macnica solutions

ゼロトラスト移行を実現する
４つのポイントについて

マクニカソリューションズ株式会社

本資料のアジェンダ

■ゼロトラスト化を実現する「４つのポイント」

■ゼロトラスト化に向けた典型的な「移行ステップ」

■ゼロトラスト化に伴う「運用高度化」のご支援について

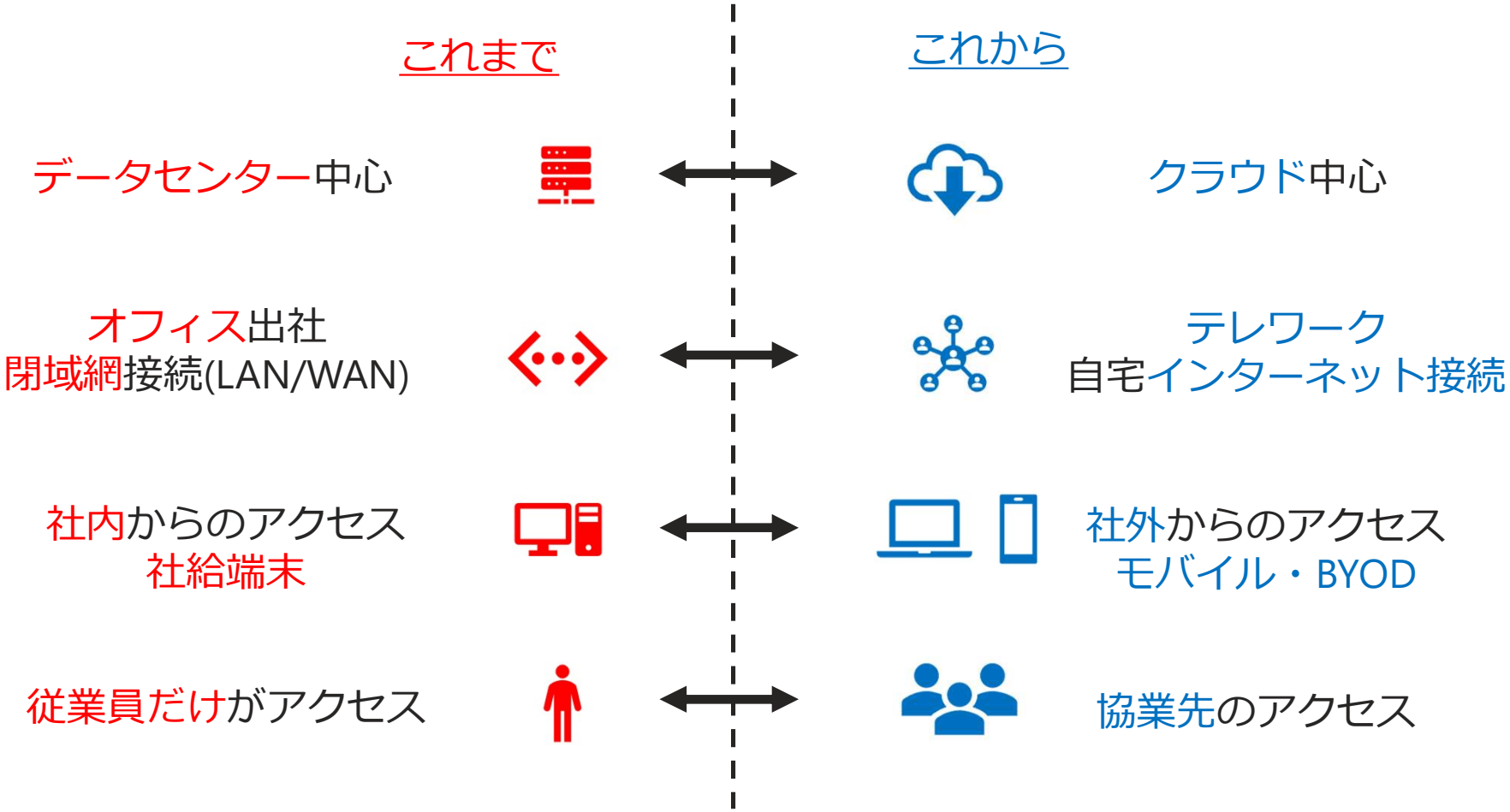
参考：弊社ブログにて検証結果等も公開しております

- https://mnc.macnica.net/zerotrust/
- https://japan.zdnet.com/it-infrastructure/sp_20_zerotrust/

参考：製品間連携を検証したホワイトペーパーも配布中

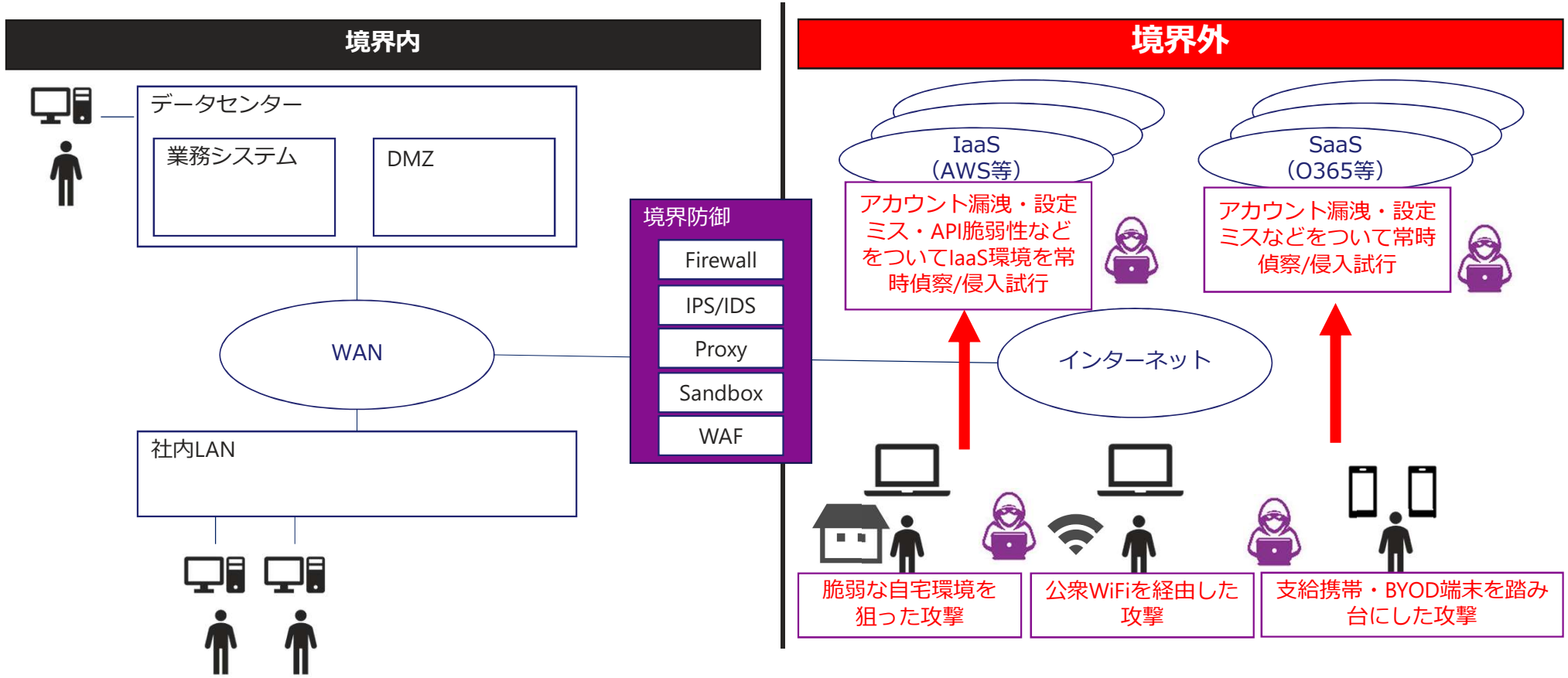
ゼロトラストの「４つのポイント」

クラウド・モバイル・インターネット登場による企業環境の変化



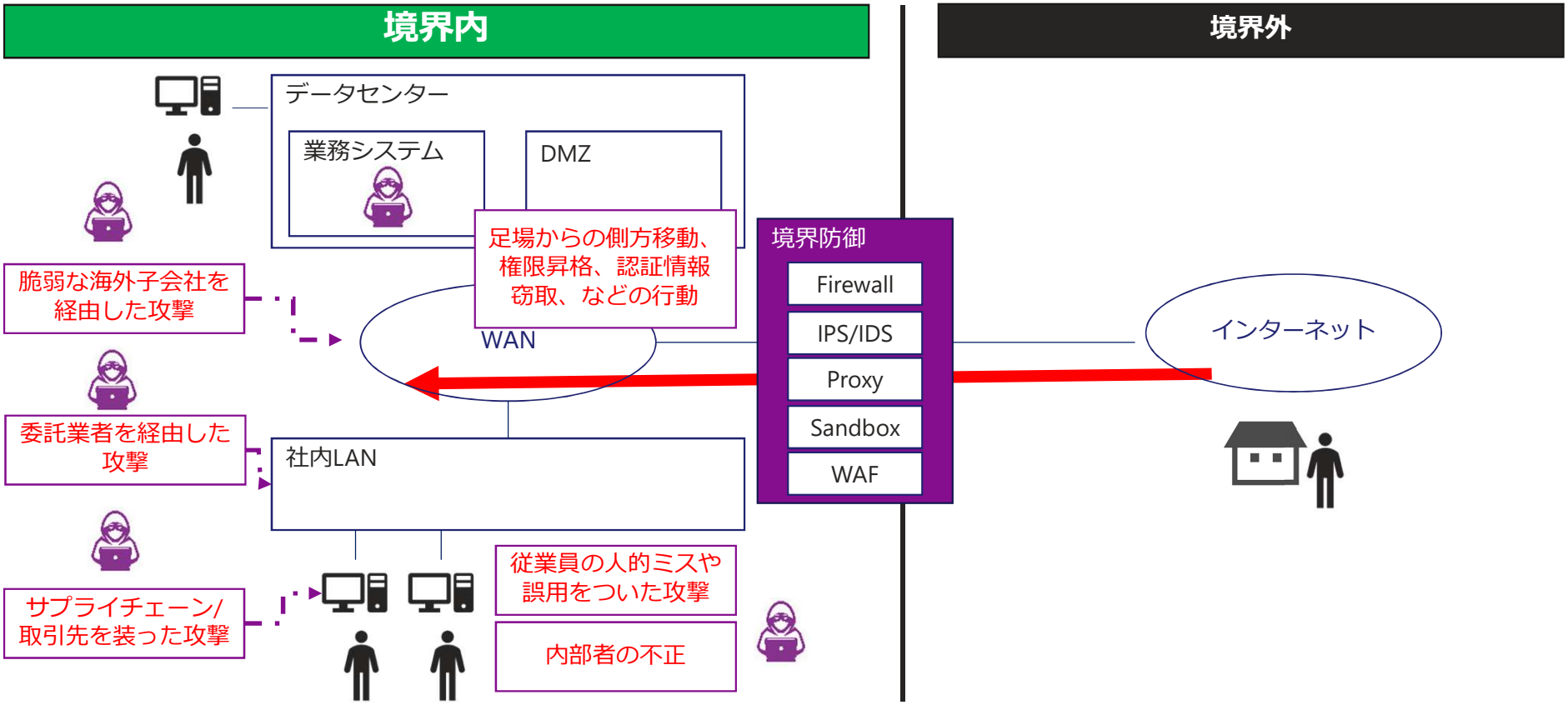
ゼロトラスト時代の環境変化①：境界“外”通信の拡大

- ダイレクトクラウド通信、システムのクラウドシフト、モバイル端末の登場、テレワーク化など
- 企業のデバイス・ユーザー・システムが社外に存在する時代（境界を通らない通信の増大）



ゼロトラスト時代の環境変化②：境界“内”通信への拡大

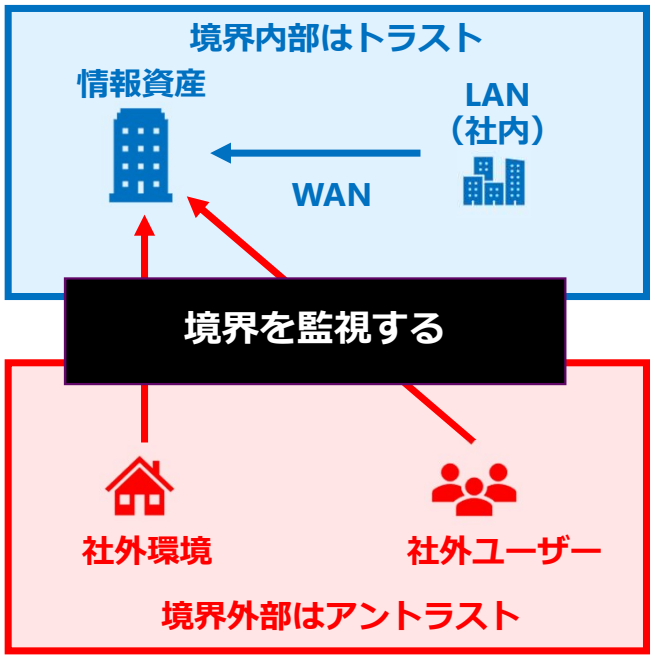
- 攻撃手法の高度化、従業員の内部不正など境界防御やVPNで侵害行為を検出・阻止することは不可能
- 侵入されていることを前提にした境界内の検知・監視が不可欠な時代



「決して信頼せず、必ず確認せよ」（Never Trust, Always Verify）

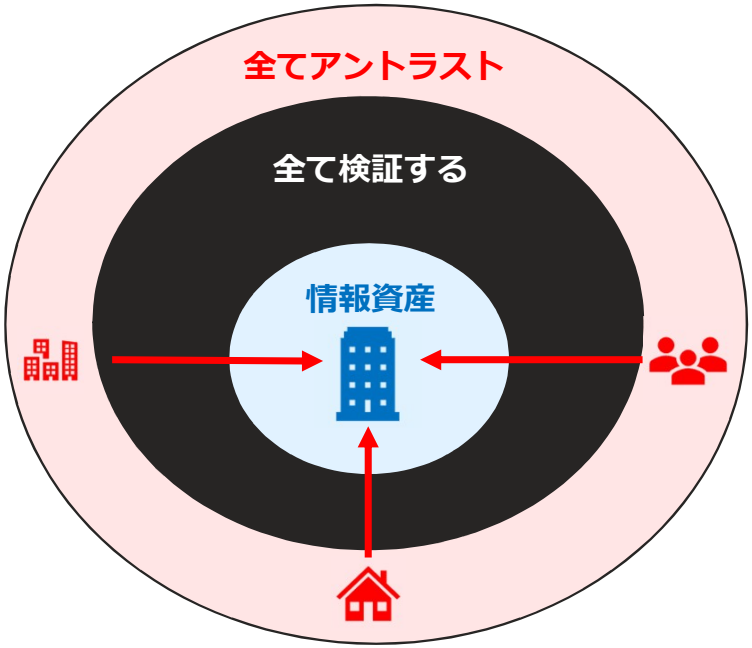
境界防御

社内ネットワークは安全で
社外ネットワークは危険なので
外からの通信のみ検証する



ゼロトラスト

全ての通信を信用せず
常に接続を検証し
最小権限でアクセス許可を与える



ゼロトラストで変わること＝「信頼」の担保の手法

境界防御

- ネットワーク（場所）
- ユーザー（ID）
- デバイス（端末）

- 信頼されたNWからの通信かどうかが重要
- 信頼されたNWからの通信であれば、暗黙的に信頼
- 善も、悪もリソースに特権的にアクセスが可能

ゼロトラスト

- ネットワーク（場所）
- ユーザー（ID）
- デバイス（端末）

- どのネットワークからの通信かは関係ない
- 主にアクセス元のユーザー・デバイスの信頼性で判断
- 信頼性に応じたリソースへの最小権限のアクセス

NISTが提唱する「７つのゼロトラスト原則」

■「NIST SP800-207　Zero Trust Architecture」

- ◆2020年8月11日にNIST（米国標準技術研究所）正式版発行
- ◆米政府がゼロトラストについて言及する際に、政府標準として扱われるべく提言されたもの

■７つのゼロトラスト原則（弊社訳）

1. データソースとコンピュータサービスは、全てリソースとして識別
2. ネットワークの場所に関係なく、通信は全て保護
3. リソースへのアクセスは、セッションごとに許可
4. リソースへのアクセスは動的なポリシーによって決定される
5. 継続的に全てのデバイスの状態を監視・測定
6. アクセスが許可される前に動的かつ厳密に認証・認可
7. 機器・インフラ・通信の状態について可能な限り多くの情報を収集

ゼロトラスト原則を実現する４つの要素

macnica solutions

7つのゼロトラスト原則（NIST）

- ⑥アクセス許可の前に認証・認可
- ⑤全てのデバイスの安全性の監視・測定
- ②あらゆる通信は全て保護される
- ③セッションごとに都度アクセス許可
- ①全てをリソースとして識別する
- ⑦NWインフラ・通信の最新状態の収集
- ④ID等の状態に基づいた動的なポリシー決定

実現するための4要素

- ①認証・認可の実現
- ②デバイスの安全性の監視
- ③ゼロトラストなアクセス許可
- ④ゼロトラスト時代の運用変革（可視化・解析・自動化）

ゼロトラストを実現する４つのポイント

	境界防御		ゼロトラスト
①認証・認可の実現	ネットワーク に基づいた認証・認可	→	デバイス・ユーザー に基づいた認証・認可
②デバイスの安全性の監視	静的な情報（証明書） に基づいて信用	→	動的な状態（脅威・振る舞い） に基づいて信用
③ゼロトラストなアクセス許可	社内の通信は安全 社外からの通信は危険	→	社内・社外の経路を問わない 最小権限のアクセス許可
④ゼロトラスト時代の運用変革（可視化・解析・自動化）	境界を越える通信の 外部脅威のみチェック	→	内部・外部の脅威検知も含めた 可視化・対応の自動化

