SecuAvail NEWS

SecuAvail
2015/4
Vol.5

Contents

情報セキュリティ通信

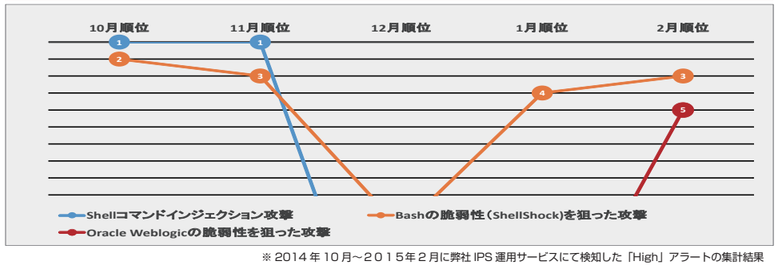
IPS が検知している脅威の動向

2014 年 10 月～ 2015 年 2 月にセキュアヴェイルの IPS 運用サービスで検知した脅威の内容と件数を集計しました。
毎月多くの脅威を検知しています。中でも検知数が最も多かった脅威は、『バッファオーバフローの脆弱性を狙った攻撃（対象 Zom-Mail)』、次いで『Shell コマンドインジェクション攻撃』です。『Shell コマンドインジェクション攻撃』は 11 月までは検知数が多かったのですが 12 月以降は全く検知がありません。にも関わらず今期間内の検知総数で 2 位に位置付けられていることから短期間での攻撃が突出していたことがうかがい知れます。
4 位の『Bash の脆弱性を狙った攻撃（ShellShock)』も昨年世間で騒がれた重大な脅威の 1 つです。
12 月に検知数が下降したものの年明け以降、検知数が増加傾向にあります。同攻撃は警察庁からの報告でも増加という認識であり引き続き要注意です。
また、新たな脅威となるのか『Oracle_Weblogic の脆弱性を狙った攻撃』が 2 月から急激に増加してしいます。多くのシステムに影響を及ぼすため、この脅威についても検知数の動向を抑え、対策を準備しておくべき事象だと認識する必要があります。
断続的に発生している脅威、新たな脅威、いずれも対策は必要ですが、現時点では特にこの 3 件の脅威への対策を万全にすることが急務です。2014 年は、Heartbleed、ShellShock といったインパクトのある脆弱性情報がありました。攻撃は公開直後に大量に発生しています。今後もこの傾向は続くと思われます。
こうした攻撃の影響を最小限とするには、パッチの適用や IPS などによる対策を迅速に行うことが重要です。
自社への影響を可視化、認識したい、脆弱性対策の必要性を理解しているが自社で効果的かつ迅速な対応が困難である場合は、セキュアヴェイルの NetStare サービスへのご加入をご検討ください。（卒区次郎）

IPS 脅威検知件数集計（2014 年 10 月～2015年2月）

検知した脅威の内容		10月	11月	12月	1月	2月	検知総数
1 位	MIME 対応電子メールのバッファオーバフローの脆弱性を狙った攻撃	2,225	180	5,230	2,896	601	11,132
2 位	Shell コマンドインジェクション攻撃	5,035	4,888	0	0	0	9,923
3 位	Web(HTTP) トラフィックに実行可能コマンド (.EXE) を組み込む攻撃	1,200	1,400	1,000	800	576	4,976
4 位	Bash の脆弱性（ShellShock) を狙った攻撃	2,348	1,107	53	330	382	4,220
5 位	URL 内の「ドット ドット」(/../) シーケンスの脆弱性を狙った攻撃	539	626	430	344	246	2,185
6 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	317	464	546	315	352	1,994
7 位	OpenSSL 脆弱性を狙った攻撃	732	336	95	122	58	1,343
8 位	PHP include 関数の脆弱性を狙った攻撃	132	203	172	258	133	898
9 位	Heartbleed の脆弱性を狙った攻撃	302	112	111	93	81	699
10 位	PHP CGI 構成の脆弱性を狙った攻撃	101	157	110	147	125	640
11 位	URL 内のスタック オーバーフローの脆弱性を狙った攻撃	109	235	233	18	10	605
12 位	ASP ファイル取得の試み	76	84	84	80	60	384
13 位	HTTP GET リクエストを利用した攻撃調査	42	95	54	96	46	333
14 位	Oracle Weblogic の脆弱性を狙った攻撃	1	1	2	0	297	301
15 位	JPEG データを含む PDF ファイルを使った攻撃	30	35	27	9	2	103

