エレクトロニックコマース・セキュリティ特集

UDC ［681.324：343.45］：［343.98：681.326.7］

高可用性ファイアウォール
High Availability Fire Wall

橘　　喜胤
Yoshitane Tachibana

要　　旨

高可用性が要求されるシステムに対応するためには，ファイアウォールの二重化が必要である。本稿では，ファイアウォールを二重化するための技術を解説した後，代表的なファイアウォール製品であるCheckPoint社のFireWall-1を二重化する場合の沖電気が推奨するソリューションを紹介している。また，もう一つの高可用性の手段としてファイアウォールのロードシェアリングについて記述している。

1．ま　え　が　き

インターネット利用におけるセキュリティ対策の要として，ファイアウォールの利用が定着してきている。最近では，電子メールやWebによる情報提供に加え，電子商取引などミッションクリティカルな用途にもインターネットを使用するシステムが増えており，セキュリティ面のみならず，障害発生時にも連続運用可能である高可用性も求められるようになってきている。

高可用性が要求されるシステムでは，サーバ，ルータ，ハブなど，システムを構成するすべての機器の二重化を行なう必要があり，ファイアウォールもその例外ではない。

本稿では，ファイアウォールの高可用性に必要とされる技術を紹介し，代表的なファイアウォール製品であるCheckPoint社のFireWall-1に対する沖電気が推奨する高可用性実現方法について述べる。

2．一般的な二重化の方式

二重化には，大きくわけて２つの方式がある。１つ目は，ACT-STANDBY方式である。

ACT-STANDBY方式では，通常動作しているのは１台のみで，残りの機器は待機状態にあり，動作していない。ここで，動作している機器はACT状態に，待機している機器はSTANDBY状態にあると言う。

もう１つの方式として，ACT-ACT方式がある。ACT-ACT方式では，すべての機器が同時に動作を行なう。いずれかの機器に障害が発生した場合は，障害の発生した機器を除いた残りの機器で継続して処理を行なう。

ACT-STANDBY方式では，障害が発生していない状態で動作を行なう機器をPrimaryと呼び，待機している機器をSecondaryと呼ぶ。

本稿では，ACT-STANDBY方式のファイアウォール二重化について解説し，最後にACT-ACT方式のロードシェアリング構成も紹介する。

3．一般的な二重化に必要な技術

一般的に，二重化には次の技術が必要である。

１）障害の検出
２）経路の切り替え
３）二重化状態の監視

3.1　障害の検出

障害検出では，一般的にハートビート方式が用いられる。ハートビート方式では，二重化した機器間で定期的に生存確認の情報交換を行なう。

この情報交換をハートビートと呼び，これが途切れ

橘　喜胤
システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部　開発第四チーム

ることにより，障害が発生したことを検出する。

ハートビートは，EthernetやRS-232などを経由して数秒間隔で行なわれる。

ハートビート方式では，ハートビートを行う経路（ケーブルやハブなど）に障害が発生すると，二重化の状態が不安定になる。このため，ハートビートを行なう経路を２つ以上用意することが推奨される。２つ目のハートビートをセカンドハートビートと呼ぶ。

また，ハートビート以外の障害検出手段として，アプリケーションの動作をコマンドなどを用いて定期的に確認し，その結果によって障害検出を行なうなどのカスタマイズが可能な製品もある。

3.2　経路の切り替え

障害を検出し，PrimaryからSecondaryに切り替えを行なう場合，経路も同時に切り替える必要がある。経路の切り替えには，次の方式がある。

１）IPアドレスのみを引継ぐ

２）IPアドレス，MACアドレスの両方を引継ぐ

３）上記以外（動的ルーティングの利用など）

１つ目の方式は，IPアドレスのみを引き継ぎ，MACアドレスについてはそれぞれの機器が持つものを使用する方式である。この方式では，同一セグメントに存在する他の機器が切り替え前のMACアドレスをキャッシュしていた場合には，このエントリが無効になるまでは経路が切り替わらないことになる。

