なるほど～ NetStare

～監視間隔ってどうやって決めているの？？～

お客様

セキュアヴェイルでは監視の間隔を５分としているって聞いたけれど、５分だと障害に気がつくまでに時間がかかってしまうような気がするなぁ・・もっと短くすることはできないの？

SA 

そうですね、NetStare の稼動監視では弊社監視システムから５分に１度 Ping や SNMP を発行し、３回連続して応答がない場合に障害と判断します。
単純に考えると、障害の発生に気づくまでに最大 15 分かかることになります。

お客様

えーーっ！ 15 分も気づかないなら大問題だよ。
やっぱりもっと間隔を短くした方がいいんじゃないかな。

SA 

では、どのくらいの間隔が相応しいと思いますか？

お客様

うーん・・・１分とか？２分とか・・そのくらいかな？
とにかくもっと短いほうがいいと思う。

SA 

なるほど、確かに１分や２分に監視の間隔を縮めたいという相談を受けることはあります。しかし、何分なら正解という明確な答えはなく、皆さん感覚的に仰っているのです。そのため、基準を決めるのは実はとても難しいのです。
セキュアヴェイルでは今までの運用の実績からネットワークへの負荷を考慮して５分という基準を採用しています。

お客様

でも、やっぱり障害には早く気づきたいし・・

SA 

もちろん障害の発生にいち早く気づくことは大切ですし、仰っていることは理解できます。しかし、例えば監視間隔を１分に変更すると、頻繁に連絡が入ることになり本当に障害が発生しているのかを判断することが難しくなるんです。

お客様

監視するだけなのに難しいな・・

SA 

そのために、私たちはお客様のシステムを止めないサービスを提供しています。
Ping や SNMP の監視だけではなくログ監視や分析も 24 時間 365 日行っており、お客様のシステムの異常をすぐに検知できる体制で、システムのダウンを未然に防ぐための運用を行っています。障害を検知したらすぐに連絡をいたしますので、お客様は常に監視している必要はありません。

お客様

なるほど！ NetStare を利用していれば監視の間隔を気にする必要がないんだね。

（甲斐）

コラム

「脆弱性が発見された！自社は大丈夫？」

これは、私が某インターネットプロバイダのネットワーク運用をしていた頃の話です。
当時運用していた Web サーバで重要な脆弱性が発見される事態が起こり、
①攻撃を受けた場合、いつサービスが止まるかわからない
②検証環境はすぐに用意できない
③本番環境にパッチを適用するのはほかの問題が出てくる可能性もあり危険
という状況下での対処を迫られました。
こうした状況に出くわした時に皆さんならどのような対処をされていますか？
当時私が行ったことは、
・「公表されていた脆弱性の内容の徹底調査」
・「攻撃が実際に起こりやすいのか、相当な技術がないと無理なのかの確認」
でした。
結果として、相当な技術が必要という判断に至りました。しかし、特定ポートへアクセスが来た時点で攻撃の判断がつくことから、
・「Firewall で暫定防御を行いながら検証」
・「本番環境へパッチの適用」
という手順で対処し、ことなきを得たことを今でも覚えています。

「脆弱性」という一言に慌てるよりも、その内容（攻撃手法や影響）を正確に知ったうえで、自身が守っている環境の状況を把握して的確な対処を考える、ということが何よりも有効な対策といえると思います。
何より怖いのは脆弱性を放置していることだと思いませんか？

