LogStareシリーズ 機能一覧

監視・ログ管理 機能一覧

C: LogStare Collector, R: LogStare Reporter, M: LogStare Manager, Q: LogStare Quint,
NX: 次期対応予定, AL: 連携による機能

監視（C・Q）
- Ping監視
- SNMP監視
- PORT監視
- SNMPトラップ監視
- URL監視（外形監視）
- 応答コード監視（死活監視）
- METRICS監視（時系列による差分閾値監視）
- 改ざん監視（前回）
- 改ざん監視（原本）
- レスポンスタイム監視
- 文書指定文字列監視
- トラフィック監視
- リソース監視（性能監視）
- インターフェース監視
- ログ監視（テキストマッチング）
- Ping監視のエラー判定指定(注意回数・警告回数)

ログ収集（C・Q）
- SYSLOG(TCP)によるログ収集
- SYSLOG(UDP)によるログ収集
- WMIによるWindowsログ収集
- FTP (put) / FTP (get)による定期的なログ収集
- SCPによるログ収集
- HTTP(S)によるログ収集
- COPY(local)によるログ収集
- MOVE(local)によるログ収集
- 圧縮されたファイルのログ収集
- ログ収集時の特定文字列フィルタリングによるログ収集
- ログ収集時の一定時間内にログ収集が無い状態の検知
- ログ収集時の特定文字列があった場合のアラート
- 収集時の1回に収集できる最大取得件数指定
- NetFlowによるログ収集（AL）
- ログ受信時のマスタデータとの紐づけ機能
- ログ受信時の事前処理カスタマイズ機能

ログ検索（C・R・Q）
- キーワードによる検索
- 正規表現にマッチする・マッチしないによる検索
- 含む・含まない・一致・異なる・開始・終了による検索
- 複数ログの横断検索
- 条件複数指定による検索
- 各条件のAND、ORによる組み合わせ検索
- 直近指定時間(3分・1時間・今日・昨日等)範囲指定検索
- 任意の期間範囲指定検索
- 検索結果のダウンロード（CSV等加工可能なテキスト形式）
- インデックスによるログの高速検索（R・Q）
- サーバー分散構成によるログの高速検索（R・Q）

アラート・検知（C・R・Q）
- ログインやエラー等任意の文字を含むログ検知
- 条件に該当した監視データの検知
- 検知条件条件の複数指定
- 複数項目指定（ログ種別詳細・イベントや検知タイプ・攻撃回数）
- IPアドレスからのログアラート指定（IPアドレスの特定値・前方一致等）
- ログ検知時の通知メール
- ログ検知時のSlack/ChatWork/Teams等への通知
- 一定時間内にログ収集が無い場合のアラート通知

分析・レポート（R・Q）
- 特定ログのドリルダウン分析
- 複数ログの相関分析
- 外部ファイル（PDFファイル）への出力
- 標準で用意された集計軸の集計レポート出力
- 任意の条件に従って設定する集計レポート出力
- 定期自動レポート作成（日・週・月・ログ取得対象の指定日前）
- レポートの自動メール添付

ダッシュボード・リアルタイムモニタリング（C・R・Q）
- 該当デバイスのリアルタイムステータス表示（取得失敗・警告等）
- 任意のデバイスを複数指定表示
- 任意の表示項目(CPUやメモリ使用率/ログ件数)を指定表示
- 複数ダッシュボード指定表示
- 円グラフ・折れ線・インタフェースアイコン
- ダッシュボード表示期間指定(1時間/6時間/1日/7日/任意範囲等)
- 更新周期設定（5分/10分/1時間）
- 手動によるダッシュボード更新表示

DSV（Dynamic Status Viewer）（C・R・Q）
- 標準アイコンによるネットワーク図（デバイス配置図）作成
- 日本地図や任意のマップ・建物などのインポート
- 視覚的なアイコンによるデバイスのリアルタイム異常・障害表示
- デバイスアイコンからのドリルダウン分析

ログパーサー（ログフォーマット定義）（R・Q）
- 標準テンプレートによる収集ログの解析
- 独自形式のログに対する任意のテンプレート作成
- かんたん設定によるテンプレート自動作成・解析
- 複数フォーマット（SSV/CSV/TSB/JSON）に対応
- Key-Value形式に対応
- ログ取得開始位置指定
- テンプレート作成時のサンプルログ読み込み機能
- ログカラムの型（日付・文字・数値）とカラムサイズ指定

AI予測（R・Q）
- AIによるコンピュータリソース使用状況など定量的なデータの将来予測

ユーザー管理機能（C・R・Q）
- ユーザ毎のアクセスコントロール

その他機能
- 監視対象デバイスのグルーピング
- 次世代SIEMとの連携（C）
- 管理サーバー冗長化機能（Q）
- 管理サーバー分散化機能（Q）
- 設定エクスポート機能
- サポートデータエクスポート機能（C）
- IPV6対応（NX）
- 生ログ保存・出力機能
- ログ転送機能
- 監視対象デバイスのステータス異常時通知機能
- お知らせや最新情報の通知機能

