

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5498102号  
(P5498102)

(45) 発行日 平成26年5月21日 (2014. 5. 21)

(24) 登録日 平成26年3月14日 (2014. 3. 14)

(51) Int. Cl. F 1  
G 0 6 F 11/20 (2006. 01) G 0 6 F 11/20 3 1 0 F

請求項の数 9 (全 60 頁)

<p>(21) 出願番号 特願2009-202297 (P2009-202297)                  (22) 出願日 平成21年9月2日 (2009. 9. 2)                  (65) 公開番号 特開2011-53918 (P2011-53918A)                  (43) 公開日 平成23年3月17日 (2011. 3. 17)                  審査請求日 平成23年12月7日 (2011. 12. 7)</p>	<p>(73) 特許権者 504411166                  アラクサラネットワークス株式会社                  神奈川県川崎市幸区鹿島田一丁目1番2号                  (74) 代理人 110000028                  特許業務法人明成国際特許事務所                  (72) 発明者 新井 雅也                  神奈川県川崎市幸区鹿島田890 アラク                  サラネットワークス株式会社内                  (72) 発明者 野崎 信司                  神奈川県川崎市幸区鹿島田890 アラク                  サラネットワークス株式会社内                  審査官 ▲高▼橋 正▲徳▼</p>
--	---

最終頁に続く

(54) 【発明の名称】 ネットワークシステム、ネットワーク中継装置、それらの制御方法

(57) 【特許請求の範囲】

【請求項1】

ネットワークシステムであって、  
 所定のサービスを提供可能な第1の処理装置と、  
 前記所定のサービスを提供可能な第2の処理装置と、  
 前記所定のサービスを利用するクライアント装置と、  
 前記第1の処理装置と、前記第2の処理装置と、前記クライアント装置とインターフェースを介して直接的または間接的に接続され、各装置間のパケットを中継するネットワーク中継装置と、

を備え、

前記第1の処理装置と、前記第2の処理装置のアドレスは同一に設定され、  
 前記ネットワーク中継装置は、

第1の仮想ネットワークの経路情報を記憶する第1の経路情報記憶部と、

第2の仮想ネットワークの経路情報を記憶する第2の経路情報記憶部と、

前記第1の処理装置と、前記第2の処理装置と、前記クライアント装置のそれぞれが、前記第1の仮想ネットワークと、前記第2の仮想ネットワークのいずれに所属するのかを定義したVRF定義情報を記憶するVRF定義情報記憶部と、

パケットを受信した際に、前記VRF定義情報に従って前記パケットの送信元の装置が所属する仮想ネットワークを判定し、前記送信元の装置が所属する仮想ネットワークに対応した経路情報を用いて経路探索をするパケット転送処理部と、

前記第 1 の処理装置および前記第 2 の処理装置の少なくともいずれか一方の状態を監視し、前記監視の対象である処理装置の状態を判定する状態監視部と、

前記処理装置の状態に基づいて、前記経路情報および前記 V R F 定義情報の少なくともいずれか一方を更新するフェイルオーバー処理部と、  
を備え、

前記ネットワーク中継装置は、前記クライアント装置が接続されている前記インタフェースから受信したパケットであって、前記アドレスを先とする受信パケットを、前記第 1 の処理装置または前記第 2 の処理装置のうち、前記所定のサービスを提供可能な状態の一方の処理装置へ中継する、ネットワークシステム。

【請求項 2】

所定のサービスを提供可能であり、かつ、アドレスが同一に設定された第 1 の処理装置および第 2 の処理装置と、前記所定のサービスを利用するクライアント装置とインタフェースを介して直接的または間接的に接続され、各装置間のパケットを中継するネットワーク中継装置であって、

第 1 の仮想ネットワークの経路情報を記憶する第 1 の経路情報記憶部と、

第 2 の仮想ネットワークの経路情報を記憶する第 2 の経路情報記憶部と、

前記第 1 の処理装置と、前記第 2 の処理装置と、前記クライアント装置のそれぞれが、前記第 1 の仮想ネットワークと、前記第 2 の仮想ネットワークのいずれに所属するのかを定義した V R F 定義情報を記憶する V R F 定義情報記憶部と、

パケットを受信した際に、前記 V R F 定義情報に従って前記パケットの送信元の装置が所属する仮想ネットワークを判定し、前記送信元の装置が所属する仮想ネットワークに対応した経路情報を用いて経路探索をするパケット転送処理部と、

前記第 1 の処理装置および前記第 2 の処理装置の少なくともいずれか一方の状態を監視し、前記監視の対象である処理装置の状態を判定する状態監視部と、

前記処理装置の状態に基づいて、前記経路情報および前記 V R F 定義情報の少なくともいずれか一方を更新するフェイルオーバー処理部と、  
を備え、

前記クライアント装置が接続されている前記インタフェースから受信したパケットであって、前記アドレスを先とする受信パケットを、前記第 1 の処理装置または前記第 2 の処理装置のうち、前記所定のサービスを提供可能な状態の一方の処理装置へ中継する、ネットワーク中継装置。

【請求項 3】

請求項 2 記載のネットワーク中継装置であって、

前記 V R F 定義情報には、

前記第 1 の処理装置と、前記クライアント装置とが前記第 1 の仮想ネットワークに所属し、

前記第 2 の処理装置が前記第 2 の仮想ネットワークに所属する、  
ことが予め定義され、

前記状態監視部は、少なくとも前記第 1 の仮想ネットワークに所属する前記第 1 の処理装置の状態を監視し、

前記フェイルオーバー処理部は、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第 1 の仮想ネットワークに所属している前記クライアント装置を、前記第 2 の仮想ネットワークに所属させるように、V R F 定義情報を更新する、ネットワーク中継装置。

【請求項 4】

請求項 2 記載のネットワーク中継装置であって、

前記 V R F 定義情報には、

前記第 1 の処理装置と、前記クライアント装置とが前記第 1 の仮想ネットワークに所属し、

前記第 2 の処理装置が前記第 2 の仮想ネットワークに所属する、

10

20

30

40

50

ことが予め定義され、

前記状態監視部は、少なくとも前記第1の仮想ネットワークに所属する処理装置の状態を監視し、

前記フェイルオーバ処理部は、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第2の処理装置と、前記クライアント装置とを前記第1の仮想ネットワークに所属させ、前記第1の処理装置を前記第2の仮想ネットワークに所属させるように、V R F定義情報を更新する、ネットワーク中継装置。

【請求項5】

請求項2記載のネットワーク中継装置であって、

前記V R F定義情報には、

前記第1の処理装置と、前記クライアント装置とが前記第1の仮想ネットワークに所属し、

前記第2の処理装置が前記第2の仮想ネットワークに所属する、

ことが予め定義され、

前記状態監視部は、少なくとも前記第1の仮想ネットワークに所属する前記第1の処理装置の状態を監視し、

前記フェイルオーバ処理部は、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第2の仮想ネットワークの経路情報に、前記第1の仮想ネットワークの経路情報中の前記クライアント装置に関する経路情報をコピーし、

前記第1の仮想ネットワークの経路情報中の、前記第1の処理装置のアドレスをアテ先アドレスとするエントリの出力先インタフェースを、前記第2の処理装置が接続されているインタフェースへと更新する、ネットワーク中継装置。

【請求項6】

請求項2記載のネットワーク中継装置であって、

前記V R F定義情報には、

前記第1の処理装置が前記第1の仮想ネットワークに所属し、

前記第2の処理装置が前記第2の仮想ネットワークに所属し、

前記クライアント装置が前記第1の仮想ネットワークおよび前記第2の仮想ネットワークの両方に所属する、

ことが予め定義され、

前記パケット転送処理部は、さらに、

前記クライアント装置からパケットを受信した際は、予め定められた規則に従って、前記パケットの送信元である装置毎に、前記第1の仮想ネットワークの経路情報および前記第2の仮想ネットワークの経路情報のいずれか一方を用いて経路探索をし、

前記状態監視部は、前記第1の仮想ネットワークに所属する前記第1の処理装置と、前記第2の仮想ネットワークに所属する前記第2の処理装置の両方の状態を監視し、

前記フェイルオーバ処理部は、監視されている一方の処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第1の仮想ネットワークおよび前記第2の仮想ネットワークの両方に所属していた前記クライアント装置を、前記障害状態であると判定された一方の処理装置が所属する仮想ネットワークから除外するように、V R F定義情報を更新する、ネットワーク中継装置。

【請求項7】

請求項2ないし6のいずれか一項記載のネットワーク中継装置であって、さらに、

前記ネットワーク中継装置を管理する管理装置と接続され、

前記フェイルオーバ処理部は、前記管理装置から前記経路情報および前記V R F定義情報の少なくともいずれか一方を更新するためのフェイルオーバ指示を受信し、前記経路情報および前記V R F定義情報の少なくともいずれか一方を更新する、ネットワーク中継装

10

20

30

40

50

置。

【請求項 8】

請求項 3 または 6 または 7 のいずれか一項記載のネットワーク中継装置であって、  
 前記状態監視部は、さらに、  
 前記監視の対象である処理装置が、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された後においても前記処理装置の監視を継続し、  
 前記フェイルオーバー処理部は、前記処理装置が前記所定のサービスを提供可能な状態へ復旧したと判定された場合に、  
 前記経路情報および前記 V R F 定義情報の少なくともいずれか一方を、前記障害状態であると判定される前の状態へと更新するリカバリ処理と、  
 前記経路情報および前記 V R F 定義情報の更新を行わないロック処理と、  
 を選択的に実行可能な、ネットワーク中継装置。

10

【請求項 9】

所定のサービスを提供可能な第 1 の処理装置および第 2 の処理装置と、前記所定のサービスを利用するクライアント装置と、前記第 1 の処理装置と、前記第 2 の処理装置と、前記クライアント装置とインタフェースを介して直接的または間接的に接続され、各装置間のパケットを中継するネットワーク中継装置と、を備えるネットワークシステムの制御方法であって、

前記第 1 の処理装置と、前記第 2 の処理装置のアドレスを同一に設定する工程と、

第 1 の仮想ネットワークの経路情報を記憶する工程と、

20

第 2 の仮想ネットワークの経路情報を記憶する工程と、

前記第 1 の処理装置と、前記第 2 の処理装置と、前記クライアント装置のそれぞれが、前記第 1 の仮想ネットワークと、前記第 2 の仮想ネットワークのいずれに所属するのかを定義した V R F 定義情報を記憶する工程と、

パケットを受信した際に、前記 V R F 定義情報に従って前記パケットの送信元の装置が所属する仮想ネットワークを判定し、前記送信元の装置が所属する仮想ネットワークに対応した経路情報を用いて経路探索をする工程と、

前記第 1 の処理装置および前記第 2 の処理装置の少なくともいずれか一方の状態を監視し、前記監視の対象である処理装置の状態を判定する工程と、

前記処理装置の状態に基づいて、前記経路情報および前記 V R F 定義情報の少なくともいずれか一方を更新する工程と、

30

前記ネットワーク中継装置が、前記クライアント装置が接続されている前記インタフェースから受信した前記アドレスをあて先とする受信パケットを、前記第 1 の処理装置または前記第 2 の処理装置のうち、前記所定のサービスを提供可能な状態の一方の処理装置へ中継する工程と、

を備える、ネットワークシステムの制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワークシステムに関する。

40

【背景技術】

【0002】

高い信頼性 ( R e l i a b i l i t y ) および可用性 ( A v a i l a b i l i t y ) を有するサーバネットワークシステムを構築するための方法として、フェイルオーバーが知られている。フェイルオーバーとは、運用系サーバ ( もしくは、システム、ネットワーク ) で異常事態が発生したとき、自動的に冗長な待機系サーバ ( もしくは、システム、ネットワーク ) に切り換える機能を意味する。例えば、コールドスタンバイによるフェイルオーバー方法では、サービス ( 例えば、 W E B サービス等 ) を提供する運用サーバと、通常は他の処理を行っている、或いは、電源を切って待機している予備サーバとによりシステムを構成する。コールドスタンバイでは、運用サーバで障害が発生した場合、運用サーバに設定

50

していた情報（例えば、IPアドレス）を、予備サーバへ再設定することによってフェイルオーバー処理を実現する（例えば、特許文献1）。

【0003】

他の例としては、ホットスタンバイによるフェイルオーバー方法がある。ホットスタンバイによるフェイルオーバー方法では、サービスを提供可能な複数のサーバと、ロードバランサまたはDNS（Domain Name System）サーバとによりシステムを構成する。ホットスタンバイでは、サービスを提供している複数のサーバのいずれかに障害が発生した場合、システムの構成に応じて、次のようにしてフェイルオーバー処理を実現する。ロードバランサを使用する構成では、ロードバランサにおいて、障害が発生したサーバへ処理要求を送信しないようにすることで、フェイルオーバー処理を実現する（例えば、特許文献2）。DNSを使用する構成では、DNSサーバにおいて、障害が発生したサーバのIPアドレスを通知しないようにすることで、フェイルオーバー処理を実現する（例えば、特許文献3）。

10

【0004】

従来のコールドスタンバイによるフェイルオーバー方法では、運用サーバから予備サーバへサービスを引き継ぐ際の情報の再設定に時間を要する。このため、長時間サービスが停止してしまうという問題があった。一方、ホットスタンバイによるフェイルオーバー方法では、短時間でのサービス再開が可能である反面、ロードバランサやDNSサーバといったネットワークシステムの構成要素の導入が必要となる。このため、ネットワークシステムが複雑になるという問題があった。