4つのポイントを実現する各種ソリューション

macnica solutions

デバイス・ユーザー
に基づいた認証・認可

動的な状態（脅威・振る舞い）
に基づいて信用

社内・社外の経路を問わない
最小権限のアクセス許可

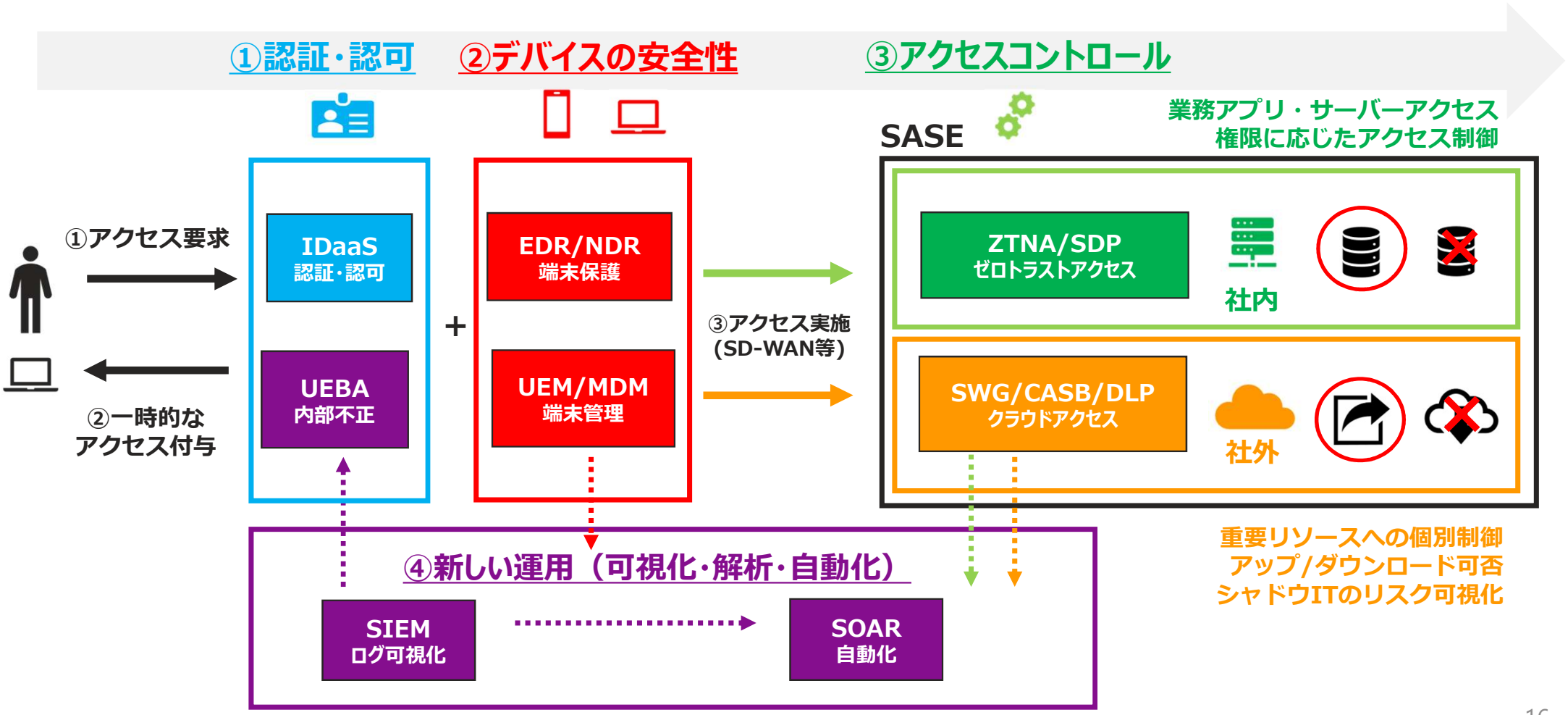
内部・外部の脅威検知も含めた
可視化・対応の自動化

①認証・認可の実現	IDaaS
②デバイスの安全性の監視	NDR EDR EMM
③ゼロトラストなアクセス許可	SASE クラウドセキュリティ（SWG/CASB） ゼロトラストアクセス（ZTNA/SD-WAN）
④ゼロトラスト時代の運用（可視化・解析・自動化）	SIEM UEBA SOAR

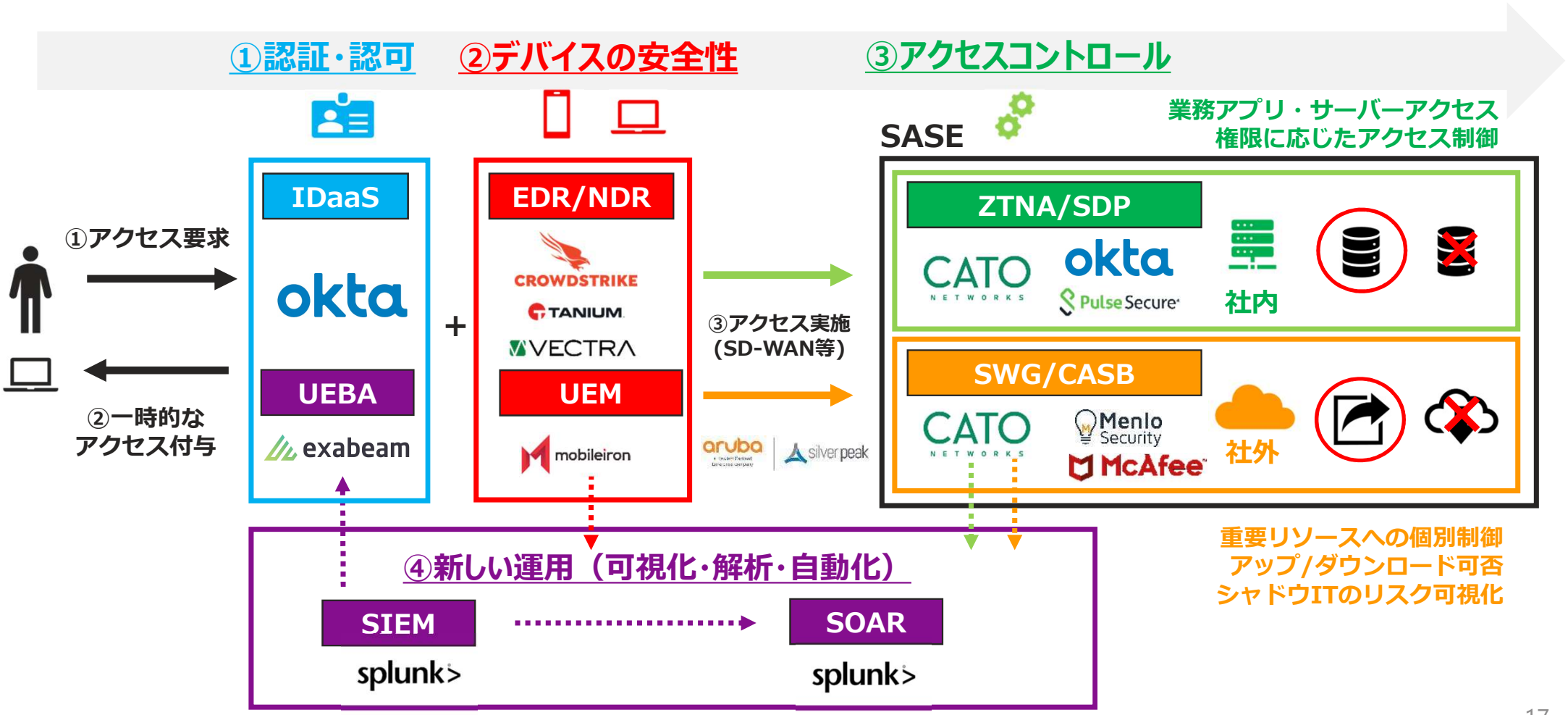
マクニカ取り扱いの製品・ソリューション一覧

カテゴリー	ソリューション		ソリューション概要	マクニカ取り扱い	
①認証・認可	IDaaS		統合ID基盤	Okta	
②デバイスの安全性	EDR		エンドポイント脅威検知	CrowdStrike/Tanium	
	UEM		エンドポイント管理	MobileIron	
	NDR		内部脅威検知	Vectra/Gigamon	
③アクセス コントロール	SASE	クラウドセキュリティ	SWG/RBI/CASB/DLPなど	Cato	McAfee/Menlo
		SD-WAN	社“内”拠点→社内システム		Aruba/Silver Peak
		ZTNA/SDP	社“外”端末→社内システム		PulseSecure/Menlo
④ゼロトラスト運用	SIEM		通信ログの横断的な解析	Splunk/Exabeam	
	UEBA		ログのユーザー毎のAI解析		
	SOAR		セキュリティ連携		

ゼロトラストを実現する全体構成

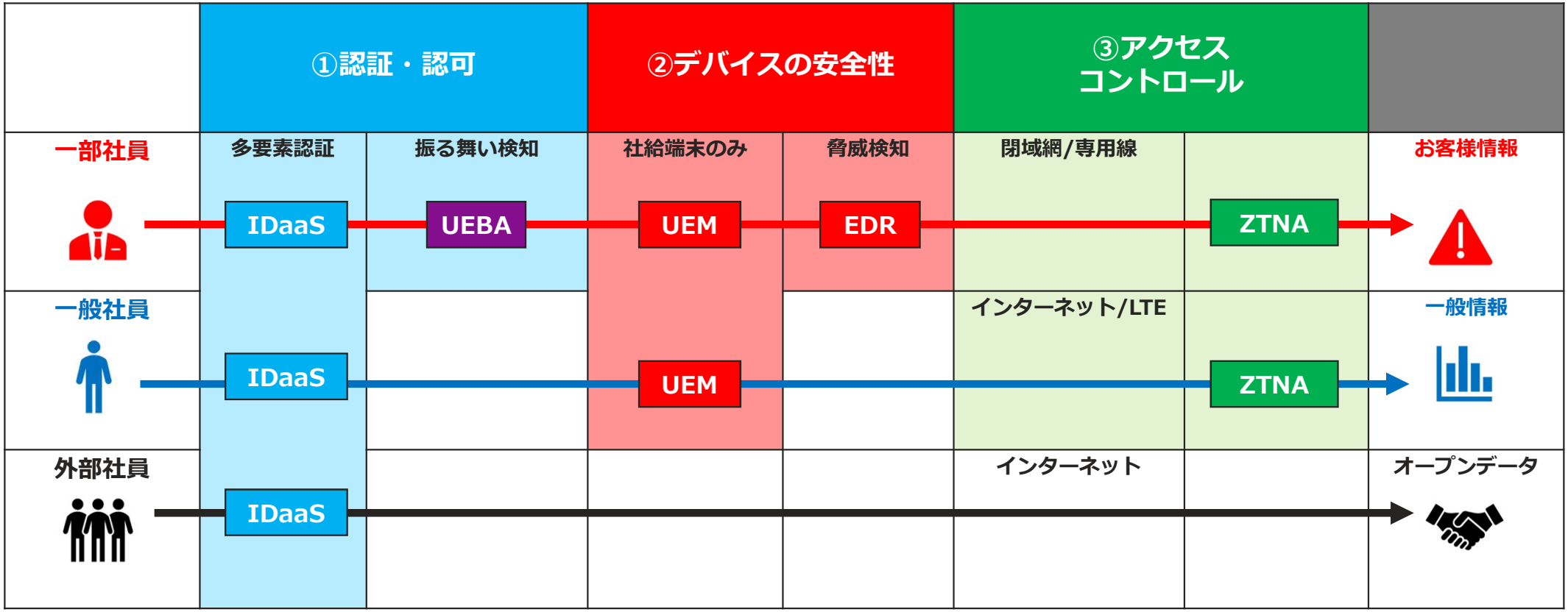


マクニカ取り扱いの製品・ソリューション一覧

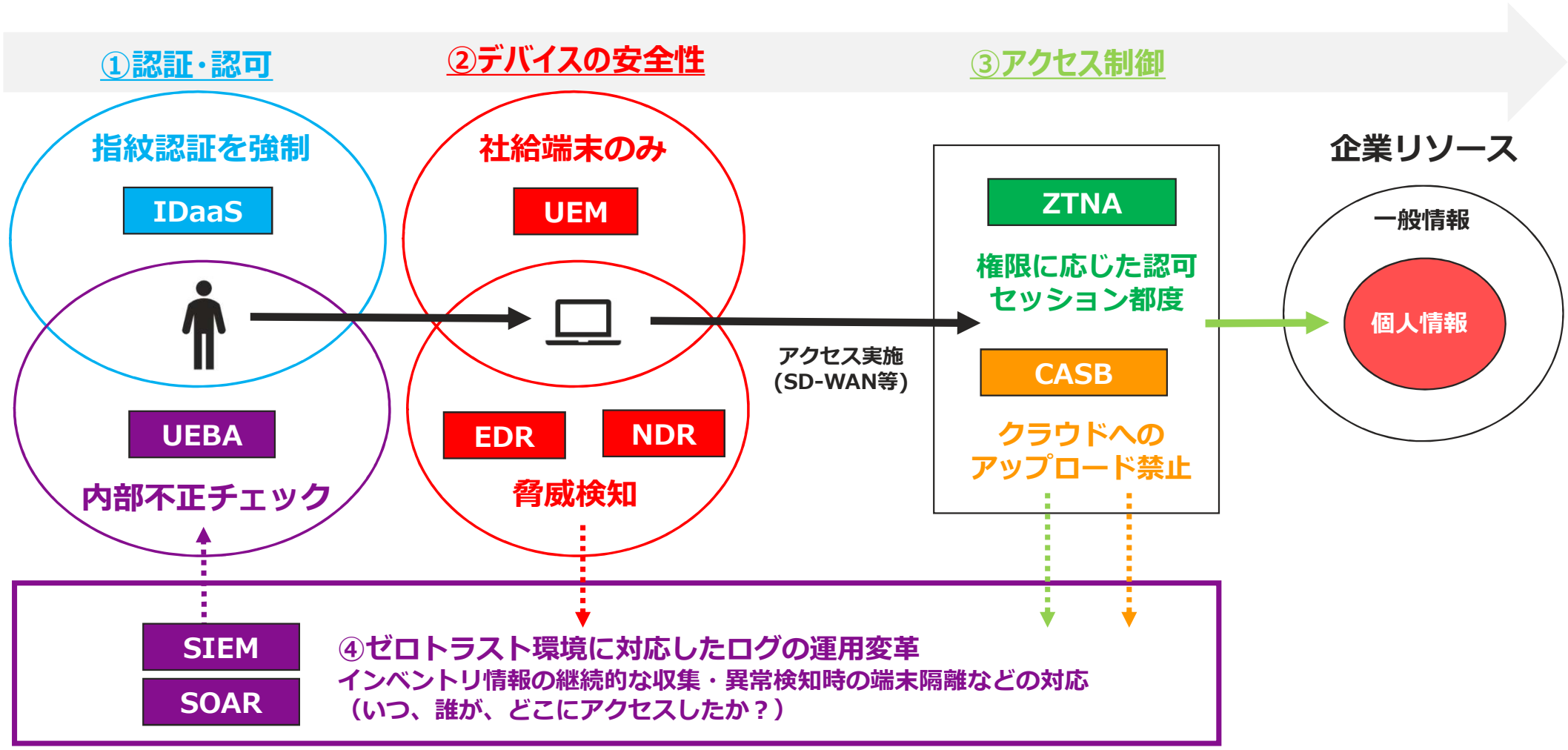


ユーザー・デバイスの状態に基づいた条件付きアクセスの実現

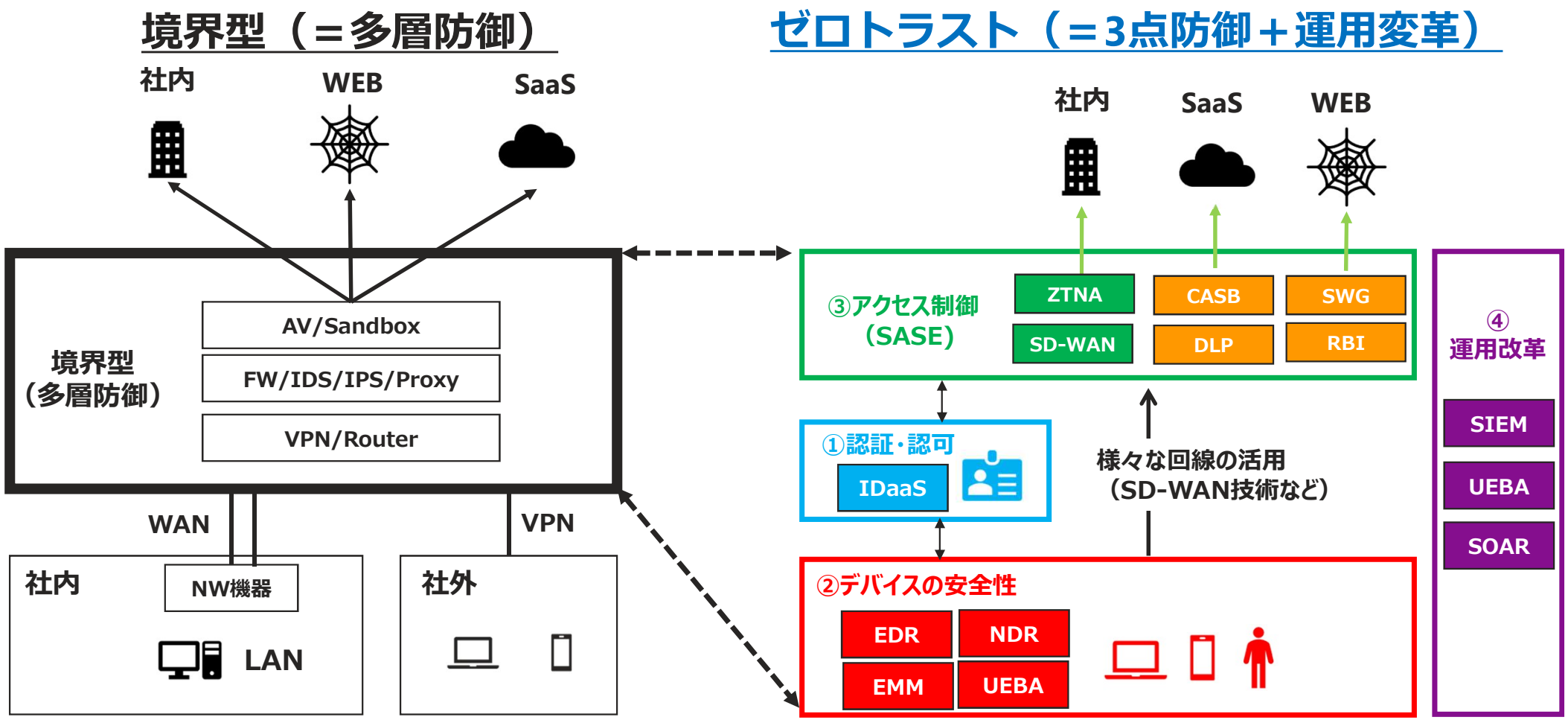
- 信頼のアルゴリズムを繋いで、最小権限のアクセスを許可する
- 漏洩してはならない重要な企業リソースをどう守るか



