MAY+JUN 2015 SecuAvail

SecuAvail NEWS vol.6

セキュアヴェイルの新しいスタンダード 未来型CS

NEWS CONTENTS

CONTENTS 01

検知件数はなんと先月の3倍に！

情報セキュリティ通信　3倍に膨らむ脅威

2015年3月・4月脅威件数による動向

2015年3月、4月に弊社IPSで検知した脅威件数を集計しました。
全体を見ると、4月の検知件数（6,856件）は3月（1,924件）の3倍以上になっています。特に増えた脅威は、『MIME 対応メールのバッファオーバフローを狙った攻撃』と『Bash（ShellShock）の脆弱性を狙った攻撃』です。
この攻撃は昨年 9 月後半に報告があった攻撃なので、既にほとんどの企業では、対策実施済みかと思いますが、今一度自社システムの設定を見直しておいたほうが良さそうです。
また、『Heartbleed の脆弱性を狙った攻撃』も少しずつではありますが、増加傾向です。影響度が広範囲に渡るため、引き続き注意が必要です。
最近は、脆弱性情報の公開直後からその脆弱性を狙った攻撃が急激に増える傾向が顕著です。
ますますIPS機能の重要性が高まっています。

IPS 脅威検知件数集計（2014年3月～2015年4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	3月	4月	検知総数
1位	MIME 対応電子メールのバッファオーバーフローの脆弱性を狙った攻撃	546	2,958	3,504
2位	Bash の脆弱性 (ShellShock) を狙った攻撃	80	2,756	2,836
3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	479	478	957
4位	Heartbleed の脆弱性を狙った攻撃	97	150	247
5位	HTTP GET リクエストを利用した攻撃	64	173	237
6位	PHPinclude 関数脆弱性を狙った攻撃	96	80	176
7位	PHP CGI 構成の脆弱性を狙った攻撃	78	60	138
8位	EMF の脆弱性を狙った攻撃	138	0	138
9位	Mozilla のバッファ オーバーフローの脆弱性を狙った攻撃	96	0	96
10位	MS IIS の脆弱性を狙った攻撃	60	36	96
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	21	10	31
12位	Shell コマンドインジェクション攻撃	7	24	31
13位	McAfee VirusScan Enterprise バッファオーバーフローの脆弱性を狙った攻撃	21	9	30
14位	MS Exchange でリモートでのコードの実行を引き起こす攻撃	0	10	10
15位	MS Excel の配列インデックスに関するエラー処理の脆弱性を狙った攻撃	0	9	9
ー	その他	141	103	8
	合計	1,924	6,856	8,544

今後の傾向と対策

今後自社で IPS システムの導入をご検討の際は、是非、セキュアヴェイルの NetStare サービスも併せてご検討ください。
また、自社で IPS システムを運用したい企業様は、運用に必要なレポートテンプレート、アラートテンプレートをセキュリティログ管理システム『LogStare』の導入をご検討ください。

特集記事担当：卒区次郎

CONTENTS

02 2015年4月本年度より新体制 特集！セキュアヴェイルの新しいスタンダード

本年度より営業部は発展的に廃止 カスタマーサービス(CS)部となりました

組織変更内容と業務内容

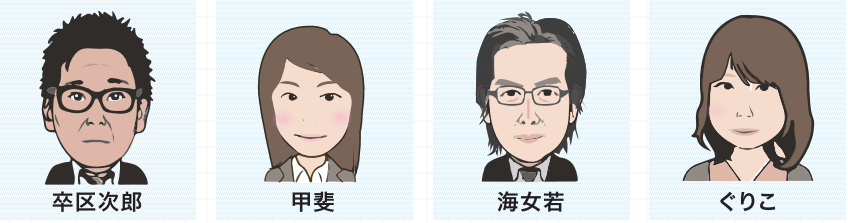
セキュアヴェイルは、本年度より大幅に組織を変更しました。自分として一番大きい変更点は、営業部門を発展的に廃止し、カスタマーサービス部に変身したことです。業務上の大きな変更点は、既存のお客様（特に NetStare 顧客）に定期的にカスタマーサービス部（CS 部）のメンバーが個々の顧客環境を考慮した運用レポートを作成し、レポートの解説とセキュリティ対策強化のアドバイスを実施することです。旧営業マンも前期よりセキュリティログ分析の研修を受けセキュリティエンジニアに生まれ変わりました。

