応募区分：事例型論文

脅威中心型セキュリティモデルで実現する次世代サイバーセキュリティ

尾山　和宏（おやま　かずひろ）
ネットワンシステムズ株式会社　ビジネス推進本部　第2応用技術部　セキュリティチーム

角田　玄司（かくだ　もとし）
ネットワンシステムズ株式会社　ビジネス推進本部　第2応用技術部　セキュリティチーム

浜田　貴里（はまだ　たかのり）
ネットワンシステムズ株式会社　ビジネス推進本部　第2応用技術部　セキュリティチーム

大竹　雄介（おおたけ　ゆうすけ）
ネットワンシステムズ株式会社　ビジネス推進本部　第2応用技術部　セキュリティチーム

大畑　光介（おおはた　こうすけ）
ネットワンシステムズ株式会社　ビジネス推進本部　第2応用技術部　セキュリティチーム

■ 要約

近年、標的型攻撃によるセキュリティ被害が増加している。標的型攻撃では巧妙に作成された Email や Web を介して未知のマルウェアに感染する。サンドボックスやヒューリスティック解析など未知のマルウェアに対する防御テクノロジーは存在するが、攻撃者も回避技術を開発するためマルウェア感染を完全に防ぐことは不可能である。これらの脅威に対し、Cisco はマルウェアに感染してしまうことを想定して攻撃後（After）の対策にも注力している点が特徴である。
本論文では実際の利用シーンを想定した検証を実施することで、攻撃前（Before）、攻撃中（During）、攻撃後（After）の各フェーズを包括的に保護する脅威中心型セキュリィモデルの有効性を実証した。さらに、各製品を連携させることでリモート端末のプロビジョニング、攻撃端末の隔離、未知のマルウェアへの対策を自動化できることを確認した。自動化することで、運用管理者の負担軽減、ヒューマンエラーの防止、脅威の早期封じ込めによる情報流出の阻止が期待できる。

目次

1. はじめに 4
2. Cisco セキュリティモデル 5
2.1. 攻撃前（Before） 5
2.2. 攻撃中（During） 5
2.3. 攻撃後（After） 5
3. 検証目的 6
3.1. 攻撃前（Before）対策の課題 6
3.2. 攻撃中（During）対策の課題 6
3.3. 攻撃後（After）対策の課題 6
4. 検証環境 7
4.1. 検証構成 7
4.2. 検証製品一覧 7
4.3. 製品説明 8
5. 攻撃前（Before）対策の検討 10
5.1. リモートアクセス端末へのプロビジョニング 10
5.2. プロビジョニングの流れ 10
5.3. AnyConnect Module の働き 12
5.4. 考察 14
6. 攻撃中（During）対策の検討 15
6.1. 入口、出口対策 15
6.2. 内部脅威の検知、ブロック、端末隔離 16
6.3. 検知、ブロック、端末隔離の流れ 17
6.4. コリレーションルール設定 18
6.5. 考察 19
7. 攻撃後（After）対策の検討 19
7.1. AMP によるレトロスペクティブセキュリティ 19
7.2. マルウェア検査の仕組み 20
7.3. クラウドリコール 21
7.4. トラジェクトリ 21
7.5. トラジェクトリを用いたフォレンジック 23
7.6. 考察 27
8. まとめ 28
9. 参考文献 29

1. はじめに

近年、情報セキュリティに対する脅威が高まっている。理由の一つに攻撃の性質、目的の変化が挙げられる。以前は悪戯や技術力のアピール等、愉快犯的な攻撃が多かったが、現在はプロの攻撃集団が金銭的な利益のために企業や官公庁の機密情報を狙って攻撃する。そのため、攻撃が成功した場合の被害は大きくなる。また、攻撃方法も日々進化している。標的型攻撃では偵察、侵入、潜伏を経て最終的に情報が搾取される。単発の攻撃ではなく継続的な攻撃が行われるのが特徴である。攻撃の多くは未知のマルウェアやゼロデイ・エクスプロイトが用いられるため、シグネチャベースのマルウェア対策では検知できない。入口、出口で全ての攻撃をブロックするのは困難であり、組織内に感染端末が潜んでいる前提で対策を施す必要がある。

このような状況に対して、Cisco は最新の脅威に対応するために新たなテクノロジーを組み込み、ポートフォリオを拡充してきた。現在、Sourcefire や ThreatGRID のテクノロジーを ASA や WSA、ESA など既存の Cisco セキュリティ製品にフィードバックし、機能の連携や統合が行われている。また、Cisco は攻撃前（Before）、攻撃中（During）、攻撃後（After）の各フェーズを包括的に保護する脅威中心型セキュリティモデルを提唱している。その中でもマルウェアに感染してしまうことを想定して攻撃後（After）の対策に注力している点が他社にはない特徴である。

本論文では実際の利用シーンを想定した検証を実施することで、脅威中心型セキュリィモデルの有効性を実証し、その特徴を明らかにする。さらに、各製品を連携させることで得られる効果について考察を行う。次章以降の概要を記載する。2 章では Cisco が提言する脅威中心型のセキュリティモデルについて説明する。3 章では攻撃前（Before）、攻撃中（During）、攻撃後（After）の各フェーズにおいて課題となる問題を考察し、その解決方法を提示する。4 章では本論文で用いる検証環境や製品に関して説明する。5 章では攻撃前（Before）対策としてリモートアクセス端末に対する自動的なプロビジョニングとアクセス制御、ポリシー適用の検証を実施する。その上で、プロビジョニングの詳細動作を説明し、自動化によるメリットについて考察する。6 章では攻撃中（During）対策として内部サーバへの攻撃を検知し、ブロックすると同時に自動的に攻撃元端末を隔離する検証を実施する。また、各製品をどのように連携させて端末隔離を行うかを説明する。7 章では攻撃後（After）対策として、端末内に存在するファイルがマルウェアと判明した場合に自動的に隔離される動作を確認する。また、マルウェアの侵入経路や拡散状況を速やかに確認できるかを検証する。8 章では検証を通した得られた結果を総括し、今後のサイバーセキュリティの展望を述べる。

2. Cisco セキュリティモデル

Cisco は攻撃エリアの拡大、巧妙化する攻撃・脅威に対応するため、一連の攻撃の流れ（Before/During/After）に沿って包括的なセキュリティを実現する脅威中心型のセキュリティモデルを提言している。[1] 図 1 に Cisco の新しいセキュリティモデルを示す。

2.1. 攻撃前（Before）

発見、適用、堅牢化を行う。ASA with FirePOWER Services によるネットワークの可視化とアクセス制御、ISE による認証、検疫、ポリシー適用、AnyConnect によるエンドポイントのセキュアな接続などがこれらに当たる。脅威を可視化し事前に対策を行うことで攻撃を軽減することができる。

2.2. 攻撃中（During）

攻撃の検出・ブロック、攻撃者の侵入から防御する。WSA や ESA によるコンテンツセキュリティ、FirePOWER による攻撃の検知とブロックがこれらに当たる。全ての攻撃をブロックすることは困難なため、攻撃後の対策が必要となる。

2.3. 攻撃後（After）

侵入経路の特定、被害範囲の確認を行い、脅威の拡散防止、再発防止、修復を行う必要がある。AMP（Advanced Malware Protection）のレトロスペクティブ機能や CTA（Cognitive Threat Analytics）を利用したネットワークのふるまい分析が有効な手段となる。

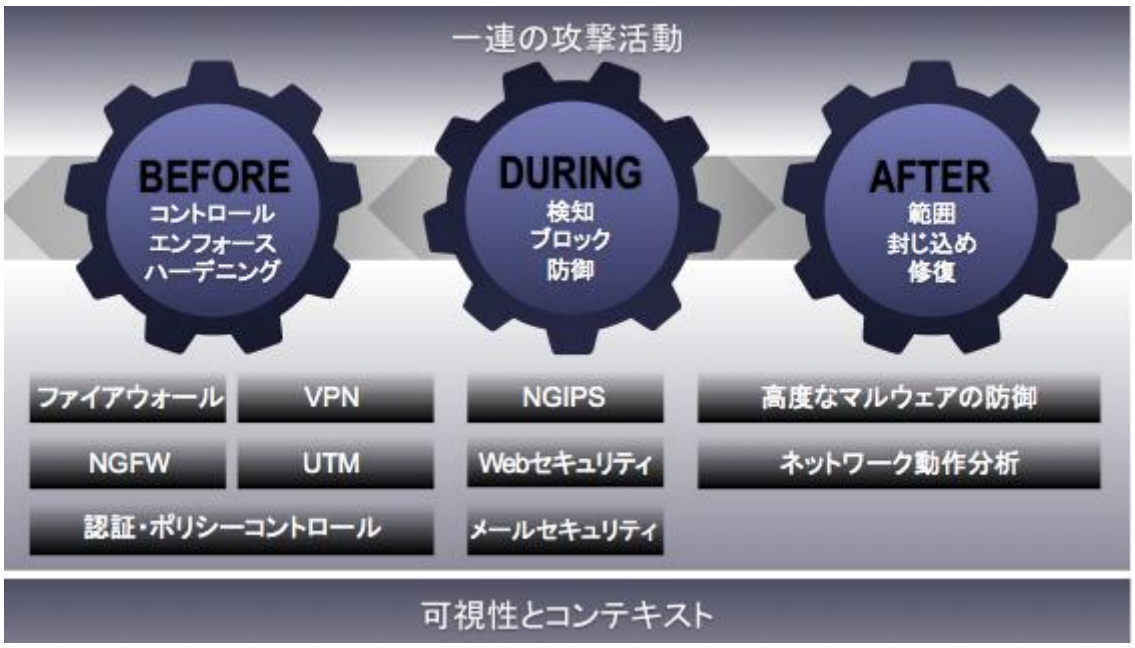


図 1. Cisco の新しいセキュリティモデル

3. 検証目的

3.1. 攻撃前（Before）対策の課題

攻撃前（Before）対策ではネットワークや端末を可視化し、適切なアクセス制御、ポリシー適用を行うことが要求される。近年、デバイスの多様化、働き方の多様化によって様々な形態のネットワーク接続が用いられる。無線 LAN を用いた BYOD やゲストアクセス、社内フリーアドレス、外出先や自宅からのリモートアクセス、VDI 接続など様々な環境に対して「いつ」、「どこから」、「誰が」、「どのデバイス」で接続しても利用者に応じた適切なアクセス制御、ポリシー適用が行われる必要がある。また、人事異動が発生した際にファイアウォールやスイッチ、セキュリティ機器、エンドポイント端末などを都度、設定変更するのは煩雑である。一元管理されたマネージャによって自動的にポリシーを配信することで、運用管理者の負担を軽減し設定ミスを防止することができる。

本論文では攻撃前（Before）対策として ISE、AnyConnect、ASA を用いてリモートアクセス端末に対する自動的なプロビジョニングとアクセス制御、ポリシー適用の有効性を確認する。

3.2. 攻撃中（During）対策の課題

攻撃中（During）対策ではマルウェアやエクスプロイトなどの攻撃を検知し、ブロックすることが求められる。入口、出口の対策は実施されているが、内部に侵入された場合の対策が十分に行われていないケースが多いのが課題である。また、インシデントが発生した端末は速やかに隔離する必要があるが、「報告やログの確認を経て LAN ケーブルを抜線する」といった対処では端末を隔離するまでに時間を要するため、その間に感染拡大や情報流出が発生する可能性が高くなる。