20

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2005-258847号公報

【特許文献2】特開2005-56347号公報

【特許文献3】特開2005-250626号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

本発明は、サーバネットワークシステムにおいて、構成要素の追加をすることなく、かつ、短時間でのフェイルオーバーが可能な技術を提供することを目的とする。

30

【課題を解決するための手段】

【0007】

本発明は、上述の課題の少なくとも一部を解決するためになされたものであり、以下の形態として実現することができる。ネットワークシステムであって、所定のサービスを提供可能な第1の処理装置と、前記所定のサービスを提供可能な第2の処理装置と、前記所定のサービスを利用するクライアント装置と、前記第1の処理装置と、前記第2の処理装置と、前記クライアント装置とインタフェースを介して直接的または間接的に接続され、各装置間のパケットを中継するネットワーク中継装置と、を備え、前記第1の処理装置と、前記第2の処理装置のアドレスは同一に設定され、前記ネットワーク中継装置は、第1の仮想ネットワークの経路情報を記憶する第1の経路情報記憶部と、第2の仮想ネットワークの経路情報を記憶する第2の経路情報記憶部と、前記第1の処理装置と、前記第2の処理装置と、前記クライアント装置のそれぞれが、前記第1の仮想ネットワークと、前記第2の仮想ネットワークのいずれに所属するのかを定義したVRF定義情報を記憶するVRF定義情報記憶部と、パケットを受信した際に、前記VRF定義情報に従って前記パケットの送信元の装置が所属する仮想ネットワークを判定し、前記送信元の装置が所属する仮想ネットワークに対応した経路情報を用いて経路探索をするパケット転送処理部と、前記第1の処理装置および前記第2の処理装置の少なくともいずれか一方の状態を監視し、前記監視の対象である処理装置の状態を判定する状態監視部と、前記処理装置の状態に基づいて、前記経路情報および前記VRF定義情報の少なくともいずれか一方を更新するフ

40

50

フェイルオーバー処理部と、を備え、前記ネットワーク中継装置は、前記クライアント装置が接続されている前記インタフェースから受信したパケットであって、前記アドレスをあて先とする受信パケットを、前記第1の処理装置または前記第2の処理装置のうち、前記所定のサービスを提供可能な状態の一方の処理装置へ中継する、ネットワークシステム。そのほか、本発明は、以下の形態又は適用例として実現することが可能である。

【0008】

[適用例1]

ネットワークシステムであって、  
 所定のサービスを提供可能な第1の処理装置と、  
 前記所定のサービスを提供可能な第2の処理装置と、  
 前記所定のサービスを利用するクライアント装置と、  
 前記第1の処理装置と、前記第2の処理装置と、前記クライアント装置とインタフェースを介して直接的または間接的に接続され、各装置間のパケットを中継するネットワーク中継装置と、  
 を備え、

前記第1の処理装置と、前記第2の処理装置のアドレスは同一に設定され、  
 前記ネットワーク中継装置は、前記クライアント装置が接続されている前記インタフェースから受信したパケットであって、前記アドレスをあて先とする受信パケットを、前記第1の処理装置または前記第2の処理装置のうち、前記所定のサービスを提供可能な状態の一方の処理装置へ中継する、ネットワークシステム。

この構成によれば、第1の処理装置と、第2の処理装置は、共に所定のサービスを提供可能であり、かつ、同一のアドレスが設定される。また、ネットワーク中継装置は、クライアント装置からの受信パケットを、第1の処理装置と第2の処理装置のうち、所定のサービスを提供可能な状態の一方の処理装置へ中継する。このため、サーバネットワークシステムにおいて、構成要素の追加をすることなく、かつ、短時間でのフェイルオーバーが可能となる。

【0009】

[適用例2]

適用例1記載のネットワークシステムであって、  
 前記ネットワーク中継装置は、  
 第1の仮想ネットワークの経路情報を記憶する第1の経路情報記憶部と、  
 第2の仮想ネットワークの経路情報を記憶する第2の経路情報記憶部と、  
 前記第1の処理装置と、前記第2の処理装置と、前記クライアント装置のそれぞれが、前記第1の仮想ネットワークと、前記第2の仮想ネットワークのいずれに所属するのかを定義したVRF定義情報を記憶するVRF定義情報記憶部と、

パケットを受信した際に、前記VRF定義情報に従って前記パケットの送信元の装置が所属する仮想ネットワークを判定し、前記送信元の装置が所属する仮想ネットワークに対応した経路情報を用いて経路探索をするパケット転送処理部と、

前記第1の処理装置および前記第2の処理装置の少なくともいずれか一方の状態を監視し、前記監視の対象である処理装置の状態を判定する状態監視部と、

前記処理装置の状態に基づいて、前記経路情報および前記VRF定義情報の少なくともいずれか一方を更新するフェイルオーバー処理部と、  
 を備える、ネットワークシステム。

この構成によれば、第1の処理装置と、第2の処理装置に、同一のアドレスを設定することができる。また、状態監視部は、第1の処理装置および第2の処理装置の少なくともいずれか一方の状態を監視する。フェイルオーバー処理部は、処理装置の状態に基づいて、経路情報およびVRF定義情報の少なくともいずれか一方を更新する。このため、サーバネットワークシステムにおいて、構成要素の追加をすることなく、かつ、短時間でのフェイルオーバーが可能となる。

【0010】

10

20

30

40

50

## [ 適用例 3 ]

適用例 2 記載のネットワークシステムであって、

前記 V R F 定義情報には、

前記第 1 の処理装置と、前記クライアント装置とが前記第 1 の仮想ネットワークに所属し、

前記第 2 の処理装置が前記第 2 の仮想ネットワークに所属する、

ことが予め定義され、

前記状態監視部は、少なくとも前記第 1 の仮想ネットワークに所属する前記第 1 の処理装置の状態を監視し、

前記フェイルオーバー処理部は、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第 1 の仮想ネットワークに所属している前記クライアント装置を、前記第 2 の仮想ネットワークに所属させるように、V R F 定義情報を更新する、ネットワークシステム。

この構成によれば、状態監視部は、クライアント装置に所定のサービスを提供する第 1 の仮想ネットワークに所属する第 1 の処理装置の状態を監視し、フェイルオーバー処理部は、当該処理装置がサービスを提供することができない障害状態であると判定された場合に、第 1 の仮想ネットワークに所属しているクライアント装置を、第 2 の仮想ネットワークに所属させるように、V R F 定義情報を更新する。このため、運用系サーバである第 1 の処理装置に障害が発生した場合であっても、V R F 定義情報の更新によって、スムーズに待機系サーバである第 2 の処理装置へのフェイルオーバーが可能となる。この結果、サーバネットワークシステムにおいて、構成要素の追加をすることなく、かつ、短時間でフェイルオーバーが実現できる。

## 【 0 0 1 1 】

## [ 適用例 4 ]

適用例 2 記載のネットワークシステムであって、

前記 V R F 定義情報には、

前記第 1 の処理装置と、前記クライアント装置とが前記第 1 の仮想ネットワークに所属し、

前記第 2 の処理装置が前記第 2 の仮想ネットワークに所属する、

ことが予め定義され、

前記状態監視部は、少なくとも前記第 1 の仮想ネットワークに所属する処理装置の状態を監視し、

前記フェイルオーバー処理部は、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第 2 の処理装置と、前記クライアント装置とを前記第 1 の仮想ネットワークに所属させ、前記第 1 の処理装置を前記第 2 の仮想ネットワークに所属させるように、V R F 定義情報を更新する、ネットワークシステム。

この構成によれば、状態監視部は、クライアント装置に所定のサービスを提供する第 1 の仮想ネットワークに所属する処理装置の状態を監視し、フェイルオーバー処理部は、当該処理装置がサービスを提供することができない障害状態であると判定された場合に、第 2 の処理装置と、クライアント装置とを第 1 の仮想ネットワークに所属させ、第 1 の処理装置を第 2 の仮想ネットワークに所属させるように、V R F 定義情報を更新する。このため、適用例 1 と同様の効果を得ることができる。また、フェイルオーバー処理部は、処理装置についての V R F 定義情報を更新する。このため、例えば、ネットワーク中継装置に接続される処理装置の数が、ネットワーク中継装置に接続されるクライアント装置の数よりも少ない場合には、V R F 定義情報の更新量を少なくすることができる。

## 【 0 0 1 2 】

## [ 適用例 5 ]

適用例 2 記載のネットワークシステムであって、

前記 V R F 定義情報には、

前記第 1 の処理装置と、前記クライアント装置とが前記第 1 の仮想ネットワークに所属し、

前記第 2 の処理装置が前記第 2 の仮想ネットワークに所属する、  
ことが予め定義され、

前記状態監視部は、少なくとも前記第 1 の仮想ネットワークに所属する前記第 1 の処理装置の状態を監視し、

前記フェイルオーバー処理部は、前記処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第 2 の仮想ネットワークの経路情報に、前記第 1 の仮想ネットワークの経路情報中の前記クライアント装置に関する経路情報をコピーし、

前記第 1 の仮想ネットワークの経路情報中の、前記第 1 の処理装置のアドレスをあて先アドレスとするエントリの出力先インタフェースを、前記第 2 の処理装置が接続されているインタフェースへと更新する、ネットワークシステム。

この構成によれば、状態監視部は、クライアント装置に所定のサービスを提供する第 1 の仮想ネットワークに所属する処理装置の状態を監視し、フェイルオーバー処理部は、当該処理装置がサービスを提供することができない障害状態であると判定された場合に、第 2 の仮想ネットワークの経路情報に、第 1 の仮想ネットワークの経路情報中のクライアント装置に関する経路情報をコピーし、第 1 の仮想ネットワークの経路情報中の、前記第 1 の処理装置のアドレスをあて先アドレスとするエントリの出力先インタフェースを、第 2 の処理装置が接続されているインタフェースへと更新する。この結果、例えば、ネットワーク中継装置の 1 つのインタフェースに対して、アドレスの異なる複数の処理装置が接続されている場合であっても、互いの処理装置の状態に影響されないフェイルオーバー処理が可能となる。

【 0 0 1 3 】

[ 適用例 6 ]

適用例 2 記載のネットワークシステムであって、

前記 V R F 定義情報には、

前記第 1 の処理装置が前記第 1 の仮想ネットワークに所属し、

前記第 2 の処理装置が前記第 2 の仮想ネットワークに所属し、

前記クライアント装置が前記第 1 の仮想ネットワークおよび前記第 2 の仮想ネットワークの両方に所属する、  
ことが予め定義され、

前記パケット転送処理部は、さらに、

前記クライアント装置からパケットを受信した際は、予め定められた規則に従って、前記パケットの送信元である装置毎に、前記第 1 の仮想ネットワークの経路情報および前記第 2 の仮想ネットワークの経路情報のいずれか一方を用いて経路探索をし、

前記状態監視部は、前記第 1 の仮想ネットワークに所属する前記第 1 の処理装置と、前記第 2 の仮想ネットワークに所属する前記第 2 の処理装置の両方の状態を監視し、

前記フェイルオーバー処理部は、監視されている一方の処理装置が前記所定のサービスを提供することができない障害状態であると判定された場合に、

前記第 1 の仮想ネットワークおよび前記第 2 の仮想ネットワークの両方に所属していた前記クライアント装置を、前記障害状態であると判定された一方の処理装置が所属する仮想ネットワークから除外するように、V R F 定義情報を更新する、ネットワークシステム。

この構成によれば、パケット転送処理部は、クライアント装置からパケットを受信した際に、パケットの送信元である装置毎に、予め定められた規則に従って第 1 の仮想ネットワークの経路情報および第 2 の仮想ネットワークの経路情報のいずれか一方を用いて経路探索を行う。このため、2 台の処理装置の両方をサービスの提供に使用することができる。従って、設備投資の観点から効率の良いネットワークシステムを提供することができる。さらに、状態監視部は、第 1 の仮想ネットワークに所属する第 1 の処理装置と、第 2 の

10

20

30

40

50

仮想ネットワークに所属する第2の処理装置の両方の状態を監視する。また、フェイルオーバー処理部は、監視対象であるいずれか一方の処理装置が障害状態であると判定された場合に、第1の仮想ネットワークおよび第2の仮想ネットワークの両方に所属していたクライアント装置を、障害状態であると判定された一方の処理装置が所属する仮想ネットワークから除外するように、V R F 定義情報を更新する。このため、適用例1と同様の効果を得ることができる。

【0014】

[適用例7]

適用例2ないし6のいずれか一項記載のネットワークシステムであって、さらに、前記ネットワーク中継装置を管理する管理装置を備え、  
前記管理装置は、

10

前記フェイルオーバー処理部に対して、前記経路情報および前記V R F 定義情報の少なくともいずれか一方を更新するためのフェイルオーバー指示を送信するフェイルオーバー管理部を備える、ネットワークシステム。

この構成によれば、管理装置のフェイルオーバー管理部は、ネットワーク中継装置のフェイルオーバー処理部に対して、経路情報およびV R F 定義情報の少なくともいずれか一方を更新するためのフェイルオーバー指示を送信する。このため、ネットワーク中継装置の管理装置が予め外部に設けられているような構成においても、適用例1と同様の効果を得ることができる。また、管理装置は、ネットワーク中継装置よりも高度な処理能力を有する場合が多い。従って、例えば、状態監視処理において、障害状態であるか否かの判定以外のより高度な判定（例えば、処理装置のC P U利用率等）を行うこともできる。

20

【0015】

[適用例8]

