ゼロトラストネットワークの現在と実装

2020/07/10

なぜゼロトラストなのか

ゼロトラストは歴史の積み上げ

- 2007年、ホストで防御すれば多層防御要らない説
- セキュリティの進化と攻撃の変化
- インターネット側に便利なサービス多すぎ状態
- コロナという強烈な強制力

ゼロトラストとは何なのか

- 徹底的なマイクロセグメンテーション
- 全アクセス拒否という大前提
- どうやってアクセス許可するかという考え方
- セキュリティモデルであり設計の指針
- ゼロトラスト対応製品など存在しない

ゼロトラストなぜやりたいのか

- 仕事でインターネットを使いたいから
- 仕事でインターネットを使いたいから
- 仕事でインターネットを使いたいから

ゼロトラスト

常に評価されるトラスト(信頼)を付与することで
リソースを保護するサイバーセキュリティの規範。

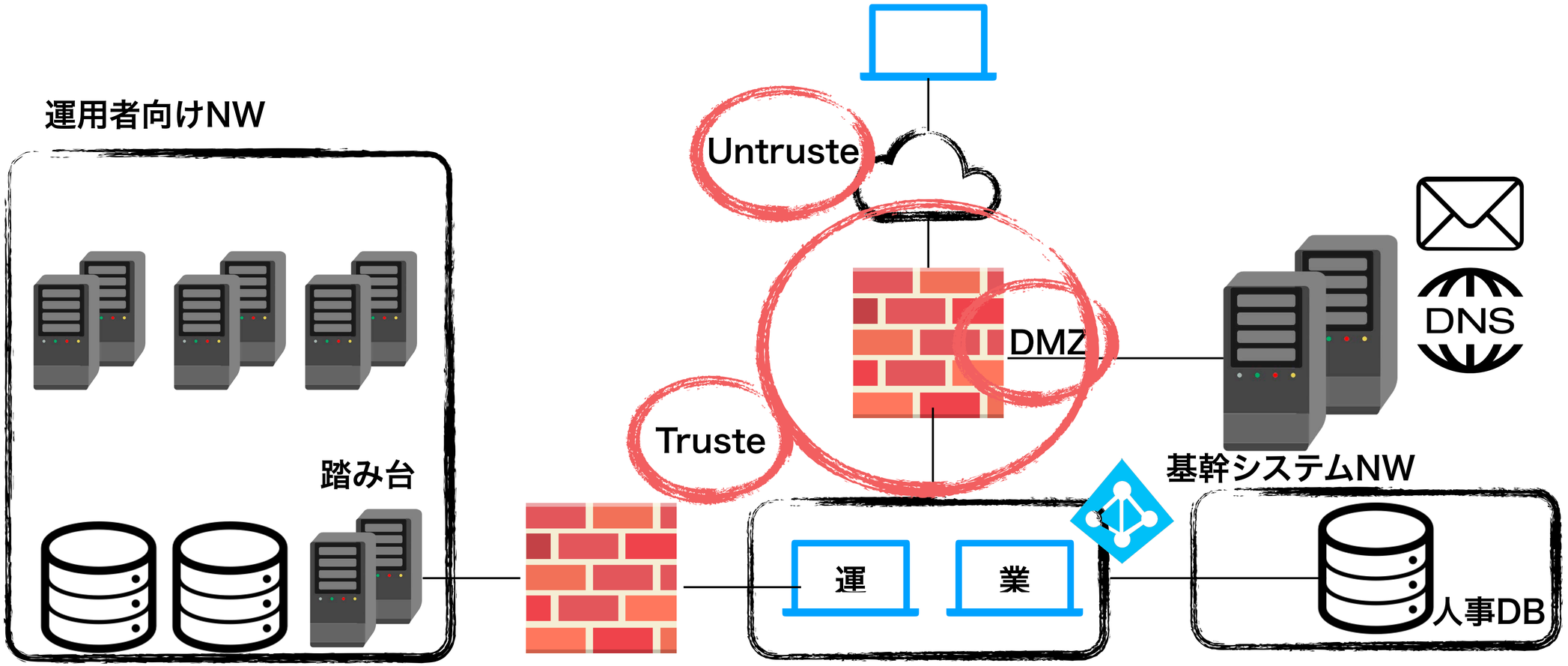
ゼロトラスト

リクエスト毎の適切なアクセス可否を、
適用する際の不確実性を低減する
考え方の集合

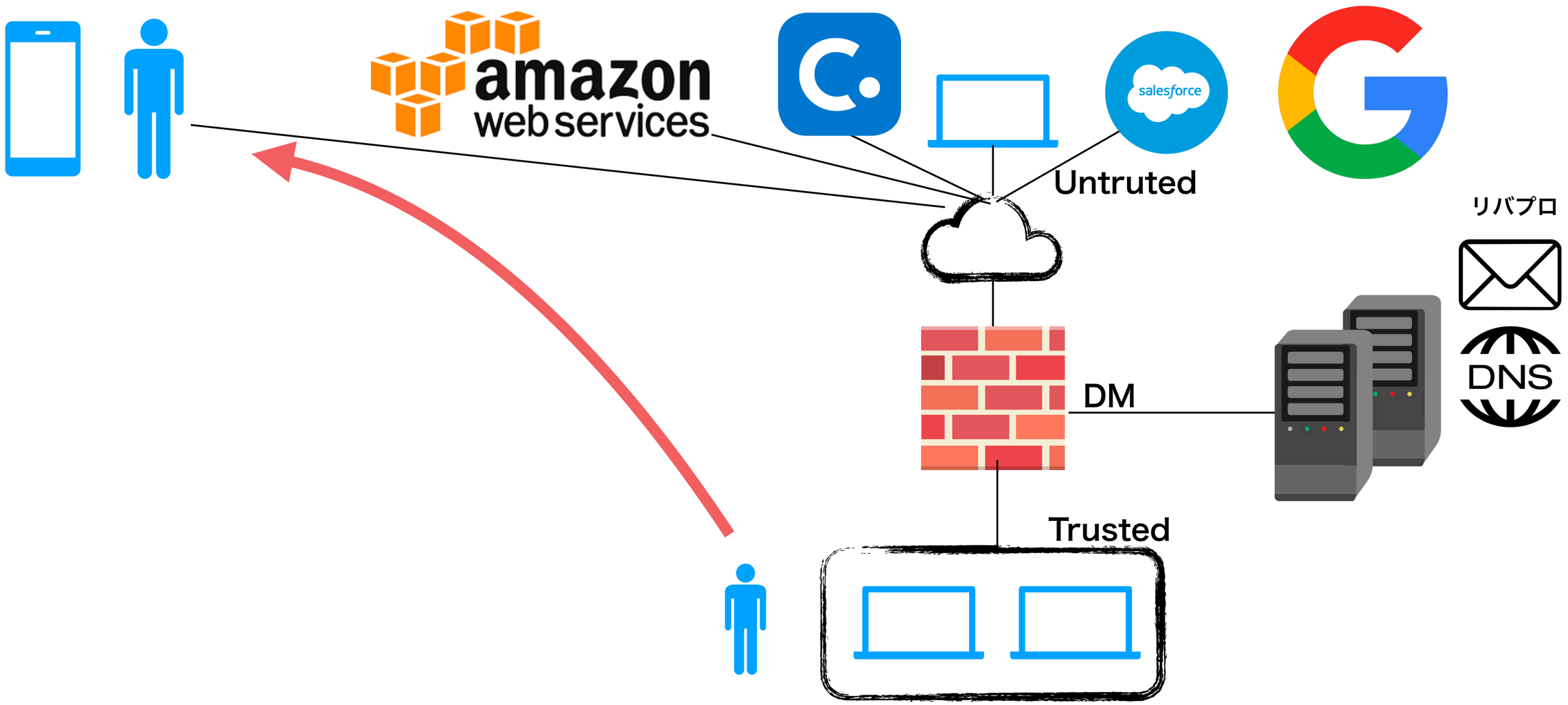
ゼロトラスト・アーキテクチャ

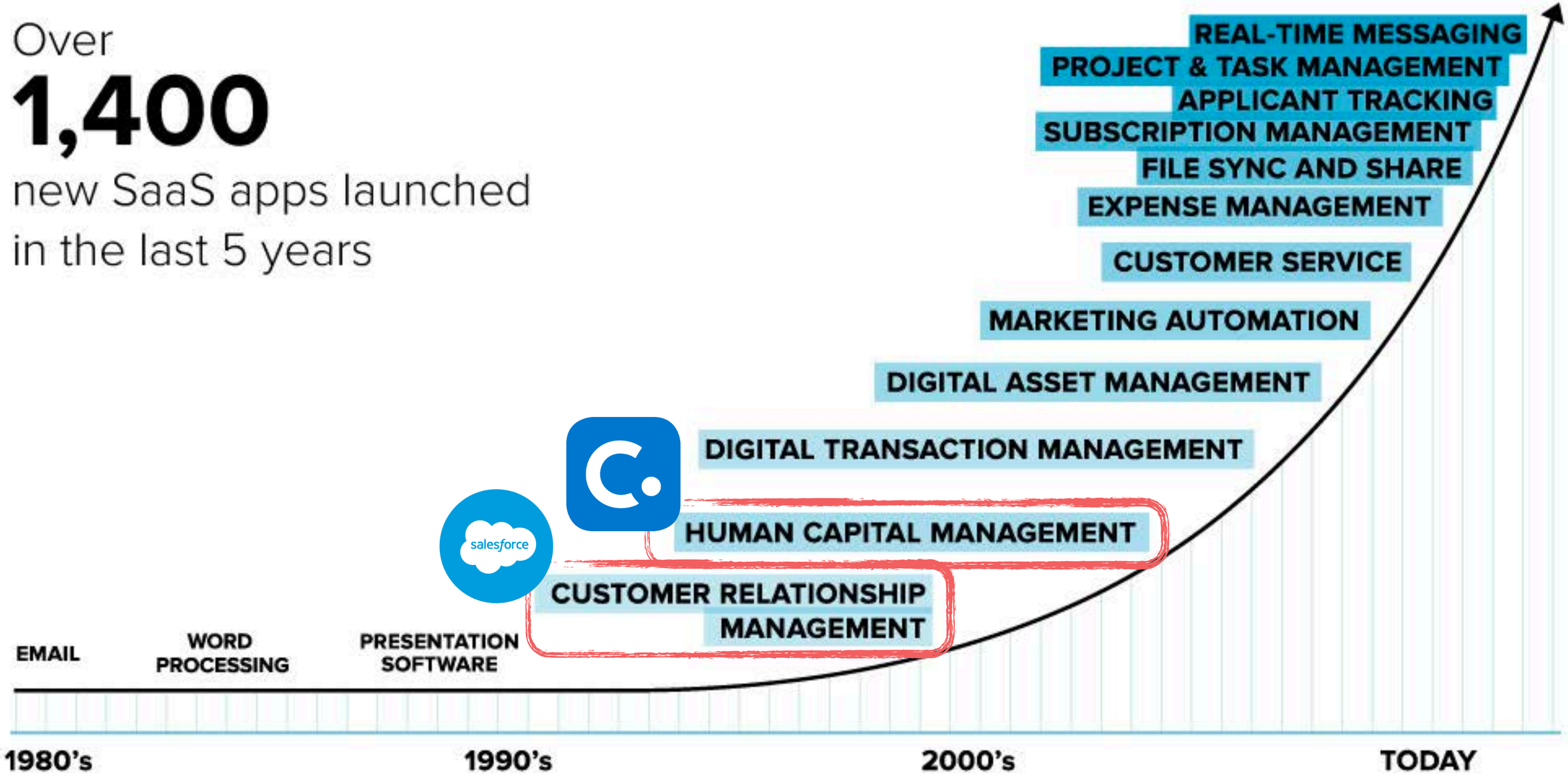
ゼロトラストの考え方をベースにした
各種コンポーネントの関係性、ワークフロー、アクセスポリシーを
包含したサイバーセキュリティ戦略

社内リソースで業務が（ほぼ）完結する時代は、
トラストの基点がFW・NWだったのが



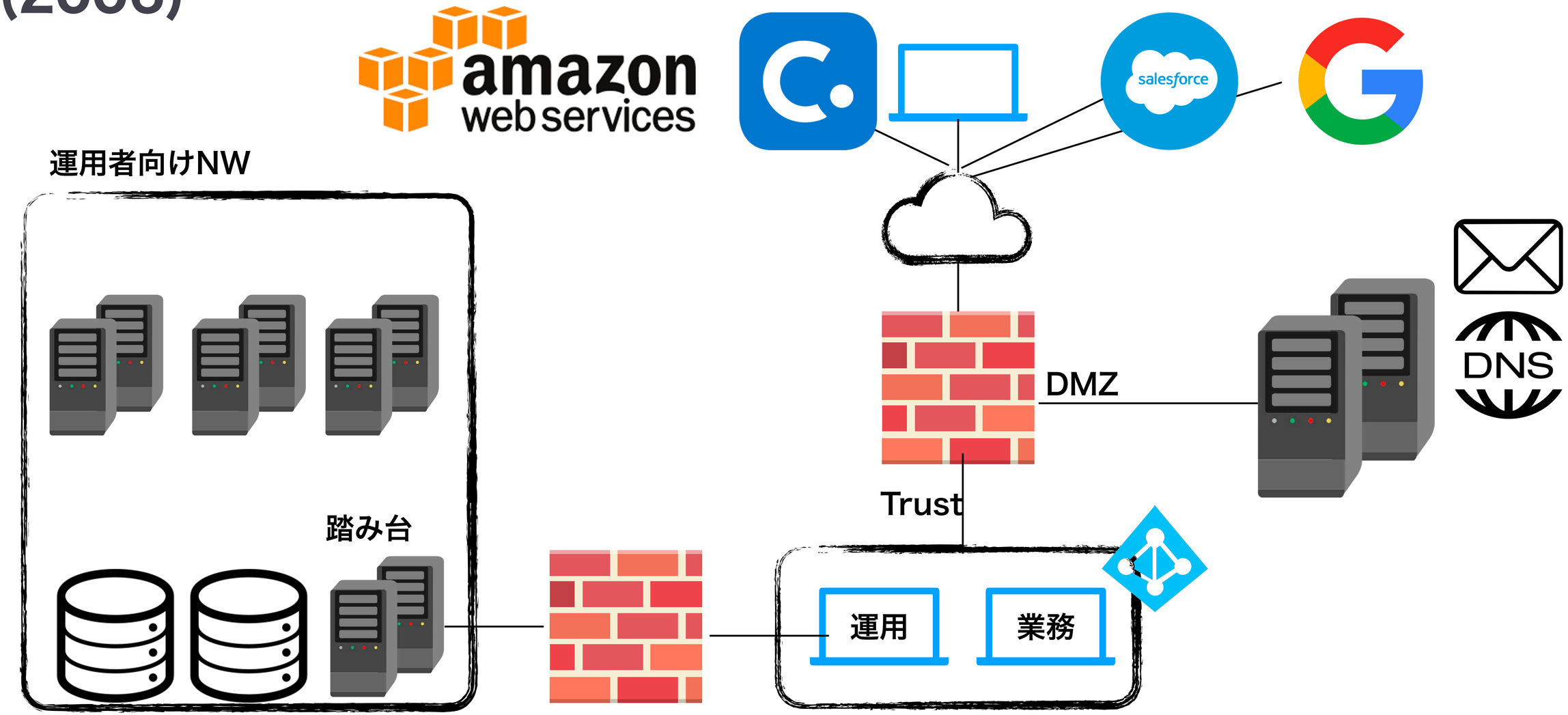
もろもろがインターネット側へ



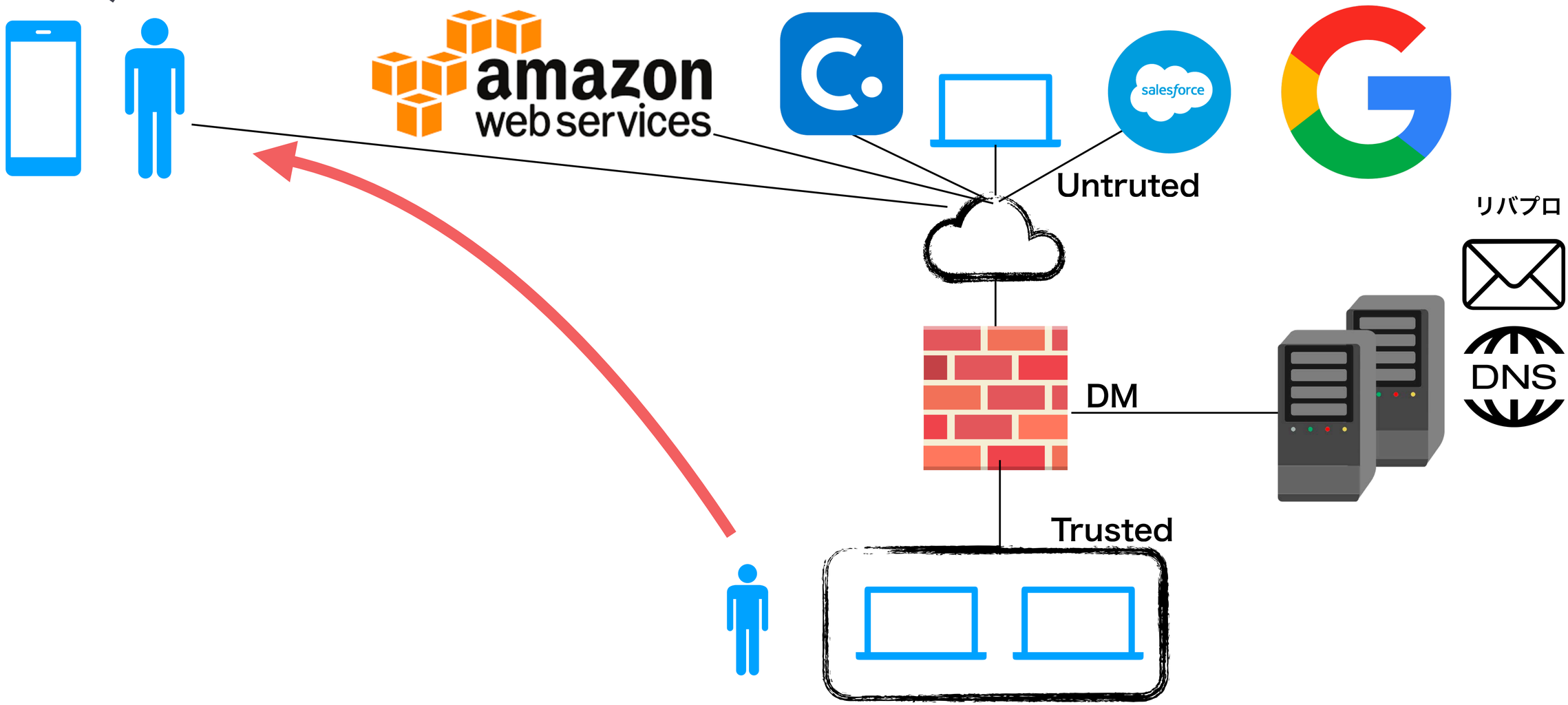


The SaaS-Powered Workplace: The Present & Future of Work
: https://www.bettercloud.com/monitor/saas-powered-workplace-multi-saasmanagement/

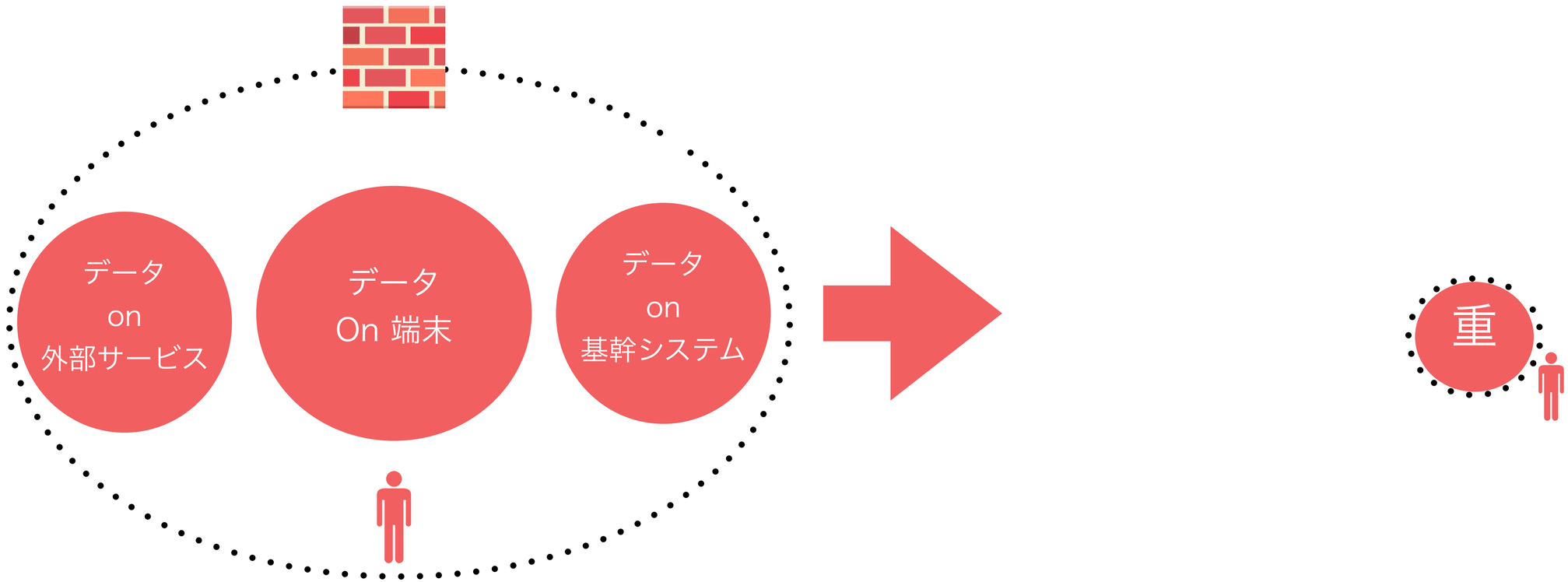
情報システム基盤もUntrust側へ (2006)



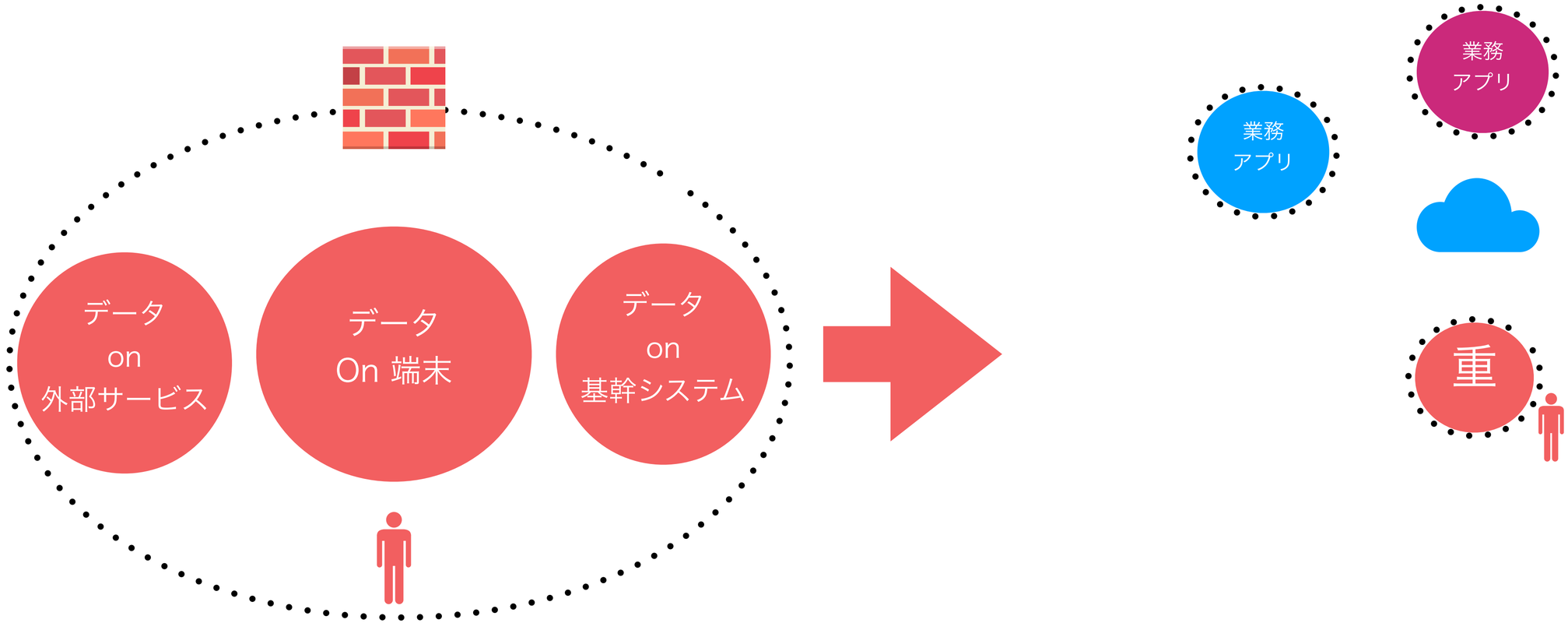
業務執行の主体(人、デバイス）の物理的活動領域のUntrust化(2010)