例えば・・重要な個人情報へのアクセスイメージ



まとめ：境界防御からゼロトラストへの移行



ゼロトラスト化が解決する様々な課題

ゼロトラスト

企業課題の解決

デバイス・ユーザー
に基づいた認証・認可

① 働き方改革（テレワーク）
コロナ等の災害対応

動的な状態（脅威・振る舞い）
に基づいて信用

② タブレット・私物端末など
様々な端末の利活用

社内・社外の経路を問わない
最小権限のアクセス許可

③ 企業データのクラウド移行
ITガバナンスの強化

内部・外部の脅威検知も含めた
可視化・対応の自動化

④ 新セキュリティ脅威への対応
（内部不正・攻撃の巧妙化）

①ユーザー認証・認可の実現
②デバイスの安全性の確保

ゼロトラストの出発点＝IDを中心とした境界への移行

①多要素認証

指紋等の多様な方式
ユーザーの状態に応じた認証
EDR等と連携した端末認証

②シングルサインオン

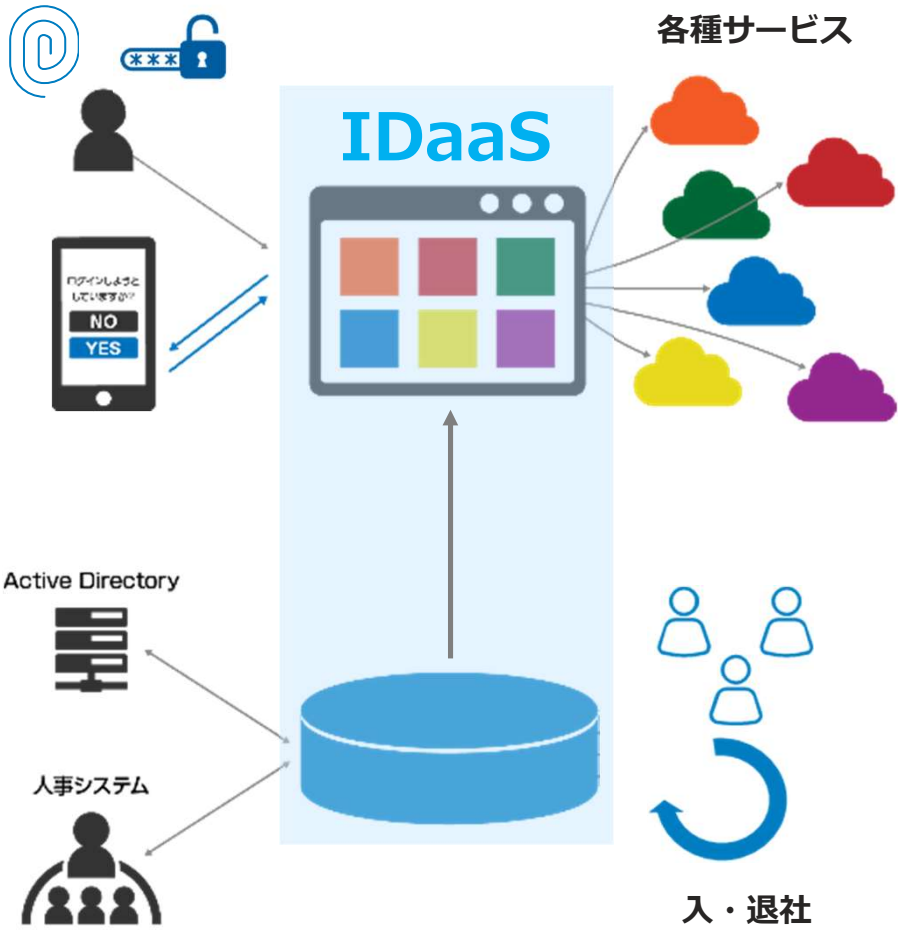
ログインポータルの提供
あらゆるサービスの窓口
オンプレ・クラウドに対応

③ディレクトリ統合

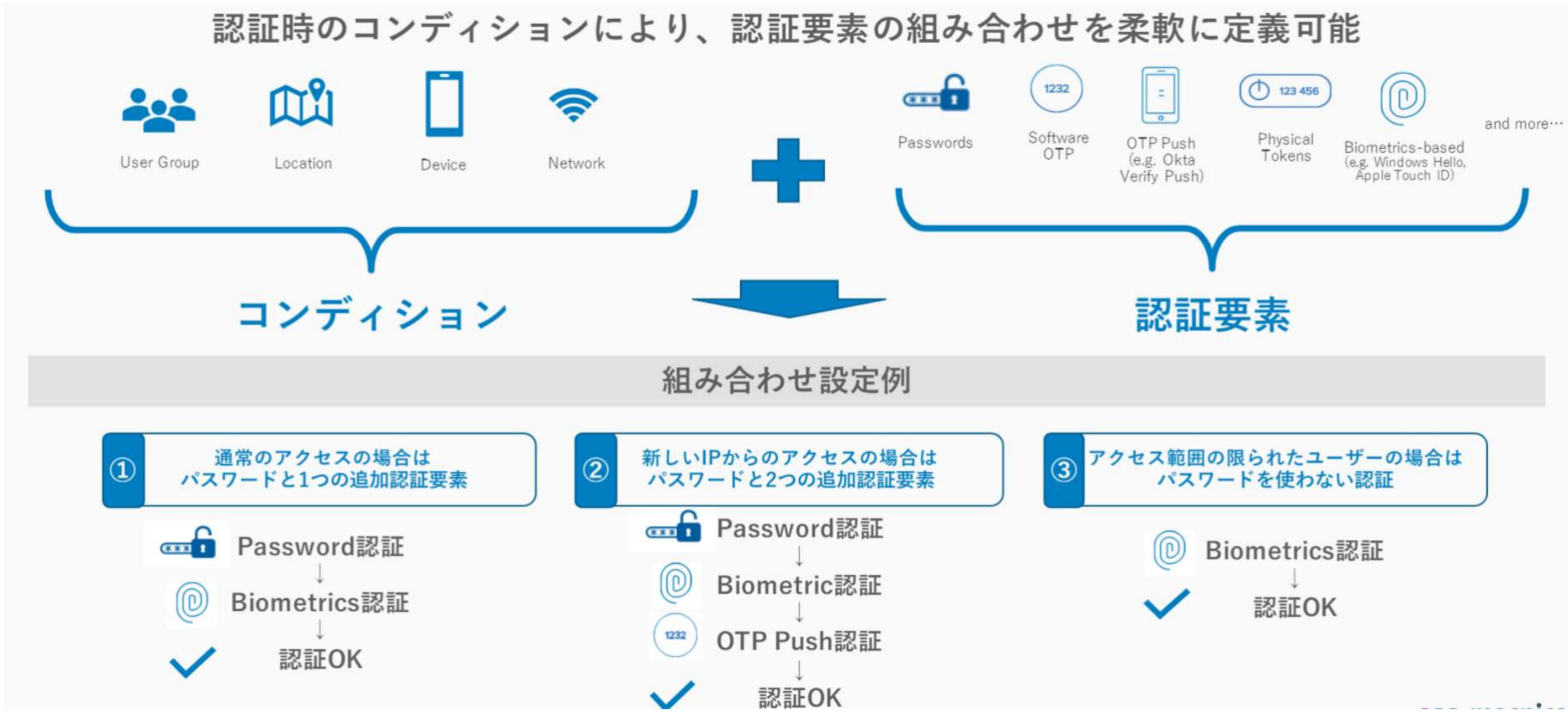
既存システムとの同期・連携
複雑な環境への対応
（マルチフォレスト等）

④ライフサイクルプロビジョニング

徹底的な自動化の実現
（アカウント管理・サービス登録）

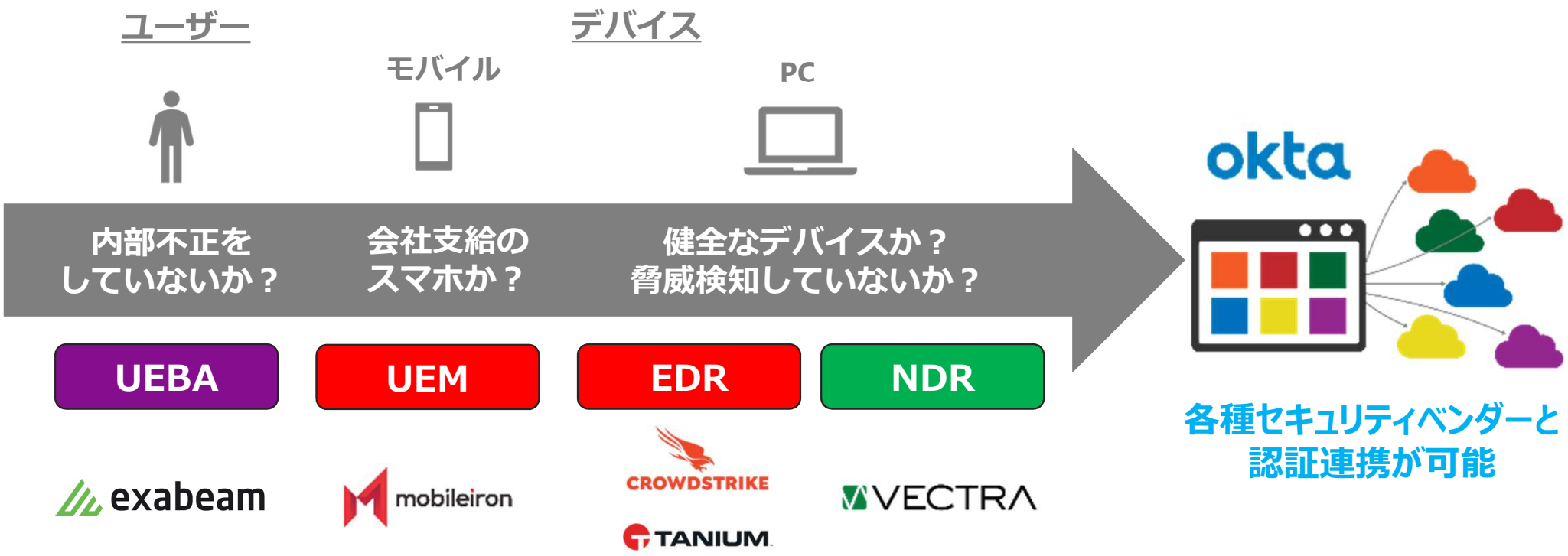


ユーザーの状態・属性に基づいた認証の実現（ユーザートラスト）

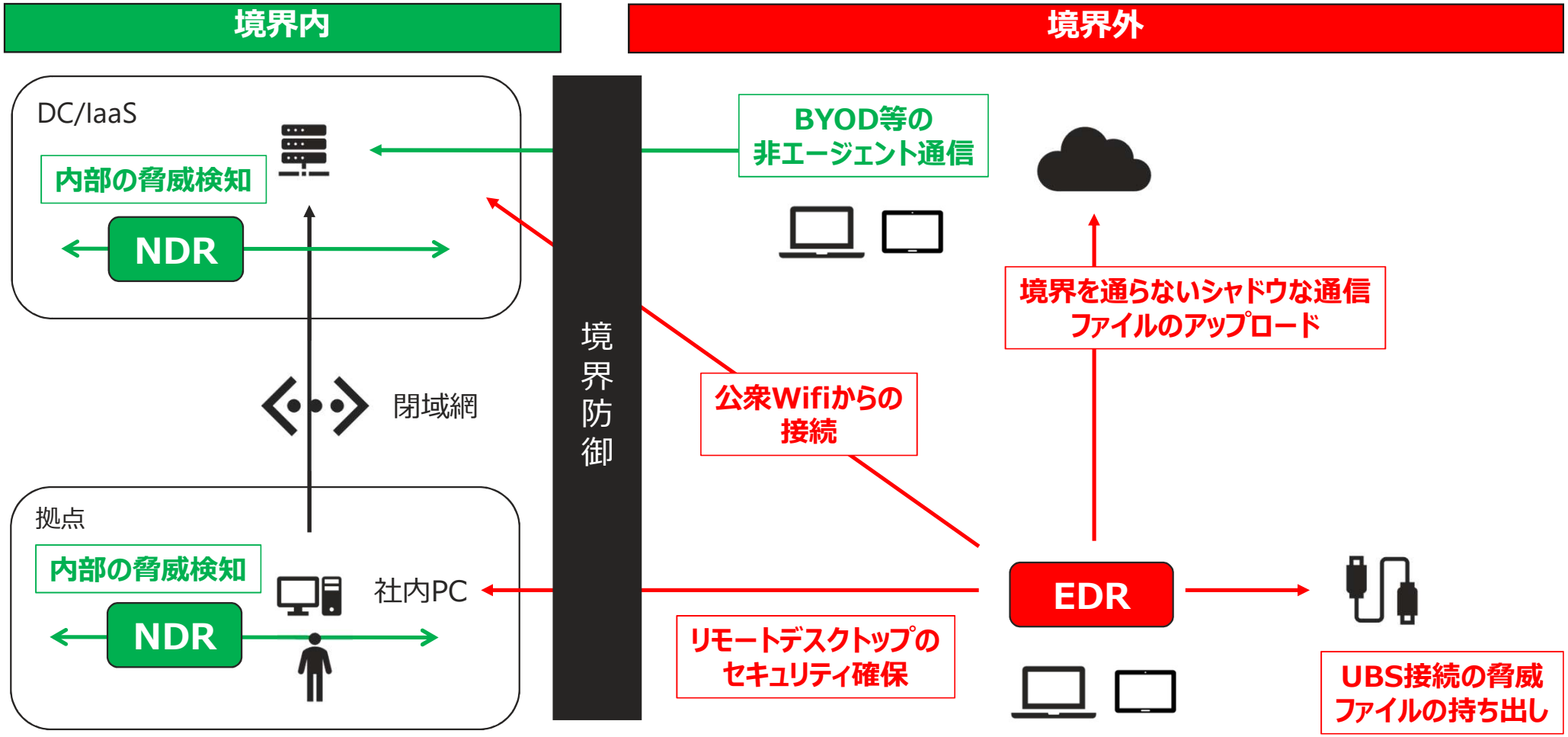


セキュリティ製品と連動したユーザー・デバイス認証の実現

- お客様に最適なベストオブブリードなご提案
- 既に投資済みのEDR/UEM等のセキュリティ製品との連携を提案します

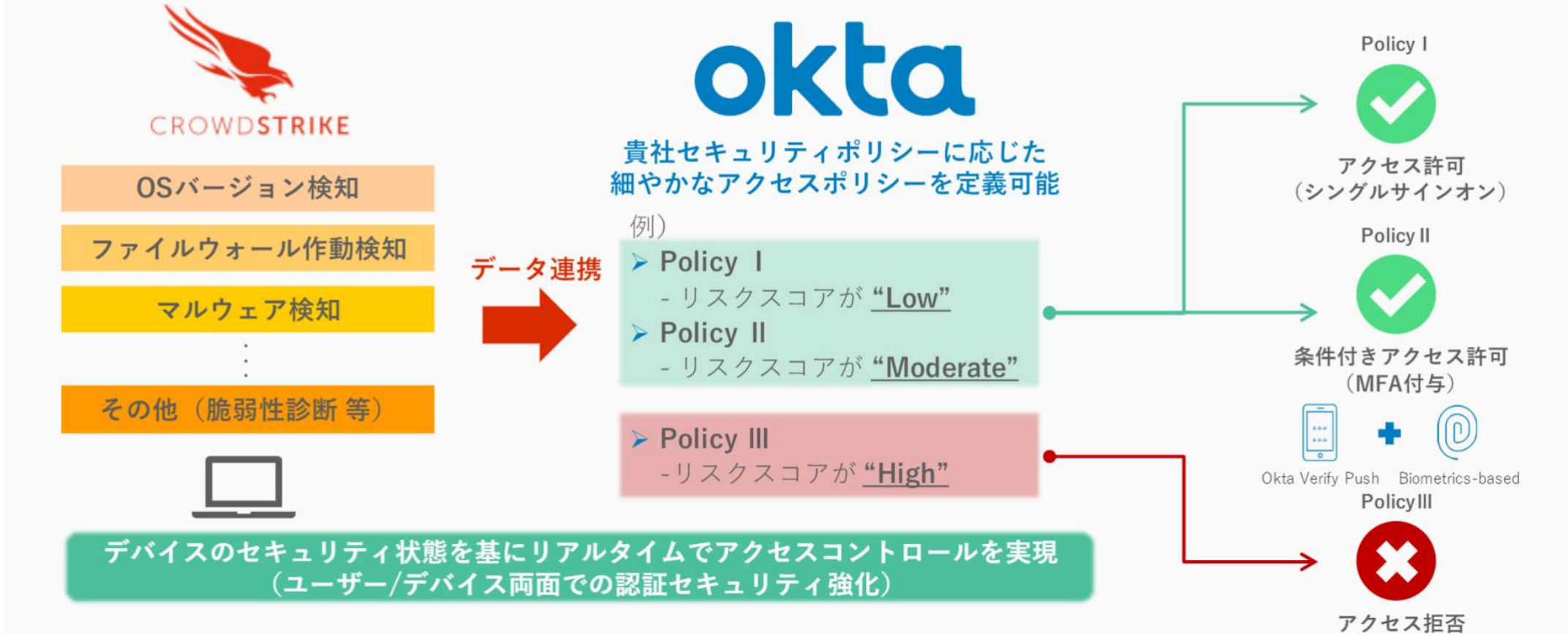


デバイスの健全性をチェックするソリューション



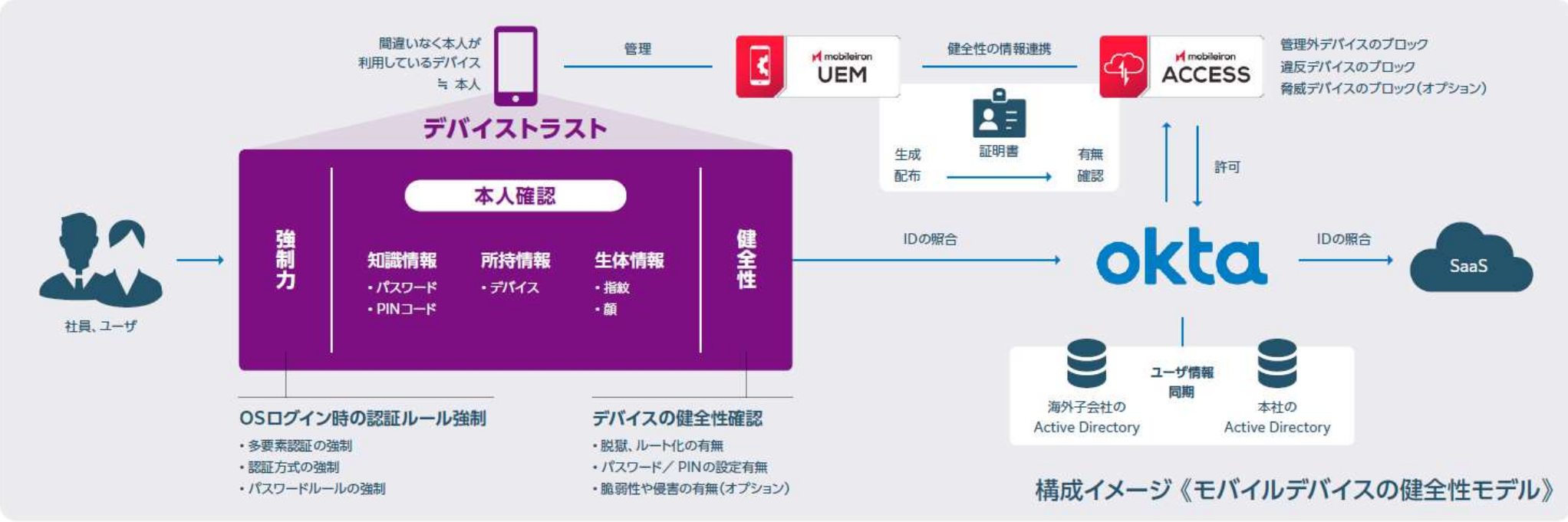
PCデバイスの健全性チェックと連動した認証（EDR連携）

≪ 連携イメージ ≫



モバイルデバイスの健全性チェックと連動した認証(UEM/MTD連携)