ランキング推移から動向を注視したい脅威（単位：位）



※ 2014 年 10 月～2015 年 2 月に弊社 IPS 運用サービスにて検知した「High」アラートの集計結果

なるほど～ NetStare

～ブラックリストブロックってどんな意味があるの？？～


お客様

ブラックリストブロックというサービス項目があるけれど、これは何をしているの？


SA

弊社が不正と判断した IP アドレスからの通信をお客様のファイアウォールでブロック（遮断）する様に設定する定期サービスです。
不正と判断する IP アドレスは、弊社が運用している数百台のセキュリティ機器が検出した攻撃者 IP アドレス情報と、米国の SANS というセキュリティ機関が定期的に発表している攻撃者 IP アドレス情報を元に決定しており、3 ヶ月に 1 回対象となるアドレスリストを作成しています。
このリストをブラックリストと呼び、お客様のファイアウォールで遮断する様に設定しています。


お客様

ふ～ん。すごそうだけれど、3 ヶ月に 1 回で大丈夫？攻撃者の IP アドレスって、日々変わっていくものではないの？例えば 1 週間前まではブラックリストのアドレスだったけれど今は悪意のない人が使うアドレスになっているとか。


SA

3 ヶ月に 1 回が妥当かどうかはわかりませんが、1 度ブラックリストの対象になったアドレスがすぐに悪意のない人に渡るということは考えにくいんです。
実際、弊社がこれまで 10 年以上サービスを提供してきた中でも、ブラックリストとしてブロックしたアドレスが、実は正常なアドレスだったということは 1 度もないですよ。


お客様

そうなんだ～。あ、だけど UTM（統合脅威管理機器）だったら、ブラックリストの IP アドレスで通信を止めなくても、URL フィルタリングや IPS 機能で不正なアドレスからの通信は止めてくれてるって聞いたけど。


SA

確かに UTM の場合は、ブラックリストブロックで通信を遮断しなくても、他の機能で遮断する方法があると思います。にもかかわらずブラックリスト IP ブロックを実施するのは、機器に余計な負荷をかけないためでもあるんです。


SA

弊社では、ブラックリスト IP アドレスの設定投入はお客様のファイアウォールポリシーの最上段・・・つまり一番優先度が高いポリシーとして設定します。
UTM の通信検査は、ファイアウォールのポリシーから始まり、様々な機能に対して順番にチェックしていきます。


SA

ブラックリスト IP アドレスを優先度の高いファイアウォールポリシーとして設定しておくと、UTM の通信検査時に余計なチェックをすることなく真っ先に遮断されます。
そのため、UTM の通信検査時に無駄なチェックをなくすことができ、機器のパフォーマンス向上もなるんですよ。


お客様

なるほど！ NetStare サービスに加入していれば、ブラックリストブロックで攻撃者からの不正な通信を防げるだけでなく機器のパフォーマンスを維持するメリットもあるんだね。

（ぐり子）

コラム

「IPS は高い？適切な価格？…」

IPS はセキュリティ対策ツールの中でも高額だと言われている。
高いものを買っても運用も難しいし…うちには贅沢だから…。
20 年程前にほかのセキュリティ対策ツールを提案していた時も、同じ様な反応だったと記憶している。外部の脅威やセキュリティ事件の社会的影響が大きくなっているが、導入を検討するフェーズでの反応はあまり変わっていない。
IPS は確かに安くないのかもしれないが、そもそも IPS が高いとか贅沢だというのは何を判断基準にしているのだろうか？
セキュリティ対策は投資対効果が不明だとか、どこまでやったらいいのだろうか？と聞くことがあるが、それは誰に聞いているのだろう？
セキュリティ対策は自社のためにやるものであり、どこまでやるかは自社で決めるべきことである。まして、セキュリティ対策の投資対効果？セキュリティ対策に投資をしても直接的に利益向上に繋がることなどない。
何を守るのか？個人情報、顧客情報、企業秘密と位置付けられる情報なのか…
IPS、セキュリティ対策にかかる費用が高いか安いかを検討する前に、守るべき対象とそれが損失した場合に被るリスクを「円換算」してみたらどうだろうか？
数十億のリスクヘッジに 1000 万円の投資は果たして…高いか？適切か？その答えは自分自身で出すしかないのである。
（海女若）

