Secure Wide Area Network

# SWANStor

CASE STUDY

東ソー株式会社

## 導入企業情報

### 東ソー株式会社

TOSOH

http://www.tosoh.co.jp

設　　立　1935年2月11日
資 本 金　406億円(2008年3月現在)
従業員数　11,088人(連結 2008年3月現在)
本社所在地　東京都港区芝三丁目8番2号
事業内容
単一工場としては日本最大規模となる南陽事業所を有する総合化学メーカ

[基礎原料事業]　化学品、セメント
[石油化学事業]　オレフィン、ポリマー
[機能商品事業]　有機化成品、バイオサイエンス、機能材料、電子材料

東ソー株式会社　南陽事業所

## インタビュー

### 東ソー情報システム株式会社

システムサービス事業部
ネットワーク・グループ
リーダー　岡 幸一 氏

システムサービス事業部
内田 和哉 氏

東ソー情報システム株式会社

設　　立　2000年1月11日
本社所在地　東京都港区芝2丁目5番10号
事業内容
東ソー株式会社、東ソーグループ会社に対して、情報システムサービスを提供

・ビジネスソリューションサービス
・システムマネジメントサービス
・システムコンサルティングサービス
・プロダクト提供サービス

# 数百を超えるリモートユーザに配布する専用端末や通信カードの管理に限界

SWANStorの導入で、従来と変わらないセキュリティを確保しながら、管理効率も大きく向上。

## 1 専用端末・通信カードを利用したリモートアクセス基盤の課題

東ソー情報システムのシステムサービス事業部は、東ソーグループ26社、約6000ユーザに対して、ネットワークサービスを提供している。グループ企業の業務効率を向上させるために、社外にいる従業員や出向者が社内システムにリモートアクセスするための安全な基盤を提供し管理していくことも同社のミッションの一つだ。

東ソーでは、全国各地のグループ会社に出向している従業員への業務連絡に、イントラネットの掲示板など、特別な情報サービスを利用している。同社は旧来、これらの情報サービスを提供するのに、希望者に対して専用のデータ通信カードや専用PCを配布し、通信キャリアと結ばれた専用ネットワークを経由して社内システムにアクセスさせる方式を採用してきた。

数百を超えるユーザに通信カードや端末を配布することは、管理面での課題が多い。主なものには、都度発生する台帳管理とユーザサポートの負荷がある。特に、ユーザサポートに関しては、通常のネットワーク接続やサービスの利用に関するサポートと同時に、ハードウェアそのものの故障や不具合についても対応する必要があり、要員や体制面での悩みは甚大であった。

また、旧来の仕組みでは、海外に出張している従業員が利用できない状況にあり、国外にも多くの拠点を有する同グループにとって、拡張性への不安も指摘されていた。

将来のグローバルなビジネス展開に対応できる拡張性と、管理の手間を極限まで低減できる新たなネットワーク基盤の構築は急務となっていた。そこで同社が目指したのが、公衆インターネット網を利用できる新たな情報共有基盤の構築である。

## 2 譲れないセキュリティレベル

通信カードを利用したネットワーク基盤は、管理面での負荷が高い一方、安心感の高いアクセス制御ができるというセキュリティ面でのメリットが高かった。これまでの仕組みでは、配布した通信カードからのみアクセスが許可されるというフィルター、さらにRADIUSによるユーザの認証の2重の制御を行っていた。リモートアクセス基盤の刷新を検討する中では、従来のセキュリティレベルを維持・強化するという点が、譲れない条件となった。

同社は、公衆インターネット網を利用した基盤で、かつ高いレベルを維持・強化できる仕組みを模索した。SSL-VPNアプライアンスなど、リモートアクセス用の各種のサービスや製品を比較検証する中で、有力な候補となったのが、エリアビイの「SWANStor」だ。同社が「SWANStor」に注目したのは、ファイアウォールにインバウンドポートを空ける必要がなく、ユーザのIDやパスワードが安全に社内LANに格納されているというセキュリティレベルの高さである。さらに、同社が「SWANStor」の利用に踏み切ったのには、別の理由もある。それは、ユーザにとって不安の多いセキュリティ基盤の再構築において、「SWANStor」が小規模でのトライアル利用に対応できたことだ。「中継サーバーのSWANStor GatewayのASPサービスを利用して、小規模から試験的にスタート出来たのが大きかった。」と、内田氏は「SWANStor」採用の経緯を語る。

2004年、エリアビイ社提供のASPサービスを利用する形でSWANStor Gatewayを試験的に導入することとなった。翌2005年までの約1年の間、限られた規模で利用し要件に合致していることが確認できた。こうして同社は、「SWANStor」の本導入を決定し、以降、情報共有システム全体の設計に着手することとなった。

