ソリューション概要

不審なプログラムに対する対策

不審なプログラム（PUP）については『**McAfee® Labs脅威レポート: 2015年2月**』に詳しい解説があります。ユーザーがメリットを感じていても、具体的なリスクを伴うアプリケーションはPUPの可能性があります。アプリケーションは通常、使用上のリスクをユーザーに通知しません。トロイの木馬、ウイルス、ルートキットなどのマルウェアと異なり、PUPはユーザーの認証情報（ソーシャル メディア、オンラインバンキングなど）を盗み出したり、システム ファイルを改ざんすることはありません。リスクをもたらすだけでなく、ユーザーにとって便利な面もあるため、PUPはグレーゾーンに存在するといえます。分類も難しく、検出も容易ではありません。

PUPには次のような特徴があります。

- ブラウザーなどのシステム設定を許可なく変更する
- 正規のアプリケーションの中に不要なプログラムを隠す
- ユーザーの情報、閲覧習慣、システム設定などを密かに収集する
- アプリケーションのインストールを隠す
- 簡単に削除されないようにする
- 偽の広告や紛らわしい広告で配布される

PUPは次の種類に分類できます。

- **アドウェア**: 主に、ブラウザーに広告を表示します。
- **パスワード クラッカー**: アプリケーションで非表示のパスワードを表示します。
- **リモート管理ツール**: インストールされたマシン上でのユーザーの操作を監視します。ユーザーに気づかれずに、あるいはユーザーの許可なくシステムをリモートから制御します。
- **キー ジェネレーター**: 正規のアプリケーションのプロダクト キーを生成します。
- **ブラウザー ハイジャッカー**: ホームページ、検索ページなどのブラウザーの設定を変更します。
- **ハッキング ツール**: システムへの侵入や重要なデータの流出を容易にする単独のアプリケーション。
- **プロキシ**: リダイレクトを行ったり、IP関連の情報を隠します。
- **トラッキング ツール:** ユーザーのキー操作、個人的なやり取りを記録したり、ユーザーのオンライン操作を監視するスパイウェアやキーロガー。また、ユーザーに気づかれずに画面イメージを取得します。

intel Security

PUPと他のマルウェア（トロイの木馬、ランサムウェア、ボット、ウイルスなど）との主な違いは次のとおりです。

技術	不審なプログラム	その他のマルウェア: トロイの木馬、ウイルス、ボットなど
インストール方法	標準のアプリケーション インストール手順。EULAを表示するものもある。インストールを完了するには、ユーザーの同意や入力が必要になることが多い。	単独のプログラムとしてインストールされるが、ユーザーの入力は必要としない。大半は独立したファイルとして動作する。
パッケージ	マルウェアに感染していないアプリケーションにバンドルされ、このアプリと一緒にインストールされる。	追加コンポーネントを含む単独ファイル。インストーラーはない。
削除	パッケージにアンインストーラーが付いていることもある。削除は可能。ただし、簡単には削除できないことが多い。	実行ファイルが他のプロセス、プロセス ハンドル、複雑なリンクをフックするため、簡単に駆除できない。インストーラー パッケージではないため、コントロール パネルには表示されない。
動作	不要な広告、ポップアップ、ポップアンダーを表示する。ユーザーに気づかれずに、あるいはユーザーの許可なくブラウザーの設定を変更したり、ユーザーとシステムのデータを収集する。リモートからシステムを制御する場合もある。	個人情報やオンライン バンキングの認証情報を盗み出す。システム ファイルを改ざんし、システムを使用不能にする。身代金を要求する。
ステルス性	通常、ステルス性はない。	ファイル、フォルダー、レジストリ エントリ、ネットワーク トラフィックを隠蔽する場合がある。

PUPの中でセキュリティ ベンダーの関心を最も集めているのがアドウェアです。迷惑な広告を表示することではなく、アドウェアが信用を悪用する方法が問題となっています。最近のアドウェアは様々な技術を駆使し、感染先のシステムで持続的に存在するようになっています。たとえば、次のような技術を悪用しています。

