

株式会社アイアイジェイテクノロジー

社外に持ち出される700台のノートPCのリモート接続を確実にセキュアに。
ネットワーク構成を変更せずに検疫ネットワークを導入。エンドポイントを統制/管理。

日本のインターネットの黎明期からのリーダー企業、株式会社インターネットイニシアティブ(IIJ)の子会社として、IT サービスを提供するアイアイジェイテクノロジー。同社は700台のノートPC利用を背景に、社外からリモートで接続するエンドポイントを制御し、セキュアな状態で社内へ接続させるため、柔軟性の高い検疫ソリューション「Symantec Network Access Control」を導入した。これにより、社員の意識に頼ることなく、ITとしてポリシーの遵守を強制させる仕組みを確立し、全てのノートPCの統制と管理を実現している。

ティ推進部門として情報セキュリティ管理室を発足させ、同社の実情に合わせた形で、情報セキュリティを整備、ISMS(情報セキュリティマネジメントシステム)認証を取得した。それ以降、同室が体系的に情報セキュリティ関連の社内施策やサービス施策を決定、関係部門に指示している。デスクトップ、ノートPCなどのエンドポイントにおけるセキュリティ施策に対してもISMSの基準に沿って、早い時期から実施してきた。しかし、ビジネス現場において最も活用されるエンドポイントであるノートPCは、顧客プロジェクトにおいて有用に活用され、さらに一層セキュアなりモート接続が必要になっていた。このような状況において、個々のノートPCは、ISMSの基準に従ってディスク暗号化やトークンによる認証など様々な情報保護施策が施されていたが、運用面では社員一人一人に管理を委ねられていた。そのため、そのPCが社内ネットワークにおける統制上の弱点となるリスクがあり、全てのノートPCにセキュリティポリシーを強制し、統制することが課題になっていた。「ISMSにもとづいたセキュリティの運用を進めていく中で、情報セキュリティ管理室が描いているセキュリティ像と現場の状況が次第にかけ離れていってしまうことが分かりました。例えば、管理室が多数の文書を作成し、情報セキュリティの啓蒙に努力しても、現場で守られていなくては意味がない。という声が上がってきたのです」と語るのは業務改革推進部 情報システムグループ 課長代理の関 一夫氏。

現状のネットワーク環境を変更せず、柔軟に対応できることから導入を決定

実際に社内的な調査を行った結果、リモートアクセスユーザーの増加に伴い、個人用のPCや会社で定めたセキュリティ対策が未完のPCが利用されたとしても、情報システム部門はそのような利用状況を探知できないことが顕在化し、利用実態を明らかにすることが急務となった。このように、(1)ノートPCをセキュアな状態で社内ネットワークに接続させる(2)会社から貸与され、管理されたPC以外の接続を禁止する(3)全てのノートPCにポリシーを強制し統制する、ことを目的として、IJJ-TechはノートPCを対象にしたエンドポイントに対する検疫ソリューションの導入を本格的に検討することにした。導入に当たっての要件は、(1)自宅や社外からリモートで社内ネットワークへアクセスするノートPCの制御、修復(矯正)を自動的に行えること(2)グループ会社に一部横断した物理ネットワーク構成になっているため、関連他社に影響しないように物理構成を変更せずに導入できること(3)現在使っている『IJJセキュアリモートアクセス』によるリモートアクセスの方式を変更せずに導入できること(4)ディスク暗号化ソフト、ウイルス検疫ソフトの正常稼働チェックをはじめ、社内のセキュリティ基準を満たしていることをチェック可能であること、の4つだった。その条件にもとづいて、4つの検疫ソリューション製品サービスを比較検討した結果、IJJ-Techが選んだのはシマンテックの検疫ネットワークソリューション「Symantec Network Access Control」だった。「『IJJセキュアリモートアクセス』にてアクセス制限の役割を担う『IDゲートウェイ』との連携が一つの問題だったのですが、クライアントPCとSymantec Network Access Controlサーバーとの通信要件を満たせる