適用例3または6または7のいずれか一項記載のネットワークシステムであって、前記状態監視部は、さらに、

前記監視の対象である処理装置が、前記障害状態であると判定された後においても前記処理装置の監視を継続し、

前記フェイルオーバー処理部は、前記処理装置が前記所定のサービスを提供可能な状態へ復旧したと判定された場合に、

前記経路情報および前記V R F 定義情報の少なくともいずれか一方を、前記障害状態であると判定される前の状態へと更新するリカバリ処理と、

30

前記経路情報および前記V R F 定義情報の更新を行わないロック処理と、  
を選択的に実行可能な、ネットワークシステム。

この構成によれば、状態監視部は、監視の対象である処理装置が障害状態であると判定された後においても監視を継続する。そして、当該処理装置がサービスを提供可能な状態へ復旧したと判定された場合、フェイルオーバー処理部は、経路情報およびV R F 定義情報の少なくともいずれか一方を、障害状態であると判定される前の状態へと更新するリカバリ処理と、経路情報とV R F 定義情報との更新を行わないロック処理とを選択的に実行することができる。このため、例えば、システム管理者は、処理装置の復旧と同時にシステムが自動的にフェイルオーバーする運用方法（リカバリ処理）と、自ら処理装置の復旧を確認したうえで手動によりフェイルオーバーさせる運用方法（ロック処理）とを選択することができる。この結果、ネットワークシステムの運用の幅を広げることができる。

40

【0016】

なお、本発明は、種々の態様で実現することが可能である。例えば、ネットワークシステム、ネットワーク中継装置、それらの方法または装置の機能を実現するためのコンピュータプログラム、そのコンピュータプログラムを記録した記憶媒体等の形態で実現することができる。

【図面の簡単な説明】

【0017】

【図1】本発明の一実施例としてのネットワークシステム10の概略構成を示す説明図で

50

ある。

【図 2】 2 台のサーバの IP アドレス情報の一例を示す説明図である。

【図 3】 ホスト 3 0 1 の IP アドレス情報の一例を示す説明図である。

【図 4】 ホスト 3 0 2 の IP アドレス情報の一例を示す説明図である。

【図 5】 ネットワーク装置 1 0 0 の構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。

【図 6】 インタフェースデータベース 1 4 0 の一例を示す説明図である。

【図 7】 インタフェースデータベース 1 4 0 が図 6 で示した状態である場合における V R F 1 ルーティングテーブル 1 2 1 の一例を示す説明図である。

【図 8】 インタフェースデータベース 1 4 0 が図 6 で示した状態である場合における V R F 2 ルーティングテーブル 1 2 2 の一例を示す説明図である。 10

【図 9】 状態監視データベース 1 7 0 の一例を示す説明図である。

【図 1 0】 障害切替データベース 1 8 0 の一例を示す説明図である。

【図 1 1】 復旧切替データベース 1 9 0 の一例を示す説明図である。

【図 1 2】 運用サーバ 2 0 1 がサービスを提供し得る状態である場合のネットワークシステム 1 0 の動作を示す説明図である。

【図 1 3】 ネットワーク装置 1 0 0 におけるパケット転送処理の手順を示すフローチャートである。

【図 1 4】 状態監視処理の手順を示すフローチャートである。

【図 1 5】 図 1 4 のステップ S 5 0 7 において更新された後の状態監視データベース 1 7 0 を示す説明図である。 20

【図 1 6】 フェイルオーバー処理（図 1 4：ステップ S 5 0 8）の手順を示すフローチャートである。

【図 1 7】 図 1 6 のステップ S 6 0 1 において更新された後のインタフェースデータベース 1 4 0 を示す説明図である。

【図 1 8】 図 1 6 のステップ S 6 0 2 において更新された後の V R F 1 ルーティングテーブル 1 2 1 を示す説明図である。

【図 1 9】 図 1 6 のステップ S 6 0 2 において更新された後の V R F 2 ルーティングテーブル 1 2 2 を示す説明図である。

【図 2 0】 運用サーバ 2 0 1 に障害が検出された場合におけるネットワークシステム 1 0 の動作を示す説明図である。 30

【図 2 1】 復旧検出時処理（図 1 4：ステップ S 5 0 6）の手順を示すフローチャートである。

【図 2 2】 運用サーバ 2 0 1 の復旧が検出された場合におけるステップ S 6 5 1（図 2 1）で更新された後のインタフェースデータベース 1 4 0 を示す説明図である。

【図 2 3】 運用サーバ 2 0 1 の復旧が検出された場合におけるステップ S 6 5 2（図 2 1）で更新された後の V R F 1 ルーティングテーブル 1 2 1 を示す説明図である。

【図 2 4】 運用サーバ 2 0 1 の復旧が検出された場合におけるステップ S 6 5 2（図 2 1）で更新された後の V R F 2 ルーティングテーブル 1 2 2 を示す説明図である。

【図 2 5】 運用サーバ 2 0 1 の復旧が検出された場合におけるネットワークシステム 1 0 の動作を示す説明図である。 40

【図 2 6】 インタフェースデータベース 1 4 0 を初期化するためのコマンドの一例を示す説明図である。

【図 2 7】 第 2 実施例におけるネットワーク装置 1 0 0 の構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。

【図 2 8】 第 2 実施例における障害切替データベース 1 8 0 の一例を示す説明図である。

【図 2 9】 第 2 実施例におけるフェイルオーバー処理（図 1 4：ステップ S 5 0 8）の手順を示すフローチャートである。

【図 3 0】 図 2 9 のステップ S 6 0 1 において更新された後のインタフェースデータベース 1 4 0 を示す説明図である。 50

【図31】図29のステップS602において更新された後のVRF1ルーティングテーブル121を示す説明図である。

【図32】図29のステップS602において更新された後のVRF2ルーティングテーブル122を示す説明図である。

【図33】図29のステップS611において更新された後の障害切替データベース180を示す説明図である。

【図34】第3実施例におけるネットワークシステム10aの概略構成を示す説明図である。

【図35】第3実施例において第2のサービスを提供する2台のサーバのIPアドレス情報の一例を示す説明図である。

10

【図36】第3実施例におけるネットワーク装置100aの構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。

【図37】第3実施例におけるVRF1ルーティングテーブル121の一例を示す説明図である。

【図38】第3実施例におけるVRF2ルーティングテーブル122の一例を示す説明図である。

【図39】第3実施例における状態監視データベース170の一例を示す説明図である。

【図40】第3実施例における障害切替経路データベース181の一例を示す説明図である。

【図41】運用サーバ211に障害が発生し図14のステップS507において更新された後の状態監視データベース170を示す説明図である。

20

【図42】第3実施例におけるフェイルオーバー処理(図14:ステップS508)の手順を示すフローチャートである。

【図43】図42のステップS701において更新された後のVRF1ルーティングテーブル121を示す説明図である。

【図44】図42のステップS703, S704において更新された後のVRF2ルーティングテーブル122を示す説明図である。

【図45】図42のステップS706において更新された後の障害切替経路データベース181を示す説明図である。

【図46】第3実施例において運用サーバ211の障害が検出された場合の第1のサービス提供時の動作を示す説明図である。

30

【図47】第3実施例において運用サーバ211の障害が検出された場合の第2のサービス提供時の動作を示す説明図である。

【図48】第3実施例において予備サーバ212の障害が検出された場合の第1のサービス提供時の動作を示す説明図である。

【図49】ルーティングテーブルの内容を消去するためのコマンドの一例を示す説明図である。

【図50】ルーティングテーブルから任意の経路情報を消去するためのコマンドの一例を示す説明図である。

【図51】第4実施例におけるネットワークシステム10bの概略構成を示す説明図である。

40

【図52】第4実施例におけるネットワーク装置100bの構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。

【図53】第4実施例におけるインタフェースデータベース140の一例を示す説明図である。

【図54】第4実施例におけるVRFロードバランスデータベース141の一例を示す説明図である。

【図55】第4実施例におけるパケット転送処理の手順を示すフローチャートである。

【図56】第4実施例におけるVRF1ルーティングテーブル121の一例を示す説明図である。

50

【図57】第4実施例におけるVRFルーティングテーブル122の一例を示す説明図である。

【図58】第4実施例におけるロードバランス切替データベース182の一例を示す説明図である。

【図59】運用サーバ201と予備サーバ202とがサービスを提供し得る状態である場合のネットワークシステム10bの動作を示す説明図である。

【図60】第4実施例におけるフェイルオーバー処理(図14:ステップS508)の手順を示すフローチャートである。

【図61】図60のステップS801において更新された後のVRFロードバランスデータベース141を示す説明図である。

【図62】運用サーバ201に障害が検出された場合におけるネットワークシステム10bの動作を示す説明図である。

【図63】第4実施例における復旧検出時処理(図14:ステップS506)の手順を示すフローチャートである。

【図64】運用サーバ201の復旧が検出された場合におけるステップS852(図63)で更新された後のVRFロードバランスデータベース141を示す説明図である。

【図65】コマンドの一例を示す説明図である。

【図66】第5実施例におけるネットワークシステム10cの概略構成を示す説明図である。

【図67】第5実施例におけるネットワーク装置100cの構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。

【図68】第5実施例におけるインタフェースデータベース140の一例を示す説明図である。

【図69】第5実施例における状態監視処理の手順を示すフローチャートである。

【図70】フェイルオーバー処理(図69:ステップS904)の手順を示すフローチャートである。

【図71】復旧検出時処理(図69:ステップS906)の手順を示すフローチャートである。

【発明を実施するための形態】

【0018】

次に、本発明の実施の形態を実施例に基づいて以下の順序で説明する。

A. 第1実施例:

(A-1) システム構成:

(A-2) 障害検出前の動作:

(A-3) 状態監視処理:

(A-4) フェイルオーバー処理:

(A-5) 障害検出後の動作:

(A-6) 復旧検出時処理:

(A-7) 復旧検出後の動作:

B. 第2実施例:

(B-1) 第2実施例におけるシステム構成:

(B-2) 第2実施例における状態監視処理(1):

(B-3) 第2実施例におけるフェイルオーバー処理(1):

(B-4) 第2実施例における状態監視処理(2):

(B-5) 第2実施例におけるフェイルオーバー処理(2):

C. 第3実施例:

(C-1) 第3実施例におけるシステム構成:

(C-2) 第3実施例における状態監視処理(1):

(C-3) 第3実施例におけるフェイルオーバー処理(1):

(C-4) 第3実施例における障害検出後の動作:

10

20

30

40

50

- ( C - 5 ) 第 3 実施例における状態監視処理 ( 2 ) :
- ( C - 6 ) 第 3 実施例におけるフェイルオーバ処理 ( 2 ) :
- ( C - 7 ) 第 3 実施例における状態監視処理 ( 3 ) :
- ( C - 8 ) 第 3 実施例における予備サーバの障害検出後の動作 :

D . 第 4 実施例 :

- ( D - 1 ) 第 4 実施例におけるシステム構成 :
- ( D - 2 ) 第 4 実施例における障害検出前の動作 :
- ( D - 3 ) 第 4 実施例における状態監視処理 :
- ( D - 4 ) 第 4 実施例におけるフェイルオーバ処理 :
- ( D - 5 ) 第 4 実施例における復旧検出時処理 :

10

E . 第 5 実施例 :

- ( E - 1 ) 第 5 実施例におけるシステム構成 :
- ( E - 2 ) 第 5 実施例における状態監視処理 :
- ( E - 3 ) 第 5 実施例におけるフェイルオーバ処理 :
- ( E - 4 ) 第 5 実施例における復旧検出時処理 :

F . 変形例 :

【 0 0 1 9 】

A . 第 1 実施例 :

- ( A - 1 ) システム構成 :

図 1 は、本発明の一実施例としてのネットワークシステム 1 0 の概略構成を示す説明図である。ネットワークシステム 1 0 は、2 台のサーバ ( 運用サーバ 2 0 1、予備サーバ 2 0 2 ) と、ネットワーク装置 1 0 0 と、2 台のホストコンピュータ ( ホスト 3 0 1、ホスト 3 0 2 ) とを備えている。

20

【 0 0 2 0 】

第 1 の処理装置としての運用サーバ 2 0 1 は、所定のサービス ( 例えば、WEB サービス等のサービス ) をホストに対して提供するためのサーバコンピュータである。第 2 の処理装置としての予備サーバ 2 0 2 は、運用サーバ 2 0 1 がサービスを提供し得る状態の間は、サービスを提供せずに待機する。運用サーバ 2 0 1 がサービスを提供し得ない状態の場合は、運用サーバ 2 0 1 に代わって所定のサービスを提供する。すなわち、運用サーバ 2 0 1 はいわゆる運用系サーバ、予備サーバ 2 0 2 はいわゆる待機系サーバである。なお、以降、処理装置のことを「サーバ」とも呼ぶ。

30

【 0 0 2 1 】

ネットワーク中継装置としてのネットワーク装置 1 0 0 は、2 台のサーバと、2 台のホストコンピュータとの間のパケットによる通信を中継するレイヤ 3 のネットワーク中継装置である。ネットワーク装置 1 0 0 は、4 つのインタフェース ( インタフェース 1 3 1 ~ 1 3 4 ) と、コンフィギュレーションデータベース 1 1 0 と、第 1 の経路情報記憶部としての V R F 1 ルーティングテーブル 1 2 1 と、第 2 の経路情報記憶部としての V R F 2 ルーティングテーブル 1 2 2 と、V R F 定義情報記憶部としてのインタフェースデータベース 1 4 0 と、パケット転送処理部 1 5 0 と、フェイルオーバ処理部 1 6 0 と、状態監視データベース 1 7 0 と、障害切替データベース 1 8 0 と、復旧切替データベース 1 9 0 とを備えている。

