



国内物流と海外物流における情報システムの安全対策事例紹介

～RFIDなど新技術によるモノと情報の結びつけでの要望～

佐野弘明 日本通運(株)

物流業界の概要

物流は、国内輸送、国際輸送などの輸送作業をはじめとして、貨物を安全に運ぶための梱包作業、物流センターでの保管業務、物流の過程で貨物に加工をする流通加工など、さまざまな活動を伴っています。また近年、物流業界においても、情報システムが不可欠な存在となり、事業が停止するようなシステムリスクに対する対応が求められています。

日本通運(株)は、1872年に設立された「陸運元会社」を前身とし、1937年に創立され、2007年3月末現在、運送事業、販売事業、その他の事業を世界37カ国、196都市に展開をしています。

では、当社の事例を元に、海外物流と国内物流における情報システムの安全対策の現状、および先端技術であるRFID活用の事例を紹介します。

海外物流における情報システムの安全対策

【海外物流関連システム】

まず安全対策をお話する前に、当社の海外および国際業務にかかわるシステムについて簡単にご説明します。

当社の海外システムは、大きく分けると海外拠点の経理業務、輸出入業務など基幹業務をサポートするシステムと、お客様のご要望にお応えするためのサプライチェーンマネジメントやサードパーティロジスティクスをグローバルにサポートする在庫管理システム、調達管理システムから構成されています。

それでは、国際貨物輸送と在庫管理システムについて、少し詳しくふれます。

【国際貨物輸送システム】

輸送形態が、飛行機でも船でも輸出入のオペレーションの流れに、大きな違いはなく、海外のどの国でも、言

語の違いはありますが、業務オペレーションの流れにも大きな違いはありません。

このため、当社の輸出入の業務システムは、世界で均一なサービスをお客様にご提供するために、標準オペレーション、同一のシステムを展開しています。

発地、着地それぞれで国際貨物輸送システムが稼働していますが、日本では税関のAIR-NACCS(エア・ナックス)との接続により輸出入申告のスピードアップが可能であるため、国際通信ネットワークを経由した海外現法のシステムとリアルタイムにデータ交換を行い、情報の共有化、事務の簡素化を実施しています。

【倉庫管理システム】

お客様のワールドワイドでのサプライチェーンマネジメントをサポートするため、当社では倉庫管理システムを構築し提供しています(図-1)。

このシステムの特徴は、倉庫内の多様な業務を機械化する機能を装備していることのほかに、国内外を問わず、当社の倉庫に保管されている貨物の在庫管理が、一括してお客様の端末からできることです。

たとえば、日本のお客様が、米国とシンガポールの当社の倉庫に製品を保管していただいている場合、製品ごとの在庫状況、もしくは倉庫単位での状況を保管場所に関係なく、全世界どこからでもインターネット経由で把握することが可能です。

【日本通運の海外ネットワーク】

それでは、国際物流サービスをグローバルに展開することを可能としている、当社の海外ネットワークについてご紹介いたします。

当社の国際業務をサポートしているサーバは、日本以外に、欧州ではイギリス、ドイツ、オランダ、ベルギーの計4拠点、アジア・オセアニアでは香港、シンガポール、マレーシア、タイ、オーストラリアの計5拠点、米州ではアメリカの1拠点に設置しています。

