ホワイト ペーパー

Web セキュリティ：クラウドのデータを保護する

概要

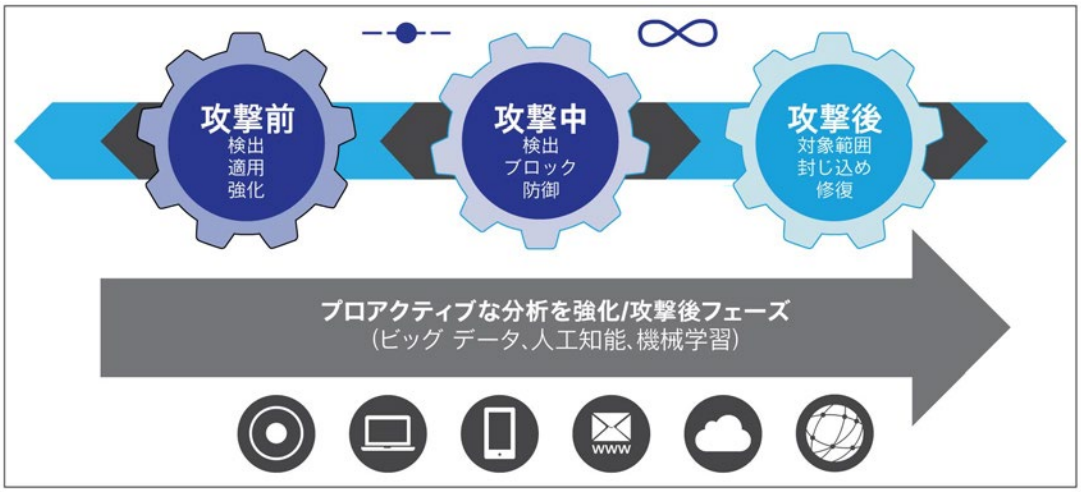
すべての場所にセキュリティ チームを配備することは不可能ですが、現代の企業には、脅威が生じうるあらゆる場所でデータを保護することが求められます。この「あらゆる場所」には、ネットワーク、モバイル デバイス、仮想環境、クラウド、データセンターなどが含まれます。

今日の脅威は、あらゆる保護対策を突破するように設計されています。攻撃者は、どのようなセキュリティ ソリューションが導入されているかを積極的に研究しています。さらに、攻撃のパターンはさらに見えにくく、検出されにくい方向に変化してきています。**シスコ年次セキュリティ レポート（2014 年）**によると、攻撃者の大部分は価値の高いデータを盗むことを第一の目的としています。[1]

その一方で、分散型企業の広がりや、クラウド コンピューティング、モビリティ、個人所有デバイスの持ち込み（BYOD）環境などの新しいビジネス モデルの登場によって、従来のセキュリティ境界は次第に危うくなり、攻撃対象範囲（Attack Surface）は広がっています。セキュリティ チームは、この変化に対応するために苦心しています。調査すべき脅威の優先順位をどのように判断したらいいかわからず、単純に「見えていない」ことで多くの脅威を見逃しています。

予防的なポイントインタイム（point-in-time）型セキュリティ ソリューションが現代のビジネスにおいて十分な防御対策にならない理由はすぐにおわかりでしょう。もちろん、完璧な脅威検出システムはありませんし、今後、何重もの防御対策をすべて出し抜くほど洗練されたステルス性の高い脅威が必ず出てくると考えられます。では、何が必要なのでしょうか。求められるのは、「攻撃前」、「攻撃中」、「攻撃後」の各フェーズを連続的な攻撃サイクル（攻撃コンティニューム）として捉える継続的でレトロスペクティブなセキュリティです。

図 1. 一連の攻撃



[1] シスコ年次セキュリティ レポート（2014 年）：http://www.cisco.com/web/JP/solution/security/literature/pdf/Cisco-2014-ASR.pdf 。

