NEXTシステムズ株式会社　2005年設立・創業17年目（2021/12/16現在）

私たちは、ITの恩恵を誰もが享受出来る、次世代の社会システムづくりに貢献します。

ビジョン

1. 地域におけるITプラットフォームサービス提供企業を目指し、社会から信頼され必要とされる企業となります。
2. オープンソースやオープンデータを駆使し世界と繋がりながら、自らのサービスで地域社会に貢献します。
3. 次世代の育成に積極的にあたり、ITを駆使して、福岡のアカデミックでサイエンスな街づくりに貢献します。

NEXTシステムズ事業内容

1. IT運用支援/IT保守サービス
2. オープンソースでのITサービスの構築・サポート
3. 会員管理/地図情報システム/電力関連システムなどの開発
4. 情報セキュリティマネジメントシステムコンサルティング

IT運用管理・ITサービス開発・プロジェクト管理支援

本日のキーワード

- DX
- ゼロトラスト
- SD-WAN（Software Defined Wide Area Network）
- ローカルブレイクアウト
- アイデンティティ認証型プロキシ（IAP）

お客様の声

クラウドでのITサービス構築（オープンソース）

■DX/ITサービスプラットフォーム（オンラインストレージ）

Mattermost ■チャット

OTRS ■ヘルプデスク管理

REDMINE ■プロジェクト管理

knowledge ■ナレッジ共有

GitLab ■DevOps

ZABBIX ■監視

さくらインターネットのサービスラインナップ

各サービスは連携が可能。お客様要件に合わせたシステム構築を実現

SAKURA internet

レンタルサーバ

さくらのレンタルサーバ
さくらのマネージドサーバ

<用途>
メール・ブログ・ホームページなど

1台を共有 | 1台を占有

VPS

さくらのVPS(Linux)
さくらのVPS(Windows)

<用途>
お客様サービスの検証・開発環境など

仮想サーバを占有

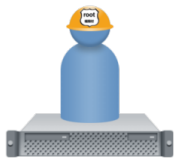
クラウド

さくらのクラウド
sakura cloud

<用途>
お客様サービスの検証・開発環境・本番環境
手軽にリソースを増減可能

- 仮想サーバ
- 仮想ネットワーク
- 仮想アプライアンス
- オプションサービス

専用サーバ



さくらの専用サーバ

<用途>
お客様サービス等の本番環境
仮想サーバがNGなお客様向け

1台～複数台

データセンター

ハウジング

<用途>
お客様サーバールームの代替

1ラック～ゾーン専有

その他サービス

高火力
KOUKARYOKU

GPU 搭載の専用サーバプラン
研究・学術に向けに提供する
計算処理特化のサーバプランン

セキュアモバイルコネクト

IoTモジュール、モバイルルータを
クラウドサービスと閉域網接続を
マルチキャリアで提供するサービス

その他サービス

- ウェブアクセラレータ
- ImageFlux
- マーケットプレイス
- ハイブリッド・ブリッジ接続
- 簡単にCDNを提供するサービス
- 手軽に画像を加工、配信するプラットフォームサービス
- パートナーが提供するサービスをクラウド上で販売する制度
- VPS、クラウド、専用サーバ、データセンターを繋ぐサービス

参考文献、参考コンテンツ

- NIST（アメリカ国立標準技術研究所）
「SP800-207：Zero Trust Architecture(ZTA)」（PWC翻訳版）

- IPAゼロトラスト導入指南書（2021年6月）
（独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 4期生 ゼロトラストプロジェクト）

- すべてわかる「ゼロトラスト大全」（日経BPムック、日経XTECH編）

- 経済産業省 DXレポート2.0 中間取りまとめ（令和2年12月28日）→2.1追補版（令和2年8月31日）

- フォーティネットのセキュアSD-WAN（ソリューションの概要とアーキテクチャガイド）

おすすめ書籍


NIST Special Publication 800-207

ゼロトラスト・アーキテクチャ

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

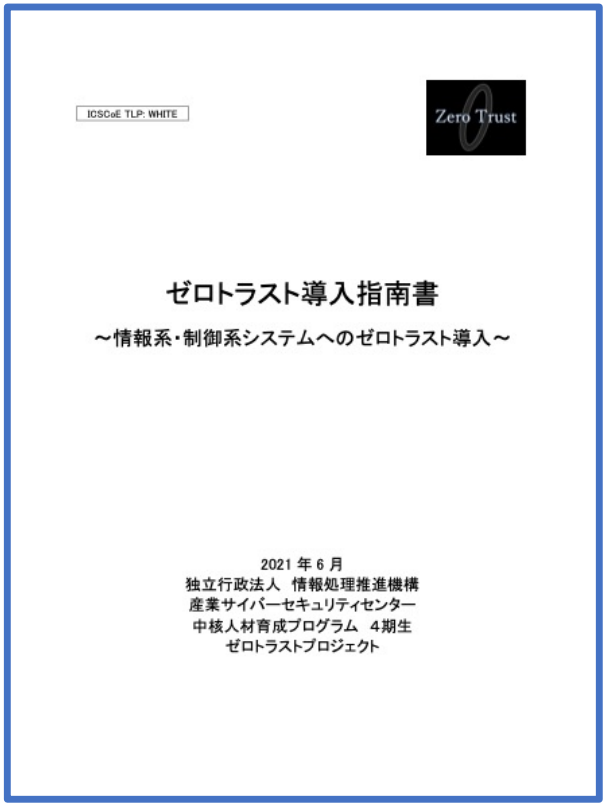
本書は、以下より無料で利用可能である:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

邦訳:PwCコンサルティング合同会社

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は、本文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体についても責任を負うものではありません。


ICSCoE TLP: WHITE

Zero Trust

ゼロトラスト導入指南書

～情報系・制御系システムへのゼロトラスト導入～

2021 年 6 月
独立行政法人 情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム 4期生
ゼロトラストプロジェクト

経済産業省 DXレポート2.0 中間取りまとめ
（令和2年12月28日）→2.1追補版（令和2年8月31日）

ユーオスグループデジタルフェア2021

UOS Digital Fair 2021、11月4日・9日・11日開催

時代を読み解く9講演

「デジタル化の本質とデジタル産業の創出」

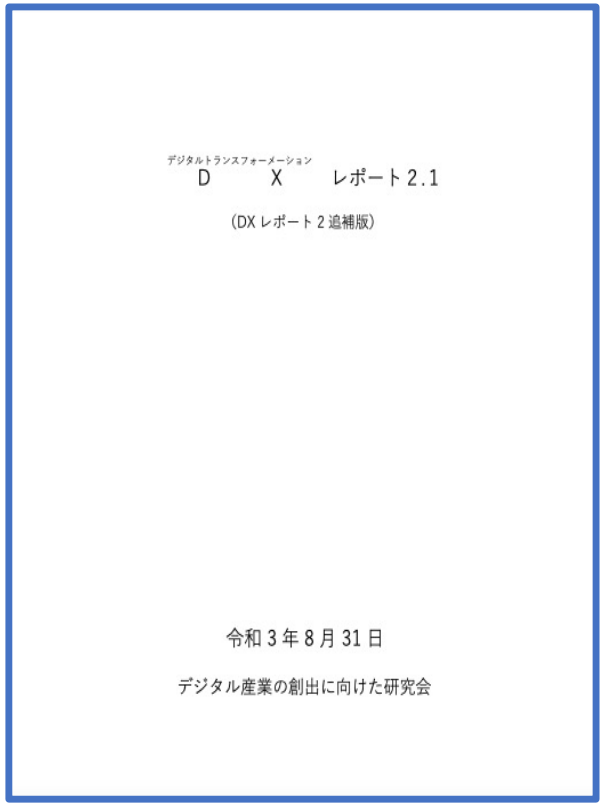
– 成長ビジネスへの変革にむけたDX推進の現状とこれから –

経済産業省

商務情報政策局情報経済課アーキテクチャ戦略企画室長

和泉 憲明 様

（政府の方向性） https://www.youtube.com/watch?v=QdYZ-hRIQTU



DXレポート2.1（DXレポート2.0追補版）

- つまり、DXの終着点における企業の姿とは、

価値創出の全体にデジ タルケイパビリティ（=価値を創出するための事業能力をソフトウェアによってデジタル化したもの)を活用し、デジタルケイパビリティを介して他社・顧客とつながり、エコシステムを形成している姿と考えられる。

