攻撃に強いIT環境づくりのためのエッセンス

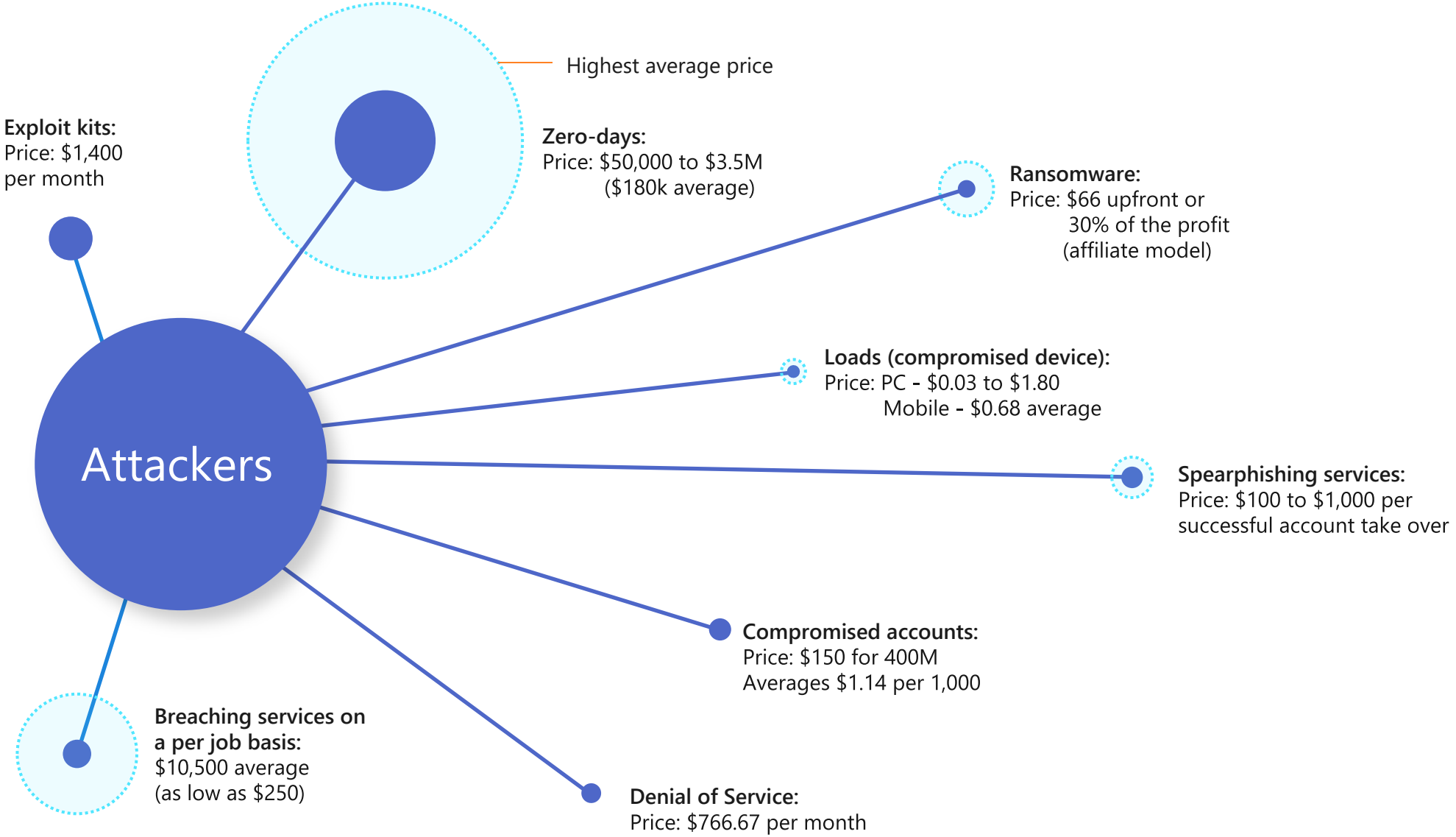
日本マイクロソフト株式会社
Chief Security Officer
河野省二, CISSP

Microsoft

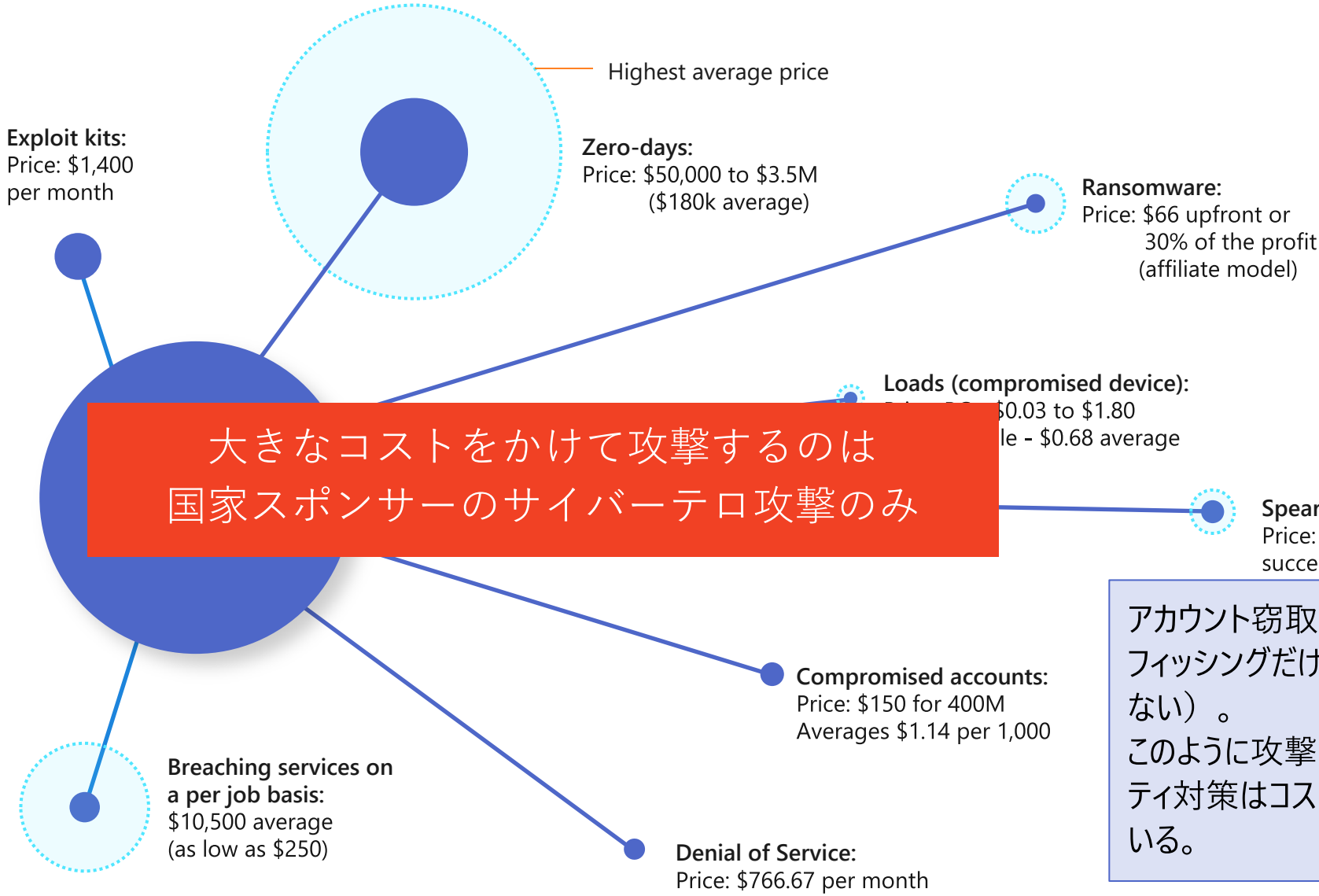
セキュリティのトレンド

最近のセキュリティの話題を理解するために

攻撃のトレンドと対応の限界 - サイバー攻撃ビジネス



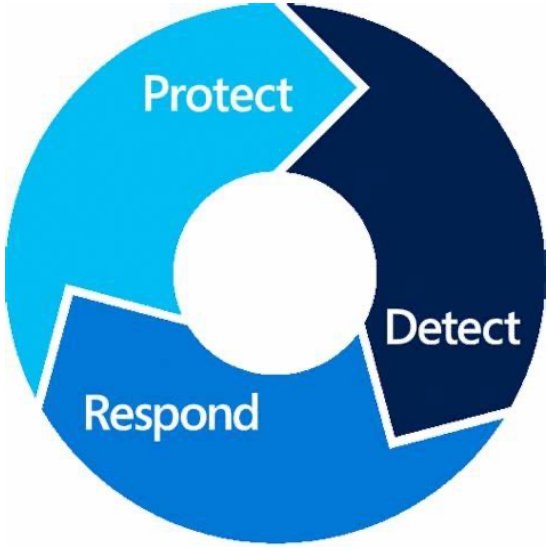
攻撃のトレンドと対応の限界 - サイバー攻撃ビジネス



アカウント窃取は、もはやウイルスをばらまくことなく、フィッシングだけで事足りている（技術もコストもかからない）。
このように攻撃が安価に提供されることから、セキュリティ対策はコスト面でも攻撃者に優位な状況となっている。

対症療法では問題は解決しない

Cyber Security Frameworkによるセキュリティフェーズの追加とビジネスモデルの変化



「攻撃への迅速な対応」ではなく、
どんな攻撃にも耐えながら、ビジネスを継続していくための
基盤づくりとして、IDENTIFYとRECOVERが含まれた。
個別のベンダーでは対応できないために、大手による買収が進んでいる。→ **予防とサイバーレジリエンスへのシフト**

対症療法では問題は解決しない

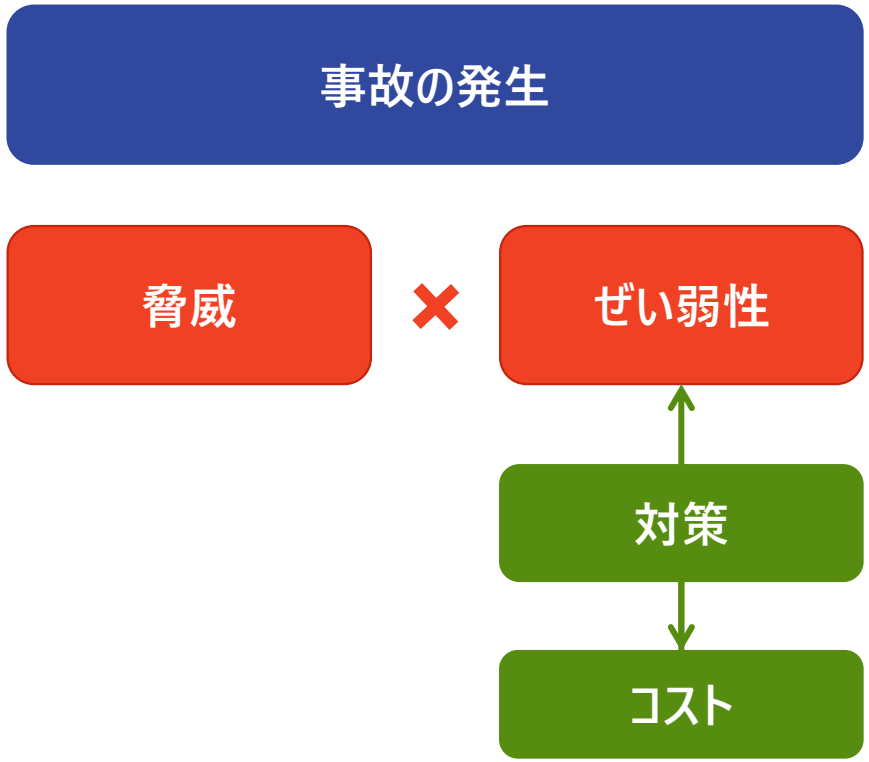
Cyber Security Frameworkによるセキュリティフェーズの追加とビジネスモデルの変化

「すばやい検知、すばやい対応」では不十分

サプライチェーンを含む全ての環境を
把握して、事故に強い環境を作る

「攻撃への迅速な対応」ではなく、
どんな攻撃にも耐えながら、ビジネスを継続していくための
基盤づくりとして、IDENTIFYとRECOVERが含まれた。
個別のベンダーでは対応できないために、大手による買収が進んでいる。→ **予防とサイバーレジリエンスへのシフト**

