HITACHI
Inspire the Next

SaaS Security Posture Managementサービス

AppOmni のご紹介

株式会社日立ソリューションズ

HITACHI
Inspire the Next

Contents

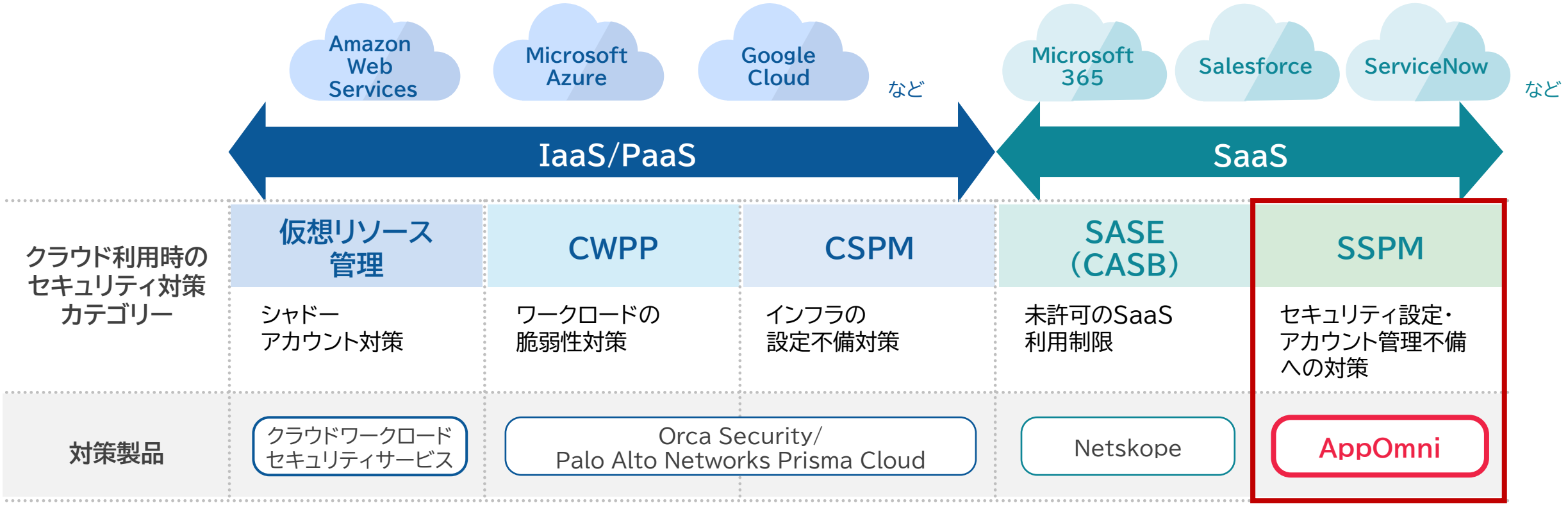
HITACHI
Inspire the Next

Contents

SSPMとは

製品ジャンル SSPM(SaaS Security Posture Management)

クラウドサービス利用時のセキュリティ対策の1つ。Microsoft 365、Salesforceなどの
SaaSで**セキュリティ設定やアカウント管理・権限の不備**がないか**常時監視するもの**



SaaS:Software as a Service, IaaS:Infrastructure as a Service, PaaS:Platform as a Service, CWPP:Cloud Workload Protection Platform, CSPM:Cloud Security Posture Management, SASE:Secure Access Service Edge, CASB:Cloud Access Security Broker

Contents

利用者側の設定不備により情報漏洩が発生しています

HITACHI
Inspire the Next

01	2020年11月	某電機会社 Microsoft 365不正ログイン	▶ 約10,000件の取引先情報・個人情報が流出 ▶ 多要素認証なし。ID窃取のみで侵入
02	2021年1月	某ECサイト、某銀行 Salesforce不正アクセス	▶ 約150万件の企業・個人情報が流出 ▶ 設定ミスでゲストユーザーに情報公開
03	2022年10月	某製造業 GitHub不正アクセス	▶ 開発委託先がシステムのアクセスキーを第三者公開、約30万件の個人情報が流出の可能性 ▶ 設定ミスでゲストユーザーに情報公開
04	2023年1月	某大学 Microsoft Teams情報公開	▶ 個人情報約900人分を含む会議資料や大学院入試問題など300件が設定ミスで公開

サイバー攻撃による損害額は一社当たり平均約15億円

調査・分析の実施主体	対象の地理的範囲	対象年	経済的損失の概要	損失額
Accenture	日本	2018年	サイバー犯罪により生じる1社当たり平均コスト	1,357万ドル 約14億9,867万円
JNSA	日本	2018年	個人情報漏えいにより生じる1件当たり平均損害賠償額	6億3,767万円
トレンドマイクロ	日本	2017年	セキュリティインシデントにより生じる1組織当たり平均年間被害額	2億1,153万円

