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 ～標的型攻撃対策版～

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

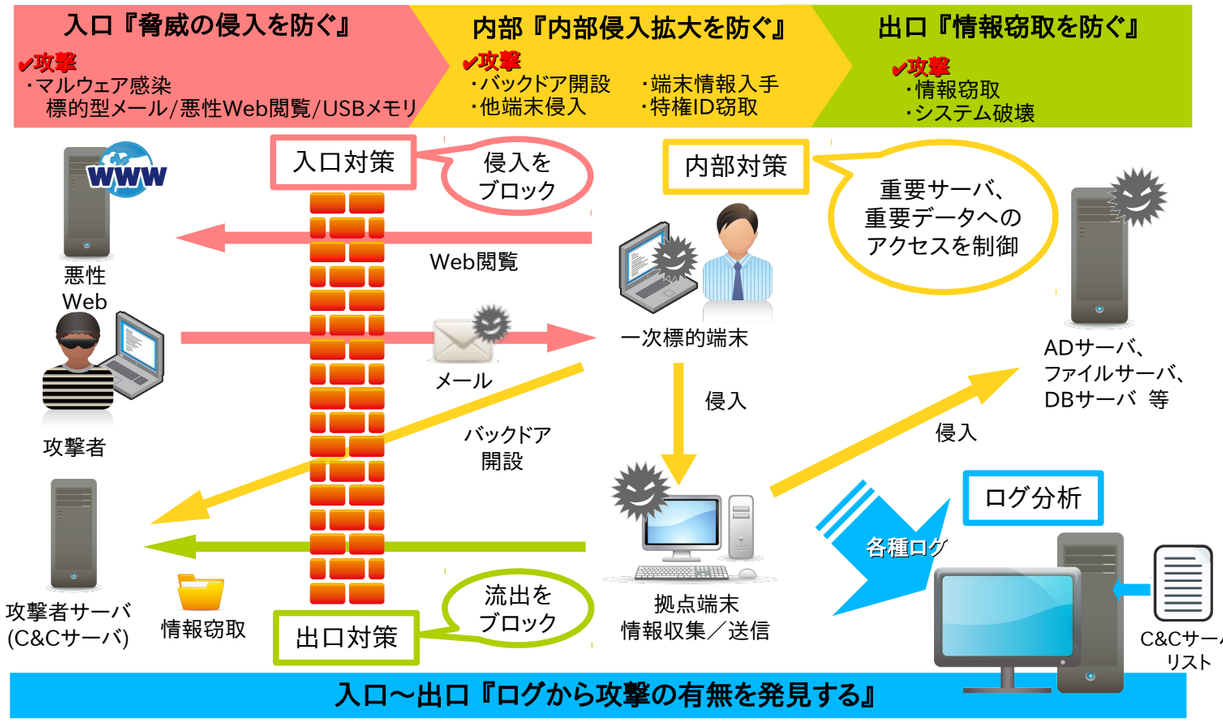
情報漏えい対策、監査対応等で、さまざまなログを一元管理した統合ログ管理システムの環境を持っている企業は少なくないはずです。
しかし、ログの利用用途としては、不正操作のチェックのみ、監査対応で年に数回しか利用しないというように、限定した用途でしか利用出来ていないといった状況も多々見受けられます。アシストの『ログ活用ソリューション』は、これらの貯めこまれたただけになっているログの有効活用を目指し、これまでのログ管理システム構築の実績や、ノウハウから得た、ログの活用方法をご提案するオリジナルソリューションです。

アシストの『セキュリティログ分析ソリューション ～標的型攻撃対策版～』

年々巧妙化する標的型攻撃の完全な防御は難しく、対策を行っていても新たな攻撃により被害を受ける可能性があります。また、外部からの通報により、攻撃を受けていることが判明するケースも多く見られます。発見の遅れに比例して被害は拡大するため、自社内に攻撃発見の仕組みを整備することが急務と考えられます。アシストは、マルウェア感染による不正操作等の攻撃状況や予兆をお客様自身で分析／発見できる「標的型攻撃対策向けセキュリティ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!

標的型攻撃の全体像



入口～出口『ログから攻撃の有無を発見する』

アシスト's 標的型攻撃に対し、なぜログ分析が有効か?

標的型攻撃を入口で防ぐことは大切ですが、未知の脅威を完全に防御する術はありません。防御を破られ侵入されてしまった場合、一番初めにしなければならないこととは?

