



マクニカラポ便り  
ITサーチャエンジン「Splunk」で  
ファイルサーバへのアクセス履歴の監査ができるのか？

「マクニカラポ便り」は、ちょっとやってみみたい検証や、このテクノロジー、こう使ってみたらどうなる？など、マクニカネットワークスのエンジニアが気になった製品や技術について、ディープな検証や評価を行い、面白かったら皆さんにも公開しようという、ちょっと気まぐれなコーナーです。

第一回の今回は、2009年1月に取扱いを開始し、先日のInterop Tokyo 2009 のBest of Show Awardアプリケーション部門でグランプリを受賞したITサーチャエンジン「Splunk」を使った、新たな試みにチャレンジしてみたいと思います。

By 須田 賢一  
Macnica Networks Corp.

## 【今回のチャレンジ】

ITサーチャエンジン「Splunk」でアクセス履歴の監査ができるのか？

多くのお客様からお問い合わせをいただいている「Splunk」ですが、その中にWindowsファイルサーバのアクセス履歴の監査用に活用できないか？というものがありません。

SplunkはITインフラが生成するログやコンフィグレーションファイルなどを取り込み、検索、アラート、レポートが可能なソリューション。Splunk自体にDBを持たないため、ログフォーマット等を問わず自由にデータ取り込みが可能で、検索、アラート、レポートに関して自由のカスタマイズすることができます。もちろん、Windows上の各種ログデータを取り扱う事も可能です。それならば、Splunkを通してWindowsのログデータを収集、加工し、アクセス履歴の監査に役立てられる方法があるのでは？

今回はファイルサーバのアクセス履歴の監査に役立つかどうか、実際にSplunkで試してみます！

1. 用意するもの
2. 実際にSplunkを使ってログを取ってみよう！
3. 仕事で役立つ場面とは？

### 1. 用意するもの

本日の実験に必要な環境

- ・ Windows Server 2003 英語版\* 1台  
ファイルサーバとして利用します。簡易的にVMware上の環境を用意しました。
- ・ Splunk バージョン 3.4.10フリー版  
弊社Splunkページからフリー版ダウンロードページへジャンプします。  
[http://www.splunk.com/download/?ac=Partner\\_Macnica](http://www.splunk.com/download/?ac=Partner_Macnica)

\* 日本語版Windows OSのサポートは2009年7月リリース予定のSplunk バージョン4.0以降となります。

### 2. 実際にSplunkを使ってログを取ってみよう！

#### ステップ1: Windowsファイルサーバ側での設定

Windowsファイルサーバに対して、ファイルアクセス時に監査情報がセキュリティイベントとして記録されるように設定を行います。マイクロソフト社のホームページなどに設定方法が説明されています。

ポイントは2つあります。

1. ローカルセキュリティの設定(もしくはドメインのセキュリティポリシー)にて、「オブジェクト アクセスの監査」に対する監査設定を有効にします。「成功」「失敗」チェックボックスを有効にします。
2. 監査対象の共有フォルダに対して、監査ポリシーを設定します。共有フォルダのプロパティから、セキュリティタブを選択。[詳細設定]ボタンをクリックし、[監査]タブをクリック。監査エントリのダイアログにて、監査対象のユーザグループ等の設定を行います。

これにより、ファイルサーバの共有フォルダ上でファイルを読み込んだり、書き込んだりするたびにセキュリティ ログがイベントログに記録されます。イベントビューアを使ってイベントが記録される事を確認しておきます。