（いっちゃん）

次号予定

情報セキュリティ通信

Security News を斬る！

セキュリティレポート解説！

顧客を知る　事例紹介

なるほど～ NetStare

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

SecuAvail NEWS

SecuAvail
2014/12
Vol.2

Contents

情報セキュリティ通信

IPS が捉えた 10 月の脅威

今年 10 月に弊社 IPS で検知した脅威件数のランキングです。
９月に比べ、全体の検知数が大幅に増加しています。内容を見ていくと、９月後半から世間で話題になった Bash の脆弱性を狙った攻撃が４位、９月は９位だった OpenSSL ハートビート機能の脆弱性を狙った攻撃が６位と７位に入ってきました。OpenSSL の脆弱性を狙った攻撃の検知数は、先月から約７倍の攻撃数でした。TOP10 にランクインしているその他の脅威も、順位は変動していますが軒並み先月と同じような攻撃が検出されています。なお、15 位まで広げて見ていくと、全体的にクライアント端末を狙った攻撃が増えている傾向が見られ、最近ではクライアント端末を狙った攻撃も顕著になっていることがうかがえます。
この状況から、サーバだけでなくクライアント端末を狙った攻撃にも対応策を検討していくことが必要だと言えます。
弊社で運用している UTM 製品は、IPS シグネチャのターゲットをクライアント、サーバという様に使い分けることが出来ます。UTM 製品の導入場所や、通信の方向ごとに IPS シグネチャのポリシーをチューニングすることが可能です。IPS 専用機は、ハードルが高いとうお客様は、是非 UTM 製品の導入をご検討ください。

IPS 脅威検知件数ランキング（2014 年 10 月）

	検知した脅威の内容	影響を受けるシステム	検知件数
1 位	バッファオーバフローの脆弱性を狙った攻撃	Windows 98、Zom-Mail: 1.0.9	231652
2 位	SSLv3 に対する通信検知	SSL v3.0	93399
3 位	Shell Command インジェクション攻撃	Windows NT、95、98、XP、2000、2003、Mac OS X	5071
4 位	Bash の脆弱性（ShellShock）を狙った攻撃	Linux 系 OS 全般	3216
5 位	Web(HTTP) トラフィックへの実行可能コマンド (.EXE) 組み込みを試みる攻撃	Windows NT 4.0、2000	1200
6 位	OpenSSL の脆弱性を狙った攻撃	OPEN SSL	825
7 位	TLS/DTLS ハートビート機能の脆弱性を狙った攻撃	OPEN SSL	763
8 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	Web サーバ全般	539
9 位	MIME 対応電子メールクライアントのバッファオーバーフローの脆弱性を狙った攻撃	Windows 95、98、NT4.0、UNIX OS	536
10 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	Sendmail	428
11 位	メールを介した ZIP ファイル型ウィルス	OS 全般	345
12 位	Conficker ワーム	Windows OS 全般	196
13 位	Microsoft Excel の脆弱性を狙った攻撃	Microsoft Excel	155
14 位	Adobe Reader および Acrobat におけるバッファオーバーフローの脆弱性を狙った攻撃	Adobe Acrobat	120
15 位	RTF ドキュメントに埋め込まれたオブジェクトを使った攻撃	Microsoft Office	117

※ 2014 年 10 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

Security Operation Center 裏話

今回は、機器障害についてのお話です。弊社の Security Operation Center（SOC）ではパートナー様やエンドユーザー様から日々いろいろな問い合わせをいただきます。その中でも一番緊張するのが、障害に関する問合せです。「障害の発生＝お客様のシステムが止まっているのでは？」という懸念が真っ先に考えられるためです。SOC には、迅速な障害要因の切り分けと再発しないための対応策の提示が求められます。
今年発生した障害に関して言えば、機器の交換で問題を解決している件数が例年より多く見受けられます。機器交換の大半がハードディスクに絡んだ故障です。ハードディスクについては経年劣化による障害の発生を避けることが難しいこともあり、弊社のサービスを長くご利用いただいている特定のお客様で、EOL でなくてもハードディスクの寿命を迎えた年だったのかもしれません。
年末年始にかけて作業をされるお客様も多いと思いますが、故障を防ぐことは難しいです。ただし、事前に保守ベンダーに作業予定の旨を伝えておけば、交換作業がスムーズに進むかもしれません。（卒区次郎）

Security News を斬る！

" にわか "SOC に気を付けろ！機能的な SOC を見極める視点！

大規模情報漏洩事件を受けての影響なのか？… 大手 SIer がこぞって Security Operation Center（SOC）を開設している。セキュリティ対策強化にあたって専門業者への外部委託需要は高まる傾向にある。が、しかし…SOC 事業はそれほど簡単にできるのだろうか？…

決して容易ではない SOC 事業の開設と運営

SOC とは、シンプルに定義すると「顧客のネットワークを 24 時間 365 日監視し、必要に応じて機器の設定変更や何らかの攻撃にさらされた時に迅速に対処するサービス」ということになる。専門知識を有する技術要員が監視センターにてその業務に当たるのである。SOC を運営するにあたって必要となるのが、監視サービスを提供する設備である。