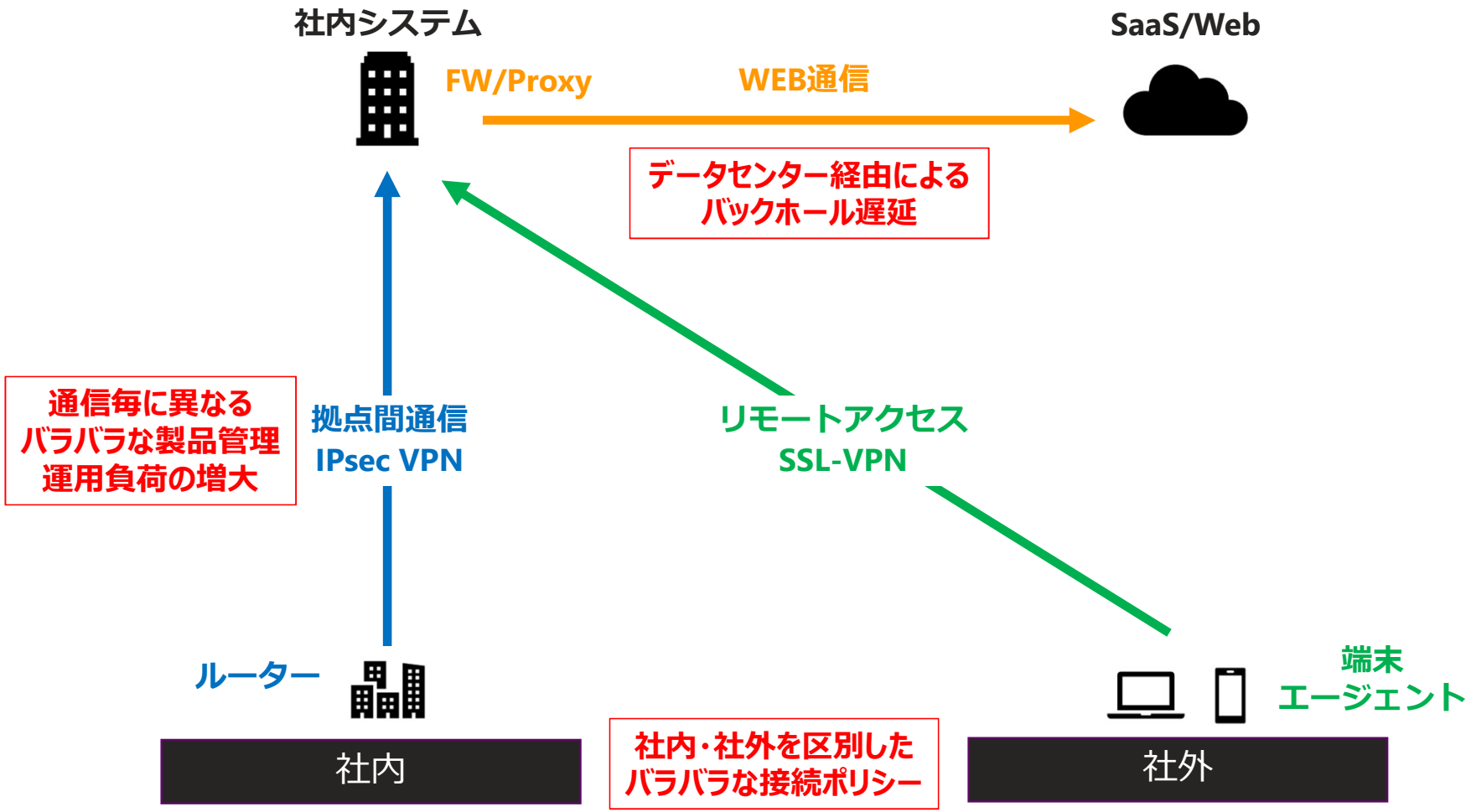
- PCデバイスとは別にiOS等のモバイルOSに対応したソリューションが必要
- モバイルに特化した脅威検知のソリューションも存在する（MTD）



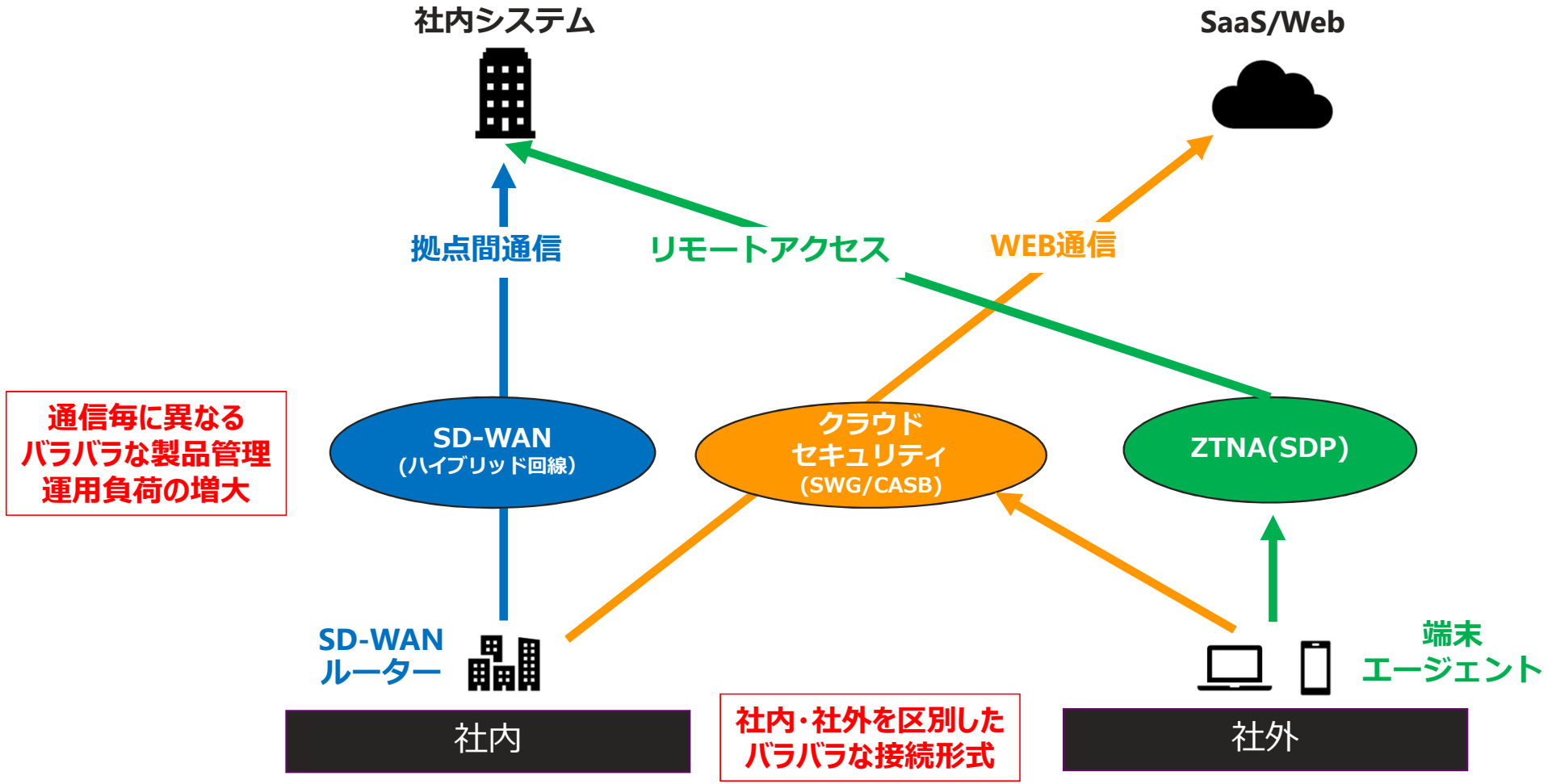
構成イメージ《モバイルデバイスの健全性モデル》

③ネットワーク・セキュリティのクラウド化
最適な「SASE」の選択

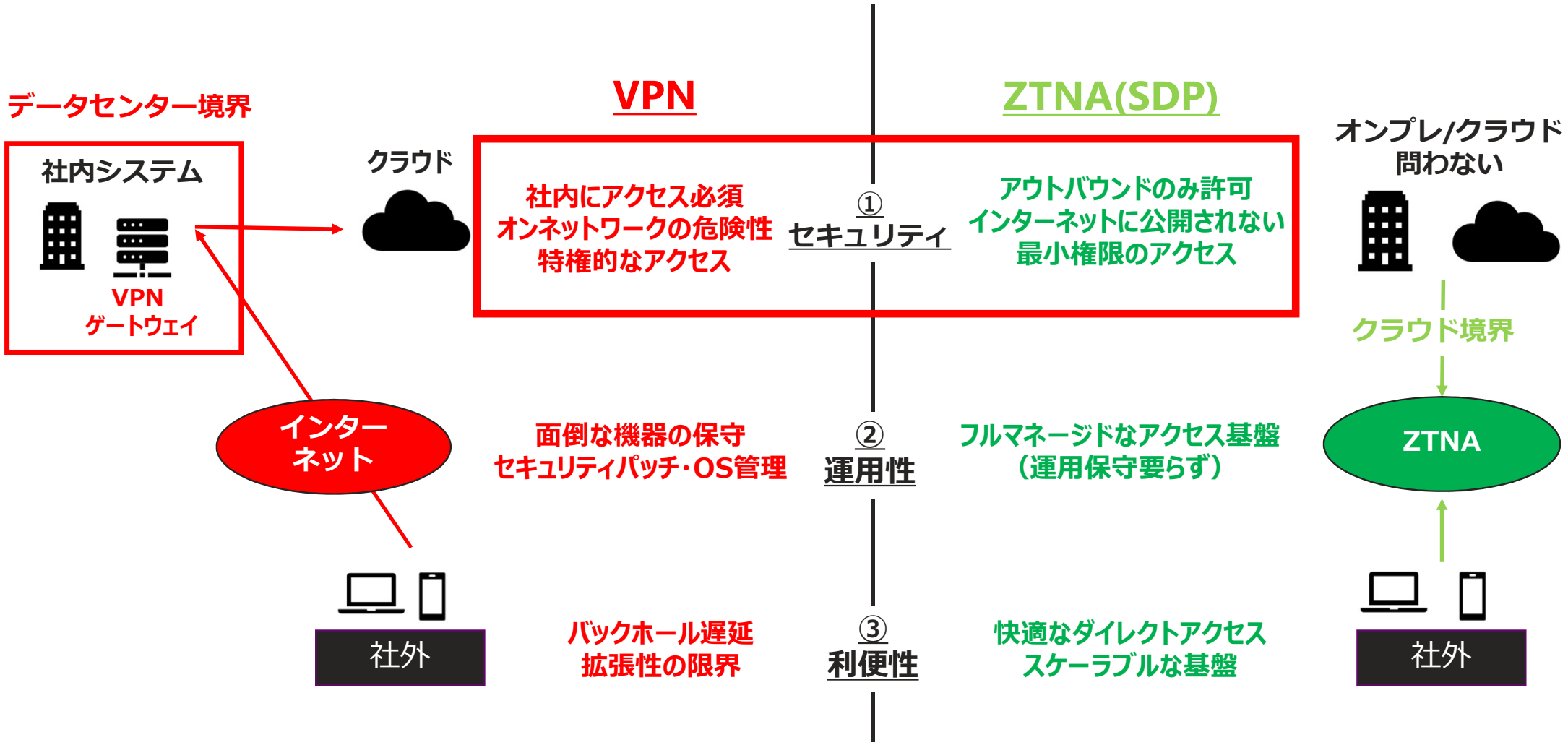
現状：企業を取り巻く３つのバラバラな通信



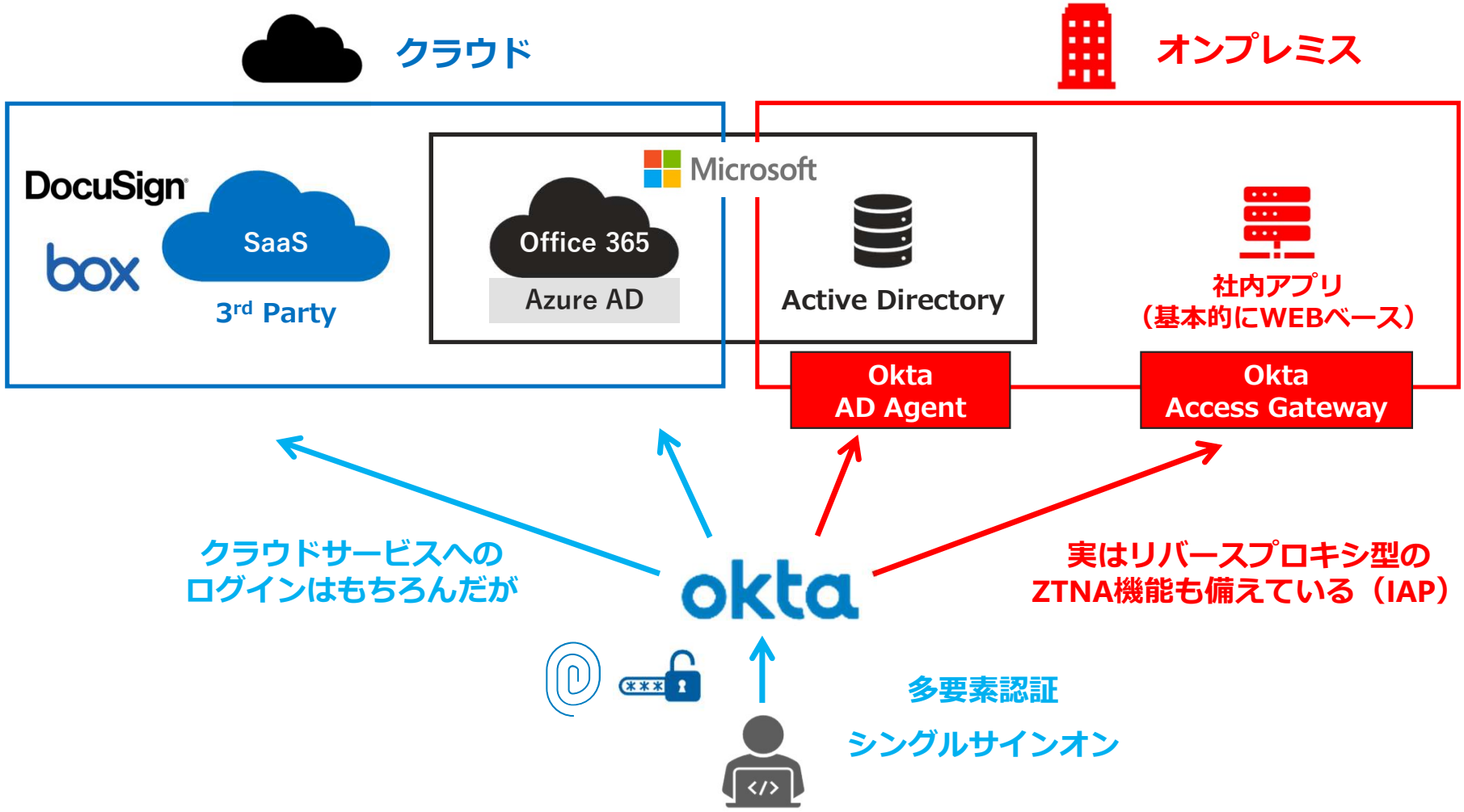
３つの通信のクラウド化が進む現状



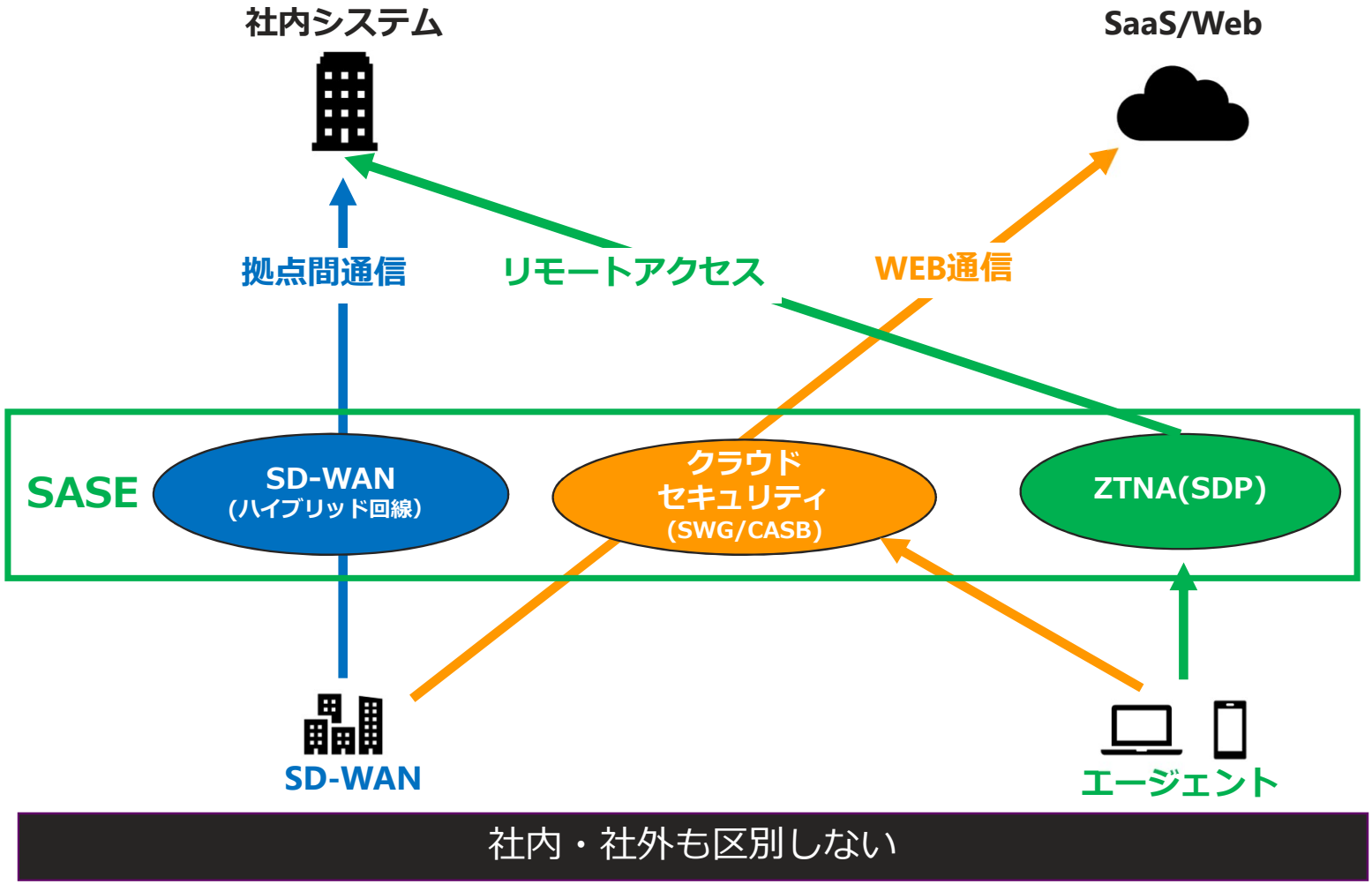
VPNの課題を解決するZTNAの登場



IDaaSは実はZTNAの機能も備え始めている(IAPとも呼ばれる)



