ケーススタディ：AKAMAI IT

ENTERPRISE THREAT PROTECTOR を AKAMAI が使用する理由

目次

エグゼクティブサマリー

2017 年 3 月、Akamai IT は、Akamai の有線および無線の企業ネットワークに Enterprise Threat Protector を導入しました。

3 月から 5 月の期間に、Enterprise Threat Protector によってもたらされたメリットは非常に大きく、かつ定量化可能です。

たとえば、次のようなメリットがもたらされました。

- 既存のエンドポイント防御ソリューションにより特定されたマルウェアインシデント件数が大幅に減少 — 3 月から 4 月までの期間で **54% 減少**、3 月から 5 月までの期間で **37% 減少**。
- 既存の高度な検出ソリューションにより生成されたイベント件数が減少 — 3 月から 4 月までの期間で **30% 減少**、3 月から 5 月までの期間で **15% 減少**。
- 既存のエンドポイント防御と高度な検出ソリューションにより検出されたインシデント件数とアラート件数の減少に伴い、**0.75 人のフルタイム従業員（FTE）**相当の時間を節約。

エンドポイント防御

Akamai が導入したエンドポイント防御ソリューションには、マルウェア検出機能や侵入防止機能が装備されています。

マルウェア感染インシデント

マルウェア評価基準をフィルタリングして、「アドウェア」と「潜在的に不必要なソフトウェア」のアラートを除外し、マルウェア感染に焦点を絞りました。Enterprise Threat Protector を導入した結果、特定されたマルウェア感染インシデント件数は 3 月（199）から 4 月（92）の期間で 54% 減少し、3 月から 5 月（125）の期間で 37% 減少しました。

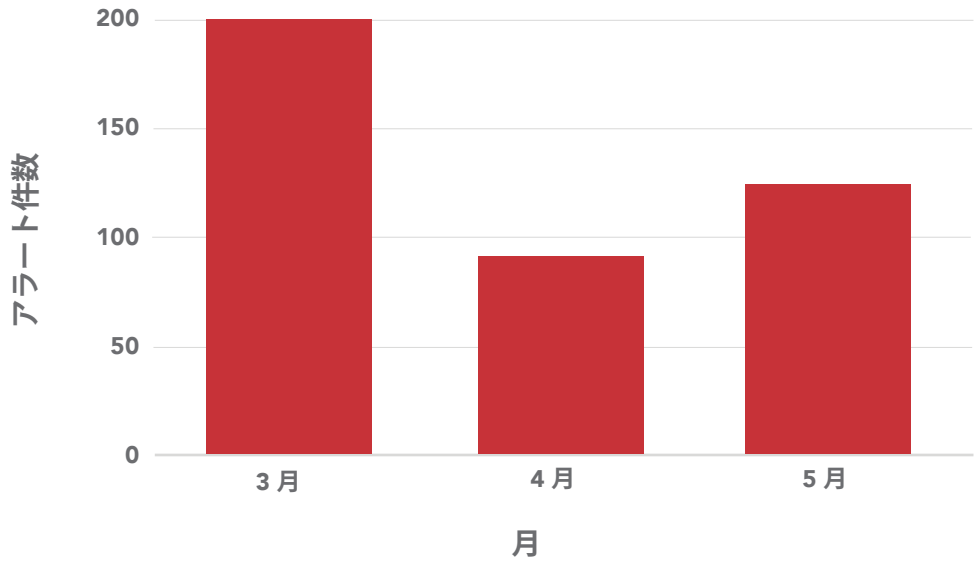

図 1 – Enterprise Threat Protector の導入によるマルウェアインシデント数の減少

侵入防止システム（IPS）のアラート

エンドポイント IPS によるアラート件数にも同様の減少が見られます。発生したアラートの大多数は Torrent 形式によるものでしたが、3 月から 4 月の期間、さらに 5 月までの期間で目に見えて減少しています。