40

【 0 0 2 2 】

4 つのインタフェース ( インタフェース 1 3 1 ~ 1 3 4 ) は、ネットワーク装置 1 0 0 と、ネットワーク装置 1 0 0 に接続される外部装置との間でパケットを送受信する機能を有する。インタフェース 1 3 1 は、運用サーバ 2 0 1 と回線を介して接続されている。同様に、インタフェース 1 3 2 は予備サーバ 2 0 2 と、インタフェース 1 3 3 はホスト 3 0 1 と、インタフェース 1 3 4 はホスト 3 0 2 と、それぞれ回線を通じて接続されている。

【 0 0 2 3 】

コンフィギュレーションデータベース 1 1 0 は、ネットワーク装置 1 0 0 の構成情報を保持するためのデータベースである。インタフェースデータベース 1 4 0 は、ネットワー

50

ク装置 100 における全てのインタフェースの構成情報を保持するためのデータベースである。パケット転送処理部 150 は、いずれかのインタフェースからパケットを受信した際に、当該パケットを出力すべきインタフェースを判断し、転送を行う処理部である。

#### 【0024】

フェイルオーバ処理部 160 は、サーバの状態を監視し（以降、「状態監視処理」とも呼ぶ。）、フェイルオーバを実行する（以降、「フェイルオーバ処理」とも呼ぶ。）処理部である。状態監視データベース 170 は、状態監視処理に用いられる情報を保持するためのデータベースである。障害切替データベース 180 は、フェイルオーバ処理に用いられる情報を保持するためのデータベースである。復旧切替データベース 190 は、運用系サーバが障害から復旧した場合に、待機系サーバから運用系サーバへ切り替える処理（以降、「復旧検出時処理」とも呼ぶ。）において用いられる情報を保持するためのデータベースである。

10

#### 【0025】

VRF ルーティングテーブル 121 は、2 台のサーバと、2 台のホストとの間の通信を行うために必要なルーティングテーブルである。VRF ルーティングテーブル 122 は、VRF ルーティングテーブル 121 と同様に、2 台のサーバと、2 台のホストとの間の通信を行うために必要なルーティングテーブルである。このように、本実施例におけるネットワーク装置 100 は、2 つのルーティングテーブル（121、122）を備えている。これら 2 つのルーティングテーブルは、ネットワーク装置 100 が具備する VRF（Virtual Routing and Forwarding）技術によって保持さ

20

#### 【0026】

VRF 技術とは、レイヤ 3 転送を行うネットワーク中継装置に組み込まれている技術であり、複数のルーティングテーブルを保持し、それら複数のルーティングテーブルが同時に機能することを可能とする技術である。同一の装置内に存在するルーティングテーブルが異なれば、互いに干渉されず、独立した動作が可能となる。すなわち、複数のルーティングテーブルに対して、同一のレイヤ 3 アドレス（以降、「IP アドレス」とも呼ぶ。）を設定することも可能となる。このように、ルーティングテーブルが異なり、同一の IP アドレスを設定可能であるということは、ネットワークが分離されている（すなわち、異なる仮想ネットワークを構成している）ということになる。

30

#### 【0027】

クライアント装置としてのホスト 301 と、ホスト 302 とは、いわゆるパーソナルコンピュータであり、いずれもネットワーク装置 100 を経由して、運用サーバ 201（または予備サーバ 202）が提供するサービスを利用する。なお、図 1 では便宜上、説明上必要としない、他のネットワーク装置、回線、ネットワーク装置 100 の内部構造については図示を省略している。このことは、後述する図においても同様である。なお、以降、クライアント装置のことを「ホスト」とも呼ぶ。

#### 【0028】

図 2 は、2 台のサーバの IP アドレス情報の一例を示す説明図である。本実施例における運用サーバ 201 と、予備サーバ 202 には、図 2 に示す IP アドレスと、サブネットマスク長と、デフォルトゲートウェイとがそれぞれ設定される。すなわち、運用サーバ 201 と、予備サーバ 202 には、同じ IP アドレスが設定される。通常のネットワークシステムにおける IP アドレスは、ネットワーク内における装置やインタフェースを一意に識別するための識別子であるため、同一の値を設定することはできない。しかし、本実施例では、後述する VRF の設定により運用サーバ 201 が所属するネットワークと、予備サーバ 202 が所属するネットワークとが異なるため、同一の IP アドレスを設定することが可能となる。

40

#### 【0029】

図 3 は、ホスト 301 の IP アドレス情報の一例を示す説明図である。本実施例におけるホスト 301 には、図 3 に示す IP アドレスと、サブネットマスク長と、デフォルトゲ

50

ートウェイとが設定される。

【 0 0 3 0 】

図 4 は、ホスト 3 0 2 の I P アドレス情報の一例を示す説明図である。本実施例におけるホスト 3 0 2 には、図 4 に示す I P アドレスと、サブネットマスク長と、デフォルトゲートウェイとが設定される。

【 0 0 3 1 】

図 5 は、ネットワーク装置 1 0 0 の構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。このコンフィギュレーション情報は、コンフィギュレーションデータベース 1 1 0 に保持される。行 C 1 は、第 1 の V R F を定義している。行 C 2 は、第 2 の V R F を定義している。

10

【 0 0 3 2 】

行 C 3 は、インタフェース 1 3 1 を定義している。インタフェースの種類はイーサネット（登録商標）である。なお、後述するインタフェース 1 3 2 ~ 1 3 4 についても、インタフェースの種類は全てイーサネット（登録商標）である。行 C 4 は、インタフェース 1 3 1 が、第 1 の V R F のネットワークに所属することを定義している。行 C 5 は、インタフェース 1 3 1 の I P アドレスと、サブネットマスク長とを定義している。行 C 6 は、インタフェース 1 3 2 を定義している。行 C 7 は、インタフェース 1 3 2 が、第 2 の V R F のネットワークに所属することを定義している。行 C 8 は、インタフェース 1 3 2 の I P アドレスと、サブネットマスク長とを定義している。

【 0 0 3 3 】

20

ここで、インタフェース 1 3 1 の I P アドレス（行 C 5 ）と、インタフェース 1 3 2 の I P アドレス（行 C 8 ）とは、同じ値が定義されている。通常のネットワークシステムにおける I P アドレスは、ネットワーク内における装置やインタフェースを一意に識別するための識別子であるため、同一の値を設定することができない。しかし、インタフェース 1 3 1 と、インタフェース 1 3 2 とは、異なる V R F に属している（行 C 4、C 7）。このため、インタフェース 1 3 1 が所属するネットワークと、インタフェース 1 3 2 が所属するネットワークとが異なるため、同一の I P アドレスを設定することが可能となる。

【 0 0 3 4 】

行 C 9 は、インタフェース 1 3 3 を定義している。行 C 1 0 は、インタフェース 1 3 3 が、第 1 の V R F に所属することを定義している。行 C 1 1 は、次の a )、b ) のことを定義している。

30

a ) 状態監視ルール 5 0 （詳細は後述）により運用サーバ 2 0 1 の障害を検出した際に、インタフェース 1 3 3 を第 2 の V R F のネットワークに所属するよう切り替えを行うこと。

b ) 状態監視ルール 5 0 により運用サーバ 2 0 1 の復旧を検出した際に、インタフェース 1 3 3 を第 1 の V R F のネットワークに所属するよう切り替えを行わず、第 2 の V R F に所属したままにする（ロックする）こと。

行 C 1 2 は、インタフェース 1 3 3 の I P アドレスと、サブネットマスク長とを定義している。

【 0 0 3 5 】

40

行 C 1 3 は、インタフェース 1 3 4 を定義している。行 C 1 4 は、インタフェース 1 3 4 が、第 1 の V R F に所属することを定義している。行 C 1 5 は、次の c )、d ) のことを定義している。

c ) 状態監視ルール 5 0 （詳細は後述）により運用サーバ 2 0 1 の障害を検出した際に、インタフェース 1 3 4 を第 2 の V R F のネットワークに所属するよう切り替えを行うこと。

d ) 状態監視ルール 5 0 により運用サーバ 2 0 1 の復旧を検出した際に、インタフェース 1 3 4 を第 1 の V R F のネットワークに所属するよう切り替えを行う（リカバリする）こと。

行 C 1 6 は、インタフェース 1 3 4 の I P アドレスと、サブネットマスク長とを定義し

50

ている。

【 0 0 3 6 】

行 C 1 7 は、状態監視ルール 5 0 として、第 1 の V R F のネットワーク内に存在する、I P アドレスが 1 0 . 1 . 1 . 1 を識別子とする装置へのパケットの到達性の監視を規定する。換言すれば、行 C 1 7 は、運用サーバ 2 0 1 の状態監視ルールを定義している。なお、図 5 では、便宜上、説明上必要としないネットワーク装置の構成情報を規定するコンフィギュレーションについては省略している。このことは、後述する図においても同様である。

【 0 0 3 7 】

図 6 は、インタフェースデータベース 1 4 0 の一例を示す説明図である。インタフェースデータベース 1 4 0 は、インタフェース番号フィールドと、V R F 番号フィールドと、I P アドレスフィールドと、サブネットマスク長フィールドとを含んでいる。インタフェース番号フィールドには、ネットワーク装置 1 0 0 が有するインタフェースの識別子が格納されている。V R F 番号フィールドには、インタフェースが属する V R F ネットワークの識別子が格納されている。I P アドレスフィールドには、インタフェースの I P アドレスが格納されている。サブネットマスク長フィールドには、サブネットマスク ( I P アドレスのうちの何ビットをネットワークアドレスに使用するかを定義する 3 2 ビットの数値 ) が格納されている。

10

【 0 0 3 8 】

このインタフェースデータベース 1 4 0 は、ネットワーク装置 1 0 0 における構成情報を定義したコンフィギュレーションデータベース 1 1 0 ( 図 5 ) に基づき保持される。すなわち、インタフェースデータベース 1 4 0 のエントリ E 1 には、図 5 で説明したコンフィギュレーション情報の行 C 3 ~ C 5 で定義された情報が格納される。同様に、エントリ E 2 には行 C 6 ~ C 8 で定義された情報が、エントリ E 3 には行 C 9、C 1 0、C 1 2 で定義された情報が、エントリ E 4 には行 C 1 3、C 1 4、C 1 6 で定義された情報が、それぞれ格納される。なお、パケット転送処理部 1 5 0 は、いずれかのインタフェースからパケットを受信した際に、パケットの転送先を決定するために検索するルーティングテーブルを決定するために、このインタフェースデータベース 1 4 0 を用いる。詳細については後述する。

20

【 0 0 3 9 】

図 7 は、インタフェースデータベース 1 4 0 が図 6 で示した状態である場合における、V R F 1 ルーティングテーブル 1 2 1 の一例を示す説明図である。V R F 1 ルーティングテーブル 1 2 1 は、あて先 I P アドレスフィールドと、サブネットマスク長フィールドと、ネクストホップ I P アドレスフィールドと、出力インタフェースフィールドとを含んでいる。あて先 I P アドレスフィールドには、あて先の I P アドレスが格納されている。サブネットマスク長フィールドには、サブネットマスクが格納されている。ネクストホップ I P アドレスフィールドには、ネットワーク装置 1 0 0 が次にパケットを転送すべき装置の I P アドレスが格納されている。出力インタフェースフィールドには、パケット転送処理部 1 5 0 がパケットを出力するインタフェースの識別子が格納されている。

30

【 0 0 4 0 】

V R F 1 ルーティングテーブル 1 2 1 には、インタフェースデータベース 1 4 0 の V R F 番号フィールドの値が「 1 」であるインタフェースの情報と、当該インタフェースに回線や他のネットワーク装置を介して接続されている装置の情報とが保持される。すなわち、インタフェース 1 3 1、1 3 3、1 3 4、および、運用サーバ 2 0 1、ホスト 3 0 1、ホスト 3 0 2 の情報が保持される。

40

【 0 0 4 1 】

エントリ E 1 には、運用サーバ 2 0 1 の情報が保持されている。具体的には、あて先 I P アドレスフィールドには、運用サーバ 2 0 1 の I P アドレスが格納されている。サブネットマスク長フィールドには、装置あてであることを示す「 3 2 」が格納されている。ネクストホップ I P アドレスフィールドには、運用サーバ 2 0 1 の I P アドレスが格納され

50

ている。これは、ネットワーク装置100と、運用サーバ201とが、他の装置を経由せず、回線を介して直接接続されているためである。例えば、ネットワーク装置100と、運用サーバ201とが、他の装置を経由して接続されている場合、ネクストホップIPアドレスフィールドには、当該他の装置のIPアドレスが格納される。出力インタフェースフィールドには、運用サーバ201と接続されているインタフェースの識別子が格納されている。

#### 【0042】

エントリE2には、ネットワーク装置100のインタフェース131の情報が保持されている。ネットワーク装置100が、インタフェース131のIPアドレスをあて先IPアドレスとしたパケットを受信した場合、当該パケットは転送せずに、ネットワーク装置100で処理をする必要がある。そのため、ネクストホップIPアドレスフィールドと、出力インタフェースフィールドには値が格納されていない(図中では「-」で示している)。

