

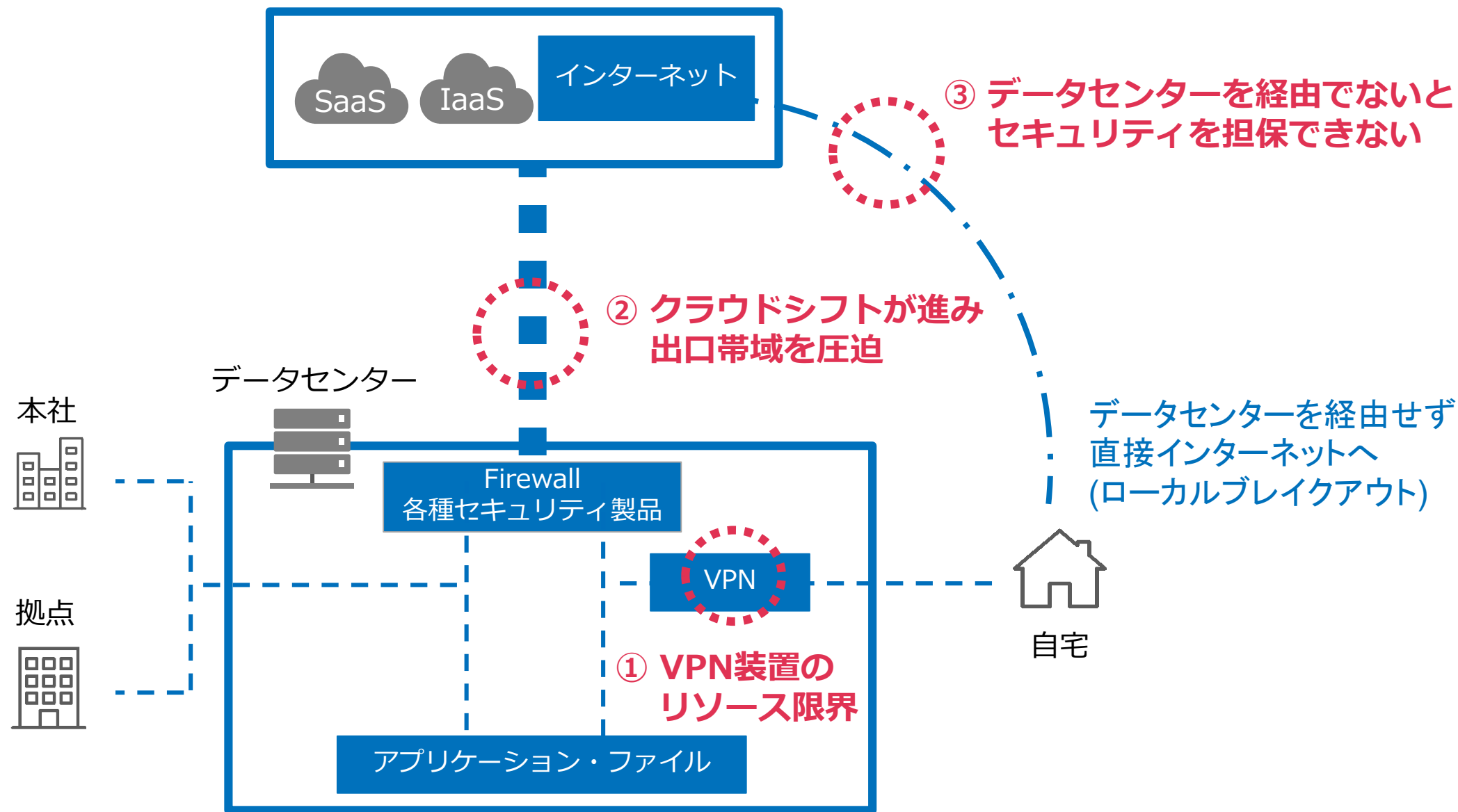


働く場所やデバイスに依存しない 高速で安全なリモートアクセスを実現

伊藤忠テクノソリューションズ株式会社
サイバーセキュリティサービス部

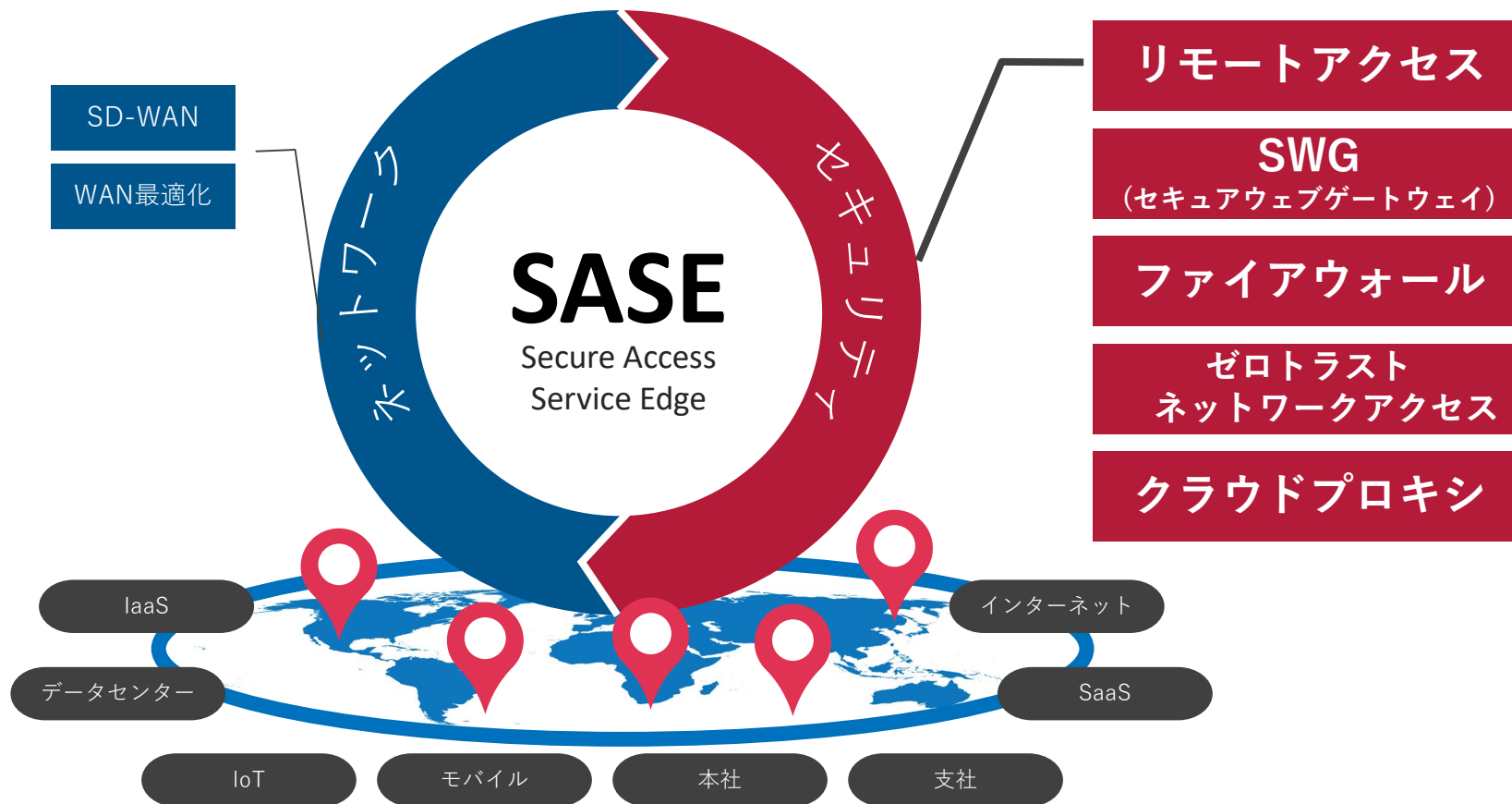
2020/11/6

テレワークユーザ増加によるネットワーク・セキュリティの課題

