サプライチェーン セキュリティ評価制度 に 少人数で立ち向かう

AI診断 × プロの運用 で実現する
無理のない継続対策

株式会社エーアイセキュリティラボ
事業企画部ディレクター
阿部 一真

株式会社ハートビーツ
クラウド・アクセラレーション事業部
ビジネス推進グループ マーケティングチームマネージャー
谷川 隼人

配信日
2026.5.14 木
16:00-17:00

アジェンダ

16:00〜16:05	イントロダクション
16:05〜16:30	Part.1｜株式会社エーアイセキュリティラボ 「サプライチェーンの「穴」をふさぐ、AIによる脆弱性診断の内製化アプローチ」
16:30〜16:55	Part.2｜株式会社ハートビーツ 「見つかった脆弱性を「放置」しないー評価制度の要件を満たし続ける運用支援体制ー」
16:55〜17:00	質疑応答・クロージング

サプライチェーンの「穴」をふさぐ

AIによる 脆弱性対策の内製化 アプローチ

登壇者紹介

株式会社エーアイセキュリティラボ

事業企画部 ディレクター **阿部 一真**（あべ かずま）

新卒でNTTデータに入社し、Salesforceビジネス推進部門で
コンサルティングセールス・カスタマーサクセスを経験。
その後、AIベンチャー企業・SaaSスタートアップ企業にてCS責任者
およびプロダクトマネージャー・事業統括責任者を歴任し、エーアイ
セキュリティラボに入社。
現在は、新規プロダクト企画・事業開発をリードしながら、
各種セミナー・講演への登壇などエバンジェリストとしても活動。

AeyeSecurityLab

登壇者紹介

株式会社エーアイセキュリティラボ

事業企画部 ディレクター **阿部 一真**（あべ かずま）

フォローお願いします！

AeyeSecurityLab

誰でも簡単に

プロさながらの高度な

脆弱性診断を

AeyeScan

サプライチェーンの「穴」をふさぐ

AIによる 脆弱性対策の内製化 アプローチ

昨年はサイバー攻撃、特にランサムウェアによる被害が話題に

大手飲料メーカー

2025年9月、ランサムウェア攻撃により、システム障害が発生。**国内グループ各社の受注・出荷業務が停止。**さらに個人情報が流出した可能性があると発表された。

大手通販業者

2025年10月、ランサムウェア攻撃によりシステム障害が発生し、受注・出荷業務が停止。**同社の子会社に配送の一部を委託する別会社のECサイトも停止に。**

業務停止・システム停止による事業影響、社会的信頼・株価への影響だけでなく

取引先やグループ会社、サプライチェーンを巻き込む被害に発展

多様化するランサムウェアの「侵入経路」

NW機器/VPN

クラウド

Webサイト

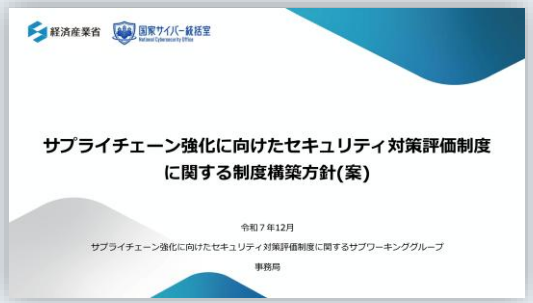
CMS/SaaS

PC/社用端末

メール/ファイル

セキュリティ対策水準の向上を図る「サプライチェーン対策評価制度」

経済産業省は、サプライチェーン全体の強靭性の確保と、対策要求の共通化による対策適正化・確認の効率化を目的とした「サプライチェーン対策評価制度」を導入する方針を示している。



セキュリティ対策の
成熟度を3段階で評価

	★3	★4	★5
想定脅威	一般的な サイバー攻撃	供給停止・情報漏洩 など大きな影響を もたらす攻撃	未知の攻撃も含めた 高度なサイバー攻撃
対策の基本的な 考え方	全てのサプライチェーン企業が 最低限 実装すべき対策	サプライチェーン 企業等が標準的に 目指すべき対策	サプライチェーン 企業等が到達点と して目指すべき対策
評価スキーム	専門家確認付き 自己評価	第三者評価	第三者評価

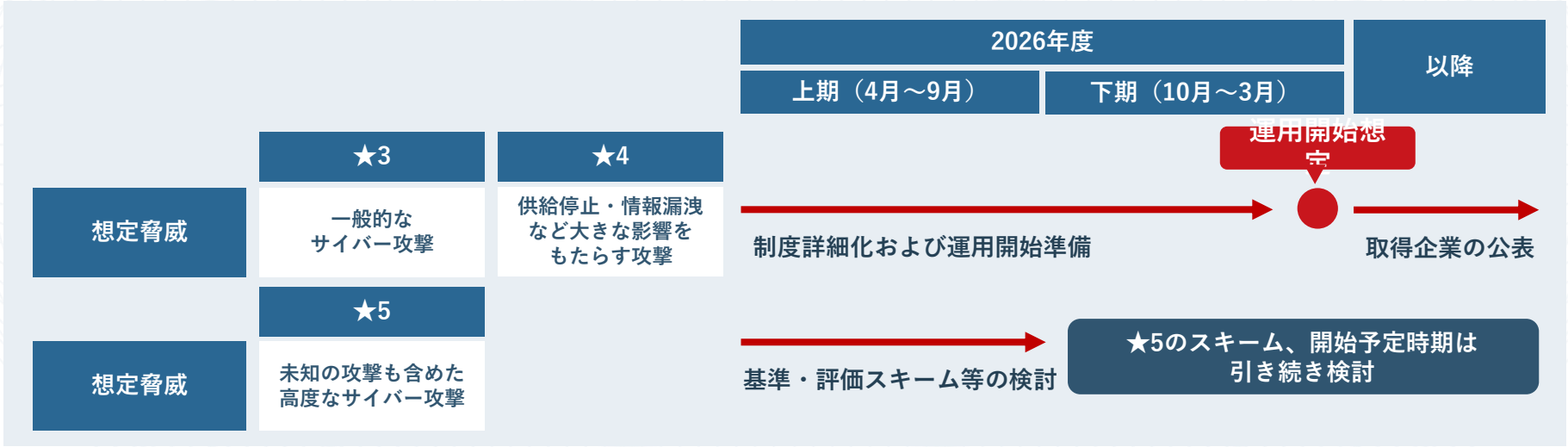
※★1、★2に関しては、先行する自己評価制度の仕組みである「SECURITY　ACTION」にて制度化

