SEPTEMBER + OCTOBER2015 SecuAvail

SecuAvail NEWS 8

意外な落とし穴!?UTM 流行期における Proxy の存在

vol.8

NEWS CONTENTS

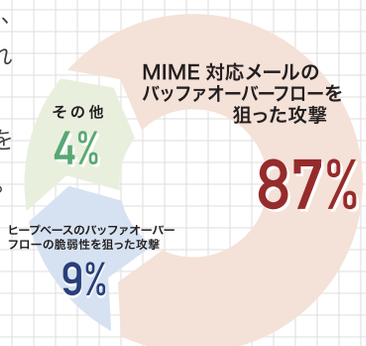
CONTENTS 01

MIME 対応メールのバッファオーバーフローを狙った攻撃

情報セキュリティ通信

2015年 6 月 脅威件数による動向

2015 年 6 月に弊社 IPS で検知した脅威件数の集計である。
5 月に比べて脅威件数自体は増えているが、1 位の『MIME 対応メールのバッファオーバーフローを狙った攻撃』の件数増加に起因する。
それ以外は、概ね脅威内容、件数ともに大きな変化は見られない。ランキング上位は、HTTP系の攻撃とMailサーバを狙った攻撃が多い傾向にある。



※弊社 IPS 運用サービスにて検知した「High」アラートの集計結果

IPS 脅威検知件数集計 (2015年 6 月)

※弊社 IPS 運用サービスにて検知した「High」アラートの集計結果

	検知した脅威の内容	
1位	MIME 対応メールのバッファオーバーフローを狙った攻撃	6,971
2位	ヒープベースのバッファオーバーフローの脆弱性を狙った攻撃	725
3位	MS Exchange でリモートでのコードの実行を引き起こす攻撃	80
4位	Bash（ShellShock）の脆弱性を狙った攻撃	77
5位	MS IIS の脆弱性を狙った攻撃	40
6位	Apache の脆弱性を狙った攻撃	24
7位	Shell コマンドインジェクション攻撃	20
8位	PHP include 関数を狙った攻撃	20
9位	Heartbleed の脆弱性を狙った攻撃	15
10位	HTTP GET リクエストを利用した攻撃	14
	その他	58
	合計	8,050

今号の特集について

今号は Proxy サーバの必要性について特集号とした。通常 DMZ に配置され、内部からの Web アクセスのゲートウェイとして稼働する。導入メリットは、Web アクセスを一元管理できることである。そのため、Web アクセスのポリシーや効果的なセキュリティ対策の設定を一箇所で行うことができる。また、キャッシュにより、トラフィックを削減できるという効果もある。しかしながら、ゲートウェイ機能を担うものが FW（UTM）製品と Proxy サーバの 2 つになるとログ管理が煩雑になるという問題が出てくる。更に可能性は低いが、Proxy サーバの稼働自体がセキュリティリスクになる恐れがある。

それは、あるユーザが危険なサイトでマルウェアに感染した場合違うユーザが同じサイトにアクセスすると Proxy サーバで保持しているキャッシュを介して同じマルウェアに感染する可能性がある。当該のサイトで既に対策されていたとしてもである。一方で、近年では、UTM 製品の台頭で一元的な運用管理は、Proxy サーバを設置しなくても可能となった。どちらも一長一短ではあるが最終的には、自社の運用体系に合致するよう UTM と Proxy サーバの導入を決定する必要がある。システムを見直すタイミングで新機能を増やすことに目が向きがちになるが不要なものをなくす方向への視点も重要である。

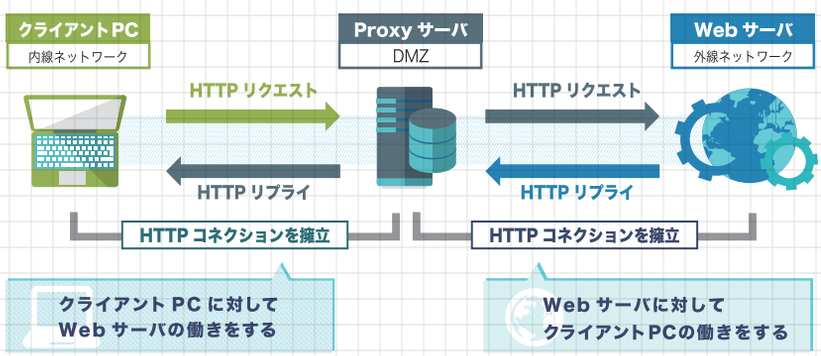
担当：卒区次郎

CONTENTS

02 特集！意外な落とし穴!?

