

Proofpoint Smart Search



Proofpoint Smart Search™は、先進的メッセージ追跡、フォレンジック、ログ分析の各機能で Proofpoint の内蔵ロギングおよびレポーティングを強化し、メッセージングインフラ全体にわたってメッセージの流れを簡単にリアルタイムで見られるようにしています。グローバルに分散した導入済 Proofpoint 全体にわたってさえ便利で使用が簡単な単一の GUI からメッセージログのすべてを検索・分析します。

特徴

エンタープライズクラスのログ検索、メッセージ追跡および分析

Proofpoint Smart Search は、インバウンドとアウトバウンドの両方のメッセージを迅速に追跡し、メッセージが Proofpoint システムによってどのように処理されたかを分析し、そして電子メールメッセージの処理とステータスをレポートするのに役立ちます。

Proofpoint Smart Search があれば、電子メール管理者または IT ヘルプデスクスタッフは、即座にメッセージの場所を見つけ、そのメッセージがどのように取り扱われたかを理解し、さまざまな電子メールトラブルシューティングまたは調査のリクエストに迅速に対応することができます。以下に例を掲げます。

- **メッセージ追跡**：ビジネスパートナーがまったく受信しなかった重要なメッセージに何があったのかと重役からヘルプデスクに問い合わせがあるとします。Proofpoint Smart Search は迅速にそのメッセージを見つけて、配信ステータスについてレポートすることができます。
- **調査**：エンドユーザは競合会社と電子メールを交換してきたのだろうか？ それらのメッセージのサブジェクトは何だったのだろうか？ Proofpoint Smart Search がそれにお答えします。
- **フォレンジック**：法務部は、重要な通知がいつ、どのサーバに配信されたかを正確に知る必要があります。Proofpoint Smart Search はメッセージ取り扱いと配信について理解しやすい内容を提供します。
- **コンプライアンス**：特定のコンプライアンス事故またはあらゆるクラスの違反に関連するすべてのメッセージを迅速に見つけます。Proofpoint Smart Search は、どの Proofpoint ルールが起動し、結果としてメッセージがどのようにルート決定されたかを迅速に理解する手助けをします。
- **トレンド分析**：特定の Proofpoint ルールを起動したのは先月の何通のアウトバウンドメッセージだったのだろうか？ Proofpoint Smart Search があれば、大きくて複雑なログファイルの連結アーカイブから情報を容易に採取できます。

リアルタイムの連結ログ索引付け

Splunk の IT サーチテクノロジーに支えられた Proofpoint Smart Search は、Proofpoint 導入全体にわたって数秒でどんなメッセージでも見つけることができます。

Proofpoint Smart Search はグローバルに導入されたクラスタ全体にわたってさえ、すべての Proofpoint エージェントからのログを連結し、それらのログに迅速な検索を目的として索引を付けます。複数ソースからのログはメッセージの取り扱いと処理が全面的にわかるように自動的に相関付けられます。

Proofpoint Smart Search の使用簡単な GUI を使用すれば、メッセージの受信または送信の数分以内に、そのメッセージについての詳細を知ることができるように、ログ情報は継続的に更新されます。

Proofpoint Smart Search は Proofpoint 以外のメッセージングシステムとの統合を目的に設計されており、ダウンストリームメールサーバ、暗号化サーバおよびその他のゲートウェイ装置を含むメッセージングシステム全体からのログを連結することができます。メッセージはメッセージングインフラ全体にわたって追跡可能です。

IT ヘルプデスクスタッフに力を

IT ヘルプデスクスタッフが Proofpoint Smart Search を使用すれば、特別なトレーニングを受けたり、Proofpoint システムにアクセスしたりしなくても、もっとも一般的な電子メールトラブルシューティングや調査リクエストに回答することができます。Proofpoint Smart Search が備えている強力な検索・分析機能は、ミッションクリティカルな電子メールシステムの性能に影響を与えることなく使用することができます。なぜかという、Proofpoint Smart Search は Proofpoint Protection Server® ソフトウェアや Proofpoint Messaging Security Gateway™ アプリケーションから独立して動作するからです。



一目でわかる

Proofpoint Smart Search

- すべての Proofpoint ログのリアルタイム処理、索引付け、相関付け
- すべてのエージェントにわたってメッセージを数秒で追跡する強力な検索機能
- わかりやすい検索結果はあらゆるインバウンドまたはアウトバウンドメッセージの配信、タイミング、ルートルリガリング、処理を表示します。

複数データ表示

- **要約**：規定時間フレーム内のメッセージに関する参照時間、差出人、宛先、サブジェクト、そして実施された Proofpoint フィルタ処理
- **詳細**：わかりやすい詳細テーブルによる個別メッセージに関する掘り下げ
- **RAW ログ**：メッセージデータを本来のログ形式で表示。任意のログエレメントをクリックすれば、検索基準を簡単に狭めることができます。

全方位的洞察

以下を含む Proofpoint サーバおよびその他のメッセージングシステムからのログ情報を連結するよう設計。

- ダウンストリームメールサーバ
- アーカイブ化システム
- 暗号化装置

サードパーティシステムのためのサポートや統合に関する最新情報については Proofpoint にお問い合わせください。

Proofpoint Smart Search

特徴 (続き)