認定取得の有無が取引基準となる可能性もあり、どの企業も無関係ではいられない

参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

2026年度下期から運用開始想定

2025年12月下旬（昨年末）に制度構築方針（案）が更新され、★3、★4については2026年度下期の運用開始を想定していると記載された。

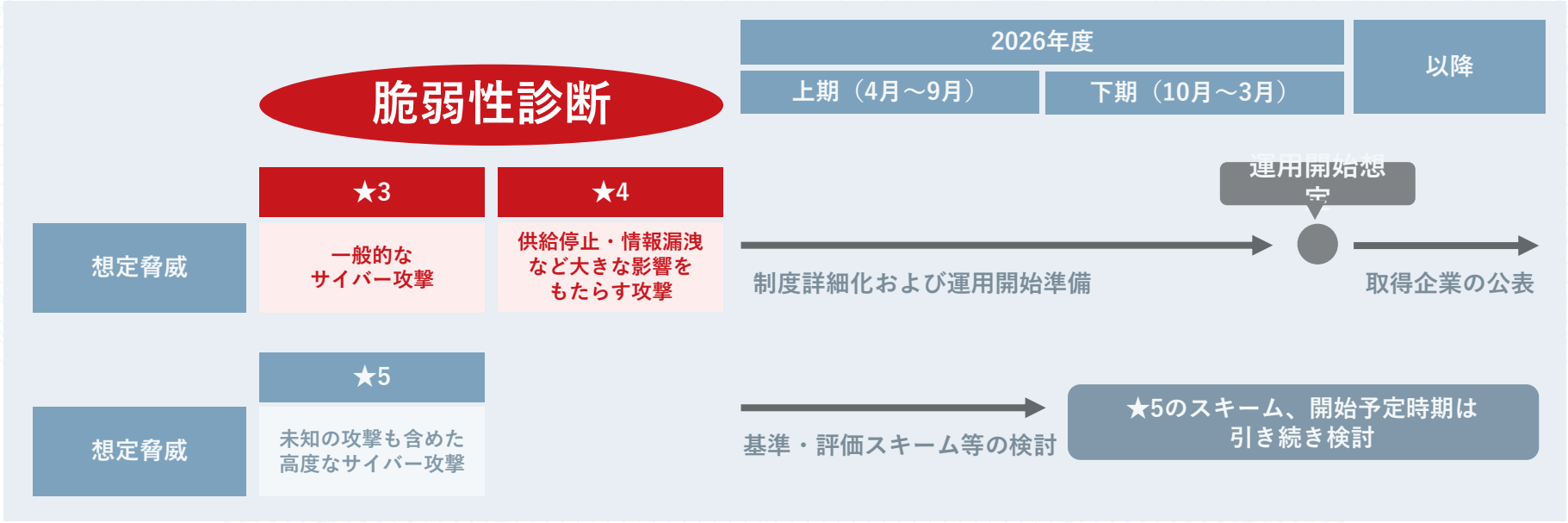


運用開始に向けて、自社のセキュリティ対策状況の見直しが急務となっている

参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

まずは「攻撃手法・対策方法が分かっている」部分から対策

★3、★4で想定されている“既知の脆弱性”から対策する＝穴を塞ぐことが最優先。
未知の攻撃への防護策を考えるのは、その次でOK。



参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

脆弱性診断の「内製化」に立ちはだかる壁

脆弱性診断を網羅的・継続的に実施するために「内製化」を考える

「内製化できればいいんだけどな…」

? 診断の品質を維持できるだろうか？

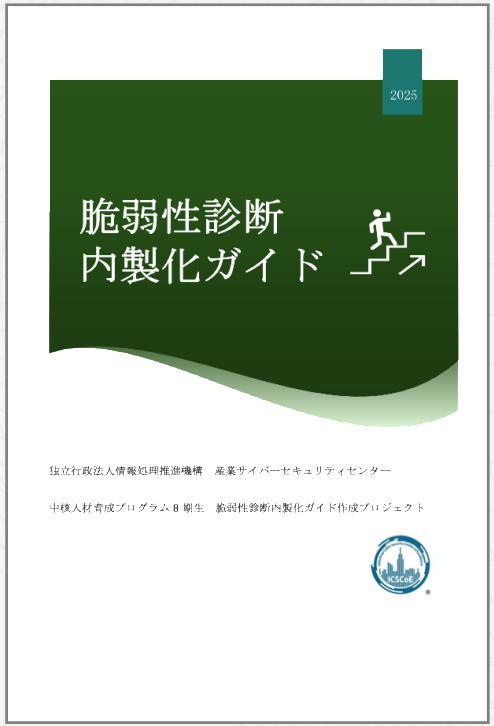
? コスト（費用・時間）を抑えられるか？

? 社内メンバーで対応できるだろうか？

＋

内製化に向けた体制を組み、運用にのせられるか？

IPA（独立行政法人情報処理推進機構）から脆弱性診断内製化ガイドが公開



公開の背景

脆弱性の早期発見がますます重要に

- 事業継続
- 信頼性維持の観点

内製化への関心が高まっている

- 新たな脆弱性の増加
- リリースサイクルの高速化

主な内容

- 外部発注と内製の違い
- 内製化に必要な組織体制と人材
- 内製化の進め方と継続的改善プロセス
- 関係組織との連携とセキュリティ意識の醸成
- ツール選定におけるポイント

参照：IPA「脆弱性診断内製化ガイド」 https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2025/Vulnerability-assessment.html

脆弱性診断内製化のポイント（参考）

脆弱性診断の内製化は、STEP 0～5の段階に分けて考えることができます。

「死角」になっている
Webサイト・Webアプリはどうする？

DXの進展：Web資産の把握が難しくなっている

Phase 1

情報のデジタル化

＜主なリスク＞

- 人的リスク(漏洩・持出)
- ストレージの安全性
- 不適切な認証・権限設定

Phase 2

業務のデジタル化

＜主なリスク＞

- クラウド環境の設定不備
- ネットワークへの攻撃
- 不完全なエンドポイント管理

Phase 3

事業のデジタル化

＜主なリスク＞

- 頻繁なサービスアップデート
- 潜在的なデジタル領域の攻撃面
- サプライチェーンの拡大

情シス・セキュリティ部門が認識しやすい
社内ITを中心とした「静的」IT資産がほとんど

どこで何やってるか
分からない…！

Web資産を把握する難しさはどこにある？

人力で探索・精査が必要

広範囲から検出することはできるが、
不要なものも多く紛れ込んでおり、
人手による精査が必要。

リスク評価が困難

リスクをどう評価するか悩ましい。
システム観点からだけでなく、
事業観点での優先順位付けが必要。

AeyeSecurityLab

高度な生成AI活用により、効率的かつ信頼性の高い探索が可能

生成AIをASMに活用することで…！

会社名だけ
で攻撃面を探索

検索結果に上がってきた
組織名(文字列)を解読

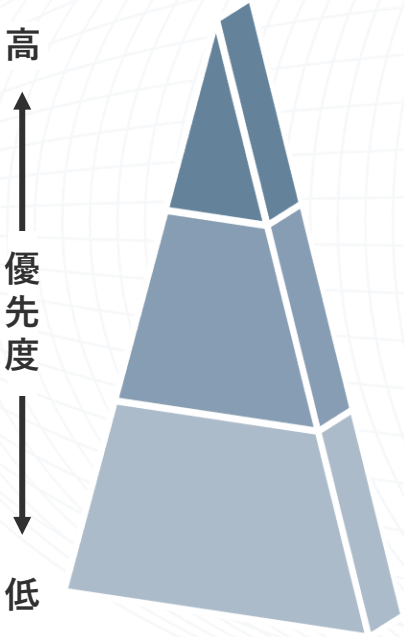
膨大な情報源
から総合的に判定

- SSL証明書の情報
- IR情報(Web公開済み)　など

発見経路/理由
が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートを説明

資産の優先度・診断の優先度に応じた、対策の棲み分け（弊社整理）



手間と時間を惜しみなく投下して何が何でも十全の対策をする必要あり	専門家の手動診断で精密検査・優先対応	外部診断
多少の予算・手間をかけてでも一定レベルのセキュリティを担保したい／しなければならない	内製化による診断で定期検査・随時対応	AIを活用した内製化診断
本番環境しかないので、診断により何らかの影響がある可能性を踏まえ診断するのが難しい 予算も手間もかけられないが放置するわけにはいかない	全自動で定期的な検査（簡易スキャン）でモニタリングできている状態を作る	AIを活用したASM内製化