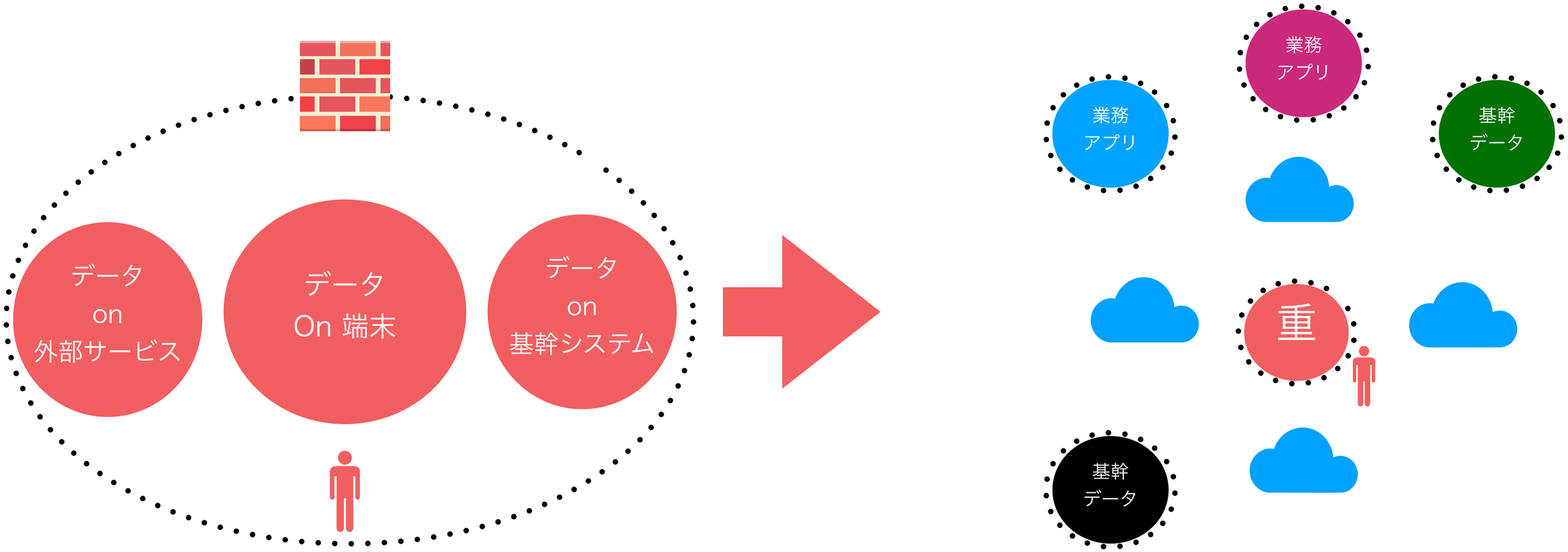
社会情勢やサービスの変化に伴う業務データの分散と経路の多様化



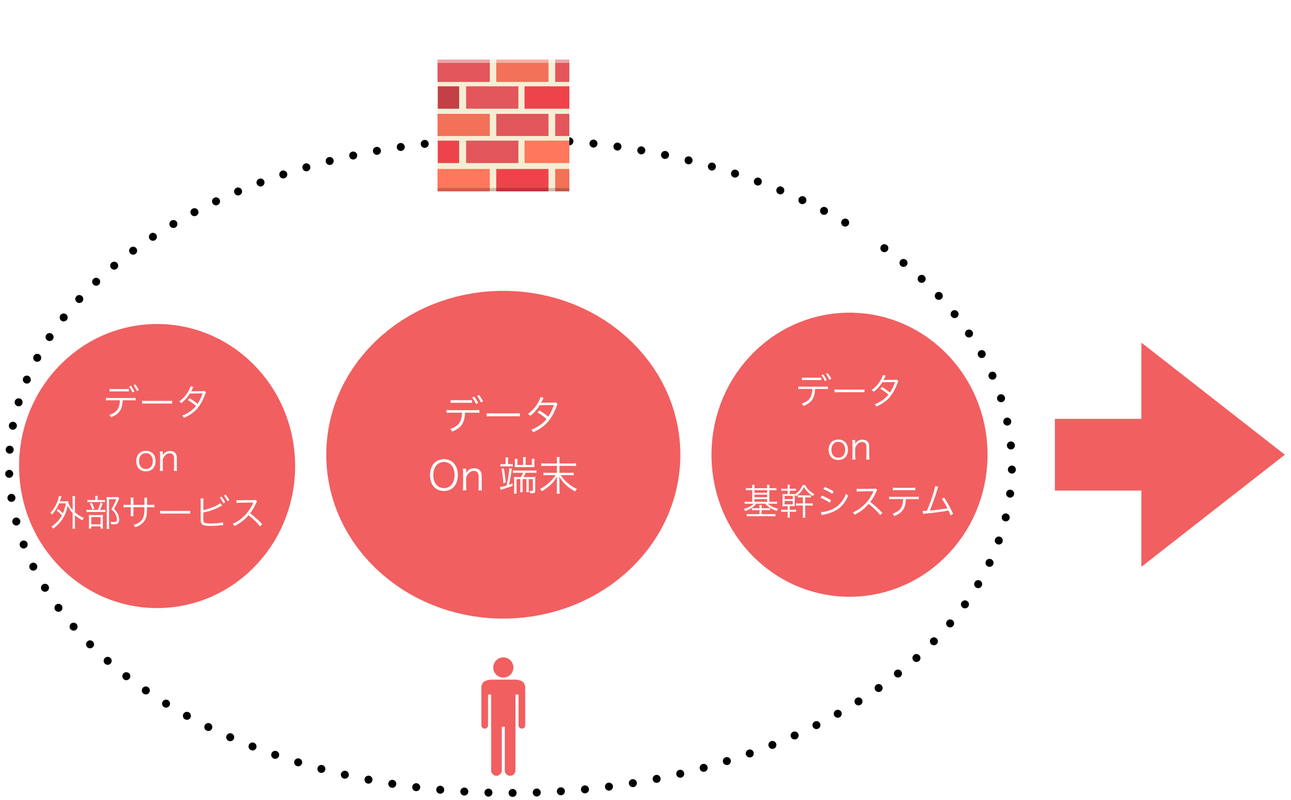
社会情勢やサービスのデジタル化に伴う業務データの分散とUntrust化

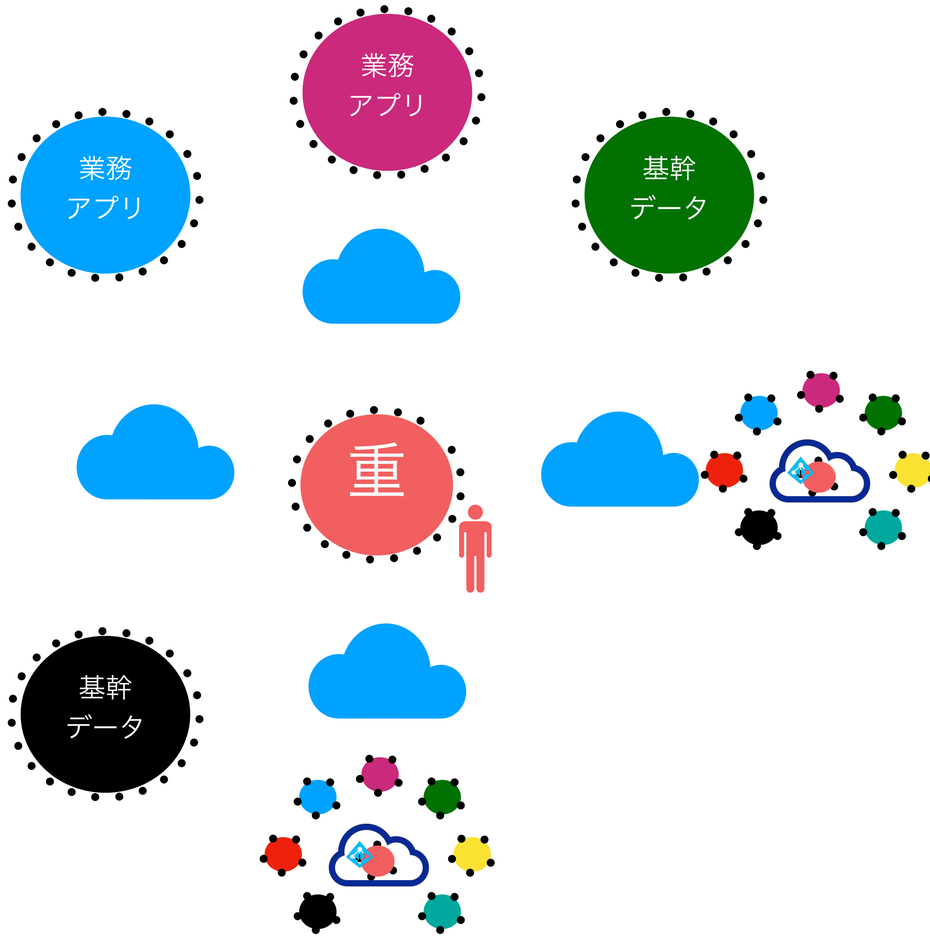


社会情勢やサービスのデジタル化に伴う業務データの分散とUntrust化

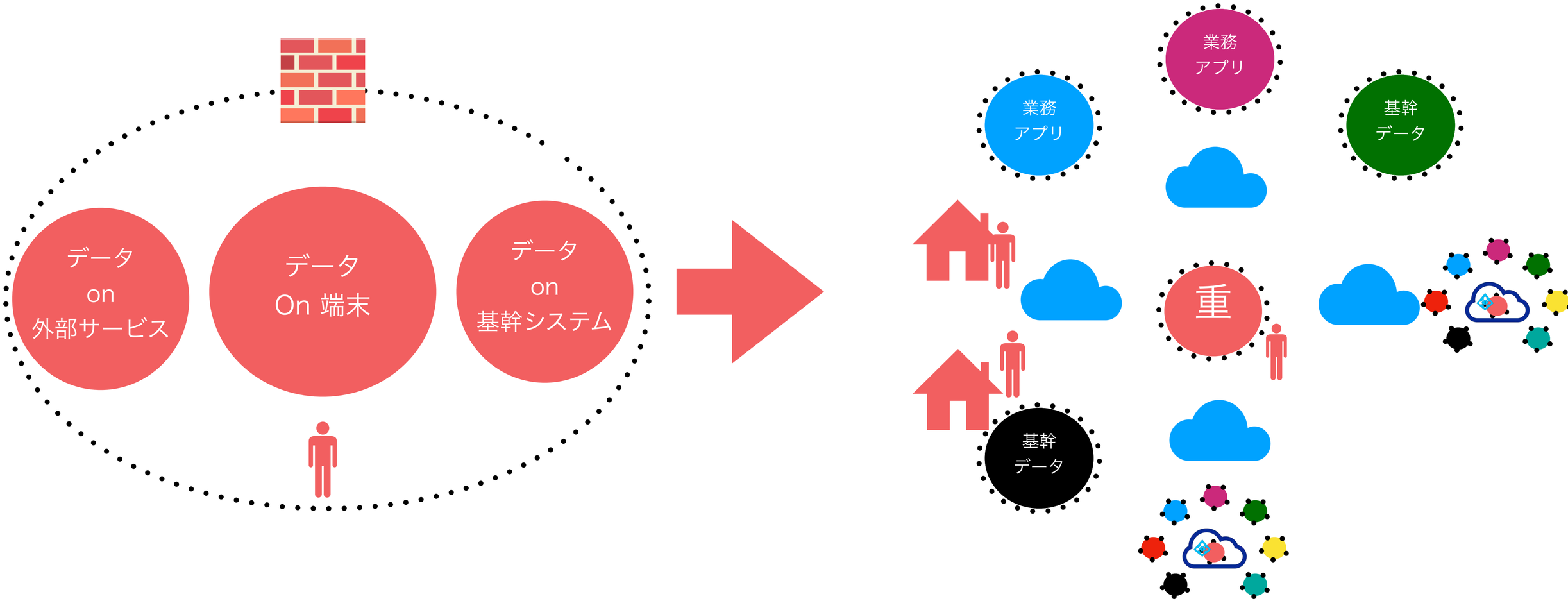


社会情勢やサービスのデジタル化に伴う業務データの分散とUntrust化

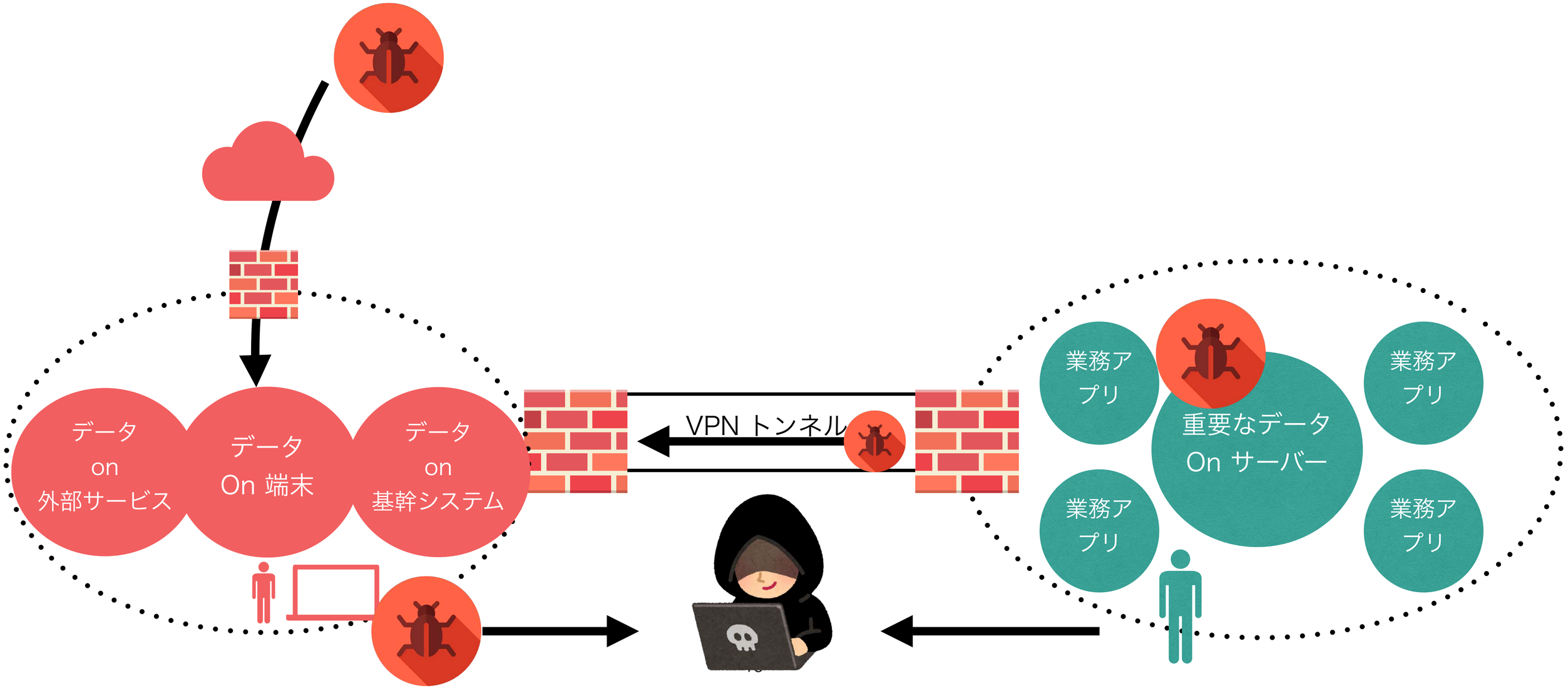




社会情勢やサービスのデジタル化に伴う業務データの分散とUntrust化

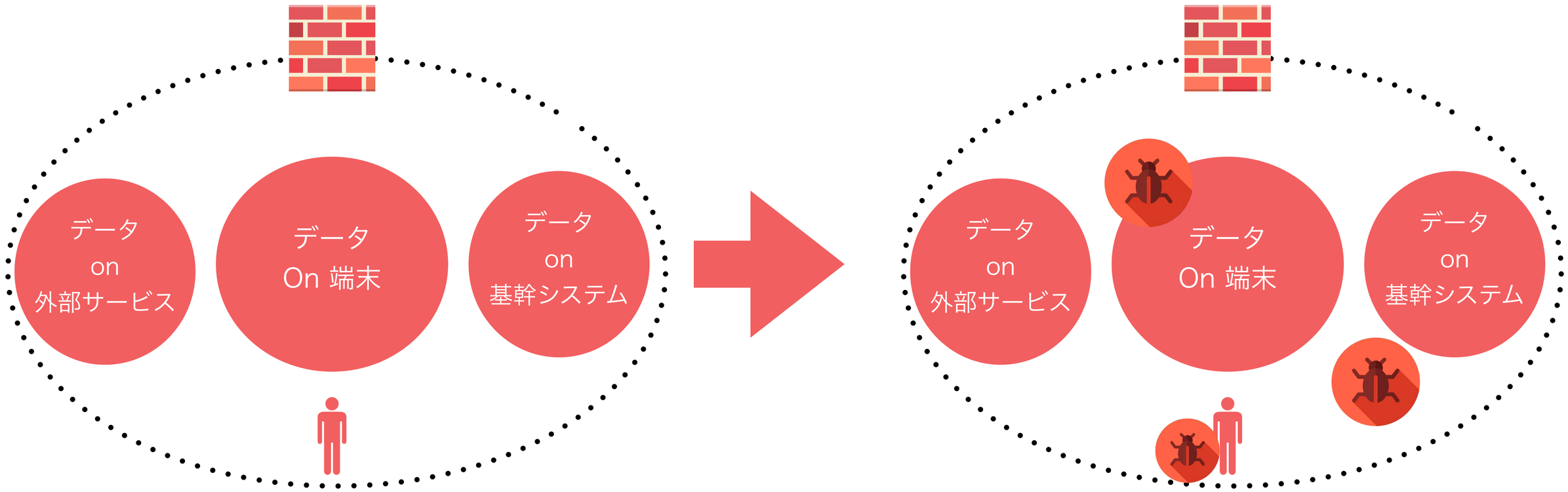


あるいは社内のトラストが保証できなくなって

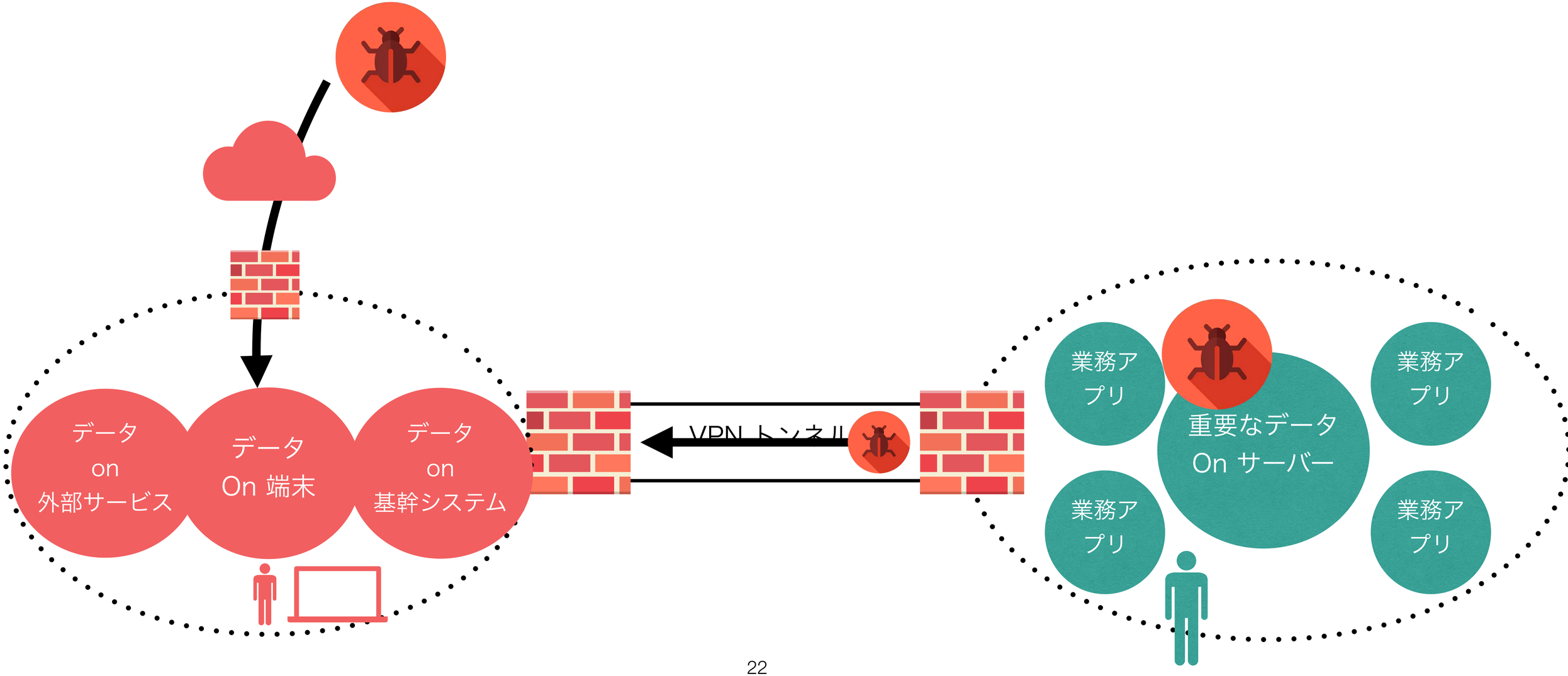


脅威の変化

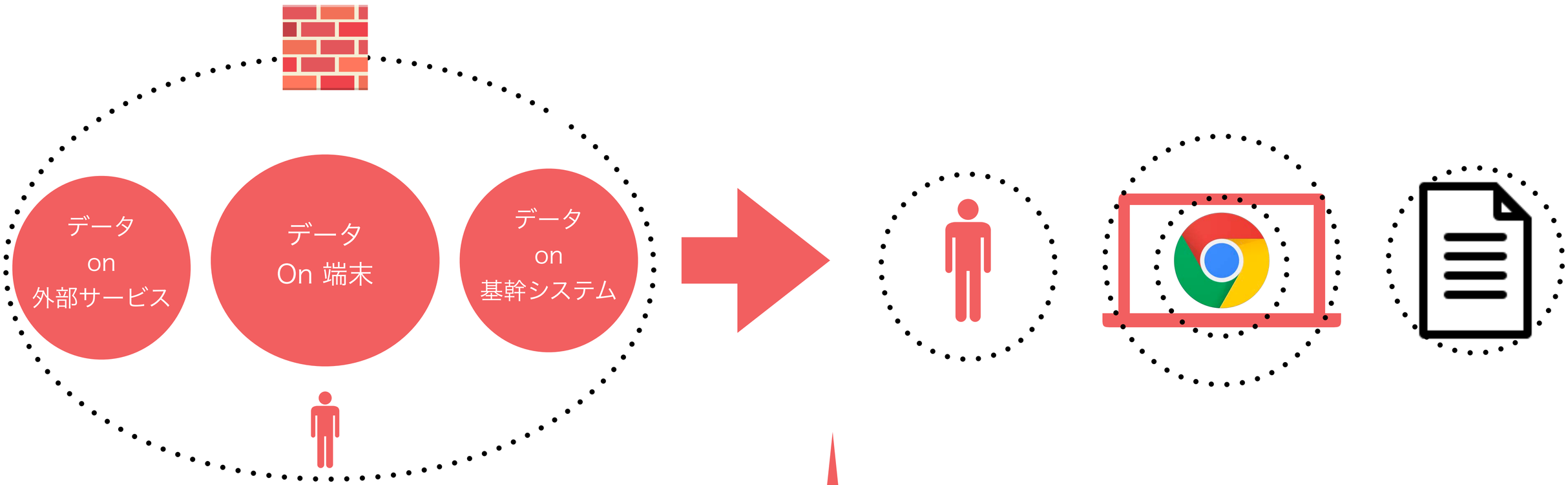
Trust領域の時間経過による劣化



Trust領域の根本的な根拠の毀損



トラストを物理からデジタルへ



- 個あるいは小さな集合単位での境界 => 「Identity Centric」
- 場所や時間を問わない検証 =>「Always Verify」

要件はかわらず、されど産業周辺の環境が変化

1. アクセス制御
2. 意識向上と訓練
3. 監査と責任追認性
4. 構成管理
5. 識別と認証
6. インシデント対応
7. メンテナンス
8. メディア保護
9. 人的セキュリティ
10. 物理的保護
11. リスクアセスメント
12. セキュリティアセスメント
13. システムと通信の保護
14. システムと情報の完全性

ゼロトラストの原則が生まれました

- 全データソースとコンピュータ資源はリソースである
- ネットワークに関係なく通信をセキュアにする
- リクエストごとにリソースへのアクセス権限が付与される
- リソースへのアクセス権限は動的ポリシーにより決定される
- デバイスのセキュアな状態維持と監視をする
- 全リソースにはアクセス前に認証・認可を動的かつ確実に適用する

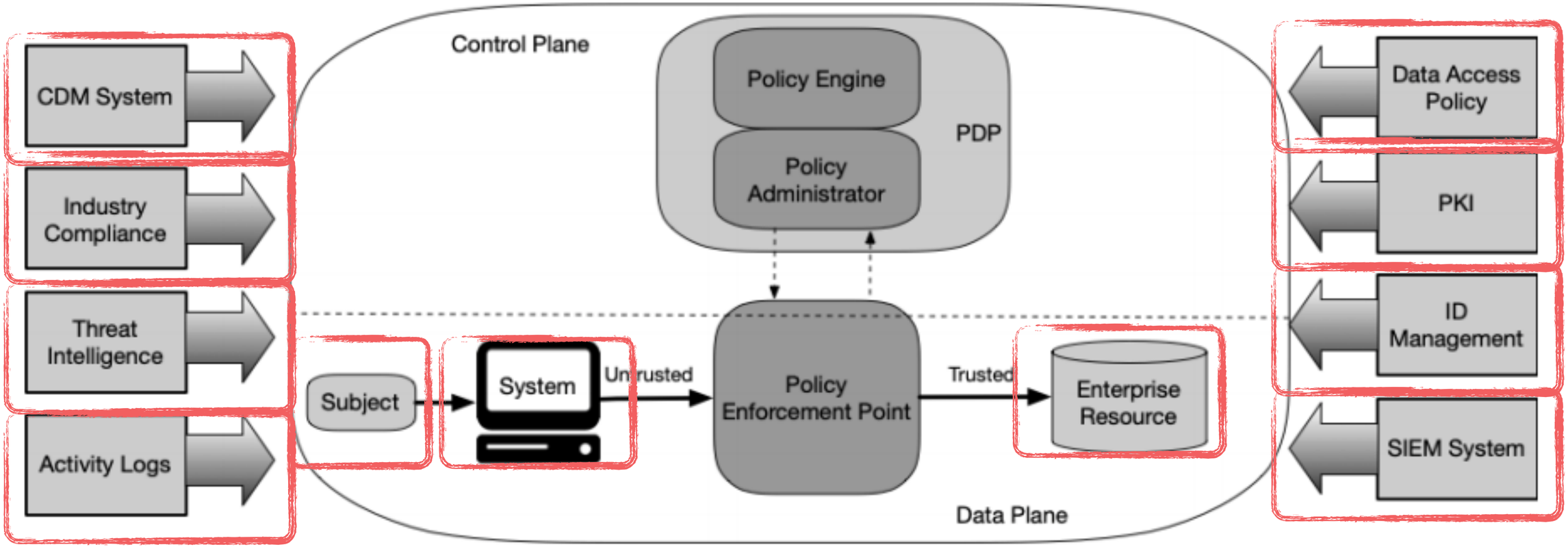
ここまでのまとめ

ゼロトラストという呼称や定義について議論する意味ない

現代ではゼロトラスト的な考え方・設計・思想をしないと

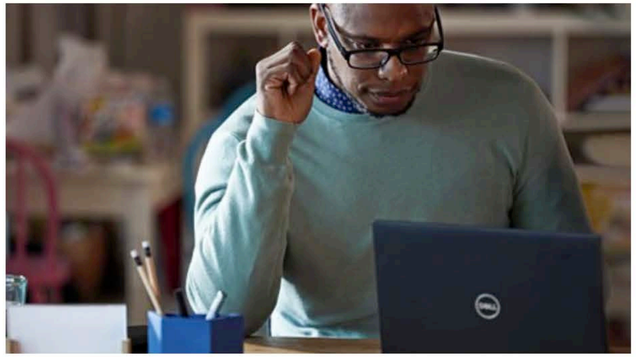
話にならない（仕事が行えない）

トラストを付与するためのソースが分散化・多様化



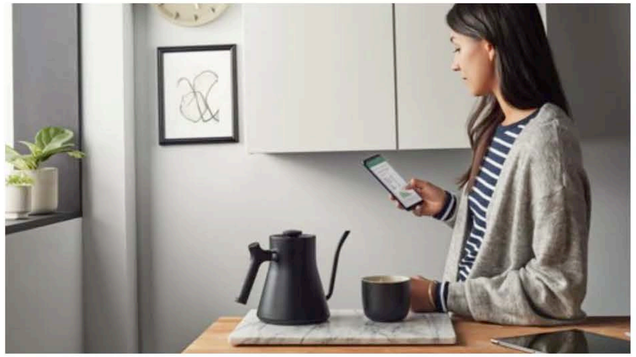
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

データソース



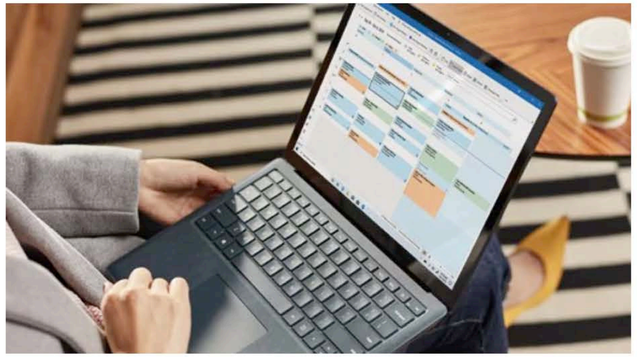
アイデンティティ

組織のデジタル資産全体にわたって、各アイデンティティの確認とセキュリティ保護を強力な認証で行います。



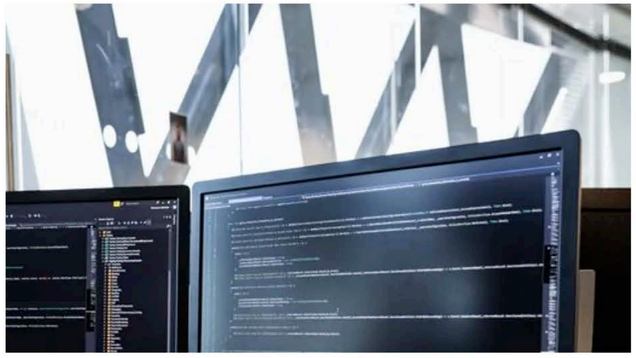
デバイス

ネットワークにアクセスするデバイスを可視化します。規則への準拠と正常性を確認してからアクセスを許可します。



アプリケーション

シャドウ IT を発見し、アプリ内でのアクセス許可を適切に行い、アクセスの許可/不許可の判断をリアルタイムのアナリティクスに基づいて行い、ユーザーのアクションを監視して制御します。

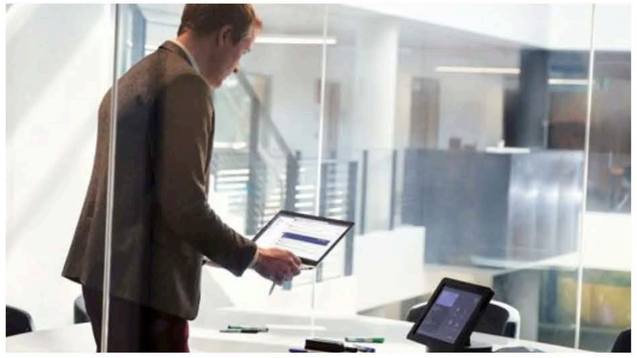


データ

境界ベースのデータ保護から、データ主導の保護に移行します。インテリジェンスを利用してデータを分類し、ラベルを付けます。暗号化とアクセス制限を、組織のポリシーに基づいて行います。

インフラストラクチャ

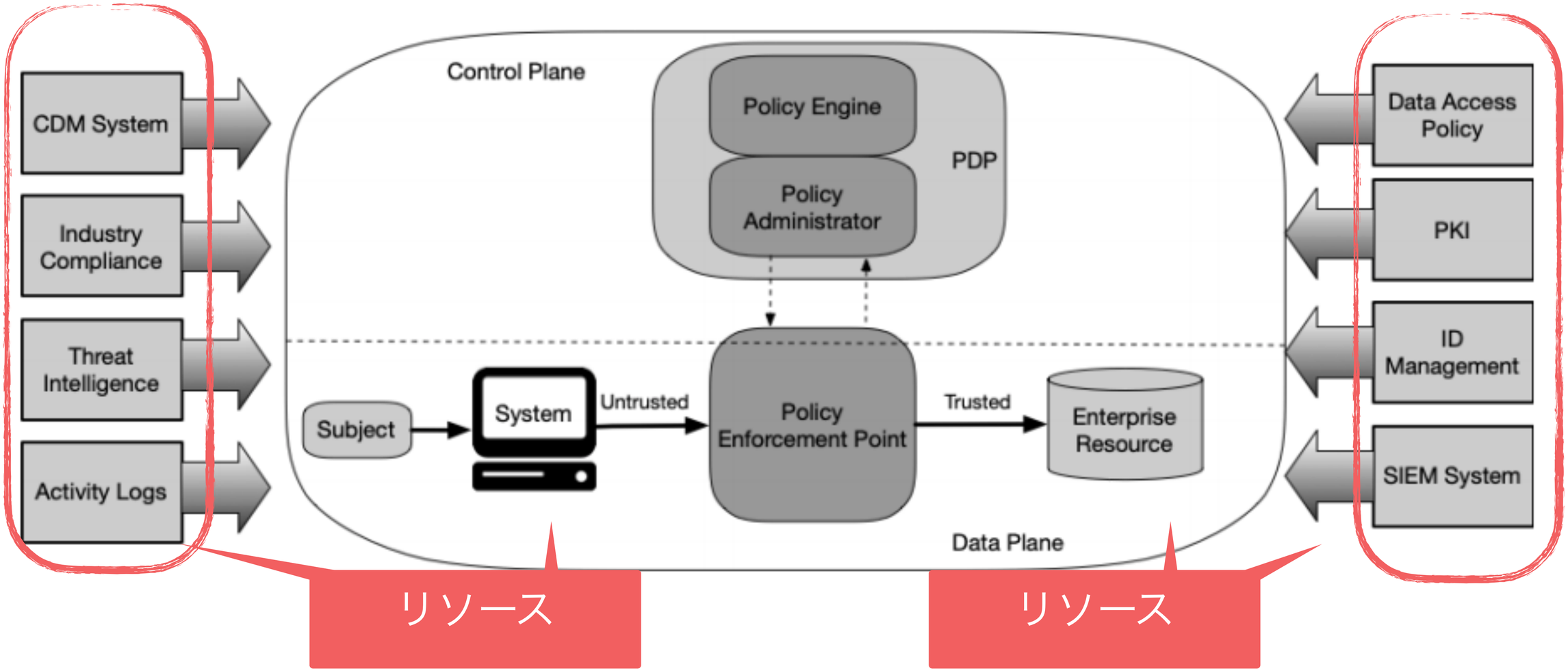
テレメトリを使用して攻撃と異常を検出し、リスクのある行動を自動的にブロックしてフラグを立て、最小特権アクセスの原則を採用します。



ネットワーク

デバイスとユーザーを、内部ネットワーク上にあるという理由だけで信頼しないことを徹底します。内部の通信をすべて暗号化し、アクセスをポリシーで制限し、マイクロセグメンテーションとリアルタイムの脅威検出を実

