



## ファイアウォールのロードバランシングに Cisco ACE 4710 を採用 ロードバランサの冗長化で耐障害性を強化

### 北海道旅客鉄道株式会社

北海道旅客鉄道株式会社（以下、JR 北海道）は、鉄道事業を基軸として、多角的事業を展開する企業だ。同社ではいくつかの Web サービスを提供しているが、なかでも列車の運行情報システムは非常にアクセス数が多く、特に冬期はアクセス数がピークを迎える。このピーク時における膨大なトラフィックを処理するために、Web システムには複数のファイアウォールを設置し、Active/Active 構成での冗長化を実装している。2009 年 6 月、それまで遠隔施設に設置していた Web 環境の本社社屋への移設に伴い、老朽化していたロードバランサの見直しが行われ、現状のファイアウォールの冗長構成を維持しつつ、ロードバランサ自身を冗長化することで可用性をさらに向上させることになった。このような設計を可能にするロードバランサとして採用されたのが Cisco ACE 4710 である。

#### ●導入の背景 / 課題

- Web システムを本社社屋と離れた遠隔施設に設置していたため、通信費のほか、メンテナンス人員の移動時間などのコストが発生していた。
- 本社社屋内に設置場所を確保し、メンテナンスの効率化および運用コストの削減とともに、既存のシステムを見直し、老朽化していた設備を置き換えることになった。
- 移設時のダウンタイムを最小限に抑えることが重要であり、既存のシステムの構成をできるだけ踏襲する設計とした。
- ファイアウォールの負荷分散を行っているロードバランサが老朽化していたため、これを置き換えることとした。機器選定にあたっては、既存のファイアウォールを継続使用しながら、ロードバランサ自身を冗長化することが要件となった。

#### ●導入ソリューション

- Cisco ACE 4710

#### ●導入効果

- MAC-address sticky 機能により、従来必要とされていた特別なルーティング設計を施す必要もなく、容易にファイアウォールのロードバランシングを実現できた。
- ファイアウォールの Active/Active 構成での冗長化に加え、ロードバランサの冗長化により、システムの耐障害性が強化された。
- 機器保守などのランニング コストが削減された。

### システム移設に伴い、ロードバランサをリプレース ロードバランサ自身の冗長化が要件

JR 北海道では、これまで通信機器類を本社社屋から離れた遠隔施設に設置し、Web システムをそこで運用していた。しかし、Web 環境にアクセスするための通信費、メンテナンス時の手間や移動時間がかかることから、本社社屋への移設が検討されるようになった。そして 2009 年、設置スペースが確保されたこともあり、Web システム全体の本社社屋への移設が決定された。

システム移設にあたっては、既存の構成をできる限り踏襲し、速やかに移設できることも重要視された。「道内の拠点も多いため、基幹の構成を変えてシステムに障害が発生しないよう、ネットワークの構成はなるべく変えない形で設計しました」と JR 北海道・経営企画部の大河原 久雄氏は語る。しかし、機器の見直しは必要である。継続使用できる既存の機器はそのまま移設するが、老朽化している機器はこれを機会に置き換える。今回の移設では、サーバおよびファイアウォールの負荷分散を行っていたロードバランサが置き換え対象となった。さらに、耐障害性を考慮してロードバランサ自身を冗長化することとなった。

### Cisco ACE に組み込みのロードバランシング機能が採用の決め手に MAC-address sticky 機能で複雑な経路制御の問題を解消

JR 北海道では、当初、1 台のファイアウォールで Web サービスを運用していた。しかし、アクセスが集中する冬期にトラフィックの問題が発生したことがあり、5 年ほど前からファイアウォールを 2 台に増設し、Active/Active の冗長構成で運用している。ただし、ファイアウォールの冗長化には、サーバの負荷分散とは異なる設計上の注意点がある。それは、ファイアウォールが「通信経路上にあるデバイス」であるため、複数のファイアウォールに負荷分散しようとすると、宛先 IP アドレスを変えずにトランスペアレントに転送を行う機能や、往きと帰りのパケットが同じファイアウォールを経由するようなルーティング設計が必要になるということだ。そのために JR 北海道では、以前はルーティング デザインを工夫することでこれを実現してい

## ファイアウォールのロードバランシングに Cisco ACE 4710 を採用 ロードバランサの冗長化で耐障害性を強化

北海道旅客鉄道株式会社



「ファイアウォールを Active/Active で負荷分散し、かつ障害時には接続するファイアウォールを切り替えることができ、機器自身も冗長化可能なロードバランサを求めています」

