株式会社 アシスト
http://www.ashisuto.co.jp/

セキュリティログ分析ソリューション　～個人情報保護対策版～

ログ活用ソリューション

SECURITY Plus α Ashisuto

ログ活用ソリューションとは

情報漏えい対策、監査対応等で、さまざまなログを一元管理した統合ログ管理システムの環境を持っている企業は少なくないはずです。
しかし、ログの利用用途としては、不正操作のチェックのみ、監査対応で年に数回しか利用しないというように、限定した用途でしか利用出来ていないといった状況も多々見受けられます。アシストの『ログ活用ソリューション』は、これらの貯めこまれたただけになっているログの有効活用を目指し、これまでのログ管理システム構築の実績や、ノウハウから得た、ログの活用方法をご提案するオリジナルソリューションです。

アシストの『セキュリティログ分析ソリューション　～個人情報保護対策版～』

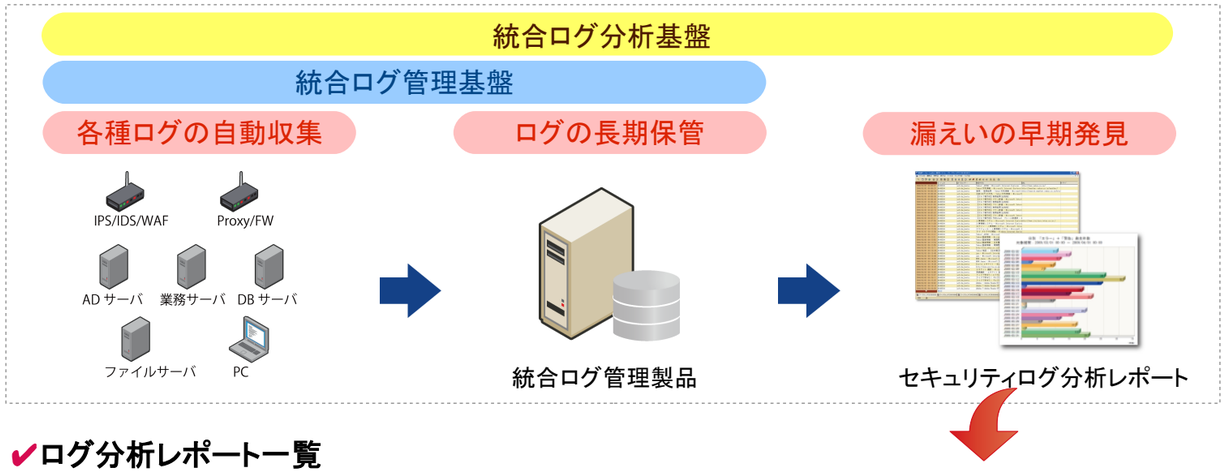
企業が所有している多くの個人情報。これらのデータは企業活動に非常に有効なものですが、管理の不備や、内部者の不正行為により、データが窃取・漏えいするといったリスクもあります。漏えいした場合、個人情報の本人の実害が無かったとしても、漏えいさせた企業には莫大な損失が生じます。そのためデータ窃取の予兆や窃取されたことを発見する仕組みの整備が急務と考えられます。アシストは、外部・内部者による情報窃取の状況や予兆をお客様自身で分析／発見できる「個人情報保護対策向けログ分析ソリューション」を提案いたします。

- チェックすべきログがわかる！
- ログ分析の切り口がわかる！
- すぐ取り組める！

個人情報保護対策の全体像

ソリューション全体イメージ

情報漏えいの予兆検知・早期発見が、迅速な対応策に繋がります。当ソリューションはそれら予兆検知・早期発見を強力にサポートします。



✔ログ分析レポート一覧

リスク	分析レポート
端末への不正ログイン	・ログインエラーログ一覧 ・ログインエラー件数一覧
サーバへの不正ログイン	・管理者ユーザログイン一覧 ・不正アクセス一覧 ・ログイン試行（パスワードミス）一覧 ・なりかわり失敗一覧
情報への不正アクセス	・重要フォルダアクセス一覧 ・重要フォルダアクセス件数一覧 ・大量検索実行の一覧 ・勤務時間外の重要フォルダへのアクセス一覧
情報の不正持ち出し	・禁止デバイス接続一覧 ・デバイス接続件数 ・外部メディア持ち出し一覧 ・ユーザ（PC）別持ち出し件数一覧 ・部署別持ち出し件数一覧 ・印刷操作一覧 ・勤務時間外のデバイス接続ログ一覧 ・勤務時間外の外部メディア持ち出し一覧 ・勤務時間外の印刷一覧