(出典)総務省「令和元年版 情報通信白書 第3節 3(2)サイバー攻撃等の経済的損失」をもとに作成

なぜ事故が起こったのか

SaaS利用者側のアカウント管理やセキュリティ設定の不備

利用者責任

クラウド事業者責任

1 アカウント・権限設定

2 ユーザーデータ

3 通信路・通信データ

4 アプリケーション

5 ミドルウェア（OS、DBサーバー、Webサーバーなど）

6 仮想インフラ（ネットワーク、ストレージ、VM、コンテナなど）

7 物理インフラ

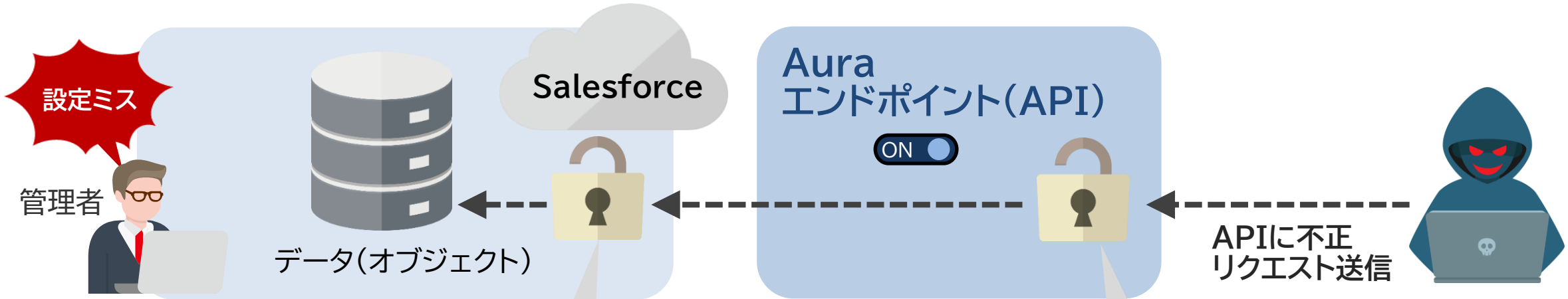
SaaS

参考：CSA（Cloud Security Alliance）によるクラウドサービスのシステム階層

某有名ECサイトの情報漏洩はこうして起こった

HITACHI
Inspire the Next

Salesforce利用時の設定ミスが起因となり、ゲストユーザーがAPI経由でデータ参照可能



問題 1

ゲストユーザーの共有設定が「公開」

問題 2

Lightningのサイト機能を
有効にしたことで
Auraエンドポイント(API)が有効

2つの設定不備の組み合わせで脆弱に

※事件について公開されていない情報もあるため、日立ソリューションズの推測や見解も含みます。

HITACHI
Inspire the Next

Contents

どこが危険か

問題 1　SaaS利用時のセキュリティ設定に不備

- ⚠ パスワードポリシーが弱い
- ⚠ ゲストユーザーへの情報が「公開」設定になっている
- ⚠ ゲストユーザーからのAPI利用が「有効」になっている

問題 2　アカウントの管理がずさん

- ⚠ 退場者のアカウントや、使われていないアカウントを放置
- ⚠ 便宜性を優先し管理者権限・権限昇格権限を持つユーザーが増大
- ⚠ 一時的に他部門のデータへのアクセスを許したつもりがそのまま放置