２つ目の方式では，切り替えが発生すると，Primaryで使用していたIPアドレス，MACアドレスともSecondaryに移動する。これにより切り替え前と同じMACアドレスを使って通信ができるため，同一セグメントの機器がMACアドレスをキャッシュしていても，問題なく切り替えることができる。

この２つ以外に，動的ルーティングやネームサービスを用いる方式が存在する。しかし，これらの方式では，使用するアプリケーションに依存したり，キャッシングの問題があるため，あまり汎用的ではない。

3.3　二重化状態の監視

二重化したシステムで障害が発生した場合には，自動的にSecondaryへの切り替えが行なわれ，システムの運用は続行される。しかし，このままの状態でシステムを放置しておくと，二重障害によりシステムがダウンする危険性が高く，できるだけ早く障害の原因をとり除く必要がある。

このため，二重化状態の監視を行ない，障害発生を早期に発見する必要がある。一般的に，ネットワーク機器はSNMP(Simple Network Management Protocol)をサポートしており，これにより状態の監視が可能となる。

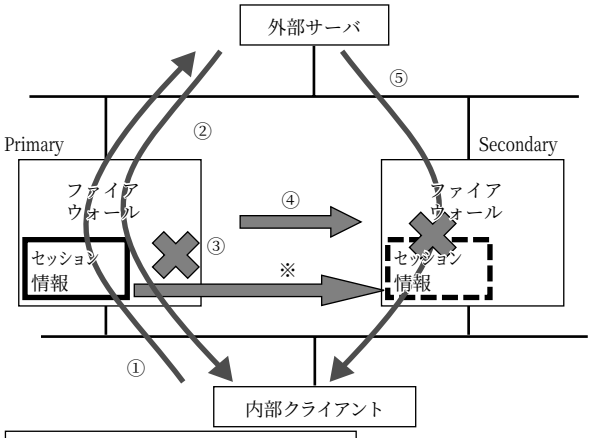
また，専用の監視ツール（GUIなど）が提供される製品や，システムに合わせてカスタマイズできるインタフェースを持つ製品も存在する。

4．ファイアウォールの二重化に必要な技術

前節で，一般的な二重化に必要とされる技術について解説した。ファイアウォールを二重化する場合には，これらの技術に加えて，通信中のセッション情報の引き継ぎが大変重要である。

ファイアウォールの場合，障害発生時に通信中であったTCPセッションが，切り替え発生後も中断されることなく通信を継続するためには，セッション情報を引き継ぐ必要がある。

これは，通信の方向性が，通信途中のパケットだけでは判断できず，通信開始時の情報を元に判断する必



①内部クライアントから外部サーバへの通信開始
②外部サーバから内部クライアントへの応答
③Primary に障害発生
④Primary からSecondary へ切り替え
⑤外部サーバから内部クライアントへの応答は、
Secondary へ届くがファイアウォールは、外部サーバから
内部クライアントへの接続とみなし、通信を遮断

※セッション情報の同期ができていれば⑤の返送通信は、
Secondary でも許可される

図１　切り替え時のTCPセッション切断
Fig. 1　Abortion of TCP session at switching

要があるためである（図１参照）。

ファイアウォールで管理しているセッション情報の交換を定期的に行なうことにより，これらの情報を共有することができる。

ファイアウォール製品によっては，二重化に対応していてもこの機能を持たないものもあるため，注意が必要である。この場合は，切り替え発生時に，通信中のTCPセッションは切断されてしまう。

5．沖電気が推奨する高可用性ファイアウォール

沖電気は，1995年よりCheckPoint社のFireWall-1によるファイアウォール構築を行なっている。

FireWall-1は世界的にNo.１のシェアを持つ代表的なファイアウォール製品であり，二重化に必要な複数ファイアウォール間のセッション情報の同期機能を標準機能として提供している。