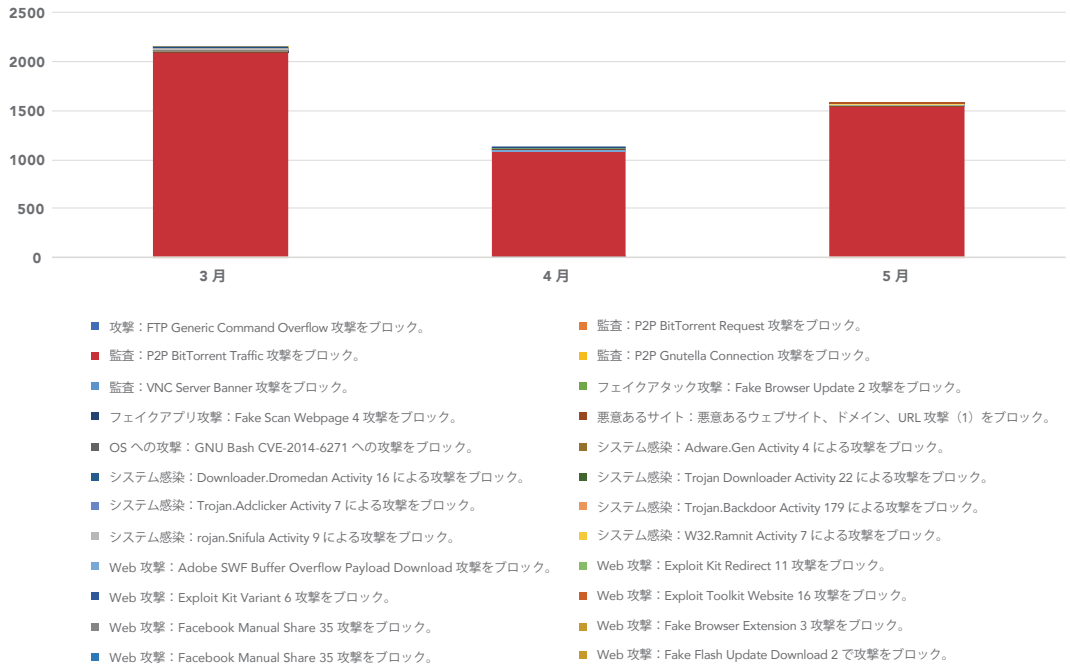

図 2 – Enterprise Threat Protector の導入による IPS アラートの減少（Torrent を含む）

アラートから Torrent を完全に除外した場合でも、3 月から 4 月までの期間で大きな減少（27%）が認められ、3 月から 5 月の期間では、およそ 35% 減少しています。

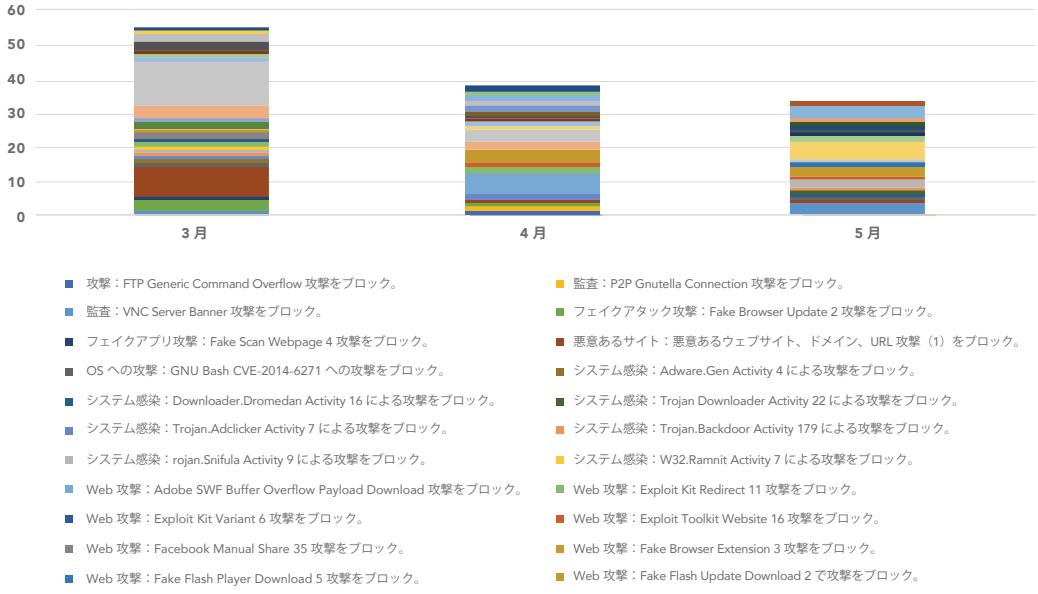

図 3 – Enterprise Threat Protector の導入による IPS アラートの減少（Torrent を除く）

Torrent を除外すると、IPS でのアラート件数が最も多いのは、悪意あるウェブサイト、ドメイン、URL に関するものです。ウェブ攻撃と偽のスキャン・ウェブ・ページによる攻撃が僅差で続きます。

アラート	3 月のアラート件数	4 月のアラート件数	5 月のアラート件数
悪意あるウェブサイト、ドメイン、URL	13	1	1
Web 攻撃と Fake Scan Web Page 攻撃	12	4	1