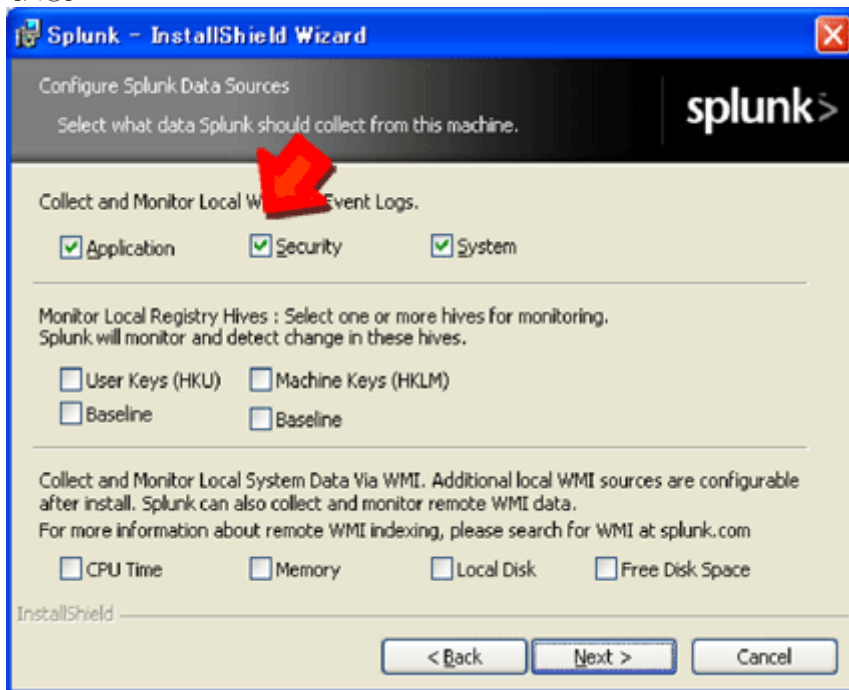
Windowファイルサーバ側での設定は以上です。以降はSplunk側での設定となります。

#### ステップ2: Splunkのインストール、設定

今回は、Windowsファイルサーバ上にSplunkをインストールします。Splunkのインストール方法については、弊社のSplunk製品ページから『Splunk インストール&クイックリファレンスガイド』をご参照ください。今回の実験では、Splunkインストール時に表示される「Security」のチェックボックスを有効にするだけです。

(図①参照)

[図①]



# LANch BOX online Magazine

夏号 2009

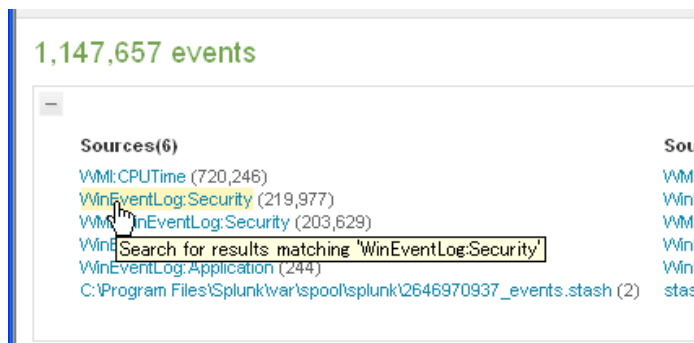
既にSplunkをインストールしている場合には、Splunkの設定ファイル「inputs.conf」を編集して、次のように変更します。

```
[WinEventLog:Security]
disabled=0
```

Splunk バージョン4.0以降では、インストール後にGUIから設定確認・変更ができるように機能拡張されます。

## ステップ3: Splunkのインストール、設定

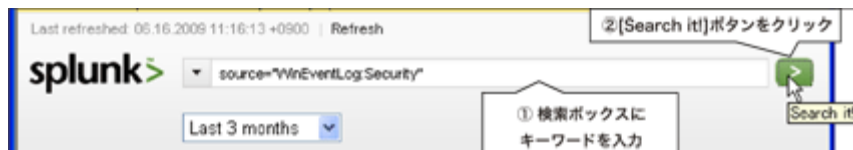
Splunkに読み込ませたWindowsのセキュリティログを参照します。(図②)「All indexed data」欄から、セキュリティログを意味する「WinEventLog:Security」をクリックします。