SASE＝３つの通信経路のクラウド統合



異なる通信の
一元的な集中管理の実現

ネットワークとセキュリティの
クラウド統合

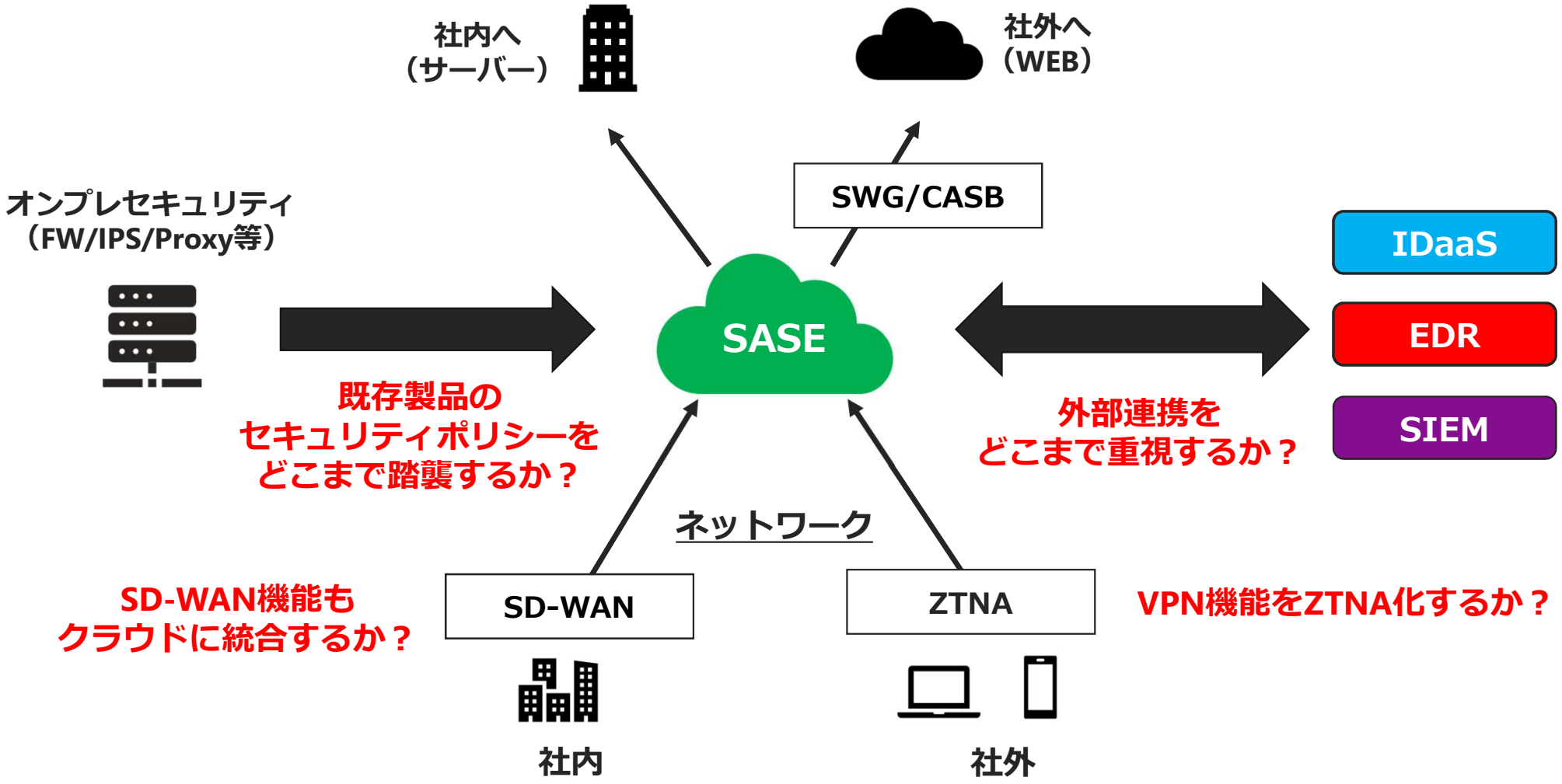
アクセス元に関わらず
社内・社外も同一の経路

どのSASEをゼロトラスト構成の軸に据えるか？（強み・弱みの着眼点）

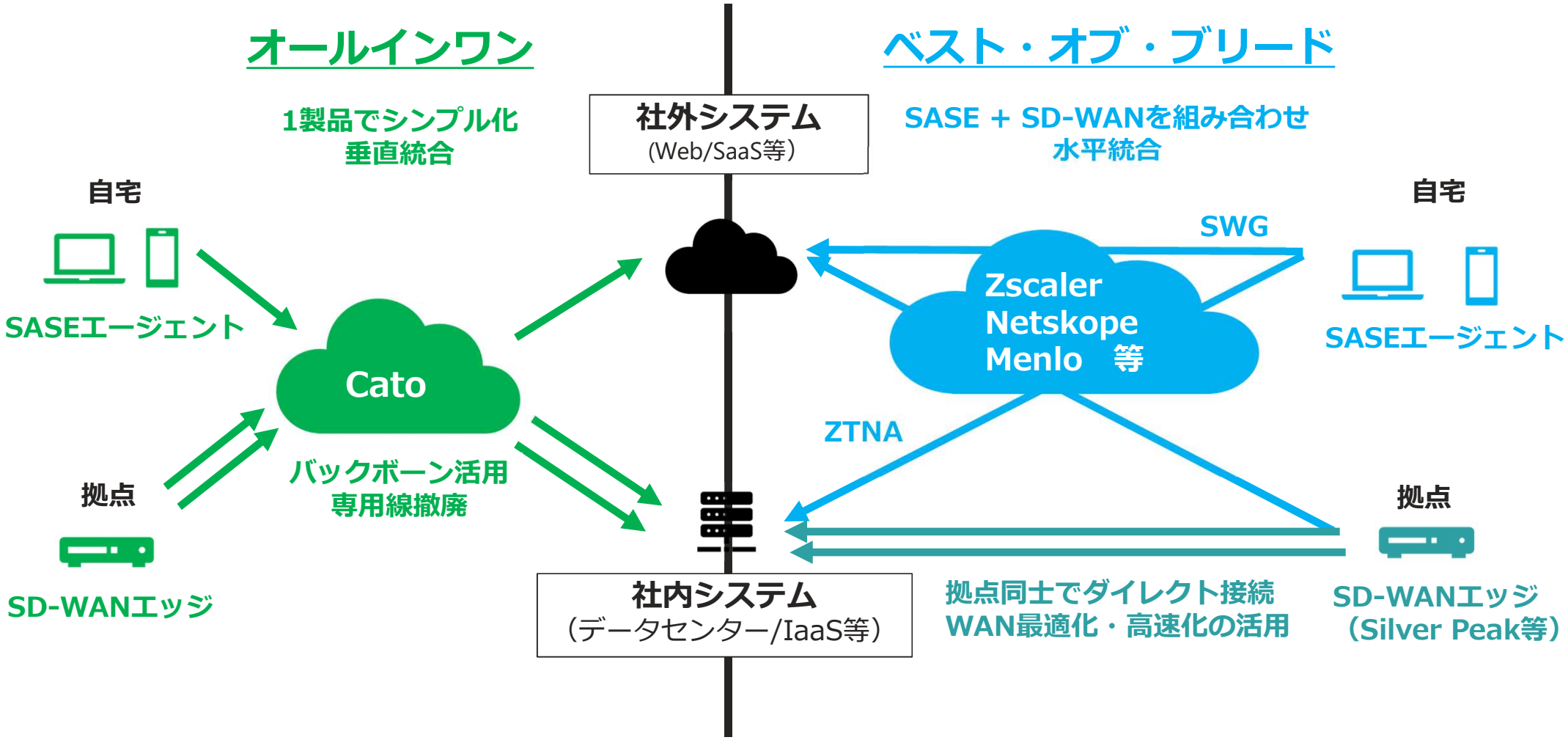
- 現状完璧なSASEは存在しないので、**重要視する機能**に着目する
- 今後の**将来性**や、**外部連携・相性**を加味した上で選定することが重要

			マクニカ取り扱い製品			マクニカ非取り扱い製品	
			Cato	Menlo	McAfee	Zscaler	Netskope
			NW機能も統合 海外間接続	WEB分離リーダー	CASBリーダー	SWGリーダー 豊富なAPI連携	CASBリーダー 豊富なAPI連携
SASE	セキュリティ	SWG Webセキュリティ	○	○	○	◎ SWGリーダー	○
		RBI ブラウザ分離	-	◎ RBIリーダー	○ 買収	○ Menlo連携可	Ericom連携可
		FWaaS FWサービス	○	実装予定	○	○	実装予定
		CASB/DLP SaaS可視化・制御	実装予定	実装予定 MS連携可	◎ CASBリーダー	○ McAfee連携可	◎ CASBリーダー
	ネットワーク	ZTNA リモートアクセス	◎ エージェントレス対応	実装予定	-	○	○
		SD-WAN 拠点間通信	◎	外部SD-WAN連携（Silver Peak等）			
		バックボーン 海外専用線	◎ 全世界をカバー	-			

最適なSASEベンダーを選定する着眼点



オールインワン型か？ベスト・オブ・ブリード型か？

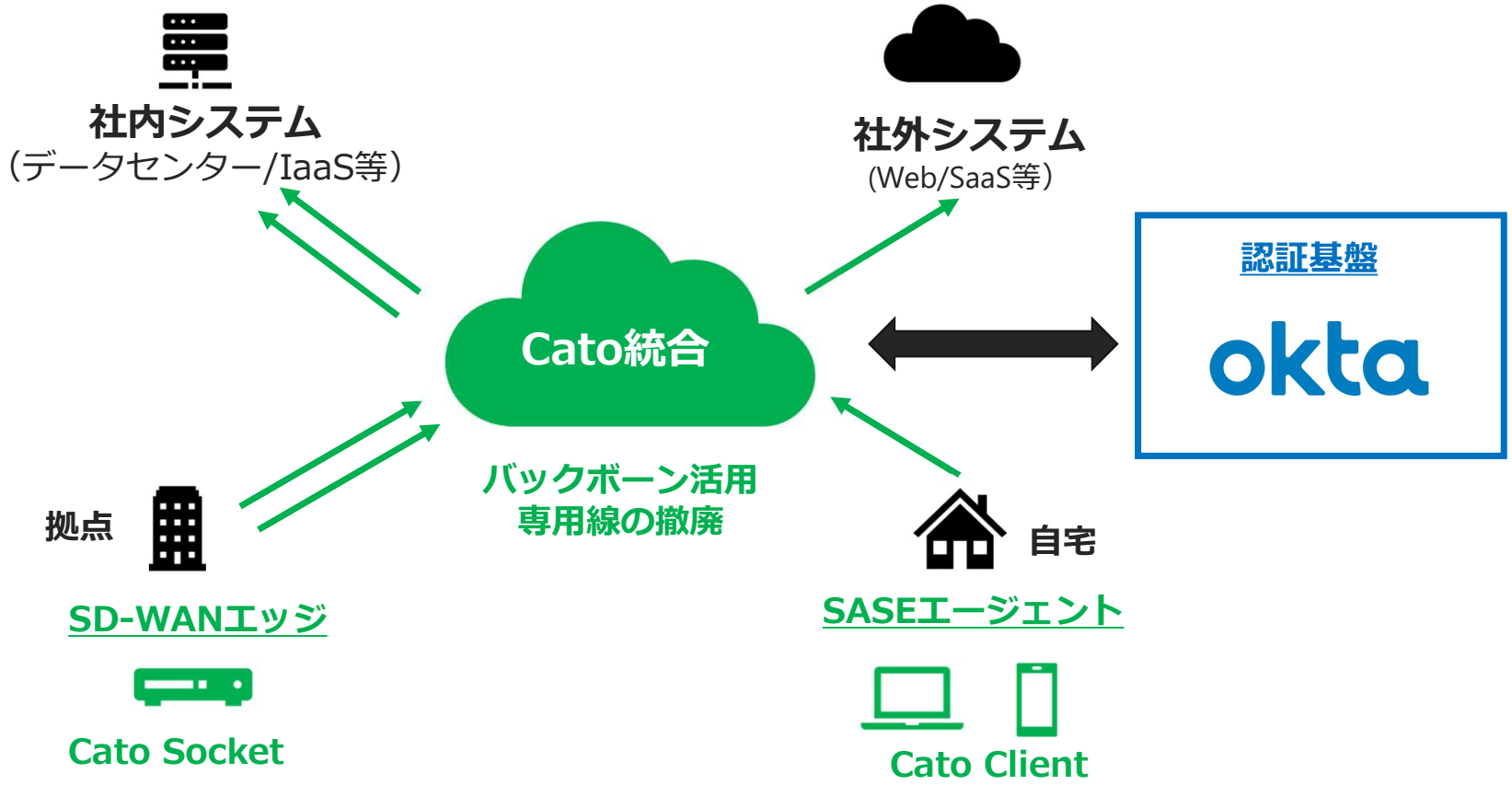


ゼロトラストにおけるベスト・オブ・ブリード構成の考え方

- シングルベンダー構成は導入が容易だが、中長期でロックインの危険性がある
- ベスト・オブ・ブリードは自由度が高いが、ベンダー間の連携性をきちんと確認する

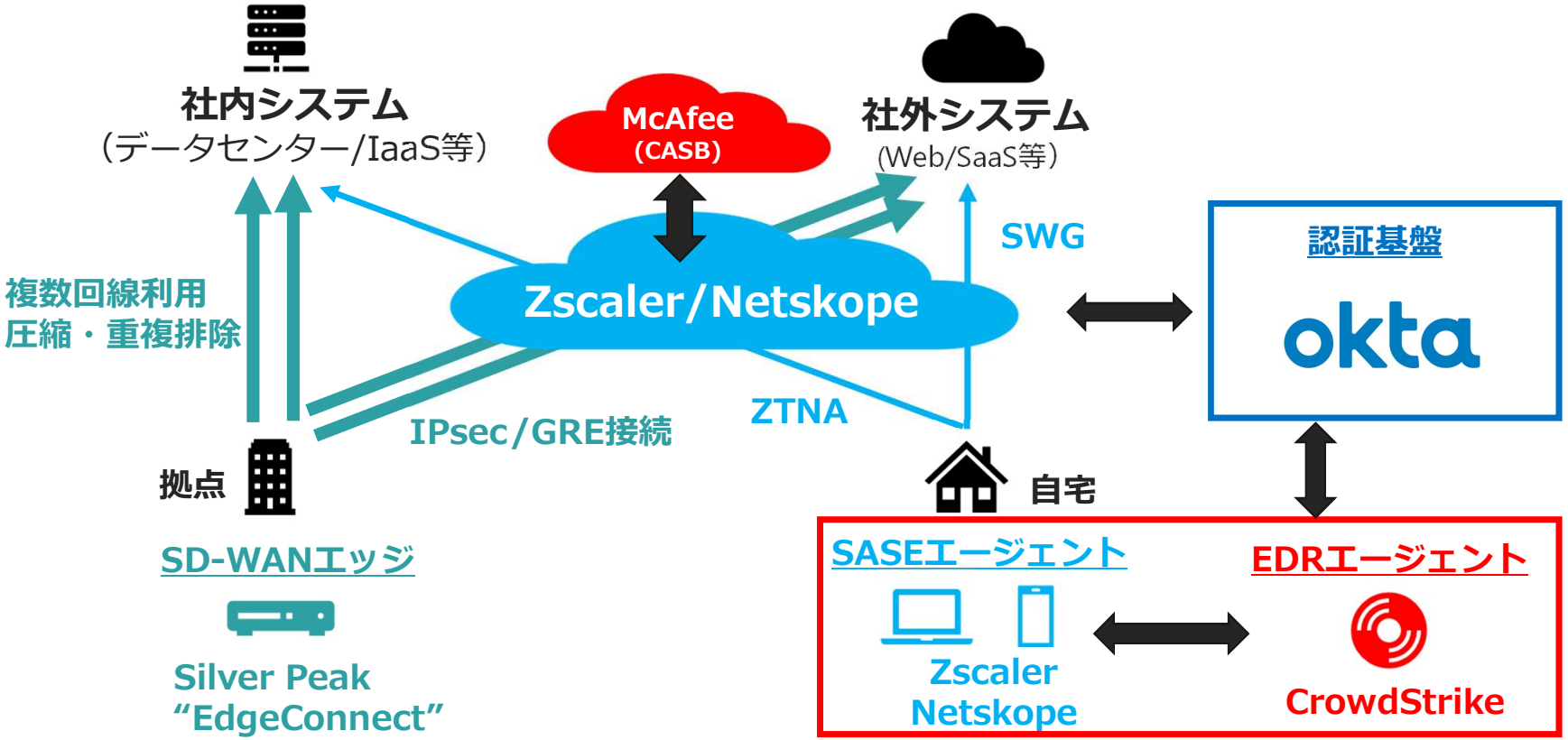
オールインワンなシンプルな構成例

- 拠点間通信も含め全ての通信を例外なくクラウドゲートウェイ上で全てコントロールが可能
- ガバナンス統一・専用線の撤廃が期待出来るためグローバル企業での採用事例が多い