- メモリーで実行される単独のプロセス
- ファイルアプリ固有の機能が組み込まれたCOM（Component object model）型とCOM型以外のDLL
- ブラウザー ヘルパー オブジェクトのレジストリ キー
- システム プロセスにフックするDLL
- ブラウザー拡張とプラグイン
- 登録済みのシステム サービス
- デバイス制御を実行するデバイス ドライバー コンポーネント
- 低レベルのフィルター ドライバー
- ペイロードとして配布されたトロイの木馬

PUPはユーザーの信用を悪用して拡散します（信用の悪用については『**McAfee Labs脅威レポート: 2014年11月**』を参照）。PUPの一般的な拡散方法は次のとおりです。

- 正規のアプリケーションの悪用
- ソーシャルエンジニアリング
- Facebookの「いいね」
- Facebookへの詐欺メッセージの掲載
- Google AdSenseのハイジャック
- 不要なブラウザー拡張やプラグイン
- 正規のアプリケーションと一緒に強制的にインストール

PUPから保護するIntel Securityのソリューション

McAfee Application Control

McAfee Application Controlでは、動的ホワイトリストとポリシーの施行により、環境内で実行を許可するアプリケーションを制御できます。この機能は、ネットワークに接続しているエンドポイントだけでなく、接続していないエンドポイントにも実行できます。これにより、PUPから組織を保護します。

- **動的ホワイトリスト**: システムにパッチが適用され、最新の状態になると、ホワイトリストが自動的に作成されます。これにより、ホワイトリストに登録されたアプリケーションを効率的に管理できます。McAfee Application Controlは、既知のマルウェアの実行を許可しないため、PUPによるリスクを軽減できます。
- **ファイル レピュテーション**: **McAfee Global Threat Intelligence**（McAfee GTI）との統合により、McAfee Application Controlはファイルの評価情報（正常、不正、不明）をリアルタイムに取得します。PUPを常に監視し、対策を講じることができます。
- **接続状態に関係のない保護**: 接続または切断状態のサーバー、仮想マシン、エンドポイント、POSなどの専用端末を保護します。

McAfee Web Gateway

マルバタイジング、ドライブバイ ダウンロード、信頼されたWebサイトに埋め込まれた不正なURLはPUPを配布する手口の一例に過ぎません。**McAfee Web Gateway**は、このような脅威を阻止し、会社の保護対策を強化する強力な製品です。

- **McAfee Gateway Anti-Malware Engine**: シグネチャを使用しない意図解析により、Webトラフィックから不正なコンテンツをリアルタイムで排除します。McAfee Gateway Anti-Malware Engineはファイルを検査し、不正なファイルのダウンロードをブロックします。
- **McAfee GTIとの統合**: McAfee Web Gatewayは、McAfee GTIからリアルタイムで提供されるファイル レピュテーション、Web レピュテーション、Web カテゴライゼーションにより、最新の脅威を阻止します。既知の不正なサイトに対する接続だけでなく、不正な広告ネットワークを使用しているサイトへの接続も拒否します。

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence（McAfee GTI）は、包括的な脅威情報をリアルタイムで提供するクラウド ベースのサービスです。マカフィー製品はこの情報を利用して、ファイル、Web、メッセージ、ネットワークを利用したサイバー脅威をブロックしています。次の機能でPUPをプロアクティブに阻止します。

- **攻撃の相関分析**: ファイル、Web、メール、ネットワークなど、主な脅威の侵入源からデータを収集し、相関分析を行います。これにより、署名付きの不正なマルウェアを配布する広告ネットワークなど、複合型の脅威を検出できます。
- **包括的な脅威情報プラットフォーム**: 数百万台のセンサーを使用して、顧客に配備されたマカフィー製品（エンドポイント、Web、メール、ネットワーク侵入防止（IPS）、ファイアウォール機器など）から脅威情報を収集します。

- **証明書のレピュテーション**: 証明書の評価情報をリアルタイムで提供します。不正な広告ネットワークで配信される可能性がある署名付きのマルウェアなどの脅威を阻止できます。
- **Security Connected**: 他のマカフィー セキュリティ製品との統合により、総合的な脅威データを相関分析し、包括的な保護対策を実施します。これにより、アドウェアによる攻撃を防ぐことができます。

