ゼロトラスト ってなんだろう？

株式会社 クラウドネイティブ

目次

自己紹介

五戸 禎人 (gonoway)

Yoshihito Gonohe

Cloud Native Inc.

Cloud Security Architect

経歴

- セキュリティ製品のデプロイ（前職）
- MDM分野（Intune、Jamf）→育休（1年。CISSP取得）→ IDaaS分野（Okta、Azure AD等）

業務内容

- 情報システム部門へのコンサルティング
- 新製品の調査・検証

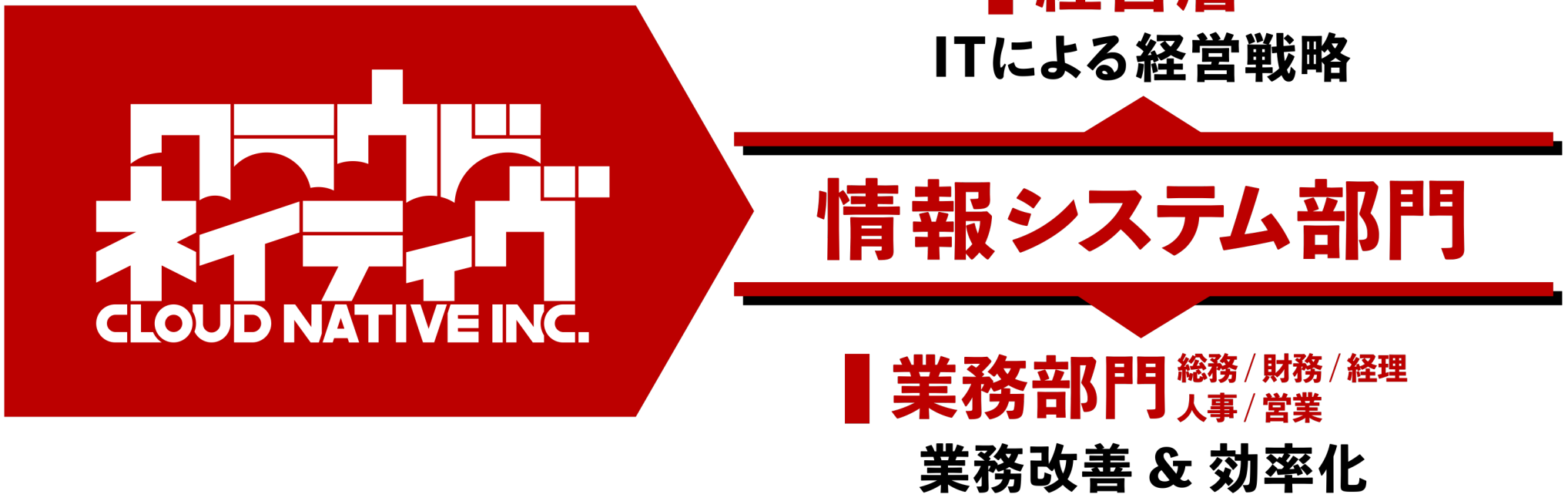
会社概要

社名	株式会社クラウドネイティブ　（Cloud Native Inc.）
設立	2017年5月
従業員数	29名
代表者	齊藤 愼仁
事業内容	情報システム部門へのコンサルティング クラウドコンピューティングに関わる全てのコンサルティング、設計、開発、構築及びそれらに関わる代理店業務

情報システムコンサルティング

情報システムは企業のコア　攻めのITへの変革

企業からITが無くなると事業継続が困難である今の時代、情報システム部門は企業のコアと言えます。
ITによって自在に変化適応できる組織へ再設計し、企業価値を最大化するご支援をします。



実績

クラウドネイティブ CLOUD NATIVE INC.

スタートアップからグローバルエンタープライズまで

製造業

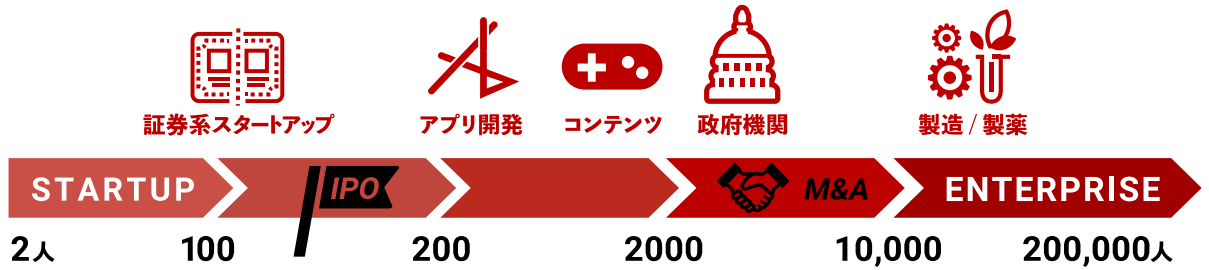
- 年間売上1兆円規模のグローバルエンタープライズ
- 中長期IT戦略の立案支援と実行支援
- クラウド活用に向けた組織・体制の構築と運用技術支援
- サービスインフラ、社内基幹システムのセキュリティリスク監査

金融業

- 中長期IT戦略の立案支援と実行支援
- グローバル展開に向けたインフラ基盤の構築支援
- サービスインフラにおけるAWS活用支援とセキュリティ対策支援
- 情報システム部門の先端ソリューションを活用した業務効率化支援

アプリ

- 国内売上トップのソーシャルアプリプロバイダー
- サービスインフラにおけるセキュリティ監査/認証取得支援
- 社内ITガバナンス強化に向けたインフラ基盤の構築支援
- 外部攻撃の応急対応支援と恒久対策の立案と実行支援



TEPCO FUJITEC NIKKO CHEMICALS SHIONOGI LIXIL Link to Good Living 経済産業省 Ministry of Economy, Trade and Industry 文部科学省 JAPAN INFRA WAYMARK

ADK 株式会社ADKクリエイティブ・ワン Akatsuki ABEJA mixi GROUP Money Forward folio Power Solutions hey RakSul ALL CONNECT bellFace The Pokémon Company TOEI ANIMATION Since 1956

私たちの価値

クラウドネイティブ
CLOUD NATIVE INC.

- ベンダーフリー
- 組織を育成 自立を目標
- 実現可能な設計とロードマップ

クラウドネイティブは、
オンプレミスのシステムから育ったエンジニアが、
国内外に存在する全てのクラウドサービスを、
特定の代理店やベンダーに依存せず、
フラットな立場で評価し、
企業のビジネスサイクルを加速させる
コンサルティングを主力として提供しております。

Information Technology →

Business Technology

利便性とセキュリティを両立するIT基盤

クラウドネイティブ CLOUD NATIVE INC.