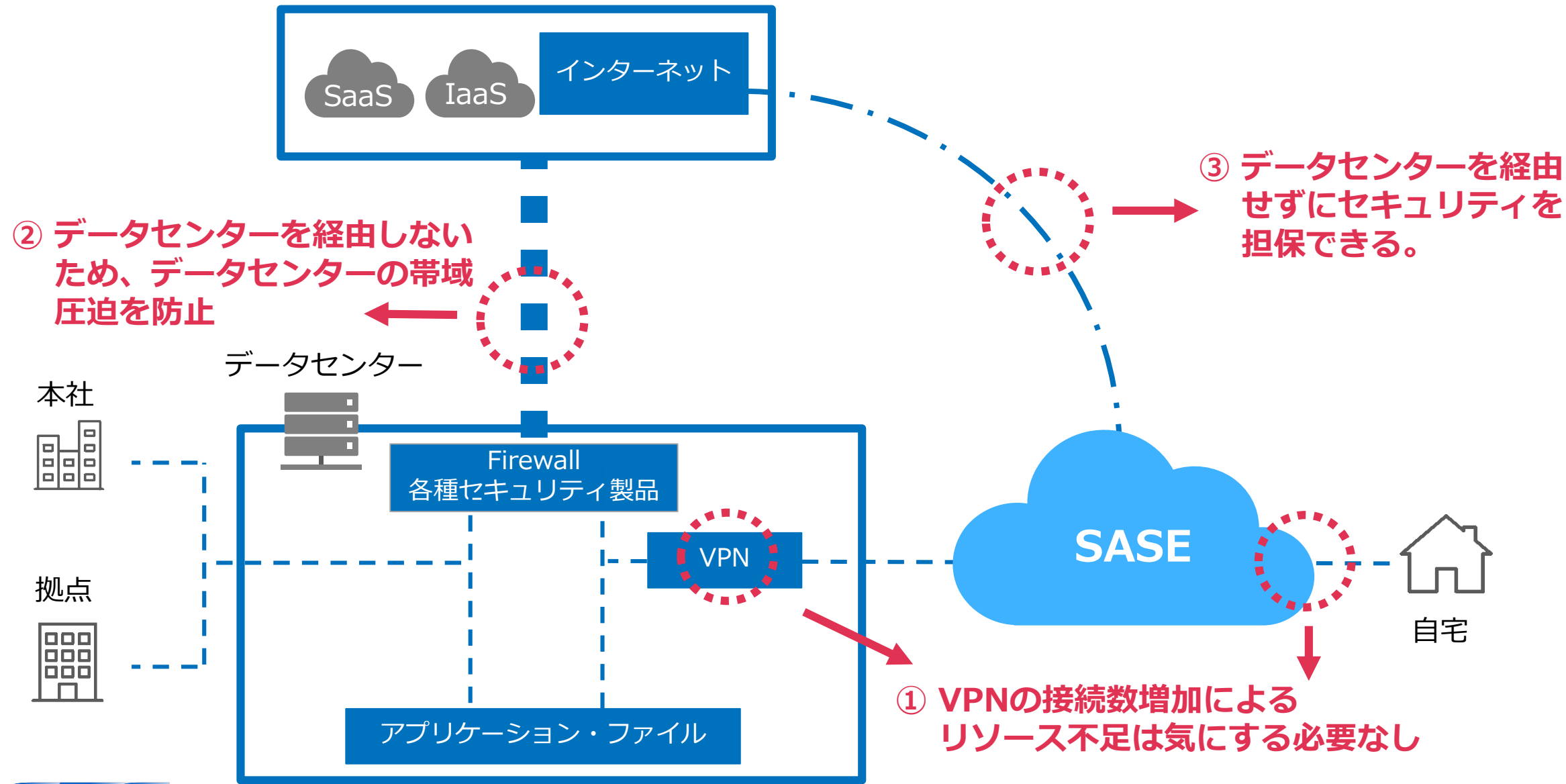


セキュリティのトレンド “SASE”

ネットワークセキュリティをクラウドで提供



SASEを利用したテレワーク環境の例





Zscalerのご紹介

Zscaler社の会社概要

• Zscaler, Inc.

Co-Founder, CEO: Jagtar S. Chaudhry

創業: 2008年

住所: 110 Rose Orchard Way San Jose, CA, USA

従業員: 1500 (1/31/2019)

売上:	FY2016	\$80M	(YoY +49.5%)
	FY2017	\$125M	(YoY +56.5%)
	FY2018	\$190M	(YoY +51.3%)
	FY2019	\$272M	(YoY +43.5%)

