Infoscience

統合ログ管理シェア No.1「Logstorage」から生まれた国産SIEM

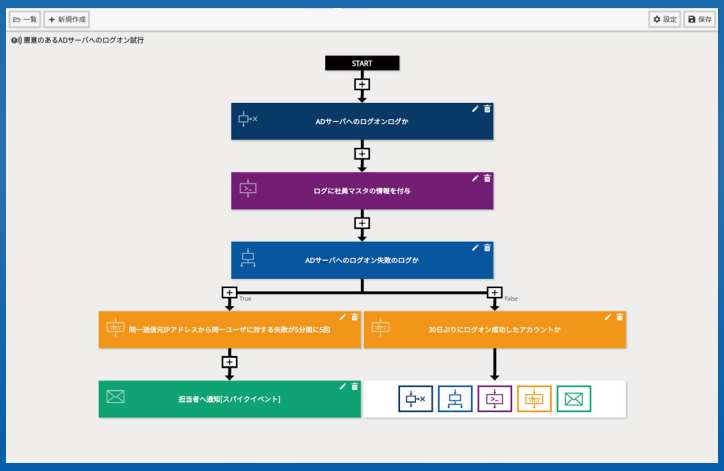
Logstorage-X /SIEM

logstorage.com

Logstorage-X/SIEM 統合ログ管理市場で圧倒的なシェアを持つ Logstorage が開発した純国産 SIEM 製品です。

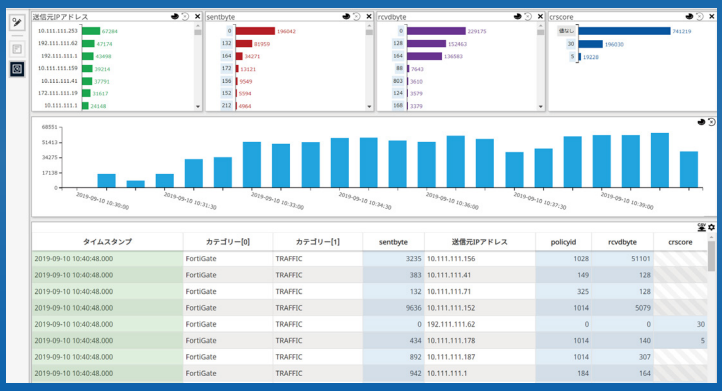
情報システム部門で設計・運用可能　運用が容易な Logstorage のコンセプトを踏襲

