

# すべてのマルウェアに効く特效薬はない

## 継ぎ接ぎのセキュリティ

エンドポイントセキュリティの場合、新たな攻撃に継続的に対応することは難しくないように思えます。実際、このように対処している組織も少なくありません。新しいマルウェアが登場すると、その攻撃を防ぐために新しい保護製品を投入します。6か月後、新たな手口で攻撃するマルウェアが出現すると、その対策として新しい製品を追加します。さらに6か月後、同じことを繰り返します。そして、このサイクルが続きます。

## エンドポイント セキュリティの統合

エンドポイントの保護に万能薬は必要ありません。複数の技術を連携し、自動化することで同じ効果を得ることができます。たとえば、防御層の1つが突破されても、その情報を利用して別の保護技術で脅威を阻止し、被害を未然に防ぐことができます。

次世代のMcAfeeマルウェア対策とエンドポイントセキュリティ技術は、真に統合されたエンドポイント保護ファブリックを提供します。それぞれの保護対策が相互に連携して機能するので、新しい情報からリアルタイムにアクションを実行できます。McAfeeの保護ファブリックは次の機能を提供します。

- **機械学習を利用した静的な動作分析:** McAfee® Real Protectの高度な機械学習技術により、シグネチャを使用せずに、既知の脅威と不審なファイルを比較します。
- **不審なアプリケーションの封じ込め:** McAfee アプリケーションの動的隔離機能により、マルウェアが頻繁に使用するプロセスをブロックします。これまで検出できなかったゼロデイ マルウェアからエンドポイントを保護できます。
- **サンドボックスの解析:** McAfee Advanced Threat Defenseの安全な環境でコード全体を詳しく分析し、不審なファイルを特定します。最も高度な標的型マルウェアも検出できます。

## エグゼクティブ サマリー

これらの技術がそれぞれ重要なマルウェア対策機能を提供します。これらの技術は多層型の保護システムを構成し、最初の感染を未然に防ぎます。また、脅威対応をリアルタイムに行うことができます。

### 継ぎ接ぎのセキュリティを放置しない

マルウェアの脅威は進化を続けています。すべてのマルウェアに効く特効薬はありません。独立した複数のソリューションを継ぎ接ぎで使用すると、より多くの時間とリソースが必要になり、作業も複雑になります。セキュリティ チームにはさらなる負担がかかります。よりスマートな対策が必要です。

### 詳細情報

『**すべてのマルウェアに効く特効薬はない**』をダウンロードして、McAfee Real Protect、アプリケーションの動的隔離、Advanced Threat Defense が連携して機能する仕組みをご覧ください。



〒150-0043  
東京都渋谷区道玄坂1-12-1  
渋谷マークシティウエスト20F  
[www.mcafee.com/jp](http://www.mcafee.com/jp)

McAfeeおよびMcAfeeのロゴは米国法人McAfee, LLCまたは米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2017 McAfee, LLC. 2933\_0317  
2017年3月