CASB+機械学習

クラウドサービス時代のセキュリティはどう変わるのか？

株式会社 Imperva Japan

シニアセールスエンジニア　福本　淳

IMPERVA®

0

Who’s Imperva

Impervaについて

Imperva Inc.

設立　　：2002年

本社　　：3400 Bridge Parkway, Redwood Shores, CA, US

創業者　：Shlomo Kramer

現CEO　：Anthony Bettencourt

CTO　　：Amichai Shulman

従業員数　：約1000+名

事業展開　：100ヶ国以上、23オフィス

売上　　：$264.5M（2016）

IMPERVA®

導入実績

5,000＋社のエンタープライズ企業
100,000＋のクラウドユーザー

- **275+**
  政府機関／部門
- **400+**
  Forbes グローバル2000に選出された企業
- **トップ10の7社**
  グローバル電気通信事業者
- **トップ10の5行**
  米国商業銀行
- **トップ5の3社**
  - グローバル金融サービス企業
  - グローバルコンピュータ・ハードウェア企業
  - グローバルバイオテクノロジー企業
  - グローバル保険サービス企業

IMPERVA®

IMPERVA®

ビジネス・組織活動に不可欠な
データとアプリケーションを守る

DISCOVER
資産をおよび脆弱性を検出

PROTECT
情報を保護

COMPLY
規則、法令の遵守

マーケットでの評価（第3者機関）

Webアプリケーションファイアウォール

3年連続唯一のリーダー（～2016）

DDoS対策ソリューション 2016年

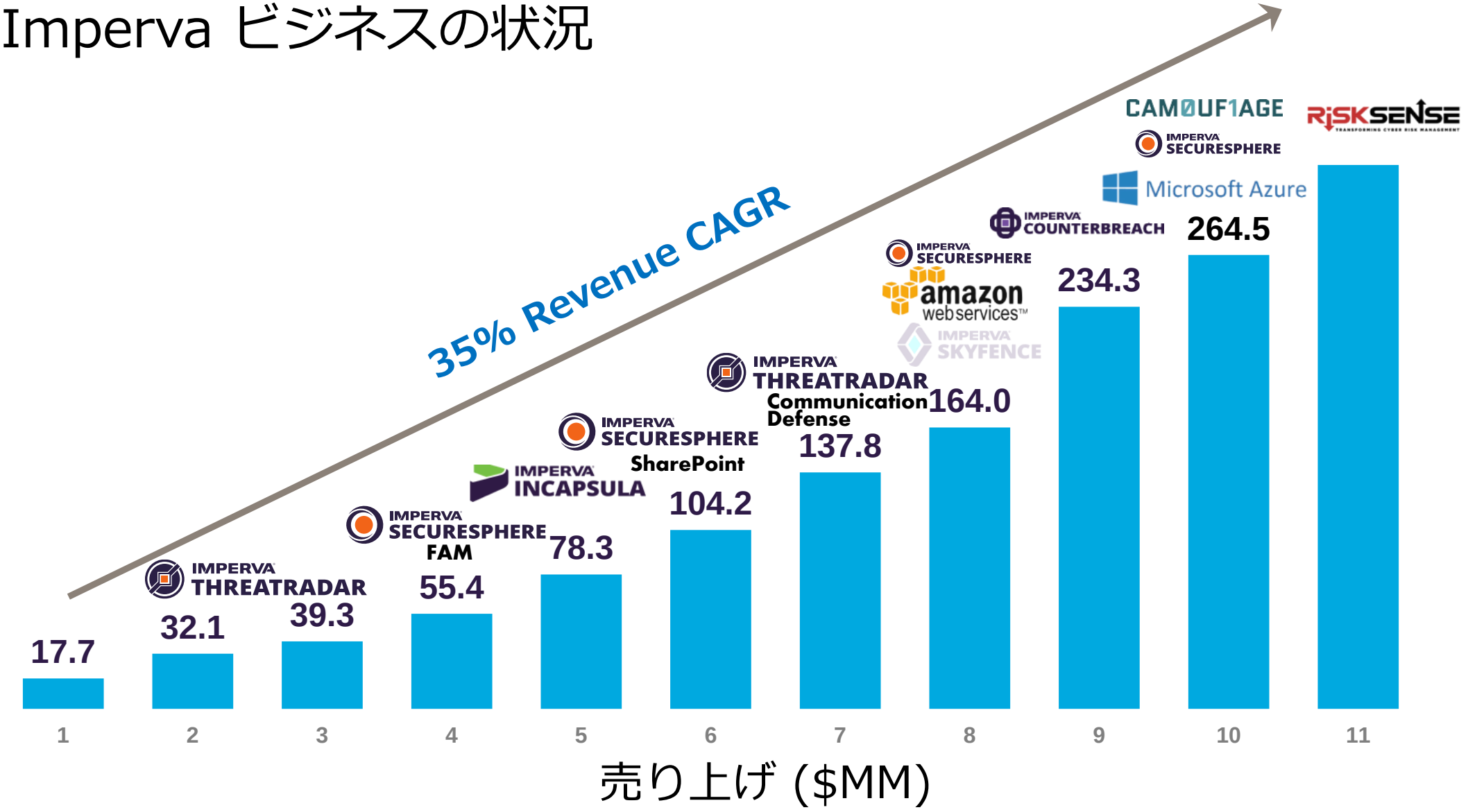
提供されている機能で**最高の格付け、かつリーダー**ポジション

データセキュリティガイド 2016年

IMPERVAが、現代に適したデータセキュリティ市場を**主導しているリーダー**

IMPERVA®

Imperva ビジネスの状況



2016 Excellence in Information Security Testing Award

2016 Most Innovative Cloud Security Solution

2016 Most Innovative Data Center Security Solution

2014 Global Web Application Firewall Market Leadership Award

2014 Network World Asia Information Management Awards For Most Promising Data Protection Solution

IMPERVA®

株式会社 Imperva Japan

設立：2007年

本社：東京都中央区京橋2-7-14 BUREX京橋

Japan Area Vice President：長坂 美宏

主要パートナー：マクニカネットワークス株式会社
ソフトバンク・テクノロジー株式会社
株式会社ネットワークバリューコンポネンツ（NVC）
ＮＲＩセキュアテクノロジーズ株式会社
CTC、ユニアデックス、NEC、Fujitsu、NTTデータ、KEL、LAC、NS-SOL他

