

CYBER RESILIENCE × SCS CERTIFICATION

強靱なサイバーレジリエンスを 構築・証明するクラウド基盤

「防ぐ」だけでなく「耐え抜く・回復する」力を診断し、
SCS格付取得までの最短ロードマップを自動生成。経営層への報告書も即座に完成します。

Grade S～D

6段階のセキュリティ評価

最短5分

アカウント開設～診断開始

157要件

SCS全要件に自動対応

専任不要

IT担当者なしで導入可

サイバーセキュリティ対策の考え方を転換する

中小企業のための「止めない経営基盤」としてのレジリエンス（復旧力）

🏢 大企業の考え方：予防に多額の投資

EDR / XDR

SIEM / SOC

脆弱性管理

教育・訓練

多額のセキュリティ投資を行い、「攻撃を受けない会社」を目指すアプローチ。

しかし、攻撃を100%防ぐことは現実的ではなく、中小企業が追随するのは資金的・人材的に困難です。

💡 KEY CONCEPT 中小企業の考え方：最低限の予防 + 強力な復旧

最低限の予防（必須）

- ✓ OS・ソフト自動更新
- ✓ MFA（多要素認証）
- ✓ 統合メールサーバーセキュリティ

攻撃を受けた後の体制（サイクル）

早期検知 → 初動対応



早期復旧 → 事業再開 → 再発防止

この両方を RASHIN が完全にカバーし、対策ロードマップとして提示します

「風邪をひかない会社」ではなく、「風邪をひいても翌日には仕事ができる会社」へ

セキュリティ業界における「RASHIN」の位置付け

EDR・SIEM等の技術対策とは競合しない、自走と伴走を両立するガバナンス基盤



復旧力を支える鍵 — ゼロトラスト

侵入されることを前提とし、認証基盤を強化して被害範囲を最小化する設計思想

01

認証基盤の強化

ゼロトラストの最優先要諦。多要素認証や端末ログイン制御を徹底。

02

被害範囲を極小化

権限の最小化とアカウント分離により、1アカウントの被害から他システムへの侵入を防ぐ。

03

復旧スピードの向上

被害箇所が特定されているため、迷うことなく早期にバックアップから復元が可能。

04

事業停止リスクの低減

事業停止期間（ダウンタイム）を最小限に抑え、致命的な経営損失を完全に回避。



セキュリティ診断

設問に回答するだけでGrade S～Dと想定被害額を自動算出



対策ロードマップ

診断結果に基づき優先度・担当者付きのタスク一覧を自動生成



財務リスク定量化

インシデント被害額を3項目に分解。対策効果を数値で可視化



チャット相談

専門家への相談がチャットで完結。規程雛形の提供も対応



SaaS認証リスク分析

各SaaSのMFA・SSO設定状況をスコア化しリスクを一覧表示



規程・ポリシー生成

SCS要件準拠の規程文書を自動生成。審査提出用に出力可

オプション



SCS格付取得シミュレーター

★3/★4取得に必要な残要件数と充足率をリアルタイム表示。申請証跡PDF出力まで一気通貫でサポート

オプション

SCS格付制度 完全対応

経産省「サイバーセキュリティ格付制度（SCS）」対応

★3/★4の全要件をRASHINタスクに自動紐付け。可視化から申請証跡出力まで一気通貫でサポート。

- 複雑な要件の噛み砕き：専門用語の多いSCS要件を、自社で実行可能なタスクレベルまで翻訳します。
- 申請プロセスの短縮：規程・ポリシー自動生成により、審査に必要なドキュメント準備の手間を削減します。
- 取引先への信頼証明：取得したSCS格付は、サプライチェーンセキュリティ要件をクリアする武器になります。



SCS ★3



SCS ★4

初期診断ウィザード

利用中のシステムや情報資産を対話形式で選択するだけで、自社のセキュリティ実態と課題を自動抽出。

セキュリティ診断ウィザード

データ保存先

SaaS / クラウドサービス

利用サービスを選択...