いきなり全部やるのは難しい
➡３階層に分けて、一歩ずつ！

生成AI時代の脆弱性診断なら

AeyeScan

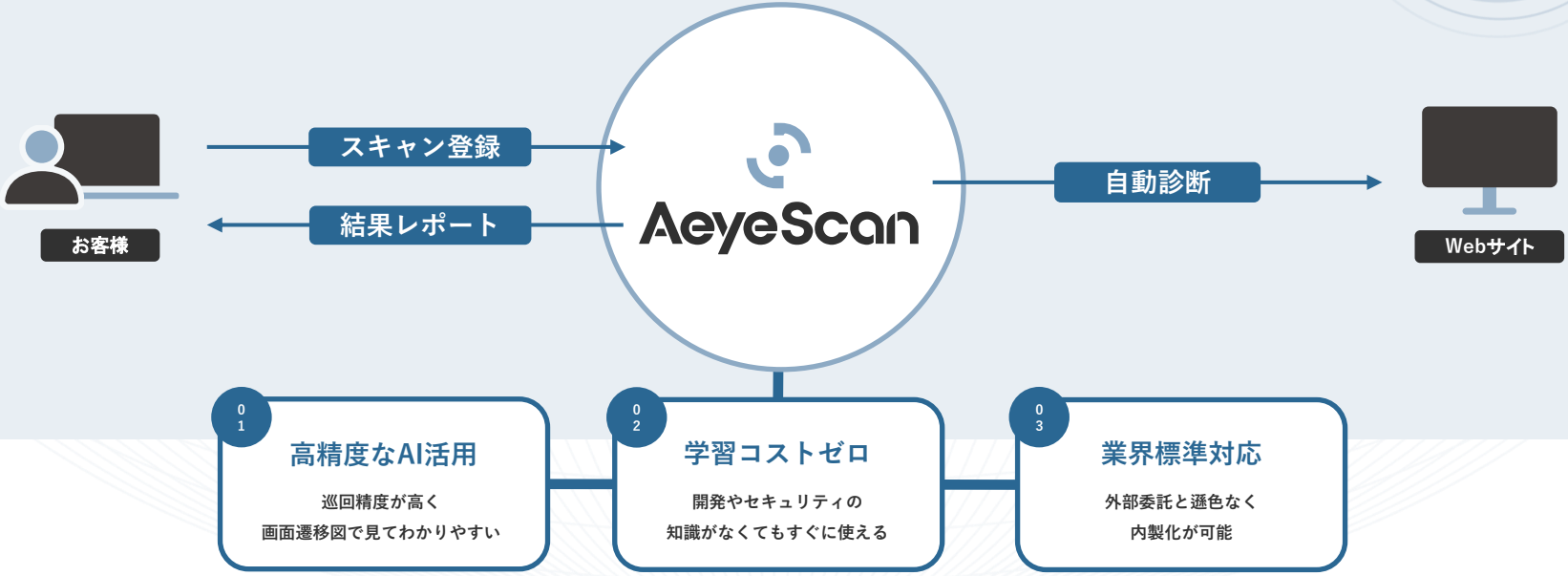
クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1※

※富士キメラ総研調べ「2025 ネットワークセキュリティビジネス調査総覧 市場編」
Webアプリケーション脆弱性検査ツール ベンダーシェア（2024年度実績）

※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2025」SaaS型
Webアプリケーション脆弱性管理市場：ベンダー別売上金額シェア（2023年度実績）

有償契約
300社以上



AeyeScanが選ばれている理由

誰でもかんたん操作

開発やセキュリティの知識がなくても、
トレーニングなしで診断可能。

AIによる自動診断

圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

わかりやすいレポート

各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

AeyeScanが選ばれている理由

誰でも使える操作性 × プロが認める機能・性能

AeyeSecurityLab

さまざまな企業さまに導入いただいております

ユーザー企業

人材・教育

ORIENTAL DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / Leverages / workport

インフラ

EPARK / AIRE / HIS / H.I.S. / NTT EAST / odakyu / 近鉄情報システム株式会社 / SymEnergy / 水ing / Suzuyo / NANKAI / 日本調剤 / JARMeC / HITOWA GROUP / BOOK-OFF / ベルーナ / MEDIA / Looop / Loyalty Marketing, Inc.

金融

アイフル / MS&AD インターリスク総研 / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century / Net Protections

メディア

集英社 / 中日新聞 / NIKKEI / Media Do

製造

AICA / AISIN / KITZ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

エンタメ

イープラス / CAPCOM / GungHo / とらラボ! / BookLive

SaaS

Advanced Media, Inc. / Lexica / M-aid / エムティーアイ / OZ INTERNATIONAL / Classi / COACH A Co.,Ltd. / cybozu / Speee / SecureNavi / Diamond head / DMM Boost / TAL / Digital Garage / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / freee / vector / porters / hokan / Money Forward / RUN.EDGE / RVSTA / Rescuenow

SI・IT企業

Rworks / アクモス株式会社 / AVANT GROUP / Insight Edge / Infcurion / 80&Co. / SBWorks / NTT Integration / NTT DATA / NTT ビジネスソリューションズ / OMRON / Globalway / KDDI / KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / tdi 情報技術開発株式会社 / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / 電通総研 / TOPPAN / JOPS / AST / PCNET / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / YONA / リピスト

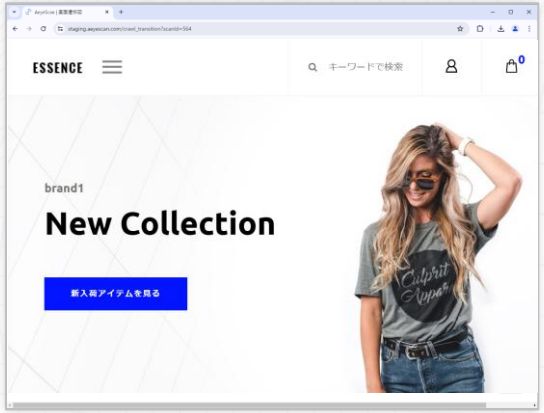
セキュリティ企業

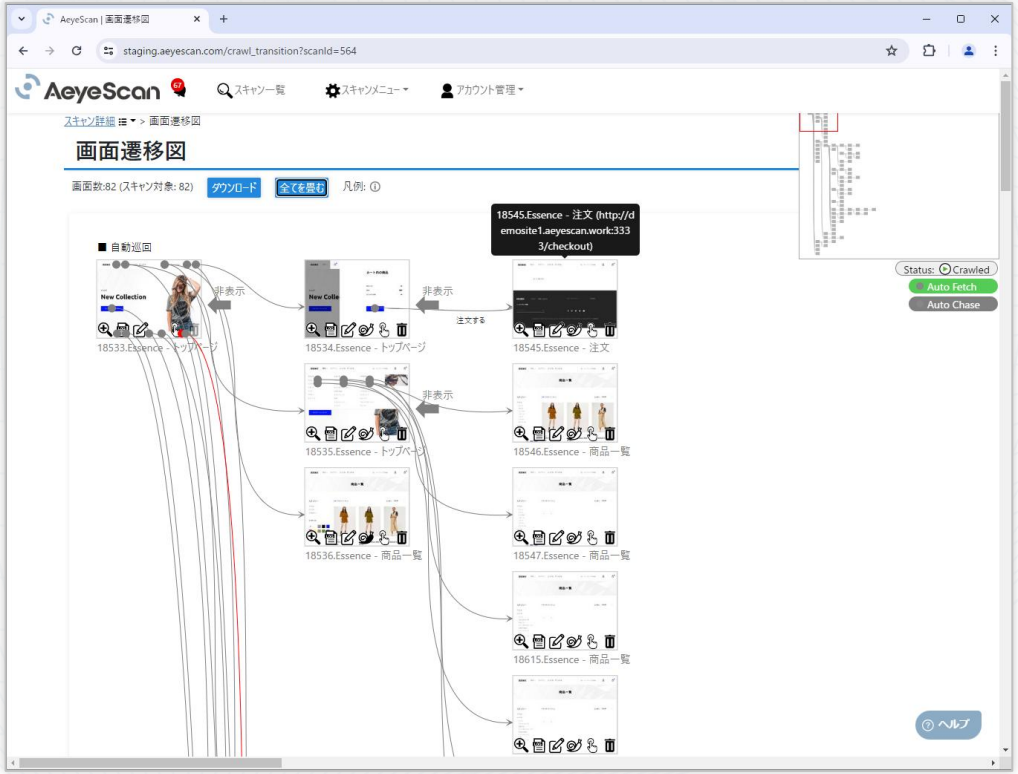
NEC / NECセキュリティ / NTT DATA / GSX / cybertrust / LAC

社名五十音順（導入いただいた企業様の一部です） 会社名及びロゴは各社の商標または登録商標です

AeyeSecurityLab

巡回時に、自動で画面遷移図を生成





結果がわかりやすく、すぐさま修正作業に取り組めるレポート

AeyeScanの導入を検討してみませんか？

操作性の確認、実際に利用してみたい方へ

AeyeScanの 無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうなの？
またどのように脆弱性が発見されるのか？
などの疑問は無料トライアルで解消しましょう。

無料トライアルの申し込み

お見積りの希望・導入をご検討している方へ

AeyeScanへの お問い合わせ

お見積りの希望・導入をご検討してくださっている方は
お問い合わせフォームよりご連絡ください。
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせフォーム

定期開催中！ AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを検討してみたい方へ

AeyeScanがどんなものか知りたい方向けに、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

AeyeScanデモ動画を視聴

AeyeScanの操作を体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

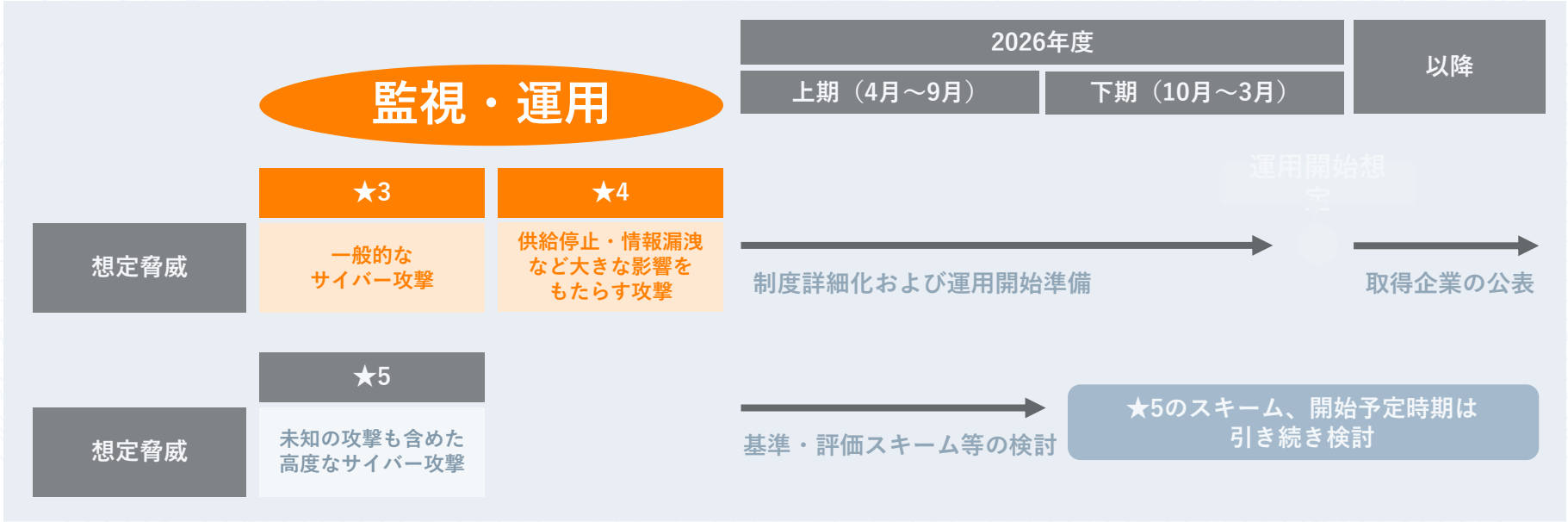
ハンズオンセミナーの日程を確認

セキュリティ対策にお悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認

評価制度をさらに推し進めるべく、運用体制を強化したい場合は？



参考：サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)より抜粋および意訳

株式会社ハートビーツ様のセッションにてご紹介いただきます！

AeyeScan

セキュリティに、確かな答えを。

セッション2

株式会社ハートビーツより

見つかった脆弱性を「放置」しない ―評価制度の要件を満たし続けるプロの運用支援体制―

登壇者紹介

株式会社ハートビーツ
クラウド・アクセラレーション事業部
ビジネス推進グループ マーケティングチーム マネージャー

谷川 隼人

EC・金融商品などのマーケティング領域に携わり、2024年にハートビーツに入社

Web広告のオンライン施策、展示会等のオフライン施策など幅広く担当しながら、既存のお客様への事例インタビュー等でお客様の声を収集しサービス改善・マーケティングに活かしている。

お客様の声から得られたインフラ運用の”リアル”を元に各種ウェビナーに登壇中。

株式会社ハートビーツ

HEARTBEATS

設立：2005年4月15日

所在地：東京都新宿区新宿1-28-11 小杉ビル5F

- 20年以上のITインフラ運用で培った豊富なノウハウ
- エンジニアが全社員の約8割を占める技術者集団

【認定資格】

- プライバシーマーク認証 (JIS Q 15001)
- ISMS認証(JIS Q 27001 (ISO/IEC 27001))
- AWS アドバンストティアサービスパートナー
- AWS 100 APN Certification Distinction
- AWS MSSPコンピテンシー
- Backed by AWS Support

【加盟団体】

- 日本MSP協会 会員
- デジタルトラスト協議会
- 国立大学法人 電気通信大学 大学発ベンチャー認定
- 日本シーサート協会

aws PARTNER Advanced Tier Services

- Solution Provider
- Backed by AWS Support
- MSSP Services Competency

17000063(09)

ICMS-SR0611 / JIS Q 27001

様々なサイト・システムのインフラ支援実績

ECサイトやSaaSサービス、人材紹介サービス、ゲーム
通常のサービスサイト・公式サイトなど幅広いWebサイトやシステムをご支援
現在150社＋、300案件＋、8,000台＋のサーバーを運用中

パシフィックリーグマーケティング株式会社

PLM

同時間帯に数万人のアクセスが想定されるサービスでも、負荷テストやサーバーのスケールアウト・スケールアップを行ってもらって万全の準備を整えられている。

#スポーツ

ネットイヤーグループ株式会社様

NET YEAR GROUP

HANEDA Japan Airport Terminal

オンプレミスからAWSへのサーバレス構成へ移行し、羽田空港Webサイトのダウンを一度も起こさない安定稼働に。DDoS攻撃や通常の数十倍のアクセスにも迅速な対応で稼働を継続。

#開発会社 #インフラ

株式会社システムアイ様

株式会社システムアイ

他社と比べて1/4のコストで費用対効果高く、安心して任せられる体制を構築できた。開発のみでなく、監視・保守まで一貫した提案が可能になった。

#開発会社

株式会社Kaizen Platform様

KAIZEN PLATFORM

短時間ストップするだけでも顧客へ影響が及ぶため、監視対応のすべてを安心しておまかせできる点は非常に心強い。
以前の委託先と比較しても明確な違いを感じる。

#ITコンサル

ISM / Vitabrid Vitabrid Japan / MARVELOUS! / TVer Technologies / hacomono / 1-グルナ / Omiai / ウェルネスダイニング / bstyle group / GIZMODO / NINESIGMA Accelerating the Innovation Cycle / FuRyu / GiGWorks IT / ASAHI 朝日新聞出版 / テレAI / Tricycle / glucose / Georepublic / ANDO FOUNDATION 公益財団法人 安藤スポーツ・食文化振興財団 / ·Y·U·K·A·I· ·E·N·G·I·N·E·E·R·I·N·G· / 徳間書店

本ウェビナーの目的と到達ゴール

解決すべき課題

診断で脆弱性を見つけたものの、対応のリソースや判断基準がなく「放置」されてしまう。これが多くの企業が抱えるセキュリティ対策の実態です。

本日のゴール

ISMSの規程を超えた「技術実証ベース」の運用を理解し、脆弱性を放置しない運用モデルを再確認します。

Chapter 1

評価制度の理解

単発の「診断」から、継続的な「安全性」の証明へ

SCS制度ピラミッド：★1〜★4の階層

★1〜★2：基礎

Security Action。自己宣言。中小企業を含む全事業者が取り組むべき最低限の意識付け。

★3：基本実装

一般的脅威への対応。組織的対策とIT基盤の防御。専門家確認付きの自己評価。

★4：標準運用

高度な脅威への対応。検知・拡大防止・復旧能力。第三者評価と技術検証（証跡）が必須。

✓事業中断で事業継続上重要な業務に遅延が生じうるか
✓サイバー攻撃等で機密等に係る情報管理に重大な影響が出るか

★3と★4の差：実証の壁

★4審査では「見つかった脆弱性をいかに迅速に、確実に是正したか」のプロセス履歴が問われます。

Chapter 2

ISMSとの実運用ギャップ

「構え」のISMSと、「打ち返し」のSCS制度

ISMS vs SCS

ISMS（マネジメント体制）
リスク評価に基づき、管理策の手順を「規程化」することが主眼。

SCS制度（実運用の実効性）
指定された管理策が、技術的に「稼働」し、是正されていることを重視。

「手順がある」ことと、「是正が完遂されている」ことの間には巨大なリソースの溝が存在します。

「通知は来る」と
「運用できている」は違う

Chapter 3

評価項目の差

「放置」を許さないISMS vs SCSの具体的ギャップ

フォーカスすべき4つの評価項目

3.2.1

脆弱性管理。単なる「入手」ではなく「継続的把握と是正完遂」が問われる。

1.2.2

脅威監視。24/365の相関分析による、放置箇所への攻撃検知。

4.4.3

ログ点検。保管ではなく「侵害の有無」をトリアージする能動的分析。

5.2.1

不審な認証試行やアラートに対して、どのレベルのインシデントか分析し判断。

脆弱性管理[3.2.1]：放置を許さない運用

管理策区分	ISMS A.8.8 (技術的脆弱性管理)	SCS 3.2.1 (脆弱性の管理)
要求の核心	手順の確立と情報入手	**継続的把握と是正の完遂**
具体的アクション	JVN等の情報を収集し、対策を講じる手順を文書化する。	資産に対し継続的スキャンを行い、リスク判定に基づき迅速に是正した証跡を残す。
実運用の壁	「年に一度の診断」で止まる	対応漏れをなくす「対応ライフサイクル」の証明が不可欠。

