

「JP1/秘文」で情報漏えいをシャットアウト。 IT資産管理との連携で 情報インフラ整備の取り組みを支える「JP1」

沖縄電力株式会社(以下、沖縄電力)は、2005年に情報インフラ整備計画を策定し、その具体策の1つとして社内IT環境のセキュリティ強化に取り組んでいる。その一環で2008年4月、日立の情報漏えい防止「JP1/秘文」を全社PCへ導入。外部へのファイル持ち出しを管理・制御する環境を確立した。さらに、JP1/秘文の持ち出しログ・印刷ログと、ソフトウェア資産・配布管理「JP1/NETM/DM」のファイル操作ログを、統合資産管理「JP1/NETM/AIM」で一元管理する環境を実現。多種多様なセキュリティ情報を統合管理できる日立の「JP1」は、情報インフラを段階的に整備していく沖縄電力の取り組みを、しっかりと支えている。



沖縄電力株式会社
IT推進本部
情報システム部
部長
奥間 美枝子氏



沖縄電力株式会社
IT推進本部
情報システム部
次長
田仲 茂氏



沖縄電力株式会社
IT推進本部
情報システム部
システムグループリーダー
(課長)
下地 登志喜氏



沖縄電力株式会社
IT推進本部
情報システム部
システムグループ
(主任)
儀間 洋一氏

情報インフラ整備計画に沿って セキュリティを強化

東西約1,000km、南北約400kmにおよぶ広大な海域に点在する島々で構成される沖縄県。そのうち約40の有人島に電力を供給しているのが、日本で唯一、一県のみを事業地域とする電気事業者・沖縄電力である。

同社はその地理的・地形的特徴から、本土以上に制約の厳しい事業環境の中、徹底した業務効率化とコスト低減による競争力の強化などを推進している。

「スケールメリットを出すことが難しい沖縄電力が、安定供給とユニバーサルサービスを堅持するためには、社員全員が効率よく動き、経営戦略を着実に実現していかなければなりません。情報システムが果たす役割はきわめて大きいのです」と奥間氏は説明する。

2004年、同社は、従来から取り組んできた高度情報システム基本構想を発展させ、「業務システムの高度化」「情報インフラの標準化」という2つのテーマを打ち出した。

「情報インフラの標準化」については、2005年に情報インフラ整備計画を策定。

「この計画策定を支援してくれるパートナーとして選んだのが日立でした。わたしたちは、EA(Enterprise Architecture)をベースに標準化を進めていきたいと考えていましたが、

日立はEAフレームワークに沿って、長期的な視点で総合的な提案をしてくれました」と下地氏は言う。

情報インフラ整備計画は、信頼性や可用性、利便性、性能に優れた情報インフラの構築とセキュリティ強化をはじめとし、効率的なシステム投資やアーキテクチャ等の標準化によるTCOの削減、これらに関する作業の明確化など多数の実施項目がある。

その一環として取り組んだのが、日立の情報漏えい防止「JP1/秘文」を活用した社内IT環境のセキュリティ強化である。

「JP1/秘文」で 「安全な持ち出し」を実現

セキュリティ強化施策は、2007年から開始した。

「いままでもセキュリティポリシーを制定して運用しながら、社外からの攻撃対策を講じてきました。現在、内部からの情報漏えいを防ぐ対策も強化しています。その中で重視したのが、USBメモリーやフロッピーディスクなどの外部記憶媒体経由による情報漏えいの防止です」(下地氏)。

情報の持ち出し制御を実現するシステムとしては、複数の製品を比較検討したうえで、JP1/秘文を選択した。

USER PROFILE

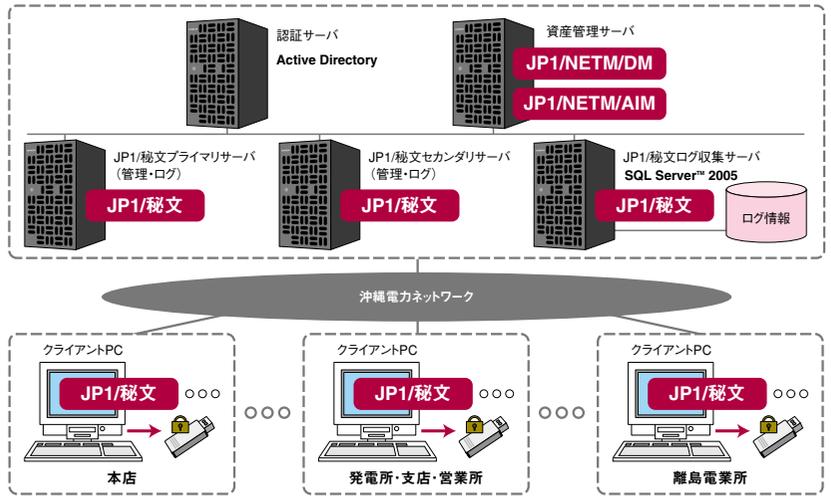
沖縄電力株式会社
www.okiden.co.jp

本社 沖縄県浦添市牧港5-2-1
設立 1972年5月15日
資本金 75億8,600万円
従業員数 1,568名(2008年3月31日現在)
東西1,000km、南北400kmの海域に点在する160の島々で構成される沖縄県。沖縄電力はそのうち約40の有人島に電力を供給。基本使命として、「安定供給とユニバーサルサービスの堅持」と「本土並み電気料金水準の確保」を掲げる。1支社6支店2営業所を持ち、12の島で発電。「残波しおさいの森づくり」など環境活動も盛ん。