これらの企業はインターネットを介してそれを顧客に提供する。これによって、労働量によらない収益拡大(=高い生産性)と、グローバル規模でのビジネス拡大が実現される。

デジタルケイパビリティ（組織能力）

（=価値を創出するための事業能力をソフトウェアによってデジタル化したもの）

↑ ↓

DX/ITサービスプラットフォーム

（サービスがオープンなアーキテクチャーのもとで相互に接続する）

↑ ↓

ネットワークのパフォーマンス要求とセキュリティ

↓

ゼロトラストアーキテクチャ on SD-WAN

ネットワークのパフォーマンス要求とゼロトラスト

レガシーWANの模式図

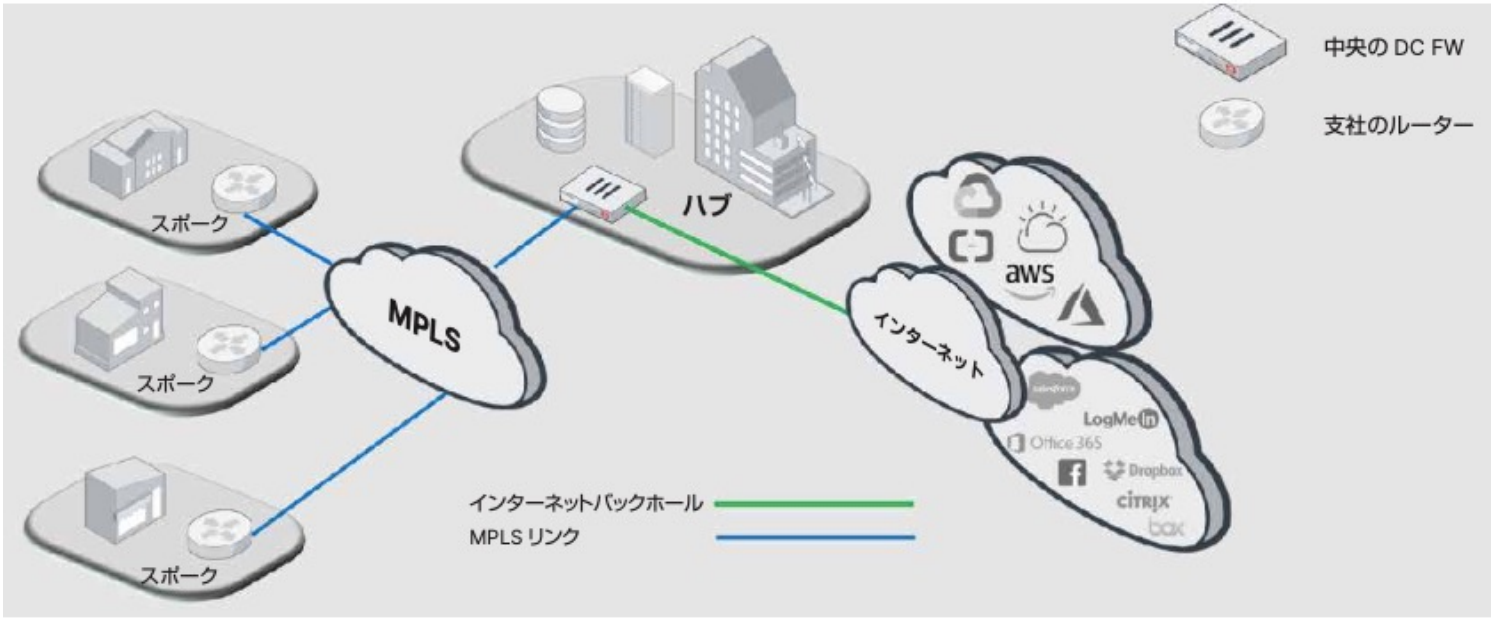
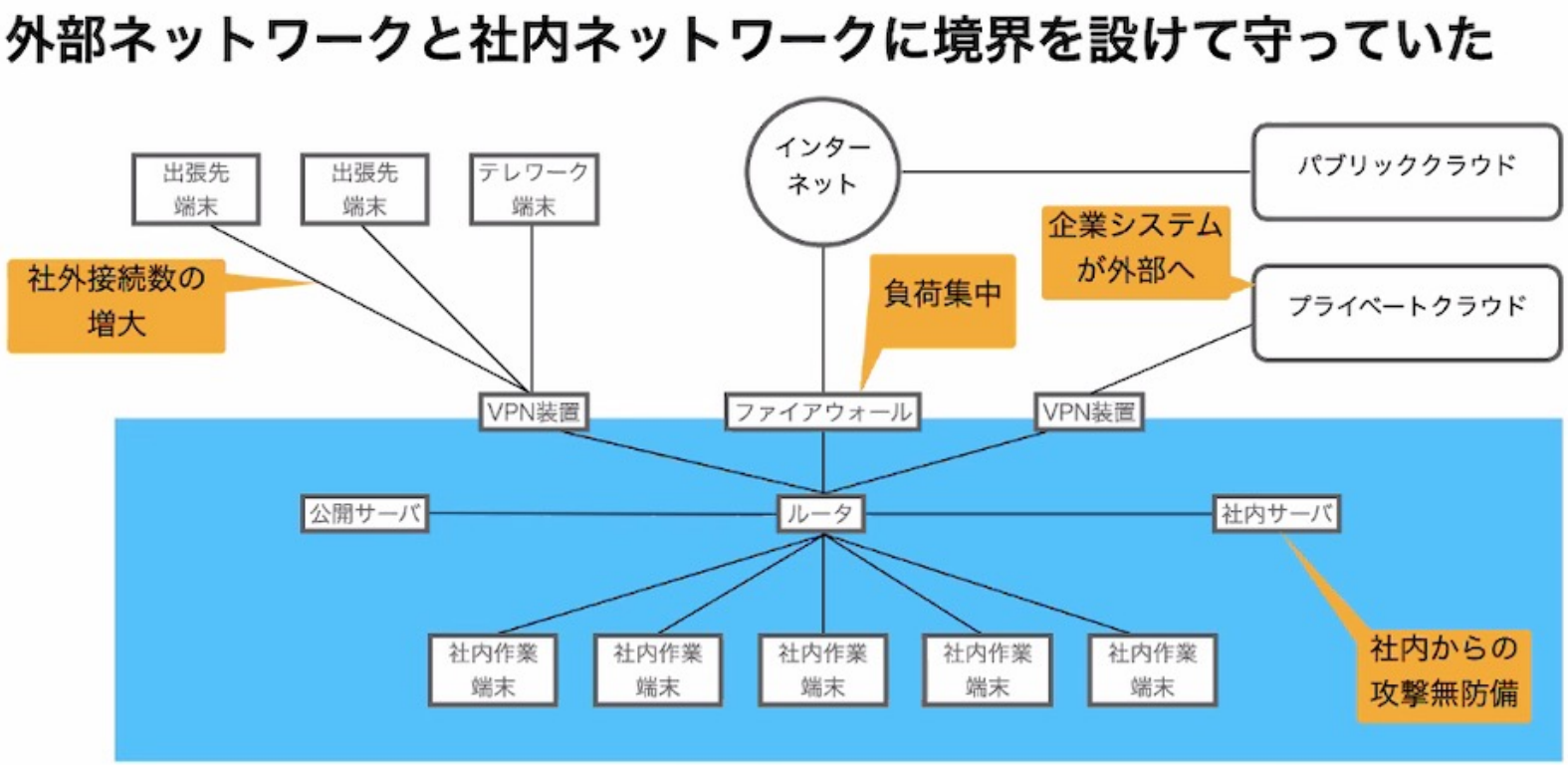
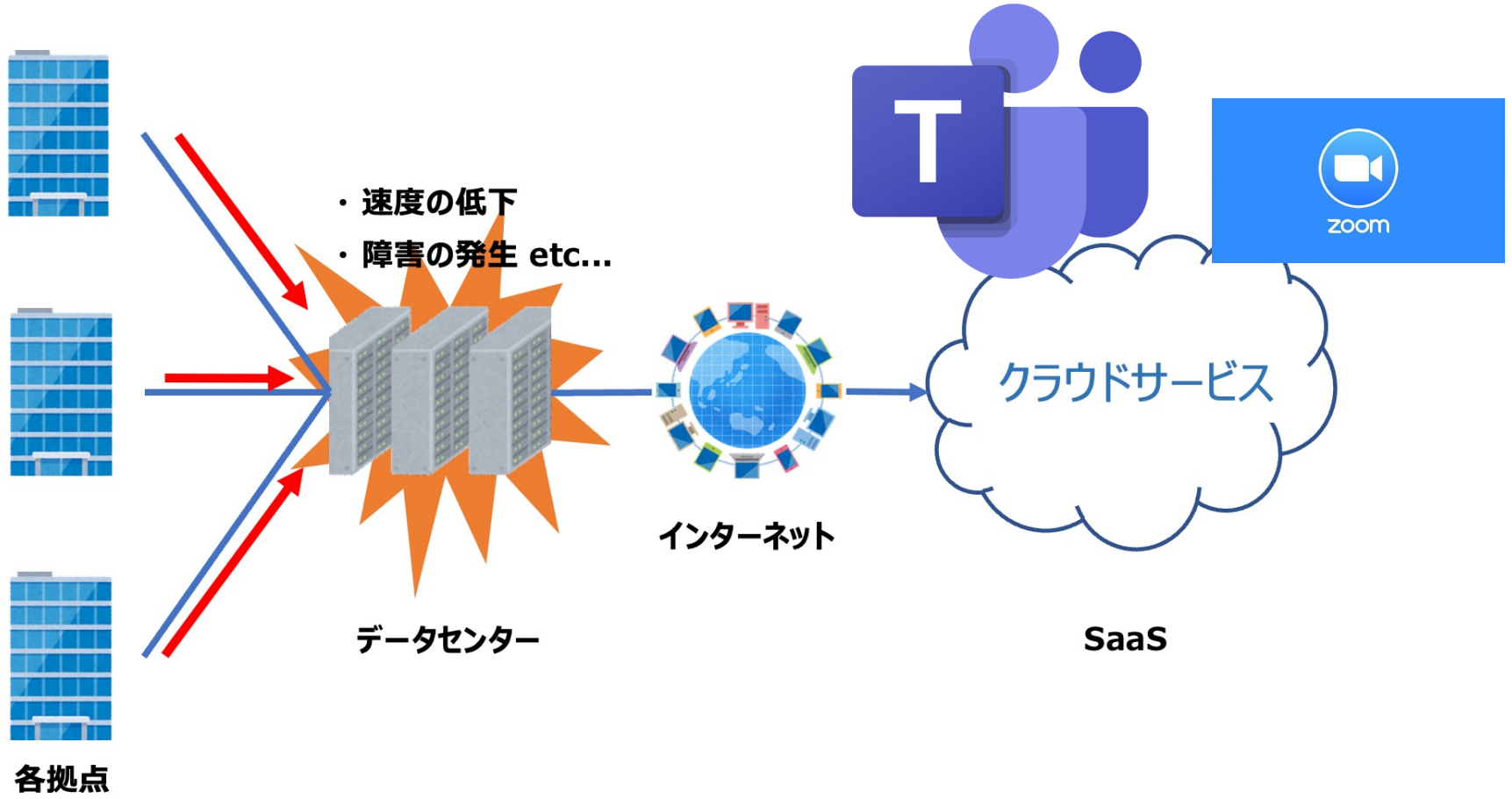


