Cloud Native Infrastructure 構築を実現するアカマイEAA

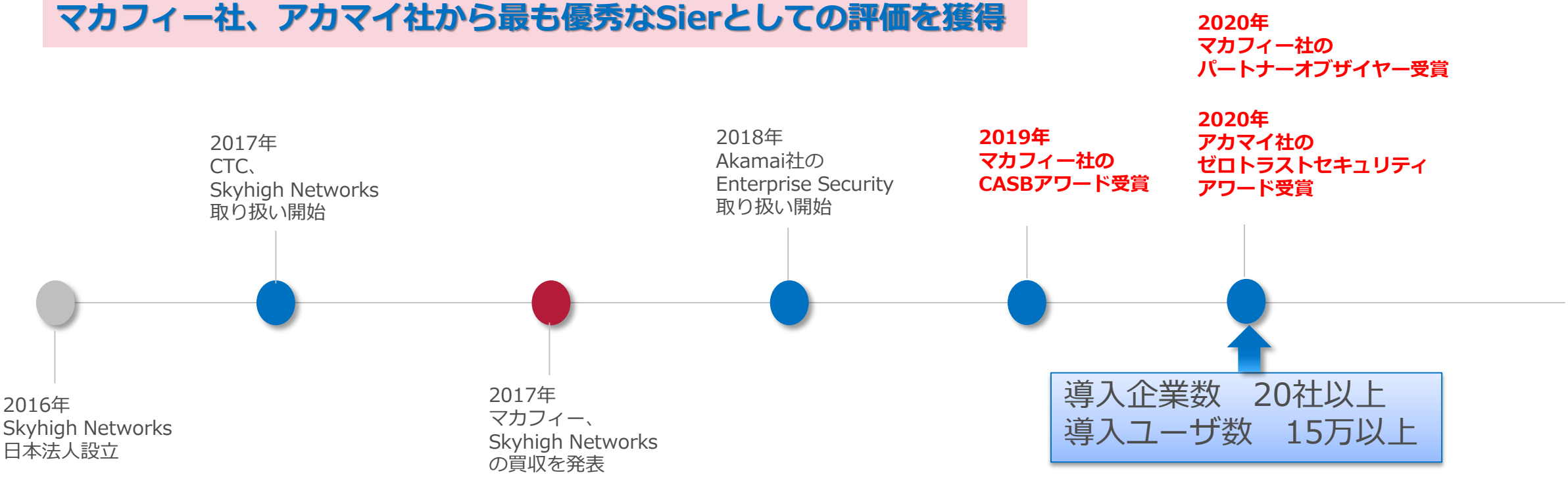
2020/10/22

ITサービス事業グループ
DXビジネス技術部

伊藤忠テクノソリューションズ株式会社

クラウドセキュリティ・領域におけるCTC

CASB、ゼロトラスト領域で業界リーダの
マカフィー社、アカマイ社から最も優秀なSierとしての評価を獲得



CASB

Cloud Base Remote Access

Cloud Base ATP

Cloud Proxy

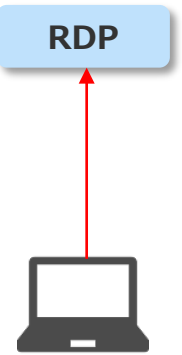
CASBから始まりクラウドセキュリティ
を構成する周辺ソリューション群も
導入実績を積み重ねてきました。

COVID-19による問い合わせの推移

2020年4月末~5月末

■外部要因
・日本国内で緊急事態宣言が発令

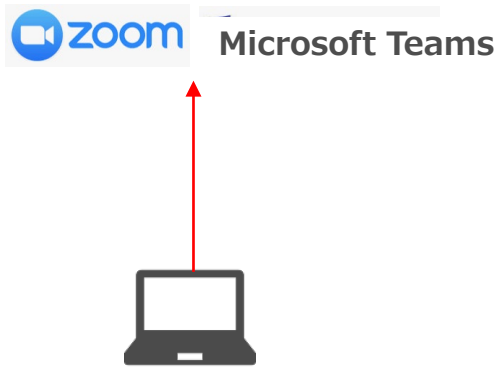
■ITトピック
・VPNによるリモートアクセスが逼迫。
・急遽リモートアクセス環境を整備。
・社用PCを自宅に持ち帰り、RDP接続を急遽実施する等の対応が急増。



2020年6月~現在

■外部要因
・緊急事態宣言解除。Withコロナを見据えた働き方改革
・テレワーク化の混乱に乗じたサイバー攻撃の増加

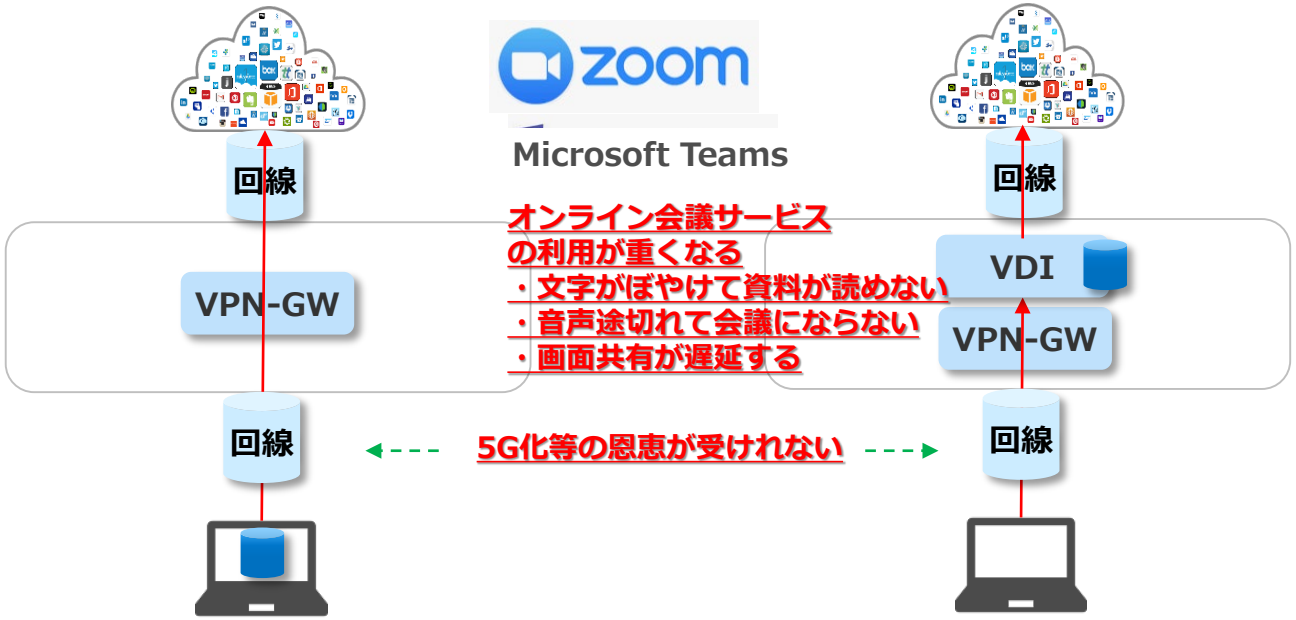
■ITトピック
・テレワーク化の定着を見据えたクラウドネイティブなインフラ構築相談の増加
・サイバー攻撃対策視点での問い合わせ増加
・オンライン会議に対応可能なインフラデザイン



