脆弱性診断の内製化を成功に導くAeyescan

～いつでもだれにでも診断できる環境をご提供～

Tokio dR

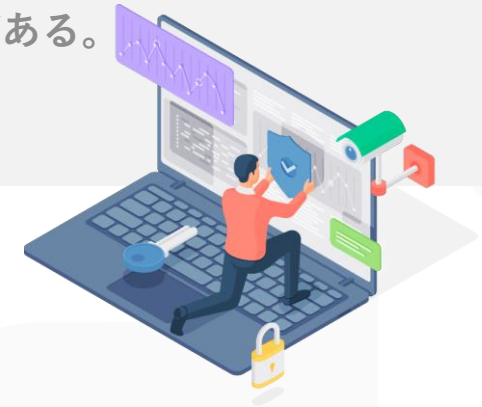
To Be a **Good Company**

東京海上ディーアール株式会社

脆弱性診断内製化のメリット

開発・CSIRT・リスクマネジメントの現場において、このような課題・要望がありませんか？

- セキュリティコードレビュー、テストに時間がかかり生産性が低下している。
- サイトの公開、リリースの事業状況にあわせて柔軟に脆弱性診断したい。
- コストが理由で脆弱性診断の実施を断念しているサイトがある。
- 脆弱性診断費用を抑えたい。



・・・

内製化で解決します。

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

内製化のパターン

脆弱性診断の内製化には大きく２つのパターンがあります。

セキュリティエンジニア

高度なセキュリティ技術をもった
エンジニアによる診断が可能な状態

担当者	診断の担当者を選任または、セキュリティベンダからの中途採用
ツール	様々な設定や制御が可能なツール。使いこなすには、ベンダートレーニングの受講が前提。
プロセス	関係者からの診断の依頼をもとに実施。
目指すゴール	セキュリティの専門知識をもったメンバーが、システムのセキュリティを評価するチーム

プロ向けツールで実現する内製化

セキュリティエンジニアではない人

だれでもいつでも診断が可能な状態

担当者	立場や利用頻度を問わず関係者全員
ツール	簡単な設定で自動化されたツール。教育不要
プロセス	システムのライフサイクルに自動的に組み込む。
目指すゴール	システムのライフサイクルに携わる全員が、セキュリティの役割を担う

DevSecOps

だれでも使えるツールで実現する内製化

内製化の課題は？

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

内製化におけるよくある課題

脆弱性診断の内製化に課題がありませんか？

自社で出来るか不安

導入前

ツールを導入したいがツールを使いこなせるか不安。使いこなすまでに時間がかかりそう。

導入後

担当者に属人化してしまう。 ツール操作者の熟練度によって脆弱性の検出率が異なる。

専任者が必要

導入前

要員計画の変更や、ツールのトレーニングが必要。

導入後

ツールを導入したが、操作に時間がかかり本来の業務と両立できない。育成期間やコストのため要員追加が困難。

診断項目が不足
レポートが分からない

導入前

脆弱性の対応項目が狭いため差分を埋める対応が必要。

導入後

レポートが難解なため脆弱性の修正対応が遅れる。何が問題か正しく把握できない。

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

選ばれる理由

内製化を実現し、セキュリティ対策にかかるコストを低減できます。

簡単操作

いつでも誰でも始められる

Webセキュリティの知識や、Webアプリの開発経験がなくても始められます。
マウス操作のみで、幅広い脆弱性を検出。
WordPressなどCMS固有の問題、
オープンポートの診断などにも対応。