• ゼットスケラー株式会社

住所: 東京都千代田区大手町1-9-2

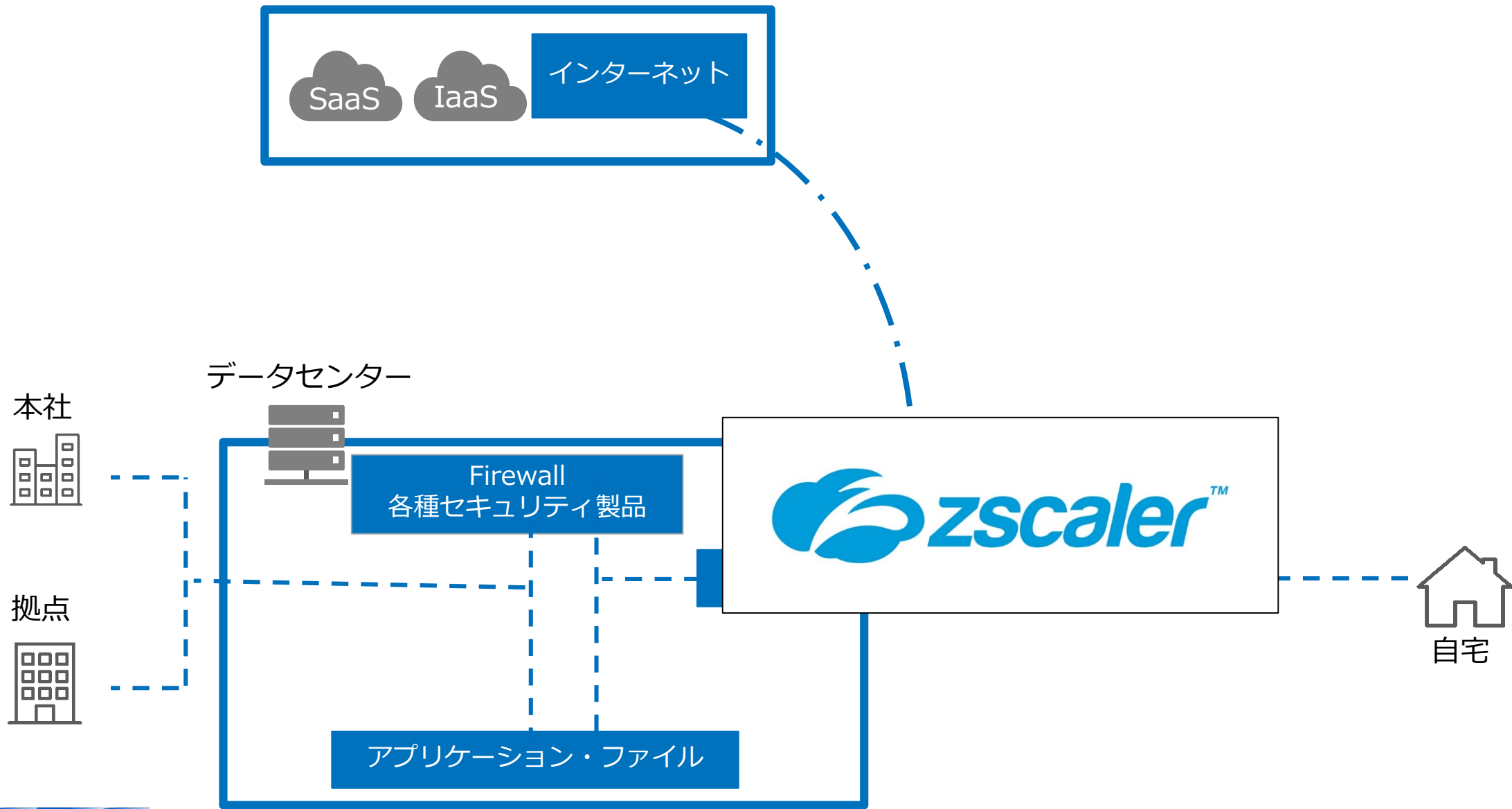
大手町フィナンシャルグランキューブ3階

カントリーマネージャ: Darren McKellin



- Zscaler goes public, largest tech IPO of 2018, as of March 16th, 2018
- Initial valuation of more than \$1.5B
- Market Cap: \$4.3B (10/12/2018)