Cisco Cloud Web Security Essentials

Cisco® Cloud Web Security（CWS）は、企業の拡張ネットワーク全体にわたって継続的なセキュリティを維持するという目標を実現するために役立ちます。このソリューションは分散型企業に業界最高レベルのセキュリティと管理をもたらすもので、幅広い導入オプションが用意されています。Cisco Web セキュリティのクラウドベース版である CWS のプラットフォームは、モバイル機器および分散環境へ拡張された Web セキュリティを提供します。シスコの世界的な脅威インテリジェンスと、高度な脅威防御機能、ローミング ユーザ保護を通じて、ユーザを安全に保護します。

Cisco CWS では、わかりやすいツールを使用してインバウンドとアウトバウンドの Web ポリシーを作成、適用、監視でき、インターネット コンテンツにアクセスするエンド ユーザの行動をきめ細かく制御できます。つまり、Cisco CWS はクラウド上におけるセキュリティ境界なのです。Cisco CWS はコンテキスト認識型のポリシー制御と適用を可能にし、 さらに次のことを実現します。

- 脅威をリアルタイムで動的にブロック
- ネットワークやユーザを望ましくない Web コンテンツから保護
- 帯域幅の輻輳を緩和して、ネットワーク リソースを最適化
- オンライン活動の広範囲におよぶレポートやモニタリングの実現を支援します
- データ漏洩の防止

Cisco CWS は Cisco の ファイアウォール、ブランチ ルータ、および顧客ベースのソフトウェアと統合し、ユーザがどこで作業しているかに関わらず保護します。すべてのトラフィックは、それが本社、支社、モバイル、リモート ユーザからのトラフィックであるに関わらず、データセンターのグローバル・ネットワークを通して提供されます。Cisco CWS はバックホールを排除し、Web セキュリティのすみやかな導入を可能にし、既存のシスコソリューションへの投資価値を高めます。

シスコは数年前にセキュリティ企業 Sourcefire と Cognitive Security を買収したことで、Cisco CWS をさらに強化し、攻撃コンティニュームの「攻撃後」フェーズで高度なマルウェア脅威を軽減するとともに、「攻撃中」フェーズでリアルタイムの脅威検出を行うことを可能にしています。シスコはこのソリューションを以下に示すオプションの Premium サブスクリプションで提供しています。

Cloud Web Security Premium

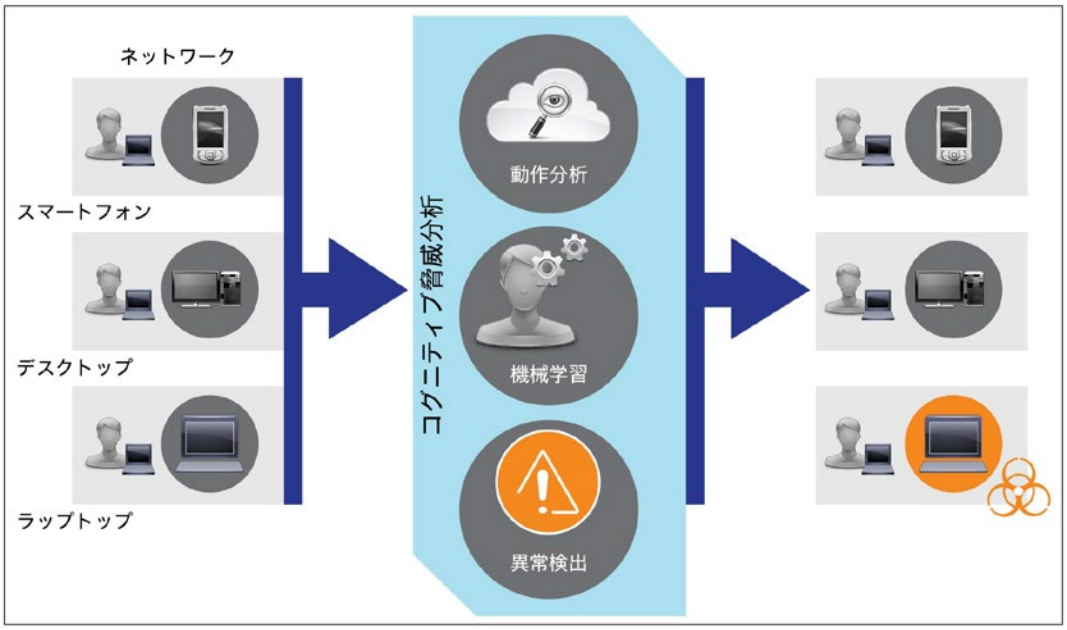
Cloud Web Security Premium のプレミアム バンドルには、エッセンシャル バンドルに含まれる機能すべてが含まれるだけでなく、2 つの革新的なマルウェア検出システムである Cognitive Threat Analytics（CTA）と Advanced Malware Protection（AMP）が組み込まれています。これらのシステムは、組織の Web トラフィックにリスクの高い脅威が紛れていないかどうかの探索を自動化します。また Cisco CWS Premium は、重大な脅威を検出して対処するために役立つポイントインタイム保護、レトロスペクティブなセキュリティ、継続的分析の機能を提供します。さらに、すでにネットワーク内部で活動している脅威を発見するまでの時間を短縮します。