しかし，FireWall-1単体では障害の検出や経路の切り替えを行なうことができないため，これらの動作を行なう方式を組み合わせて構成する必要がある。これらの動作を行う方式にはさまざまなものがある。

本稿では，FireWall-1専用機を用いたソリューションと，FireWall-1専用の二重化ソフトを用いたソリューションの２つを紹介する。

6．ソリューション１

１つ目のソリューションとして，FireWall-1が動作する専用機を用いた二重化ソリューションを紹介する。従来，FireWall-1は，HP-UX＊1），Solaris＊1），Windows-NT＊1）などのOSの上で動作していた。しかし最近では，初期設定，メンテナンス性に優れた専用機が登場している。ここでは，二重化に必要な機能を標準で持ち，メンテナンス性に優れているNOKIA社のNOKIA　IPシリーズ（以下NOKIAと略）を紹介する。構成例を図２に示す。

6.1　障害の検出

NOKIAでは，障害の検出にRFC2338準拠のVRRP（Virtual Router Redundancy Protocol）を用いる。

VRRPはハートビートを行ない相互に生存確認を行なう。

VRRPでは，それぞれの機器が優先度を持ち，最も優先度の高い機器がPrimaryとなる。

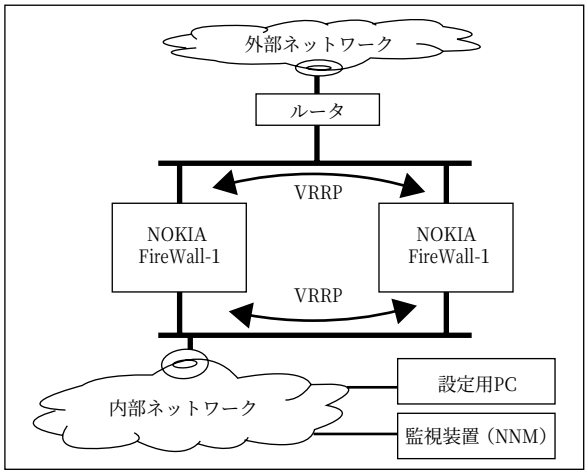


図２　NOKIAによる二重化
Fig. 2　Redundant fire wall configuration by NOKIA

ハートビートの交換間隔は秒単位で設定可能であり，最小間隔は1秒である。いずれかの機器に障害が発生し，連続して３回パケットが途絶えると，残った機器の間で最も高い優先度の機器がACT状態になる。

6.2　経路の切り替え

VRRPでは，障害が発生したインタフェースでのみ切り替えが発生し，他のインタフェースでは切り替えが発生しない。このため，経路を動的ルーティングを利用して切り替える必要がある。

しかし，動的ルーティングはネットワークの構成によっては使用できないことがあり，またセキュリティに脆弱性を持たせることにもつながる。

この問題を解決するために，NOKIAではMonitored Circuitと呼ばれる独自の機能を提供している。この機能は，VRRPの動作に加え，他のインタフェースの監視を行なうものである。

Monitored　Circuitを用いることにより，すべてのインタフェースを同時に切り替えることができる。

また，障害時の切り替えでは，MACアドレスとIPアドレスの両方が引き継がれるため，他の装置がMACアドレスをキャッシュしていても，通信に問題が発生することはない。

6.3　状態の監視

NOKIAでは，SNMPを用いて二重化の状態を監視することが可能である。SNMPを用いて監視を行うためには，Hewlett-Packard（HP）社のネットワークノードマネジャ（NNM）＊2）などの装置が必要である。

NNMなどの監視装置がない場合は，定期的にWebイ

＊1）HP-UX, Solaris, Windows-NTは，それぞれHewlett-Packard社，Sun Microsystems社，Microsoft社の商標。　＊2）ネットワークノードマネジャ（NNM）はHewlett-Packard社の商標。