ログ管理機能
- 監視データ・ログの高圧縮保管機能
- 監視データ・ログの長期間保管機能
- ログ暗号化機能（C）
- 監視データ・ログのリストア機能（NX）

運用サービス（R・M）
- ２４時間３６５日監視
- 異常ステータス等のアラート通知

サポートサービス（R・M）
- 定期レポート報告会等
- セキュリティ関連の課題サポート・ドキュメント作成・コンサル等

対応OS・動作環境

LogStare Collector
- Red Hat Enterprise Linux 7 / 8
- Windows Server 2012 R2 / 2016 / 2019
- ※上記対応OSが動作するクラウド基盤・仮想環境も可
- CPU ：Intel 互換 2GHz 4コア以上
- メモリ：4GB以上
- ブラウザ：最新版Google Chrome, Chromium版Edge, Internet Explorer 11（非推奨）

LogStare Reporter
- SaaSサービスへアクセスできるネットワーク環境
- ブラウザ：最新版Google Chrome, Chromium版Edge, Internet Explorer 11（非推奨）

LogStare Manager
- SaaSサービスへアクセスできるネットワーク環境
- ブラウザ：最新版Google Chrome, Chromium版Edge, Internet Explorer 11（非推奨）

LogStare Quint
- Red Hat Enterprise Linux 7 / 8
- Windows Server 2012 R2 / 2016 / 2019
- ※上記対応OSが動作するクラウド基盤・仮想環境も可
- CPU ：Intel 互換 2GHz 16コア以上
- メモリ：32GB以上
- ブラウザ：最新版Google Chrome, Chromium版Edge, Internet Explorer 11（非推奨）

ライセンス体系等

LogStare Collector（保守・サポート込み ※構築費別途）
初年度ライセンス
- LogStare Collector Pro 初年度ライセンス (LSCPRO-01)
- LogStare Collector Limited 監視 初年度ライセンス（LSCLMM-01）
- LogStare Collector Limited ログ 初年度ライセンス（LSCLML-01）

次年度ライセンス
- LogStare Collector Pro 次年度ライセンス 1年～ (M-LSCPRO-01)
- LogStare Collector Limited 監視 次年度ライセンス 1年～ (M-LSCLMM-01)
- LogStare Collector Limited ログ 次年度ライセンス 1年～ (M-LSCLML-01)

LogStare Reporter（サポート込み）
初期費用
- LogStare Reporter - 初期費用 (LSRINI-01)

年間ライセンス（監視レポート）
- LogStare Reporter - Monitor 20 Device 年間ライセンス 1年～ (LSRLMM-20)
- LogStare Reporter - Monitor 50 Device 年間ライセンス 1年～ (LSRLMM-50)
- LogStare Reporter - Monitor 100 Device 年間ライセンス 1年～ (LSRLMM-100)
- LogStare Reporter - Monitor 101台目以降追加10 Device 1年～ (LSRLMM-ADD10)

年間ライセンス（ログレポート）
- LogStare Reporter - Log 1 Device 年間ライセンス 1年～ (LSRLML-01)
- LogStare Reporter - Log 5 Device 年間ライセンス 1年～ (LSRLML-05)
- LogStare Reporter - Log 10 Device 年間ライセンス 1年～ (LSRLML-10)
- LogStare Reporter - Log 11台目以降追加1Device 1年～ (LSRLML-ADD1)

年間費用（追加オプション）
- LogStare Reporter ストレージ容量追加10GB (LSROP-S10G)

LogStare Manager
別途お見積り

LogStare Quint（保守・サポート込み ※構築費別途）
年間ライセンス（監視）
- LogStare Quint - Monitor 20 Device 年間ライセンス 1年～ (LSQLMM-20)
- LogStare Quint - Monitor 50 Device 年間ライセンス 1年～ (LSQLMM-50)
- LogStare Quint - Monitor 100 Device 年間ライセンス 1年～ (LSQLMM-100)
- LogStare Quint - Monitor 101台目以降追加10 Device 1年～ (LSQLMM-ADD10)

年間ライセンス（ログ）
- LogStare Quint - Log 1 Device 年間ライセンス 1年～ (LSQLML-01)
- LogStare Quint - Log 5 Device 年間ライセンス 1年～ (LSQLML-05)
- LogStare Quint - Log 10 Device 年間ライセンス 1年～ (LSQLML-10)
- LogStare Quint - Log 11台目以降追加1Device 1年～ (LSQLML-ADD1)