リスクマネジメントフレームワーク：事故の発生



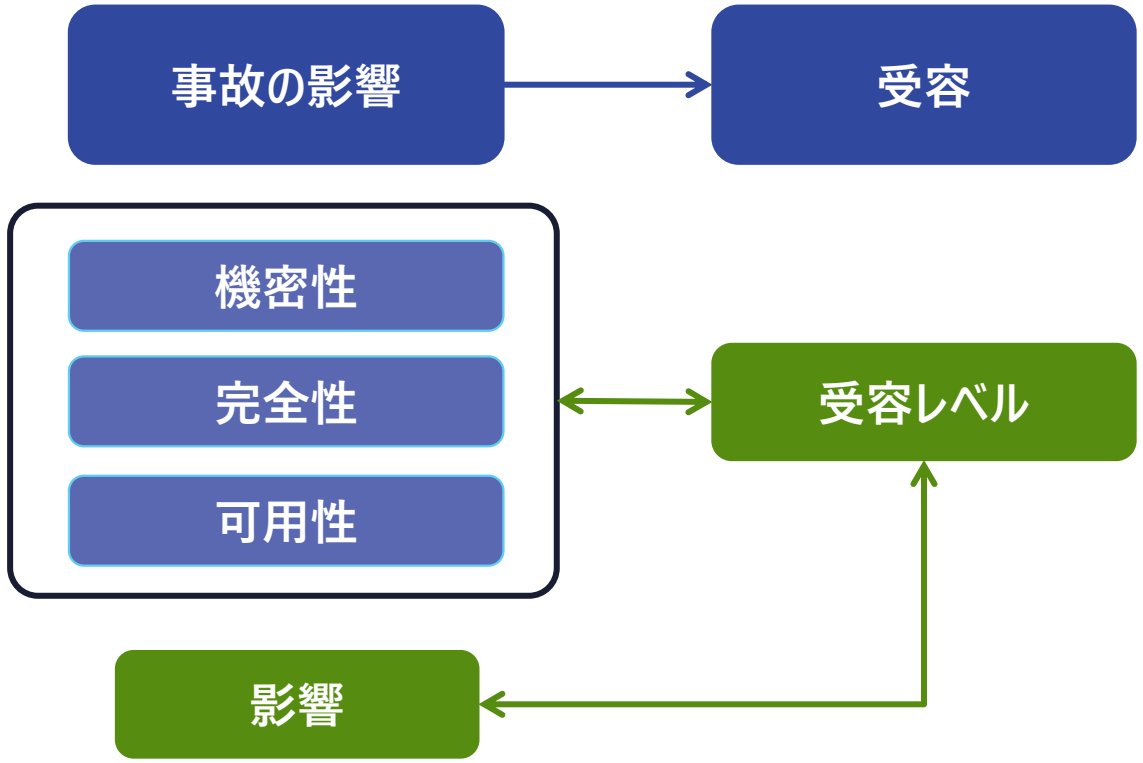
事故が発生するのは脅威と脆弱性が合致するから

- 脅威は外部にあるためにコントロールすることが難しい（抑止）
- ぜい弱性は内部にあるためにコントロールが可能。ぜい弱性を低減することをセキュリティ対策という（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

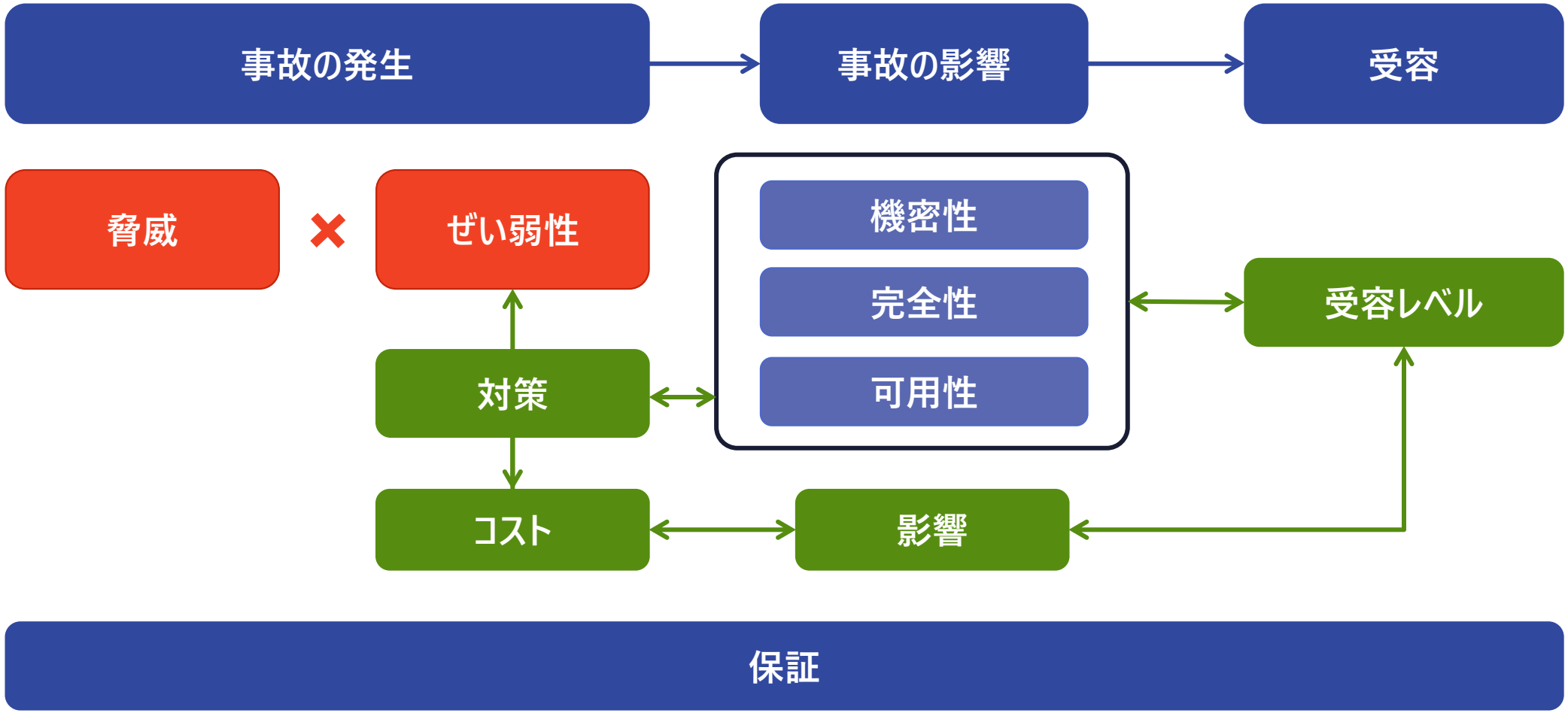
リスクマネジメントフレームワーク：事故の影響

影響を受容できるまで、セキュリティ対策を行う

- 事故の影響は、機密性、完全性、可用性が維持されなくなることによって算出される（損失）
- 影響は3つの視点のそれぞれの合計となるため、情報漏洩だけを考えていると、費用対効果を適切に判断できない