そもそも Proxy サーバとは？

Proxy サーバを一言でいうと、「クライアント PC の代理としてインターネット接続を行うサーバ」である。ここでの Proxy サーバは、HTTP トラフィックを対象とした Web (HTTP) プロキシを指す。
一般的には DMZに配置し、図のような通信を行う。(右図参照)
企業が Proxy サーバを導入する目的・メリットは大別すると以下の 3 つが挙げられる。



企業が Proxy サーバを導入する目的・メリットは大別すると以下の 3 つ

1. 匿名性確保によるセキュリティレベルの向上

Web サーバにはクライアント PC ではなく、Proxy サーバがアクセスすることになるため、クライアント PC の固有情報 (IP アドレス、OS、ブラウザなど) が漏れることなく Web ページを閲覧することができるため、情報漏えい防止の 1 つの手段となる。

2. 内部から外部への通信の一元管理実現

内部から外部への HTTP 通信が全て Proxy サーバを通過する設定にすることで、無許可端末の通信制御や業務外のサイトアクセスの禁止ができる。

3. キャッシング機能による Web 通信の高速化

Proxy サーバは過去に Web サーバから受信した Web ページの情報を自身の HDD などに一時的に記録するため、再アクセス時には Proxy サーバのキャッシュ情報を素早く送り返し、Web 通信の高速化を実現させる。

Proxy サーバが存在する環境への UTM 導入における悩み所

UTM の設置場所により取得可能なログは異なる。実環境では、下図 2 種の構成がほとんどであろう。
A は、Proxy サーバとインターネットの間にUTMを設置する構成。ログから宛先はわかるが送信元は全てProxyサーバからの通信として認識される。一方、B はクライアントと Proxy サーバの間に UTM を設置する構成。この構成のログからは、送信元のクライアント IP はわかるが、反対に全て Proxy サーバ宛ての通信と認識されることになる。

つまり AB 共に、クライアントがどのような Web サイトにアクセスしたかを把握するためには UTM ログ +αの情報が必要になる。これは実運用を考えた場合、非常に厄介である。何かおこると、UTM と Proxy サーバのログをおよその時間やクライアント情報から突合する必要がある。UTM のログは FW や IPS、AV 等多くの機能を使っておりその量は膨大である。Proxy サーバの場合、例えば Yahoo Japan のページへのアクセス時に出力されるログはページ上に表示される広告等へもセッションが張られログ出力されるため目的のログを調査・分析する工数は膨大なものになり運用設計を熟考する必要がある。

UTM 流行期における Proxy の存在

現実的な UTM 導入に向けて

『Proxy サーバが存在する環境への UTM 導入における悩み所』で記載したように、
UTM 導入の検討対象となっている既存環境に Proxy サーバが存在している場合には、
「Proxy サーバをどうするか？」検討の初期段階で関係各位に認識させて具体的な
設計や提案を受けることがスムーズな導入に繋がる。
既設 Proxy サーバに対する方針としては、大別すると以下の 2 つが挙げられる。

方針 1　UTM導入に伴い、Proxyサーバを撤去する

対 象

Proxyサーバが担っている役割がUTMでも実現可能な環境

（例）HTTPプロキシや FTPプロキシ、Webフィルタリング機能など。

ポイント

【Proxy で利用している機能を整理し、UTM へコンバート】

単純な HTTP プロキシや FTP プロキシとしての利用以外に、Web フィルタリングやウイルスチェックの機能も利用している Proxy サーバを撤去するには、これらの付加機能を UTM にコンバートすることが必須となる。
UTM 製品毎に、Web フィルタリングのカテゴリ分類やウイルスチェックの仕組みは異なるため、ヒアリング形式で導入ベンダーとクライアント間の齟齬が生じないように進めることを推奨する。
また、導入ベンダー側が UTM の情報を提供するだけではなく、Proxy サーバ側の現行情報をクライアントから早期に提供してもらうように働きかけることも重要である。