北海道旅客鉄道株式会社  
総合企画本部  
経営企画部  
大河原 久雄氏

だが、複雑な経路制御は運用上の問題となっていた。しかし、ファイアウォールを Active/Active 構成で冗長化し、かつロードバランサまで冗長化できる機能を持った製品は、かなり限定されたという。ここで採用されたのが、Cisco ACE である。Cisco ACE は、ファイアウォールの負荷分散に伴う経路制御に関する問題を、MAC-address sticky 機能によって解決する。これは、ソース アドレスの MAC アドレスを参照することによって、帰りのパケットを往きのパケットと同じ経路を経由させる機能である。もちろん、MAC アドレスを参照するので、ルーティング デザインの工夫は不要である。ファイアウォールの負荷分散に必須の機能とも言えるが、この MAC-address sticky 機能をサポートしているロードバランサは Cisco ACE だけであった。

さらに、ロードバランサ自体を冗長化するという構成に欠かせないもう 1 つの機能がステートフル フェイルオーバーだった。ステートフル フェイルオーバーをサポートしていないロードバランサが非常に多いなかで、Cisco ACE にはステートフル フェイルオーバー機能が備わっている。つまり、Cisco ACE の 1 台に障害が発生すると、既存の接続を維持したまま、最短 1 秒で透過的に別の Cisco ACE へ処理が移行する。MAC-address sticky 機能とステートフル フェイルオーバー機能を含め、必要条件をすべて満たすことができたのは、Cisco ACE だけであり、これが採用の決め手になった。

### すべての機能を冗長化

#### ロードバランサはステートフル フェイルオーバーにも対応

「冗長化」は今回の移設で重要なキーワードであった。JR 北海道のネットワークの運用を担当する、株式会社北海道ジェイ・アール・システム開発の佐藤 敦氏も、移行の大きな成果として「冗長化」を挙げる。障害対策が強化され、どこで障害が起きてもフェイルオーバーされることは、担当者はもちろん企業にとつ

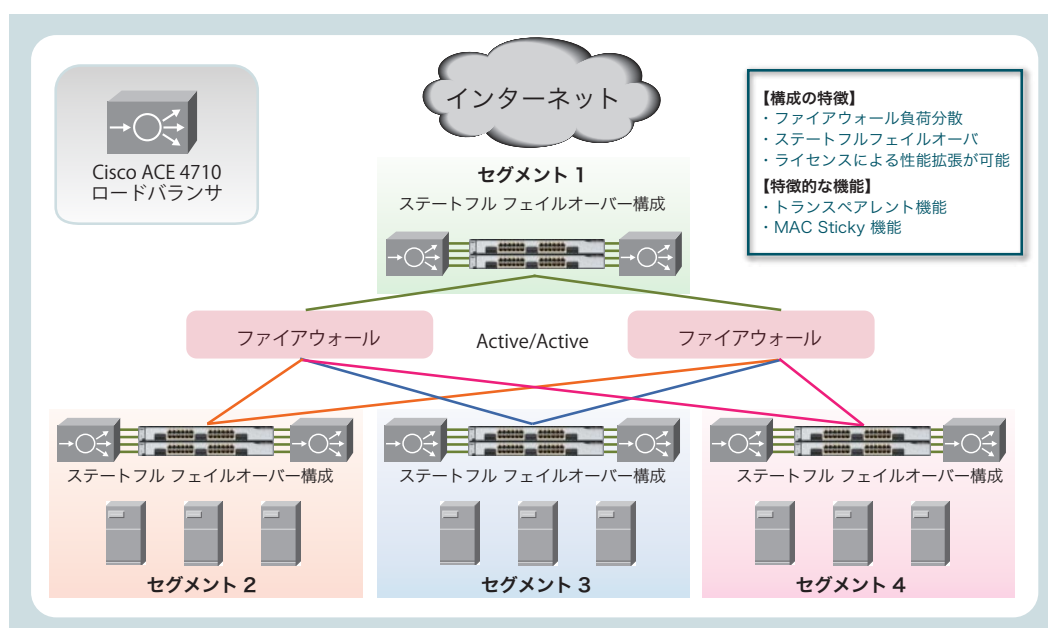


図 Cisco ACE 4710 を使用した冗長構成

## ファイアウォールのロードバランシングに Cisco ACE 4710 を採用 ロードバランサの冗長化で耐障害性を強化

北海道旅客鉄道株式会社



「ファイアウォール周辺の機器がすべて冗長化され、ダウンタイムを最小限に抑えられるようになりました」

株式会社北海道ジェイ・アール・システム開発  
運用部  
ネットワーク運用  
佐藤 敦氏

でも大きな安心につながる。「冗長化によってダウンタイムを最小限に抑えられるようになった。現時点では障害は起きていないが、ダウンタイムを短くするというコンセプトに合致している」（佐藤氏）。

ファイアウォールの Active/Active 冗長構成はもちろん、ロードバランサをステートフルフェイルオーバーで冗長化した。これ以外にも、スイッチである Cisco Catalyst 2950 を二重化、スタッキング構成の Cisco Catalyst 3750 によるハードウェア冗長も実装した。これで、Web システム関連の通信機器をすべて冗長化したことになる。

