



Symantec社 ProxySGとCitrix NetScalerを併用し インターネット基盤を全面刷新 セキュリティ対策とパフォーマンス改善を同時に実現

Point

- WEBレピュテーションとアンチウイルス強化によるセキュリティレベルの向上
- プロキシのボトルネックが解消しWebアクセスのパフォーマンスが大幅に改善
- ログ抽出時間を短縮しリアルタイムの外部脅威検知が可能に

安全で高品質かつ拡張性の高い インターネット基盤を整備

1965年に部品メーカーの愛知工業と新川工業が合併して誕生したアイシン精機は、50年以上もダイナミックに革新し続ける自動車業界において絶え間ない技術開発で業界をリードし、自動車を構成する要素のほぼ全てをカバーする総合自動車部品メーカーとして発展。常に顧客の期待を超えるソリューションを提供し続けている。

同社は、2011年から運用してきたインターネット基盤の見直しを検討し、2017年3月(2016年度末)を目処に社内メール環境やWebアクセス基盤の全面更改を計画した。その狙いについて、アイシン精機情報システム部 第三開発グループ グループマネージャーの井上 健司氏は次のように説明する。「近年の高度化するサイバー攻撃などへの迅速かつ柔軟な対応や、Office365™に代表されるような高負荷なインターネット上のサービスを全社員が快適に利用できることを前提に、安全で高品質、かつグループ内への展開も容易な拡張性の高いインターネット基盤を整備することが目的でした。」

更改のポイントとしては主に次の3つを重視した。第1はマルウェア対策。同社では、メールや外部媒体経由よりもWeb経由によるエンドポイントでのマルウェア検知数が多く、またプロキシに関連したトラブルも頻発し、フィルタリングがうまく働かなくなるなどの問題もあった。そこで、既存の国産プロキシ(URLフィルター)とゲートウェイ型アンチウイルス製品を刷新することでWeb経由のマルウェア感染を抑えようと考えた。

第2に情報漏えい対策。一般のファイル共有サービスを利用した不正な情報持ち出しや、マルウェア感染により情報をアップロードされる可能性もあり、データが漏えいするリスクを仕組みで制限することを検討した。

第3にネットワークレスポンスの改善。当時のURLフィルターはセッション数に制限があり、アクセスが増えるに従ってプロキシのレスポンスが次第に悪化。社内からは改善を求める要望が相次いで寄せられていたという。

このような要望があった場合、その都度対象となるサイトを確認し、業務上重要なサイトを優先接続できるように振り分ける必要があった。

Symantec社 ProxySGと Citrix NetScalerを併用し 効率的なネットワーク負荷分散を実現

2016年の3月にプロジェクトが本格的に始動。2016年7月にSlerやベンダー 8社に提案依頼をかけ、うち5社から提案を回収し比較検討した結果、同社はSymantec(旧Blue Coat)に注目した。

特に他社プロキシに比べ、1) Webアプリ制御による不正なアップロードの禁止、2) SSLデコードの柔軟な除外設定、3) PACファイル自体をProxyに設定することで、端末側の設定変更の手間を省略。かつ、ポリシーをProxy側で設定できるのでVPN接続などの柔軟な設定が可能 4) 各種認証基盤の柔軟な活用、5) ネットワーク設計の柔軟性、6) 持ち出し端末の厳格かつ柔軟な制御、などの条件が有利だったという。

User Profile



アイシン精機株式会社

所在地：愛知県刈谷市朝日町二丁目1番地
導入時期：2017年3月
URL：http://www.aisin.co.jp/

1965年の創業以来「品質至上」を基本理念とし、自動車業界の発展と共に事業をグローバルに拡大。現在ではドライブトレイン関連製品、ブレーキ及びシャシー関連製品、ボディ関連製品、エンジン関連製品を中心に商品づくりに取り組み、世界屈指の総合自動車部品メーカーとしての地位を確立。また、クルマづくりのノウハウを活かし住生活関連分野やエネルギー関連分野にも事業を展開して豊かな暮らしを支える多彩な商品を提供している。



