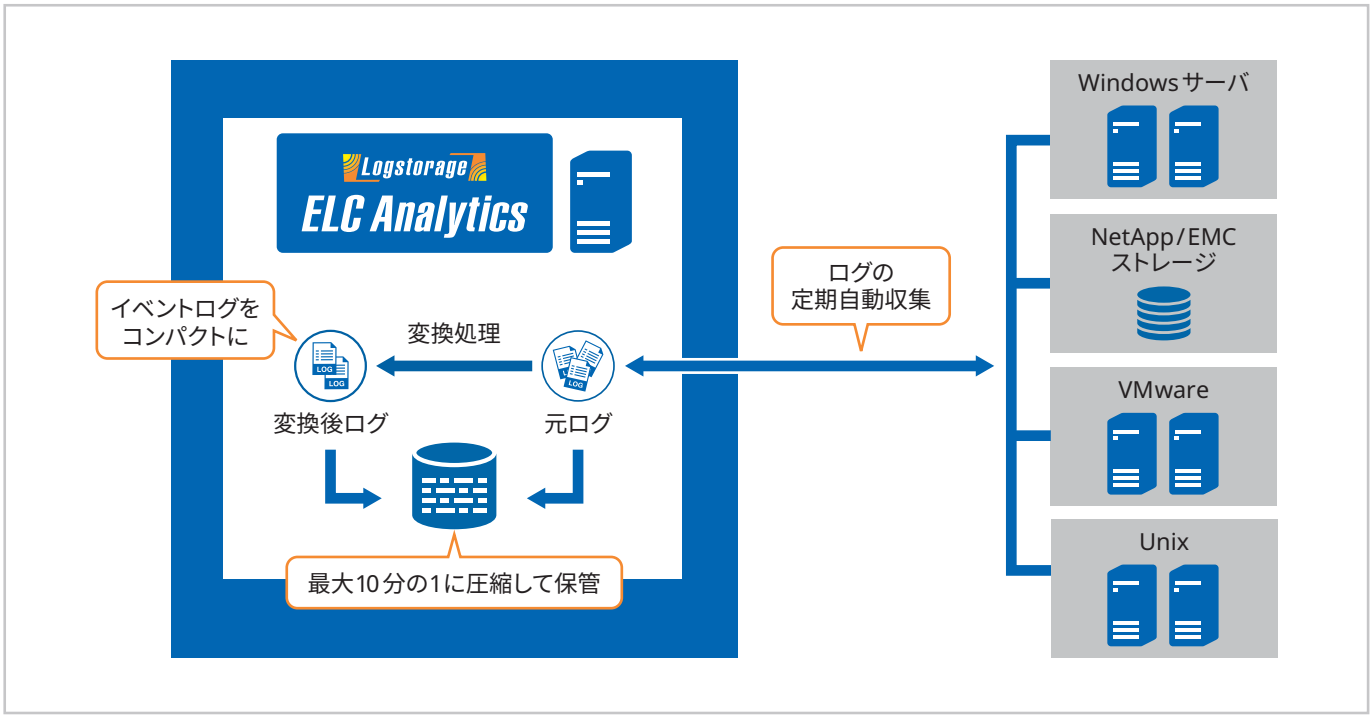
Infoscience

サーバログの管理機能がオールインワン

Logstorage ELC Analytics

ELC Analyticsの特長

ELC Analytics（イー・エル・シー・アナリティクス）は、サーバのアクセスログやステータスログを「収集・解析」「保管」「検索・分析」「レポート」するための、サーバログ管理ツールです。セキュリティ対策、システム監査などの他、ストレージ・リソースの利用状況の把握など、幅広く活用することができます。



収集・解析

- エージェントレスによる自動ログ収集機能
- イベントログの解析／変換機能

保管

- ログの圧縮保存／高速検索機能
- ログの暗号化／改ざんチェック機能
- ログの自動アーカイブ機能

分析

- ログの検索／集計／レポート
- 検索結果からクリック操作による絞込み
- レポートの定期自動出力

サーバログの管理機能をフル装備！

複雑なログを見やすく

OSのイベントログは複雑で、そのままの形で保管しても、それを分析する事は極めて困難です。
ELC Analyticsはイベントログを変換し「誰が」「いつ」「何に対して」「何をしたか?」という、実際のユーザ操作に変換することが可能です。