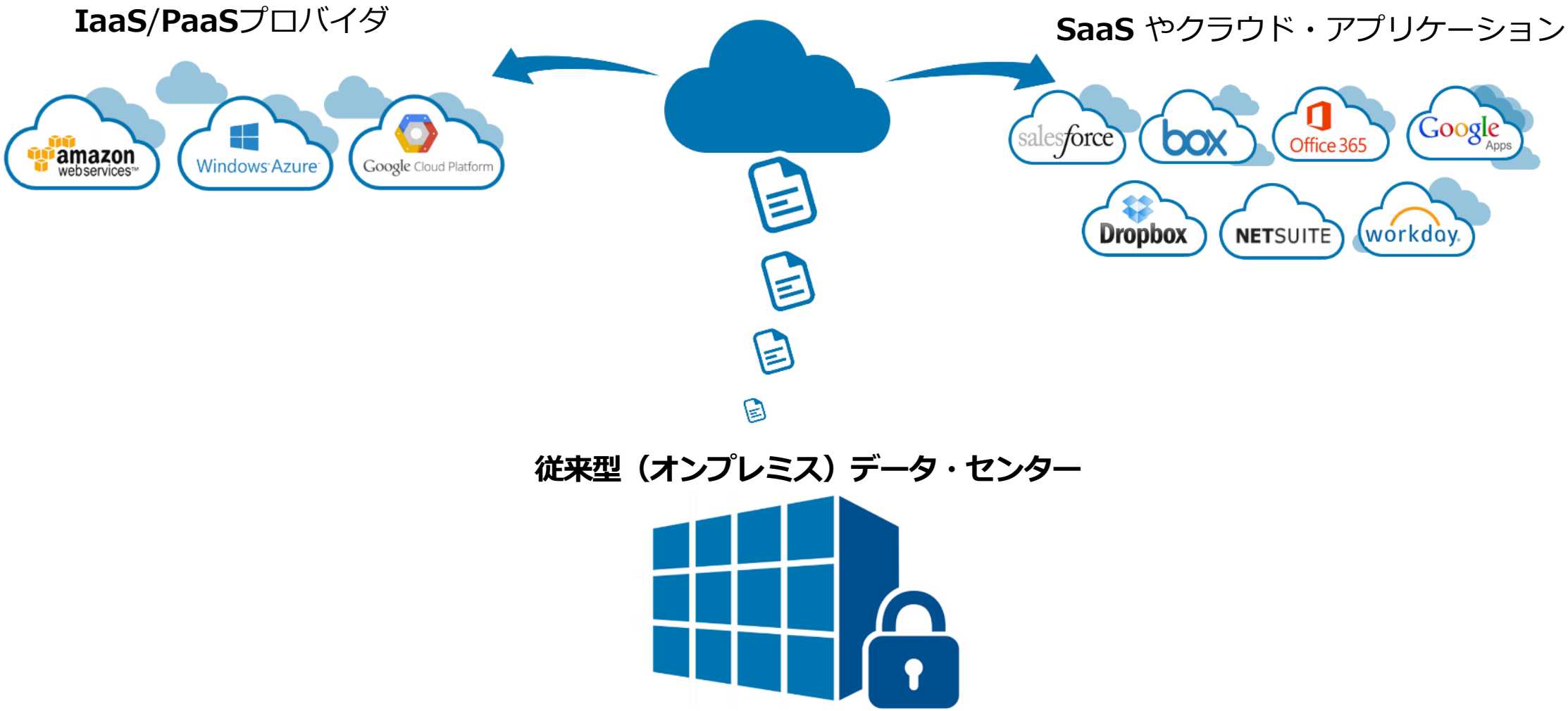
2010年以降、日本国内WAF市場シェアNo.1、および最高の評価

1

What’s CASB

CASBとは

クラウドへのデータ移行が進行中



IMPERVA®

クラウドアプリケーションの普及と死角

生産性、利便性、コストを考えた場合、広く普及しているクラウド・アプリケーションの利用を止められる組織はない

生産性向上
(Office 365, Google Apps)

ファイル共有
(Box, Dropbox, Google Drive)

ビジネスサポート
(Salesforce, AWS, ServiceNow, NetSuite, etc.)

既存のクラウド・アプリケーションで提供する標準機能は、IT管理者にとって、可視化やコントロールの面でセキュリティの死角を創出

IMPERVA®

Cloud Access Security Brokers（CASB）とは？

Cloud Access Security Brokers（CASB “キャスビー”） ← Gartnerが提唱

ガートナーの定義によれば、企業や組織が利用する複数のクラウドサービスに対して、認証／シングルサインオンやアクセス制御、データ暗号化、ログ取得、マルウェア対策といった、一貫したセキュリティポリシーを適用できるクラウドサービスを指す

Cloud Access Security Broker (CASB)

“CASB は、クラウドサービスを利用する組織にとって不可欠なセキュリティプラットフォームです ”

https://www.gartner.co.jp/press/html/pr20160711-01.html

2016年の情報セキュリティ・テクノロジのトップ10

IMPERVA

なぜ、CASBが注目されているか

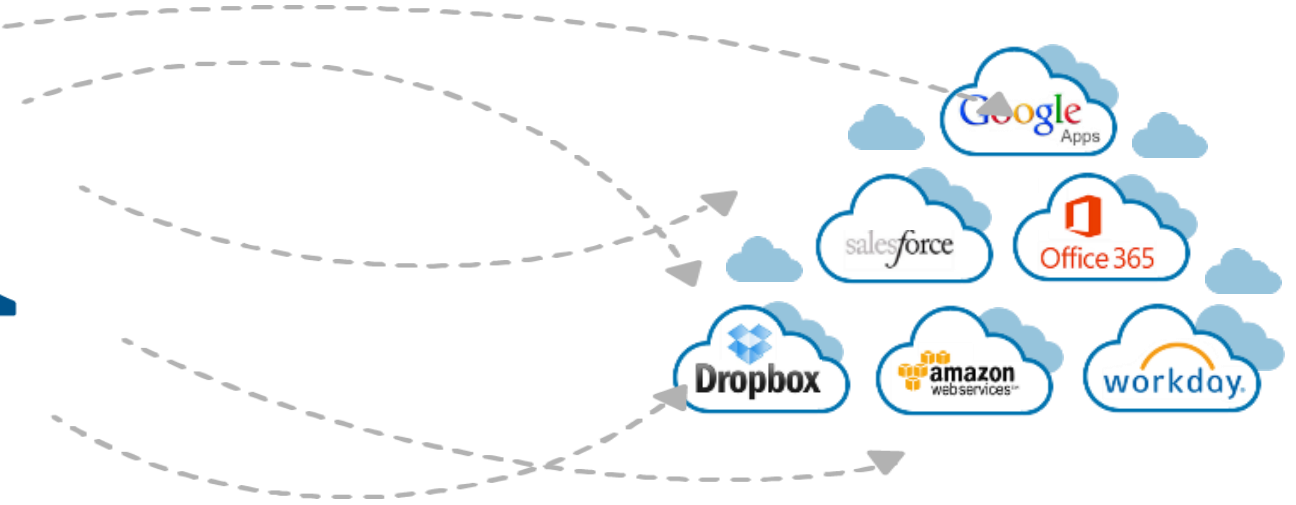
- ITコスト削減に伴い、 SaaSやPaaS、IaaS等のクラウド利用が加速
  - AWSやAzure等の利用でネットワークインフラコストを8割削減
  - オンラインストレージの利用でファイルストレージのコストを7割削減
  - Office365への移行によりオフィスツールやメールシステムのコストを○割削減

