なるほど～ NetStare

～コールドスタンバイ機も運用サービスの対象なの？？～

お客様

障害に備えてコールドスタンバイ構成にしているけれど、
コールドスタンバイ機に対する運用はしてもらえないの？

SA

NetStare の運用サービスは、アクティブ機だけでなく
コールドスタンバイ機に対しても実施しています。

お客様

そうなんだ。でも、普段ネットワークに接続していない
のに、どうやって運用してくれるの？

SA

コールドスタンバイ機はネットワーク未接続や電源 OFF の状態であるため、ネットワークを経由してのサービス提供はできません。
実施するサービスは、今のファームウェアがどのバージョンかを管理し、いざ機器交換をする時にアクティブ機と差異が発生しないようにするというものです。

お客様

バージョンが違うとダメなの？

SA

機器の設定情報はバージョンが違うと正常に動かないことがあります。
機器交換をした時に、アクティブ機と同じ設定を投入したら全然動かないなんてこともありえます。
そのため、コールドスタンバイ機はアクティブ機と同じバージョンにしておかないと障害復旧にとても時間がかかってしまうのです。

お客様

つまり、アクティブ機をバージョンアップした時にコールドスタンバイ機も一緒にバージョンアップしなくてはいけないってことか・・・

SA

その通りです。バージョンを揃えておくことが、素早い障害復旧のカギです。
メジャーバージョンアップ、マイナーバージョンアップのどちらでも差異は発生しますし、その更新頻度は機種によってまちまちです。それらを管理するのはとても負担がかかるので、私たちが代わりに管理して、コールドスタンバイ機のバージョンアップ作業を行います。
そのため、お客様には定期的にコールドスタンバイ機をネットワークに接続いただくようお願いしています。
設定情報は SOC にて３世代分（現在の設定情報と過去２世代分）保管しているので、バージョンさえ揃っていれば障害復旧までも私たちが行います。

お客様

なるほど！コールドスタンバイ機に必要な運用を任せておけば、”いざ”という時もちゃんと交換できるようになっているから安心だね。

（平沼）

コラム

「便利なクラウド！
ビジネス利用するために欠かせないこと…」

Office365 や Google Apps などのクラウド型のサービスが広まり、低価格で様々なサービスが利用できる昨今、ビジネスシーンでもクラウドサービスの利用検討は珍しくありません。

以前私がメールセキュリティ対策を支援していた頃、「Google Apps をビジネスで利用したい。そのために誤送信メール対策は最低限実施したい」と相談いただいたことがありました。
使い慣れた Outlook から Gmail へとインターフェースが大幅に変わることで、オペレーションミスによる「悪意のない情報漏えい」を発生させてしまうのでは・・・という懸念が浮上し、これを払拭してクラウドサービスを利用したいという趣旨でした。
この時は、設定したキーワードがメール本文にヒットした場合に一時保留させる機能と自己承認機能を利用する方法で、メール環境を変更しました。事前に対策を行っていた甲斐もあり、誤送信は発生していないと伺っています。

プライベートで利用しているサービスが私たちのビジネスシーンでも活用されるようになるなど個人と法人に対するサービスのボーダレス化は進んでいくのではないか。私はそう思います。

クラウドをビジネス利用するにあたって、利便性による効率化や運用も含めたコストメリットを重視しがちですが、忘れてはいけない重要なことがあります。サービスベンダーに依存するセキュリティ対策だけではなく、自社の運用環境にとって必要なセキュリティ対策を自己責任において十分考慮することがクラウドサービスをビジネス利用する上では欠かせないことなのだと思います。

（くるり）

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
2015/1・2
Vol.3

Contents

情報セキュリティ通信

2014 年 11 月の脅威

2014年11月に弊社IPSで検知した脅威件数のランキングです。1位のSSL v3に対する検知数が、378,433件と非常に増加しています。SSL v3 の通信は様々なシステムで広く利用されており、影響を受けるシステムは大多数に上る見込みです。気になる方は情報処理推進機構にて公開されている情報も参照ください。<https://www.ipa.go.jp/security/announce/20141017-ssl.html >
≪参考 URL ≫ 情報処理推進機構ホームページ「SSL 3.0 の脆弱性対策について (CVE-2014-3566)」