リスクマネジメントフレームワーク

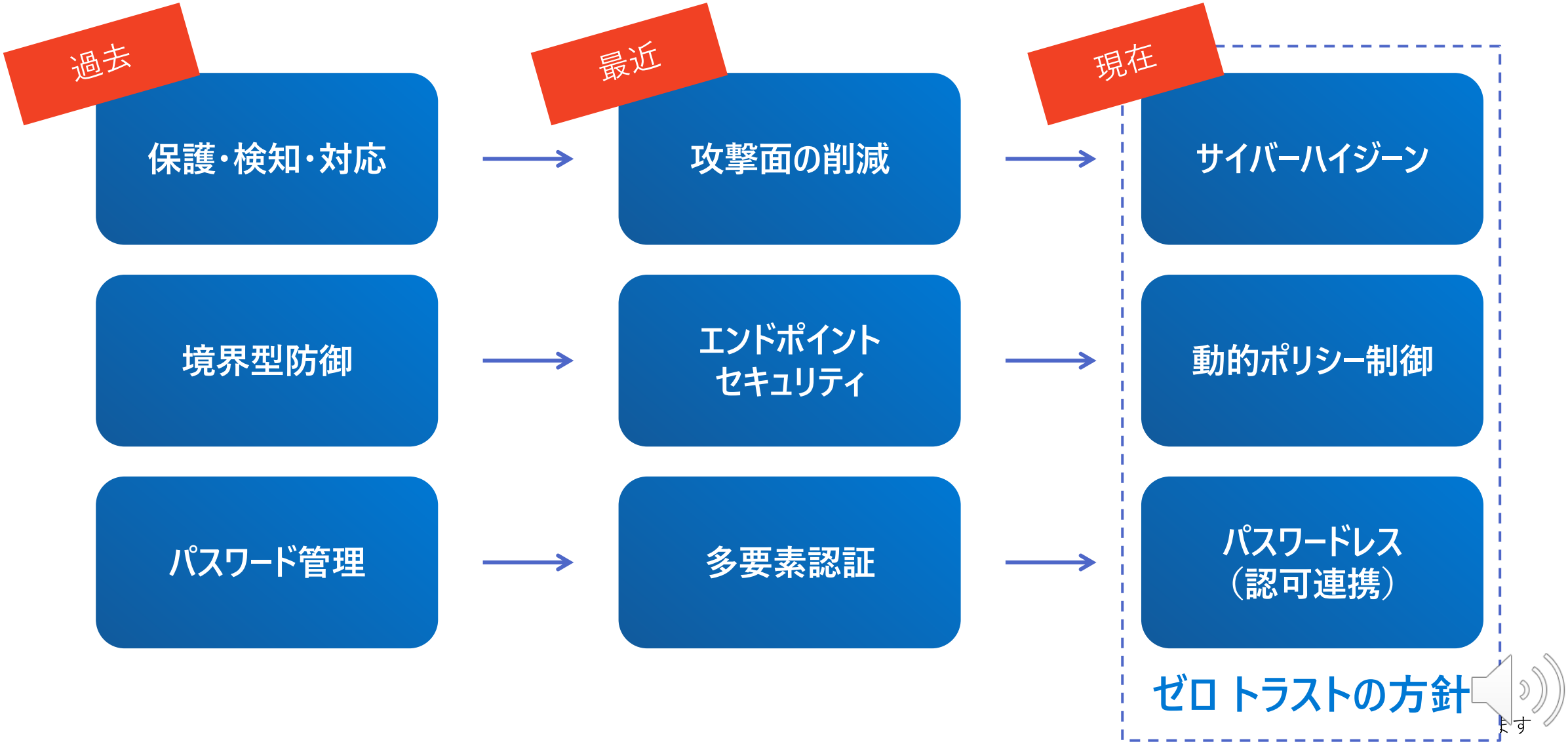


いつでも脆弱性のない状態を作る

サイバーハイジーン

資産を全て管理して
その状態を把握することで
求める状態を維持する

サイバーセキュリティ対策の変化



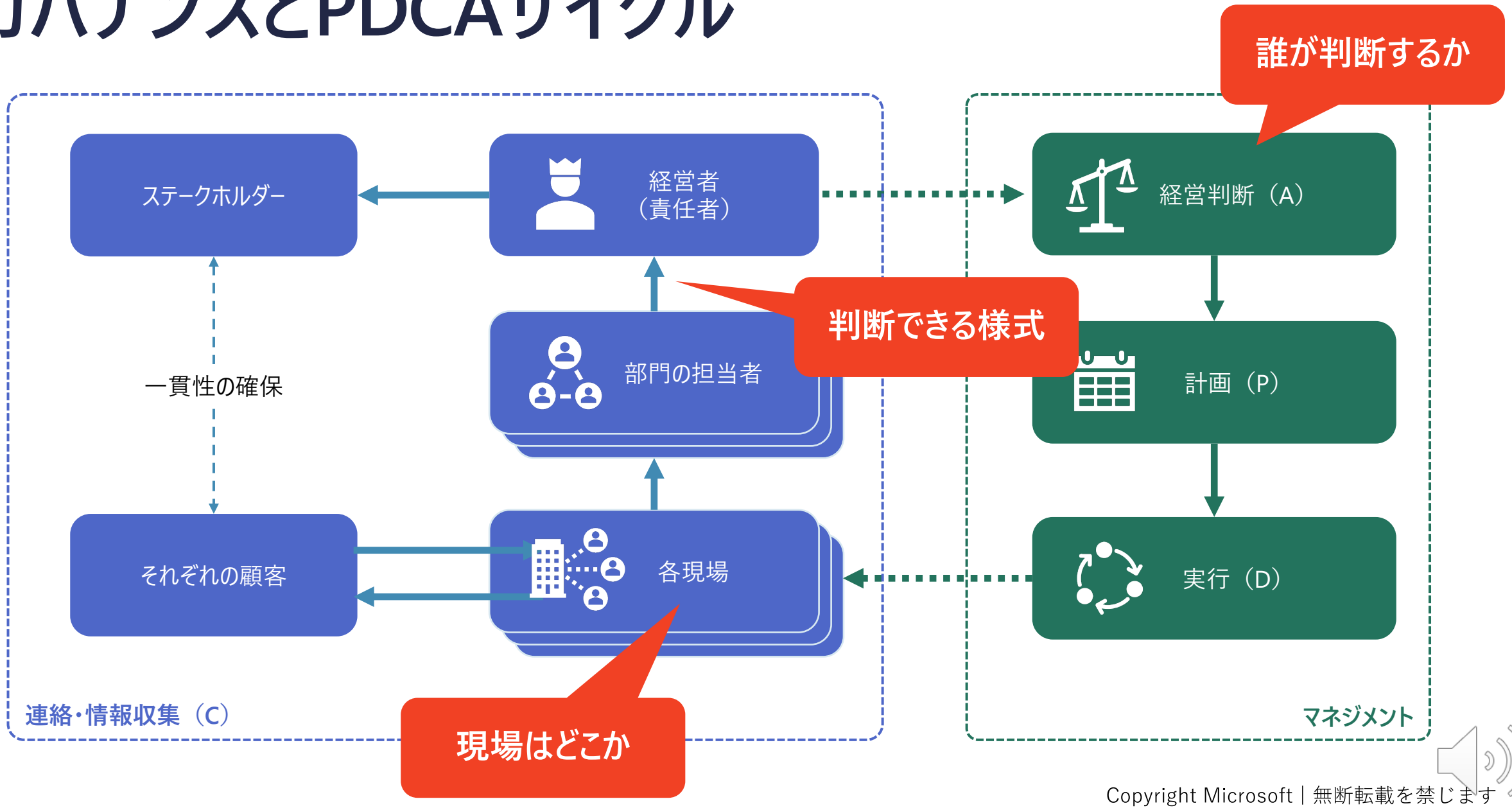
セキュリティに求められるもの

どのような方針を立てて計画をしていくか

個別のセキュリティ対策ではなく、共通項を探る

説明責任を果たすためには全ての把握が必要、そして事業継続を行っていくためには、リアルタイムに適切な判断が必要。そしてガバナンスの意味の理解が必要になる

ガバナンスとPDCAサイクル



現場をすべて把握するための仕組みづくり

全ての資産を把握

インベントリ管理

資産の状態を把握

構成管理

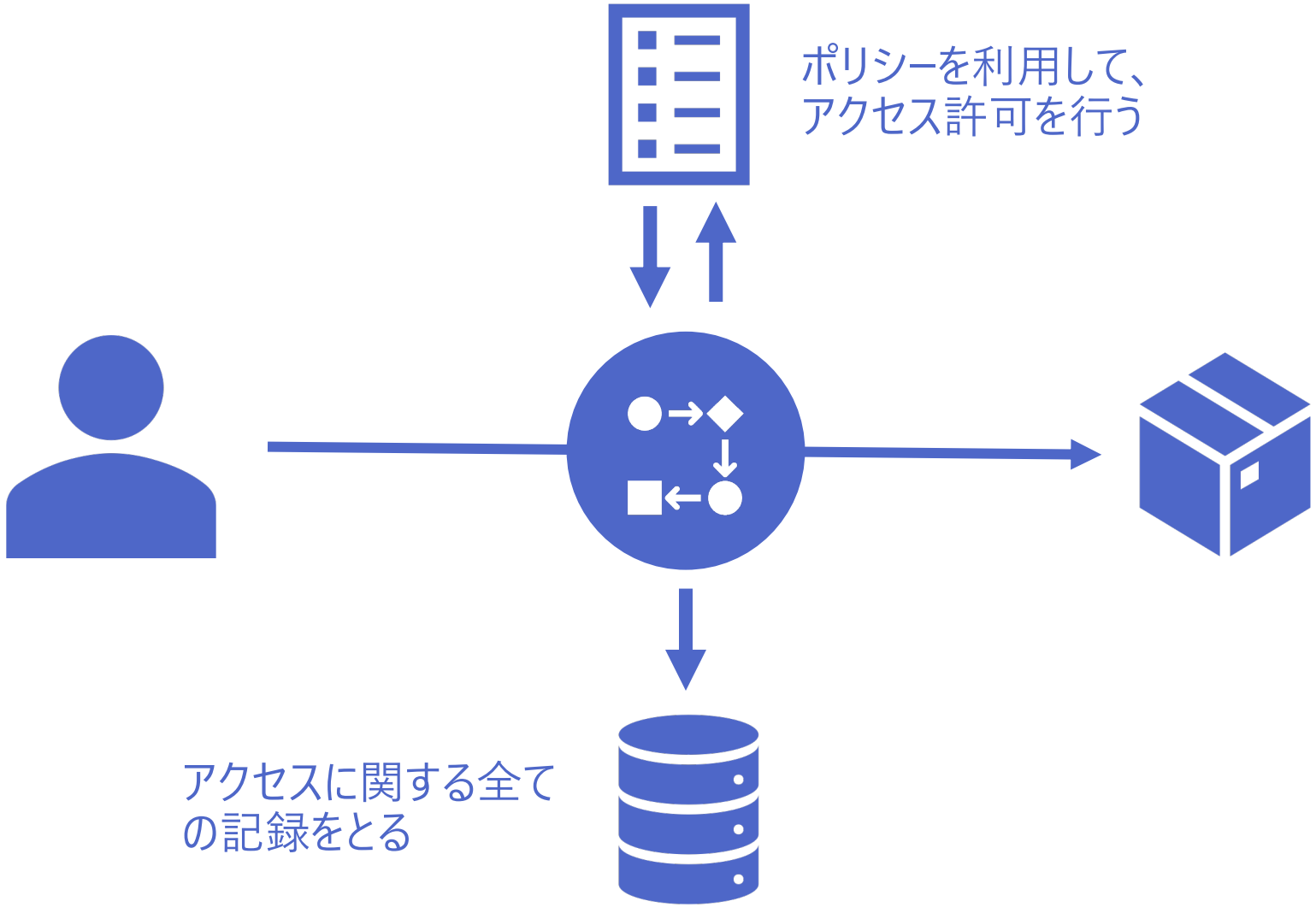
やりとりを把握

管理の連鎖

デジタライゼーションによるリアルタイムでの把握

リアルタイムな判断とカイゼン

全てのやりとりを把握するための仕組み



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
- ネットワーク属性とイベント

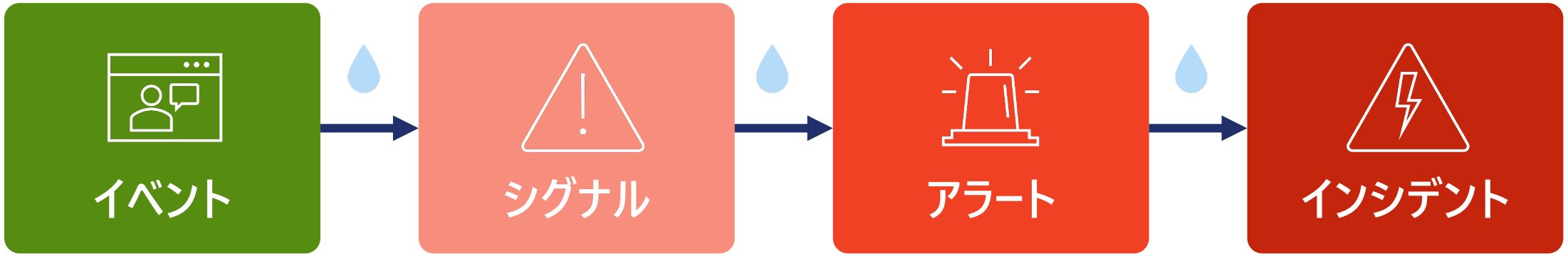
AND / OR

ユーザ・エンティティ

ID管理サービスで、ユーザ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
- ユーザとエンティティの属性とイベント

インシデントをすべて把握するためには



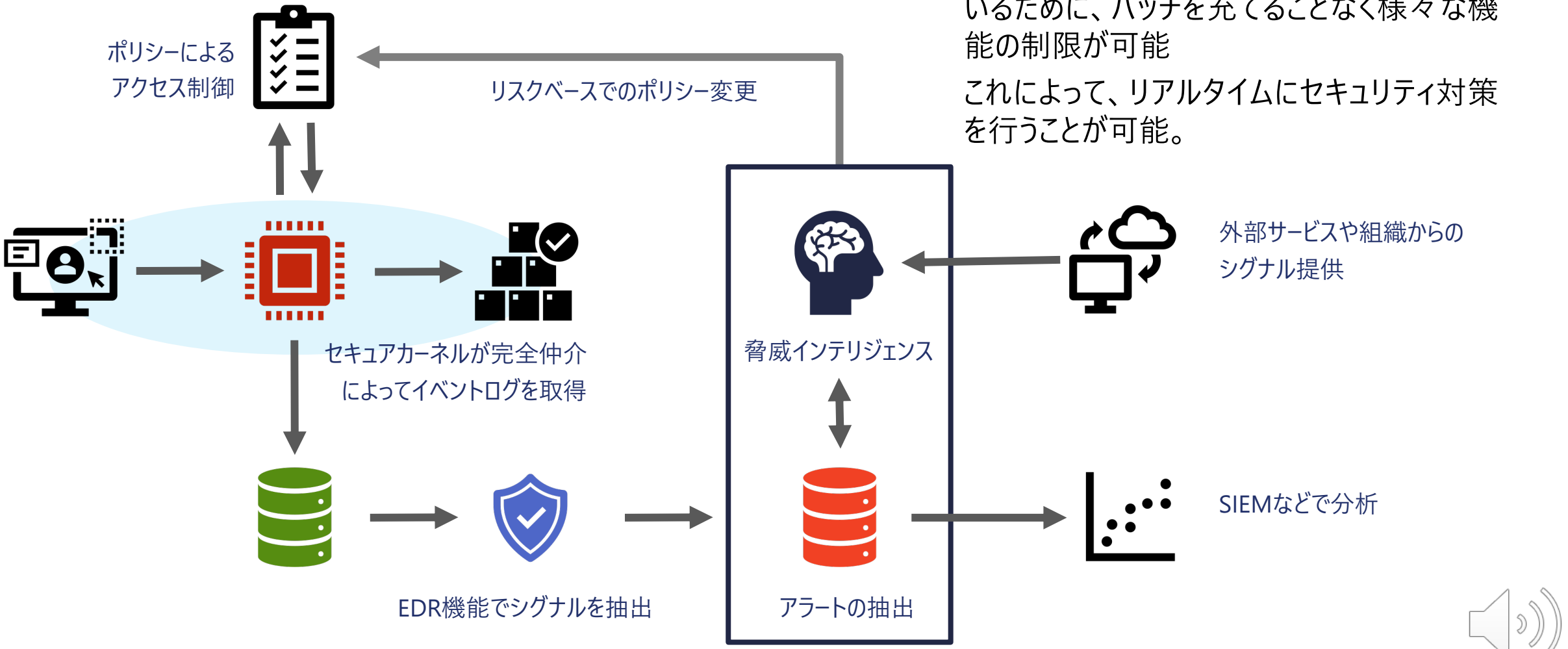
インシデントはイベントログの中の怪しい情報をまとめあげることで、検出される

すべてのインシデントを把握するためには、すべてのイベントを記録しておく必要がある。いわゆるセキュリティログというのは、シグナルやアラートだけをまとめたもので、その有効性を図るためには、イベントログを正確に取得しておく必要がある

Windows 10でのイベントログ取得とシグナル活用

モダンOSやモダンアプリはAPIで構成されているために、パッチを充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可能。



エンドポイントセキュリティとゼロトラスト

ネットワークセキュリティからエンドポイントセキュリティへの変革

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ウォールで行っていた

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

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る

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

ファイアウォールで守られたローカルネットワーク

信頼できなくなりました・・・

理由その1：ファイアウォールはIPアドレスとポート番号でフィルタリングしている
理由その2：攻撃はウェブやメール経由で行われている
理由その3：VPN経由で内部に侵入することが難しくなくなってきた

信頼できないのはネットワークだけではない

ゼロ トラスト ~~ネットワーク~~

匿名でのインターネット利用は信用できない

理由その1： 攻撃のほとんどがなりすまし
（アカウント、メール、ファイル、アプリのなりすましなど）

理由その2： 脅威の変化により、セキュイリティのベストプラクティスが役に立たない

エンティティの動的な検証と、リスクに応じた動的ポリシーの実践

NIST SP800-207におけるゼロ トラストの基本原則

1. 全てのデータソースとコンンピュータサービスはリソースとみなされる
2. 場所に関係なく全ての通信が保護される
3. 個々のリソースへのアクセスはセッションごとに設定される
4. リソースへのアクセスはモニタリング可能な属性を利用した動的ポリシーによって決定される
5. 完全性とセキュリティの状態管理のために、全ての資産をモニタリングする
6. 全てのリソースの認証は事前に厳密に行われ、動的な認可が与えられる
7. ネットワークにおいても同様に多くの情報を収集し、セキュリティの状態を改善する