図 1：ハブ & スポークアーキテクチャのレガシー WAN

DEPLOYMENT GUIDE|フォーティネットのセキュアSD-WAN:ソリューション概要/アーキテクチャガイド、より

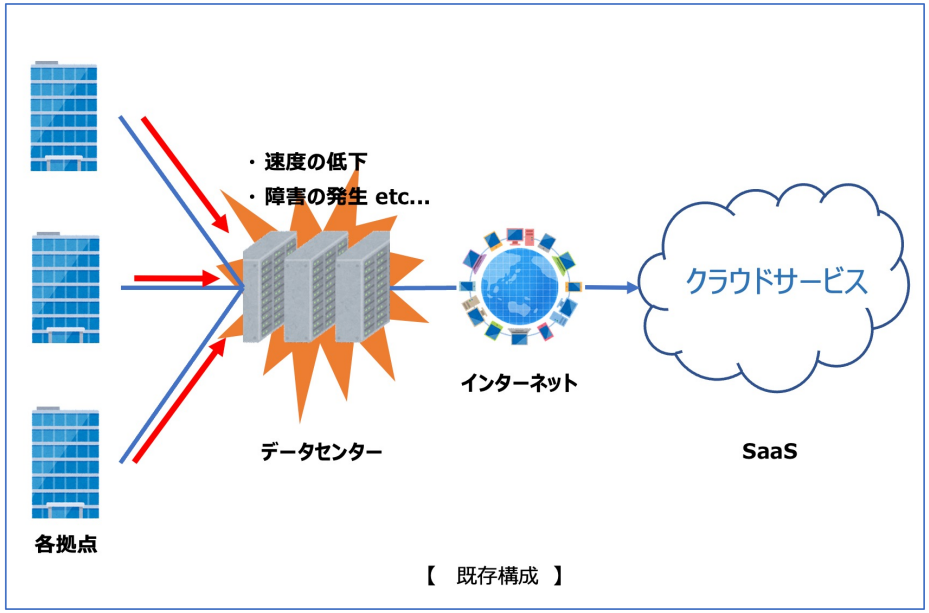
現在のネットワークデザイン

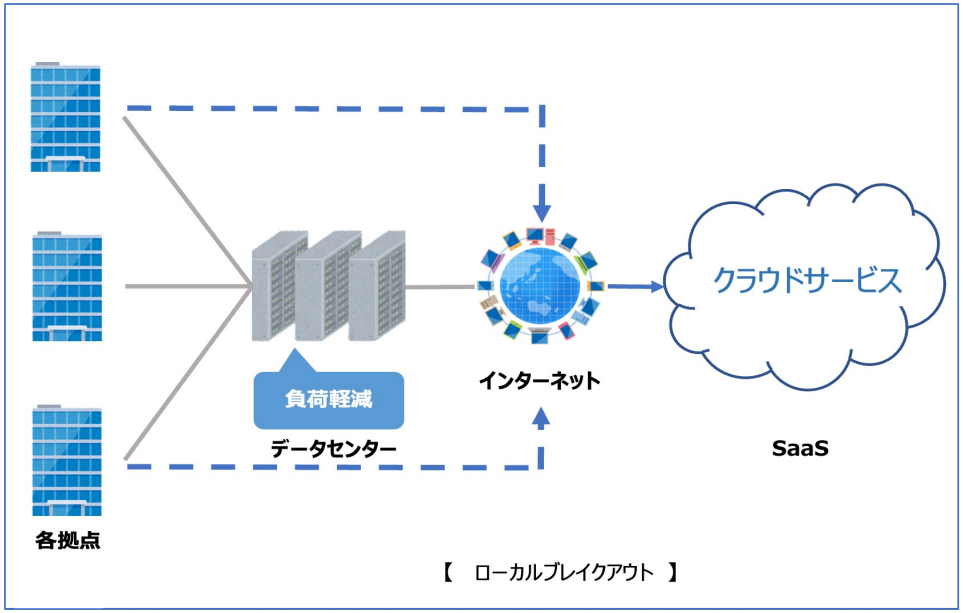




【　既存構成　】

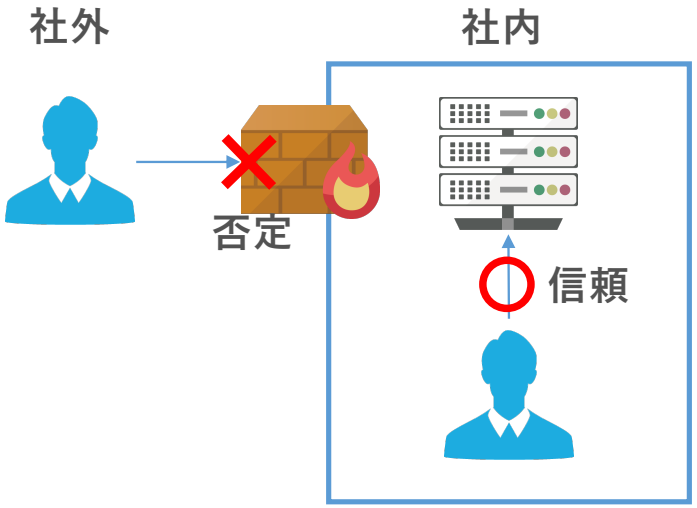
ローカルブレイクアウト





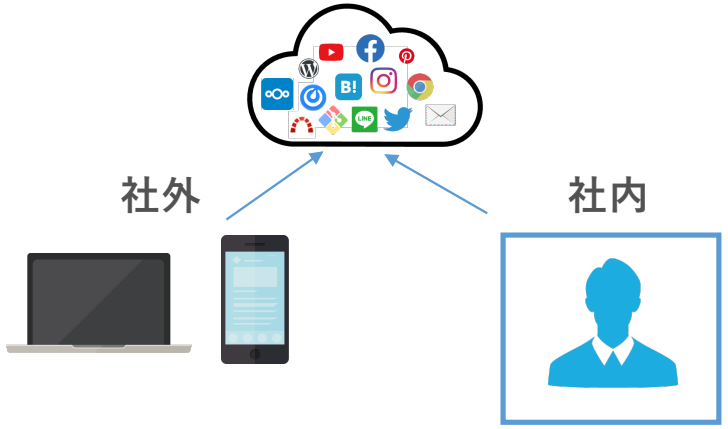
セキュリティモデルを変化させる必要がある

従来のセキュリティ・モデル



社内/社外といった「アクセス元の場所」によって、境界を設け、社外からのアクセスは禁止し社内からのアクセスは「信頼できる」として、柔軟なアクセスや権限を提供する。

ゼロ・トラストセキュリティ・モデル



どんなユーザ、端末、場所からのアクセスに対しても検証し、認証し、最小限のアクセス権限を提供する。

アクセスされた場所は考慮せず、常に「認証」＋「最小権限」を与える、クラウド時代に対応したセキュリティを考えるモデル。

ゼロトラスト（ZT）

現状のセキュリティ対策は、境界型防御が主流であり、社内を信用できる領域、社外を信用できない領域として外部からの接続を遮断している。

しかし上記の社会変化から、社内のシステム環境へ社外から接続するということが行われていることから、境界型防御で考えていたセキュリティモデルではサイバー攻撃の脅威を防ぎきれない状況になってきている。

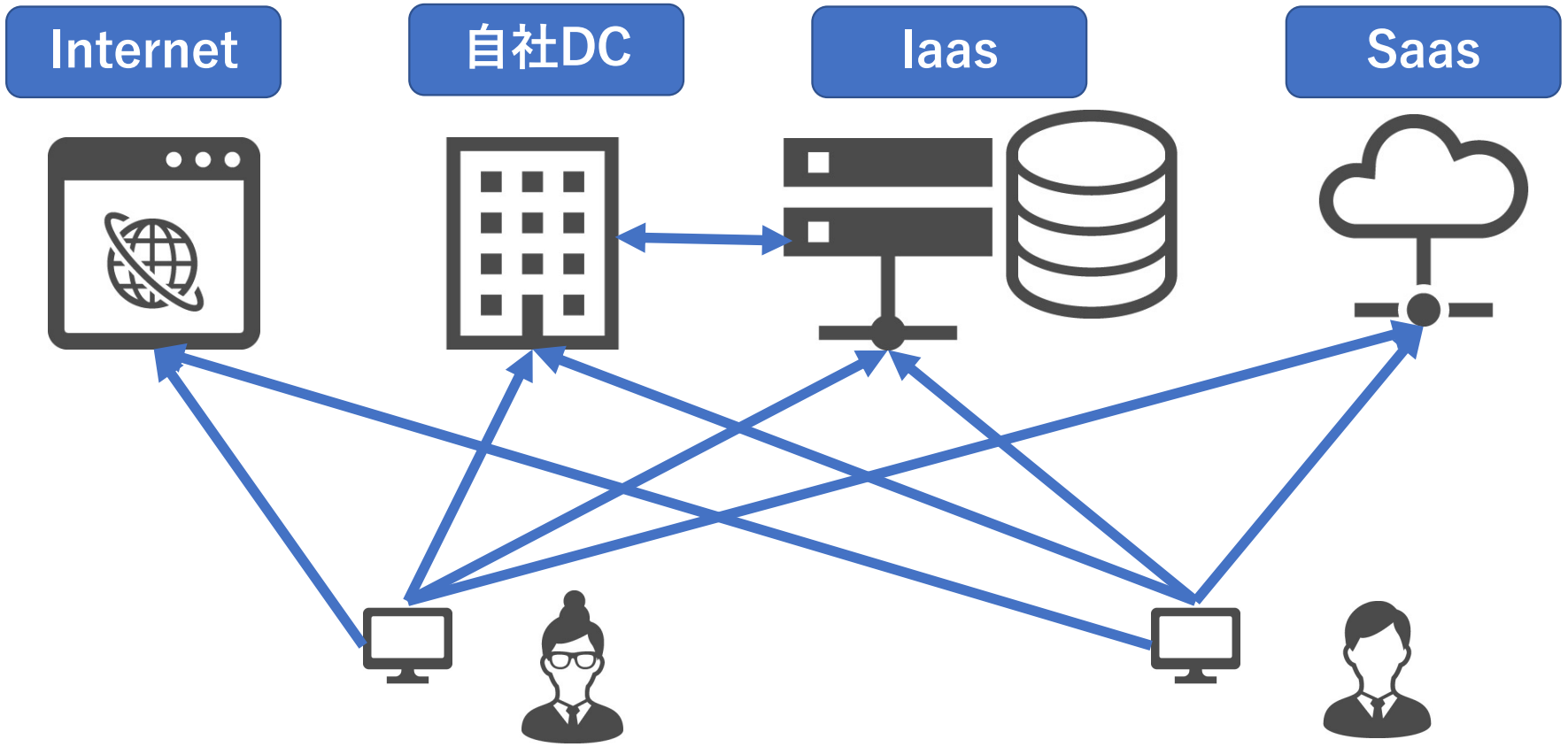
また、標的型メールによる社内端末のウイルス感染の事象も増加しているなど、社内が信用できる領域として考えることが困難な状況となってきている。

