SecuAvail

［セキュアヴェイルニュース］

SECUAVAIL NEWS

セキュリティ運用監視サービスを提供しているセキュアヴェイルがお届けする
情報セキュリティの指針となるコンテンツ満載のフリーペーパー

2017
リニューアル特別号

「運用」

この言葉が持つ本質的な意味を徹底解剖！

- 作業代行と本来の「運用サービス」は別モノ!…混同するなかれ!
- セキュリティ対策機器の落とし穴
- 事例から学ぶ ー 出口対策における「運用」の重要性

CONTENTS 01

セキュリティマネジメントサービスの歩み その1

2001年、運用サービスをスタート！

2016年1月、セキュリティマネジメントサービス「NetStare」のVer.8をセキュアヴェイルよりリリースしました。このコーナーでは、私たちのサービスの誕生からこれまでの歩みを世の中のセキュリティ動向とあわせてみていきたいと思います。

セキュリティは作ったときから陳腐化が始まる

2001年、インターネットの利用が当たり前になり、セキュリティ対策の1つとして企業にファイアウォールの導入が広まってきました。ファイアウォールはネットワーク環境、組織の体制、利用しているアプリケーション等に合わせて設定変更が必要となります。導入して終わりではなく、都度見直していかなければなりません。「セキュリティは作ったときから陳腐化が始まる」ため、そうならないためには“運用”が必要不可欠なのです。

「NetStare」誕生！

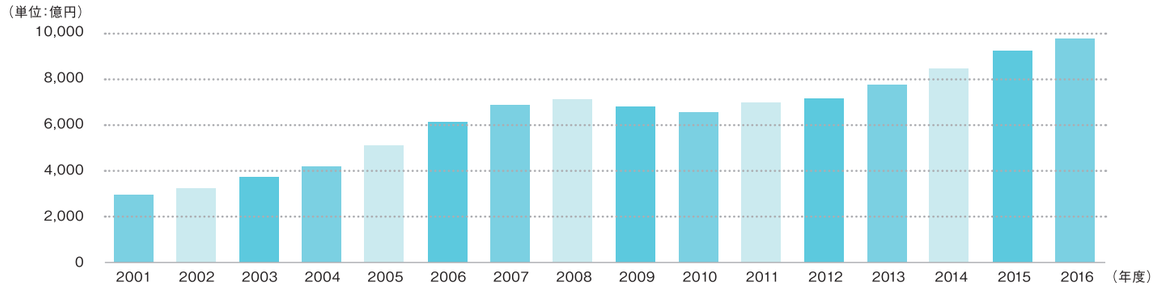
では、“運用”とは何をしたらよいのか?専門性が高い上にそのための体制を構築するのはお客様にとって大変負荷を要する内容です。そこでセキュアヴェイルは、お客様の代わりに「お客様がやるべきこと」をサービスとして提供し始めました。

しかし会社設立当時は24時間365日の運用体制を最初から作ることは難しく、まずは平日9:00-17:00の対応を行い、それ以外の時間はシステム的な監視として予め取り決めた閾値や条件でアラートを出すというサービスからスタートいたしました。

また、商用のツールを購入してサービスをすることも経済的に厳しい状況だったため、監視システムもログ分析システムも自社で作成していく計画で「NetStare」の提供が始まりました。

それまでなかったサービスを立ち上げたため経験者もいませんし、セキュリティシステムに精通した人材もほとんどいない時代でした。それでも、お客様から求められるニーズはとても高いサービス内容でした。そのため、ここから「NetStare」は弊社のポテンシャルを最大限に発揮して急速な勢いで成長していくことになります。

2001年 ～ 2015年のセキュリティ市場の成長グラフ



※2001年度～2002年度は、当社推定の値
※2003年度以降は、JNSA調査研究部会「2015年度 国内情報セキュリティ市場調査速報」資料を参考にした値
（2015年度は見込値・2016年度は予測値）