業務の片手間で診断可能

自動化された脆弱性診断

SaaS環境なので24時間放置
AIによる自動操作によって最短10分で
診断可能。

業界標準の項目
わかりやすいレポート

わかりやすいレポート

業界標準の脆弱性診断項目と評価基準レポート。
画面遷移図の見やすいレポート。

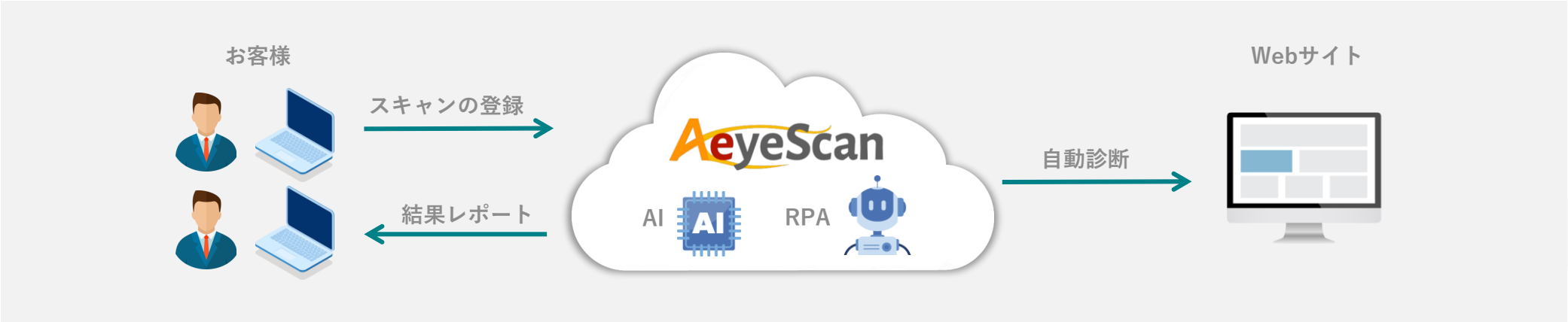
©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

Aeyescanとは

SaaS型のWebアプリケーション脆弱性診断プラットフォームです。

診断内製化に必要な、簡単・高精度な脆弱性診断を、
AI＋RPA (Robotic Process Automation)を活用し実現させます。



お手軽に診断を開始

高精度・レポートが分かりやすい

SaaS プラットフォーム共有

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

Aeyescanを使った診断の流れ

AeyeScanを使った脆弱性診断の流れに沿ってご説明します。

STEP01

ドメイン アクティベーション

- お客様管理ドメインであることを確認いたします
- 初回登録時のみ必要となります（2回目以降は不要）
- 有償オプションにて無効化（スキップ）可能です

STEP02

対象設定

- 対象ドメイン・ログイン情報の設定のみで完了
- 必要に応じて診断負荷・除外範囲・通知等を設定可能

STEP03

巡回・スキャン

- AIがブラウザを自動操作し巡回を行います
- スケジュール機能によりスキャン(開始・停止)を予約可能

STEP04

結果確認

- 画面遷移図により診断範囲を確認
- 結果一覧画面により検出脆弱性の一覧を確認可能
- 報告書をPDFでダウンロード可能

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

ドメインアクティベーション機能

診断対象ドメインがお客様管理であることを確認するための手続きです。

「サーバへのファイル設置」と「管理者メールによるURLリンク認証」の**2種類から選択可能**です。

※有償オプションにて本機能を無効化可能です

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

AIを活用したブラウザ操作と正確なフォーム入力値の推測

AIがフォームの入力内容を判断し巡回。**事前設定の排除と巡回範囲の拡大**を実現。

AIによるフォーム入力値の判断処理

フォーム画面（初期表示画面）

入力値の事前設定は不要

登録フォーム
姓名
郵便番号(ハイフンあり)
住所
電話番号(ハイフンあり)
メールアドレス
確認

フォームを自動認識しラベル化

登録フォーム
姓名
郵便番号(ハイフンあり)
住所
電話番号(ハイフンあり)
メールアドレス
確認

自動認識したラベル（赤枠）に応じ、適切な入力値を設定

姓名
姓名(カタカナ)
姓名(ひらがな)
姓
名
姓(カタカナ)
名(カタカナ)
姓(ひらがな)
名(ひらがな)