脅威監視[1.2.2]：分析と予兆検知・攻撃防御

管理策区分	ISMS A.8.16 (監視活動)	SCS 1.2.2 (不正侵入等の検知)
要求の核心	異常の監視とレビュー	**予兆とインシデントの検知〜対応まで**
具体的アクション	システムの異常を監視し、定期的にレビューする記録を残す。	複数ログを相関分析し、インシデントの防止及びインシデント発生時の対応が導き出せること
実運用の壁	「点検」は月次や週次	相関分析が可能な環境と、予兆及びインシデント発生の検知体制

ログ分析[4.4.3]：ログの取得と不審な認証の検知

管理策区分	ISMS A.8.15 (ログ記録)	SCS 4.4.3 (ログの確認・分析)
要求の核心	記録の保管と保護	**不審な認証試行を含むログの取得・モニタリング**
具体的アクション	事象ログを記録・保管し、改ざん防止の措置を講じる。	認証ログや外部アクセスを詳細分析し、侵害の予兆を月次で評価する。
実運用の壁	「念のための保管」	ログを取得するだけでなく、不審な認証試行を月1回以上モニタリングし、検知する必要性

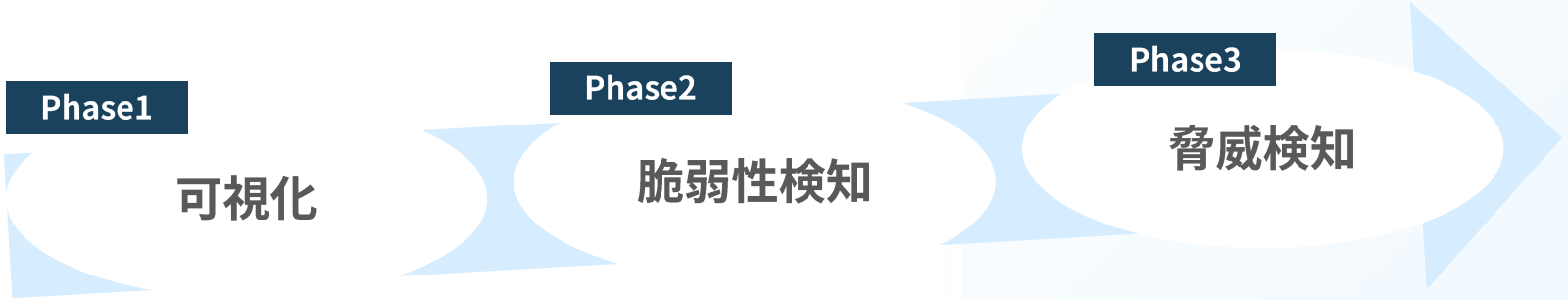
インシデント判断[5.2.1]：インシデントかどうかの分析と判断

管理策区分	ISMS A.5.25	SCS5.2.1 (インシデント分析・判断)
要求の核心	インシデントであるか判断する	**アラートのトリアージができること**
具体的アクション	セキュリティイベントを評価し、インシデントに該当するか判断する	不審な認証試行や機器/サービスのアラートを受けた場合、どのレベルのインシデントか分析し判断
実運用の壁	「インシデントかどうかの判断」	「どのレベルのインシデントか」まで判断

フォーカスすべき4つの評価項目

- 脆弱性を放置しないこと
- 能動的な分析をすること
- ”気づける”だけでなく、”切り分けと対応もできる”こと

「放置」を許さない運用の循環サイクル



具体的な内容	現在のインフラ環境にある設定不備やリスクを把握し、優先的に対処すべき課題を明らかにします	新たに発生する脆弱性や構成変化に継続的に気づける状態をつくります	侵入や不審な挙動を早期に捉え、被害拡大を防ぐための備えを整えます