本論文では未知のマルウェアに感染した端末が内部のサーバに対して管理者権限の窃取を試みる攻撃シーンを想定した。攻撃中（During）対策として FirePOWER、FireSIGHT、ISE、Catalyst を用いて攻撃を検知し、ブロックすると同時に自動的に感染端末を隔離する検証を行う。

3.3. 攻撃後（After）対策の課題

攻撃後（After）対策ではインシデントに対して、迅速に対応することが重要となる。発見が遅れるほど、情報流出の危険性が高まる。また、事故発生時の発表が遅れることで、企業の信用やイメージ低下を引き起こし、多額の損害賠償に繋がる恐れがある。例えば、未知のマルウェアが社内に侵入していたことが判明した場合、早期に侵入経路、被害範囲の特定、脅威の隔離を行い情報流出の有無を確認する必要がある。しかしながら、侵入から数週間経過して感染が発覚した場合、マルウェアがどのような活動を行っていたか特定することが困難なため、調査には通常、数週間を要してしまうのが実情である。

本論文では攻撃後（After）対策として、Cisco AMP for Endpoints を用いて端末に侵入した未知のマルウェアが後日、マルウェアと判明した場合に自動的に隔離される動作を確認し、侵入経路や拡散状況を速やかに確認できるか検証する。

4. 検証環境

4.1. 検証構成

本論文の検証環境構成を図 2 に示す。

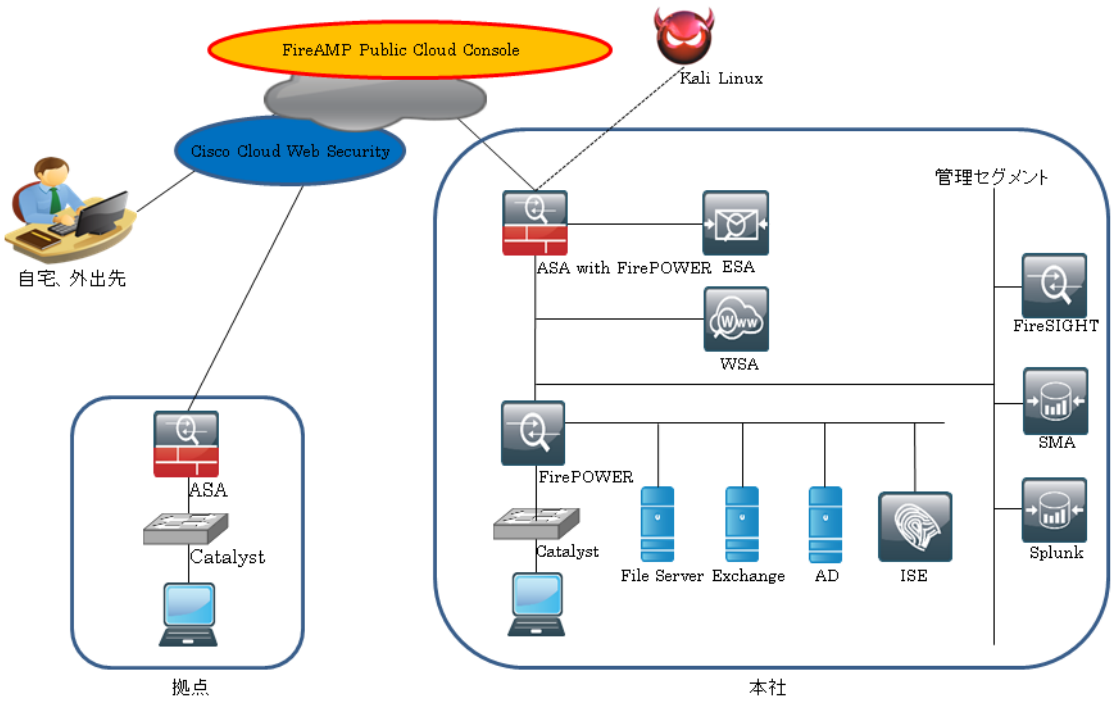


図 2. 検証環境構成

4.2. 検証製品一覧

本論文の検証に用いた製品を表 1 に示す。

表 1. 検証製品一覧

Product	Version
Cisco FirePOWER Virtual Appliance	5.4.0.3
Cisco FireSIGHT Management Center Virtual Appliance	5.4.1.2
Cisco ASA5515 with FirePOWER Services	ASA 9.4(1) / FirePOWER 5.4.0.3
Cisco Advanced Malware Protection for Endpoints	5.2.2015082115
Cisco Identity Services Engine	1.4.0.253
Cisco Email Security Virtual Appliance C000V	9.0.0-500
Cisco Web Security Virtual Appliance S000V	8.5.1-021
Cisco Security Management Appliance M000V	9.0.0-087
Cisco Cloud Web Security	5.2

Cisco AnyConnect Secure Mobility Client	4.1.02011
Splunk Enterprise	6.2.1 build 245427
Cisco Catalyst 3560	15.0(2)SE6
Kali Linux	1.0.6
Windows 8.1(Client PC)	Windows 8.1 Pro 64bit
Windows Server（File Server）	Windows Server 2012 R2
Windows Server（Exchange Server）	Windows Server 2012 R2
Windows Server（Active Directory Server）	Windows Server 2012 R2

4.3. 製品説明

本論文の検証に用いたセキュリティ製品について説明する。

① Cisco FirePOWER Appliance（FirePOWER）

ネットワークの可視化と学習機能、IPS の自動チューニングに特徴がある次世代 IPS 製品である。アプリケーション、ユーザ、ホストの可視化と制御、次世代 IPS、URL フィルタ、Web レピュテーション、AMP による高度なマルウェア対策、サンドボックス解析など脅威に対応する機能が充実している。

② Cisco FireSIGHT Management Center（FireSIGHT）

FirePOWER、ASA with FirePOWER Services の管理マネージャである。コンテキスト認識に優れており、物理ホストと仮想ホスト、オペレーティング システム、アプリケーション、サービス、プロトコル、ユーザ、位置情報、コンテンツ、ネットワークの動作、ネットワークへの攻撃、マルウェアなどネットワーク上のすべてを包括的に把握できる。イベント モニタリング、分析、インシデントの優先順位付け、レポートなどのネットワーク セキュリティおよび運用の機能を一元管理する。

③ Cisco ASA with FirePOWER Services（ASA）

ASA はステートフルファイアウォール、VPN 終端装置として優れた機能、豊富な実績、信頼性がある。ASA に FirePOWER の脅威に対応する機能を統合することでファイアウォールによる保護と次世代 IPS による保護を両立している。

④ Cisco Advanced Malware Protection for Endpoints（AMP for Endpoints）

エンドポイント向けの次世代マルウェア対策ソリューションである。過去に遡ってマルウェアを追跡、隔離できるレトロスペクティブ機能が特徴である。ThreatGRID によるサンドボックス解析も提供される。

⑤ Cisco Identity Services Engine（ISE）

社内外の有線、無線やリモートアクセスネットワークのユーザ/デバイス認証を行う統合型認証サーバである。ユーザ/デバイスに合わせたアクセス制御、ポリシー適用を行い検疫や修復を提供する。BYOD ソリューションにも用いられる。

⑥ Cisco Email Security Appliance（ESA）

Email 経由のセキュリティ脅威からの防御を提供する。迷惑メール、マルウェアなどの脅威から迅速かつ徹底的に Email を保護し、攻撃前、攻撃中、および攻撃後も継続的な保護を行う。AMP によるハッシュベースのマルウェア検知、サンドボックス解析も提供する。

⑦ Cisco Web Security Appliance（WSA）

Web 経由のセキュリティ脅威からの防御を提供する。コンテンツフィルタ、アンチマルウェア、Web プロキシを 1 台で提供する。Web レピュテーションや L4 トラフィックモニタ（L4TM）など高度な脅威防御や複数エンジンによるマルウェア検知が可能である。AMP によるハッシュベースのマルウェア検知、サンドボックス解析も提供する。

⑧ Cisco Content Security Management Appliance（SMA）

複数の ESA および WSA をサポートする集中管理プラットフォームである。複数の ESA、WSA の統計情報、ログ、レポートを一元化して表示する機能を提供する。また、複数の WSA の設定ポリシーを SMA で一元管理できる。

⑨ Cisco Cloud Web Security（CWS）

Cisco が提供するクラウドベースの Web セキュリティサービスである。ASA や AnyConnect、WSA などをコネクタとして使用することでクラウド上のセキュリティサーバを経由したセキュアな Web アクセスが可能となる。WSA とほぼ同等の機能を持つ。

⑩ Cisco AnyConnect Secure Mobility Client（AnyConnect）

ASA や Cisco ルータを終端装置として SSL-VPN、IPsec-VPN で接続できるリモートアクセス VPN ソフトウェアである。VPN を繋ぐだけでなく、アクセス制御や Web セキュリティ、検疫などエンドポイントを安全に保つための機能も統合されている。豊富なプラットフォームに対応する。

⑪ Splunk Enterprise（Splunk）

Splunk 社が販売する統合ログ管理ソフトウェアである。データ収集とインデックス化による横断的なログの検索、分析が特徴である。Apps と呼ばれる特定のデバイスに対応したテンプレートが存在し、これを用いることで対象デバイスのデータ分析やダッシュボード作成を効率的に行える。Cisco のセキュリティ製品に対応する Apps が Cisco 社から提供されている。SIEM（Security Information and Event Management）としても利用可能である。

5. 攻撃前（Before）対策の検討

5.1. リモートアクセス端末へのプロビジョニング

攻撃前（Before）対策ではネットワークや端末を可視化し、適切なアクセス制御、ポリシー適用を行うことが要求される。社内 LAN の端末に対してこれらを実装するだけでなく、インターネットを経由するリモートアクセス端末に対しても同様のポリシーを適用できることが望ましい。本検証では、ISE と AnyConnect、ASA を用いて、リモートアクセス端末にこれらの機能をプロビジョニングし、その有効性を示す。

5.2. プロビジョニングの流れ

リモートアクセス端末へのプロビジョニングは次のように行われる。図 3 にプロビジョニングの流れを示す。

① リモートアクセス端末から ASA のグローバル IP アドレス宛にアクセスすると、Web の認証画面が表示される。利用者は証明書やユーザ名、パスワード等を用いてログインを試行する。

② ASA は ISE にユーザ名、パスワードなどが含まれた認証要求を送信する。ISE はユーザ名を Active Directory（AD サーバ）内のユーザ情報と照合し、ユーザ名、パスワードが一致すると属性情報と共に認証許可を ASA に送信する。

③ リモートアクセス端末は ASA のリモートアクセスポータルページにログインし、同時に VPN 接続が開始される。この際、端末に AnyConnect がインストールされていない場合は自動的に VPN モジュールがインストールされる。

④ AnyConnect の接続が完了すると、ISE はリモートアクセス端末に AnyConnect の各モジュールがインストールされているか確認する。モジュールがインストールされていない場合、リモートアクセス端末をプロビジョニング用の Web ページにリダイレクトさせる。リダイレクトされたページで AnyConnect の各モジュールのインストールが行われる。