- SaaSやPaaS、IaaSのメリットを殺さずリスク・コントロールを実現
  - クラウドの利用状況を監視し、ユーザや機能毎に利用の許可、遮断、アラート等が可能
  - SSO-IdPとの連携により、エンドユーザの利便性を保ちつつセキュリティを向上

- BYOD環境へのセキュリティ対応
  - クラウドベンダによっては対応できない場合がある

クラウド・アプリケーションと “Shadow IT” の課題

職員
学生
モバイルユーザー
部外者



クラウド
アプリケーション

- 誰がどのアプリケーションを利用しているかわからない
- クラウド・アプリケーションのリスク評価の方法がない
- 使用状況を監視・分析することができない
- エンドポイントをコントロールできない
- クラウド・アプリケーションはハッカーや悪意ある内部関係者の格好の標的となっている

IMPERVA®

クラウド・アプリケーションの可視性および統制 - Skyfence

職員
学生
モバイルユーザー
部外者

クラウド
アプリケーション

Cloud Discovery & Governance (API-based)

- “Shadow IT” アプリケーションの検出とリスク
- クラウド・アプリケーション上の重要データ管理
- 非アクティブ・ユーザ抽出のため、ユーザ権限レビュー
- クラウド・アプリケーションのセキュリティ＆設定を一元的に評価・検証
- SIEM 連携

Cloud Audit & Protection (Proxy-based)

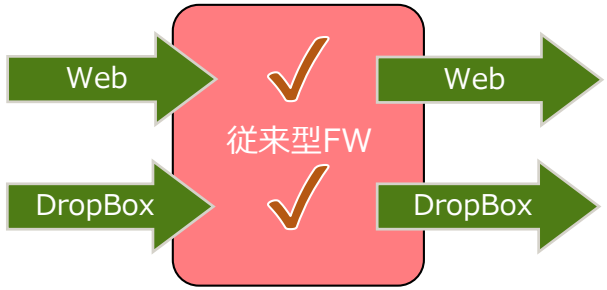
- 制御下にないデバイスの検出
- リアルタイム, 包括的なアクティブモニタリング
- DLPポリシー適用によるデータ・アクセスの制御
- 不審な振舞いの検出 & アカウント乗っ取り防止
- リスクベースの複数要素認証によるエンドポイント

IMPERVA®

従来型FW・次世代FW・Skyfence(CASB) 役割と違い

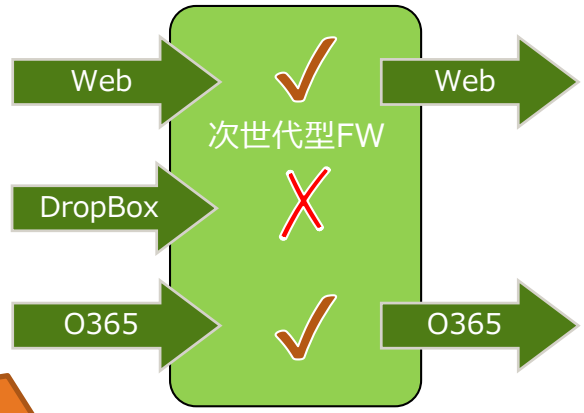
従来型FWはポート番号で制御

FW ルール: TCP:80 を許可



次世代型FWはアプリケーションを識別して制御、業務利用を禁止する

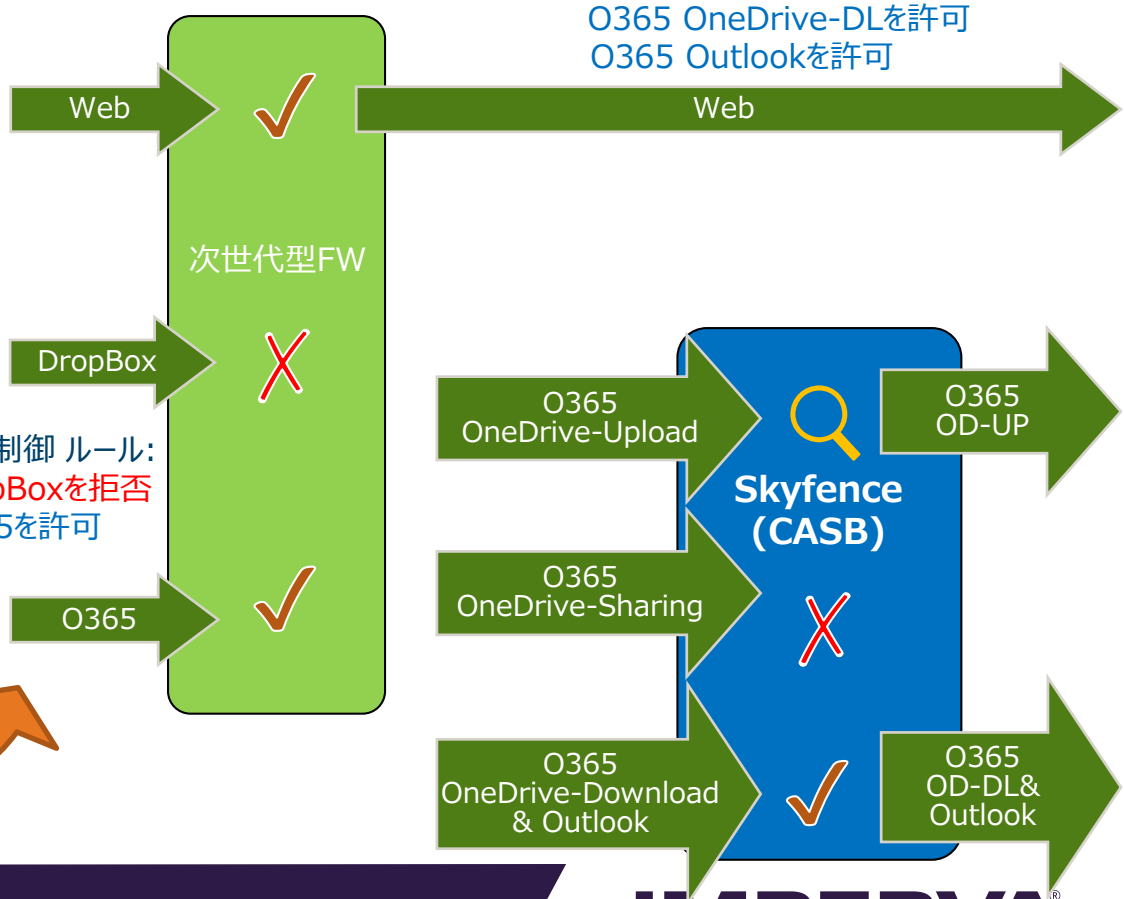
FW ルール: TCP:80 を許可
App制御 ルール: DropBoxを拒否、O365を許可