それらのサーバをネットワークで接続し、当社の海外

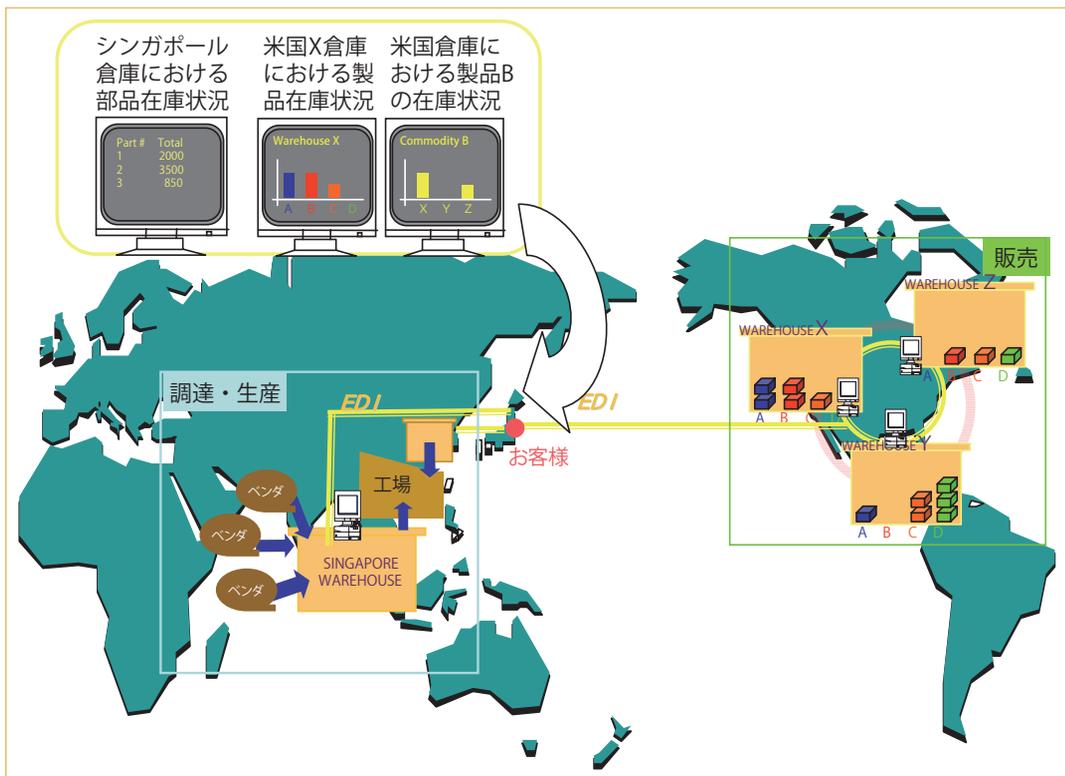


図-1 倉庫管理システム

現地法人 37 カ国, 196 都市の運用を行っています。

【海外の安全対策の考え方】

米国で 2001 年 9 月 11 日に発生した同時多発テロ, 2005 年 8 月に中国, 東欧を襲った大洪水, そして米国でのハリケーン “カトリーナ” などの経験から, 海外では多くの企業が災害復旧体制の改善を実施してきました。

また, システムの復旧をふまえた情報システムの安全対策について, お客様のビッド条件に入ることも多くなっています。

このため, 当社では, 「大規模災害, テロなどによりシステム障害が発生した場合でも 48 時間以内にシステムを復旧する」, 「障害後も顧客, 従業員, およびベンダとの通信能力を確保する」をビジネスの継続要件とし, 免震構造設計のデータセンターの利用, バックアップセンターの設置, およびネットワーク回線の二重化を推進しています。

それでは, 海外における災害対策について, 米国を例にご説明します。

現在, 米国のサーバは本番用をニュージャージー (東海岸), バックアップ用をコロラド (西海岸) のデータセンターに設置しています。

本番用とバックアップ用とで, 直線距離で 4,000km 以上離れており, この距離は東京か

らベトナムまでと同じぐらいの距離となります。

また, ネットワークについては ニューヨーク中継局とサンノゼ中継局の 2 カ所に接続しています。

米国に設置しているサーバには, 米国内の約 60 拠点およびカナダ, メキシコ内の拠点が, すべて接続されています。

米国内のネットワークを簡単に表しますと, 図-2 のようになります。基本的に, データセンターと各支店を結ぶ回線は二重化を実施し, 通信障害に備えています。イメージをつかんでいただくために, 図は簡略化していますが, 同様の構成で米国内の約 60 拠点に敷設されています。

