



● <http://www.meiden-mst.co.jp/>

明電システムテクノロジー株式会社

Meiden System Technologies Corporation



藤森康行氏 青山徹氏

(右)取締役 ソリューションシステム部 部長
(左)ソリューションシステム部
営業企画グループ 主管技師

※肩書き・役職等は取材時のものです

クライアント数 **700**

明電システムテクノロジーは、ソフトウェア技術者集団として「技術と製品を通して、より豊かな未来社会の実現」に貢献する企業を目指し、様々な分野のソフトウェア開発に長年取り組んできました。太陽光・風力発電によるグリーンエネルギー分野から、ビル内環境の省エネルギー分野、家庭や工場からの排水を環境に優しい水に再生する環境分野、電車や自動車の運行の安全を守るための交通分野、最先端技術に貢献する半導体分野、情報通信分野などのシステム開発を通して、お客様に満足いただけることを第一に考え、最適なシステム提案から、製作、運用、保守に至るまで一貫したサービスとソリューションをご提供しています。

TotalSecurityFort導入後の効果…

- 社員のセキュリティに対する意識が大きく向上し、他人事ではないという認識が生まれた
- Web参照、電子メールの使用に際し、業務外の使用が無くなるという抑止効果
- TotalSecurityFortを用いた実効的な情報漏洩対策に対しお客様からの高い評価

- システム管理
- ローカルセキュリティ
- ネットワークセキュリティ
- ソフトウェアセキュリティ
- ハードウェア資産管理
- ソフトウェア資産管理
- リモート機能
- レポートセンター
- トレンドセンター
- 統計センター
- 分析センター
- ソフトウェアセキュリティ追加

導入の背景

なぜTotalSecurityFort(以下、TSF)などのセキュリティ商品が必要だったのですか？

藤森氏：第一に、公共性の高いシステムの開発に携わっており、情報漏洩事件・事故の発生は、企業として致命的なダメージを受けると同時に、お客様への多大なご迷惑をお掛けすることになってしまいますので、それは何としても防止しなければなりませんでした。

第二に、近年多発している情報漏洩事件を受け、お客様から、確実な情報漏洩防止対策の強いご要望をいただいていた。

第三に、当社の情報セキュリティマネジメントシステム (ISMS) を構築するに当たり、物理的対策、組織的対策、人的対策に関しては、規程作成や教育等で対応できますが、技術的対策に対しては、ツールを導入して体系的に対策を講じることが重要かつ効果的であると考えたからです。

青山氏：当社は、電力会社様や自治体様などの仕事を多く行っており、いろいろな情報をお預かりしています。それに対して当社は「こういうツールを導入して、こういう対策をやっています」と具体的に説明したほうが説得力があり、お客様にも安心していただけます。

導入前にどんな課題・問題点がありましたか？

藤森氏：当社では以前より、外部からの不正なアクセスに対しては、ファイアウォール、ルータ、ウイルススキャンなどで対策を講じていました。しかし、内部からの情報持ち出しに対しては、ドメインコントローラによるアクセス管理が主な対策であり、ルールを定め社員のモラルを向上させるだけでは、いつ事故が発生するかわかりません。特に、内部からの情報持ち出しに対する脅威や脆弱性に関してはしっかりとツールを使って防ぐことが必要でした。

青山氏：社員のセキュリティ意識をあげるというのは簡単ではありません。上から押し付けようとしても、なかなか社員には浸透しません。またいくらお客様から情報漏洩対策に課する要求があっても、対策がその場しのぎになってしまいがちです。

導入の経緯

幾つもある競合商品の中からTSFを選んだ理由・ポイントは何ですか？

藤森氏：導入にあたり、まず10社ほどの競合製品を比較調査しました。

TSFは監視・制御・記録・資産管理といった全ての機能がオールインワンで提供されていますが、選んだ当時、そういう製品は他には見当たりませんでした。また管理機能が一箇所に集約されているので、システム管理者の負担が少なく、TSFのポリシーの設定も現場の管理者が柔軟に対応できるのです。そうした点も大きな評価ポイントとなりました。さらにTSFはサーバライセンス料や細かいオプションがなく、価格体系がシンプルで、しかも機能の割に価格が安い点も高い評価となりました。