Skyfence(CASB)は業務利用を許可した「クラウドアプリケーション」の操作を識別して制御

Skyfence ルール: O365 OneDrive-UPを監査
O365 OneDrive-Sharingを拒否
O365 OneDrive-DLを許可
O365 Outlookを許可

App制御 ルール:
DropBoxを拒否
O365を許可



IMPERVA®

完全な可視化と制御のためのプロキシ構成

(3) クラウド・アプリケーションへのアクセスを管理するため、アプリケーションは、Skyfence Gatewayのリクエストに応答

(2) Skyfence ゲートウェイがユーザ・リクエストをアプリケーションに転送。Skyfenceはアクセスを分析し、イベントログを保管し、ポリシー違反にチャレンジを実行、もしくはブロック

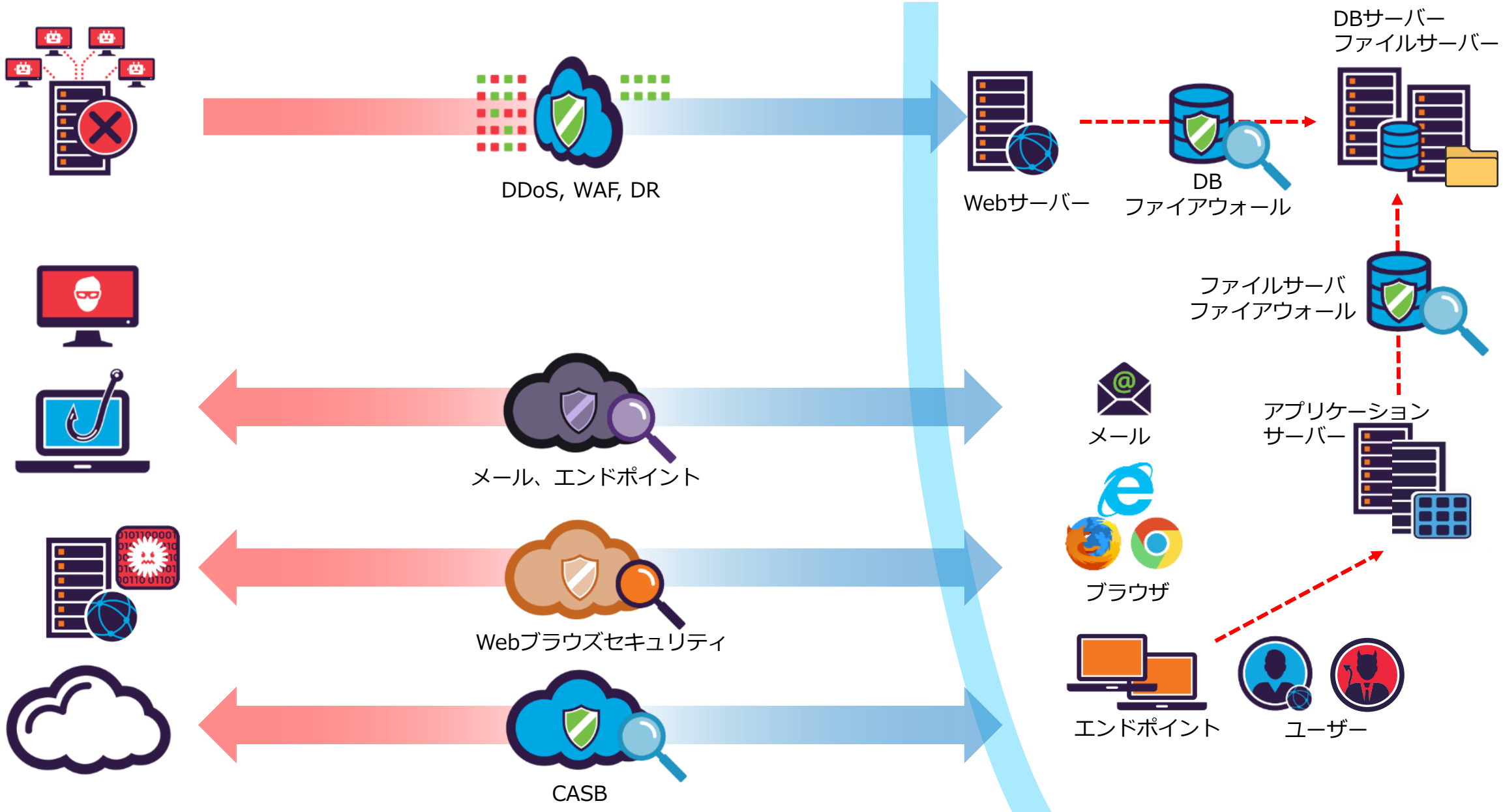
(1)モバイルや企業ユーザーが有効なIDPにより認証
（サービス・プロバイダー/エンタープライズ・ディレクトリ経由）

Active Directory Federation Services
okta PingIdentity
SECUREAUTH Centrify
onelogin