地域とともに、地域のために



沖縄電力(株)の情報漏えい防止システム概要



選定理由は大きく分けて3つある。

第1に、JP1/秘文は、外部記憶媒体による持ち出し制御だけでなく、ファイルの暗号化、持ち出しログ監視を、すべて標準で実現する総合的な情報漏えい防止のソフトウェアであることだ。

「取引先へフロッピーディスクを持って行かなければならない部署もありますし、外部記憶媒体による持ち出しや印刷を、全面禁止することは仕事の支障になります。大事なことは、制限と活用のバランスを取ること。『禁止』ではなく『安全な持ち出し』を実現するためには、暗号化とログ取得の機能は不可欠でした」と儀間氏は語る。

第2に、IT資産管理で導入済みのソフトウェア資産・配布管理「JP1/NETM/DM」および統合資産管理「JP1/NETM/AIM」と、JP1/秘文とを連携させて、ログを統合管理できることだ。

沖縄電力では、JP1/秘文が記録する外部記憶媒体による持ち出しログおよび印刷ログと、JP1/NETM/DMのファイル操作関連のログを抽出して、JP1/NETM/AIMで、両者を一括して監視できるようにした。これにより、何か問題が発生したとき、きめ細かい原因追跡が短時間でできる。

第3に、統合システム運用管理「JP1」は拡張性に優れており、他のさまざまな機能を

追加導入しながら、運用管理を強化していくことができる。

さらに、JP1/秘文は、国内シェアが高く、沖縄県内でも実績豊富であることも評価したという。

今回のJP1/秘文導入にあたっては、わずか3ヵ月で全社展開を実現するなど、日立のSI力で強力にバックアップ。製品・サポートの両面からセキュリティ強化施策を支援した。

検疫ネットワークの実現など
さらなるセキュリティの強化

JP1/秘文の導入により、不正な手段での情報の持ち出しは一切できなくなった。持ち出せるのは、暗号化、または特別に許可された情報のみであり、万一、外部記憶媒体を紛失しても、情報漏えいの心配はない。さらに、印刷ログは、全ユーザー・全ファイルを対象に確実に記録される。

また、JP1/秘文のユーザー情報はActive Directoryとの連携によって自動化されているため、部署や社員ごとに管理している外部記憶媒体による持ち出し権限の設定は、人事異動や職制変更の際にも反映され、情報システム部門の管理負担が増える心配もない。

「『安全な持ち出し』の環境ができたことで、ユーザーも安心して外部記憶媒体が使えて、仕事がやりやすくなったはずです」(下地氏)。

今後は持ち出しログやファイル操作関連のログを集計して利用状況を分析し、セキュリティ環境をさらに改善するために活用していく方針だ。

「セキュリティポリシーに従った運用が、日々のPC操作の中でも強固に守られる環境が整い、社員のセキュリティ意識のさらなる向上にも役立っています」と奥間氏は評価する。

次の目標は、検疫ネットワークの実現である。

「会議室にもどンドンPCを持ち歩き、オフィスを柔軟に使うといったワークスタイル改革を進めるには、暗号化に加えて検疫ネットワークの実現が不可欠です」と田仲氏は語る。

そこで、まずはネットワーク接続機器監視システムを導入し、許可されていないPCをLAN接続すると管理部門にアラームが通知されるようにする計画だ。その監視ツールの一つとして「JP1/NETM/NM」を検討している。

「Webアクセスのログ管理やファイルのアクセス権限管理など、今後の沖縄電力の運用改善・高度化に有効な機能は、積極的に導入したいと思います。JP1の機能強化にも期待しています」と奥間氏は語る。

今後、どのような機能強化を行っていったとしても、そのすべての情報を一元管理できるJP1は、沖縄電力の今後のワークスタイル改革や業務効率向上を、情報インフラ面で長期にわたって支えていく。



* 下地氏の所属は2008年6月当時のもの。 JP1/NETM/AIM:JP1/NETM/Asset Information Manager JP1/NETM/NM:JP1/NETM/Network Monitor
●Active DirectoryおよびSQL Serverは、米国Microsoft Corporationの米国およびその他の国における商標、または登録商標です。
●その他記載されている会社名、製品名は、それぞれの会社の商標もしくは登録商標です。