News Release

2024 年 12 月 17 日

報道関係各位

サービス&セキュリティ株式会社

サービス＆セキュリティ株式会社(SSK)のセキュリティ運用監視サービス 新たに「Cortex XSIAM」に対応

サービス＆セキュリティ株式会社（本社：東京都渋谷区、代表取締役社長：姜 昇旭、以下「SSK」）は、自社が運営するセキュリティオペレーションセンター（SOC）で提供しているセキュリティ運用監視サービスにおいて、新たにパロアルトネットワークスの自律型 SOC プラットフォーム「Cortex XSIAM」をラインアップに加え、2025 年 1 月より提供開始いたします。

１．背景

当社は、2018 年にセキュリティオペレーションセンター(SOC)を開設して以来、UTM、IPS などのセキュリティ機器の運用監視に加え、お客様の環境とニーズに合わせた、クラウドセキュリティ、SASE セキュリティ、EDR（エンドポイントセキュリティ）など、最新セキュリティソリューションの運用監視サービスを提供してきました。セキュリティ運用監視サービス、セキュリティ脆弱性診断サービスなど SSK の高度セキュリティソリューションは、官公庁、教育機関、金融機関、一般企業を含め約 3,000 を超えるプロジェクトに幅広く提供しています。

さらに、これら多くのお客様のセキュリティソリューションを通じて得たノウハウや知見を活かし、新たなサービス拡大にも迅速に対応することが可能な体制を構築しています。

従来、監視対象となる機器はオンプレミス環境が主流で、セキュリティアラートの分析もその環境内での SIEM（セキュリティ情報イベント管理）を利用して行われていました。しかし近年では SASE の導入をはじめとするクラウド環境の利用が急速に進んでおり、それに伴いクラウド型 SIEM による分析ニーズが高まっています。

こうした変化に対応するため、当社では新たにパロアルトネットワークス社の「Cortex XSIAM」を活用したセキュリティ運用監視サービスの提供を開始いたします。これにより、オンプレミス環境だけでなく、クラウド環境にも柔軟に対応できる体制を整え、お客様のニーズに応えてまいります。

２．Cortex XSIAMセキュリティ運用監視サービスのポイント

今回開始する運用監視サービスのポイントは以下の通りです。

① 「インシデント分析・遠隔処置」の実施

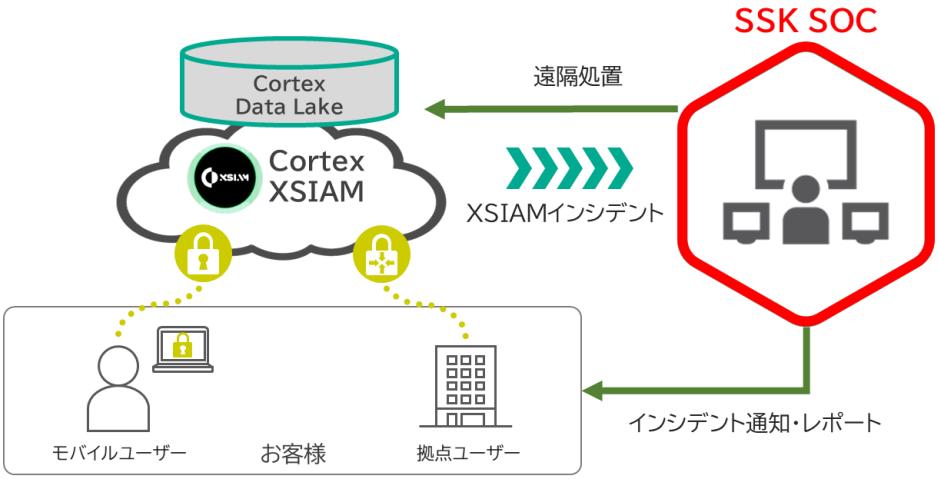
・Cortex XSIAM のインシデントを 24 時間／365 日監視対応

・管理コンソールを用いた遠隔操作による各種お客様対応の実施

② 「運用・サポート」の実施

・問い合わせ対応、セキュリティ分析月次レポートの提供

・セキュリティニュースの発信



【サービス提供イメージ】

SSK のトータルセキュリティサービスは、今回のラインナップ強化を通じて、これまで培ってきたセキュリティ運用監視サービスの実績を最大限に活かし、新たなニーズに迅速かつ柔軟に対応してまいります。引き続き、日本国内のさまざまな課題に応え、高品質で革新的な製品・サービスを提供し続けることで、さらなる成長を目指します。