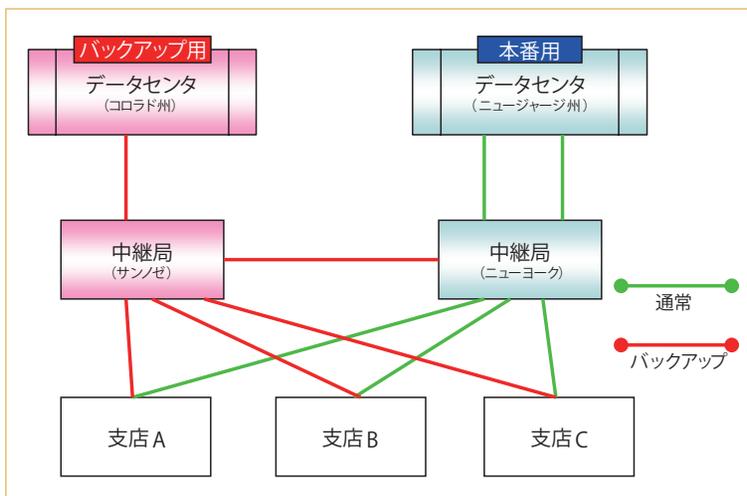


図-2 米国内ネットワーク概要図

それでは、実際に障害が発生した場合に、どのようにバックアップが行われるのかを説明します。

通常は支店からニューヨーク中継局を経由してニュージャージーのデータセンタに接続しています。

たとえば、支店と中継局間で回線障害が発生したとします。その場合、支店からはサンノゼ中継局を経由しニューヨーク中継局、ニュージャージーの本番データセンタに接続します。現在、この切り替え作業は手動ですが、自動で切り替えが可能ないように支店ごとに設定変更作業を実施していく予定です(図-3)。

また、バックアップルートが正常に稼働するか、現時点では不定期ではありますが、バックアップ試験を実施しています。

続いて、サーバ機器の障害が発生した場合をご紹介します。

先ほどの回線障害と同様に、通常は支店からニューヨーク中継局を経由してニュージャージーのデータセンタに接続しています。

今度は、災害等の原因でニュージャージーのデータセンタで障害が発生したとします。

その場合、支店からはサンノゼ中継局を経由しバックアップ用のコロラド州のデータセンタへ接続します。

このように、障害場所が特定できれば、バックアップルートにより、早急な運用回復が図れると考えています。

米国の例をご説明しましたが、当社では欧州およびアジア・オセアニアにおいても、同様にサーバ、回線の二重化を推進しています。

【対応事例① 9.11 米国同時多発テロ】

2001年9月11日に起こった米国同時多発テロにより、世界貿易センタービルが倒壊し、地下に埋設されていた通信回線ケーブルが切断されました。当時、米国の本番用サーバはニューヨークのスタテン島にあり、この影響で、データセンタの機能が停止しました。

この時点で、回線復旧の見込みがまったく立たなかったことから、バックアップセンタで運用を再開すべく、バックアップ機にデータのセットアップ作業を開始し、9月14日にはバックアップセンタで運用を開始しました。なお、本番データセンタの機能が回復するまで、その後10日間ほどかかっています。