アイシン精機株式会社
情報システム部
第三開発グループ
グループマネージャー
井上 健司氏



アイシン精機株式会社
情報システム部
第三開発グループ
BCP・セキュリティチーム
大西 裕之氏

アイシン精機 情報システム部 第三開発グループ BCP・セキュリティチーム 大西 裕之氏は、上記に加え、「最近のセキュリティの課題であるSSLなど暗号化通信の中身に対する検知と、ファイル共有サービスなどを使った不正なアップロードの制限などが可能で、細かな制御が統合的に実現できる点も評価しました。」と語る。

アイシン精機は、8月末にSymantecの採用を正式に決定。「Symantec社 ProxySG S400」2台を採用し、単体での冗長構成と2台の処理リソースの共有による機器のパフォーマンス最大化を可能にする構成とした。また、デュアルAVスキャンと脅威情報DBの組合せで既知のマルウェアをブロックするアプライアンス「Symantec社 Content Analysis System」(以下、Symantec社 CAS)も採用し、KasperskyとCylancePROTECTのダブルでウイルススキャンを実施するよう設定。Symantec独自のGlobal Intelligence Network(脅威情報DB)の組合せによって既知のマルウェアを高精度にブロックできる体制が整った。

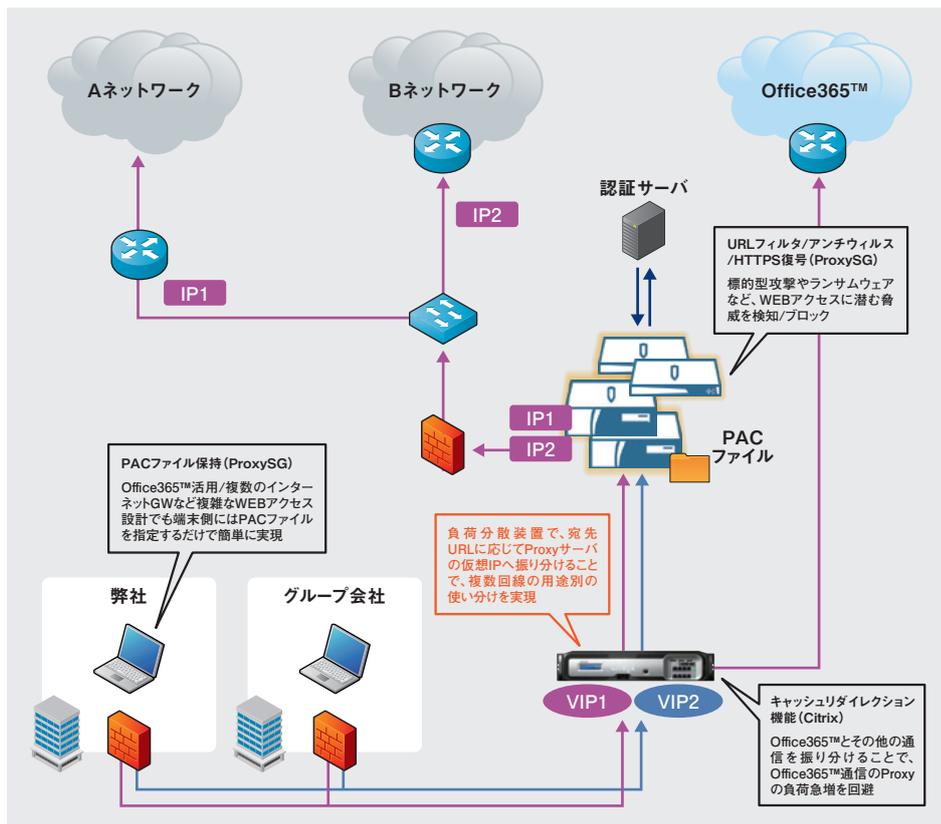
他にも、ネットワークトラフィックを監視しそれらのログをグラフィカルに可視化する仮想アプライアンス「Reporter VA」の活用も決め、2017年3月に本格稼働をスタートさせた。

