

# Proofpoint Zero-Hour Anti-Virus モジュール



電子メール媒介ウィルスがネットワーク全体にわたってますます悪質になり、より急速に拡散するにつれて、エンタープライズは新しいウィルス攻撃のごく初期の段階において新しい形態の対策が必要になります。Proofpoint Messaging Security Gateway™と Proofpoint Protection Server® のコンポーネントである Proofpoint Zero-Hour Anti-Virus は、新しいウィルスが放出されてから決定的な最初の数時間中に、そしてウィルス対策シグナチャが更新される前に、新しいウィルスやその他の形態の悪意あるコードからエンタープライズを守り、ユーザのゲートウェイディフェンスに最新のウィルス対策レイヤを付加します。

## 特徴

### グローバルな分析、ローカルな対策

ウィルス攻撃から大きな組織を守るために、Proofpoint Zero-Hour Anti-Virus はインターネットトラフィックパターンのグローバルな分析と、疑わしいメッセージや添付物のローカルな封じ込めを組み合わせています。Proofpoint Zero-Hour Anti-Virus は、潜在的なウィルス攻撃を示す異常がないか何百万ものインターネットメッセージを絶えず分析します。先進的パターン認識テクノロジーを用いて新しいウィルスを識別しますが、それはインターネット上でそれらのウィルスが大量に配信されて数分以内に 95% を超える精度で行われます。

カスタマサイトでは、Proofpoint Zero-Hour Anti-Virus は疑われるウィルスメッセージと類似性がないか着信メッセージを分析します。新生ウィルスの再発パターン特性を示すメッセージや添付物はエンタープライズゲートウェイで自動的に検疫を受け、ここで生産準備が整ったウィルスシグナチャの可用性が得られるまで保持することができます。

### Zero-Hour ギャップを閉じる

シグナチャベースのウィルス対策テクノロジーを打ち負かすよう設計されたいくつかの新ウィルス配信方法は、「ショートスパン」攻撃、シリアルバリエーション攻撃、ボットネットから開始された攻撃を含めて、上昇傾向にあります。現在のエンタープライズが必要とするのは、新種の脅威に対してほとんど即座に反応することができる対策です。Proofpoint Zero-Hour Anti-Virus は新しいウィルスアクティビティを特定し、ウィルス発生 of 早期段階で予防措置を講じ、新しいウィルス対策シグナチャが更新されるまで、メッセージングシステムを安全に保ちます。Proofpoint のソリューションは、競合する「発生フィルタ」が反応する数時間前にウィルス対策を実施します。

### 正確な検出、最小限の混乱

他のウィルス発生ソリューションと違って、Proofpoint Zero-Hour Anti-Virus は正当な電子メールを停止することなく、発生ウィルスに関連するメッセージだけを正確に検出し、検疫します。添付物の種類が危険だと思われる電子メールをすべて検疫する代わりに、Proofpoint のソリューションは発生の一部として分類される特定メッセージだけを一次的に遅らせます。

### カスタマイズ可能なポリシー

Proofpoint のポリシー管理、システム管理、レポート管理といったすべての機能に対する便利なグラフィカルユーザインターフェイスである Proofpoint Messaging Security Console™を使用すれば、Proofpoint ユーザは Zero-Hour Anti-Virus ポリシーを簡単にカスタマイズすることができます。こういった自由度の高い、お客様が構成できるポリシーに基づいて、ウィルス発生の一部として特定されたメッセージに対しては、更新されたウィルスシグナチャおよびその他の条件の可用性に基づいて、再スキャンとクリーニング、削除、解除、またはその他の処理が自動的に行われます。

### 総合的レポート

Proofpoint のすべてのモジュラ式メッセージングディフェンスと同様に、Proofpoint Zero-Hour Anti-Virus には統合されたレポートが含まれており、これらのレポートは Zero-Hour ディフェンスの業務と一般的なウィルスの活動を詳しく述べています。内蔵のグラフィカルレポートは Zero-Hour ポリシーによって分類されるメッセージの量、Zero-Hour ウィルストレンド、未確認メッセージを含む上位 Zero-Hour ウィルスタイプ、そして確認済みウィルス量トレンドを明らかにし、自社のウィルス対策イニシアチブのための ROI を直ちに示すことができます。