COVID-19対応によって変化する通信要件

COVID-19感染拡大によって、オンラインビデオ会議が必須に。RDPやVDIでは品質面が課題に。

社内引き込み方式



メリット
- **IPによるアクセス制限が可能**

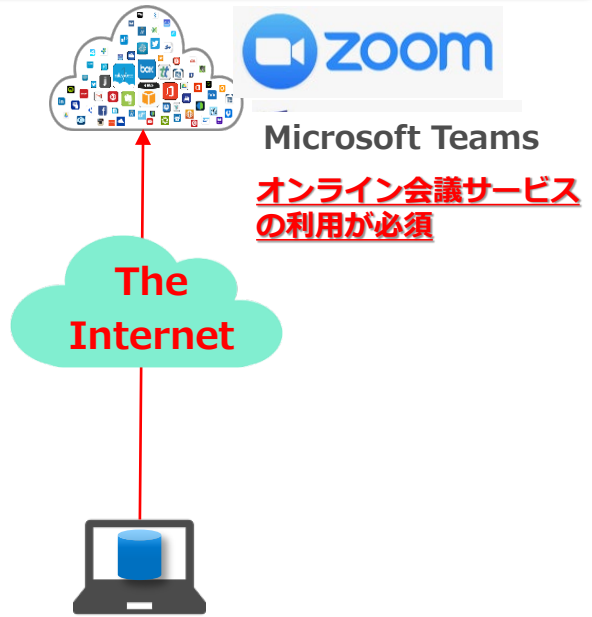
デメリット
- 回線契約がボトルネックになる
- ビデオ会議等で映像や音声が乱れやすい
- アクセス回線高速化の恩恵を受けれない

VDI方式

メリット
- IPによるアクセス制限が可能
- **端末にデータが保存されない**

デメリット
- 回線契約がボトルネックになる
- **SaaSが全体的に重くなる(生産性低下)**
- アクセス回線高速化の恩恵を受けれない

ダイレクトアクセス方式



メリット
- **最も低遅延で生産性向上に繋がる**
- アクセス回線高速化の恩恵を享受可能
- クラウド利用に最適な方式

デメリット
- **端末へのデータ保護施策が別途必要**

※ストレージ暗号化、IRM等

CTCが考えるクラウドを安全に活用する
Cloud Native Infrastructure

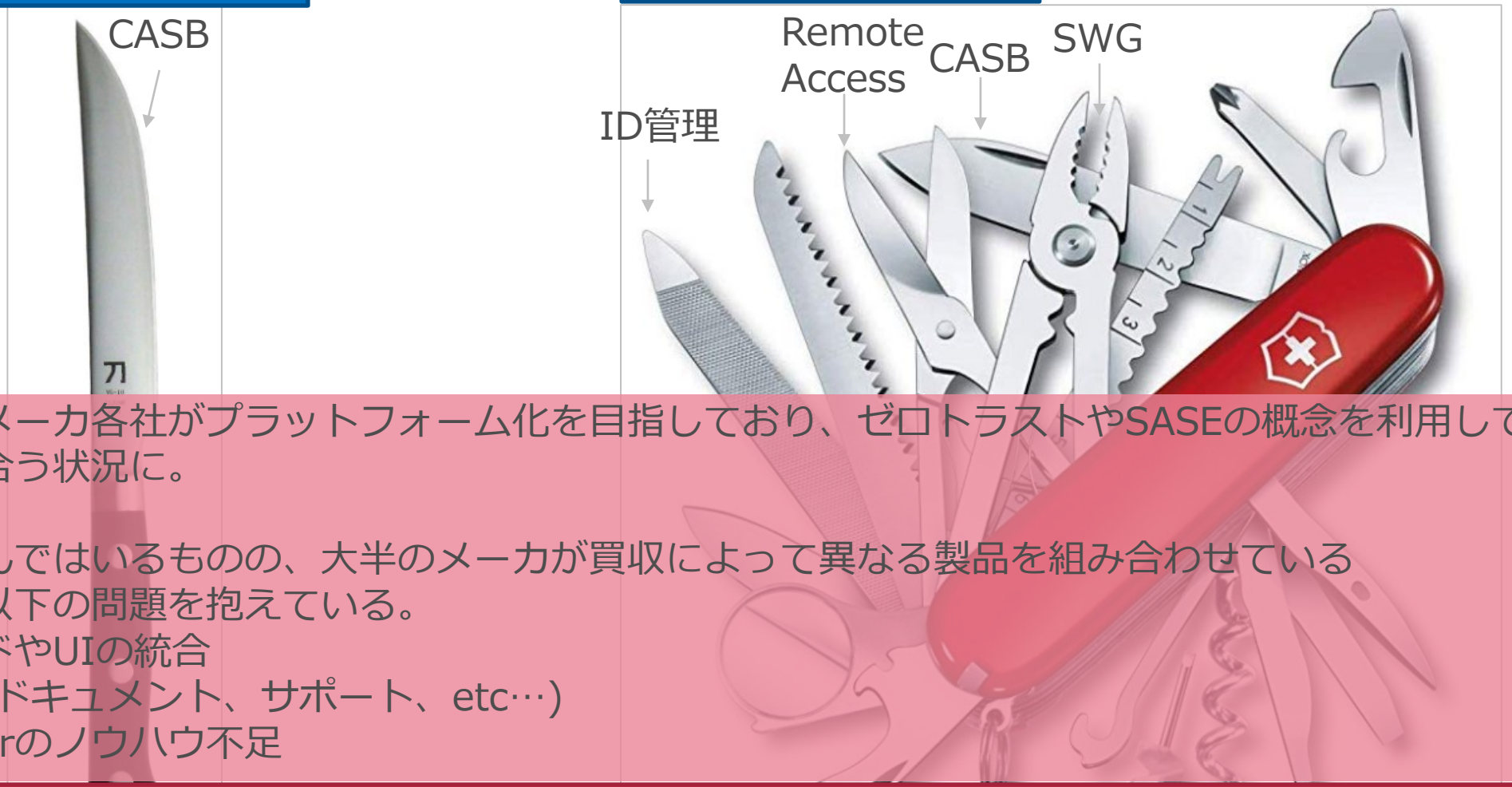
ステーキを食べる時にどちらのナイフを使いますか?

