企業向けサイバーセキュリティソリューション

Q-SOC

サイバードミノ

自社が原因で、取引先の業務まで止まるかも…

ウイルス対策ソフトだけでは防げないかも…

業務停止より怖いのは、取引停止かも…

から事業を守る

中堅・中小企業の約7割がサイバー攻撃の入り口に

「うちは標的にならない…」そう思っていませんか？

セキュリティ対策がされていない
中堅・中小企業が標的にされています

取引先企業、グループ企業など
自社に関わりのあるさまざまな企業に飛び火
サイバー攻撃の入り口となってしまいます。

かかりつけ医『Q-SOC』にお任せください！

平時のうちに**自社のシステム状況を把握**をして
有事に備えた**インシデントレスポンス**の準備を進めませんか

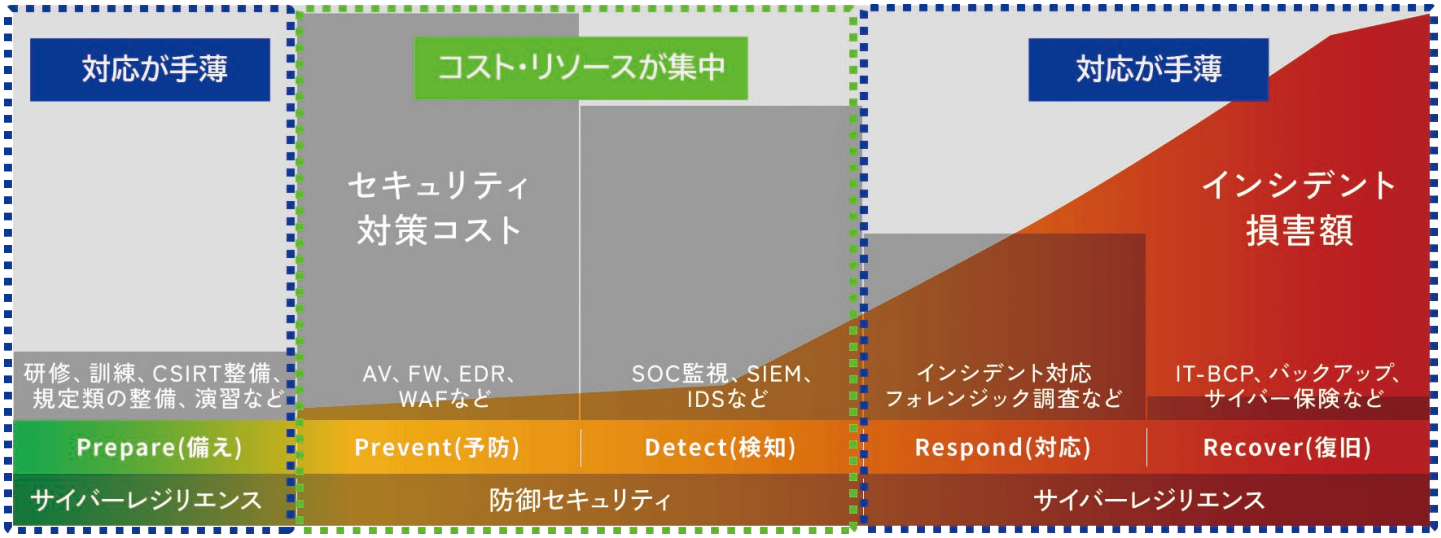
Q-SOCページへ

Step1.セキュリティリスク箇所を診断・処置

※かかりつけ医は、イメージです。いざという時に業務を早期復旧する為には、セキュリティカルテを作成することを推奨しています。
※各サービスの詳細につきましては、お気軽に弊社Webフォームからお問合わせください。