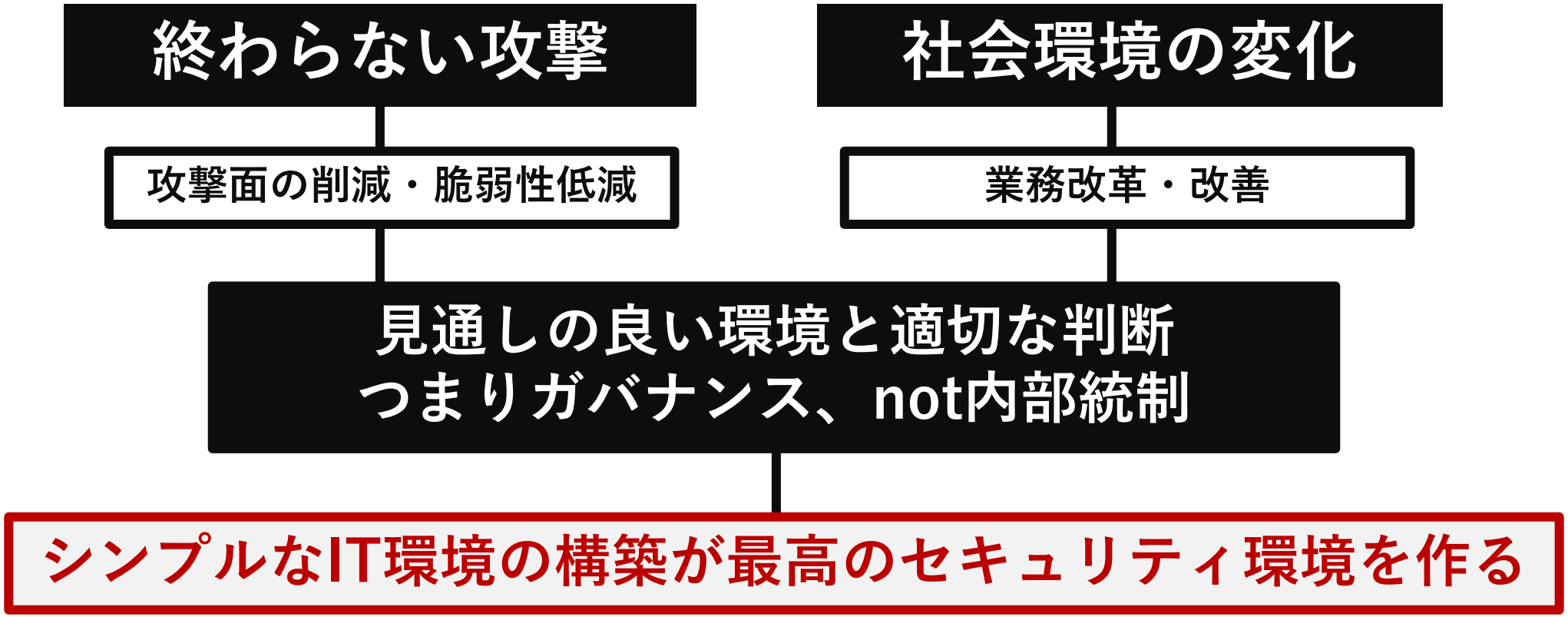
ゼロトラストネットワークの思想を取り入れ

利便性とセキュリティを追求した次世代の働き方を実現するIT基盤を構築

ゼロトラスト の おさらい

0. IT環境をシンプルにしよう
1. 脆弱性のない環境を構築する
2. 適切な構成を設定し管理する
3. 動的な検証とポリシーの構築
4. セキュリティをITに組み込んでいく

IT環境をシンプルにすることを目標にすると…



01 脆弱性のない環境を構築する

サイバーハイジーンを実現するには？

事故の発生する原因：リスクマネジメントの基本

事故の発生

脅威 ✖ **脆弱性**

脅威は外部にあるためコントロールできず、抑制は難しい。ゼロにすることはできない。　（抑止）

セキュリティ対策

コスト

事故が発生するのは
脅威と脆弱性が合致した時

脆弱性は組織の内部にあるためコントロール可能。

脆弱性をコントロールすることを
セキュリティと呼ぶ（防止）

セキュリティ対策にはコストが発生するため、
費用対効果を考慮する必要がある。

いつでも脆弱性のない状態を作る

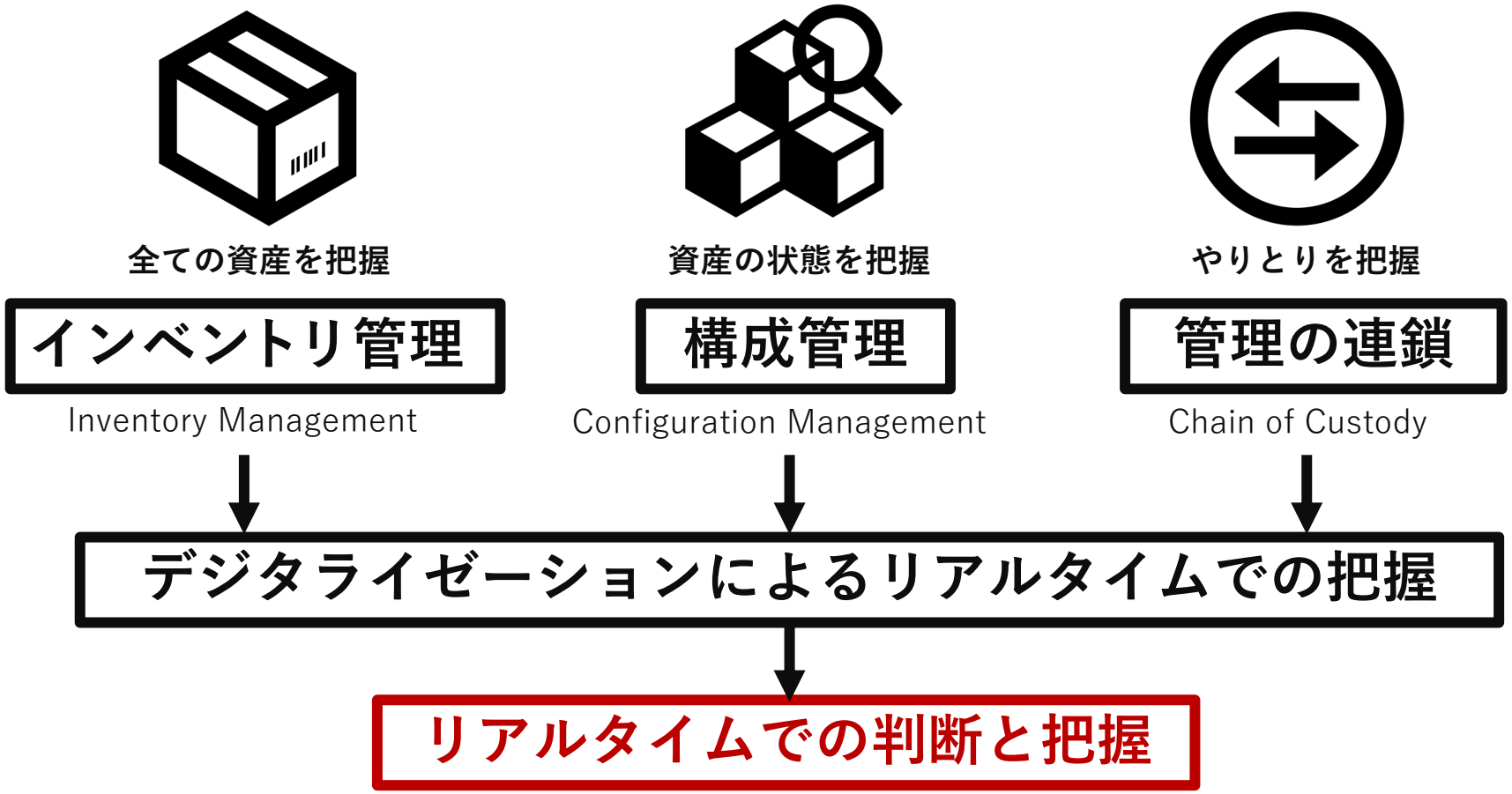
サイバーハイジーン

資産をすべて管理し

その状態を把握することで

期待される状態を維持する

