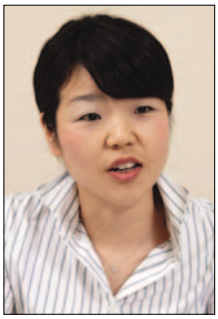
国際コンテナターミナル株式会社

体系的かつ先進のアプローチで情報を守る。「JP1」を全社システムの運用管理基盤に据えてEDIの効率的な運用と着実なセキュリティ対策を実現

商船三井グループの港湾運送会社として、首都圏の玄関口である東京・大井埠頭と横浜・本牧埠頭で港湾荷役を担う国際コンテナターミナル株式会社（以下、国際コンテナターミナル）。同社では、専用線によるSea-NACCS*1接続とWeb-EDIとを単一ソリューションでカバーする統合EDIシステムが実現できたことを契機に、日立の統合システム運用管理「JP1」を全社システムの運用管理基盤と位置づけている。JP1はセキュリティにおいても、統一ブランドのもとで体系的かつ網羅的なソリューションを実現。複数の対策を積み重ね、連携させていく国際コンテナターミナルの先進的な取り組みを支えている。

国際コンテナターミナル
株式会社
管理部
専任部長
林　正孝氏

国際コンテナターミナル
株式会社
管理部
部長補佐
渡辺 照夫氏



国際コンテナターミナル
株式会社
管理部
情報システム課
金　恩慶氏

Sea-NACCSとWeb-EDIを統合するEDIシステムを構築

国際コンテナターミナルは、1999年に横浜国際ターミナル（本牧）で、さらに2005年4月には東京国際ターミナル（大井）でも、Web-EDIを構築し、その運用に日立の統合システム運用管理「JP1」を用いてきた。

大井ターミナルの場合は、最近まで船会社や他のターミナル会社とのデータ交換に国際VANを用いていた。別途、運用していた通関情報システムSea-NACCSへの接続システムがリプレース時期を迎えるのを契機として、両者を統合して、運用を簡素化したいと考えたのである。

数社の提案を慎重に検討した結果、採用したのは日立の提案であった。

「送受信データをEDIFACT*2に変換し、インターネット・メールの添付ファイルとして自動送受信するしくみと、2つのEDIシステムを統合管理する提案は日立だけでした」と林氏は語る。

日立の提案は、インターネット回線を用いるWeb-EDIと専用線を用いるSea-NACCSゲートウェイを同一サーバ／同一ミドルウェアで一元的に管理する点が、他社の提案と根本的に異なっていた。

Web-EDIを運用するには、通信ソフト、トランスレータ、データベースの3種類のソフトを連携させる必要があるが、日立は、EDIゲートウェイのための「Cosminexus（コズミネクサス）」のモジュール、多様なデータフォーマット変換を実現するXMLおよびEDI対応トランスレータ「uCosminexus（ユーコズミネクサス） Interschema（インタースキーマ）」、ノンストップデータベース「HiRDB（ハイアールディービー）」という3種類のオープンミドルウェアを、JP1のジョブ管理「JP1/Automatic Job Management System 2（JP1/AJS2）」で密接に連携させながら動かすことで、信頼性の高いWeb-EDIを実現する。

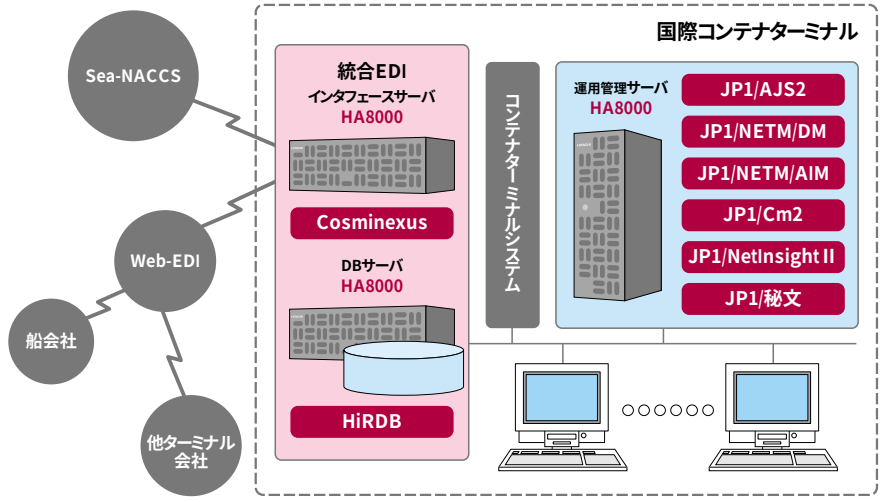
しかも、EDIゲートウェイモジュールはSea-NACCSに対応しているため、1台のインタフェースサーバと1台のデータベースサーバだけで、Web-EDIとSea-NACCSをカバーする統合EDI環境を実現できるのである。