CONTENTS 02

Secupedia 今号のテーマをセキュアヴェイルが表現すると…

情報セキュリティの「運用」ってどういうこと？

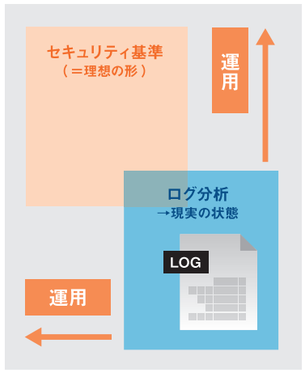
＜Wikipedia＞

主にコンピュータ上で稼動し、さまざまなサービスを提供しているシステムが停止することなく、利用顧客に対してつつがなくサービスを提供できるよう当該環境を維持管理すること。

＜Secupedia＞

稼働状態を「可視化」すること。

運用とはシステムまたは機器の持つ機能をうまく働かせて本来の目的に対する結果を得ることである。目的に対して現状の立ち位置がどこにあるのか把握することが必須となり、それをすることが「可視化」である。これを実現するにはログを取得し分析しなければならない。ログがあるが故に定量的かつ客観的にシステムが機能しているか（目的に合致しているか）把握できる。これを繰り返し実施していくことが「運用」である。



東京オフィス移転いたしました。

株式会社セキュアヴェイルは、10月3日より業務拡大に伴い東京オフィスを築地の聖路加タワーへ移転いたしました。新オフィスは築地駅にほど近く、よりアクティブなサービス活動の拠点として、お客様へのより一層サービスの向上を図り、信頼されるセキュリティパートナーとして邁進します。皆様のネットワークセキュリティのセキュアな環境を維持サポートするコンピテンスセンターをはじめ、景観のよいセミナー会場もご用意いたしました。是非、皆様のお越しをお待ちしております。

こだわりのデザインを施したエントランス

聖路加タワービル40階

景観のよいセミナールームを完備

様々なネットワーク機器を検証し万全の体制でお客様をサポートするコンピテンスセンター

CONTENTS 03

Security Newsを斬る!

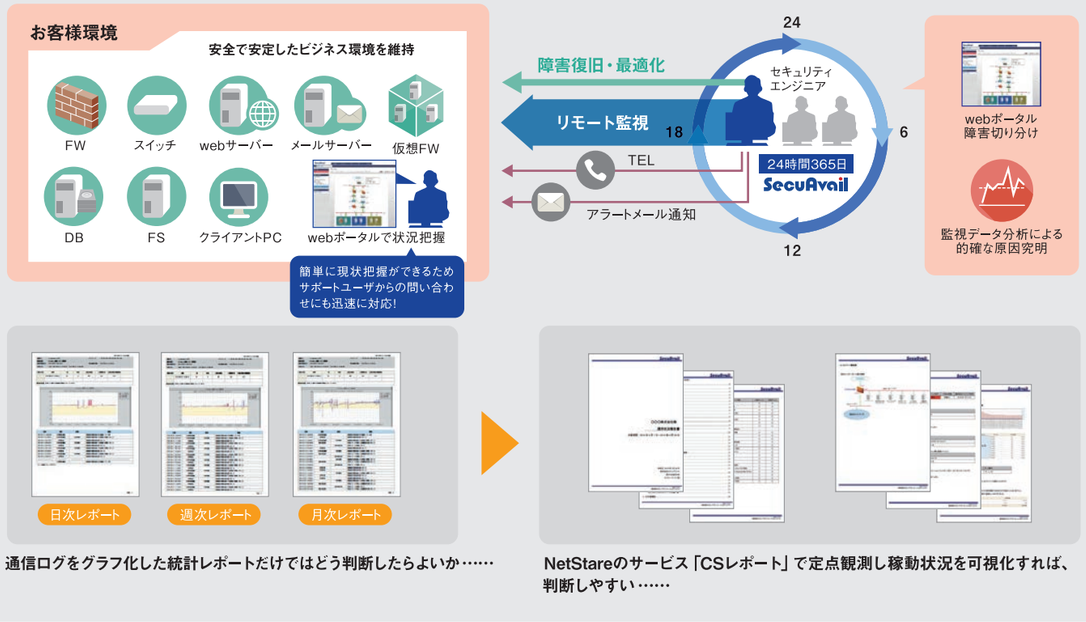
作業代行と本来の「運用サービス」は別モノ!… 混同するなかれ!