もしくは、Splunkの検索ボックスで次の検索キーワードを入力します。

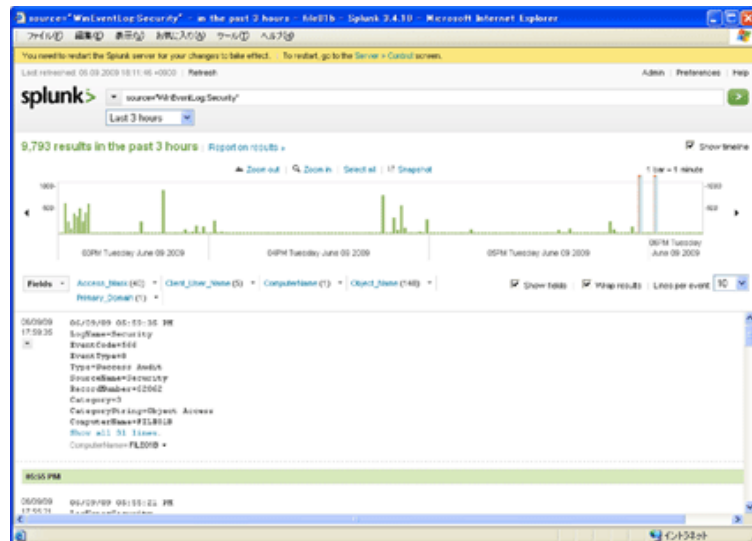
```
source="WinEventLog:Security"
```

右の[Search it!]ボタンをクリックします。



これにより、セキュリティログが表示されます。図②

[図②] Splunk 3.4.10での表示例



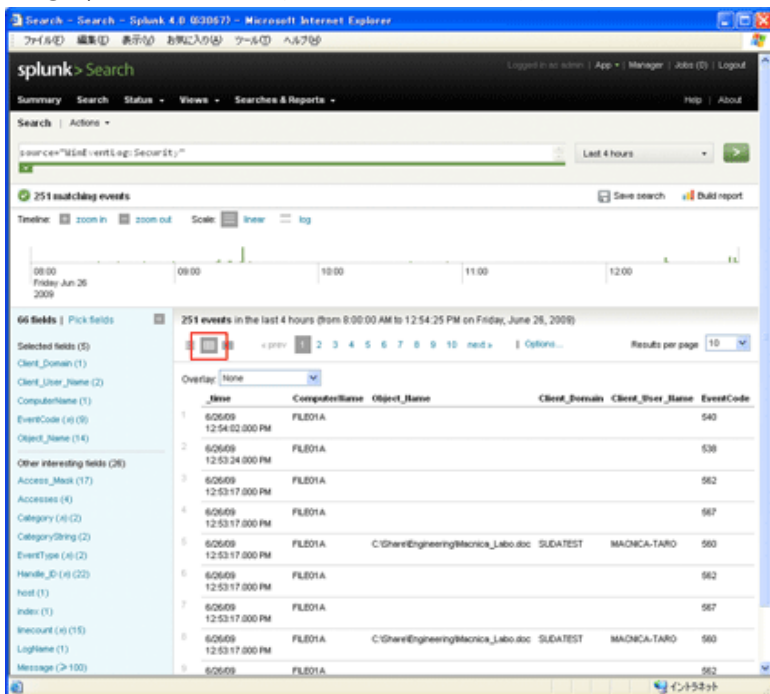
# LANch BOX online Magazine

夏号 2009

なお、Splunkバージョン 4.0以降では、この一覧表示に加えて、表形式の表示を選択できる機能が追加される予定です。図

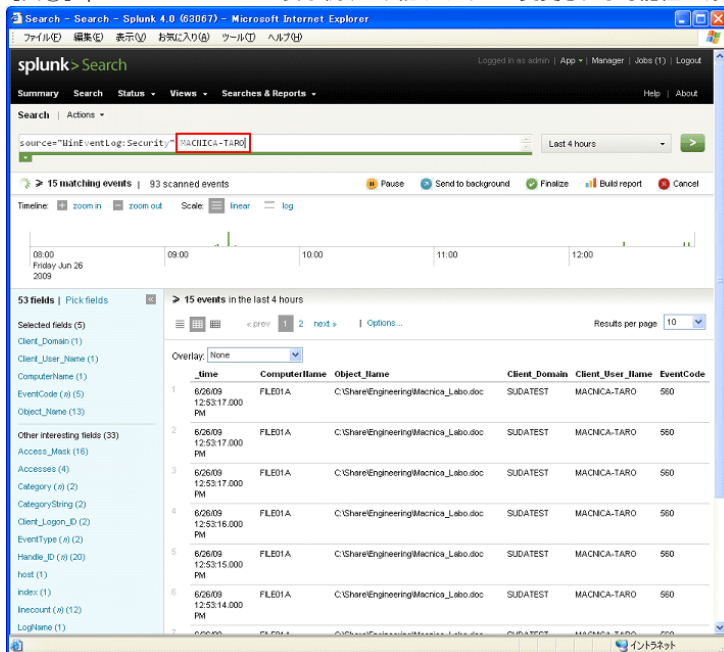
③

[図③] Splunk バージョン4.0の表示例(※下記デザインは変更される可能性があります。)