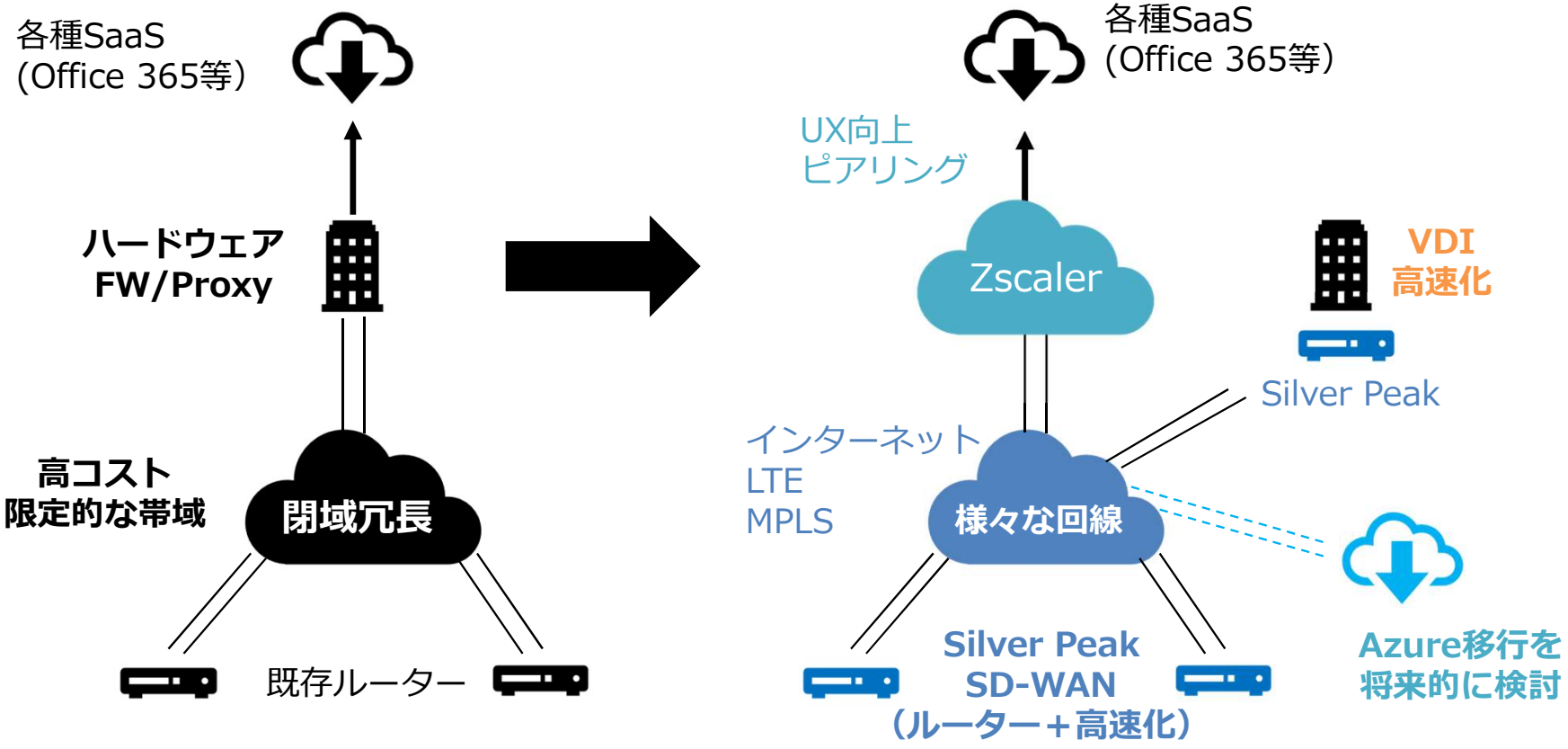
複数製品によるベスト・オブ・ブリードな構成例

- 専用製品を組み合わせることで複雑な要件にも対応が可能（製品間の密連携による自動化など）
- 複数製品を組み合わせるため運用性・コストなどの課題は残る



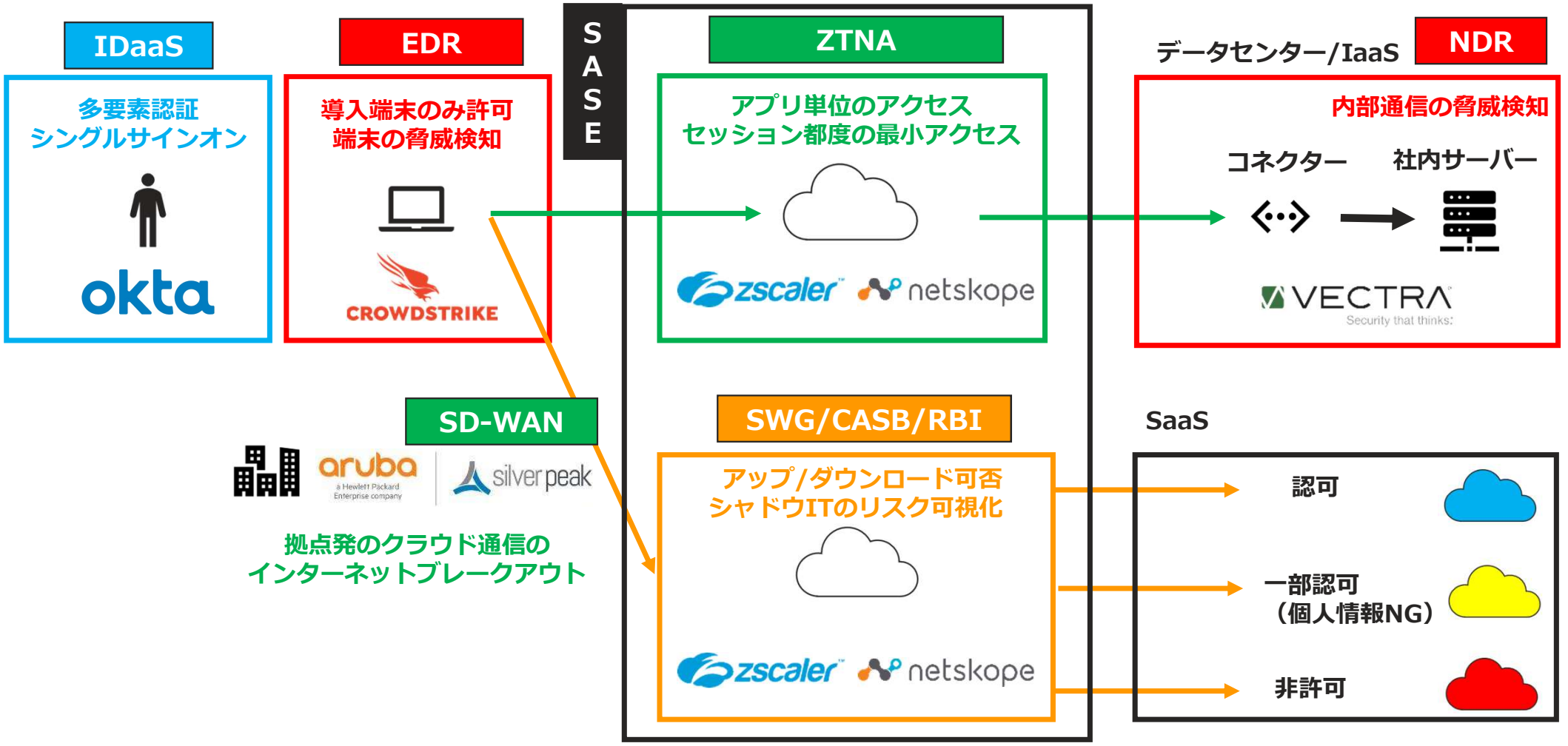
ベスト・オブ・ブリード構成の国内導入事例（SD-WAN + SASE）

- 愛知本社の自動車部品製造業が国内30拠点をSilver Peak＋Zscaler構成に刷新
- データセンター中心の境界防御から、SASE中心のクラウド境界へと変革を実現



ベスト・オブ・ブリード構成を選択する際は相性・連携の深さも重要

APIレベルでベンダー間連携する製品は導入が非常に楽



④ゼロトラスト化に伴う運用変革

ゼロトラスト環境では広範なログに基づいた可視化・自動化が求められる

①３つの可視化・脅威検知

SASE
SWG/CASB
VPN/SDP

IDaaS

EDR

NDR

などなど

①ログデータ起点

②エンドポイント

③ネットワーク

②解析・相関分析

SIEM

各種ログの集積・解析
ログの正規化・データ統合

UEBA

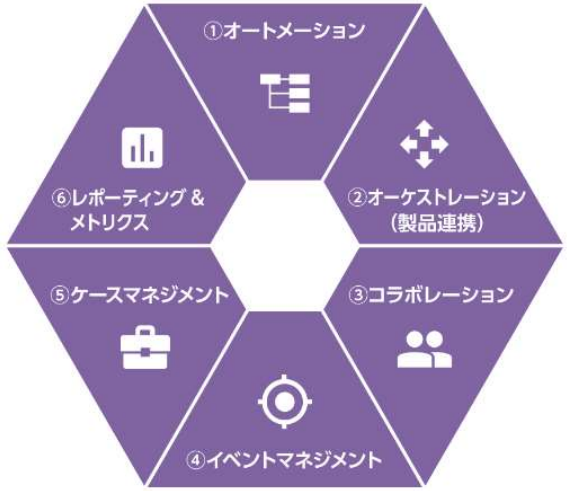
ユーザー中心の相関分析
リスクスコアの自動計算
AIによる自動的な閾値学習

優先アラート
検知トリガー

③連携・対応の自動化

SOAR

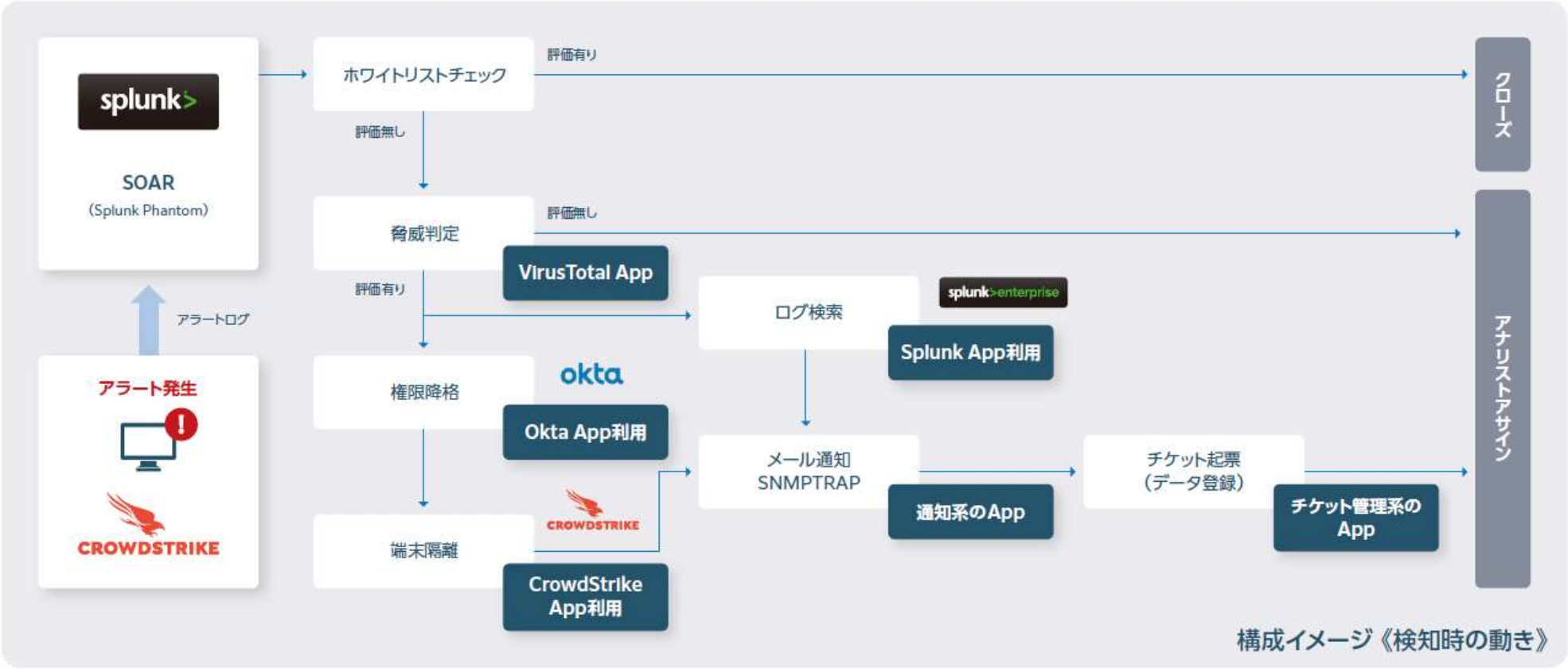
インシデント対応のタスクを自動実行
運用者の意思決定、対応を迅速化



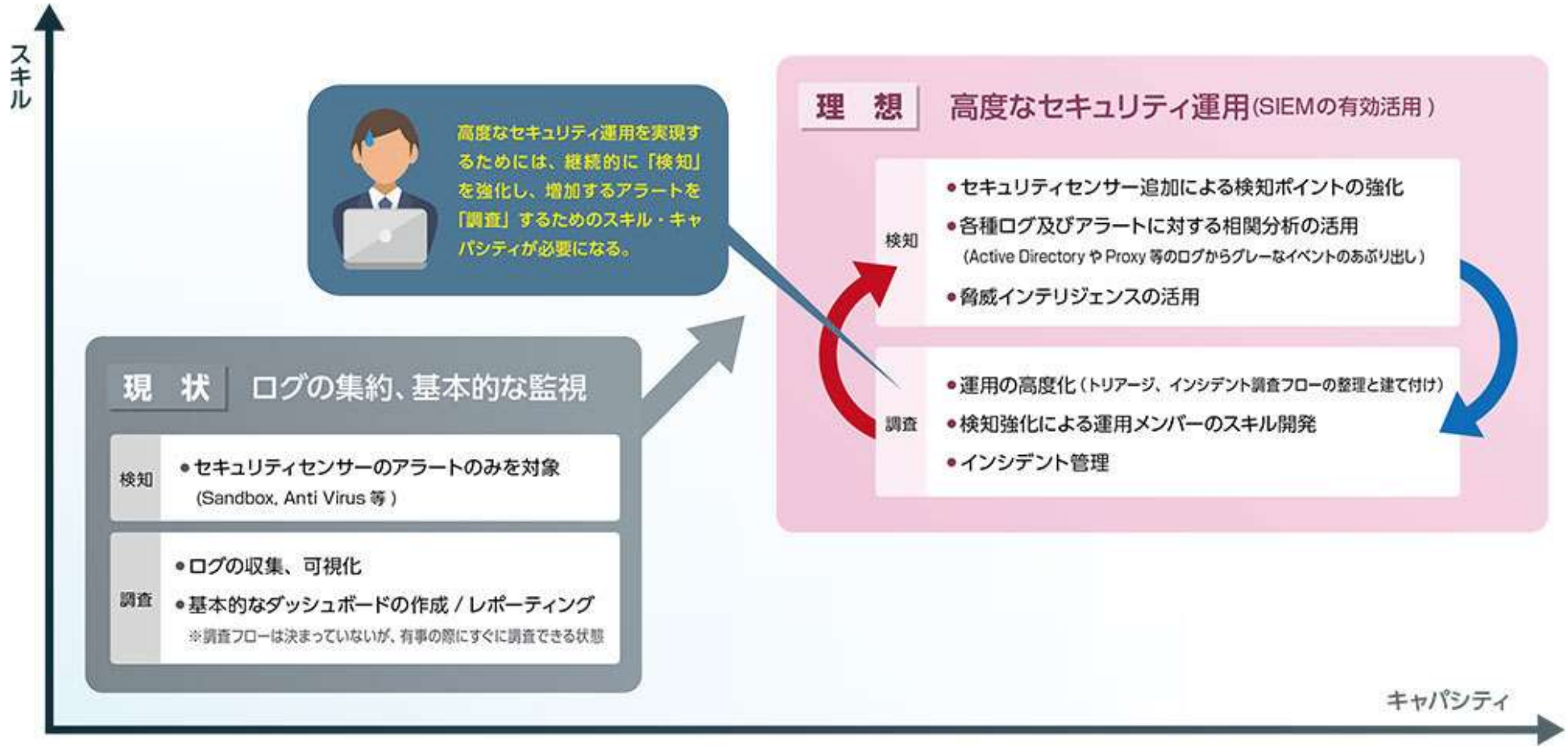
認証権限の降格、端末の隔離などの対応

EDR検知をトリガーとしたSOARによる端末隔離の自動化

例：端末脅威検知をトリガーとした運用自動化の例



ゼロトラスト移行ではセキュリティ運用の高度化が問われる



弊社マクニカが提供する各種セキュリティ運用・支援サービス

- ゼロトラスト移行に伴って IDaaS, EDR, SASE 等新たなソリューション導入が不可欠です
- 移行に伴うセキュリティ運用改革をコンサル・実装・運用までご支援いたします
- 下記は “Splunk”を用いたお客様のセキュリティ運用体制のご支援サービスとなっております

コンサルティング

- セキュリティドメインコンサルティング
- 簡易セキュリティコンサルティング
- Splunk Phantom 自動化アセスメントサービス
- SIEM業務改善コンサルティング

実装・構築支援

- 環境構築支援 ※構築パートナー様
- ダッシュボード作成パック
- ダッシュボードメンテナンスパック
- バージョンアップサービス

独自App・その他サービス

- SIEM運用監視サービス
- セキュリティログ分析スタートパッケージ
- はじめてセットシリーズ（プロキシログ／セキュリティログ）
- Splunk×CrowdStrike Falcon Insight, Macnica Original App
- 政府統一基準対応App
- Cloud Security Monitoring App
- Smart Security Monitoring App

お客様のライフサイクル・運用方針に応じたサービス提供が可能です

splunk>

macnica networks

全世界115か国以上、15,500社以上に導入されているSplunk
マクニカネットワークスは**国内導入実績No1の一次販売代理店**です

2009年よりSplunkの取扱いを開始して10年、導入社数500社。日本語ローカライズを支援した技術者を含む専任技術者やSplunk認定セールスが多数在籍しています。セキュリティやITインフラ管理、ビックデータ活用などの多様なシーンにおけるお客様の課題解決に向けて、ご提案から導入、構築、運用までをワンストップでサポートいたします。

	セキュリティポリシー設計	Splunk / SIEM 設計 / 仕様策定	Splunk / SIEM 実装	認定メンテナンス	運用改善	運用
コンサルティング	セキュリティドメインコンサルティング				SIEM業務改善コンサルティング	
	簡易セキュリティコンサルティング		Smart Security Monitoring App			
	SOARアセスメント Playbookデザイン		クラウドセキュリティはじめてパック			
構築支援 実装			環境構築支援		バージョンアップサービス	
			ダッシュボード作成パック			
				ダッシュボードメンテナンスパック		
運用サービス 独自App					SIEM運用監視サービス	
					セキュリティログ分析スタートパッケージ	
			はじめてセット			Macnica Original App

アウトソース？ or 自社運用？ お客様の運用方針に合わせた支援が可能です

方針 アウトソース

SIEM 活用	×
スキル	×
人員	×
運用体制の維持	×

SIEM運用監視サービス

- Splunk を活用した監視サービス
- トリアージ、通知、チューニングまで一気通貫で対応
- 基盤となる Splunk は自社に置き、監視業務のみアウトソース

方針 自社運用

SIEM 活用	○
スキル	○
人員	×
運用体制の維持	×

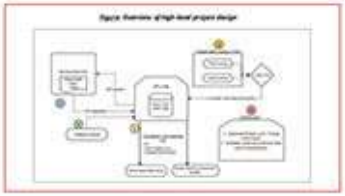
SOAR

- 調査に必要な製品、サービスとの連携
- インシデント調査の自動化
- 運用状況の可視化
- イベント管理・記録

SIEM 活用	×
スキル	△
人員	×
運用体制の維持	×

セキュリティコンサルティング

- 簡易アセスメント
- SIEM ユースケースデザイン



アウトソース）マクニカ24/365 SIEM運用監視サービス

分析官による膨大なアラート調査と対応アドバイス

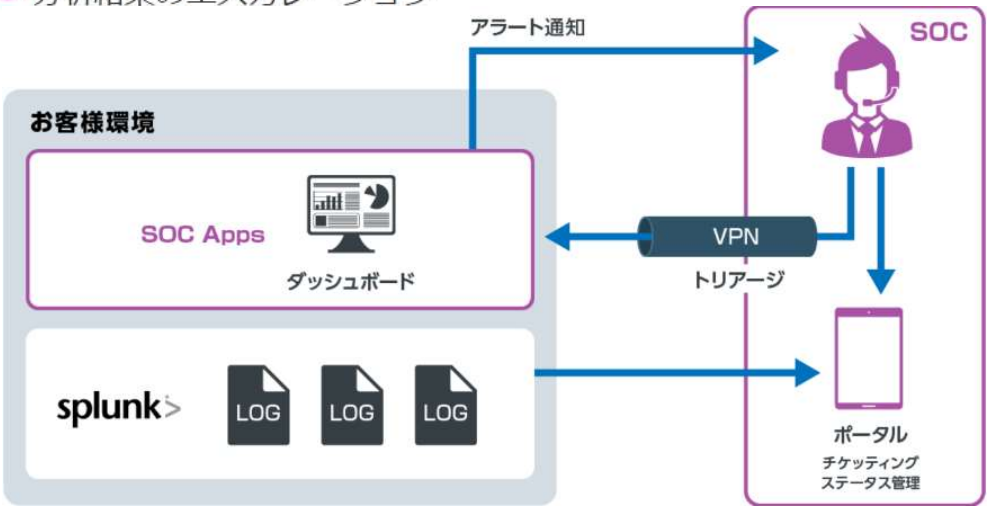
お客様はデータ分析基盤としてSplunkの継続活用が可能

単なるアラートの通知ではなく、対処アドバイスまで実施します。

- 検出した通信に脅威があるかどうかの分析
- 脅威の影響範囲の分析
- 脅威に対する対処方法の検討
- 分析結果のエスカレーション

- お客様のSplunkを利用し、24/365のセキュリティ監視
- 生ログの調査まで実施し、お客様へ対処方法をご提案
- Splunkに保管したログはお客様が自由に利用可能

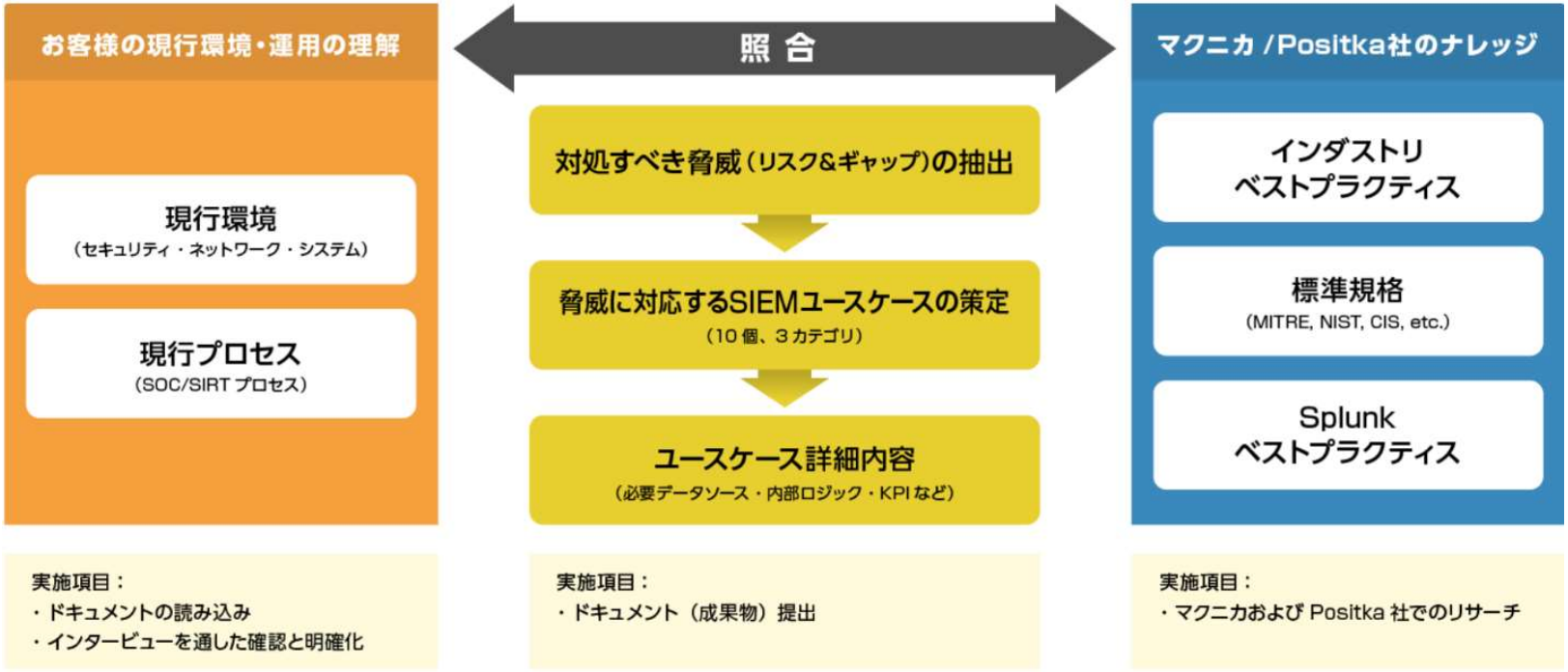
※Splunk、サーバー、VPNは本サービスのご提供内容に含まれません。別途ご相談ください