セキュリティ運用サービスを検索すると、各社一様に同じようなサービスメニューが並ぶ。セキュリティ機器の監視、設定変更、脆弱性診断…等々…システム管理者の負担を軽減することがメリットだと謳われているものが多い。確かにシステム管理者が動かす手の代わりとなるのであれば負担軽減になるだろう。ただ、これが「運用サービス」であるとするならば違和感を禁じ得ない。

セキュリティ対策の運用とは、ポリシーに則ったシステムの利用状況になっているかを把握し乖離があればそれを是正し、新たな脅威発見時にポリシーの改善や見直しをする。つまり、利用実態とポリシーを合致させるようにすること(乖離を正しく認識することも含めて)である。機器の監視や設定変更はシステムを最適(適切な)状態で稼働させるための作業であり、運用の一要素だが、「運用サービス」というには不十分だ。内容からすると、システム管理者の代わりにオペレーション(作業)を実行する「作業代行サービス」と表現する方が現実に近い。

「運用サービス」の本質とは、設定変更や監視だけではなく、通信状況などを含めた現実の稼働状態を可視化(ログ分析)し、ポリシーと乖離した状態になっていた場合には、その原因と対策を提示するなど、システム管理者が気付いてないであろうことを提供する。現行システムから将来の脆弱性を予見し対策案の提示とともに検討を促すなど、複数顧客の運用経験と実績から得たノウハウでシステム管理者に「気付き」を与え、適切な判断につなげる。これがシステム管理者の求める支援のカタチではないだろうか。

通信ログをグラフ化した統計レポートだけで可視化されてもシステム管理者はどうすべきか判断に困るであろう…それに比べ、定点観測と、複数顧客の運用実績からくる相対的な観測レポートは顧客にとって価値の高いものとなるのは間違いない。これがあれば、システム管理者に専門知識や経験がなくても、適切な(専門家の視点で)判断ができるようになる。NetStareでは「CSレポート」という呼称にて、各顧客にエンジニアが定期的に稼働状況を可視化して報告するサービスメニューが存在する。NetStareはサービスという無形物を一部、有形物として提供する「運用サービス」です。



通信ログをグラフ化した統計レポートだけではどう判断したらよいか……

NetStareのサービス「CSレポート」で定点観測し稼動状況を可視化すれば、判断しやすい……

CONTENTS 04

セキュリティエンジニアが語る!

～セキュリティ機器の落とし穴～

お客様環境へセキュリティ機器を導入後、一部クライアントにおいてインターネットへの通信が不通になるという事象が発生しました。

セキュリティ機器の導入後に問題が発生していたことからセキュリティ機器の設定に問題があることは明白でした。

原因特定のためお客様に詳細をヒアリングした結果、通信不可となっているクライアントが特殊な通信経路(非対称ルーティング)を取っていることが判明しました。セキュリティ機器はセッション管理を厳格に行っており、セキュリティレベルの向上を目的として導入をしていますが、非対称ルーティングなど特殊な通信経路をとっている場合は既存のネットワーク構成に十分注意した上で導入を行う必要があります。もしくは、ネットワーク機器を増設された場合にも同じようなトラブルが発生するリスクがあるため、通信経路自体を最適化した上で、セキュリティ機器を導入することが望ましいでしょう。

