

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](#)



## 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

CISSP

CCSP



# 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(アシユアード)」

# 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)総務省「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)

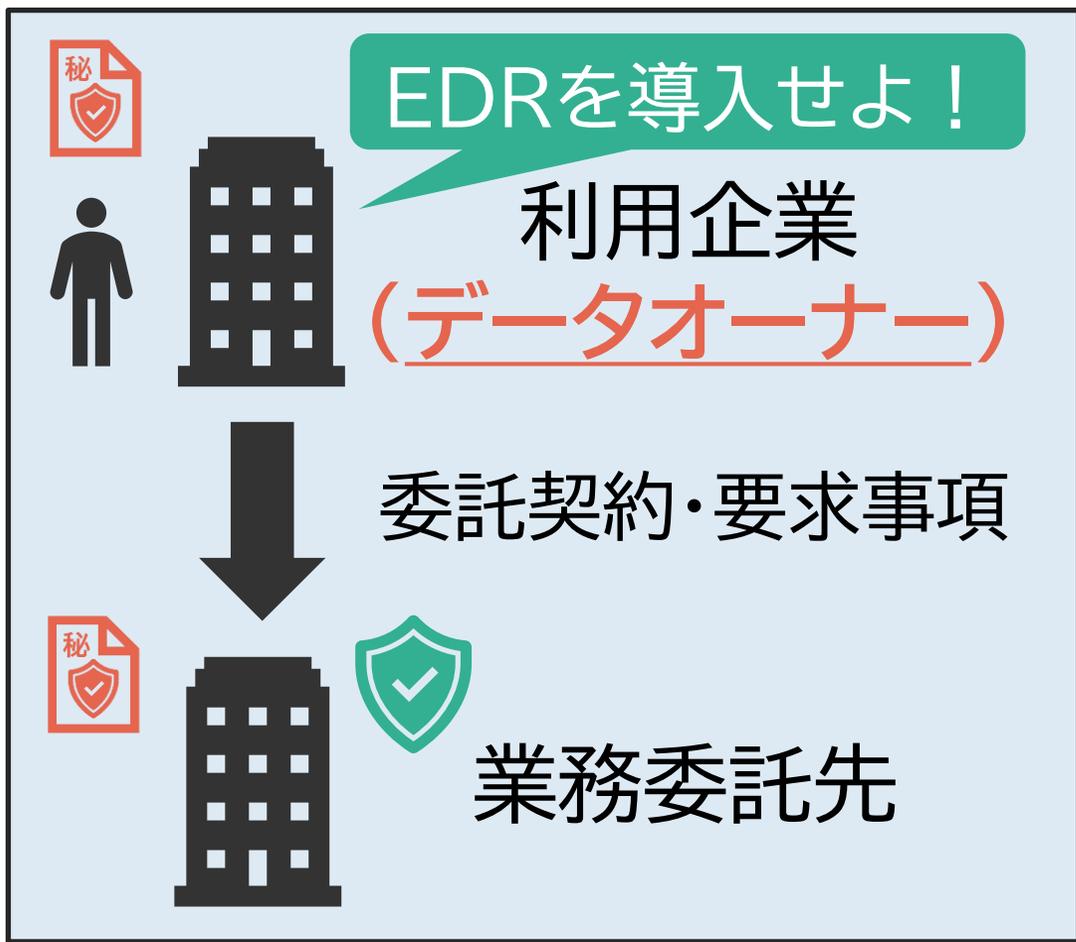