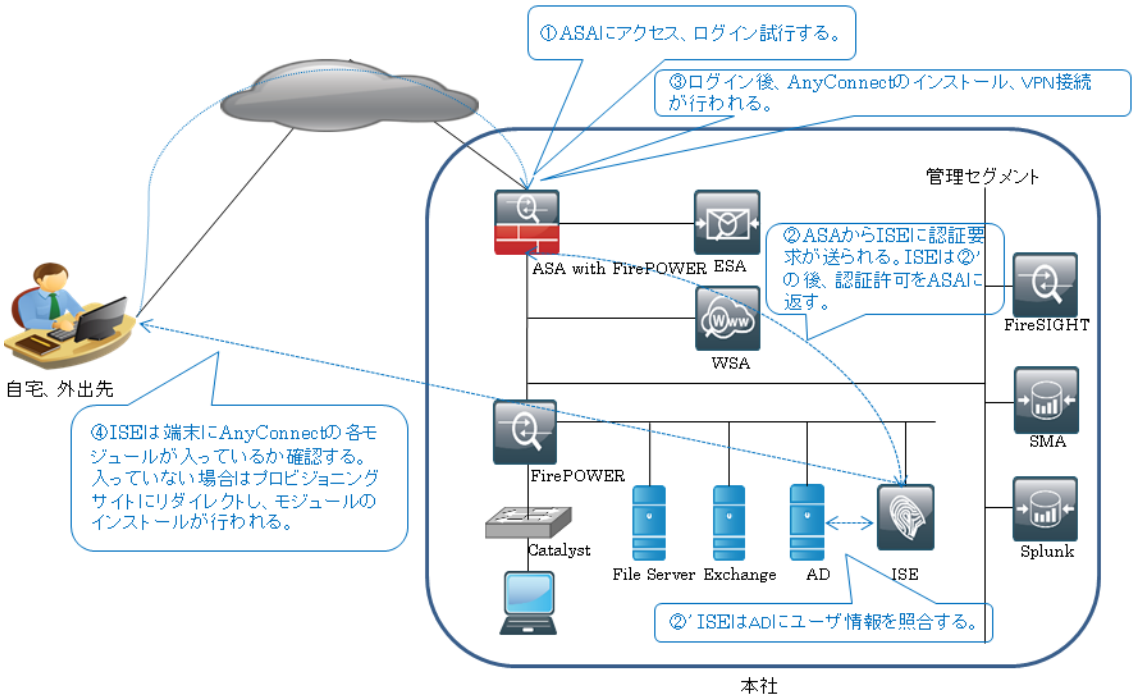


図 3. プロビジョニングの流れ

プロビジョニングは一連の流れで自動的に行われ、VPN、ネットワークアクセス制御、検疫、Web セキュリティ、マルウェア対策の各モジュールがまとめてインストールされる。利用者は各モジュールを個別にインストールする必要はなく、同時に管理者が予め設定しておいた設定ファイルが配布される。AnyConnect には VPN だけでなく、エンドポイントに必要なセキュリティ機能が統合されている。図 4 に AnyConnect Security Module の統合を示す。

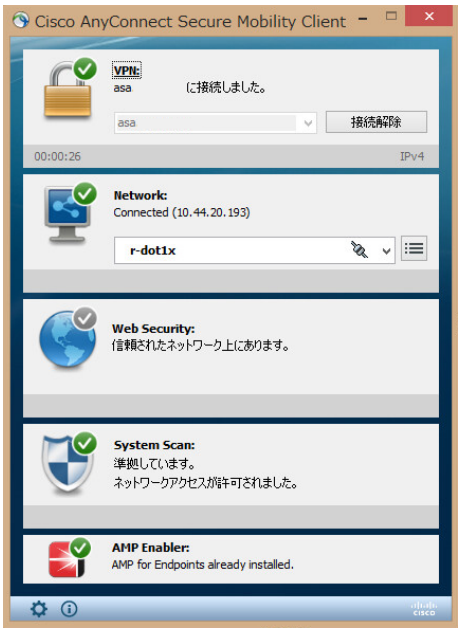


図 4. AnyConnect Security Module の統合

5.3. AnyConnect Module の働き

AnyConnect の各モジュールで、提供されるセキュリティ機能について述べる。

① VPN

VPN モジュールは SSL-VPN/IPsec-VPN をサポートする。また、グループポリシーやトンネルグループ、ダイナミックアクセスポリシーといった機能を組み合わせることで、VPN ユーザに合わせたアクセス制御を行うことが可能である。

② Network Access Manager

Network Access Manager は無線/有線ネットワークにおけるレイヤ 2 レベルのセキュリティを維持するためのソフトウェアモジュールである。主な機能には、認証に関する IEEE 標準である IEEE 802. 1X サプリカント（認証クライアント機能）、無線 LAN 通信における認証および暗号化、有線ネットワークにおけるデータの機密性と整合性を確保するための認証および暗号化である。
本モジュールの機能は 6 章の検証で IEEE 802. 1X サプリカントとして使用する。

③ Web Security

Web Security は CWS を利用するためのモジュールである。端末の Web トラフィックを CWS プロキシに透過的にリダイレクトするため、ユーザが明示的にプロキシ設定をする必要はない。AnyConnect のドライバレベルで動作するため、VPN を繋ぐことなく CWS を経由した安全な Web 通信を行うことができる。CWS は WSA と比較してローカルキャッシュ機能など、一部使用不可能な機能も存在するが、セキュリティ機能に関しては WSA とほぼ同等に機能する。

社内では WSA を利用し、WSA が利用できない外出時には CWS を利用するなど、ロケーションに応じて適切なサービスを利用するには、TND (Trusted Network Detection)機能を使用する。TND はプロファイルに指定したサーバ証明書への接続性の有無により、端末が社内ネットワークに存在するか外部ネットワークに存在するかを判定する。サーバ証明書への接続性がある場合は「信頼されたネットワーク」と判定され、Web Security モジュールは無効となり、WSA を用いた接続が行われる。サーバ証明書への接続性がない場合は、Web Security モジュールは有効となり CWS を経由した通信が行われる。また、CWS プロキシは世界中に配置されており、端末に最も近い地域の CWS プロキシが選択される。図 5 に TND によるネットワークの判定を示す。

ロケーションにより CWS と WSA を使い分けた場合は、それぞれのログを統合することが望まれる。Splunk と Cisco から提供されている Splunk の Apps である Cisco Web Security Advanced Reporting を用いることで、CWS と WSA のログや統計データを統合できる。図 6 に CWS と WSA のログ、統計データの統合を示す。

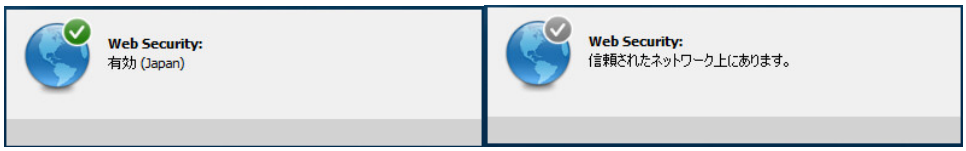


図 5. TND によるネットワークの判定

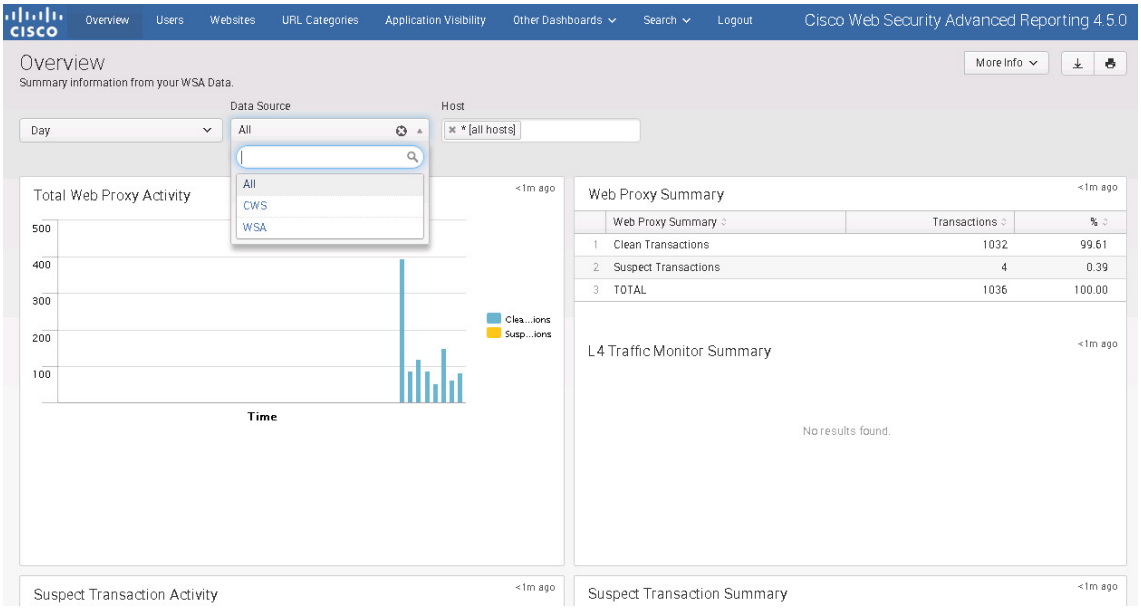


図 6. CWS と WSA のログ、統計データの統合

④ System Scan

System Scan は ISE で検疫を行うためのモジュールである。AnyConnect は ASA で検疫を行うモジュールも存在するが、ISE を用いた検疫の方がより詳細に条件設定やポリシー適用を行うことが可能である。OS やアプリケーションのパッチ適用状況、マルウェア対策ソフトウェアのバージョン、起動の有無、特定ファイルの存在有無などをトリガーにポリシー適用を行う。検疫の結果、セキュリ

ティポリシーを満たさなかった端末は接続の拒否や、検疫ネットワークへの隔離を実施することができる。検疫ネットワークではパッチの適用サイトにリダイレクトさせるなど、修復のための作業を実行させることができる。

⑤ AMP Enabler

AMP Enabler はプロファイルで指定されたダウンロードサイトから FireAMP Connector(AMP for Endpoints)を自動的にインストールする。AMP for Endpoints はマルウェア防御やレトロスペクティブ機能など、攻撃中（During)、攻撃後（After）で効果を発揮する製品である。さらに、最新のバージョンでは端末にインストールされたアプリケーションの脆弱性を取得する機能が追加された。Adobe Reader、Oracle Java、Microsoft Office、各種ブラウザのバージョン情報を取得し、そのアプリケーションが持つ脆弱性とともに管理画面から確認できる。図 7 に Cisco AMP for Endpoints による脆弱性のスキャン結果を示す。