2 位の Shell Command インジェクション攻撃は 4,888 件と 2014 年 10 月とほぼ同じ件数を検知しました。主に Windows Server 2003 が対象です。Windows Server 2003 は 2015 年 7 月でサポート終了のため、リプレイスを検討されている方も多いと思います。リプレイス前の Windows Server 2003 に対しては、パッチ適用 / バージョンアップ / 設定変更などで Shell Command インジェクション攻撃を回避しましょう。3 位は Bash の脆弱性 (ShellShock) を狙った攻撃で、1,936 件と先月に比べ件数はやや減少しています。しかし、Bash や ShellShock という単語が有名になることで一部の WEB サイトで攻撃手法の情報を入手できる様になるなど、状況は決してよくありません。上記脅威に対しては、IPS を設置して正しく運用することで大幅にリスクを回避できます。
IPS の運用が負担という場合は、弊社営業担当にご相談下さい。

IPS 脅威検知件数ランキング（2014 年 11 月）

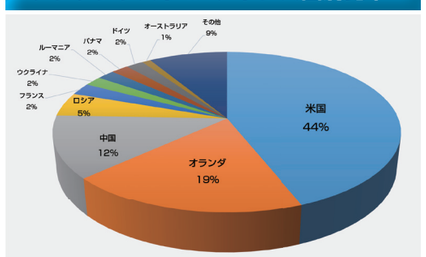
	検知した脅威の内容	影響を受けるシステム	検知件数
1 位	SSLv3 に対する通信検知	SSL v3.0	378,433
2 位	Shell Command インジェクション攻撃	Windows NT、95、98、XP、2000、2003、Mac OS X	4,888
3 位	Bash の脆弱性（ShellShock）を狙った攻撃	Linux 系 OS 全般	1,936
4 位	Web(HTTP) トラフィックへの実行可能コマンド (.EXE) 組み込みを試みる攻撃	Windows NT 4.0、2000	1,400
5 位	URL 内の「ドット ドット」(/../) シーケンスの脆弱性を狙った攻撃	Web サーバ全般	626
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	Sendmail	464
7 位	TLS/DTLS ハートビート機能の脆弱性を狙った攻撃	Open SSL	375
8 位	MIME 対応電子メールクライアントに対して過度に長いファイル名で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	346
9 位	OpenSSL の脆弱性を狙った攻撃	Open SSL	336
10 位	MIME 対応電子メールクライアントに対して過度に長いヘッダーでバッファオーバーフローの脆弱性を狙った攻撃	Zom-Mail: 1.0.9	260

※ 2014 年 11 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

注意喚起を目的に、不正アクセスの送信元として利用されている IP アドレスを公表しているセキュリティ機関があります。
弊社では、こうした国内外のセキュリティ機関の情報や弊社サービスをご利用のお客様に対する不正アクセスの検知実績を基にして、不正アクセスの送信元 IP アドレスブラックリストを作成しています。
右図は、2014 年 7 月から 9 月に弊社の対象機器で検知 / 防御した不正と思われる IP アドレスを、国別に集計したものです。
日本の国内に設置しているシステムが外国からアクセスされることは稀であるため、セキュリティ機関から注意が促されている IP アドレスからの通信は遮断した方がより高度なセキュリティを維持することができます。
弊社のサービスをお申込いただければ、３ヶ月に１回、ブラックリストからの通信を遮断するようセキュリティエンジニアがチューニングいたします。
セキュリティ維持のために、ブラックリストブロックサービスも是非ご利用ください。（Mr.160）