表 1 – Enterprise Threat Protector の導入による IPS アラートの減少

高度な検出

Akamai の導入した高度な検出ソリューションは、セキュリティの追加レイヤーとなる補完的な防御メカニズムです。このソリューションにより検出されるアラートは、件数こそ少ないものの、はるかに重大な脅威をもたらします。

図 4 に示されているように、このソリューションにより検出されるアラート件数も、Enterprise Threat Protector の導入後は減少しています。

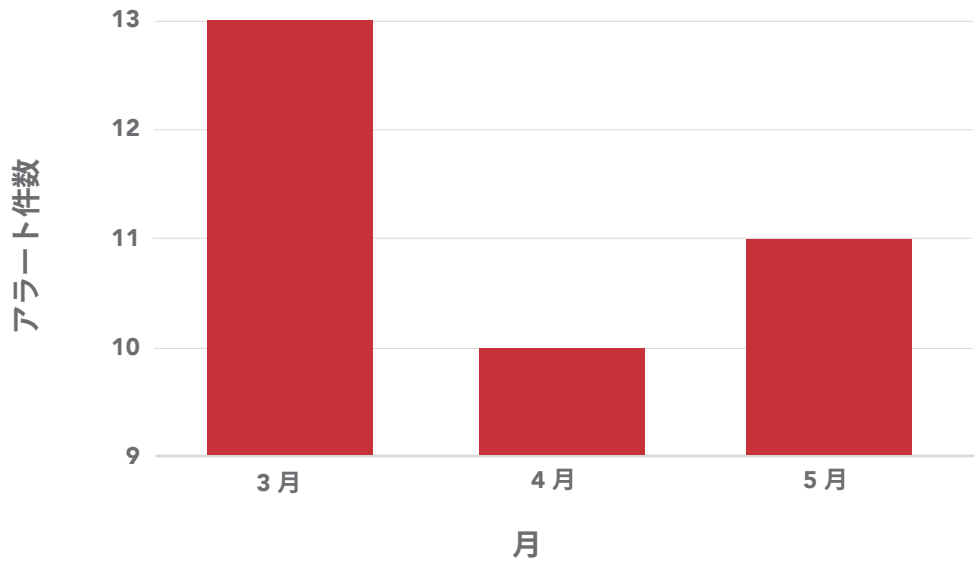

図 4 – Enterprise Threat Protector の導入による高度な検出アラートの減少

ROI

Enterprise Threat Protector の導入によりインシデント件数とアラート件数が減少したのは明らかですが、その真の価値は時間の節約にあると考えられます。

「節約された時間」は、マルウェアインシデントに対する推定平均応答時間と修復時間、Torrent ソフトウェアの除去時間を使用して計算されました。これらのアクティビティーは、いずれも毎月の標準的な運用タスクです。Torrent 件数にも減少が見られることに注意してください。

月	ユーザー数	ブロックされた Torrent IP 数
3 月	56	2,089
4 月	48	1,100
5 月	40	1,546

表 2 – IPS モジュールのアラート件数

マルウェアの調査では、調査、応答、修復にかかった時間をインシデント当たりで算出し、使用しています。

これらの基準を使用した場合、Enterprise Threat Protector の導入によって節約された時間は、1 か月当たりおよそ **0.75 人のフルタイム従業員**（FTE）相当でした。

エンドポイント保護のマルウェア検出モジュールと IPS モジュールを合わせて、4 月から 6 月までの平均応答時間を計算し、3 月の Enterprise Threat Protector 導入前と比較しました。

結果は次のとおりでした。

- **マルウェア検出モジュール**における推定節約時間は、**27 時間**。
- **IPS モジュール**のインシデント応答における推定節約時間は、**8 時間**。

節約された応答時間（単位：時間）	
マルウェアモジュール	27
IPS モジュール	8
合計	**35**

表 3 – マルウェアモジュールと IPS モジュールのアラート（Enterprise Threat Protector の導入による応答時間の節約）

同様に、初期応答時におけるインシデント当たりの平均修復時間を計算に入れると、エンドポイントのマルウェアモジュールでは推定で **51 時間**、IPS モジュールでは **24 時間**の分析時間／月が節約されました。

節約された修復時間（単位：時間）	
マルウェアモジュール	51
IPS モジュール	24
合計	**75**

表 4 – マルウェアモジュールと IPS モジュールのアラート（Enterprise Threat Protector の導入による修復時間の節約）

全体として、Enterprise Threat Protector の導入により、1 か月当たりおよそ **110 時間**が節約されたと推定されます。