冗長化された回線や電源設備、監視ツール、顧客管理システム等々…初期投資額は決して安価とは言えない。また最も重要なのが「要員の確保」である。「24H365D 運用サービスを提供します。」という文言を Web サイトで目にすることは多いものの、実際に 24H365D の要員を常駐させて運用している事業者は少ないのが実態である。

労働基準法などに照らし合わせても、この体制を構築するにあたって必要となる要員は最低でも 8 名は確保しなければいけない。ある程度の顧客数がなければこの事業は成り立たない。

SOC を活用する場合、どんなサービスメニューがあって月額いくらで提供してもらえるか、ということに目が向いてしまいがちだが、サービスメニューの内容と月額の費用を基準に委託先を選定することは正しい選択と言えない。しっかりとした体制が構築されてない SOC へ委託してしまうと、何かとトラブルが絶えないということになりかねない。

「正しく機能する」SOC を選定するポイント

こうした点をふまえると、サービスメニューはもちろん大事ではあるが、ホントに自社にとって役に立つには、正しく機能してくれる SOC を選ぶことが大切である。

正しく機能しているかどうかの基準として外せない重要なポイントは、

①冗長化された設備を有しているか？
② 24H365D 稼働できる要員の体制が構築されているか？
③監視システムと顧客管理のシステムが連動して動く仕組みとなっているか？
④レポート出力が属人的（人依存）ではなく自動化されいるか？
⑤必要なサービスがメニュー化されていて価格が適切か？

この５つである。

10 年以上のノウハウを蓄積して誕生した「 NetStare 」のサービスは、この５つの条件を満たした数少ない SOC から提供されている。（海女若）

" 機能する SOC" の５大条件

1. 冗長化された設備を保有していること
2. 24H365D 稼働できる要員の体制が構築されていること
3. 監視システムと顧客管理システムが連動して動く仕組みであること
4. レポート出力が自動化されていること
5. 必要なサービスがメニュー化されておりその価格が適切であること

顧客を知る　事例紹介

LogStare 事例
～私立大学様（学生数 約 10000 名）～

スピーディなログ検索で不正行為のピンポイント発見と本人注意に効果を発揮。複数の機器が出力するアドレス情報を連携し、アドレス情報の集中管理も実現。

導入前の課題・導入の経緯

既にログ検索システムを導入し、ログの検索や気になるアクセスについては誰がいつどの端末からアクセスしてきたのかを確認できる体制を整備していた。しかし、ログから調査を行うにあたって課題を持った状態で運用を行っていた。

主な課題は、

1．アクセスしている端末と人の特定に時間がかかる点
2．ログの検索スピードが遅い点

であった。

アクセスしている端末と人の特定に時間がかかる要因として、有線と無線の Web 認証システムや DHCP を利用しているシステムなどが混在しており、アクセスしている端末と個人を特定するには複数のレポートからログを追いかける必要があるという点だった。また、ログの検索スピードが遅いため、なかなか欲しい情報が入手できず、ログ検索システムを有効に活用できているとは言えない状態だった。

そんな中、ネットワーク機器やサーバの老朽化でリプレイスを実施することになり、ログ検索システムも見直すことになった。

セキュリティレポート解説！

自社への攻撃準備が進んでいる？編

通りすがりの攻撃か、意図的な攻撃かを見極める

一口に不正アクセス（本来アクセス権を持っていない人がログインできる様にする攻撃）と言っても、「広範囲にわたって無作為に行われている不正アクセス」の場合もあれば、「集中的に狙われている不正アクセス」の場合もあります。

無作為の不正アクセスは、ファイアウォールのルール設定を間違っていなければそれほど問題はありません。

一方、集中的に狙われている場合、ファイアウォール内部への侵入を目的として何者かが意図的に不正アクセスしている可能性が考えられます。ログ件数が多いのに送信元のユニークアドレス数が少ない場合は集中的に狙われている不正アクセスが発生している可能性があります。例えば、ポートスキャニングが行われている場合、一般的には「ログ件数÷送信元ユニークアドレス数」が「10 前後」となりますが、この値を大きく上回る場合が様々な手口でファイアウォール内部への侵入を試みている可能性があります。ログを解析し、どの様なアクセスが発生しているのか見極めていくことがポイントです。