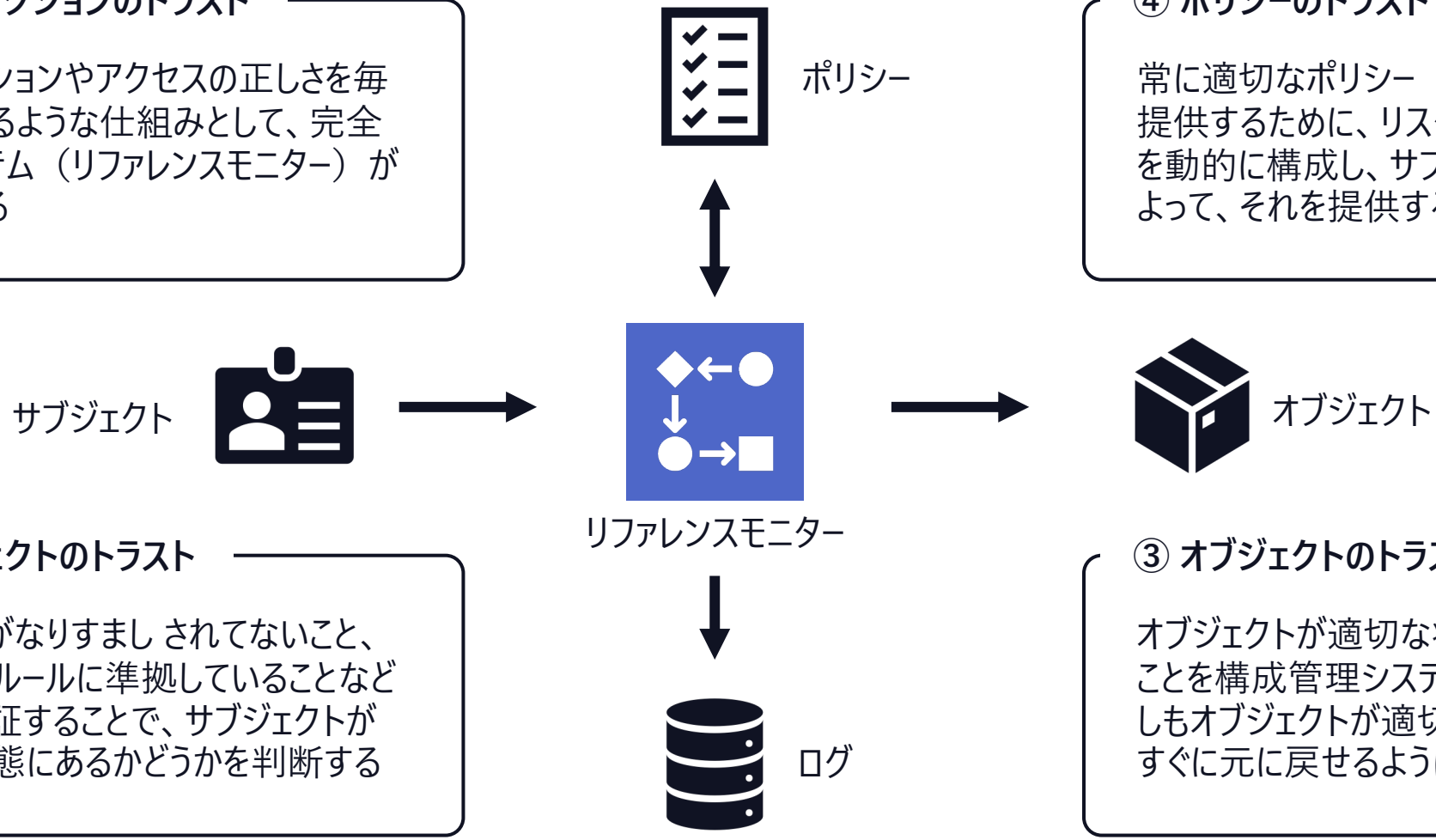
ゼロトラストの実践のために

① 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

② 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



④ ポリシーのトラスト

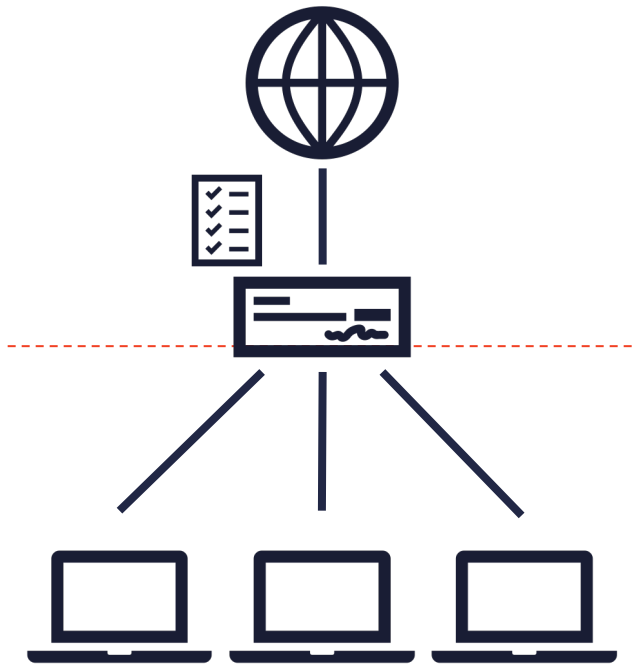
常に適切なポリシー（判断基準）を提供するために、リスクに応じてポリシーを動的に構成し、サブジェクトの属性によって、それを提供する

③ 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でない場合にはすぐに元に戻せるようにしておく

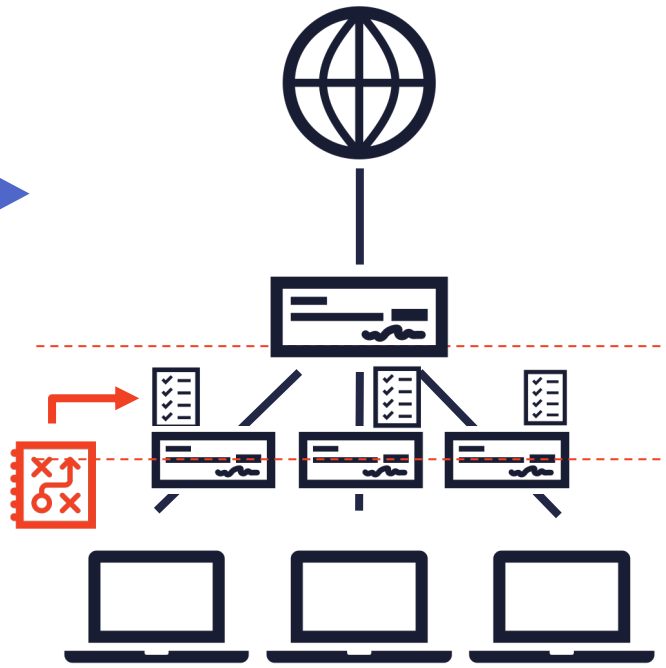
ピュア ゼロ トラスト - マイクロセグメンテーションの先にあるもの

典型的な境界型防御



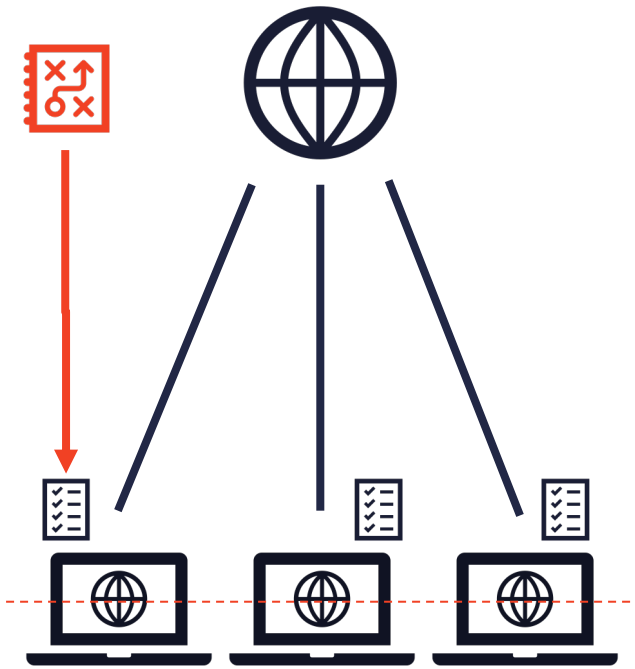
ファイアウォールによって配下のPCやサーバは共通のセキュリティポリシーが適用される。結果として、一番厳しいポリシーが全てに適用されるか、全てが甘くなる。

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。SDNを使ってさらに効率化をした

ピュア ゼロトラスト

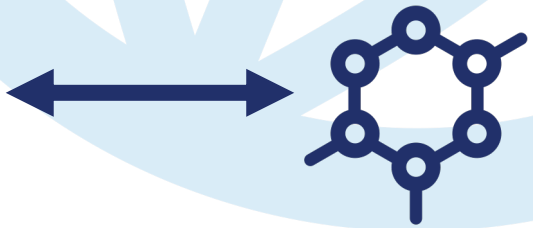


端末の中にファイアウォールが導入されたことで、直接インターネットに接続しても問題のない状態を作り、さらに効率化ができるようになった

ピュア ゼロ トラストの実現

ゲートウェイタイプのセキュリティソリューションからの脱却

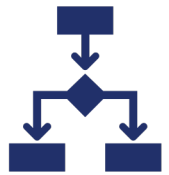
ネットワーク上のセキュリティサービスは
全て端末に持ってくることができるようになった



脅威インテリジェンスによる
リアルタイム保護

ビルトインセキュリティ機能

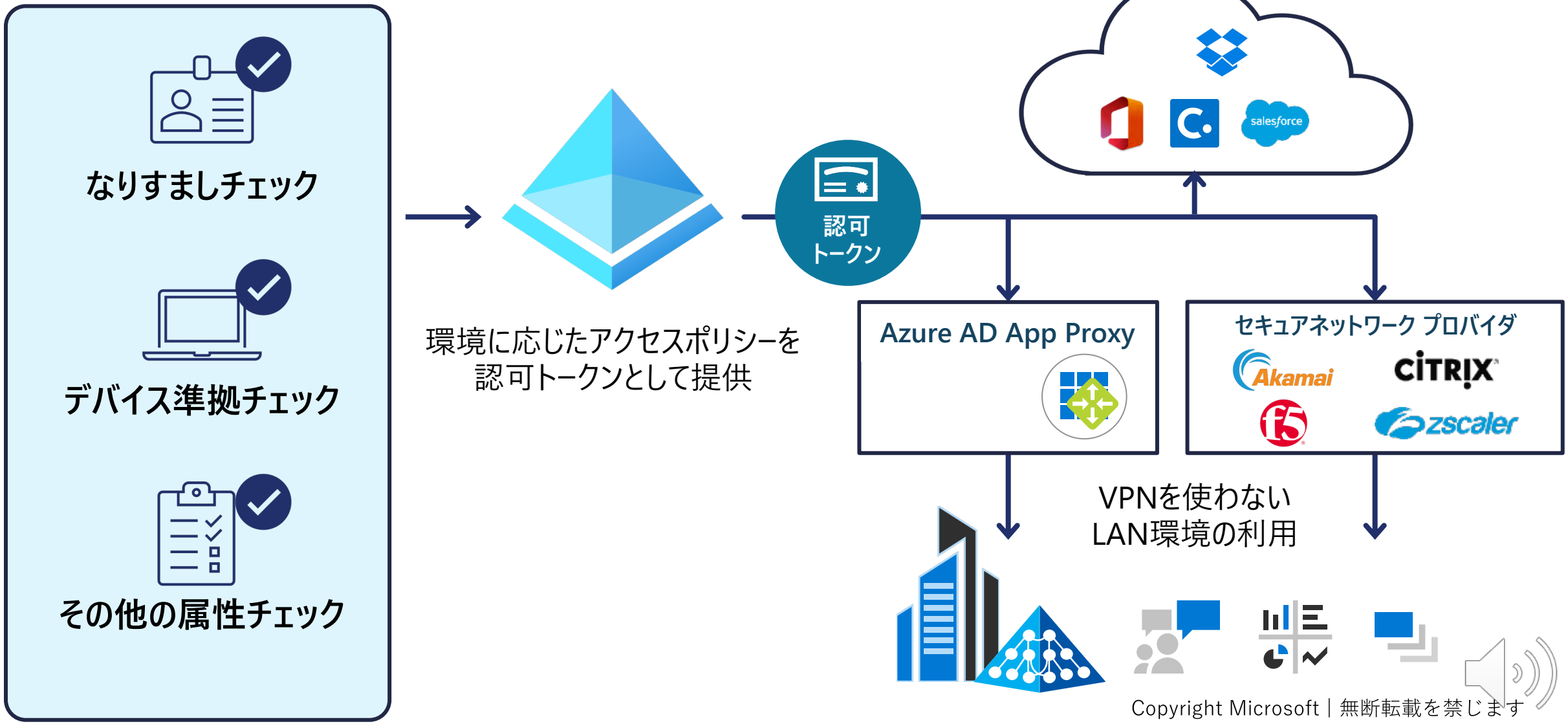
- ファイアウォール
- URLフィルター
- CASB　など



セキュアOSによる完全仲介

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

IDaaSによるクラウドとオンプレミスの統合管理



クラウドセキュリティにおけるガバナンス

- クラウドサービスの検出と管理
- 攻撃対応の自動化
- リアルタイムな情報の保護

管理を一元化することで、
運用コストを80パーセント削減

データガバナンス

適切なデータ管理とそれを実践するための手順

トラストの意識合わせから・・・ 暗号化Zipの限界

Q. ファイルの暗号化において、十分な信頼（トラスト）がおける状態とは？

①ファイルをZipにまとめて暗号化

② ファイルとパスワードを別に転送

共有パスワードを使った暗号化にトラストはない

Q. ファイルの暗号化において、十分な信頼（トラスト）がおける状態とは？

× ファイルは総当たり攻撃でいつか開かれてしまう

× 仲介者による開封、改ざんに気がつくことができない

× パスワードが漏れてしまったときにパスワードの変更ができない

①ファイルをZipにまとめて暗号化

× Zipファイルを展開すると平文に戻ってしまう

② ファイルとパスワードを別に転送

× ファイルと鍵を他社に転送されてしまう

情報流出？それとも不正アクセス？

データ流出・漏洩

データが流出したが、不正に利用されているかどうかはわからない。単純にデータが手元から離れたということで、インターネット上の暗号化されたデータもある意味では流出状態にあると言える。