これらに対するセキュリティ対策として、「ゼロトラスト」という概念が提唱されている。

これは社内外 すべてを信用できない領域として、全ての通信を検知し認証を行うという考え方であり、ゼロトラストを完全に導入すれば境界型防御をなくすことができるという考え方でもある。

出典：NIST（アメリカ国立標準技術研究所）「SP800-207：Zero Trust Architecture(ZTA)」

ユーザーの居場所が分散し、アプリケーションへの経路が分散する



ゼロトラストアーキテクチャ（ZTA）の要求事項

NIST「SP800-207：Zero Trust Architecture(ZTA)」からの要約

1. すべてのデータソースとコンピューティングサービスをリソースとしてみなし、ネットワークの場所に関係なく、全ての通信を保護する。
2. 企業リソースへのアクセスは、セッション単位で付与され、リソースへのアクセスは、クライアントのアイデンティティ（不変性、独自性）やアプリケーション・サービスの特性など動的でそれぞれのポリシーにより決定される。
3. すべての資産の整合性とセキュリティ動作を監視し、測定する。
4. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に行われる。
5. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。

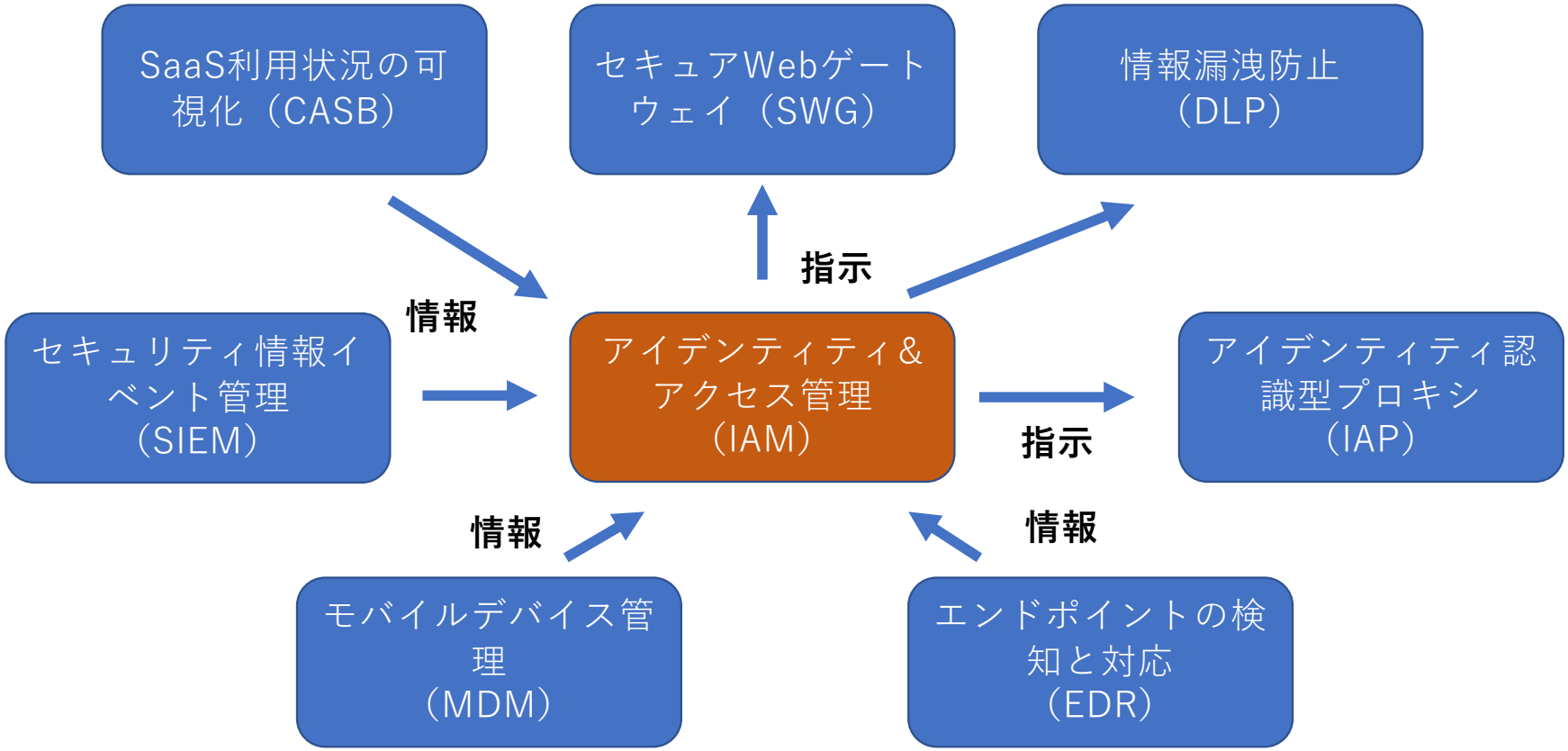
ZTAを支える8つの技術

IAM（Identity and Access Management） ID&アクセス管理	ユーザーの「認証」やアプリケーションやデータに対するアクセスの「認可」を制御する機能
IAP（Identity-Aware Proxy） ID認識型アクセスプロキシ	アプリケーションへのアクセス制御と社内にあるシステムへのコネクターを提供する機能
EDR（Endpoint Detection and Response） エンドポイントセキュリティ	エンドポイントの検知と対応 検知・拡散防止・遮断・調査・修復
MDM（Mobile Device Management） モバイルデバイス管理	モバイルデバイスの遠隔制御機能
SEIM（Security Information and Event Management） セキュリティ情報イベント管理	ログデータ収集分析