## 総合的ウィルス対策

現在のウィルス脅威に対する効果的な防衛には、単なるシグナチャベースの対策や発現フィルタ以上のものが必要であると Proofpoint は理解しています。テクノロジーと情報サービスの組み合わせを通じて、Proofpoint は悪意のあるコードに対して総合的な対策を提供します。

### Proofpoint Zero-Hour Anti-Virus モジュール

新種ウィルスに対して即時対策を実施します。

- 早期で正確な検出
- リアルタイムの対策
- きめ細かいポリシーコントロール
- 強化された相関性のあるレポート
- 競合するゼロデイソリューションと比較してもっとも低い TCO

### Proofpoint Virus Protection モジュール

F-Secure または McAfee から業界をリードするウィルス対策エンジンを採用したシグナチャベースの対策を実施します。

- 最新ウィルス脅威に対して継続的に更新される対策
- インバウンドおよびアウトバウンドの両方の「ゾーン」トラフィックをスキャンします。
- 自由度の高いポリシーおよび処理

### ウィルスのライフサイクルに関する情報

Proofpoint は野放しのウィルスと貴社エンタープライズに影響するウィルス関連の脅威の状態に関する最新の情報を提供します。

- 貴社ユーザを教育するための警報チャンネルとニュースチャンネル
- 貴社エンタープライズに影響するウィルスアクティビティの全面的観点のための集中的レポート

# Proofpoint Zero-Hour Anti-Virus モジュール

## Zero-Hour ポリシーとデータの流れ

### 自由度の高いポリシー管理とメッセージ処理

Proofpoint Zero-Hour Anti-Virus は Proofpoint Virus Protection モジュールと協同して、総合的なウイルス防御を行います。これらのモジュールは共に積極的なウイルス対策層（シグナチャに依存しません）と高速かつ効果的なシグナチャ／ヒューリスティクスエンジンを備え、悪意のあるコードを効率的に確認します。

Proofpoint Zero-Hour Anti-Virus は、ほとんどの組織のウイルス発生防御ニーズに応えるよう設計された事前構成済みのデフォルトポリシーにより、細かい設定なしですぐに動作します。それでも、Proofpoint の使用簡単なグラフィカルインタフェースにより、Zero-Hour ポリシーのあらゆる面に対して細かいコントロールを行うこともできます。

### カスタマイズ可能なルール

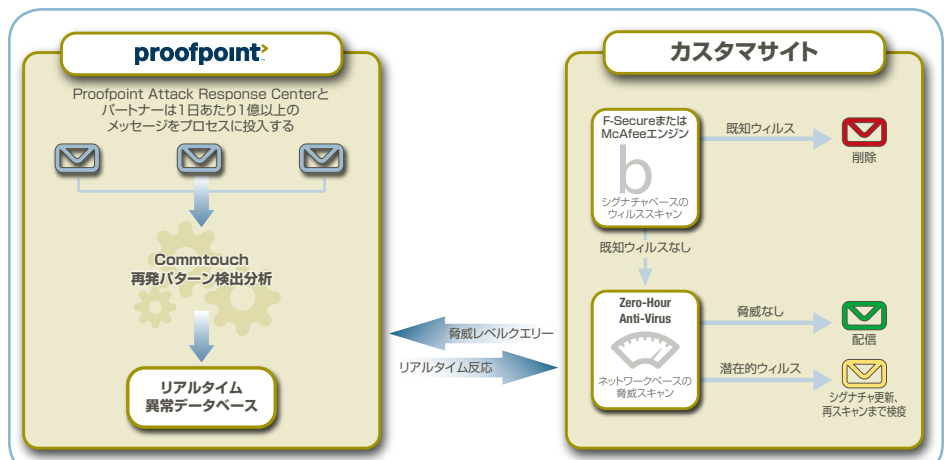
疑わしいメッセージの取り扱いに関するルールはさまざまなやり方でカスタマイズすることができます。Proofpoint Zero-Hour Anti-Virus では、以下を含む任意の数のポリシーを定義することができます。