社員が社外で使用するノートPCの統制と管理が大きな課題に

株式会社アイアイジェイテクノロジー(<http://www.ijj-tech.co.jp/>)は、日本のインターネットの黎明期から強かなリーダーシップを発揮してきたIJJのネットワーク技術と高品質な運用力をDNAとして受け継ぎ、ハイレベルで高品質なITサービスを提供する企業だ。IJJ-Techの掲げるITサービスのコンセプトはIBPS(Integration & Business Platform Service)。各分野のプロフェッショナルが集まったプロジェクトチームのもと、自社内のコア技術とサービスコンポーネント、さらには社外のリソースをインテグレートすることで、最適なソリューションを大手企業や官公庁など多くの顧客に提供している。2002年に、IJJ-Techは全社横断的な情報セキュリ

企業情報

株式会社アイアイジェイテクノロジー(以下、IJJ-Tech)は、ITシステムのコンサルティング、インテグレーション、アウトソーシングを3本柱とするトータルITサービスを提供している企業だ。IJJ-Techは、IJJグループが持つ充実したバックボーン回線と最先端のデータセンターを背景に、IBPS(Integration & Business Platform Service)と呼ばれる革新的なトータルITサービスを提供している。

業種

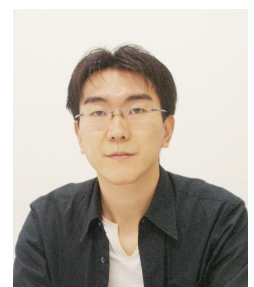
IT サービス業

エンドースメント

「ネットワークの構成を変えず、最適な制御方法を選んで、ノートPCのセキュリティレベルの統一と統制を手間とコストをかけずに実現することができました」

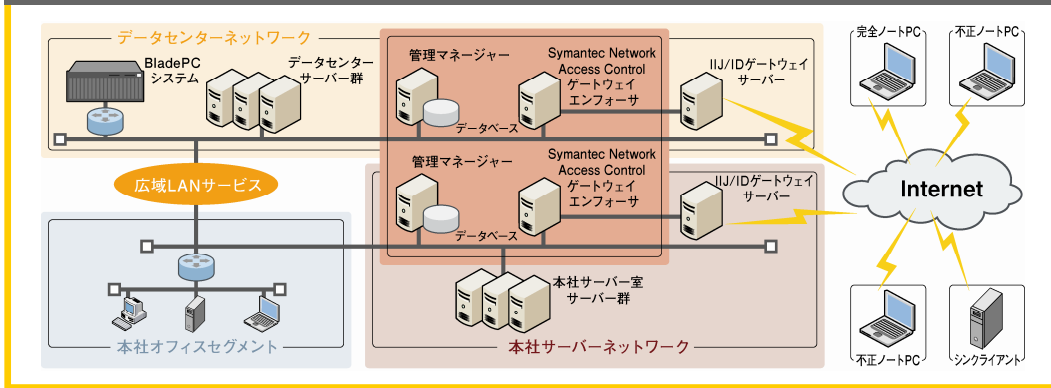


株式会社アイアイジェイテクノロジー
業務改革推進部
情報システムグループ
課長代理
関 一夫 氏



株式会社アイアイジェイテクノロジー
業務改革推進部
情報システムグループ
三浦 博文 氏

図 検疫ネットワークシステムの概念図



ビジネス上の必要条件

- ・セキュリティポリシーに合致したノート PC の利用
- ・ノート PC の透明性を持った管理の実現

環境

- (監査対象プラットフォーム)
- ・ Windows XP

導入製品

- ・ Symantec Network Access Control

製品導入による効果

- ・ ノート PC の適切なセキュリティの確保
- ・ ノート PC の統制と管理レベルを大幅に向上
- ・ ノート PC の管理にかかる工数とコストの大幅削減

かIIJサービス技術部門と検討し、対応可能であることを確認しました。また、チェック項目がカスタマイズでき、意図したとおり動作することやサポート体制がしっかりしているかということも評価項目としました。」と説明するのは業務改革推進部 情報システムグループ 三浦 博文氏。