クラウドサービスの有効性を感じる企業

87.9%

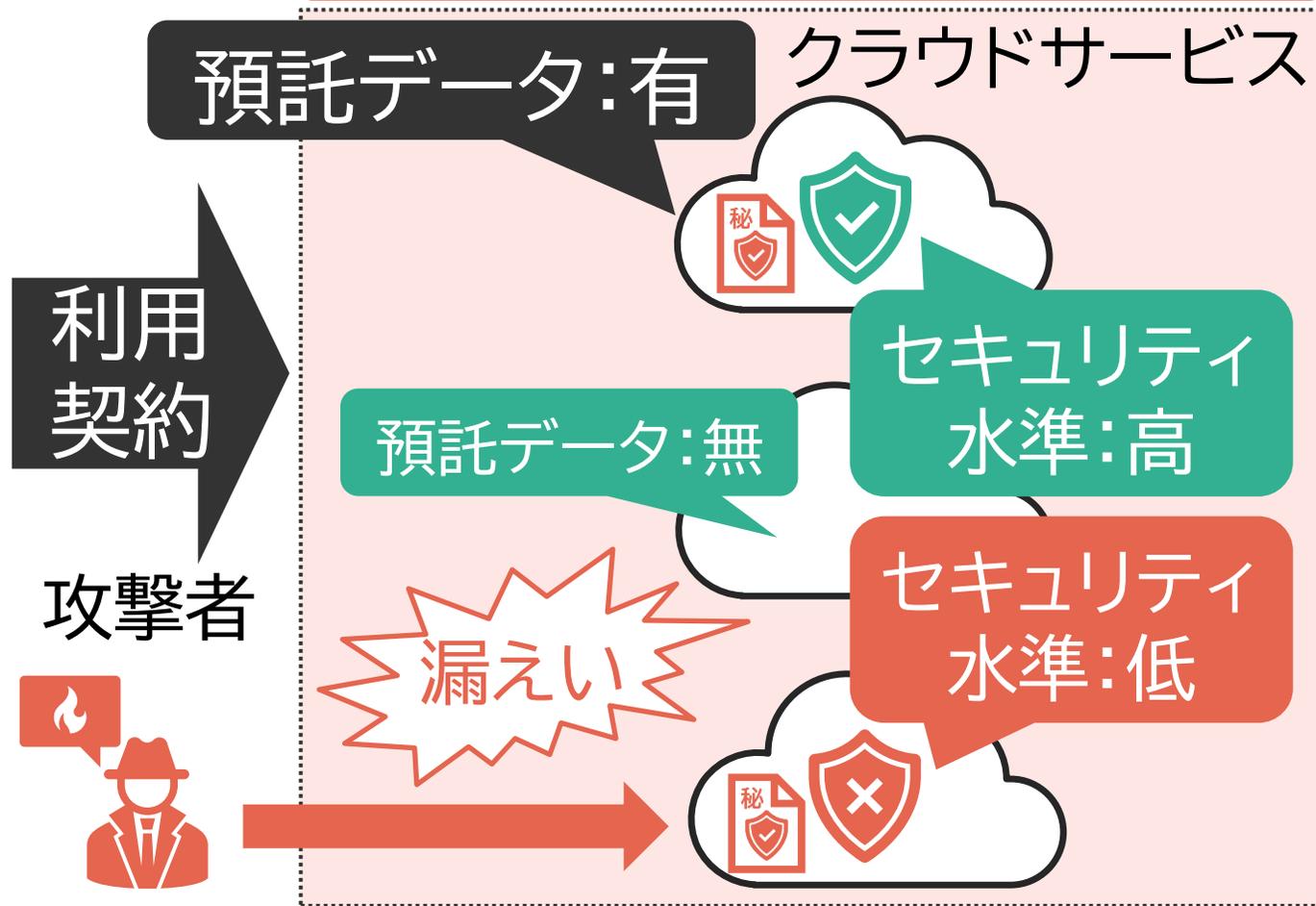
(出典)総務省「令和5年 通信利用動向調査報告書(企業編)」

# クラウドサービスも自社ITサプライチェーンの一つ

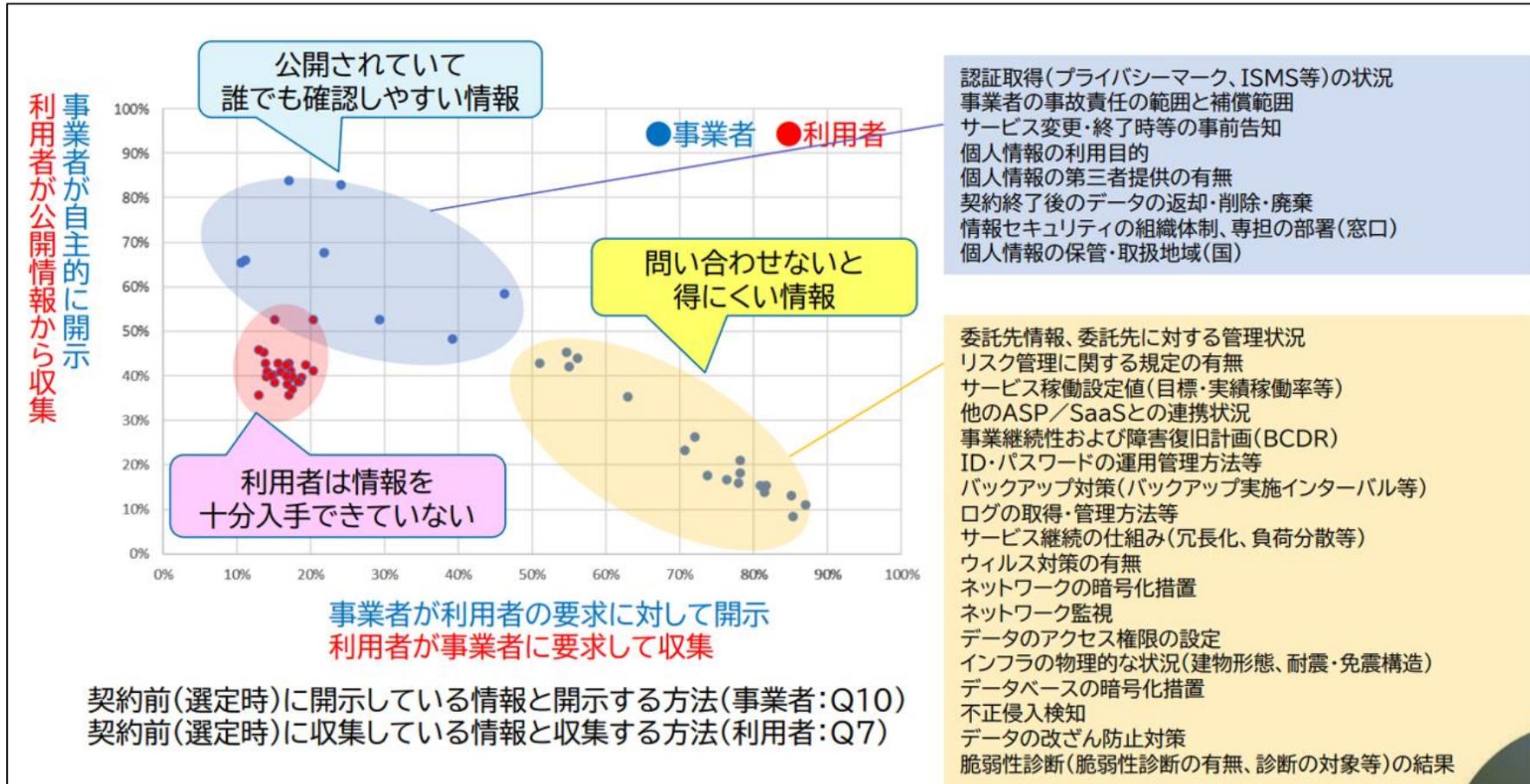
ガバナンスを効かせやすい関係



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」

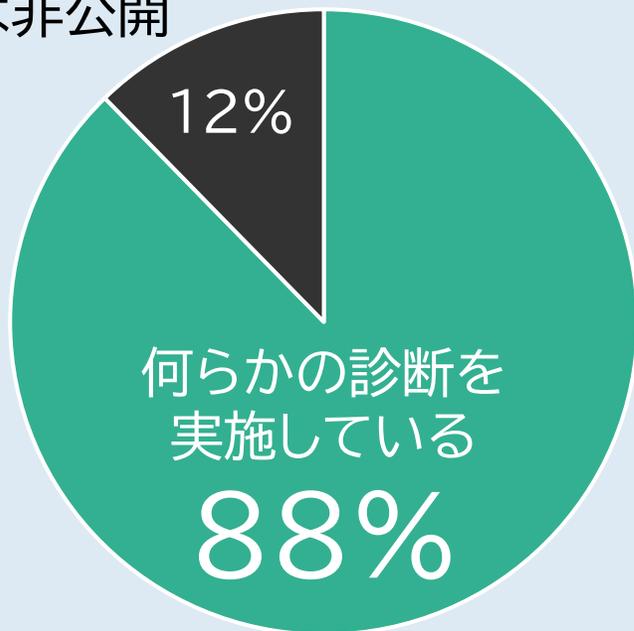


出典:IPA「2022年度クラウドサービス(SaaS)のサプライチェーンリスクマネジメント実態調査概要説明資料」

# 【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

実施していない  
又は非公開



何らかの診断を  
実施している  
88%



インフラ  
診断実施  
74%

未実施

アプリ診断実施 76%

未実施

インフラ・アプリ  
両方を診断  
58%

インフラ  
のみ診断  
16%

アプリのみ診断  
18%

ペンテスト  
その他  
8%

【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

マルウェア対策ソフトを導入

66.8%

その他の対策  
(EDR利用、その他の総合対策を含む)