ZTAを支える8つの技術

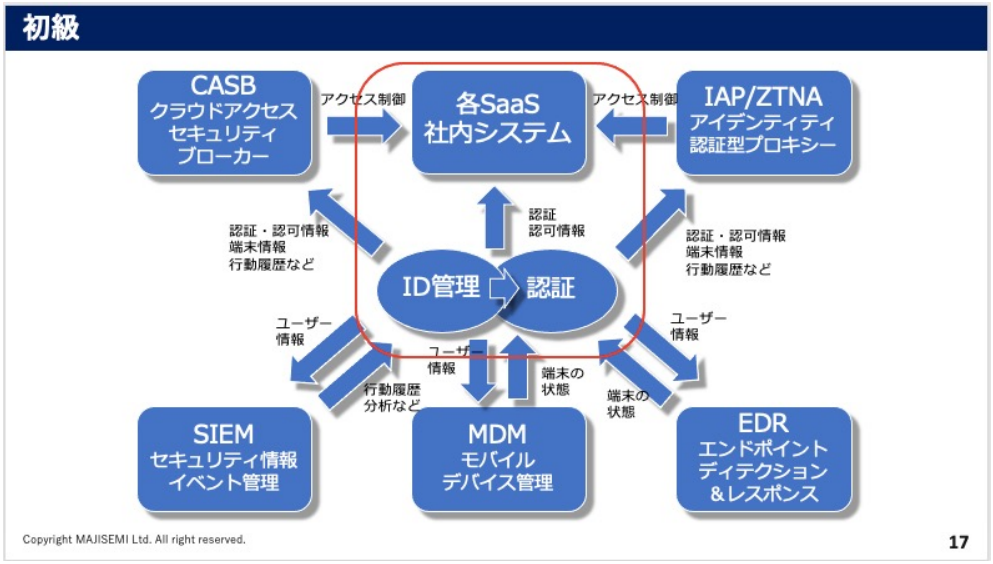
CASB（Cloud Access Security Broker） クラウドアクセスセキュリティブローカー	SaaS利用状況の可視化
SWG（Secure Web Gateway） セキュアWebゲートウェイ	インターネット上のWebセキュリティプロキシ
DLP（Data Loss Prevention） 情報漏洩防止	機密性を保持するデータの保護

ZTA技術とその関係性



2021年7月30日開催　ゼロトラスト「超」入門
～ゼロトラストの概要を初級・中級・上級の3段階で解説～

マジセミ



- https://majisemi.com/e/c/ncipher-20210730

2021-12-17（金）15:00 - 17:00
ゼロトラストの「実装パターン」を解説 ～難しいゼロトラスト、具体的な構成はどうなる？～
https://majisemi-security.doorkeeper.jp/events/130280
■ゼロトラストの「実装パターン」を解説

2021-12-22（水）13:00 - 14:00
Zscalerでセキュリティと性能を両立
https://majisemi-security.doorkeeper.jp/events/130573
■Zscalerの概念や原理、特徴を紹介するとともに、Zscalerを用いたゼロトラストの実現についてもお伝えします。

ゼロトラストアーキテクチャ（ZTA）での要求事項

NIST「SP800-207：Zero Trust Architecture(ZTA)」からの要約

1. すべてのデータソースとコンピューティングサービスをリソースとしてみなし、ネットワークの場所に関係なく、全ての通信を保護する。

2. 企業リソースへのアクセスは、セッション単位で付与され、リソースへのアクセスは、クライアントのアイデンティティ（不変性、独自性）やアプリケーション・サービスの特性など動的でそれぞれのポリシーにより決定される。