わかっていても対策を徹底できない・・・

なぜ事故が後を絶たない？

人手での対策維持がほぼ無理だから

理由 1

攻撃ポイントが
雪だるま式に増加

理由 2

SaaSのセキュリティ
監視のノウハウが
ない

理由 3

SaaSごとに
仕様が違う

理由1　攻撃ポイントが雪だるま式に増えている

HITACHI
Inspire the Next

① 利用数増

Microsoft 365
全社利用
（OA・グループウェア）

GitHub
開発・生産管理部門

Workday
人事・財務部門

Slack
サポート業務部門

② 入口増
（インターネット経由での利用増）

ゲスト
ユーザー

委託業者
MSPなど

Salesforce

API

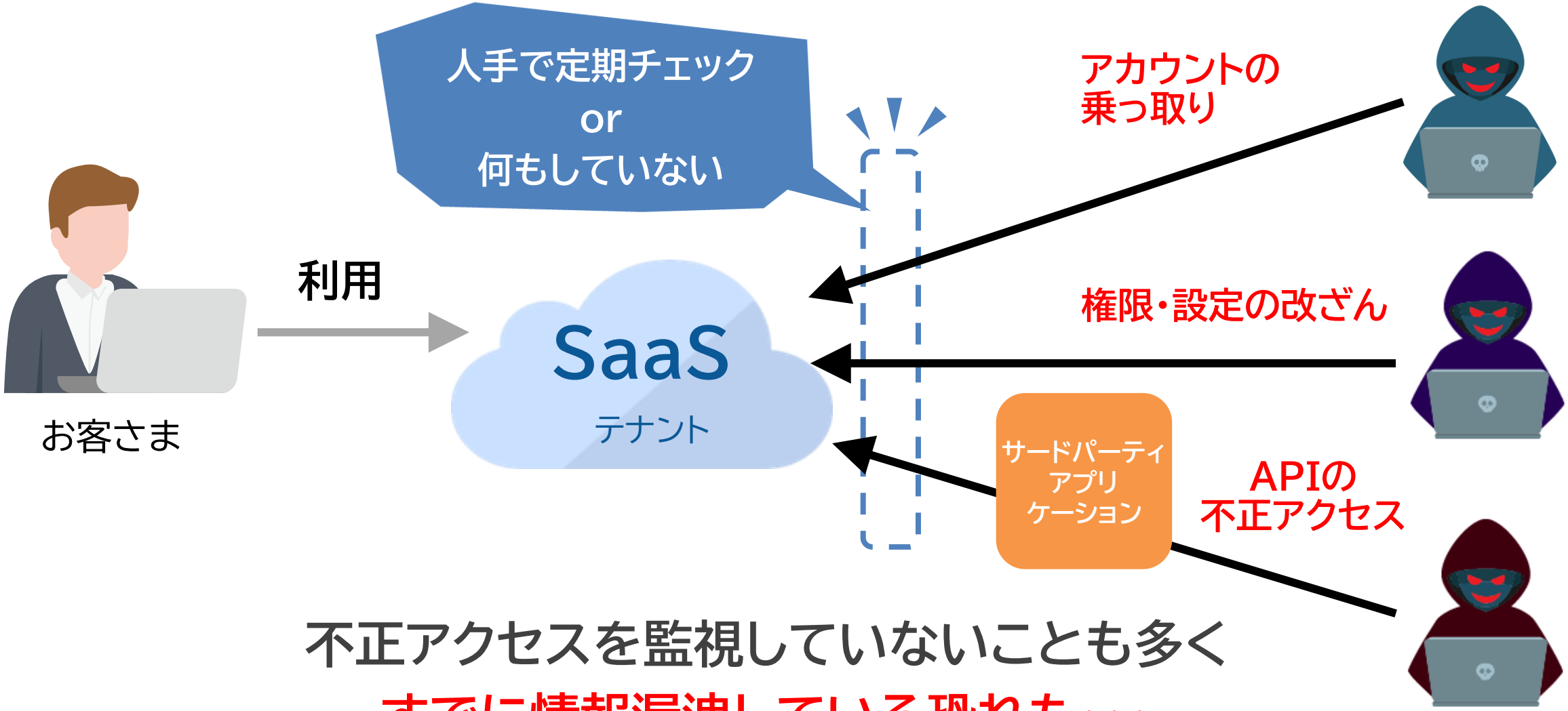
サードパーティ
アプリ
ケーション

③ サプライチェーン増