当時は、本番機とバックアップ機の間でのデータ同期はリアルタイムに行われておらず、バックアップした磁気テープを送付し手動でローディングする必要がありますが

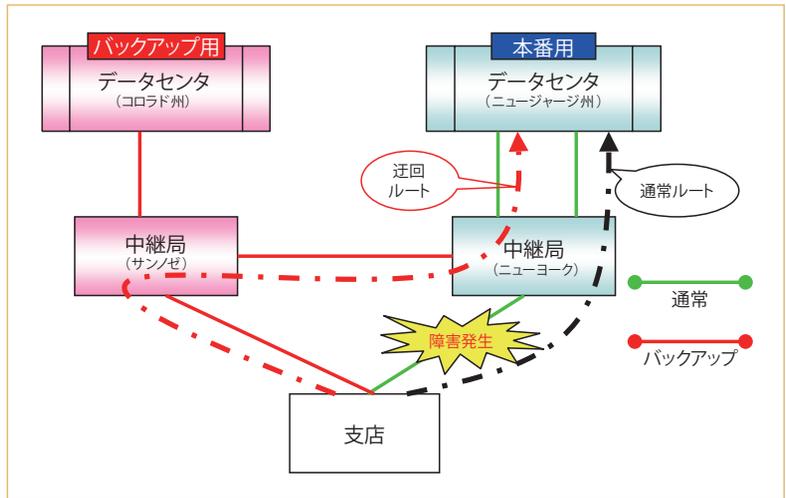


図-3 回線障害発生時の対応

した。

実際に復旧作業を行ってみて、いくつかの問題が判明しました。

1つは磁気テープによるデータセットアップに予想以上の時間がかかったこと、もう1つはバックアップセンタのリソースが十分でないため縮退運転を余儀なくされ業務上の制約が生じたことがあげられます。

当社では、そのことをふまえ、本番サーバとバックアップサーバ間でデータのリアルタイム複製の実施、十分なリソースを持ったバックアップサーバの準備、セキュリティに優れたニュージャージーのデータセンタへの移転をその後実施しています。

【対応事例② 台湾沖地震】

2006年12月26日台湾沖で地震が発生し、多くの通信キャリアの国際海底ケーブルが切断されました。

当社でも日本—香港間のデータ通信回線が不通となり、アジア・オセアニア域内のデータ通信が停止いたしました。しかし、その災害の翌日には通信経路を日本—米国—香港に切り替え、通信の確保を行いました。

以上、対応事例についてご紹介いたしました。当社では、2007年度から特定の地域だけに限らず、全世界中のネットワークの冗長化を推進しており、障害時の復旧時間短縮に取り組んでいます。