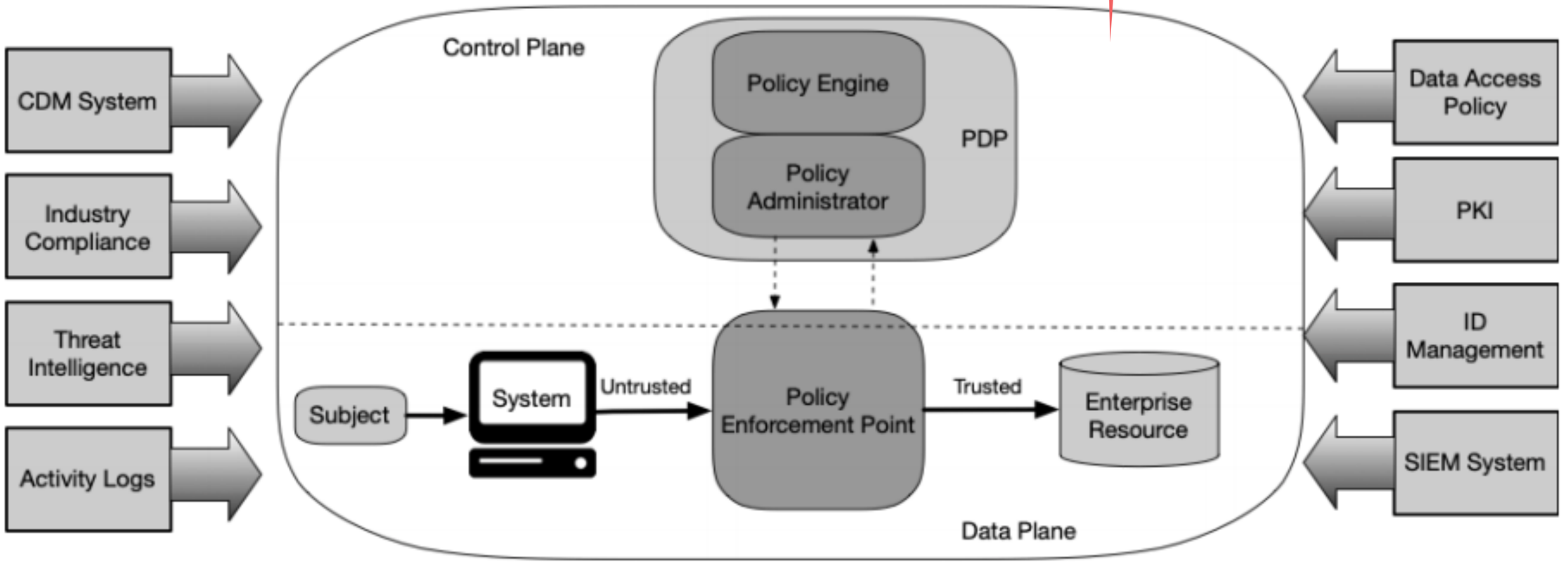
コンポーネント



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

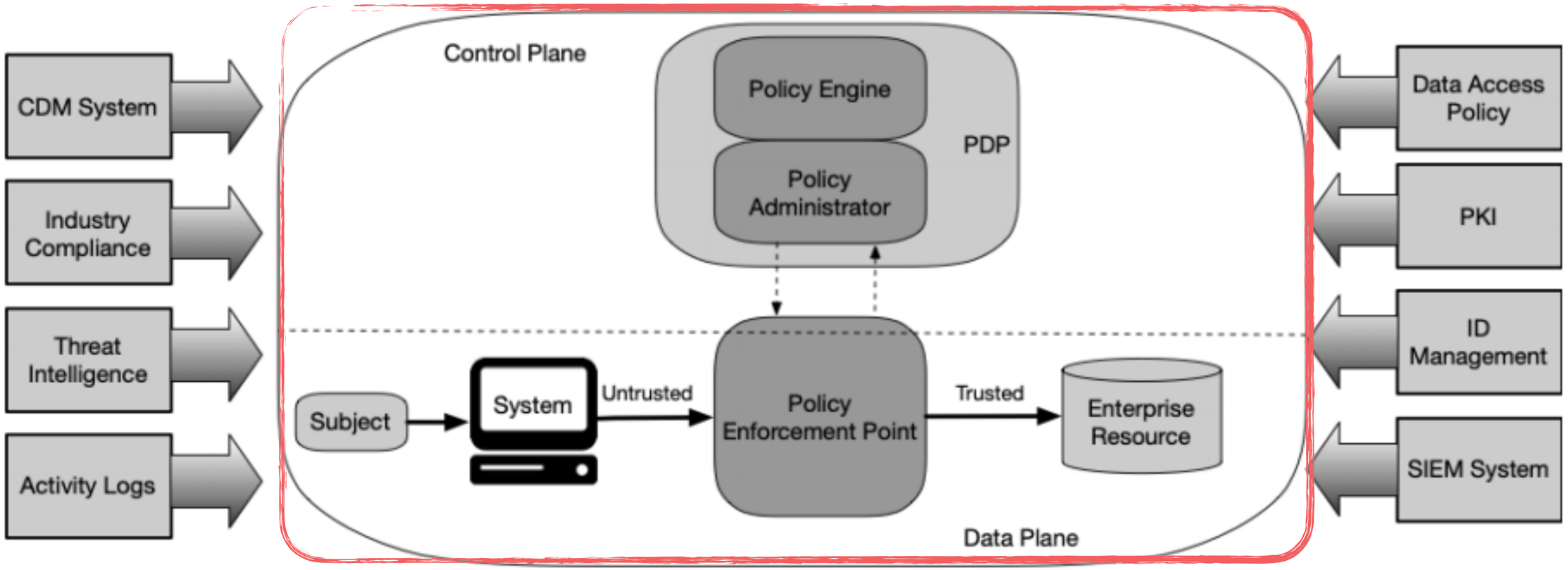
コンポーネント

Networkそれ単体では
セキュアな通信の決定を
考慮しない



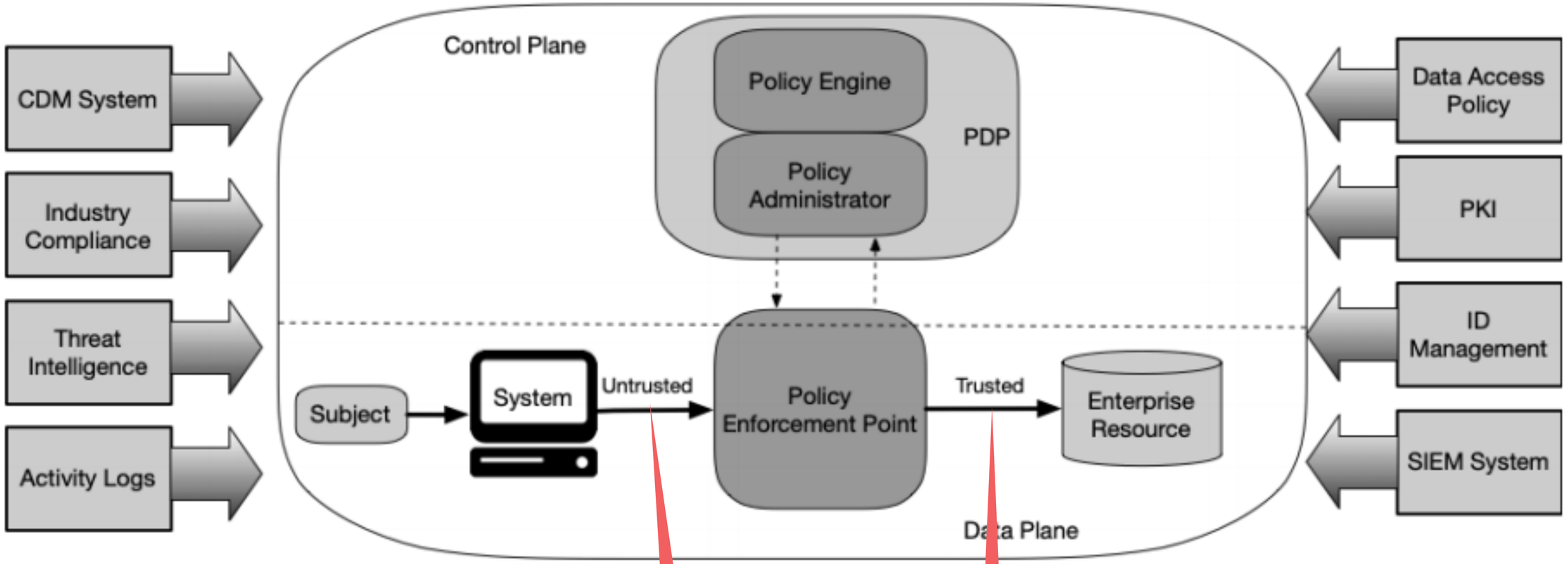
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

コンポーネント



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

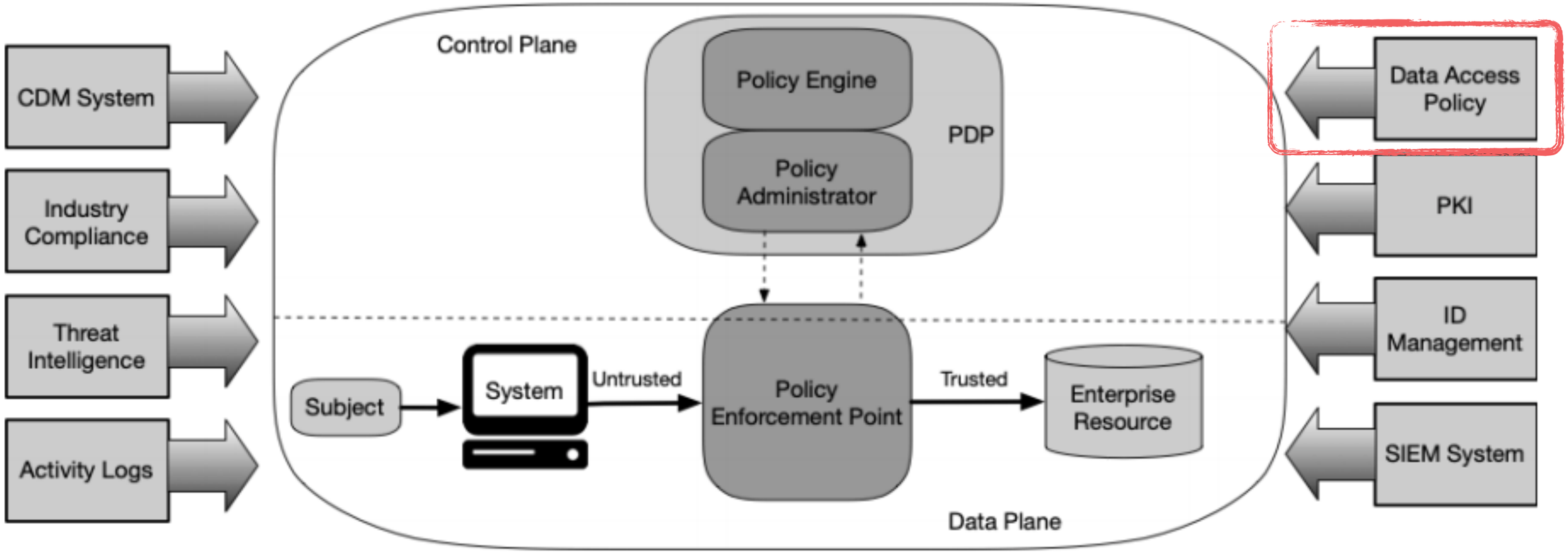
コンポーネント



TrustはPDP
によって検証された後に付与

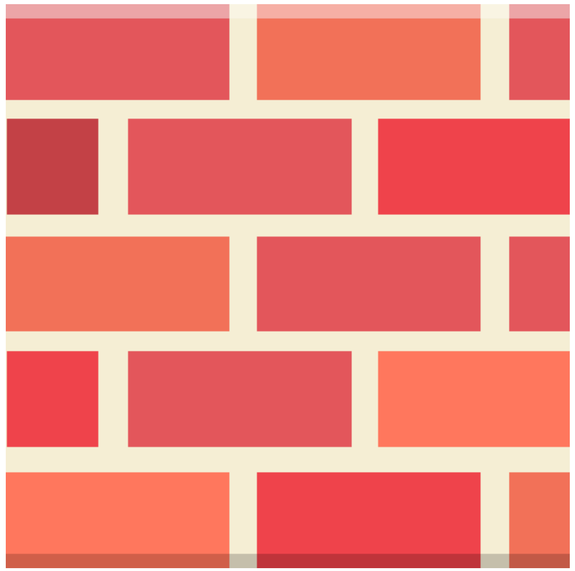
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

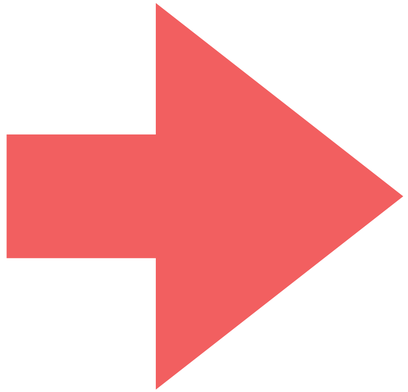
コンポーネント

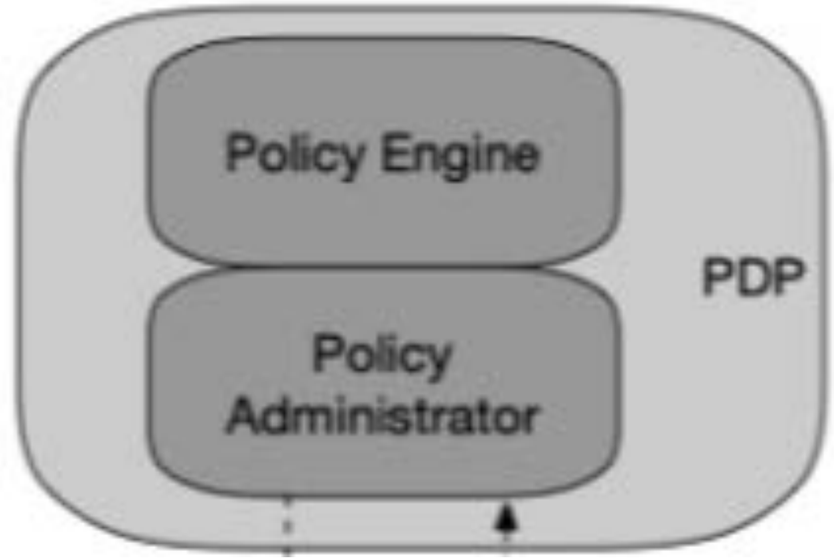


https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

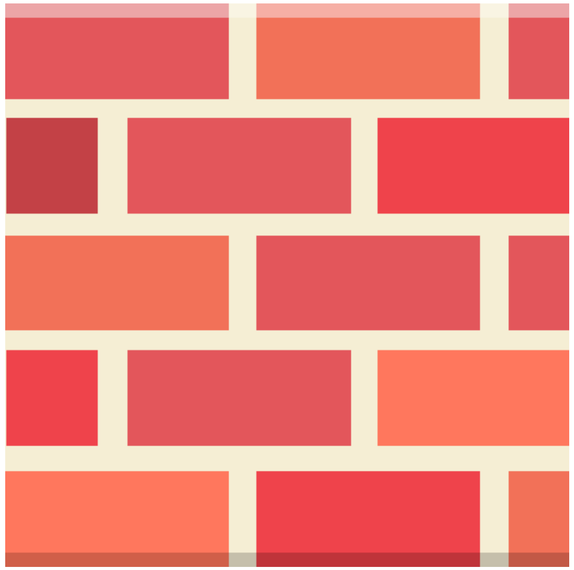
Trust判断・付与機関の抽象化

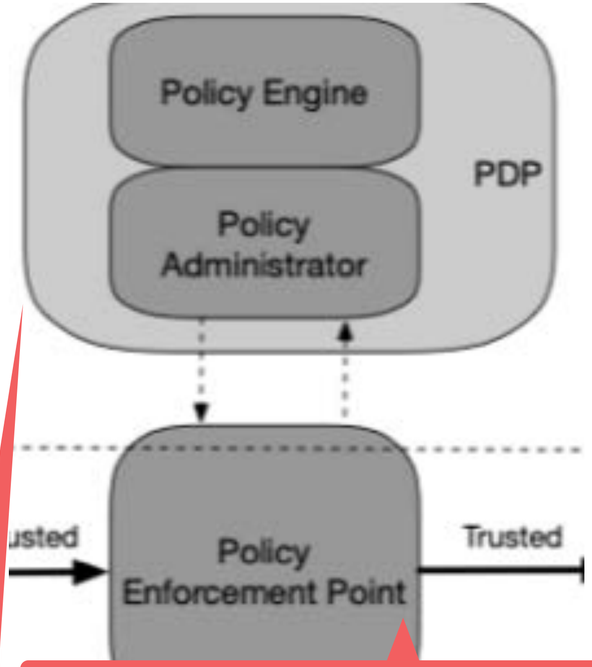






Trust判断と適用機関の分離

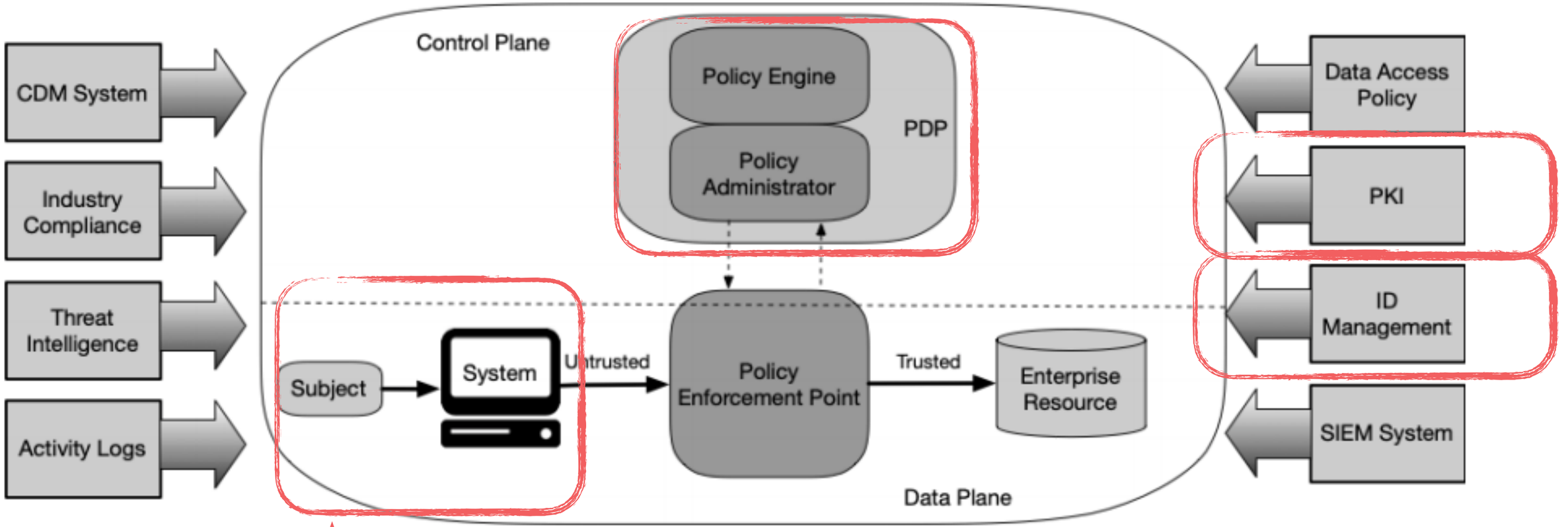




Trust判断のみ

Trust判断の適用

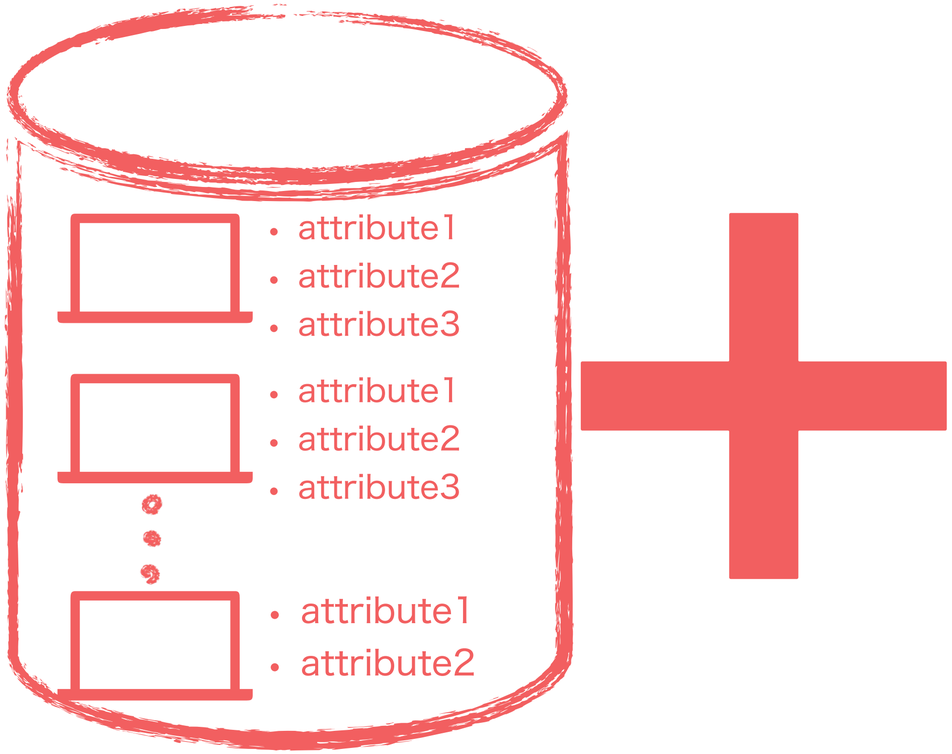
コンポーネント

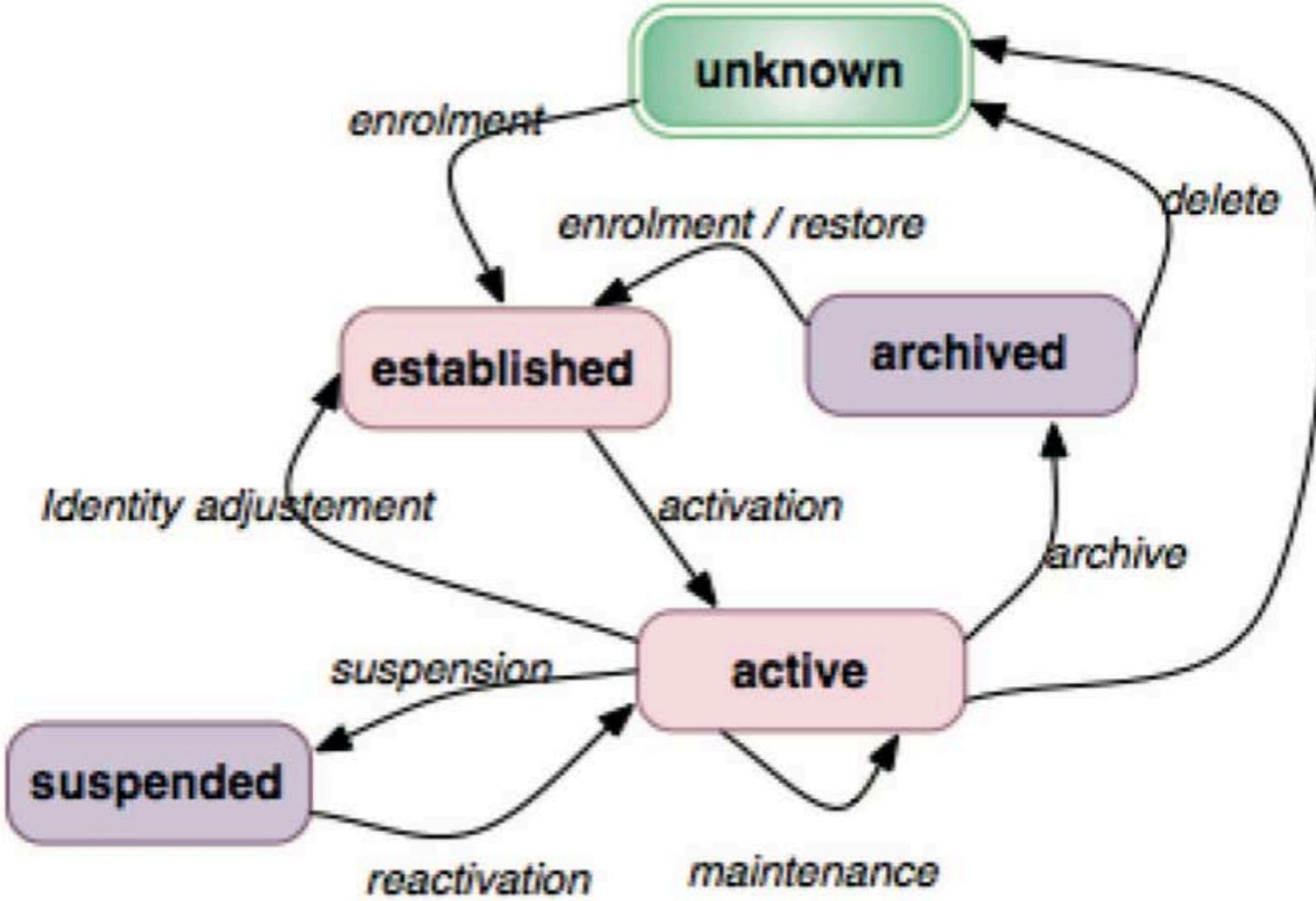


ユーザー、デバイス、(デバイス属性)としてのNW

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

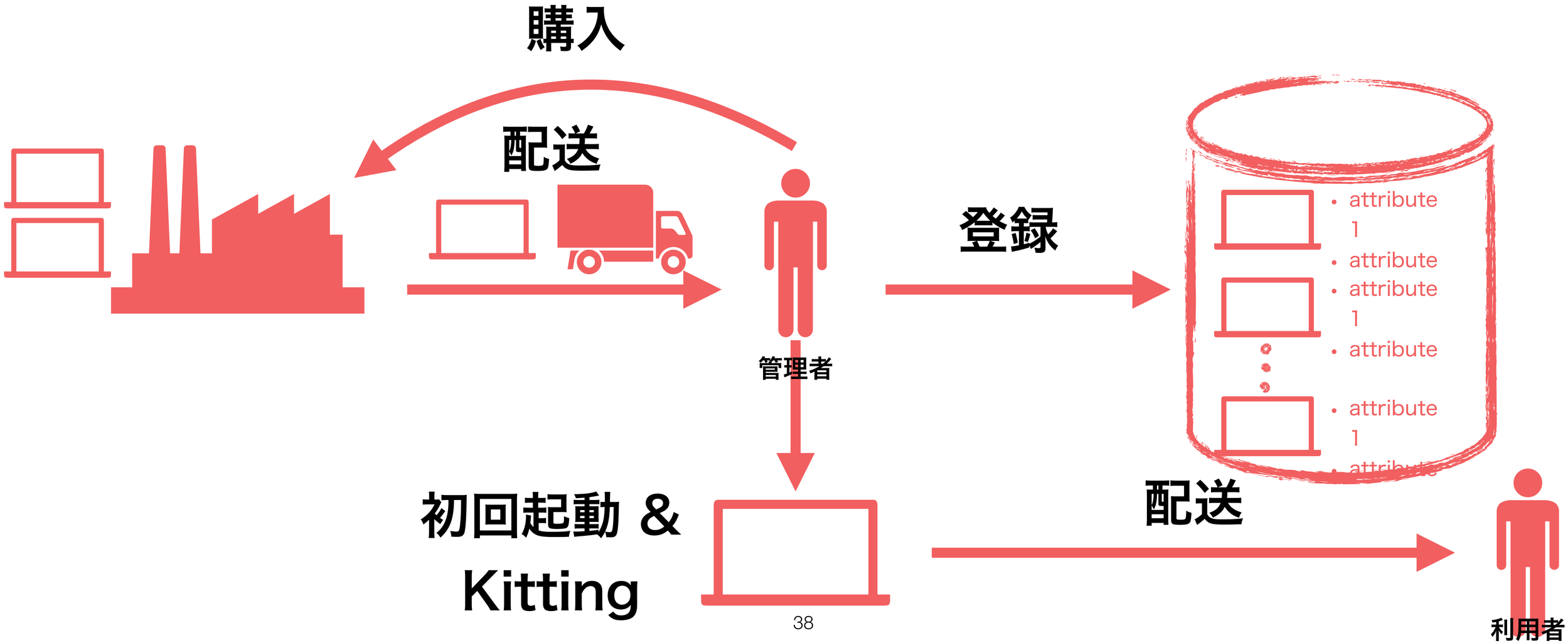
データベース化とライフサイクル



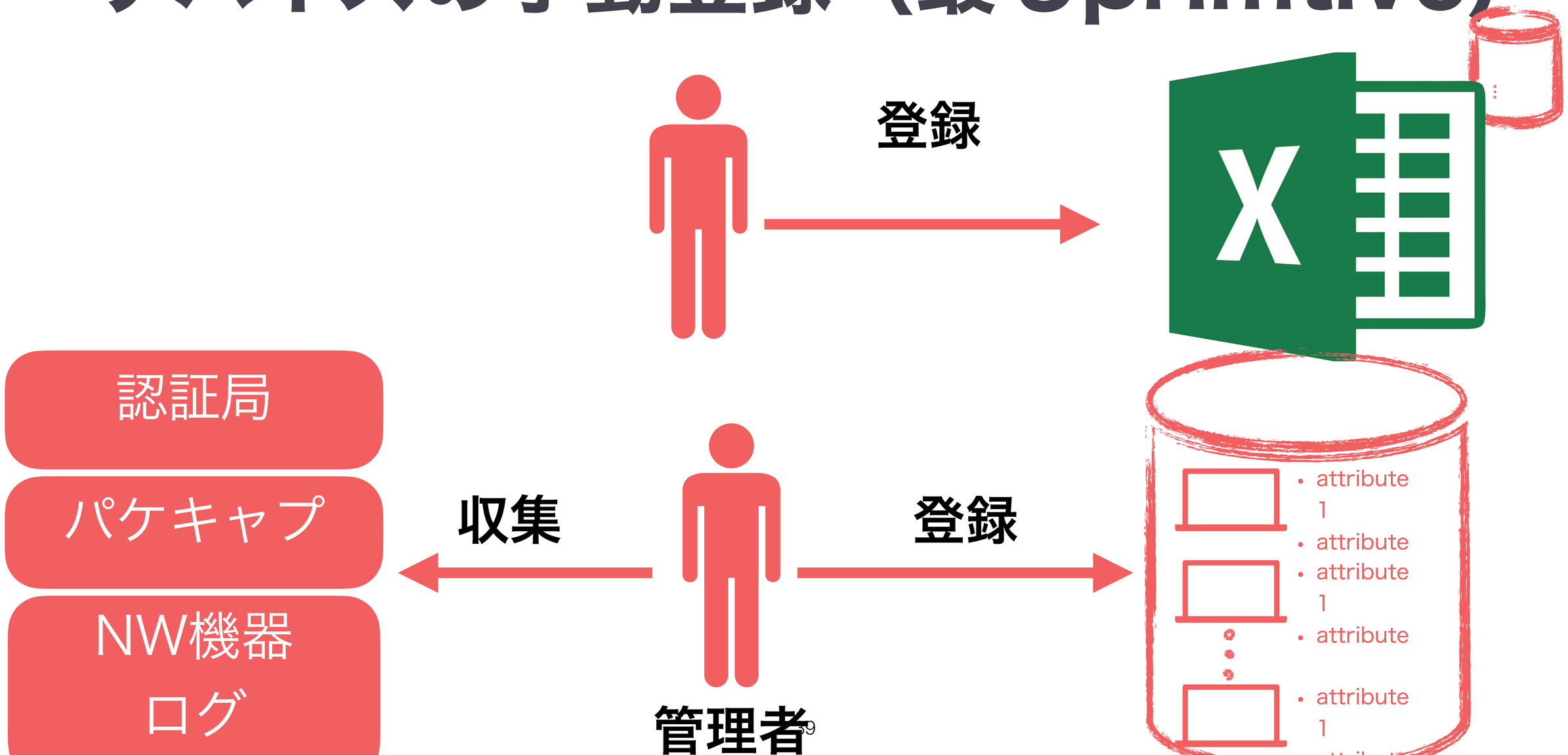


https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html > ISO/IEc 24760-1:2019