次に、TSFの評価試験を行ったところ、外部デバイス (USBメモリなど) を用いた情報持ち出しに対する暗号化がドラッグ&ドロップ操作で意識せずに自動的に行えました。他社製品では専用の暗号化フォルダにデータを入れてから暗号化するというアクションが必要でしたので、TSFのワンアクションでの暗号化は、技術的には大きなポイントになりました。

TSF導入後に気付いた点としては、情報の持ち出しに対する承認ワークフロー機能がとても使える機能だと思いました。

青山氏：当社でセキュリティ製品の導入を検討していた際、これをやりたいという特定のニーズがあったわけではありません。むしろセキュリティ全体を考えたいという観点から入っていきました。そうすると「機能の網羅性」が評価ポイントになるわけです。その当時、製品比較表を作って各製品を評価していましたが、全ての機能に○がつくのはTSFだけでした。ですからTSFを導入すれば、当社のセキュリティ対策に柔軟に対応できると感じました。

TSF導入に際して現場にはどのように説得されましたか？

藤森氏：当社は、ソフトウェア開発を業務としている関係上、ソフトウェアのソースや設計資料をかなり頻繁に持ち出します。そういう状況で「データは勝手に持ち出せなくなります」とか、「持ち出すときには自動的に暗号化されます」という説明をすると、使い勝手が悪くなるという思いが先に来て、やはりかなり抵抗がありました。「ファイルが平文で自由に持ち出せないと業務に支障が出る」とか、「PCが重くなって生産性が落ちるのは困る」とか、色々な意見がありました。そこで、まず各部門の管理者に対し、「情報漏洩は絶対に起こさないのだ!」というトップの声を伝えました。その後、昨今の情報漏洩事件・事故の発生状況やその原因は何であるか、また一度でも情報漏洩事件・事故が発生させた場合の会社の損害・

(表面からのつづき)

ダメージについてセキュリティ教育を行い、セキュリティ製品の必要性を理解してもらいました。さらにTSFのポリシーをうまく設定することで現場に合わせた運用ができますという説明も行いました。
導入に際しては、いきなり厳しいポリシーを設定するのではなく、ログの収集とP2Pソフトの使用禁止から始め、次に持ち出す情報の暗号化、持ち出し承認ワークフロー運用というように、段階を踏みながらTSFのポリシー運用を強化し、あるべき姿に近づけてきました。
導入して運用を始めると、半年くらいで特に意識せずに運用されるようになり、今ではTSFの環境が当たり前の状態となっています。

導入の概要

TSFを導入された施設、ネットワーク規模を教えてください。

藤森氏：本社の他、岩手県盛岡市、群馬県太田市、愛知県清洲市、兵庫県尼崎市に支社・事務所があります。本社と各拠点はVPNで接続されており、本社に設置したTSFサーバで、各拠点を含めた全社700台を管理しています。

TSFの優れていると思った点は何ですか？

藤森氏：TSFを選んだ理由の部分でも述べましたが、特に、以下の5点が挙げられます。

- ・必要な機能がオールインワンで提供されており、管理が簡単なこと。
- ・外部デバイスを使用した情報の受け渡しに対する暗号化／復号化が意識せずに簡単かつ確実に行えること。
- ・重要な情報を持ち出す場合、管理者承認のワークフローが提供されていること。
- ・現場管理者にポリシーの運用を任せられるため、部門にあったポリシー運用が容易に行えること。
- ・全ての操作履歴がログとして収集できること。