これにより、セキュリティ チームは攻撃コンティニュームの全フェーズにまたがってシステムを保護する継続的な Web セキュリティを実現できます。以降では、前述の 2 つのマルウェア検出システムについて詳しく説明します。

コグニティブ脅威分析

Cognitive Threat Analytics（CTA）は、Cognitive Security で開発されたほぼリアルタイムのネットワーク動作分析システムです。機械学習と高度な統計に基づいて、ネットワーク上の異常なアクティビティ、つまり感染の症状を検出します。このソリューションはルールセットに依存しないため、テクノロジーを「調整」するために手動で介入する必要はありません。CTA を有効にすると、ただちに脅威の探索が始まります。CTA の異常検出機能のスピード、俊敏性、および深度を向上させるために、データはクラウド内で相互に関連付けされます。

図 2. CTA の概要



CTA は収集したデータから学習します。時間経過とともに適応を深め、セキュリティ業界が以前は検出できなかった新しい指揮統制チャネルを認識するようになります。CTA はネットワーク内のエンティティ（個々のユーザなど）の動作を評価し、行動モデリングに基づいて、そのエンティティがどのような動作をするかを予測します。ネットワーク動作の長期的なモデリングに基づいて、一見関連のなさそうなアクティビティを相互に関連付けます。そして、関連付けられたデータを特定の顧客ネットワークにおける個々のユーザの動作と比較することで、よりすみやかに脅威を検出します。

CTA では、脅威の種類はあまり重視されません。予期される動作との不一致が大きい場合、または継続的に認められる場合に、フラグが立てられます。CTA の動作は、万引き犯を未然に特定しようとする防犯チームのそれに似ています。つまり、他の買い物客と違う行動をしている人物はいないかに注目するのです。ショッピング カートを押す代わりに、大きなバッグを持っている人はいないか、 正面ドアの代わりに裏口から出ようとしている人はいないか、という点に注目します。疑わしく見えた行動が実際には正当なものだと判明する場合もありますが、調査するだけの価値はあります。

CTA は異常を見つけ、問題の可能性をセキュリティ アナリストに知らせることで、セキュリティ アナリストの負担を減らし、対応すべき脅威の優先順位を付けることに貢献します。また、シスコの既存のセキュリティ テクノロジーを補完し、これらのソリューションがより正確に、より的確にネットワーク上の未知の動作や普通でない動作を検出できるようにします。これにより、シスコのセキュリティ機能の守備範囲が、一連の攻撃の「攻撃後」フェーズにまで広がります。最も重要なのは、CTA は変化し続ける脅威にも対応可能なセキュリティをもたらすという点です。