アラートまでのフローが可視化できるルール作成画面



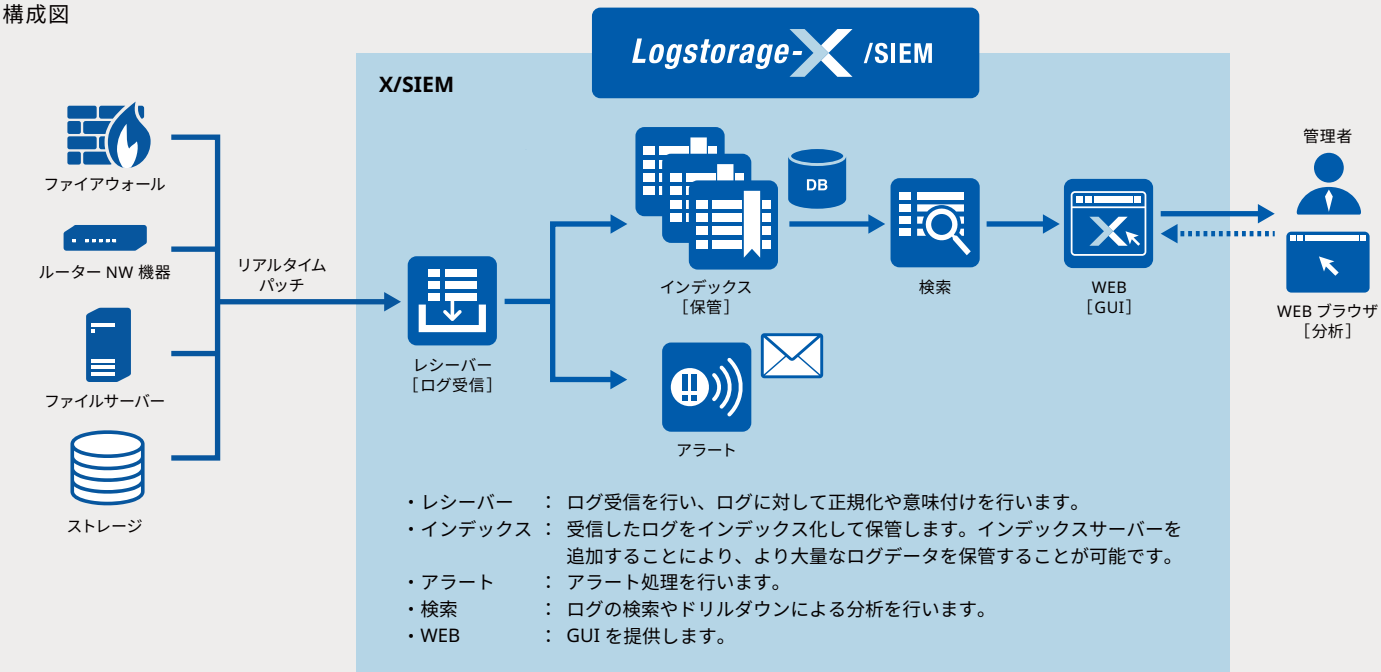
ある一部分の条件や閾値を運用しながらチューニング可能です。

分析画面によるドリルダウン



リアルタイムにログの状況を集計やタイムラインのグラフ、および一覧で確認できます。グラフや一覧の値をクリックすることでドリルダウンが可能です。

構成図



- レシーバー　：ログ受信を行い、ログに対して正規化や意味付けを行います。
- インデックス：受信したログをインデックス化して保管します。インデックスサーバーを追加することにより、より大量なログデータを保管することが可能です。
- アラート　：アラート処理を行います。
- 検索　：ログの検索やドリルダウンによる分析を行います。
- WEB　：GUI を提供します。

純国産

国内企業だからこそできる親切・丁寧なサポート

日本国内の情報システム部門で検討しやすい価格帯

ライセンス体系

0.5GB　1GB　2GB　5GB　10GB　20GB　30GB　40GB　50GB　100GB　100GB ～　MSP 向け

1 日あたりのログ受信量によるライセンスとなります。ログ量は過去 30 日間で 1 日あたりの平均の上限バイト数とします。

セキュリティ脅威へのリアルタイム検知を実現し、IT 部門の継続運用を支援します。

コマンドによる相関分析

```
search 'meta.cat = "proxy"' |
group IP (subsearch 'meta.cat = "FireWall" and IP = ${log.IP}' )
```

Proxy ログに含まれる IP アドレスと同じ IP アドレスを持つファイアウォールのログを検索

タイムスタンプ	カテゴリー	IP アドレス	URL
2017/06/23 10:56:31	proxy	192.168.0.1	http://xxx.com/
2017/06/23 10:56:31	proxy	192.168.0.3	http://xxx.com/
2017/06/23 10:56:31	proxy	192.168.0.1	http://xxx.com/
2017/06/23 10:56:32	proxy	192.168.0.2	http://xxx.com/
2017/06/23 10:56:32	proxy	192.168.0.1	http://xxx.com/

Proxy のログ

タイムスタンプ	カテゴリー	IP アドレス	URL
2017/06/23 10:56:37	FireWall	192.168.0.1	http://xxx.com/
2017/06/23 10:56:37	FireWall	192.168.0.3	http://xxx.com/
2017/06/23 10:56:37	FireWall	192.168.0.3	http://xxx.com/
2017/06/23 10:56:37	FireWall	192.168.0.3	http://xxx.com/
2017/06/23 10:56:39	FireWall	192.168.0.2	http://xxx.com/

