先進のユーザー事例❺ HAソリューションによる２重化体制

大阪シーリング印刷株式会社

ネットワークの4重化やHA導入で
業務継続性を最大化する安全なインフラを構築

POINT

- ●AS/400時代からさまざまな工夫で障害・災害対策を実施
- ●Power 520の導入を機にHAソリューションを「Bitis HA」へ
- ●ネットワークの4重化／ルータの2重化で出荷業務の安全性を高める

COMPANY PROFILE

創業：1927年　設立：1954年
本社：大阪府大阪市
資本金：3億2443万9200円
売上高：706億5100万円　(2008年1月)
従業員数：2530名　(2008年1月)
http://www.osp.co.jp/

Power 520の導入を機に HAソリューションを「Bitis HA」へ

大阪シーリング印刷の主要業務は、シールやラベル、フィルム製品といった各種のパッケージ印刷である。商品ラベルやステッカー、プリンタ用ラベルなどのラベル類は年間60万種類、販売量は500億枚に上り、業界のトップシェアを誇る。最近は特にペットボトルや農産物に使われるフィルム包装が好調で、今年はその製造に特化した新工場が竣工した。

同社はシステム/360、システム/34時代からのユーザーで、販売管理・生産管理・会計の各システムを現在もSystem i上で自社開発によりさらに発展させ運用している。

同社は、早くから災害対策・障害対策に取り組んできた。1988年にAS/400を導入した当時は、それまで使用していたシステム/38をバックアップ機とし、2台体制のホットスタンバイを自社開発により実現している。

トランザクション量の増大で、本番機からバックアップ機へのデータ転送が次第に長時間に及ぶようになり、やがてこの体制は維持できなくなった。しかしその後も障害対策としてAS/400のミラーリング機能を利用するとともに、前日分の全データを記録したカートリッジテープを大阪本社と、距離の離れた名古屋支店へ毎日送付し保管することで、前日の全データが安全に常に2カ所に存在する仕組みを作り、広域災害を想定したデータの保全に努めてきた。

本格的な2重化体制が実現したのは、2004年12月。阪神・淡路大震災の発生から10年が経過した当時、いくつかの大地震や水害が発生し、再び災害の危険性が指摘され始めたのを受け、本格的な災害対策を実施することになった。この時は、「System i 520」を大阪本社と小倉工場に導入し、HA（ハイ・アベイラビリティ）ソリューションを利用して、完全ホットスタンバイの体制を整えた。

この体制は約5年続いたが、今年3月、POWER6を搭載した2台の「Power 520 Express i Edition（9408-M25）」へのリプレースを機に、HAソリューションを「Bitis HA」（ビーティス）へ移行した。

「今回Bitis HAへ移行しても特にコスト増にならないこともあり、またビーティスのサポート力の高さは以前からよく分かっていたので、思い切ってHAソリューションのリプレースに踏み切り、さらに万全を期したホットスタンバイの構築を目指しました。Bitis HAの機能性の高さに加え、520のマシンスペックが大きく向上したこともあって、本番機・バックアップ機間の同期スピードは以前と比較にならないほど速くなりました。幸い、現在までのところバックアップ機へ切り替える事態は発生していませんが、インフラの安全性はさらに向上しました」（管理本部 システム部の大森良和次長）

大森良和氏
管理本部 システム部
次長

ルータの2重化・回線の4重化で万全のセキュリティ体制

同社では520へのリプレースやBitis HAへの移行と同時期から、内部統制を念頭に置いたセキュリティ体制の強化にも取り組んでいる。

内部統制では事業の継続性が求められることもあり、社内のインフラ環境を再調査し、セキュリティ面の問題点を洗い出した。2006年11月に一部の回線障害が発生したことを契機に、業務の中でも特に出荷業務に支障をきたさないよう、同社では、サーバーマシンの障害、広域災害の発生、ネットワーク回線の不通、落雷などによるルータの故障、ウイルス感染など、想定し得るあらゆるリスクを検討し、事業継続性を高めるための「考え得る最大の対策」(大森次長)を実施することになったのである。