適切な入力値で正常遷移を実現

フォーム入力を間違えた場合、入力エラーとなり遷移不可で、診断が進まない。

フォーム入力後の画面（AIによる判断後）

適切な値を入力

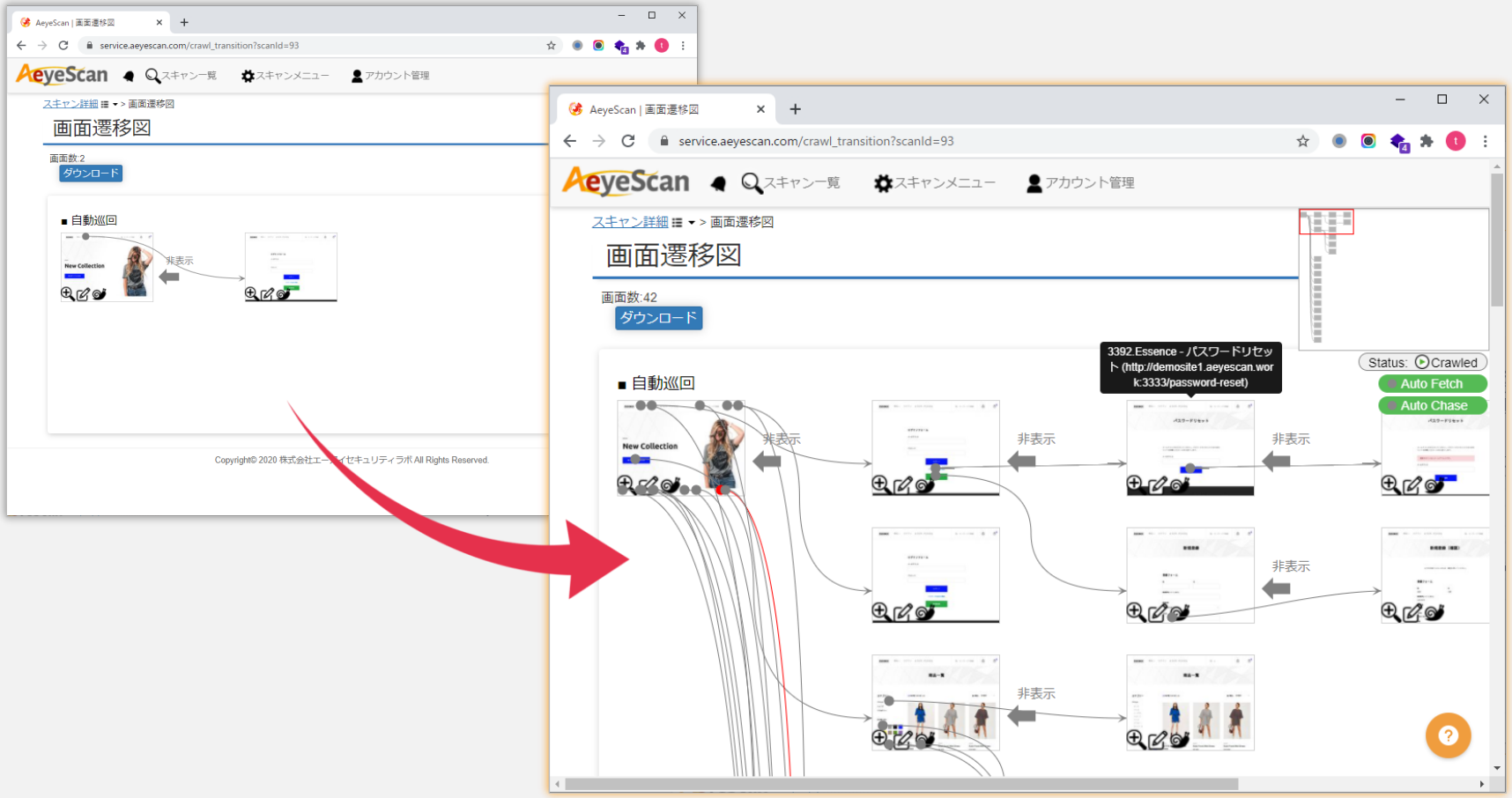
登録フォーム
姓名
巡回
郵便番号(ハイフンあり)
136-0076
住所
東京都江東区南砂１－１－１
電話番号(ハイフンあり)
03-1111-1111
メールアドレス
taro@exmaple.com
確定