現状:十徳ナイフ化するセキュリティソリューション

専用ソリューション

多機能ソリューション

一言で言えば「十徳ナイフ」



セキュリティメーカ各社がプラットフォーム化を目指しており、ゼロトラストやSASEの概念を利用して多機能化を競い合う状況に。

多機能化が進んではいるものの、大半のメーカが買収によって異なる製品を組み合わせている状況であり、以下の問題を抱えている。

・バックエンドやUIの統合
・品質(製品、ドキュメント、サポート、etc…)
・メーカやSIerのノウハウ不足

買って貰うために「多機能化」は進むが、買って貰ったあとの「対応」は十分ではない。
目的の無い機能表による比較は× -> 十徳ナイフを買うパターン
何の脅威に対する対策かを明確にした上で比較するのが〇 -> 適切な道具を選べる

混乱の原因の1つであるゼロトラスト、SASEに関する見解

外部脅威への対応

サイバー攻撃に関するトレンド
・レガシー型境界防御の陳腐化
・ラテラルムーブメントの脅威
・標的型攻撃が高度化

・認証、認可を強化するゼロトラストが注目される。

内部脅威への対応

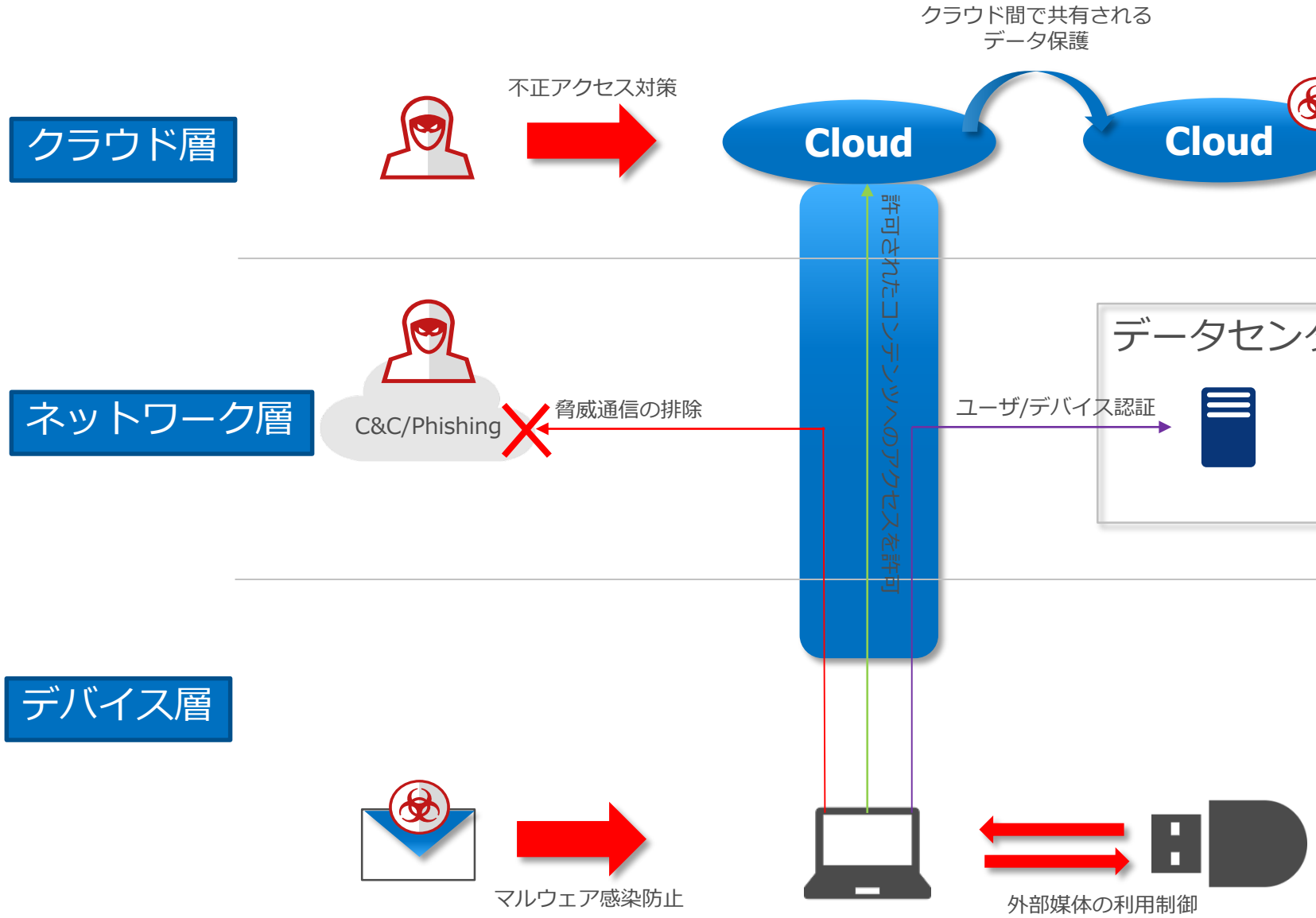
内部不正対策に関するトレンド
・シャドーITの蔓延
・在宅勤務者に対するセキュリティの考慮
・オンラインビデオ会議の急速な普及

・クラウドにも対応可能な機密情報や従業員の行動に関する制御を可能にするSASE。

ゼロトラスト、SASEどちらが優れているという議論ではなく、概念を適材適所に取り込むことが重要。

CTCの考えるクラウドセキュリティの考え方　三階層に分類

デバイスからクラウドに到達するまでを三階層に
分けて、保護する資産、リスク、技術を整理します。



クラウド層のセキュリティの主な役割

クラウド上で生成、共有されるデータの保護や
クラウドに対する攻撃、設定ミスから保護します。
・クラウド上で生成されるデータの保護
・クラウド上に仕掛けられる不正アクセス
・クラウド間で共有されるデータの保護
・クラウドの設定監査