35.8%

33.2%が未導入

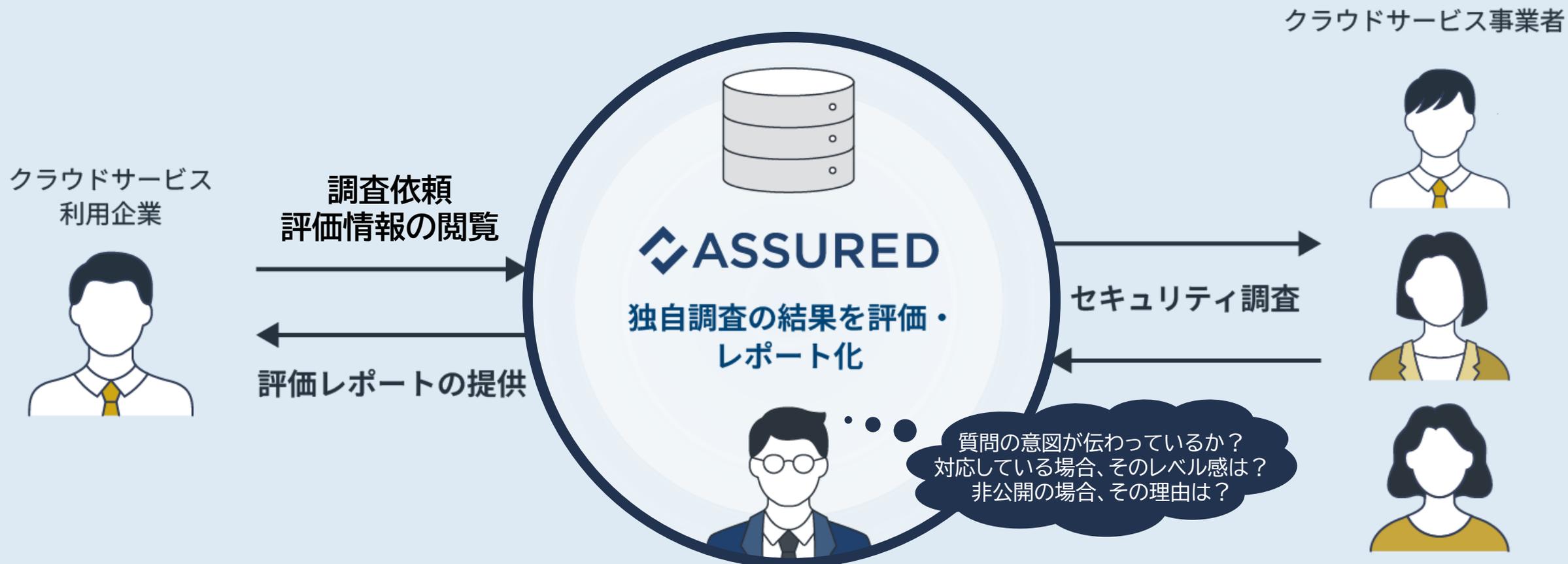
未実施

9.0%

0% 10% 20% 30% 40% 50% 60% 70%

【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

# 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

現在のプランではチケットを使わずに「評価開示を依頼」できます

すべてのカテゴリの一覧

企業名、サービス名など 検索

ウェブ評価のみのサービスも表示

クラウドサービスA  
ベンダー企業A株式会社  
パスワードマネージャ  
調査結果の開示を依頼 ウェブ評価を開覧

クラウドサービスB  
ベンダー企業B株式会社  
アフィリエイト管理画面  
調査結果の開示を依頼 ウェブ評価を開覧

クラウドサービスC  
ベンダー企業C株式会社  
マーケティングオートメーション  
ウェブ評価を開覧

クラウドサービスD  
ベンダー企業D株式会社  
データベース  
調査結果の開示を依頼 ウェブ評価を開覧

クラウドサービスE  
ベンダー企業E株式会社  
営業電話支援  
調査結果の開示を依頼 ウェブ評価を開覧

クラウドサービスF  
ベンダー企業F株式会社  
デザインツール  
調査結果の開示を依頼

サービス  
を選択

## スコア + 評価レポートを提供

総合評価

78 / 100

以下の点について懸念されるため、預託データの内容や業務上の重要性を見極め、対策を講じていただくことを推奨します。

- ・ データセンターの場所にUS/EU/中国が含まれるため、個人情報を取り扱う場合は、適切なセキュリティ対策を講じていただくことを推奨します。
- ・ ツールによる脆弱性診断は行われているものの、専門家による手動の診断は実施されていないか懸念されます。
- ・ 災害や大規模なシステム障害に備えて複数地点にまたがって冗長化されたシステムに切り替えるための計画が、サービス停止期間にわたりサービスが停止する可能性があります。
- ・ 外部委託先との合意内容の確認や定期的な評価が行われていないため、外部委託先との合意内容を確認いただくことを推奨します。

クラウドサービス事業者による回答

対応状況	設問の重要度	組織ポリシー (抜粋項目)
未対策	高	(未選択)
非公開	中	(未選択)
	低	(未選択)

PU 公開情報

PU-1 情報セキュリティについて企業としての方針を定め、経営陣の承認を得ていますか。

◎ いいえ

○ はい

○ 非公開

また組織の内々へ周知していますか。

▲ サービス検索画面

▲ 調査結果レポート

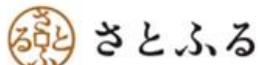
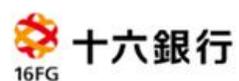
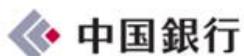
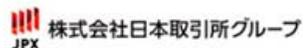
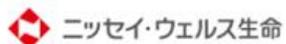
レポートの特徴