国内物流における 情報システムの安全対策

【国内の安全対策の考え方】

国内の安全対策の考え方ですが、大規模災害が発生しメインのシステムに障害が発生した場合でも、最低限データ、プログラムなどの資産の保全が可能なバック

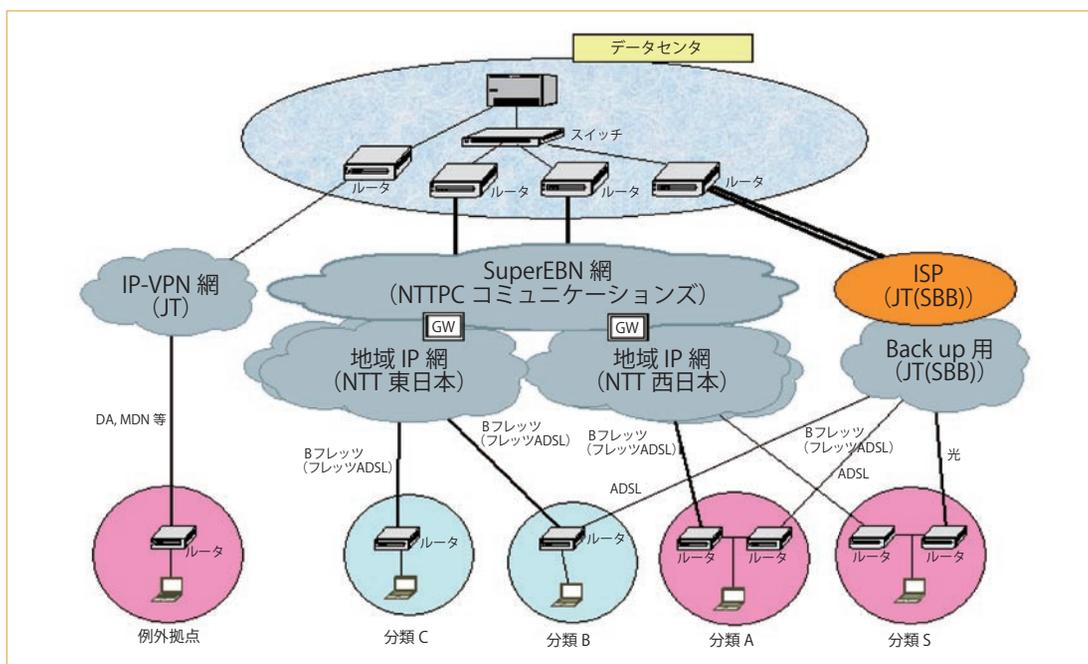


図-4 国内ネットワーク概要図

アップ体制の整備、および障害が発生した場合でも顧客、従業員、およびベンダとの通信能力の確保が可能な構成を目指しています。

また、当社は、災害対策基本法の指定公共機関として、公共のために協力する責務を負っており非常時の通信手段の確保は特に重要となっています。

このため、主要なネットワーク回線の冗長化を実施し、非常時の通信手段として、災害時優先電話の設置、衛星携帯電話の主要拠点への配備、全国900拠点にIP電話を使用した内線電話網の構築を実施し非常時の連絡手段を確保しています。

【ネットワークの冗長化】

現在の国内ネットワークは、光回線、ADSL回線など低価格で高速な回線の普及が進んできたため、2006年にデジタルアクセス回線、ATM回線を使用したネットワークから切り替えを実施しました。

新ネットワークの構築にあたっては、データ量の増加に対応するため通信速度の高速化、コストの削減に加えて、耐障害性の向上を盛り込んでいます。

このため、回線はNTTとソフトバンク2社の回線を組み合わせて使用し回線の冗長化を図っています。

また、冗長化に伴うコスト増を最小限に抑えるため、拠点を、最重要拠点、重要拠点、通常拠点、簡易拠点に分類した上で、それぞれの重要度に応じた対策をきめ細かく実施しました（図-4）。

たとえば、最重要拠点では、2社の回線をそれぞれ引き込み二重化した上でルータなどの通信機器も二重化

し、回線障害、機器障害が発生した場合は最大でも90秒後にはバックアップに切り替わるように設計していますが、簡易拠点では、回線の冗長化は行わず、論理的なパスの二重化のみで対応しています。

