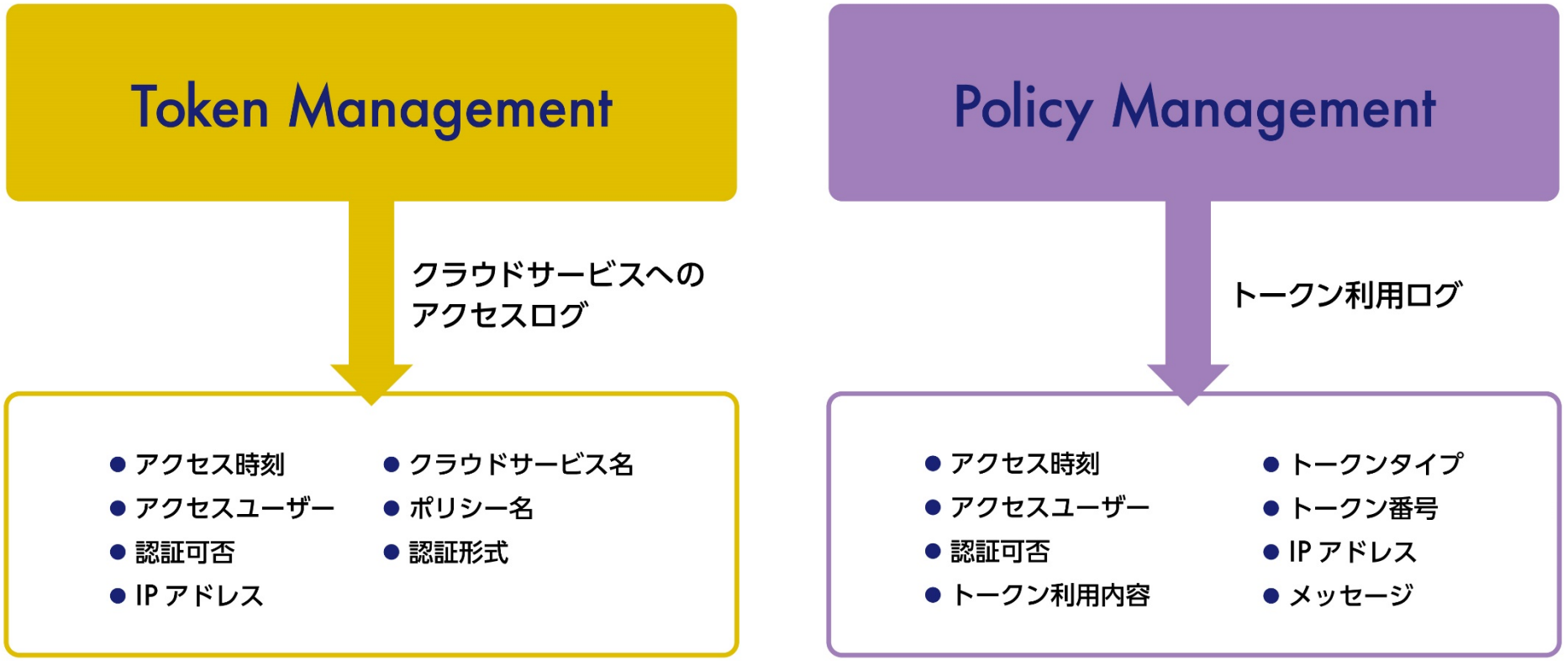
ライセンス、機能

STAのライセンスには「STA」「STAプレミアム」の2種類が存在し、扱える機能に差異は「STAプレミアム」がPKI証明書を用いた認証の1つのみで、それ以外は同等です。

STA	STA プレミアム
● パスワード認証 ● プッシュ OTP ● MobilePASS+ SW ● SMS/ メール認証 ● グリッド認証 ● ケルベロス認証 ● グループ / クラウドサービスへの ポリシー適用 ● IP アドレス制御 ● ユーザーデバイス制御 ● OS 制御 ● セッションタイムアウト ● 認証要求頻度 …etc	STA の機能に加え、 トークンやスマートカードを活用した PKI 証明書による認証 STA 機能 ＋ 

アクセスログ、Auditログ

STAではクラウドサービスへアクセスした際のログと、トークンを利用した際のログ二種類を取得可能です。
また、CSV形式でダウンロードも可能なので、データ収集、ログ管理ツール等に活用頂けます。

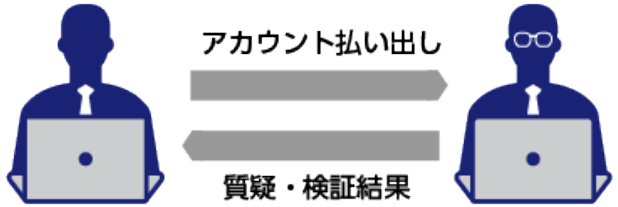


導入イメージ

「SafeNet Trusted Access」を導入頂く際には、お客様用のデモアカウントを作成し、事前に検証・質疑を実施します。
その後ご注文頂き、本番アカウント開設作業を行います。

