なるほど～ NetStare

～定期レポートを見ると何が分かるの？？～

お客様

問題を検知すると、いつも対応してもらっているけど…定期的にレポートも配信されてくるんだよね～。どうして、定期レポートという形態で配信しているの？

SA 

定期的にレポートを配信している理由は２つあります。
１つは、現在の運用状態をお客様にお伝えするため。
もう１つは、どのような攻撃が多いか、通信状況から社員の不審と思われる動きがないかなど障害の予兆をお伝えするためです。
お客様のなかにはこれらの内容をまとめ、自社での定期報告に利用されているケースもあるんです。

お客様

そうなんだ。
具体的にはどんなレポートが配信されるの？

SA 

そうですね～、例えば、「P2P 通信」や「不審なファイアウォールアクセス」などがありますが、どのレポートも、セキュリティ対策上、特に気付いていただきたいことを月次と週次で配信しています。

お客様

気付きかぁ。。。例えばどんなことが分かるの？

SA 

例えば「P2P 通信」のレポートでは未許可の P2P ソフトが使用されていないか簡単にチェックできたり、「不審なファイアウォールアクセス」のレポートに大量のアクセス失敗情報が出力されていた場合は、ブルートフォースアタック等で管理者権限を奪取しようとしている可能性なんかを読み取ることができます。

お客様

へぇ～。でもレポートから不審な動きが読み取れても、その影響範囲や対応方法を知っていなければ何をしたらいいか分からないしなぁ。。。

SA 

そんな時は、迷わず弊社のヘルプデスクにお問い合わせください！
レポートの見方や、お客様環境への影響や最適な対策案などを分かりやすくご案内しています。

お客様

おおーっ！定期レポートとヘルプデスクを使えば、日々の運用をセキュアヴェイルに任せながら、社内で報告する場合に知っておきたい問題の影響範囲や対策の情報も集めることができるね。
これなら運用の負担も報告用の情報を整理する負担も減らせる！！
なるほど、レポートって貴重な情報が分かるんだね。

（てくさん）

コラム

「ログから正しい意思決定をするために」

ログ調査という言葉を耳にすると、ファイアウォール運用サービスを古くから提供しているお客様を思い出します。
３ 年ほど前のことです。当時、著名な企業への不正アクセスが頻繁化しておりサービスダウンまで追い込まれた事例を耳にされ、なるべく早く新型機への移行を完了させたいという背景でした。
そんなある日、「外部からの DoS 攻撃でシステムがダウンした」との通報を受けました。
SOC ですぐにセキュリティエンジニアがログ調査を開始しました。ほどなく判明した調査結果は、「外部からの通信量は通常とほぼ変わらない。従って、通信量を圧迫する DoS 攻撃を受けた可能性は低い」との結論でした。さらに調査を進めた結果、「サーバで予期せぬバージョンアップ処理が実行され、一時的にサービスが停止した瞬間があった」ということが判明しました。大事には至らずほっとしたと同時に、ログ調査の意義を実感しました。もしこの時ログ分析ができない環境下であれば、適切な判断ができず間違った対応を取っていたかもしれません。
何かあった時のために…と、ログ収集されているお客様は多数ありますが、重要なことはログが蓄積されているかどうかはもとより、ログを詳しく調査し分析する体制があるかどうかです。
正しい意思決定を行うためには的確な現状把握が必須です。現象に反応すると判断を誤るおそれがあります。ログという客観事実を元に、調査、分析した結果によって最終的に人が判断や意思決定を下す。そのような体制があってこそ、活きたログ調査になると考えます。ログは収集するシステム（ツール）と調査する体制との融合によって存在価値が見出せるのです。
（Mr.160）