【データセンターの安全対策】

当社のデータセンターは、経済産業省、総務省などの安全基準に適合した施設に設置しています。

主な災害対策として、耐震構造設計に加えて、電源の2系統受電の実施、ガスタービン自家発電機の設置などを行っています。

また、災害時に運用要員が確保できなくなる事態を避けるため、24時間365日体制で保守運用要員を常駐させています。

【国内の安全対策の問題点】

以上、国内の安全対策について、ご説明いたしました。国内の安全対策についての問題点について少し触れます。

情報システムの安全対策において、バックアップのデータセンター設置が米国の例などから考えても有効な対策であると考えています。

海外においては、バックアップセンターの設置を実施していますが、国内についてはバックアップセンターを設置していません。

その理由として、最も大きな要因はコストの問題です。低コストを阻害する要因として、バックアップセンターやバックアップ機器を災害時に低コストでレンタルする

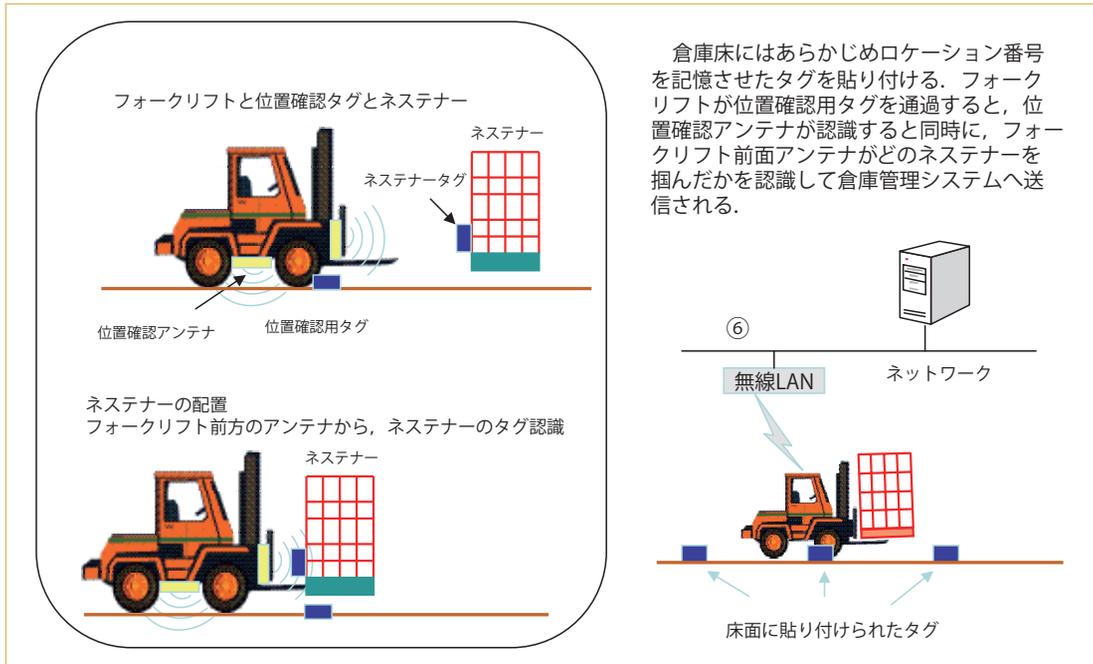


図-5 トランクルームロケーション管理

ようなサービスが国内では提供されていないこと、システムの標準化が遅れているために、さまざまな機器、OS、ミドルウェアを個別に用意しなくてはならないなどが原因と考えられます。

なお、国内で低コストのレンタルサービスが提供されない理由として、日本は、東京一極集中が進んでいるため、東京が壊滅した場合を想定して、多くのリソースを準備する必要がありますが、米国の場合は、大都市が分散されているため全体の20%程度のリソースを用意するだけで対応が可能という側面があると考えています。

また、国内の運送業界では、海外のようにバックアップセンターの設置がピットの要件に挙げられることはまだなく、安全対策のコストを価格に転嫁できないなどの要因も挙げられます。

以上、当社の国内外の安全対策について説明をいたしました。お客様とのEDIによるデータ交換や全世界規模の在庫管理など、物流の現場において情報システムはなくてはならない存在となっています。

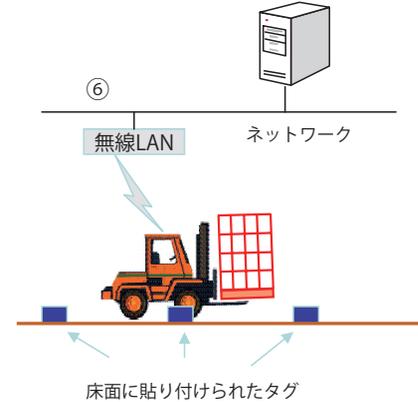
特に、ネットワークは物流の神経というべき重要な存在となっており、これらの障害が物流の麻痺に繋がる可能性が高く、企業の危機管理上も安全対策は重要となっています。

~~~~~  
RFIDなどの新技術による  
モノと情報の結びつけ  
~~~~~

【当社のRFIDへの取り組み】

当社では、2006年1月にEPCグローバルに参加し、

倉庫床にはあらかじめロケーション番号を記憶させたタグを貼り付ける。フォークリフトが位置確認用タグを通過すると、位置確認アンテナが認識すると同時に、フォークリフト前面アンテナがどのネステナーを掴んだかを認識して倉庫管理システムへ送信される。



物流分野におけるRFIDの活用方法について、実証実験を実施し、実際の業務への導入も行うなど積極的に取り組んでいます。

当社においては、2003年から2006年にかけては、多くのRFIDプロジェクトはウォールマートをはじめとしてリテーラーの納入条件をクリアするために行ってきました。