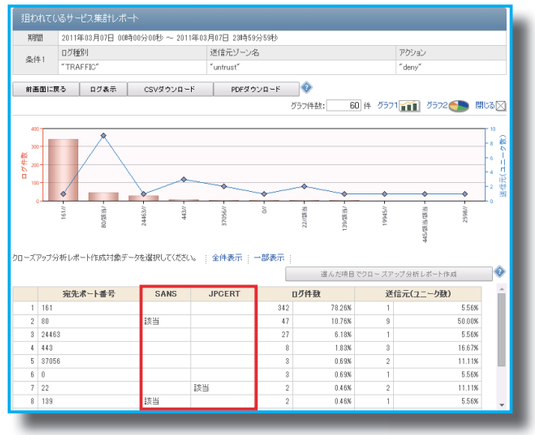
不正アクセスを許してしまった場合のリスク

ウイルスの流し込み、情報漏洩（通信盗聴、データ抜き取り）、データ破壊、機器障害

不正アクセスを許してしまう要因

ファイアウォールのルール設定の不備
（許可すべきでない通信を許可しているなど）

狙われているサービス集計レポート



ファイアウォールの安全基準とそれを維持するための対応策

最も安全なのは、解析結果で 1 件もアクセスが検知されていない場合です。及第点と言えるのが、「SANS」欄と「JPCERT」欄に「該当」と表示されるアクセスのみが検知されていて、このアクセスの「ログ件数÷送信元ユニークアドレス数」が「10 前後」の場合です。安全な状態を維持するには、定期的なファイアウォールのルール見直しをお奨めします。例えば、業務上起こりうる通信とそうでない通信に対するファイアウォールの設定の整合性をチェックし、使用していないポートは閉鎖するなどの対応を行っていきましょう！（ぐり子）

製品決定の決め手

・機器が出力する数種類のログを LogStare サーバに集約させることができ、1 つのレポート画面操作で情報が検索できる点。
・高速でログ検索の処理を行うことができる点。

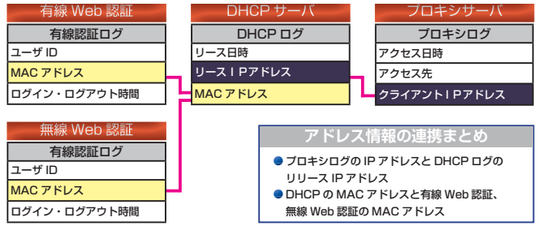
以上を評価いただき、LogStare を導入。

主な運用方法

有事の際にアクセスした人の情報がすぐに確認できる様、複数の機器が出力するアドレス情報を連携させて台帳化。

UTM 機器や LogStare から P2P 通信等のアラートが発生した時は、アラートの発生日時を確認し、LogStare の「ピンポイント分析レポート」で誰がどこにアクセスを行ったのか調査する。LogStare の導入後、P2P ソフトを使用し不正なデータをやり取りしている疑いのある学生に注意を促すことができた。

アドレス情報の連携イメージ

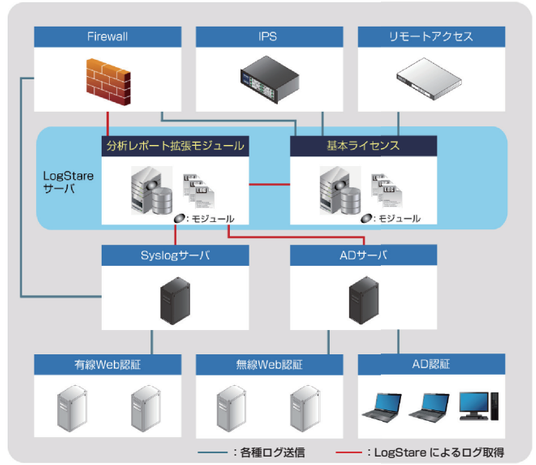


導入製品

製品		導入数
LogStare	基本ライセンス（5 ノード）	1Set
	分析レポート拡張モジュール（5 アプリケーション）	1Set

ライセンス費用：￥3,980,000　保守費用：￥796,000

構成図



（ひき氏）