現場をすべて理解するための仕組みづくり



02 適切な構成を設定し管理する

Mis-Configurationをコントロールしたい

Mis-Configurationは単なる設定ミスではない

資産の状態を把握

構成管理

Configuration Management

・場所/管理状態
・OS/アプリのバージョン
・設定など…

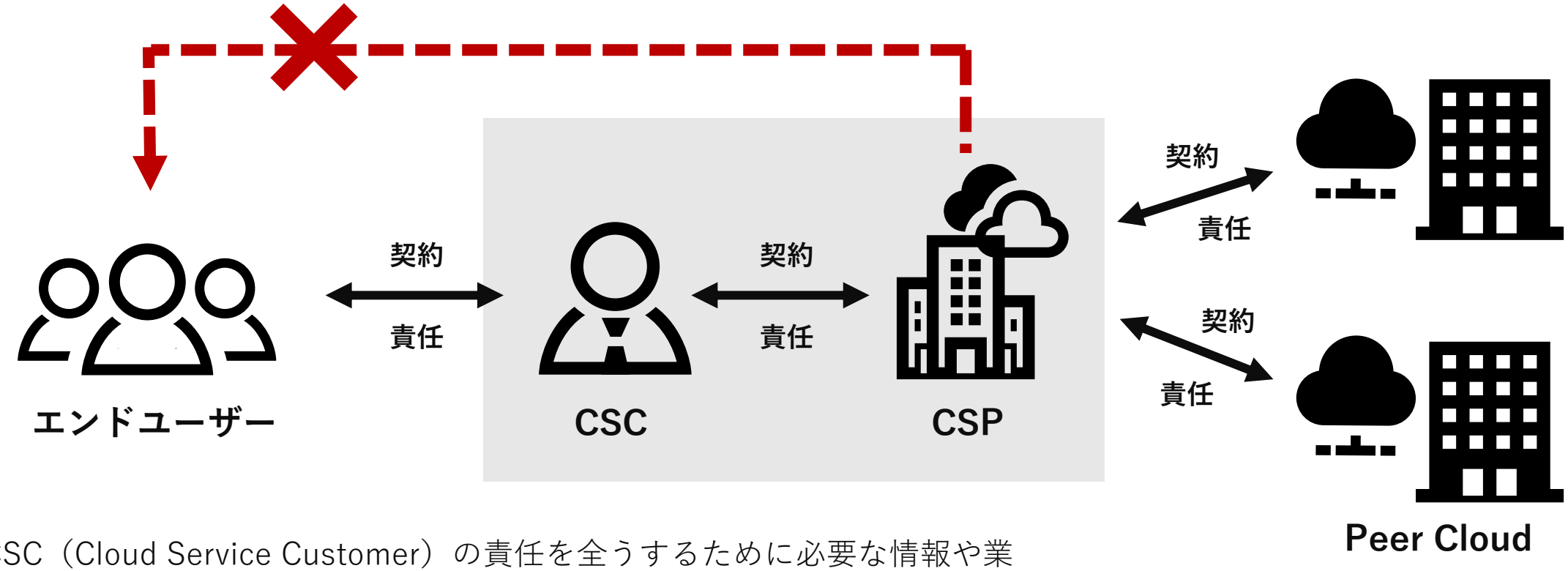
→ システムや資産の期待される状態

→ 期待される状態になっていない Mis-Configuration

クラウド上の様々な機能が期待された状態になっているかどうか確認するためには、構成管理を厳密に行う必要がある。
セキュリティの課題ではこれらを、 CSPM（Cloud Security Posture Management）と呼ぶこともある。

すべての資産の構成（Configuration）をリアルタイムに把握するためには、デジタライゼーションが必要になり、クラウドの利用は避けられない。

クラウドサービスにおけるShare Responsibility



CSC（Cloud Service Customer）の責任を全うするために必要な情報や業務をCSP（Cloud Service Provider）が提供もしくは支援する。