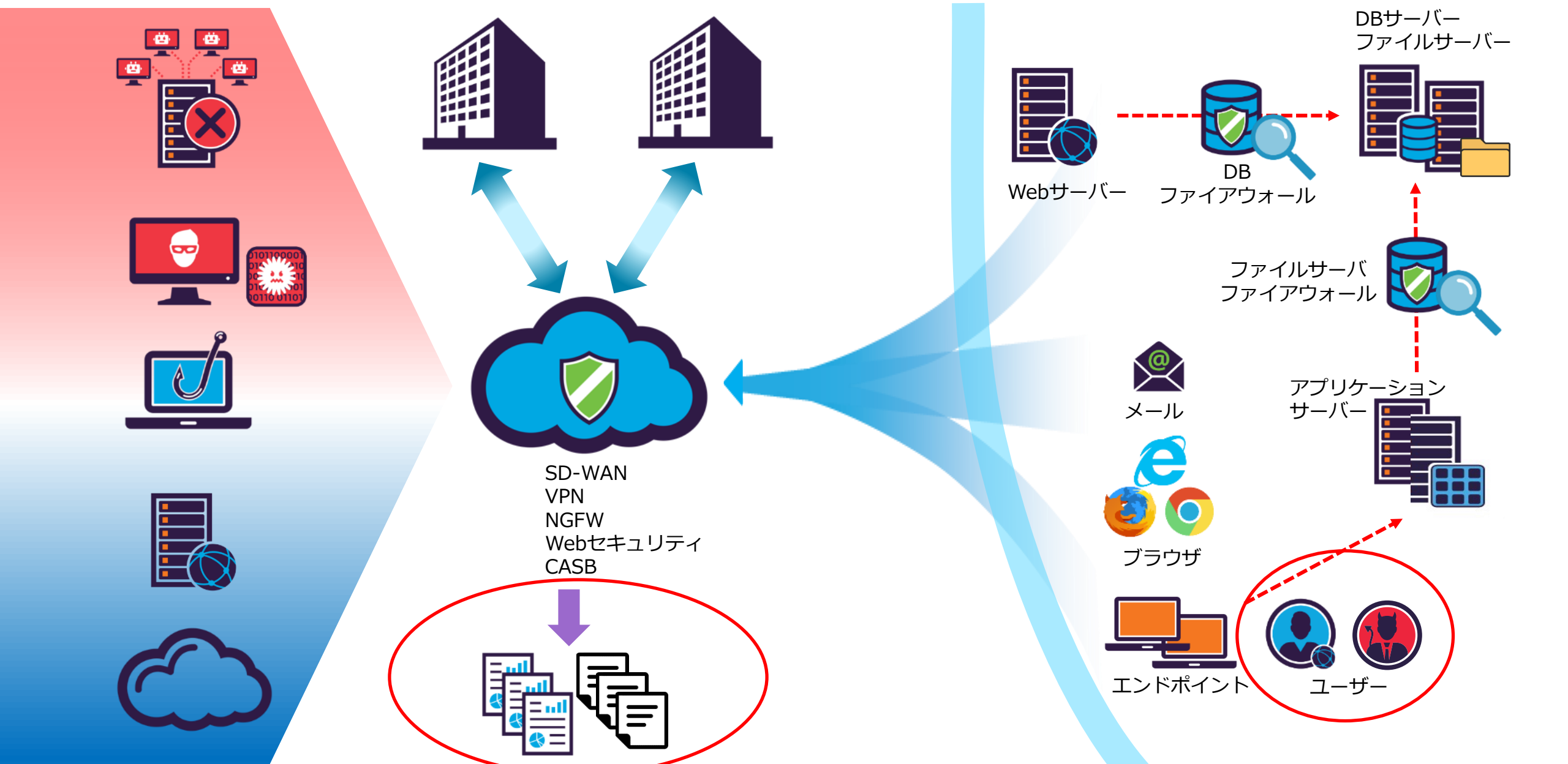
- Auto-Discovery
- Active-sync
- Mobile thick apps
- Browser-based