Symantec Network Access Controlは、(1)クライアントファイアウォールのポリシーを切り替えることでアクセスを制御し、矯正を行うセルフエンフォースメント(2)IEEE802.1XベースのLANスイッチと連動して、検疫を行うLANエンフォースメント(3)DHCPサーバーの認証を利用する検疫方式DHCPエンフォースメント(4)ネットワークにインラインに配置して検疫を行うゲートウェイエンフォースメントの中から、接続形態やネットワーク構成に応じて最適な制御方式を選ぶことができる。今回のスコープがリモートアクセスPCなので、ゲートウェイエンフォースメント方式は必須。なおかつ今後の展開も考慮した上で各種方式に柔軟に対応できるという理由から本製品を選定した。また、Symantec Network Access Control では、ビルトインで用意されているチェック項目だけでなく、If~then~else 構文で実現するカスタムチェック項目も利用可能なため、ディスク暗号化ソフトなどセキュリティ基準に従ったソフトウェアの稼働のチェックも含めたチェック項目を作成した。

2007年初めからシステムの実装を開始し、システム要件などのヒアリングにもとづくポリシーの作成、導入/運用フェーズで予想される問題への対応ドキュメントの作成支援などのコンサルティング提供を受け、導入作業を進めていった。

セキュリティレベルの統一を実現、ノート PC 管理の手間とコストを大幅に削減

こうして検疫ネットワークが稼働、2007年10月段階で700台のノートPCを対象に、検疫を行っている(図)。システムは、本社サーバーネットワークとデータセンターネットワークのIDゲートウェイの下に、それぞれ設置されたSymantec Network Access Control ゲートウェイエンフォースサを使ってネットワークアクセスを制御する。データベース内蔵の管理マネージャーでセキュリティ要件を定め、ネットワークにアクセスするノートPC上にインストールされたSymantec Network Access Control エージェントが定められたセキュリティ要件に合致しているかどうかをチェックする。そして、万一満たしていない場合は要件に合った状態に矯正して、ネットワーク接続を許可する。Symantec Network Access Controlは、ネットワーク環境に応じて柔軟に選択できる4つの制御(検疫)方式を提供するため、既存のネットワーク構成を変更することなく導入できた。また、ネットワークへアクセスする際に接続許可の判断を行うためのチェック項目は、ビルトインだけでなく、カスタマイズも可能であり、必要な条件にあわせて柔軟なチェック項目の作成ができた。そのため、IIJ-Techの要件を満たして、当初の要件通り、ネットワーク環境を一切変更することなく、確実なノートPCの検疫を行うことができるようになった。

「社外からのリモートアクセスするノートPCのセキュリティ確保だけでなく、従来は明確につかむことができなかったノートPCの最新のセキュリティ状態を把握できるようになりました。また、セキュリティ対策ソフトが稼働していない場合も手間をかけずにわかるので、ノートPCの統制と管理のレベルを大幅に向上させることができました」と関氏は語る。こうして、導入した検疫ネットワークによって、同社は従来、PC管理台帳で突き合わせて行っていたノートPCの管理負荷とコストを大幅に削減、透明性を持った管理が手間をかけずに行うことができるようになった。IIJ-Techでは現在、セキュリティ対策としてのリモートアクセス用シンクライアント展開も検討しており、それらのクライアントにもSymantec Network Access Control エージェントを配布し、検疫システムを適用して、管理していく考えだ。

*©2007 Symantec Corporation. All rights reserved. Symantec, Symantec ロゴは Symantec Corporation の登録商標です。その他の会社名、製品名は各社の登録商標または商標です。
*製品の仕様/価格は、都合により変更することがあります。本カタログの記載内容は 2007 年 11 月現在のものです。

株式会社シマンテック

〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ
www.symantec.com/jp/contact

お問い合わせ先



マクニカネットワークス株式会社

本社 〒222-8562 横浜市港北区新横浜 1-5-5
TEL.045-476-1973 FAX.045-476-1976
大阪営業所 〒532-0003 大阪市淀川区宮原 3-4-30 ニッセイ新大阪ビル 17 階
TEL.06-6397-1055 FAX.06-6397-1056