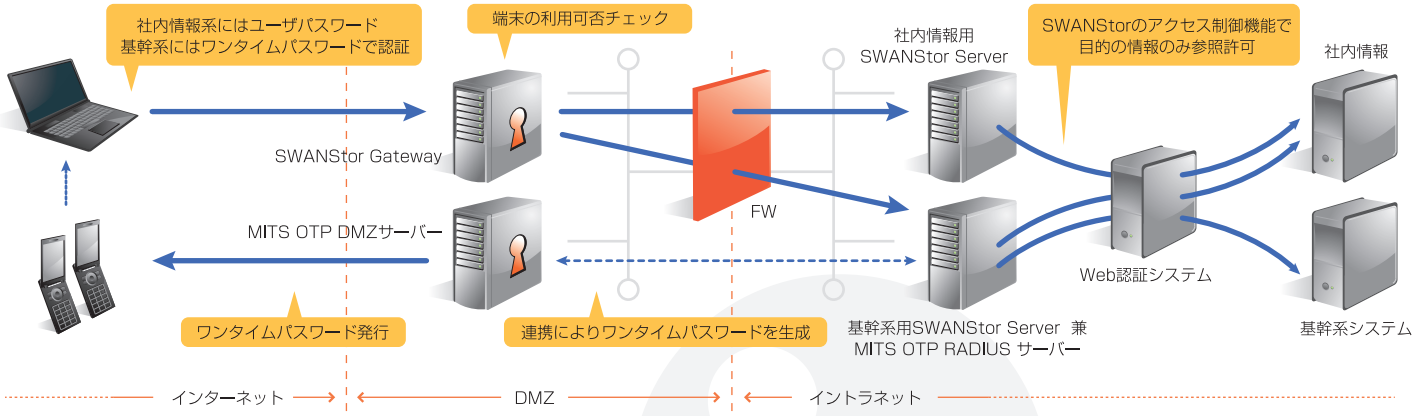
## 3 基幹システムへのアクセスにも不安のないセキュリティ

業務要件により基幹系システムのリモート環境アクセスの要求があったが、リモート環境から基幹系システムにアクセスするためには、前述のイントラネットを介した業務連絡よりも、一段高いセキュリティが必要だ。ユーザが利用する範囲や用途に応じて、セキュリティレベルを多段階に設定しなければならないという新たな課題が浮上することとなった。

様々な対応策を模索する中で、ワンタイムパスワードを並行利用し、本人認証を強化する方法を検討することとなった。そこで、候補に挙がったのが、「SWANStor」との連携実績の高い株式会社アイディーエスの「MITS OTP」だ。携帯電話にワンタイムパスワードを発行し本人認証を行うMITS OTPと連携することにより、基幹系システムへのアクセスに別の認証方式を提供できる仕組みが完成した。岡氏は、情報の種類によってネットワークの使い分けができる今回の仕組みについて、次のように語る。「会社からの業務連絡と比べると、基幹系システムへの情報共有には、もう一段高いセキュリティを用意する必要があった。SWANStor Gatewayをはさんで2系統のSWANStor Serverを用意することによって、公開する情報の種類によりセキュリティレベルを分けるという要件に合致した仕組みを構築することができた。」

基幹系システムへのアクセスを想定したセキュリティ対策は、携帯ワンタイムパスワードのみにとどまらない。基幹系システムにアクセスするには、更に端末の利用可否チェックも行うようにした。これにより、アクセス端末認証と、MITS OTPのワンタイムパスワードによる個人認証という、極めて高度な認証基盤を構築することに成功した。

こうして「SWANStor」を利用した新基盤は、2008年2月、基幹系システムの利用も含めた全対象範囲について、無事稼動した。




## 4 公衆インターネット網を利用した手間のかからないセキュリティ基盤の完成

SWANStorの利用を開始することにより、手間のかかる通信カードの配布による管理を、ソフトウェア上での管理に全面的に置き換えることができた。また、ユーザへの技術サポート面でも、ハードウェアや通信回線部分を切り離して対応することが出来るようになり、管理効率が格段に向上するとともに、サポート面での負荷が激減した。

国内外を問わずインターネットがあれば、SWANStorとMITS OTPの組み合わせで、不正アクセスの不安なく社内情報を共有することができる。このことは、多くのグループ会社、出向者が存在する同社には大きなメリットとなった。

### エリアビイジャパンについて

今回の新たなセキュリティ基盤の刷新は、同社にとって非常に大きいチャレンジであった。大きい変化には、それ相応のメーカサポートも必要となる。内田氏は、構築段階におけるエリアビイのサポートについて、次のように語る。「構築中は、課題や進捗具合が良く見える形で報告いただいて、要望にも柔軟に対応いただきました。」また、「数年越しのプロジェクトをなんとしても完成させたいというこちらの熱意を感じ取っていただき、非常に安心感がありました。」と、岡氏はエリアビイの協力がなくてはならなかったと振り返った。

futurecore areabe
エリアビイジャパン株式会社
https://www.areabe.com
〒163-1103 東京都新宿区西新宿6-22-1 新宿スクエアタワー3階
TEL : 03-6758-0540 FAX : 03-6758-0541

お問い合せ先