Ekran System
User activity videorecording system

Ekran v.5.0 の新機能

Rev. 1.0

2016.9.1

JTC-i Jupiter Technology corp. ジュピターテクノロジー

Ekran System
User activity videorecording system

Ekran（エクラン） v. 5.0 の変更点を紹介します。

- **Enterprise 版の機能**: Enterprise 版のシリアルキーをアクティベートすることで、Ekran の以下の機能が有効化されます。
  - **データベースのアーカイブ & クリーンアップ**: データベースのアーカイブ機能が追加されました。この機能により古くなった記録データをアーカイブしてサーバーコンピューターのディスクから削除し、容量の不足を防止することができます。アーカイブしたデータはセキュアなストレージに保存して、いつでもセッションプレイヤーで参照することができます。
  - **SIEM との統合**: Ekran のアラートイベントや記録済みデータを ArcSight または Splunk のインターフェースから参照、分析することが可能になりました。
  - **ワンタイム パスワード**: Windows Server へのログイン用にワンタイムパスワードを生成する機能が追加されました。Windows Server にログインするときに Ekran クライアントが表示する二次認証画面で、ユーザーは直接ワンタイムパスワードを要求できます。
  - **ハイ アベイラビリティ(HA)**: Ekran サーバーの HA 構成サポートが追加されました。これにより高レベルの運用パフォーマンスが実現され、ダウンタイムとサービスの中断を最小限に抑えることができます。

- **アラートのエクスポートとインポート**: 構成済みのアラートを.xml ファイルにエクスポートする機能が追加されました。エクスポートした .xml ファイルを他の Ekran でインポートすれば、同じアラートを再作成することなくすばやく展開することができます。
- **事前定義アラート**: Ekran のインストール後、直ちに使用できる事前定義済みアラートが追加されました。潜在的に有害または危険な操作が行われた時にアラートが生成されるよう、ルールが定義されています。
- **複数アラートの管理**: 複数アラートをまとめて管理する機能が追加されました。これによりアラートの編集がより簡単で効率的になりました。
- **アラートのリスクレベル**: アラートにリスクレベルを設定し、色分け表示する機能が追加されました。アラートイベントは、セッション一覧、セッションプレイヤー、最近のアラートダッシュボードで、リスクレベルに応じて色分けしてハイライト表示されます。これにより、重要なアラートイベントを一瞬で見分けることが可能になりました。
- **ログインメッセージへのユーザーの返信**: コンピューターへのログイン時に Ekran クライアントが表示するログインメッセージ画面で、ユーザーにコメントの入力を要求する機能が追加されました。システム管理者はコメントを確認することで、ユーザーのログインと操作の目的を把握することができます。
- **デジタル署名と改ざんの検知**: Windows で記録されたスクリーンショットと付随テキストにデジタル署名を行う機能が追加されました。この機能を有効にした場合、データベース内に保存さ

れた記録の改ざんの有無を確認できるようになります。

- **キーワードによる記録の開始**: ユーザーが特定のキーワードを入力した時に、ユーザー操作の記録を開始する機能が追加されました。この機能を使用すると、ユーザー操作を常に記録するのではなく、疑わしい操作があったときのみ記録を行うことができます。
- **レポートの追加**: レポート機能に、以下のレポートが追加されました。
  セッション一覧レポートは、Ekran クライアントをインストールしたコンピューターに注目して、コンピューターにログインした全ユーザーとユーザーの作業時間に関する詳細情報を提供します。
  ユーザー統計レポートは、ユーザーに注目して、ユーザーのログイン先コンピューター、ログイン元コンピューターの IP アドレス、そしてすべてのコンピューターでのユーザーの総作業時間に関する要約を提供します。
  USB ストレージ一覧レポートは、指定した時間中に発生した、すべての USB ストレージイベントに関する情報を提供します。
- **レポートの XML での出力**: レポートの出力フォーマットに .xml が追加されました。これにより、レポートの情報を外部ツールで活用することが可能になりました。

発行日　2016 年 9 月 1 日

ジュピターテクノロジー株式会社