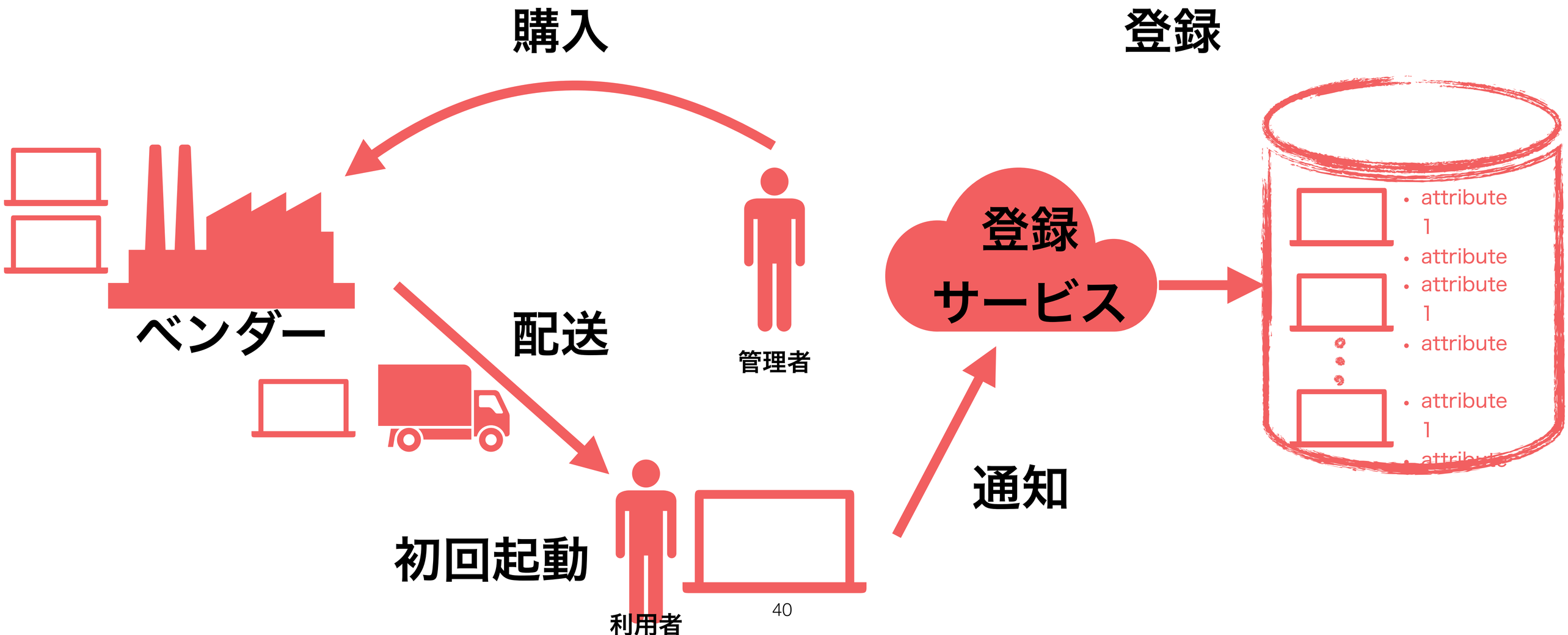
デバイスのDB登録の流れ



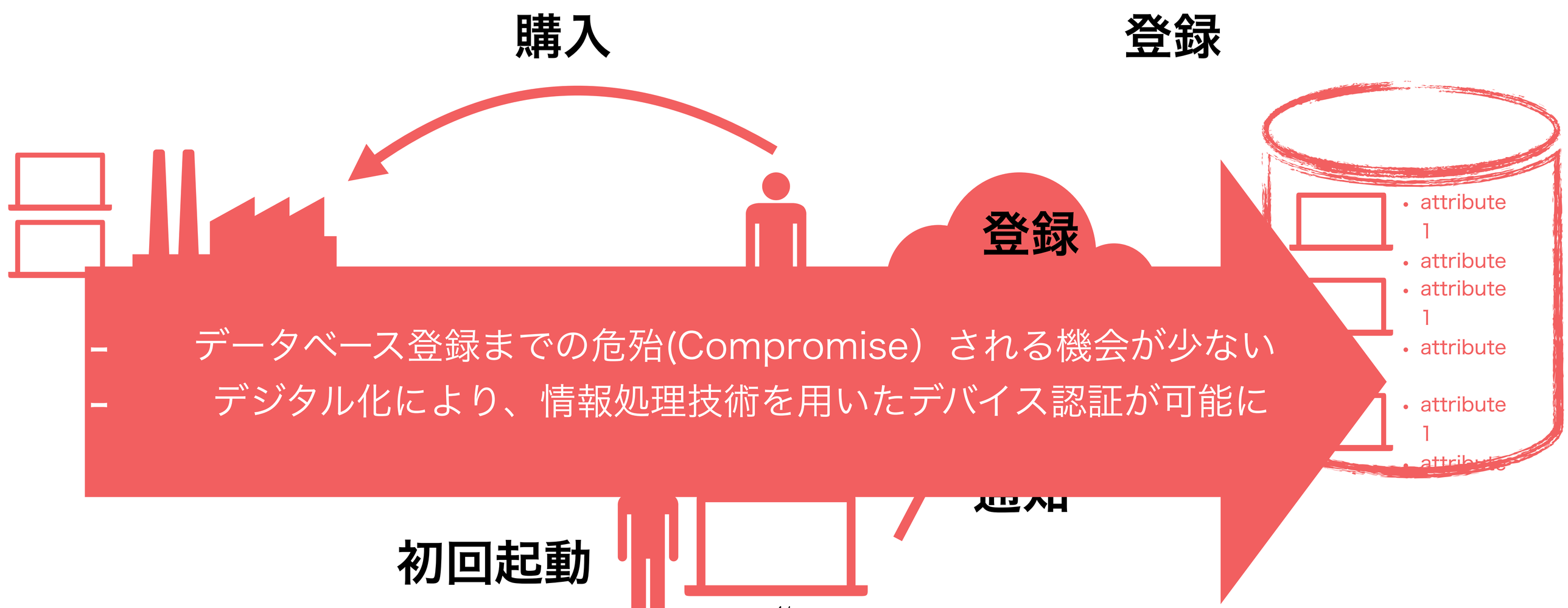
デバイスの手動登録（最もprimtive）



デジタル化されたセキュアなデバイス登録

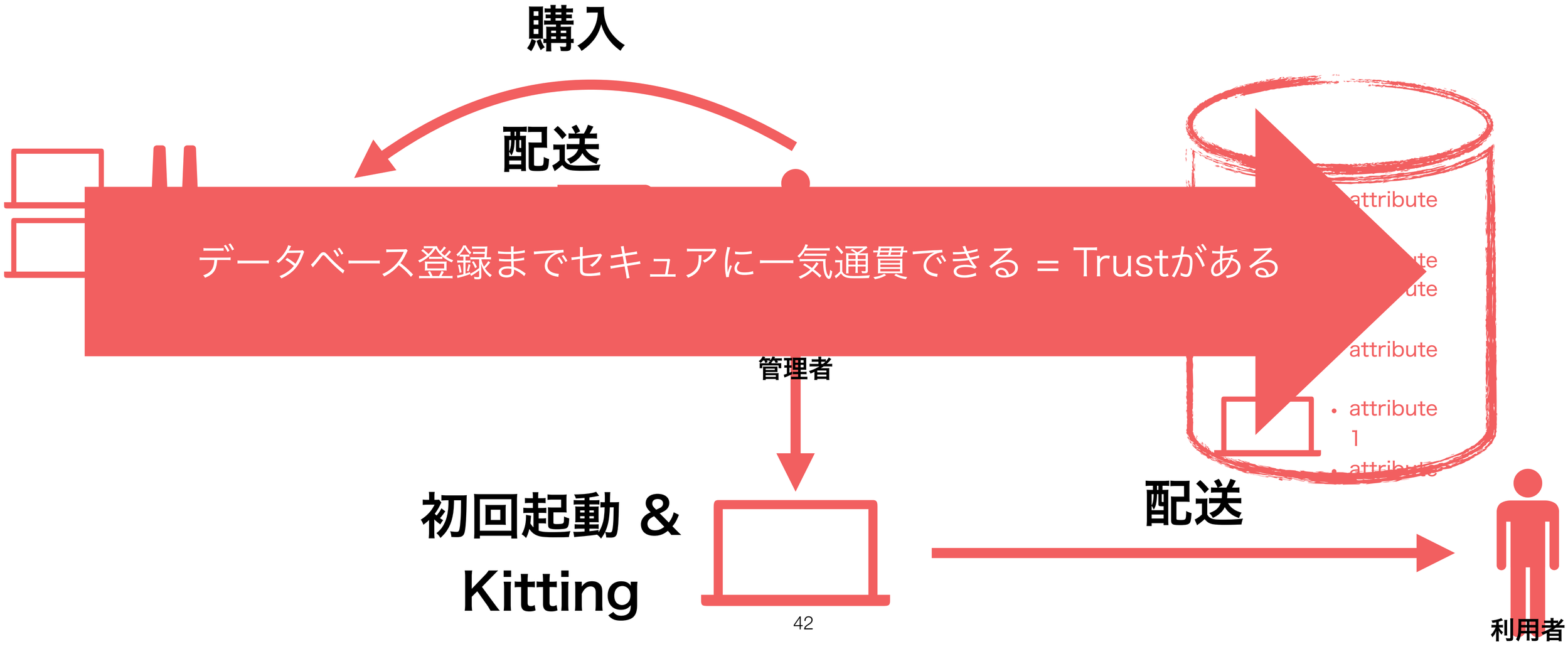


デジタル化されたセキュアなデバイス登録

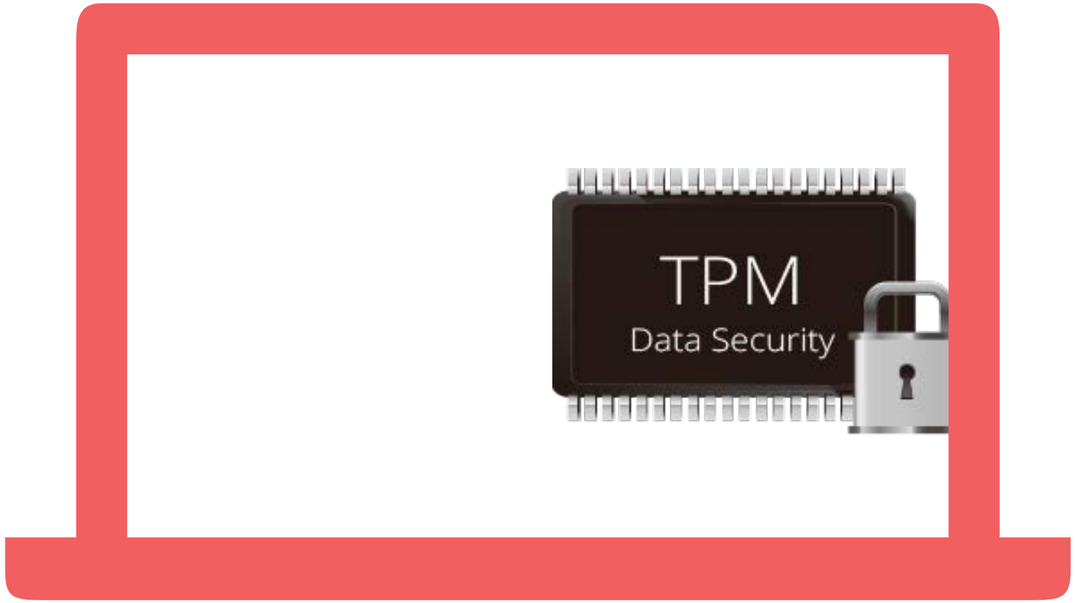


- データベース登録までの危殆(Compromise）される機会が少ない
- デジタル化により、情報処理技術を用いたデバイス認証が可能に

デバイスのDB登録の流れ

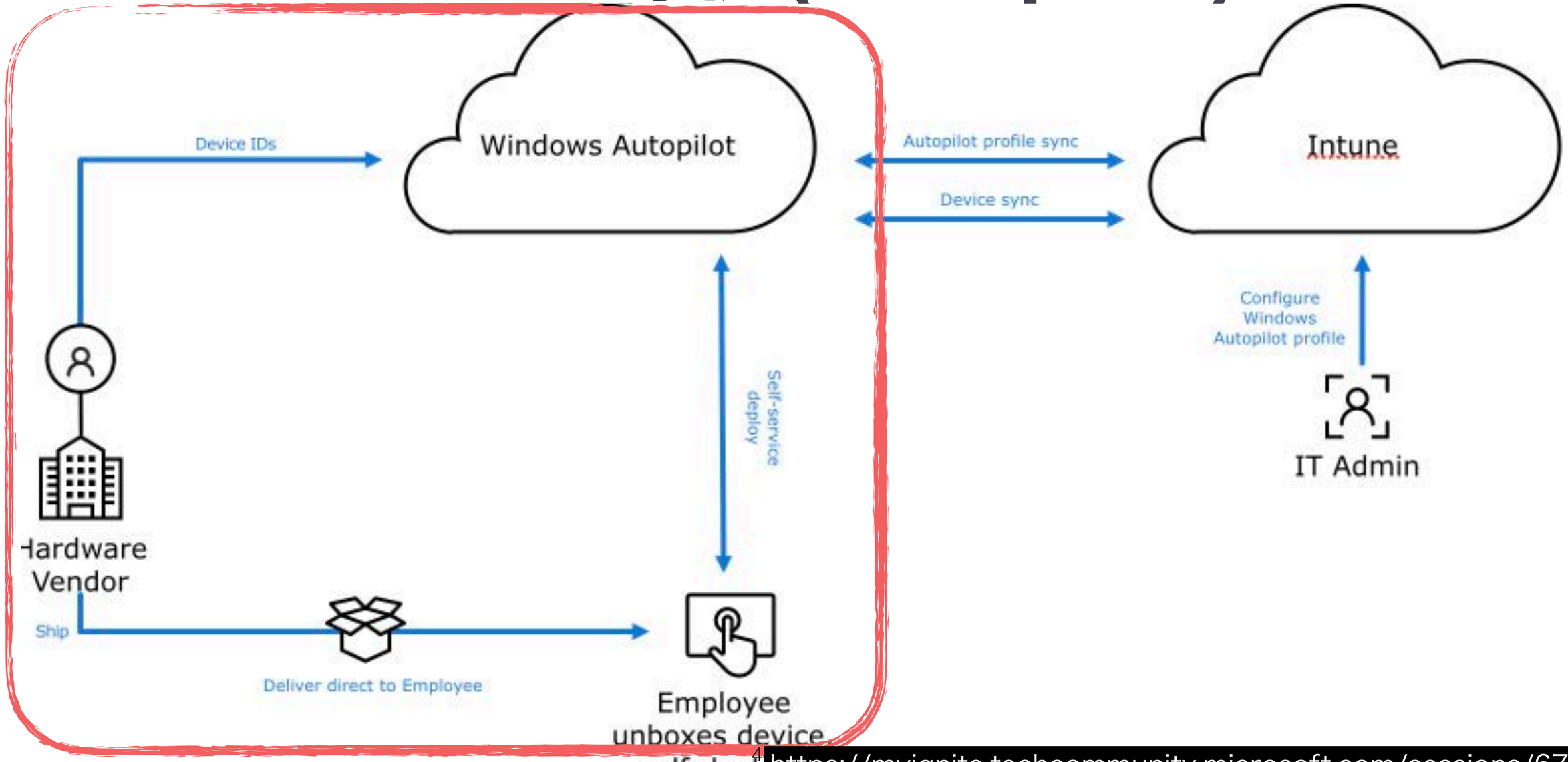


TPM



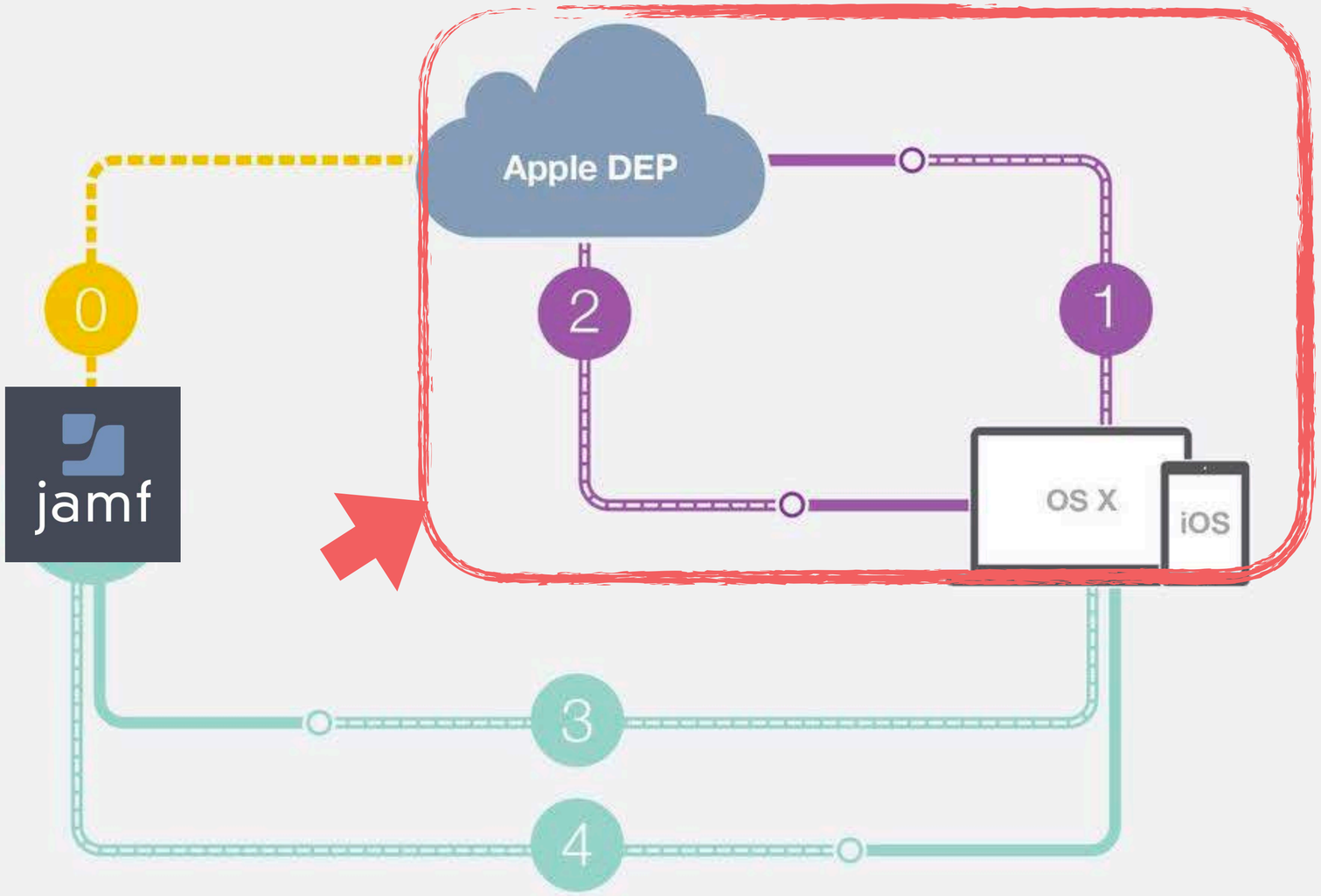
- provides methods for collecting and reporting these identitties.
- セキュアな暗号プロセッサーの国際標準
- ブート時のソフトウェア監査(pltaform integrity)
- 機密データの保管、暗号鍵の管理

Windows10登録例(Autopilot)



https://myignite.techcommunity.microsoft.com/sessions/67110

Mac登録(ADE + Mac)



DEP enrollment with the Casper Suite

0 Setup: connect JSS with Apple DEP service

1 During activation, device checks in with Apple DEP service

2 DEP service returns the enrollment details for the Casper Suite server

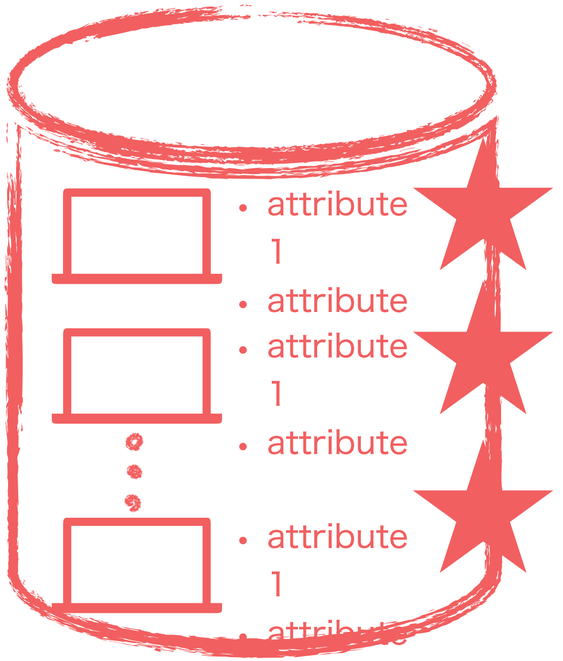
3 Device enrolls with the Casper Suitet

4 After enrollment, configuration profiles are installed

https://www.jamf.com/blog/apple-device-enrollment-program-apple-it-innovation/

デバイスの構成情報の収集

- セキュアな状態監視のためには構成(属性)情報
  - 最後に状態確認された時間
  - 起動時間
  - ログインしたユーザー
  - HW情報
  - OSバージョン
  - SWやそのバージョン
  - ディスク暗号化の状態
  - 上記にひもづく脆弱性情報
- 健康状態の収集



Software inventory

65 Applications

Search software

Customize columns | Export

Name	Vendor	Weaknesses	Threats	Exposed machines	Impact
Chrome	Google	51		95 / 109	18.49
Windows 10	Microsoft	185		16 / 130	6.37
Internet Explorer	Microsoft	38		16 / 130	3.45
Edge	Microsoft	59		16 / 130	3.37
Rapid Storage Technology	Intel	1		13 / 13	3.12
Forticlient	Fortinet	5		13 / 13	3.12
Supportassist	Dell	2		10 / 10	2.71
.net Framework	Microsoft	7		8 / 128	2.17
Digital Delivery	Dell	1		9 / 10	2.16

Weaknesses

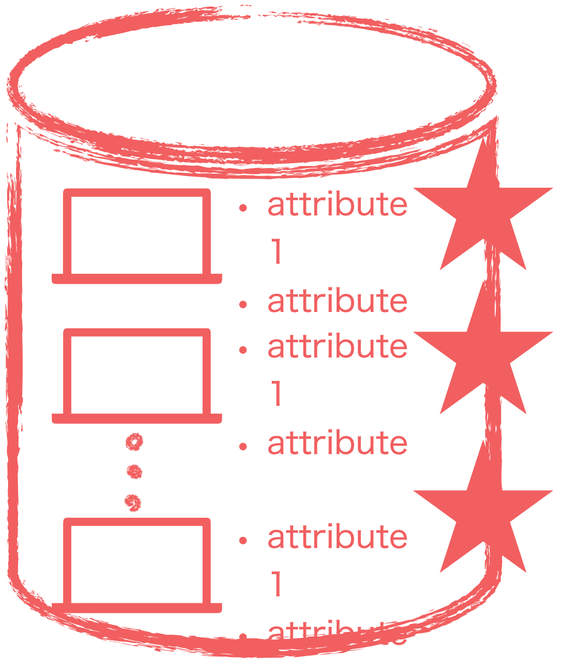
113k Vulnerabilities

Search vulnerabilities

Name	Severity	CVSS V3	Related Software	Age
CVE-2019-5853	Medium	6.3	Chrome	8 days
CVE-2019-5864	Medium	4.3	Chrome	8 days
CVE-2019-5862	Medium	4.3	Chrome	8 days
CVE-2019-5852	Medium	4.3	Chrome	8 days
CVE-2019-5861	Medium	4.3	Chrome	8 days
CVE-2019-5863	Medium	6.3	Chrome	8 days
CVE-2019-5855	Medium	6.3	Chrome	8 days
CVE-2019-5857	Medium	4.3	Chrome	8 days

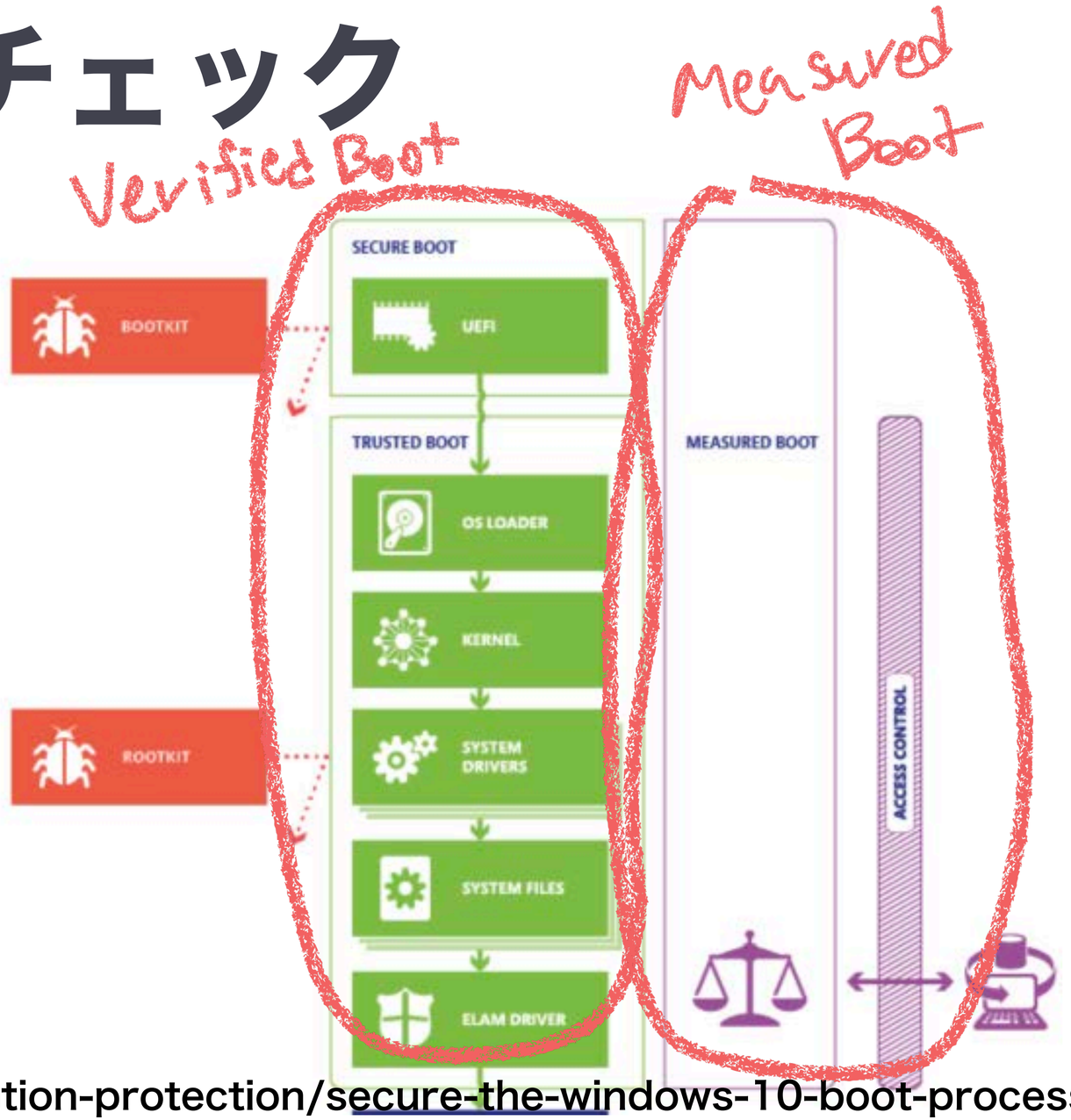
デバイスの構成情報の収集

- セキュアな状態監視のためには構成(属性)情報
  - 最後に状態確認された時間
  - 起動時間
  - ログインしたユーザー
  - HW情報
  - OSバージョン
  - SWやそのバージョン
  - ディスク暗号化の状態
  - 上記にひもづく脆弱性情報
- **健康状態の評価**



デバイスのヘルスチェック

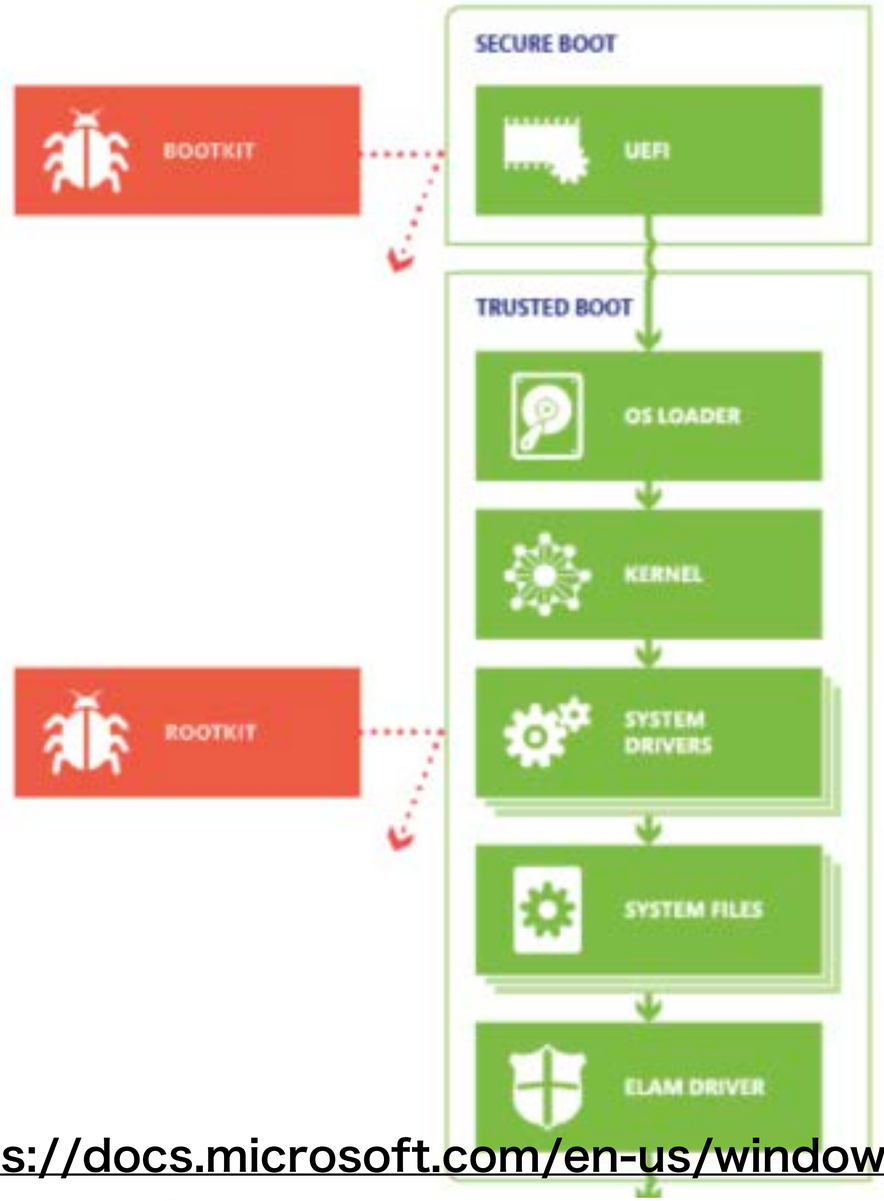
- Verified Boot
- Measured Boot



https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

Verified Boot

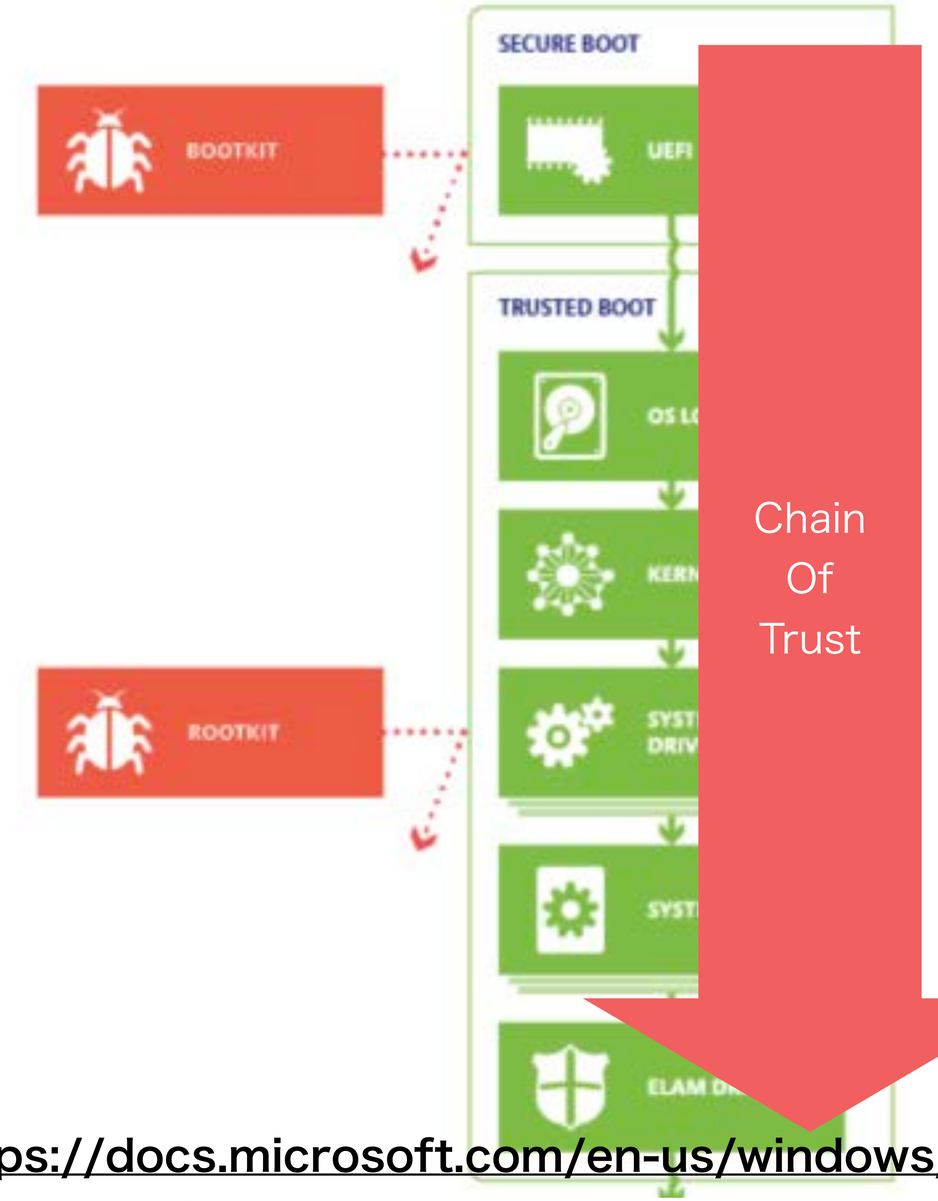
- Secure Boot
- Trusted Boot
- ELAM
  - Early Launch Anti-Malware