情報セキュリティ
部門

利用数×入口数×サプライチェーン数＝？？？

理由2　SaaSのセキュリティ監視のノウハウがない



不正アクセスを監視していないことも多く

すでに情報漏洩している恐れも・・・

理由3　SaaSごとに仕様が違う

Microsoft 365
全社利用（OA・グループウェア）

Salesforce
営業部門

Slack
サポート業務部門

SaaS利用がどんどん増えている

個々のSaaSの仕様に詳しくない…

Workday
人事・財務部門

GitHub
開発・生産管理部門

情報セキュリティ部門

各SaaSの仕様把握、仕様変更への追従は困難

なぜ事故が後を絶たない？（再掲）

人手での対策維持がほぼ無理だから

理由 1

攻撃ポイントが
雪だるま式に増加

理由 2

SaaSのセキュリティ
監視のノウハウが
ない

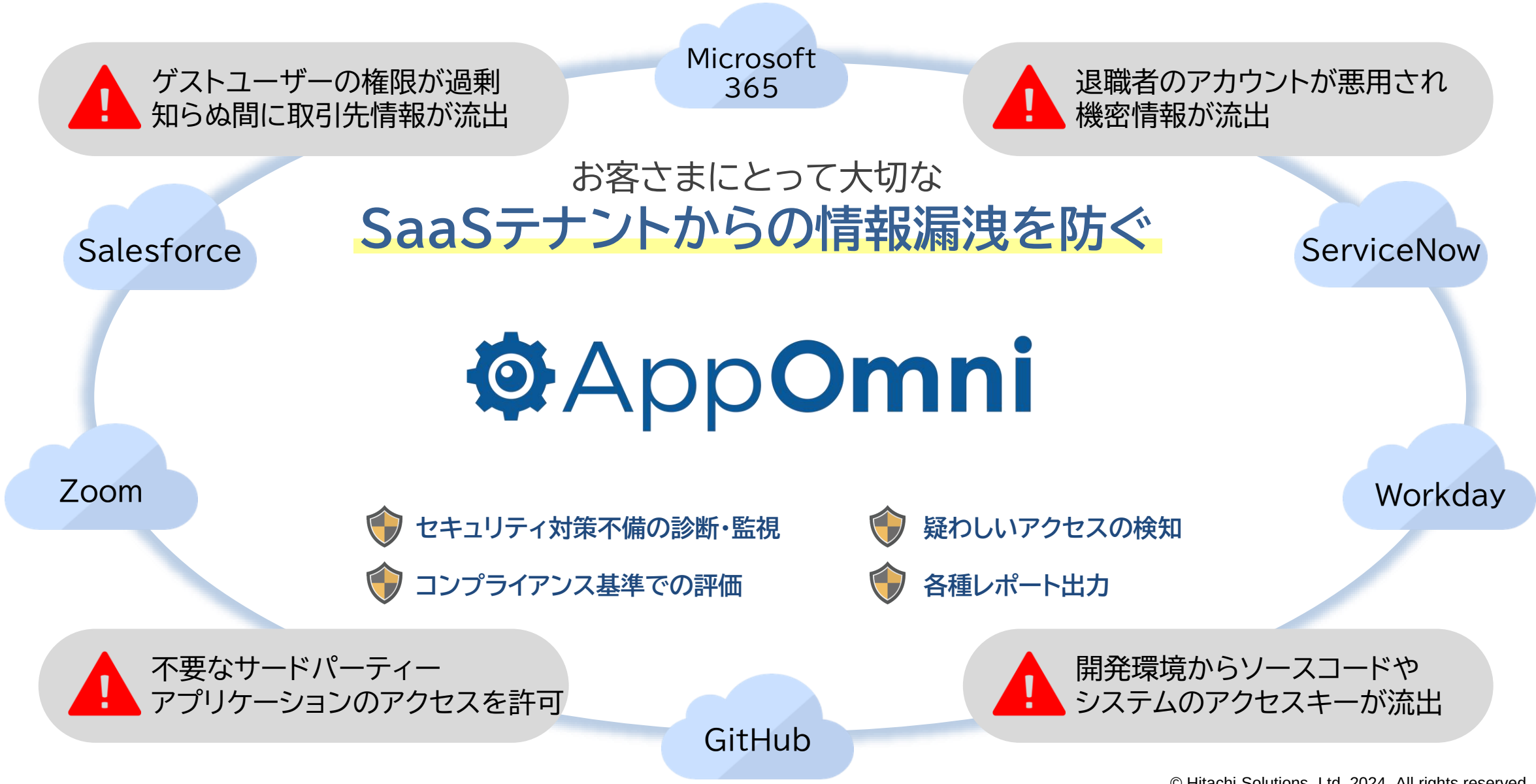