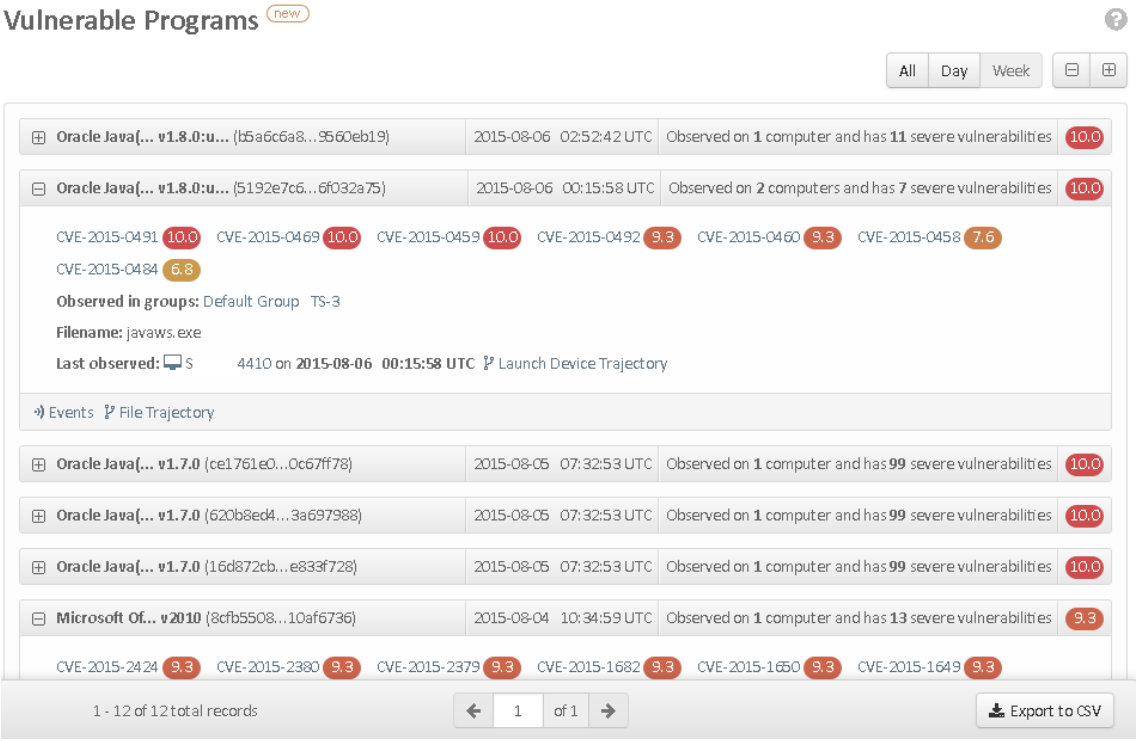


図 7. Cisco for Endpoints による脆弱性のスキャン結果

5.4. 考察

本章では、リモートアクセス端末に対して ISE、AnyConnect、ASA を用いて各モジュールのプロビジョニングを行った。今回は、リモートアクセス端末に対して検証を実施したが、無線や有線で社内 LAN に接続する際も無線 LAN コントローラや L2 スイッチと連携し同様のプロビジョニングを行うことが可能である。

一般的にこれらの機能をプロビジョニングするためには、複数のソフトウェアを個別に導入する必要がある場合や、利用者側での設定が必要である場合がみられ、設定ミスなどによる運用負荷の増大

が課題である。これに対して、本章で確認したように ISE、AnyConnect、ASA を用いることにより、自動的にプロビジョニングを行うことができるため、利用者の負担は軽減される。管理者にとっても ISE で設定を一元管理できる、利用者からの設定に関する問い合わせを削減できるなどの利点がある。

前述のように運用面の大きな利点があるが、さらに以下のような実装を期待したい。

- AMP Enabler は AMP for Endpoints 本体ではないため、今後は AMP for Endpoints の AnyConnect への完全統合が望まれる。
- AMP for Endpoints の脆弱性可視化は有用な機能であるため、FirePOWER の IPS の自動チューニングや ISE でのポリシー配信等と連携可能となれば、より柔軟なセキュリティ保護が可能であると考える。
- WSA や CWS は Splunk などのログ統合製品を使用することでログの統合が可能だが、SMA に、WSA のみならず、CWS のログに関しても統合管理可能となる機能が実装されることが望ましい。

6. 攻撃中（During）対策の検討

6.1. 入口、出口対策

攻撃中（During）対策ではマルウェアやエクスプロイトなどの攻撃を検知し、ブロックすることが求められる。社内⇔社外のセキュリティは FirePOWER や ESA、WSA の多層的な防御テクノロジーによって保護することが可能である。特に ESA、WSA はそれぞれ Email、Web のセキュリティに特化した製品であり、レピュテーション、複数のアンチウイルスエンジンによるマルウェア検知、AMP によるレトロスペクティブなマルウェア防御、L4TM による出口での C&C 通信遮断など強力な防御機能を持つ。他にも様々なテクノロジーで防御しており、入口、出口対策で多くの攻撃を阻止することが可能である。図 8 に ESA、図 9 に WSA の内部フローを示す。

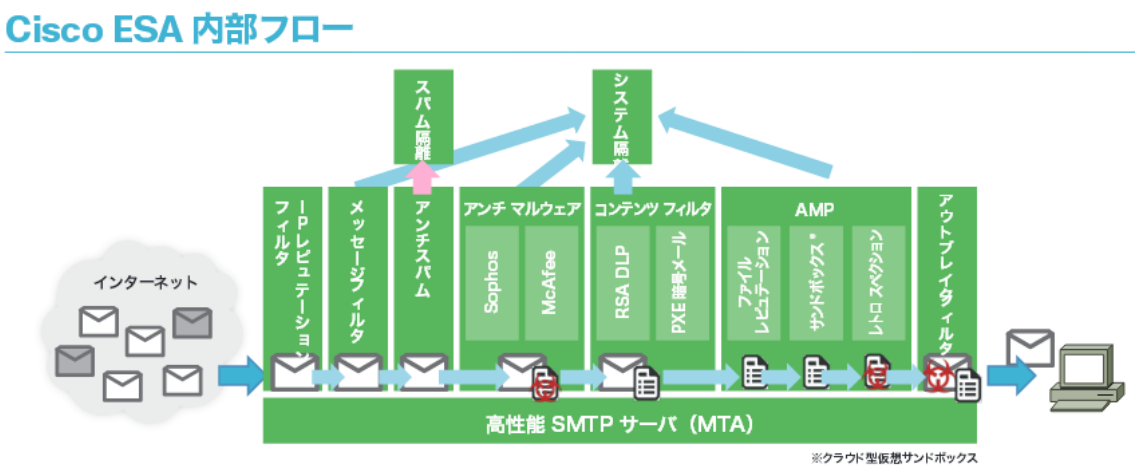


図 8. Cisco ESA 内部フロー[2]

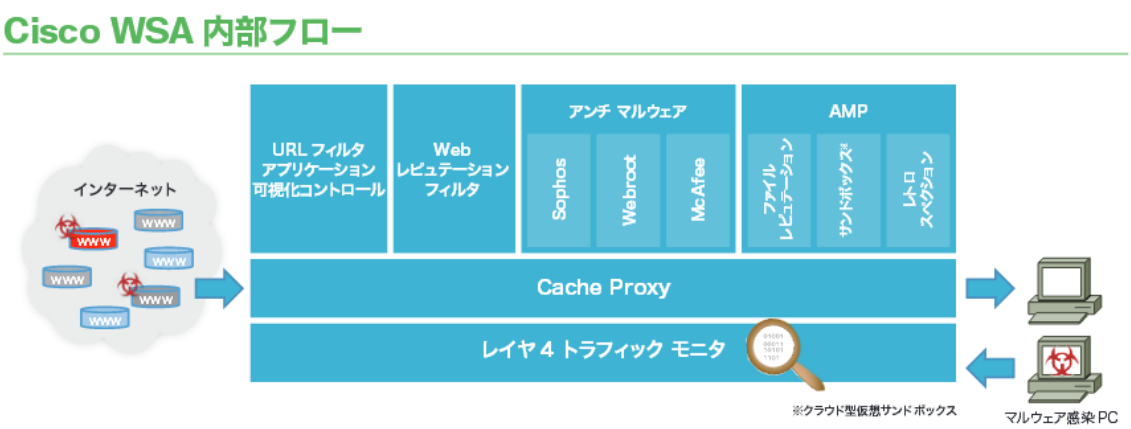


図 9. Cisco WSA 内部フロー[3]

6.2. 内部脅威の検知、ブロック、端末隔離

全ての攻撃を入口、出口で検知し、ブロックすることは困難であるため、内部に侵入した攻撃者に対しても対策を施す必要がある。攻撃者は社内に侵入するとアクセス権限のない機密情報を入手するために、管理者権限の奪取を試みる。具体的にはディレクトリサーバへの攻撃やシステムの脆弱性を突く攻撃を試行する。内部サーバは外部サーバと比べてセキュリティ設定や最新パッチの適用が疎かになっているケースが多く、攻撃者が取り得る攻撃手段も多様である。そのため、内部からの攻撃を検知した場合は更なる攻撃が行われる前に、端末を速やかに隔離する必要がある。

今回、社内の端末が未知のマルウェアに感染し、遠隔操作によって内部サーバに攻撃が行われるシーンを想定した。内部サーバに対する攻撃を検知し、ブロックすると同時に、該当端末を自動的に隔離する検証を行う。検証環境として FirePOWER、FireSIGHT、ISE、Catalyst3560 を用いる。図 10 に内部端末隔離の関連図を示す。

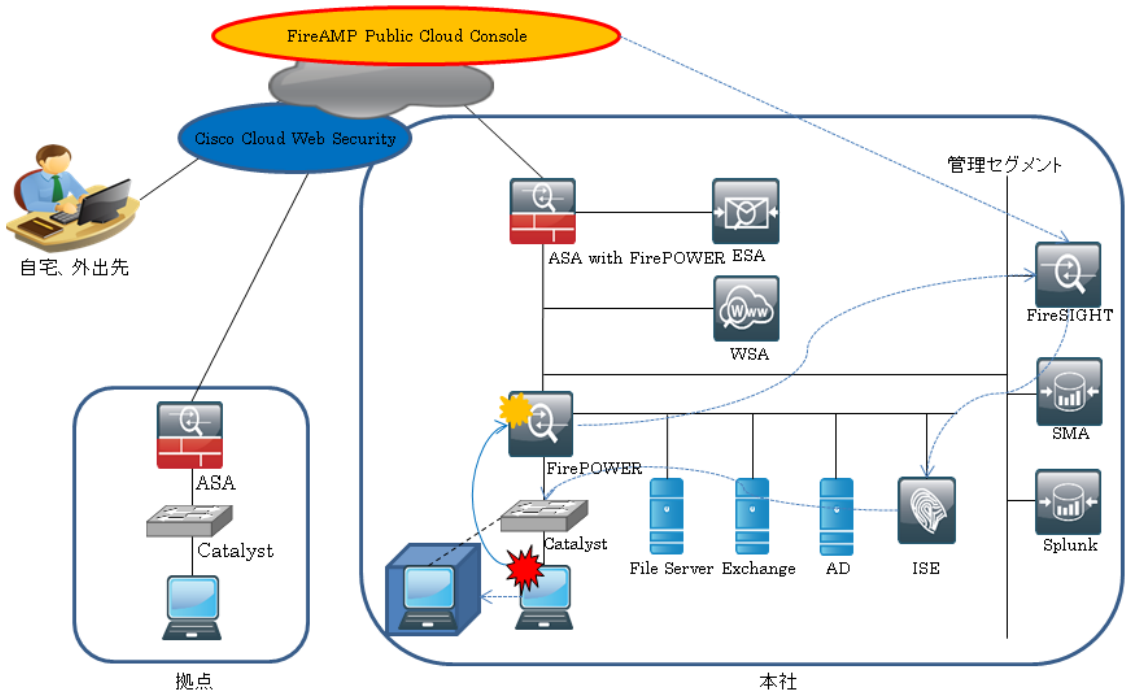


図 10. 内部端末隔離の関連図

6.3. 検知、ブロック、端末隔離の流れ

次のような流れで検証を行った。図 11 に内部端末隔離の流れを示す。

① ユーザが社内 LAN に接続する際、802. 1X 認証が行われる。ISE で認証、検疫を終えたユーザは AD ユーザのグループ属性に従って適切な VLAN に配置される。