活用方法を教えてください。

藤森氏：基本的に平文情報の持ち出しは禁止し、外部デバイスやノートPCで、社外に情報を持ち出す場合には、必ず暗号化して持ち運びしています。そうすることで、万が一、置き忘れ、紛失、盗難があった場合に備えています。またファイル共有ソフト(P2P)などの業務に不要なソフトの使用を禁止にし、印刷はすべてウォーターマークを付けています。さらに個人情報、お客様からお預かりしている機密情報、社内の秘密情報等は、管理者の持ち出し承認ワークフローにより、勝手な持ち出しを統制しています。
青山氏：ISMS(ISO27001:2005)の認証取得の際にもTSFの存在はとても大きかったです。ISMS要求事項の中の具体的な対策や根拠を提示する際にTSFの仕組み(データ持ち出し制御や承認機能、資産管理など)やエビデンス(ログ管理)を活用できました。TSFのツールを使ってきちんと運用、管理していることが目に見える形で示せますので、非常に有効な手段です。審査員からは、「どの会社も業務フローや規定集は色々作るが、実際にこうしたシステムまで入れて確実に運用しているところはあまりありません。素晴らしいですね。」とお褒めの言葉をいただきました。
藤森氏：ISMSの認証取得には、技術的対策が求められています。具体的には、操作ログの取得、データ持ち出し時の暗号化、不正アクセス防止等が挙げられていますが、そうした部分はTSFでほとんどカバーできています。

セキュリティの運用管理はどのように行っておられますか？

藤森氏：運用に関しては、定期的に現場管理者が、自部門のログをチェックし、セキュリティインシデントの発生有無を確認しています。またポリシー運用は現場管理者に任せているので、監査者が管理者操作ログを定期的にチェックし、適正なポリシー運用がされていることを確認しています。
さらにTSFが収集したログからセキュリティインシデントを検出する“ログ解析ツール”を当社で独自に開発し、それを活用して予防に役立てています。
青山氏：TSFは機能が豊富で柔軟ですので、TSFの機能に合わせて業務を変更しなければならないということは特になく、当社の業務やセキュリティポリシーに合わせた運用が行えています。

導入後の効果

TSFを導入してどんな効果がありましたか？

藤森氏：技術的な効果は先ほどからお話していますが、それ以外では、セキュリティに対する意識が大きく向上しました。今までは情報漏洩事件に対して、他人事という雰囲気がありました。TSFを導入したことで、他人事ではないという認識が生まれました。またWeb参照、電子メールの使用に際し、業務外の使用が無くなるといった効果が出ています。さらにTSFを用いた実効的な情報漏洩対策に対して、お客様から高い評価をいただいています。仕事の獲得、会社の信用アップにも非常に役立っています。
青山氏：お客様にセキュリティ対策を説明する上で、「TSFというツールで厳しく持ち出し統制をしていますから情報は勝手に持ち出せません」と説明できるので非常に説得力があります。
藤森氏：今までは情報持ち出しの際に紙の台帳に書いて申請するという運用でした。ただこれですと非常に手間がかかり、しかも社員のモラルに頼ることになってしまい、確実な情報漏洩対策とは言えませんでした。しかしTSFを導入したことで、情報の持ち出し時に承認ワークフロー機能を使って、体系的にしっかりと抑えられているので、とても安心です。

将来の展望

今後TSFをどのように使っていきたいですか？

藤森氏：現在、TSFの制御機能を中心に運用していますが、今後はソフトウェアの資産管理にもTSFの資産管理機能を活用していこうと考えています。
また、当社はISMSの認証を取得しており、その中で、体系的なセキュリティ対策として、TSFを引き続き効果的に活用する方法を検討・実施していく予定です。また、自社開発した“TSFログ解析ツール”とTSFを組み合わせてセキュリティインシデント発生の予防を更に進めていくつもりです。
青山氏：時代の流れに応じて情報セキュリティ対策も常に変化し、さまざまな対策が必要となります。しかしTSFの持っている機能を使えば、ムリなく自然にその変化に対応していけると思います。これはトータルに機能を網羅しているTSFのメリットだと思います。

FineArt 日本ファインアート株式会社

お問い合わせ

日本ファインアート株式会社
〒160-0023 日本東京都新宿区西新宿6-16-6 新宿タツミビル10F
TEL:03-5909-1888(代表) FAX:03-3345-3180
e-mail:tsf@fineart-tech.com

技術協力：NTTデータセキュリティ株式会社

※TotalSecurityFortはFineArt Technology Co., Ltd. の商標および登録商標です。
※その他記載された社名および製品名は一般に各社の商標または登録商標です。
※本印刷物の記載事項は変更になる場合がございます。
※内容は取材当時のものです。