誰もが安全にクラウドサービスを活用するために

セキュリティ評価プラットフォーム「Assured」
脆弱性管理クラウド「yamory」のご紹介

2024/10/10

株式会社アシュアード　植木 雄哉

yamory ASSURED

自己紹介(植木 雄哉)

繋がりましょう！

@ueki62

CISSP

CCSP

PMP

経歴

- 国内大手SIerにて、公共・金融・法人の各業界向けにOAインフラ・セキュリティ領域のコンサルティングや開発支援を実施。
- 外資系総合コンサルティングファームにManagerとして参画し、セキュリティコンサルティング案件に従事。
- 現在はアシュアードにて、ドメインエキスパートとして、コンサルティング、クラウドサービスリスク評価、情報発信を担当。

参加歴

2024

会社概要（当社サービスについて）

セキュリティ評価プラットフォーム

ASSURED

SaaSにおける
セキュリティリスク評価

脆弱性管理クラウド

yamory

オンプレミス／IaaSにおける
構成管理と脆弱性管理

SaaSにおけるセキュリティリスクと

セキュリティ評価プラットフォーム

「Assured(アシュアード)」

民間企業におけるクラウドサービスの利用実態

クラウドサービスを利用している企業割合

77.5%

（出典）総務省「令和5年 通信利用動向調査報告書（企業編）」

2024年国内クラウド市場規模予測

3兆円

（出典）総務書「情報通信白書令和5年版」
（出典）IDC「国内パブリッククラウドサービス市場予測を発表」（2022年9月15日）

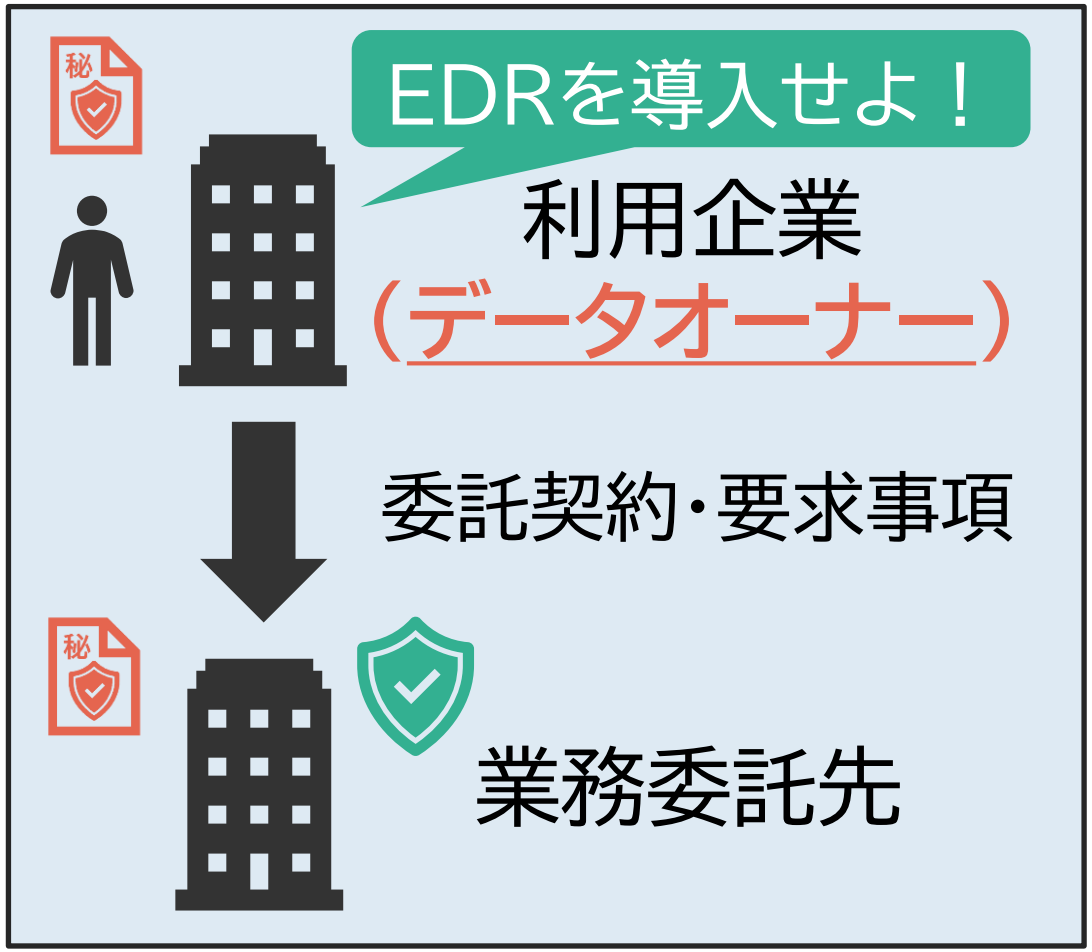
クラウドサービスの有効性を感じる企業

87.9%

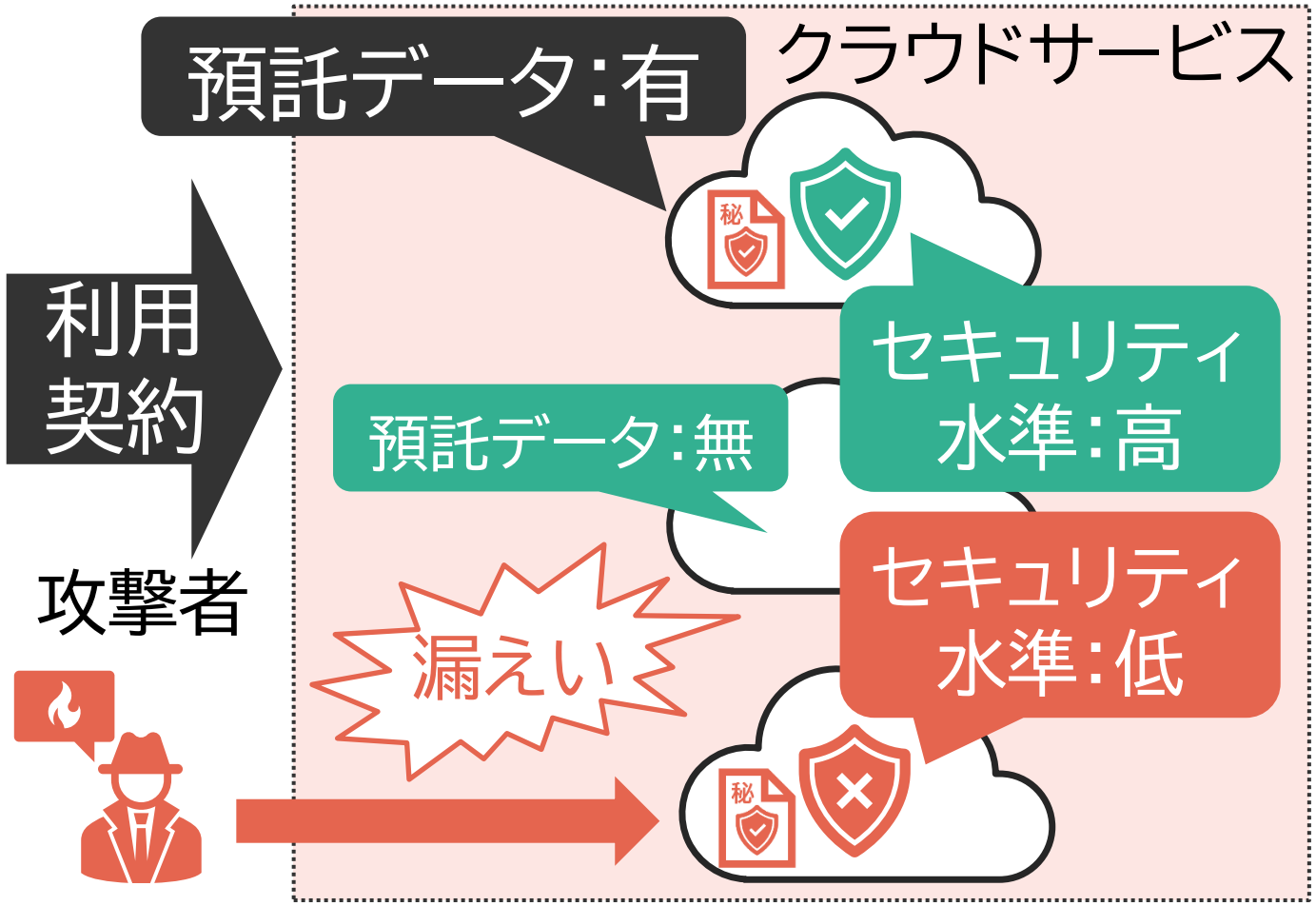
（出典）総務省「令和5年 通信利用動向調査報告書（企業編）」

クラウドサービスも自社ITサプライチェーンの一つ

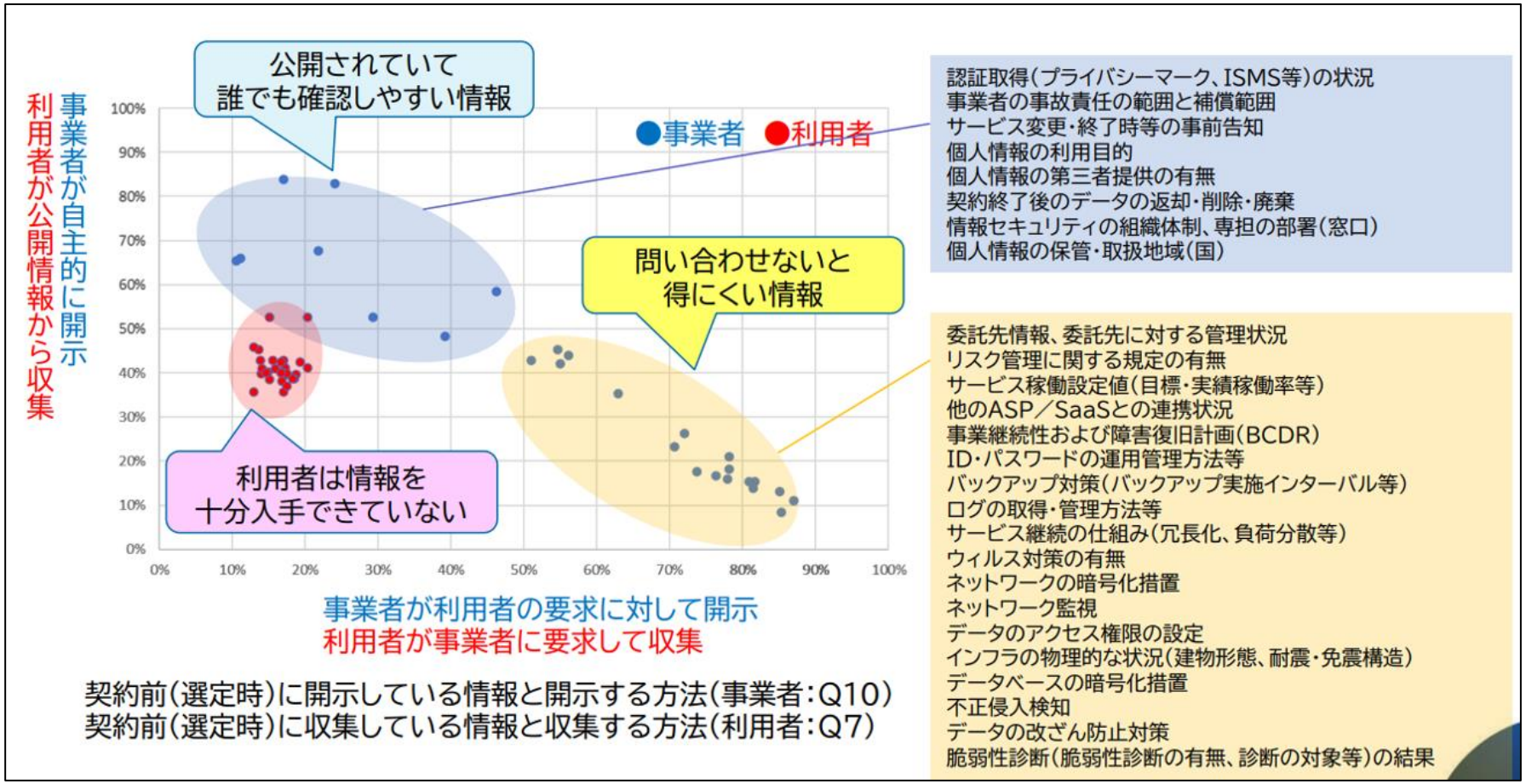