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

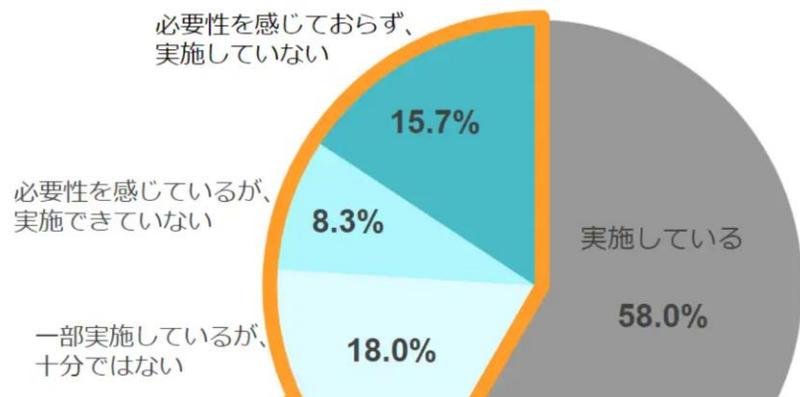
オンプレミス／IaaS環境における  
構成管理(SBOM含む)と脆弱性管理

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

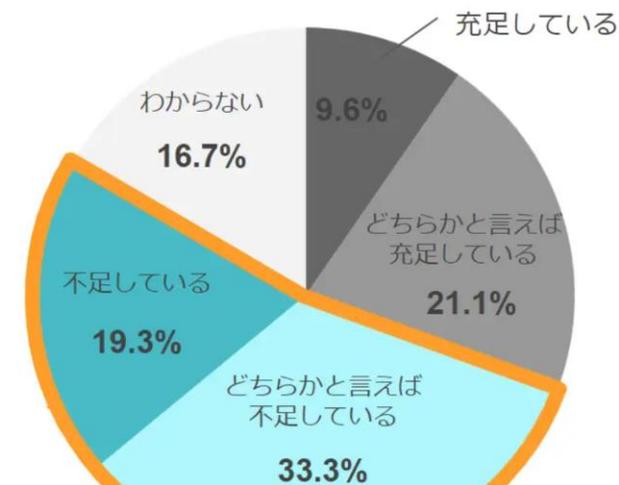


不十分・未対策：  
42%

(N=300)

yamory

## 脆弱性対策に従事する人員



不足：52.6%

(N=228)

yamory

# 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



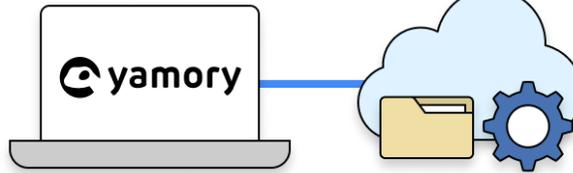
SBOM



セキュリティ

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

クラウド上のソフトウェア  
クラウド設定(CSPM)

