eltes

SOFTWARE PACKAGE
RUNEXY

そのログ 本当に活かせてますか?

業界トップクラスのPC操作ログ情報を利用して、人工知能で不正を防ぐ

MylogStar × INTERNAL RISK INTELLIGENCE

セキュリティを強化するため、詳細なユーザー証跡管理を行うには、クライアントの操作ログを取得することが非常に有効です。操作ログ管理は導入していることをユーザーが知るだけで、「抑止効果」として情報漏洩の予防になります。そしてもしもの有事には、その情報漏えいの「原因追究」をすることが可能です。

しかし、それだけではせっかく取得した貴重な資産(ログ情報)を最大限活用しているとは言えません。

MylogStar(マイログスター)は業界トップクラスのログ収集力で、PC利用ユーザーの証跡を把握します。そして内部脅威検知サービス「Internal Risk Intelligence」なら、"AIを取り入れた独自の分析システム"と"専門アナリストによる再分析"により、取得したログデータから「人」に潜むリスクを検知します。さらに最もリスクの高い行動についてはクライアントに緊急通知されます。クライアント側で、行動監視ツールの習熟や人員リソースを割く必要はありません。

また、ハイリスク従業員の全てのリスク行動を詳細にレポーティングしたり、専門のアナリストが最適かつ具体的な対応策を迅速にご提案いたします。これにより、企業は効率的に社内に潜むあらゆる内部リスクを検知することが可能となります。

Mylogstar + Internal Risk Intelligence 連携詳細は裏面へ

MylogStar×AI（人工知能）：ログデータから「人」に潜むリスクを検知

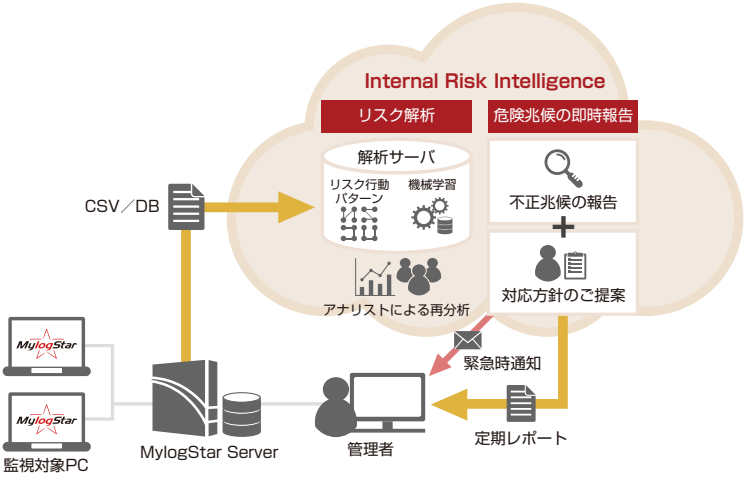
MylogStar + Internal Risk Intelligence 連携概要

MylogStar（マイログスター）とInternal Risk Intelligence を連携することにより、MylogStarで収集したPC操作ログをInternal Risk Intelligence で常時分析することが可能となります。

Internal Risk Intelligenceは国立研究機関との共同研究により実現した、人の行動分析に特化した人工知能（AI）技術が使われており、企業の持つ膨大なログデータから従業員が引き起こす“情報漏洩に繋がる予兆”を検知し、未然に防ぐことが可能です。

常時分析により、不正に繋がる従業員の行動（リスク行動）は人工知能（AI）がリアルタイム検知。高度な相関分析・スコアリング技術と専門のアナリストによるリスク評価により、「Emergency」「Caution」「Information」の3つに分類され、最もリスクの高い「Emergency」行動は、クライアントに緊急通知されます。

これにより、従来では困難だった内部不正の未然防止を実現します。



連携メリット（効果）

MylogStarが持つ業界トップクラスのPC操作ログ収集力により、他では取得できない精度の高いログ情報と豊富なログ項目の種類によって、監視対象者の行動をより正確かつ広範囲に把握可能となります。

そのログ情報を Internal Risk Intelligence の解析サーバでリスク解析することで、行動パターン・リスクシナリオから従業員が引き起こす「情報漏洩に繋がる予兆」を検知できるようになります。

そして危険度が高い事象が発生した際には電話かメールで「緊急通知」をおこないます。また、通常時は Internal Risk Intelligence の「月次レポート」にて分析結果を報告します。

Internal Risk Intelligence の相関分析による検知実績事例

Internal Risk Intelligence では MylogStar も含め、さまざまなログデータを組み合わせて分析を行うことで、単一のログデータでは発見できない通常の状態とは違う動きを見つけ出すことも可能です。

このサービスを利用すれば、各企業は情報漏洩・不正会計・横領等の一般的な内部不正から、通常把握することが困難な、従業員の背信行為、社内紛争、不平不満まで、あらゆる内部リスクを検知することが可能となります。

検知事象	関連データ	詳細
情報持ち出し	Webアクセス／ファイルアクセス	転職懸念者がローカルPCに大量ファイルコピー
情報持ち出し	Webアクセス／ファイルアクセス	金銭問題を抱えている可能性+普段と違うファイル探索行動
情報漏洩	アプリケーション	ファイル転送アプリケーションを利用
不就労	Webアクセス／出退勤記録	ブログサイト、美容系予約サイトの恒常的な長時間閲覧
労務管理	PC認証／メール	サービス残業が過大＋業務ファイル持ち出し（本人プライベートアドレスへの転送）
ルール違反	Webアクセス／windowタイトル	プライベートのGmailアドレス利用（社用メールもGmailの会社）
脆弱性発見	アプリケーション	古いバージョンのAdobe利用（標的型攻撃の被害を受けやすい）
転職	Webアクセス	同業種／同職種の求人ページを熱心に閲覧

詳細はWebサイトをご覧ください。　http://www.mylogstar.net

RUNEXY®
Run in the Next!

株式会社ラネクシー
http://www.runexy.co.jp

E-Mail:mls_sales@runexy.co.jp

お問い合わせ