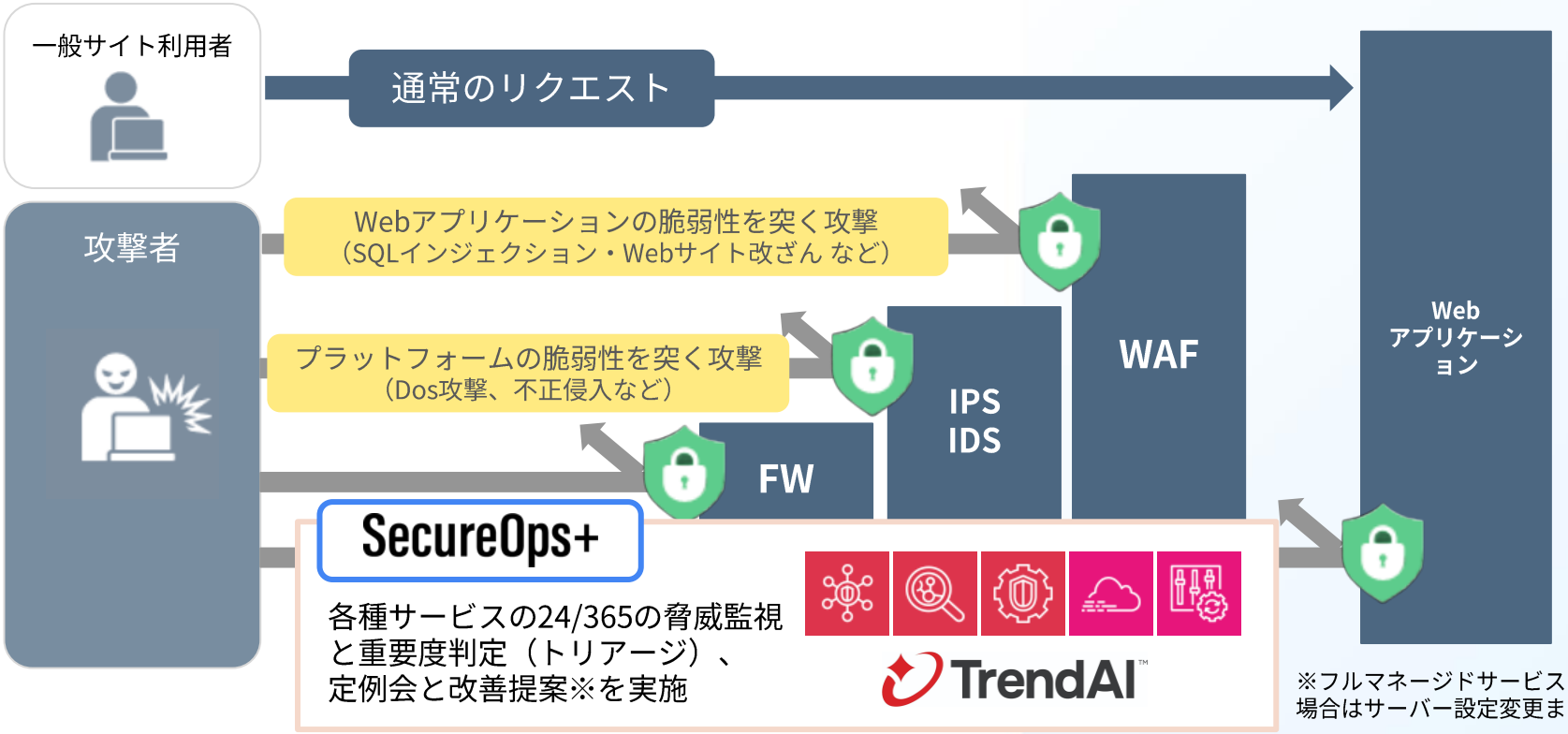
Chapter 4

ハートビーツのソリューション

判断と実務を「外部化」し、脆弱性を塩漬けにしない

セキュリティソリューション

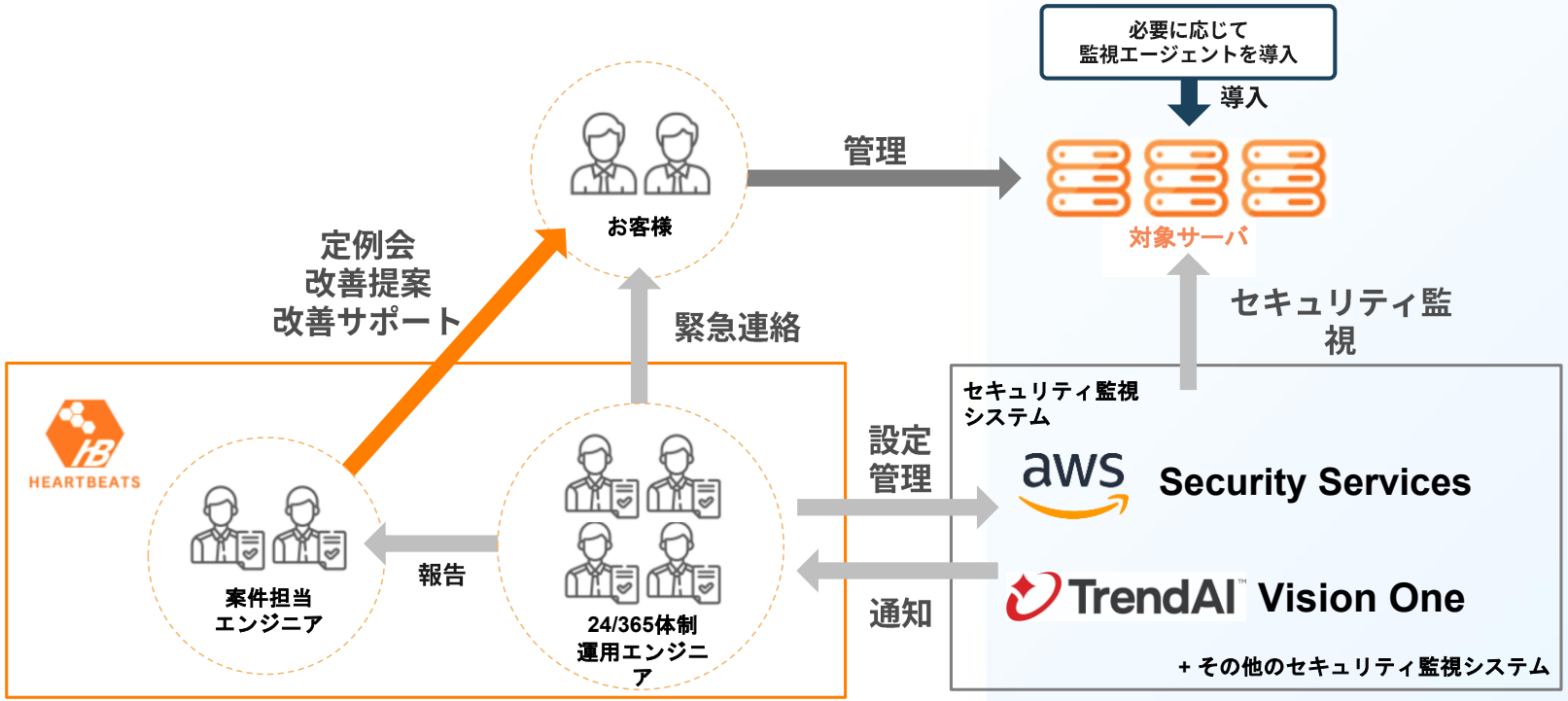
お客様のサービスやご要望に合わせて、WAFやIDS/IPS等の導入～運用などを最適にご提供します。
SecureOps＋では24/365で脅威を監視し、重要度判定と初動判断までお任せ頂くことが可能です。



※フルマネージドサービスご契約の場合はサーバー設定変更まで対応

SecureOps+

AWSのマネージドセキュリティサービス および **Trend AI VisionOne™** を利用したセキュリティ監視を行います。その他のツールを用いたセキュリティ運用も可能ですのでご相談ください。



「放置」を許さない運用の循環サイクル

資産の棚卸し

AWSネイティブ連携による
正確な構成把握

継続的スキャン

Inspector等による24時間の
穴探し

トリアージ/是正

専門家が判断し、
対応の緊急性を評価

証跡管理

★4審査に活用できる
運用レポート

モデルケース 1

■ 企業背景

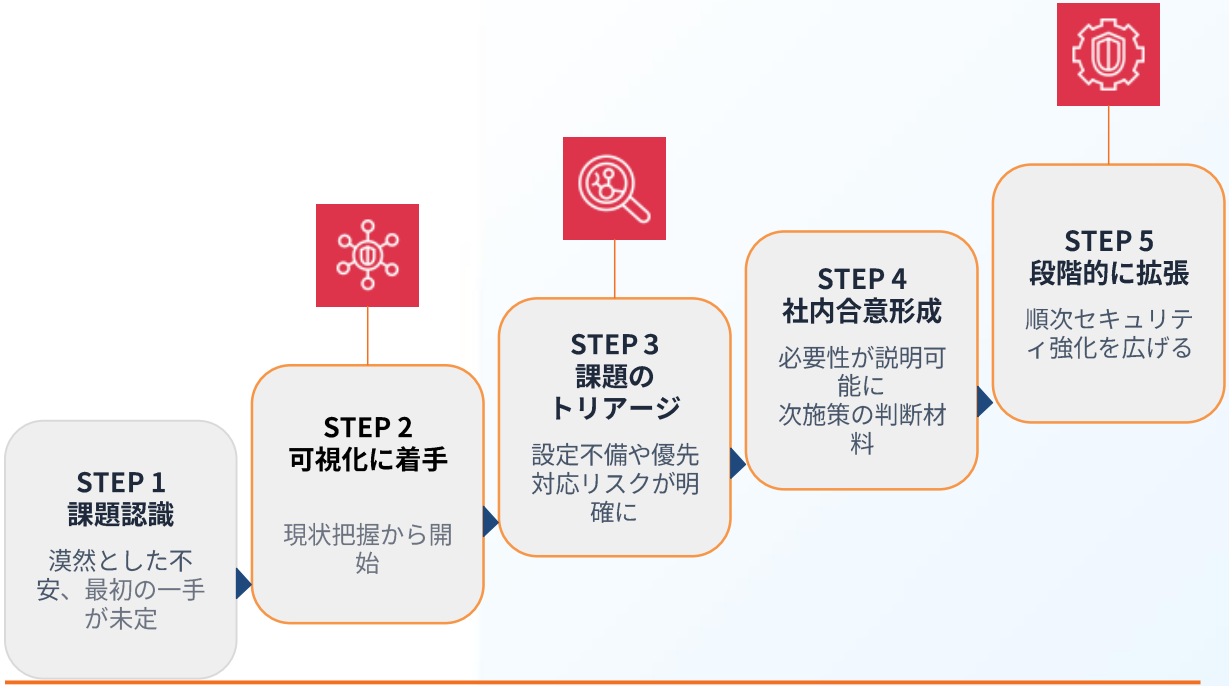
- ✔ 事業拡大に伴い、運用・統制の重要性が向上
- ✔ セキュリティ強化の必要性は認識していた

