RiskScope

お問い合わせ ›

現場から生まれたセキュリティ対策

セキュリティ情報を次の行動に変える。

自社環境に関連する脅威だけを抽出し、
優先度と推奨アクションを提示する
セキュリティ・インテリジェンス・プラットフォームです。

情報収集から検索、証跡生成までをシンプルに。
ISMS Annex A.5.7（脅威インテリジェンス）対応を支援。

お問い合わせ ›

セキュリティ担当者が直面する現実

01

情報の過不足

セキュリティニュースや脆弱性情報など、多くの情報が溢れる中で、担当者が「自社に関係あるもの」を判断することが難しい。
結果として、本当に優先すべきリスクの見極めが遅れ、対応の判断に迷いが生まれる。

02

優先順位付けの難しさ

収集した情報をもとに、何から対応すべきか判断する基準が明確でない。
そのため、現場ではすべてが重要に見え、優先順位が曖昧なまま対応が進んでしまう。

03

証跡作成の手間

ISMS準備や運用における、監査のための記録・説明資料の作成に多くの時間がかかる。
手作業による調査と整理が負担となり、本来のセキュリティ対策に使える時間が削られてしまう。

このような状況が続くと意思決定は属人化し、組織としてのセキュリティ成熟度が上がりません。

RiskScope導入で実現すること

情報の混乱をなくし、判断と実行が進むセキュリティ運用へ。

判断スピードの向上

自社環境に関連する脅威だけが整理されることで、
「何を確認すべきか」「対応が必要かどうか」の判断が迅速になります。
情報収集に費やしていた時間を削減し、意思決定を加速します。

無駄な情報確認の削減

優先順位の明確化

収集された情報は分析され、対応優先度と推奨アクションが提示されます。
「全部重要」に追われる状態から脱却し、
限られたリソースを本当に重要な対策に集中できます

プロセスの標準化

監査・報告負担の軽減

分析結果はレポートとして整理され、
社内報告やISMS対応の証跡として活用可能です。
運用と記録を一体化することで、監査対応の準備工数を削減します。

PDF出力・証跡管理

RiskScopeでセキュリティ情報を「行動」に変える

RiskScopeは単なる情報収集ツールではありません。
自社環境に関連する脅威を抽出し、優先順位と推奨アクションまで提示する
セキュリティ・インテリジェンス・プラットフォームです。

セキュリティ情報を整理し、意思決定を最適化

Riskscopeは大量のセキュリティニュースや脆弱性情報の中から、
数分で自社に関係するものだけを抽出。
分析・優先順位付け・推奨アクションの提示、レポート生成までを
一体化します。

自社に関係する脅威だけを抽出
大量のセキュリティ情報から、業種・環境・利用サービスに関連するものを自動整理。

インテリジェントな優先順位付け
戦略的目標に基づき、最も重要なタスクを自動的にハイライト

証跡生成までシンプルに
収集・分析・レポート化を一体化し、ISMS Annex A.5.7対応を支援。

RiskScopeの使い方

STEP 1

自社のIT資産をプロファイル登録

自社の業種、利用しているクラウドサービスやセキュリティ製品、ネットワーク構成などの情報を登録します。

STEP2

セキュリティ情報をAIで収集・分析

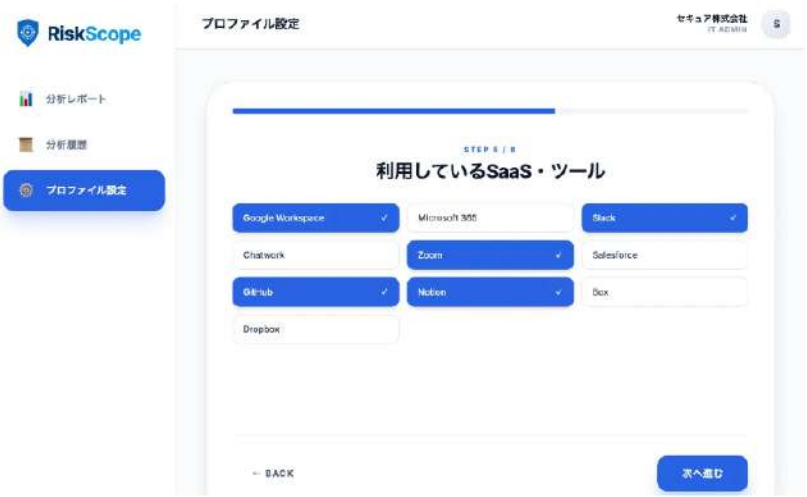
脆弱性情報やセキュリティ関連の情報源からAIで最新情報を収集し、自社環境との関連性をもとに整理・分類します。

STEP3

推奨アクション提示、レポート生成

収集・分析された情報は、優先度や推奨アクションとともに提示され、担当者が次に取るべき行動を明確にします。結果はレポートとして整理され、社内共有やISMS運用における証跡として活用できます。


RiskScope
分析レポート
分析履歴
プロファイル設定
プロファイル設定
セキュア株式会社
IT ADMIN
S
STEP 1 / 8
事業内容を教えてください。
医療・ヘルスケア
キャンセル
次へ進む


