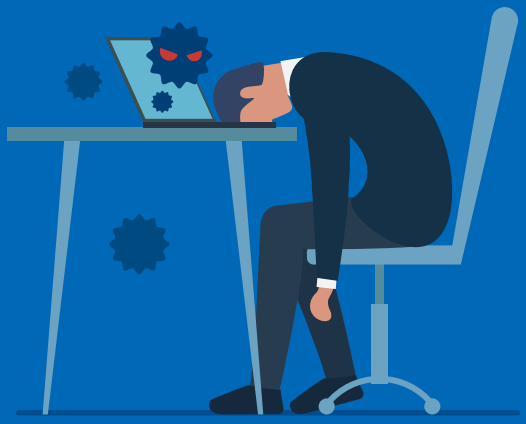
標的型攻撃・情報漏えい対策に課題を抱えていませんか？

日々巧妙化していく標的型攻撃をはじめとしたサイバー攻撃！
ウイルス感染を100%防ぐことは不可能となっています。



セキュリティにあまり
コストは
かけられない

どう対処したら
いいんだろう

どの端末が
ウイルス感染
したのかな

情報漏洩は
防がないと

情報セキュリティの被害発生・拡大を防ぐためには、
ウイルス感染後の不審な通信を早期に発見し、いち早く対策を実施することが重要です！

不審な通信を監視、早期発見で被害を防ぐ

セキュリティ運用（SOC）サービス

RiskAdvisor

早期発見！

日々の検知ログをリアルタイムで分析するため、標的型攻撃や情報漏洩の予兆をすぐに見つけ、早めに対策することができます。

初期コストなし！

クラウドサービスのため、新たに専用のシステムを導入することなく、簡単にご利用いただけます。

※別途、ポータル登録とUTMのログ転送設定は必要です。

安価！

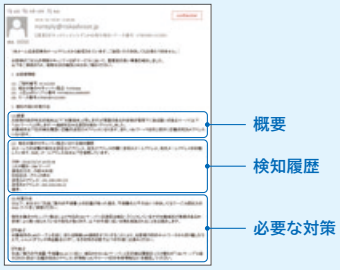
月額数十万円を超えるSOCサービスが多い中、月額数千円～*簡易SOCサービスを提供します。

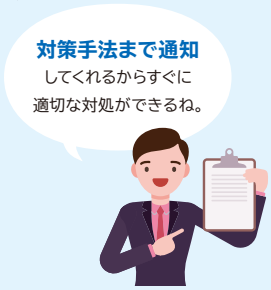
*金額は分析対象の機種によって異なります。

提供サービス／機能一覧

機能 1 インシデント発生の疑いがある時にメールで通知

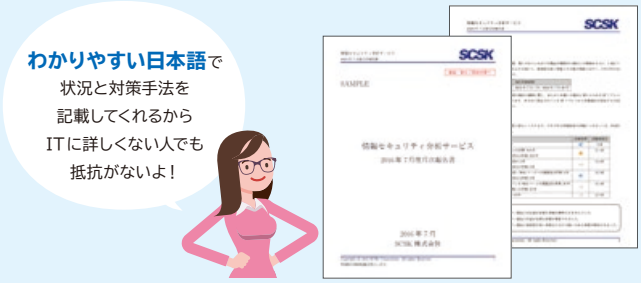
検知ログを監視／分析し、感染等のインシデント発生の可能性が高い場合にはメールで即時通知。





機能 2 毎月の検知状況を月次でレポート

1ヶ月の検知状況をPDFレポートにしてメールで送信。



機能 3 ログ送信停止時に通知（簡易ネットワーク監視）

ログの通信が止まった際には故障や周辺ネットワークの設定ミスなどの疑いありとしてメールで通知。

機能 4 専用ポータルサイトからレポートや対策手順書を確認

サービス利用者様には専用ポータルサイトのアカウントが発行され、UTM の設定や感染後の対策に関する資料をダウンロード可能。

導入イメージ

※無償でご試用いただけます。詳細は販売店にお問い合わせ下さい。

SCSK SCSK株式会社
http://www.scsk.jp/
ITプロダクト&サービス事業本部
ネットワークセキュリティ部
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント
E-mail：riskadvisor-info@ml.scsk.jp