



## InCharge Institute、F5 Application Security Managerを使いリスク管理戦略をサポート

「F5のApplication Security Managerは弊社のリスク管理モデルの要です。このような高度なトラフィック提供を可能にする技術はF5の他にありません。F5のASMは素晴らしい製品です。」

InCharge Institute (フロリダ州オーランド)  
VP of IT and Information Security  
Mark Nagiel 氏

### 業界

個人向けの金融教育およびクレジット・カウンセリング

### 課題

- ポート 80 とポート 443 の未監視という従来からのリスク
- システム内の機密データのセキュリティと保護
- 社内開発/サードパーティのアプリケーションとの統合の課題

### ソリューション

F5 BIG-IP® Application Security Manager

### 導入効果

- リスク管理能力の向上
- DMZ に関する洞察と知識の獲得
- トラフィックの種類とリスクの理解

### 概要

フロリダ州オーランドに本拠を置くInCharge® Institute of America (以下InCharge Institute)は、個人向けの金融教育およびクレジット・カウンセリングを専門に行う全米規模の非営利コミュニティ組織です。同組織の傘下には以下のような複数の事業体が存在します。

- Brightscore.com では、調査機関が提供する最新情報をクライアントが監視/入手できるようになっています。
- InCharge Educational ファウンデーションでは、全米の消費者のファイナンシャル・リテラシー・ニーズをサポートする教育製品/サービスを提供しています。
- InCharge Debt Solutions は、専門家による極秘のクレジット・カウンセリング、債務管理、金融教育プログラムを提供します。
- InCharge ラジオネットワークは、400 近くの市場で金融教育プログラムを放送しています。

これらの組織は連携して、経済的に困窮した家庭や個人が負債を返済し、責任あるクレジットの利用法について学べるよう支援を行っています。

InCharge Institute では、金融機関として顧客およびその財務記録の機密性を厳格に保護しており、積極的なリスク管理プログラムの導入が欠かせない要件となっています。

### 課題

IT and Information Security の Vice President である Mark Nagiel 氏は、従来のネットワークや Web 環境から、バックエンド/フロントエンドのサポート、ビジネス継続性、社内/サードパーティのソフトウェア開発まで、InCharge Institute の IT の監督を一手に引き受けています。また、総勢 50 人の IT スタッフが働いています。

InCharge Institute では、成熟した情報システム・アーキテクチャと共に、社内で開発した

いくつかのキーアプリケーションを持っています。プライマリ・アプリケーションの「Freedom」は Web ベースのモデルであり、個人のカウンセリングの処理/サポート、および顧客とのやりとりを可能にします。

InCharge Institute にとって、顧客の機密データの保護は重要な課題です。「弊社では総合的なアプローチをとっており、プレゼンテーション層、クライアントへの SSL 接続、バックエンドのデータベースへの SSL 接続でのセキュリティ基準を提供しています。システムの周辺を社内保護する必要があるのです」と Nagiel 氏は述べています。リスクの種類としては、クロスサイト・スクリプティング、クッキーの改ざん、SQL/OS インジェクション、および HTTP (ポート 80) インターフェイスが未監視のままという従来からのリスクなどがあげられます。

Nagiel 氏が InCharge Institute の職員になってまず行ったことは IT 環境の監査でした。標準ポート 80 と HTTPS (ポート 443 の SSL/TLS) のトラフィックはオープンな状態であり、セキュリティを高める必要がありました。「製品を選択するにあたり、綿密な分析を行いました。弊社ではアプリケーションを社内開発しているため、IT とセキュリティの両方をカバーすることが課題となってきます」と Nagiel 氏は説明します。

Nagiel 氏はまたこうも言います。「リスク管理能力を強化する必要があると取締役会に提案したところ、緊急ニーズとして取り上げてくれました。InCharge Institute では大規模な個人ポートフォリオを所有しており、この資産を保護することは弊社の責務です」

### ソリューション

Nagiel 氏はほかの組織にいるときから F5 の BIG-IP ソリューションを利用していただけから、InCharge Institute のリスク管理プログラムを強化するソリューションを探す際に、BIG-IP Application Security Manager (ASM) を候補に加えることにしました。





F5のASMは、Webアプリケーションと運用インフラストラクチャを包括的に保護します。BIG-IP ASMではアプリケーション・デリバリー・セキュリティの自動適用アプローチを採用しており、観測されるトラフィックパターンに基づきセキュリティポリシーが自動で更新されるようになっています。このシンプルな設定アプローチによって導入と保守が容易になり、総所有コストが削減されます。BIG-IP ASMはBIG-IPの製品モジュールとして提供されていますが、InCharge Instituteのケースのようにスタンドアロン・アプライアンスとして導入することも可能です。