RiskScope
分析レポート
分析履歴
プロファイル設定
プロファイル設定
セキュア株式会社
IT ADMIN
S
STEP 6 / 8
利用しているSaaS・ツール
Google Workspace
Microsoft 365
Slack
Chatwork
Zoom
Salesforce
GitHub
Notion
Box
Dropbox
← BACK
次へ進む


RiskScope
分析レポート
分析履歴
プロファイル設定
分析レポート
セキュア株式会社
IT ADMIN
S
16%
リスク分析を実行中
ITプロファイルと最新の脅威情報を照合し、依頼別リスクを評価しています。
最新の脅威データベースを照合中...
分析を中止する


RiskScope
分析レポート
分析履歴
プロファイル設定
分析レポート
セキュア株式会社
IT ADMIN
S
セキュリティ分析レポート
対象業界: 医療・ヘルスケア
2026/02/25 05:41:20
PDF出力
再分析
セキュリティ動向
2026年初頭、医療・ヘルスケア業界はかつてないサイバー脅威の波に直面しています。特に、貴社の開発スタックの中核であるNext.jsおよびReactエコシステムにおいて、CVSSスコア10.0の極めて深刻なリモートコード実行（RCE）脆弱性「React2Shell」が発見され、活発な悪用が確認されています。これはWebアプリケーションの根本を揺るがすリスクです。インフラ面では、Google Cloud（GCP）やGitHub Actionsを標的としたサプライチェーン攻撃が高度化しており、CI/CDパイプラインへの侵害や、Terraform状態ファイルの不適切な管理による機密情報漏洩が懸念されます。さらに、医療機関を狙ったランサムウェア攻撃（Qilin、SAFEPAY等）は、単なるデータの暗号化から、二重脅迫、さらには患者の生命に関わるシステム停止を引き起こす手法へと進化しています。SaaS利用においては、AI機能（Shadow AI）の無秩序な利用によるデータ流出リスクも新たな課題として浮上しています。組織全体として、既知の脆弱性への即時パッチ適用と、サプライチェーン全体の信頼性検証が急務です。
推奨アクション
分析レポート
セキュア株式会社
IT ADMIN
S
推奨アクション
最優先事項として、ReactおよびNext.jsフレームワークのバージョンを確認し、脆弱性「React2Shell」に対する修正パッチを即時に適用する必要があります。並行して、GitHub Actionsのワークフローで使用されているサードパーティ製アクションの監査を行い、バージョンを固定化することでサプライチェーン攻撃のリスクを低減させてください。また、中長期的な視点では、Terraformの状態管理（State file）におけるアクセス制御と暗号化の徹底、およびGoogle WorkspaceやSlack等で利用されるAI機能に関するセキュリティポリシーの策定と監視プロセスの確立が不可欠です。ランサムウェア対策としては、オフラインバックアップの定期的な検証に加え、Google Cloud Identityを活用した堅牢な多要素認証（MFA）の適用範囲を全ユーザーに拡大することを推奨します。
7
10
9
NEXT.JS / REACT FRAMEWORK
Next.jsおよびReact関連パッケージを修正済みバージョンへ即時アップグレードしてください。
WAF | CLOUD ARMOR
WAFルールによる攻撃リクエストの遮断設定を追加してください。
分析レポート
セキュア株式会社
IT ADMIN
S
検知アラート詳細
12
10
3
2025-12-03
100%
NVD / GITHUB ADVISORY DATABASE
【緊急】React/Next.jsにおけるRCE脆弱性「React2Shell」
詳細を検索
2026-02-02
98%
NCI (NHS CYBERSECURITY COORDINATION CENTER)
医療機関を標的としたランサムウェア攻撃の激化 (Qilin, SAFEPAY)
詳細を検索
2026-01-28
95%
GITHUB ADVISORY DATABASE | NETLIFY
2026-01-01
CISA / WIZ RESEARCH
92%
GitHub Actionsにおけるサプライチェーン攻撃

01

他のセキュリティツールとの違いは何ですか？

多くのツールが「情報提供」に留まる中、RiskScopeは自社環境に基づいた関連性判断、優先順位付け、推奨アクション、レポート生成までを一体化しています。情報収集から意思決定までを支援する点が特徴です。

02

導入や設定は難しくありませんか？

基本的な設定は数分で完了します。自社環境のプロファイルを登録するだけで、関連情報の収集と分析が自動的に開始されます。専門的なセキュリティ知識がなくても利用可能です。

03

自社のセキュリティ情報が外部に漏れることはありませんか？

RiskScopeでは、必要最低限のプロファイル情報のみを利用し、機密性の高い内部情報の登録は不要です。登録された情報は暗号化された通信および安全な環境で管理され、外部公開や第三者提供は行いません。

また、本サービスは「自社に関連する可能性のある脅威情報の抽出」を目的としており、内部構成や詳細なセキュリティ情報を外部に送信する設計ではありません。安心してご利用いただけます。

04

ISMSを取得していなくても利用できますか？

はい、ISMS未取得の企業でも問題なく利用できます。日々の情報収集やリスク把握を効率化することで、結果的にISMS Annex A.5.7（脅威インテリジェンス）への対応基盤としても活用できます。

共に広げるパートナーを募集しています

- 共同開発・技術連携パートナー
- 販売・導入支援パートナー
- 業界特化モデルの共創パートナー

お問い合わせ ›