ガバナンスを効かせやすい関係



ガバナンスを効かせづらい関係



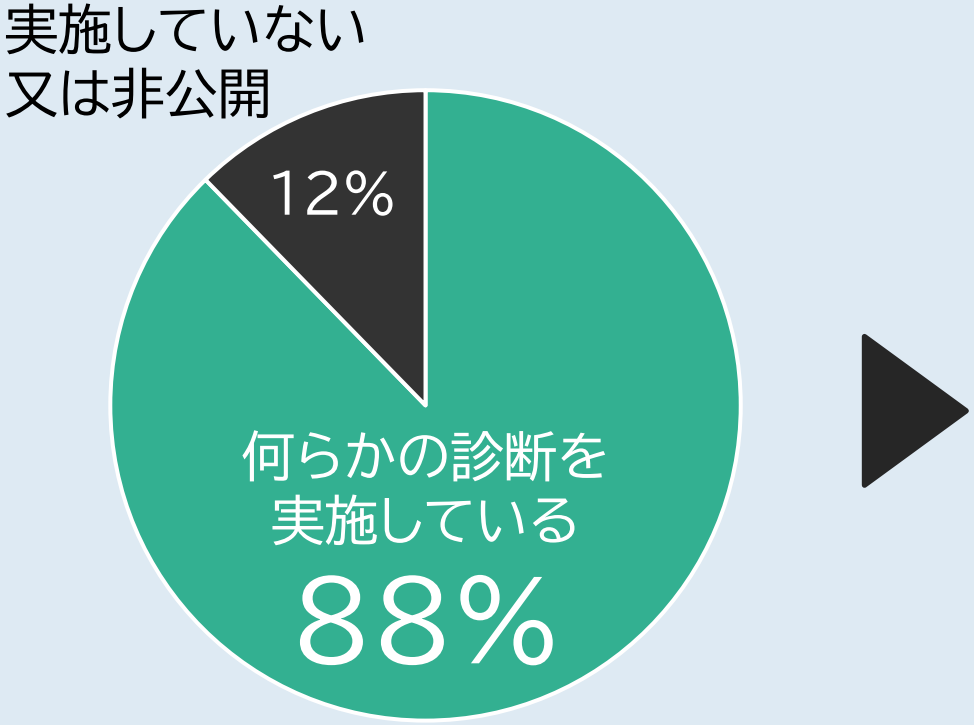
セキュリティ関連情報は「問い合わせないと得にくい」

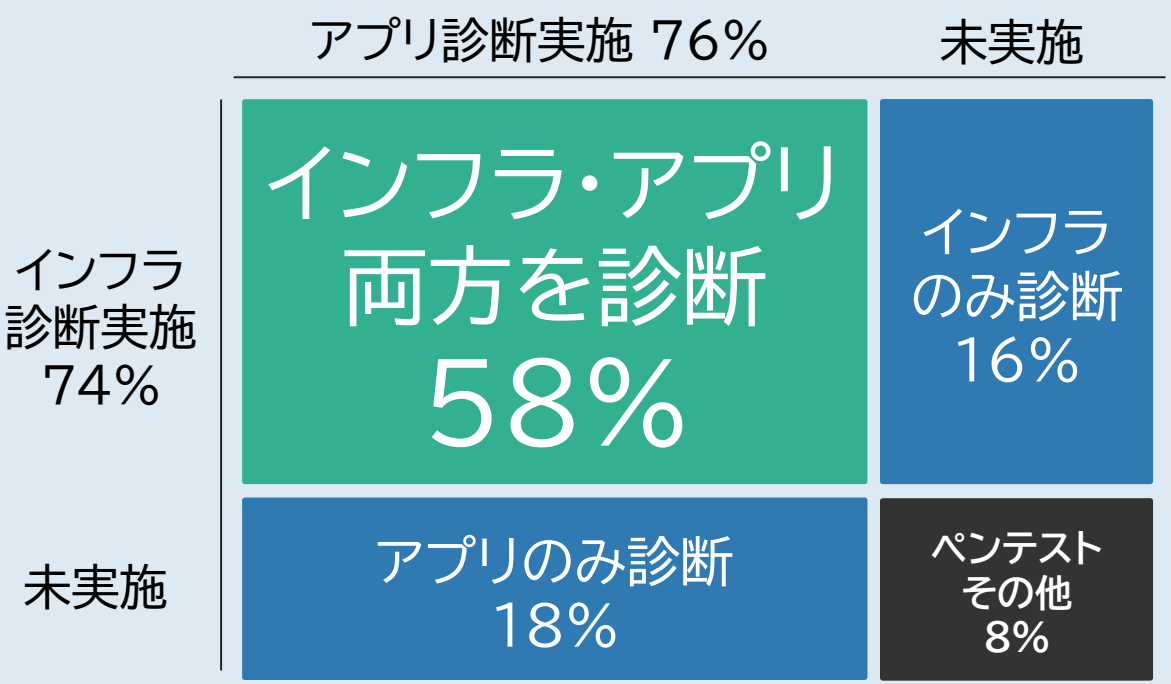


出典:IPA「2022年度クラウドサービス(SaaS)のサプライチェーンリスクマネジメント実態調査概要説明資料」

【調査結果①】脆弱性診断・ペネトレーションテスト

設問　脆弱性診断やペネトレーションテストを実施していますか

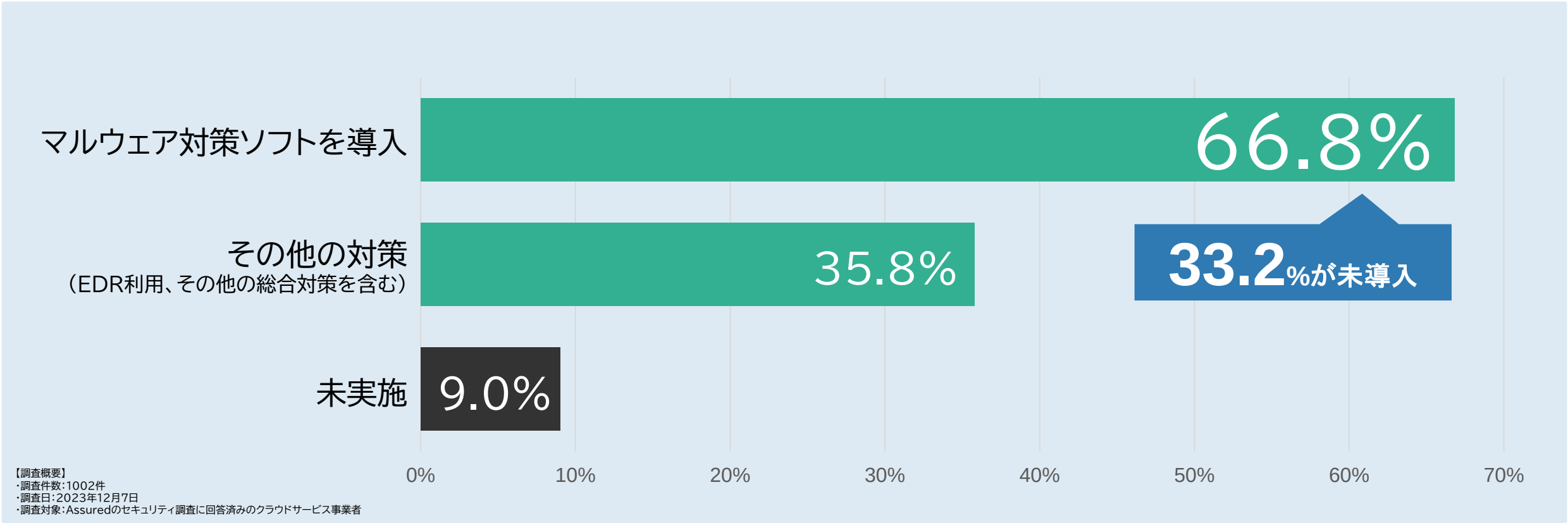




【調査概要】
・調査件数:1179件
・調査日:2024年7月23日
・調査対象:Assuredのセキュリティ調査に回答済みのクラウドサービス事業者

【調査結果②】サーバにおけるマルウェア対策状況

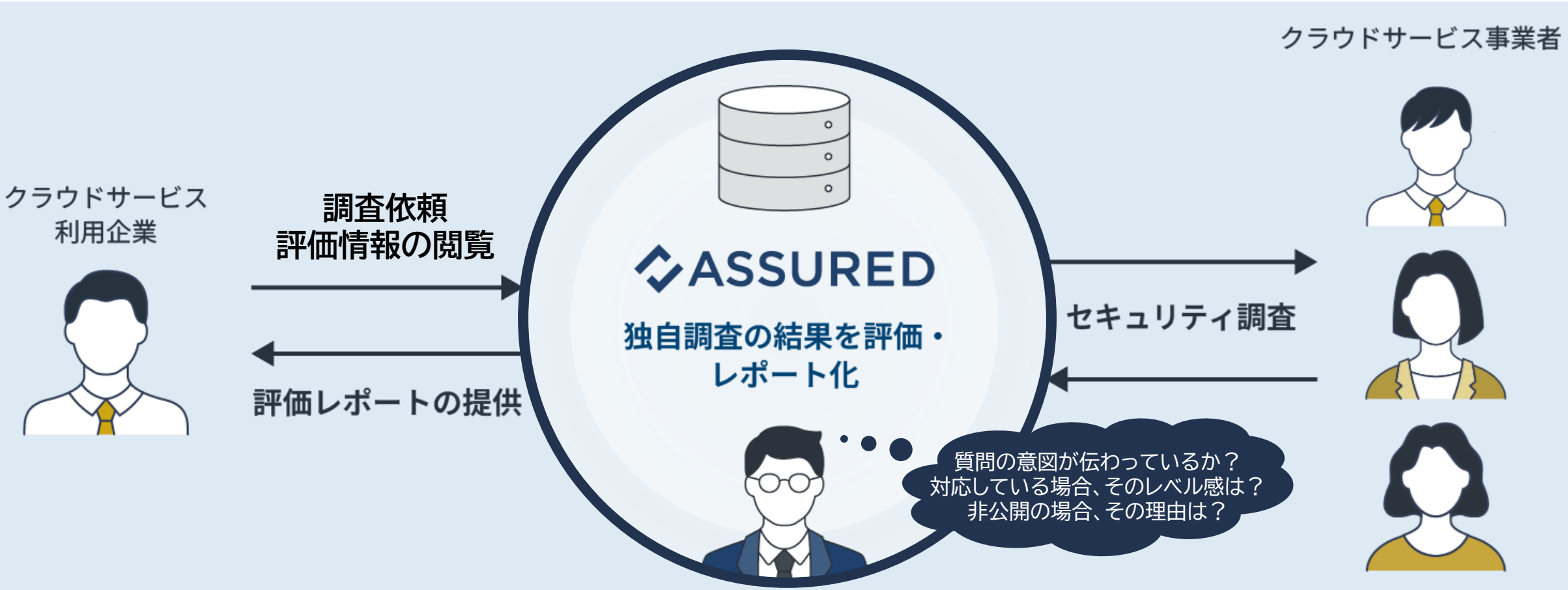