強力で使用簡単な検索インタフェース

Proofpoint Smart Search は、メッセージ情報の参照や検索を行うための便利なウェブベースのインタフェースを特徴としています。検索結果ページでは、RAW メッセージログからのデータを読みやすいすぐに使用可能な情報に翻訳します。要約表示では、メッセージ時間、宛先、サブジェクトおよびすべてのフィルタアクションを示します。個別メッセージについて掘り下げ、起動された Proofpoint ルール、Proofpoint メッセージ処理、MTA 処理、宛先 IP アドレスなどを含む詳細表示を明らかにします。メッセージデータはその本来の RAW ログ形式で表示することもできます。

Proofpoint Smart Search の使用簡単な検索インタフェースを使用すれば、メッセージは数秒のうちにピンポイント精度で見つけることができます。メッセージ差出人、メッセージ宛先、サブジェクト、相対的または絶対的時間フレーム、sendmail QID、Proofpoint セッション ID など幅広い規準を使用してメッセージを検索します。拡張自由テキスト検索により、規定表現およびブール演算子を使用してカスタム検索を構築できます。

簡単な導入

Proofpoint Smart Search は、既存の Proofpoint サーバと並んで迅速かつ簡単にインストールされる別個のアプリケーションとして導入します。場合によっては、Proofpoint Smart Search は既存の Proofpoint マスタアプリケーション上のソフトウェアモジュールとして導入することができます。

Proofpoint Smart Search インタフェース

The screenshot shows the Proofpoint Smart Search Professional 2.1.3 interface. At the top, there are search filters for Sender (service@chaseonline.com), Recipient, QID, SID, and Time (Absolute, Start: 02/24/2007 00:00:00, End: 02/24/2007 23:59:59). Below the filters is a bar chart titled 'Events by Time' showing event counts from Thursday Feb 22 to Monday Feb 26. The chart highlights Saturday Feb 24 with a green bar. Below the chart is a list of events, with one event selected and its details shown in a table below. The details include fields like Time, Sending Host, SID, Sender, Recipient, subject, GUID, Sender IP, Duration, Message Summary, PPS Filter Actions, PPS Filter Action Detail, and MTA Actions.

Field	Value
Time	2007-02-24 22:01:46 -0800
Sending Host	www.chaseonline.de
SID	2421495017
Sender	service@chaseonline.com
Recipient	jkambro@mbay.net
subject	Please restore your account.
GUID	f95393f633d677e6d63452fa404ef5a0
Sender IP	85.214.58.118
Duration	0.060
Message Summary	<ul style="list-style-type: none">Spam: triggered rule spam spamscore: 100 adultscore: 0 using engine: 3.1.1-0702090085 definitions: main-0702240027Virus: triggered rule clean
PPS Filter Actions	Modified, Discard.
PPS Filter Action Detail	<ul style="list-style-type: none">av : clean : add-header X-Proofpoint-Virus-Version="\$VirusVersion"spam : spam : discard
MTA Actions	<ul style="list-style-type: none">Milter add: header: X-Proofpoint-Virus-Version: vendor=secure engine=4.65.5502:2.3.11.1.2.37.4.0.164 definitions=2007-02-24_02-2007-02-24_2007-02-23_2007-02-24_sinnatures=0

Splunk を装備

Proofpoint Smart Search は Splunk の IT 検索テクノロジーを組み込んでおり、リアルタイム索引付け、高速検索、メッセージングログの迅速な分析が可能です。



動作中の Proofpoint Smart Search をご参照ください。

Proofpoint Smart Search のデモンストレーションをご覧になりたい場合は、以下の URL をご参照ください。

<http://www.proofpoint.com/pssdemo>

Proofpoint Smart Search GUI

左のスクリーンショットは Proofpoint Smart Search のグラフィカルユーザインタフェースを示しています。メッセージは直感的なコントロールを使用して迅速かつ簡単に見つけることができます。

この例では、検索を特定日に狭めるためにイベントタイムラインが使用されました（緑色のバーは 2 月 24 日の土曜日を示しています）。この対話型タイムラインにより、特定の期間についてグラフィカルに掘り下げることが簡単になります。

さらに、メッセージリストを Proofpoint のフィッシングスコアとスパムスコアが高いメッセージだけに狭めるために、「拡張」検索機能が使用されました。Proofpoint Smart Search のポイントアンドクリックインタフェースを使用すれば、こういった種類の検索は作成が簡単です。RAW ログ表示のときは、ログデータの任意の部分をクリックして、拡張検索フィールドに追加フィルタリング条件を自動的に追加し、関心のあるメッセージタイプだけに迅速に絞ることができます。

タイムラインの下には、わかりやすい形式でメッセージ取り扱い情報をすべて表示した単一メッセージのための詳細表示があります。

©2007 Proofpoint, Inc. Proofpoint Protection Server は米国およびその他の国々における Proofpoint, Inc. の登録商標です。Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Smart Search は米国およびその他の国々における Proofpoint, Inc. の商標です。ここに含まれる他のすべての商標はそれぞれの所有者の所有物です。05/07