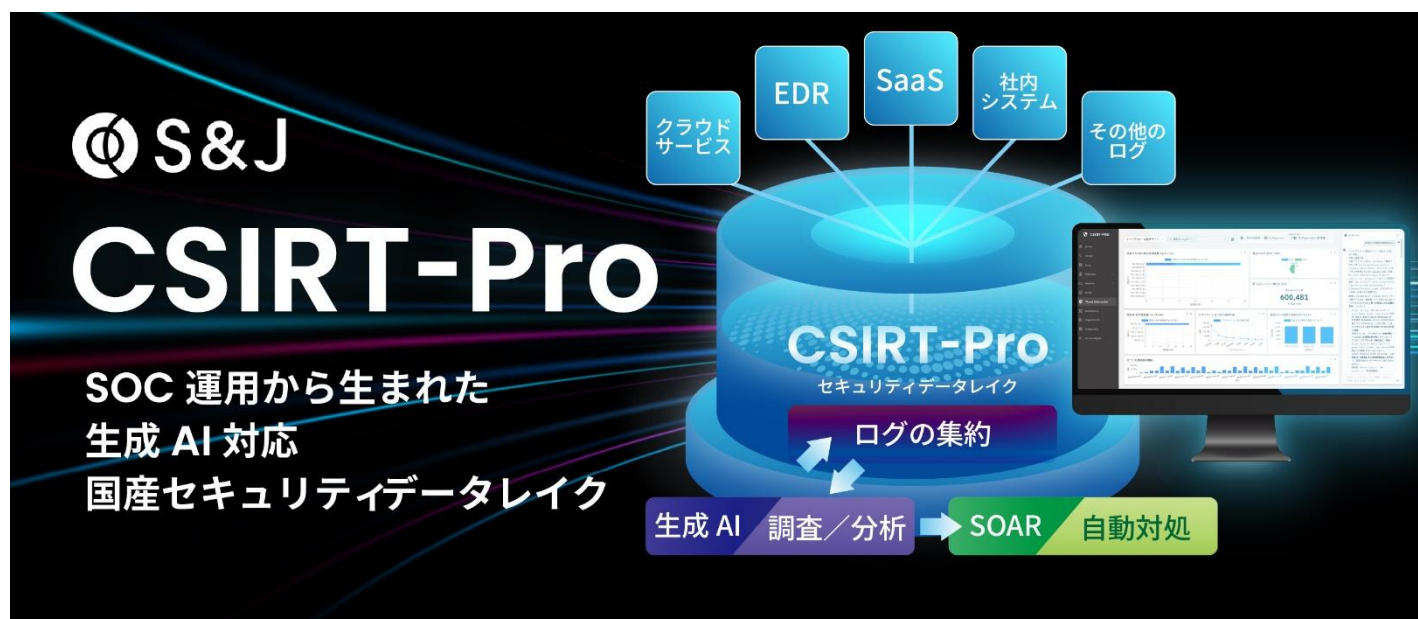


S&J、SOC 運用から生まれた生成 AI 対応の 国産セキュリティデータレイク「CSIRT-Pro」を提供開始

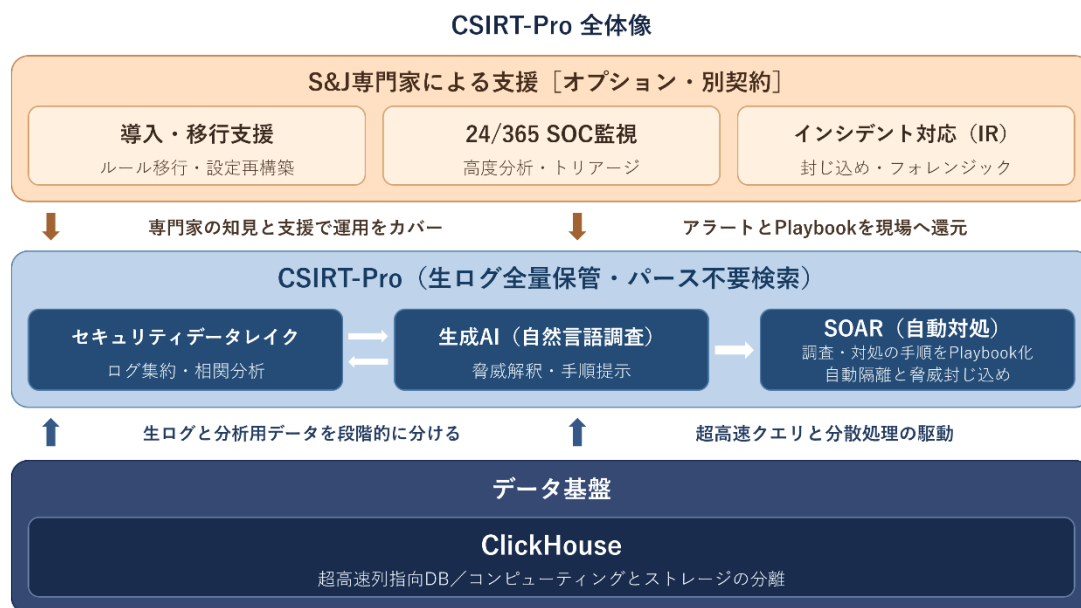
～主要クラウド型 SIEM の約 3 分の 1 の価格で、多様なセキュリティログを集約・長期保管し、
必要なときに生成 AI による調査と SOAR による自動対応を実現～