- ✔ **攻撃を受けていることの早期発見**
- ✔ **攻撃段階/範囲の把握**

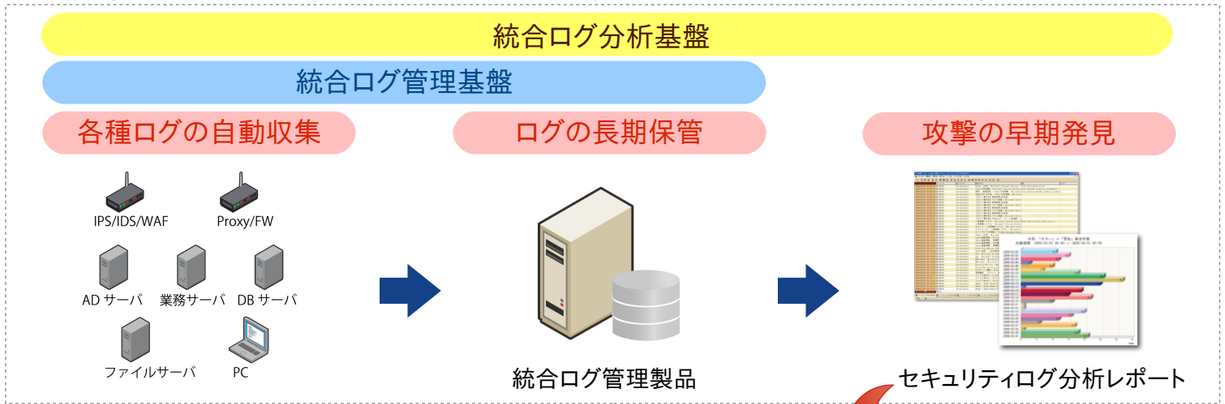
そのため、ログを分析して、標的型攻撃に備えることが重要です。

アシスト's ログ分析のポイント

分析対象とすべきログは、各種ネットワーク機器、サーバやPC等の端末等、多岐に渡ります。これらのログを個々に確認することで要する工数を削減する目的において、**統合ログ管理基盤**の構築は極めて効果的ですが、あくまでログ管理を主目的としております。
アシストは、この主目的を管理から分析へ移し、**統合ログ分析基盤**へとブラッシュアップした
セキュリティログ分析ソリューションをご用意しました。
お客様ご自身で、標的型攻撃を**工数をかけずに早期発見**できるソリューションです。

ソリューション全体イメージ

標的型攻撃の早期発見が、迅速な対応策に繋がります。当ソリューションはその早期発見を強力にサポートします。



✔ログ分析レポート項目一覧

攻撃	分析レポート	対応策
バックドア開設 / 情報流出	URLカテゴリを付与したWebアクセスログ一覧 F/W内部から外部への不正な通信結果一覧	FireWall/Proxyでの遮断 マルウェア検知 Webフィルタリング 情報の暗号化
不正なパスワード入力	サーバへのログイン失敗一覧	ネットワーク経路制限
ハッキングによる情報収集	サーバや他クライアントへのアクセス件数表	ネットワーク経路制限
特権IDの不正使用	サーバログインのログと申請情報との突合一覧	ネットワーク経路制限 アクセス制御
不正アクセス	重要ファイルへのアクセス失敗一覧	
機密ファイルアクセス	特権IDによる機密ファイルアクセス一覧	
外部へのファイル送信	外部へのFTPファイル送信一覧	ネットワーク経路制限 アクセス制御 情報の暗号化
情報システムの破壊	レジストリの変更ログ一覧	アクセス制御
スパムメールの送信	クライアント別メールの送信件数表	メールフィルタリング
内容の改ざん	重要ファイルの変更一覧	アクセス制御

成果物

セキュリティログ分析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しております。

	統合ログ分析基盤の構築	セキュリティログ分析レポート仕様書
提供パターン 1	○	○
提供パターン 2	―	○

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 ～標的型攻撃対策版～

ログ活用ソリューション

『セキュリティログ分析レポート仕様書』サンプル（標的型攻撃「バックドア開設 / 情報流出」についての分析レポート仕様書一例）

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**
  - 攻撃を発見する為の11カテゴリのログを選定
- **お客様自身でレポート作成できる**
  - ログからどの項目を抽出すべきかを記載
- **出力されるレポートのイメージを掴みやすい**
  - ログとレポートのサンプルを例示
- **あらゆるログから、レポート作成できる**
  - 特定ツールのログに依存しない
- **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ない
- **今後のログ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