SOCアプリイメージ

自社運用の場合）簡易セキュリティコンサルティングサービス

1. MITRE ATT&CKフレームワークとお客様環境の照合分析（主要リスク/ギャップの特定）
2. フレームワークから必要な検知ルール（SIEMユースケース）を特定
3. 具体的かつ詳細な検知ルールのデザイン/設計案を提供
4. ①～③の結果を詳細なドキュメント形式（アセスメントレポート）で納品



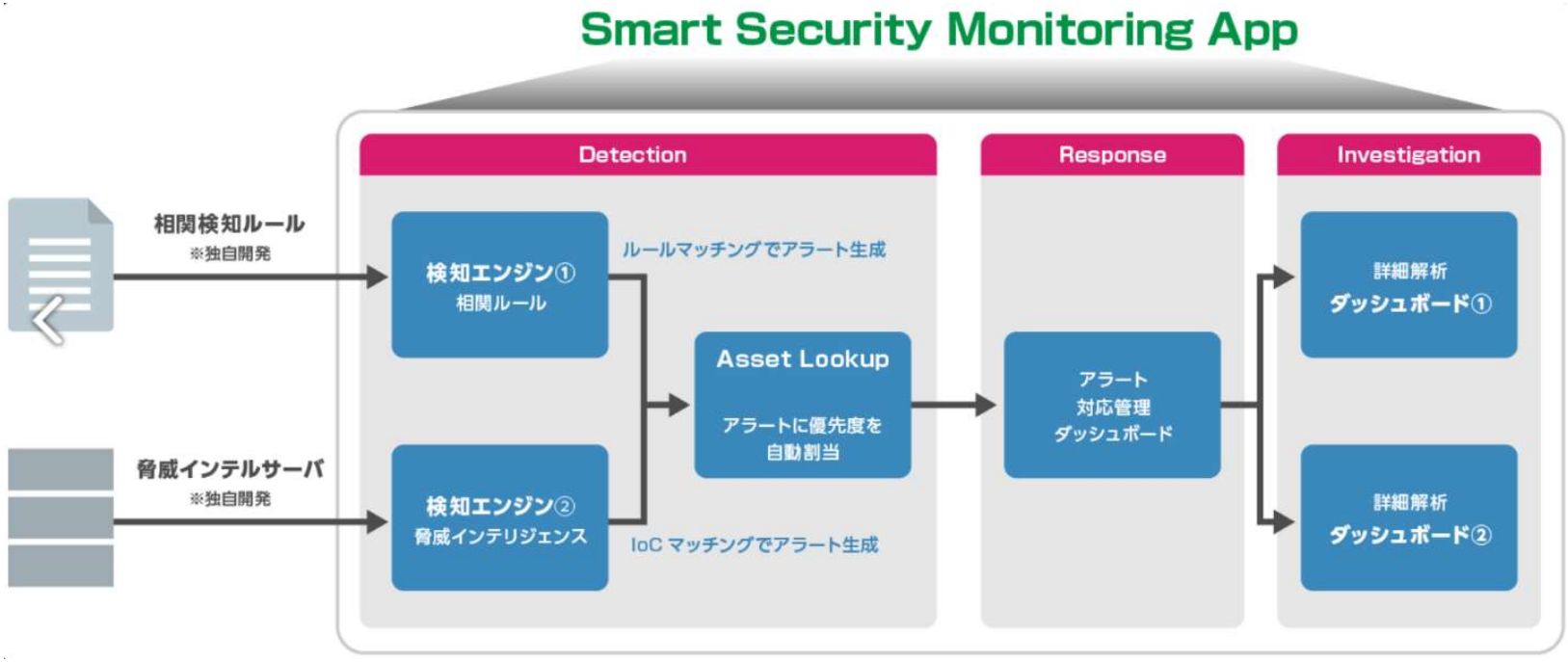
自社運用の場合）弊社独自アプリ②（ゼロトラスト対応の独自ダッシュボード）

3つの機能群を初期搭載

1. 広範なログの相関解析による検知機能
2. 脅威インテリジェンスを活用したIoC※1マッチングによる検知機能
3. 効率的で無駄のないアラート管理/トラッキング/詳細調査のためのダッシュボード群

監視対象データソースを選択（12カテゴリ）

Security infrastructure
Endpoint protection / Anti-Malware
Firewalls
Active Directory
Web Proxy
Network IDS / IPS
Authentication
Network Infrastructure
Routers (via syslog server)
Switches (via syslog server)
Server Infrastructure
Windows server
Linux server
Web server
DNS server
VPN server
Mail server



自社運用の場合）弊社独自アプリ①（EDR連携に特化した連携）

自動隔離機能による運用簡素化

端末の自動隔離
CrowdStrike Falcon導入端末から発砲されるアラートに対し、FalconのAPI（Streaming API）を用いて検知情報の集約→端末の自動隔離を指示

セキュリティ運用を強力バックアップ
自動端末隔離によって、セキュリティ運用部隊のオンサイトでの工数削減、休日深夜帯など時間外のセキュリティ運用を強力にバックアップ

ダッシュボード・レポーティングによる検知状況の分析

エンドポイントの検知状況を可視化
検知ログの統計・解析から脅威にさらされたエンドポイントの可視化、お客様固有の要望に応じたカスタマイズダッシュボードを作成可能

全てのログを一元管理
既にお持ちの他のセキュリティ・ネットワークログもSplunkに取り込むことで、全体的なログ運用をSplunkで一元管理が可能に

自社運用の場合）運用自動化の事前評価サービス

1. お申込み
   - お申込書提出
   - 簡易ヒアリングシート
2. プロセスのたな卸し
   - 詳細ヒアリングシート
   - 電話会議
   - インタビュー
   - ワークショップ
   - ドキュメント提出
3. 自動化のスコープ定義
   - マッピング作業
   - ドキュメント提出
4. 自動化の難易度調査
   - 各種難易度調査
   - ドキュメント提出
5. ROI シュミレーション
6. 導入検討プラン案作成

運用自動化の目指すべきゴールを一緒に描きます

構成イメージ《運用を自動化するモデル》

まとめ：ワンストップでゼロトラスト移行を支援いたします

- お客様の導入フェーズに合わせたゼロトラスト導入支援サービスを提供いたします
- アライアンスパートナー様と連携したサービス提供も可能です

	フェーズ1 ヒアリング・方針策定	フェーズ2 検証・構築・導入	フェーズ3 運用・監視・最適化
			
macnica networks	課題ヒアリング・相談 幅広い製品提案	POC・検証支援 設計・構築支援	技術QA支援 カスタマーサクセス
アライアンスパートナー	コンサルティングパートナー	設計・構築パートナー	マネージドサービスパートナー