- **疑わしいメッセージのポリシー**：このポリシーは疑わしいウイルスを含むメッセージの取り扱い方法を定義します。メッセージルート（インバウンド、アウトバウンドなど）、脅威分類レベル（ウイルス汚染の確率が中それとも高）、ドキュメントタイプおよび／または MIME タイプに基づいて、独自のポリシーを定義することができます。Proofpoint の標準的なメッセージ処理オプション（たとえば、継続、受信拒否、検疫など）はすべて用意されています。通常、疑惑メッセージは Zero-Hour 検疫に回され、そこで将来的なウイルスシグナチャアップデートによる再スキャンに備えて保持されます。
- **推定ウイルスポリシー**：このポリシーは検疫や再スキャンを受けたあとでもウイルス汚染が疑われるメッセージの取り扱い方法を定義します。ポリシーは先に説明したすべての条件に基づいて定義できます。通常、こういったメッセージは「推定ウイルス」検疫に回され、そこで永久的な削除の前に一定期間は保持することができます。

### カスタマイズ可能な検疫フォルダ

Proofpoint Zero-Hour Anti-Virus モジュールをインストールすると、特定の条件が充足されるまでメッセージを保持してから、Proofpoint Virus Protection エンジンによるスキャンのためにそれらのメッセージを再提出する「Zero-Hour 遅延」行動で検疫フォルダをカスタマイズすることができます。フォルダはさまざまなやり方でカスタマイズすることができ、そのようなやり方の例として、再提出まで待つべきウイルス対策シグナチャ更新回数や最小／最大検疫時間が挙げられます。

## 一目でわかる Proofpoint Zero-Hour Anti-Virus



Proofpoint Zero-Hour Anti-Virus は再発パターン検出テクノロジー、Zero-Hour ヒューリスティクス、メッセージ別マッチングの組み合わせを用いて新ウイルスを特定します。Proofpoint Zero-Hour Anti-Virus は Proofpoint Virus Protection が提供するシグナチャベースの対策と協調して動作し、あらゆる種類の悪意あるコードから守ってくれます。

### 比類なき Zero-Hour Anti-Virus

Proofpoint Zero-Hour Anti-Virus はその他の Proofpoint 防御と協調して動作し、ウイルス、ワーム、およびその他の形態の悪意あるコードに対してほとんど侵入不可能な防御を行います。

着信メッセージはさまざまな防御システムによって処理され、これらのシステムでは正当なメッセージだけが貴社エンタープライズに入ることが許されます。メッセージはまず正当性についてとその他のポリシー違反がないかをスキャンします。次に Proofpoint のシグナチャベースのウイルス対策防御によってスキャンされます。

### Zero-Hour スキャンング

シグナチャベースのウイルス対策フィルタによってクリーンだと宣言されたメッセージは、次に Zero-Hour Anti-Virus モジュールに引き渡され、メッセージが従来のシグナチャをまだ利用できない最近の発生の一部を構成しているかどうかを判断します。

- Zero-Hour Anti-Virus 対策モジュールがメッセージはクリーンであると判断すれば、そのメッセージは目的の宛先に配信されます。
- このモジュールがメッセージは新しいウイルス発生の一部であると判断すれば、そのメッセージは疑わしいと分類され、Zero-Hour ポリシーによって指定されたように取り扱われます。

### Zero-Hour 検疫

疑わしいメッセージには重大度（確認済みウイルス、高リスク、中リスク）が割り当てられ、このリスクレベルとその他のメッセージ属性に基づいてさまざまなポリシーが起動します。

通常、疑わしいメッセージは Zero-Hour 検疫に回され、そこで規定時間（たとえば、2 回のウイルス対策シグナチャ更新が受信されるまで）保持されてから、当該メッセージは再スキャンを受けるために Proofpoint Virus Protection に再提出されます。

### Proofpoint Zero-Hour Anti-Virus を更に詳しく知りたい方のために

Proofpoint の新生ウイルス脅威に対する先進的対策の詳細については、以下のサイトにて、当社の無料ホワイトペーパー「Zero-Hour ギャップを閉じる」をダウンロードしてください。

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

©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 Virus Protection、Proofpoint Spam Detection、Proofpoint Messaging Security Console、Proofpoint Messaging Security Gateway、Proofpoint Zero-Hour Anti-Virus 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