IMPERVA

クラウド型セキュリティゲートウェイサービス



クラウド型セキュリティ／ネットワークサービスゲートウェイ



2

Machine Learning

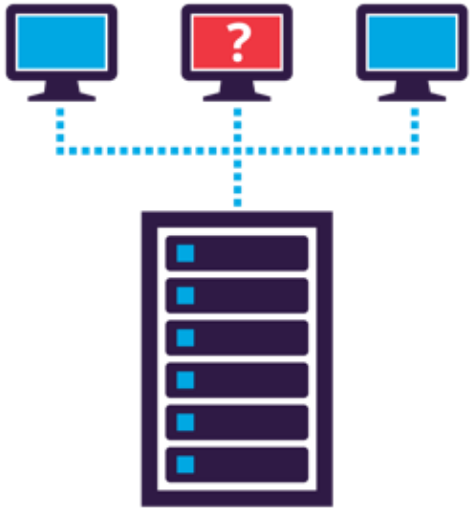
機械学習による脅威の検知

現在のIT環境において、特定多数のユーザーによる
データ共有は避けらない


ユーザーにはセキュリティポリシーやパッチを
適用できない

過剰かつフラットな情報の海から、異常を特定することの難しさ

ユーザーからの正当なデータアクセスでさえ膨大に

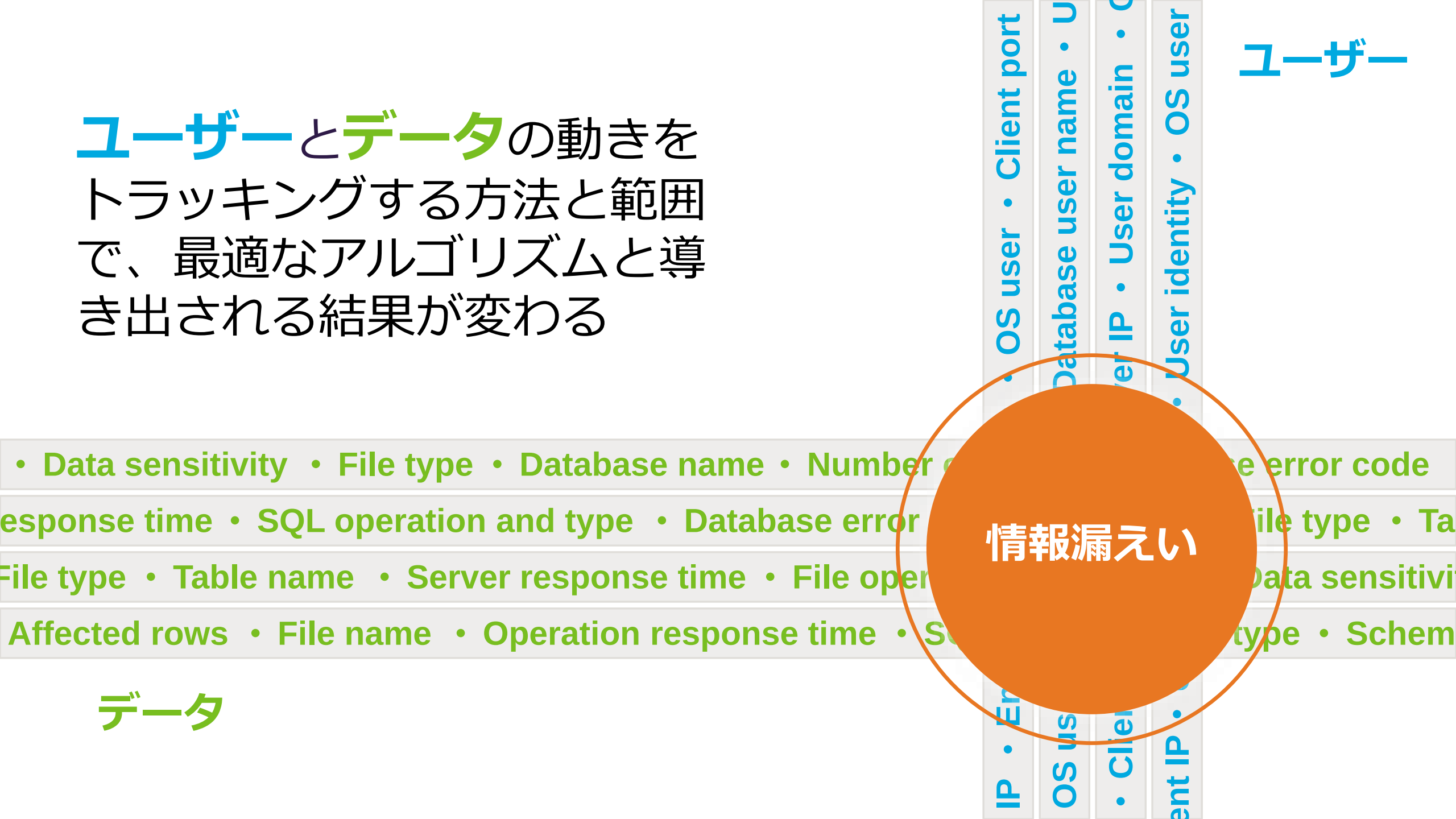


ログの詳細も完全ではなく、他社が発するアラート情報と一致しないことも多い

膨大なセキュリティアラートを選別することは、干草の中の針を探すに等しい

IMPERVA®

ユーザーとデータの動きを
トラッキングする方法と範囲
で、最適なアルゴリズムと導
き出される結果が変わる



データ侵害を識別するための要素

	アプリケーションデータへの不審なアクセス	過剰なデータベースレコードアクセス	サービスアカウントの不正利用	トラフィックの増加を抑止したファイルアクセス	過剰なファイルアクセス
ユーザ	User identity Client IP Server IP Client app	User identity User department	User identity Client IP Server IP Client app	User identity User department	User identity User department
データ	Database name Table name Data sensitivity Schema SQL operation SQL operation Type	Database name Data sensitivity Table name Schema Number of rows SQL operation	Database name Table name SQL operation SQL operation type	File operation File path File name Folder type File share name Operation response time	File operation File path File name File type File share name

IMPERVA®

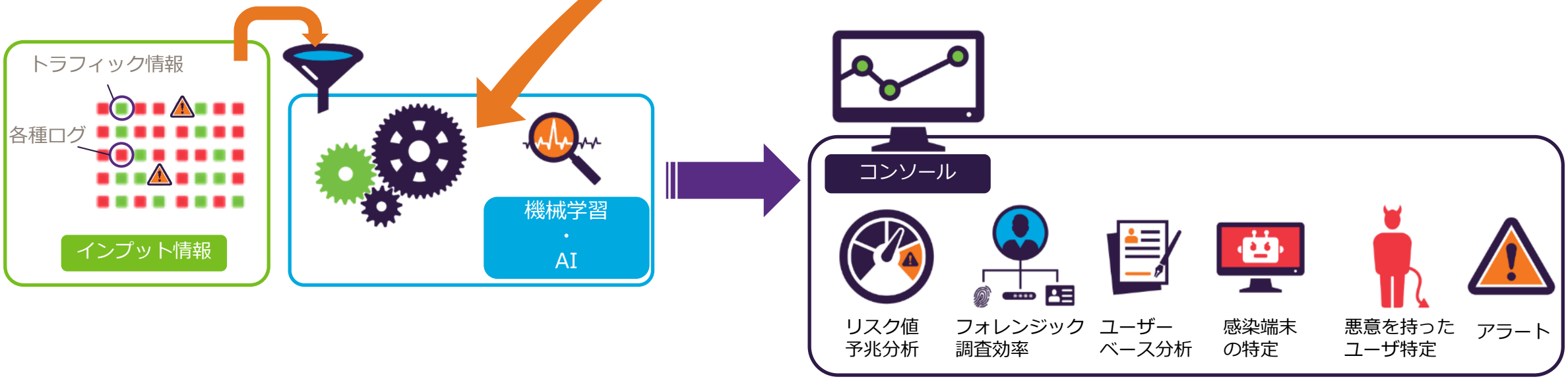
User Behavior Analytics(UBA)/User and Entity Behavior Analytics(UEBA)とは

Deep Learning/AI技術の発達

ロガー/セキュリティデバイスの浸透

ハードウェアスペックの向上

- 集められたログなどをAI/機械学習の技術を用いてユーザを中心に置いた分析を実施
- さまざまなエンティティにわたる分析の相関関係によって分析結果の精度を高めるとともに、より効果的に脅威を検知することを目的とした技術



IMPERVA®

情報漏えいインシデントに至るライフサイクルの理解も必要

1 偵察

- **マルウェア**
- 感染アカウント
- **痕跡**
- ログイン失敗

2 潜入

- **ネットワーク異常**
- 末端間通信
- **異常ログインパターン**

3 データアクセス・収集

- **過剰なデータアクセス**
- アプリケーションデータアクセス
- **サービスアカウントの不正利用**

4 データ送出

- **外部への異常な通信**
- ネットワークトラフィックの増加

UBA（User Behavior Analytics）
行動分析 → 行動ベースラインの作成

そのデータベースにアクセスするのは誰か？

どのようにデータベースに接続するのか？アクセスデバイスはいくつあってどういうデバイスなのか？

どのデータにアクセスするのか？

同僚は同じ方法、同じデバイスでアクセスしているのか？

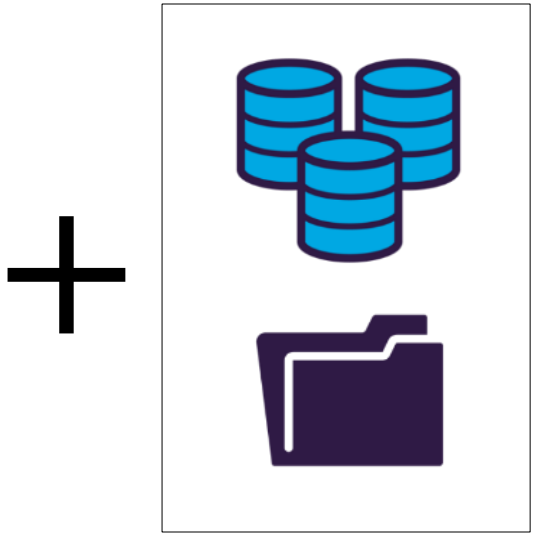
ユーザーは、一度にどのくらいのデータ量を扱うのか？
組織の平均値はどのくらいか？

ユーザーや組織は通常いつ活動しているのか？

Imperva CounterBreach ユーザーとデータのプロファイリング

アクターの分類	アプリケーション	**or**	インタラクティブ ユーザー（人間）
アカウントタイプ	サービス アカウント	**or**	個別 DBアカウント
テーブルの分類	メタデータ	**or**	ビジネス クリティカルなデータ