② 社内 LAN に接続したユーザは Email 経由で未知のマルウェアが添付されたメールを受信する。添付ファイルはパスワードにより暗号化されているため、ESA によるマルウェアのスキャンは回避される。メールを開封したユーザは、添付ファイルをパスワードで解凍し、実行することによりマルウェアに感染する。マルウェアは端末に遠隔操作ツールをダウンロードし、実行する。C &C サーバは国内の実在企業の正規サイトが乗っ取られて利用されており、レピュテーションでは検知できなかった。結果、攻撃者により端末は遠隔操作されることになる。

③ 攻撃者はドメインの管理者権限を奪取するため、遠隔操作端末から AD サーバに『CVE-2014-6324』を用いた攻撃を実施する。[4]

④ AD サーバ宛てに攻撃が行われると、経路上の FirePOWER は攻撃を検知しブロックする。同時に FireSIGHT は ISE に対して攻撃を行った端末を隔離するよう指示を出す。

⑤ ISE は既に認証済みの端末のアクセスポリシーを変更するために CoA（Change of Authorization）を Catalyst に送信する。Catalyst は端末に再認証を要求する。

⑥ 端末は再認証要求に応答し、再認証が行われる。

⑦ Catalyst は攻撃端末を隔離 VLAN に配置するように自身の設定を動的に変更する。端末の安全性が確認された場合は、ISE から隔離解除を実行することで元の VLAN に戻すことができる。

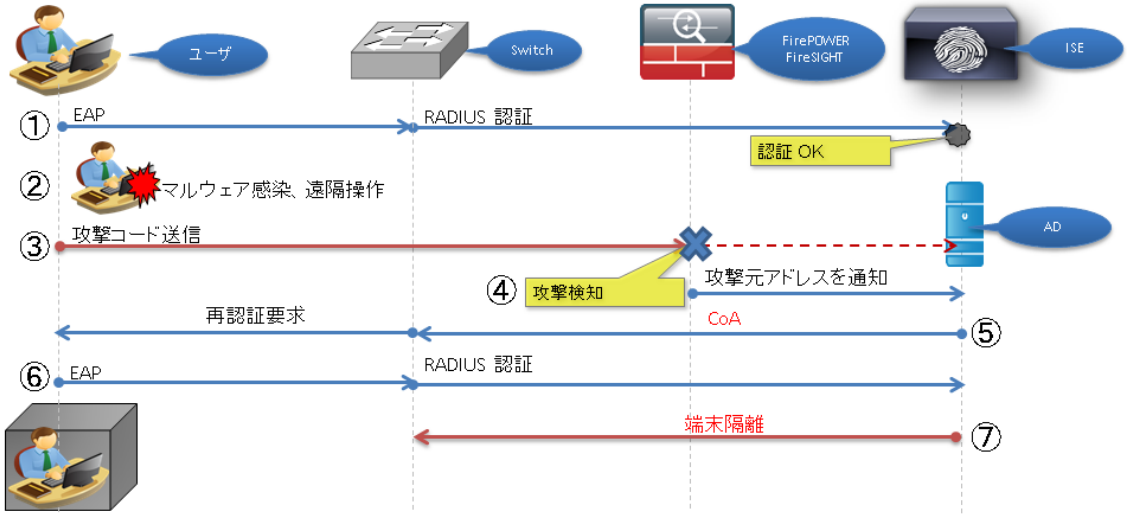


図 11. 内部端末隔離の流れ

6.4. コリレーションルール設定

FireSIGHT から ISE への指示は、ISE Remediation モジュールを FireSIGHT に導入し、コリレーションルールと合わせて使用することで可能となる。コリレーションルールは送信元、送信先、イベント内容といった詳細な条件を指定することが可能である。図 12 にコリレーションルールの設定を示す。

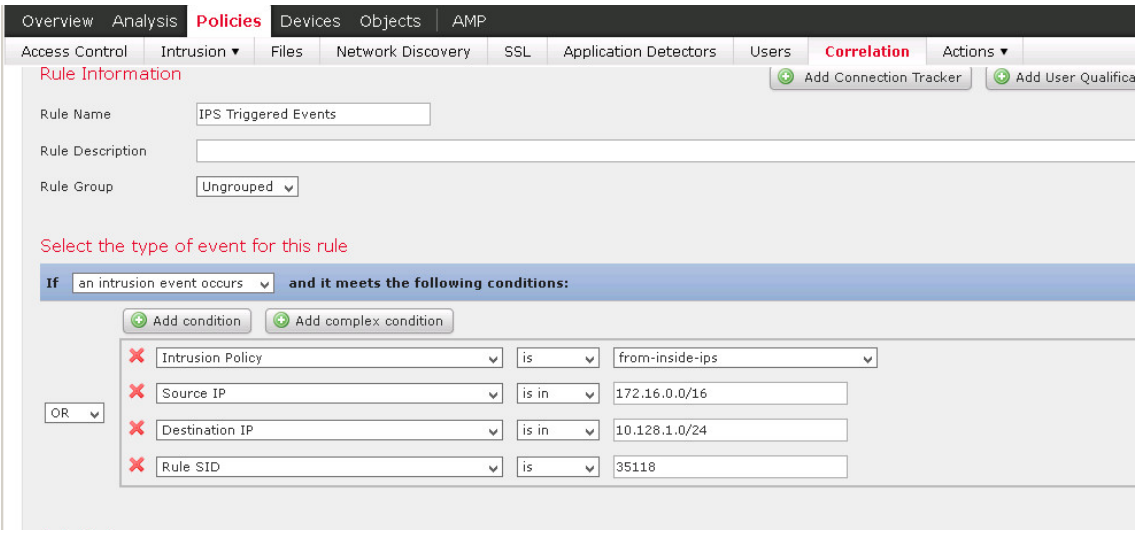


図 12. コリレーションルールの設定

IPS や端末隔離は誤検知や実際の運用上の負荷が気になるところだが、自動チューニングの機能やコリレーションルールの詳細な条件指定を用いることで現実に沿った運用が可能である。

FireSIGHT の自動チューニング機能は、FireSIGHT は監視するトラフィックから、ホストや OS

が利用するアプリケーションを学習し、適切な IPS ルールを自動的に適用する機能である。また、コリレーションルールは IPS ルールだけではなく、様々な条件を指定し、対応するアクションを設定することが可能である。例えば、AMP for Endpoints と FireSIGHT を連携させることにより、エンドポイントで発見したマルウェアをトリガーに端末を隔離させることも可能である。マルウェアの状態に対する条件指定も柔軟に行えるため、なんらかの理由でマルウェアを直接、隔離できなかった場合のみ端末そのものを隔離することができる。したがって、実運用を考慮した設計となっている。

6.5. 考察

本章では、攻撃端末の検知、ブロック、隔離までの動作を検証した。本検証では Catalyst と ISE を連携させたが、無線 LAN コントローラと ISE を連携することで無線端末に対しても同様に隔離することが可能である。脅威は発生源に最も近い場所で封じ込めるべきあり、端末が最初にアクセスする L2 レベルで隔離するのは最適な対処法と考える。

検証を進める中で改善が望まれる点も確認された。以下の実装を期待したい。

- AMP for Endpoints から FireSIGHT に送信されるファイル検知時の情報には、端末の IP アドレス情報が含まれない。DHCP 環境など頻繁に IP アドレスが変動する環境下では、正確な IP アドレス情報を基に端末隔離が行えないため、IP アドレス情報を含む形での実装が望まれる。

7. 攻撃後（After）対策の検討

7.1. AMP によるレトロスペクティブセキュリティ

攻撃後（After）対策では Cisco AMP のレトロスペクティブ機能が有効である。レトロスペクティブ機能にはクラウドリコールとトラジェクトリがある。また、Cisco AMP は FirePOWER で実行される AMP for Networks や WSA、ESA 等のコンテンツセキュリティで実行される AMP for Content Security、Windows や Mac、Android 等エンドポイントにインストールする AMP for Endpoints が存在し、様々な環境で用いることが可能である。これらの違いや効果的に使用する方法を検討する。図 13 に Cisco AMP の検知ポイントを示す。

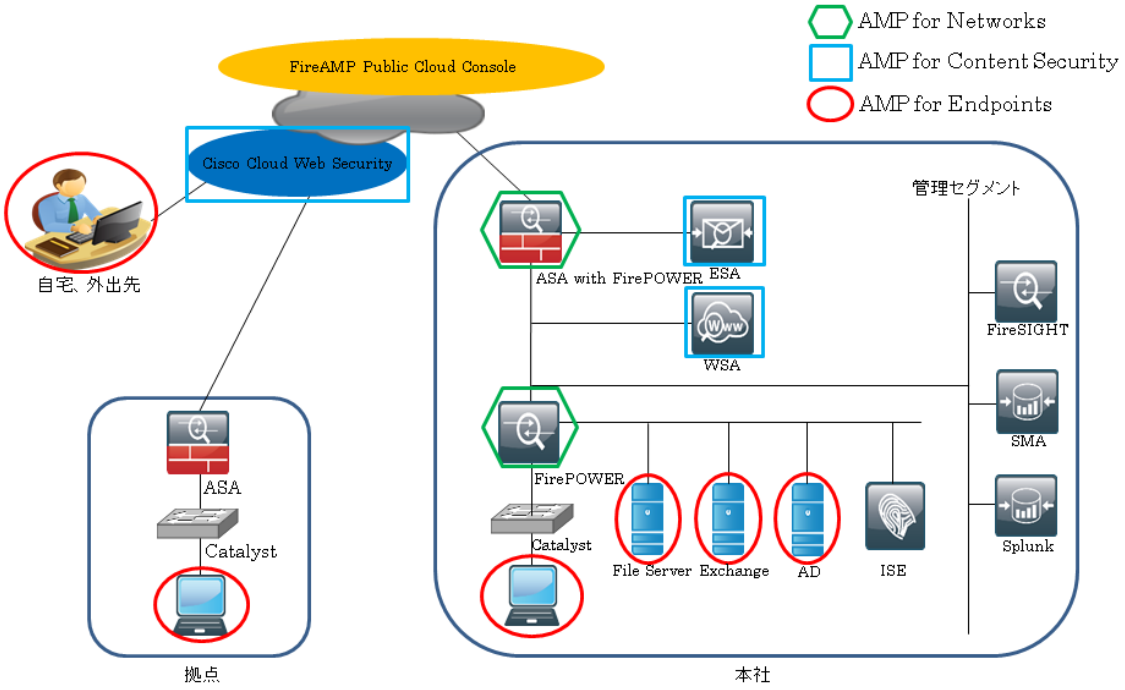


図 13. Cisco AMP の検知ポイント

7.2. マルウェア検査の仕組み

AMP for Networks は対応するプロトコル上で、FirePOWER を通過したファイルのマルウェア検知、ブロックを行う。ファイルの SHA-256 ハッシュがクラウド上のデータベースに送信され、ハッシュ値の照合が行われる。その結果、ファイルは Clean、Malware、Unknown の 3 種類に分類される。Clean は信頼できるベンダーのファイル、Malware はマルウェアファイル、Unknown は不明なファイルを意味する。Malware と判定されたものはその場でブロックされるが、Unknown となったファイルの内、実行形式のものは動的にサンドボックス上で検査される。AMP for Content Security も AMP for Networks と同様に Web や Email に特化した形で提供される。

