Empowered by Innovation NEC

RSA enVision™ powered by Express5800 導入事例

株式会社ゴルフダイジェスト・オンライン 様

SQLインジェクション攻撃を契機に統合ログ管理システムを導入
157万人もの会員数を誇るWebサイトの見える化を実現

ゴルフに関する様々なサービスをインターネット経由で提供することにより、日本のゴルフ人口の拡大に貢献するゴルフダイジェスト・オンライン様。同社では、ピーク時のアクセス負荷にも対応できるWebサイトの運営を実現し、悪意のある攻撃を未然に予防する目的から、NECの提供する統合ログ管理ツール「RSA enVision™ powered by Express5800」を導入しました。これにより、散在していたログを迅速に解析できるようになり、Webサーバへのアクセス負荷の把握や不審なアクセスの見える化を実現。システム障害やセキュリティ事故を未然に予防できる基盤が整いました。

株式会社ゴルフダイジェスト・
オンライン
システム部　部長
渡辺 信之 氏

GDO GOLF DIGEST ONLINE

社　　名：株式会社ゴルフダイジェスト・オンライン
所 在 地：東京都港区虎ノ門三丁目4番8号
設　　立：2000年5月1日
資 本 金：824百万円（2009年12月31日現在）
従業員数：354名（2009年12月31日現在）
　　※臨時雇用者数含
事業概要：「新しいゴルフスタイルを創造、提供し、あらゆるゴルファーの満足の最大化実現を目指す」ことをモットーに、インターネットを軸とした「ゴルフ場サービス事業」「ゴルフ用品Eコマース事業」「ゴルフメディア事業」の3つのコア・ビジネスを展開。国内外のゴルフ場予約サービスやゴルフの上達のための情報が満載のWebサイトは、業界有数のポータルサイトとして、ゴルフ愛好家の高い評価を獲得している。

Webサーバにかかる負荷の把握に加えて、リスクマネジメントの強化が急務に

石川 遼選手や若手女子ゴルファーの活躍で、人気が再燃する国内のゴルフ市場。その活性化に貢献している企業が、株式会社ゴルフダイジェスト・オンラインです。約157万人※1もの会員が登録している同社のWebサイトは、ゴルフの基礎知識の提供をはじめ、ゴルフ用品の販売、ゴルフ場の予約、スコア管理など、ゴルフライフを楽しむための多彩なコンテンツで成り立っています。

「Webサイトへのアクセスは、月間1.5億ページビュー。平日のお昼休み、特に、12：45～13：00の15分間にアクセスのピークタイムを迎えます。息抜きで閲覧したり、週末のゴルフ場の予約に利用されたりする方が多いようです」と説明するのは、同社システム部の部長 渡辺 信之氏。人気のWebサイトだからこそ、Webサーバに想定以上の負荷がかかり、システム障害などでサービス停止に陥れば、ユーザに多大な迷惑をかけることになります。「最悪の事態を招かないためにも、Webサーバのログを解析し、どこに負荷がかかっているかをきちんと把握した上で、最適な対策を打ちたいと考えていました。しかし、各サーバのログはバラバラに保存されており、解析自体が困難な状態であったため、サーバの増設で乗り切っていたのが実情でした」と渡辺氏は打ち明けます。

そうした中、2008年9月、同社のWebサイトが、SQLインジェクション攻撃の被害に遭いました。二次被害の拡大を防ぐため、同社ではビジネスの柱であるWebサイトを10日間閉鎖するという決定を下しました。

「この事故を契機に、個人情報保護やISMS、Pマークの認証取得を見据えた、部門横断型のリスク統括室を発足させるとともに、業務プロセスの見直しや再発防止に向けたWebアプリケーションの改修を実施しました。ログの統合管理は、ユーザのアクセス集中によるシステムダウンを未然に防ぐ増強整備計画の一環に加え、悪意のある攻撃の予兆を見抜くセキュリティ上の予防的措置という側面からも急務となったのです」と渡辺氏は語ります。

（※1）2010年1月現在

導入の容易さ、ログの圧縮保存率の高さが選定の決め手に

もともとWebサーバの負荷を把握するために、ログの保存を行っていた同社ですが、各Webサーバのログをバラバラに保存していたため、どこにアクセスの負荷がかかっているか解析することが困難でした。「ログのデータ量はサーバ1台につき、1時間あたり平均2GB。現状、Webサーバは20台稼働しており、1時間で平均40GBに

達します。容量の大きいファイルは分割した上で抽出していましたが、転送には少なくとも数時間かかっていました。SQLインジェクション攻撃を受けた際は、攻撃の手口や被害の影響範囲を把握するために、ログの解析をセキュリティベンダーに依頼しましたが、数十GBのログをコピーするだけで1日以上を費やしました」と渡辺氏は振り返ります。

散在する膨大なWebサーバのログを統合管理するツールとして、同社が「RSA enVision™ powered by Express5800」を選定した決め手は大きく2つありました。1つ目は、短期間に導入できるアプライアンス製品であること。2つ目は、ログの圧縮保存率と検索性能の高さです。ログの保存に多くのストレージを割けば、その分の物理的なスペースが必要になる上、検索速度も低下します。その点、「RSA enVision™ powered by Express5800」なら、こうした課題をクリアすることができると判断されたのです。