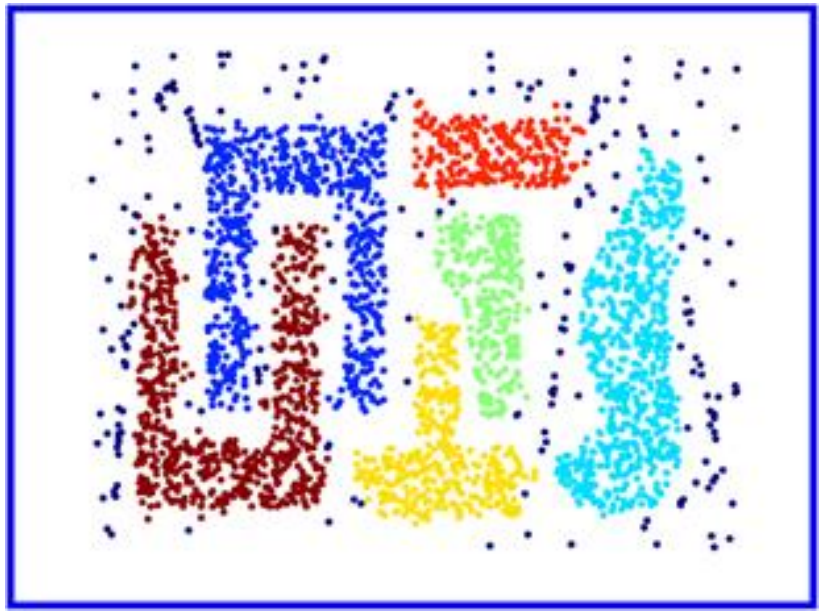
継続的な
データアクセスモニタリング



**インシデント
の検知**

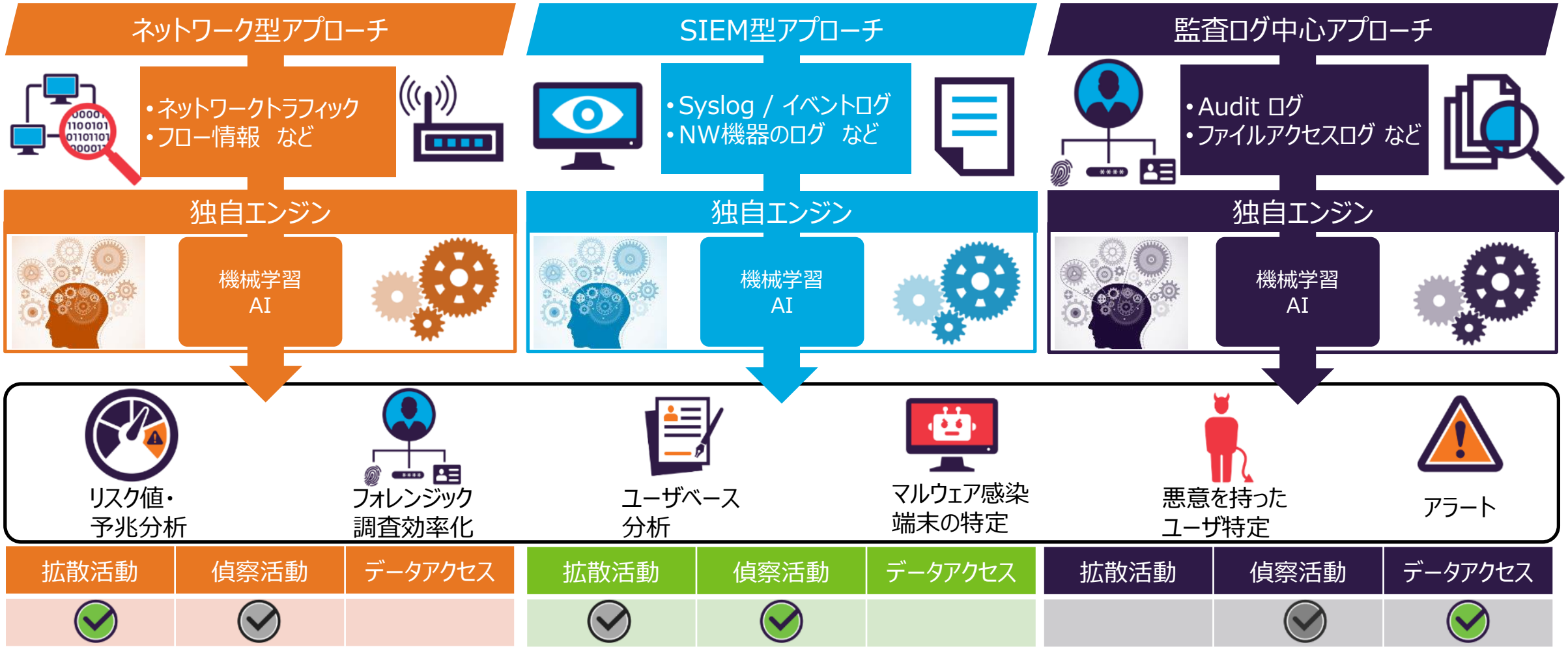
次世代ピア･グループ分析

- マシーン・ラーニングを活用して、“仮想”ワーキンググループを動的に検知する
- **Learn**：ファイルアクセスパターンを分析して、ピア･グループを学習
- **Detect：** ピア･グループ外のファイルに不適切にアクセスした内部者を検知