Cisco AMP for Endpoints はエンドポイント端末上でのファイル I/O をトリガーにマルウェアを検査する。ファイル I/O が発生すると、ファイルの SHA-256 ハッシュをクラウド上のデータベースに送信し、Malware と判定されたものはその場で隔離される。

AMP for Endpoints の特徴的な機能として Prevalence と呼ばれる機能が存在する。Prevalence は組織内の端末上に存在する実行形式ファイルの中で、数が少ないファイルを検知する。OS のシステムファイルや一般的によく利用されるアプリケーションに対し、極端に数が少ない実行形式ファイルはマルウェアの疑いがある。これらのファイルを動的にサンドボックスに送信し、分析することでマルウェアの早期発見、駆除を実現する。

さらに、単純な 1 対 1 のハッシュチェック以外にも ETHOS や SPERO といった亜種のマルウェアを発見するエンジンを持つ。また、TETRA や ClamAV といったパターンファイルを利用する従来型のウイルス対策も可能である。

7.3. クラウドリコール

以下のイベントが発生した場合に、端末上で Unknown と判定されていたファイルはマルウェアとして自動的に隔離される。

① サンドボックス分析によりマルウェアと判定

② Cisco のクラウド上での継続的な調査情報が反映

③ サードパーティからの情報伝達

ファイルの I/O が発生した際に、端末内のファイル位置情報を記録しているため、再度、検索を行うことなく瞬時に隔離することが可能である。本検証では、過去に実行した際は Unknown と判定されたファイルがクラウドリコールにより Malware と判定され自動的に隔離される挙動を確認した。8 月 9 日時点では未知のファイルだった nc-2.exe が、8 月 17 日にはマルウェアと識別されて隔離されている。図 14 にクラウドリコールの流れを示す。

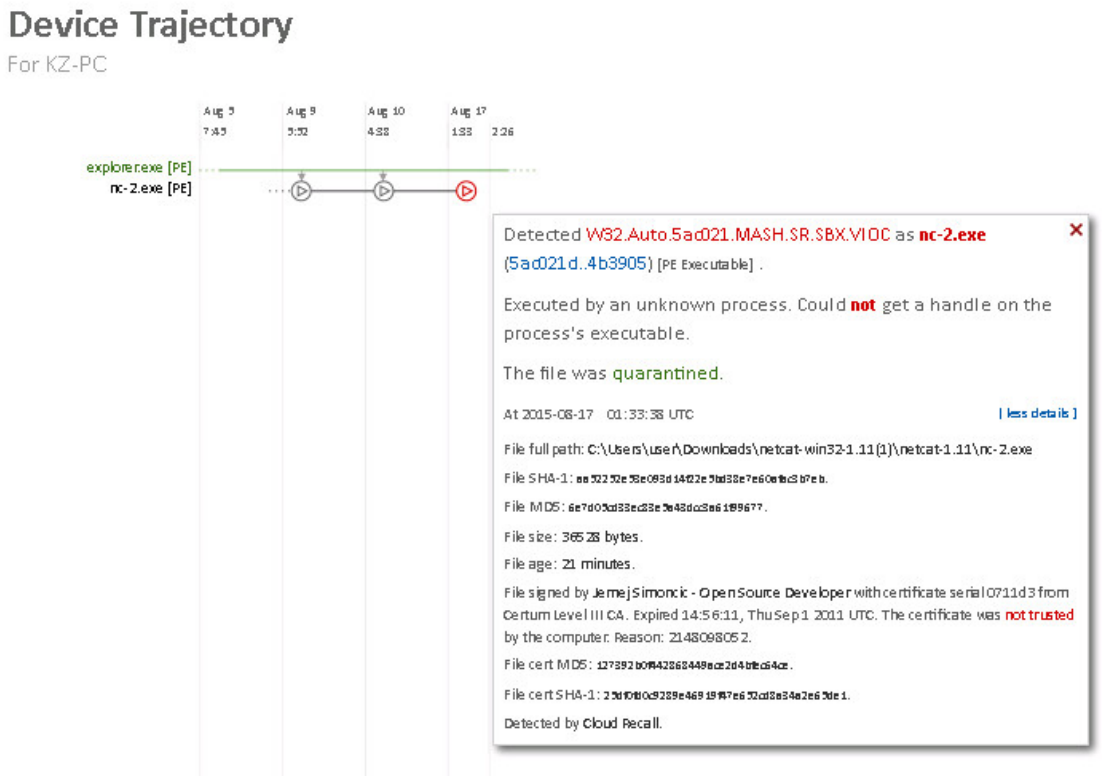


図 14. クラウドリコールの流れ

7.4. トラジェクトリ

トラジェクトリ機能はデバイス内のマルウェアの動作を記録するデバイストラジェクトリ、組織内でのマルウェアの拡散状況を記録するファイルトラジェクトリ、ネットワーク上のマルウェアの感染経路を記録するネットワークファイルトラジェクトリが存在する。

デバイストラジェクトリ、ファイルトラジェクトリは Cisco AMP for Endpoints で、ネットワークファイルトラジェクトリは FireSIGHT で確認することが可能である。また、Cisco AMP for

Endpoints と FireSIGHT を連携させることで、Cisco AMP for Endpoints で検知したマルウェア情報を FireSIGHT に通知することが可能である。図 15 にデバイストラジェクトリ画面の説明を示す。

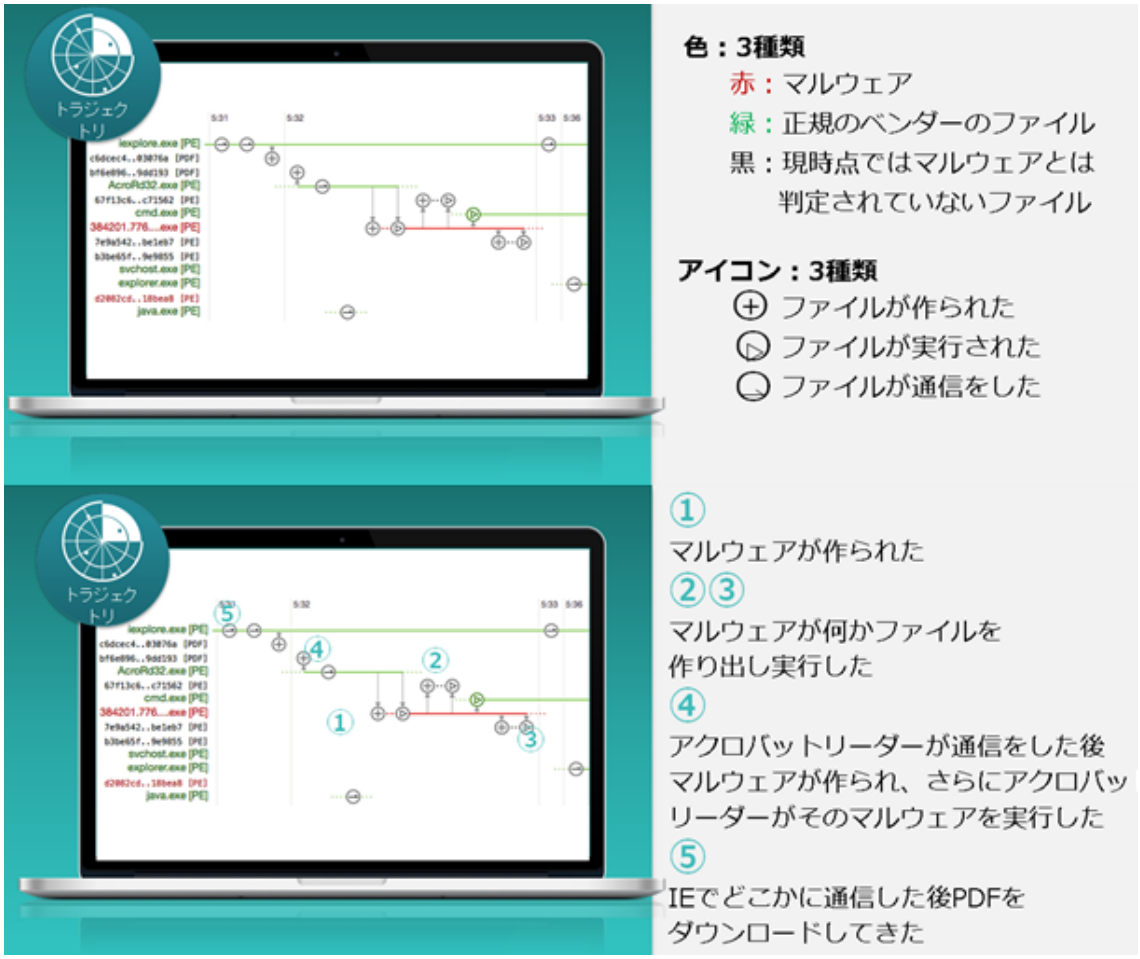


図 15. デバイストラジェクトリ画面の説明[4]より

7.5. トラジェクトリを用いたフォレンジック

本検証では、Kali Linux の Metasploit を利用して、端末のマルウェア感染、C&C サーバ接続、ファイル流出に至る動きをシミュレーションし、その動作をトラジェクトリで確認した。図 16 にトラジェクトリの検証に用いた構成図、表 2 に検証端末情報を示す。