Zscalerを利用したテレワーク環境の例



Zscalerのスケールビリティ

国境を越えた保護

最大事例：185カ国

保護対象の拠点数

最大事例：11,000

保護対象の従業員数

最大事例：130万人

Office365 月間トラフィック

最大事例：83TB

Unparalleled Cloud Scale

600億+

Transactions Processed
every day

1.7億+

Threats Detected
every day

12万+

Unique Security Updates
every day

最大のセキュリティクラウド

— 信頼性、可用性、高速 —

150カ所のデータセンタ - 5つの大陸

600億超

要求数/日

1億7,000万超

ブロックする脅威/日

12万超

セキュリティアップデート/日



安全性

第三者機関による
テストの継続的な実施

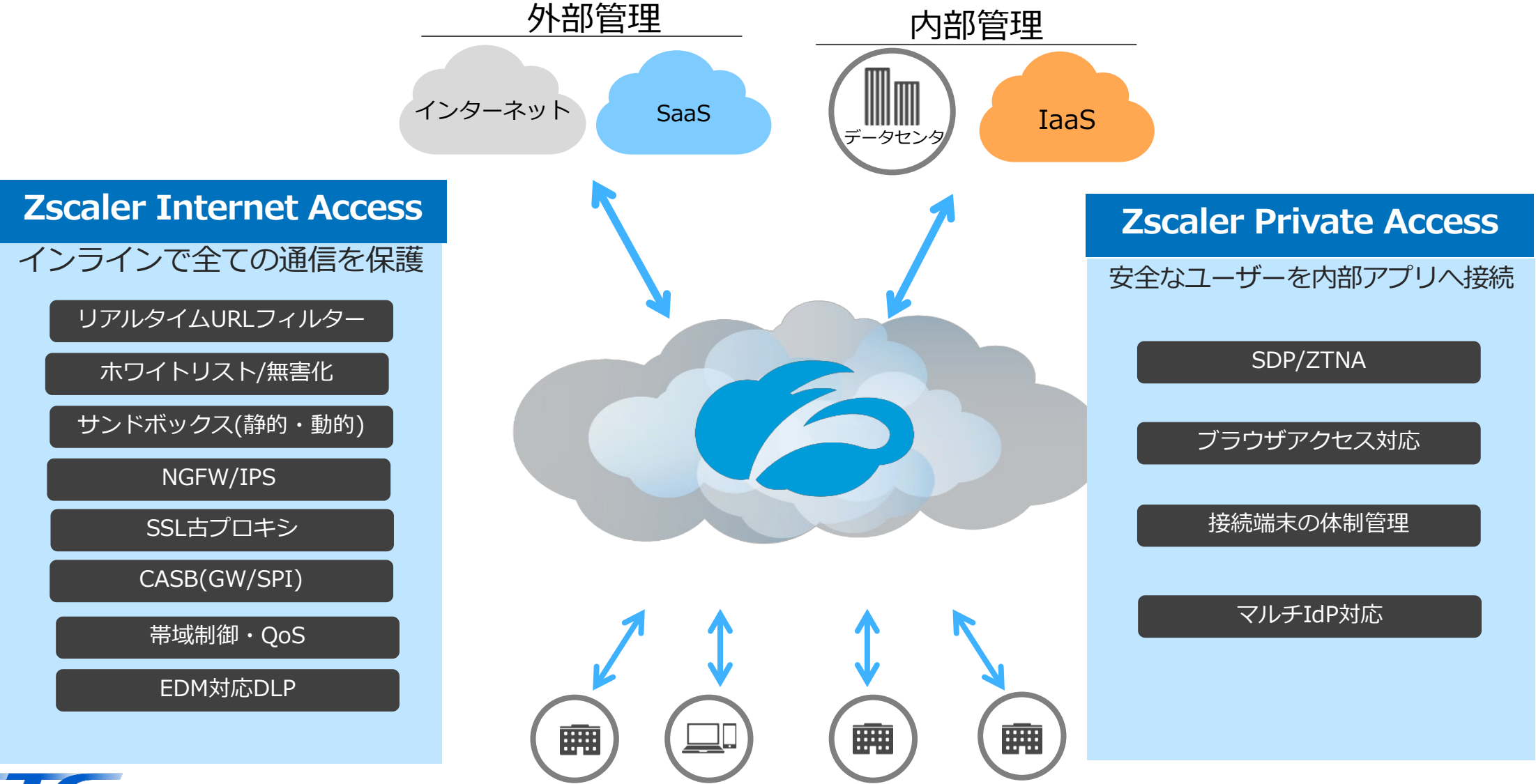
信頼性

DC内での冗長性とDC間での
フェールオーバ

透明性

サービス可用性監視のための
Trust Portal

Zscalerのプラットフォームサービス