ネットワーク層セキュリティの主な役割

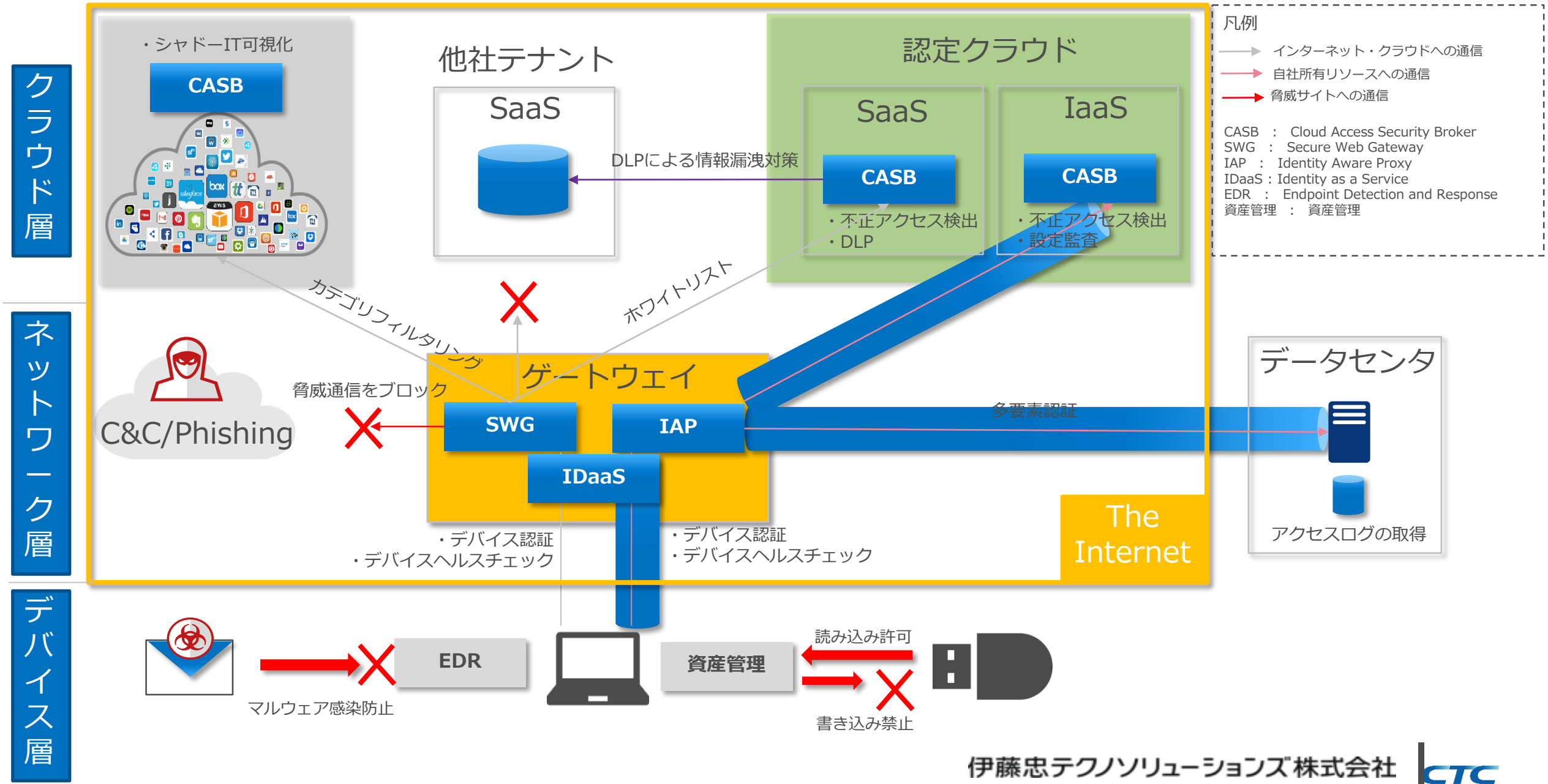
デバイスから、クラウド上のリソースに対して
安全なアクセス手段を提供し、通信を保護します。
・稼働率に関する高いSLA
　※システム停止時は業務に多大な影響を与える
・コンテンツへのアクセス制限
・各リソースへの認証の一元管理
・各リソースに対するアクセスログの取得
・通信経路の暗号化
・脅威通信の排除

デバイス層セキュリティの主な役割

デバイス上で生成、保存されるデータの保護や
外部媒体へのデータ流出、端末の紛失、盗難対策
といったリスクから保護します。
・マルウェアの感染防止
・外部媒体の利用制御
・端末紛失対策