「F5のASMによって、リスク管理モデルを完成させるためのニーズを満たすことができました。同ソリューションは適応性に優れており、長期にわたって利用可能なことが分かります。今回のプロジェクトによってセキュリティ・インフラストラクチャのループを閉じることが可能になることから、経営陣と取締役会はこのミッションに対して大変協力的です」とNagiel氏は言います。

ASMは、InCharge Instituteがトラフィックの種類とリスクについて理解することを可能にします。「ASMはDMZに関する洞察と知識を与えてくれるだけでなく、コードの適切な記述法を教えてくれるツールでもあります」とNagiel氏は言います。アプリケーション・ファイアウォールはInCharge Instituteの必須要件の1つです。「これは、環境を制御するための一般的かつ基本的な方法の1つです。今後、プロセスにセキュリティが組み込まれることになるでしょう。なぜなら、ますます多くの組織が、それによってリスク管理が強化されることに気づき始めているからです」とNagiel氏は説明します。

Nagiel氏は、ASMのことを、開発段階にあるセキュリティへの移行を支援するツールだと考えています。「開発ではセキュリティよりも機能性に重点が置かれるものだと思われています。セキュリティを重視するように開発者を再教育することは容易ではありません」とNagiel氏は言います。ASMファイアウォールは、短・長期のセキュリティ管理を支援します。「弊社では、開発と品質保証の両方の要素にセキュリティチェックを組み込むようにしています」とNagiel氏は説明します。

InCharge Instituteは米国のすべての州で事業を展開していますが、規制は州によって異なり、規制自体が存在しないケースもあります。「私たちのプロセスは、さまざまな州の規制に対応する非常に効率的なものとなっています。たとえばニューヨーク州では、弊社は銀行と同じカテゴリに分類されます。したがって、大手銀行の場合と同じようにプロセスの監査と確認が行われます。ASMによって、弊社が規制に対応できることを示しやすくなります」とNagiel氏は説明します。

ASMを導入するのにかかる日数は、オーダーを受けてから45日となっています(トレーニングを含む)。Nagiel氏はこう言います。「弊社には非常に優秀なITクルーが揃っていますが、あえてF5に出向してもらい、アドバイスと指導を受けることにしました。これは大変有益な経験であり、社員の知識を増やすよい機会となりました。F5のサポートは群を抜いており、フォローアップも充実しています」。Nagiel氏によると、ソリューションの導入が第2、第3のサイトへと広がるにつれ、統合プロセスはさらに容易になっていっているということです。「簡単になる一方です。機能を理解しているため、より効率的に対処できます。これはどこにでもあるアプリケーションではありません。私たちが求めていたのは堅牢な

ソリューションですから。ですが、初期投資はすでに回収することができました」とNagiel氏は言います。

要件について言えば、InCharge Instituteでは暗号化とモニタリングの標準を定めています。「クレジットカードとWebサイトに関しては、標準がベストプラクティスとなっているため、それらに従うことにしています」とNagiel氏は言います。InCharge Instituteの環境は信用調査所によって毎年監査されています。「1年目はDMZとIAS環境の調査に時間がかかりました。ですが、前回、ASMを導入した後の監査ではそこに時間が割かれることはありませんでした。あらゆる脆弱性がカバーされているとの判断が下がったようです」とNagiel氏は説明します。

Nagiel氏によると、ROIの特定は容易ではないとのこと。「弊社のリスクの捉え方はごくシンプルです。インシデントの発生ほど高くつくものはないと考えています。リスクが最小限に抑えられれば、ASMの購入と保守にかかる金額などわずかなものです。ポート80とポート443の特性をそのままに、このような水準のトラフィックを実現できる技術はありません」

周辺とバックエンドを強化することが不可欠だ、とNagiel氏は断言します。「これをやっていないということは、注意を怠っているにほかなりません。ポート80とポート443を無防備なまま放置することは決してあってはならないのです。私は自分が『ベルトとサスペンダーを使う男』だということを認めます。つまり、リスクを避けたいのです。それだけの手間とコストをかける価値はあります。F5のASMは素晴らしい製品です。声を大にしてそう言います」とNagiel氏は述べています。



## F5 ネットワークス ジャパン 株式会社

### 東京本社

〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階  
TEL 03-5114-3210 FAX 03-5114-3201

### 西日本支社

〒530-0001 大阪市北区梅田2-2-2 ヒルトンプラザウエスト オフィスタワー19階  
TEL 06-6225-1250 FAX 06-6225-1111

お問い合わせはF5 First Contactまで：[www.f5networks.co.jp/fc/](http://www.f5networks.co.jp/fc/)

### ● お問い合わせ先