McAfee SiteAdvisor® Enterprise
脅威は常に変化しています。このような脅威を常に阻止するのは容易なことではありません。特に、ユーザーの利便性を阻害するポリシーを施行することなく、PUPの脅威からオンライン ユーザーを保護すること簡単ではありません。

- **正規のサイトを装う不正なWebサイトを簡単に見分ける**: **McAfee SiteAdvisor Enterprise**は、分かりやすい色別のコードでサイトの評価結果を表し、デスクトップに新たな保護層を追加します。既知の不正なサイトに対する接続を拒否し、ユーザーにサイトの危険性を通知します。
- **McAfee GTIによるセキュリティの強化**: McAfee SiteAdvisor Enterpriseは、McAfee GTIからリアルタイムで提供される最新の脅威情報に基づいてサイトの評価を行います。

McAfee Threat Intelligence Exchange
情報プラットフォームは環境の要件に合わせて拡張していく必要があります。**McAfee Threat Intelligence Exchange**を使用すると、環境内で実行される不明なファイルやアプリケーションなど、組織の脅威状況を正確に把握できます。これにより、攻撃のリスクを劇的に減らすことができます。

- **包括的な脅威情報**: グローバルなソースから総合的な脅威情報を収集できます。これらの情報ソースは簡単に調整できます。McAfee GTIだけでなく、サードパーティのソースも利用できます。エンドポイント、ゲートウェイ、その他のセキュリティ コンポーネントからリアルタイムで受信したローカルのイベント データや履歴データも使用できます。
- **実行防止と修復**: McAfee Threat Intelligence Exchangeは環境内で不明なアプリケーションの実行を防止します。実行が許可されたアプリケーションが後で不正なプログラムと認識された場合、McAfee Threat Intelligence Exchangeは、強力な一元管理機能とポリシー施行機能により、アプリケーションに関連する実行中のプロセスを無効にします。
- **証明書のレピュテーション**: McAfee GTIとの統合により、既知の不正な証明書に関する情報をリアルタイムで取得し、署名付きの不正コードによる攻撃を迅速に検出して阻止します。McAfee Threat Intelligence Exchangeは、ポリシーを一元管理して不正な証明書からエンドポイントを保護します。このポリシーは、ネットワークに接続していないエンドポイントにも配備されます。

McAfee VirusScan® Enterprise

McAfee VirusScan Enterpriseを使用すると、アドウェアを含むマルウェアを検出し、簡単に駆除することができます。McAfee VirusScan Enterpriseは、実績豊富なマカフィーのスキャン エンジンを搭載し、ウイルス、ワーム、ルートキット、トロイの木馬などの高度な脅威からシステムを保護します。

- **攻撃からプロアクティブに保護**: マルウェア対策と侵入防止機能が統合され、アプリケーションに存在するバッファー オーバーフローの脆弱性を攻撃するエクスプロイトを阻止します。
- **非常に強力なマルウェア検出・駆除機能**: 高度な動作分析により、ルートキットやトロイの木馬などの脅威を阻止します。ポート ブロック、ファイル名でのブロック、フォルダー/ディレクトリのロック、ファイル共有のロック、感染の追跡/ブロックなどの技術により、マルウェアの侵入を阻止します。
- **McAfee GTIの統合でリアルタイムのセキュリティを実現**: 市場で最も包括的な脅威情報プラットフォームにより、ファイル、Web、メール、ネットワークを介して侵入する脅威を検出します。既知の脅威だけでなく、新たに発生する脅威も阻止します。

従来の信頼モデルを密かに悪用するPUPから組織を保護することは簡単なことではありません。業界最高のMcAfee LabsとIntel Securityのテクノロジを組み合わせることで、組織をPUPから保護することができます。

McAfee. Part of Intel Security.

東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1
渋谷マークシティウェスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480

西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2
近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517

名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内 3-20-17
中外東京海上ビルディング 3F
TEL 052-954-9551（代）FAX 052-954-9552

福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8
アクア博多 5F
TEL 092-287-9674（代）

www.intelsecurity.com