セキュリティ監視サービスやセキュリティ事故対応などのサイバーセキュリティ事業を展開する S & J 株式会社（本社：東京都港区、代表取締役社長：三輪 信雄、証券コード：5599、以下「S&J」）は、次世代 SIEM であるセキュリティデータレイクを基盤に、SOAR による自動対応、生成 AI による調査支援を統合した「CSIRT-Pro（シーサート・プロ）」を、2026 年 9 月 15 日（火）より提供を開始しました。



CSIRT-Pro は、顧客が利用する SaaS や EDR など、企業環境のさまざまな場所に日々生成される膨大なセキュリティログ（以下、ログ）を集約し、必要なときに検索・分析できるセキュリティデータレイクを備えています。ログの収集・保管から、検知、調査、対応までを一貫して実現します。

CSIRT-Pro が提供する生成 AI は、S&J の SOC 運用やインシデント対応で培ってきたセキュリティの知見を組み込んでおり、ログの調査から対応までを自然言語で行えます。



図：「CSIRT-Pro」の全体像

CSIRT-Pro の主な特長

1. 約 9.3 倍の高効率圧縮により、生ログの保管コストを大幅に削減

主要クラウド型 SIEM の約 3 分の 1 の価格を実現

CSIRT-Pro は、自社ベンチマーク環境で約 9.3 倍（※1）のデータ圧縮率を実測しており、顧客のログをセキュリティデータレイクへ効率的に保管します。内部のエンジンには列指向型オープンソースデータベースである「ClickHouse」を活用することで、この高い圧縮率と検索の高速性を両立しました。また、ログ本体をオブジェクトストレージ上に置く設計とすることで、アプリケーション層でのデータ複製を不要とし、保管コストを抑制しています。こうしたコスト構造により、主要クラウド型 SIEM と比較して、サービス価格を約 3 分の 1（※2）に抑えています。

※1 自社ベンチマーク環境での実測値。圧縮率はログの種類や内容により変動します。

※2 コスト比較の算出根拠：主要クラウド型 SIEM において 1 日あたり 50GB のログを 1 年間保管した場合の標準的な公表料金と、CSIRT-Pro 「Medium プラン」の費用を比較した当社試算に基づく。

2. 「必要なとき、解析・構造化が可能」なデータレイク方式で、運用負荷を軽減

従来の SIEM はログの取り込み時に形式を定義する必要があり、機器追加やログ仕様変更のたびに設定作業が発生します。CSIRT-Pro は、ログをそのまま蓄積し、必要になった時点で解析する「データレイク」方式を採用。これにより、ログの仕様変更に伴う設定作業を減らし、日々の運用負荷を軽減します。

3. セキュリティ専門ベンダーの知見を組み込んだ生成 AI が、自然言語による調査を実現

CSIRT-Pro では、S&J がサイバー攻撃の監視・事故対応で蓄積してきた知見を組み込んでいる生成 AI によるセキュリティ調査機能を提供します。

「このアカウントの直近 30 日間における異常な挙動を洗い出して」といった自然言語による指示により、生成 AI が検索結果の解釈や、次に確認すべき観点の提示を支援します。

4. 生成 AI による調査・対処の手順を Playbook 化し、継続的な自動対応を実現

CSIRT-Pro では、生成 AI との対話で組み立てた調査・対処の手順を、SOAR の Playbook として保存できます。例えば、不審なアカウントを検知した場合、自然言語で過去の挙動を調査し、その結果に応じてアカウントの無効化や関連端末の隔離などの Playbook を実行できます。