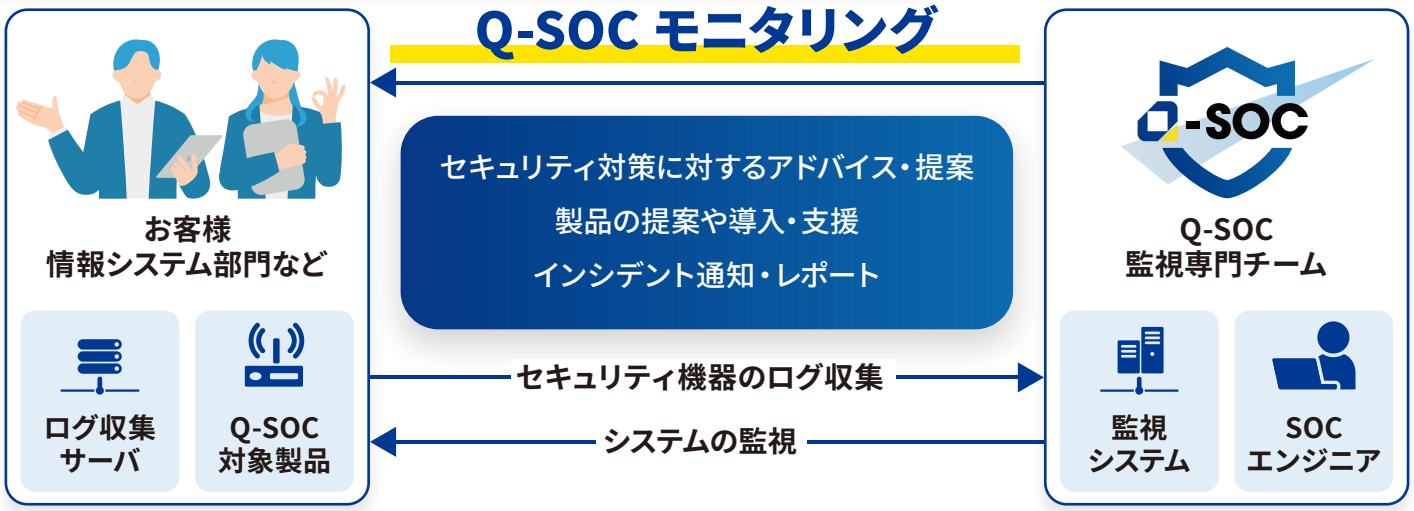
Step2.セキュリティ投資コストを診断

防御だけでは守り切れない被害を最小化して早期に事業復旧する力＝**サイバーレジリエンス**が重要



※アセスメントサービス・サイバーレジリエンスパッケージは、サイリーグホールディングス株式会社とのアライアンスメニューとなります。

Step3.プロアクティブモニタリングの開始



※対象となるセキュリティデバイスについてや、SOCサービスの乗り換えなど、お気軽にご相談ください。

Q-SOC サービスメニュー

サービスの全体像	Lite UTMモニタリング セキュリティサービス	Entry インシデント対応付き セキュリティサービス	Standard インシデント対応付き セキュリティサービス	Trial クラウド セキュリティサービス
想定される課題・要望	■UTM等、境界防御の監視	■UTM等、境界防御の監視 ■セキュリティカルテ作成 ■インシデントレスポンス	■ASMサービス ■UTM等、境界防御の監視 ■セキュリティカルテ作成 ■インシデントレスポンス	■サーバー機器の死活監視
基本価格（税抜）	300万円/年～	440万円/年～	600万円／年～	90万円/年～
24時間365日監視	○	○	○	○
メール・Web相談	○	○	○	○
月次報告	○	○	○	○
監視システム設定	○	○	○	○
障害通知	○	○	○	○
障害一次対応	○	○	○	○
セキュリティデバイス監視	○	○	○	
インシデント検知・通知	○	○	○	
バージョンアップ支援	○	○	○	
ハードウェア保守支援	○	○	○	
セキュリティカルテ作成・更新		○	○	
脅威インテリジェンス提供（年4回）		○	○	
定例会（年4回）		○※1	○※1	
インシデント初動対応支援		○※2	○※3	
インシデントハンドリング		○※2	○※3	
ASMサービス	オプション	オプション	○※4	オプション