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

自動巡回機能

自動巡回時に、**自動的に画面遷移図**を生成



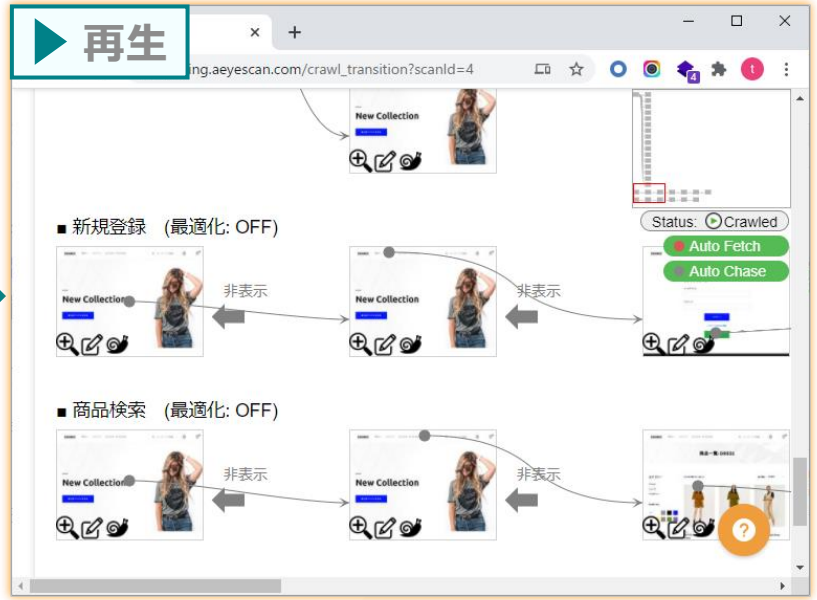
©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

手動巡回機能

機能修正を行った少ない画面を素早く確認したい、またはAIが巡回できない画面も簡単に診断が可能。

ブラウザの操作履歴を記録し再現することで複雑な設定方法を排除



ここがポイント

- **特定範囲のみの診断を実現**
  自動巡回の弱点である、診断対象の特定・限定を実現し、より柔軟な診断の実施が可能となります
- **スキャン設定不要**
  ブラウザで記録した操作内容をインポートするだけでスキャン設定が完了します。