組織変更の方針と理念

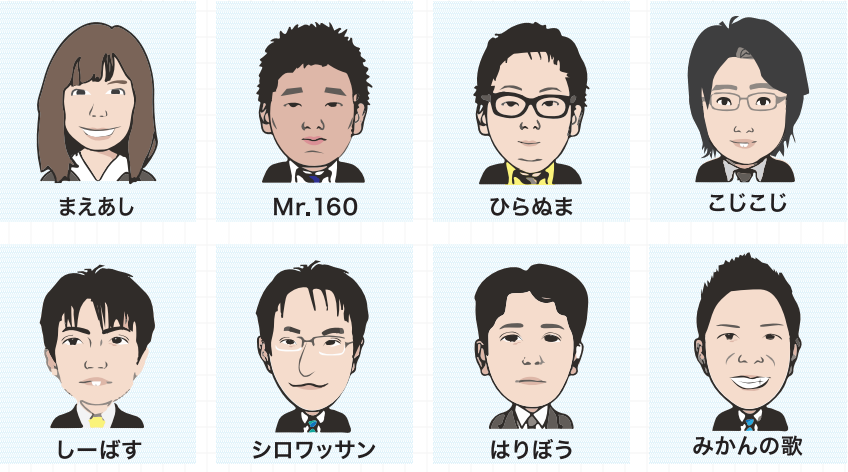
今回のこの方針は、セキュアヴェイル創業者の強い理念があってのものです。当社は、元々 SIer で Firewall 販売をしていた営業マン（創業者）とエンジニア（現当最高技術顧問）が創業した会社です。Firewall を販売・導入がゴールではなく、導入がスタートでありセキュリティ対策を効果的に実施するには「運用」が欠かせないとの考えから Firewall を運用する会社として、当時はあまりなかった SOC を作り、お客様に代わってセキュリティマネジメントをする運用サービス専門の会社を創りました。

今後のカスタマーサービス(CS)部

OSAKA CS MEMBER
大阪カスタマーサービス部 CSメンバー紹介



TOKYO CS MEMBER
東京カスタマーサービス部 CS メンバー紹介



必見！公式 Facebook

セキュアヴェイル　Facebook

CS メンバーとその役割

セキュリティ機器の運用サービスは、ログマネジメントとほぼ同義であるとの考えから、ログ管理 / 分析システムを自社開発し、そのログ管理システムを基にセキュリティログレポートをお客様に提供をしてまいりました。
このセキュリティログレポートのコンセプトは、お客様にセキュリティ対策の基準を提供することです。セキュリティ基準と自社環境との乖離（かいり）が自社の問題点です。つまり問題点を気付かせるレポートが当社のセキュリティログレポートです。その気付きを具体的な改善策へと導く支援をするのがカスタマーサービス部の役割です。

今年は積極的にセキュアヴェイルを露出していきます。
セミナー開催や Facebook 等ソーシャルメディアの活用も積極的に行っていきます。また、今夏には、新運用監視エンジンのリリース予定があります。次号 SAN（SecuAvail NEWS）では、新運用監視エンジンの紹介したいと考えてます。

特集記事担当：卒区次郎

CONTENTS

03 対策すべき脅威と未然のトラブル防止 特集！運用状況報告会がスタートしました

セキュアヴェイルのメリット

運用状況報告会って何をするの？

本年度はカスタマーサービス部の提案活動の一環として、NetStareサービスを御契約頂いているお客様に定期的に運用状況の報告会を行います。
NetStare ではサービス仕様として年 1 回の運用報告会が含まれていますが、この運用報告会とは別に、よりお客様に近い立場で一緒に課題を見つけ対策を提案していきます。

運用状況報告会内容をちょっとだけ教えます!