ブラックリスト IP アドレス国別比率



※ 2014 年 7 月～ 9 月の弊社運用監視サービスでの検知・防御結果

Security News を斬る！

氾濫する「運用サービス」…「運用」とは何をすることなのか？

運用サービスを開始した。というニュースを目にすることは少なくない…しかし、「運用レポート」と称して提供されるレポーティングサービスの多くは通信ログを集計してグラフ化しただけで、このサービスに不満を唱える顧客もまた少なくない…「運用サービス」とは何を提供することで顧客に価値をもたらすのか…その定義を考察する。

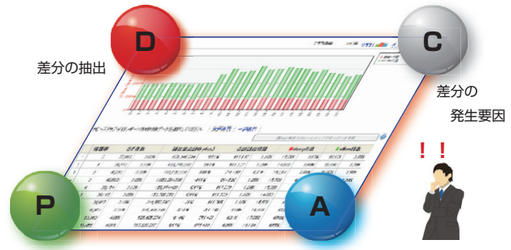
「セキュリティマネジメント（運用）」に必要な要素

IT インフラを運用するには、①監視、②管理、③制御の３つの要素で構成する必要がある。
監視とは、本来の稼働とは違う状態になったら瞬時に検知できること。
管理とは、現状の不備を本来の稼働に戻す（近づける）または、不正を防止するための行為。
制御とは不正を排除する仕組。
と定義付けられる。この３つの要素を機能させるために必要なのが通信等の稼働ログである。このログを可視化したものが運用レポートである。

「運用レポート」の価値は“気付き”を与えること

ログを統計的にグラフ化するだけではただ単に現象の表現に留まり、それを見ても何も判断ができない。このようなレポートを月次運用サービスの成果物として顧客に提示するサポートベンダーが少なからず存在する。その運用レポート？とは顧客にどんな価値をもたらすのか？…疑問を禁じ得ない。
運用レポートのベースになるのはログ管理である。ログ管理はある一定の基準が必要であり、その基準値と現状の差分を抽出し、差分が生じた要因を特定し改善に繋げることが基本である。
だからこそ、運用レポートも「一定の基準」、「差分抽出」、「差分の発生要因」、「改善手法（案）」の４つの視点がなければ顧客は何も判断ができない。顧客に判断を促す…“気付き”を与える、チェック機能が働く…それが価値ある「運用レポート」である。これは、セキュリティマネジメントサイクルの”PDCA”と同じことである。
「一定の基準」は経験値や専門知識から蓄積されたノウハウに他ならない。このノウハウを多く蓄積しているのがセキュリティマネージドサービスの専門ベンダーであり運用を委託する顧客の価値になる。（海女若）

価値ある「運用レポート」に必要な４つの視点



セキュリティレポート解説！

ファイアウォールの ルールを見直そう!! 編

ファイアウォールのリプレイスが発生するケースと課題

企業の合併や新サービスの開始に伴い社員やサーバ数が増加、その影響でトラフィックが慢性的に上昇する状況が発生し、既存のファイアウォールを上位の機種へリプレイスする必要性に迫られている企業が少なくありません。しかし、ファイアウォールのリプレイスには予算の確保をはじめ、機器の選定や利用者への告知など計画から移行が完了するまでに多くの時間がかかってしまいます。
トラフィックの上昇によるファイアウォールのリプレイスを実施する前に、既存のファイアウォールのルールを見直してみてはいかかでしょうか。