機器の特性や環境によるトラブルを起こさないためにも導入の目的やネットワーク構成を把握した上で導入を行いましょう。

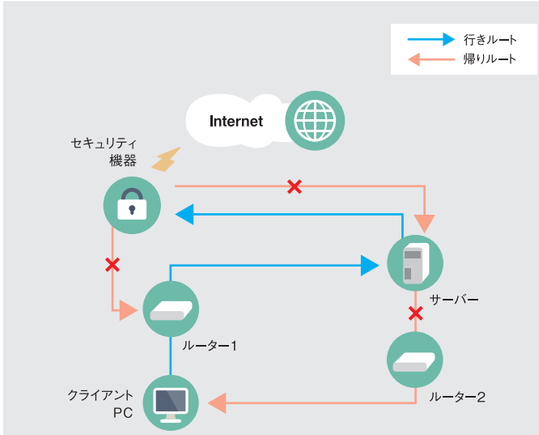


図1 非対称ルーティングの通信経路により通信不通の事象発生

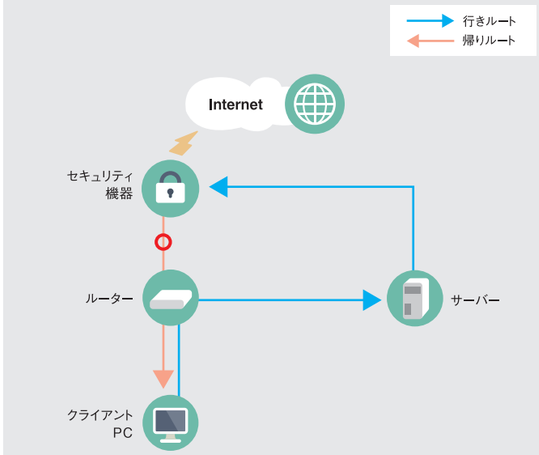


図2 通信経路が最適化され通信が開通

また、機器の選定についても、注意が必要です。例えば、UTM(統合脅威管理)では、その機器の特性上、複数のセキュリティ対策がUTMに集約されています。もしそのUTMに脆弱性があった場合、そこを攻撃されると防ぎようがないというデメリットがあるため、UTMの導入には実績のある信頼性の高いベンダーを慎重に選ぶ必要があります。

社内システムと外部とを行き来する情報はすべてUTMを経由しますので、社内システムが大規模になればなるほど、UTMにかかる負荷は非常に大きくなります。UTMは多くのセキュリティ機能を搭載しているため、個別のセキュリティ機器を複数導入しなくとも、統合管理できるメリットはありますが、複数機能を搭載しているために負荷が大きくなると通信速度が低下する可能性があるため、UTMの導入にあたっては十分な時間あたりの処理能力を持つなど、機器の性能も考慮し製品を選定することが重要となります。

CONTENTS 05

事例から学ぶ〔Case1〕－出口対策における運用の重要性－

～ログ分析による現状の把握と備え～

公共性の高い事業を展開しているA社に、外部に「不正アクセスをしている」との通報が外部機関より入った。それに伴い、万全を期したセキュリティ対策ができるまで社内からインターネットへのアクセスを停止するよう求められ、1,500台の端末で業務に支障が出る状態となってしまった。

原因調査を行ったところ、A社に入り込んだマルウェアが、A社システムを踏み台にし、他団体のシステムに不正アクセスを試みていたことがわかった。しかし、どのような経路でマルウェアに感染し、どのような通信を外部に行っていたのか把握することができず、対応する上で困難を極めた。

セキュリティ機器を導入していても適切なログ管理をしていなかったため、どのような通信が行われていたかを調査することができなかったのである。

そこで対策として、現在稼働中のセキュリティ機器の運用を見直した。

IPSの運用を行う中で、危険度が低いシグネチャやP2P通信の利用等はすぐに遮断は行わず、管理者が確認できるよう検知状態でとどめておく設定が多い。しかし、これらの通信を予め遮断設定にし、社内から業務外の通信を外に出さないようにすることで強固な出口対策を実施した。

導入の際には業務通信の誤検知をなくすために、ログをモニタリングし業務通信の利用状況を分析することで適切な設定を行った。

もし、誤遮断が発生した場合にはすぐに設定変更を実施する体制作りも行っている。

また、毎月定例会を実施し、ログから通信状況を分析する事で、不審な傾向があれば業務内容に合った適切な設定変更を実施している。

このような対策をもし以前から実施できていたならば、前述のマルウェア潜伏中に外部に行っていた通信や実影響が出始めた通信のログを確認することで迅速な対処ができただろう。更にいえば、そもそもマルウェアが侵入する経路自体を発見し、侵入そのものを防げたのかもしれない。