設問　本番サーバに対してマルウェア対策を実施していますか



【調査概要】
・調査件数：1002件
・調査日：2023年12月7日
・調査対象：Assuredのセキュリティ調査に回答済みのクラウドサービス事業者

株式会社アシュアード | yamory ASSURED

セキュリティ評価プラットフォーム「Assured」



当社調査員

（CISAやCISSPなどの、セキュリティの専門資格有する専門家）

調査依頼に対してセキュリティ評価レポートを提供

クラウドサービスの調査依頼

▲サービス検索画面

サービスを選択

スコア＋評価レポートを提供

評価コメント（懸念点等）

設問回答（120項目）

▲調査結果レポート

レポートの特徴

1. 利用の目安となる総合点数・所感
2. リスク項目を抽出
3. 具体的な想定リスクの解説

導入実績（500社以上）

ほか多数

※2024年7月時点の契約状況を元に掲載しております

オンプレミス／IaaS環境における

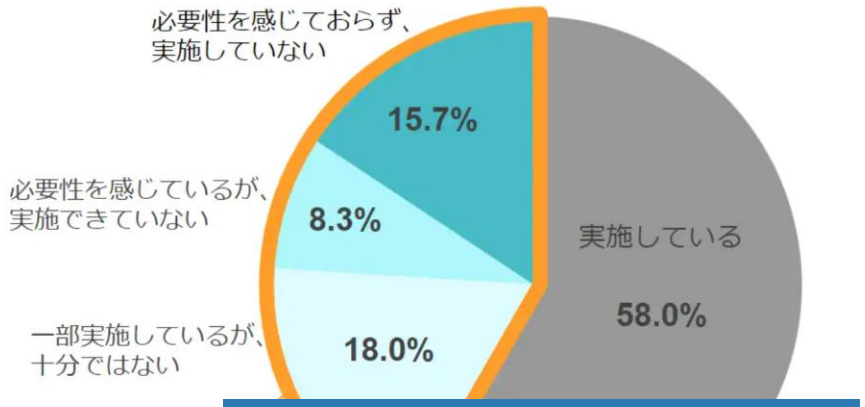
構成管理（SBOM含む）と脆弱性管理

脆弱性管理クラウド
「yamory」

脆弱性管理における各企業の対応状況

サイバー攻撃が激化する中で必須となる「脆弱性管理」
しかし、全ての企業が十分な対策や人員確保をできているわけではない…

脆弱性対策の実施状況

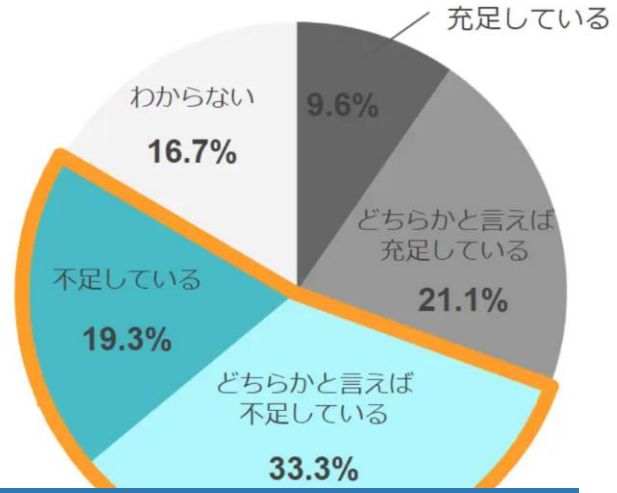


不十分・未対策：
42%

（N=300）

yamory

脆弱性対策に従事する人員



不足：52.6%

（N=228）

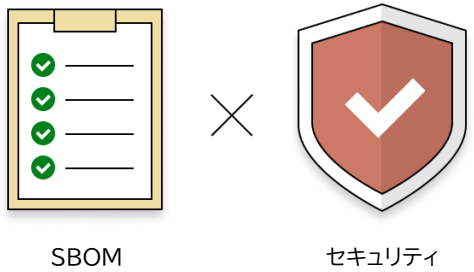
yamory

株式会社アシュアード | yamory ASSURED

脆弱性管理クラウド「yamory」

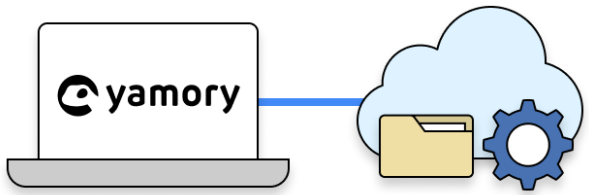
オンプレミス／IaaS環境におけるの構成管理・脆弱性管理とSBOM対応をオールインワンで実現