ベンダー側のバックアップ体制

ベンダー標準バックアップあり

バックアップ・保全設定

1次バックアップ

クラウド同期

2次バックアップ

未設定

データ保存先

SaaS / クラウドサービス

給与奉行

ベンダー側のバックアップ体制

ベンダー標準バックアップあり

バックアップ・保全設定

1次バックアップ

未設定

2次バックアップ

未設定

財務諸表・決算データ

改ざん・消失時の事業停止リスク大。

C:2 I:3 A:3

データ保存先

SaaS / クラウドサービス

勘定奉行

ベンダー側のバックアップ体制

ベンダー標準バックアップあり

バックアップ・保全設定

1次バックアップ

クラウド同期

2次バックアップ

遠隔地転送・保管

営業・技術機密情報

営業秘密・技術ノウハウ。漏洩時の競争力喪失リスク。

C:2 I:2 A:2

データ保存先

SaaS / クラウドサービス

Google Workspace

ベンダー側のバックアップ体制

ベンダー標準バックアップあり

バックアップ・保全設定

1次バックアップ

ベンダー自動バックアップ

2次バックアップ

クラウド同期

受注・売上データ

流出時の信頼失墜リスク。

C:3 I:2 A:3

営業顧客リスト

営業活動の基盤データ。

C:3 I:2 A:2

戻る

一時保存 08:04

次へ



自社の実態に即した診断

SaaSや社内システム、業務端末など、実際に使っている資産を選択するだけで、想定されるサイバーリスクを自動で洗い出します。



対話形式で専門知識不要

セキュリティの専門用語が分からなくても、5つのステップに沿って質問に答えるだけで、誰でも簡単に「現在地」を把握できます。



SCS要件への自動マッピング

ウィザードで回答した内容は、SCS格付取得に必要な要件や「ロードマップ」のタスクへ即座に反映され、次にすべき行動が明確になります。

経営サマリダッシュボード

想定年間被害額・セキュリティGrade・現在のスコアを一画面で把握。経営層への報告もここから。

株式会社関通

Enterprise+

分析ダッシュボード

再診断を実行

セキュリティ格付と財務リスクシミュレーション

経営サマリ

情報資産・インフラ

SaaS分析

ロードマップ

想定年間被害額

3,034,300,000

93,000,000 -¥58,700,000

インシデント対応費

¥15,000,000

情報漏えい賠償費

¥2,800,000,000

事業停止損失額

¥75,000,000

セキュリティ格付 (Grade)

S Superior

リスク減額率: 70% 適用中

CGL CORE MANDATE / 最優先対応事項

CYBER RESILIENCE FIRST

では「データ保全」と「認証基盤」を事業継続の2大基盤と定義しています。



財務リスクの定量化

想定年間被害額を「インシデント対応費・情報漏えい賠償費・事業停止損失額」に分解。対策前後の差額で費用対効果を可視化し、保険料削減交渉にも活用できる。



セキュリティGrade (S～D)