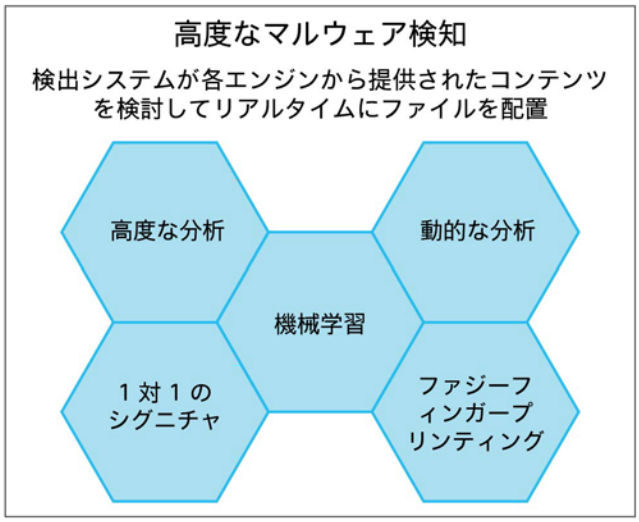
高度なマルウェア防御

Cisco CWS Premium の 2 つ目の検出システムは、Sourcefire で開発された Advanced Malware Protection（AMP）です。AMP は、シグニチャに基づくマルウェア検出システムではありません。シグニチャに頼る方式では、新しいマルウェアのサンプルを作成するのに数週間から数ヵ月かかる場合があるためです。その代わりに、ファイル レピュテーション、ファイル サンドボックス、レトロスペクティブ ファイル分析を組み合わせて使用することで、一連の攻撃全体にわたって脅威を特定、阻止します。

ファイル レピュテーション

ファイル レピュテーションとは、ファイルのデータベースを参照して、そのファイルが「クリーン」か、既知のマルウェアか、未知のファイルかを判別する機能です。AMP では、Cisco CWS サービスを通過する各ファイルの「フィンガープリント（痕跡）」を取得し、シスコと Sourcefire が管理するクラウドベースの集積型インテリジェント ネットワークに問い合わせて、ファイルの評価（レピュテーション）または「スコア」を入手します。この結果に基づいて、悪意のあるファイルを自動的にブロックし、管理者が定義したポリシーを適用します。図 3 に、高度なマルウェアを検出し、ファイルの評価を判定するためにリアルタイムで動作するさまざまなエンジンを示します。

図 3. 高度なマルウェア防御



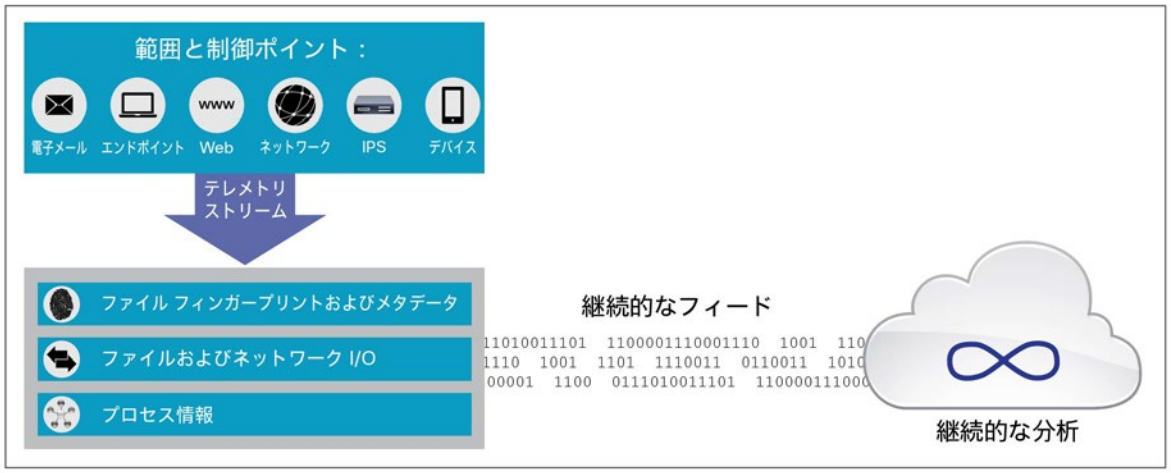
ファイル サンドボックス機能

ファイル サンドボックスは AMP の究極の機能で、Cloud Web Security Premium のみに含まれます。AMP では、ネットワークを通過する未知のファイルをファイル サンドボックスで分析します。安全性が高いサンドボックス環境で、AMP はファイルの動作について正確な詳細情報を収集し、そのデータを人間およびマシンによる詳細分析と組み合わせて、ファイルの脅威レベルを判定します。その後、この情報をクラウドベースの集積型インテリジェント ネットワークに提供して、AMP のクラウド データセットを動的に更新します。アクティブなレポート機能により、セキュリティ チームは分析対象ファイルに関する詳細で読みやすいレポートを入手することができます。