1. 製品のご紹介

2. デモアカウントで検証・質疑



3. ご注文

STA
OR
STA プレミアム

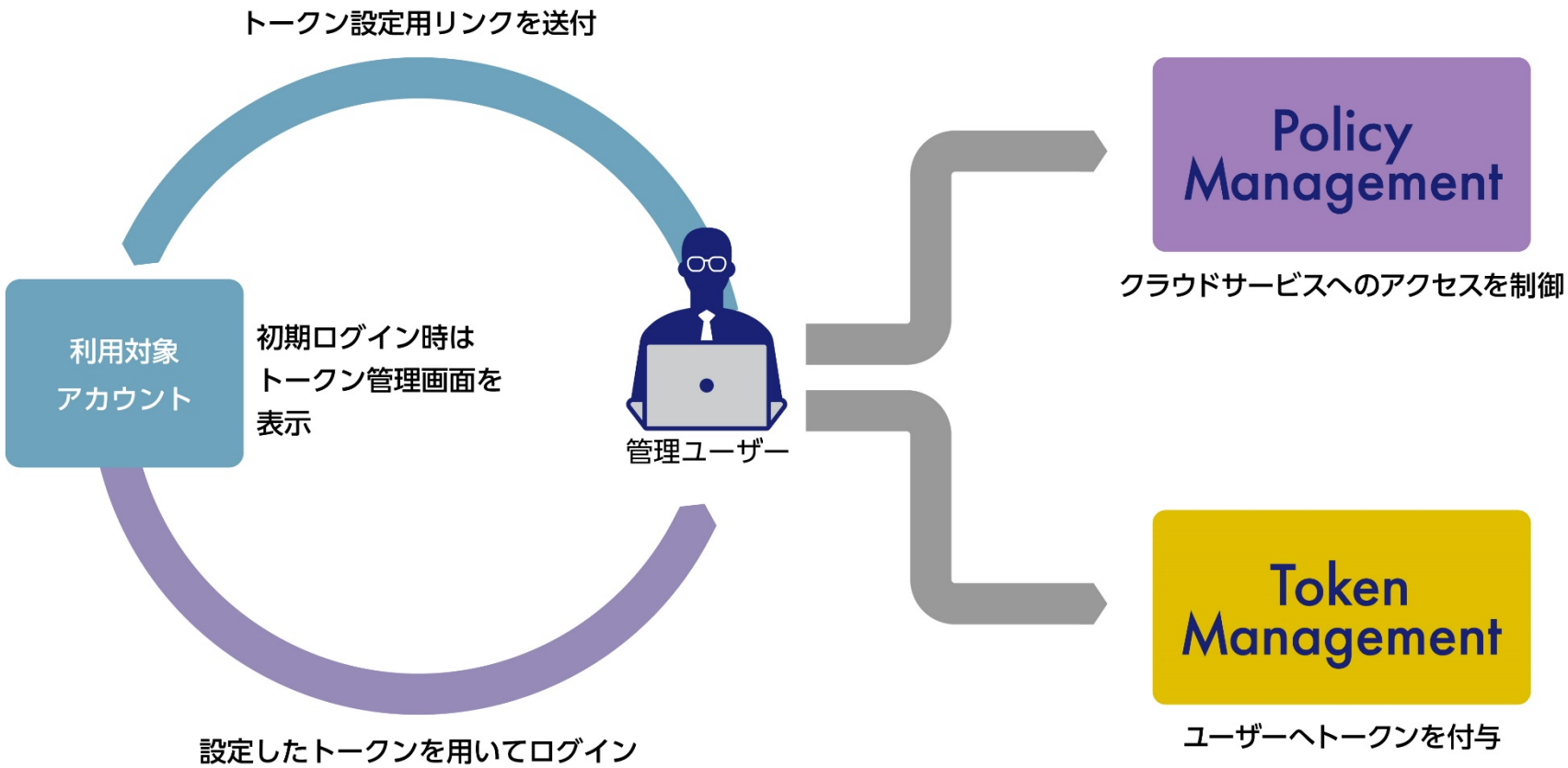
導入後は…

お客様をサポート

- 質疑・障害対応
- 日本語サポート対応
- トークン追加の受付
- Thales サポートへのエスカレーション …etc

管理ユーザー利用手順

「SafeNet Trusted Access」を利用開始すると、管理ユーザのメールアドレスへ、2通のトークン割り当て手順メールが送付されます。メールの設定に従いトークンを設定後、トークン管理画面へログイン可能になります。



SafeNet Trusted Access
統合認証・アクセス管理サービス

- シンプルな構成・容易な設定
- 短期間での導入
- ハイパフォーマンス
- セキュアな管理

FIDO認証にも対応予定

SafeNet Trusted Accessを
ご検討ください。

Canon キヤノンマーケティングジャパン株式会社

https://cweb.canon.jp/it-sec/solution/safenet-trusted-access/

STA 評価版無償貸出サービス実施中！