パートナー様と連携したサービス提供も可能です

- ゼロトラストの中核となる製品の供給元としてパートナー様と技術提携をしております
- 提案から導入後の運用までワンストップでサービス提供が可能となっております

マクニカ

海外ベンダーと直接取引
全製品を一次店で取り扱い
製品に精通した技術者集団
製品間連携もサポート

IDaaS
EDR
SASE

okta
CROWDSTRIKE
CATO NETWORKS
Menlo Security

パートナー様取り扱い商材

マクニカで取り扱っていない製品についても
パートナー様にご相談が可能です

zscaler
netskope

ゼロトラストパートナー様

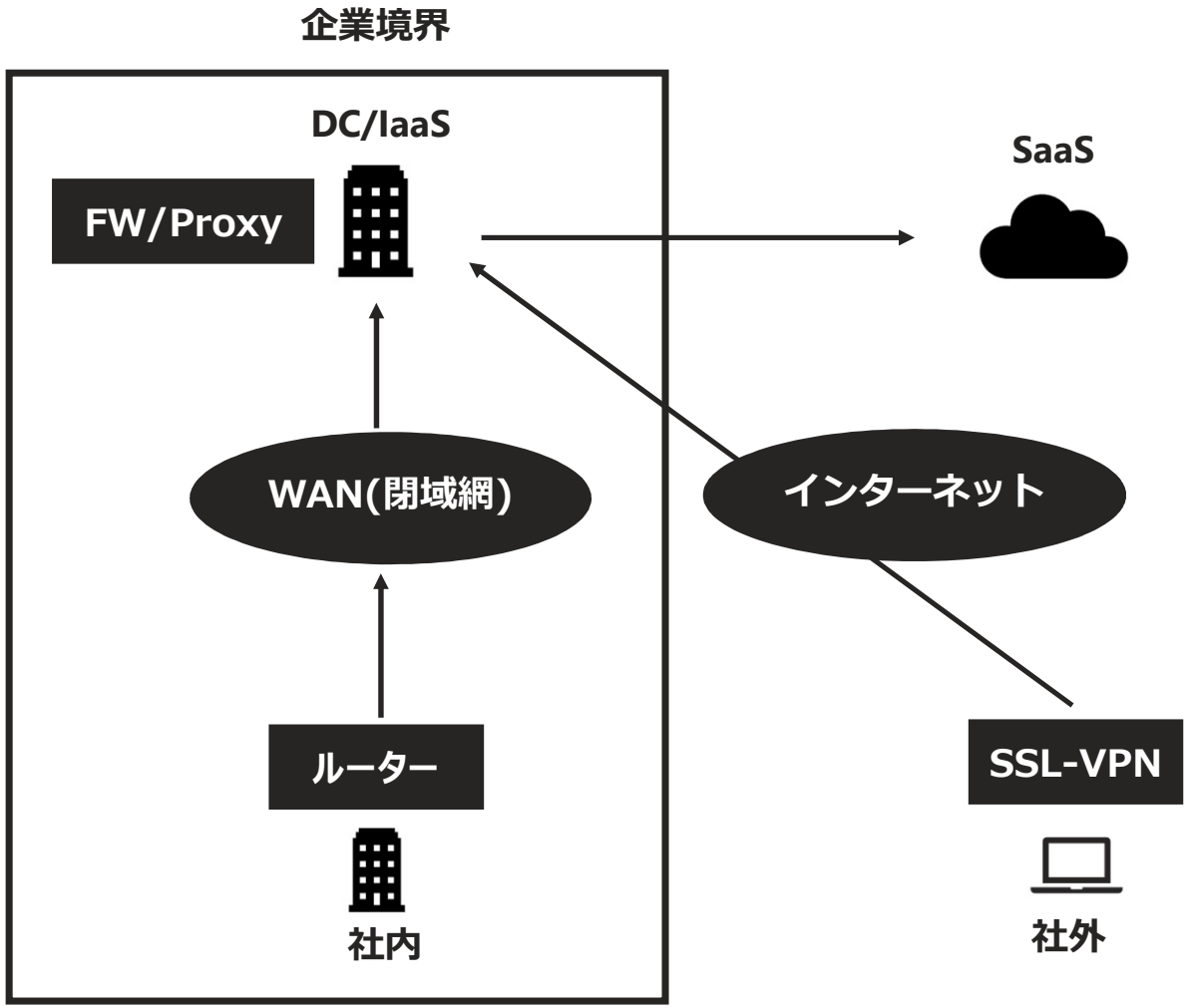
統合的なゼロトラストサービス提供
ログ監視含めた運用支援

コンサル → 提案 → POC検証 → 設計構築 → 運用保守 → 最適化

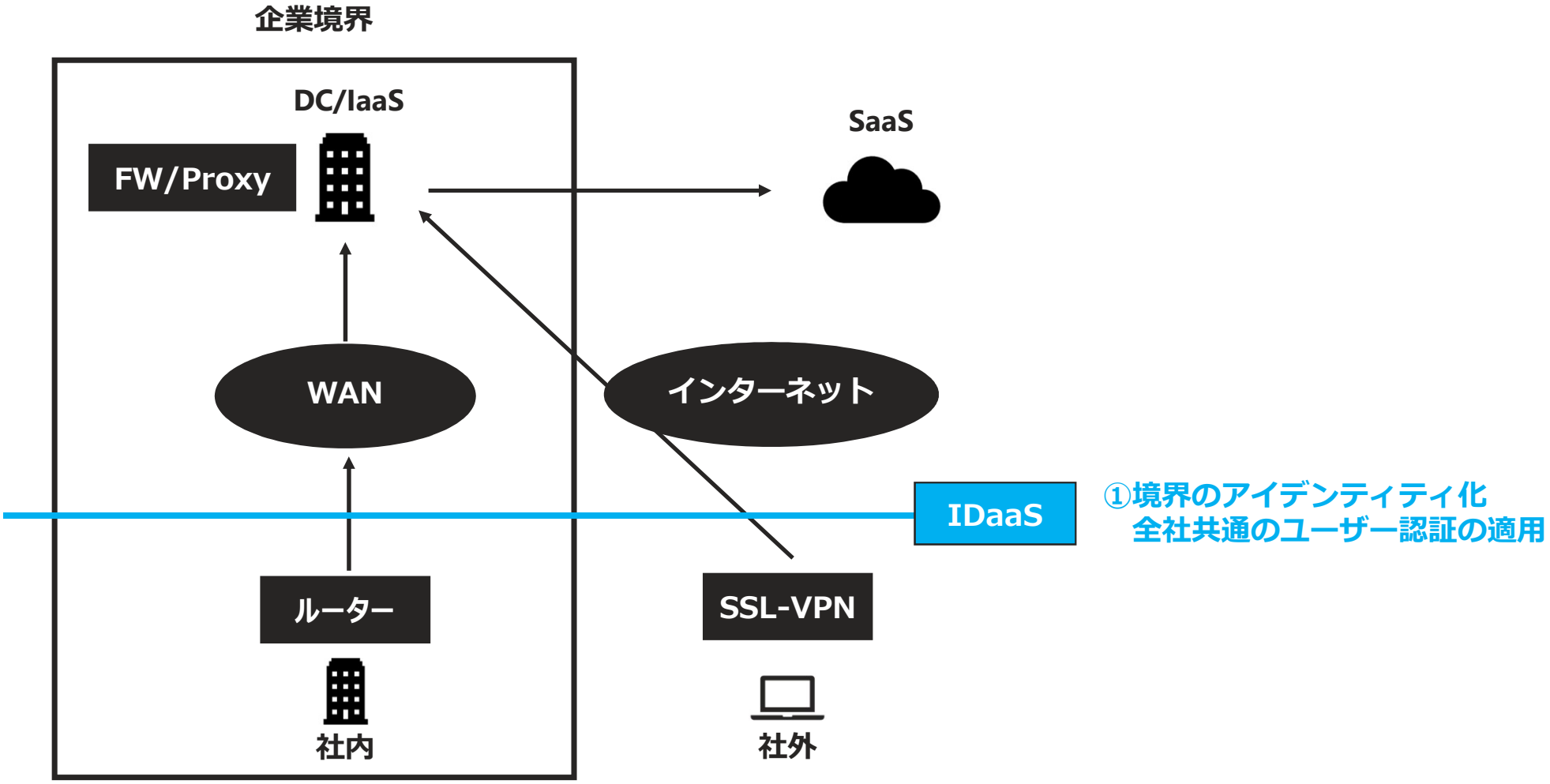
エンドユーザー様

ゼロトラスト化の移行ステップ

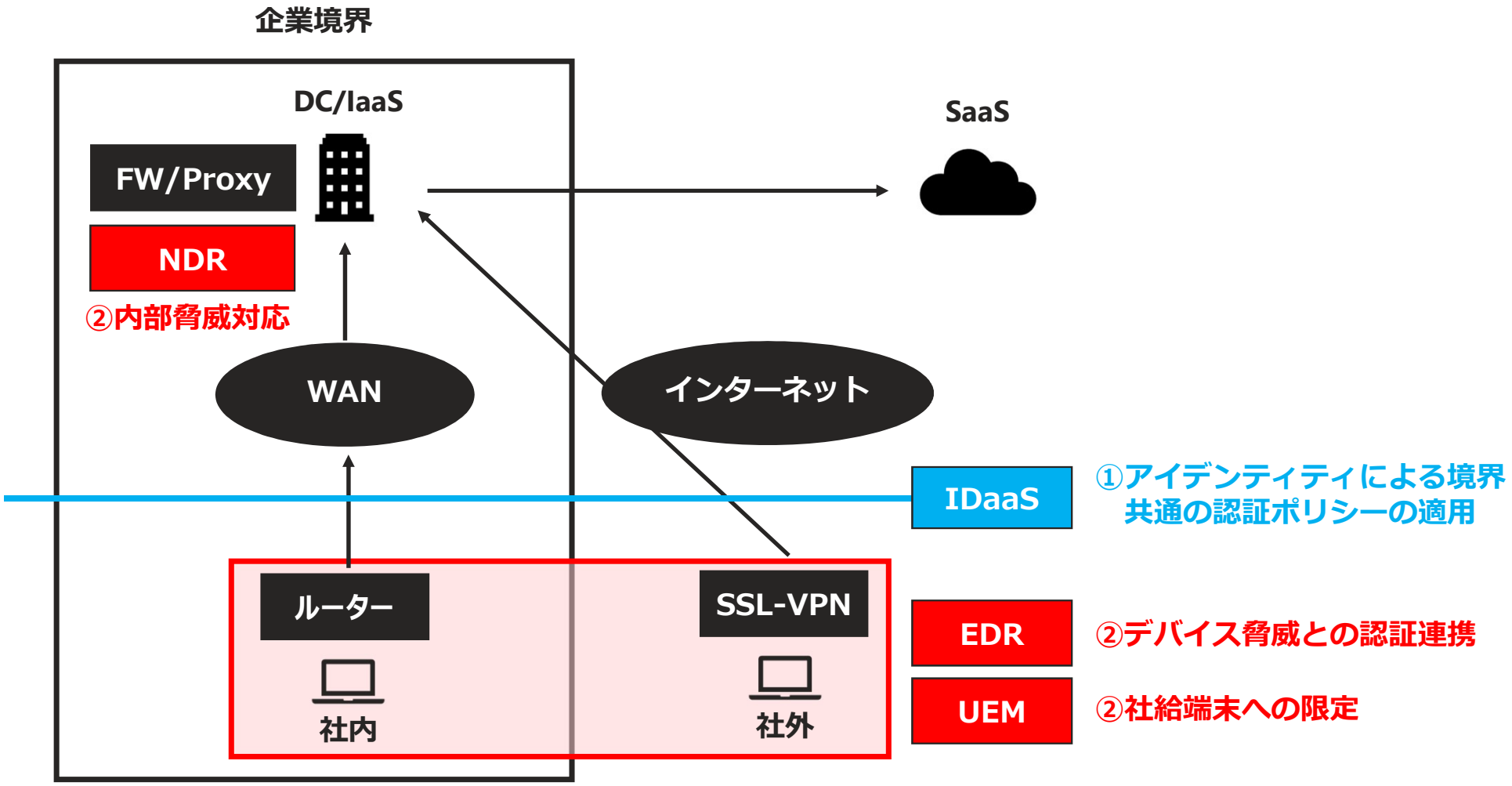
ステップ０：既存の企業環境



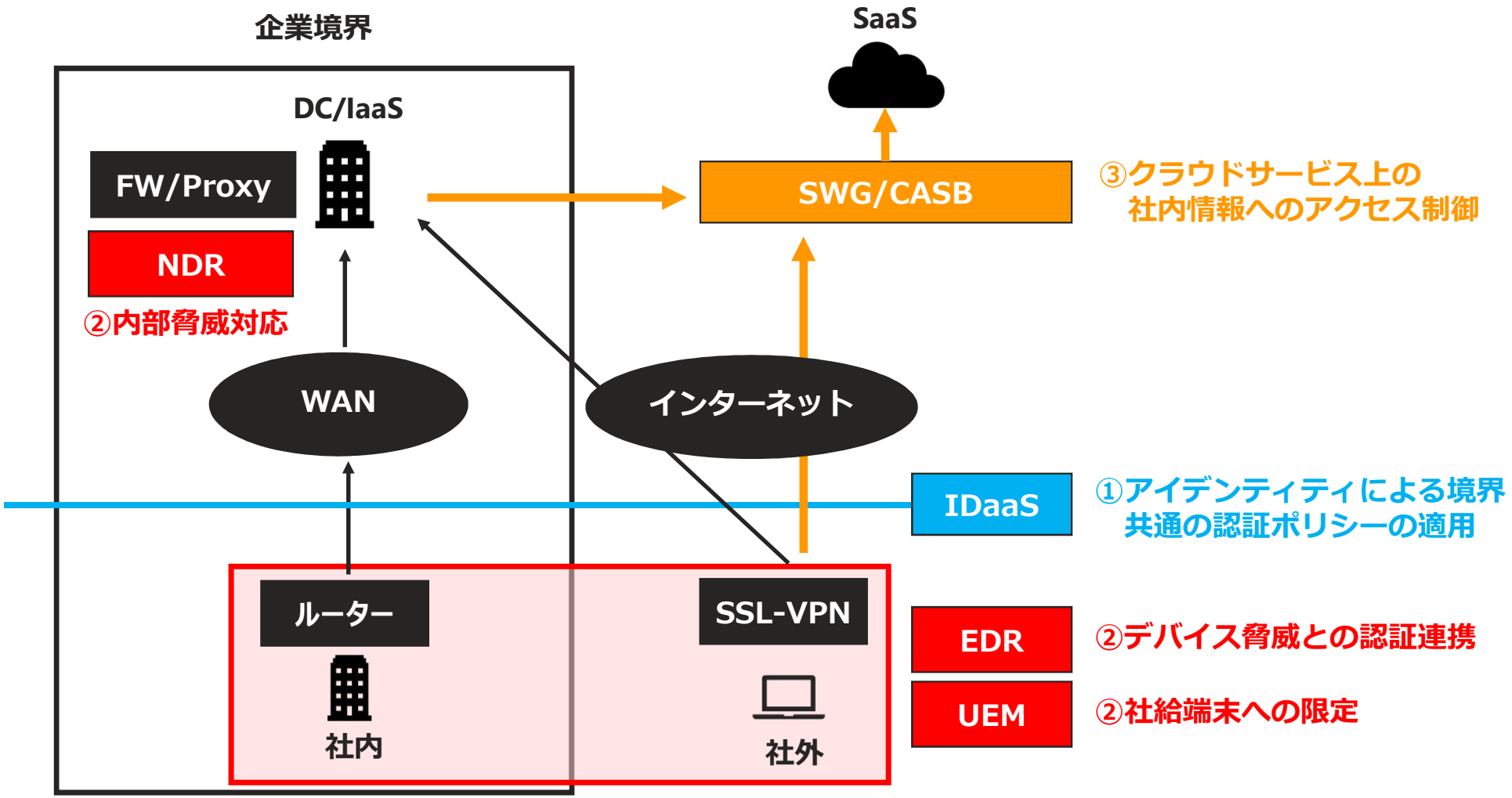
ステップ1：ユーザー認証基盤の整備(IDaaS)



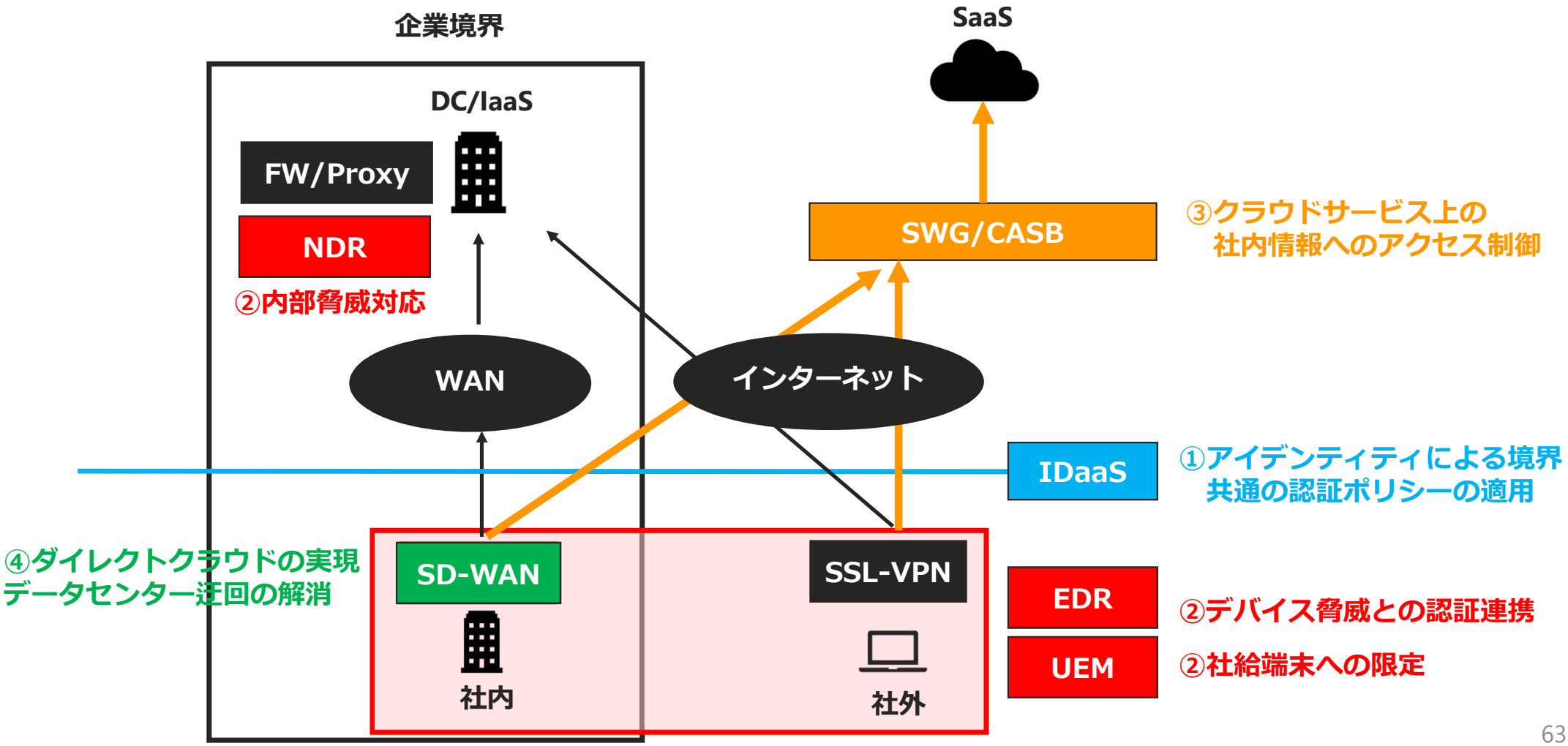
ステップ2：デバイストラストの実現(EDR/UEM)



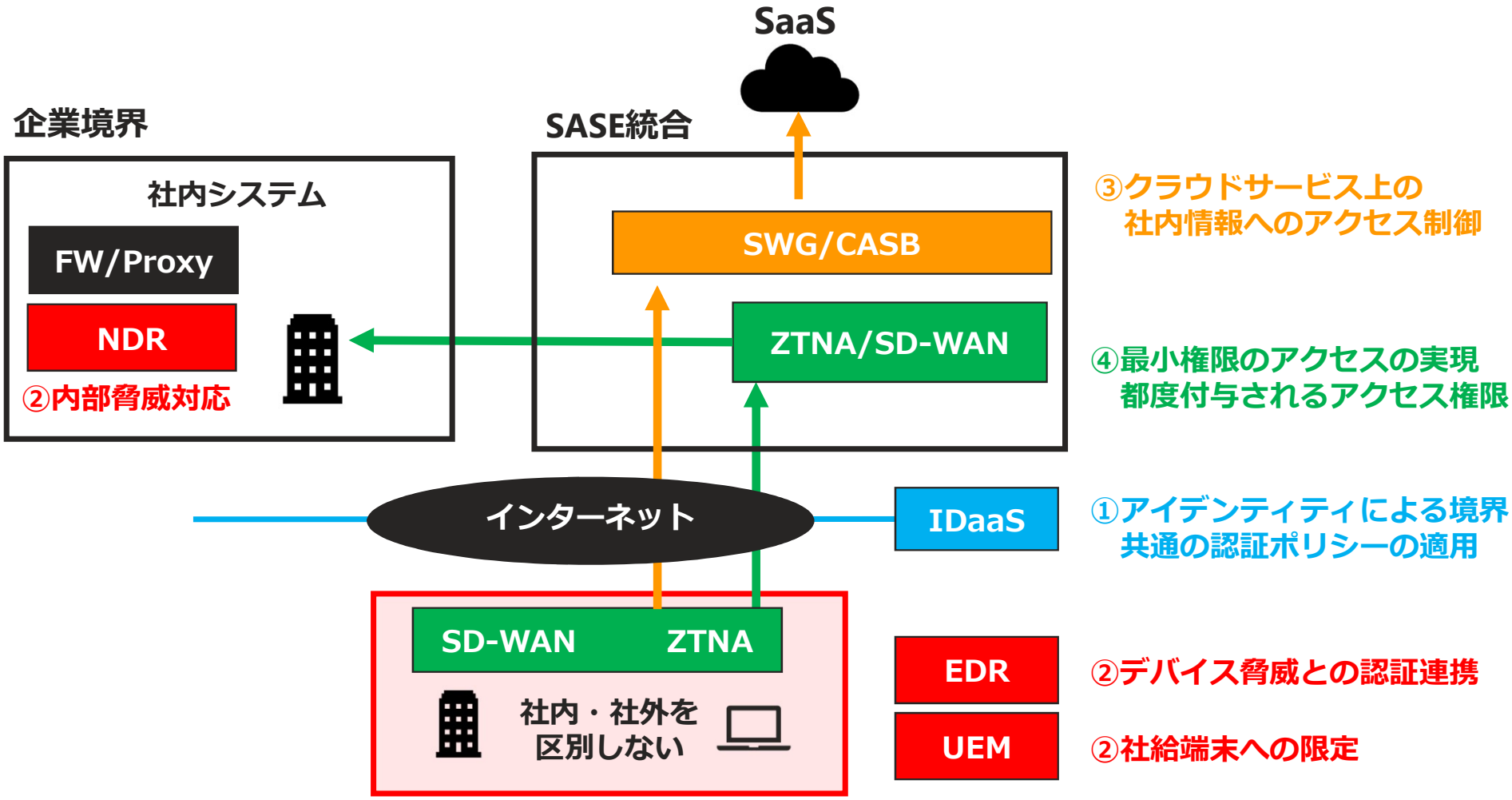
ステップ３：クラウド通信の保護（CASB）



ステップ4：拠点発通信のインターネットブレークアウト



ステップ5：アクセス経路の共通化（ZTNAの採用/VPN廃止）



付録
お客様環境の情報整理シート

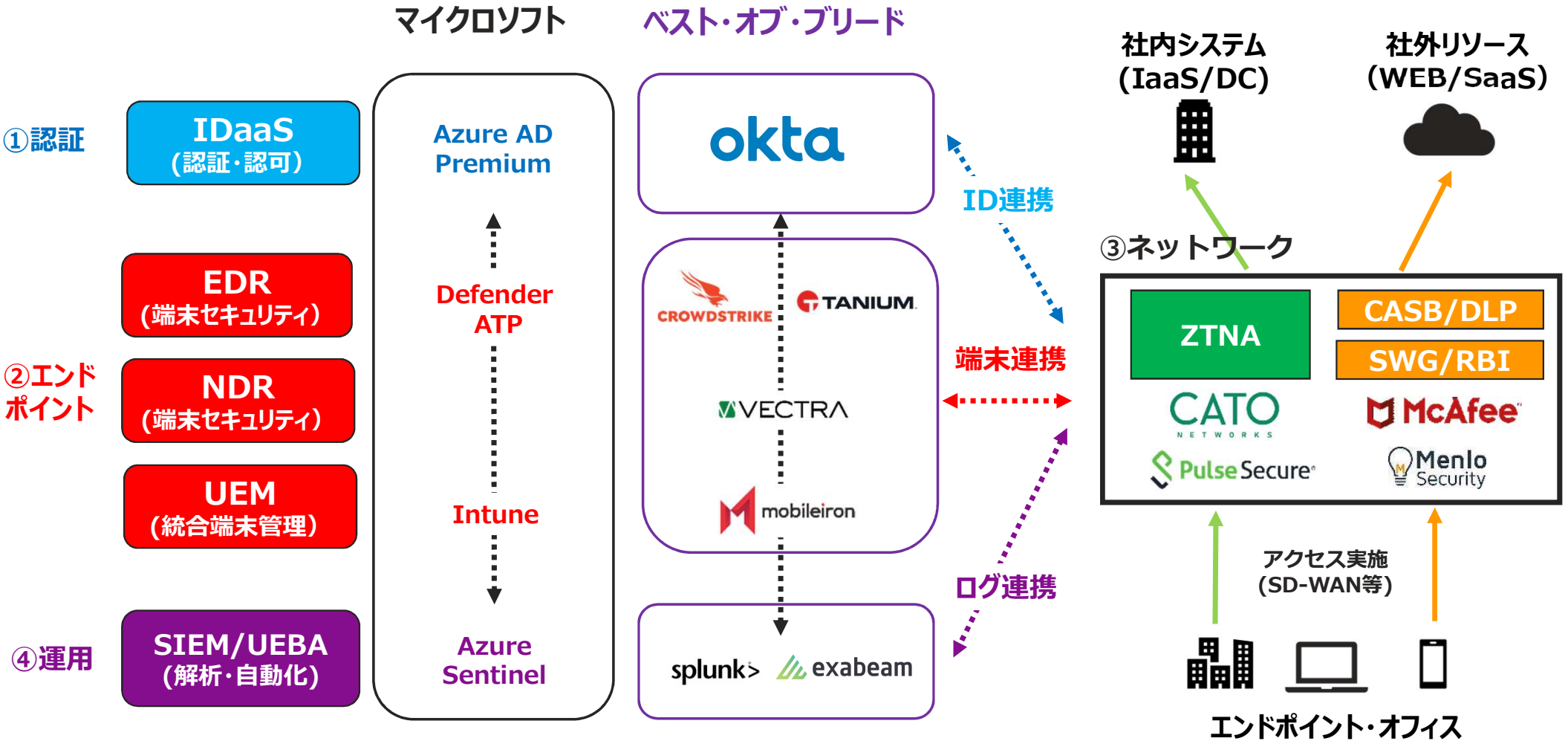
既存導入製品の情報整理シート

ゼロトラスト化の4つの要素		御社導入済み製品	カテゴリー	マクニカ取り扱い製品		マクニカ非取り扱い
①認証・認可			IDaaS	Okta Auth0		Azure AD
②エンドポイント強化			EDR	CrowdStrike Tanium		Defender ATP
			NDR	Vectra		-
③ネットワーク・セキュリティのクラウド化	ネットワーク		SD-WAN	CATO	Silver Peak (Aruba)	Cisco VMware
			ZTNA		PulseSecure	Zscaler Netskope Paloalto Akamai
	セキュリティ		SWG/RBI		Menlo	
			CASB/DLP	McAfee		
④運用のゼロトラスト化 （可視化・解析・自動化）			SIEM	Splunk		
			UEBA	Exabeam		
			SOAR	Phantom(Splunk)		

記入例

ゼロトラスト化の4つの要素		御社導入済み製品	ゼロトラ商材	マクニカ取り扱い製品		その他ソリューション
①認証・認可		Active Directory	IDaaS	Okta Auth0		Azure AD
②エンドポイント強化		アンチウィルス	EDR	CrowdStrike Tanium		Defender ATP
		パケット解析装置	NDR	Vectra		-
③ネットワーク・セキュリティのクラウド化	ネットワーク	ルーター	SD-WAN	CATO	Silver Peak (Aruba)	Cisco VMware
		SSL-VPN	ZTNA		PulseSecure	Zscaler Netskope Paloalto Akamai
	セキュリティ	各種多層防御 FW Proxy サンドボックス　等	SWG/RBI		Menlo	
			CASB/DLP	McAfee		
④運用のゼロトラスト化 （可視化・解析・自動化）		ログサーバー	SIEM	Splunk		
		-	UEBA	Exabeam		
		-	SOAR	Phantom(Splunk)		

マイクロソフトソリューションとの相関図



現状を把握するチェックリスト①

1. リソース管理

- 重要な社内リソースをどのように定義しているか？（個人情報、人事情報、取引情報）
- リソースは、オンプレだけでなくクラウド上にも存在しているか？
- セグメント分けはされているか？（物理、仮想、ネットワーク、アプリケーション）

2. ユーザー認証

- どのような要素でユーザーが本人であるかを確認しているか？
- （弱）パスワード、ワンタイムパス、生体認証（強）
- ユーザーのコンテキスト（振る舞い・置かれている状況）を加味した認証は？
- どのようなツールでユーザー管理をしているか？（AD、IDマネージャーなど）
- ディレクトリ管理に課題はあるか？（複数、分散、バラバラなADなど）

3. デバイス認証

- どのようなデバイスに現状アクセスを許可しているか？（社給だけ、BYODも可）
- どのようなツールでデバイス管理をしているか？（MDM、UEM、VPN機能）
- デバイスの脅威保護は現在行っているか？（AV、EDR、NDRなど）

現状を把握するチェックリスト②

1. リソース管理

- 重要な社内リソースをどのように定義しているか？（個人情報、人事情報、取引情報）
- リソースは、オンプレだけでなくクラウド上にも存在しているか？
- セグメント分けはされているか？（物理、仮想、ネットワーク、アプリケーション）

2. ユーザー認証

- どのような要素でユーザーが本人であるかを確認しているか？
- （弱）パスワード、ワンタイムパス、生体認証（強）
- ユーザーのコンテキスト（振る舞い・置かれている状況）を加味した認証は？
- どのようなツールでユーザー管理をしているか？（AD、IDマネージャーなど）
- ディレクトリ管理に課題はあるか？（複数、分散、バラバラなADなど）

3. デバイス認証

- どのようなデバイスに現状アクセスを許可しているか？（社給だけ、BYODも可）
- どのようなツールでデバイス管理をしているか？（MDM、UEM、VPN機能）
- デバイスの脅威保護は現在行っているか？（AV、EDR、NDRなど）

有難うございました