10

#### 【0043】

エントリE3にはホスト301の情報が、E5にはホスト302の情報が、それぞれ格納されている。詳細については、上述した運用サーバ201(エントリE1)と同様であるため説明を省略する。エントリE4にはインタフェース133の情報が、E6にはインタフェース134の情報が、それぞれ格納されている。詳細については、上述したインタフェース131(エントリE2)と同様であるため説明を省略する。

#### 【0044】

図8は、インタフェースデータベース140が図6で示した状態である場合における、VRF2ルーティングテーブル122の一例を示す説明図である。VRF2ルーティングテーブル122は、VRF1ルーティングテーブル121と同様のテーブル構成を有している。VRF2ルーティングテーブル122には、インタフェースデータベース140のVRF番号フィールドの値が「2」であるインタフェースの情報と、当該インタフェースに回線や他のネットワーク装置を介して接続されている装置の情報とが保持される。すなわち、インタフェース132、および、予備サーバ202の情報が保持される。

20

#### 【0045】

エントリE1には予備サーバ202の情報が格納されている。詳細については、上述した運用サーバ201(図7:エントリE1)と同様であるため説明を省略する。エントリE2にはインタフェース132の情報が格納されている。詳細については、上述したインタフェース131(図7:エントリE2)と同様であるため説明を省略する。

30

#### 【0046】

図9は、状態監視データベース170の一例を示す説明図である。状態監視データベース170は、監視IDフィールドと、監視先IPアドレスフィールドと、監視先VRFフィールドと、監視状態フィールドとを含んでいる。監視IDフィールドには、監視対象のグループを識別するための識別子が格納されている。監視先IPアドレスフィールドには、監視対象の装置のIPアドレスが格納されている。監視先VRFフィールドには、監視対象の装置が属するVRFネットワークの識別子が格納されている。監視状態フィールドには、監視対象の装置の状態を表す文字(または記号等)が格納されている。

40

#### 【0047】

本実施例では、運用サーバ201と予備サーバ202とは、異なるVRFに属し、同じIPアドレスが付与されている。このため、監視先IPアドレスフィールドの値と、監視先VRFフィールドの値との組合せによって、監視対象となる装置を一意に識別することができる。図9の例では、監視ID50の監視対象の装置は、監視先IPアドレスフィールドの値が10.1.1.1、かつ、監視先VRFフィールドの値が第1のVRFであるため、運用サーバ201であることがわかる。また、状態監視フィールドの値が「通信可」であるため、運用サーバ201は、現在サービスの提供が可能な状態であることがわかる。

#### 【0048】

50

図10は、障害切替データベース180の一例を示す説明図である。障害切替データベース180は、監視IDフィールドと、切替対象インタフェースフィールドと、切替先VRFフィールドと、切替後動作フィールドとを含んでいる。監視IDフィールドには、監視対象のグループを識別するための識別子が格納されている。切替対象インタフェースフィールドには、状態監視処理によってフェイルオーバが実行されるインタフェースの識別子が格納されている。切替先VRFフィールドには、フェイルオーバ処理によって切替が行われる、新しいVRFの識別子が格納されている。切替後動作フィールドには、装置の復旧を検出した際に、インタフェースを元のVRFに戻すか否かを表す文字（または記号等）が格納されている。

#### 【0049】

この障害切替データベース180は、ネットワーク装置100における構成情報を定義したコンフィギュレーションデータベース110（図5）に基づいて保持される。すなわち、障害切替データベース180のエントリE1には、図5で説明したコンフィギュレーション情報の行C11で定義された情報が格納される。同様に、エントリE2には行C15で定義された情報が格納される。

#### 【0050】

図11は、復旧切替データベース190の一例を示す説明図である。復旧切替データベース190は、監視IDフィールドと、切替対象インタフェースフィールドと、切替先VRFフィールドとを含んでいる。監視IDフィールドには、監視対象のグループを識別するための識別子が格納される。切替対象インタフェースフィールドには、復旧検出時処理によってVRFの切替が行われるインタフェースの識別子が格納される。切替先VRFフィールドには、復旧検出時処理によって切替が行われるVRFの識別子が格納される。復旧切替データベース190は、後述するフェイルオーバ処理においてエントリが追加されるデータベースであり、初期状態においては、エントリは格納されていない。

#### 【0051】

（A-2）障害検出前の動作：

図12は、運用サーバ201がサービスを提供し得る状態である場合の、ネットワークシステム10の動作を示す説明図である。まず、図12に示すように、ホスト301はサービスを提供するサーバ（運用サーバ201もしくは予備サーバ202）にアクセスするため、あて先IPアドレスを10.1.1.1とする要求パケットを送信する。このパケットは、図3で説明した自身のデフォルトゲートウェイで指定されているIPアドレス（換言すれば、インタフェース133のIPアドレス）へ送信する。

#### 【0052】

図13は、ネットワーク装置100におけるパケット転送処理の手順を示すフローチャートである。ネットワーク装置100は、ホスト301から送信されたパケットを、インタフェース133において受信する（ステップS11）。次に、ステップS12において、パケット転送処理部150は、インタフェースデータベース140を検索する。具体的には、パケット転送処理部150は、インタフェースデータベース140のインタフェース番号フィールドの値と、パケットを受信したインタフェースの識別子とが一致するエントリを検索する。そして、パケット転送処理部150は、当該一致したエントリのVRF番号フィールドの値を取得する。図6および図12の例では、パケット転送処理部150は、インタフェースの識別子133に一致するエントリE3のVRF番号フィールドの値「1」を取得する。

#### 【0053】

ステップS13において、パケット転送処理部150は、VRF番号に対応するルーティングテーブルを検索する。本実施例の場合は、VRF番号が「1」の場合は第1のVRFのルーティングテーブル（VRF1ルーティングテーブル121）を使用する。一方、VRF番号が「2」の場合は、第2のVRFのルーティングテーブル（VRF2ルーティングテーブル122）を使用する。図12の例では、ステップS12において求めたVRF番号は「1」であるため、パケット転送処理部150は、VRF1ルーティングテーブ

10

20

30

40

50

ル121を検索することとなる。すなわち、パケット転送処理部150は、パケット送信元の装置が所属するVRFネットワーク(仮想ネットワーク)に対応した経路情報を用いて経路探索をする。

【0054】

パケット転送処理部150は、VRF1ルーティングテーブル121のあて先IPアドレスフィールドの値と、受信したパケットのヘッダ中に含まれるあて先IPアドレスを示す情報とが一致するエントリを検索する。そして、パケット転送処理部150は、当該一致したエントリの、ネクストホップIPアドレスフィールドの値と、出力インタフェースフィールドの値を取得する。図7および図12の例では、パケット転送処理部150は、あて先IPアドレス10.1.1.1に一致するエントリE1のネクストホップIPアドレスフィールドの値「10.1.1.1」と、出力インタフェースフィールドの値「131」とを取得する。ステップS14において、パケット転送処理部150は、ステップS13で求めた出力インタフェースからパケットを出力する。

10

【0055】

上述のようにして、ホスト301からの要求パケットは、運用サーバ201へ転送される。運用サーバ201は、ホスト301から受信したパケットをもとにしてサービスを行った後、ホスト301に対して応答パケットを送信する。この応答パケットのあて先IPアドレスは、ホスト301のIPアドレス20.1.1.1である。このパケットは、図2で説明した自身のデフォルトゲートウェイで指定されているIPアドレス(換言すれば、インタフェース131のIPアドレス)へ送信する。

20

【0056】

ネットワーク装置100は、運用サーバ201から送信されたパケットを、1インタフェース131において受信する。その後、パケット転送処理部150は、当該受信パケットについて、図13で説明したものと同様の処理を行うことによって、該当する出力インタフェースからパケットを出力する。この結果、運用サーバ201からの応答パケットは、ホスト301へ転送される。なお、図12では、ホストからの要求を白抜きの矢印、サーバからの応答を斜線を施した矢印で表している(このことは、後述する同種の図においても同様である。)。このようにして、ホスト301と、運用サーバ201との間で、双方向の通信が行われることによって、運用サーバ201によるサービスの提供が実現する。なお、ホスト302についてもホスト301と同様の動作となる。

30

【0057】

以上のように、運用サーバ201の障害検出前においては、運用サーバ201が運用系サーバとして機能している。

【0058】

一方、予備サーバ202が接続されているインタフェース132は、図6のVRF番号フィールドの値が「2」であるため、第2のVRFに属している。すなわち、第1のVRFに属するインタフェース131、133、134に接続されている運用サーバ201と、ホスト301と、ホスト302とは、同一のネットワークである第1のVRFに所属している。また、第2のVRFに属するインタフェース132に接続されている予備サーバ202は、第2のVRFに所属している。このため、図6に示したインタフェースデータベース140の状態においては、ホスト301およびホスト302は、予備サーバ202とは異なるVRFネットワークに所属することとなり、予備サーバ202と通信を行うことはない。すなわち、障害検出前においては、予備サーバ202は待機系サーバとして機能している。

40

【0059】

上述の通り、あるサーバを運用系サーバとするためには、サーバが回線を介して接続しているインタフェースのVRF番号と、ホストが回線を介して接続しているインタフェースのVRF番号とを同じにすればよい。一方、あるサーバを待機系サーバとするには、サーバが回線を介して接続しているインタフェースのVRF番号と、ホストが回線を介して接続しているインタフェースのVRF番号と、を異なる番号にすればよい。

50

## 【 0 0 6 0 】

( A - 3 ) 状態監視処理 :

図 1 4 は、状態監視処理の手順を示すフローチャートである。状態監視部としてのフェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 を使用し、図 1 4 のフローチャートに従ってサーバの運用状態を監視する。まず、ステップ S 5 0 1 においてフェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 に記録されている監視 ID に対応する監視先 IP アドレスフィールドと、監視先 V R F フィールドの値を読み出す。

## 【 0 0 6 1 】

そして、ステップ S 5 0 2 においてフェイルオーバー処理部 1 6 0 は、読み出された監視先 IP アドレスと、監視先 V R F の組をもとにして監視先を特定し、当該監視先に対してパケットを送信する。具体的には、ステップ S 5 0 1 において得られる V R F 番号に対応するルーティングテーブルを、ステップ S 5 0 1 において得られる監視先 IP アドレスをキーとして検索することにより得られる出力先へパケットを出力する。詳細は図 1 3 のステップ S 1 3、S 1 4 で説明した通りである。

10

## 【 0 0 6 2 】

例えば、図 9 のエントリ E 1 ( 監視 ID : 5 0 ) の例では、監視先 V R F フィールドの値は「 1 」であるため、フェイルオーバー処理部 1 6 0 は V R F 1 ルーティングテーブル 1 2 1 を検索する。このとき、監視先 IP アドレスフィールドの値「 1 0 . 1 . 1 . 1 」をキーとして、V R F 1 ルーティングテーブル 1 2 1 のあて先 IP アドレスフィールドに一致するエントリを検索する。すると、ネクストホップ IP アドレスは「 1 0 . 1 . 1 . 1」、出力インタフェースは「 1 3 1 」( エントリ E 1 ) であることが分かる。このようにして、フェイルオーバー処理部 1 6 0 は、インタフェース 1 3 1 から運用サーバ 2 0 1 へ向けてパケットを送信する。

20

## 【 0 0 6 3 】

なお、このとき送信されるパケットは、I C M P ( I n t e r n e t C o n t r o l M e s s a g e P r o t o c o l ) E c h o R e q u e s t パケットであることが好ましい。なお、B F D ( B i d i r e c t i o n a l F o r w a r d i n g D e t e c t i o n ) E c h o パケットや、そのほか本ステップを実施するための独自のパケットであってもかまわない。

## 【 0 0 6 4 】

次に、ステップ S 5 0 3 においてフェイルオーバー処理部 1 6 0 は、ステップ S 5 0 2 で送信したパケットに対する応答パケットを待つ。例えば、ステップ S 5 0 2 において送信したパケットが I C M P E c h o R e q u e s t である場合、応答パケットは、I C M P E c h o R e p l y パケットになる。この応答パケットがない場合、フェイルオーバー処理部 1 6 0 は、監視の対象である装置が正常に所定のサービスを提供することができない障害状態であるものと判定する。

30

## 【 0 0 6 5 】

ステップ S 5 0 4 において、フェイルオーバー処理部 1 6 0 は、応答パケットの有無を判断する。応答パケットがあった場合、ステップ S 5 0 5 においてフェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 を更新する。具体的には、フェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 の監視 ID フィールドの値が現在監視中の監視 ID であって、かつ、監視先 IP アドレスフィールドの値がステップ S 5 0 4 における応答パケットの送信元であるエントリについて、当該エントリの値を「通信可」へ更新する。その後、ステップ S 5 0 6 においてフェイルオーバー処理部 1 6 0 は、復旧検出時処理( 詳細は後述 ) を行う。

40

## 【 0 0 6 6 】

一方、応答パケットがなかった場合、ステップ S 5 0 7 においてフェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 を更新する。具体的には、フェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 ( 図 9 ) の監視 ID フィールドの値が現在監視中の監視 ID であって、かつ、監視先 IP アドレスフィールドの値がステップ S 5 0 4 にお

50

いて、応答パケットの送信がなかった装置を示すエントリについて、当該エントリの値を「通信不可」へ更新する。その後、ステップS 5 0 8においてフェイルオーバ処理部1 6 0は、フェイルオーバ処理（詳細は後述）を行う。

【0067】

図15は、図14のステップS 5 0 7において更新された後の状態監視データベース170を示す説明図である。障害検出前の状態監視データベース170を示す図9との違いは、監視IDフィールドの値が「50」、かつ、監視先IPアドレスが「10.1.1.1」を示すエントリ（エントリE1）の監視状態フィールドの値が「通信不可」となっている点である。