不正アクセス・危殆化

データが不正に、もしくは誰にでもアクセスできる状態になっている。

情報の安全な状態とは・・・？

データ管理のライフサイクルとデータガバナンス

データオーナーはライフサイクルにわたって、
データを適切に管理する

データマネジメント

データを常にモニタリングし、
適宜修正する

データガバナンス

① 作成と入手

所有しているデータの
把握

② 保存と管理

データの状態の管理
バックアップ

③ 利用と共有

アクセス権の設定
共有設定の確認

④ 廃棄

適切な廃棄
残留データの確認

データ管理の要件

データオーナーはライフサイクルにわたって、データを適切に管理する

データマネジメント

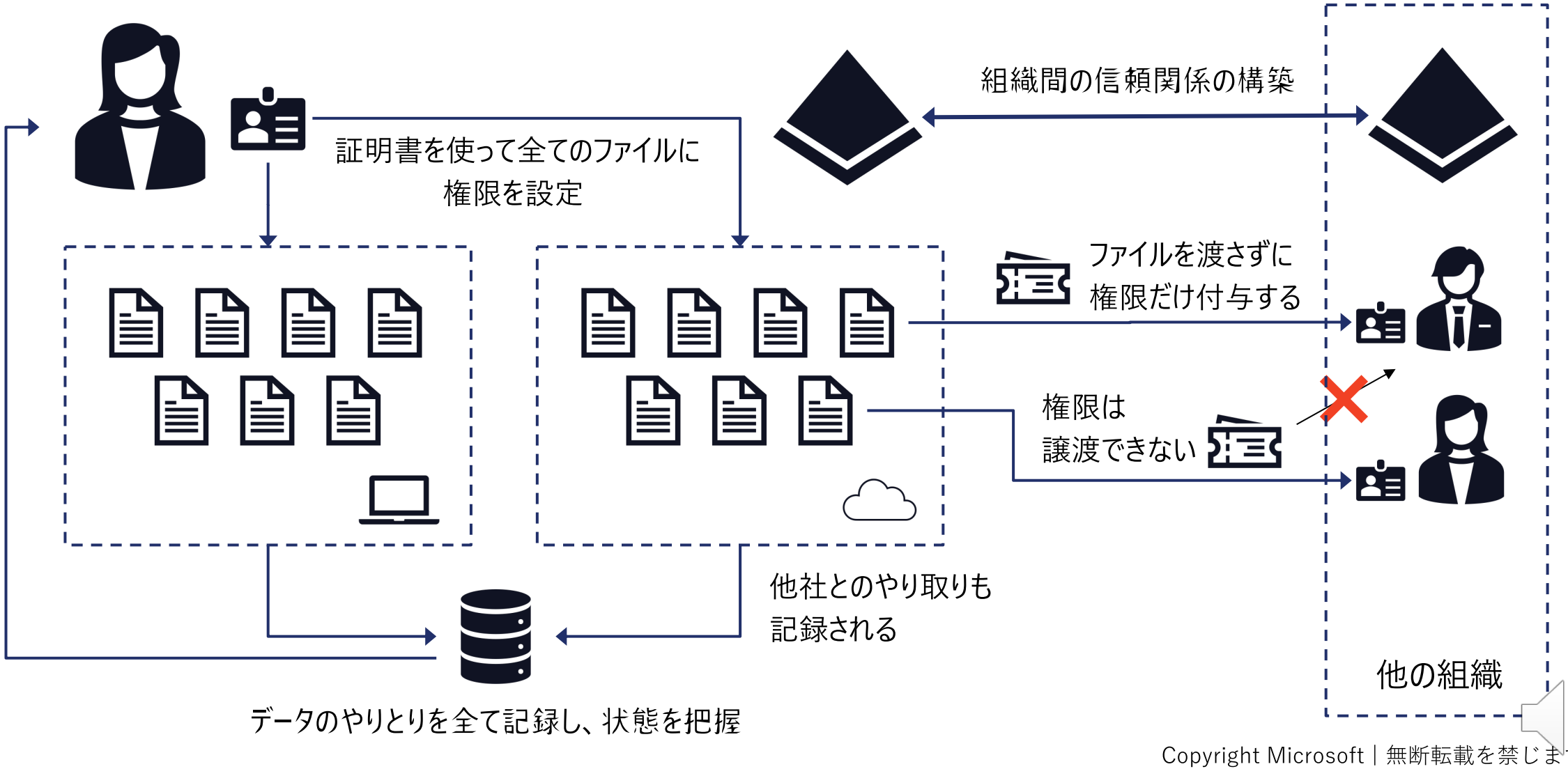
- 全てのデータにオーナーを設定する
- データオーナーはデータを分類し、ラベルをつける
- 分類に応じた保護を行う
- 分類に応じたアクセス制御を実施する
- 必要なくなったデータはアーカイブするか、廃棄する
- 必要に応じてバックアップを行う