https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

Verified Boot

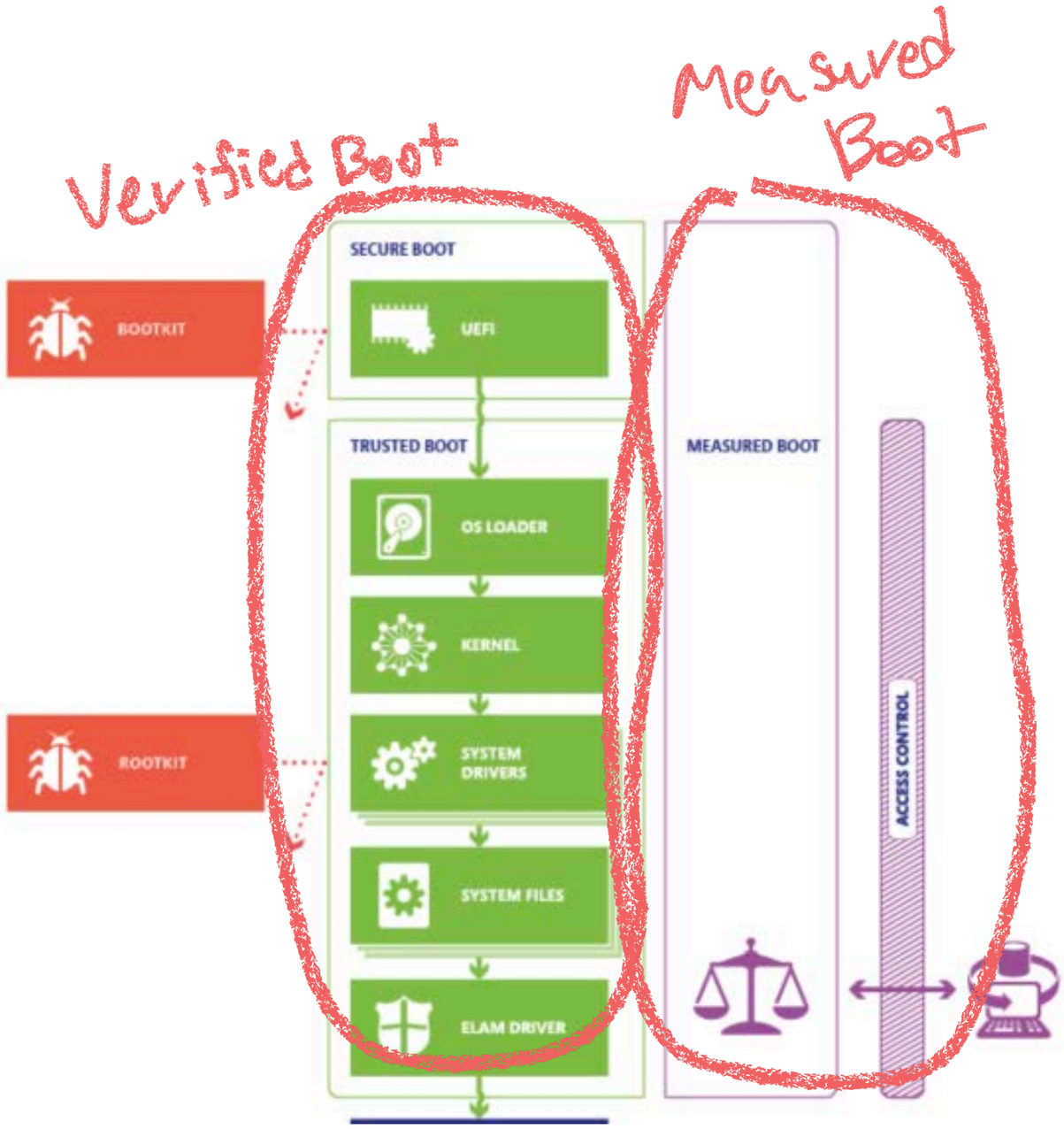
- Secure Boot
- Trusted Boot
- ELAM



https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

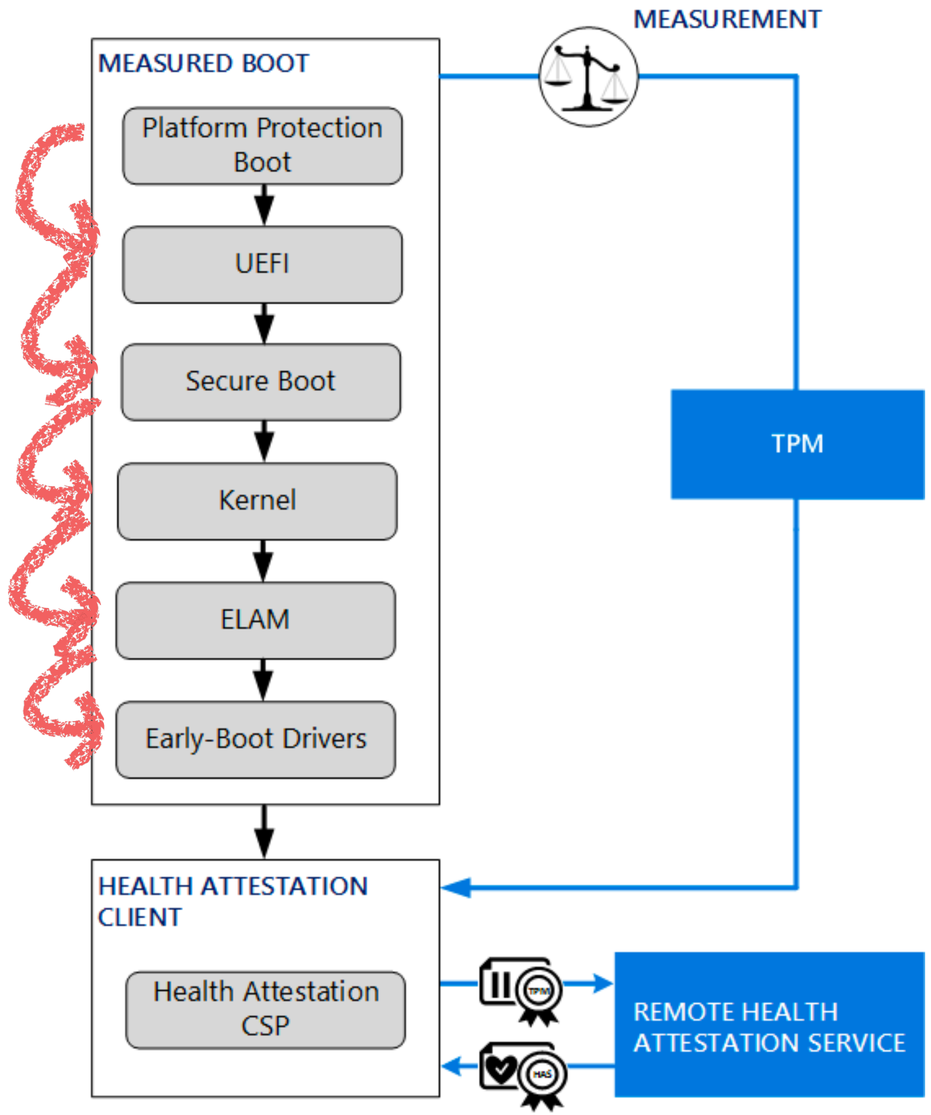
Measured Boot

- Generates immutable log which is in expression of hashes of booting compo
- Can be remotely verified
  - separation of measurem and verification



Measured Boot

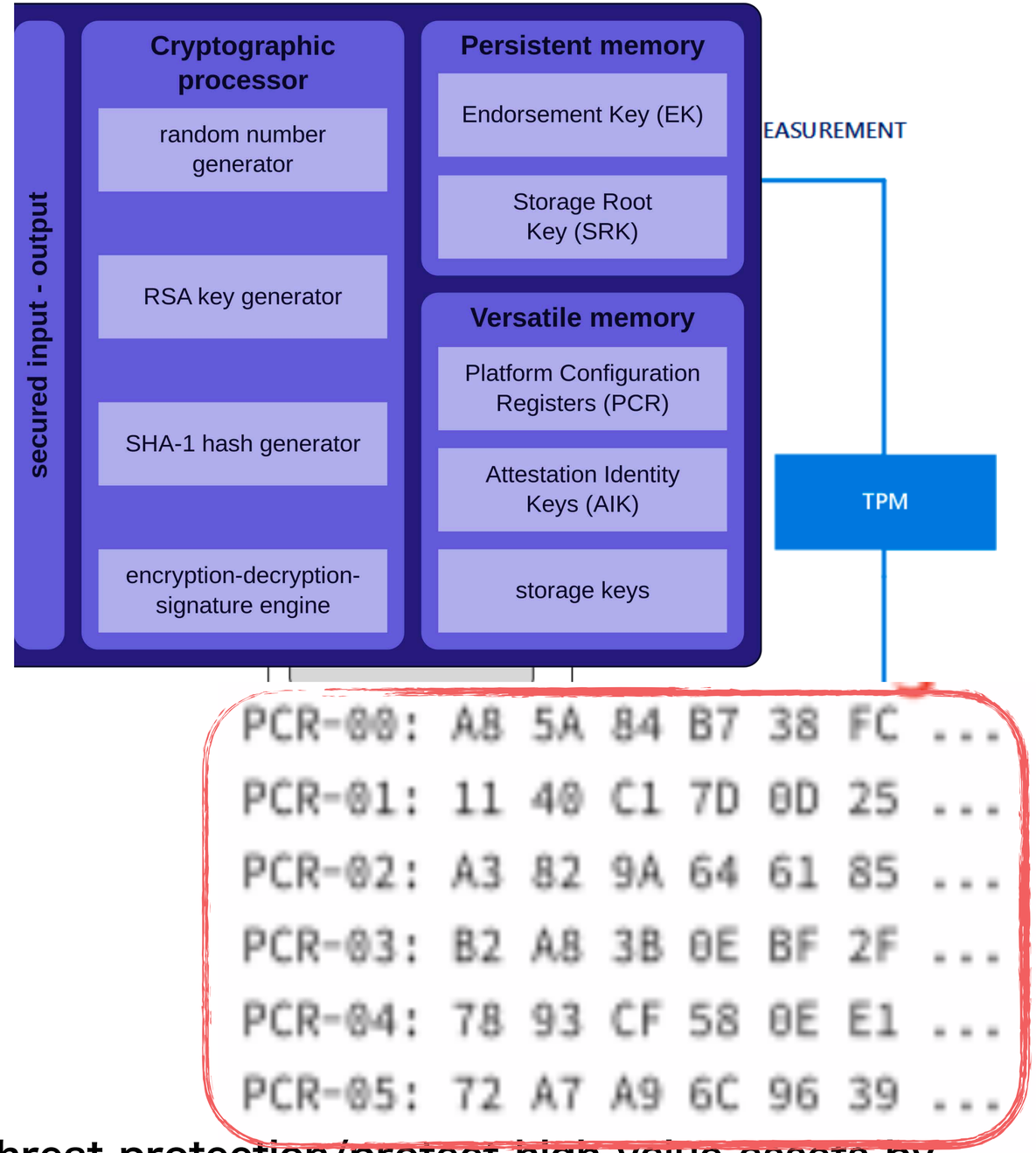
- 各ブートコンポーネントが次のコンポーネントのハッシュ値を取得
- ハッシュをTPM内のPCRに補完
- この値はログとして記録
- PCRとログを検証するコンポーネントに電子署名された上で送信



https://docs.microsoft.com/en-us/windows/security/threat-protection/protect-high-value-assets-by-controlling-the-health-of-windows-10-based-devices

Measured Boot

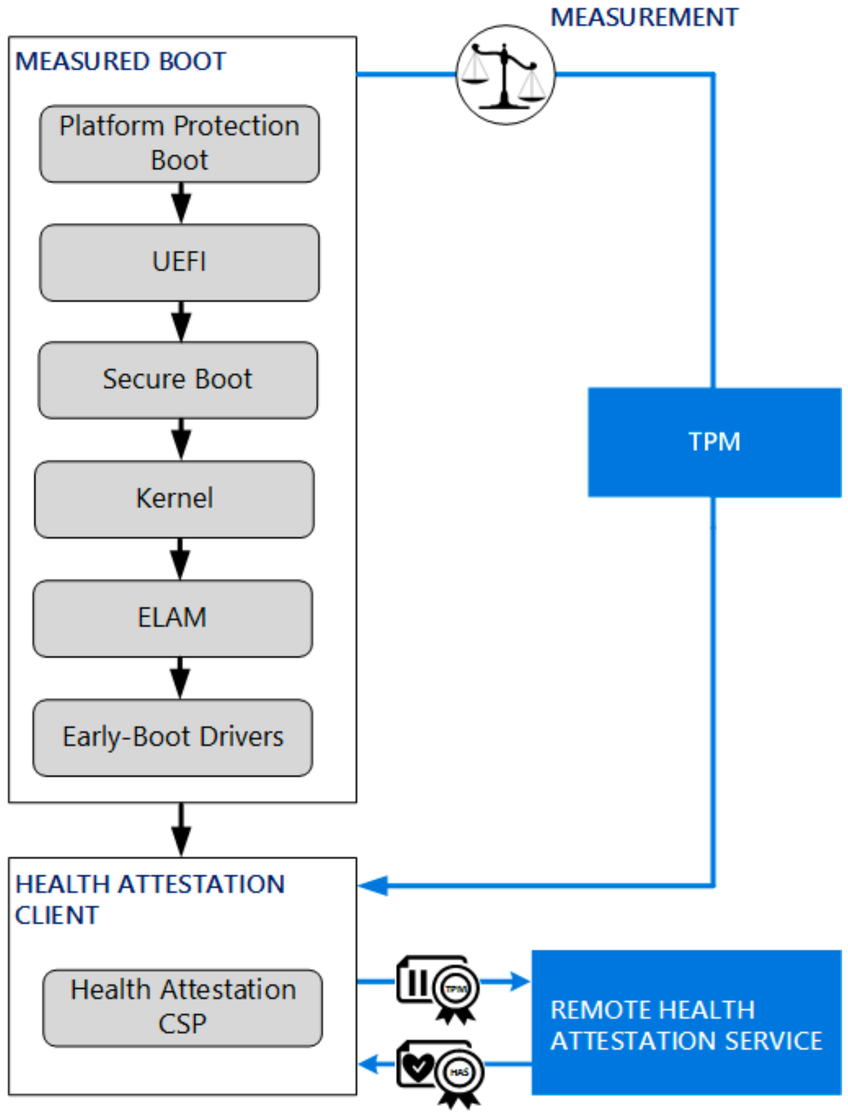
- 各ブートコンポーネントが次のコンポーネントのハッシュ値を取得
- **ハッシュをTPM内のPCRに補完**
- この値はログとして記録
- PCRとログを検証するコンポーネントに電子署名された上で送信



https://docs.microsoft.com/en-us/windows/security/threat-protection/protect-high-value-assets-by-controlling-the-health-of-windows-10-based-devices

Measured Boot

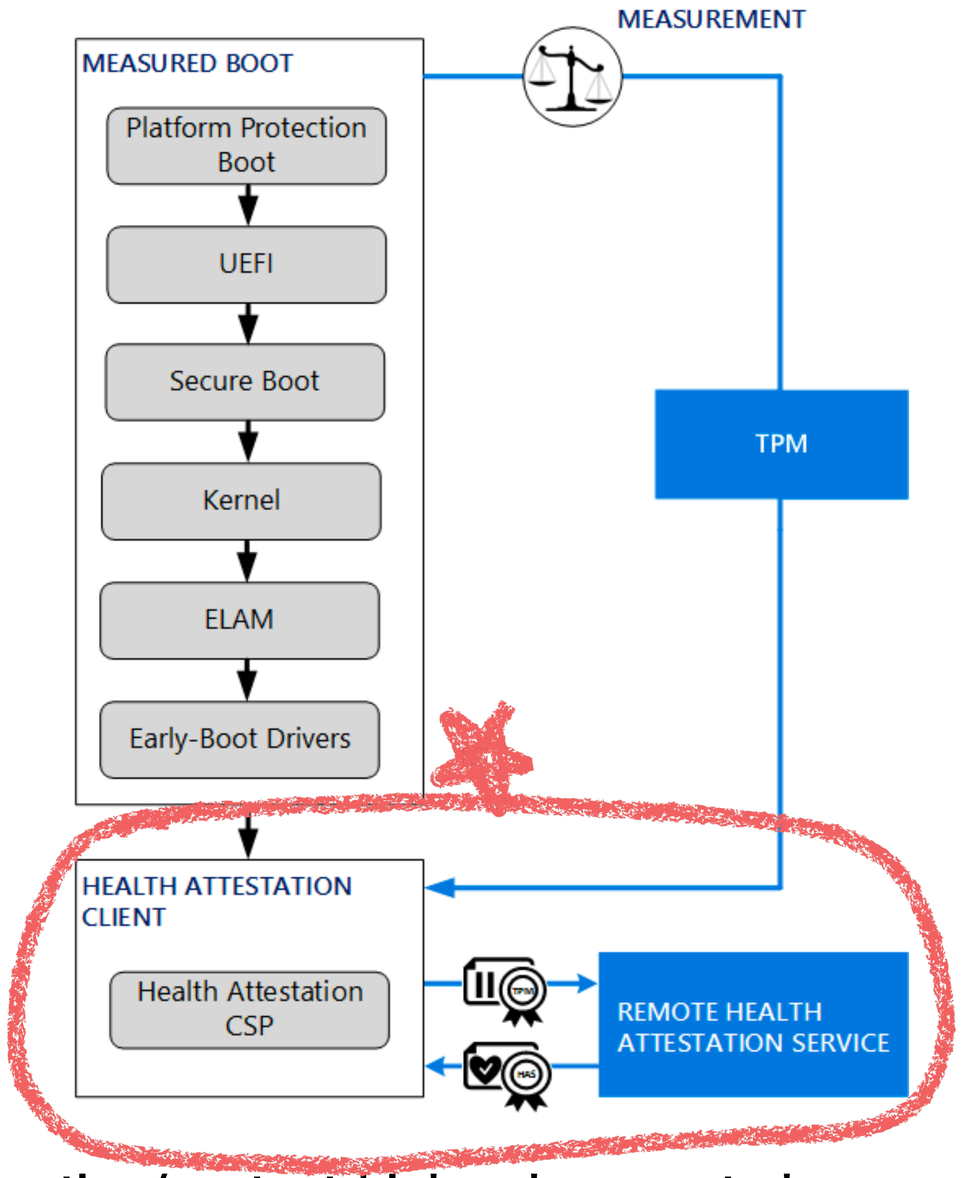
- 各ブートコンポーネントが次のコンポーネントのハッシュ値を取得
- ハッシュをTPM内のPCRに保管
- **この値はログとして記録**
- PCRとログを検証するコンポーネントに電子署名された上で送信



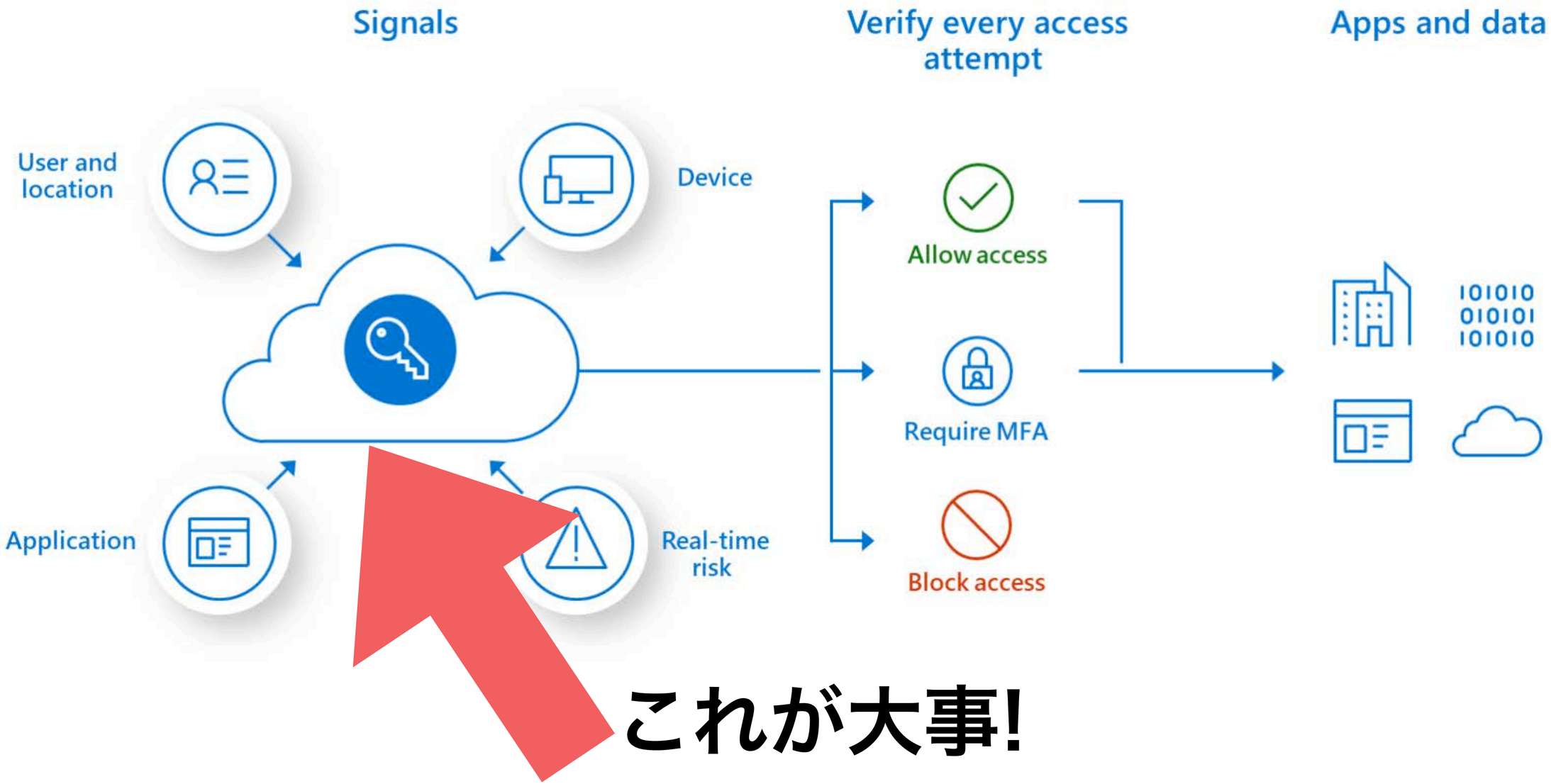
https://docs.microsoft.com/en-us/windows/security/threat-protection/protect-high-value-assets-by-controlling-the-health-of-windows-10-based-devices

Measured Boot

- 各ブートコンポーネントが次のコンポーネントのハッシュ値を取得
- ハッシュをTPM内のPCRに保管
- この値はログとして記録
- **PCRとログを検証するコンポーネントに電子署名された上で送信**
  - **Remote Health Attestation**



https://docs.microsoft.com/en-us/windows/security/threat-protection/protect-high-value-assets-by-controlling-the-health-of-windows-10-based-devices


Signals
Verify every access attempt
Apps and data
User and location
Device
Application
Real-time risk
Allow access
Require MFA
Block access
101010
010101
101010

これが大事!

SP800-171:　民間企業が講じるべきセキュリティ対策の要件

1. アクセス制御
2. 意識向上と訓練
3. 監査と責任追認性
4. 構成管理
5. 識別と認証
6. インシデント対応
7. メンテナンス
8. メディア保護
9. 人的セキュリティ
10. 物理的保護
11. リスクアセスメント
12. セキュリティアセスメント
13. システムと通信の保護
14. システムと情報の完全性

ここまでのまとめ

個別のデータソースおよび管理ツール間でデータ連携できないと、

最終的に確保したい信頼が下がる or 工数が極端に上がる

ゼロトラストしたくなった
何をどうする

VPN捨てました
は
ゼロトラストではない

現在の技術で実装できる部分的なもの

- 社内外のID管理の為の基盤作成（統合認証環境）
- トラストデバイスの作り込みと統制
- トラストアプリケーション決めと統制
- 物理の排除とクラウド化

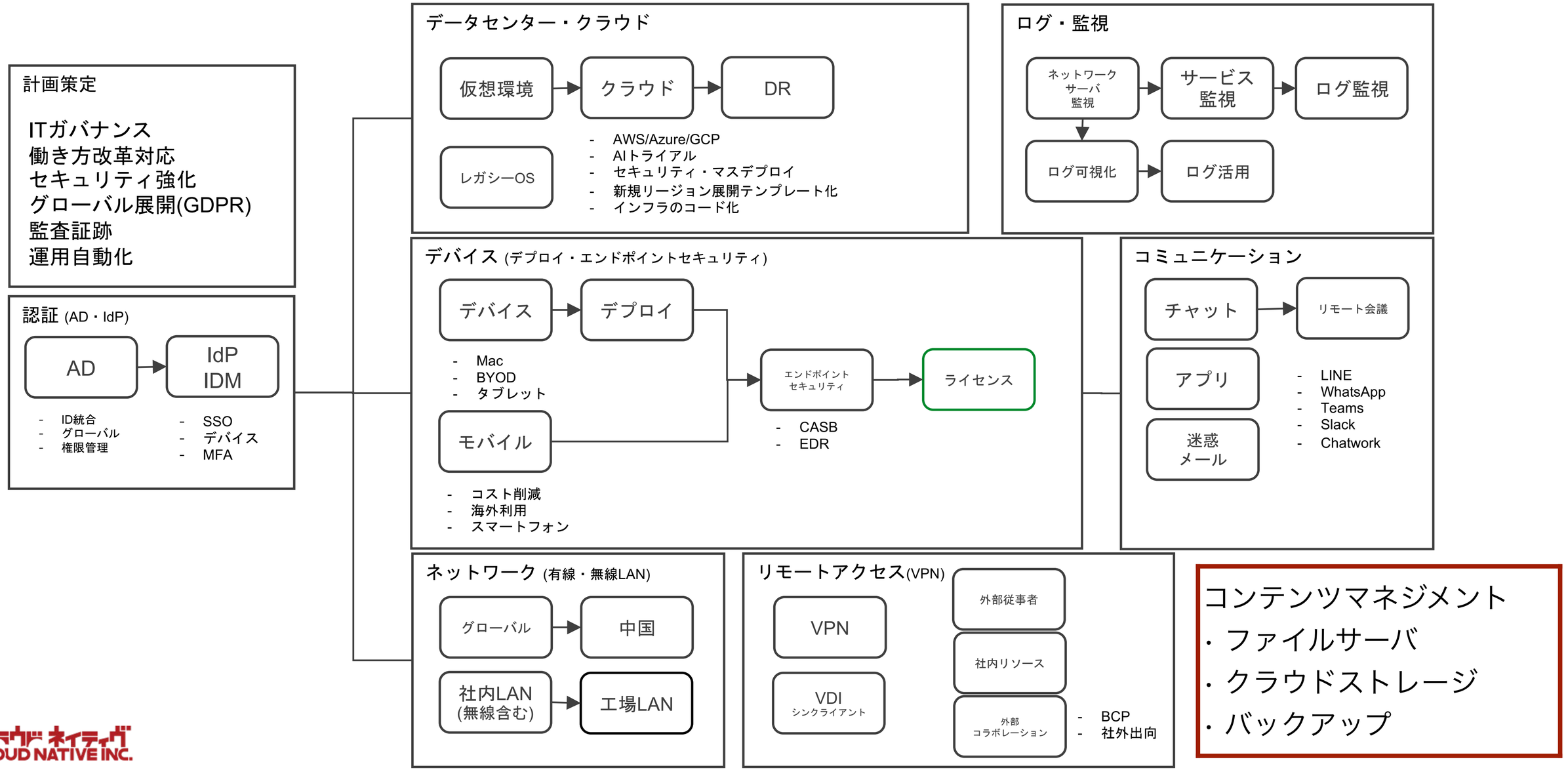
トラストできるならBYODかどうかは関係無い

現在の技術で難しいものオシイもの

- アクセス先サービスの完全なマイクロサービス化
- 厳密な信頼度スコアの計算
- 動的ポリシーの適用と積極的な証明書破棄
- クラウドサービス側でセキュリティが高額
- OSでばらける対応非対応
- 複合機やIoTという地獄

トラストアンカーが沢山設置されることになる

ゼロトラストの範囲はIT守備範囲全部



クラウドネイティブ
CLOUD NATIVE INC.