上記に続けて、検索ボックスにファイル名を入力すると、指定したファイルにアクセスしたイベントのみが表示されます。ファイル名の代わりにユーザ名を指定すると、指定したユーザに関連するイベントが表示されます。これで、「誰が、どのファイルへ、いつ」アクセスを行ったかを確認できるようになりました。(図④)

[図④] Splunk バージョン4.0の表示例(※下記デザインは変更される可能性があります。)



# LANch BOX online Magazine

夏号 2009

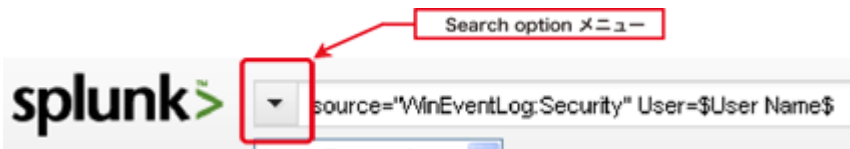
## ステップ4: フォームを使った検索

次に、ユーザ名はユーザ名として、また、ユーザ名を指定するための個別の検索ボックスを用意するフォームを作ってみます。

まず、Splunkの検索ボックスに次の検索キーワードを入力します。

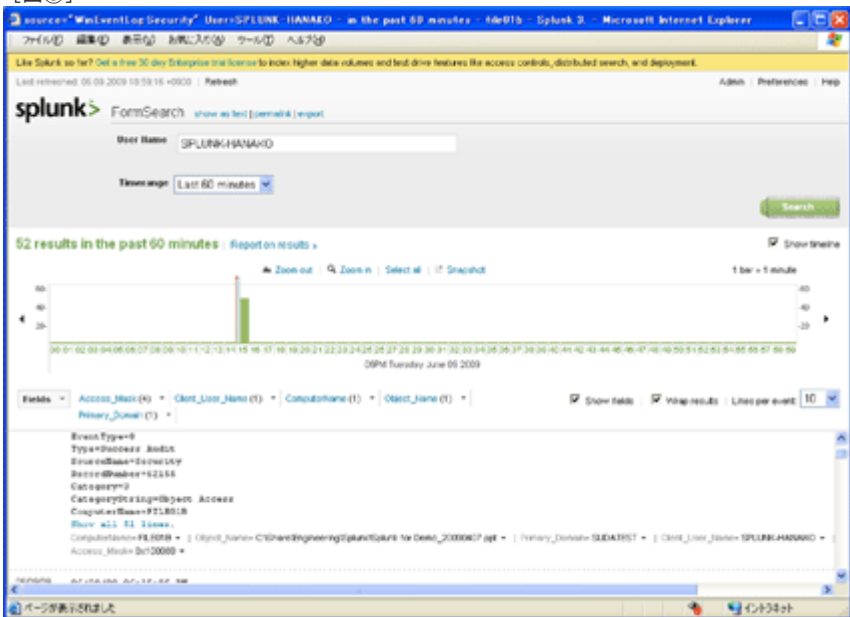
```
source="WinEventLog:Security" User=$User Name$
```