データを常にモニタリングし、適宜修正する

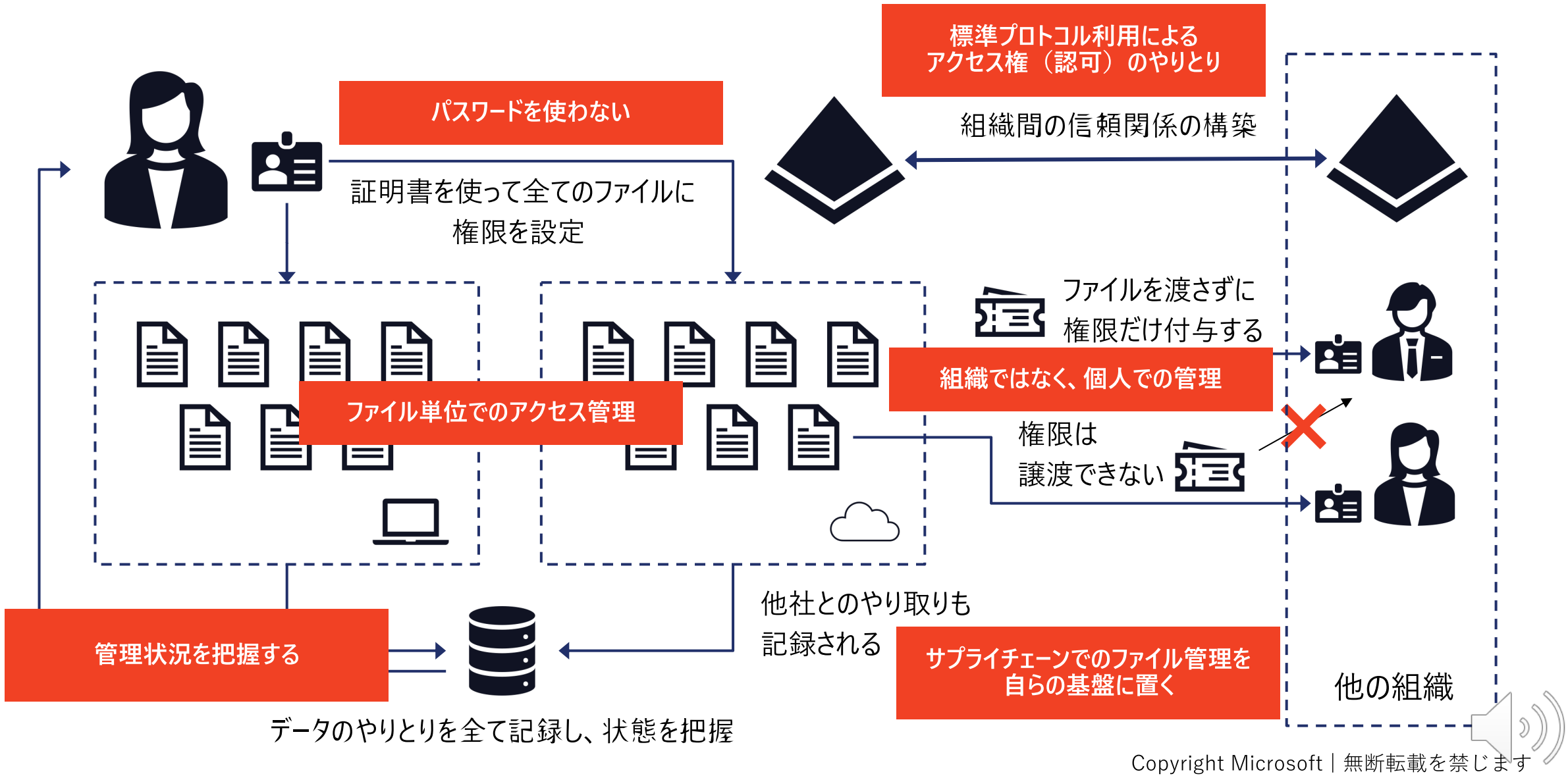
データガバナンス

- データオーナーは自らのデータの状態を把握する
- 期待する状態にない場合は修正する
- データのやり取りの全てを記録する

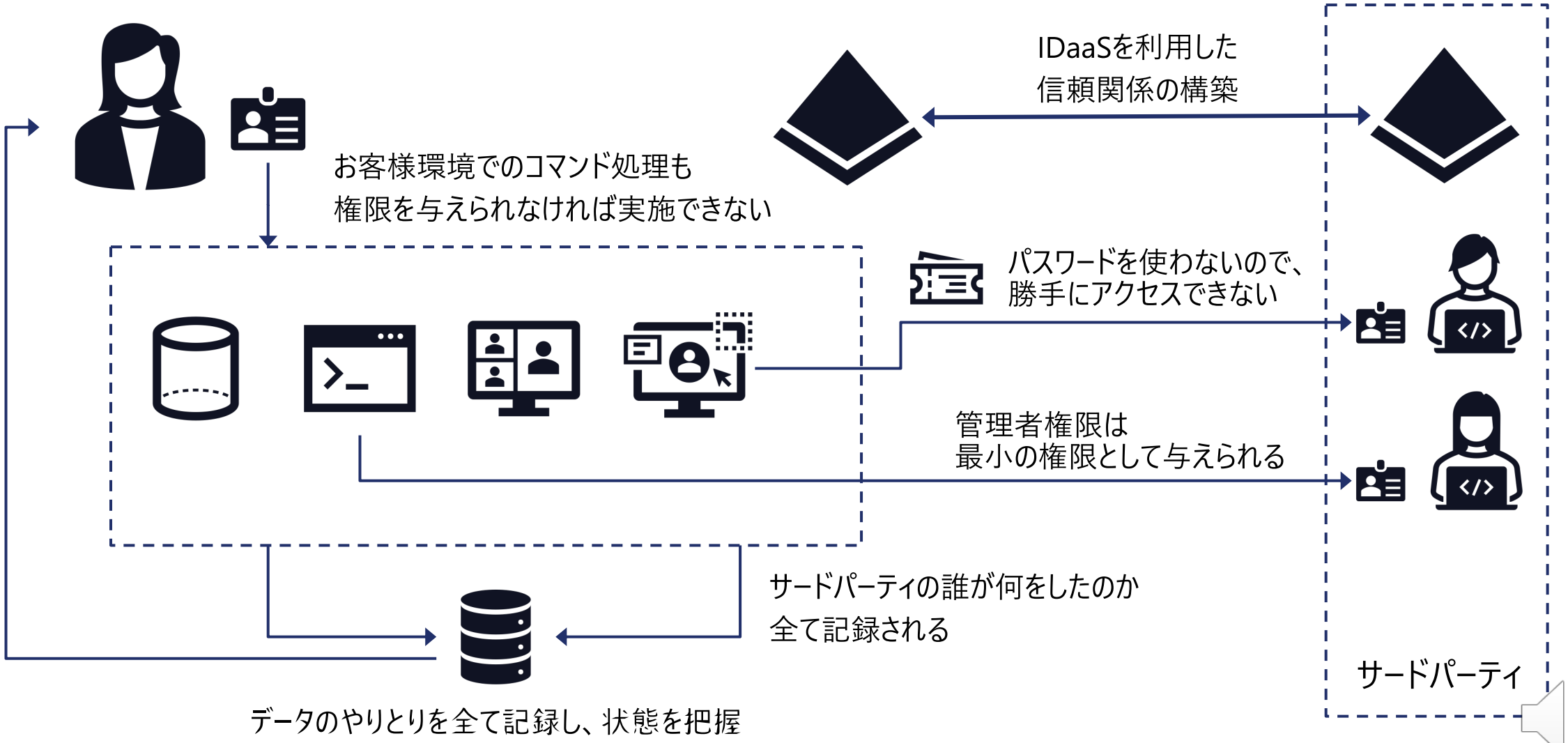
データ管理の理想的な形



データ管理の理想的な形



データ以外の処理も個別に権限付与が必要



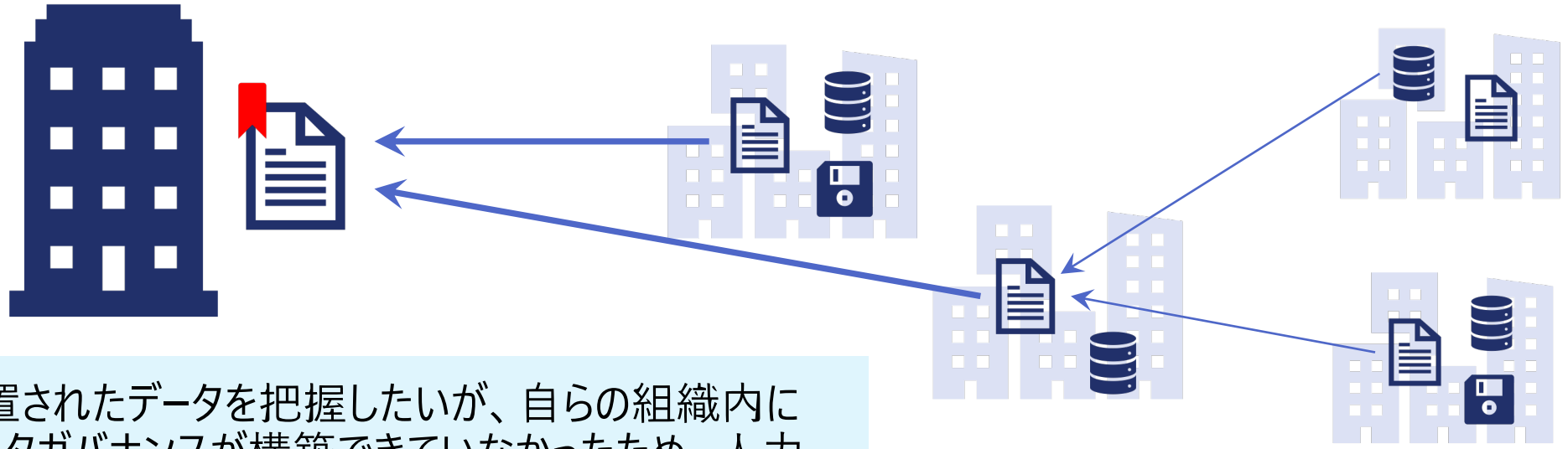
米政府におけるデータガバナンス – NIST SP800-171

Unclassified information (CUI) in nonfederal information systems

政府の機密情報

政府機密分類ではないが、関連する情報

連邦政府の情報システム外に存在する



バラバラに配置されたデータを把握したいが、自らの組織内にないため、データガバナンスが構築できていなかったため、人力で把握せざるをえない状況

データが分散された状態

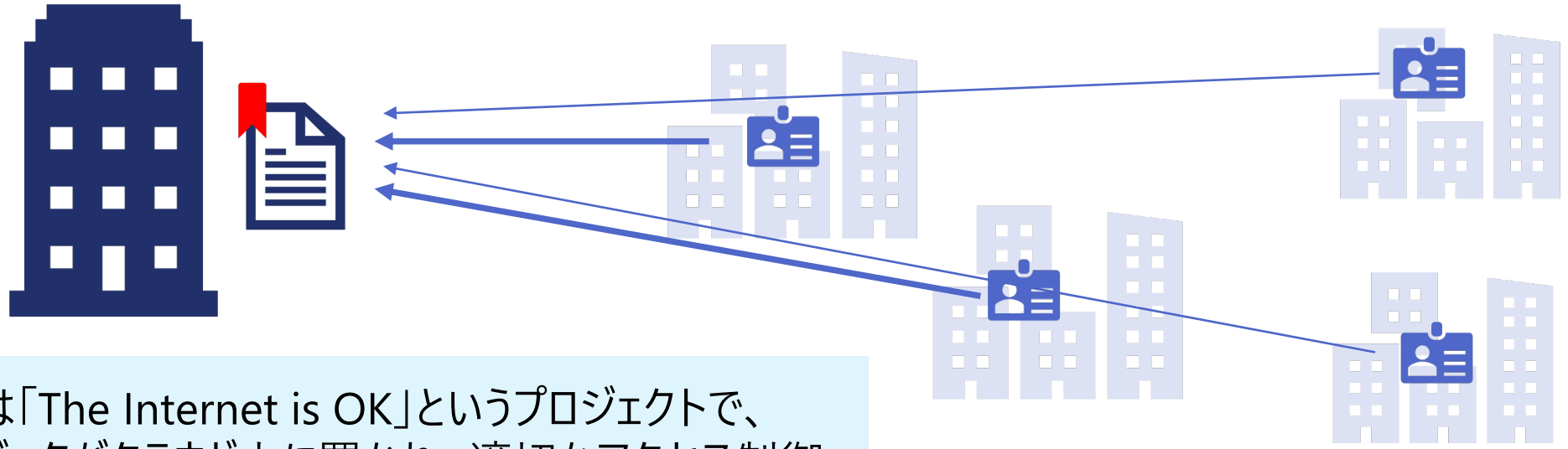
管理の連鎖 - Chain of Custody

「いつ・どこで・だれが・どのように・データに触れたか」を、
証拠として提出されるまで適切に扱い、記録する

もちろんこの記録も同様にCoCが保たれていることを証明する必要がある

データガバナンスのこれからの方向性

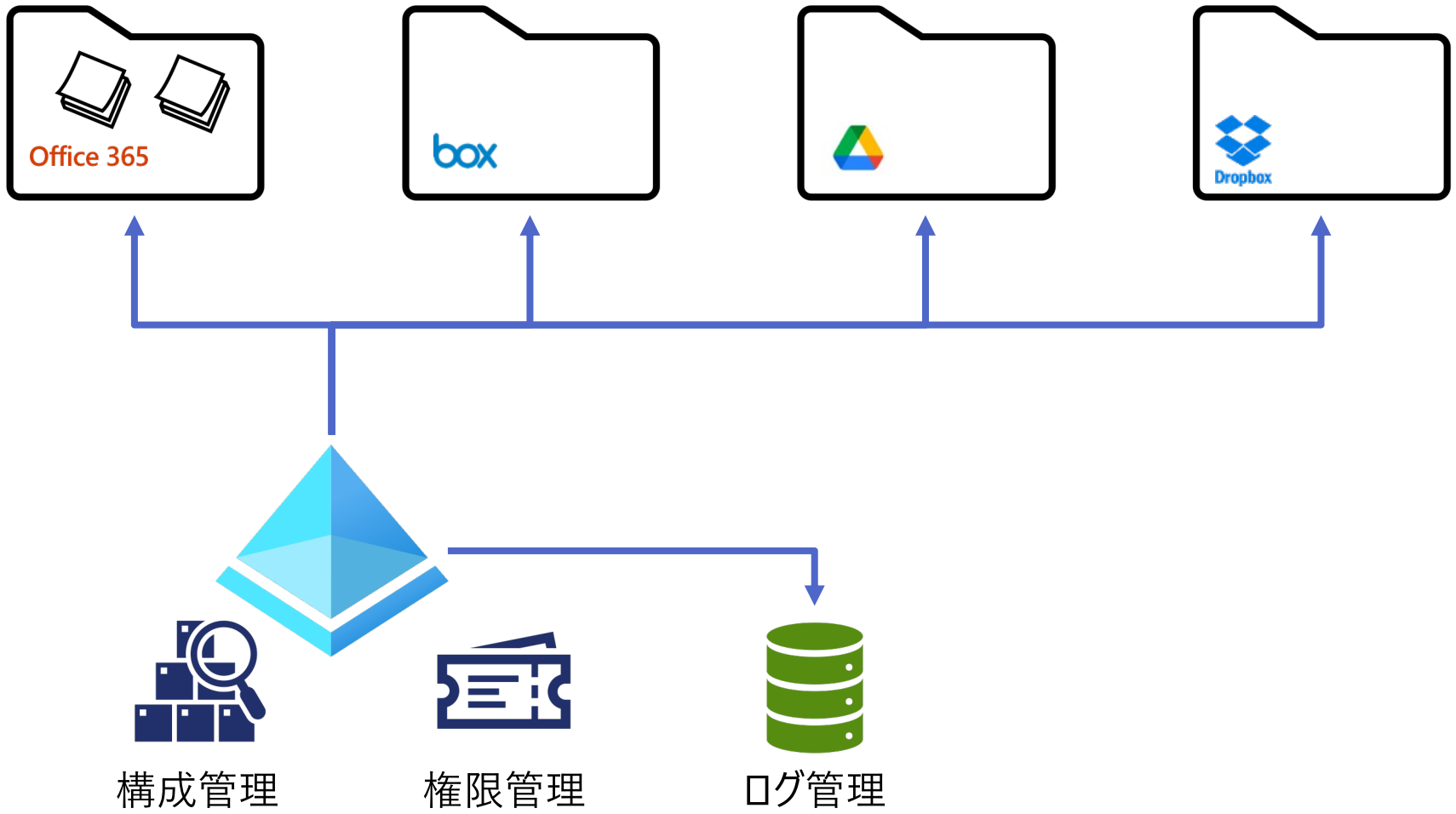
データの利用範囲を明確にし、アクセス権を設定することで、データオーナーがいつでもデータのを把握し、適切な管理ができるようになっている



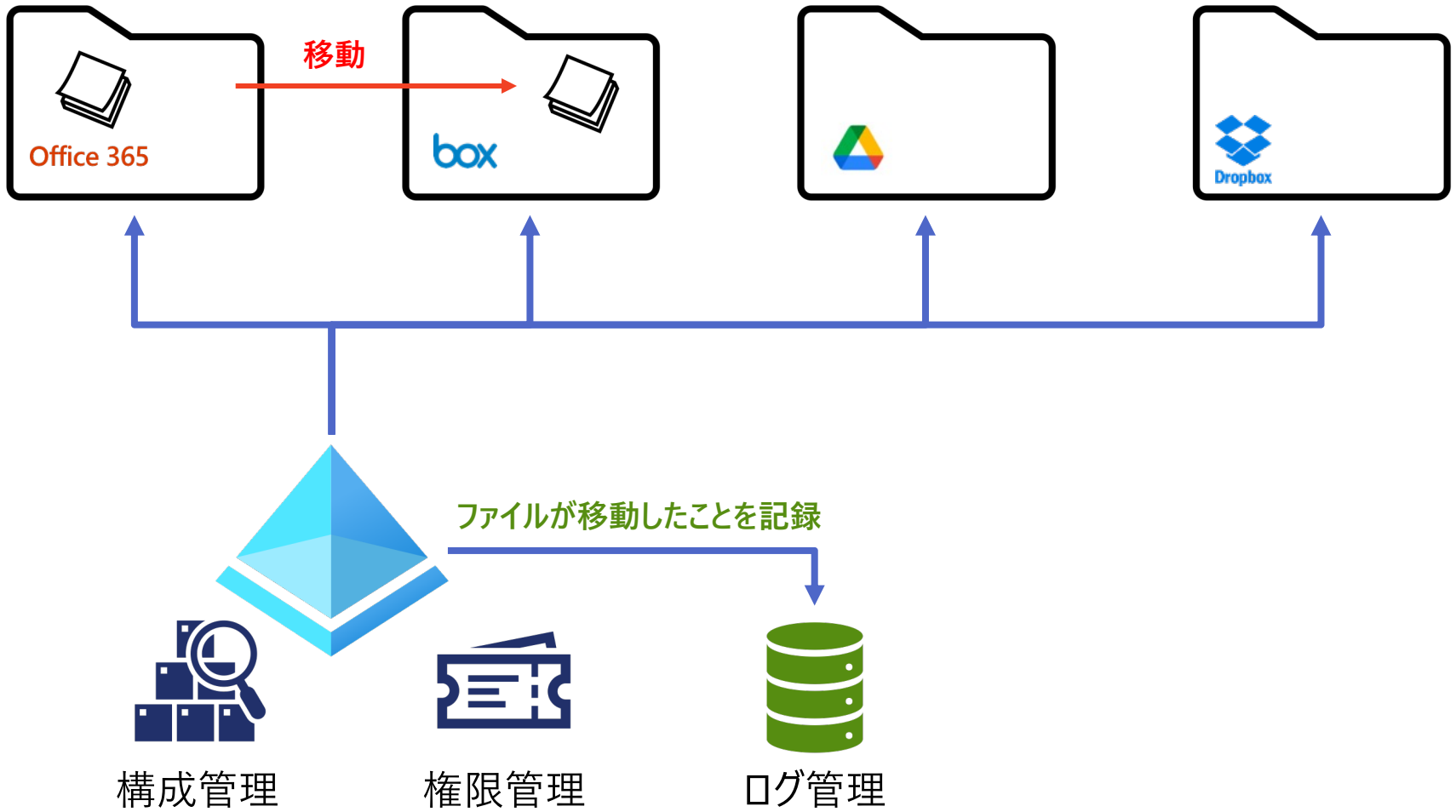
英国政府では「The Internet is OK」というプロジェクトで、70%以上のデータがクラウド上に置かれ、適切なアクセス制御により、データガバナンスが実現している