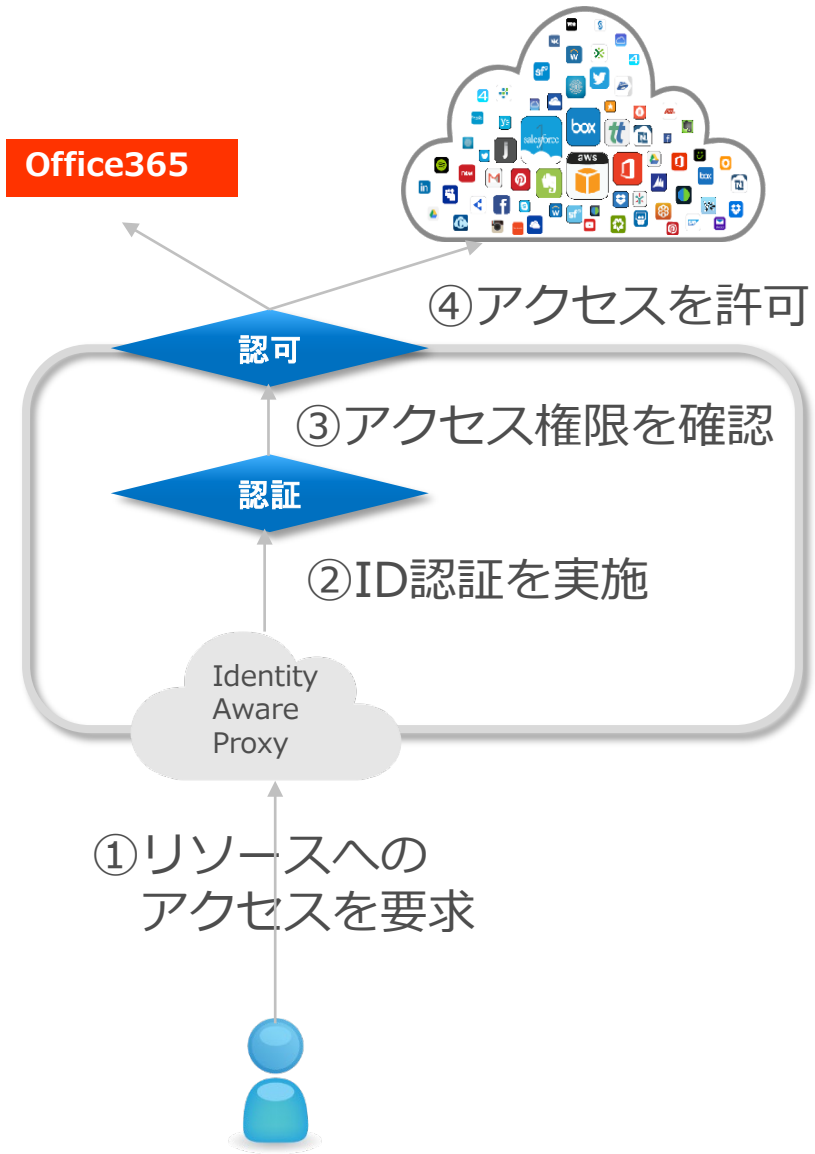
伊藤忠テクノソリューションズ株式会社

各階層毎に考慮すべき脅威と保護機能をマッピング。
Cloud Native Infrastructureを構築。



伊藤忠テクノソリューションズ株式会社

IAP：Identity Aware Proxy



クラウド上にユーザとリソースの間に認証レイヤを設けて、ユーザIDの一元的な認証や、デバイスのチェック等を担う。

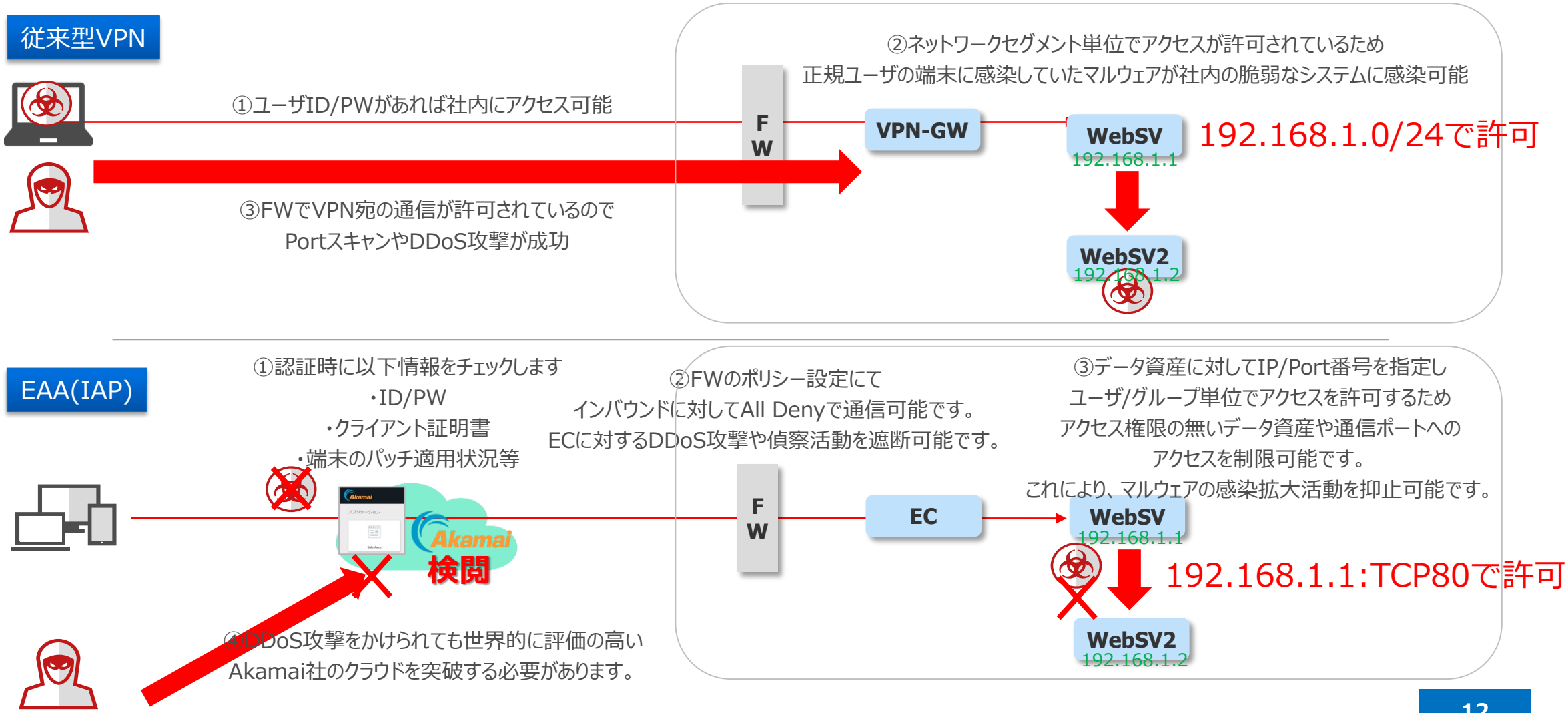
■なぜ、必要か?
クラウドサービス事業者毎に実装している認証レベルが異なる。一般的にスタートアップが提供するリリースされたばかりのクラウドサービスは成熟したサービスと比較して、認証機能が弱かったりする。