今回は、インターネット基盤刷新プロジェクトの「フェーズI」(2016年度計画)となり、アイシン精機本体と機能分社と呼ばれる一部の子会社の社員約1万4000人が対象となる。

また、併せて全社員のメール環境もNotes®からOffice365™へと全面的に切り替えることとなり、全てのメールセッションがプロキシを経由して負荷増大によるトラブルを回避するため、アプリケーション高速化と負荷分散を実現する「Citrix NetScaler MPX8005c」も導入された。

**1ヶ月のログ2~3億レコードの中から
わずか数10秒で目的のログ抽出が完了**

SymantecとCitrix NetScalerの導入によってWebアクセスのパフォーマンスが顕著に改善した。有名ポータルサイトへのアクセス時間を比較したところ、導入前は昼休み時間帯で5~6秒かかっていたものが、Symantec導入後は遅延がほとんど感じなくなったという。「Symantecによって、レスポンスが改善され、今



ではアクセス先を振り分ける必要もなくなり運用負荷が軽減されました。」と井上氏は感想を述べる。

また、「以前はエンドポイントまですり抜けていたマルウェアが、上流のゲートウェイで、格段に検知、ブロックされるようになりました。」と大西氏。ファイル共有サービスの利用も厳格に制限できるようになり、情報漏えいのリスクも少なくなっているという。

さらに、Reporter VAのログ抽出機能も高いレベルにあるという。例えば、あるサイトを検索した履歴を分析するため、今まではログ抽出ツールなどを使い、約1ヶ月間のログ2~3億レコードを数時間かけて検索していたが、Reporter VAはわずか数10秒程度で完了。当初1時間以内に完了することが目標だったが、それを大幅に短縮する結果となった。「これまで一両日かかっていた悪質サイトとの通信ログの調査が、ほぼリアルタイムにできるようになりました。」と大西氏は満足そうに話す。

今後の計画としては、「フェーズII」(主要子会社とサブ連と呼ばれる国内の直轄子会社の40,000人を対象)、そして「フェーズIII」(海外を含めた連結子会社全体の100,000人を対象)

へと拡大していく見通しだという。

また、Symantec社CASと親和性の高いハイブリッド型サンドボックスアプライアンス「Symantec Malware Analysis Appliance」(MAA)を導入することで、通常の仮想化環境では発動しない未知のマルウェアも検知可能にしたいとも考えている。

今回のプロジェクトを振り返り、井上氏は、「Symantecのパラメータ設計に関してはマクニカネットワークスの協力のおかげで支障なく進めることができ、提案いただいたSymantecとCitrix NetScalerの組み合わせも極めて有効に機能しています。フェーズII以降はSymantec基盤の強化が必要となりますが、引き続き優れた提案を期待しています。」と語る。

アイシン精機のインターネット基盤の統合によるグループガバナンスの強化はまだ道半ば。マクニカネットワークスはオンプレミス製品の拡大及び、フェーズIIIに向けたクラウドサービスであるSymantec Web Security Serviceの展開も含め、今後も知見を総動員して同社を支援する構えだ。

<https://www.macnica.co.jp/>



株式会社マクニカ ネットワークス カンパニー

〒222-8563 横浜市港北区新横浜1-5-5
TEL.045-476-2010 FAX.045-476-2060
西日本オフィス
〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル14階
TEL.06-6227-6916 FAX.06-6227-6917
symantec-sales@macnica.co.jp

©Macnica, Inc.
● 本カタログに掲載の製品仕様は、予告なく変更する場合があります。予めご了承ください。
● 本カタログに掲載されております社名および製品名は、各社の商標及び登録商標です。