方針 2　UTM と Proxy サーバを共存させる

対 象

Proxyサーバが担っている役割がUTMでは実現不可な環境

（例）外部サーバのコンテンツキャッシュ、ドメインユーザ単位でのアクセスログなど。

ポイント

【導入後の運用設計にも注力する】

新しく機器を導入する際には、パラメータ設計や導入・移設など「設置・稼動までの工程」にどうしても意識が傾く。しかしながら、方針 2 では UTM と Proxy サーバが共存する形となるため、「インシデント発生時のログ調査フロー」等、導入後の運用方針にも目を光らせる必要がある。
なお、UTM と Proxy サーバの両方でセキュリティ機能を併用するような構成となる場合には、「どちらの機器のセキュリティ機能が先に働くか？」を導入前の時点で整理しておくと導入効果を最大限に活かすことになる。

上記 2 案に関しては、導入後の運用負荷や物理障害ポイント数の観点から、基本的には [方針 1] が推奨となる。

特集まとめ

今号の特集では、「UTM」と「Proxy サーバ」を焦点とし、UTM 導入における本質的な理解の 1 つとして「導入対象のネットワーク環境について熟慮すること」が挙げられる。上記ポイントは、UTM に限らずインフラ構築では基本中の基本であることは承知の上だが、UTM は多機能であるがゆえに導入によって Proxy サーバ以外の様々な機器に対しても相性や機能競合が生じるリスクはやはり念頭に置いておくべきである。　**『一利あれば一害あり』**

記事担当：卒区次郎、しーばす、まえあし

CONTENTS 03

保護対象サーバの情報って必要？

なるほど～NetStare

保護対象サーバの情報
提示してもらう理由とは？


お客様

NetStare のサービス申込書に保護対象サーバの情報を記入するシートがあるけれど、
記入しなくてもサービスって受けられるよね？


セキュアヴェイル

保護対象サーバの情報は IPS イベント対応アドバイスや脆弱性診断を提供するために必要となります。


お客様

IP アドレスだけあればサービスは提供してもらえそうだけど・・
OS とかアプリケーションとか、申込書に記入する情報が多くて正直面倒だな・・


セキュアヴェイル

確かに IP アドレスだけでも IPS イベント対応アドバイスや脆弱性診断を提供することは可能です。しかし、それだけでは十分なアドバイスができません。


お客様

そうなの？どんな違いがあるの？


セキュアヴェイル

例えば IPS イベント対応アドバイスでは検知した攻撃内容だけでなく、お客様環境にて影響を受けるシステムの有無を確認した上で推奨する対策をご連絡しています。


セキュアヴェイル

保護対象サーバの情報をいただくことで、より具体的な対策を提示することが可能です。
その結果、お客様自身で何をするべきか最適な判断が行えます。


お客様

それは必要かもしれないなぁ。


セキュアヴェイル

脆弱性診断についても同様に、結果に対して適切なアドバイスを提示することが可能となります。


お客様

なるほどね～！
自社の環境にあったアドバイスを受けるには保護対象サーバの情報が必要なんだね。

記事担当：甲斐

McAfee NSP セミナー開催！

McAfee NSP 運用サービスのリリースに伴い McAfee 社と合同でセミナーを開催します。機器や運用サービスの特徴だけではなく、セキュリティ対策の根本的な考え方を交えてご説明いたします。詳細はこちらをご覧ください。
【セミナー情報 URL】http://www.secuavail.com/seminar/

CONTENTS 04 セミナー情報
Seminar information

担当：甲斐

SecuAvail 株式会社セキュアヴェイル (SecuAvail Inc.)

大阪本社
〒530-0044　大阪府大阪市北区東天満1-1-19
アーバンエース東天満ビル
TEL:06-6136-0020　FAX:06-6136-0018

東京ブランチ
〒103-0025　東京都中央区日本橋茅場町1-6-17
トラッドビル 6F
TEL:03-5643-0208　FAX:03-5643-0207

次号予告 /・特集 !! McAfee NSP
・情報セキュリティ通信脅威動向　・コラム

www.secuavail.com