※1：セキュリティカルテは、契約時に作成し、四半期ごとに更新します。
※2：エントリープランのインシデント初動対応は、年間1件（3時間）、インシデントハンドリングは、年間1件（40時間）が目安です。詳細は、お問合せください。
※3：スタンダードプランのインシデント初動対応は、年間4件（12時間）、インシデントハンドリングは、年間1件（60時間）が目安です。詳細は、お問合せください。
※4：ASMサービスは、お客様のネットワーク環境や、対象となるセキュリティデバイスに合わせてプランニング（個別見積）させて頂きます。
※UTM/NGFW/EDR/MDR製品の新規導入・リプレイスなど、お客様のご要望にあわせたSI提案も可能です。お気軽にお問合せください。

Q-SOC サイバーレジリエンスパッケージ

※現在ご利用しているセキュリティ機器（UTMなど）にパッケージの追加もできますので、詳細はお問い合わせください。

		エントリープラン 年間140万円（税別）	スタンダードプラン 年間240万円（税別）
平時	定例会	1時間×年間4回 ※その場でのQA1問対応	1時間×年間4回 ※事前QA1問対応＋その場でQA対応
平時	脅威インテリジェンス提供	年間4回	
平時	セキュリティカルテ作成	契約時に作成。四半期ごとに更新	
有事	インシデント初動対応支援	年間1件 3時間まで	年間4件 12時間まで※1 ※四半期ごとに1件 3時間まで
有事	インシデントハンドリング	年間1件 40時間まで	年間1件 60時間まで

※1：各四半期あたり1件3時間までが上限です。未使用分の繰越や超過分の利用はできません。
※有事の対応時間については、人時ベースになっております。事象やタイミングに応じて、参加人数が1名～3名になる場合があります。
※本サービスは、サイリーグホールディングス株式会社とのアライアンスメニューによる「事前契約型インシデント対応サービス」となります。

有事対応における主なサービス範囲

1	事象分析・初動方針の助言	発生状況をヒアリングし、感染拡大防止・優先対応項目を助言
2	判断支援	「ネットワーク遮断」「端末切り離し」「バックアップ復元」等の意思決定を支援
3	対応計画の整理	システム別に対応手順・優先順位・報告項目を整理し共有
4	ログ調査・フォレンジック調査	収集されたログ・イメージデータを分析し、侵入経路・感染経路・被害範囲を特定 ※ ログ容量・端末台数に応じて別途見積もり
5	復旧フェーズ支援	復旧可否判断やベンダー調整等のアドバイス

※ ログ・証跡・感染ファイル等の収集・保全、共有・フォルダや外部ストレージへのアップロード等、お客様側で実施いただく作業もあります。
詳しくは、契約時の打合せにてご説明させて頂きます。

Questは、デジタルの未来を探究する企業

OMOTENASHI Japan service quality ★★

ISO26000対応 SDGs follow-up and review ★★★ JCSRA

ISO23592対応 SE follow-up and review ★★★ JCSRA

経済産業省が創設した「おもてなし規格認証」において、情報通信業界では稀有な存在である紺認証を取得し、さらにサービスエクセレンス成熟度評価（ISO23592準拠）の最高ランク「SE★★★（LV4）」を継続更新いたしました。これに加えて、SDGs成熟度評価認定（ISO26000対応）も新たに取得し、最高ランクの評価を受けています。

ARIGATOU

ITの未来は「ありがとう」の中にある。

「技術を探究し、価値を創造し、お客様とともに成長する」という企業理念のもと、コンサルティングからシステムの構築、運用・保守に至るワンストップサービスをご提供してまいりました。今後とも、お客様へのご支援を通じて社会に貢献し、お客様とともに持続的な成長ができますよう、より一層精進してまいります。

Quest

株式会社クエスト

本社：東京都港区芝浦 3-1-1 msb Tamachi 田町ステーションタワー N 14F
TEL：050-3785-3977
Mail：market@quest.co.jp
URL：https://www.quest.co.jp/security/

お問い合わせはこちら

2026年3月時点