脆弱性をリアルタイム検出



SBOMを活用した資産管理と
脆弱性の一元管理が可能

クラウドを一括スキャン

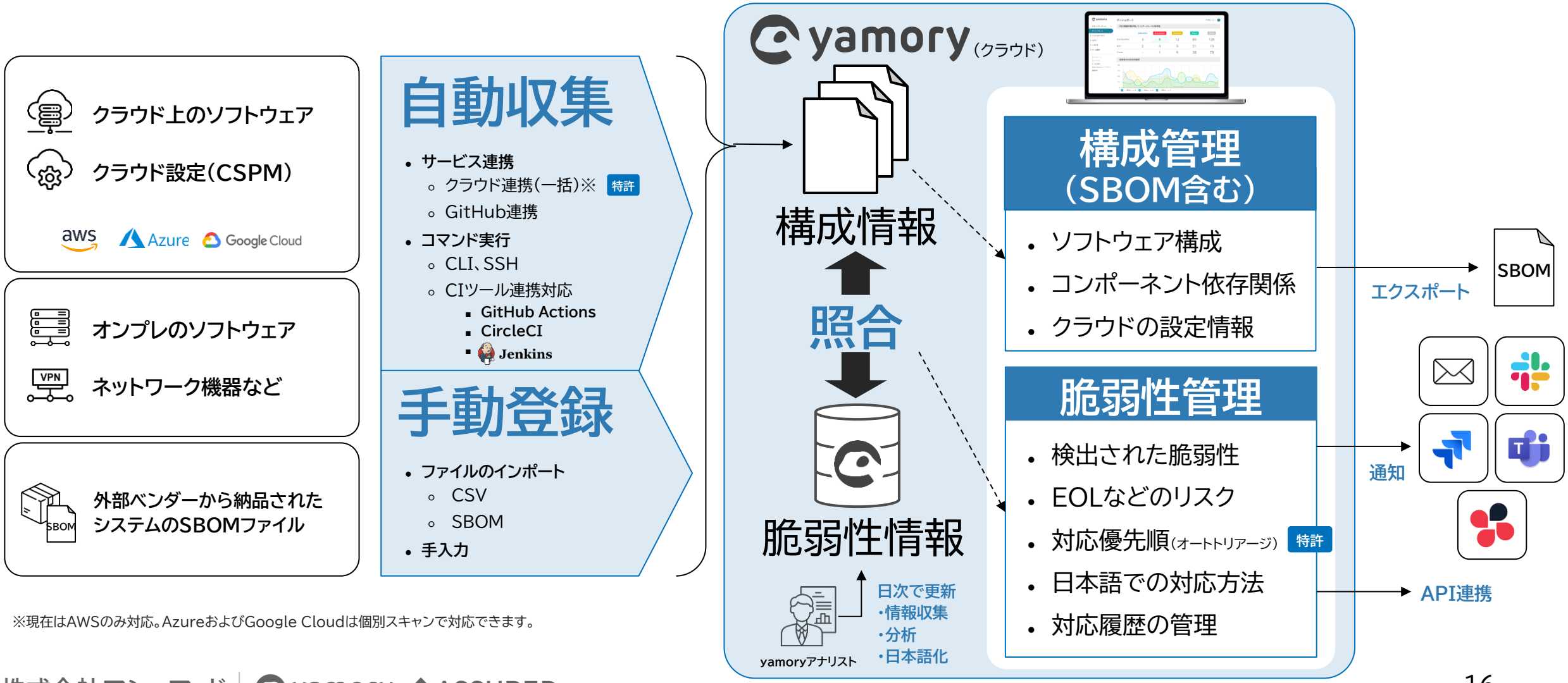


クラウドアカウントと連携するだけで
ソフトウェア構成と設定情報を取り込み

国産唯一経産省手引に記載

安心の国産脆弱性管理ツールで
スムーズな導入を実現

yamoryの仕組み



※現在はAWSのみ対応。AzureおよびGoogle Cloudは個別スキャンで対応できます。

yamoryの対応範囲と提供価値

幅広いレイヤに対応

多角的にリスクを検知

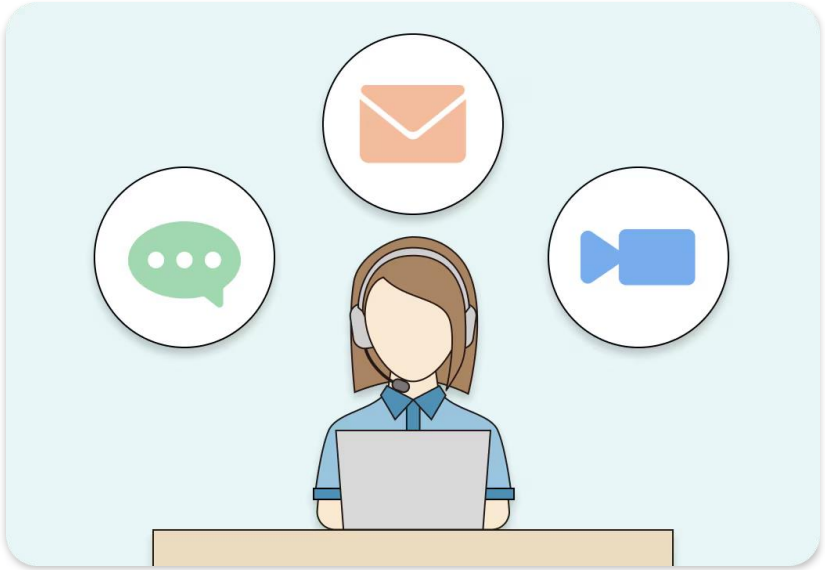
- 脆弱性
- EOL
- OSSライセンス
- CSPM
- SBOM管理

組織的な脆弱性管理の支援

- オートトリアージ
- チーム機能
- 対応管理

安心の国産ツール

日本語表記の使いやすいシステムでスムーズな導入・運用が可能



国産サービスならではの手厚いサポート体制
テクニカルサポート、オンボーディング支援体制も構築

株式会社アシュアード | yamory ASSURED

特許

オートトリアージ

「客観的根拠」と「攻撃観測リスト」から対応優先順位を自動判定
セキュリティの専門家が不在でも効率良く脆弱性対応が可能に

オートトリアージ × CISA KEV Catalog

トリアージ結果 / 対応例		None 現時点では対処しない	Minor 定期メンテナンスで対処	Delayed 2週間以内に対処	Immediate 日次で対処
危険性	脆弱性スコアの高さ		×	×	×
	└ 共通脆弱性評価システムCVSSのスコアがCriticalもしくはHighである脆弱性か（情報漏洩や機能停止に直結する脆弱性）				
影響度	外部からのアクセス可否			×	×
	└ 脆弱性を有するシステムが外部（Internet）からアクセス可能であり攻撃が可能な状態にあるか　※手動にて設定				
攻撃手段	攻撃コード流通の有無				×
	└ 検出された脆弱性に関連する攻撃コード（PoC）が流通しているか（流通している攻撃コードを用いた攻撃が容易に可能）				

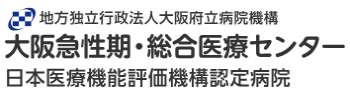
CISA（アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁）が2021年に公開した、**「実際に攻撃者が積極的に悪用していることが確認されており、対応が急がれる脆弱性」**の一覧