セミナー情報

Vol.5 執筆現在、東京、大阪にて定期セミナーの開催を計画中です。
SecuAvail News の紙面だけでは紹介しきれないセキュリティ情報やセキュアヴェイルのサービス、プロダクトの紹介、パートナー様やユーザー様との個別相談会などを計画しております。
詳細は Web 等でお知らせしていきます。
ご期待ください。

SecuAvail http://www.secuavail.com
株式会社セキュアヴェイル

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
E-mail:sales@secuavail.com

東京ブランチ
〒130-0025　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

特集

不正侵入検知防御システム（IPS）

標的型攻撃対策にはずせない 機器選定ポイントと運用方法

ファイアウォールと IPS。巧妙化する標的型攻撃！対策手段に IPS が必須となる本質的な考察。

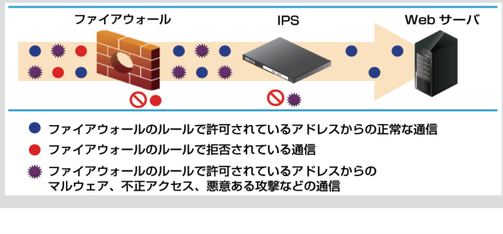
ファイアウォール（以下、FW）と IPS（Intrusion Prevention System）の違いは、シンプルに言うならば許可 / 遮断を判断する階層とプロトコルが違う点にある。
FW はポート番号、IP アドレス、プロトコル、通信方向をアクセス制御ルールに基づき、通信の許可 / 遮断を判断する。通信内容まではチェックしない。通信内容とは、マルウェア、不正アクセス、攻撃など”振る舞い”を意味する。一方、IPS は不正侵入検知防御システムと呼ばれ、FW が許可した通信のパケットを監視し、内容を含む全体を解析する。結果、怪しい振る舞いや攻撃、不正侵入の可能性を検出した場合に遮断 / 破棄する。

階層	プロトコル	FW	IPS
アプリケーション層	HTTP		↕
プレゼンテーション層			↕
セッション層			↕
トランスポート層	TCP	↕	↕
ネットワーク層	IP	↕	↕

仮に、外部から社内の Web サーバに HTTP（ポート番号 80 番）のアクセスを許可している環境で悪意のある通信が送られてきた場合、FW で通信を許可し、IPS で不正通信を遮断するということなる。では、FW と IPS どちらが現状の脅威に合致するのか。様々なネットワーク構築と運用監視業務の経験から IPS が有効と判断する。もちろん、併用が一番有効である。

それは、標的型攻撃が巧妙化していることが第一の理由である。攻撃者は事前に対象システムの脆弱性を認識し侵入可否を調査してから攻撃を行う。多くの攻撃は脆弱性を狙って行われるためシステムを常に最新の状態にアップデートし、修正プログラムを適用することが不可欠となる。しかし、現実的な問題として修正プログラムが存在していない脆弱性を狙った攻撃や修正プログラムをすぐには適用できない事象は決して少なくはない。その時に有効手段となり得るのが IPS の導入・稼働である。時には高額な投資となることもあるが、利益を守るためのセキュリティ対策という本質を鑑みると、尽きることなき脅威と攻撃への対策が利益貢献とも認識できるであろう。

ファイアウォールと IPS の通信遮断イメージ



IPS の選択視点！「IPS 運用の成否は IPS 専用機の導入が最適」

セキュアヴェイル独自の視点で IPS 専用機（ネットワーク型）と UTM 製品の IPS 機能を比較した結果、IPS 専用機が最適であるとの結論に至った。その背景を解説する。
IPS 選択の最大のキモは導入後の運用にある。その観点から、攻撃の検知 / 防御機能、オペレーション、インシデント対応の３要素で比較した。

