

ユーザーによる脅威の 監視、検出、分析

増大する内部脅威と脆弱性

ユーザーによる企業データへの不正操作や、これによるビジネスへの被害は 2014 年以降増加し続けています。被害を受ける企業はマイナスイメージを被り、その回復は困難、かつその影響は長く尾を引きます。内部脅威に対する展望は今後ますます厳しくなり、セキュリティ監視の対象は、社内の従業員とシステム管理者だけでは収まらなくなっています。

現在では、ビジネスパートナー、サプライヤ、アクセス権限を与えられた委託業者、管理者権限を持つサードパーティサービスプロ

バイダの監査も必要となっているのです。このような状況下では、全てのユーザーの企業ネットワークにおける行動を正確に把握し、機密情報の取り扱いを分析し、サービスの品質を管理し、問題を調査し、全体を分析することが極めて重要です。

2014 年、40% の企業が情報漏洩を経験したか、またはコンプライアンス監査を達成できませんでした。89% の企業は内部脅威に対する何らかの脆弱性を感じています。*

ソリューション

Ekran は企業のセキュリティ監視のための、最新のソフトウェアソリューションです。Ekran は操作画面（ターミナル、ローカル PC、バーチャルマシン）を記録し、全てのユーザー操作を分析します。

Ekran を使うことで、サーバー上の設定変更や、その他ユーザー管理やシステム管理のアクションなど、あらゆる操作が可視化され、インシデント調査に必要なあらゆるデータが取得できます。Ekran が提供する検索可能な画面記録や、指定イベントに対するリアルタイムアラート機能、簡単に分析できる監視結果、柔軟なレポート生成機能は、企業が内部脅威から身を守り、内部データの悪用や競合企業との連絡、データとインフラの破壊、および不正行為等を抑止し、ならびに ISO、PCI、SOX、DPD を遵守するのに有用です。

機能

サーバーやワークステーションにインストールすると、Ekran クライアントは全てのログインユーザーの操作画面をビデオのように記録し、画面に対応するメタデータ（アクティブなアプリケーション名、現在開かれているウィンドウタイトル、URL、キーストロークなど）も同時に記録します。Ekran は、メタデータキーワードによる検索に加え、全ての画面記録に対する完全な再生機能を提供します。これにより、インシデント調査に必要なキーエピソードを素早く見つけ出すことができ、一般 / 特権ユーザーの操作を分析できるようになります。リアルタイムアラートはアラートが生成された瞬間の画面へのダイレクトリンクを含んでおり、これを活用することで事前対策的な管理が可能となります。

Ekran 無償版・トライアル版はこちらから

<https://www.jtc-i.co.jp/support/download/downloadlist.php>



Ekran

アメリカ、イギリス、韓国、スペイン、イスラエルなどワールドワイドな導入実績



特権ユーザー監視



コンプライアンス対策



市場のコストリーダー

国内販売代理店
ジュピターテクノロジー
株式会社
〒183-0023
東京都府中市宮町
2-15-13
第 15 三ツ木ビル 8F
TEL : 042-358-1250
FAX : 042-360-6221
URL : <http://www.jtc-i.co.jp/>

全てのインシデントを発見・調査・抑止

ユーザー操作を監視

— 全ての操作を記録した検索可能なビデオを作成

Ekran を使えば、システム管理者やその他の特権ユーザーを含む企業内のネットワークユーザーを管理し、常に全ての操作を明確にすることができます。

Ekran は全てのローカル、リモート、ターミナルセッションの完全な画面記録を作成します。Ekran があれば、何も隠すことはできません。ユーザーが行った操作は全て画面に映し出されます。これをキャプチャすることにより、画面記録システムは全ての状況に対応することができるのです。Ekran は、どのようなネットワークプロトコルでも、どのようなアプリケーションでも、どのようなタイプのアーキテクチャ（AD であっても非 AD ユーザーであっても）でも機能します。Ekran はターミナルサービス、VNC、リモートデスクトップ接続など様々な構成をサポートします。

監視結果を分析 — 疑わしいユーザー操作を発見

Ekran は特権ユーザーの操作を含む、全てのユーザーセッションを記録します。記録を妨害することはほとんど不可能です。画面記録はアクティブなアプリケーション名や開いたウィンドウのタイトル、URL アドレス、キーストロークなどのテキストメタデータでインデックス化されます。キーワード検索機能は過去にさかのぼってのユーザー操作の分析やインシデント調査に効果的です。アラート機能は疑わしいイベントやユーザー操作に素早く反応できるため、セキュリティに関する事前対策になります。またいつでも“ライブ”セッションに接続することができ、リアルタイムで何か起こっているかを知ることができます。

悪質な行動を調べる — 一連のイベントを再現

企業セキュリティに対する違反が疑われる場合、実際に何が起こったのか、誰が関与したのか、どんな操作が行われたのか、問題の範囲を特定することが難しいケースがほとんどです。Ekran は企業内の各コンピューターやターミナルサーバーで何が行われたのか、完全に詳細な情報を提供します。関連のある全てのコンピューターの記録を使えば、インシデントの正確な状況を再現し、決定を下すために必要な間違いのない事実を知ることができます。

ビデオエピソードのエクスポート機能で画面記録を証拠として、法執行機関や弁護士などの適切な関係者と共有したり、社内ミーティングでマネージャーや幹部に提示したりすることができます。

ワールドワイドな導入実績

BBVA

renfe

bankinter.

서울대학교
SEOUL NATIONAL UNIVERSITY

YBM Si-sa

tel

Redsys

VIRTUAL OFFICEWARE
HEALTHCARE SOLUTIONS

헌법재판소



Ekran



ターミナル、リモート、ローカルユーザーセッションを記録



ビデオ再生とキーワード検索



リアルタイムアラートと“ライブ”セッションのリアルタイム再生

※記載の会社名及び商品名は、各社の商標または登録商標です。

H28.7.22

STC-i ジュピターテクノロジー

【本社】〒183-0023 東京都府中市宮町2-15-13 第15三ツ木ビル8F
TEL:042-358-1250 FAX:042-360-6221
【大阪営業所】〒530-0001 大阪府大阪市北区梅田1-1-3
大阪駅前第3ビル11F
TEL:06-6131-8471 FAX:06-6131-8472
【URL】<http://www.jtc-i.co.jp/>