膨大なログを圧縮保管

ログは膨大な量になりやすく、その保管は頭の痛い問題です。
ELC Analyticsは、独自開発したログ専用のデータベース「LogDB」を内部で使用しており、高い圧縮率でログを保管しつつ、高速な検索・分析を行うことが可能です。

データベース不要

多くのログ管理製品ではRDBMSを外部に用意する必要があり、ライセンス上、また性能上の問題を抱えている事が少なくありません。
ELC Analyticsは「LogDB」を内部で使用しており、外部にRDBMSなどを必要としません。

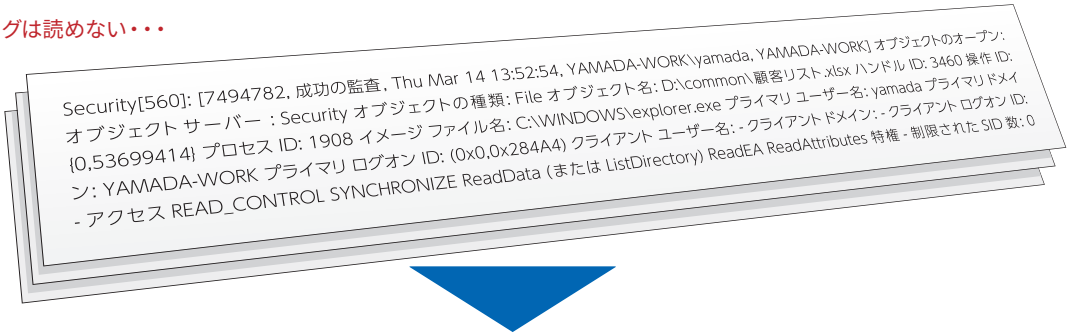
ストレージの利用効率も向上

NetAppストレージ向けに「ステータスコレクタ機能」を持っています。これは、NetAppストレージのリソース使用状況を収集・管理する機能で、ストレージの適切なリソース配分を行い、利用効率を劇的に改善することが可能です。

イベントログを分かり易く！

イベントログは、そのままの形式では内容の理解が非常に困難です。例えば、Windows OS 上で1度ファイルをオープンしただけで、10レコード以上のログが出力される事があります。
イベントログを正しく管理・監査する為には、ユーザの操作とログを結びつける解析処理が必須です。

生ログは読めない・・・



ELC Analytics は複雑なログを解析し、人間が見て理解できる形式に変換します

日時	サーバ名	アクション	ドメイン名	ユーザ	接続元ホスト名	接続元IPアドレス	成功／失敗
2021-03-01 01:00:00	FS01	ログオン（リモート認証）	infoscience	yamada	YAMADA-WORK	192.168.0.1	成功

日時	サーバ名	アクション	ドメイン名	ユーザ	ファイルパス	ファイル名	成功／失敗
2021-03-01 00:00:00	FS01	ファイル読み込み	infoscience	yamada	D:¥common¥	顧客リスト.xls	成功
2021-03-01 01:00:00	FS01	ファイル書き込み	infoscience	yamada	D:¥common¥	顧客リスト.xls	成功

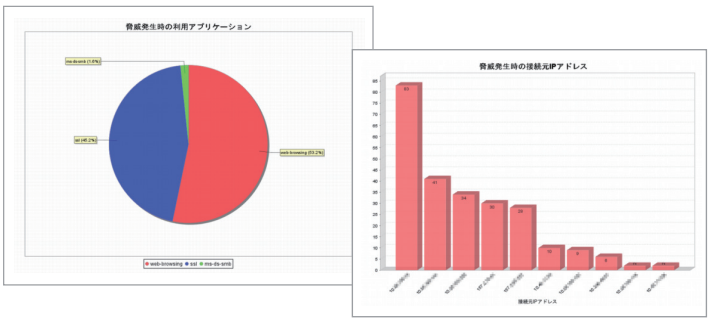
ログ可視化機能

高速に検索・追跡！

異なるサーバやデバイスから出力される、フォーマットの異なるログを横断的に検索でき、また検索結果からクリック操作で追跡できますので、ユーザの行動や、ファイルの流れ、エラーの原因など、高度なスキル無しに調査が可能になります。