データは一元化された状態

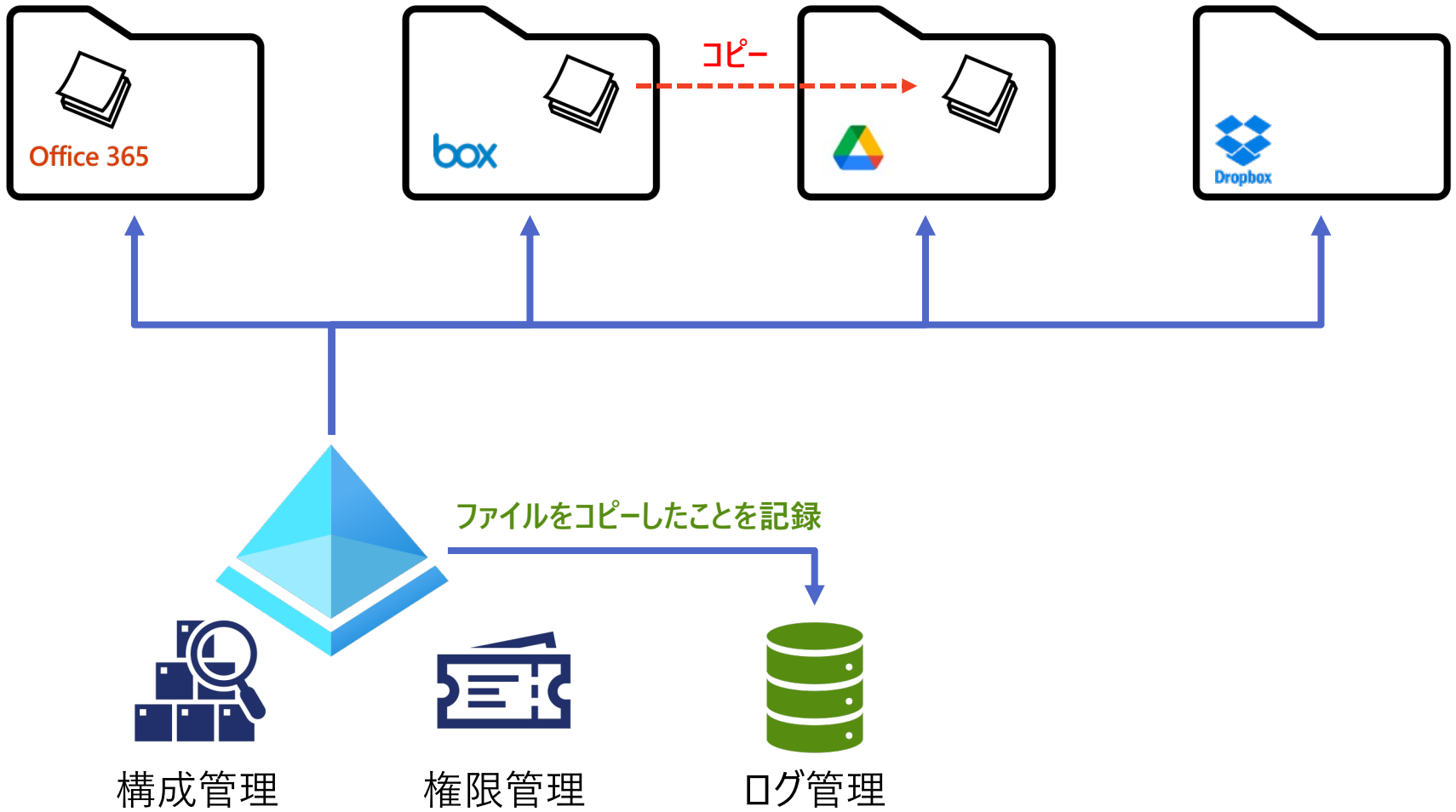
データのアクセス権を維持できることが最優先



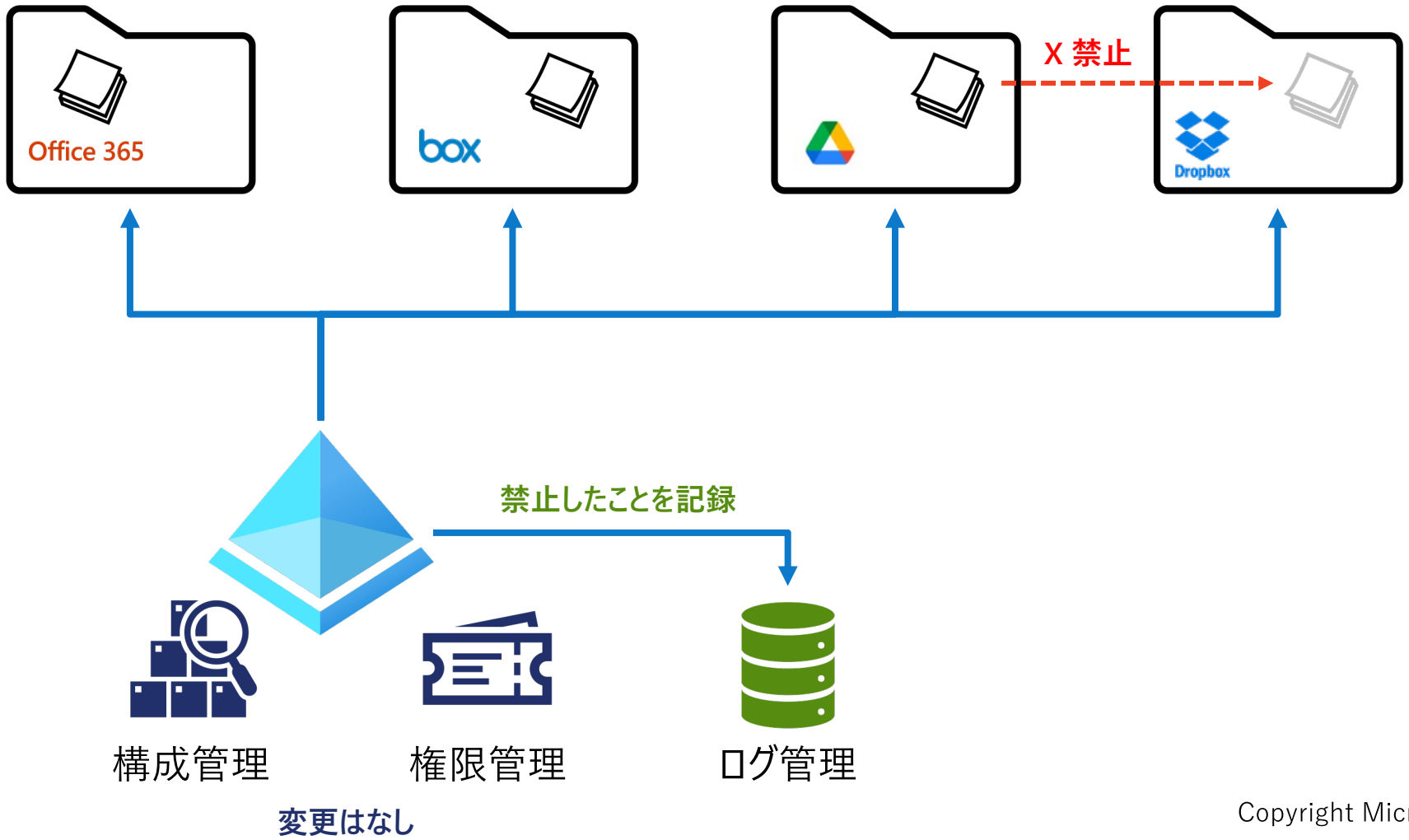
データのアクセス権を維持できることが最優先



データのアクセス権を維持できることが最優先



データのアクセス権を維持できることが最優先



ハコのセキュリティからモノやデータのセキュリティへ

利用者向けのセキュリティガイド

- 経済産業省 2011年

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

「クラウドセキュリティ活用ガイドブック」

- 内閣情報セキュリティセンター

「政府機関等の情報セキュリティ対策のための統一基準 」

- 海外 2010～2015年

FedRAMP（NIST）

ISO/IEC 27017

クラウドサービスの選び方

プロバイダ向けのセキュリティガイド

- 総務省　2014年

「クラウドサービス提供における情報セキュリティ対策ガイドライン」

- 海外

ISO/IEC 27017

選ばれやすい運用の仕方

ハコのセキュリティからモノやデータのセキュリティへ

利用者向けのセキュリティガイド

- 経済産業省 2011年

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

「クラウドセキュリティ活用ガイドブック」

- 内閣情報セキュリティセンター

「政府機関等の情報セキュリティ対策の統一基準」

基準が決まれば
全てのプロバイダが対応するので
そこに差異はない

プロバイダ向けのセキュリティガイド

- 総務省　2014年

「クラウドサービス提供における情報セキュリティ対策ガイドライン」

- 海外

ISO/IEC 27017

選ばれやすい運用の仕方

英国政府では個人情報をクラウド上で管理

“The Internet is OK”

Government Digital Service
Technology and Digital Leaders Network

政府機関の多くのシステムをパブリッククラウドサービスに移行するにつれて、PSN(注:政府機関向けの閉域網)を介しネットワーク通信することは、関係者に混乱や複雑さもたらすこと、や、標準的なアプローチでのセキュリティ対策を施しつつ、インターネット接続でのサービス利用に移行していくことについて確認。

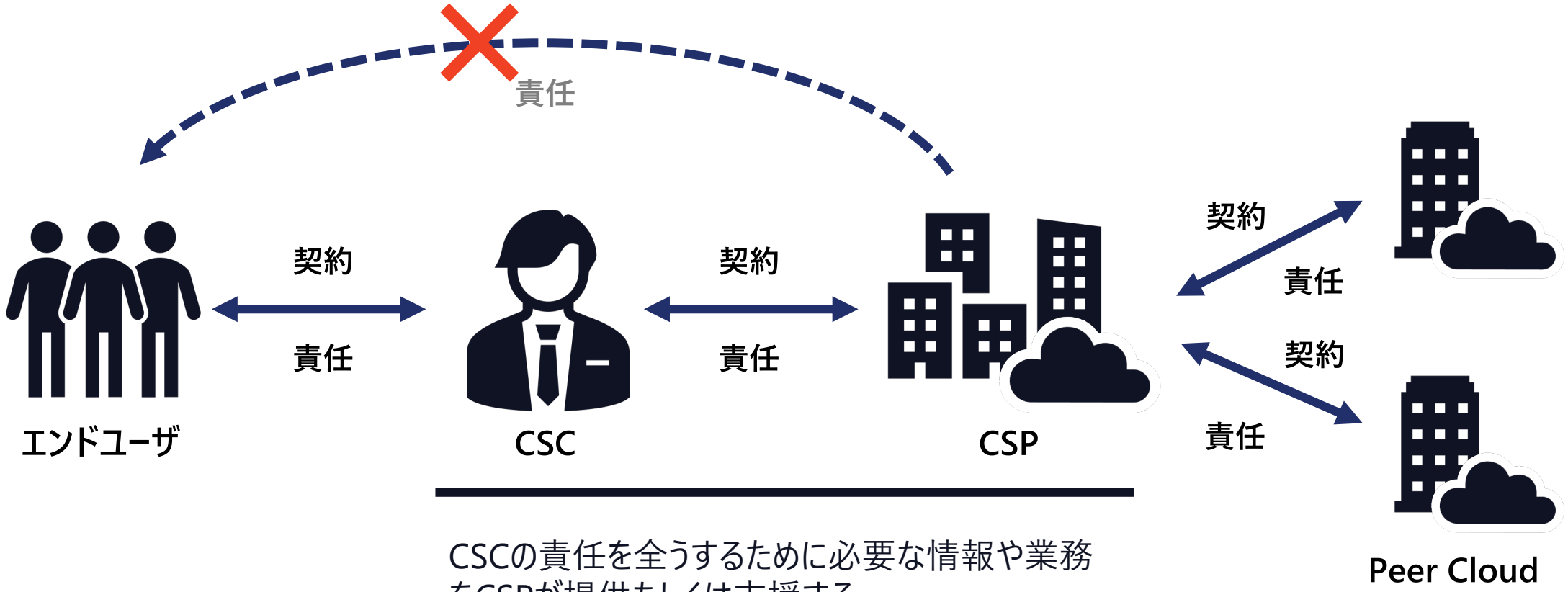
Data Classification

1. OFFICIAL（クラウドOK）： 政府機関の日常業務で利用するデータ、公共安全や犯罪・法務、個人情報(例として医療データ)等。
2. SECRET: 国民の自由や生命に関わる類の情報、軍事タスクに影響を及ぼす類の情報、等。
3. TOP SECRET: 国益や国体に深刻な影響を及ぼす情報。