攻撃事例

KEVに登録される条件（抜粋）

- **CVE番号が割り振られている**
- **実際に攻撃が観測されている／悪用されている**
- **明確な是正ガイダンスが公開されている**

導入実績



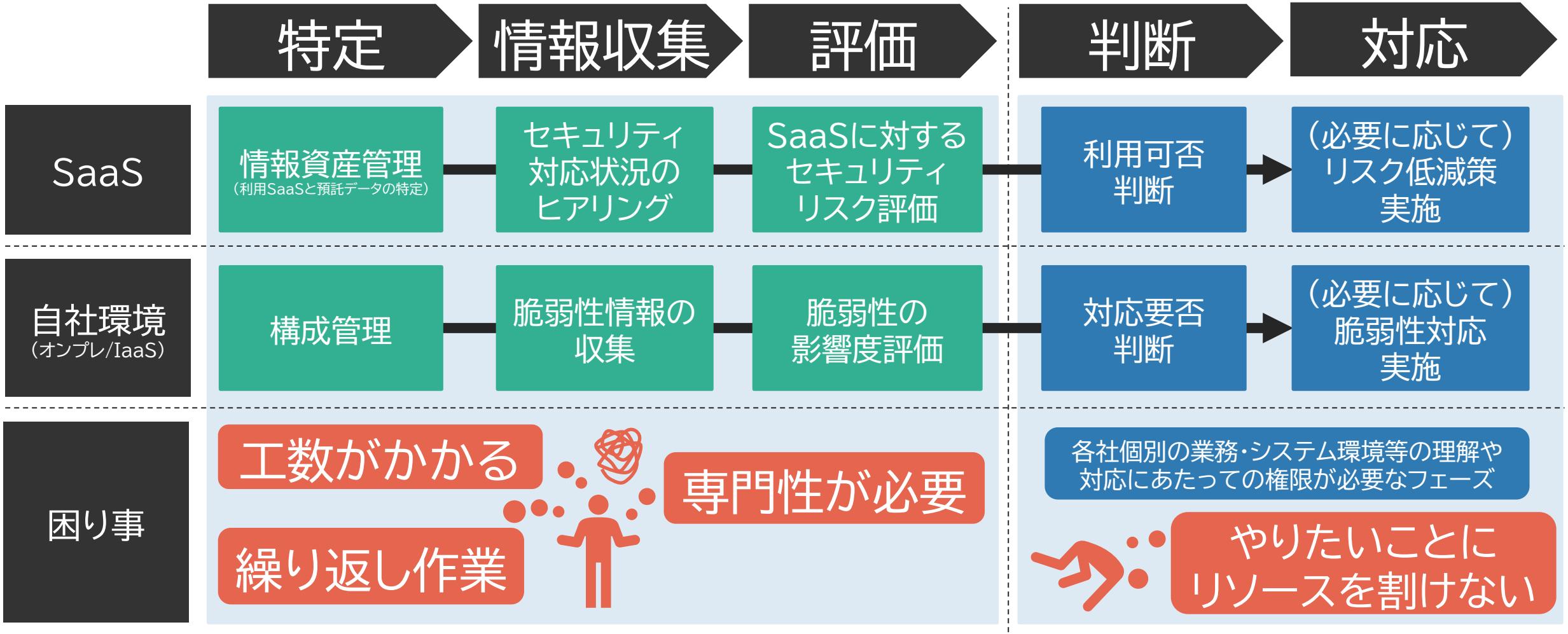
株式会社アシュアード | yamory ASSURED

一部抜粋／2024年7月現在

アシュアード社として

実現したい世界観

誰もが安全にクラウドサービスを活用するために



誰もが安全にクラウドサービスを活用するために

特定 → 情報収集 → 評価 → 判断 → 対応

SaaS

自社環境
（オンプレ/IaaS）

困り事

ASSURED

一丁目一番地となる重要領域

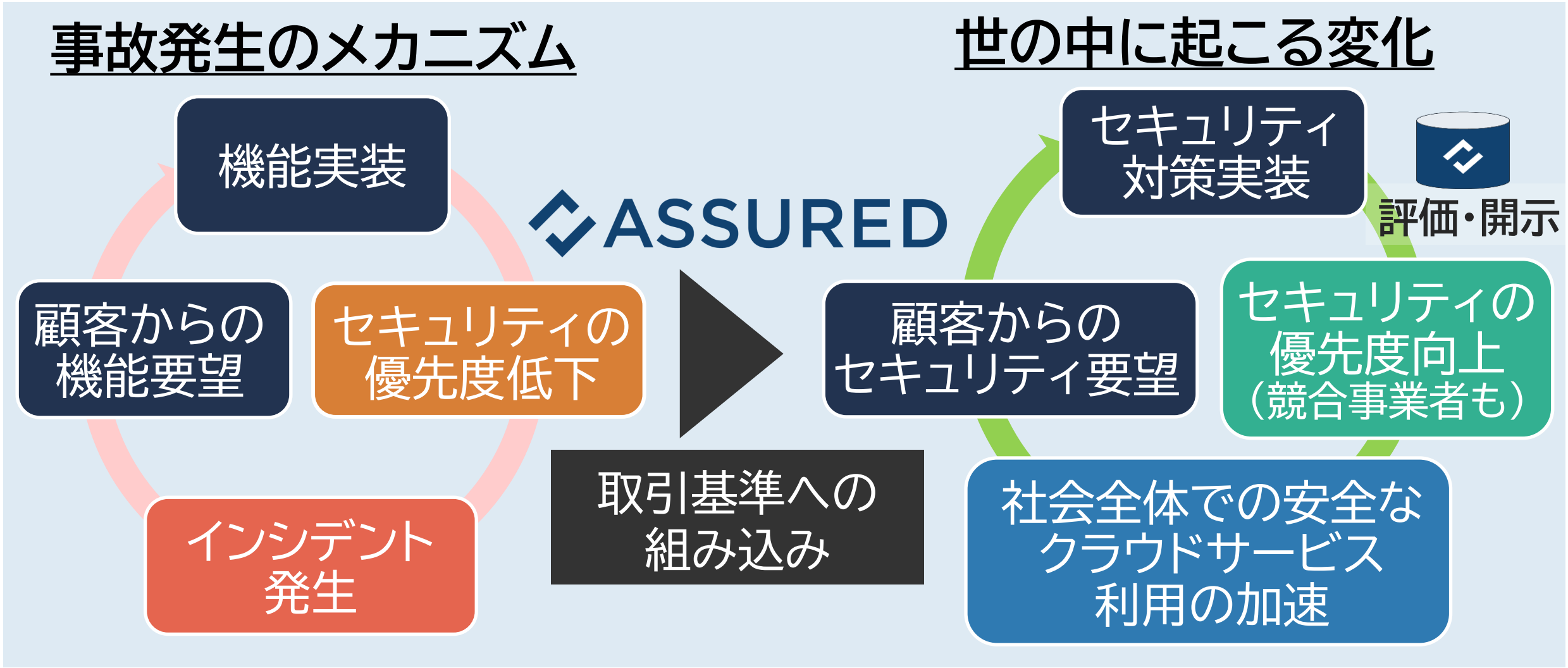
yamory

「誰もが」第三者の専門家による
「品質向上」と「効率化」の
両立を可能に！

各企業様でしか
対応できない領域

注力領域への
リソース集中

誰もが安全にクラウドサービスを活用するために



https://www.brighttalk.com/webcast/14253/626440?utm_source=ISC2AsiaPacific&utm_medium=brighttalk&utm_campaign=626440