ロードマップの作成

真っ先にやるべきは統合ID管理基盤

他の優先度が高くてもIDは絶対、これは絶対

並行して進めるのはありよりのあり

統合ID基盤の構築

統合ID基盤の構築

・既に既存の何かがある場合
それでよかったっけ、再検討

・何もない場合
このケースはまずありえない

統合ID基盤の構築

よくあるケース

- Active Directory（オンプレ）
- Azure AD（Office365）
- G Suite

統合ID基盤の構築

絶対に悩むポイント

人事のID基盤との連携
社員ではないIDの扱い

統合ID基盤、作り方のコツ

クラウド化

ADやIdPは複数あっても良い

ただし可能な限り1つに

統合ID基盤の構築

SAMLなIdP基盤を持っても

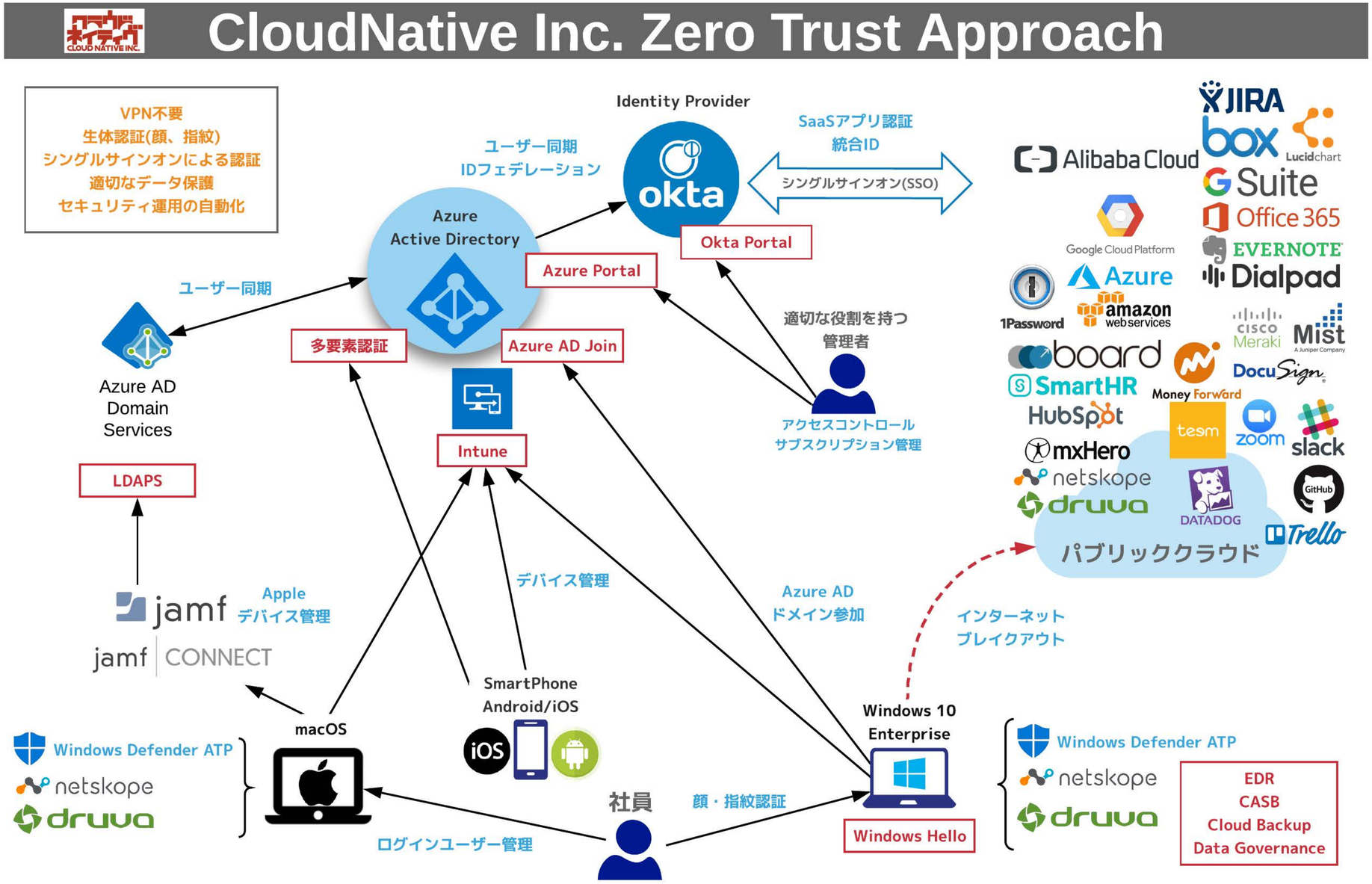
繋ぐ先が喋らなければ意味がない？

ユーザ属性

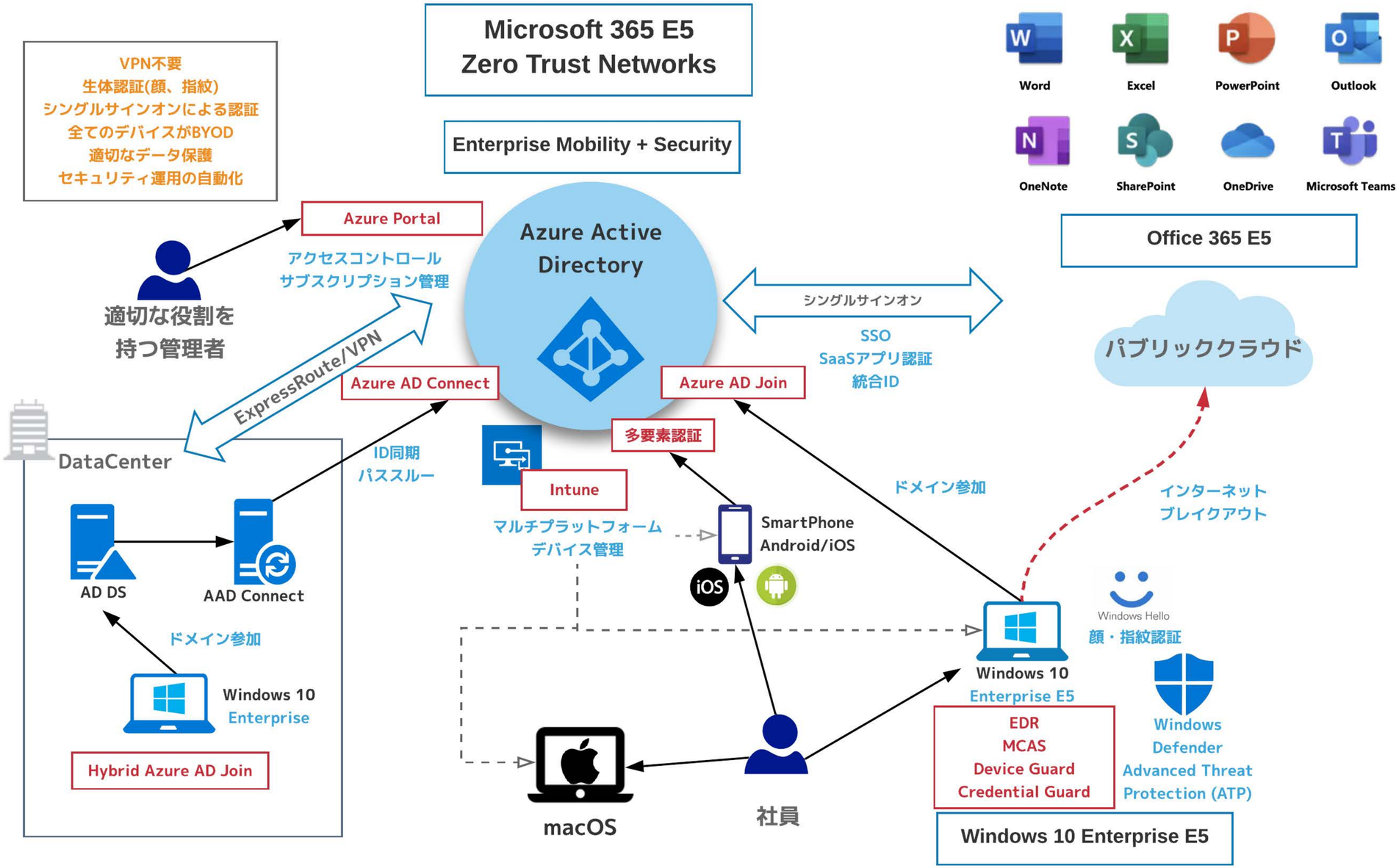
デバイス属性

認証（認可）

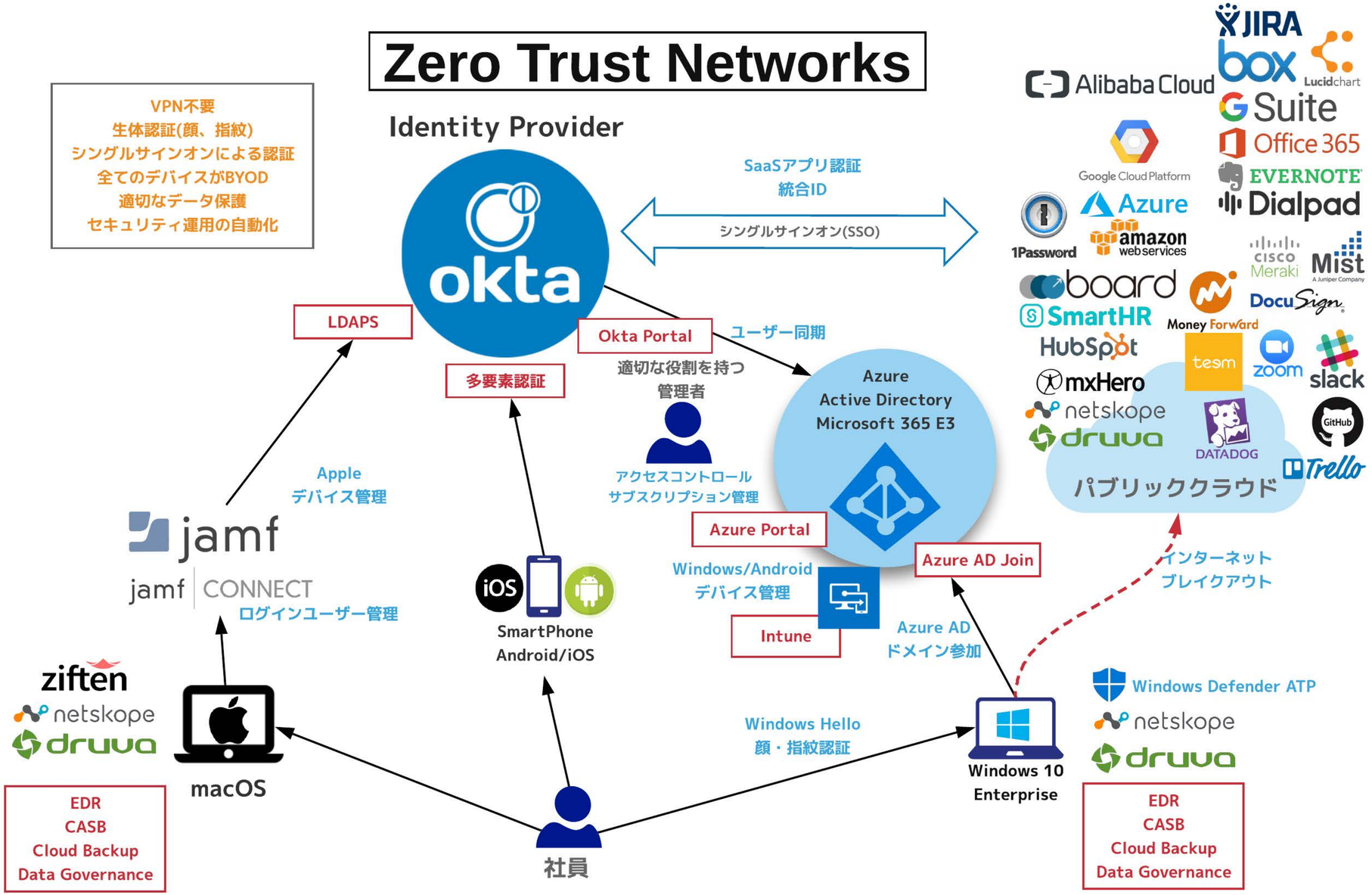
統合ID基盤の構築


CloudNative Inc. Zero Trust Approach
VPN不要
生体認証(顔、指紋)
シングルサインオンによる認証
適切なデータ保護
セキュリティ運用の自動化
Identity Provider
ユーザー同期
IDフェデレーション
SaaSアプリ認証
統合ID
シングルサインオン(SSO)
okta
Okta Portal
Azure
Active Directory
Azure Portal
ユーザー同期
Azure AD
Domain
Services
多要素認証
Azure AD Join
Intune
適切な役割を持つ
管理者
アクセスコントロール
サブスクリプション管理
LDAPS
jamf
Apple
デバイス管理
jamf CONNECT
デバイス管理
Azure AD
ドメイン参加
インターネット
ブレイクアウト
SmartPhone
Android/iOS
iOS
macOS
Windows 10
Enterprise
Windows Defender ATP
netskope
druva
社員
顔・指紋認証
ログインユーザー管理
Windows Hello
Windows Defender ATP
netskope
druva
EDR
CASB
Cloud Backup
Data Governance
パブリッククラウド
Alibaba Cloud
JIRA
box
Lucidchart
G Suite
Office 365
EVERNOTE
Dialpad
Google Cloud Platform
Azure
1Password
amazon web services
CISCO Meraki
Mist
board
SmartHR
Money Forward
DocuSign
HubSpot
tesm
zoom
slack
mxHero
netskope
druva
DATADOG
GitHub
Trello

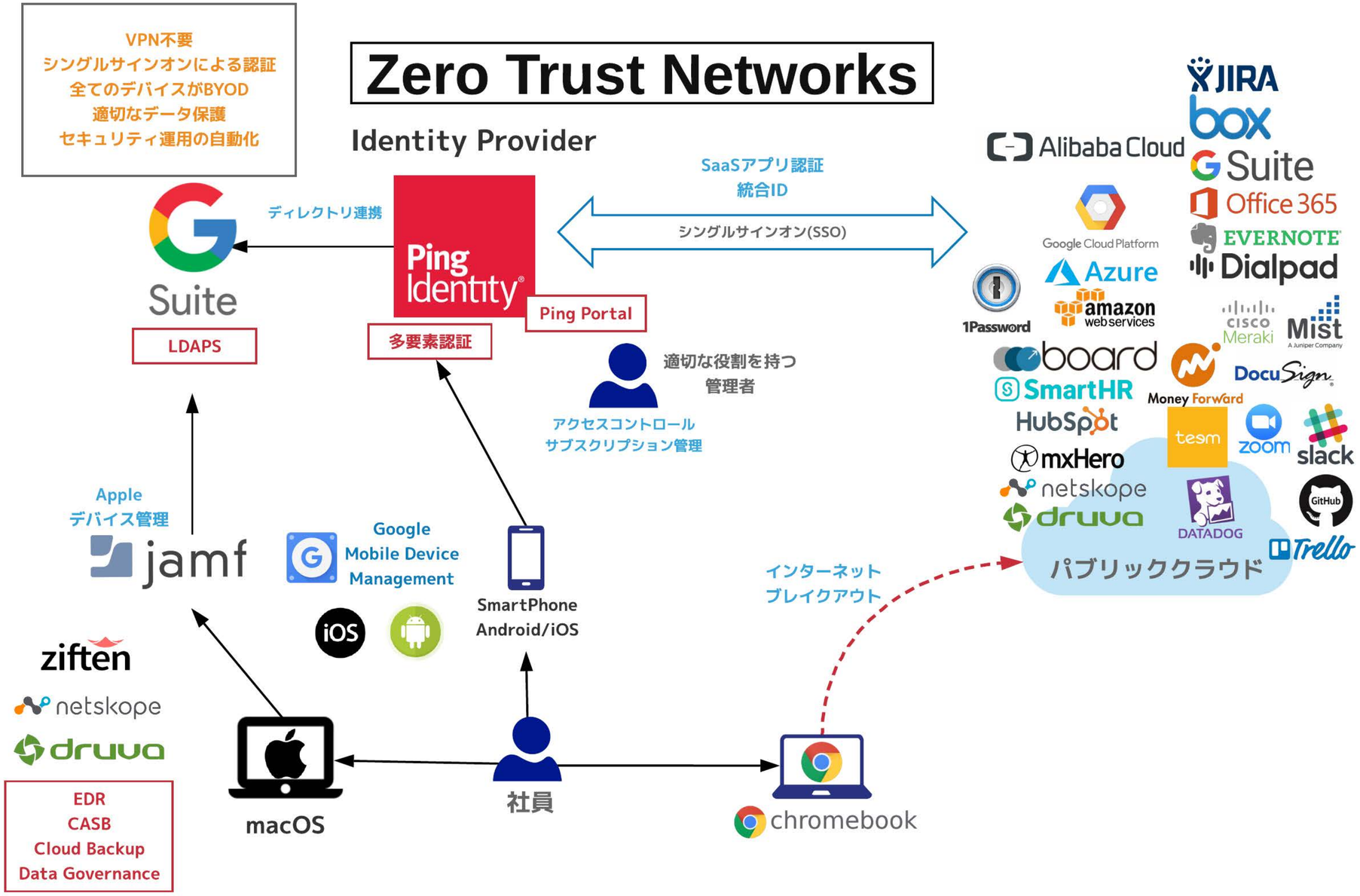
統合ID基盤の構築


VPN不要
生体認証(顔、指紋)
シングルサインオンによる認証
全てのデバイスがBYOD
適切なデータ保護
セキュリティ運用の自動化
Microsoft 365 E5
Zero Trust Networks
Enterprise Mobility + Security
Word
Excel
PowerPoint
Outlook
OneNote
SharePoint
OneDrive
Microsoft Teams
Office 365 E5
Azure Portal
アクセスコントロール
サブスクリプション管理
適切な役割を
持つ管理者
Azure Active
Directory
シングルサインオン
SSO
SaaSアプリ認証
統合ID
パブリッククラウド
ExpressRoute/VPN
Azure AD Connect
Azure AD Join
多要素認証
DataCenter
ID同期
パススルー
Intune
マルチプラットフォーム
デバイス管理
SmartPhone
Android/iOS
iOS
ドメイン参加
インターネット
ブレイクアウト
AD DS
AAD Connect
ドメイン参加
Windows Hello
顔・指紋認証
Windows 10
Enterprise
Windows 10
Enterprise E5
EDR
MCAS
Device Guard
Credential Guard
Windows
Defender
Advanced Threat
Protection (ATP)
Hybrid Azure AD Join
macOS
社員
Windows 10 Enterprise E5

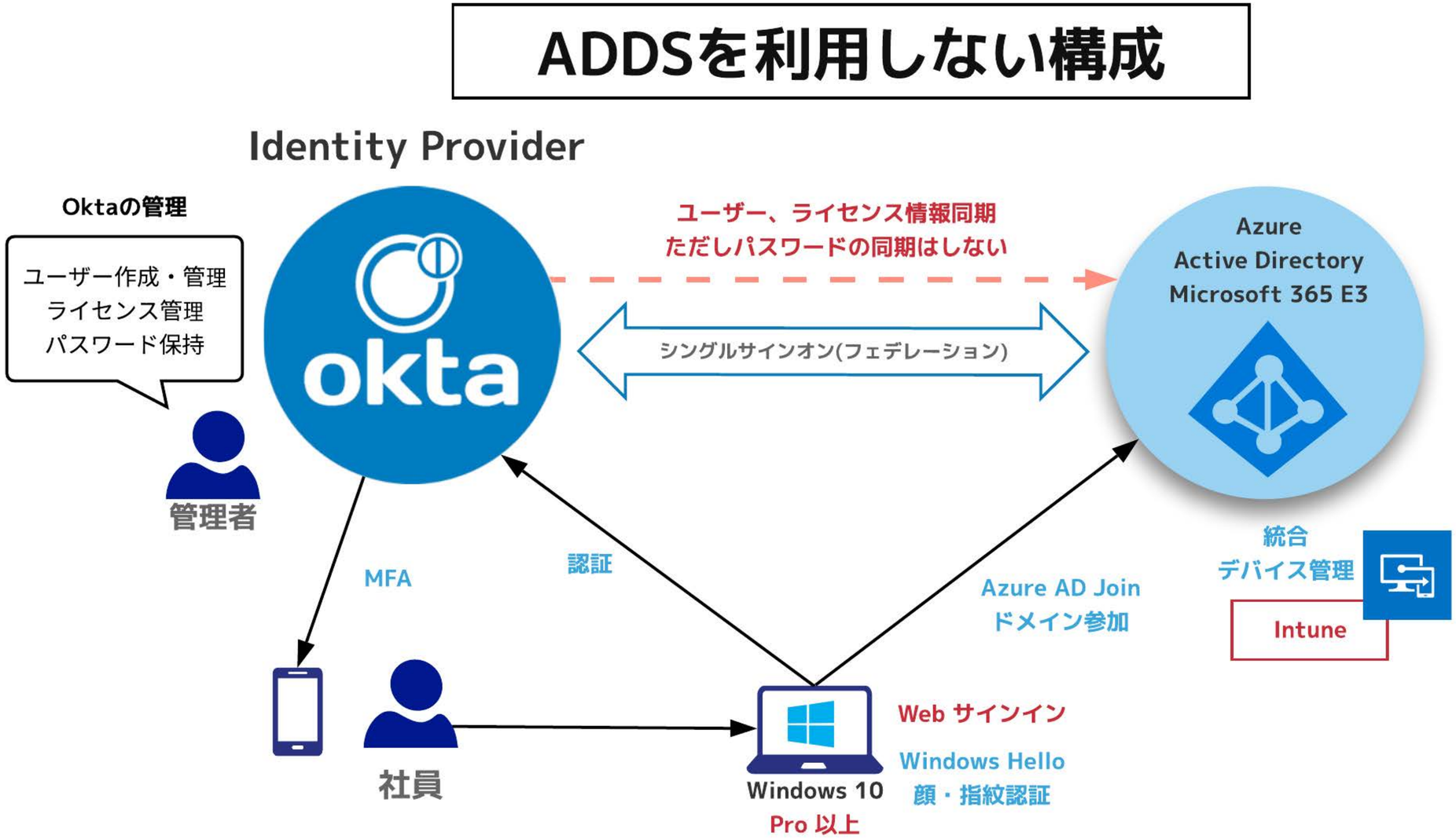
統合ID基盤の構築


Zero Trust Networks
VPN不要
生体認証(顔、指紋)
シングルサインオンによる認証
全てのデバイスがBYOD
適切なデータ保護
セキュリティ運用の自動化
Identity Provider
okta
SaaSアプリ認証
統合ID
シングルサインオン(SSO)
LDAPS
Okta Portal
ユーザー同期
多要素認証
適切な役割を持つ
管理者
Azure
Active Directory
Microsoft 365 E3
Azure Portal
アクセスコントロール
サブスクリプション管理
Apple
デバイス管理
jamf
jamf CONNECT
ログインユーザー管理
iOS
SmartPhone
Android/iOS
Windows/Android
デバイス管理
Intune
Azure AD Join
Azure AD
ドメイン参加
インターネット
ブレイクアウト
パブリッククラウド
Alibaba Cloud
JIRA
box
Lucidchart
G Suite
Office 365
Google Cloud Platform
EVERNOTE
Azure
Dialpad
1Password
amazon web services
CISCO Meraki
Mist
board
DocuSign
SmartHR
Money Forward
HubSpot
tesm
zoom
slack
mxHero
netskope
druva
DATADOG
GitHub
Trello
ziften
netskope
druva
macOS
EDR
CASB
Cloud Backup
Data Governance
Windows Hello
顔・指紋認証
社員
Windows 10
Enterprise
Windows Defender ATP
netskope
druva
EDR
CASB
Cloud Backup
Data Governance

統合ID基盤の構築


VPN不要
シングルサインオンによる認証
全てのデバイスがBYOD
適切なデータ保護
セキュリティ運用の自動化
Zero Trust Networks
Identity Provider
SaaSアプリ認証
統合ID
シングルサインオン(SSO)
ディレクトリ連携
Ping Identity
Ping Portal
多要素認証
G Suite
LDAPS
適切な役割を持つ
管理者
アクセスコントロール
サブスクリプション管理
Apple
デバイス管理
jamf
Google
Mobile Device
Management
iOS
SmartPhone
Android/iOS
インターネット
ブレイクアウト
パブリッククラウド
JIRA
box
G Suite
Office 365
EVERNOTE
Dialpad
Alibaba Cloud
Google Cloud Platform
Azure
amazon web services
1Password
cisco Meraki
Mist
board
SmartHR
Money Forward
DocuSign
HubSpot
tesm
zoom
slack
mxHero
netskope
druva
DATADOG
GitHub
Trello
ziften
netskope
druva
EDR
CASB
Cloud Backup
Data Governance
macOS
社員
chromebook

統合ID基盤の構築


ADDSを利用しない構成
Identity Provider
Oktaの管理
ユーザー作成・管理
ライセンス管理
パスワード保持
okta
ユーザー、ライセンス情報同期
ただしパスワードの同期はしない
シングルサインオン(フェデレーション)
Azure
Active Directory
Microsoft 365 E3
管理者
MFA
認証
Azure AD Join
ドメイン参加
統合
デバイス管理
Intune
社員
Web サインイン
Windows Hello
顔・指紋認証
Windows 10
Pro 以上

統合ID基盤の構築

MFAデバイスどうする問題

私物スマホor会社支給スマホ
Yubikey
SMSと電話は非現実的

統合ID基盤の構築

IdPの選び方
どれがいいとかあんまりない
世界で戦えてるサービスかどうか

AzureAD P1P2, Okta, Ping Identity, Auth0

OneLogin, G Suite, Lastpass Enterprise…

デバイスの統制

デバイスの統制

管理対象を定義する
会社のデータにアクセスできる端末
MFAだけなら対象外

保存、持ち出し、ではなくアクセス

デバイスの統制

デバイスは製造元と流通経路を
信頼するしかない（トラストアンカー）

戦略的なデバイス固定もありよりのあり

デバイスの統制

Apple	Jamf Pro
Win10 Pro	Intune
Chromebook	G Suite
Android	Android Enteprise
それ以外	諦めよう

デバイストラスト
（オプション）

デバイストラスト

IdPもしくはアプリ、
データへのアクセス時のポリシー定義

デバイストラスト

よくやる構成(Intune)

- OSバージョン
- ディスク暗号化
- 脱獄andRoot化
- 不要機能無効化
- USBストレージOFF/RO
- AppLocker（アプリ禁止）
- 証明書配付
- Endpoint Protection関係

- ブラウザ設定（Chromeとか
- Microsoftストア制御
- Defender ATPぶっこみ
- WinUpdate制御
- Edgeのデフォルトサーチエンジンをgoogleに変える
- ロック画面強制
- ログイン画面でのセルフパスワードリセット

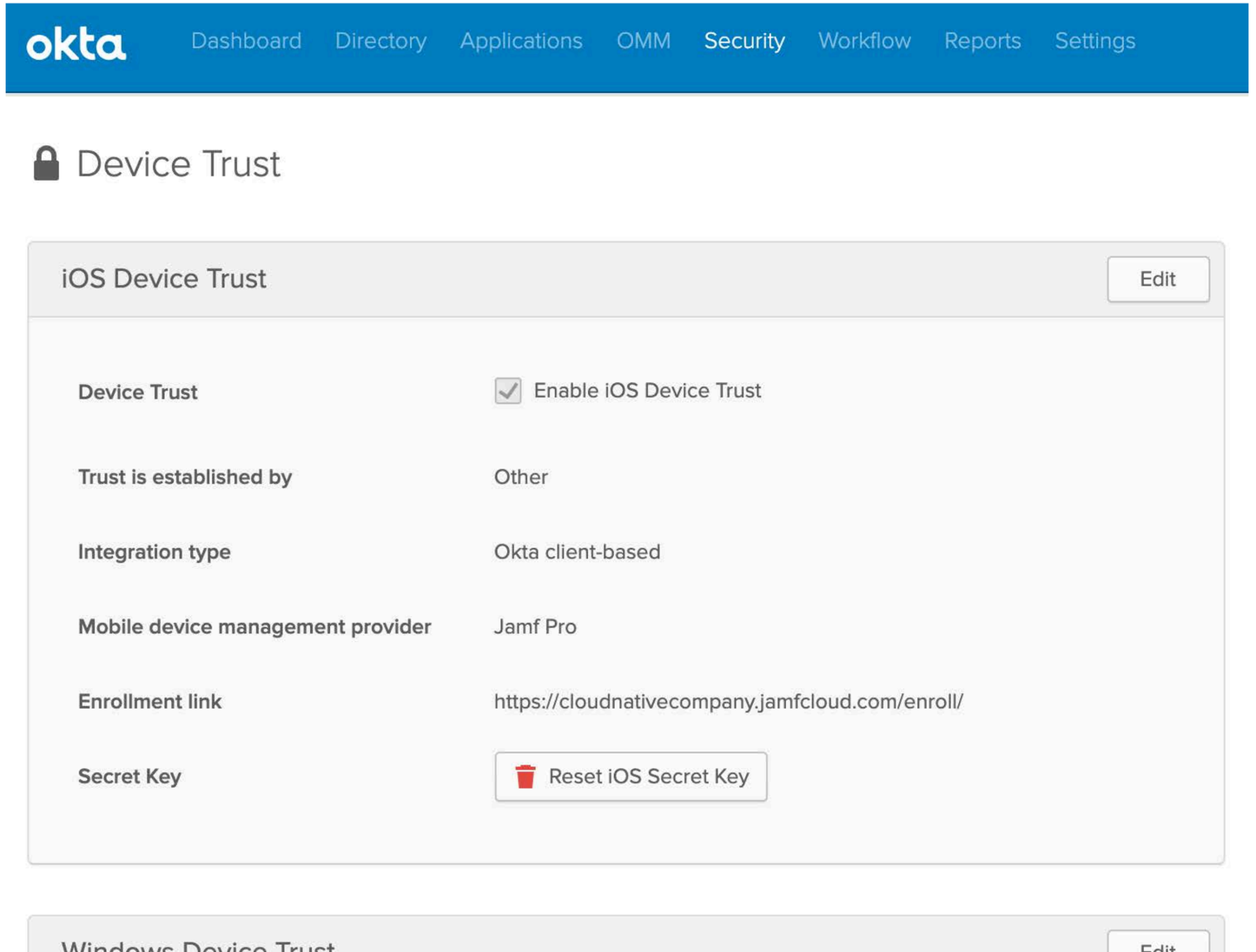
デバイストラスト

よくやる構成(Jamf Pro)

- OSバージョン
- ディスク暗号化
- コンピュータ名変更
- アプリインストール
- brewコントロール
- 証明書配付
- Endpoint Protection関係

デバイストラスト

よくやる構成(IdP)(Okta)



デバイストラスト

Boxにもあるんだが…

マスデプロイ環境

マスデプロイ環境

設定やアプリを一括制御

デバイス暗号化鍵の管理

脆弱アプリのバージョン制御

ゼロタッチデプロイ

データ破棄エビデンス

AuditLog

デバイスの統制

Apple	Jamf Pro
Win10 Pro	Intune AutoPilot
Chromebook	G Suite
Android	Android Enteprise
それ以外	諦めよう

マスデプロイ環境

Windows10の場合

製造元から送られるデバイスIDを
AzureADに取り込むことでゼロタッチデプロイ
ゼロタッチは必須ではない

AzureAD JoinあるいはHybrid AD Join
Intuneがコントロール

マスデプロイ環境

macOSの場合

Apple Business Manager(旧DEP)を利用

Jamf ProにデバイスIDを取り込むとゼロタッチ

ゼロタッチは必須ではない

Jamf Pro単体ではデバイスしか見ない

Intune連携、Jamf Connectでユーザも

マスデプロイ環境

Androidの場合

Android Enterpriseを利用

G Suite, Cloud Identity, O365

対応デバイス、対応EMMが存在

例えばIntuneやVMwareが対応

G Suiteも

フル機能使うには初期化必須

マスデプロイ環境

iOSの場合

Apple Business Manager(旧DEP)を利用

Jamf ProにデバイスIDを取り込むとゼロタッチ

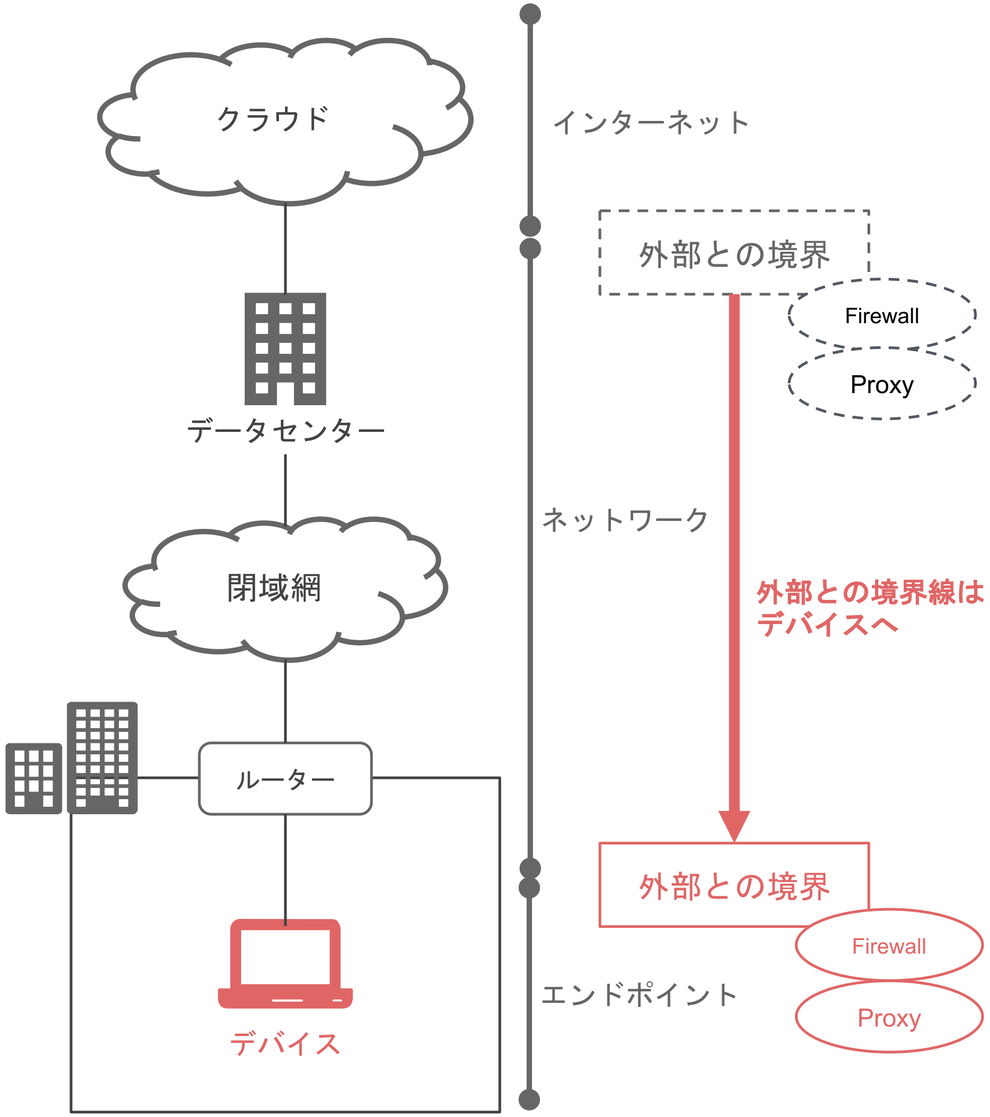
ゼロタッチは必須ではない

端末にプロファイルをインストールする

フル機能使うには初期化必須

エンドポイントセキュリティ
EDR/XDR

改善 - エンドポイントセキュリティ導入によるネットワークの境界の変化



外部との境界が 「ネットワーク」	外部との境界が 「エンドポイント」
自社のネットワーク以外は セキュリティが担保できない	セキュリティはエンドポイントで担保 場所やネットワークに依存しない
自社のネットワークでセキュリティを担保 VPNが必要	どこからでも安全に インターネットへアクセスできるようになる
ルールが厳しくシャドーITが発生	適切な監視により自由な環境を提供 = シャドーITの撲滅
大規模な回線やプロキシの増強対応が必要	拠点ごとの小規模な増強の対応
自社のネットワークのすべてのエリアで 安全性を確保する必要がある	守るべきネットワークの範囲が限定的 必要な箇所のみ保護する

ネットワークが持っている機能をエンドポイントに寄せることで
セキュリティと利便性が向上する
リモートワークでもセキュアな環境になる

クラウドネイティブ
CLOUD NATIVE INC.