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
2015/3
Vol.4

Contents

情報セキュリティ通信

脅威の動向と今月の裏話

昨年 12 月に弊社 IPS で検知した脅威件数のランキングです。
11 月に引き続き、SSL v3 に対する通信の検知数が群を抜いています。自社システムで利用されていないか今一度、確認しましょう。
危険度が高い通信の検知総数は 11 月と比べて 10 万件近く減少しましたが、Windows や Sendmail など広く一般的に使われているシステムを標的とした攻撃が増加傾向にあります。日々発生する脅威への対策として、自社環境にセキュリティホールが潜在していないか診断することは今や企業にとって必須の課題です。弊社でも「セキュリティ診断」のサービスをご用意しております。
「セキュリティ診断」は保護対象となるサーバやネットワーク機器に対してアタックシミュレーション（仮想的なサイバー攻撃）を実施し、現状のシステムに潜在する脆弱性を可視化し有効な対策手段をレポートするサービスです。
システム更改前に診断を行うことで、アプリケーションのバージョンを最適化した状態でのリプレイスが可能となります。また、半年ごとに定期的な診断を行うことで、今必要とされるセキュリティ対策の優先度を決定する指標として有効利用できます。
「システムの健康診断」による現状把握が適切な対策と投資を導くためには欠かせない取り組みです。
自社システムの健康状態が気になるお客様は、弊社担当営業までお声かけください。

IPS 脅威検知件数ランキング（2014 年 12 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	276,784
2 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	5,225
3 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 95、98、NT4.0、XP、2000、2003、Mac OS X	1,000
4 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	546
5 位	TLS/DTLS ハートビート機能の脆弱性を狙った攻撃	Open SSL	503
6 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	458
7 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	430
8 位	Conficker ワーム	Windows OS 全般	179
9 位	リモートから Web サーバ上で任意のコマンドの実行を試みる攻撃	listrec.pl: 1.0	126
10 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	103

※ 2014 年 12 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

今回の裏話は、弊社サービスで評価が高いログの活用術です。Security Operation Center（SOC）では毎月数千件発生するインシデント対応や、機器の設定変更、お問い合わせへの対応など様々な運用業務を行っています。創業当初より 24 時間 365 日の運用を続けていますが、技術要員によるサービス品質のギャップが出ない運用業務を確立するために、まず客観的な事実である『ログ』を取得し現状を把握することから始めました。自社開発の運用基盤システムで検知したインシデントへの対応履歴（ログ）を自社開発の統合ログ管理ツール「LogStare」で月次レポートとして出力しています。また、お問い合わせ対応や機器の検証など運用基盤システムの管理範囲外となる業務はタスク登録を行うシステムを活用し、そのシステムのオペレーションログを抽出し同様に月次レポートで出力しています。このレポートで可視化された客観的な業務実態と本来提供するべきサービスとの差異や品質上の問題がないかを分析し業務改善を行っています。
例えば、インシデントやお問い合わせが集中する平日の昼間への監視担当者増員やスキルの高い技術要員を配置するための判断材料の１つとして活用しています。ログから得られる定量化された稼働状況があるからこそ技術要員の最適配置という運用体系が構築されます。この運用体系がお客様へ提供するサービス品質向上へとつながっていきます。
ログは単にシステムの稼働状況や障害原因特定のみならず、活用の視点を変えると、『人の動き』まで把握し、業務効率改善やサービスレベルの維持・向上にも寄与するという実践的な事例の１つとしてご紹介しました。　（まえあし）

Security News を斬る！

自社 SOC と SIEM 製品でセキュリティ対策強化は実現するか？ 期待が膨らむ「理想」と厳しい「現実」…

大手企業が自社内に SOC を立ち上げて SIEM（Security Information and Event Management）を導入する動きが増えている、そんな情報を多く耳にするようになった。しかし、SIEM を有効活用し対策効果があったという声を耳にすることは少ない・・・そこにある理想と現実のギャップとは何か…運用視点から考察する。

SIEM 製品で取得する「ログ」とは

SIEM とは、ネットワーク機器やアプリケーションから得られる膨大なログを集約し、インシデント発生時に管理者に通知したりその対策方法を知らせるなど、セキュリティ情報を俯瞰して管理できる手法のことである。インシデントを迅速に把握し対応できることから、大手企業を中心に SIEM 製品の導入が広がりつつある。

SIEM 製品で集約するログは、主に「インシデントログ」、「ログインログ」、「OS イベントログ」であり、それぞれのログを俯瞰的視点で関連付けることで適切な対策手段が導き出される。インシデントとログをマッチングさせるという分析手法で活用できるかどうかが SIEM 製品導入効果へ大きく影響を与えることになる。しかしながら、現実に運用するとなると、この関連付け（俯瞰的に分析する視点）が難しい…とされ、SIEM 製品の導入効果が発揮されているという事例を耳にすることが少ないのである。