3. すべての資産の整合性とセキュリティ動作を監視し、測定する。

4. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に行われる。

5. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する。

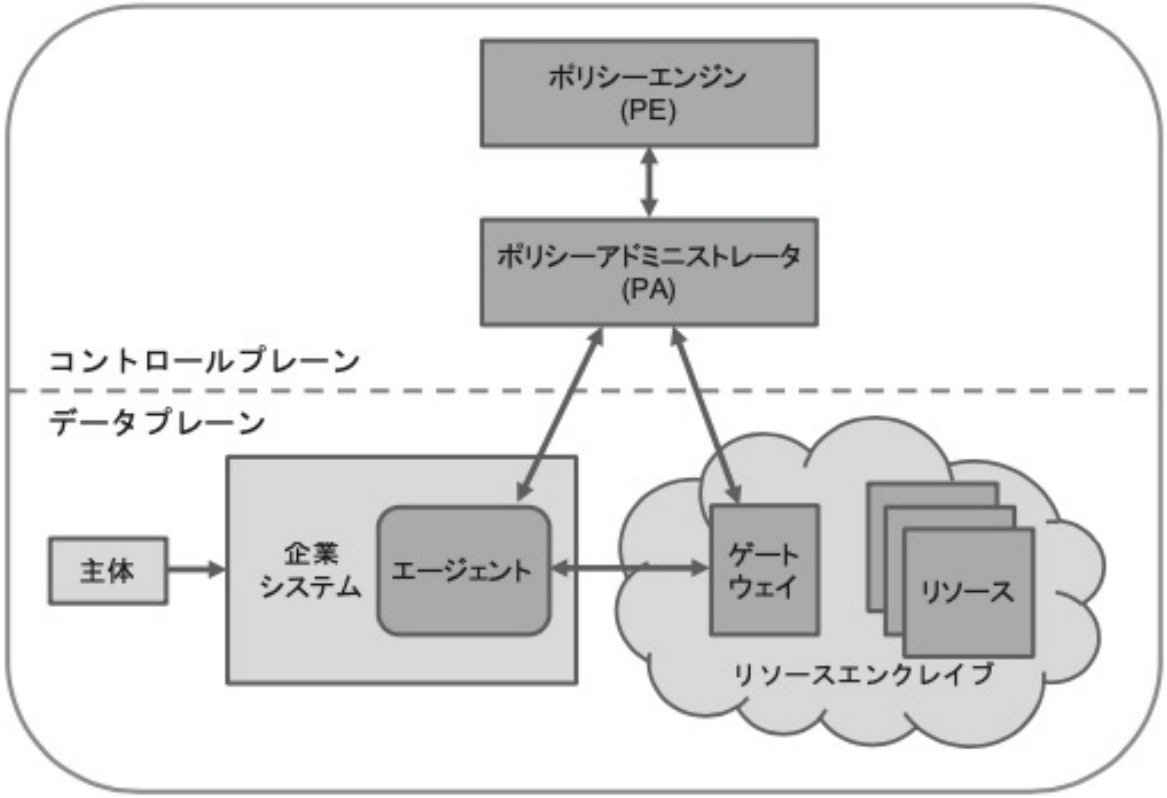
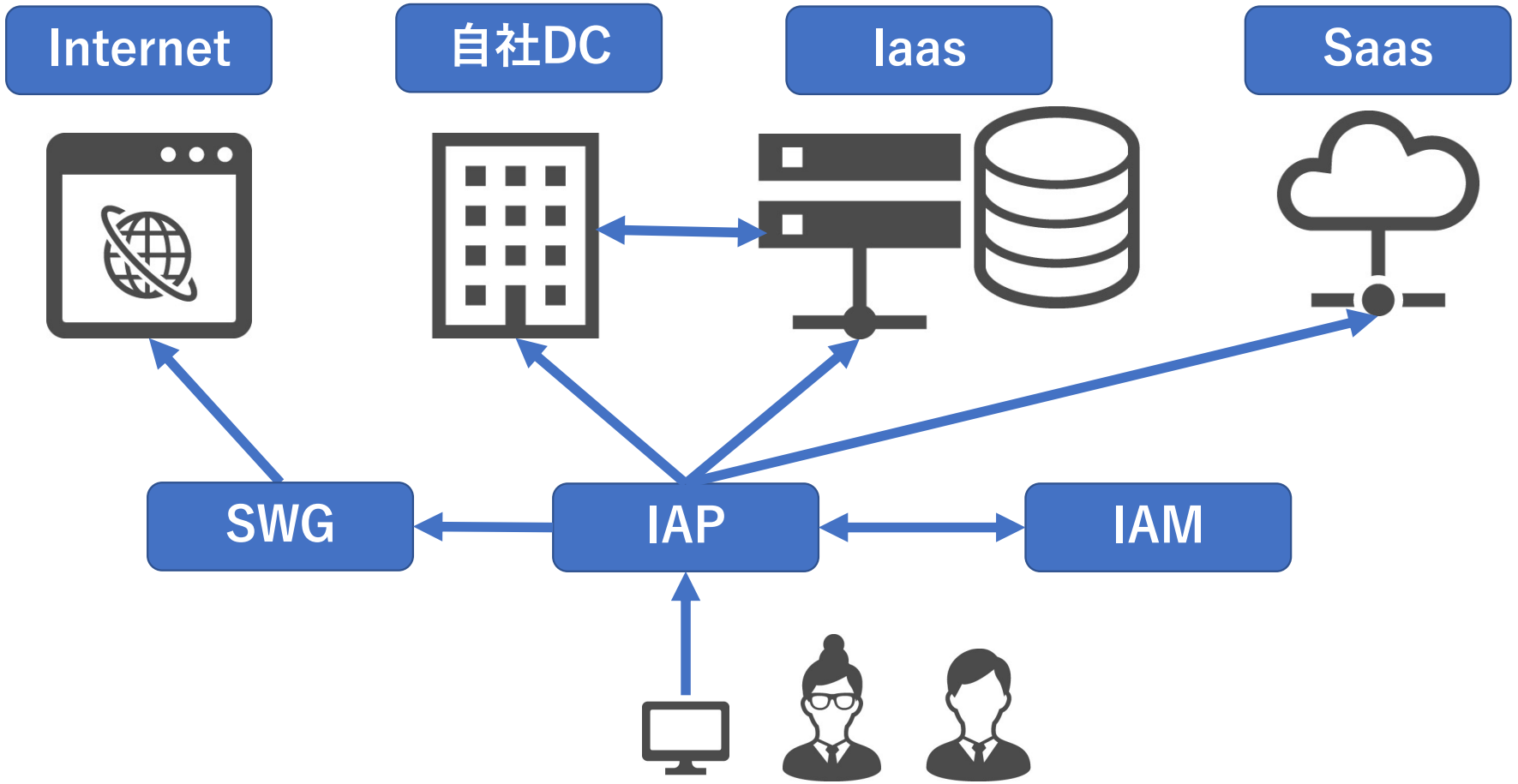
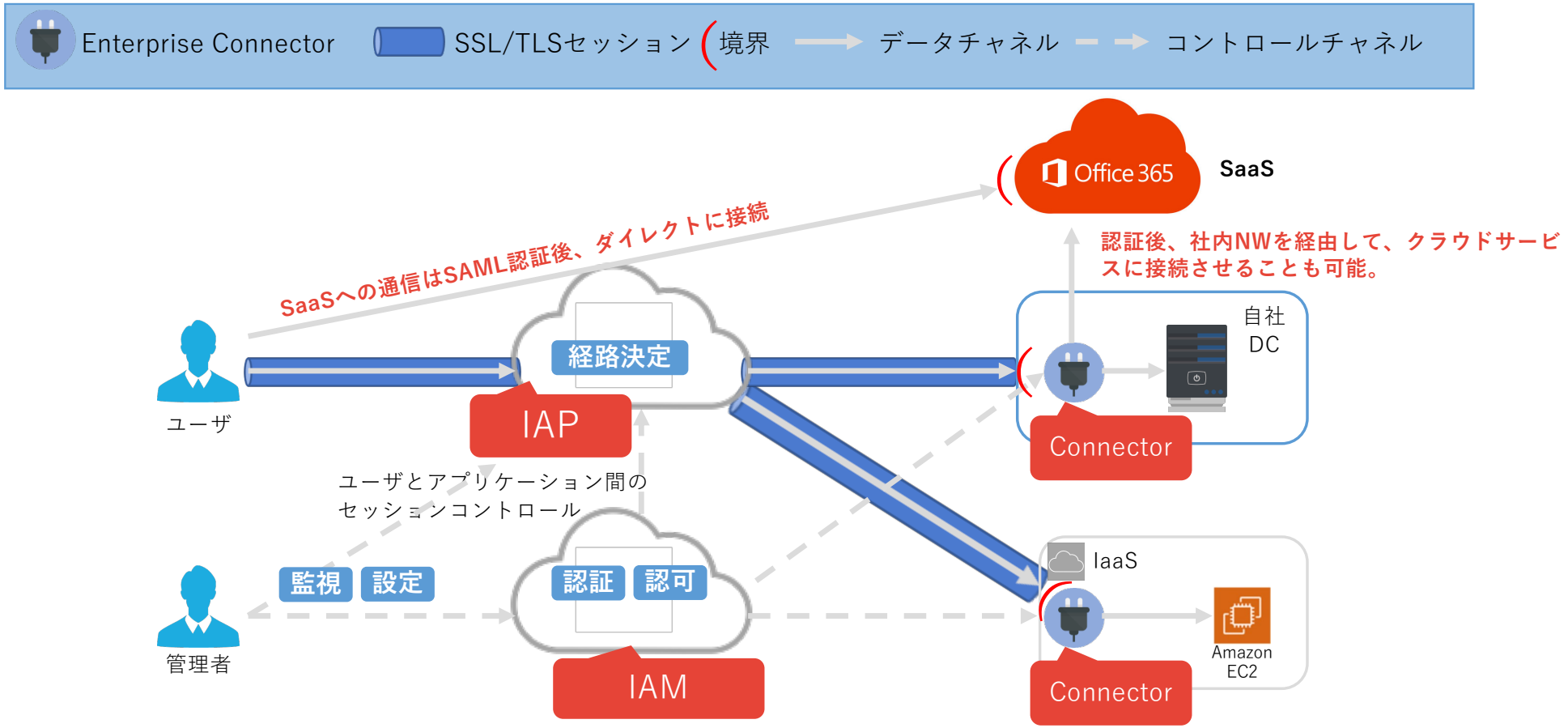


図4：エンクレイブゲートウェイモデル

アクセスを個別に制御する



IAPの機能模式図


Enterprise Connector
SSL/TLSセッション
境界
データチャネル
コントロールチャネル
Office 365
SaaS
SaaSへの通信はSAML認証後、ダイレクトに接続
認証後、社内NWを経由して、クラウドサービスに接続させることも可能。
自社
DC
ユーザ
経路決定
IAP
Connector
ユーザとアプリケーション間の
セッションコントロール
監視
設定
認証
認可
IAM
管理者
IaaS
Amazon
EC2
Connector

境界型防御からZTNへアプローチの第1歩

IAM	IAP
ID&アクセス管理	ID認識型アクセスプロキシ
ユーザーの「認証」やアプリケーションやデータに対するアクセスの「認可」を制御する機能	アプリケーションへのアクセス制御と社内にあるシステムへのコネクターを提供する機能
TrustLogin（GMOグローバルサイン） **Azure Active Directory（米マイクロソフト）** **Cloud Identity（米グーグル）** **OneLogin（米ワンログイン）** **Okta Identity Cloud（米オクタ）**	**Akamai Enterprise