クラウドセキュリティの動向

「どのプロバイダが良いのか」ではなく、どの機能が必要かを考える

クラウドサービスにおけるShared Responsibility



CSCの責任を全うするために必要な情報や業務をCSPが提供もしくは支援する

つまり、CSCが次組織もしくはエンドユーザに対して追う責任が明確にならない限り、CSPへの要求事項も決まらない

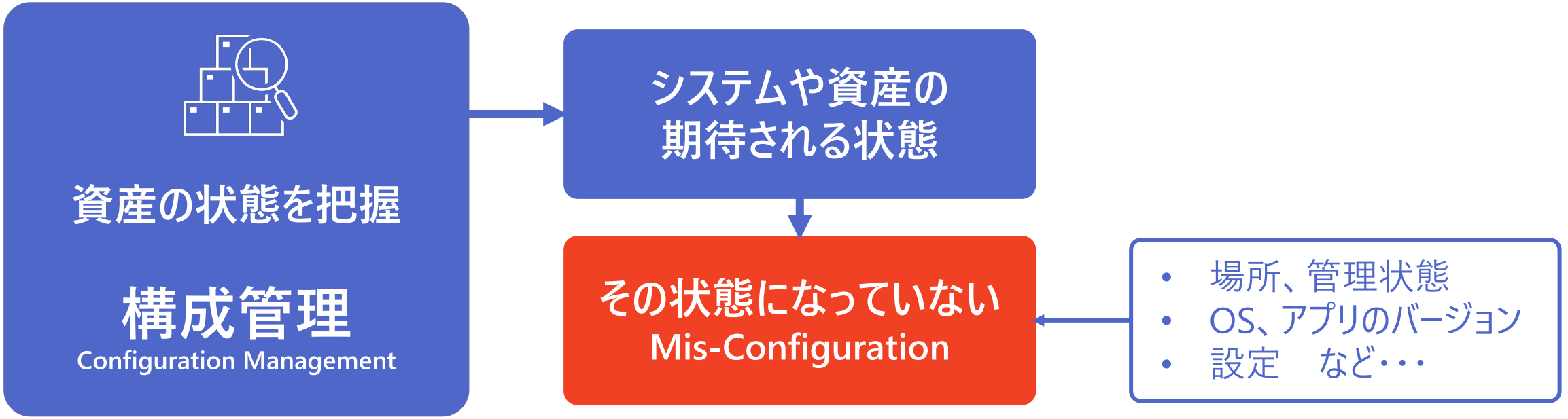
「データの暗号化」の場合

- 「データの暗号化をすること」という対策基準がある場合は、以下のように共同責任を設定することができる

状態	プロバイダ	ユーザ	エビデンス
保存	暗号機能の提供	暗号機能を利用した暗号化もしくは自動暗号化の設定を実施	データを暗号化している状態を示す構成管理データ（ユーザが設定）
転送中	暗号機能の提供（経路、データ本体）	暗号機能を利用した暗号化もしくは自動暗号化の設定を実施	データを暗号化している状態を示す構成管理データ（ユーザが設定）
処理中	適正なデータ処理	–	適正な処理をしていることを示す監査結果（プロバイダが提供）

注）暗号化においては鍵の管理こそが重要だが、ここでは暗号化しているかしていないかだけを示している。鍵の管理の責任主体はユーザにあり、適切な管理をしていない場合のデータの危殆化はユーザの責任となる。プロバイダは鍵管理をユーザ自身が実施できる機能を提供する必要がある

Mis-Configurationは単なる設定ミスではない

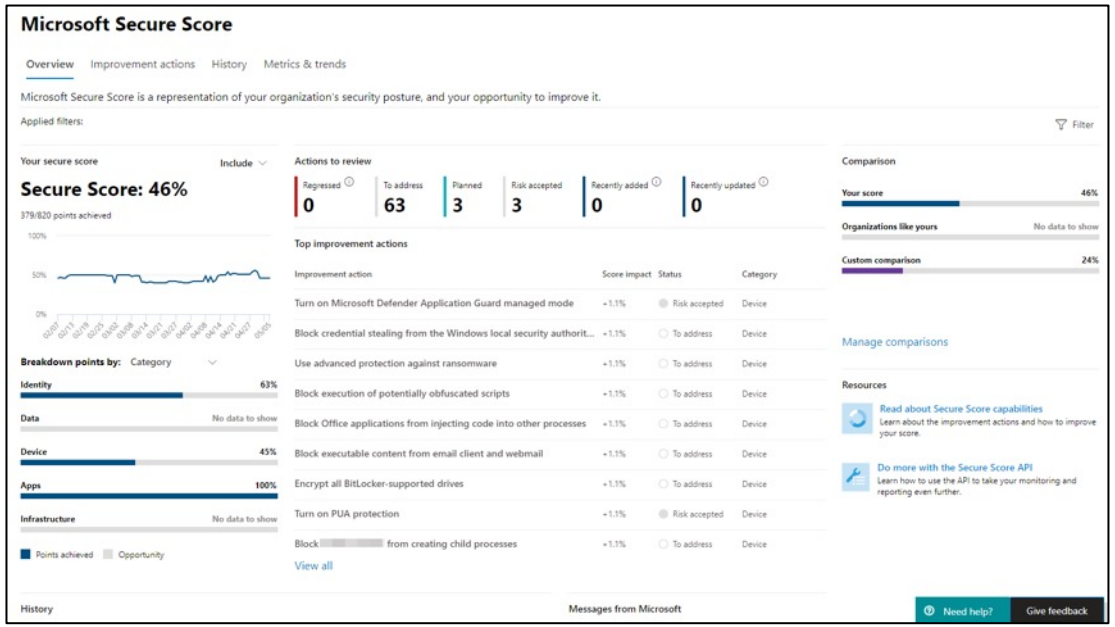


クラウド上の様々な機能が期待された状態になっているかどうを確認するためには、構成管理を厳密に行う必要がある。
セキュリティの課題ではこれらがCloud Security Posture Managementなどと呼ばれることもある。

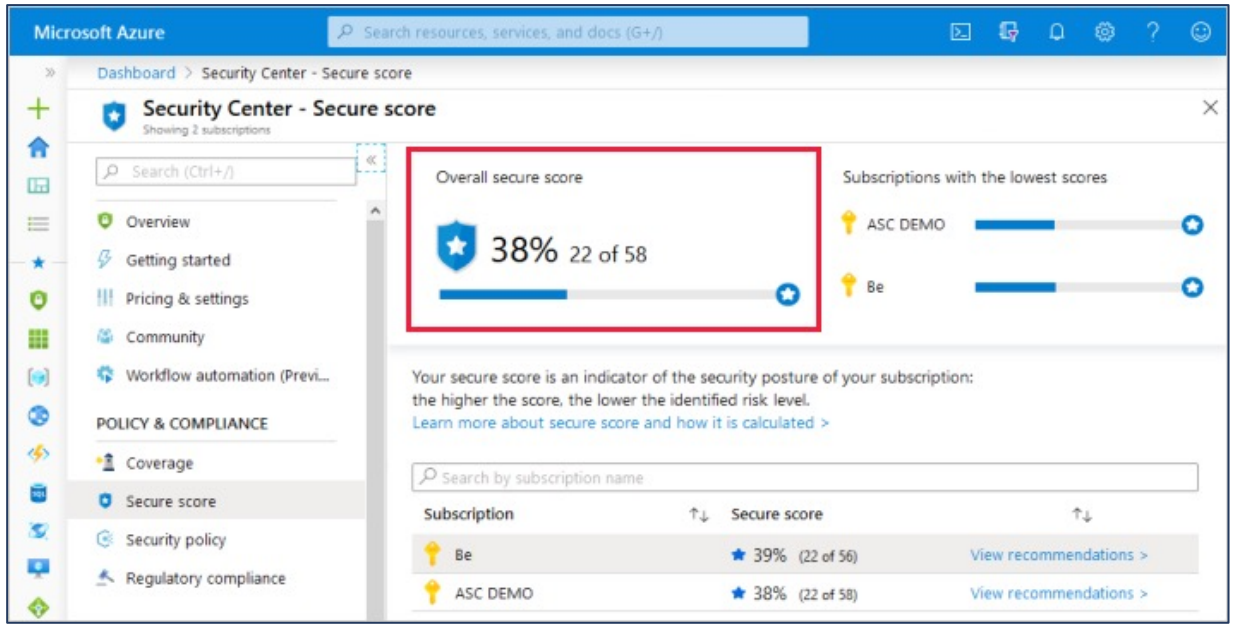
全ての資産の構成（Configuration）をリアルタイムに把握するためには、デジタルトランスフォーメーションが必要になり、
クラウドの利用を避けることはできない。

自組織のセキュリティの状態を知り、目標を達成する

Microsoft Security Scoreによる脆弱性管理と成熟度管理



Microsoft 365 Security Score



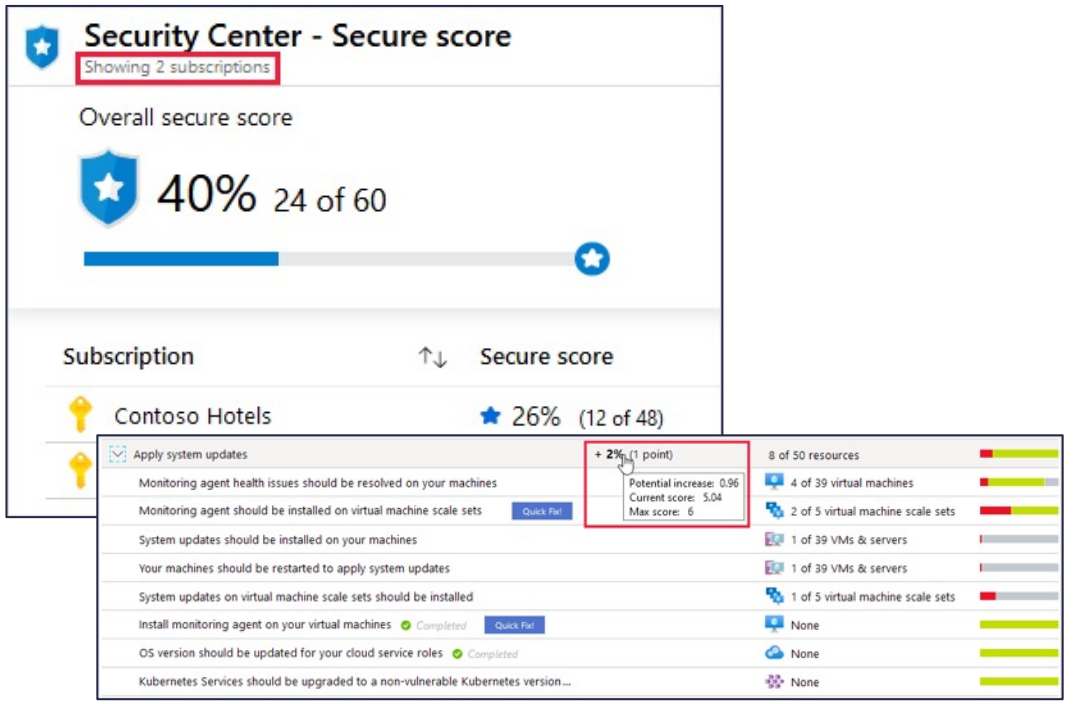
Azure Security Center Security Score

Azure Security Scoreによる構成管理

セキュリティのベースライン準拠と推奨対策の実施を支援

最低限のセキュリティ対策の実施

- MFAの有効化
- 管理ポートのセキュリティ保護
- 更新の適用
- 脆弱性の修復
- データ保存時の暗号化
- 転送中のデータの暗号化
- 認可の管理
- セキュリティ構成の修復
- ネットワークアクセス制御　など・・・



脆弱性の状況を知り、自動で修復する

Microsoft Security

Microsoft