診断結果からGrade S～Dを算出。リスク減額率（例：70%適用中）を数値で示し、経営層への説明資料として即日活用できる。



レポート出力・稟議対応

「レポート出力」ボタンで役員報告・稟議書用PDFを即時生成。CGL CORE MANDATEへの対応状況を一覧表示し、経営層への説明資料として即日使える。

セキュリティロードマップ

カテゴリ別進捗・優先度・Lv別に整理されたタスク管理。担当者・期日を設定してPDCAを回す。

株式会社関通

Enterprise+

セキュリティロードマップ

分野別：段階的なセキュリティ実装ガイド

55

完了

12

未完了

3

受容

20,600

/ 25,200 pts

獲得スコア

🗂️ カテゴリ別進捗

🏢 組織・ルール

14/15 完了

💻 PC・端末

7/8 完了

📁 カテゴリ別

☰ リスト

🔍 セキュリティLv

🔖 未完了のみ

📄 全表示

🟢 Lv.1

🟠 Lv.2

🟡 Lv.3

🏢 組織・ルール

tasks

🔑 ID・認証・SaaS

1 tasks

T-029

Lv.1

優先セキュリティ評価の実施

緊急度: B

📅 6月22日まで

+300 pts

T-038

Lv.2

対応中

シングルサインオン(SSO)の導入

緊急度: B

📅 7月16日まで

+600 pts

T-040

Lv.1

★ おすすめ

対応中

【重要】SamuraiAI のIDパスワード管理・制限の見直し

緊急度: C

📅 6月14日まで

+100 pts



カテゴリ別進捗管理

組織・ルール／ID認証・SaaS／PC端末／インフラの4カテゴリ別に進捗率をリアルタイム表示。どのカテゴリが弱いかを一目で把握できる。



優先度・難易度フィルター

「緊急S」「Lv.1〜4」「経産省要件のみ」などで着手すべきタスクに絞り込み。担当者・完了目標日を設定してチームで進捗管理ができる。



ロードマップエクスポート

現在のロードマップをスプレッドシート形式でエクスポート。タスク状況・担当者・期日・スコアを含む一覧表として外部報告や記録管理にそのまま利用できる。

SaaS・クラウド 認証リスク分析

利用中のSaaSツールごとに認証状態のリスクを可視化。多要素認証の設定状況や認証強度をスコア化。

株式会社関通

Enterprise+

分析ダッシュボード

再診断を実行

セキュリティ格付と財務リスクシミュレーション

経営サマリ

情報資産・インフラ

SaaS分析

ロードマップ

SaaSセキュリティ・マトリクス (Shadow IT & ID Governance)

管理対象SaaS

8 システム

SSO連携率 (ID統合)

50%

サービス名	カテゴリ	重要度	認証方式 (SSO)	
GoogleWorkSpace [プライマリ IdP]	認証基盤 (IdaaS)	A	連携済	
クラウドログイン [SSOハブ]	認証基盤 (IdaaS)	A	連携済	
Google Workspace	グループウェア	A	単体ID	



認証状態のリスクスコア化

GoogleWorkspace・Salesforce・Slack等の各SaaSの認証設定状況をスコア化。MFA未設定・SSO未対応などのリスクを数値で把握できる。



ツール別リスク一覧

全SaaSツールの認証リスクを一覧表示。リスクの高いツールから順に改善優先度を提示し、具体的な対策をロードマップに直接連携できる。



ロードマップ自動連携

分析結果からリスク対策タスク（ID・認証カテゴリ）を自動生成してロードマップに追加。SCS要件「3-1-4: 多要素認証の導入」の対応状況にも反映される。

SCS体制要件マトリクス / ★取得シミュレーター

全157要件の充足状況をリアルタイム可視化。★3/★4取得に必要な残タスクと達成率を一目で確認。

Enterprise+

SCS体制要件
確認できます

← 戻る

📊 ★取得シミュレーター

85%
全体充足率
134 / 157 要件

89%
★★★★ 星4水準
96 / 108 要件

📌

【重要】格付の正式取得について
本ページは「経済産業省 セキュリティ体制格付」を渡すための事前準備・体制構築（セルフチェック）です。実際の格付取得には、外部運用
が別途必要です。

▼

全レベル

★★★★ 星4

★★★★ 星3

🟢 達成

🟡 進行中

⚪ 未着手

🔍 要件ID・名称・タスクIDで検索...

