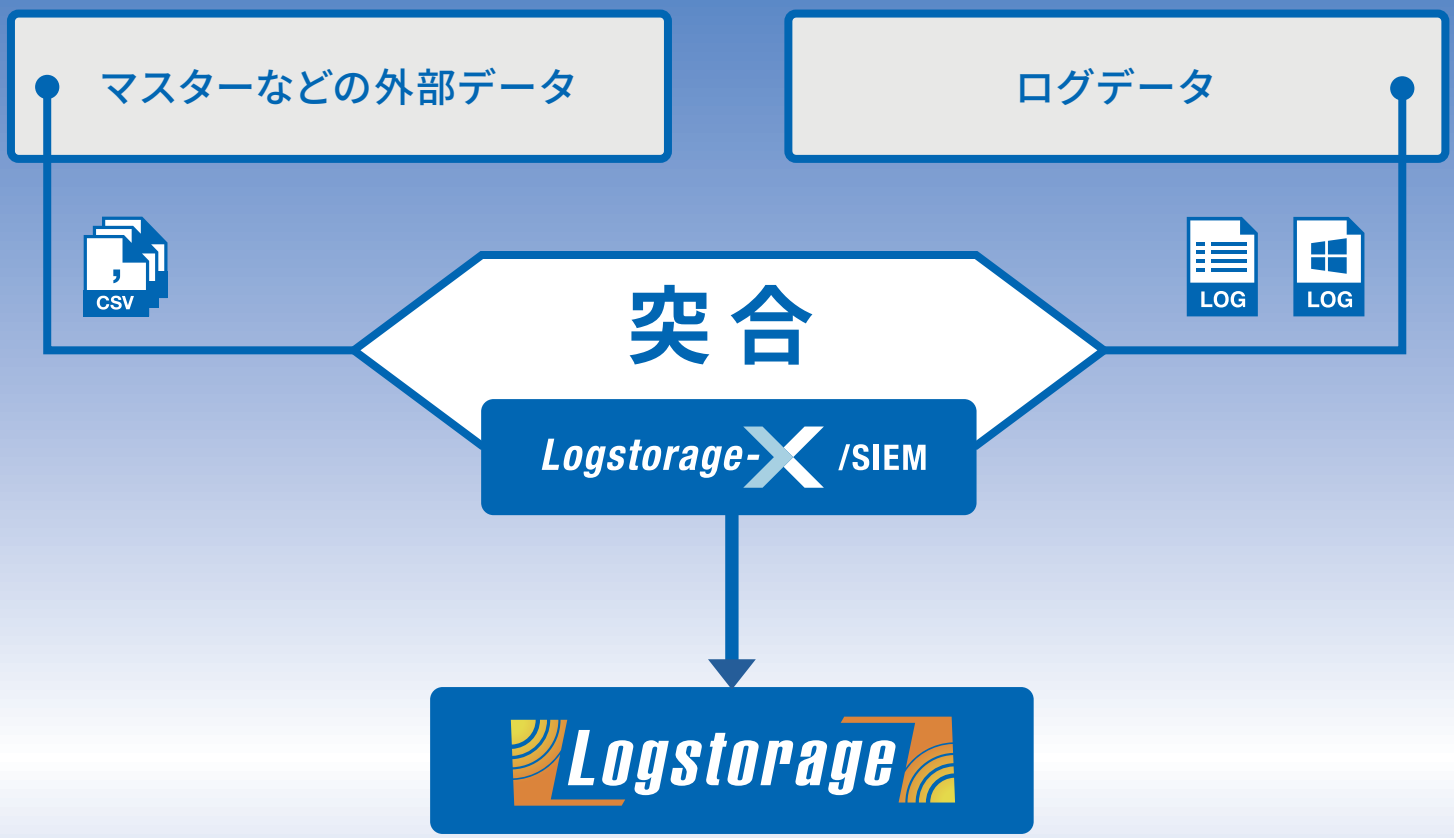
Infoscience



突合コマンド・オプション

Logstorage-X/SIEM のコマンド機能を利用し、外部データとの突き合わせ処理の自動化を実現

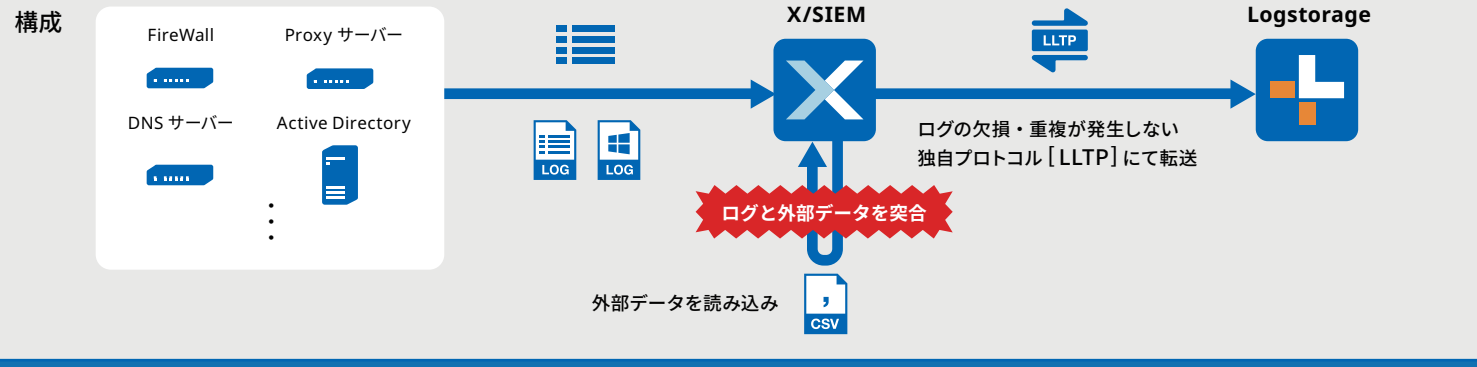
人事マスターや機器管理台帳などの情報をログに付与することで、どの部署の誰であるかの把握、管理下の機器であるかの判別が可能となります。
Logstorageでのログ管理をより幅広いものへと導きます。