国際コンテナターミナルもEDIの相手先も、専用線のVANをWeb-EDIに置き換えたことで、高価な回線使用料を支払う必要がなくなった。さらに、データ交換機能を基幹システムから独立させたことで、基幹システムのメインフレーム側の負荷も軽減され、Web-EDIも柔軟な機能拡張ができるようになったのである。

「JP1は開発者が国内にいることもあり、サポートが手厚い。問い合わせなどへの対応

USER PROFILE
国際コンテナターミナル株式会社
www.tict.co.jp
本　　社 東京都品川区八潮2-3-10 大井新3・4号バース
設　　立 1948年5月11日
資 本 金 7億円
日本におけるコンテナ船荷役のパイオニア。港湾運送、船舶代理店業などを展開。船舶のスケジュール管理、コンテナを効率よく動かすスタックプランニング、大型クレーンを駆使してのヤードオペレーションなどに高度なノウハウを発揮して、リーディング・ターミナルとしての地位を獲得してきた。

国際コンテナターミナルの統合EDIと運用管理システム概要



も迅速です」と渡辺氏は喜ぶ。

セキュリティは体系的なソリューション連携が重要

国際コンテナターミナルは、セキュリティへの取り組みにおいても、JP1を全社統一ソリューションとして採用した。運用管理をシングルブランドで統一することで、効率的かつ強力なセキュリティ管理を実現したいと考えたからである。

「われわれはもちろん、ソーラス条約*3に沿った保安体制を敷いていますが、港湾運送業は、多様なセキュリティ・リスクにさらされているのです」と林氏は説明する。

海外とのデータ交換が多いため、海外で新たに発見されたウィルスにすぐに攻撃されるリスクも高いという。

「なりすまし、スパイウェア、情報漏えいなど、脅威はたくさんあります。ウィルス感染を防ぐためにウィルスチェックソフトを導入するといった個別の対応では、新たな脅威をシャットアウトすることはできません。さまざまな対策を重層的に組み合わせ、連携させて、セキュリティへの意識が高い船会社にも安心していただける環境を実現しなければなりません」と林氏は強調する。

運用管理という大きな視点からセキュリティ機能を網羅しているJP1を用いれば、重複する機能に二重投資することなく、ソリューション間の密接な連携も確保しながら、未知の脅威に備える体制を確立できるのである。

JP1で効率的な運用と体系的なセキュリティ対策を実現

国際コンテナターミナルでは、取り組むべき情報セキュリティ対策を体系化し、段階的に実現してきた。

まず、社内システムの基礎対策としては、資産・配布管理「JP1/NETM/DM」と「JP1/NETM/AIM」を用いて、クライアントPCのハード／ソフト両面での資産管理を徹底した。資産情報の収集と分析がうまく機能してこそ、その後のウィルス対策や情報漏えい対策が可能になるからだ。

「インストール制限をかけてあるフリーウェアが稼働すれば警告が通知されます。Winnyなどが勝手に作動できない環境を第1段階で作っておいたのです」と金氏は語る。

また、ネットワーク管理「JP1/Cm2」によって、サーバ約20台で構成されるネットワークの監視と障害管理の体制も整えた。

さらに、コンピュータウィルス対策では、JP1/NETM/DMによって、セキュリティパッチの自動配布・自動インストール環境も実現。不正侵入対策では、「JP1/NetInsight II」とJP1/Cm2によって、ネットワーク管理を徹底した。不審な接続があった場合には、即刻、管理者に警告メールが送られる。

そして、社内情報漏えい対策として採用したのが、「JP1/秘文」である。

JP1/秘文は、PC上のデータをドライブ単位で暗号化し、万一その情報が盗まれた場合でも、読み取りができないようにする。さらに、ファイルが添付されたメールの制御も行い外部への情報漏えいを防止。特に重要な情報については、持ち出し制限、印刷制限、アクセス履歴の記録も実施している。

ジョブ管理による効率的な運用と、資産管理からネットワーク管理、暗号化に至る多彩なセキュリティ対策をJP1で実現しているのだ。

「運用管理やセキュリティのことはJP1に任せて、わたしたちは、次期ターミナルシステムのありかたなど、企画業務に専念したい」と林氏は力強く語る。

変化に強いデータ交換環境と先進のセキュリティ体制を手に入れた国際コンテナターミナルは、今後も、全社システムの管理基盤としてJP1をさまざまな角度から活用していく方針である。

＊1 Nippon Automated Cargo Clearance System＊2 Electronic Data Interchange For Administration, Commerce and Transport
＊3 海上における人命の安全を確保する国際条約