こういったクラウドサービス毎の差を埋める必要がある。

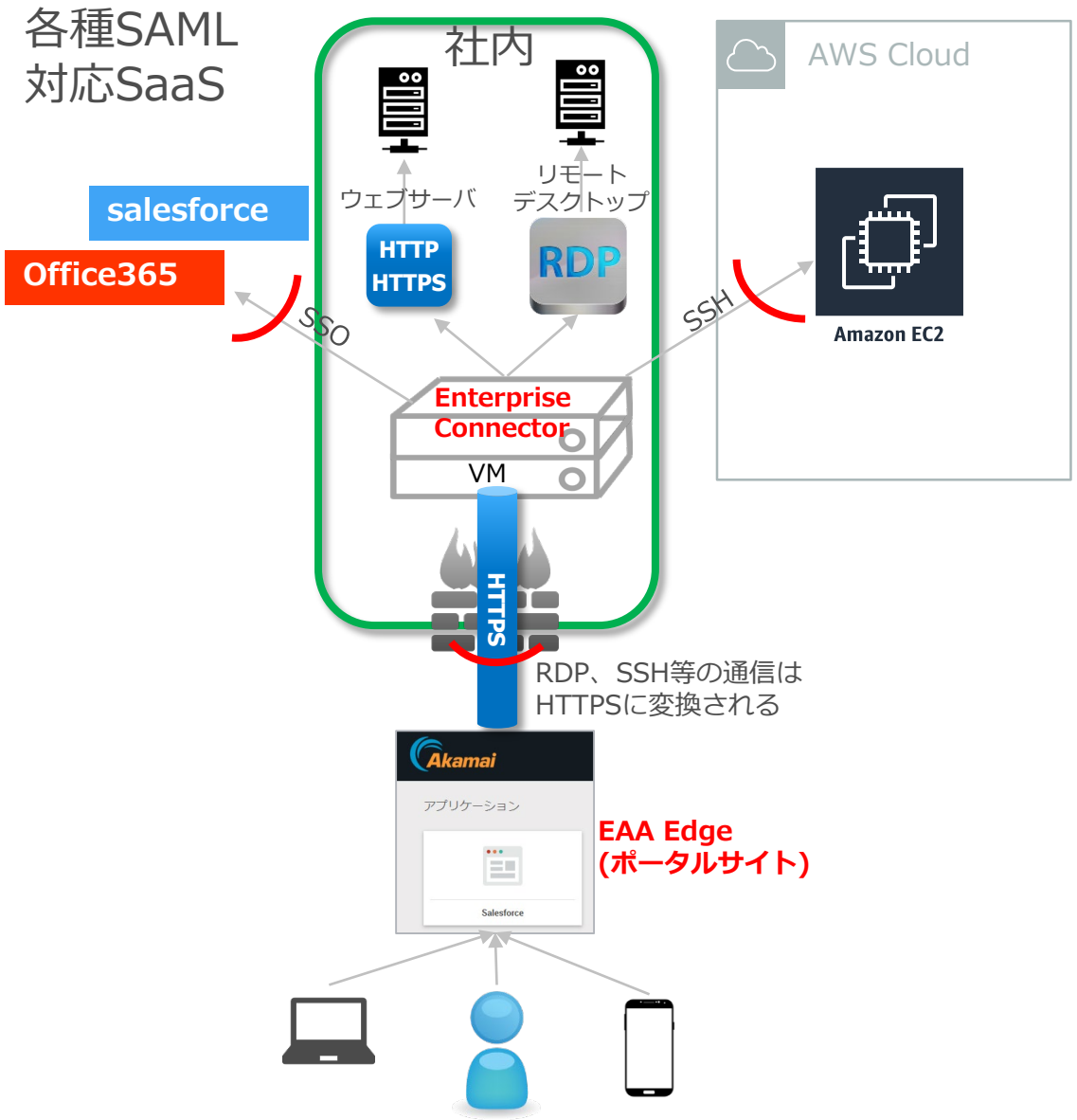
■IAPを導入するメリット
・アクセス先のリソースが高度な認証機能をサポートしていない場合にも、IAPが認証/認可を実施することでセキュリティレベルを維持することが可能になる。

検閲能力を強化するIAP

ゼロトラストモデルに採用される傾向にあるIAPは、ユーザの本人確認だけでなく、マルウェアにとって侵入しずらい状況を作り出します。



ゼロトラストIAP：アカマイEAA



■**概要**

クラウド時代に必要とされる下記三点のリソースに

1　社内リソース(従来のリモートアクセス)
2　IaaS上のリソース
3　SaaS

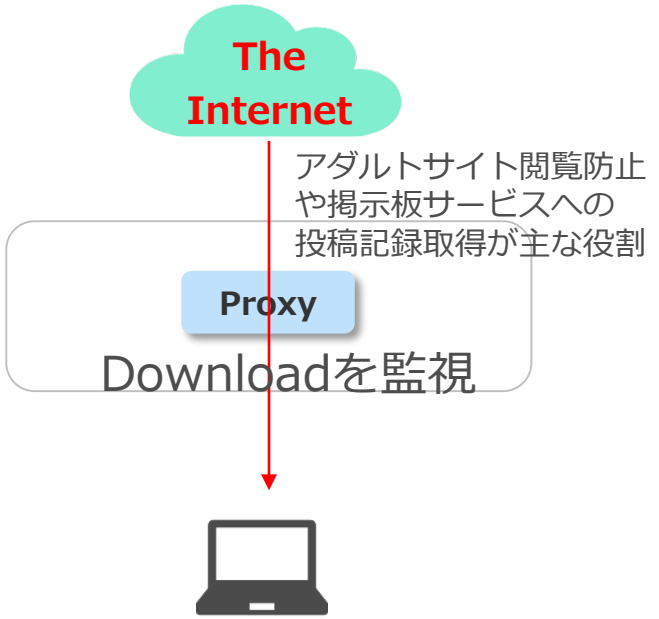
■**メリット**

・社内システム/クラウドサービスのアクセスを一元管理
・”**境界**”をソフトウェアで柔軟に定義可能
・攻撃者から、各リソースを隠蔽可能
・ウェブブラウザのみでリモートアクセス機能を提供可能
  - VPNクライアント等が配布不要
・EAAにてID認証機能を強化
  - MFAの適用
  - IPアドレス制限、地域によるアクセス制御
・FWの穴あけ不要
  FW運用コスト削減、セキュリティ向上