■サービス＆セキュリティ株式会社について

サービス＆セキュリティ株式会社は、創業 45 年を迎え、官公庁、金融機関、大手製造業など幅広い業界に対し、IT エキスパートとセキュリティサービスを提供してきたトータルセキュリティサービス企業です。豊富な経験とノウハウを持つプロフェッショナルが、システム運用や開発、インフラ構築からセキュリティ対策まで幅広く支援し、安心・安全なビジネス環境の構築をお手伝いします。

今後も、SSK は日本の情報システムを支える IT エキスパート集団として、一人ひとりの専門性を結集し、社会やお客様とともに未来を切り拓いてまいります。

・会社名　　：サービス&セキュリティ株式会社
・代表者　　：代表取締役社長　姜昇旭
・本社所在地　：東京都渋谷区東3-14-15 MOビル2階
・設立　　：1979年12月
・従業員数　　：グループ全体　1,946名（2024年4月現在）
・事業内容　　：■ITエキスパートサービス
　・システム運用管理
　・システム開発
　・インフラ構築
■総合セキュリティサービス
・セキュリティ運用監視サービス
・セキュリティ対策支援サービス
・セキュリティエキスパートサービス
・セキュリティ製品の研究、開発、販売、保守
・会社ホームページ：https://www.ssk-kan.co.jp/

※　掲載されている製品名、会社名、サービス名はすべて各社の商標または登録商標です。

別紙

１．Cortex XSIAMセキュリティ運用監視サービス内容

SSK の Cortex XSIAM にてインシデントを検知した場合、分析しお客様へ通知を行うサービスです。
詳細は以下の通りです。

分類	サービス項目
①　インシデント分析・遠隔処置	XSIAM インシデント分析・通知
	ファイル隔離
	端末隔離
②　運用・サポート	問い合わせ対応（月 3 回）
	月次分析レポート提供
	月次分析レポート報告サービス　※オプション
	セキュリティ情報発信（セキュリティニュースの提供）

２．Cortex XSIAMセキュリティ運用監視サービスの主な仕様

SSK の Cortex XSIAM セキュリティ運用監視サービスの主な仕様は以下の通りです。

（１）「インシデント分析仕様」

項目	内容
サービス概要	Cortex XSIAM で検知したインシデントを監視・分析します。
監視時間	24 時間／365 日
分析基準	Cortex XSIAM で算出されるインシデントのスコア（SMARTSCORE）、ATT＆CK の戦術や技術、インシデントに紐づいているアラートなどから攻撃状況や被害状況を総合的に分析し危険度を判定します。
通知基準	4 段階の危険度判定に沿った通知を行います。

（２）「問い合わせ対応」

項目	内容	
サービス概要	通知内容や月次分析レポートの問合せに対して回答します。	
問合せ対象	● SOC からの通知内容（メール、電話） ● SOC が発行する月次分析レポートの記載内容	
問合せ対応範囲	● 通知した内容や月次分析レポートに記載したインシデントに関する影響範囲や一般的な対策のアドバイス	
問合せ受付時間	メール	24 時間／365 日
	電話	10:00～18:00／平日
問合せ対応時間	平日 10:00～18:00	
受付回数	契約サービスごとに各月（1 日～末日）に 3 回まで	
受付対応	問い合わせメールに対して、受付メールを返信します。 また、受付メールに回答を記載して返信する場合もあります。	
一次回答	問合せ受付後、24 時間以内（休日の場合、翌平日の 10:00~18:00 の間に回答） 例 1)火曜の 15 時に問合せ → 水曜の 15 時までに一次回答 例 2)金曜の 19 時に問合せ → 月曜の 18 時までに一次回答 ※例は全て平日を想定しています。	
問合せ対応の定義	● 契約単位での受付回数となります。 ● 1 回の定義は問合せ対応が完了するまでとなります。 ● 弊社からの回答から 1 週間経過し返信がない場合は自動的にクローズします。 ● お客様からのメンテナンス連絡は受付回数にカウントされません。	
問合せフォーマット	件名(通常時)	[問合せ] 問合せ内容
	メール本文	● 監視対象機器名 ● 問合せ内容に関わる日時 ● 種別（インシデント関連・月次分析レポート関連） ● 問合せ内容