aws Azure Google Cloud

オンプレのソフトウェア  
ネットワーク機器など

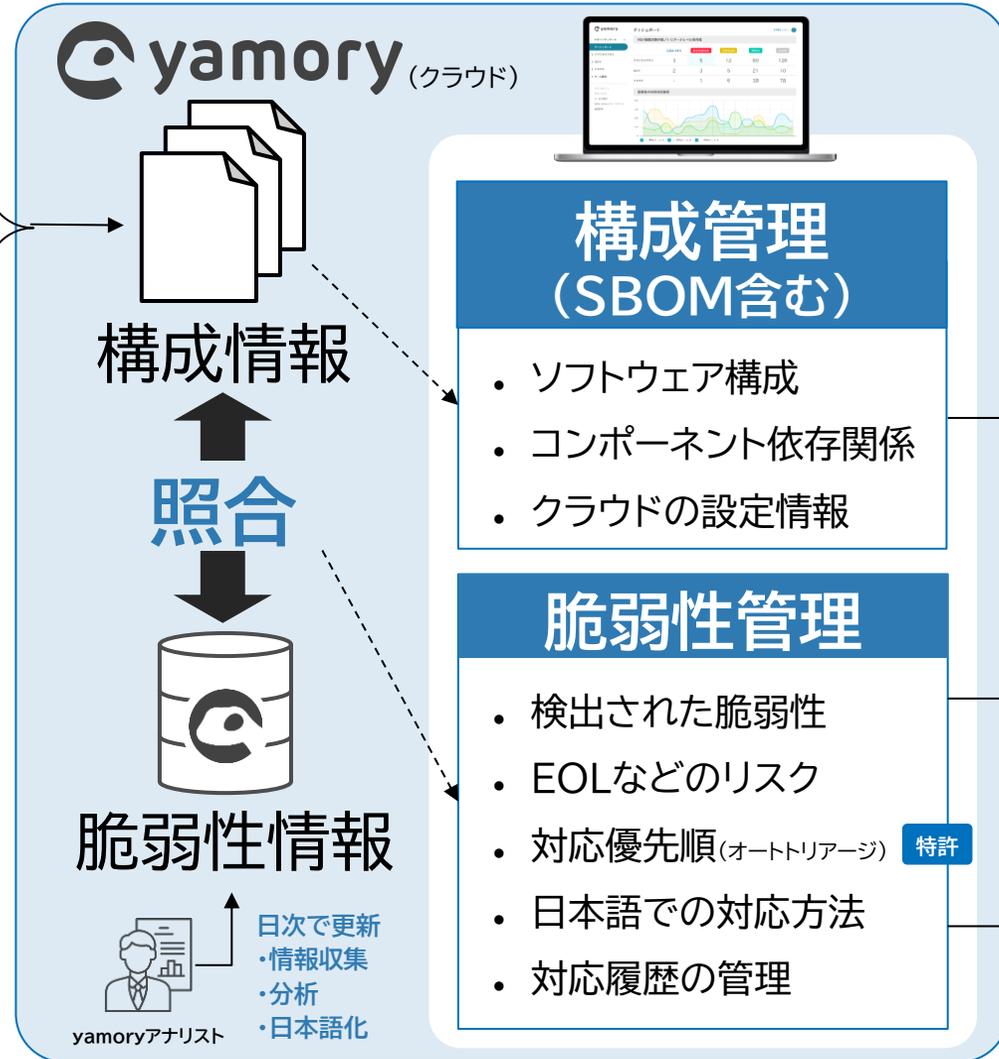
外部ベンダーから納品されたシステムのSBOMファイル

## 自動収集

- サービス連携
  - クラウド連携(一括)※ **特許**
  - GitHub連携
- コマンド実行
  - CLI、SSH
  - CIツール連携対応
    - GitHub Actions
    - CircleCI
    - Jenkins

## 手動登録

- ファイルのインポート
  - CSV
  - SBOM
- 手入力



※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

オンプレミス

クラウド

ライブラリ／フレームワーク

Spring, Struts, Laravel など

ミドルウェア

Apache, Tomcat, Java など

OS

Linux, WindowsServer など

ネットワーク機器

(PC, モバイルは対象外)

クラウド  
設定

アプリ

ホスト

インフラ

## 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

	CISA KEY	Immediate	Delayed	Minor
アプリライブラリ	4	70	49	
ホスト	83	99	54	
コンテナイメージ	3	32	29	
IT資産	22	122	228	
クラウド	0	12	57	

シンプルで  
明快なダッシュボード

この脆弱性によるリスク  
Remote Code Execution 公開サービス PoCあり にあてはま  
ります。  
情報漏洩、改ざん、不正操作、サービスの利用不能に直結する脆  
弱性です。今すぐ影響の有無を調査してください。

対応方法  
2.3.14.2以上にアップデートしてください。

トリアージ レベルを変更、脆弱性情報を詳しく見る >

チーム  
セキュリティチーム  
リポジトリ/プロジェクトグループ  
CaseStudy1  
マニフェスト/プロジェクト  
root@gradle  
ソフトウェア  
org.apache.struts:struts2-core:2.3.12  
依存関係  
すべて見る (1件)