マシーン・ラーニングが“仮想”ピア･グループを学習

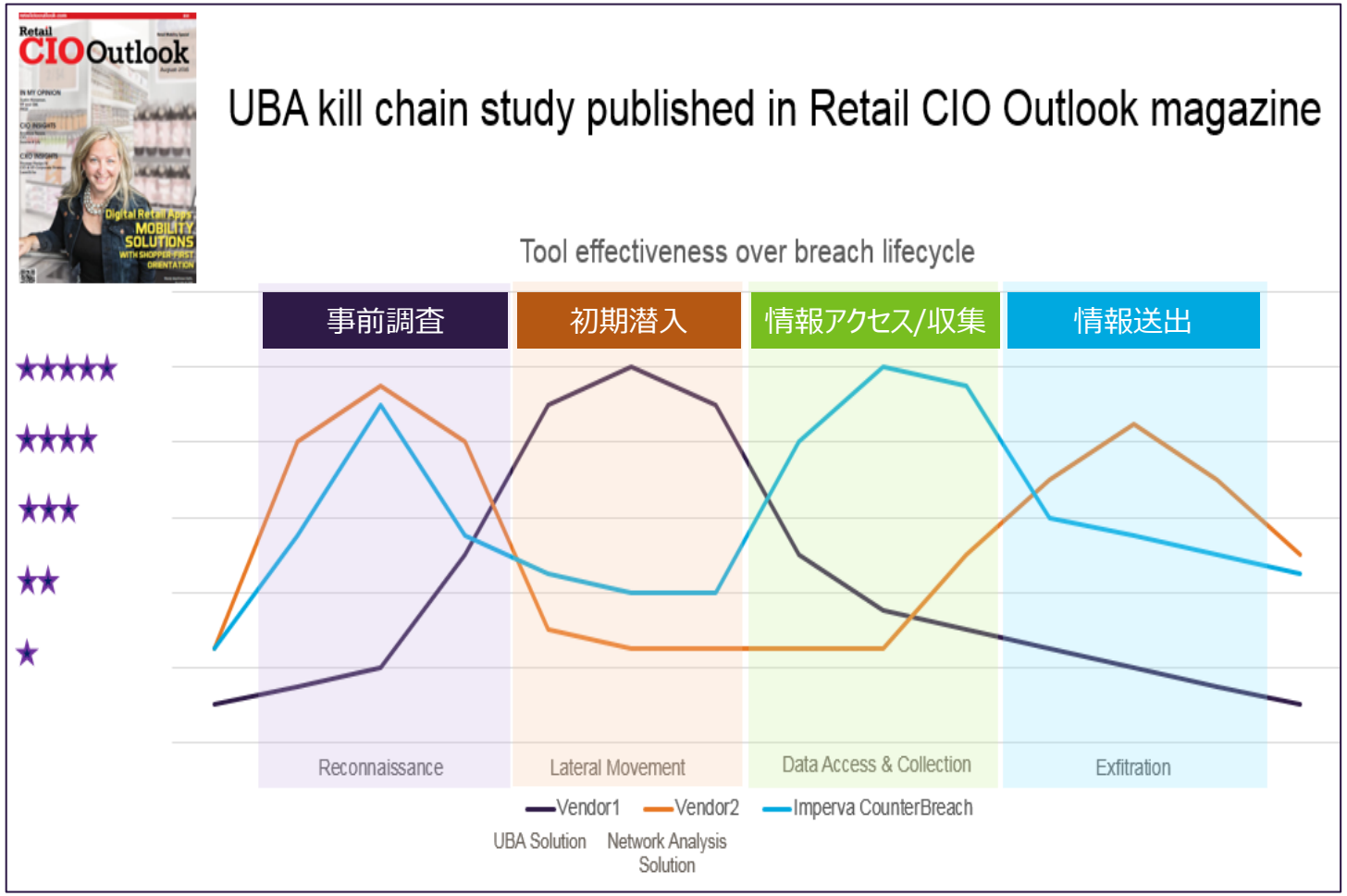
AI/機械学習を活用したセキュリティ分析



IMPERVA®

UBA キル・チェーン・スタディ

どこが重要か？　いつ浸入されたか？　いつデータ侵害されたか？ どのように止めるか？

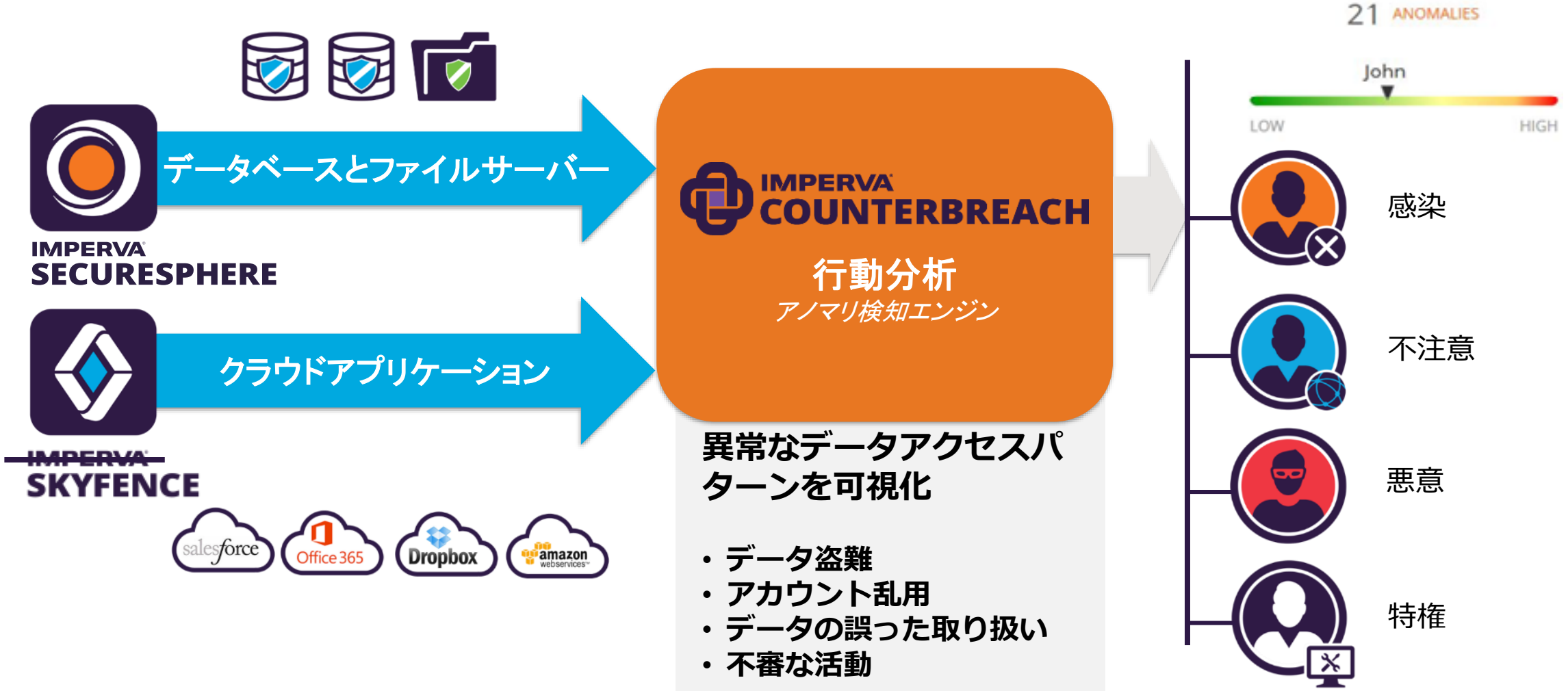


Imperva の強み:

- ✓ **データを中心とした保護**
  - 重要なデータリソースを中心に保護
  - 悪意のある内部ユーザが、重要なデータに容易にアクセスできない
- ✓ **事前調査フェーズ**
  - 疑わしい振る舞いを迅速に検知
- ✓ **データアクセス & 収集フェーズ**
  - 「誰が」「何に」「どのファイルへ」「いつ」「どのように」をリスク分析
  - ブロック/遮断を実行

IMPERVA®

内部からの情報漏えい対策



IMPERVA

本資料について

- 本書に記載されている事柄は、予告なく変更されることがありますので、予めご了承ください。
- 本書は「無保証」で提供され、市場性、特定の目的に対する適合性、または第三者の権利を侵害しないことを含むいかなる明示または暗示保証は一切付与されません。Imperva , Inc. (以下「Imperva」といいます) は、本書に含まれる技術的および編集上の誤りと欠落について、また、本書の内容の実行および使用に起因する直接的、付随的、二次的、その他のあらゆる損害について、Impervaは、そのような損害の可能性について事前に知らされていた場合でも、一切責任を負いません。
- 本書には著作権により保護されている情報が含まれています。内部での配布を除き、Imperva, Inc.の事前の書面による許可なく、本書を、いかなる形式においても複写または複製することを禁じます。
- Imperva製品の限定保証については、各製品の付属文書をご参照ください。Impervaは、Imperva製品のみを保証し、他社製品は一切保証いたしません。
- 本書に記載されているその他のすべての商品名は、該当する各社の商標または登録商標です。

IMPERVA®