ハードウェアの信頼性や耐久性も重視されました。「24時間365日、ログを収集するわけですから、サーバには堅牢性が欠かせませんし、万一の時に利用できるフルサポートも必須です。RSAセキュリティ社のソフトウェアにNECのハードウェア、それぞれの得意分野で高いブランドバリューを持つベンダーの組み合わせに安心感がありました。また、本製品を導入していたユーザの多くが、知名度の高い企業・団体であったことも、評価のポイントとなりました」と渡辺氏。

ログの高圧縮保存により、アーカイブに要する時間は大幅に短縮化

こうした経緯を経て、統合ログ管理システムは無事に導入されました。現在では、Webサーバ20台のログを自動的に収集・保存しています。「Webサーバ以外にも、ログを収集・解析したい対象はたくさんありますが、優先順位の最も高いWebサーバのログ管理に、まずは適用しました。そのおかげで、アクセスのピーク時にあわせた柔軟なシステム構成を組めるようになりました」と渡辺氏は手応えを示します。

導入したモデル「ES-7560」のEPS（1秒間あたりのイベント処理件数）は7500件。「ピークタイムのイベント数は、ほぼEPSの仕様上限に収まっています。会員数の増加にともなって、アクセスログは統合ログ管理システムの導入前よりも増えていますが、高圧縮が可能なので、アーカイブに要する時間は短縮され、スムーズに解析できるようになりました」と渡辺氏。また、従来はログの保存に高価なSANストレージを用いていましたが、それも別の用途に活用できるようになりました。

何度もWebサイトにアクセスしてくる怪しいクローラーを簡単に見つけられるようになったことも大きな成果です。「従来は、HTTPリクエストのパケットキャプチャなどから、SQLインジェクションやXSS（クロスサイトスクリプティング）などで使われる不正な文字列を探し出すため、エディタソフトのgrep機能※2を使って段階的に絞り込んでいたので、格段の差です」と渡辺氏。Webサーバの脆弱性が潜んでいる箇所に見当をつけることができれば、Webサイトの改修ポイントも見つけやすくなります。大きな事故に発展する前に、未然に予防できる基盤が、こうして構築されました。

（※2）grep機能：複数のファイルから、特定の文字列を含んだ行をすべて調べる事ができる機能のこと

Webサイトの利便性向上や、従業員の生産性向上にも活用したい

「ログを1行1行見ていくことは、事実上不可能です。しかし、現在の統合ログ管理環境の整備によって、こちらが設定した条件に抵触する不審なアクセスだけが見える仕組みが手に入りました」と渡辺氏は評価します。

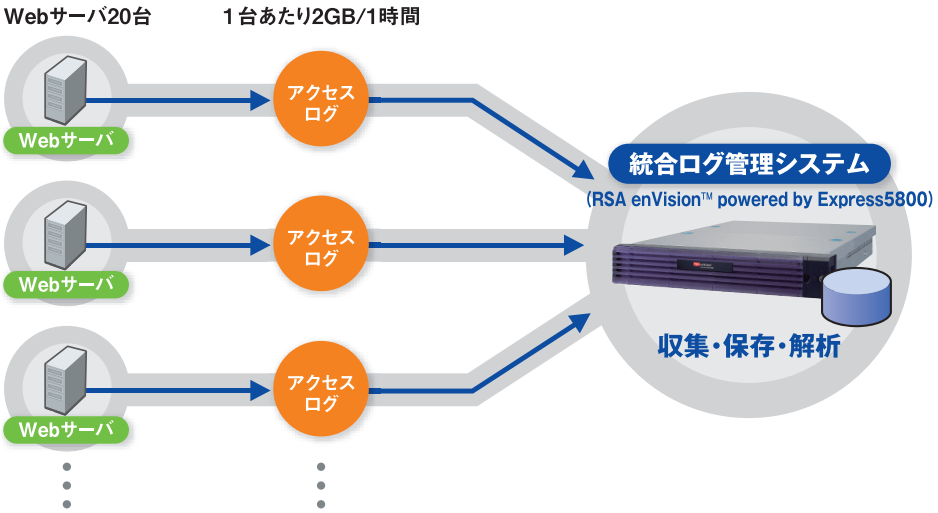
セキュリティ面に加えて、Webサーバへのアクセスログも見える化され、耐システム障害性やWebサイトの表示レスポンス向上によるユーザビリティの改善にもつながっています。

「ユーザから“動作が重い”と指摘されるコンテンツをリストアップすることで、Webシステムの障害予防という守りに加えて、利便性向上によるユーザの獲得という攻めの戦略にログを活用したいと考えています」と渡辺氏。

同社では、Webサーバのログを統合的に管理するだけでなく、社内システムのログについても見える化することを検討しています。具体的には、PCの操作ログを管理し、社内にログ管理を行っていることを告知することで、心理面での不正抑止効果やセキュリティ意識の向上に役立てていく考えです。

「さらには、従業員の生産性向上のためにもログを活用したいです。業務プロセスごとの処理時間などを見える化することで、BPR（Business Process Reengineering）を行うツールになると考えています」と渡辺氏。このように、業務改革をはじめ、渡辺氏の考えの中には、次の構想が大きく膨らんでいるようです。

● ゴルフダイジェスト・オンライン様の導入システムイメージ



お問い合わせは、下記へ
ファーストコンタクトセンター　TEL 03-3455-5800

【受付時間】9：00～12：00　13：00～17：00　月曜日～金曜日（祝日を除く）
番号はよくお確かめの上おかけください。

日本電気株式会社　〒108-8001 東京都港区芝五丁目7-1（NEC本社ビル）
2010年3月現在
Cat.No. E01-10040177J