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

業界標準の幅広い脆弱性に対応

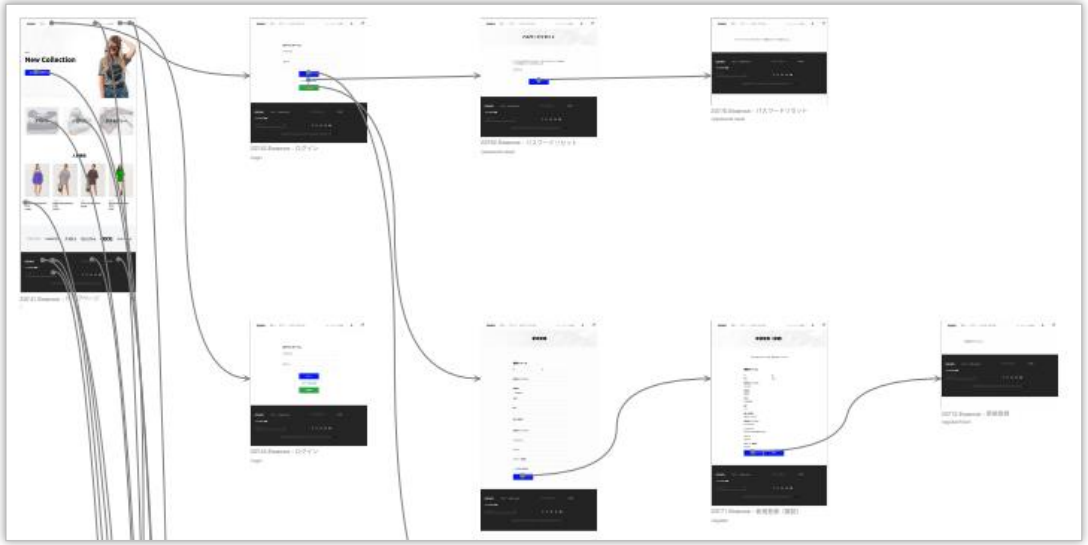
OWASP top10項目	診断項目（代表例）
A1-インジェクション	OSコマンドインジェクション・SQLインジェクション・SMTPヘッダインジェクション
A2-認証の不備	ログインIDの漏洩・セッションフィクセーション
A3-機微な情報の露出	クレジットカード番号の表示・パスワード入力欄のマスク不備
A4-XML 外部エンティティ参照 (XXE)	XML外部実体参照
A5-アクセス制御の不備	パストラバーサル
A6-不適切なセキュリティ設定	強制ブラウジング（ディレクトリリスティング・不要ファイルの公開）・ 製品情報の表示・機微情報の平文送信
A7-クロスサイトスクリプティング (XSS)	クロスサイトスクリプティング・DOMベースクロスサイトスクリプティング
A8-安全でないデシリアライゼーション	安全でないデシリアライゼーション
A9-既知の脆弱性のあるコンポーネントの使用	脆弱なWordPressの利用・脆弱なJavaScriptライブラリの利用
~~A10-不十分なロギングとモニタリング~~	Webアプリケーションの脆弱性ではないため対象除外
その他	PHPファイルインクルージョン・オープンリダイレクト・クロスサイトリクエストフォージェリ・サーバサイドリクエストフォージェリ

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

見やすいレポート

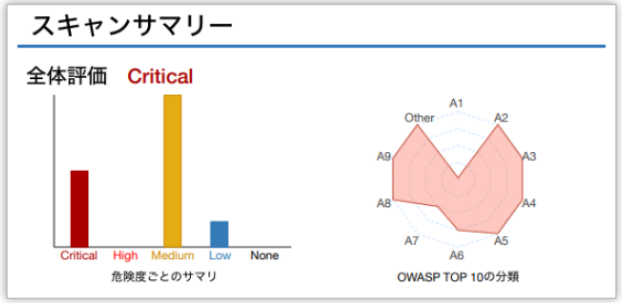
ここがポイント

画面キャプチャを取得し、画面遷移図としてご提供いたします。
また、遷移は押下したボタン位置をポイント



ここがポイント

全体の状況が一目でわかるレポート



ここがポイント

画面キャプチャや修正に必要な技術的な詳細情報も表示

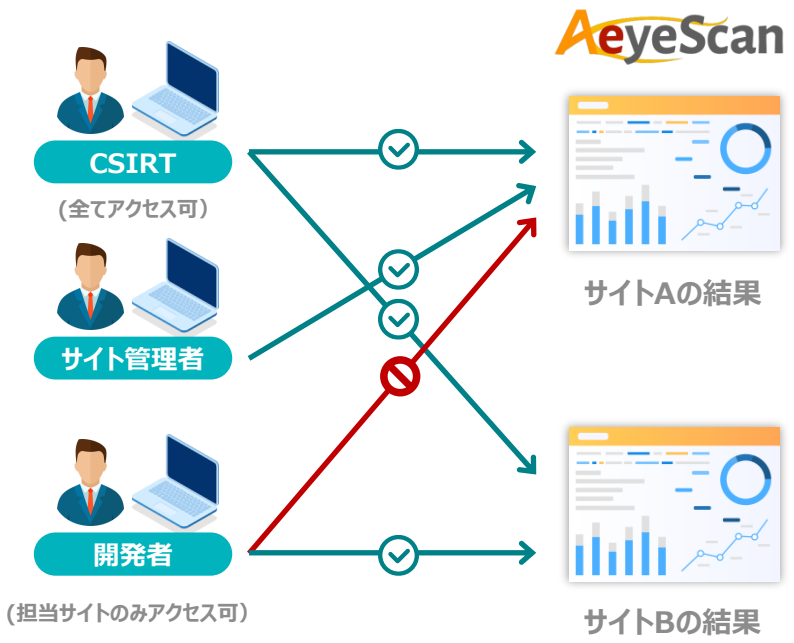
©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