理由 3

SaaSごとに
仕様が違う

HITACHI
Inspire the Next

Contents

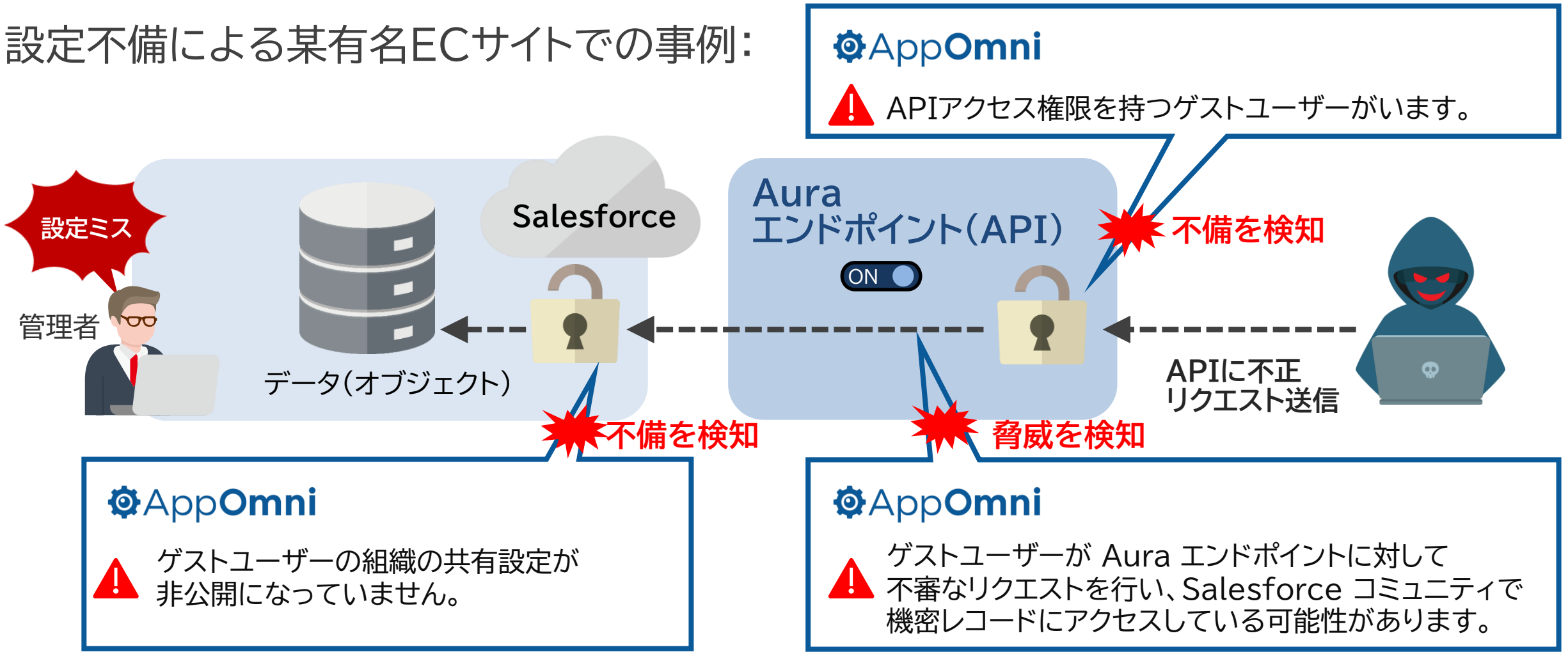
AppOmni(アップオムニ)とは



AppOmniを導入すると・・・

HITACHI
Inspire the Next

設定不備による某有名ECサイトでの事例：



Salesforceで200以上の項目をチェック、27パターンの脅威を検知

※事件について公開されていない情報もあるため、日立ソリューションズの推測や見解も含みます。

何ができるか

HITACHI
Inspire the Next

AppOmni

セキュリティ対策不備の監視
（セキュリティ設定・権限・アカウント管理）

疑わしいアクセスの検知

NIST,ISO,SOC2など
コンプライアンス基準での安全性評価