SIEM 製品…導入後そのまま使えるケースは実は少ない

SIEM 製品によっては関連付けのテンプレートが複数用意されている。しかしながら、顧客環境は千差万別である。複数のテンプレートが用意されているとはいえ、多種多様なセキュリティ製品やネットワーク機器の組合せに応じた実用的なテンプレートが実装されていることはごく稀であり、実際に活用するとなれば何らかの手を加えて調整する必要がある。立ち上げ間もない SOC の要員とノウハウでは自社環境に応じたテンプレートを構成することが運用上の大きな障壁となり、結果として、SIEM 製品本来の機能を活用するに至らず、単にログを集めるだけのツールと化す。

導入効果を発揮するためには、「ログ」をアセスメントできるシステム管理者がいるか、運用をサポートしてくれる専門のセキュリティベンダーの存在が不可欠となる。「運用をサポートする」というのは、インシデント発生時にスポット的に対応することではなく、日々インシデントの状況を把握して予防処置の提案ができ、対応の要否への適切な判断を与えることである。

SIEM 製品は導入してもなかなか有効活用ができない…。といわれているが、導入がゴールとならないよう、運用面は専門のベンダーに委託し、ノウハウを蓄積した上で自社運用に切り替えるというステップを描きながら導入を計画することが SIEM 製品の有効活用への近道となるであろうと考える。

（いっちゃん）

SIEM 製品導入成功のカギ

いきなり自社で運用するのではなく、導入時は運用面を専門のベンダーに委託し、ノウハウを蓄積しながら自社運用に切り替えていくこと

セキュリティレポート解説！ 大量通信は情報漏洩の兆候？編

大量通信は情報漏洩の原因の１つ

情報漏洩の８割が内部要因といわれていますが、昨年世間を騒がせた個人情報漏洩事件も内部からの不正行為によるものでした。内部からの情報漏洩は、システム運用者や役職者などが特権 ID を利用した不正アクセスが多く、正常に業務を行っているのか個人情報や機密データを盗み出しているのかを判別するのはなかなか困難です。

盗み出されたデータが社外に出ると情報漏洩となるわけですが、社外に出たことを気付ける仕組みを用意しておくことが被害を最小限に抑えることにつながります。

その１つに「大量通信」を検知することが挙げられます。

個人情報や機密データなどを大量に外部送信すると、通常とは異なる大きなサイズの通信が発生します。ファイアウォールを通過する通信はログとして出力されるため、この通信ログを解析し、「大量通信」の痕跡を見つけることがポイントとなります。

大量通信を許してしまった場合のリスク

・情報漏洩（内部犯もしくはマルウェアによるデータ抜き取り）
・通信帯域の圧迫

大量通信を許してしまう要因

・大量通信の制御ができていない
・大量通信を検知する仕組みがない

大量通信を発見するポイント

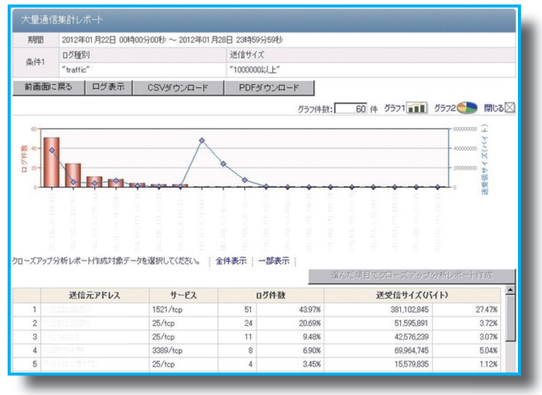
「大量通信集計レポート」は、設定した閾値（初期値 10MB）以上の送信サイズとなった通信を抽出し、その通信の送信元 IP アドレスを一覧で表示することができるレポートです。

最も安全なのは大量通信が１件も検知されず、「大量通信集計レポート」が出力されないことです。レポートが出力された場合は、行動を確認してみましょう。

送信元 IP アドレスの情報から端末や利用者を割り出し、なぜその端末から大量通信が発生したかを本人に確認することですばやい原因究明につながります。結果的に問題が発生していなかったとしても「おやっ？」と思ったら本人に確認する様にし、組織にチェック行為を浸透させて抑止効果を狙っていくことも大切です。このレポートは、システム管理者が不在となる夜間帯や休日も該当する通信が発生した場合に自動的に出力されるため、盲点となる部分も事後でチェックできます。また、退職が決まっている利用者の行為も注視すべき対象だといえます。