役割・権限に応じたアカウント設定が可能

グループ設定と役割設定により、**一元管理された結果と詳細な権限設定**が可能

グループ設定によるサイト毎のアクセス権限設定が可能



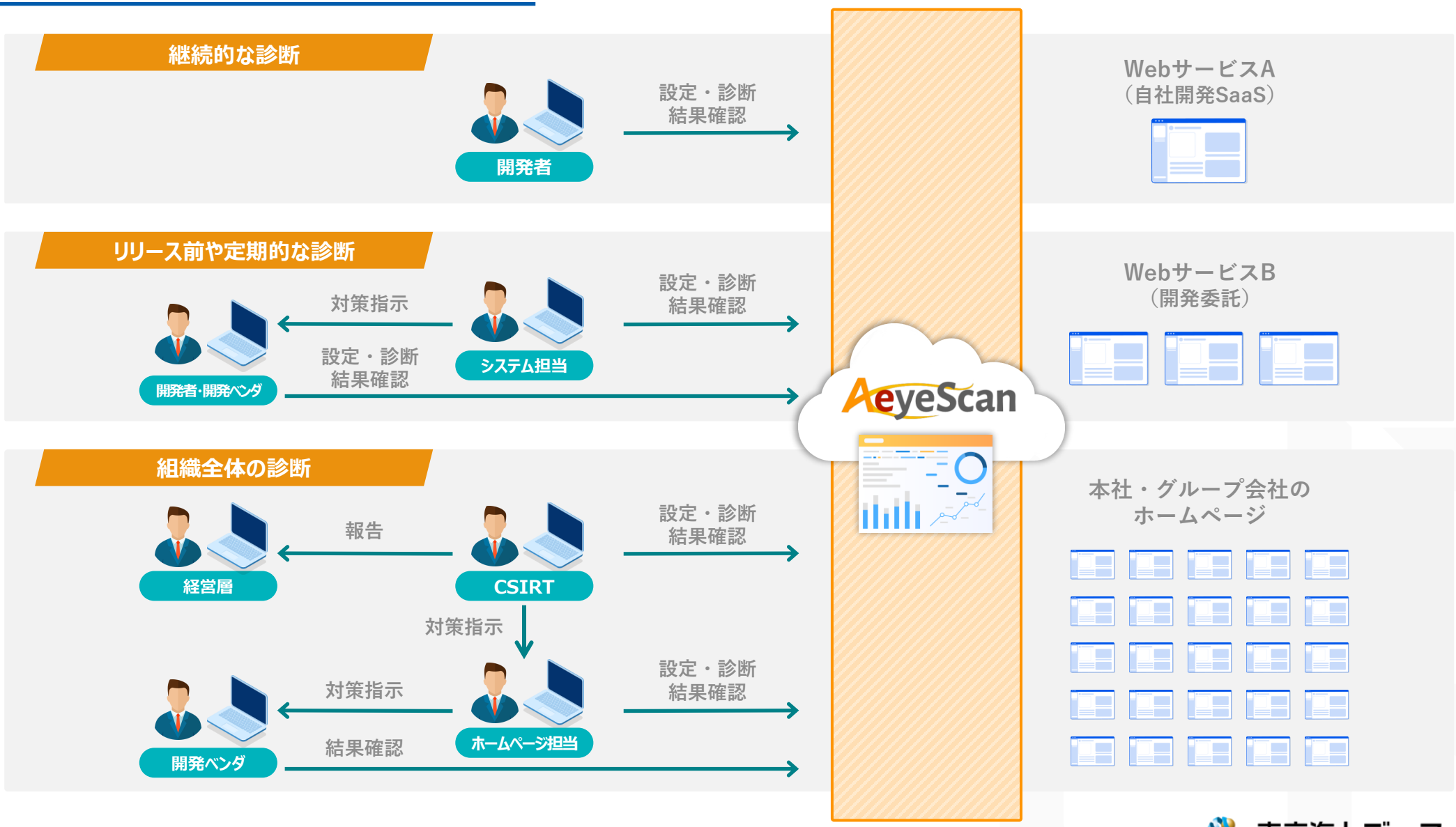
役割に応じた実行権限設定が可能

	CSIRT セキュリティ担当者	サイト管理者・開発者	パートナー
管理権限	●	○	○
実行権限	○	●	○
閲覧権限	○	○	●

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

プラットフォームとしての活用方法



©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

よくある質問

Q 内製化を検討すべきタイミングはいつですか？

A 企業規模やサイトのリリースタイミングに関わらず出来るだけ早い段階で検討を行うことで、手戻りを少なくすることができます。

Q 内製化を検討すべきサイト数は？

A 1サイトから検討可能です。1サイト向けの短期間のライセンスのご提供もございます。

Q SaaSのアクセス元IPアドレスは固定ですか？

A 固定IPアドレスです。IPアドレスを制限されている場合は許可してください。

Q サイトの所有者や責任範囲で診断対象に制限はありますか？

A 御座いません。対象サイト責任者の方の許可を頂ければご契約者様管理外のサイトのスキャンも可能です。

Q 診断を行えないサイトはありますか？

A Chromeでアクセスできないサイト、インターネットからアクセスできないサイトは診断を行うことが出来ません。その他、お客様の環境の適合性について是非ご相談ください。

Q シグネチャ更新頻度は？

A 1ヶ月に1回の追加・性能向上の見直し。緊急時は随時対応しております。