ファイル レトロスペクション機能

AMP の最も重要な側面はレトロスペクティブ分析機能でしょう。この機能により、時間をさかのぼってアウトブレイクがいつ発生したかを特定し、被害の大きさを評価することができます。ファイル レトロスペクション機能では、これまでにセキュリティ ゲートウェイを通過したファイル群を、シスコと Sourcefire が管理するクラウドベースのインテリジェント ネットワークから提供されるリアルタイム更新を利用して継続的に分析します。

図 4. AMP のレトロスペクティブな分析プロセス

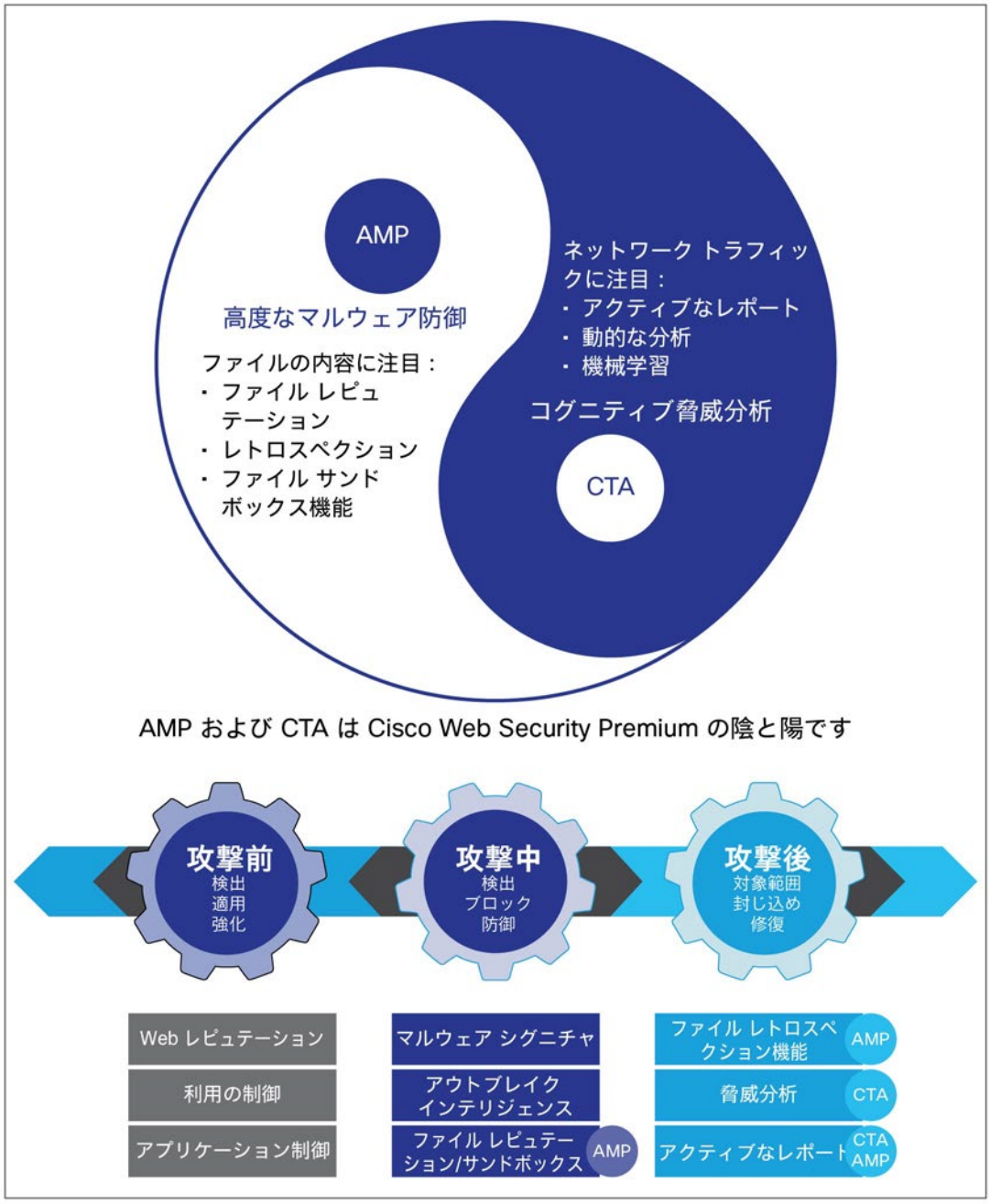


レトロスペクティブ分析により、境界防御を通過したときには「クリーン」と思われていたファイルが、実際には巧妙に偽装された高度なマルウェアだったことが判明する場合があります。その場合、AMP はただちにセキュリティ管理者に警告し、感染した可能性のあるネットワーク ユーザと感染の時期を特定します。これにより、セキュリティ チームは攻撃の範囲が広がる前に迅速に対応することができます。

まとめ

CTA と AMP を含む Cisco CWS Premium は、現在および将来における企業のセキュリティ課題にいかに対応するかというシスコの戦略に合致しており、 脅威の検出、理解、停止を支援します。継続的な分析とリアルタイム セキュリティ インテリジェンスをクラウドから提供し、あらゆるセキュリティ ソリューション間で共有することで、有効性を高めます。この 3 つのソリューションの組み合わせによって、セキュリティ業界が以前は検出できなかった新しい指揮統制チャネルを認識し、攻撃コンティニューム全体にわたるセキュリティ課題に対処することが可能になります。

図 5. AMP および CTA を活用した Cloud Web Security：攻撃コンティニューム全体に提供されるセキュリティ



攻撃前：検出、適用、強化

Cisco CWS は、Web レピュテーション、利用制御、アプリケーション制御（マイクロアプリケーションの制御を含む）、マルウェア シグニチャ、アウトブレーク インテリジェンスによって、「攻撃前」と「攻撃中」の両方のフェーズのセキュリティを実現します。