■ 当初の課題

① 何から始めるべきか不明

② 運用をどう回すかが不透明

③ 社内への説明が難しい



- 最初から網羅的に始めなくてもよい
- 可視化ができると、優先順位と社内説明の材料が揃う

モデルケース 2

■ 企業背景

- 脅威検知サービスは導入済み
- 検知は始めていたが運用が定着していなかった

■ 当初の課題

① 検知内容を精査しきれない

② 対応ルールが未整備

③ 脆弱性対策まで手が回らない

- 導入済みツールも、運用がなければ活かしきれない
- 検知の整理から始めて、段階的に対策を広げられる

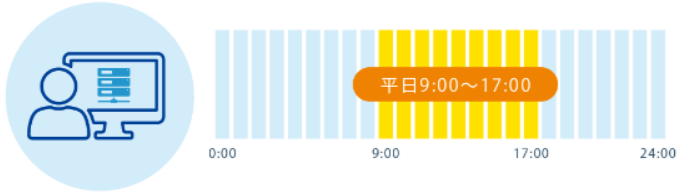
24時間365日少人数でも止まらない運用体制を実装する、フルマネージドサービス

フルマネージドサービス　インフラ兼任エンジニアも強力サポート

エンジニアの有人監視・一次対応

×

サーバー管理者代行業務



- **監視仕様書の作成、設計・構築**から対応
- **初動対応から弊社エンジニア**が対応
- **初期費用0円**。
- 対応回数で**費用変動なし**
- 障害検知から一次対応開始までを
  10分以内とするSLOを設定

- **障害の原因究明と対策、**
  各種アップデートの対応要否も判断
- インフラ運用における
  属人化・秘伝のタレ化防止に
- コスト最適化など、
  インフラ全体の改善策をご提案

監視一次対応サービス

・初期対応がエンジニアだから出来る柔軟な一次対応
・監視項目設定/手順書の作成/監視項目数の制限なし、実際の運用に即したサービスをご提供

	HEARTBEATS	A社	B社	C社
マルチクラウド対応	○	○	△ AWS,Google Cloud,Azureのみ	× AWSのみ
障害発生時の一次対応	**エンジニア対応**	オペレーター対応	オペレーター対応	外部会社へ委託
初期費用	**0円**	60,000円～	20,000円～	0円
監視項目の策定、カスタマイズ	○	△ 別途オプション	×	×
監視手順書の作成	○	○	お客様がご用意	お客様がご用意
監視項目数	**無制限**	追加別途費用	制限あり	制限あり

※24時間365日での有人監視を提供する他社群との比較

まとめ

放置をゼロにする
脆弱性公開から是正までのタイムラグを最短化し、攻撃の窓を閉じる。

証跡を積み上げる
ISMSのような「規程」だけでなく、日々の「運用事実」をレポート化する。

監視で穴をカバーする
即時の是正が困難な箇所は、予兆の検知と対応フローの整理でリスクを担保する。

専門家と伴走する
自社リソースを「本来の事業」に集中させ、運用はパートナーに委ねる。

脅威や脆弱性に”気付ける”だけでなく、
優先度も含めた脅威や脆弱性の”見える化”をハートビーツが実現します

導入事例

事例紹介

ネットイヤーグループ株式会社様

事業内容	デジタルマーケティング支援 Web・アプリ企画制作／システム開発
導入製品	フルマネージドサービス セキュリティ導入支援・運用
利用開始	2020年3月～

災害時・繁忙期にも、安定して情報を届ける 24/365止まらない羽田空港Webサイトを実現

背景

- 羽田空港は公共性が高く、災害時や交通機関の乱れでアクセスが急増しやすかった
- 24時間365日止まらない運営を維持するため、監視・運用体制の負荷が大きかった
- 「つながらない」状況は利用者の不安に直結するため、可用性確保が最優先だった

導入結果

- 災害時や繁忙期でも、サーバーダウンなく**安定して情報提供できるように**
- 夜間・休日のアラート対応から解放され、**本来業務に集中できるようになった**
- 大型台風時のアクセス急増も**迅速に検知・共有し、対応できた**
- 2025年のDDoS攻撃時も、**サーバーを落とさず稼働を継続できた**

事例紹介

株式会社システムアイ様

事業内容	デジタル改善支援サービス
導入製品	フルマネージドサービス AWS請求代行サービス
利用開始	2021年12月～

運用監視体制を強化し、顧客へ開発～保守まで一貫したサービス提供を実現

背景

- 顧客ニーズの拡大により運用監視の案件が急増
- 社内に24/365の運用体制がなく、開発提案に限界
- IT人材不足も重なり、運用・保守体制構築が困難だった

導入結果

- 24/365の監視・運用体制で**安心して任せられる体制を構築**
- 顧客システムの監視・保守まで**一貫した提案が可能に**
- ハートビーツがL1～L2まで柔軟対応し、**安定運用に貢献**
- 他社と比べて1/4でコストを抑えつつ・高品質な運用を提供でき、**顧客価値の拡大に寄与**

事例紹介

株式会社KaizenPlatform様

事業内容	デジタル改善支援サービス
導入製品	サーバー監視・一次対応サービス AWS請求代行サービス
利用開始	2024年7月～

頼れるパートナーに再び。
丁寧な対応で運用の安心を取り戻す

背景

- 過去、ハートビーツから一度他社に運用支援を乗り換えた
- しかしAWS IPv6移行後に監視が断続的に止まるトラブルが発生し、担当者の負担が増大していた
- 以前の監視委託先では質問への明確な回答が得られず不安が募った
- 他社請求代行はroot権限がなく、コスト最適化ができない状態だった

導入結果

24/365の有人監視で**監視停止の不安を解消**

技術者による 明確な回答・丁寧な対応 で**安心感向上**

監視・初動対応を任せられ、 **担当者負担が軽減**

AWS請求代行で **コスト最適化（root権限活用）** が可能に

事例紹介

テレ株式会社様

事業内容	音声通販サービス「テレAI」 ECカート「テレAIカート」
導入製品	サーバー監視・一次対応 サービス
利用開始	2024年10月～

属人化していたインフラ運用体制を解消し
開発チームの負荷を大幅軽減

背景

- 24時間稼働が前提のサービスを運営
- 少数精鋭の体制で、深夜・休日の障害対応がCTOひとりに集中
- 内製の夜間監視体制も検討したが、人件費やスキルの問題で断念
- 「ツールではなく、技術理解のある人が判断してくれる運用」を求めていた

導入結果

- 24/365の有人監視と初動対応により、**障害発生時のスピードと安心感が向上**
- CTOのオンコール業務が不要になり、**開発・リサーチへ注力可能に**
- 担当者の柔軟な判断・対応で**運用負荷が大幅に軽減**
- 請求代行サービスも導入し、**コスト削減にも成功**

事例紹介

株式会社インターナショナル
スポーツマーケティング様

事業内容	スポーツビジネス支援 会員管理・メディア運営など
導入製品	サーバー監視・一次対応サービス フルマネージドサービス AWS請求代行サービス
利用開始	2018年3月～

アクセス集中にも耐える柔軟な環境構築で、
安定したサイト運営を実現

背景

- 顧客向けにAWS含めたサービス提案・選定の判断が難しかった
- アクセス増加やイベント集中時の負荷を見越した構成の提案が必要
- インフラの技術検討・設定変更の負担が大きく、体制整備が課題だった

導入結果

- AWSサービス選定・見積作成のアドバイスにより**提案の幅が拡大**
- 余裕あるスペック確保で、スポーツイベント時の**安定運用を実現**
- 障害時の監視・一次対応・レポートまで一貫したサポートを受け、**運用負担が軽減**
- AWS請求代行で複雑な計算の負担が不要に、**請求関連作業も大幅軽減**