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

ご利用プラン

ホームページ・特定プロジェクト向け ←→ 複数サービス・開発部門・全社利用向け

ご利用プラン	Starter for Homepage	Starter for Development	おすすめ Business	Enterprise
スキャン可能FQDN数	1	1	無制限	無制限
同時実行数	1	1	1～	無制限
スキャン可能回数	1回	1回	無制限	無制限
アカウント数	5	5	30	無制限
ログイン機能、手動巡回機能対応	×	○	○	○
利用期間	30日	30日	1年間	1年間

オプション	Starter for Homepage	Starter for Development	おすすめ Business	Enterprise
アクティベーションスキップ	(追加不可)	(追加不可)	○	ー(不要)
同時実行数追加			○	○
プレミアムサポート			○	○

料金はお問い合わせください

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

ご利用の流れ

STEP 1	お問い合わせ	営業担当までお問い合わせください。
STEP 2	ヒアリング	お客様の現状や課題感を担当者がヒアリングいたします。 打ち合わせの日時についてご連絡をいたします。
STEP 3	プランのご提案	お客様の課題に対して最適なプランをご提案いたします。
STEP 4	契約・利用開始	申込書のご記入をもって利用開始となります。 導入から運用まで専任の担当者が継続的にサポートいたします。

©2021 Tokio Marine dR Co., Ltd. All rights reserved.