冗長化によって機器の数は増えたが、以前のような特別な経路制御が不要になったため、論理的な設計が以前よりシンプルになった。障害が起きにくく、万が一障害が発生したときにも原因の切り分けが容易になる。管理しやすいシステムになったのだ。

### シスコのラボで疑似環境を構築 綿密な事前検証とスムーズな移行

大河原氏は、今回の移行を「非常にスムーズにいった」と評価している。移設に失敗すれば、同社の Web システム全体が停止してしまい、列車運行にも影響を与えるような大問題を引き起こしかねない。スムーズに移設できたのは、ACE の導入に際し、システム インテグレータのネットワンシステムズ社とシスコが CPOC（Customer Proof Of Concept）というシスコのラボで共同で行った事前検証が大きく貢献している。機器の導入にあたっては、想定される問題と対策を事前に検証しておくことが重要であることはもちろんだが、今回、夜間の限られた時間で移設を完了しなければいけないことや、Web システムの物理的な移設という緊張度の高い作業であるという点で、事前検証は通常にも増して重要な作業となった。

ファイアウォールの二重化を実装しているケースは少ない。さらに Active/Active 構成で運用するという事例はきわめてめずらしい。1 週間のラボでの検証では、ACE 以外にも既存のファイアウォールを 2 台用意して冗長化するなど、実際とまったく同じ環境を再現し、どこに障害が発生してもネットワークの疎通が確保され、セキュリティが確保されること等、一連の動きをすべて検証した。

こうした綿密な事前検証により ACE を問題なく導入できることがわかったため、物理的な移設作業の準備に十分に時間を割くことができたという。移設当日は列



## ファイアウォールのロードバランシングに Cisco ACE 4710 を採用 ロードバランサの冗長化で耐障害性を強化

北海道旅客鉄道株式会社

車の遅延により、23 時からを予定していた作業開始が少し遅れたが、朝 7 時までの移設作業を 1 時間短縮して完了することができた。

### ランニング コストの削減を実現

今回の移行により、さまざまな面でランニング コストの削減を実現した。まず、Web システムを本社社屋へ移設することで、移設のそもそもの目的であった遠隔施設との通信費を削減することができた。さらに、運用管理に際してメンテナンス要員が移動時間をかけて出向くといった煩雑さも解消された。また、Cisco ACE を含め、Web システム関連の機器をすべて冗長化したことで、障害対策が強化されたと同時に、サポート コストが削減できた。「機器が冗長化されていれば、両方の機器が同時に壊れる可能性は非常に低い。これまでの 24 時間 365 日の保守契約を見直し、冗長構成になっている部分については保守契約を 8 時間契約に変更した。これがランニング コストの削減にもなった」と大原氏は語る。

### 将来の拡張には仮想化機能とライセンス アップグレードで対応

今回の機器の置き換えにより、トラフィックのピークを迎える冬期であっても帯域幅は十分にまかなえている。しかし今後、Web サービスのさらなる拡充を図るにあたり、機器を入れ換えたり、システムを停止したりせずに帯域幅の増強や機能を拡張できる「ライセンス アップグレード機能は Cisco ACE の利点ですね」と佐藤氏。拡張性の高さも評価された。将来の拡張性を考えた場合、ACE の仮想化機能は強い味方だ。今後は、イントラネットなど他のシステムも含め、仮想化機能を利用することも検討していきたいという。

#### profile

### 北海道旅客鉄道株式会社

本 社 : 北海道札幌市中央区北 11 条  
15 丁目 1-1  
設 立 : 昭和 62 年 4 月 1 日  
資 本 金 : 90 億円  
従 業 員 数 : 7,469 人  
鉄道営業キロ : 2,499.8km  
旅客列車運転本数 (1 日あたり) : 1,292 本  
車 両 数 : 1,125 両  
駅 / 施設数 : 581  
(平成 21 年 4 月現在)

北海道の基幹的輸送機関として、安全で安定した輸送をきめ細やかなサービスの提供に努めている。また、「旅とくらしのサポート事業グループ」として、常にお客様第一を実践し、交通ネットワークを基盤に旅とくらしの分野において、安心して利用できるサービスを提供するとともに、お客様の満足と感動の実現をめざす。

<http://www.jrhokkaido.co.jp/>

© 2010 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ 関係を意味するものではありません。(0809R)

この資料の記載内容は 2010 年 7 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー  
<http://www.cisco.com/jp>  
お問い合わせ先: シスコ コンタクトセンター  
0120-092-255 (フリーコール、携帯・PHS 含む)  
電話受付時間: 平日 10:00 ~ 12:00、13:00 ~ 17:00  
<http://www.cisco.com/jp/go/contactcenter/>

#### お問い合わせ先