SWG:プロキシソリューションの役割の変化

2000~2012年

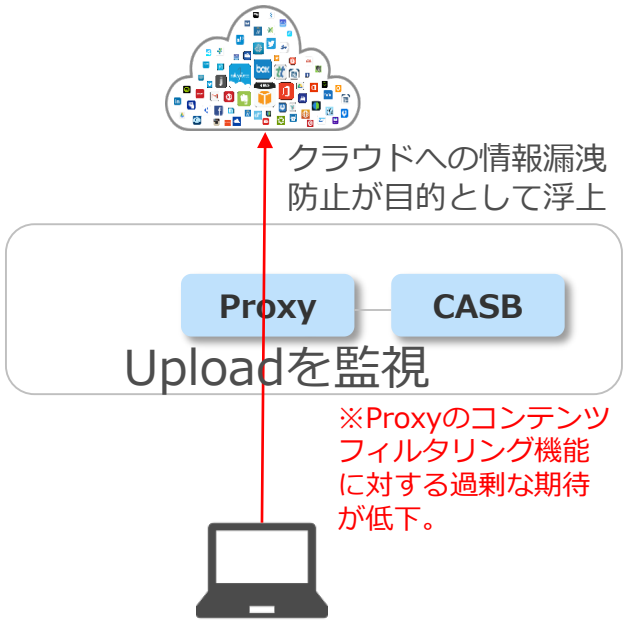
有害コンテンツの閲覧禁止



■プロキシの役割
・有害コンテンツの閲覧禁止
・アクセスログの取得

2012~2018年

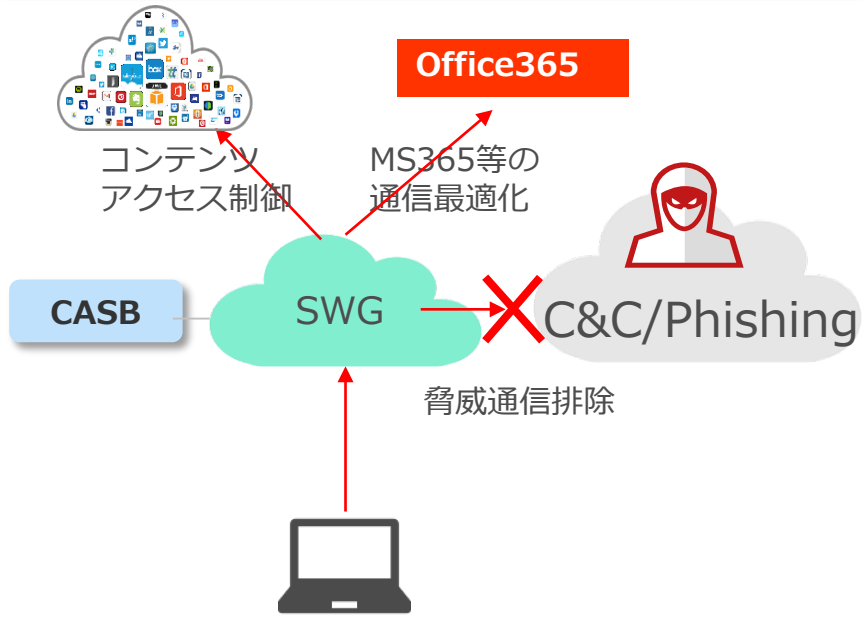
クラウドへの情報漏洩対策



■CASBの登場
・クラウドが市場に普及
・クラウド普及に伴い、有害コンテンツ閲覧を目的としたProxyのURLフィルタリングでは、クラウドサービスの多くが制御不能となりシャドーITが蔓延。
・クラウドサービスへの情報漏洩防止

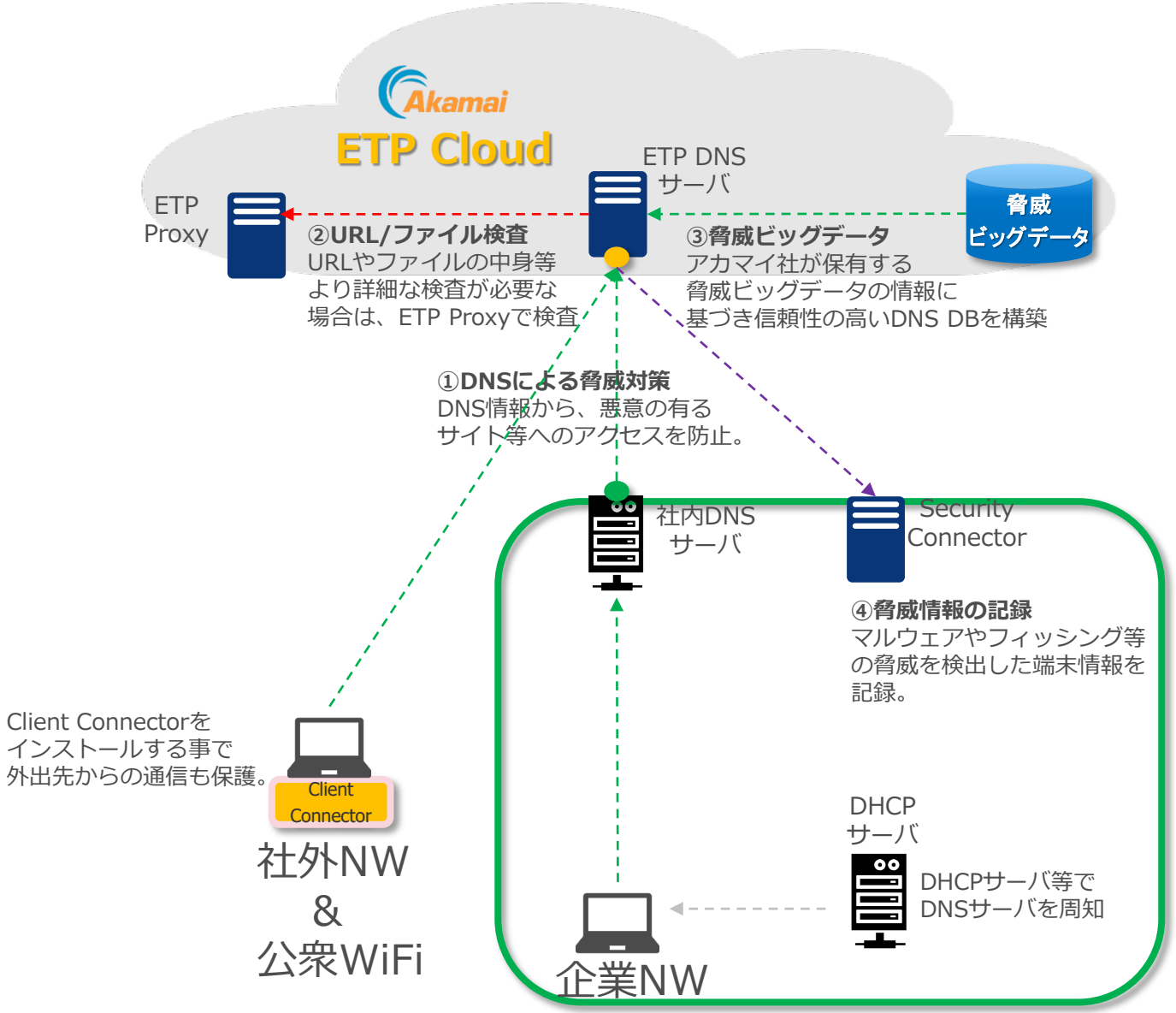
2018~2020年

クラウド最適化&脅威通信の排除



■SWG採用増加の背景
1.エンタープライズクラウド導入に伴いHTTPS通信が急増。オンプレミスプロキシの処理能力が限界に到達。
2.在宅勤務者に対する有害コンテンツ閲覧禁止。
3.C&Cサーバ等への通信を防止