Application Access（米アカマイテクノロジーズ）** **Zscaler Private Access（米ゼットスケーラー）** **Azure Active Directory Application Proxy（米マイクロソフト）** **Identiti-Aware Proxy（米グーグル）**

EDR（Endpoint Detection and Response） エンドポイントセキュリティ	トレンドマイクロ：Apex One Endpoint Sencer 米マイクロソフト：Microsoft Defender 米マカフィー：McAfee MVISION EDR
MDM（Mobile Device Management） モバイルデバイス管理	加ブラックベリー：Enterprise Mobility Suite 米マイクロソフト：Microsoft Intune 米モバイルアイアン：MobileIron
SEIM（Security Information and Event Management） セキュリティ情報イベント管理	インフォサイエンス：Logstorage-X/SEIM 米マイクロソフト：Azure Sentinel 米マカフィー：McAfee Enterprise Security Manager
CASB（Cloud Access Security Broker） クラウドアクセスセキュリティブローカー	米シスコシステムズ：Cisco Cloudlock 米マイクロソフト：Microsoft Cloud App Security 米マカフィー：McAfee MVISION Cloud
SWG（Secure Web Gateway） セキュアWebゲートウェイ	グローバルセキュリティエキスパート ：i-FILTER@Cloud トレンドマイクロ：TrendMicro WebSecurity 米マカフィー：McAfee Web Protection