次に、検索ボックスの左端にある▼印の[Search options]メニューから、[Save Search]メニューを選択し、この検索キーワードを保存します。



▼印の[Search options]メニューから、[Saved Searches]を選択し、保存した検索キーワードを呼び出します。これまでの検索ボックスの代わりに、ユーザ名を入力するための入力フォームが表示されます。フォームに入力して、Searchボタンをクリックすると、入力したユーザ名に合致するイベントだけが表示されます。(図⑤)

[図⑤]



## ステップ5: 表示形式の変更(アクセス履歴一覧、アクセス数の遷移グラフ)

さらに一歩踏み込み、時系列で、いつ、誰が、どのファイルへアクセスしているかを一覧で見たい。1回の読み込み動作によってたくさんのイベントが生成されている事がここまでの実験を通してご理解いただけたかと思います。

そこで、Splunk上で記録されたイベントのパターンを読み取り、ユーザの操作へ変換させます。この変換を実現するために、Splunkの強力な検索機能の1つである「トランザクション(transaction)」コマンドを使います。また、トランザクションコマンドを利用して得た結果を「サマリーインデックス(Summary Index)」に記録して、後から容易に参照できるようにします。これらの処理を「|」(パイプ)で連結させて実行します。これらトランザクション検索やサマリーインデックスへの記録処理を「Saved Search」として保存しておき、定期的に行うようにします。

# LANch BOX online Magazine

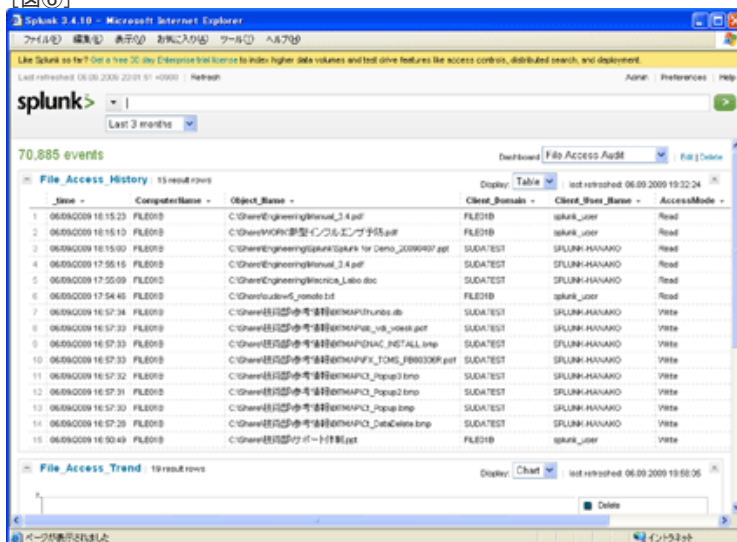
夏号 2009

さらに、アクセス監査用のダッシュボードを用意して、そのダッシュボード上一覧表示やアクセス数遷移を表示できるようにしてみました。作成したSaved Search等の詳細はさておき、このような結果を表示させる事ができました。(図⑥)

今回の実験では、Microsoft Word、Excel、Adobe Reader等を使って、ファイルアクセスを行いました。セキュリティログ上に、3,227レコードが記録されていた時間帯において、上記の処理を通す事によって、98レコードとなりました。さらに、作業ファイルなどを除外するための独自のフィルタをPython言語で作成し、そのフィルタを通す事で、監査対象として有効と考えるレコードは、85レコードとなりました。