✔ ログ変換表イメージ

操作内容			不正なURLカテゴリにアクセスした端末情報
ログ抽出		抽出対象	Squidログ
		抽出条件	URLリストの情報をログ内のURLに付与し、不正なURLカテゴリのみを抽出
ログ変換	タイムスタンプ	INPUT(サンプル)	Thu Apr 18 07:56:07 2013
		INPUT(カラム順)	1カラム～5カラム
		CONVERT	フォマット「E MMM dd HH:mm:ss yyyy」を「yyyy-mm-dd hh:mm:ss」に変換
		OUTPUT	yyyy-mm-dd hh:mm:ss
	アプリケーション	INPUT(サンプル)	ログなし
		INPUT(カラム順)	ログなし
		CONVERT	固定で、「Squid」を出力する
		OUTPUT	Squid
	クライアントIPアドレス	INPUT(サンプル)	192.168.43.94
		INPUT(カラム順)	7カラム
		CONVERT	-
		OUTPUT	192.168.43.94
	URL	INPUT(サンプル)	http://sample.com/
		INPUT(カラム順)	11カラム
		CONVERT	-
		OUTPUT	http://sample.com/
	URLカテゴリ	INPUT(サンプル)	-
		INPUT(カラム順)	-
		CONVERT	11カラム目のURLにURLリストの情報を付与
		OUTPUT	マルウェア

✔ BlackDomainリスト（オプション提供）

お客様自身で悪性サイトのリストをご準備できない場合、オプションでリストのご提供も行っております。
株式会社FFRIにて提供しているBlackURLリスト(※)のURL情報を元に生成したドメインリストになります。

（※）BlackURLリスト
FFRIの独自分析システム内でマルウェアを実行させ、感染後にアクセスするURL情報を抽出している為、出口対策において精度の高いURLリスト

■BlackDomainリスト
（弊社が提供するリストイメージ）

```
マルウェア,goooogle.net
マルウェア,yahoo-com-jp.mine.nu
マルウェア,www.xxxcode.com
マルウェア,www.hackingtool.com
マルウェア,www.hackingtool.com
```

分析レポートの特長

- **お客様自身で分析できる**
  - 攻撃を発見する為の11カテゴリのログについてレポートを実装済み
- **一目で攻撃状況が分かる**
  - 実ログから分析に必要な情報のみを抽出し表示
- **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

✔ 分析レポートイメージ

イベント発生日時	ログ種類	クライアントIPアドレス	URL	URLカテゴリ1	URLカテゴリ2
2013/11/22 7:56	Squid	192.168.16.110	http://goooogle.net/	セキュリティ・プロキシ	マルウェア
2013/11/22 12:56	Squid	192.168.16.120	http://yahoo-com-jp.mine.nu/	セキュリティ・プロキシ	マルウェア
2013/11/22 13:53	Squid	192.168.16.130	http://www.xxxcode.com/	セキュリティ・プロキシ	マルウェア
2013/11/22 23:11	Squid	192.168.16.140	http://www.hackingtool.com/	セキュリティ・プロキシ	マルウェア
2013/11/22 23:14	Squid	192.168.16.150	http://www.hackingtool.com/dl/	セキュリティ・プロキシ	マルウェア

『クライアントアドレス』としてレポート化

『URL』としてレポート化

『URLカテゴリ』はログと別途用意するURLリストのマッチングにより付与

✔ 元ログ（プロキシログ：Squid）

```
Thu Nov 22 07:56:08 2013  38 192.168.16.110 TCP_CLIENT_REFRESH_MISS/200 54039 GET http://goooogle.net - DIRECT/74.125.235.128 application/vnd.google.safebrowsing-chunk
Thu Nov 22 12:56:08 2013  11 192.168.16.120 TCP_CLIENT_REFRESH_MISS/200 28299 GET http://yahoo-com-jp.mine.nu/ - DIRECT/74.125.235.128 application/vnd.google.safebrowsing-chunk
Thu Nov 22 13:53:08 2013  29 192.168.16.130 TCP_CLIENT_REFRESH_MISS/200 28192 GET http://www.xxxcode.com/ - DIRECT/74.125.235.128 application/vnd.google.safebrowsing-chunk
Thu Nov 22 23:11:08 2013  82 192.168.16.140 TCP_CLIENT_REFRESH_MISS/200 12607 GET http://www.hackingtool.com/ - DIRECT/74.125.235.128 application/vnd.google.safebrowsing-chunk
Thu Nov 22 23:14:08 2013  33 192.168.16.150 TCP_CLIENT_REFRESH_MISS/200 93702 GET http://www.hackingtool.com/dl/ - DIRECT/74.125.235.128 application/vnd.google.safebrowsing-chunk
```