【0068】

以上のようにして、フェイルオーバ処理部160は、1つの監視対象（監視ID）についての状態監視処理を行う。その後、ステップS 5 0 9においてフェイルオーバ処理部160は、状態監視データベース170に格納されている、全ての監視IDに対する処理を行ったかを判断する。全ての監視IDに対する処理を行った場合、処理を終了する。一方、全ての監視IDに対する処理を行っていない場合、フェイルオーバ処理部160は、ステップS 5 0 1へ戻り、処理を継続する。

【0069】

（A-4）フェイルオーバ処理：

図16は、フェイルオーバ処理（図14：ステップS 5 0 8）の手順を示すフローチャートである。フェイルオーバ処理部160は、状態監視処理で障害を検出した監視IDと、図10で説明した障害切替データベース180とを使用し、図16のフローチャートに従って、障害検出に伴うフェイルオーバ処理を行う。

【0070】

まず、ステップS 6 0 1においてフェイルオーバ処理部160は、インタフェースデータベース140のVRF番号を切り替える。具体的には、フェイルオーバ処理部160は、障害切替データベース180（図10）のうち、監視IDフィールドの値が、状態監視処理において障害が検出された監視IDと同じエントリを検索する。そして、検索されたエントリについての、切替対象インタフェースフィールドと、切替先VRFフィールドと、切替後動作フィールドの値を読み出す。次に、フェイルオーバ処理部160は、インタフェースデータベース140のインタフェース番号フィールドを、読み出された切替対象インタフェースフィールドの値をキーとして検索する。そして、該当するエントリについてのVRF番号フィールドの値を、読み出された切替先VRFフィールドの値へと変更する。

【0071】

次に、ステップS 6 0 2においてフェイルオーバ処理部160は、インタフェースデータベース140に基づいたルーティングテーブルの書き換えを行う。具体的には、まず、フェイルオーバ処理部160は、インタフェースデータベース140のうち、VRF番号フィールドの値が「1」であるエントリの情報のみを格納するように、VRF1ルーティングテーブル121を書き換える。同様に、フェイルオーバ処理部160は、インタフェースデータベース140のうち、VRF番号フィールドの値が「2」であるエントリの情報のみを格納するように、VRF2ルーティングテーブル122を書き換える。

【0072】

ステップS 6 0 3においてフェイルオーバ処理部160は、切替後動作がロックか否かを判定する。この判定は、ステップS 6 0 1で読み出された切替後動作フィールドの値を元に行う。切替後動作フィールドの値が「ロック」である場合、ステップS 6 2 0へ遷移する。一方、切替後動作フィールドの値が「ロック」で無い場合は、フェイルオーバ処理部160は、復旧切替データベース190（図11）へ監視対象となるエントリの情報を登録する（ステップS 6 1 0）。

【0073】

ステップS 6 2 0においてフェイルオーバ処理部160は、全ての切替対象について処

10

20

30

40

50

理を行ったか否かを判定する。具体的には、ステップS601において検索されたエントリ（障害切替データベース180のうち、監視IDフィールドの値が状態監視処理において障害が検出された監視IDと同じエントリ）の切替対象インタフェースの全てについて、上述のステップの処理を行ったか否かを判定する。全ての切替対象について処理を行った場合、処理を終了する。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー処理部160は、ステップS601へ戻り、処理を継続する。

#### 【0074】

図17は、図16のステップS601において更新された後のインタフェースデータベース140を示す説明図である。障害検出前のインタフェースデータベース140を示す図6との違いは、インタフェース番号フィールドの値が「133」、「134」のエントリ（エントリE3、E4）のVRF番号フィールドの値が「2」となっている点である。

10

#### 【0075】

図18は、図16のステップS602において更新された後のVRF1ルーティングテーブル121を示す説明図である。障害検出前のVRF1ルーティングテーブル121を示す図7との違いは、ステップS601で更新された後のインタフェースデータベース140（図17）に基づいたルーティングテーブルの書き換えが行われている点である。具体的には、あて先IPアドレスフィールドの値がインタフェース133、134のIPアドレスであるエントリ、および、あて先IPアドレスフィールドの値がホスト301、302（インタフェース133、134に接続されている装置）のIPアドレスであるエントリが削除されている。

20

#### 【0076】

図19は、図16のステップS602において更新された後のVRF2ルーティングテーブル122を示す説明図である。障害検出前のVRF2ルーティングテーブル122を示す図8との違いは、ステップS601で更新された後のインタフェースデータベース140（図17）に基づいたルーティングテーブルの書き換えが行われている点である。具体的には、あて先IPアドレスフィールドの値がインタフェース133、134のIPアドレスであるエントリ、および、あて先IPアドレスフィールドの値がホスト301、302（インタフェース133、134に接続されている装置）のIPアドレスであるエントリE3～E6が追加されている。

30

#### 【0077】

（A-5）障害検出後の動作：

図20は、運用サーバ201に障害が検出された場合におけるネットワークシステム10の動作を示す説明図である。図20に示すように、ホスト301は、サービスを提供するサーバ（運用サーバ201もしくは予備サーバ202）にアクセスするため、あて先IPアドレスを10.1.1.1とする要求パケットを送信する。このパケットは、図3で説明した自身のデフォルトゲートウェイで指定されているIPアドレス（換言すれば、インタフェース133のIPアドレス）へ送信する。

#### 【0078】

ネットワーク装置100は、ホスト301から送信されたパケットをインタフェース133において受信する（図13：ステップS11）。次に、パケット転送処理部150は、図17に示したインタフェースデータベース140を検索し、インタフェースの識別子133に一致するエントリE3のVRFフィールドの値「2」を取得する（図13：ステップS12）。VRFが2であるため、パケット転送処理部150は、図19に示したVRF2ルーティングテーブル122を検索する（図13：ステップS13）。このようにして、パケット転送処理部150は、ステップS13で求めた出力インタフェース132からパケットを出力する。

40

#### 【0079】

上述のようにして、ホスト301からの要求パケットは、予備サーバ202へ転送される。予備サーバ202は、ホスト301から受信したパケットをもとにしてサービスを行った後、ホスト301に対して応答パケットを送信する。この応答パケットのあて先IP

50

アドレスは、ホスト301のIPアドレス20.1.1.1である。このパケットは、図2で説明した自身のデフォルトゲートウェイで指定されているIPアドレス（換言すれば、インタフェース132のIPアドレス）へ送信する。

【0080】

ネットワーク装置100は、予備サーバ202から送信されたパケットを、インタフェース132において受信する。その後、パケット転送処理部150は、当該受信パケットについて、図13で説明したものと同様の処理を行うことによって、該当する出力インタフェースからパケットを出力する。この結果、予備サーバ202からの応答パケットは、ホスト301へ転送される。なお、ホスト302についてもホスト301と同様の動作となる。

10

【0081】

以上のように、運用サーバ201の障害検出後においては、予備サーバ202が運用系サーバとして機能することがわかる。

【0082】

(A-6) 復旧検出時処理：

図21は、復旧検出時処理（図14：ステップS506）の手順を示すフローチャートである。フェイルオーバ処理部160は、状態監視処理で復旧を検出した監視IDと、図11で説明した復旧切替データベース190とを使用し、図21のフローチャートに従って、復旧検出に伴う復旧検出時処理を行う。

【0083】

まず、ステップS651においてフェイルオーバ処理部160は、インタフェースデータベース140のVRF番号を切り替える。具体的には、フェイルオーバ処理部160は、復旧切替データベース190（図11）のうち、監視IDフィールドの値が、状態監視処理において復旧を検出した監視IDと同じエントリを検索する。そして、検索されたエントリについての、切替対象インタフェースフィールドと、切替先VRFフィールドの値を読み出す。次に、フェイルオーバ処理部160は、インタフェースデータベース140のインタフェース番号フィールドを、読み出された切替対象インタフェースフィールドの値をキーとして検索する。そして、該当するエントリについてのVRF番号フィールドの値を、上読み出された切替先VRFフィールドの値へと変更する。

20

【0084】

次に、ステップS652においてフェイルオーバ処理部160は、ルーティングテーブルの書き換えを行う。具体的には、まず、フェイルオーバ処理部160は、ステップS651において検索された切替先VRFフィールドの値をもとに、切替後に使用されるルーティングテーブルを判定する。そして、切替後に使用されるルーティングテーブルへ、i) あて先IPアドレスフィールドの値がステップS651において検索された切替対象インタフェースのIPアドレスであるエントリ、ii) あて先IPアドレスフィールドの値がステップS651において検索された切替対象インタフェースに接続されている装置のIPアドレスであるエントリ、の情報を追加する。一方、切替後には使用されないルーティングテーブルからは、上記i)、ii)に該当するエントリを削除する。

30

【0085】

ステップS653においてフェイルオーバ処理部160は、復旧切替データベース190から、ステップS651、S652において処理を行った切替対象インタフェースを削除する。

40

【0086】

ステップS654においてフェイルオーバ処理部160は、全ての切替対象の処理を行ったかを判定する。具体的には、ステップS651において検索されたエントリ（復旧切替データベース190のうち、監視IDフィールドの値が状態監視処理において復旧を検出した監視IDと同じエントリ）の切替対象インタフェースの全てについて、ステップS651～S653の処理を行ったか否かを判定する。全ての切替対象について処理を行った場合、フェイルオーバ処理部160は、復旧切替データベース190から、状態監視処

50

理において復旧を検出した監視IDそのものを削除し、処理を終了する(ステップS655)。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー処理部160は、ステップS651へ戻り、処理を継続する。

【0087】

図22は、運用サーバ201の復旧が検出された場合における、ステップS651(図21)で更新された後のインタフェースデータベース140を示す説明図である。復旧検出前のインタフェースデータベース140を示す図17との違いは、インタフェース番号フィールドの値が「134」のエントリ(エントリE4)のVRF番号フィールドの値が「1」となっている点である。

【0088】

図23は、運用サーバ201の復旧が検出された場合における、ステップS652(図21)で更新された後のVRF1ルーティングテーブル121を示す説明図である。復旧検出前のVRF1ルーティングテーブル121を示す図18との違いは、i)あて先IPアドレスフィールドの値がステップS651において検索された切替対象インタフェース(インタフェース134)のIPアドレスであるエントリ、ii)あて先IPアドレスフィールドの値がステップS651において検索された切替対象インタフェースに接続されている装置(ホスト302)のIPアドレスであるエントリE3、E4が追加されている点である。

【0089】

図24は、運用サーバ201の復旧が検出された場合における、ステップS652(図21)で更新された後のVRF2ルーティングテーブル122を示す説明図である。復旧検出前のVRF2ルーティングテーブル122を示す図19との違いは、i)あて先IPアドレスフィールドの値がステップS651において検索された切替対象インタフェース(インタフェース134)のIPアドレスであるエントリ、ii)あて先IPアドレスフィールドの値がステップS651において検索された切替対象インタフェースに接続されている装置(ホスト302)のIPアドレスである図19のエントリE5、E6が削除されている点である。

【0090】

なお、運用サーバ201の復旧が検出された場合における、状態監視データベース170の内容は、図9と同様となる。

【0091】

(A-7)復旧検出後の動作：

図25は、運用サーバ201の復旧が検出された場合におけるネットワークシステム10の動作を示す説明図である。図25に示すように、ホスト301が送信した要求パケットは、ネットワーク装置100によって、予備サーバ202へ転送される。予備サーバ202は、ホスト301から受信したパケットをもとにしてサービスを行った後、ホスト301に対して応答パケットを送信する。詳細な流れは、図20において説明したものと同様である。このように、運用サーバ201が復旧した後においても、ホスト301は予備サーバ202と通信を行う。これは、障害切替データベース180(図10)において、切替対象インタフェースが「133」であるエントリの切替後動作が「ロック」とされているためである。

【0092】

一方、ホスト302が送信した要求パケットは、ネットワーク装置100によって、運用サーバ201へ転送される。運用サーバ201は、ホスト302から受信したパケットをもとにしてサービスを行った後、ホスト302に対して応答パケットを送信する。詳細な流れは、図12において説明したものと同様である。このように、運用サーバ201が復旧した後において、ホスト302は運用サーバ201と通信を行う。これは、障害切替データベース180(図10)において、切替対象インタフェースが「134」であるエントリの切替後動作が「リカバリ」とされているためである。

【0093】

10

20

30

40

50

図26は、インタフェースデータベース140を初期化するためのコマンドの一例を示す説明図である。このような運用コマンドを実行することにより、インタフェースデータベース140のインタフェース133に関する情報を初期化(図6に示した状態)することができる。なお、このコマンドは、ネットワーク装置100の管理者が、ネットワーク装置100の管理端末(図示省略)より実行することによって機能する。このことは後述する他のコマンドについても同様である。

【0094】

インタフェースデータベース140の変更に伴い、VRF1ルーティングテーブル121は図7で説明した状態へ、VRF2ルーティングテーブル122は図8で説明した状態へ、それぞれ変更される。このため、ネットワークシステム10を、運用サーバ201に障害が発生する前の状態へ復元することが可能となる。