つまり、CSCが自組織もしくはエンドユーザーに対して負う責任が明確にならない限り、CSPへの要求事項も定まらない。

03 動的な検証とポリシーの構築

ゼロトラスト ってなんだろう？

ゼロトラスト ネットワークとは何か？

ゼロ　トラスト　ネットワーク

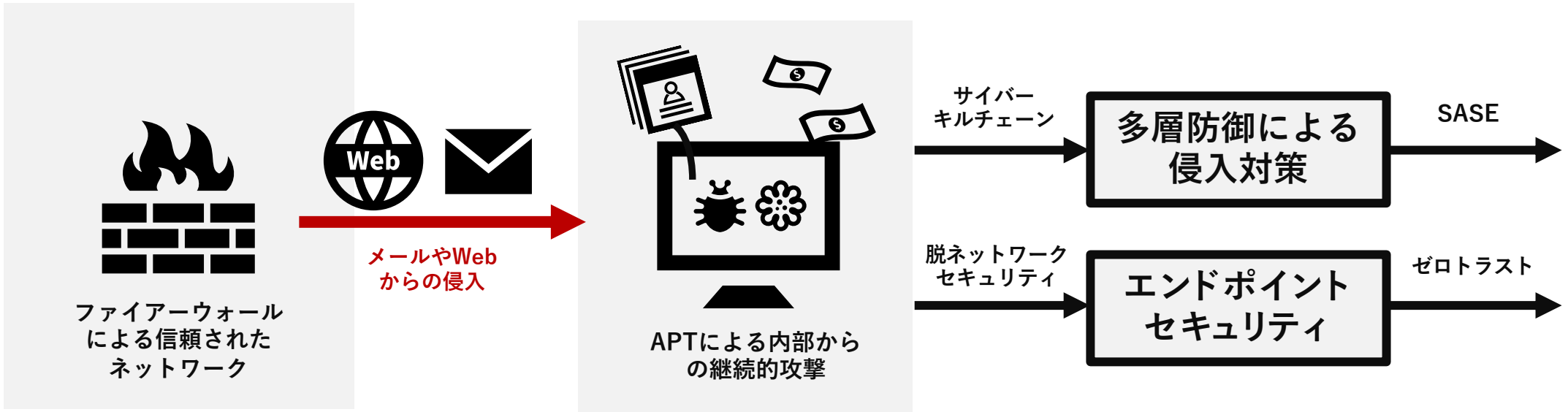
ファイアーウォールで守られたローカルネットワーク

信頼できるネットワークはゼロ

ゼロ　トラスト ~~ネットワーク~~

ネットワークだけでなく全てのものを信頼できる状態にしたい！

APT攻撃による境界型防御の限界



TCP/IP v4を利用するにあたって
ネットワークのアクセス制御を
ファイアーウォールで行っていた。

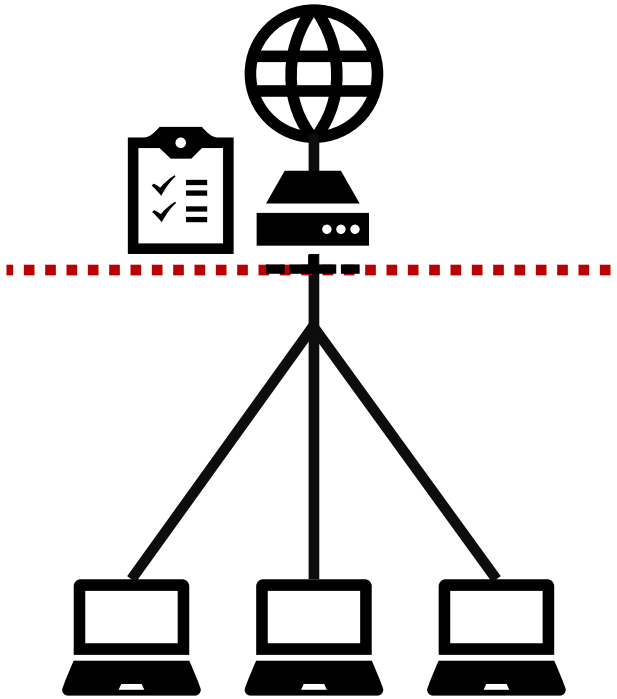
2008年ごろ

アプリケーション層からの攻撃は
フィルタリングできず、新たな
フィルタリングを検討しなくては
ならなくなった。

2010年ごろ

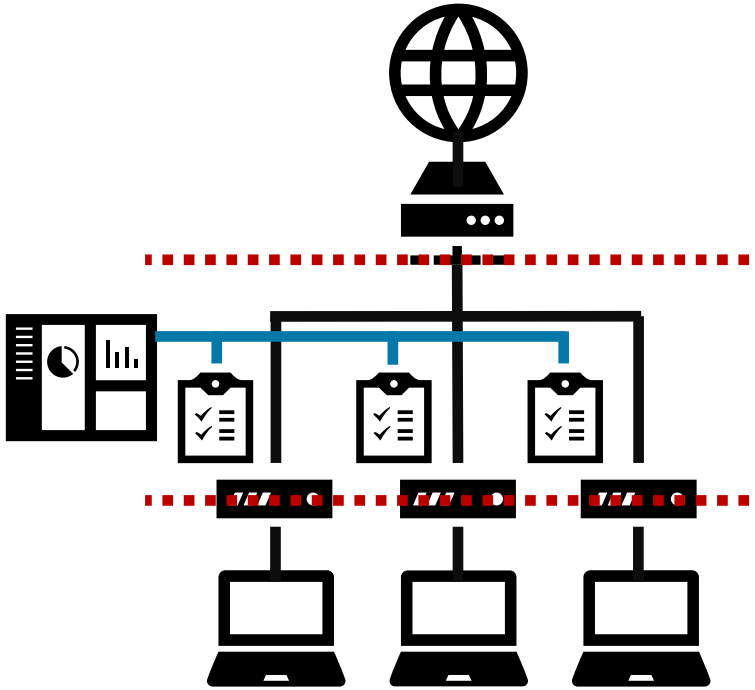
ネットワークセキュリティを拡張する形と
エンドポイントセキュリティを充実させる
形の2つに分かれ、SASEとゼロトラスト
につながっていく。

境界はエンドポイントへ



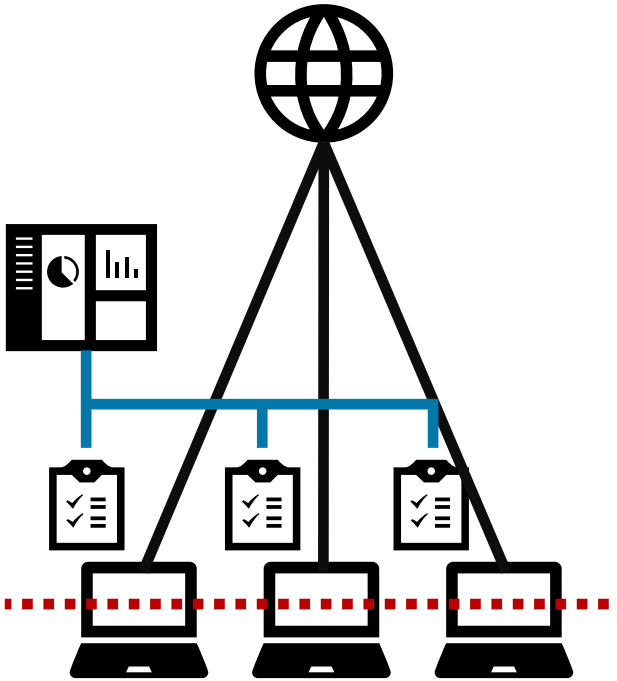
典型的な境界型防御

ファイアーウォールによって配下のPCやサーバは共通のセキュリティポリシーが適用される。結果として、一番厳しいポリシーが全てに適用されるが、同時に、全てが甘くなる。



マイクロセグメンテーション

個別のポリシーを適用するために端末単位にファイアーウォールを設置。ポリシーマネージャから個別のポリシーを配信する。
SDNを使ってさらに効率化した。



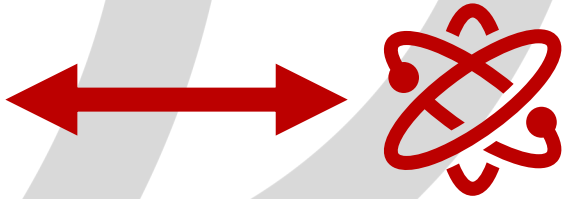
ゼロトラスト（エンドポイントセキュリティ）

端末の中にファイアーウォールが導入されたことで、直接インターネットに接続しても問題ない状態を作り、さらに効率化できるようにした。

エンドポイントセキュリティの発展

ゲートウェイソリューションからの脱却

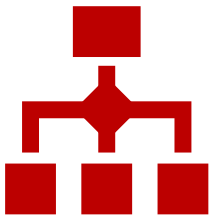
ネットワーク上のセキュリティサービスは
全て端末に持ってくることができるようになった。