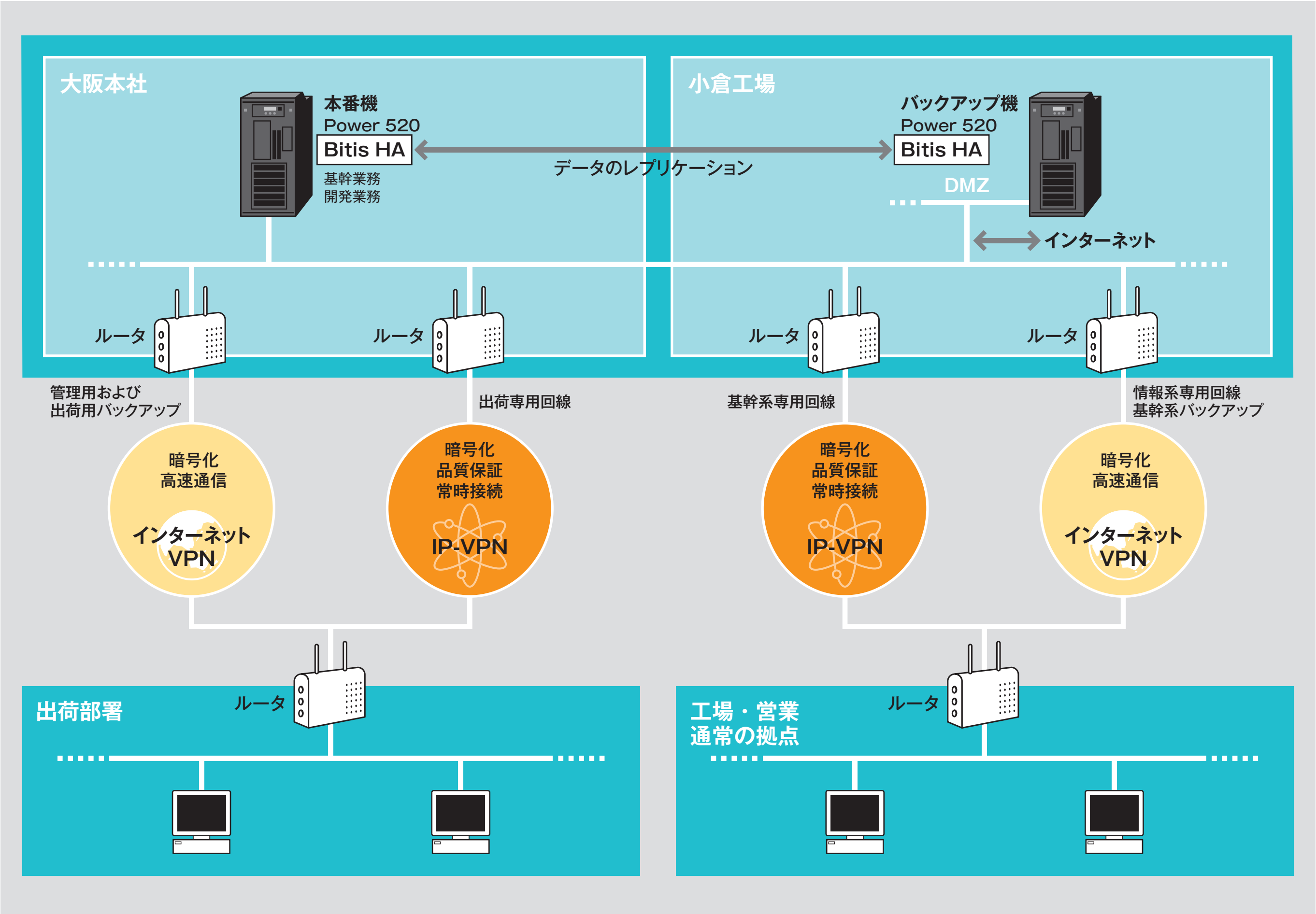
対策の中核として着手したのは、ルータの2重化とネットワークの4重化であった。つまり出荷専用回線と基幹系専用回線を完全に分離したのである。

基幹系専用回線にはIP-VPN、そのバックアップ回線および情報系専用回線にはインターネットVPN。一方の出荷専用回線としては別系統のIP-VPN、そのバックアップ回線もやはり別系統のインターネットVPNを利用し、4つのルートを確保した。

出荷専用回線はインターネットに接続できない回線とし、IPアドレスを固定し、接続できる端末を制限した。さらに出荷用端末の一部には、Windows 機能を制限してダム端末化し、業務に不要なパソコンの機能を大幅に制限した。回線障害の発生やルータの故障に加え、万一のウイルス侵入や外部からの不正アクセスといった脅威を阻止するため、出荷専用端末を基幹系の通常回線から、そしてインターネットからも完全に分離したのである。

2007年からスタートしたこのセキュリティ・プロジェクトは、今年竣工した新工場の環境整備を最後に、2009年3月に完了した。現時点で業務継続性を最大化する万全のインフラ環境が実現したといえるだろう。

次のテーマとしては、営業部門からの要望に対応し、携帯端末から基幹システムへ安全にアクセスし、出荷状況や在庫の照会・出荷依頼などを可能にするモバイル環境の構築が進行中である。安全なインフラ環境をベースに、今後は多様なWebアプリケーション開発に挑戦していくことになりそうだ。



図表 システム概要