エンドポイントセキュリティ

アンチウイルスとかどうでもいい

EDR/XDRが大前提

学習データをテナント共有できるか

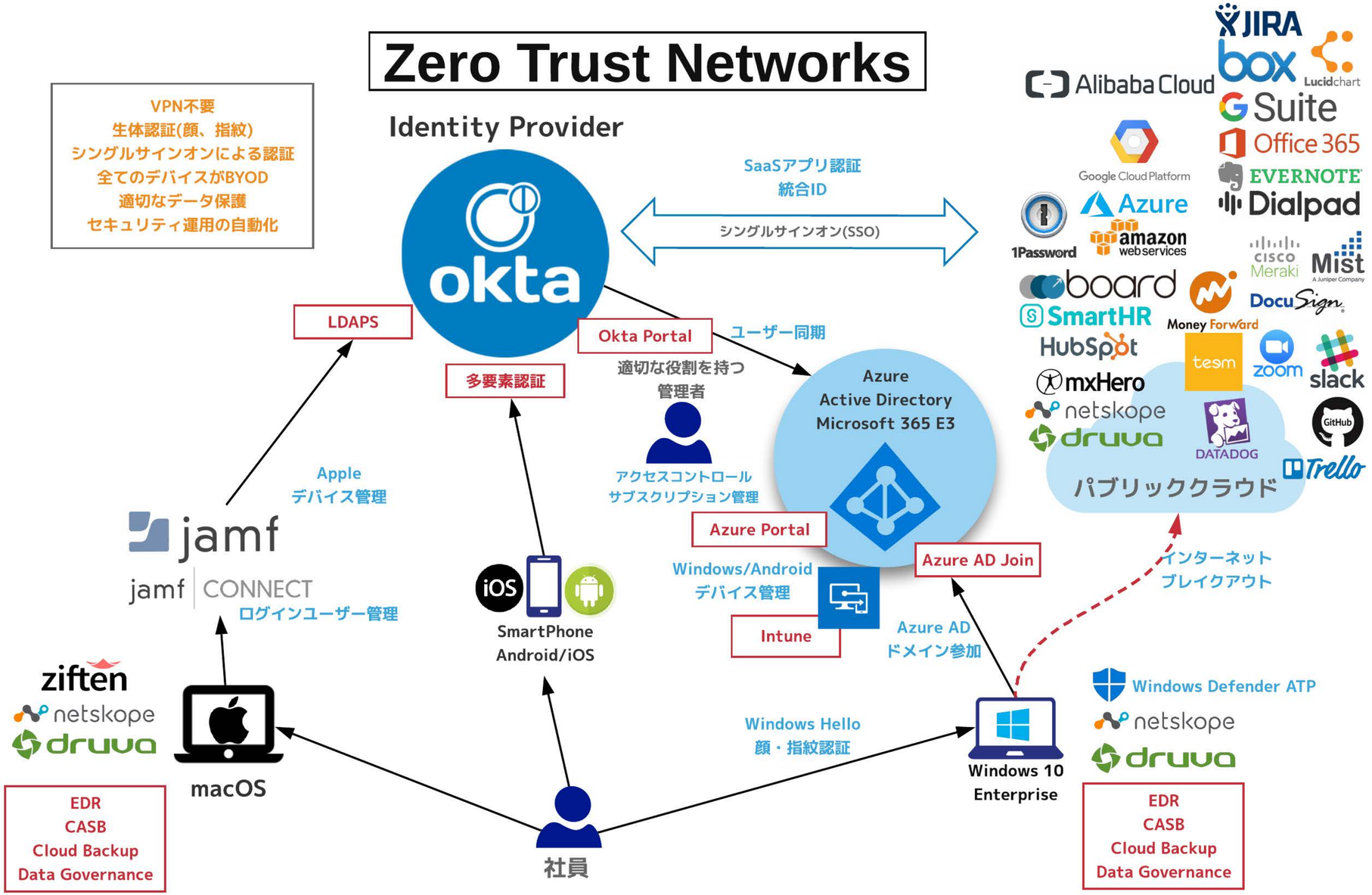
誤検知との戦い

（後ほどSIEMの話）

エンドポイントセキュリティ

Apple	Microsoft Defender ATP CrowdStrike…etc
Win10 Pro	Microsoft Defender ATP CrowdStrike…etc
Chromebook	不要
Android	Microsoft Defender ATP
それ以外	諦めよう

エンドポイントセキュリティ



エンドポイントセキュリティ
CASB

エンドポイントセキュリティ

接続先クラウドサービスへの制御
そのコンテンツは、そこにあってよいか
許可・拒否 ではない
コントロール
シャドーITを武器にできるNot許容

エンドポイントセキュリティ

Netskope

MCAS

Akamai EAA

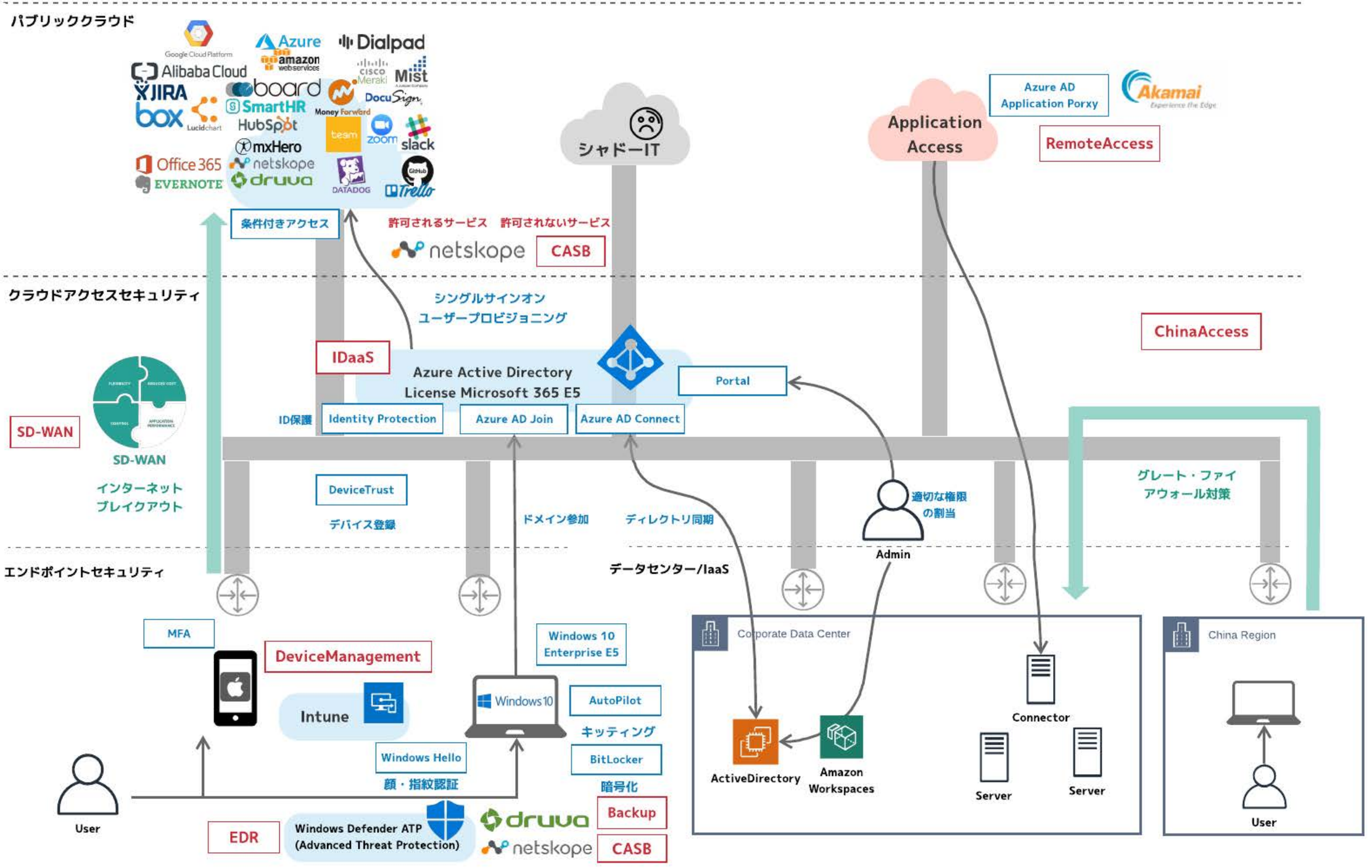
Zscaler

Skyhigh, Bitglass, Palo

エンドポイントセキュリティ

CASBをどこで効かせるか
エンドポイント、リバプロ

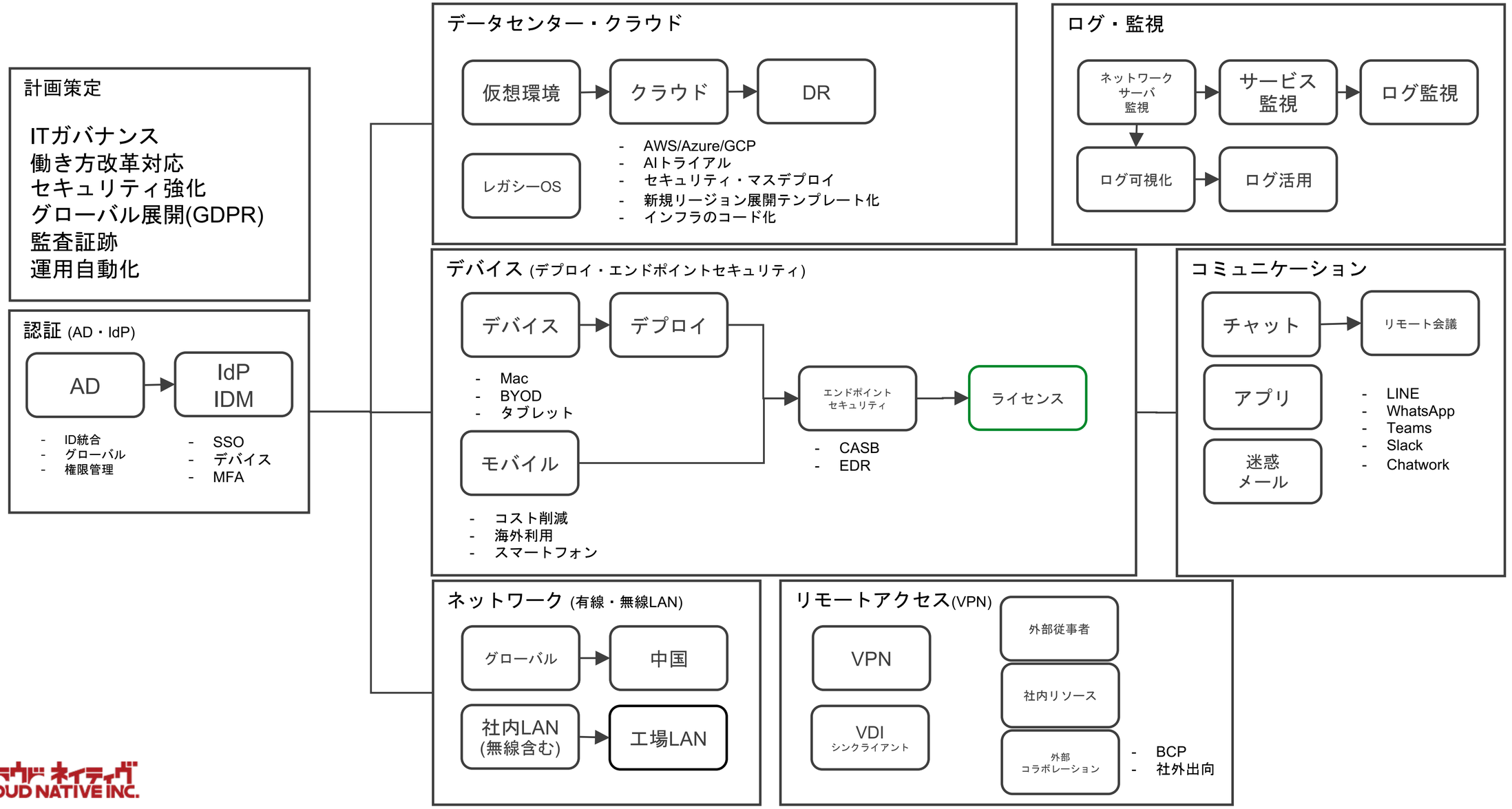
CASBをどう運用するか
SOCと同じ


パブリッククラウド
Google Cloud Platform
Azure
amazon web services
Dialpad
Alibaba Cloud
cisco Meraki
Mist
JIRA
box
Lucidchart
board
SmartHR
Money Forward
DocuSign
HubSpot
team
zoom
slack
mxHero
netskope
druva
Office 365
EVERNOTE
DATADOG
GitHub
Trello
シャドーIT
Application Access
Azure AD Application Porxy
Akamai
Experience the Edge
RemoteAccess
条件付きアクセス
許可されるサービス　許可されないサービス
netskope
CASB
クラウドアクセスセキュリティ
シングルサインオン
ユーザープロビジョニング
ChinaAccess
IDaaS
Azure Active Directory
License Microsoft 365 E5
Portal
ID保護
Identity Protection
Azure AD Join
Azure AD Connect
SD-WAN
SD-WAN
インターネット
ブレイクアウト
DeviceTrust
デバイス登録
ドメイン参加
ディレクトリ同期
適切な権限
の割当
Admin
グレート・ファイ
アウォール対策
エンドポイントセキュリティ
データセンター/IaaS
MFA
DeviceManagement
Windows 10
Enterprise E5
Intune
Windows10
AutoPilot
キッティング
BitLocker
暗号化
Windows Hello
顔・指紋認証
User
EDR
Windows Defender ATP
(Advanced Threat Protection)
druva
Backup
netskope
CASB
Corporate Data Center
ActiveDirectory
Amazon
Workspaces
Connector
Server
Server
China Region
User

CASB運用設計のコツ

- 制御よりも可視化を最優先
- 規模でかいなら外注で24/365
- ユーザトラブルへの対処
- 制御より業務優先<bypass
- 接続先サービス評価は定例で

エンドポイントセキュリティ



クラウドネイティブ
CLOUD NATIVE INC.

コンテンツマネジメント

コンテンツマネジメント

守りたいのはデータ

データが守れる証明あれば
端末とかなくなってもどうでもいい
データ＝コンテンツ

コンテンツマネジメント

代表的な保存先

- オンプレの何か
- それぞれの端末
- メールサーバ
- OneDrive, Google Drive, Box, Dropbox

コンテンツマネジメント

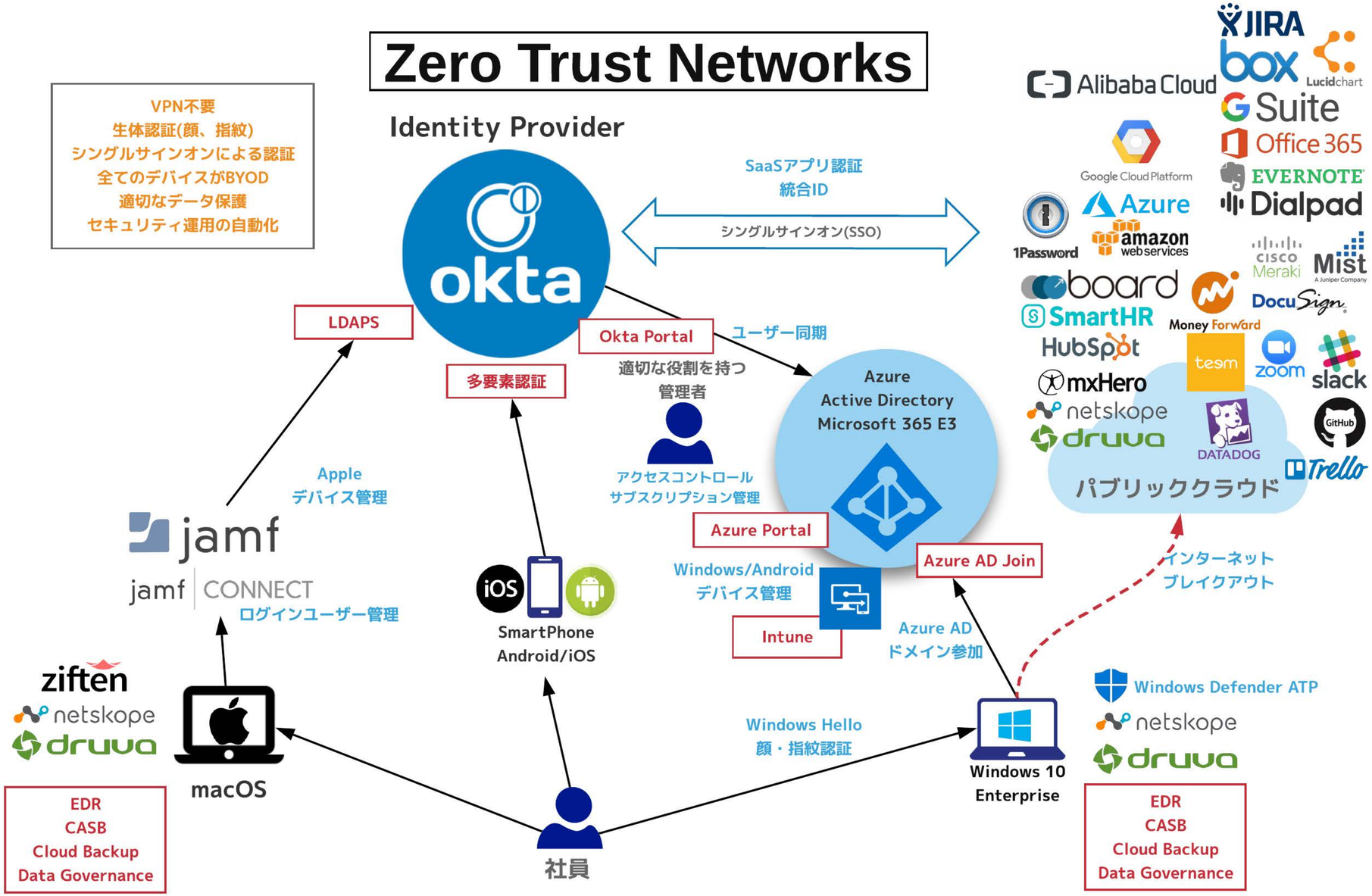
分散しがちな保存先

- Slack, LINE, Chatwork
- Zoom, Teams
- SNS
- 課題管理ツールJIRA, Backlog
- 個人利用クラウドEvernoteとか

コンテンツマネジメント

データの価値判断は？
コントロールプレーンを何にする？

コンテンツマネジメント



コンテンツマネジメント

ユーザーの検索

管理コンソール

- インサイト
- ユーザーとグループ
- コンテンツ
- レポート
- 分類
- Relay
- Shield
- ガバナンス
- Platform
- アプリ
- アカウントと請求
- Enterprise設定

ダッシュボード　検出ルール　アクセスポリシー　リスト

Shieldダッシュボード

優先度別アラート

2	重要
0	高
0	中
21	低
0	参考情報

ルール別アラート

2	異常なダウンロード
21	不審な場所
0	不審なセッション
0	悪意のあるコンテンツ

ユーザー別上位アラート

7	Satoshi U...
5	admin ad...
3	Akane Ya...
2	HiroyukiS...
2	Seiichi W...

- コンテンツ
- レポート
- 分類
- Relay
- Shield
- ガバナンス

＋ ポリシーの作成

アップロード

クレジットカード アップロード

クレジットカード アップロード

ポリシーの種類	アップロード
条件	文書にクレジットカード番号が含まれています 広い
処理	shinji@cloudnative.co.jp に通知
開始	2017/12/24 15:07

コンテンツマネジメント

分散しがちな保存先

- Slack→Boxへ（Lambda）
- Zoom→チャットOFF
- SNS→CASBで制御
- 課題管理ツール→直接アップロード禁止

コンテンツマネジメント

コンテンツ保護の完成形はまだない
多くが運用設計でカバーBut超重要

利便性を追求しつつ
会社としての説明責任を果たせるか

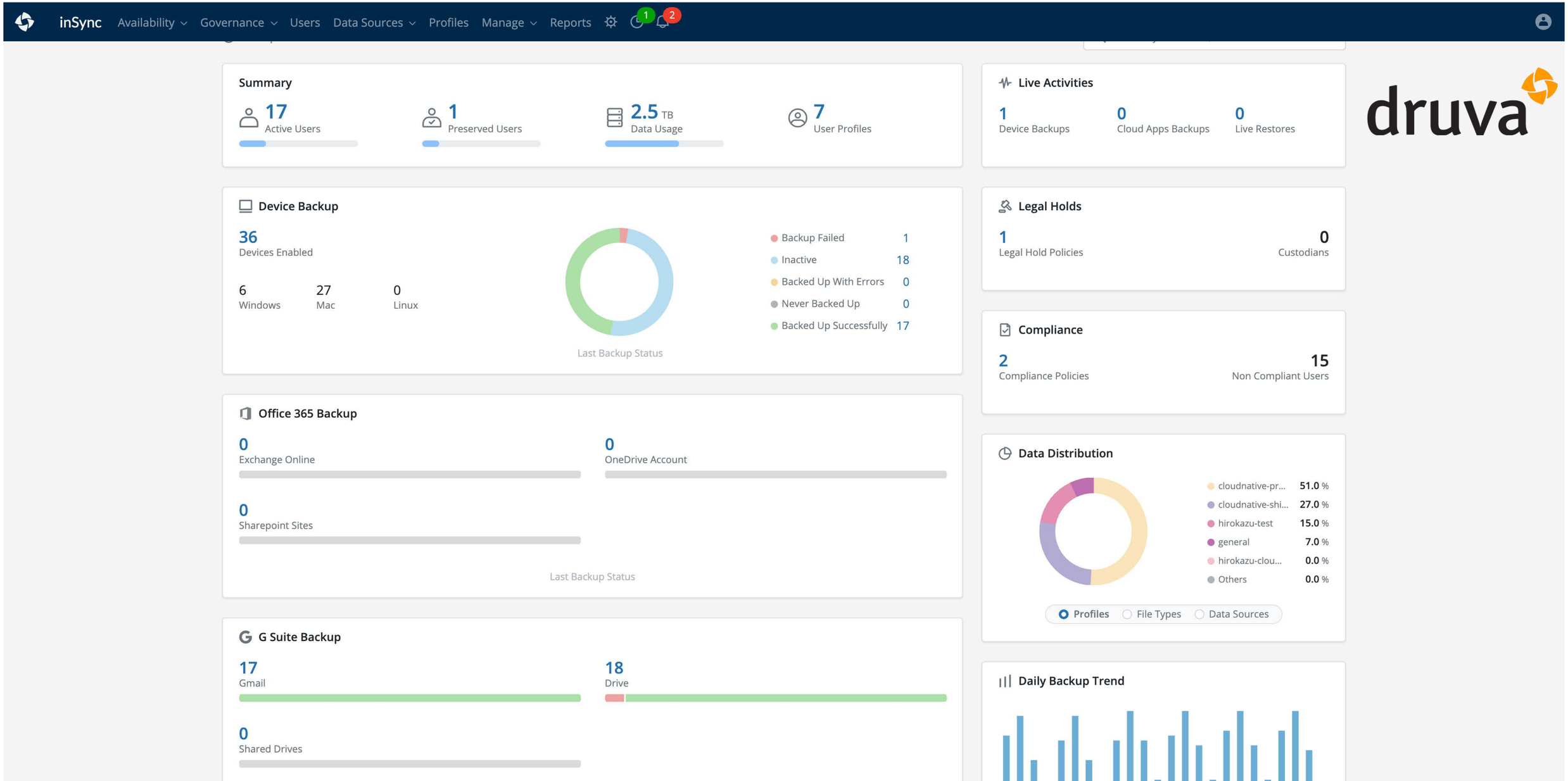
コンテンツマネジメント

最上位構成は、クラウド、サーバ、端末

全てのデータを常にバックアップ

集めたデータを解析、制御する

コンテンツマネジメント



コンテンツマネジメント

情報が集まるところに
人が集まるの法則

メインの保存先はこれです！
会社が守ってるのはここだよ！

暗号化鍵の取り扱い

鍵管理

暗号化鍵の取り扱い

鍵管理

クラウドに上げたデータは
自社のものであるか？

暗号化鍵の取り扱い

某クラウドサービス

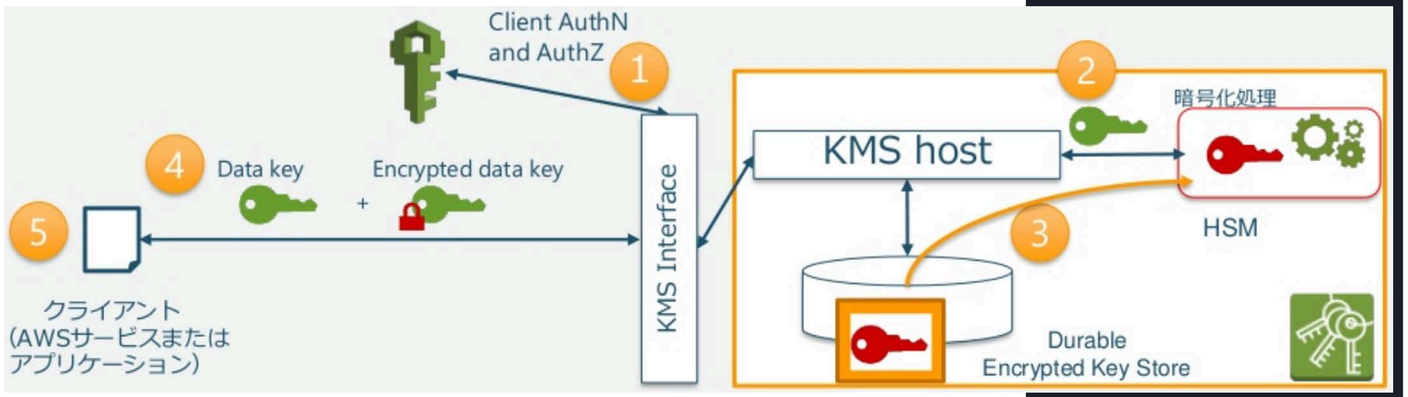
全てのデータは暗号化されているので安全です

（復号化できるのはわたしたちだけです）

（見ようと思えば見られます管理者ですもの）

暗号化鍵の取り扱い

クラウドサービスの鍵管理は限定的
Box, Slackなど



セキュリティ

Enterprise Key Management

Enterprise Key Management (EKM) は、AWS Key Management Service 経由で管理されるキーを用いてオーガナイゼーション内のすべてのメッセージとファイルを暗号化します。これらのキーが Slack に公開されることは決してありません。

Encryption status

最終更新日 : 今日の14:38 (数秒前)

メッセージ	**暗号化** 現在および今後のメッセージ
ファイル	**暗号化** 現在および今後のファイル
検索履歴	**暗号化** 現在および今後の検索履歴

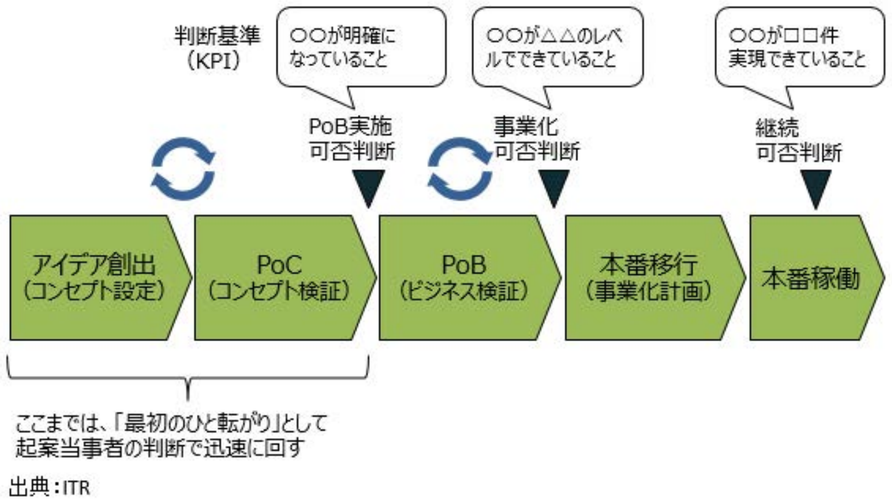
現場面

・業務量削減を体感する

小規模なPoCを行う

・デバイス買い替え(ユーザー視点)
・デバイス追加とデプロイメント(管理者視点)
・統合管理(統制、セキュリティ視点)