脅威インテリジェンスによる
リアルタイム保護

ビルドインセキュリティ機能

- ファイアーウォール
- URLフィルター
- CASB など



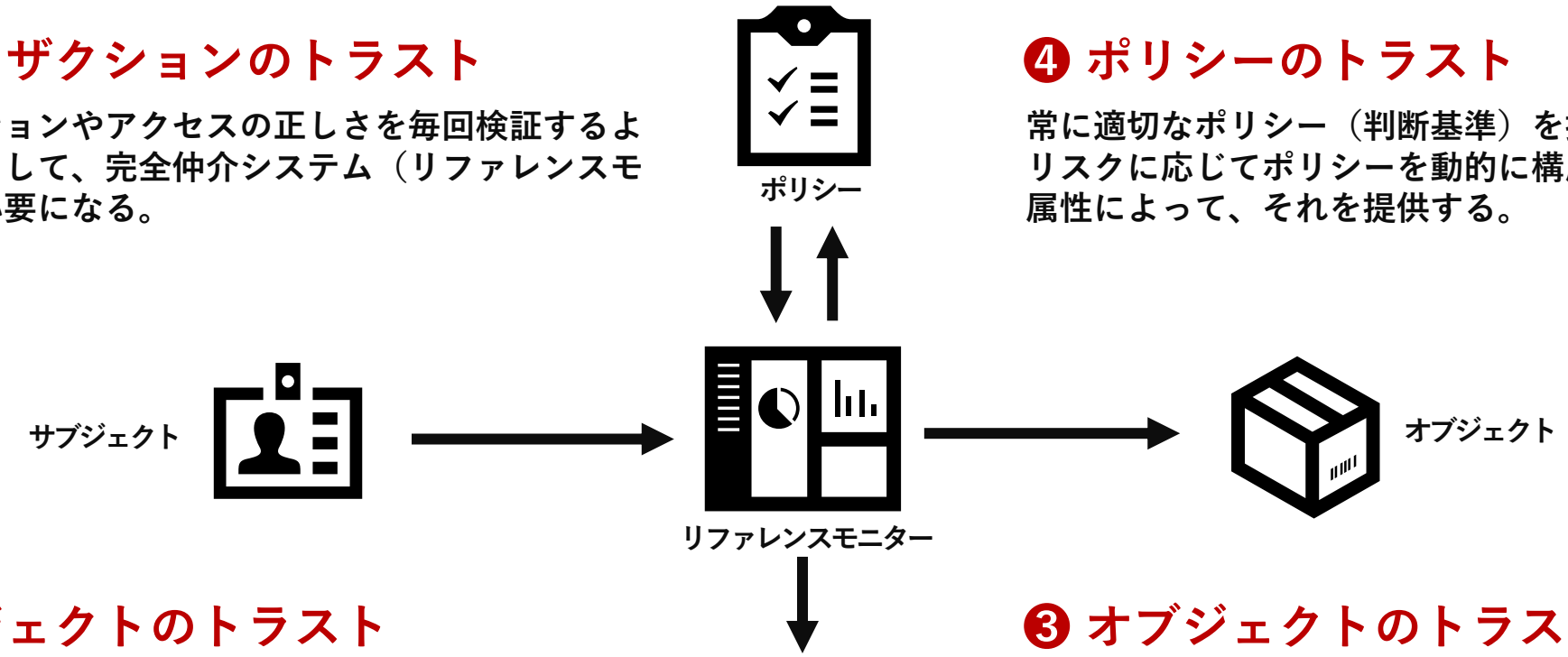
セキュアOSによる完全仲介

- UEBA（振るまい分析）
- 動的ポリシー制御
- サンドボックス など

ゼロトラストの実践のために

❶ トランザクションのトラスト

トランザクションやアクセスの正しさを毎回検証するような仕組みとして、完全仲介システム（リファレンスモニター）が必要になる。



❷ サブジェクトのトラスト

アカウントがなりすましされていないこと、デバイスがルールに準拠していることなどを毎回検証することで、サブジェクトが適切な状態にあるかどうかを判断する。

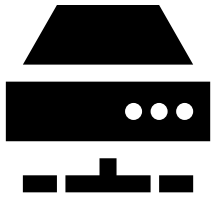
❸ オブジェクトのトラスト

オブジェクトが適切な状態になっていることを構成管理システムで判断する。もしもオブジェクトが適切な状態でない場合にはすぐに元に戻せるようにしておく。

❹ ポリシーのトラスト

常に適切なポリシー（判断基準）を提供するために、リスクに応じてポリシーを動的に構成し、サブジェクトの属性によって、それを提供する。