リスク	分析レポート
不正な権限変更	・アカウント変更操作一覧 ・スキーマ変更操作一覧
DB特権ユーザの不正操作	・特権ユーザーのアプリケーションテーブルへの不正アクセス一覧 ・特権ユーザーアクティビティ集計一覧 ・特権ユーザー利用一覧 ・特権ユーザー監視（DDL）一覧
その他	・不正アクセスポイント利用一覧 ・外部リモートアクセス失敗一覧（アウトバウンド）

アシスト's ログ分析によって何がわかる？

情報漏えいを未然に防ぐことは大切ですが、対策漏れや内部の不正行為による漏えいのリスクを完全に排除する事は簡単ではありません。そこでログを定期的にチェックすることで

- ✔ 情報漏えいにつながる不正アクセスが発生していることを発見
- ✔ 情報漏えいが発生した場合の範囲の把握

を行うことができるようになります。

株式会社 アシスト
http://www.ashisuto.co.jp/

セキュリティログ分析ソリューション　～個人情報保護対策版～

ログ活用ソリューション

SECURITY Plus α Ashisuto

分析レポートの特長

- お客様自身で分析できる
  - 情報漏えいを発見できるレポートを複数作成
    しているため、詳細な調査分析が可能です。
- 一目で状況が分かる
  - 対象となるレポート毎に、どのような脅威、事象が発生したかが明確で、かつログから必要な情報のみを抽出し表示しています。
- 運用の負荷が低い
  - 定期的に自動出力されるレポートのチェックのみで状況が把握できます。

分析レポート仕様書の特長

- チェックすべきログが分かる
  - あらかじめ情報漏えいを発見する為に必要と
    なる情報をまとめレポート対象とするログを選定しています。
- お客様自身でレポート作成できる
  - ログからどういった情報、条件を抽出してレポートを作成すべきかが記載されています。
- 出力されるレポートのイメージを掴みやすい
  - サンプルログとレポートのサンプル結果を例示
    しているのでどういった結果が出てくるのかが容易にイメージできます。
- あらゆるログから、レポート作成できる
  - OSに標準出力されるようなログからも
    レポート作成でき、特定ツールのログに依存しないレポート仕様となっています。
- あらゆるログ分析基盤にて活用できる
  - 特定のログ分析基盤に依存しておらず、ログを
    分析できる仕組みさえあれば、あらゆる環境で
    利用できます。
- 今後の出力の標準形として利用できる
  - 標準カラムとして今後のログ出力方針に利用できます。

分析レポートイメージ

✔ 重要フォルダへのアクセス一覧

アクセスの必要がないファイルへアクセス(不正アクセスの疑い)しているユーザのチェックができます。

イベント発生日時	判定	ログインユーザ	アクセス種別	監視対象リソース	接続元IPアドレス
2014/9/22 7:56	D	administrator	Read	C:¥Import¥顧客情報	192.168.11.10
2014/9/22 12:48	D	domain¥user01	Read	C:¥Import¥顧客情報	192.168.13.41

個人情報や機密情報のファイルにアクセスしている不正行為を発見できます。

✔ 禁止デバイス接続一覧

接続が禁止されている外部デバイス(USBメモリ、スマートフォンなど)を接続しようとしたユーザのチェックができます。

イベント発生日時	判定	ログインユーザ	コンピュータ名	ログオンタイプ	ファイル名
2014/5/28 4:21	War	HIBUN-GW¥loguser	B1403-10-01	CON	USB : Apple Mobile Device USB Driver
2014/8/11 9:03	War	domain¥user01	B1402-09-01	CON	USB : Apple Mobile Device USB Driver

個人情報や機密情報のファイルを外部に持ち出そうとしている不正行為を発見できます。

✔ 外部メディア持ち出し一覧

USBメモリ、スマートフォンなどの外部メディアを接続し、データの持ち出しを行ったユーザのチェックができます。

イベント発生日時	判定	ログインユーザ	コンピュータ名	ログオンタイプ	ファイル名
2014/6/11 21:42	OK	HIBUN-GW¥loguser	B1312-03-01	RES	E:¥顧客情報一覧.doc
2014/6/11 23:38	OK	B1403-10-01¥kkauser	B1403-10-01	RES	H:¥契約情報_XXX様.xls

情報を外部メディアに書き出したユーザと、対象ファイル名が確認でき、外部に持ち出される可能性のある行為を発見できます。

ご提供方法

レポート仕様書の提供から統合ログ分析基盤の構築までご支援する提供パターン1、仕様書のみ提供するパターン2の2つのパターンをご用意。

	ご支援内容	成果物	費用	備考
パターン 1	・ログ管理・分析基盤構築 ・レポート対象ログの収集 ・レポート作成	・ログ管理・分析基盤 ・レポート ・レポート仕様書	・100万円～	ログ管理基盤をお持ちでないお客様を想定して支援パターンとなります。
パターン 2	・レポート仕様書作成	・レポート仕様書	・30万円～	既にログ管理・分析基盤をお持ちのお客様を想定した支援パターンとなります。