【図5】チェックポイントを設定した可否判断



出典:ITR

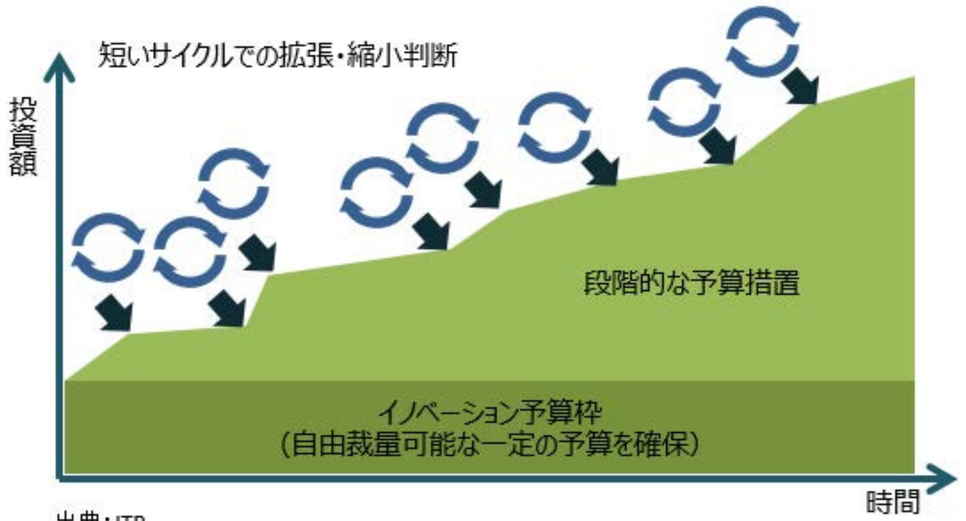
マネジメント面

・投資先の全体像を把握する

網羅されているソリューションを選択する

・推進から具体的な方法、数字で明確に
・業務と担当者の明確化
・説明責任の達成

【図4】投資管理のオンデマンド化



出典:ITR

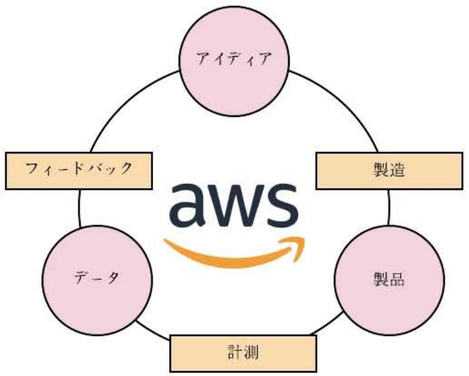
なぜクラウドなのか

- 不確実性への挑戦をするための手段を情報システム部門が提供する
- 無駄をなくす文化と仕組みを作るための手段

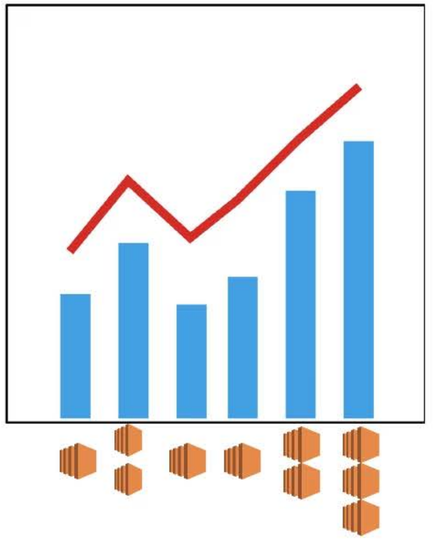
不確実性への挑戦

- 課題が曖昧
- マーケットの未来がわからない
- アイディアを即座に製品化する
- 効果を計測する
- 学習のサイクルを早く回す

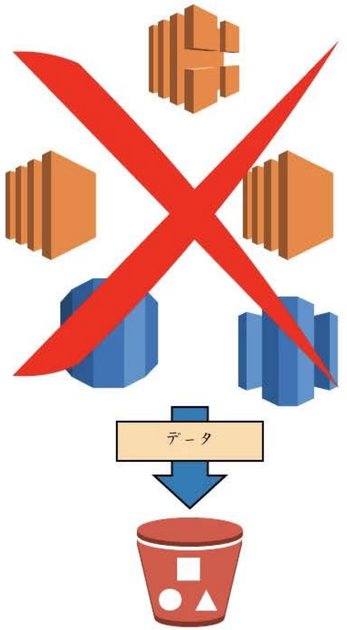
不確実性への挑戦をすばやく
実現するためのクラウド



ITサービスの需要状況にあわせて
適切なキャパシティで継続運用を実現する



データの退避と環境の迅速な破棄(クロージング)

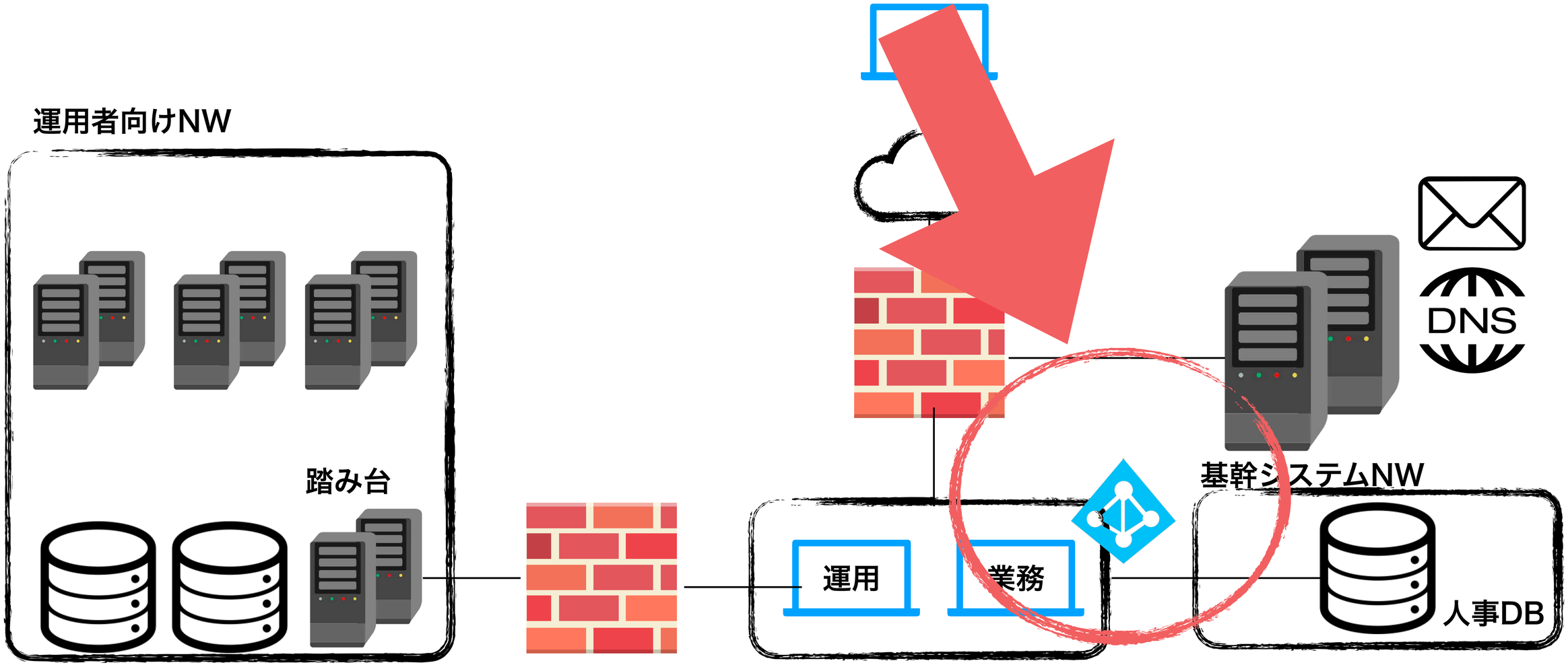


継続的な開発・テスト・リリースの実現が必要であり、これら実現するためのインフラストラクチャがクラウドであり、
様々なサービスを組み合わせて無駄を削り、運用コストを最適化し、利益を出すことを目標とする。

SP800-171:　民間企業が講じるべきセキュリティ対策の要件

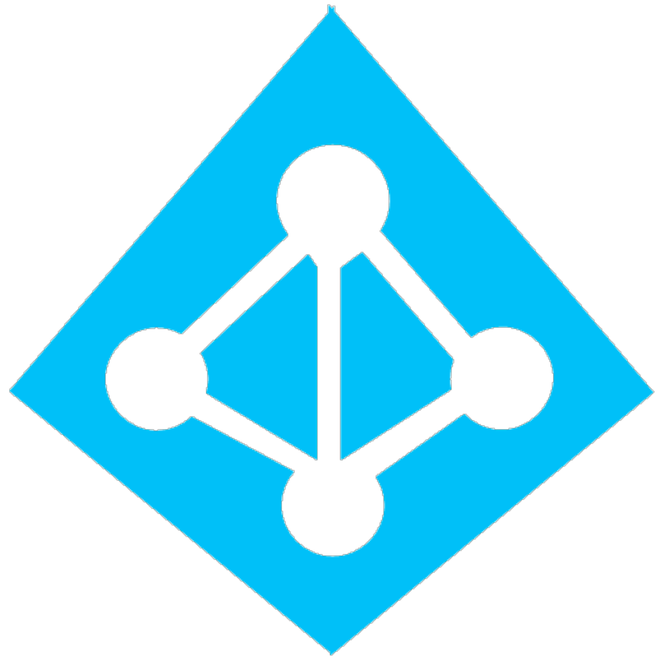
1. アクセス制御
2. 意識向上と訓練
3. 監査と責任追認性
4. 構成管理
5. 識別と認証
6. インシデント対応
7. メンテナンス
8. メディア保護
9. 人的セキュリティ
10. 物理的保護
11. リスクアセスメント
12. セキュリティアセスメント
13. システムと通信の保護
14. システムと情報の完全性

社内リソースで業務が（ほぼ）完結する時代は、MicrosoftのActive Directory（LDAP）が担ってた



実はすごいActive Directory since 2000

- ✔ユーザーオブジェクトDB
- ✔PCオブジェクトDB
- ✔構成情報取得
- ✔リモート構成
- ✔アクセス制御
- ✔他組織連携
- ✔証明書管理（CA）

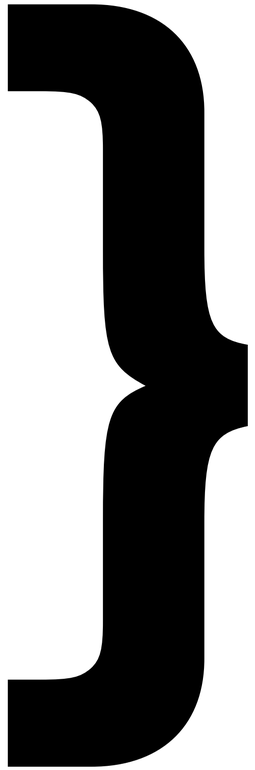


他にも色々

- PC
- サーバー
- 基幹ツール
  - メール、ファイル共有など
- モバイル
  - こけたけど…

SP800-171という要求事項を満たしたまま、デジタル化と新しいビジネス形態（サブスクビジネス）に転換

- クラウドソリューション
  - Windows10エンタープライズ
  - Office365スイート
  - Azure AD（Id管理）
  - Intune（デバイス管理)
  - Microsoft Defender(EDR)
  - Application Proxy(プロキシ)



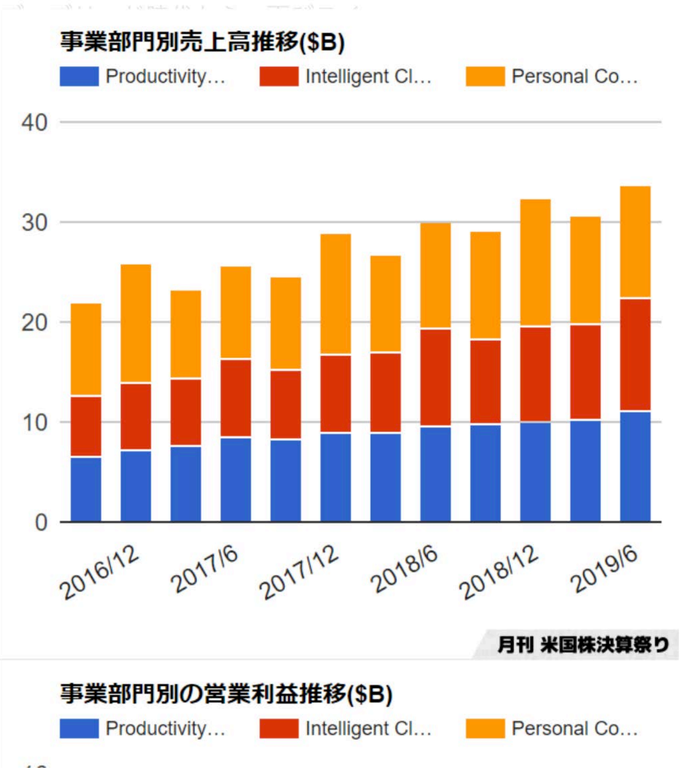
Microsoft 365

SP800-171という要求事項を満たしたまま、デジタル化と新しいビジネス形態（サブスクビジネス）に転換

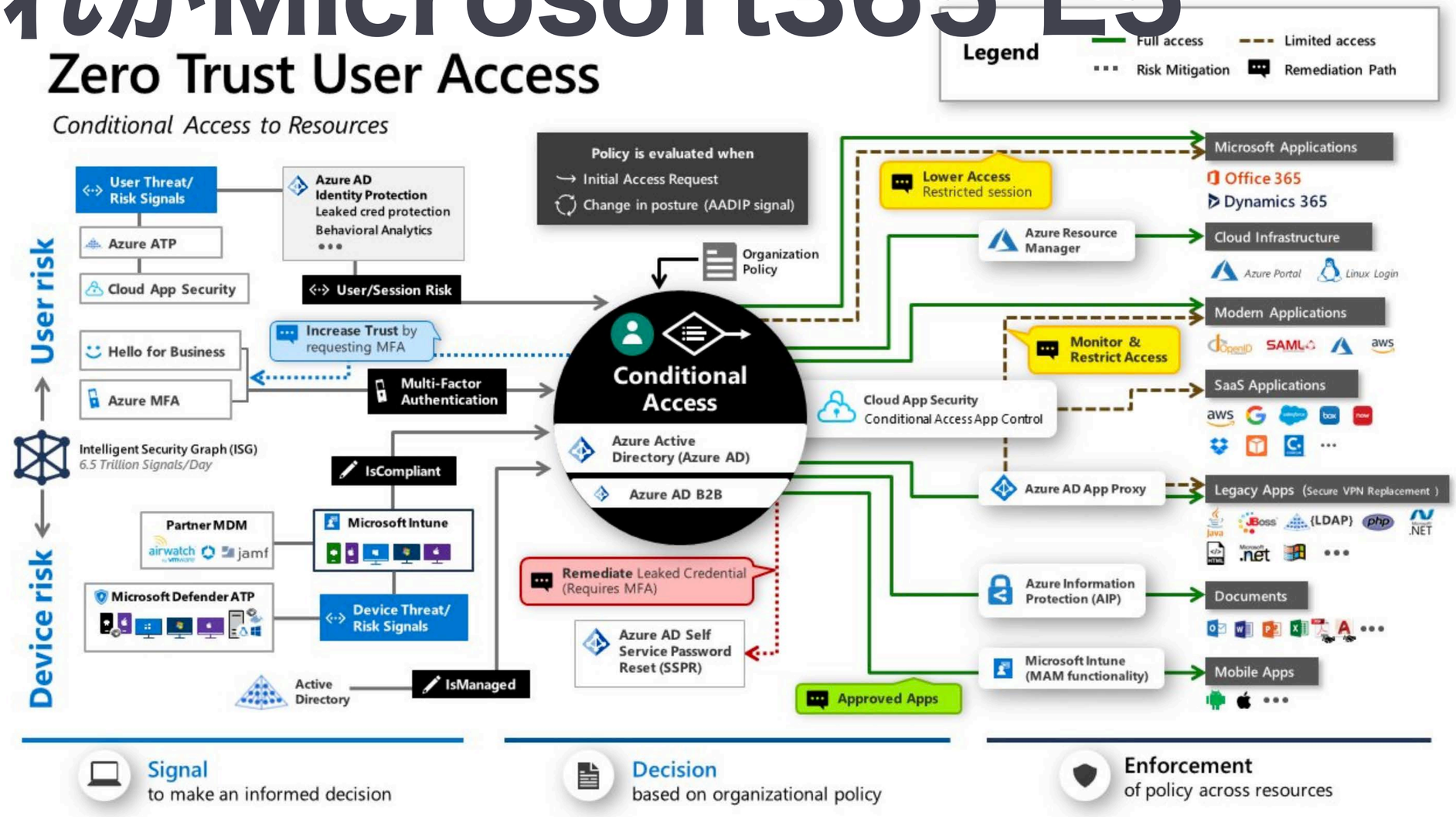
- クラウドソリューション
  - Windows10エンタープライズ
  - Office365スイート
  - Azure AD（Id管理）
  - Intune（デバイス管理)
  - Microsoft Defender(EDR)
  - Application Proxy(プロキシ)

}

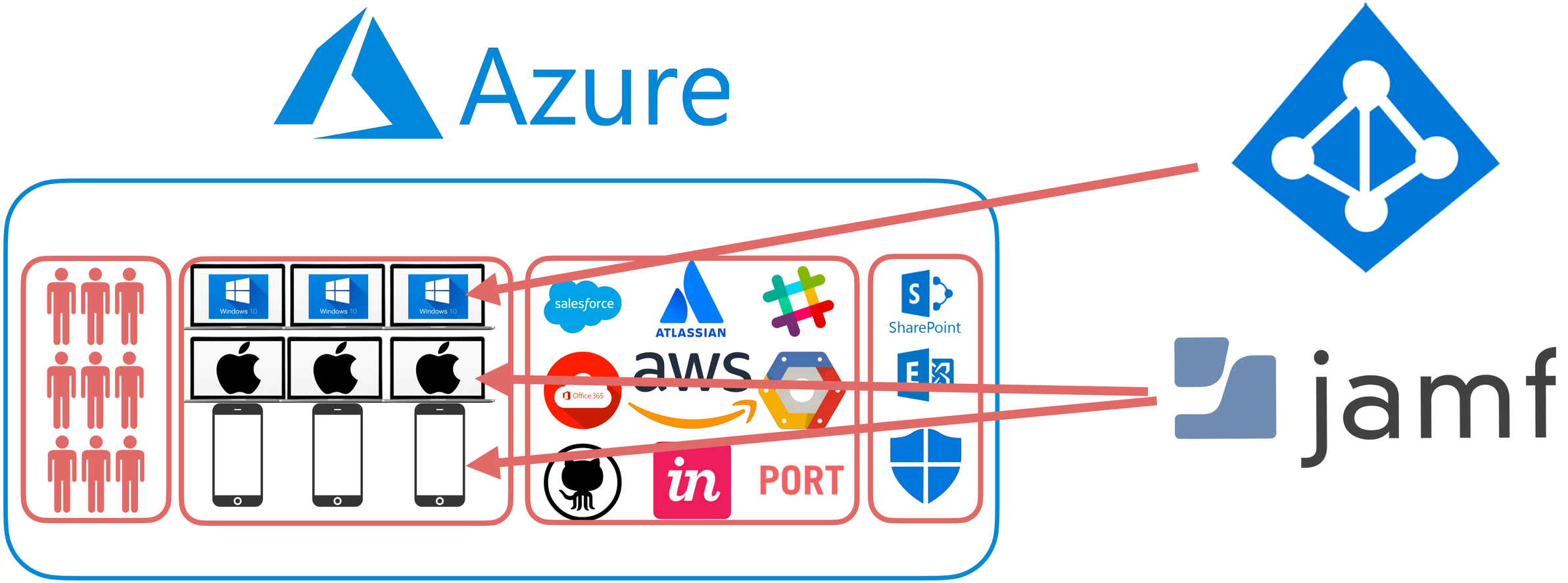
Microsoft 365



それがMicrosoft365 E5



足りない部分を連携可能とするインターフェースも揃っている



Azure Active Directory B2C GA

顧客向けアプリの ID およびアクセス管理

無料で始

Azure AD B2C

概要　機能　セキュリティ　料金設定　使用を開始するには　ドキュメント　お客様事例　パートナー

顧客体験のあらゆる要素をカスタマイズ可能

お客様の企業-消費者間 (B2C) アプリケーションに対する顧客、消費者、市民のアクセスを管理します。必要なスケーラビリティと可用性を備えているため、何百万ものユーザーとつながることができます。

数百万人の顧客にスケーリングできる高可用性

登録とサインイン エクスペリエンスのすべてのピクセルのカスタマイズ

顧客の好みの ID プロバイダーを使った強力な認証

アプリやデータベースとの統合による、サインインやコンバージョンのデータのキャプチャ

コンプライアンス マネージャー

評価　処置項目

アーカイブを含む　＋ 評価の追加　フィルター

Microsoftコンプライアンスマネージャー

Default Group
Office 365 - GDPR
処置
作成済み 7/1/2020
更新済み 7/1/2020
コンプライアンス スコア
264 / 626
顧客管理処置 0 of 65
Microsoft 管理処置 49 of 49

Default Group
Office 365 - NIST 800-53
処置
作成済み 7/1/2020
更新済み 7/1/2020
コンプライアンス スコア
1868 / 2832
顧客管理処置 0 of 215
Microsoft 管理処置 853 of 853

Default Group
Office 365 - ISO 27001:2013
処置
作成済み 7/1/2020
更新済み 7/1/2020
コンプライアンス スコア
794 / 1078
顧客管理処置 0 of 60
Microsoft 管理処置 232 of 232

Default Group
Azure - GDPR
処置
作成済み 7/1/2020
更新済み 7/1/2020
評価の状態
進行中
顧客管理処置 0 of 82
Microsoft 管理処置 45 of 48

Default Group
Azure - ISO 27018:2014
処置
作成済み 7/1/2020
更新済み 7/1/2020
評価の状態
進行中
顧客管理処置 0 of 0
Microsoft 管理処置 74 of 74

Default Group
Azure - ISO 27001:2013
処置
作成済み 7/1/2020
更新済み 7/1/2020
評価の状態
進行中
顧客管理処置 0 of 0
Microsoft 管理処置 231 of 231

Microsoftコンプライアンスセンター

Microsoft 365 コンプライアンス

データの分類
データ コネクタ
アラート
レポート
ポリシー
アクセス許可

ソリューション

カタログ

その他のリソース

ナビゲーションのカスタマイズ
すべてを表示

ンス センターへようこそ

はじめに　次のステップ　フィードバックの送信

Microsoft 365 コンプライアンス センターへようこそ。この新しいポータルでは、情報保護、情報ガバナンス、インサイダー リスク管理、検出などの統合ソリューションを使用して、コンプライアンスに関するニーズを管理できます。 Microsoft 365 コンプライアンス センターに関する詳細情報

次へ　閉じる

Office 365 セキュリティ/コンプライアンス センター　最新情報　カードを追加

Microsoft コンプライアンス スコア

コンプライアンス スコア: 76%

コンプライアンス スコアは、データ保護と規制基準に関連するリスクの削減に役立つ推奨処置の完了に向けた進展を測定します。

コンプライアンス スコアに関する詳細情報

情報の保護　0 / 427

情報の管理　0 / 119

ソリューション カタログ

コンプライアンスのニーズに対応するソリューションを見つける

組織で利用できる新規および改善されたコンプライアンスおよびリスク管理ソリューションを見つけることができます

カタログを参照して、各ソリューションのメリットと、コンプライアンスのニーズを満たすために各ソリューションがどのようにインテリジェントに連携するかについて確認できます。

クラウド アプリのコンプライアンス

クラウド アプリのコン...

一部のクラウド アプリは、これらの規制に関するコンプライアンスの要件を満たしていない可能性があります

GDPR

HIPAA

ISO-27001

SOC1

Microsoftインサイダーリスクマネジメント

アラート
レポート
ポリシー
アクセス許可

ソリューション

カタログ
監査
コンテンツの検索
コミュニケーション コンプライアンス
データ損失防止
データ主体の要求
電子情報開示
情報ガバナンス
情報の保護
内部リスクの管理
レコード管理

概要　アラート　ケース　ポリシー　ユーザー　通知テンプレート

内部関係者によるリスクや脅威をすばやく特定および調査して対処できるように、組織全体で危険性のあるアクティビティを検出します。詳細情報

Insider のリスク管理ポリシーに含まれるユーザーには、Microsoft 365 E5 Compliance ライセンスが必要です。または、Microsoft 365 E5 サブスクリプションに含まれている必要があります。この機能は、オンライン サービス条件 の対象です。

確認対象のアラート

ポリシーの一致	アラートの重要度	ユーザー	検出された時間

すべてのアラートを管理

アクティブなケース

アクティブ
0

ケース名	状態	ユーザー	最終更新日時

ここまでのまとめ

2000年からゼロトラスト（っぽい）社内基盤を提供していた
自らデジタル時代にあわせてきたのが、Microsoft365 E5
ゼロトラストを組む上でMicrosoftの存在は大きい

Next (Post2020)
Zero Trust

デジタル化・イノベーションの流れ

静岡銀行 × Money Forward

「マネーフォワード for 静岡銀行」をリリース

AnserParaSol

NTTデータの
インターネット
バンキングAPIを
国内初導入

MITSUI&CO.

LayerX

SMBC日興証券

三井住友信託銀行
SUMITOMO MITSUI TRUST BANK

自動家計簿機能を静岡銀行向けにカスタマイズ

第一波

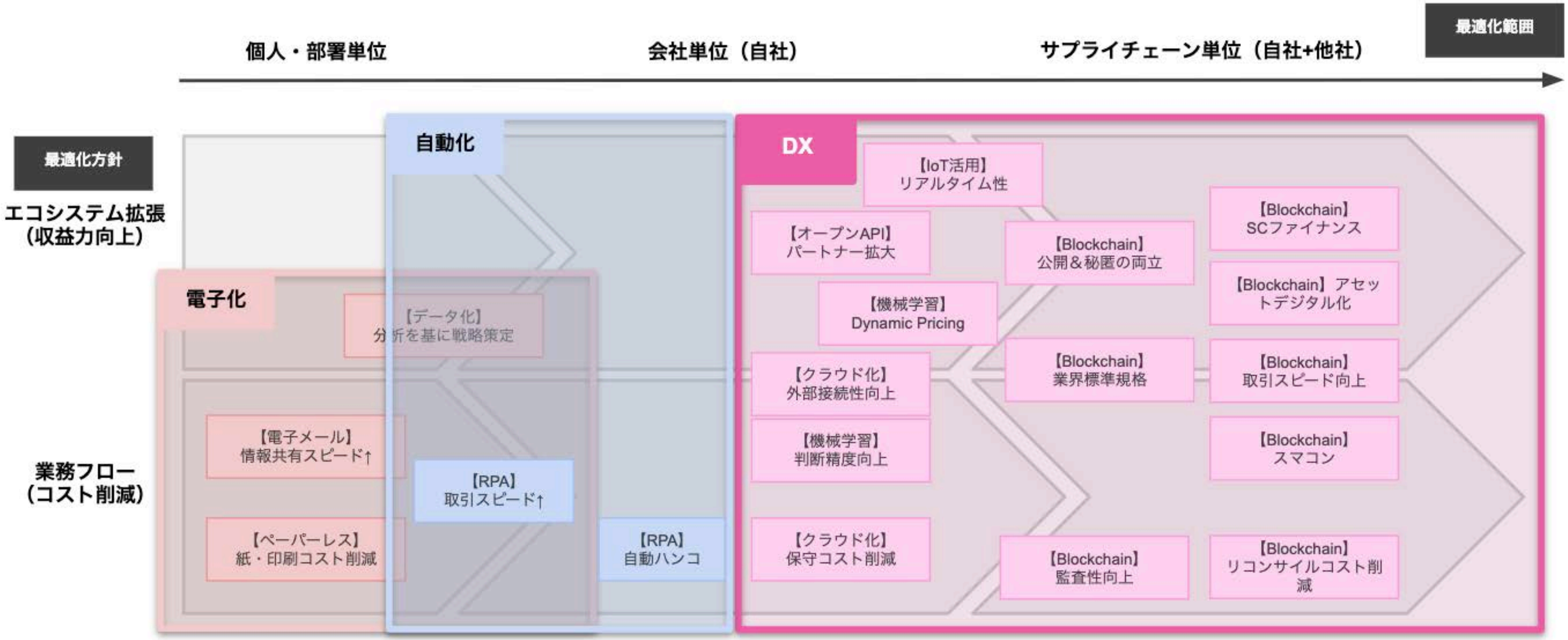
製品やサービスがデジタル化

- 通信
- メディア
- エンターテイメント

第二波

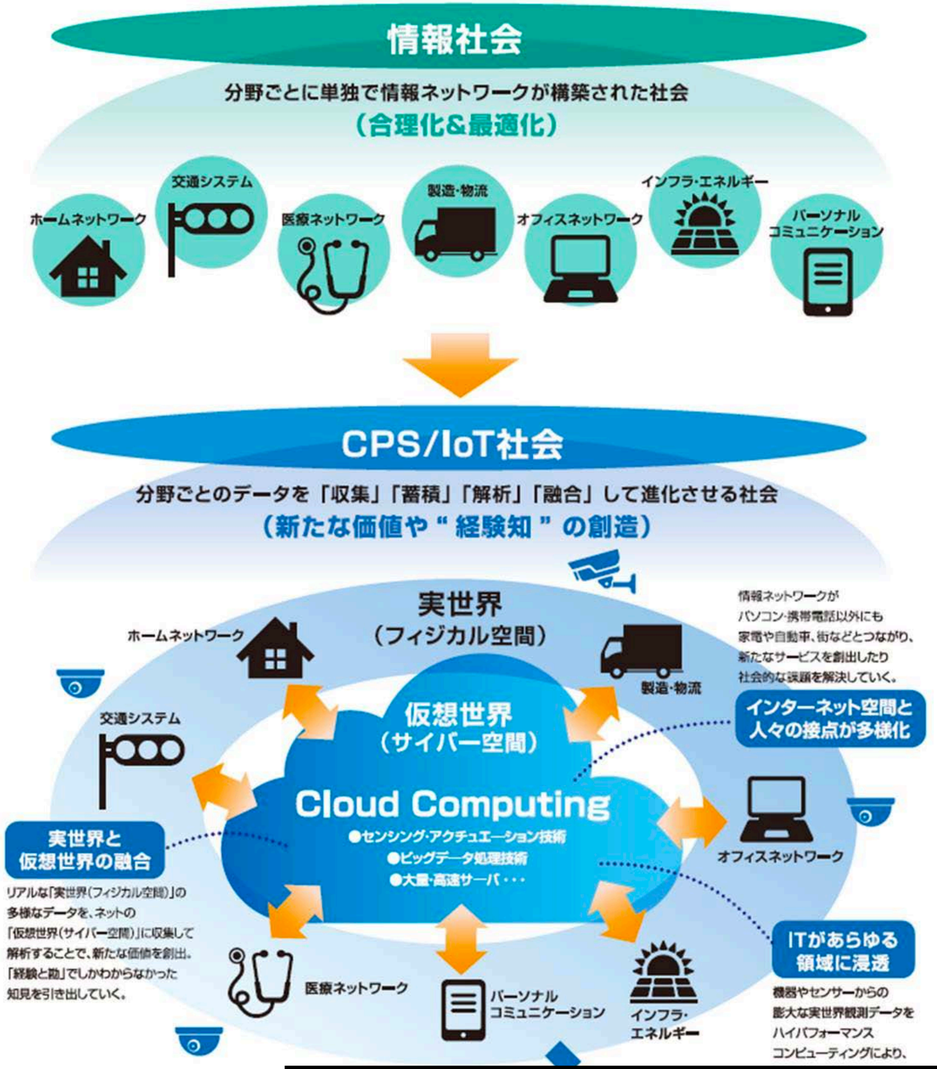
ビジネスモデル、業務フロー、バリューチェーンがデジタル化

- 金融
- 自動車
- 物流
- BtoB取引


最適化範囲
個人・部署単位
会社単位（自社）
サプライチェーン単位（自社+他社）
最適化方針
エコシステム拡張
（収益力向上）
業務フロー
（コスト削減）
電子化
自動化
DX
【データ化】
分析を基に戦略策定
【電子メール】
情報共有スピード↑
【ペーパーレス】
紙・印刷コスト削減
【RPA】
取引スピード↑
【RPA】
自動ハンコ
【IoT活用】
リアルタイム性
【オープンAPI】
パートナー拡大
【機械学習】
Dynamic Pricing
【クラウド化】
外部接続性向上
【機械学習】
判断精度向上
【クラウド化】
保守コスト削減
【Blockchain】
公開＆秘匿の両立
【Blockchain】
業界標準規格
【Blockchain】
監査性向上
【Blockchain】
SCファイナンス
【Blockchain】アセット
トデジタル化
【Blockchain】
取引スピード向上
【Blockchain】
スマコン
【Blockchain】
リコンサイルコスト削減

Cyber Physical Society / Connected Industry

- 実世界（フィジカル空間）にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析／知識化を行い、そこで**創出した情報／価値**
- 製造業を超えて、モノとモ ノ、人と機械・システム、人と技術、異なる産業に属する企業と企業、世代を超 えた人と人、製造者と消費者など、様々なものをつなげる”産業社会



https://www.jeita.or.jp/cps/about/

エコシステム全体の中でのTrust

エンドユーザー

組織を超えたトラストチェーン