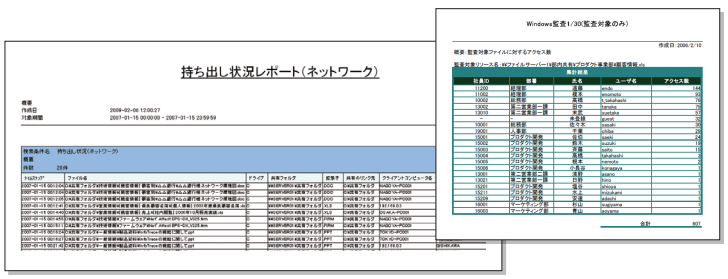
多角的に分析！

ユーザ毎のログイン回数、時間帯毎のアラート発生回数など、集計条件の縦軸、横軸に任意の項目を選択することで、様々な角度からログの分析が行えます。
また、円グラフ、折れ線グラフ、棒グラフなど、様々なグラフで表示できますので、視覚的にも分かり易く状況が把握できます。



定期的にレポート！

PCIDSS/ISMS・内部統制対応など、監査に対応するレポートを、日次や月次などのタイミングで自動的に出力できます。
作成されたレポートはメールに添付して送信することもできますので、継続的なログのモニタリングが容易になります。



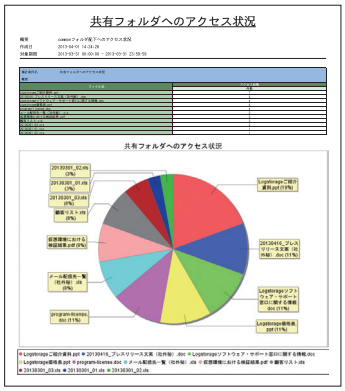
ログの分析機能

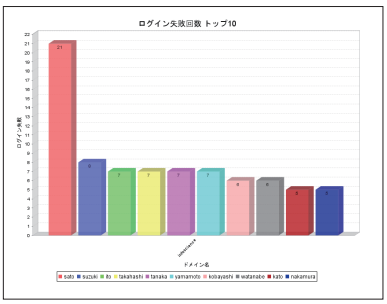
ログの検索が自由自在！

イベントログの横断検索や、クリック操作によるログの追跡により、ユーザの行動やファイルの流れ、エラーの原因など、高度なスキル無しに調査・把握が可能になります。

あらゆる角度から分析！

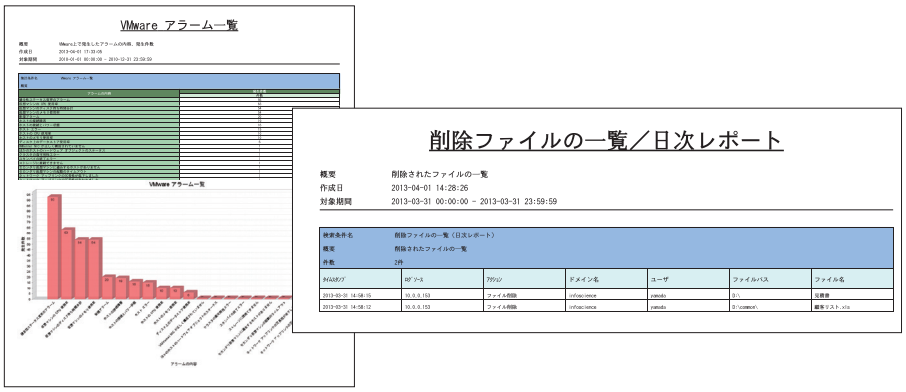
ユーザ毎のログイン回数や、時間帯毎のストレージの利用状況など、集計条件の縦軸、横軸に任意の項目を指定することで、様々な角度からログの分析が行えます。
また、円、折れ線、棒など、様々なグラフで表示できますので、視覚的にも分かり易く状況が把握できます。





モニタリングを自動化！

内部統制やセキュリティ基準への準拠など、監査に対応するレポートを日次や月次で定期的に作成することができます。
作成されたレポートを自動的にメールに添付して送信することも可能ですので、継続的なログのモニタリングが容易になります。