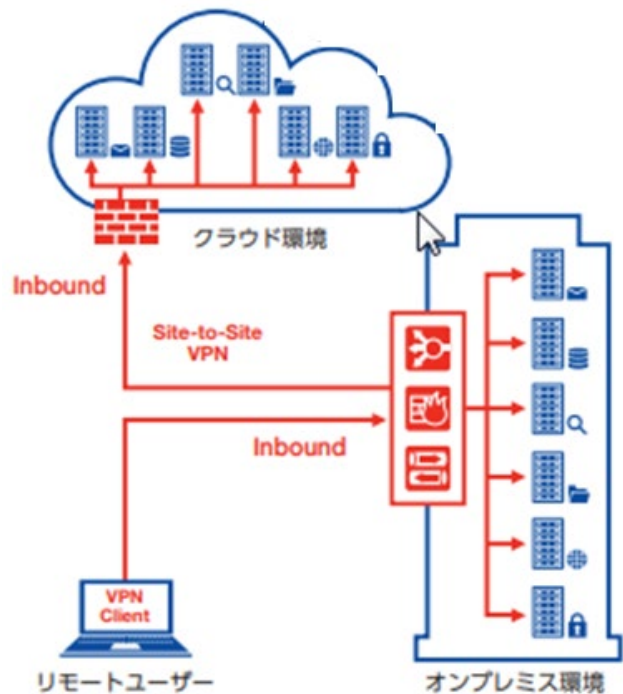


Zscaler Private Access (ZPA) ～概要～

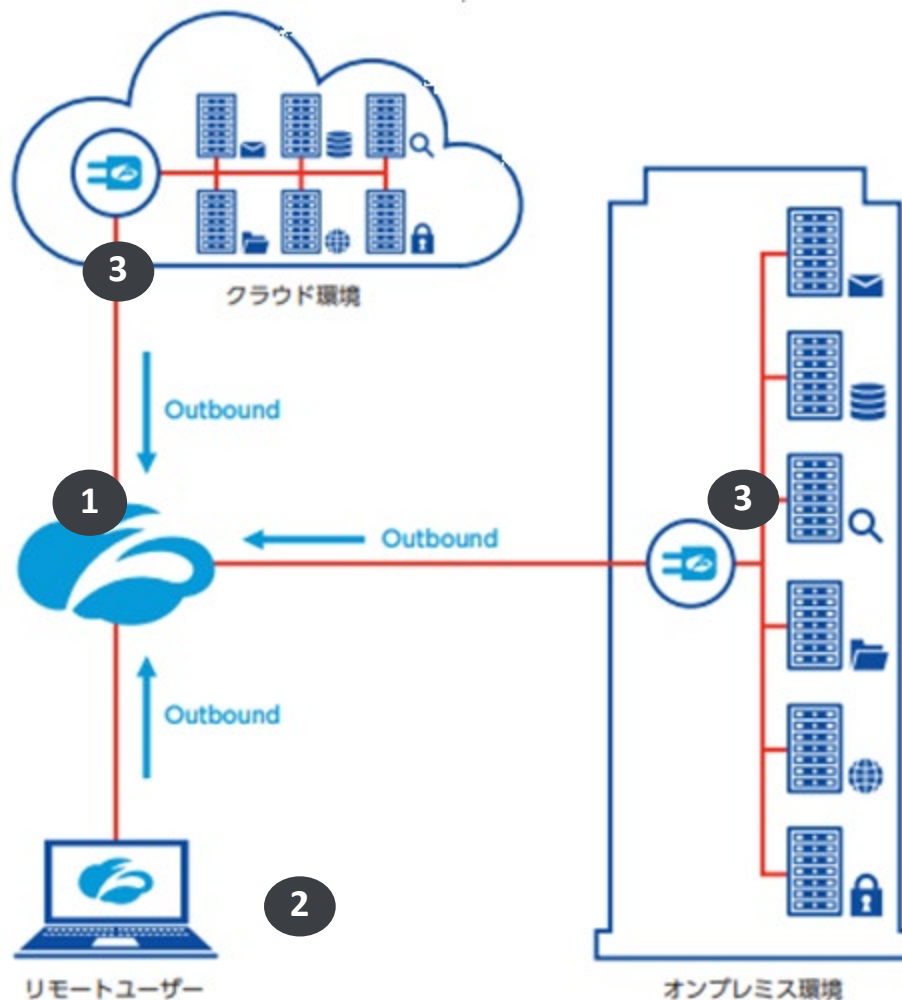
Zscaler Private Accessサービス概要

従来のリモートアクセスの課題

- ・インバウンド通信を許可するセキュリティリスク
- ・専用機器の導入コストおよび運用負荷
- ・プライベートクラウド移行時の対応が複雑



ZPAリモートアクセス構成



- 1 Zscaler Enforcement Node (ZEN)
 - ・クラウドポリシーエンジン
 - ユーザ毎のアクセスをコントロール
- 2 Zscaler App
 - リモートアクセス対象トラフィックをクラウド側に誘導
- 3 App Connector
 - アプリケーションサーバ前段に設置
 - トラフィックはアウトバウンドのみ

アウトバウンドの通信
(グローバルIPアドレス不要)

社内アプリケーション
利用状況の可視化

詳細なアプリケーション
コントロール

ZPAのリモートアクセス構成

① Zscaler Enforcement Node (ZEN)