10

【0095】

このようにすれば、第1の処理装置(運用サーバ201)と第2の処理装置(予備サーバ202)は、共に所定のサービスを提供可能であり、かつ、運用サーバ201と予備サーバ202には、同一のレイヤ3アドレス(IPアドレス)を設定することができる。フェイルオーバー処理部160は、ホストにサービスを提供する第1の仮想ネットワーク(VRF1)に所属する運用サーバ201の状態を監視し、当該サーバがサービスを提供することができない障害状態であると判定された場合に、第1の仮想ネットワークに所属しているクライアント装置(ホスト301、302)を、第2の仮想ネットワーク(VRF2)に所属させるように、VRF定義情報(インタフェースデータベース140)を更新する。なお、インタフェースデータベース140の更新に伴い、経路情報を格納するVRF1ルーティングテーブル121、VRF2ルーティングテーブル122についても更新がなされる。

20

【0096】

上述のように、運用系サーバである運用サーバ201に障害が発生した場合であっても、インタフェースデータベース140の更新によって、スムーズに待機系サーバである予備サーバ202へのフェイルオーバーが可能となる。換言すれば、コールドスタンバイによるフェイルオーバー方法における、長時間のサービス停止という課題を解決することができる。また、このようなフェイルオーバーは、ネットワーク装置100が備えるフェイルオーバー処理部160が行うため、ホットスタンバイによるフェイルオーバー方法における、ロードバランサやDNSの導入を必要としない。これらの結果、サーバネットワークシステムにおいて、構成要素の追加をすることなく、かつ、短時間でのフェイルオーバーが実現できる。

30

【0097】

また、上述の状態監視処理において、状態監視部としてのフェイルオーバー処理部160は、運用サーバ201とホストとが実際に通信に使用する回線を用いて、サーバの運用状態を監視する。そのため、運用サーバ201そのものの故障のみならず、ネットワーク装置100と運用サーバ201との間の通信回線に障害が発生した場合においても、フェイルオーバーを行うことが可能である。

【0098】

さらに、状態監視部としてのフェイルオーバー処理部160は、運用サーバ201が障害状態であると判定された後においても、運用サーバ201の監視を継続するため、運用サーバ201がサービスを提供可能な状態へ復旧したことを検知することができる。そして、運用サーバ201の復旧を検知した場合、フェイルオーバー処理部160は、VRF定義情報(インタフェースデータベース140)を障害状態であると判定される前の状態へと更新するリカバリ処理と、更新を行わないロック処理とを選択的に実行することができる。

40

【0099】

このため、例えば、システム管理者は、運用サーバ201の復旧と同時にネットワークシステム10が自動的にフェイルオーバーする運用方法(リカバリ処理)と、自ら運用サー

50

バ 2 0 1 の復旧を確認したうえで手動によりフェイルオーバさせる運用方法（ロック処理）とを選択することができる。この結果、ネットワークシステムの運用の幅を広げることができる。

【 0 1 0 0 】

B . 第 2 実施例 :

本発明の第 2 実施例では、サーバが回線を介して接続されているインタフェースの V R F 番号を変更することによって、フェイルオーバを実現する構成を説明する。ネットワークシステム 1 0 の概略構成は、図 1 に示した第 1 実施例と同様である。また、第 2 実施例においては、復旧切替データベース 1 9 0 は使用しない。なお、以下では、第 1 実施例と異なる構成および動作を有する部分についてのみ説明する。

10

【 0 1 0 1 】

( B - 1 ) 第 2 実施例におけるシステム構成 :

図 2 7 は、第 2 実施例におけるネットワーク装置 1 0 0 の構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。図 5 に示した第 1 実施例との違いは、行 C 1 1、C 1 5、C 1 7 が削除されている点と、行 C 2 0 1、C 2 0 2、C 2 0 3 が追加されている点であり、他の構成については第 1 実施例と同様である。

【 0 1 0 2 】

行 C 2 0 1 は、次の e )、f ) のことを定義している。

e ) 状態監視ルール 5 0 ( 詳細は後述 ) により運用サーバ 2 0 1 の障害を検出した際に、インタフェース 1 3 1 を第 2 の V R F のネットワークに所属するよう切り替えを行うこと。

20

f ) 状態監視ルール 5 0 ( 詳細は後述 ) により予備サーバ 2 0 2 の障害を検出した際に、インタフェース 1 3 1 を元の状態に戻す ( スイッチバックさせる ) こと。

【 0 1 0 3 】

行 C 2 0 2 は、次の g )、h ) のことを定義している。

g ) 状態監視ルール 5 0 ( 詳細は後述 ) により運用サーバ 2 0 1 の障害を検出した際に、インタフェース 1 3 2 を第 1 の V R F のネットワークに所属するよう切り替えを行うこと。

h ) 状態監視ルール 5 0 ( 詳細は後述 ) により予備サーバ 2 0 2 の障害を検出した際に、インタフェース 1 3 2 を元の状態に戻す ( スイッチバックさせる ) こと。

30

【 0 1 0 4 】

行 C 2 0 3 は、状態監視ルール 5 0 として、第 1 の V R F のネットワーク内に存在する、I P アドレスが 1 0 . 1 . 1 . 1 を識別子とする装置へのパケットの到達性の監視を規定する。換言すれば、行 C 2 0 3 は、運用サーバ 2 0 1 の状態監視ルールを定義している。

【 0 1 0 5 】

図 2 8 は、第 2 実施例における障害切替データベース 1 8 0 の一例を示す説明図である。図 1 0 に示した第 1 実施例との違いは、障害切替データベース 1 8 0 に格納されているエントリの内容のみである。エントリ E 2 1 には、図 2 7 で説明したコンフィギュレーション情報の行 C 2 0 1 で定義された情報が格納される。また、エントリ E 2 2 には、図 2 7 で説明したコンフィギュレーション情報の行 C 2 0 2 で定義された情報が格納される。

40

【 0 1 0 6 】

( B - 2 ) 第 2 実施例における状態監視処理 ( 1 ) :

第 2 実施例における状態監視処理は、図 1 4 で説明した第 1 実施例と同じ手順により行う。しかし、第 2 実施例における状態監視処理では、障害の検出と後述するフェイルオーバ処理がなされることを契機として、その監視対象が、運用サーバ 2 0 1 - 予備サーバ 2 0 2 - 運用サーバ 2 0 1 . . . と変化する点において第 1 実施例と異なる。詳細については後述する。

【 0 1 0 7 】

( B - 3 ) 第 2 実施例におけるフェイルオーバ処理 ( 1 ) :

50

図29は、第2実施例におけるフェイルオーバ処理(図14:ステップS508)の手順を示すフローチャートである。図16に示した第1実施例との違いは、ステップS603の代わりにステップS604、S605が追加されている点と、ステップS611が新しく追加されている点であり、他の動作は第1実施例と同じである。

【0108】

ステップS604においてフェイルオーバ処理部160は、切替後動作がロックか否かを判定する。この判定は、ステップS601において検索されたエントリ(図28に示した障害切替データベース180のうち、監視IDフィールドの値が状態監視処理において障害が検出された監視IDと同じエントリ)の切替後動作フィールドの値を元に行う。切替後動作フィールドの値が「ロック」である場合はステップS620へ遷移する。

10

【0109】

一方、切替後動作フィールドの値が「ロック」で無い場合、ステップS605においてフェイルオーバ処理部160は、切替後動作がスイッチバックであるか否かを判定する。この判定は、ステップS601で読み出した切替後動作フィールドの値を元に行う。切替後動作フィールドの値が「スイッチバック」で無い場合、ステップS610においてフェイルオーバ処理部160は、復旧切替データベース190(図11)へ監視対象となるエントリの情報を登録した後、ステップS620へ遷移する。

【0110】

一方、切替後動作フィールドの値が「スイッチバック」である場合はステップS611へ遷移する。ステップS611においてフェイルオーバ処理部160は、障害切替データベース180(図28)の切替先VRFフィールドの更新を行う。具体的には、フェイルオーバ処理部160は、切替先VRFフィールドの値を、インタフェースデータベース140の同じインタフェース番号を有するエントリであって、当該エントリのステップS601において変更される前のVRF番号フィールドの値へと更新する。

20

【0111】

図30は、図29のステップS601において更新された後のインタフェースデータベース140を示す説明図である。障害検出前のインタフェースデータベース140を示す図6との違いは、インタフェース番号フィールドの値が「131」のエントリ(エントリE21)のVRF番号フィールドの値が「2」、インタフェース番号フィールドの値が「132」のエントリ(エントリE22)のVRF番号フィールドの値が「1」となっている点である。

30

【0112】

図31は、図29のステップS602において更新された後のVRF1ルーティングテーブル121を示す説明図である。障害検出前のVRF1ルーティングテーブル121を示す図7との違いは、ステップS601で更新された後のインタフェースデータベース140(図30)に基づいたルーティングテーブルの書き換えが行われている点である。具体的には、以下の2点である。

・インタフェース131を示すエントリE1(図7)、および、運用サーバ201(インタフェース131に接続されている装置)を示すエントリE2(図7)が削除されている点。

40

・インタフェース132を示すエントリE21、および、予備サーバ202(インタフェース132に接続されている装置)を示すエントリE22が追加されている点。

【0113】

図32は、図29のステップS602において更新された後のVRF2ルーティングテーブル122を示す説明図である。障害検出前のVRF2ルーティングテーブル122を示す図8との違いは、ステップS601で更新された後のインタフェースデータベース140(図30)に基づいたルーティングテーブルの書き換えが行われている点である。具体的には、以下の2点である。

・インタフェース132を示すエントリE1(図8)、および、予備サーバ202(インタフェース132に接続されている装置)を示すエントリE2(図8)が削除されてい

50

る点。

・インタフェース131を示すエントリE21、および、運用サーバ201（インタフェース131に接続されている装置）を示すエントリE22が追加されている点。

【0114】

図33は、図29のステップS611において更新された後の障害切替データベース180を示す説明図である。障害検出前の障害切替データベース180を示す図28との違いは、切替対象インタフェースフィールドの値が「131」のエントリ（エントリE21）の切替先VRFフィールドの値が「1」、切替対象インタフェースフィールドの値が「132」のエントリ（エントリE22）の切替先VRFフィールドの値が「2」となっている点である。

10

【0115】

（B-4）第2実施例における状態監視処理（2）：

図9で説明した通り、監視ID50の監視対象の装置は、監視先IPアドレスフィールドの値が10.1.1.1、かつ、監視先VRFフィールドの値が第1のVRFである。これは、すなわち、運用サーバ201の障害検出前においては運用サーバ201であった。

【0116】

第2実施例において、運用サーバ201の障害が検出された場合の状態監視処理について考える。まず、状態監視処理によってサーバの障害が検出され（図14：ステップS504：なし）、フェイルオーバー処理（図14：ステップS508）が行われる。フェイルオーバー処理（図29）によって、図28に示した状態の障害切替データベース180をもとに、インタフェースデータベース140は図30に示した状態へ更新される。また、インタフェースデータベース140の更新に伴って、ルーティングテーブル（VRF1ルーティングテーブル121、VRF2ルーティングテーブル122）も、図31、32に示した状態へ更新される。

20

【0117】

その後の状態監視処理は次のようになる。状態監視データベース170が図9に示した状態の場合、エントリE1（監視ID：50）の例では、監視先VRFフィールドの値は「1」である。このため、状態監視処理（図14：ステップS502）においてフェイルオーバー処理部160は、図31に示したVRF1ルーティングテーブル121を検索する。このとき、監視先IPアドレスフィールドの値「10.1.1.1」をキーとして、VRF1ルーティングテーブル121のあて先IPアドレスフィールドに一致するエントリを検索する。すると、ネクストホップIPアドレスは「10.1.1.1」、出力インタフェースは「132」（エントリE21）であることが分かる。

30

【0118】

従って、フェイルオーバー処理部160は、インタフェース132から予備サーバ202へ向けてパケットを送信する。すなわち、このことは、図9の監視ID50の監視対象の装置が、運用サーバ201から予備サーバ202へ変更されたことを示している。

【0119】

新たな監視対象である予備サーバ202は正常に動作している。このため、状態監視処理（図14：ステップS503）においてフェイルオーバー処理部160は、応答パケットを受信する。応答パケットを受信するため、フェイルオーバー処理部160は、状態監視データベース170の監視状態フィールドの値を「通信可」へと更新し、復旧検出時処理（図14：ステップS506）を行う。しかし、第2実施例における復旧切替データベース190には何も情報が登録されていないため、フェイルオーバー処理部160は、復旧検出時処理では何も行わない。

40

【0120】

（B-5）第2実施例におけるフェイルオーバー処理（2）：

次に、予備サーバ202の障害が検出された場合のフェイルオーバー処理について考える。まず、状態監視処理によってサーバの障害が検出され（図14：ステップS504：な

50

し)、フェイルオーバ処理(図14:ステップS508)が行われる。フェイルオーバ処理(図29)によって、図33に示した状態の障害切替データベース180をもとに、インタフェースデータベース140は図6に示した状態へ更新される。また、インタフェースデータベース140の更新に伴って、ルーティングテーブル(VRF1ルーティングテーブル121、VRF2ルーティングテーブル122)も、図7、8に示した状態へ更新される。すなわち、各データベース(インタフェースデータベース140、VRF1ルーティングテーブル121、VRF2ルーティングテーブル122)が初期状態へ戻される(スイッチバックされる)ことを意味している。

#### 【0121】

その後の状態監視処理は図14で説明した流れと同じになり、監視ID50の監視対象の装置は、運用サーバ201へと変更される。このように、第2実施例におけるフェイルオーバ処理部160は、運用サーバ201の障害を検出した後は、監視対象を予備サーバ202へ変更し、予備サーバ202を監視する。また、予備サーバ202の障害を検出した後は、監視対象を運用サーバ201へ変更し、運用サーバ201を監視する。すなわち、第2実施例における状態監視処理では、現在サービスを提供しているサーバ(いわゆる運用系サーバ)を監視対象としている。