東京海上ディーアール株式会社

「事故や災害の悲しみや苦しみを、世の中からなくしたい」

わたしたちは、一世紀余にわたる東京海上日動火災保険と東京海上日動リスクコンサルティングの貴重な経験と豊富な実績を母体に、東京海上ディーアールとして新たに誕生いたしました。
わたしたち東京海上ディーアールは、デジタル技術を駆使してリスクを的確に解決するエキスパート集団として、皆様に寄り添い、様々な社会課題に挑戦していきます。

「dR」にこめた思い

リスク領域で培った膨大な知見に併せて、データ(**d**ata)・デジタル(**d**igital)・デザイン(**d**esign)の「**d**」を通じて、不確実性の高まるこの社会に対する私たちの新しい提供価値である「**R**」を達成していき、ひいては保険会社グループそのもののあり方を再定義していくこと。わたしたちはこれらのビジョンを、常にお客様に寄り添いながら、リスク対策の「ラストワンマイル」を提供する「リスクソリューションパートナー」としてのサービスを通じて実現していきます。

Tokio dR

名称 ： 東京海上ディーアール株式会社（略称：TdR）
英文名 *Tokio Marine dR Co., Ltd.*
所在地 ： 〒100-0004 東京都千代田区大手町1-5-1
大手町ファーストスクエア ウェストタワー23F
創立 ： 1996年8月1日
2021年7月1日 東京海上ディーアールに社名変更
会社HP ： https://www.tokiorisk.co.jp/

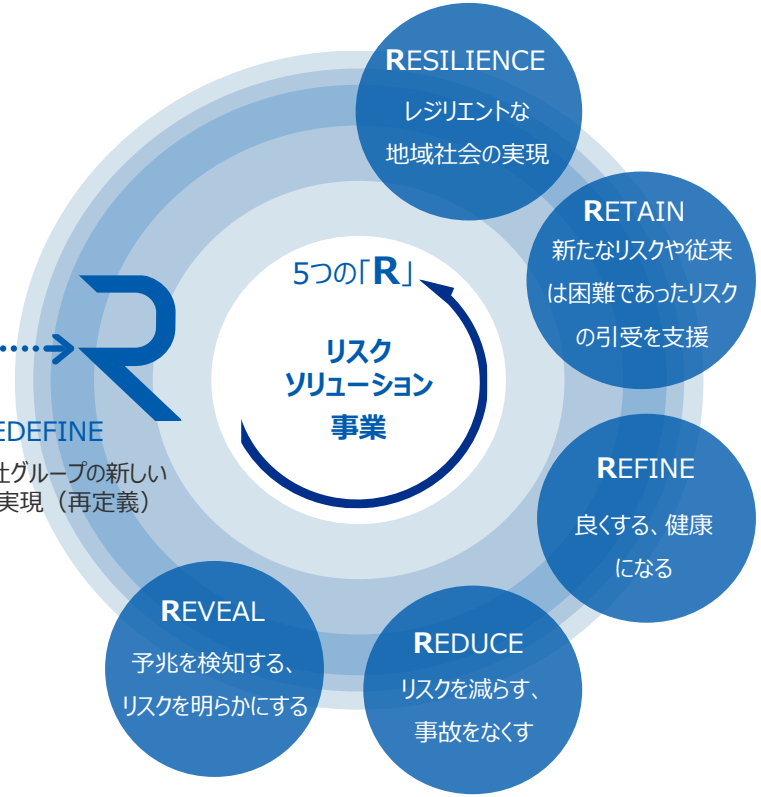
3つの「d」

data
プラットフォーム構築
高度なデータ分析体制の構築

digital
最先端テクノロジーや
IoTデバイスの研究・活用

design
アジャイルな開発実装体制

REDEFINE
保険会社グループの新しい
あり方の実現（再定義）



ご高覧ありがとうございました。
ご検討の程、何卒よろしくお願い申し上げます。

Tokio dR

お問い合わせ先：
東京海上ディーアール株式会社
サイバーセキュリティラボ
榎本　祐樹
Email：yuki.enomoto@tokiorisk.co.jp
Phone: 050-3380-6143