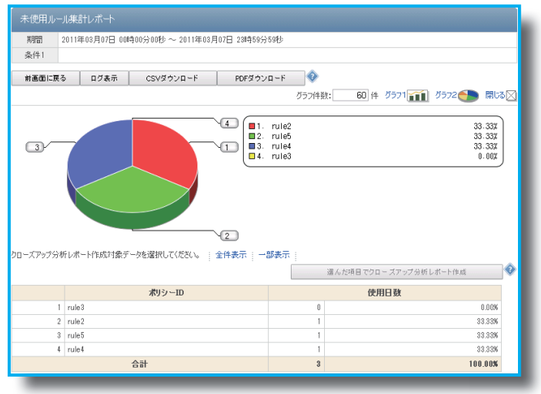
ファイアウォールのルール設定を放置した場合の影響

ファイアウォールの導入後、ルールの追加を繰り返して使用しなくなったルールを残したままにしておくと、数百行ものルールが残った状態になることがあります。
ファイアウォールは、通信が流れる際に上位に設定されているルールから順番に処理を行います。そのため、不要なルールが上位にたくさん残っていると、ファイアウォールの使用率が上がりパフォーマンスを低下させてしまいます。

ファイアウォールのルール設定を見直す

未使用ルールのレポートをチェックし、使用頻度が少ないルールを下位に配置したり削除するなどしてルールを整理しましょう。ただし、単純な使用頻度順による並べ替えは、場合によって通信ができなくなってしまうことがあるため注意が必要です。
弊社のサービスでは、お客様からご依頼をいただいた場合に２営業日以降で設定変更を実施しております。こうしたサービスもご利用いただき、リプレイスの前に最適なファイアウォール環境を整備してみませんか。
上位機種へのリプレイスは事業を拡大するためには避けられない問題です。ですが、ルールの整理によって既存のファイアウォールのパフォーマンスが改善できれば、使用期間を延ばすことができます。既存のファイアウォールを少しでも快適な環境で使用し、延ばすことができた期間を利用してリプレイスのための予算確保や機器選定などの計画を検討してはいかがでしょうか。（てくさん）

未使用ルール集計レポート



顧客を知る　事例紹介

LogStare 事例 ～小売書店様（従業員数 約４０００名）～

**ログの一括管理と特権 ID ユーザのログイン情報を「見える化」し情報漏洩対策を推進。
現状把握にかかる工数削減、特権 ID ユーザの正当性の証明と不審な行動の抑止に貢献。**

導入前の課題・導入の経緯

全国に書店を展開しており、店舗でのPOS管理、クレジットカードの決裁システム、書籍のネット販売など多様なシステムを利用している。その各システムが機密性の高い情報を持っている。機密性の高い情報に対する利用状況を管理するためにサーバ毎にログを保管している。しかし、サーバ毎にログを確認する必要があるため、効率よくログの中身を確認できているとはいえなかった。またこのシステムを管理するために、一部従業員とMSP 事業者にはあらゆるシステムへログインできる権限を持つ「特権 ID」を付与しており、個人情報保護のためにも彼らのログイン履歴を管理していく必要があった。
こうした背景から、以下の様なセキュリティ対策を実施していくことが決定した。

1. システム毎に保管しているログの情報を効率良く一括管理すること。
2. 特権 ID ユーザのアクセスログを見える化して情報漏洩対策を行うこと。

そこで、MSP 事業者から紹介を受けて弊社の LogStare を提案し、導入いただいた。

製品決定の決め手

- Windows OS や Linux OS などサーバ OS が混在している環境でもログを一元的に管理できる点。
- メールサーバや Web サーバなど、企業でよく導入されるアプリケーションはもちろん、独自開発したアプリケーションのログも収集・分析できるなど自社のシステム環境にマッチしている点。

導入製品

製品		導入数
LogStare	基本ライセンス（40 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：￥4,380,000　保守費用：￥876,000

主な運用方法

２ヶ月に１回、システム担当者が特権 ID ユーザのログインログを LogStare で確認。
LogStare から CSV データでログを抽出して自社フォーマットの報告書を作成し、経営陣の会議の場でセキュリティ上の問題があったかどうかを定期的に報告。

導入効果

- １つの Web ポータルで対象システムのセキュリティ状態を確認できるようになり、報告書作成にかける工数が削減できた。
- ログから特権 ID ユーザのログイン情報を見える化して管理していることを周知し、不正利用の抑止につながっている。

（まえあし）

構成図と活用イメージ