🏢

経営者の責任

15 / 15

状態	要件ID / 対象	要件に関する詳細内容	ロードマップ
社内ルール			
🟢	1-2-1-1 ★★★★	情報セキュリティに関する社内ルールを文書化し、経営層が承認していること	🟢 T-031
🟢	1-2-1-2 ★★★★	社内ルールを従業員に周知し、遵守状況を確認する仕組みがあること	🟢 T-031
🟢	1-2-1-3 ★★★★	社内ルールを定期的に見直し、必要に応じて改訂していること	🟢 T-031
セキュリティ推進活動部門			
🟢	1-2-1-1 ★★★	セキュリティ推進の責任部門・責任者を明確に定めていること	🟢 T-010



充足率のリアルタイム表示

全体充足率・★4水準・★3水準を個別に表示（例：全体85%・★4: 89%・★3: 82%）。要件ごとに「達成・進行中・未着手」の状況を一覧管理できる。



★取得シミュレーター

★3または★4を目標に設定すると、未達成の残要件数と対応タスクを表示。「経産省要件のみ」フィルターでSCS申請に直結するタスクだけに絞り込める。



申請書類の出力

「申請書類を出力」で審査機関提出用の対策実施状況一覧表をPDF自動生成。各要件への対応タスクIDとエビデンスが紐付いた状態で出力される。

SCS格付制度への対応詳細

経産省「サイバーセキュリティ格付制度」★3/★4 要件とRASHINの対応機能

SCS ACQUISITION FLOW



SCS REQUIREMENT MAPPING

要件ID	対象	SCS要件（概要）	RASHIN対応機能
1-1-1	★3	経営者がセキュリティ対応方針を策定・承認すること	規程自動生成 / 経営レポート
1-3-1	★3	セキュリティポリシーを役員・従業員へ周知すること	規程生成 / タスク管理
1-3-2	★3	従業員への定期的なセキュリティ教育・訓練の実施	ロードマップ / タスク管理
2-1-1	★3	取引先が管理するシステムを把握する仕組みの整備	ベンダー管理 / 資産台帳
2-1-2	★3	取引先のセキュリティ要件を契約・規程に明記すること	規程自動生成 / ベンダー管理
3-1-3	★3	クラウドサービスのアクセス制御・設定管理	SaaS認証リスク分析
3-1-4	★3	多要素認証の導入・アクセス権管理	SaaS認証リスク分析
3-2-1	★3	バックアップ・データ保護の実施と定期確認	ロードマップ / BCP対策
4-1-7	★3	インシデント対応手順の整備・訓練	規程自動生成 / BCP対策
1-4-1	★4	年1回以上、CISOへのセキュリティ推進計画報告	経営サマリレポート
1-4-2	★4	セキュリティ投資計画を経営層が承認する体制整備	経営レポート / 財務リスク算出
2-1-3	★4	重要取引先のセキュリティ対策状況を年1回点検	ベンダー管理（リスク評価）
3-1-5	★4	特権アカウントの管理・定期的なアクセス権見直し	SaaS認証リスク分析

COMPETITIVE COMPARISON

機能	RASHIN	A社（コンサル型）	B社（診断ツール型）	C社（規程作成）
セキュリティ診断・Gradeスコア算出	✓	△ 人手	✓	—
財務リスク（被害額）定量化	✓	△ 別途	—	—
対策ロードマップ自動生成	✓	△ 手動	—	—
SCS ★3/★4 対応・申請証跡出力	✓	△ 別途	—	—
規程・ポリシー自動生成	✓	△ 別途	—	✓
SaaS認証リスク可視化	✓	—	△ 別途	—
ベンダー管理・取引先リスク評価	✓	△ 人手	—	—
経営レポート・稟議書PDF出力	✓	△ 別途	—	—
専任IT人材不要で運用可能	✓	—	—	—

