

“あらゆるログが取り込める”クラウドSIEMソリューション

sumo logic®

近年、ランサムウェア被害が増加中！

多くの企業では**侵入経路の特定**ができていません。

確実かつ網羅性の高い
ログ保管・管理が重要

ログ保管・管理の重要性

平常時からの
異変察知

各製品ログ
統合・長期保管

漏えい発生時
調査 短期化



内部/外部要因
情報漏洩を
事前察知



個々製品
保存期間が
不十分



改正個人情報
保護法
報告義務期限

退職者・社員による
情報漏洩防止は
特に困難！

インシデント発生時
既にログがない！

5日以内の速報
命令違反による
罰則・罰金！

Sumo Logicで日頃から情報漏洩に備えましょう

詳しくは裏面へ

Sumo Logic の3つの特長

1 簡単なリアルタイムログ取り込み

サーバ・PC UTM/NW機器 クラウドサービス

2 CROWDSTRIKE 高度インテリジェンス標準搭載

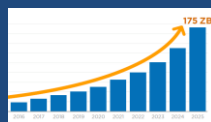
ログ突合
sumo logic CROWDSTRIKE
国・攻撃
犯人・道具

3 ログ取り込み無償の価格設計

費用はログ検索した分だけ

▶ 従来の取り込みログ量課金の課題

日々膨大な
ログデータが蓄積



データ増加のご時世

VS

従来の価格設計
ミスマッチ



【販売価格】年間750,000円～

※1、※2

新規 ログ分析サービス導入を検討のお客様

お悩み

導入時の不安



SIEM製品が初めて利用で不安

どのように利用してよいか分からない

無事に運用開始ができるか不安

解決



ALSI導入支援サービス

テナント開設・運用設計支援

ダッシュボード作成

教育トレーニング

ALSI独自サポート

日本語サポート

月5時間 無償
ダッシュボード修正・変更

お悩み

導入後の不安



情シス担当が少ない 知見もない

他業務もありログ分析に工数を割けない

稼働後に本当に運用できるのか不安

解決



ALSI SOCオプション

通知オプション

脅威分析オプション

異常行動分析オプション

AI (Copilot) 分析機能

人材・ナレッジ不足をカバー

クエリ自動生成

類似回答の提案

既存 ログ分析サービスご利用のお客様

お悩み

取り込みログ量増加傾向の弊害



またセキュリティ製品・サービスが増えた

今後も取り込みログ量は増加傾向＝費用増

障害発生時のログ追跡のためには仕方ない…

解決



Sumo Logicでスモールスタート

ログ取り込み無料 最低契約 750,000円/年～ ※1、※2

既存SIEM製品の追加費用範囲をSumo Logicで試してください

ALSI & メーカー技術がPoC伴走支援・そのまま本番移行可能

お悩み

大規模ユーザ オンプレミスの限界



オンプレミス SQL DBはログ肥大化に弱い

検索時間は、数日かかることも

ログ保管はディスク依存で1か月分のみ保管

解決



オンプレミス基盤からSumo Logic 乗換事例

ログ増大時もスケーラビリティは柔軟・迅速に対応可能

検索時間（ログ量28GB/日） 1週間 → 2～3分に短縮

会社監査要件である過去2年分の保管に対応

※1:為替により価格影響があるため都度お見積 ※2:最低契約期間 2年契約～

アルスシステムインテレーション株式会社

本社 〒145-0067 東京都大田区雪谷大塚町1-7
TEL:03-5499-8045 FAX:03-5499-0357
東京営業所／古川営業所／仙台営業所／いわき営業所／白台オフィス
横浜オフィス／名古屋営業所／大阪営業所／広島営業所／福岡営業所

<https://www.alsi.co.jp> / E-mail : ssg@alsi.co.jp



お問い合わせ、ご用命は下記へお申し付けください。