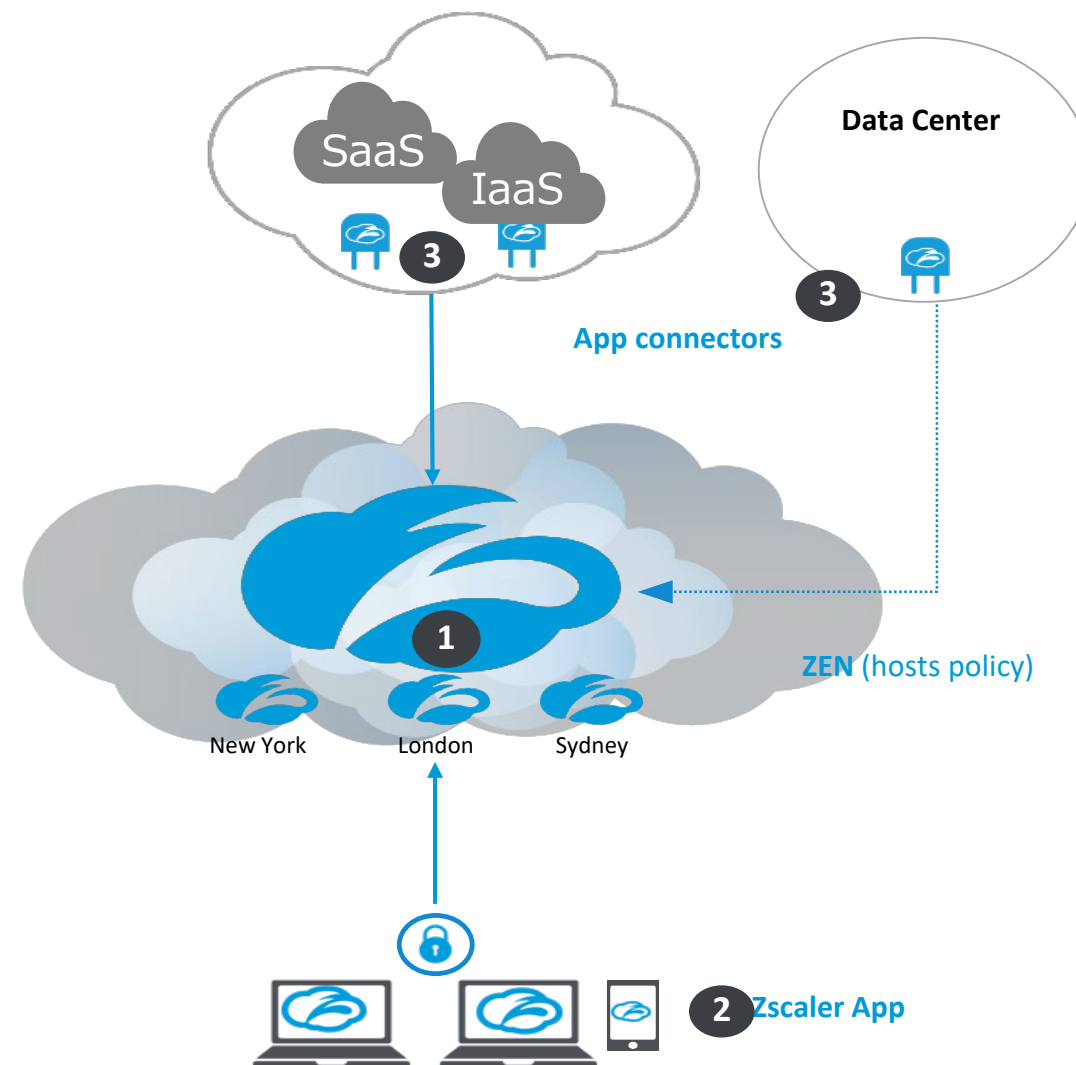
- ・ クラウドポリシーエンジン
- ユーザ毎のアクセスをコントロール

② Zscaler App

- リモートアクセス対象トラフィックをクラウド側に誘導

③ App Connector

- アプリケーションサーバ前段に設置
- トラフィックはアウトバウンドのみ



ユーザの求める使用感と、企業の求めるセキュリティを両立します。

ZPAの構成要素

Zscaler
クラウド



アクセス制御
ポリシー管理
アクセス状況の可視化

Zscaler
App



Windows MacOS
iOS Android

Agent / App on User Devices



ユーザエージェント
無料で提供
PC、モバイル端末に対応

Connector



Virtual Machine / Software



仮想アプライアンス
サーバ拠点側に配備
オンプレ環境、クラウド環境に対応

SAML認証

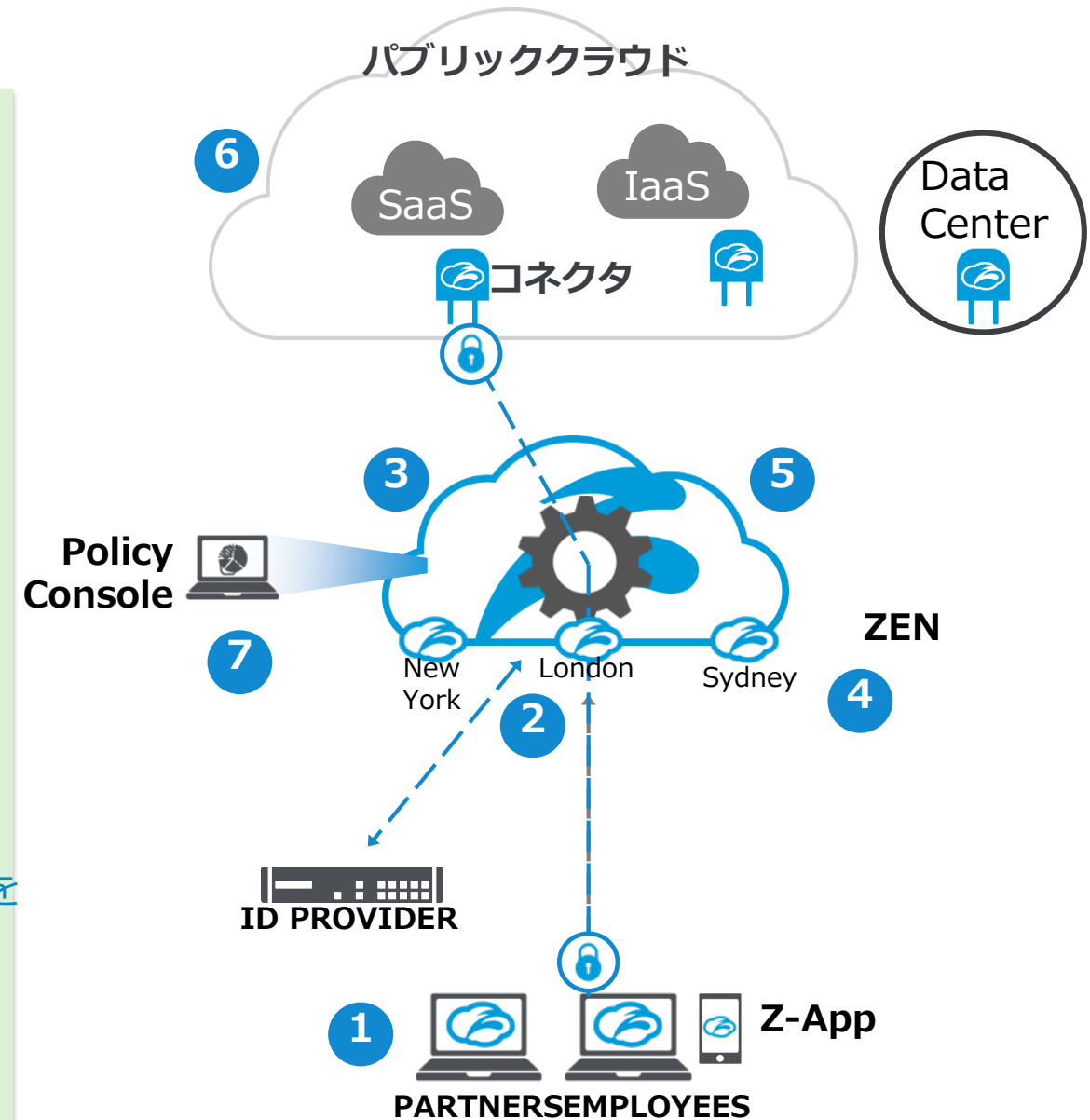
Identity Providers (SAML)



SAML 2.0
接続時のユーザ認証

通信フロー

- 1 ユーザがアプリケーションにアクセス
- 2 IDPへリダイレクトし、ID/Pass認証
- 3 ZPAでポリシーを確認（アクセス可能か否か）
- 4 アクセス先のコネクタを選択
- 5 If allowed:
 - コネクタがトンネルを確立
 - Z-Appがトンネルを確立
 - ZPAにてコネクタとZ-APPのトンネルをディスパッチ
- 6 コネクタがアプリケーションサーバにトラフィックを転送
- 7 コンソールにて接続状況を確認可能



Zscaler Private Access おもな特長



セキュアなアプリアクセス

グローバルIPの公開不要

IDPによる認証

アプリのセグメンテーション

許可されたユーザのみの
アクセス制御

ユーザと利用アプリの可視化

アプリの保護

接続性常時監視

デバイスポスチャ



Zscaler Multitenant Cloud Security Platform



伊藤忠テクノソリューションズ株式会社