ンタフェースを用いてVRRPの二重化状態を調べ，障害が発生していないことを確認する必要がある。

7．ソリューション２

２つ目のソリューションとして，二重化専用ソフトを利用したソリューションを紹介する。二重化専用ソフトには，HP社のService　Guardのようにアプリケーションを特定しない汎用的なものと，StoneSoft社のStoneBeatのようにファイアウォールに特化したものの２つがある。ここでは，StoneBeatを用いたソリューションを紹介する。構成例を図３に示す。

7.1　障害の検出

StoneBeatでは，ハートビートは，独自のプロトコルを用いて専用のLANインタフェースを通して行なう。また，ハートビート以外にテストサブシステムと呼ばれる障害検出機能が用意されておりFireWall-1のプロセスの生存確認，LANインタフェースのUp/Down，pingによる疎通確認，ログ領域あふれなどの検出が可能である。さらに，ユーザ作成のシェルスクリプトにより，システムに特化した障害検出項目の追加も可能である。

7.2　経路の切り替え

StoneBeatでは，PrimaryのみがIPアドレスおよびMACアドレスを持ち，Secondaryは持たない。（ただしハートビート用のインタフェースは除く）
StoneBeatが障害を検出し，切り替えを行なう際に，ハートビートLAN以外のすべてのインタフェースのIPアドレスとMACアドレスをPrimaryからSecondaryに引き継ぐ。

7.3　状態の監視

StoneBeatは専用のGUIを持ち，このGUIによってリアルタイムにPrimaryとSecondaryの状態表示を行なう。

また，SNMPによる通知も可能であり，NNMなどの監視装置が存在する場合には，StoneBeatも含めネットワークを統合的に監視することが可能である。

8．もう一つの高可用性 (ロードシェアリング)

内部LANや，ネットワークサービスプロバイダの基幹ネットワーク部分にファイアウォールを設置するような場合，高速なネットワークと大量のトラフィックをサポートする必要がある。

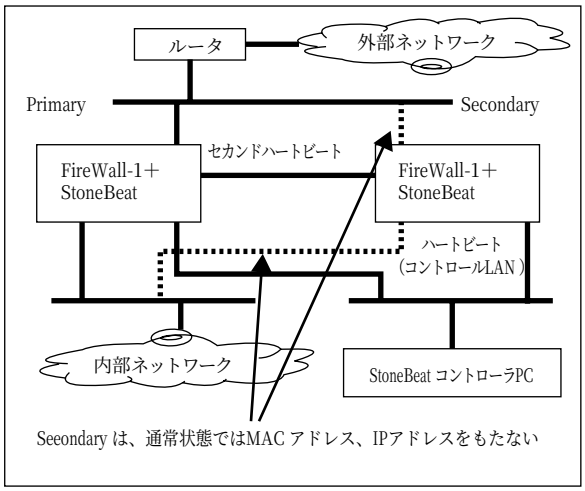


図３　StoneBeatによる二重化
Fig. 3　Redandant fire wall configuration by StoneBeat

本稿で採りあげた二重化では，通常状態で通信を行なっている機器はPrimaryのみである。このため，100Mbpsを超えるようなスループットを実現するためには，高価なマシンを用意する必要がある。また，GigaBitEthernetのような高速なネットワークの性能を十分に利用することができない。

このような高速なネットワーク性能が要求されるシステムでは，複数の機器が同時に処理を行なうロードシェアリング構成が必要である。

StoneBeatには，FullClusterと呼ばれる製品が存在し，16台までのロードシェアリング構成を採ることができ，GigaBitEthernetにも対応可能である。

9．あ　と　が　き

ファイアウォールの２つの二重化ソリューションを紹介した。沖電気では，今後，メンテナンス性を重視されるケースにはNOKIA　IPシリーズを，より高い信頼性を求められるシステムにはStoneBeatを用いた二重化ファイアウォールを提供していく。

また，より高速なネットワークには，StoneBeat FullClusterを用いたロードシェアリング構成により対応していく予定である。