ポリシーのカスタマイズ

監査に便利な各種レポート

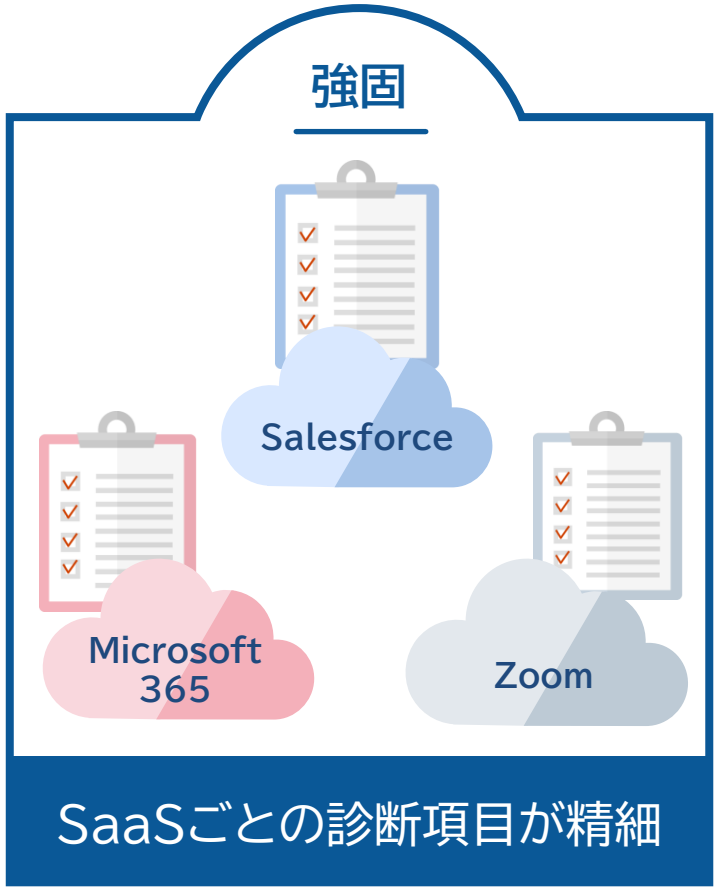
独自SaaSの監視
（開発プラットフォーム）

NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

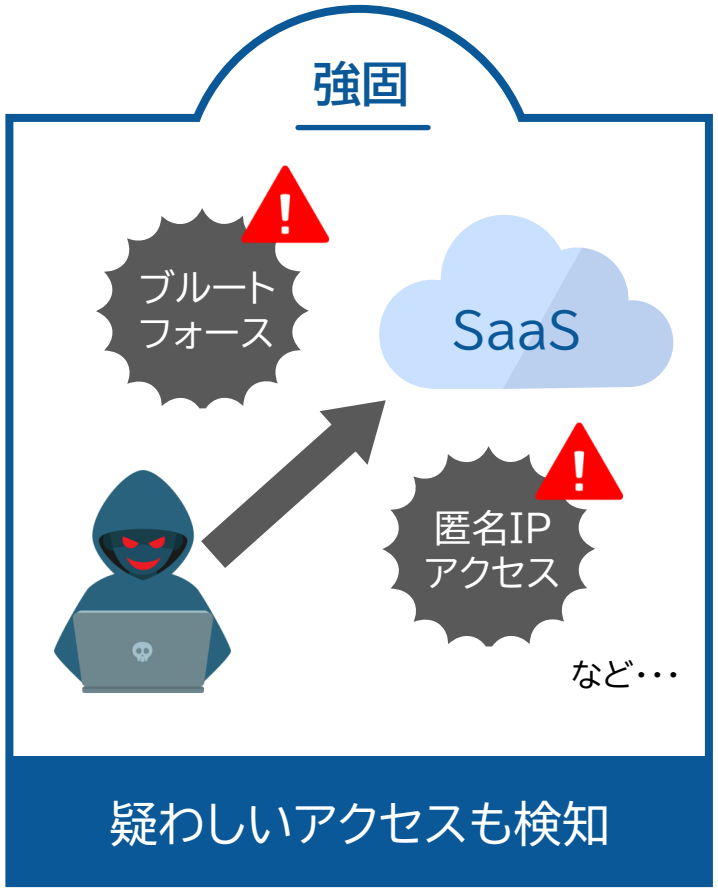
AppOmniの強み

HITACHI
Inspire the Next

強固かつ運用が楽



SaaSごとの診断項目が精細



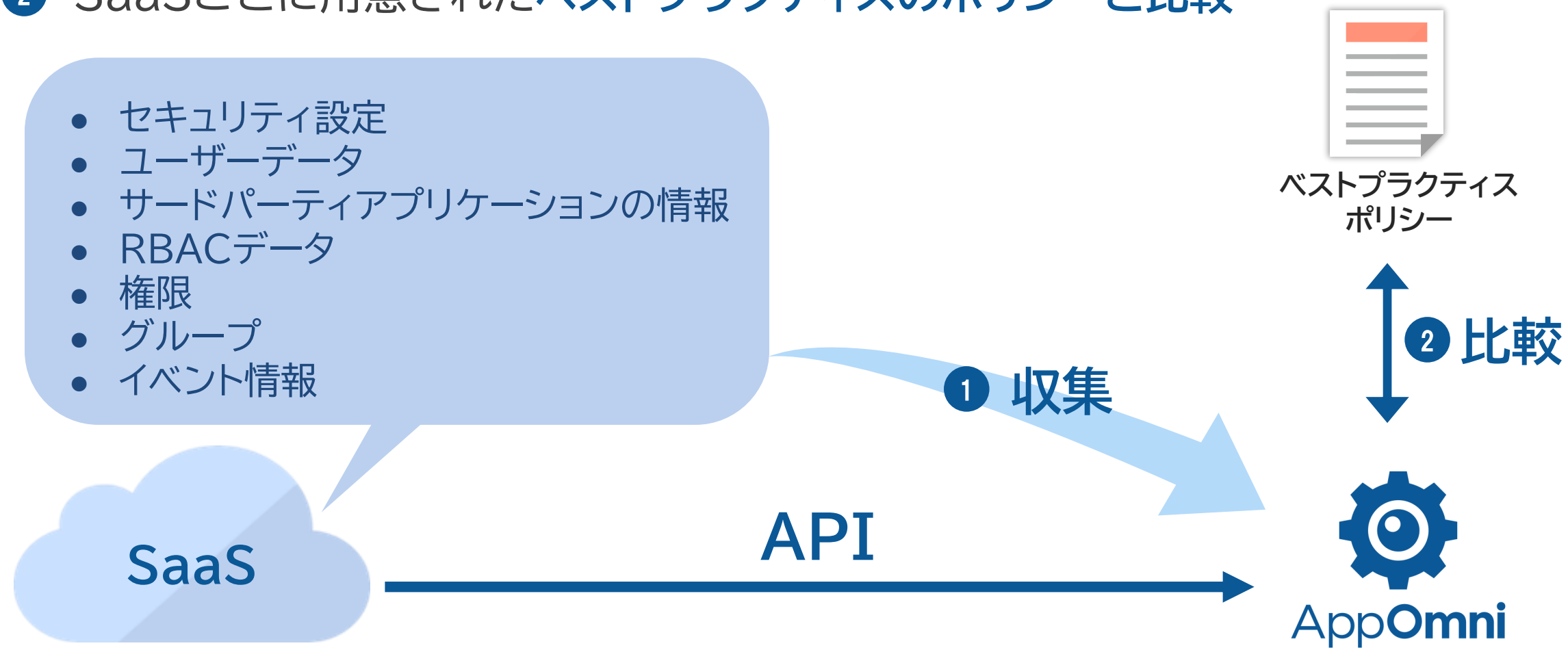
疑わしいアクセスも検知

SaaS仕様変更にも自動追従
AppOmni Insights

どんな仕組み？

HITACHI
Inspire the Next

1. SaaSの**APIからデータを収集**