★攻撃の検知 / 防御機能★　不審な通信の検知 / 防御性能比較

最近の調査機関のレポートや社内での検証を見る限り、IPS 専用機と UTM 製品の IPS 機能では、検知 / 防御機能にほとんど差はない。昨年は大きな脆弱性がみつかり、シグネチャのリリースはわずかながら UTM メーカの方が IPS 専用メーカより早かったケースはあるものの機能差とまでは言えない。
攻撃の検知 / 防御機能は差がないと判断する。

★オペレーション★　IPS 運用のオペレーションコスト比較

日常的な IPS のオペレーションで比較する。IPS は、保護対象毎に IPS プロファイルを作成し、保護対象にマッチした検知 / 防御を行う。ただし、UTM 製品の場合、IPS 機能は FW ポリシーごとに適用する / しないを実装するため、保護対象毎に FW ポリシーと IPS プロファイル作成が必要で、かつ日々そのメンテナンスが発生する。環境にもよるが、きめ細かい IPS 設定を行う場合の作業量は甚大になる。一方、IPS 専用機は IPS に特化しているため設定が容易である。設定のコストを抑えるという点で IPS 専用機に分がある。オペレーションは IPS 専用機が優位と判断する。

★インシデント対応★　インシデント発生時の調査性能比較

インシデント検知時は、自社システムへの影響、攻撃内容（手法）、攻撃が成功 / 失敗したのか、成功した場合は攻撃を受けたシステムへの調査が必要になってくる。調査に欠かせないのがログだが、攻撃検知時の情報量（ログ）は、IPS 専用機が圧倒的に多く他製品の追随を許さない。情報量が豊富な分調査も行いやすい。
インシデント対応は IPS 専用機が優位と判断する。

★比較結果のまとめ★

「IPS でインシデントを検知した後の調査スピード」、「検知 / 防御に必要な設定の完了までのスピード」という視点で、IPS 専用機が最適である。特に大きな利点はログの情報量にある。IPS 運用では情報量と内容からいかに早く対応できるかが重要になる。攻撃名が判明しても、攻撃手法、自社システムへの攻撃や影響の有無などが分からなければ対応に時間がかかる。攻撃内容と攻撃の失敗 / 成功が分かり対応速度を早められるのは IPS 専用機となる。
とはいえ、決して UTM 製品が劣るわけではない。あくまで当社視点の比較結果である。

比較項目	IPS 専用機	UTM 製品 IPS 機能
検知 / 防御機能	○	○
操作性	○	△
対応のしやすさ	○	△
パフォーマンス	○	△
情報量	◎	△
機器障害時の対処	○ 機器障害時は通信の通過が可能	× 機器障害時は通信を遮断
製品のラインナップ	△	◎

IPS の運用は難しい？「運用」とは一体何か？投資対効果を生み出す「運用体制」の選択

「IPS は導入をしても運用が難しいからなぁ…」という声は少なくない。IPS を適切な状態で稼働させ導入効果を得ようとするならば、脅威（攻撃）を検知した時に、その脅威の影響度、未知か既知か、適用可能なシグネチャが存在するか、また、シグネチャ適用時に与える影響度、対策の要不要と手法の選択など様々な見地から判断し迅速に行動することが求められる。
海外では自社で SOC（Security Operation Center）を所有し専門の要員が日々セキュリティマネジメントに従事し最適化を行っていることが多いと言われる。一方、国内で自社 SOC を所有している企業はまだごくわずかである。セキュリティエンジニアの数が圧倒的に少ないのが根本原因だと言われるが、運用面から見ると別の問題も垣間見える。例えば、情報システム部門に従事する人たちがセキュリティ対策のみを担っていることは少なく、様々な業務を兼任していることが多い。IPS またはセキュリティ対策の専任者ではない。
前述した内容を鑑みると、IPS を効果的に運用（稼働）するためには「知識量」というより、「セキュリティ対策に必要な情報量」をどれだけ保有しているかによって運用状態が左右されてしまうとも認識できる。つまり、知識（技術）不足というより人材と時間の不足が運用を難しくしているもう１つの要因とも言えるのではなかろうか。優秀なセキュリティエンジニアは売り手市場と言われているため条件によっては転職をする。エンジニアに転職（退職）されることがそのまま脆弱性に跳ね返ることになる。結果的に安全性を担保する体制を構築することが困難だと判断され、それが IPS 導入に二の足を踏ませてしまうさらなる要因となる。対策として運用の外部委託という選択肢がある。
国内では自社 SOC は少ないと述べたが、SOC を所有し IPS の運用サービスを提供する専門ベンダーは複数存在する。サービス費用は様々であるが、IPS を宝の持ち腐れにしないためにも運用を委託することも選択肢の一つである。セキュリティ対策に必要な情報を入手するために多くの時間を費やすのであれば、一度だけ SOC ベンダー選択のために時間を割いてはどうだろうか？転職される心配もなく、安定したセキュリティ対策状況を維持することが可能となる。