ところが、2007年になって、自社の業務効率化など自社の目標達成のためのRFID技術利用プロジェクトが多く見られるようになってきています。

では、いくつか事例をご紹介します。

【トランクルームロケーション管理】

海外に転勤されるお客様の荷物をお預かりするトランクルームのロケーション管理をRFIDで自動化するシステムを2007年4月から品川で稼働させています。

RFIDタグを用いて、ネステナー（荷物ラック）管理から、倉庫全体の管理までを行います。

内容は、倉庫内の床とネステナーにRFIDタグを貼り付け、フォークリフト前面と下部にRFIDリーダを設置しています。

フォークリフトがネステナーのRFIDタグを読むと同時に、床面のRFIDタグを読み取り、ネステナーと設置場所を自動認識し、ロケーション管理を行う仕組みです（図-5）。

なお、車載端末は、無線LANによりリアルタイムにデータをサーバに送っています。

システム導入により、フォークリフト運転者の作業時

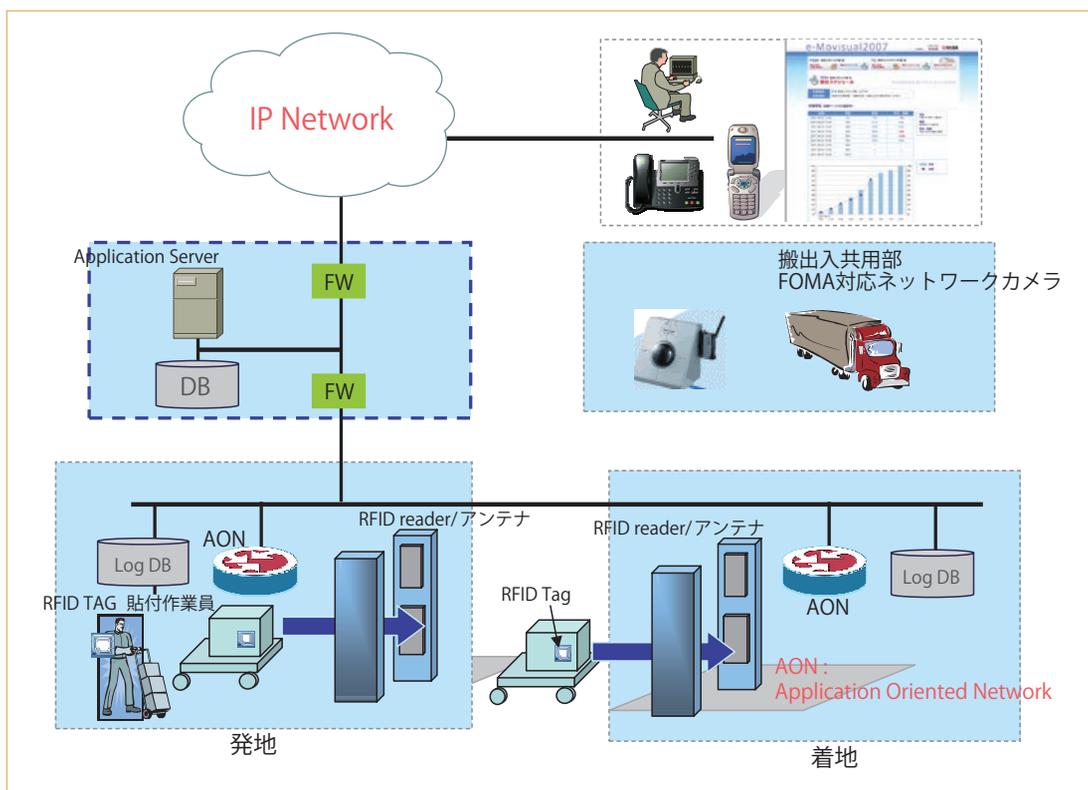


図-6 事務所移転 RFID 実証実験

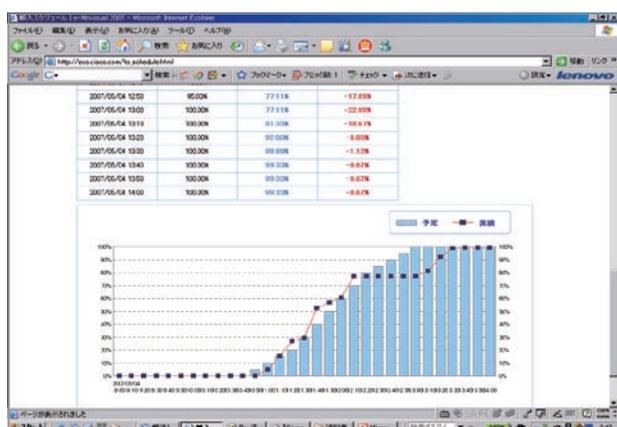


図-7 事務所移転進捗管理画面

間の短縮、手動によるデータ入力ミスの防止、倉庫内のロケーション情報のリアルタイムの把握などの効果が上がっています。

【事務所移転 RFID 実証実験】

事務所移転時に、RFIDを利用して荷物の管理を行う実証実験をシスコシステムズと共同で2007年5月に実施しました。

移転荷物にRFIDタグを貼付し発着地にリーダを設置して移転荷物の管理をリアルタイムで行います(図-6)。

図-7は、移転作業の進捗を管理する画面で、青色の

バーが予定、折れ線グラフが実績です。

このように、移転作業の進捗が、リアルタイムに把握でき、荷物の紛失などの事故も防止できる効果がありました。

また、リーダ設置付近の壁面の材質によって読み取り精度が大きく影響を受けるなど、課題も明確になっています。

【ユニホーム管理】

2007年10月にユニホームを一新すると同時にユニホーム、帽子にRFIDを埋め込み管理を実施しています。