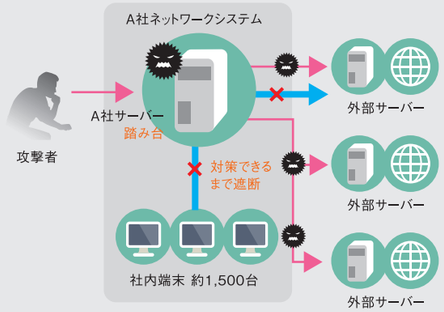


図3 マルウェアがA社システムを踏み台に

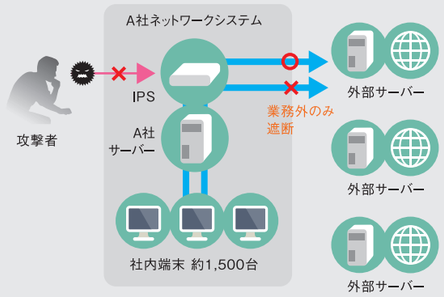


図4 IPSで遮断設定して運用

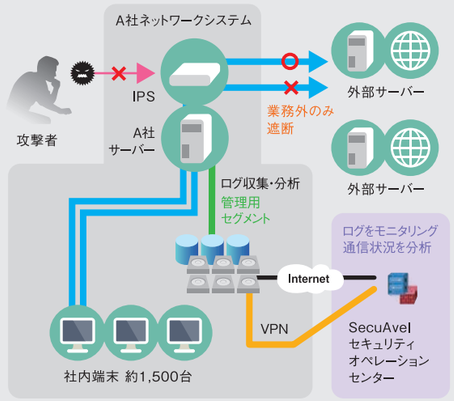


図5 ログをモニタリングして通信状況を分析

CONTENTS 06

情報セキュリティ通信

2016年1-12月 危険度の高いイベントと予防対策

2016年を通しての危険度が高いイベントの上位には「Webサーバ経由のSQLインジェクション攻撃」「PHPの脆弱性を狙ったインジェクション攻撃」そして「China Chopper Webshell通信の検知」がランクインしています。China Chopper Webshellは、Webサイトに設置する中国製のリモート操作ツール(Webshell)で、社内システムの情報を狙う攻撃が増加している可能性を示唆しています。

一昨年、2015年通年で1位となった「bashの脆弱性(ShellShock)を狙った攻撃」は順位を落としましたが、それでも4位にランクインしており、重要度もCritialと、引き続き注意が必要です。

また、同じく一昨年、猛威を振るったOpenSSLを狙った攻撃は、昨年に比べて減少してきていますが、依然としてトップ10に名前を連ねています。

月別検知件数の推移を見ると、8月が突出して多く、その後は減少していますが、これは2015年も同じ傾向でした。(2015年は7月が突出) 引き続き、2017年へ向けての傾向を注視し、新たな攻撃に備える必要があります。

今後の傾向と対策

2016年は企業の内部情報を狙った攻撃が目立ちました。昨年末にIPAが発表した「情報セキュリティ10大脅威 2016」でも、組織にとっての脅威の1位は「標的型攻撃による情報流出」であるとのことです。

標的型攻撃に対抗するためには、IPS 製品の導入だけで無く、導入後の運用をどのように行うかが重要になります。

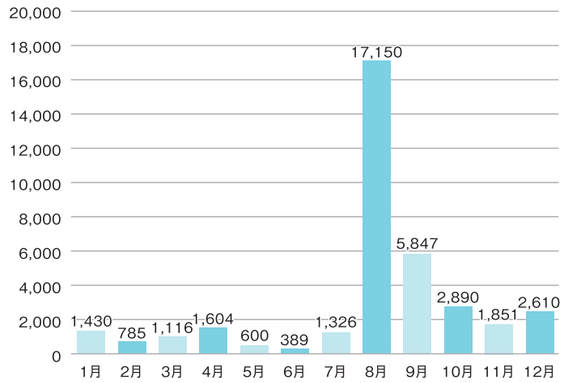
NetStare では攻撃検知の連絡だけでなく、攻撃内容及びその攻撃がお客様環境へ影響を及ぼす可能性があるのかを判断し、適切な対策を提案しております。