2. SaaSごとに用意された**ベストプラクティスのポリシーと比較**



RBAC：Role-Based Access Control

導入も簡単

監視対象SaaSと**OAuthで接続**

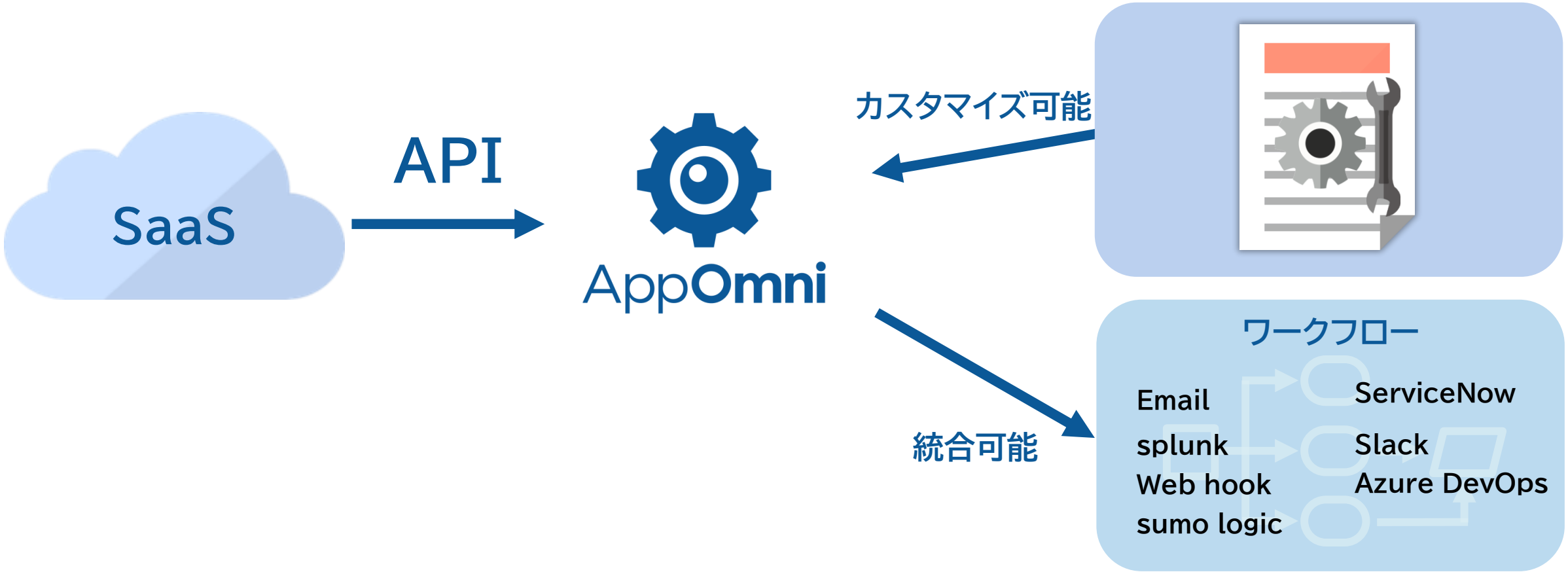
監視対象SaaSでAppOmniからの**API経由でのデータ参照を許可**

SaaS 1テナントあたり30分～1時間程度*の設定作業で完了！

＊ SaaSの種類により異なります。

監視ポリシーのカスタイズも可能

- お客さまがルールを追加・削除しポリシーをカスタマイズ可能
- アラートをメール送信したり各種ワークフローに統合可能



HITACHI
Inspire the Next

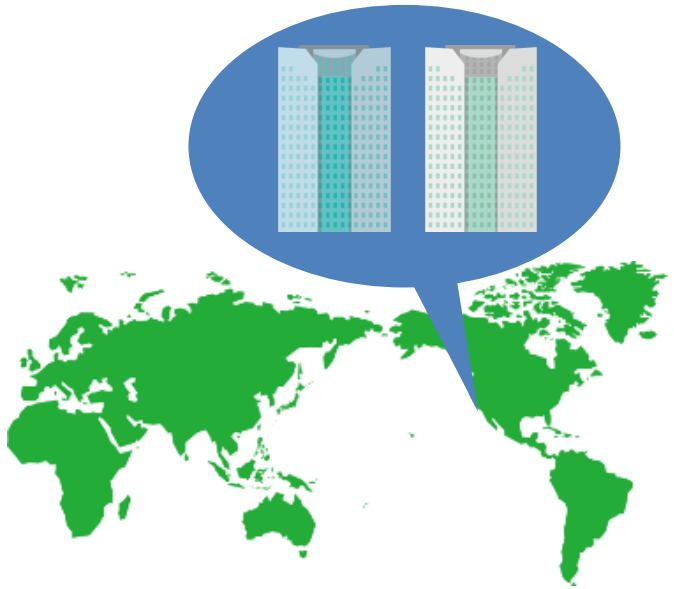
Contents

導入実績(2024年5月時点)