攻撃中：検出、ブロック、防御

AMP は、ファイル レピュテーション機能とファイル サンドボックス機能によって、攻撃コンティニュームの「攻撃中」フェーズのセキュリティを強化します。ファイルの既知のレピュテーションに基づいて、悪意のあるファイルを自動的にブロックし、管理者が定義したポリシーを適用します。また、ネットワークを通過する未知のファイルを分析し、脅威インテリジェンスを適宜更新します。このような機能は、セキュリティ アナリストが調査すべき脅威の優先順位を判断するために役立ちます。

攻撃後：対象範囲、封じ込め、修復

CTA と AMP の組み合わせによって、攻撃コンティニュームの重要な「攻撃後」フェーズにおける継続的な分析と修復が可能になります。CTA は、リアルタイムのネットワーク動作分析を行って、ネットワーク上の異常な動作を識別します。その一方で、AMP のファイル レトロスペクションは、境界防御を通過した悪意のあるファイルの問題に対応します。AMP のアクティブなレポート機能は、ネットワークに入ってきたファイルのレピュテーションや動作を可視化します。これにより、セキュリティ チームは攻撃の範囲を容易に見極め、すみやかに修復することができます。

また、CTA と AMP が「攻撃後」フェーズで行う機械学習によって、ほぼリアルタイムの検出機能が強化され、攻撃を受けている最中に Cisco CWS Premium がそれらを検出できるようになります。

詳細情報

Cisco Cloud Web Security Essentials および Cloud Web Security Premium についての詳細は、http://www.cisco.com/go/cws をご覧ください。

CTA の詳細については、http://www.cisco.com/go/cognitive [英語] を参照してください。

AMP の詳細については、http://www.cisco.com/go/amp [英語] を参照してください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

Printed in USA C11-734836-00 06/15