ログの保管機能

暗号化機能

AESやBlowfishなどの暗号方式を用い、収集したログを暗号化して保管する事が可能ですので、ログからの情報漏えいを防止できます。

圧縮機能

収集したログを最大で10分の1に圧縮して保管しますので、ログ保管に用いるストレージのコストを大幅にカットできます。

改ざん検出機能

収集したログデータに対するハッシュ値を管理、チェックする機能により、ログが改ざんされていないことの証明が可能です。

ユーザグループ管理機能

利用できる機能や閲覧できるログをユーザ、グループ毎に制限することができますので、権限に応じたアクセスコントロールが可能です。

機能一覧

機能	詳細
ログの収集・解析機能	・エージェントレスによるログの自動収集 ・イベントログの解析 ・ログ収集時にあらかじめ登録された外部マスタとの連携
ログの保管機能	・大量ログの圧縮保管 ・生ログ保管 ・指定期間を超えたログのアーカイブ/削除 ・ログの改ざんチェック
検索機能	・大量ログに対する高速検索 ・AND/OR/正規表現などによる検索条件指定 ・検索条件の保存 ・検索結果からの絞り込み(トラッキング) ・検索の中断 ・特定ログのハイライト表示
集計・分析機能	・表、棒グラフ、折れ線グラフ、円グラフによる集計結果出力 ・ログの件数、最大、最小、平均、合計、標準偏差の出力 ・集計結果のトップ表示 ・集計条件の保存 ・集計の中断 ・集計結果のCSVダウンロード
レポート機能	・毎月、毎週、毎日、毎時の自動レポート作成 ・PDF,CSV,HTML,TXT,XMLフォーマットでのレポート作成 ・レポートのメール添付送信 ・コマンドラインによるレポート作成実行
ユーザ管理機能	・グループ、ユーザ単位によるアクセス制御機能 ・LDAP/ADによるユーザ認証の連携
その他管理機能	・コンソールとのSSL通信 ・監査ログ出力 ・他のログサーバへのログ転送 ・各種設定条件のインポート、エクスポート機能

統合ログ管理システム「Logstorage」へのアップグレード

ELC Analyticsから統合ログ管理システム「Logstorage」にアップグレードにより、様々なアプリケーションやデバイスのログなど、サーバ以外のログも統合管理する事が可能になります。
ELC Analyticsからのアップグレード・パスが用意されており、スムーズな移行が可能です。

取得できるログの一覧

＜Windows / NetApp / EMC 監査ログ＞

操作	Windows	NetApp	EMC
ログオン・ログオフ	○	○	○
アプリケーション起動・終了	○	○	○
ファイル読込み	○	○	○
ファイル書込み	○	○	○
ファイルリネーム	○	○	○
プリント	○	-	-
イベントログの消去	○	○	○
時刻の変更	○	-	○
タスクの登録・編集	○	-	-
サービスの登録	○	-	-
Windowsファイアウォール 作成・変更・削除	○	-	-
Windowsファイアウォール 有効化・無効化	○	-	-
Windowsファイアウォール ポート許可・拒否	○	-	-
管理者操作	○	○	○

＜VMwareイベント＞

イベント（操作）一覧				
アップグレード	クラスタ	テンプレートアップグレード	ホスト	仮想マシン
アラーム	スケジュール設定タスク	データストア	ライセンス	許可
カスタムフィールド	セッション	データセンター	リソースプール	その他

＜Unixコマンド＞

ログソースOS	収集可能なログ
RHEL / CentOS	ログイン成功 (last), ログイン失敗 (lastb), ファイル転送 (scp), 任意コマンド (シェルスクリプト)
AIX	ログイン成功 (last), ログイン失敗 (who), ファイル転送 (scp), 任意コマンド (シェルスクリプト)
Solaris	ログイン成功 (last), ファイル転送 (scp), 任意コマンド (シェルスクリプト)
その他のUnix OS	ファイル転送 (scp), 任意コマンド (シェルスクリプト)