特に当社では、引越や宅配など、お客様のご自宅に直接伺う業務をはじめ、さまざまな分野の仕事を行っていますので、管理を厳正に行う必要があります。

また、ユニホームは、会社から従業員に貸与するものですから、貸与から返却、その後リサイクルされるまでのライフサイクルを、きちんと把握する必要があります。

従来は、ユニホームに貼付されたバーコードで管理を行っていましたが、1着ずつバーコードリーダでスキャンする必要があり、約16万点にも及ぶ物品管理に多くの手間と工数がかかっていました。

これを、RFID化を行うことにより、管理にかかる手間が大幅に低減しています。

【RFIDの問題点／要望点】

最後になりましたが、RFID普及のための問題点・要望点をお話します。

現状ではRFIDタグ、リーダー/ライター等の機器がまだコスト高であり、より一層のコスト削減が求められます。

また、読み取り精度についても、物流シーンで最大限に活用するためには、荷物に貼付した大量のタグを一括で100%に近い精度で読み取る性能が求められますが、現状のRFIDは、残念ながらまだこの条件を満たしていません。

現状では、100%近い読み取り精度を得るためには、1個1個のタグを順次読み取りする必要があり、バーコードとの差別化をどのように図るかが課題となります。

併せて、業界を超えた利用ルールの策定が必要と考えています。このままでは、バーコードのように、商品管

理タグ、輸送管理タグ、在庫管理タグなど1つの商品に多くのタグが貼付される状況になってしまう恐れがあります。

以上、情報システムの安全対策、RFIDの活用について事例をご紹介しましたが、当社は、お客様に適した物流システムを最新のIT技術を駆使して創造・構築することを目指し、今後も継続して安全対策、物流の新しい技術の導入について積極的に取り組んでいきます。

(平成20年2月18日受付)

~~~~~  
佐野弘明  
hiroaki-sano@nittsu.co.jp

日本通運(株)IT部門担当取締役執行役員。1972年日本通運(株)入社。8年間情報システム業務に従事。その後、総務人事部門業務従事後、札幌、岡山で同社支店長を経験。2005年より情報システム部長を経て現職。  
~~~~~