Logstorage の突合コマンド・オプション

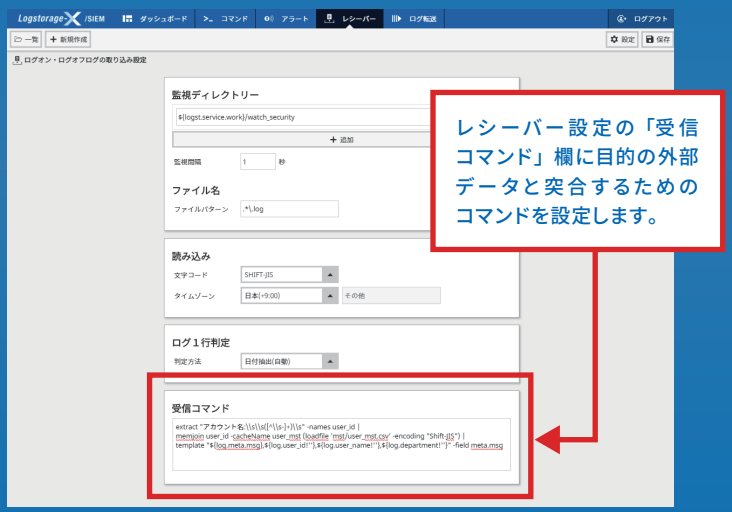
Logstorage-X/SIEMのコマンドを利用してマスターなど外部データの情報をログに付与し、Logstorageへ転送します。
Logstorage-X/SIEMのコマンド機能・レシーバー機能・インデックス機能・ログ転送機能が使用できるLogstorageのオプションです。

- 既存の Logstorage をこれまで通り利用可能
- 外部データと突合するための独自プログラムの作成が不要
- 製品バージョンによらずサポートを継続
- メンテナンス性が高い
- 属人性の排除
- 運用保守の負担を軽減

構成



突合処理



Logstorage-X/SIEM レシーバー設定画面

外部データと突合されたログを用いてレポーティング

作業申請データ

申請者	作業予定日	作業対象サーバ	使用アカウント	作業内容
山田太郎	2017/06/23 10:00-12:00	OraServ01	mente	ユーザ「admin」の削除。

突合

アクセスログ（実作業ログ）

2017/06/23 10:05:22	OraServ01	mente	ログイン
2017/06/23 11:29:03	OraServ01	yamada	ログイン
2017/06/23 13:10:54	OraServ01	mente	ログイン
…			

突合レポート

日時	サーバ	アカウント	判定	内容
2017/06/23 10:05:22	OraServ01	mente	OK	申請あり
2017/06/23 11:29:03	OraServ01	yamada	NG	申請なし
2017/06/23 13:10:54	OraServ01	mente	NG	申請あり、作業時間外

突合結果

Logstorage でのログ管理をより幅広く

■ 人事マスター × ファイルアクセスログ

社員名簿とファイルアクセス時に出力されるログを突き合わせることで、関係のない部署に所属する社員による不必要なアクセスを発見できるようになります。

■ 機器管理台帳 × デバイスの IP アドレス

機器管理台帳（デバイスのマスター）と突き合わせることで、台帳に含まれていない IP アドレスから出力されたログであるかを判別し、管理外の PC やネットワーク機器を特定できるようになります。

■ 残業・休出申請 × 入退出ログ

深夜時間の退出ログや休日の入出ログと申請台帳を突き合わせることで、申請外の入退出かを発見できるようになります。

■ レピュテーション DB × 送信元 / 送信先 IP アドレス・URL

レピュテーション DB（脅威情報）と送信元 / 送信先の IP アドレス・URL を突き合わせることで、危険度の情報をログに付与することができます。

※Logstorage および Logstorage-X/SIEM はインフォサイエンス株式会社の登録商標です。※Logstorage および Logstorage-X/SIEM はインフォサイエンス株式会社が開発しました。
※本資料に掲載されている内容は予告無く変更する場合があります。

■ 開発元・お問合せ先
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 https://www.infoscience.co.jp/
TEL.03-5427-3503 FAX.03-5427-3889 E-mail: info@logstorage.com

LF_202303