＜NetAppステータスログ＞

ログの種類	ログの項目
アグリゲート	name, size-total, files-total, size-used, size-percentage-used, size-availavble, files-used, files-private-used, state, mount-state, mirror-status, raid-status
ボリューム	Name, size-total, files-total, size-used, percentage-used, size-available, files-used, files-private-used, state, raid-status, mirror-status, containing-aggregate
クォータ	quota-type, quota-target, quota-user-name, quota-user-id, tree, volume, disk-used, disk-limit, soft-dislk-limit, threshold, files-used, file-limit, soft-file-limit
システム	sys_read_latency, sys_write_latency, sys_avg_latency, net_data_recv, net_data_sent, disk_data_read, disk_date_written, cpu_busy, avg_processor_busy, total_processor_busy

取得ログサンプル

＜認証ログ＞
「いつ」「誰が」Windows 認証を行ったかを記録します。

日時	サーバー名	アクション	ドメイン名	ユーザー	接続元ホスト名	接続元 IP アドレス	成功 / 失敗
2022-03-01-00:00:00	FS01	ログオン（ローカル認証）	infoscience	yamada	–	–	成功
2022-03-01-01:00:00	FS01	ログオン（リモート認証）	infoscience	yamada	YAMADA-WORK	192.168.0.1	成功
2022-03-01-02:00:00	FS01	ログオン（リモート認証）	infoscience	yamada	–	–	–

＜ファイルアクセスログ＞
「いつ」「誰が」ファイルにアクセスしたかを記録します。

日時	サーバー名	アクション	ドメイン名	ユーザー	ファイルパス	ファイル名	成功 / 失敗
2022-03-01-00:00:00	FS01	ファイル読み込み	infoscience	yamada	D:¥common¥	顧客リスト.xlsx	成功
2022-03-01-01:00:00	FS01	ファイル書き込み	infoscience	yamada	D:¥common¥	顧客リスト.xlsx	成功
2022-03-01-02:00:00	FS01	ファイルリネーム	infoscience	yamada	D:¥common	コピー～顧客リスト.xlsx	–
2022-03-01-03:00:00	FS01	ファイル削除	infoscience	yamada	D:¥common	コピー～顧客リスト.xlsx	成功

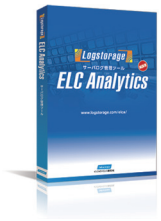
＜セキュリティイベントログの消去＞
「いつ」「誰が」セキュリティイベントログを消去したのかを記録します。

日時	サーバー名	アクション	ドメイン名	ユーザー
2022-03-01-00:00:00	FS01	セキュリティイベントログの消去	infoscience	yamada

＜管理者操作ログ＞
「ユーザの新規登録」や「ポリシー変更」など、特権管理者しか行えない操作履歴を記録します。

日時	サーバー名	アクション	ドメイン名	ユーザー	操作の詳細
2022-03-01-00:00:00	FS01	管理者操作	infoscience	Administrator	ユーザーアカウントの作成：FS01 TEST_USER
2022-03-01-01:00:00	FS01	管理者操作	infoscience	Administrator	ユーザーアカウントの変更：FS01 USER_A
2022-03-01-02:00:00	FS01	管理者操作	infoscience	Administrator	ユーザーアカウントの削除：FS01 TEST_USER
2022-03-01-03:00:00	FS01	管理者操作	infoscience	Administrator	グループの作成：FS01 GROUP_A
2022-03-01-04:00:00	FS01	管理者操作	infoscience	Administrator	グループの変更：FS01 GROUP_A
2022-03-01-05:00:00	FS01	管理者操作	infoscience	Administrator	グループの削除：FS01 GROUP_A
2022-03-01-06:00:00	FS01	管理者操作	infoscience	Administrator	グループにユーザの追加：Builtin Administrators に FS01 TEST_USER が追加された
2022-03-01-07:00:00	FS01	管理者操作	infoscience	Administrator	グループのユーザの削除：Builtin Administrators の FS01 TEST_USER が削 除された
2022-03-01-08:00:00	FS01	管理者操作	infoscience	Administrator	ポリシー設定の変更：監査ポリシーの変更

（注）統合ログ管理システム：インフォサイエンスが提唱するログを管理するために必要な機能を実現したシステムの総称。ログを蓄積するだけではなく、セキュリティ管理、データバックアップ等、ログを取り巻く多岐にわたる目的に対応したシステム。



サーバログ管理ツール

Logstorage
ELC Analytics

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-202303