ZTAの導入ステップ（例）

Step1
- ID基盤整備
- IAMなどを導入してSSOや厳密なアクセス管理を実現

Step2
- デバイス保護
- MDM/MAM/EDRなどの導入でデバイスのセキュリティ保護

Step3
- 脱VPN
- IAPによるアクセスプロキシ構成の構築

Step4
- 社内回線網の刷新
- 専用線、IP-VPNの廃止

Step5
- 監視分析
- CASB/SEIMによるSaas/アプリの監視分析

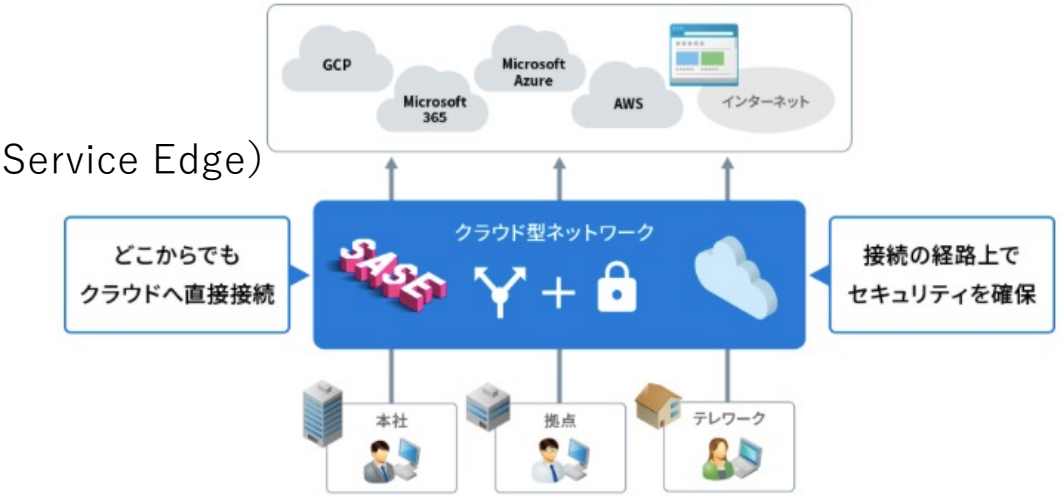
ZTAアプローチのバリエーション

1. 拡張されたアイデンティティガバナンスを利用したZTA
2. マイクロセグメンテーションを利用したZTA
3. ネットワークインフラとSDPを利用したZTA

出典：
NIST「SP800-207：Zero Trust Architecture(ZTA)」
IPAゼロトラスト導入指南書（2021年6月）

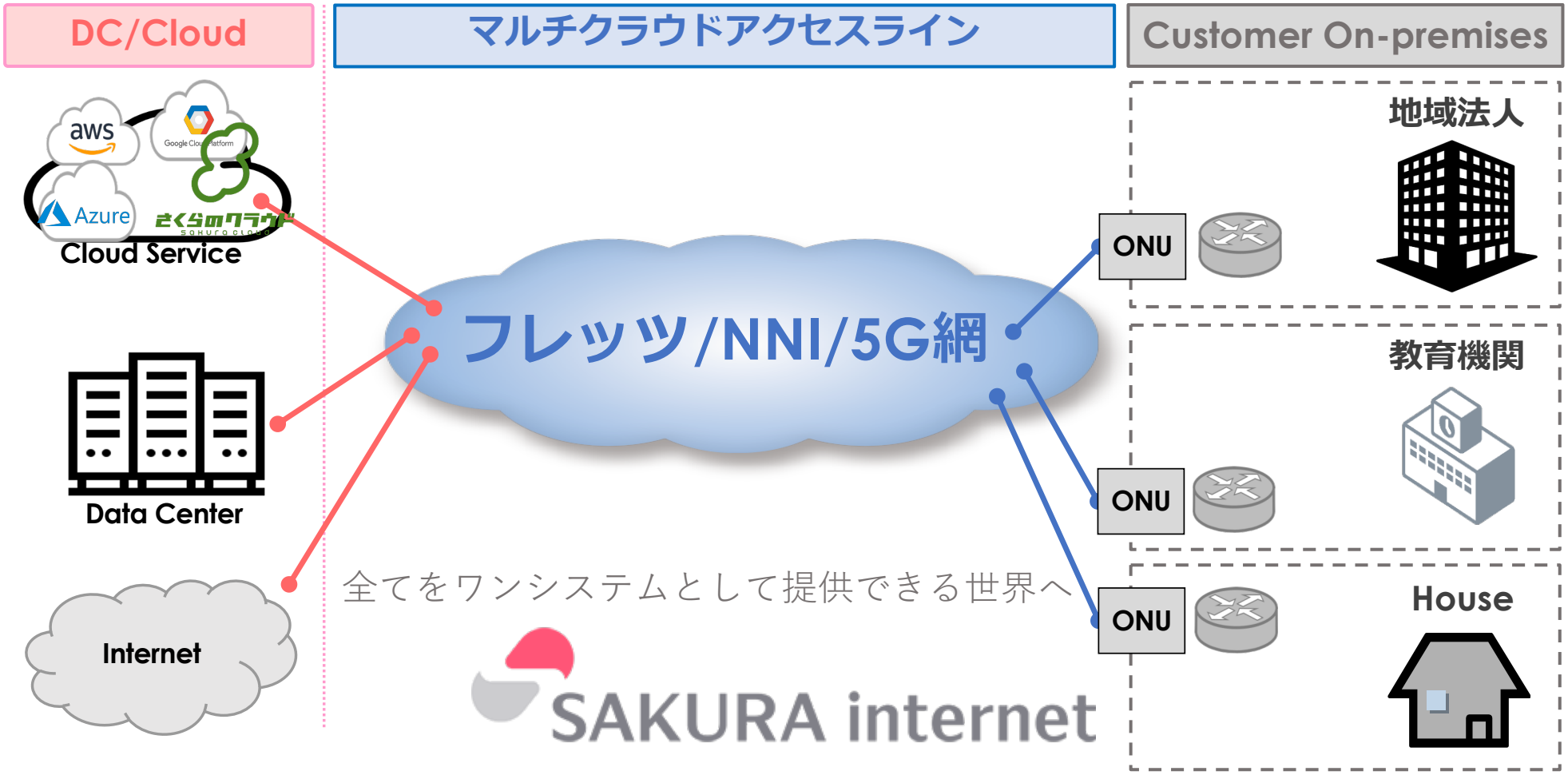
ゼロトラストアーキテクチャ on SD-WAN

SASE（Secure Access Service Edge）



出典：IIJ-WEB
https://www.iij.ad.jp/svcsol/campaign/sase_202010.html?g=KWsase01e&gclid=EAIaIQobChMI9f3zx-3k9AIVoNxMAh0i7wo5EAAYASAAEgJ9TvD_BwE

最後にCMです：さくらインターネットのマルチ構想



ご静聴ありがとうございました。

お問い合わせはこちらからお願いします。

https://saasbank.jp/inquiry/

NEXT systems Inc.