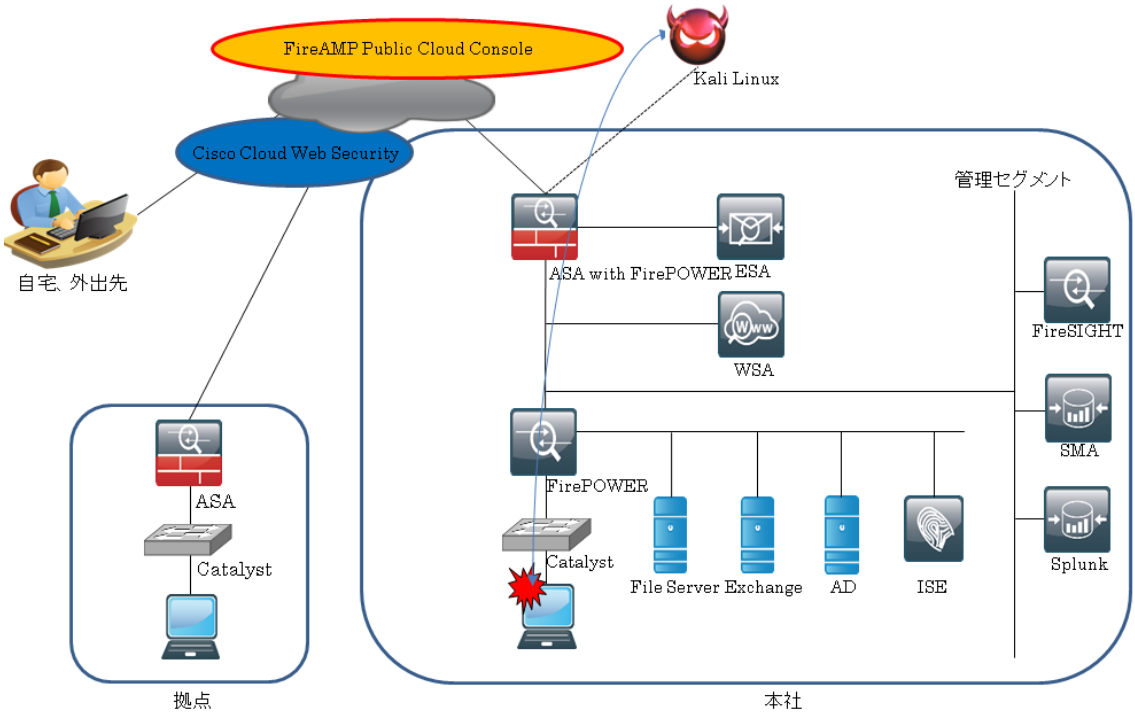


図 16. トラジェクトリ検証環境構成図

表 2. トラジェクトリ検証端末情報一覧

OS	host name	IP address	役割
Windows Server 2012 R2	r-ad.secna.local	192.168.24.200	被害者端末
Windows 8.1 Pro 64bit	r-client002.secna.local	10.128.1.10	ファイルサーバ
Kali Linux 1.0.6	kali	172.40.1.111	偽 Web サイト C&C サーバ

トラジェクトリのシミュレーションに用いる攻撃の手順を以下に示す。

① Kali Linux は正規の Web サイトをクローンし、マルウェアを仕込んだ偽の Web サイトを作成する。

② 被害者はメールや SNS により偽の Web サイトに誘導される。

③ 被害者が偽の Web サイトにアクセスすると Java アプレットが起動し、実行を促すメッセージが表示される。

④ 被害者が Java アプレットを実行することで、トロイの木馬型マルウェアに感染し、バックドアが形成され C&C サーバに接続される。

⑤ 攻撃者は被害者端末を遠隔操作し、顧客情報を収集して C&C サーバにアップロードを行う。

被害者端末が偽の Web サイトに誘導された後の動作を、トラジェクトリにより確認した結果を示す。

① 図 17, 18 にデバイストラジェクトリの実行結果を示す。図 17 から jp2launcher.exe(Java アプレット)が 172.40.1.111(偽 Web サイト)と通信を開始していることが分かる。jp2launcher.exe は 7516b104-6d179920 を作成し、実行している。また、7516b104-6d179920 は 172.40.1.111 と TCP443 ポートで通信を開始している。

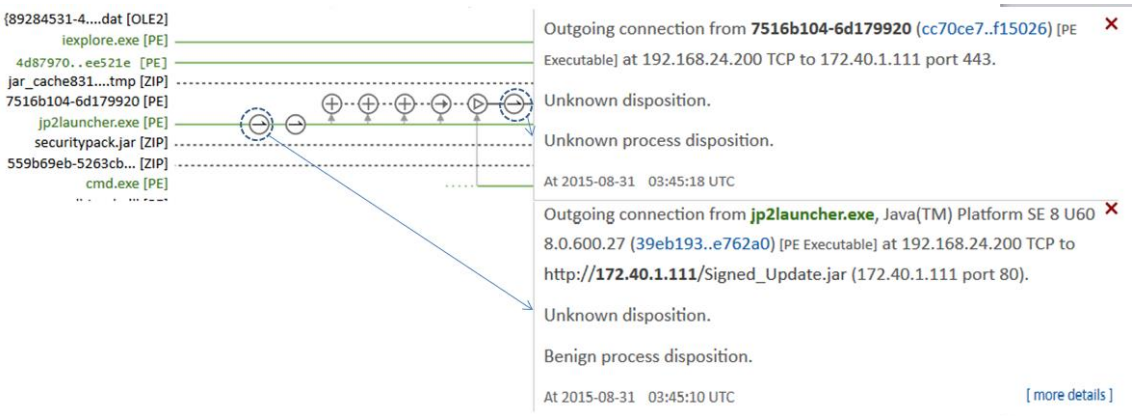


図 17. デバイストラジェクトリ_1

② 図 18 から 7516b104-6d179920 が vhlaryqi.exe、ianydypm.exe、velvdfhsj.exe を作成していることが分かる。また、作成された実行形式ファイルが実行されていることが確認される。

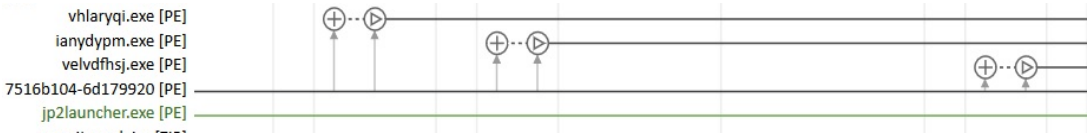
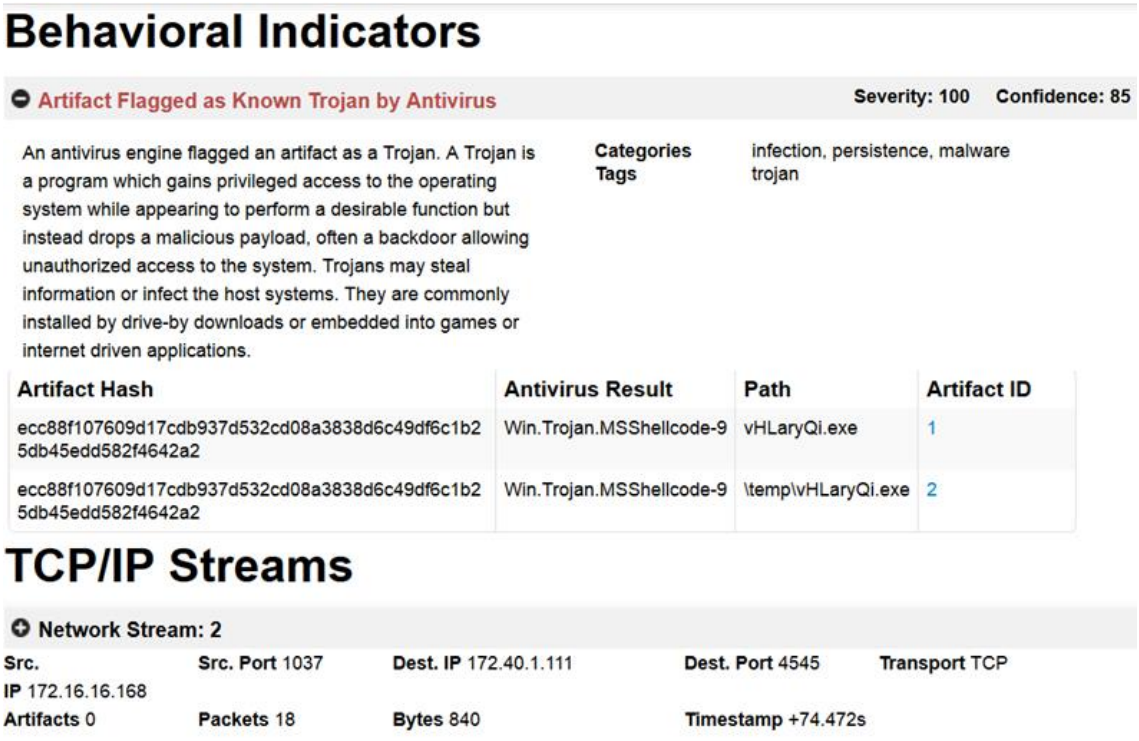


図 18. デバイストラジェクトリ_2

図 19 に Prevalence によるファイルの調査を示す。これらのファイルは Prevalence によって自動的にサンドボックスに送信される。

図 19. Prevalence によるファイルの調査

図 20 に vhlaryqi.exe のサンドボックス解析結果を示す。図 20 よりサンドボックスによる解析の結果、トロイの木馬でバックドアを形成するタイプのマルウェアであることが分かる。



Behavioral Indicators

Artifact Flagged as Known Trojan by Antivirus　Severity: 100　Confidence: 85

An antivirus engine flagged an artifact as a Trojan. A Trojan is a program which gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload, often a backdoor allowing unauthorized access to the system. Trojans may steal information or infect the host systems. They are commonly installed by drive-by downloads or embedded into games or internet driven applications.

Categories infection, persistence, malware
Tags trojan

Artifact Hash	Antivirus Result	Path	Artifact ID
ecc88f107609d17cdb937d532cd08a3838d6c49df6c1b25db45edd582f4642a2	Win.Trojan.MSShellcode-9	vHLaryQi.exe	1
ecc88f107609d17cdb937d532cd08a3838d6c49df6c1b25db45edd582f4642a2	Win.Trojan.MSShellcode-9	\temp\vHLaryQi.exe	2

TCP/IP Streams

Network Stream: 2

Src. IP 172.16.16.168　Src. Port 1037　Dest. IP 172.40.1.111　Dest. Port 4545　Transport TCP
Artifacts 0　Packets 18　Bytes 840　Timestamp +74.472s

図 20.　vhlaryqi.exe のサンドボックス解析結果

③　図 21、22 にトラジェクトリの実行結果を示す。図 21 から vhlaryqi.exe が実行されたタイミングで taskhost.exe が 172.40.1.111(C&C サーバ)と TCP4545 ポートで通信が開始され、C&C サーバによってリモートコントロールされていることが分かる。

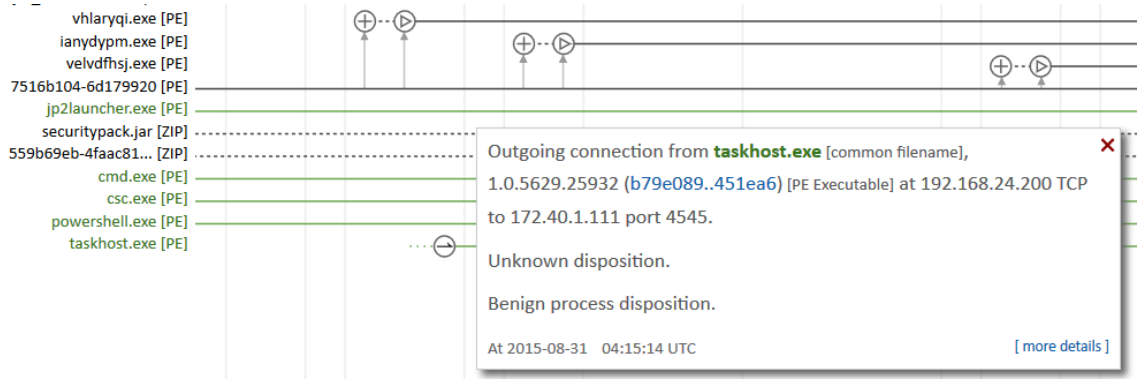


図 21.　デバイストラジェクトリ_3

④　図 22 からリモートコントロール中に、customers_info.zip が作成されていることが分かる。

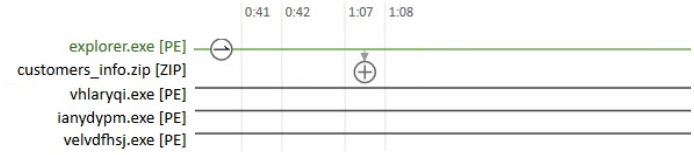


図 22.　デバイストラジェクトリ_4

⑤ 図 23 にファイルトラジェクトリの実行結果を示す。図 23 からファイルトラジェクトリのハッシュ照合によって、同時間帯にファイルサーバから端末にコピーされた顧客情報であることが判明される。ファイルトラジェクトリの結果により、攻撃者によって外部に顧客情報が持ち出されたことが推測される。