DEVELOPMENT STORY

関通：未曾有のサイバー危機を「経験資産」へと昇華する

2024年9月、ランサムウェア攻撃により全システムが停止。

物流インフラが麻痺し、多大な損害と、甚大な経営危機を経験しました。

私たちが経験した失敗、克服のプロセスをすべて注ぎ込み、サプライチェーン全体でサイバーリスクに強い体制を構築する。

CGLは、その第一歩として、自社の現在地を知る「無料リスク診断」から皆さまと共に歩み始めます。

💡 真のレジリエンスへの教訓

「防御100%は不可能。重要なのは、被害を最小化し迅速に復旧する『プランB』の備えである」

SUPPLY CHAIN RESILIENCE

私たちは、関通様と共に歩んだこの道のりを、日本のすべてのサプライチェーンを支える「盾」にしたいと考えています。

✓ ご入会企業様の声（導入実績）

愛知県 N社様

実体験の説得力

「実体験への信頼から即決。防御ではなく『早期復旧』の重要性に腹落ちし、若手責任者の成長にも繋がりました。」

大阪府 G社様

伴走ロードマップ

「何から始めるべきか不明だったが、納得の費用感で具体的な行動計画へ落とし込み。専門家不在の不安が解消されました。」

埼玉県 K社様

実務的コンサル

「ツール提供で終わらず、実務的な対策を伴走して伝授。自社のレベルに合わせた等身大な対策立案が非常に助かっています。」

大阪府 R社様

コスト最適化

「予算に合わせた最適な優先度を一覧化。今後の動きが明確になり、今後は社員教育も共に進める体制が整いました。」



注目インタビュー：名古屋眼鏡株式会社様

名古屋眼鏡株式会社

創業：1963年

本社所在地：愛知県名古屋市

事業内容：
メガネ関連商品の企画・製造・総合卸

主な取り扱い・オリジナル商品：

- ・花粉防止メガネ「スカッシー」
- ・白内障術後防護グラス「メオガード」
- ・こども用メガネ「トマトグラッシーズ」
- ・その他 コンタクトケア用品、光学機器



「実体験に基づいた対策が、社内の意識を劇的に変えました。」
未曾有の危機を乗り越えた生の声を、動画で詳しくご覧いただけます。



▶ 動画を視聴する

vimeo.com/1201299161

全プラン共通機能: ✓ セキュリティ診断 ✓ ロードマップ生成 ✓ 財務リスク定量化 ✓ 経営レポート出力 ✓ SaaS認証分析 ✓ ナレッジ共有 ✓ チャット相談 ✓ タスク進捗管理

システムのみ

Starter

セルフサード型

¥50,000 / 月

✓ システム利用

- コンサルなし

今すぐ申し込む

推奨：～50名

Standard

コンサル伴走支援

¥100,000 / 月

✓ システム利用

✓ チャット相談

今すぐ申し込む

🔥 1番人気

推奨：～100名

Plus

手厚いコンサル支援

¥200,000 / 月

✓ システム利用

✓ チャット相談

今すぐ申し込む

推奨：～200名

Enterprise

グループ統制等高度支援

¥300,000 / 月

✓ システム利用

✓ チャット相談

今すぐ申し込む

無制限

Ent Plus

超大規模向け特注対応

個別見積

✓ システム利用

✓ 要件特注対応

お問い合わせ

SCS OPTION – オプション

📄 規程 & ポリシー管理

規程の自動生成とOS・クラウドのポリシー設定管理。統合パックならさらにお得に申込可能です。

規程管理（単体）

+¥20,000/月

ポリシー管理（単体）

+¥30,000/月

📦 セットでおトク

📦 統合パック

+¥40,000/月

🏛️ 格付取得フルサポート

システムでの要件可視化に加え、監査に向けた申請証跡の出力・実運用までをフルサポート。

+¥80,000 / 月

RASHIN SCSコンパス・パッケージ

RASHIN 1年利用 + 規程自動化 & 取得フルサポート

¥2,040,000～ / 年（税抜）

20% OFF

¥1,632,000～ / 年

✓ Starter 1年利用（通常¥5.0万×12ヶ月）

✓ 規程生成・SCSシミュレーターオプション込

✓ 申請書類PDF出力・証跡管理

RASHIN

無料アカウント登録



rashin.ai/signup