（平沼）

大量通信集計レポート



顧客を知る　事例紹介　LogStare 事例 ～データセンター事業者様～（従業員数 約 90 名）～

「受け身」のログから、「能動的かつ戦略的」なログへの活用転換！ 豊富なサマリーレポートが運用体系に合致！それが導入の決め手に！そして今は・・・

導入前の課題・導入の経緯

導入いただいた企業はデータセンター事業者で、物流事業を営む親会社と製薬業界向けに EDI システム（※）のサービスを提供している。このサービスは利用する企業の中に VPN 装置を設置し、データセンターとはインターネット VPN で接続することが利用要件となっている。

EDI システムの運用面を考慮し安全な接続方式である VPN を採用したのだが、サービス事業者としてその接続の安全性を担保する必要があった。

判断材料の１つとして、不審なアクセスの有無を把握することが重要な管理視点であると認定し VPN 装置に対するアクセスログから不審または不正な行為がないかを抽出、分析し定期報告する運用体系が決定した。そのアクセスログ取得及び分析ツールとして LogStare を導入することになった。

※ EDI：「Electronic Data Interchange」の略で 「電子データ交換」を意味する。注文書や請求書などの商取引のデータを、紙ベースではなく、ネットワークで取引先と自社のコンピュータをつないで電子データで送受信すること。

製品決定の決め手となった３つのメリット

・エージェントレスのため低コスト導入ができる！
・エージェントに依存しない機構が拡張性を担保する！
・レポート作成コストをほぼゼロにできる！（自動化による）

以上を評価いただき、LogStare を導入。

主な運用方法

アクセスログの分析結果（LogStare から出力されるレポート）は親会社への月次報告で提出。設定変更があった際は、都度レポートを確認し影響範囲を判定。FTP で LAN セグメントから Internet への通信が大量に発生していることを検知した場合は、クローズアップ分析機能を活用し原因調査。

レポートから問題を発見した場合は、月１回の定期メンテナンス日に設定変更等を実施して対策。そして今は…プロキシサーバとして利用している BlueCoat のログ分析も実施する方向となり活用範囲が拡大化される方針が決定した。

導入後の効果

アクセスログの分析ツールとして LogStare を導入したが、導入時よりも分析対象が増加し、業務分析による課題をレポートするツールとして戦略的な活用にまで踏み込んでいけたことが想定を超えた効果だといえる。

例えば、Web 閲覧状況把握のために基本サマリーレポートでレポートする。また、コンテナ管理や配車システムなどの商用系 Web システムに対しても 30 種類の基本サマリレポートで物流業界の幅広い受発注システムの利用状況を可視化できたことで、業務課題がより具体的に見えるようになった。

見えてなかったものが明らかになることで、より適切に分析できる様になったことも効果としては大きい。

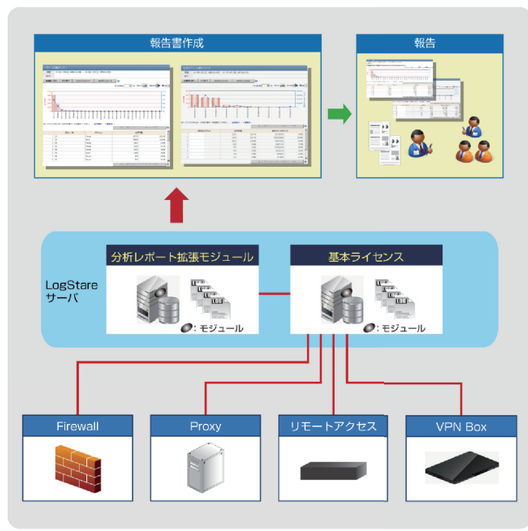
ログやレポートがここまで活用できるとは驚きであった。

導入製品

製品		導入数
LogStare	基本ライセンス（100 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：￥4,980,000　保守費用：￥996,000

運用イメージ図



（くるり）