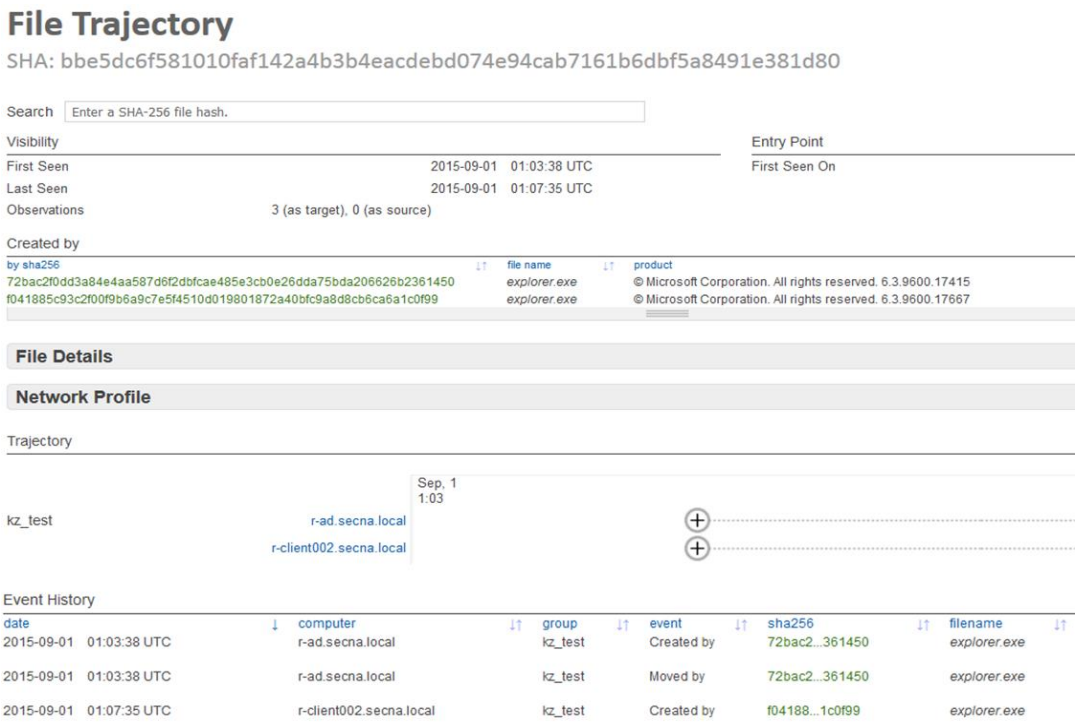


図 23. ファイルトラジェクトリ

⑥ 図 24 にネットワークファイルトラジェクトリの実行結果を示す。図 24 からネットワークファイルトラジェクトリによって、ネットワーク視点でも被害者端末と C&C サーバ間で複数回、通信が発生していたことが確認できる。

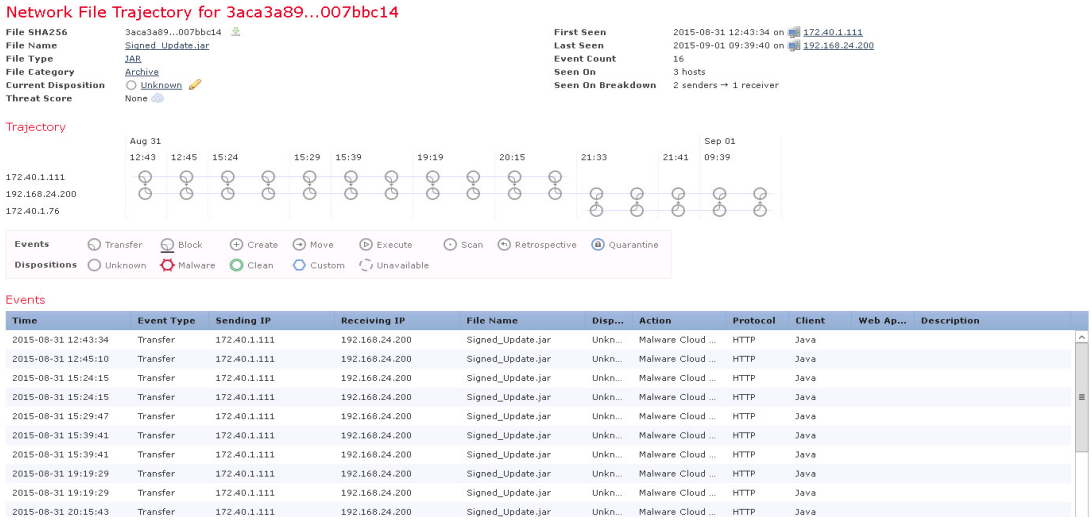


図 24. ネットワークファイルトラジェクトリ

⑦ 図 25 にデバイストラジェクトリの実行結果を示す。図 25 からマルウェアはクラウドリコールによって削除されたことが確認できる。

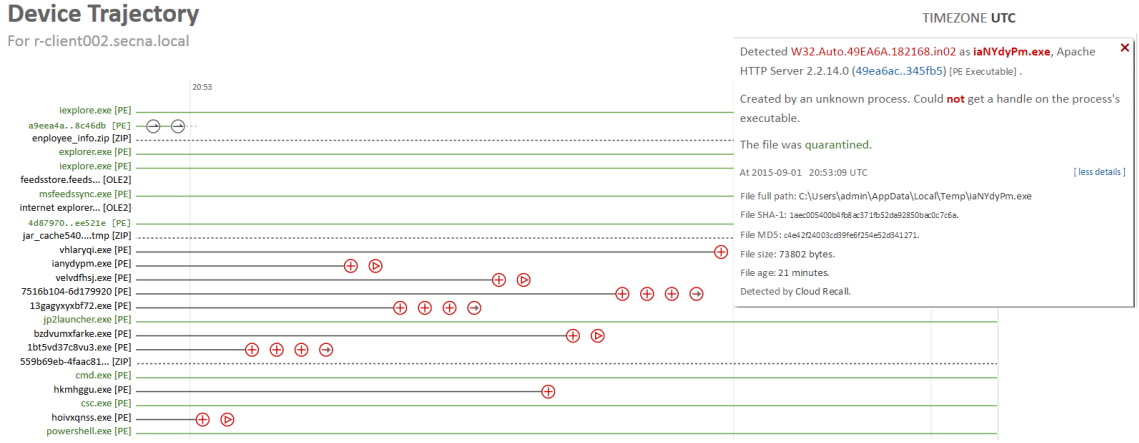


図 25. デバイストラジェクトリ_5

7.6. 考察

実際の運用を想定した場合、マルウェアが侵入していたことに気付いた際に、その都度すべての端末でフルスキャンを行うのは困難である。全ファイルの検索には数時間を要するため、その間は端末のパフォーマンスに影響を及ぼす。未知のマルウェアが発見される頻度は年々増加しているため、環境によってはフルスキャンが終了する直前に、再度スキャンが必要といった状況に陥ることが考えられる。その点、クラウドリコールは過去の I/O 情報から瞬時に端末内のマルウェアを隔離するため、管理者の運用負荷低減、利用者の利便性向上、脅威への対応時間短縮などの利点がある。脅威に素早く対応することで情報流出に至る前に対処できる可能性も高くなる。AMP for Networks と AMP for Endpoints を併用することで、FirePOWER のサンドボックス解析中にすり抜けたファイルをエンドポイントで迅速に隔離できるのも利点である。

トラジェクトリでは 3 つのトラジェクトリ機能を使い分けることでマルウェアの 4W1H を確認し、情報流出に至る動きを詳細に確認した。特にデバイストラジェクトリは端末上のファイルの I/O 動作をすべて記録するため、マルウェアが関連ファイルを作成する動きや通信先 IP、ポート、周辺ファイルの動作まで把握することが可能であった。これらを効果的に用いることで簡易的なフォレンジックツールとしても役立つと考える。

管理面に目を移すと AMP for Endpoints のプライベートクラウドコンソールでは、デフォルトで Google 認証システムを利用した 2 ステップ認証が備えられており、認証時のセキュリティも考慮された設計となっている。また、顧客によってはサンドボックスをプライベート環境に設置することが求められる場合もある。その場合は、AMP for Endpoints のプライベートクラウド版が用意されており、顧客の環境に合わせた導入が可能であるが、現時点ではプライベートクラウド版を使用した場合、サンドボックスが使用できない。よって、プライベートクラウド版のサンドボックスとの連携実装を期待したい。

8. まとめ

本論文では実際の利用シーンを想定した検証を実施することで、攻撃前（Before）、攻撃中（During）、攻撃後（After）を包括的に保護する脅威中心型セキュリティモデルの有効性を実証した。さらに、各製品を連携させることでリモートアクセス端末のプロビジョニング、攻撃端末の隔離、未知のマルウェアへの対策を自動化できることを確認した。これらの機能を自動化することで、運用管理者の負担軽減、ヒューマンエラーの防止、脅威の早期封じ込めによる情報流出の阻止が期待できる。

今後のサイバー攻撃はより一層、攻撃エリアを拡大し、攻撃手法も巧妙化していくことが予想される。これらの攻撃に対して、個々の製品でのポイント防御では、防御面でも運用面でも対応するのは困難である。したがって、次世代のサイバーセキュリティでは、システム全体を連携させて防御、修復、堅牢化までを自動的に行う必要があると考える。Cisco はネットワーク、認証、Web、メール、クラウド、エンドポイントに優れたセキュリティ製品を有しており、スイッチやルータ、無線 LAN コントローラ、サーバにも高いシェアを持つ。これらは他社にない強みである。本論文内で述べた改善点の実装とともに、より一層の機能連携に期待する。

9. 参考文献

［1］【Interop Tokyo 2014】Ciscoの新しいセキュリティ モデル
http://gblogs.cisco.com/jp/2014/06/interop-tokyo-2014-threat-centric-security/#more-3604

［2］Cisco E メールセキュリティアプライアンス　カタログ
http://www.cisco.com/web/JP/product/hs/security/prodlit/pdf/1026_Cisco_ESA_Catalog.pdf

［3］Cisco WEB セキュリティ アプライアンス　カタログ
http://www.cisco.com/web/JP/product/hs/security/prodlit/pdf/1027_Cisco_WSA_Catalog.pdf

［4］CVE-2014-6324
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6324

［5］2015 年 7 月 17 日 CiscoSystems CTU 資料 Security SEVT Redelivery AMP Everywhere