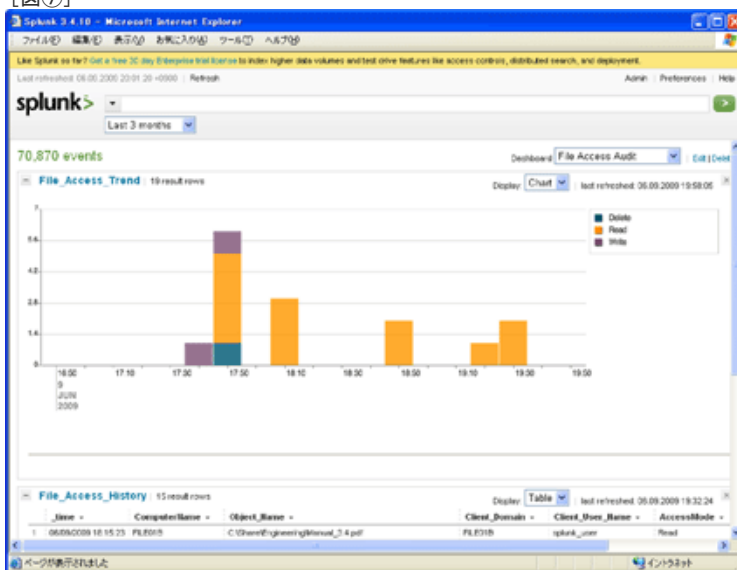
ITサーチエンジン「Splunk」を利用する事で、監査に利用する情報をより直観的に確認する事ができるようになりました。

[図⑥]



また、アクセス数の遷移を次のようにグラフ表示する事も可能です。

[図⑦]



今回は実験イメージでご説明するため、詳細ステップを追ってご説明しました。実際の運用では、あらかじめ表示させたいレポート定義を保存(Saved Search)しておき、1クリックで見たいレポートを表示させることが可能です。また、頻繁に見るレポートはダッシュボードに登録しておけば、常に表示させておくことが可能です。

### 3. 仕事で役立つ場面とは？

#### ●履歴情報の一元管理

今回の実験では、WindowsファイルサーバにSplunkをインストールしました。他のデータ取得の方法としては、WMI (Windows Management Instrumentation)を使って、SplunkをインストールしていないWindowsファイルサーバからSplunkサーバへセキュリティイベントログを一元的に収集する事ができます。ネットワーク帯域が不足しているようなケースでは、各ファイルサーバにSplunkをインストールすることでSplunkのデータ圧縮による効果が利用でき、安定的にログデータの一元化を行う事ができます。

これらにより、複数のファイルサーバをカバーするアクセス履歴を一元的に確認する事が出来るようになります。

#### ●休日深夜、誰が何している？を確認

Splunkのフィルタ機能を使うと、土日のアクセス、深夜のアクセスなど、時間帯を指定した表示する事ができます。これらの検索キーワードは保存しておき、いつでも呼び出して利用する事ができます。

#### ●重要文書へのアクセスを発見

Splunkのアラート機能を組み合わせて利用する事で、重要文書へのアクセスあった時に、管理者へ通知を行うような事も可能となります。

#### ●監査対象をもっと広げたい

監査の対象をログオン、印刷などのイベントが記録される操作に広げ、同じように一覧で表示させる事も可能になります。

ITサーチエンジン「Splunk」でアクセス履歴の監査ができるかどうか実験をしてみました。いかがだったでしょうか。内部統制やコンプライアンス強化が叫ばれるなか、アクセスログによる監査要求はこれからも高まっていくはず。ぜひ、「Splunk」をいろいろな用途に活用してみてください。

マクニカネットワークスでは、ITサーチエンジン「Splunk」の新たな活用方法について、皆さんからのご要望にお応えしながらソリューション開発・提案を行ってまいります。

---

須田 賢一

マクニカネットワークス 技術サービスコンサルティング室 室長。数々のアプリケーションのローカライズや導入コンサルティング、テクニカルサポートに従事。ITサーチエンジン「Splunk」を使った新たな技術サービスを検討中。

#### <参考>

- ・ Splunk製品詳細およびフリー版ダウンロード

<http://www.macnica.net/splunk/>

- ・ LANch BOXバックナンバー(2009年3月)

[特集]注目テクノロジー：ITサーチエンジンって何！？

～IT管理者を救え！使えるログ管理の新コンセプト

<http://www.macnica.net/lanch/lanch78/sp01.html>

- ・ Interop Tokyo 2009 Best of Show Award グランプリ受賞プレスリリース

[http://www.macnica.net/pressrelease/splunk\\_090615.html](http://www.macnica.net/pressrelease/splunk_090615.html)