ファイアウォールのログ

人手間では

一旦ある条件で検索し、その結果を控えておきます。
控えた結果を元に別の種類のログを検索します。

▼

X/SIEM のコマンドを利用すると

ある条件で抽出した内容を元に別の種類のログに対して
2 次検索を行うといった柔軟な検索を 1 回で行うことが可能です。

実際に役立つルールとログフォーマットのテンプレート

- 日本国内の実情に即したルールのテンプレートをご用意しています。テンプレートを有効化することで即運用に入ることが可能です。
- 代表的なセキュリティ機器のログや Windows イベントログのフォーマットをテンプレートとしてご用意しています。

機能一覧

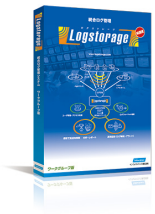
レシーバー機能 （ログ収集方式）	・Agent によるリアルタイムログ収集※ ・Syslog によるログ収集 ・ELC によるイベントログ収集※ ・受信時にコマンドを利用してログデータを加工する機能 ※詳細は Logstorage のパンフレットをご参照下さい。	アラート機能 （検知）	・シナリオベースのアラート条件の作成 ・相関分析ルールの作成 ・フローチャートのようにアラート条件を作成できる UI ・条件の一部部分や閾値を容易にチューニングできる UI ・通知をまとめ、通知量を調整する機能 ・アラート履歴機能 ・傾向分析機能
インデックス機能 （ログ保管）	・企業内のあらゆるログを一元管理 ・インデックス化による保管機能 ・生ログ (出力時の状態) 保管機能 ・インデックスデータの分散保管機能	カテゴリー機能 （ログフォーマット管理）	・ログに対して意味付けや値の正規化を行う機能 ・ログフォーマットフリー
検索機能 （検索・分析・集計）	・大量のログに対する高速検索 ・分析画面による集計グラフ表示機能 ・分析画面によるタイムライン表示機能 ・分析画面によるドリルダウン機能 ・コマンドを利用した相関分析機能	ログ転送機能	・Logstorage へのログ転送： マスター情報を付与したログデータの転送 サマリーログの転送
Agent 機能	・UDP/TCP/LLTP（独自プロトコル）によるログの送信 ・Windows イベントログを送信 ・ログの暗号化送信機能 ・ログ送信時のフィルタリング機能 ・高負荷時の動作抑制機能（ロードアベレージ、CPU 使用率）		・Agent ダウン時のリカバリ（ダウン直前からのログ送信）機能 ・LogGate ダウン時のスワップ（ダウン直前のログー時保管）機能 ・複数行ログ（ブロックログ）対応 ・複数のディレクトリに出力されるログの収集機能
ELC 機能	・Windows イベントログの収集機能 ・VMWare イベントログの収集機能 ・EMC イベントログの収集機能 ・NetApp イベントログの収集機能 ・NetApp ステータスログの収集機能 ・Unix 系 OS のログ収集機能		・検索機能と同様の条件指定による検知条件の作成 ・イベントログをコンパクトにする解析機能 ・イベントログ用のログフォーマットテンプレート ・指定時間間隔でのログ収集機能

（注）SIEM 製品：Security Information and Event Management の略称です。様々な機器やソフトウェアのログを一元的に保管・管理し、セキュリティ脅威となる事象をリアルタイムに検知・分析するセキュリティソフトです。

「Logstorage」から生まれた国産 SIEM

Logstorage-X /SIEM

セキュリティ脅威のリアルタイム検知に対応



統合ログ管理システム

Logstorage

ログの運用管理、バックアップ、検索・集計、
セキュリティ監視ツールの決定版！

製品のお問い合わせ先

インフォサイエンス株式会社 プロダクト事業部

メール：info@logstorage.com　電話：03-5427-3503

URL：https://logstorage.com/

■ 開発元

Infoscience インフォサイエンス株式会社

〒108-0023 東京都港区芝浦 2-4-1 インフォサイエンスビル

TEL.03-5427-3503　FAX.03-5427-3889

https://www.infoscience.co.jp/　E-mail: info@logstorage.com

■ 販売代理店

※価格のお問い合わせは、販売店またはインフォサイエンスの営業まで。

PP-202211