完全仲介を行う場所で取れるデータが変わってくる



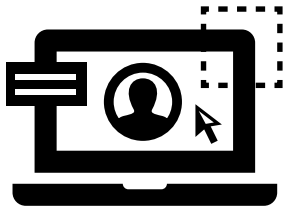
ネットワーク

ネットワークを集約して、出口と入り口を一つにすることで、完全仲介の仕組みを構築する。

ファイアウォールの設定

- ネットワーク属性
- イベント

AND/OR



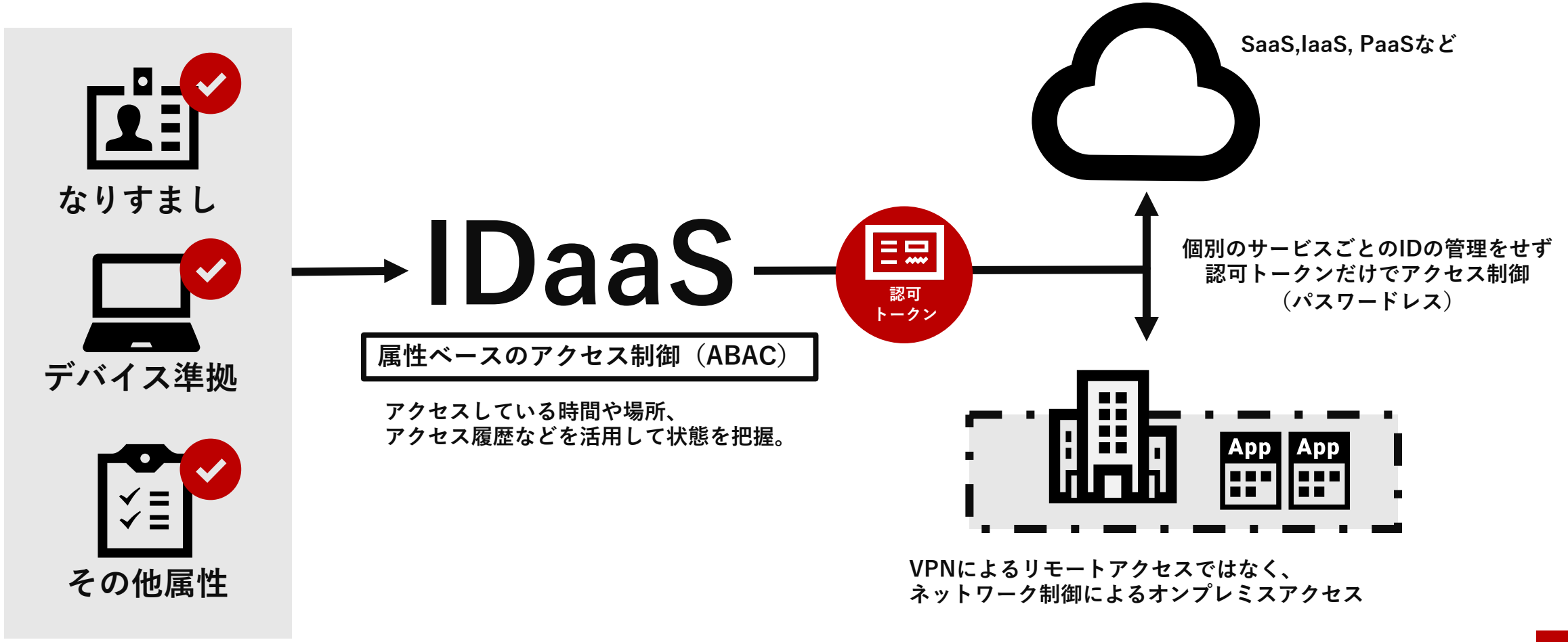
ユーザー・エンティティ

ID管理サービスで、ユーザーやエンティティを管理し、全てのアクセスを仲介する。

アクセス制御ポリシー

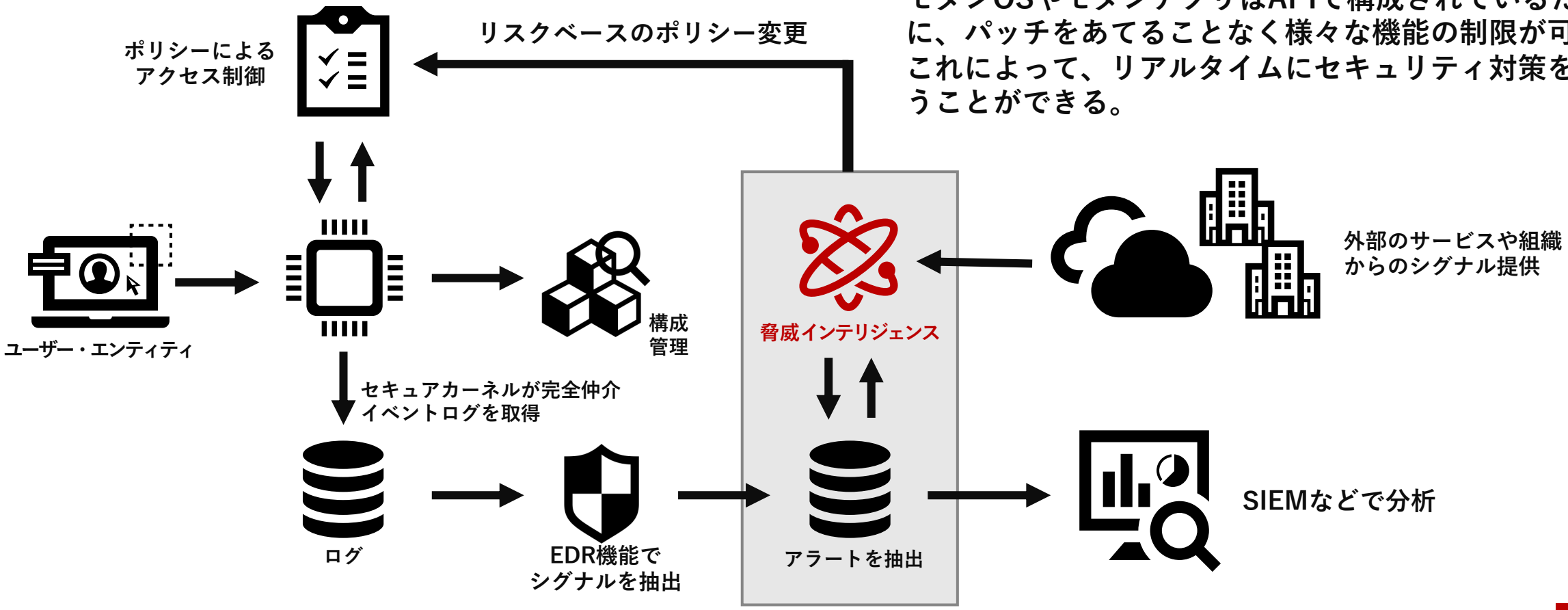
- ユーザー
- エンティティの属性
- イベント

IDaaSによるクラウドとオンプレミスの統合管理



EDRとIDaaSの連携による動的ポリシー制御

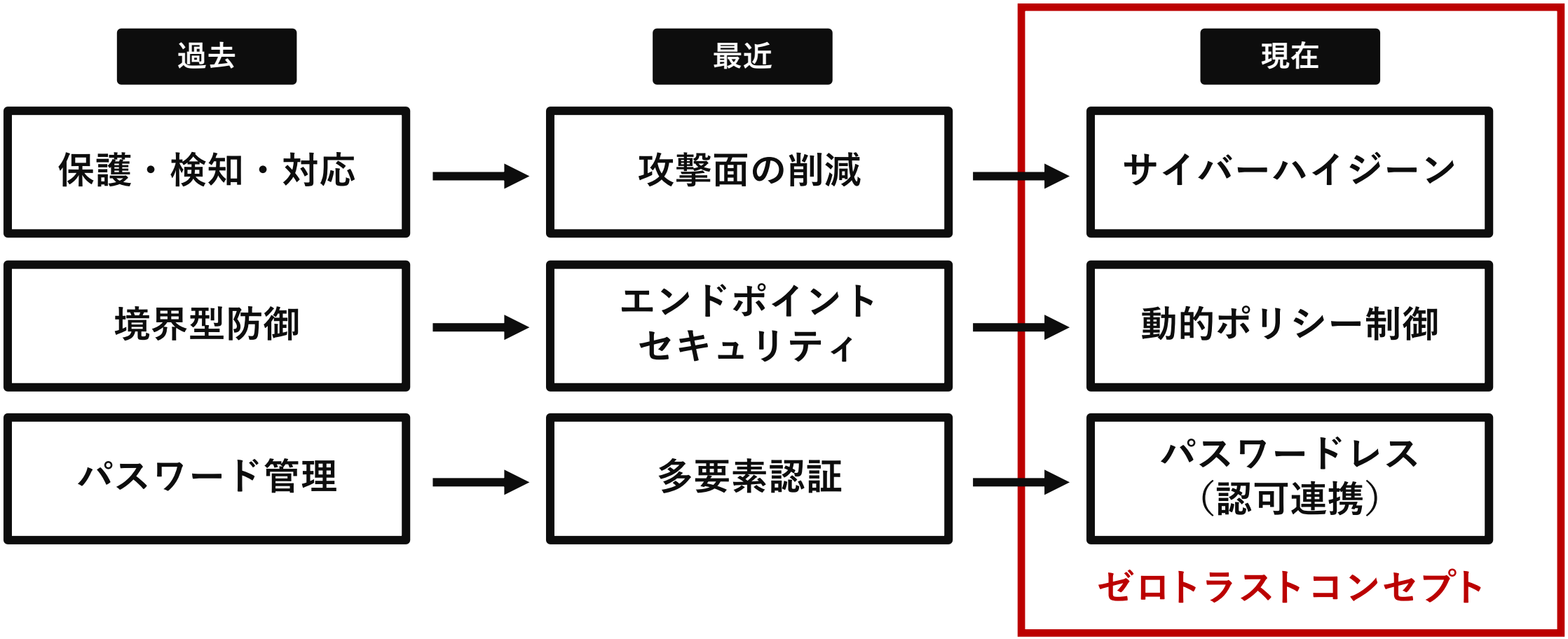
モダンOSやモダンアプリはAPIで構成されているために、パッチをあてることなく様々な機能の制限が可能。これによって、リアルタイムにセキュリティ対策を行うことができる。