ゼロトラストSWG：アカマイETP



■ETPの三つの特徴

1.1日2.2兆、全世界のDNSクエリの約50%を処理するアカマイの脅威ビックデータに基づく高検出力

2.マルウェア対策アプリケーションのインストールが困難な、プリンタやIoTデバイスもDNSさえ参照出来れば保護対象に。

3.MS365最適化機能有り。
MS365のレスポンス改善や、URL更新に自動的に対応します。

Cloud Native Infrastructureアセスメントサービス

Cloud Native Infrastructureアセスメントサービス

これまでの提案経験に基づき、簡単なヒアリングシートに記載頂く事で、現在のセキュリティ状況や欠けている箇所の可視化を行います。

目標	1.現状インフラのセキュリティ対策状況の可視化 2.クラウドシフトを見据えた、あるべき姿のセキュリティベースラインイメージの確立
サービス概要	1.現状評価 NISTの定義するゼロトラスト アーキテクチャ (SP800-207)、SASE、CTCでのクラウドセキュリティ導入経験に基づき、貴社の現状を可視化 2.ギャップ分析 現状評価 + お客様要件を加味し、ギャップを可視化。レーティングの実施および課題を明確化
納品物	・アセスメント結果報告書

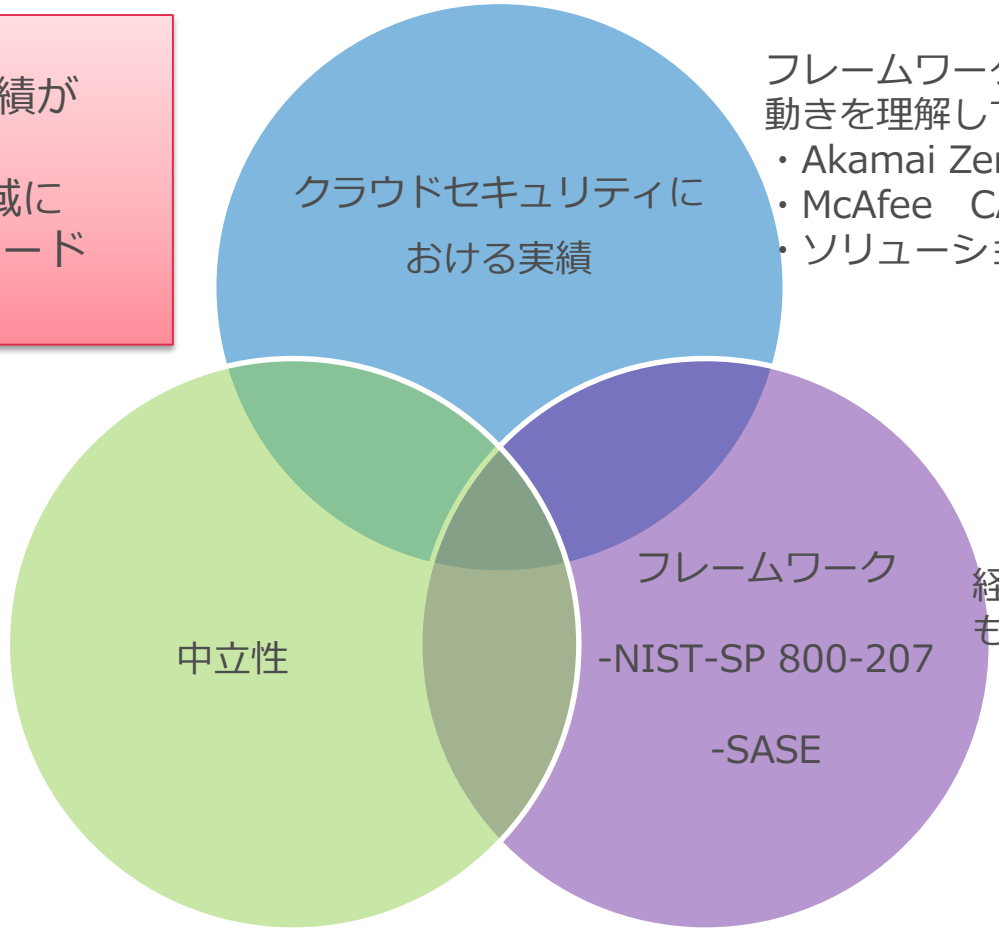
こんなお客様におススメ!

・現状把握したいが、コンサルファームに依頼するほどの費用と時間はかけられない
・メーカー提供のアセスメントサービスではメーカ縛りとなり不安

伊藤忠テクノソリューションズ株式会社

なぜ、CTCからアセスメントを受けるのか?

Cloud Nativeなインフラ構築には
CASBやZeroTrustに関する技術の実績が
不可欠です。
CTCではクラウドセキュリティの領域に
おいて2017年から取り組み各種アワード
も受賞した実績があります。



フレームワークの理解だけではなく、実機の
動きを理解してアセスメントが可能です。
・Akamai Zerotrust パートナアワード受賞
・McAfee　CASB パートナアワード受賞
・ソリューション導入実績30社以上

メーカーでは無い強みを活かして
メーカ単独の視点ではない中立的な立場
に基づいて、アセスメントを実施可能。

経験だけでなく、フレームワークの内容
も加味した上でアセスメントを実施します。

■Akamai EAAに関する問い合わせ先
本資料に関する問い合わせ先は以下にお願い致します。
CTCアカマイ主管部　akamai@ctc-g.co.jp

伊藤忠テクノソリューションズ株式会社