Appendix

AWSリセール (請求代行)サービス

AWSとの契約（アカウント発行/移管）から、アカウント管理/運用、サービス利用料のお支払い、
AWSへの技術的な問い合わせまでをお任せいただけるサービス。

導入メリット

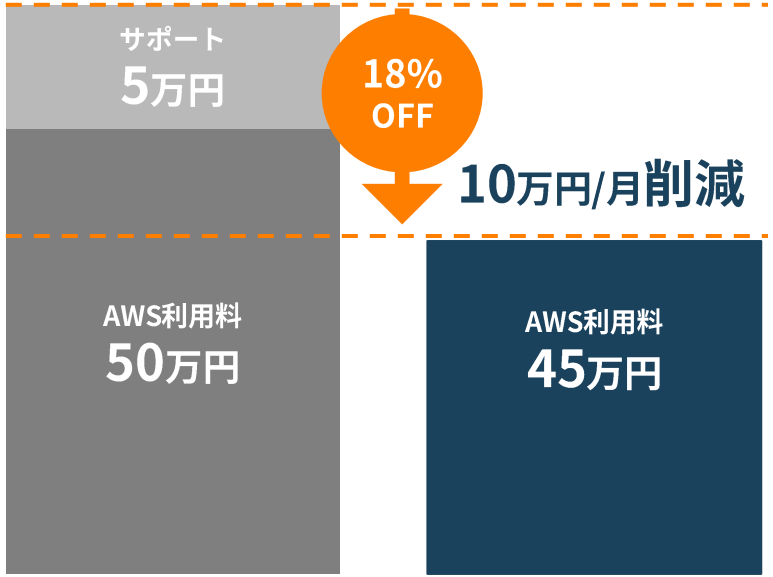
1 AWSコストが最大**18%OFF**※1
エンタープライズサポートプラン相当が**無料**

2 日本円でのご請求書発行
初期費用・代行手数料も0円

3 AWS構築/運用※2費用が、常に定価から**10%OFF**
Market Placeの特定製品が**5%OFF**

※1: 割引対象外のサービス（中国リージョン、 AWS Marketplace、Amazon Connect、 GovCloudなど）もございます。また月額$50,000以上ご利用している場合、個別のご提案となる可能性がございます。詳細は営業担当まで。
※2:フルマネージドサービス、監視一次対応サービスの新規ご契約が対象

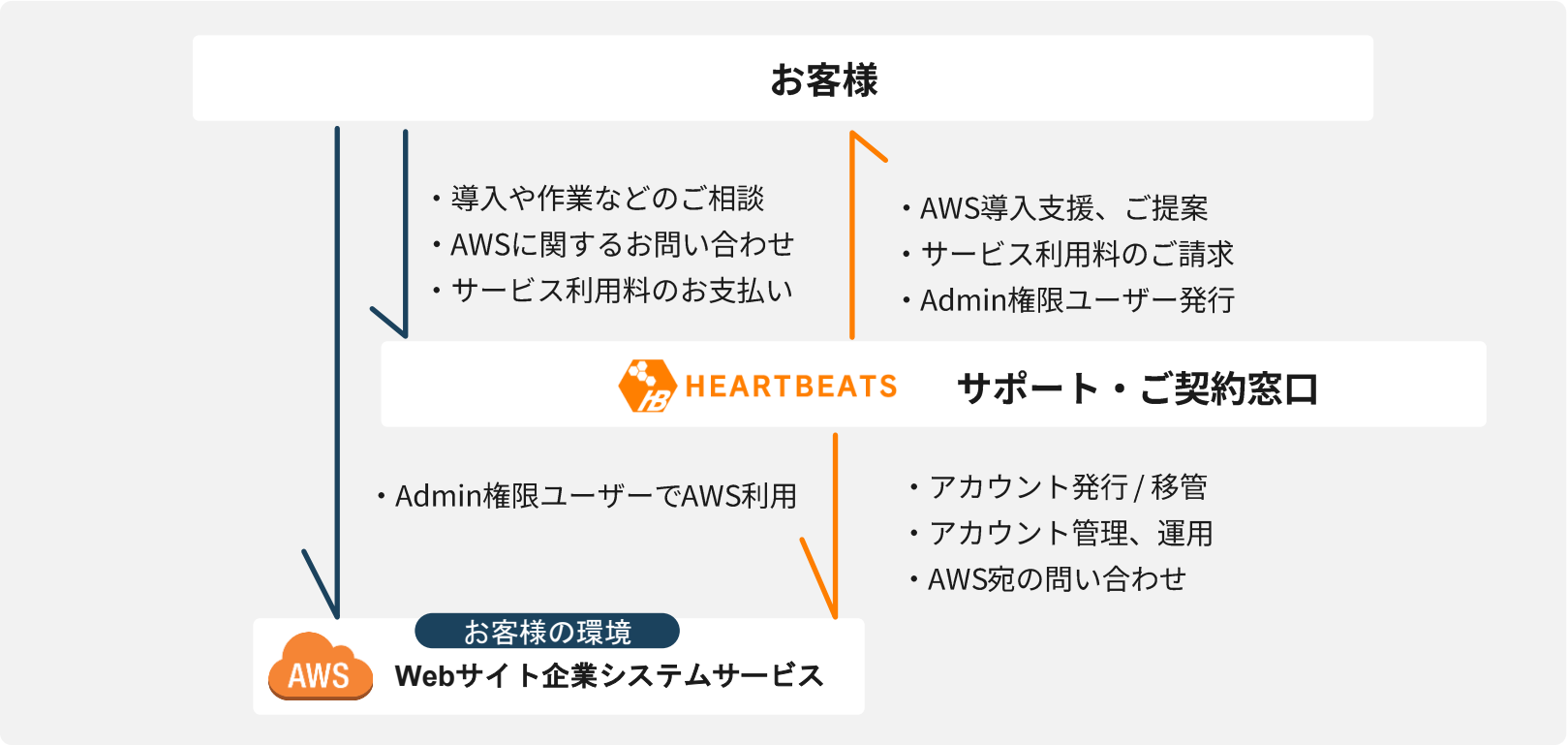
例）AWS利用料 50万円/月＋サポート5万円/月の場合



AWSリセール (請求代行)サービス / プラン

	シンプルプラン	Organizationsプラン	ダイレクトプラン	ダイレクト /Organizationsプラン
こんな方に	とにかく安く使いたい	AWSアカウントを一元化したい	AWS環境を自社でコントロールしたい	AWS環境を自社でコントロールし、アカウントを一元管理したい
AWS利用料割引	10%	5%	5%	3%
RI/SP購入	可能	ー	可能	可能
RI/SP割引	5%	ー	5%	3%
サポート費用	エンタープライズ相当無料		お客様負担	
サポート窓口	ハートビーツが24時間365日サポート ※原則、ハートビーツが一次問い合わせ窓口となります。		AWSが24時間365日サポート	
rootアカウント	ー	ー	○	○ ※支払いアカウントはハートビーツ
AWS Organizations AWS Control Tower	ー	○	ー	○
利用コストの確認	ハートビーツ発行の管理画面「WavePro」から		AWSコンソールから	

AWSリセール (請求代行)サービス / ご利用イメージ



※シンプルプラン、Organizationsプランの場合のご利用イメージ

AWS利用料割引の仕組み

AWSパートナーである当社が、お客様に代わりAWS利用料を一括して支払います。そこで受けられるボリュームディスカウントにより、お客様はパートナー割引適用の価格でAWSをご利用いただけます。

※シンプルプラン、Organizationsプランのみ対象です。他プランはサポート費用はお客様負担となります。

さくらのクラウド請求代行サービス

さくらのクラウドを弊社経由でお支払い頂くだけで、利用料が5%OFFでご利用頂けます。

導入メリット

1 さくらのクラウドコストが**5%OFF**※1

2 オンプレ・他クラウドからの移行、導入～運用、
セキュリティまで**1社完結でご支援可能**（オプション）

※1: 割引対象外のサービス（マーケットプレイス）もございます。
※ : 現在さくらのクラウドをご利用中のお客様は、さくらのクラウド内のプロジェクトの付け替えが必要になります。
譲渡における注意事項をご確認ください。

ホワイトペーパーのご紹介

ランサムウェア被害は、システム停止や復旧コストだけでなく、企業の信頼や事業継続にも大きな影響を及ぼします。
本資料では、攻撃の進行プロセスを整理しながら、クラウド環境でどの段階に何を備えるべきかを分かりやすく解説します。
AWS環境を例に、侵入防止・検知・復旧の各フェーズで押さえるべき対策と、運用で重要な視点を紹介。
さらに、少人数体制でも実践しやすい、事業を止めないためのセキュリティ運用の考え方もわかります。

ダウンロードはこちらから

ー　ご参加いただき、ありがとうございました。　ー

次回ウェビナーのお知らせ

お申し込みは
こちら