「IPS 脅威検知件数集計（2016年1月～12月）**」**

順位	検知した脅威の内容
1位	Webサーバ経由のSQLインジェクション攻撃
2位	PHPの脆弱性を狙ったインジェクション攻撃
3位	China Choppe(webshell)を利用するWebサーバを狙った攻撃
4位	Bash(ShellShock)の脆弱性を狙った攻撃
5位	AWStatsプラグインの脆弱性を狙った攻撃
6位	Joomla! の脆弱性を狙ったコード攻撃
7位	PHP-CGIの脆弱性を狙ったインジェクション攻撃
8位	Apache Strutsの脆弱性を狙った攻撃
9位	OpenSSLのバッファオーバーフロー脆弱性を狙った攻撃
10位	OpenSSLのHeartBreed脆弱性を狙った攻撃

＊重要度Critical、High、Medium

「月別検知件数の推移」（2016年1月～2016年12月）



＊重要度Criticalのみ

セキュリティ対策ガイド

セキュリティ10大脅威第1位「ランサムウェア」とは？

お客様：最近「ランサムウェア」ってよく聞くんだけどどういうものなの？

SA：ランサムウェアとは、感染したPCやデータを使用不能にして、その復旧の代償に「身代金」を要求する不正プログラムです。「身代金要求型不正プログラム」とも呼ばれています。

お客様：そういうプログラムってほとんど個人ユーザが標的になるんでしょ？

SA：当初はそうでしたが、近年では法人ユーザの被害件数も右肩上がりです。2015年は前年比で約7倍近く被害件数が増えています。

お客様：えぇ～、法人ユーザでも標的になってしまうんだ…。でも、どうして感染してしまうの？

SA：ウイルスやマルウェアと同様に、スパムメールの添付ファイル開封や Webサイトの閲覧から意図せずファイルダウンロードしてしまうことが主な感染経路です。

お客様：メールの添付ファイルは開かないように社内でも教育しているけど、Webサイトの閲覧なんて…

SA：怪しいサイトへのアクセスを制御することが理想です。ただし100%制御することはなかなか難しいため、ファイルダウンロードをしている端末を早期に発見することが大切です。

お客様：ふ～ん。でもどうやって発見すればいいの？

SA：ファイアウォールログやクライアントログをモニタリングしてファイルダウンロードがあればアラートを飛ばすように予め条件を設定しておくことで、すぐに気がつくことができます。

お客様：なるほど!100%防ごうってことばかりに目を向けるのではなく、何かあったときに適切かつ迅速に動けるようにしておくことが大事なんだね。

コラム［成長する…］

2017年4月に17名の仲間が増える。「自分を成長させることができる会社で働きたい」という学生は多いのだが、成長するってどういうこと?と、問うと曖昧な答えが返ってくる。成長という言葉は向上心があり“ヤル気”をアピールできる言葉と認識しているからであろか。社長は、自分ではなく会社を成長させたいと言う。果たしてこの両者の「成長」の意味に違いがあるのだろうか。一般的には生物や物事が大きく発達することを意味すると思われるが、会社の成長は売上、従業員数など大きさを客観視できる指標があり成長の姿はイメージできる。新入社員のその姿とは…?身長が伸びることでも太ることでもなく、自分の判断で完結する業務量(範囲)が増えること。これが成長を意味するのではなかろうか。入社時は自分で決めてできることはほとんどなく、上司や先輩に聞いてやっと完結する。経験を重ね次第に聞かずともできることが増え成果が出た。成長を実感する時である。自分で決めてできる…この理想とも言える環境を作るために創意工夫をする。その延長に成長がある。売上規模が大きいと市場影響力も持ち、更なる成長を招く。成長企業の言うことが正しいと認識される。セキュリティ対策の成長企業はどこか?どのベンダーのセキュリティアプローチが正しいのか。それを見極めて適切な判断ができるように、自分を成長させなければ自らがセキュリティホールに落ちてしまうかもしれない…

SecuAvail

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

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
〒104-0044　東京都中央区明石町8−1
聖路加タワー40階
TEL:03-6264-7180　FAX：03-6824-7181

発行日 2017.1.18