04 セキュリティはITに組み込まれていく

後付けなしで予算も一定　シンプルな環境

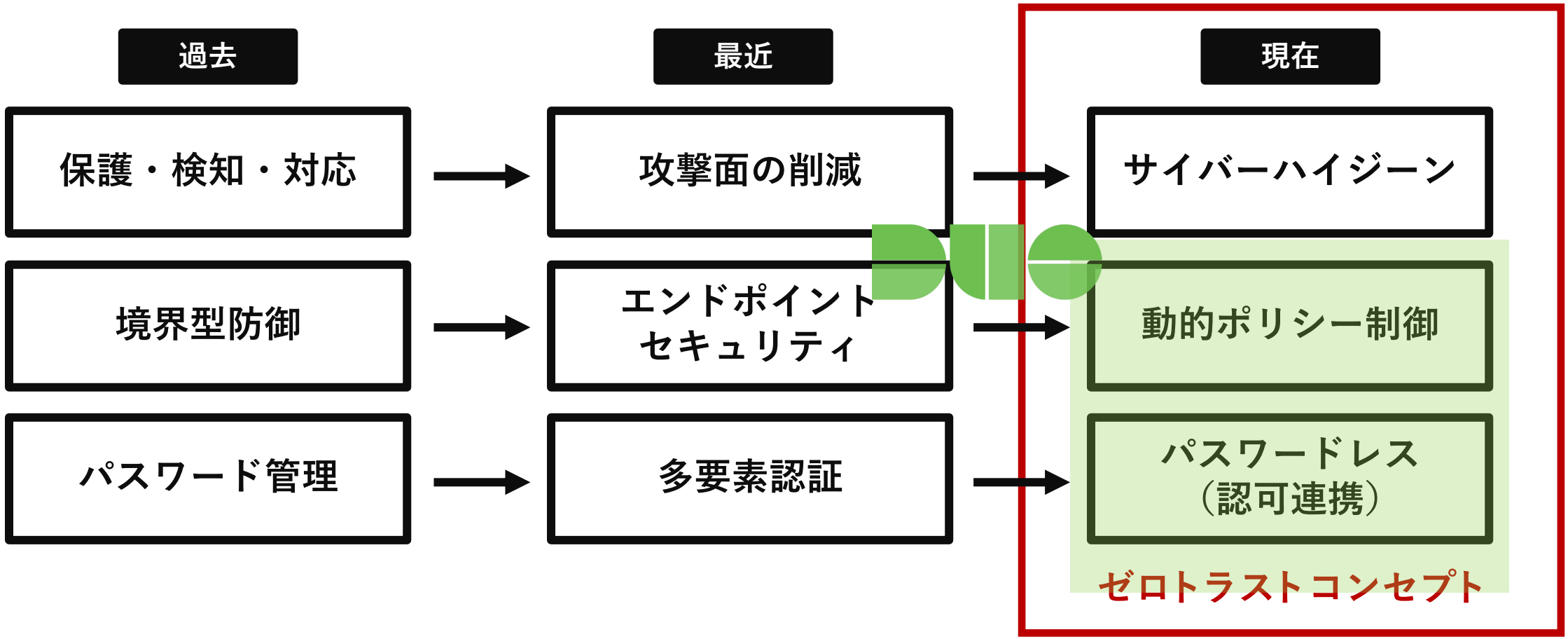
サイバーセキュリティの変化



クラウドネイティブ
CLOUD NATIVE INC.