【ご案内】Webinar／オフライン勉強会

情報発信 @ueki62

ISC2 無料ウェビナー

10/29(火)15:00～16:00

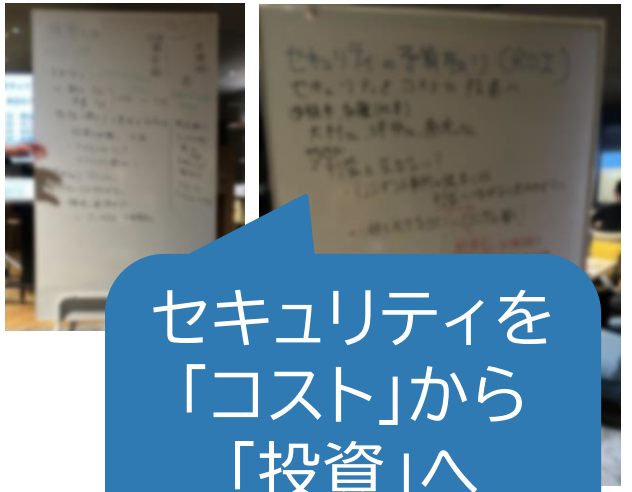
申込URL

https://www.brighttalk.com/webcast/14253/626440?utm source=ISC2AsiaPacific&utm medium=brighttalk&utm campaign=626440

ISC2 Webinar

セミナー ＋ 車座(お酒飲みながら)

セキュリティ勉強会 in 渋谷



セキュリティを「コスト」から「投資」へ変えるには？

自社セミナー

録画配信

申込URL

https://assured.jp/seminar/240910 archive?utm source=yuzawa&utm medium=website&utm campaign=event&utm content=20241009

株式会社アシュアード | yamory ASSURED

当社ホームページより各社様の導入事例公開中です！
お気軽にお問い合わせください！

EoF