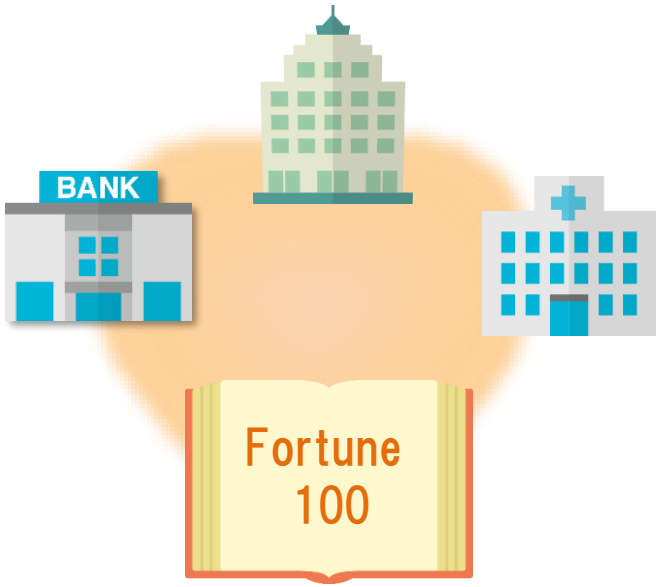
HITACHI
Inspire the Next

グローバルで1億人以上のSaaSユーザーを保護

Silicon Valleyの
3大テック企業のうちの2社



Fortune100の
銀行、保険、ヘルスケア企業



主要セキュリティ・
プロバイダーの数社

AppOmni社について

HITACHI
Inspire the Next

Salesforce, ServiceNowなどが資本提携

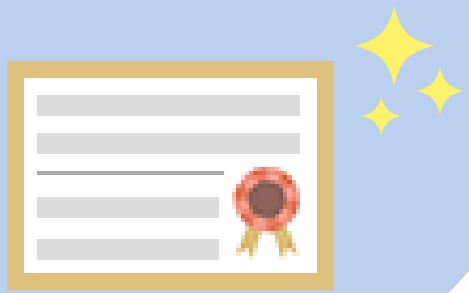
ベンダー名	**AppOmni, Inc.**
本拠地	USA　San Francisco
シリーズ 調達	Series C $123M
設立	2018年
投資会社	Scale Venture Partners Salesforce Ventures ServiceNow Ventures　etc.
創立者経歴	Brendan O ‘Connor氏 20年以上のセキュリティ業界経験を持ち、AppOmni創設前はServiceNowのCTOを務めた。 ServiceNow以前はSalesforceにてVP Product Security、グローバルのCSO（最高戦略責任者）を歴任

日立ソリューションズがご提供するもの

HITACHI
Inspire the Next

01

AppOmni(SaaSサービス)利用ライセンス



02

日本語保守サポート

(※AppOmni利用ライセンスに含みます)

03

導入支援

(※AppOmni利用ライセンスとは別に費用がかかります)

日本語保守サポート(AppOmniサービス費用に含む)

サポート内容

（1） 一般の問い合わせ

- 対象サービスの機能、使用方法などに関する事項

※ただし対象サービスが検出するセキュリティ警告に対する対策支援は保守サポートサービスには含みません。

- 対象サービスのセットアップ、オペレーションなどの操作方法に関する事項

（2） 障害に関する問い合わせ

- 対象サービスの障害に関する事項

対応時間

月曜日～金曜日(祝日、当社の非営業日を除く)9:00～17:00
対応時間外の問い合わせに関しては、当社の翌営業日での対応となります。

受付窓口

「日立ソリューションズ サポート・お問い合わせ」での受付になります。
URL：https://cs.hitachi-solutions.co.jp/

AppOmniのPoCについて

HITACHI
Inspire the Next

無償でPoCが実施できます！

2週間
まで

PoCの条件

1. AppOmni社とお客さま間でNDA契約が必要
2. PoC実施前に次の点をご提示いただく必要があります
   - ✓ PoCの目的
   - ✓ 採用・不採用の判定基準
   - ✓ 評価観点
3. PoC後の結果をフィードバックしていただくこと

PoC実施時はリモート会議で設定作業をご支援できます。

AppOmni

HITACHI
Inspire the Next

Appendix

対応SaaS

HITACHI
Inspire the Next

30種類以上のSaaSを一元管理(2024年5月時点)

拡大中

- Auth0
- Box
- Cisco Secure Access by Duo
- Confluence
- CrowdStrike
- Fastly
- GitHub
- GitLab
- Google Workspace
- HubSpot
- Jamf
- Jira Software
- JumpCloud
- Lucid
- Microsoft 365
- Microsoft Defender
- Microsoft Entra ID
- Microsoft Exchange Online
- Microsoft Intune
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- monday.com
- NetSuite
- Okta
- Ping Identity
- Salesforce
- SendGrid
- ServiceNow
- Slack
- Smartsheet
- Snowflake
- Tableau
- Veeva Vault
- Wizcloud
- Workday
- Zendesk
- Zoom

AppOmni

お問い合わせ

HITACHI
Inspire the Next

製品に関するお問い合わせ

WEBによる受付

https://www.hitachi-solutions.co.jp/inquiry/products/form/?id=appomni

メールによる受付

hs-appomni-sales@mla.hitachi-solutions.com

製品サイト

https://www.hitachi-solutions.co.jp/appomni/

※本資料中の会社名、商品名は各社の商標または登録商標です。
※本文中および図中では、TMマーク、®マークは表記しておりません。
※製品の仕様は、改良のため、予告なく変更する場合があります。
※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、上記お問い合わせ先までお問い合わせください。

HITACHI
Inspire the Next

END

SaaS Security Posture Managementサービス
AppOmni のご紹介

HITACHI

Inspire the Next