システムの現状を可視化する

高速ログ分析プラットフォーム

Soliton NK

産業機械　サーバー　ロボット　IoT　Network　クラウド

あらゆるデバイスからログ情報を収集

textlog
HTTP Post
rsyslog
syslog
binary data
NetFlow/PCAP

高速データ分析プラットフォーム
Soliton NK

AIや脅威情報など外部ツールとの連携も可能。

迅速な可視化を実現

- データ形式不問・追加課金なしのデータ収集
- grep sum chart 簡単スクリプトも組み込める柔軟な分析機能
- 頻繁に使う分析結果はダッシュボードに保存
- 検索結果に応じた自動処理（メール通知等）

サイバー攻撃検知

攻撃者の攻撃手法を踏まえると、より多くの種類のログを取得し、さらにできるだけ長期間分析できるように保存しておくことが求められます。そのためには、ログ収集分析ソフトウェアの費用は、データ量に関わらず一定であることが重要です。

また、サイバーセキュリティの専門家を確保することがまずます難しくなるので、操作は簡単であることが重要です。そして、データの量や種類が増えれば増えるほど、定常的な操作を自動化できることが求められます。Soliton NK は、それらを Kit という形で提供します。

例えば、NetFlow、Zeek、DNS、Sysmon 等の Kit を提供し、サイバー攻撃検知に役立つ、使い勝手を提供します。そして企業経営の最大リスクであるランサムウェア攻撃への対策にも活用できます。

Soliton NK は、どのようなログを取得したらいいのか分からない、ログは取得しているが分析等に活用できていない等の悩みを抱えている方々に最適なソリューションとなるログ分析ソフトウェアです。

サイバーセキュリティ経営の重要 10 項目から

項目	実践のプラクティス
リスク管理体制	✔ サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
リスクに対応するための仕組み	✔ 多層防御の実施 ✔ アクセスログの取得
インシデント発生時の緊急体制	✔ CSIRTの設置 ✔ 従業員の初動対応マニュアル

Soliton NK のサイジング

Soliton NK は Docker Hub からコンテナイメージで提供しています。Docker や Kubernetes 等のコンテナ基盤上で動作します（別途 Soliton NK のライセンスが必要）。

Soliton NK の推奨動作要件は以下の通りです。

- 16GB 以上のメモリ
- 4 コア以上の vCPU

サイジングについては以下の項目等について検討する必要があります。

- ✔ SolitonNK へ投入する想定ログ量
  （例：xx バイト / 日、yy バイト / 月）
- ✔ どの程度の期間に渡り分析を実施するか（例：3 ヶ月）
- ✔ どの程度ログを保存しておくか（例：1 年）
- ✔ SolitonNK へ投入する想定ログ量の増加について
- ✔ SolitonNK の冗長化は必要か

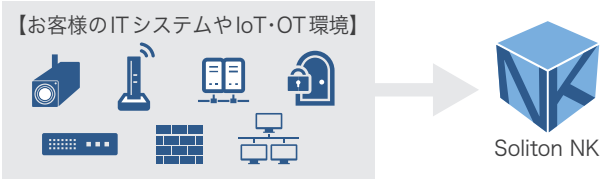
デモ実施中

Soliton NK はいつでもデモをご覧いただくことが可能です。
お気軽にお声がけください。

Soliton NK ４つの特徴

柔軟 データ形式不問・追加課金なしのデータ収集

データ形式を問わず収集が可能です。何のデータが役に立つかわからない状況で、まずはデータを集めるところから始められます。時間当たりのログ量に対する課金がないので取り込むログを絞り込む必要がありません。

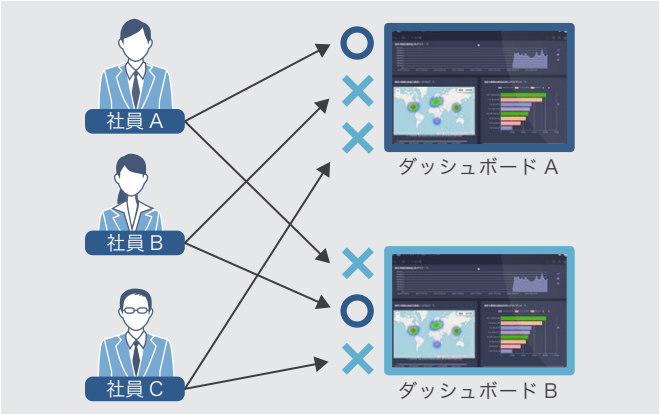


分析 コマンドを使って自由度の高い分析が可能

検索はもちろん、集計、可視化を柔軟に行うことができます。複数のログを組み合わせることや、簡単なスクリプトをコマンドに組み込むことも可能です。一度使ったコマンドは保存し、再利用、共有することができます。

運用 頻繁に使う分析結果をダッシュボードに保存して簡単アクセス

分析結果はダッシュボードに保存することができます。ダッシュボードにはクリック操作のみでアクセスすることができ、グループベースでアクセスコントロールをかけることも可能です。



自動 自動化処理を簡単に実現

ログ分析により明らかになった事象に対する自動対処機能をお客様自身で環境に合わせて開発することができます。他の機器やサービスと連携して、いわゆる SOAR（Security Orchestration Automation and Response）機能を実現することができます。

サイバー攻撃対策のご提案

Soliton NK を用いて、どのようなサイバー攻撃対策が可能かご提案できます。

- 工場のサイバーセキュリティ対策を計画・実施したい
- Active Directory周りのサイバーセキュリティ対策を計画・実施したい
- ネットワークトラフィックの可視化を実現したい

また、パイロット拠点における試験導入等についてもご提案できます。

Soliton®

株式会社ソリトンシステムズ https://www.soliton.co.jp/
〒160-0022 東京都新宿区新宿 2-4-3 TEL 03-5360-3811
お問い合わせはこちら https://www.soliton.co.jp/contact/

大阪営業所 06-7167-8881 福岡営業所 092-263-0400
名古屋営業所 052-217-9091 東北営業所 022-716-0766
札幌営業所 011-242-6111

SNK-2108AW