2020/8/27 14:39  
システムがこの脆弱性を検出しました。

脆弱性の  
詳細情報

脆弱性の種類  
Remote Code Execution

公表元データベース  
NVD

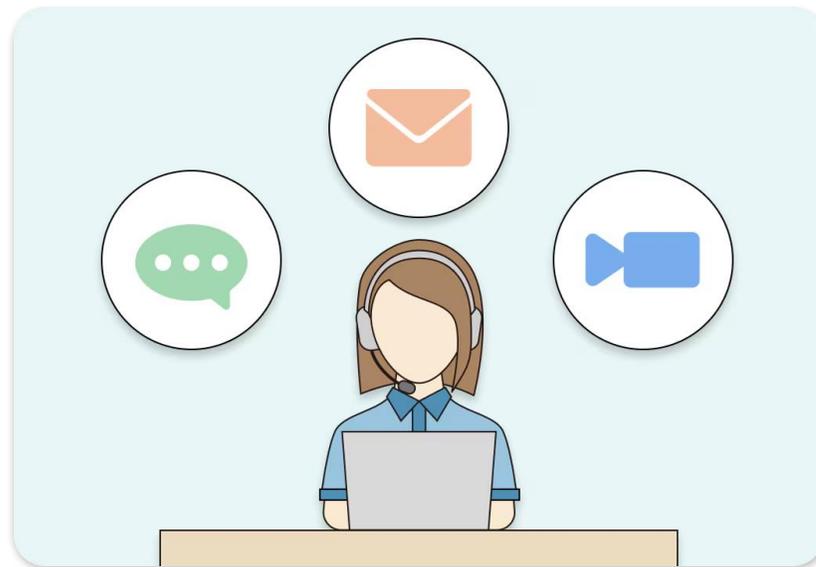
関連ID  
CVE-2013-2115

概要  
日本語 英語

Apache Struts 2.3.14.2未満に攻撃者にURLやアンカータグにincludeParams属性  
を含めたリクエストを送られることによって任意のOGNLコード実行が行われる恐れ  
があります。  
これはCVE-2013-1966の修正が不完全だったため同様の問題が発生しました。

脆弱性を含んだソフトウェア	CVSS	PoC情報	参考・関連情報	CPE
CVSS v3 による深刻度				
深刻度	8.1 (HIGH)			
攻撃元区分	NETWORK			
攻撃条件の複雑さ	HIGH			
必要な特権レベル	NONE			
利用者の関与	NONE			
CVSS v2 による深刻度				
深刻度	9.3 (HIGH)			
攻撃元区分	NETWORK			
攻撃条件の複雑さ	MEDIUM			
必要な特権レベル	NONE			
機密性への影響	COMPLETE			

対応方法



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

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

トリアージ結果	None	Minor	Delayed	Immediate
対応例	現時点では 対処しない	定期メンテナンス で対処	2週間以内に対処	日次で対処
<b>危険性</b> 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)				
<b>影響度</b> 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				
<b>攻撃手段</b> 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 KEV Catalog



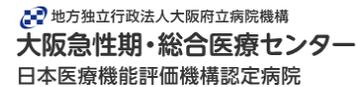
CISA(アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁)が2021年に公開した、「実際に攻撃者が積極的に悪用していることが確認されており、対応が急がれる脆弱性」の一覧

KEVI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**

### 攻撃事例

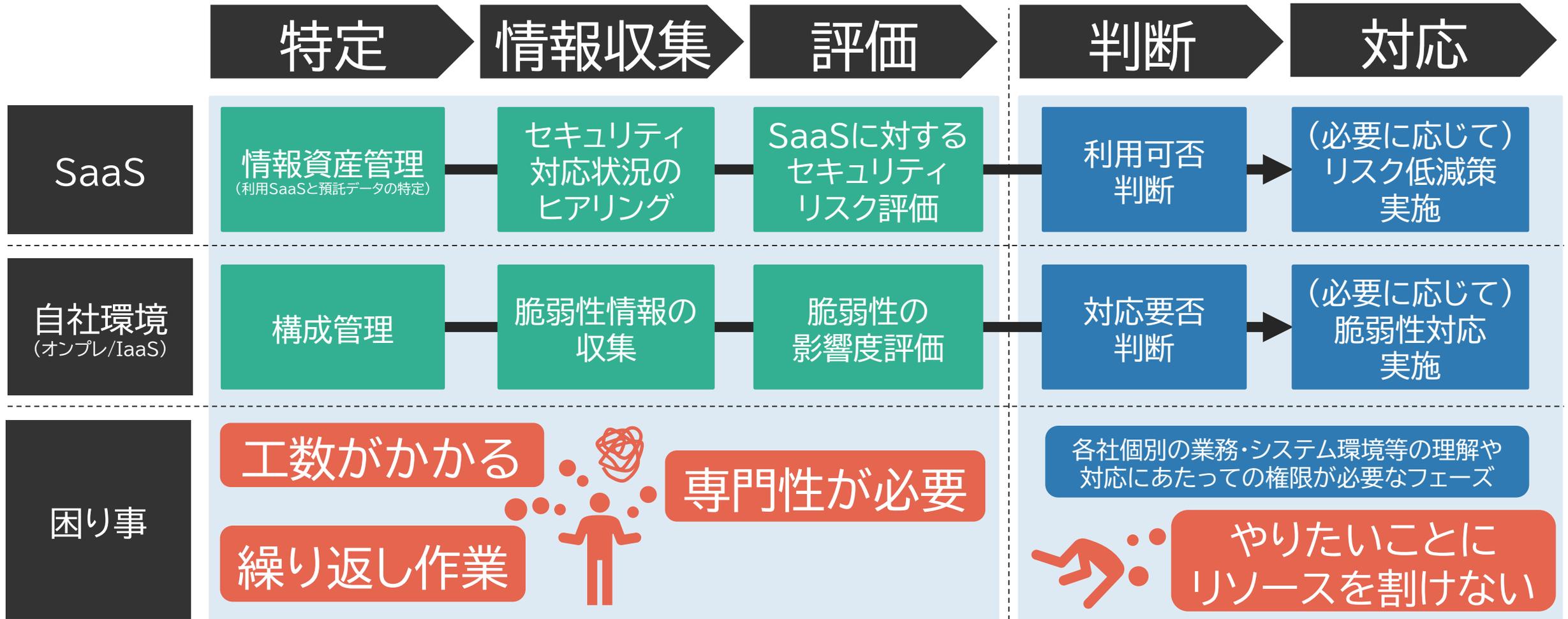
# 導入実績



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

 **ASSURED**

一丁目一番地となる重要領域

自社環境  
(オンプレ/IaaS)