セキュアヴェイルの IPS 運用の有意性。それは、「3 つの特長を”融合”させたサービス」提供にある。

セキュアヴェイルの IPS 運用サービスの特長

1. システムの安定稼働とセキュリティを維持していくサービスの両方を有している点。
2. 統計から一定の判断基準により問題点をレポート（テンプレート）する機能を有している点。
3. 自社開発のマネジメントツールにより日々変化する脅威への対策に柔軟かつ迅速に対応できる点。

まず、「安定稼働」と「セキュリティ維持」の両サービスの観点から運用監視体制の優位性があげられる。
セキュアヴェイルでは 24 時間 365 日、常に高度なスキルを持った「正社員」のエンジニアが対応している。
エンジニアすべてを「正社員」で構成している SOC は国内ではほとんどないのが実情である。「正社員」で構成された SOC は、夜間、休祝日を通して同じレベルで対応できる体制を整え、24 時間 365 日、常にサービス品質を平準化させていることを意味する。つまり、属人化によるサービス品質の低下を防止しているのだ。
また、「セキュリティを維持するためのサービス」の特長として、保護対象サーバに対する定期的な脆弱性診断を定額サービス費用内で提供している点もはずせない。
そして、最も特長的と言えるのは、顧客が危険を察知しやすい視点で作りこまれたレポートが豊富な点である。
「SecuAvail News Vol.3」の「Security News を斬る」でも触れられているが、一般的な SOC が提供する月次サービスの成果物が現象を集計した「統計レポート」であるのに対し、セキュアヴェイル社は気付きを与える「運用テンプレート」を成果物としている。IPS の運用サービスを検討するうえで、この違いをしっかりと抑えていただきたい。セキュアヴェイル社が用意している「運用テンプレート」とは、ログ件数の集計に留まらず、その中に潜む情報に着目している点が特長的である。「不正行為の疑義がある通信」をあらかじめ定義し、その視点で集計結果を確認することができる。気になる情報は様々な検索条件で更に絞り込み、ピンポイントで詳細情報をチェックできる。
例えば、一般的なレポートが「攻撃が多い IP アドレスを日付別に集計し、いつ、どのアドレスから何件」という集計レポートであるのに対し、セキュアヴェイルの運用テンプレートは、「検知した IP アドレスからどんなアラートが多く発生しているのか」、「影響度の高い攻撃がどれくらい発生しているのか」、「アラートが一時的なのか慢性的なのか」など、チェックすべき視点で絞り込み多面的にログをチェックすることができる。
表面的な情報から、なぜ？いつ？どのくらい？など疑問に思ったことをドリルダウンして把握することができる。
この手法で、一般的な集計レポートでは見えない情報に短時間でたどり着くことができる。このテンプレートは、実際にセキュアヴェイルの SOC で運用しているノウハウを元に作成しており、実効性が高い。
テンプレートは今後、50 種以上に強化してリリースする予定があり、より詳細に現状をチェックできる見込みである。
運用で蓄積した経験とノウハウを体制とサービスに組み込み、３つの特長を融合させることで顧客に価値ある IPS 運用を日々実施している。　（特集記事：甲斐／卒区次郎／海女若／千代路弓）