NetStareのサービスのコンポーネントである「システムマネージメント」と「セキュリティマネージメント」で提供しているサービス項目に沿って運用状況の報告を行います。例えば…
「1 回も障害は発生していないけどこのまま利用し続けてもリソースには問題がないのか？」「ブラックリストブロックの設定をしたことによって、不正な IP アドレスからの通信を何件ブロックしているのか？」など、普段 SOC から発信していない情報をお伝えしていきます。

運用状況報告会の特徴 メリット

- 障害発生の有無に関わらず運用状況を定期的に把握することができる
- 今まで以上にお客様の会社に適したサービスを利用することができる
- ログの分析結果から対策すべきことを把握することができる

お客様のメリット

「障害を検知してからの対策」から「将来的な障害を未然に対策」へ。

NetStare サービスでは機器の障害や IPS イベントを検知した際にお客様に連絡をし対策していきますが、トラブルが起きていないからと言って何も対策しなくて良いということではありません。
NetStare ではポータルサイトや定期配信しているセキュリティログレポートをお客様自身で確認し状況を把握することができます。このセキュリティログレポートを定期的に確認し分析、日々改善をしていくことで将来的な障害や事故を未然に防ぐことができます。
セキュリティログレポートでは「一定の基準」を設けて、その基準との差分を把握し改善策を考えることができるように作られています。機器の障害や攻撃を検知した際には弊社からご連絡させて頂きますが、現在問題が発生していない場合でもポータルサイトやセキュリティログレポートを利用して定期的に分析することで、過去や現在の分析だけではなく未来を予測し未然のトラブル防止などに役立てることができます。
また運用状況報告会を通してお客様環境をお教え頂くことで、今まで以上にお客様のシステム利用状況にあわせたサービスを提供していきます。

特集記事担当：甲斐

さらに、ここがすごいカスタマーサービス部

- また上記に加え、セキュリティログレポートをもとにカスタマーサービス部のメンバーが様々な視点から調査し、傾向、課題、対策についてコメントをします。
- セキュリティのプロ集団が下記の観点からご提案させて頂きます。

今すぐ対策すべきこと | 中長期的に対策すべきこと | 推奨する対策

CONTENTS 04

設定変更にかかる時間と品質維持

なるほど～NetStare

設定変更に2営業日!?
なんでそんなにかかるの？


お客様

NetStare のサービス内容で設定変更というのがあるけど、依頼から2営業日以降に実施というのは…結構時間がかかってるように思うんだけど。
こちらの頼んだことをするだけなんだから早くしてほしいな。


セキュアヴェイル

もちろん、ご依頼いただいてから迅速に実施するのが一番理想的ですし、不可能ではありません。NetStare には緊急・時間指定オプションというものもご用意しております。つまり、できるだけ安く、品質の維持されたサービスをしようと思うと標準サービスでは2営業日必要となってしまうのです。


お客様

品質の維持…って…
こちらが頼んだものをそのままやってくれたらいいんだよ？なんで品質が関係あるの？


セキュアヴェイル

弊社の実施する設定変更はご依頼頂いたものをそのまま設定するというものではなく、例えばご依頼のFirewallポリシーを追加することで全体のポリシーに矛盾が生じないかどうか、


セキュアヴェイル

お客様が本当に望んだネットワーク環境になるかどうか。というものを精査し、実装するようにしております。そのため、少しお時間をいただいております。


お客様

そうなんだね。それは有難いな。
でも例えば緊急で防御したい攻撃があるのに「2営業日かかる」と言われたら、オプション料金を払っていないにせよ実際困るなあ。それを標準のサービス内容にしているというのは、問題じゃないの？


セキュアヴェイル

いえ、IPS のチューニングに関してはおっしゃる通り緊急性がありますので、即日対応させていただいています。こちらは4時間以内に対応するというのが標準サービス内容です。


お客様

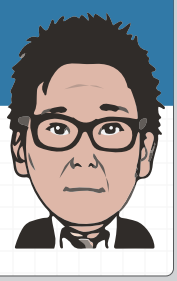
なるほどね～！これなら緊急で実施してほしい不正アクセスに対して迅速に対応できるし、きちんと精査してほしい Firewall ポリシーに対しても良い品質のものが提供されて安心だね。

記事担当：ぐりこ

プロが教える Firewall の設定

Firewall は、ハッカーまたは悪意のあるソフトウェア（ワームなど）がネットワークやインターネットを経由してコンピューターにアクセスするのを防ぐために役立ちます。また、Firewall を使用して、自分のコンピューターが他のコンピューターに悪意のあるソフトウェアを送信しないようにすることもできます。
今回のセミナーではプロから観た Firewall の設定プロセスと評価をお話いたします。

セミナー情報
Monthly column 13



予定講師：卒区次郎

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

大阪本社
〒533-0044　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 /・クラウドサービス『NetStare Suite』
・McAfee NSP 運用サービス

www.secuavail.com