 **yamory**

困り事

「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

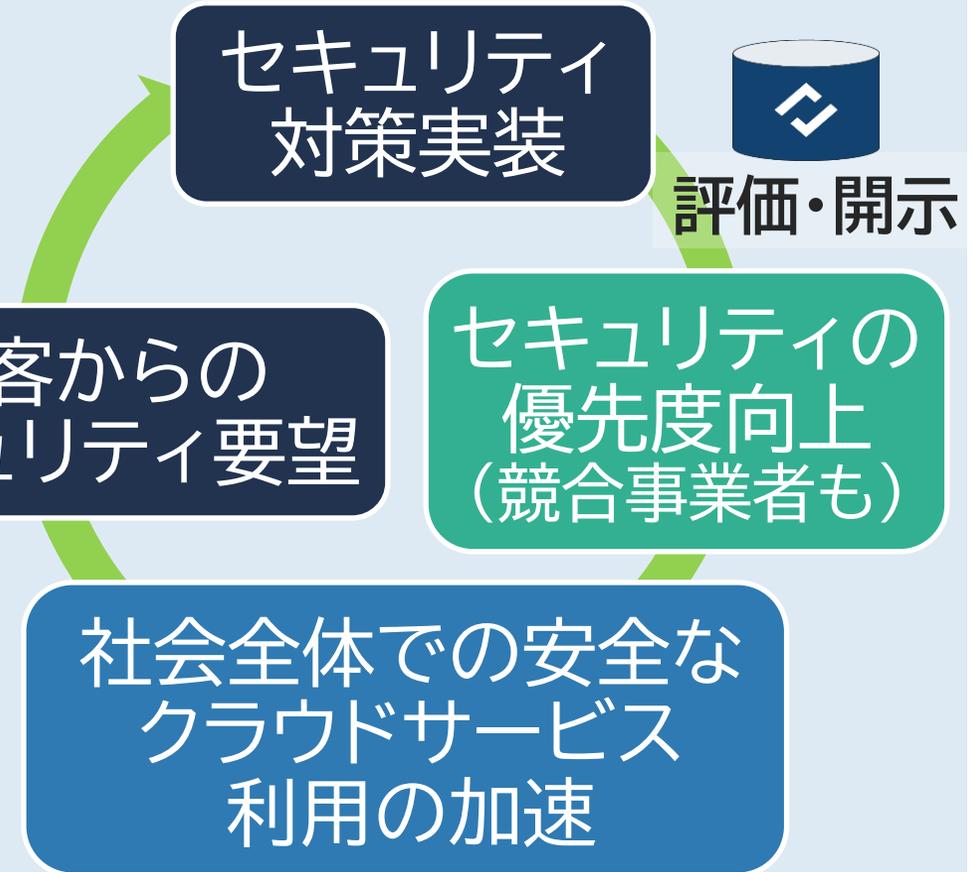
## 事故発生メカニズム



◇ ASSURED

取引基準への組み込み

## 世の中に行き起こる変化



# 【ご案内】Webinar／オフライン勉強会

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



ISC2  
Webinar

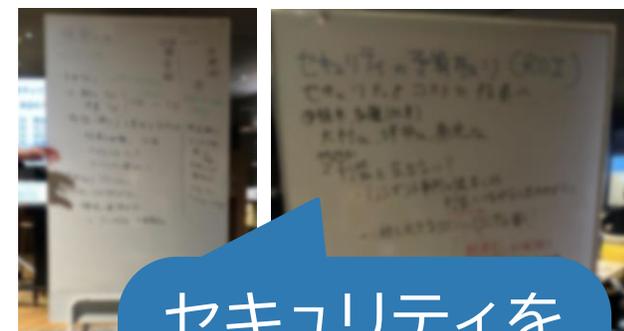
セキュリティ  
勉強会  
in 渋谷

自社セミナー

セミナー



車座(お酒飲みながら)



セキュリティを  
「コスト」から  
「投資」へ  
変えるには？



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](https://assured.jp/seminar/240910_archive?utm_source=yuzawa&utm_medium=website&utm_campaign=event&utm_content=20241009)



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**