Cisco Secure Access by Duo を使ったアプローチ

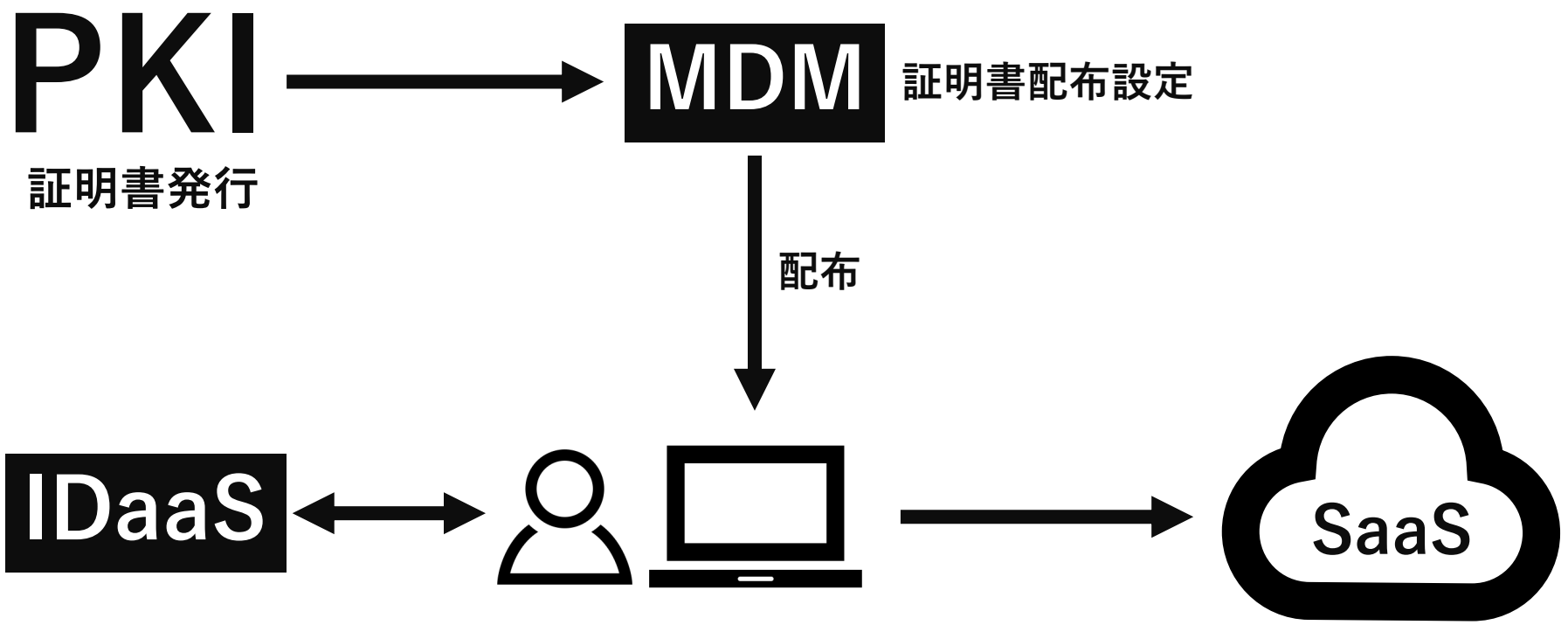
サイバーセキュリティの変化



Cisco Duoの特徴

1. 証明書だけではなくアプリケーションの選択肢がある
2. デバイスの状態をみれる
    a. EDRとの連携によるデバイス侵害のチェック
    b. ハードウェアの暗号化状態
    c. OSのバージョン
    d. ブラウザのバージョン 他.

デバイス認証の1つのパターン



証明書が存在するかどうかでアクセス可否を判断する

いろいろと難点がある

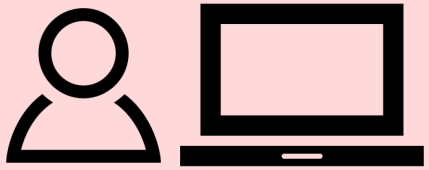
PKI

証明書発行/管理が手間

MDM

MDMや資産管理ソフトによっては
証明書を配れない

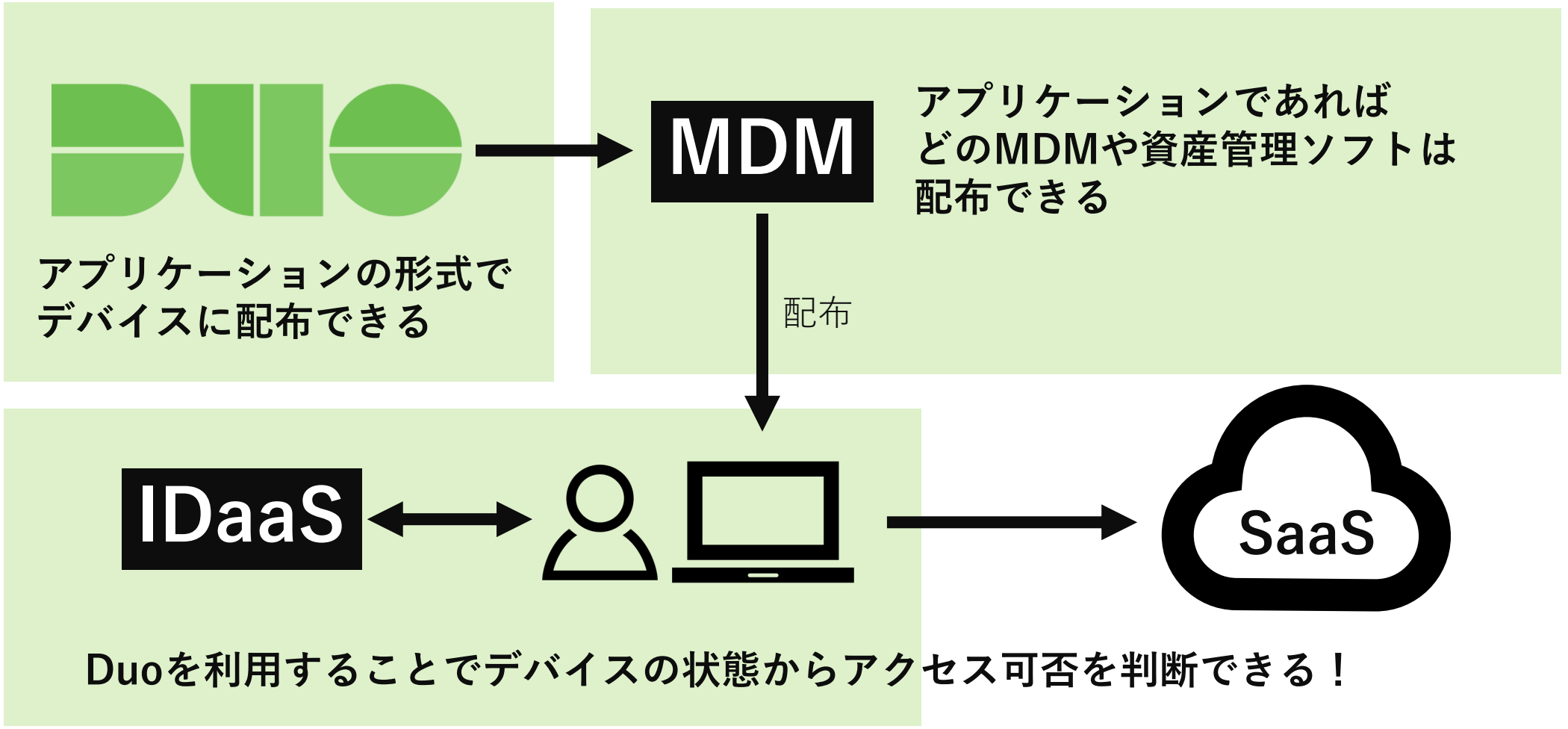
IDaaS



SaaS

デバイスの状態からアクセス可否を判断できない

Duoはデバイスの状態も確認できる



まとめ

Duoで信頼を積み上げよう

1. ゼロトラストはエンドポイントセキュリティ
2. ゼロトラストは信頼の積み上げを行うもの
3. Duoはサブジェクトの信頼を積み上げるもの
4. DuoはIDaaSやMDMの環境に依存されにくい

https://cloudnative.co.jp

ITの世界だからこそ、人と人とのコミュニケーションを最重要視し、
全員が前を向いて楽しく仕事を進められる世界を作るのが最大のミッションです。

株式会社クラウドネイティブ
Cloud Native Inc.
設立：2017年5月
所在地：〒106-0032 東京都港区六本木1-4-5
アークヒルズサウスタワー 16F
代表電話番号：050-1791-0450
Eメールアドレス：info@cloudnative.co.jp

Thank you !!