CSIRT-Pro では一度確立した手順が Playbook として蓄積され、同じ事象が再び起きた際には自動で実行されます。



5. 国内データ保管と国内事業者による提供

CSIRT-Pro は、顧客のログを国内のデータセンターに保管し、国外へ移転することはありません。企画・開発からサポートまでを国内で行っており、契約・サポートともに日本語で完結します。調達時にサプライチェーンの説明を求められる場合も、国内で完結した体制として説明できます。

CSIRT-Pro サービス概要

サービス名	CSIRT-Pro（シーサート・プロ）
サービス概要	セキュリティデータレイクを基盤に、 SIEM・SOAR・生成 AI を統合したセキュリティプラットフォーム
主な機能	セキュリティログの長期保管、SIEM による検知、SOAR による自動対処、 生成 AI による調査支援、ダッシュボード
提供開始日	2026 年 9 月 15 日（火）
料金	1 日あたりのログ取り込み量に応じた 6 段階の契約プランを提供。 有償プランは月額 40,000 円（5GB/日）から ※税抜
新規導入相談の受付	専用 Web ページにて受付
専用 Web ページ	https://www.sandj.co.jp/services/csirt-pro/

料金プラン

プラン名	1 日あたりログ取り込み量	月額（税抜）
Free	100 MB まで	0 円
Small	5 GB まで	40,000 円
Medium	50 GB まで	265,000 円
Large	200 GB まで	960,000 円
XLarge	500 GB まで	2,050,000 円
Critical	1 TB まで	3,610,000 円

・各プランには、ログ取り込み量のほかにも以下の上限を設けています。

・データ保存容量、検索実行量、検索スキャン量、検索通信量、Playbook 実行回数、AI 利用トークン数、Case 作成件数、ログ取り込み量の範囲内であっても、いずれかの上限を超える場合は、契約プランに加えて従量課金となります。各プランの詳細な上限値は製品サイトに掲載しています。

また、契約プランはカスタマイズ可能になっており、Medium に対してログ取り込みを 50GB 追加するといった対応も可能です。

・ログの保存容量は、ログの圧縮率を考慮して設定しています。CSIRT-Pro では、圧縮率 4.56 倍を下限として保存容量を設計しており、実際の圧縮率がこれを下回った場合でも、1 年間ログを保存できるよう、S&J が追加の保存容量を無償で提供します。

S&J のセキュリティサービスとの連携

CSIRT-Pro は、S&J が提供するセキュリティ監視、インシデント対応、コンサルティングサービスと組み合わせて利用することができます。他社 SIEM 製品や既存のログ管理基盤からの乗り換えにおいて課題となる「検知ルールの移行」や「ログ取り込み設定の再構築」なども、セキュリティの専門家である S&J が導入・移行を支援します。

また運用開始後も、自社のセキュリティ運用体制では対応が難しい深夜・休日を含む 24 時間 365 日の監視を S&J の SOC（Security Operation Center）に委託し、インシデント発生時にはシームレスに S&J の事故対応チームに支援を依頼するといった運用が可能です。



※これらのサービスは CSIRT-Pro とは別契約となります。

■ S & J 株式会社について

S&J は、サイバー攻撃や内部関係者による情報漏えい等の内部犯行など、情報セキュリティは経営課題として認識されてきている状況下、「防御・検知・対処」や「技術・体制」のバランスを重視した製品やサービスを提供しています。

SOC（Security Operation Center）は、従来のアラート監視での脅威お知らせサービスに加え、顕在化した脅威による顧客環境での高度な影響分析やトリアージをアナリストが行い、影響に応じて事故の封じ込めのハンドリングやフォレンジックまで迅速な対応をすることにより、業務継続と再発防止策を支援しています。

商号	S & J 株式会社
所在地	〒105-0004 東京都港区新橋一丁目 1 番 1 号 日比谷ビルディング 8F
設立	2008 年 11 月
資本金	4 億 4162 万円
代表者	代表取締役社長 三輪 信雄
事業内容	サイバーセキュリティ事業 ・セキュリティ監視／運用 ・コンサルティングサービス ・セキュリティ事故対応
Web サイト	https://www.sandj.co.jp

■ プレスリリースに関するお問い合わせ

S & J 株式会社 広報担当 E-mail : pr@sandj.co.jp / TEL : 03-6205-8500（代表）

=====

※本リリースのすべての内容は、作成日時点でのものであり、予告なく変更される場合があります。

また、様々な事由・背景により、一部または全部が変更、キャンセル、実現困難となる場合があります。予めご了承ください。

=====

※本文中に記載されている会社名および製品名などは、各社の登録商標または商標です。

※ClickHouse は、ClickHouse, Inc.の商標または登録商標です。

※CSIRT-Pro は、S & J 株式会社の商標です。