#### 【0122】

このように、第2実施例では、状態監視部としてのフェイルオーバ処理部160は、クライアント装置(ホスト301、ホスト302)に所定のサービスを提供する第1の仮想ネットワーク(VRF1)に所属する処理装置(運用サーバ201)の状態を監視する。そして、フェイルオーバ処理部160は、当該処理装置(運用サーバ201)がサービスを提供することができない障害状態であると判定された場合に、第2の処理装置(予備サーバ202)と、クライアント装置(ホスト301、ホスト302)とを第1の仮想ネットワーク(VRF1)に所属させ、第1の処理装置(運用サーバ201)を第2の仮想ネットワーク(VRF2)に所属させるように、VRF定義情報であるインタフェースデータベース140を更新する。このため、第1実施例と同様の効果を得ることができる。

#### 【0123】

さらに、処理装置(運用サーバ201、予備サーバ202)についてのVRF定義情報を更新するため、例えば、ネットワーク中継装置100に接続されるサーバの数が、ネットワーク中継装置100に接続されるホストの数よりも少ない場合は、VRF定義情報の更新量を少なくすることができる。このような場合は、フェイルオーバに要する時間を、より短縮することが可能である。

#### 【0124】

C. 第3実施例:

(C-1) 第3実施例におけるシステム構成:

図34は、第3実施例におけるネットワークシステム10aの概略構成を示す説明図である。図1で示した第1実施例との違いは、運用サーバ201の代わりに2台の運用サーバ211、221を備える点と、予備サーバ202の代わりに2台の予備サーバ212、222を備える点と、障害切替データベース180の代わりに障害切替経路データベース181を備える点と、復旧切替データベース190を備えない点であり、他の構成については第1実施例と同様である。なお、以下では、第1実施例と異なる構成および動作を有する部分についてのみ説明する。

#### 【0125】

運用サーバ211は、第1のサービス(例えば、WEBサービス等)をホストに対して提供するための運用系サーバコンピュータである。運用サーバ221は、第2のサービス(例えば、メールサービス等)をホストに対して提供するための運用系サーバコンピュータである。予備サーバ212は、運用サーバ211がサービスを提供し得ない状態の場合にサービスを提供する待機系サーバコンピュータである。予備サーバ222は、運用サーバ221がサービスを提供し得ない状態の場合にサービスを提供する待機系サーバコンピュータである。

10

20

30

40

50

## 【 0 1 2 6 】

ネットワーク装置 1 0 0 a は、4 台のサーバと、2 台のホストコンピュータとの間の通信を中継するレイヤ 3 のネットワーク中継装置である。ネットワーク装置 1 0 0 a は、4 つのインタフェース（インタフェース 1 3 1 ~ 1 3 4 ）と、コンフィギュレーションデータベース 1 1 0 と、V R F 1 ルーティングテーブル 1 2 1 と、V R F 2 ルーティングテーブル 1 2 2 と、インタフェースデータベース 1 4 0 と、パケット転送処理部 1 5 0 と、フェイルオーバー処理部 1 6 0 と、状態監視データベース 1 7 0 と、障害切替経路データベース 1 8 1 とを備えている。

## 【 0 1 2 7 】

インタフェース 1 3 1 は、運用サーバ 2 1 1 および運用サーバ 2 2 1 と回線を介して接続されている。同様に、インタフェース 1 3 2 は、予備サーバ 2 1 2 および予備サーバ 2 2 2 と、インタフェース 1 3 3 はホスト 3 0 1 と、インタフェース 1 3 4 はホスト 3 0 2 と、それぞれ回線を通じて接続されている。障害切替経路データベース 1 8 1 は、フェイルオーバー処理に用いられる情報を保持するためのデータベースである。

10

## 【 0 1 2 8 】

第 3 実施例において第 1 のサービスを提供する 2 台のサーバ（すなわち、運用サーバ 2 1 1 および予備サーバ 2 1 2 ）には、図 2 に示す I P アドレスと、サブネットマスク長と、デフォルトゲートウェイがそれぞれ設定される。すなわち、運用サーバ 2 1 1 と、予備サーバ 2 1 2 には、同じ I P アドレスが設定される。

## 【 0 1 2 9 】

20

図 3 5 は、第 3 実施例において第 2 のサービスを提供する 2 台のサーバの I P アドレス情報の一例を示す説明図である。第 2 のサービスを提供する 2 台のサーバ（すなわち、運用サーバ 2 2 1 および予備サーバ 2 2 2 ）には、図 3 5 に示す I P アドレスと、サブネットマスク長と、デフォルトゲートウェイがそれぞれ設定される。すなわち、運用サーバ 2 2 1 と、予備サーバ 2 2 2 には、同じ I P アドレスが設定される。

## 【 0 1 3 0 】

図 3 6 は、第 3 実施例におけるネットワーク装置 1 0 0 a の構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。図 5 に示した第 1 実施例との違いは、行 C 1 1、C 1 5 が削除されている点と、行 C 3 0 1、C 3 0 2、C 3 0 3 が追加されている点であり、他の構成については第 1 実施例と同様である。

30

## 【 0 1 3 1 】

行 C 1 7 は、状態監視ルール 5 0 として、第 1 の V R F のネットワーク内に存在する、I P アドレスが 1 0 . 1 . 1 . 1 を識別子とする装置へのパケットの到達性の監視を規定する。換言すれば、行 C 1 7 は、運用サーバ 2 1 1 の状態監視ルールを定義している。行 C 3 0 1 は、状態監視ルール 5 1 として、第 1 の V R F のネットワーク内に存在する、I P アドレスが 1 0 . 1 . 1 . 2 を識別子とする装置へのパケットの到達性の監視を規定する。換言すれば、行 C 3 0 1 は、運用サーバ 2 2 1 の状態監視ルールを定義している。

## 【 0 1 3 2 】

行 C 3 0 2 は、第 1 の V R F のネットワーク内にある I P アドレス 1 0 . 1 . 1 . 1 をあて先とする経路情報に関して、状態監視ルール 5 0 で規定した監視先が障害となった場合に、出力インタフェースをインタフェース 1 3 2 に切り替えることを定義している。行 C 3 0 3 は、第 1 の V R F のネットワーク内にある I P アドレス 1 0 . 1 . 1 . 2 をあて先とする経路情報に関して、状態監視ルール 5 1 で規定した監視先が障害となった場合に、出力インタフェースをインタフェース 1 3 2 に切り替えることを定義している。

40

## 【 0 1 3 3 】

図 3 7 は、第 3 実施例における V R F 1 ルーティングテーブル 1 2 1 の一例を示す説明図である。図 7 に示した第 1 実施例との違いは、エントリ E 3 1 に運用サーバ 2 1 1 の情報が保持されている点と、エントリ E 3 2 に運用サーバ 2 2 1 の情報が保持されている点だけである。

## 【 0 1 3 4 】

50

図38は、第3実施例におけるVRFルーティングテーブル122の一例を示す説明図である。図8に示した第1実施例との違いは、エントリE31に予備サーバ212の情報が保持されている点と、エントリE32に予備サーバ222の情報が保持されている点だけである。

【0135】

図39は、第3実施例における状態監視データベース170の一例を示す説明図である。図9に示した第1実施例との違いは、監視ID51を定義するエントリE32が追加されている点である。図39の例では、監視ID50の監視対象の装置は、監視先IPアドレスフィールドの値が10.1.1.1、かつ、監視先VRFフィールドの値が第1のVRFであるため、運用サーバ211であることがわかる。一方、監視ID51の監視対象の装置は、監視先IPアドレスフィールドの値が10.1.1.2、かつ、監視先VRFフィールドの値が第1のVRFであるため、運用サーバ221であることがわかる。また、運用サーバ211、221共に現在サービスの提供が可能な状態であることがわかる。

10

【0136】

図40は、第3実施例における障害切替経路データベース181の一例を示す説明図である。障害切替経路データベース181は、監視IDフィールドと、切替対象VRFフィールドと、切替対象経路フィールドと、切替先出力インタフェースフィールドとを含んでいる。監視IDフィールドには、監視対象のグループを識別するための識別子が格納されている。切替対象VRFフィールドには、状態監視処理によってフェイルオーバーが実行されるVRFネットワークの識別子が格納されている。切替対象経路フィールドには、フェイルオーバー処理によって切替が行われる対象の経路を示す先IPアドレスが格納されている。切替先出力インタフェースフィールドには、フェイルオーバー処理によって切替が行われる、新しい出力インタフェースの識別子が格納されている。

20

【0137】

この障害切替経路データベース181は、ネットワーク装置100aにおける構成情報を定義したコンフィギュレーションデータベース110に基づいて保持される。すなわち、障害切替経路データベース181のエントリE31には、図36で説明したコンフィギュレーション情報の行C302で定義された情報が格納される。同様に、エントリE32には、行C303で定義された情報が格納される。

【0138】

(C-2) 第3実施例における状態監視処理(1)：

第3実施例における状態監視処理は、図14で説明した第1実施例と同じ手順により行う。

30

【0139】

図41は、運用サーバ211に障害が発生し、図14のステップS507において更新された後の状態監視データベース170を示す説明図である。障害検出前の状態監視データベース170を示す図39との違いは、監視IDフィールドの値が「50」、かつ、監視先IPアドレスが「10.1.1.1」を示すエントリ(エントリE31)の監視状態フィールドの値が「通信不可」となっている点である。

【0140】

(C-3) 第3実施例におけるフェイルオーバー処理(1)：

図42は、第3実施例におけるフェイルオーバー処理(図14：ステップS508)の手順を示すフローチャートである。フェイルオーバー処理部160は、状態監視処理で障害を検出した監視IDと、図40で説明した障害切替経路データベース181とを使用し、図42のフローチャートに従って、障害検出に伴うフェイルオーバー処理を行う。

40

【0141】

まず、ステップS701においてフェイルオーバー処理部160は、切替対象経路に対応する出力インタフェースを、切替先出力インタフェースに変更する。具体的には、フェイルオーバー処理部160は、障害切替経路データベース181(図40)のうち、監視IDフィールドの値が、状態監視処理において障害が検出された監視IDと同じエントリを検

50

索する。そして、検索されたエントリについての、切替対象VRFフィールドと、切替対象経路フィールドと、切替先出力インタフェースフィールドと、の値を読み出す。

【0142】

フェイルオーバー処理部160は、ルーティングテーブルのあて先IPアドレスフィールドを、読み出された切替対象経路フィールドの値をキーとして検索する。このとき検索の対象とするルーティングテーブルは、読み出された切替対象VRFフィールドの値に対応するルーティングテーブルである。すなわち、読み出された切替対象VRFフィールドの値が「1」の場合はVRF1ルーティングテーブル121を検索し、「2」の場合はVRF2ルーティングテーブル122を検索する。フェイルオーバー処理部160は、検索の結果、一致したエントリについての出力インタフェースフィールドの値を一時的に記憶する。さらに、一致したエントリについての出力インタフェースフィールドの値を、読み出された切替先出力インタフェースフィールドの値へと更新する。

10

【0143】

次に、ステップS702においてフェイルオーバー処理部160は、切替対象出力インタフェースのVRF番号を検索する。具体的には、インタフェースデータベース140(図6)のインタフェース番号フィールドを、読み出された切替先出力インタフェースフィールドの値をキーとして検索する。そして、一致するエントリのVRF番号フィールドの値を取得する。

【0144】

ステップS703においてフェイルオーバー処理部160は、切替対象VRFのあて先が切替対象出力インタフェースのVRFのルーティングテーブルにあるか否かを判定する。具体的には、i)ステップS701で読み出された切替対象VRFフィールドの値に対応するルーティングテーブルに登録されているエントリについてのあて先IPアドレスが、ii)ステップS702で取得したVRF番号フィールドの値に対応するルーティングテーブルに存在するか否かを判定する。

20

【0145】

フェイルオーバー処理部160は、ステップS703において存在しないと判定した場合、上記i)のルーティングテーブルに登録されているあて先IPアドレスの経路情報を、上記ii)のルーティングテーブルにコピーする(ステップS704)。一方、ステップS703において存在すると判定した場合、ステップS705へ遷移する。

30

【0146】

ステップS705においてフェイルオーバー処理部160は、全ての経路を処理したか否かを判定する。具体的には、フェイルオーバー処理部160は、上記i)のルーティングテーブルに登録されている全てのエントリについて、ステップS703、S704の処理を行ったか否かを判定する。全ての経路を処理していない場合、フェイルオーバー処理部160は、ステップS703へ遷移する。

【0147】

一方、全ての経路を処理した場合、ステップS706においてフェイルオーバー処理部160は、切替対象出力インタフェースを、ステップS701で記憶したインタフェースに変更する。具体的には、フェイルオーバー処理部160は、障害切替経路データベース181の切替対象出力インタフェースフィールドの値を、ステップS701で一時的に記憶した値へ更新する。

40

【0148】

ステップS707においてフェイルオーバー処理部160は、全ての切替対象について処理を行ったか否かを判定する。具体的には、ステップS701において検索されたエントリ(障害切替経路データベース181のうち、監視IDフィールドの値が、状態監視処理において障害が検出された監視IDと同じエントリ)の切替対象インタフェースの全てについて、上述のステップの処理を行ったか否かを判定する。全ての切替対象について処理を行った場合、処理を終了する。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー処理部160は、ステップS701へ戻り、処理を継続する。

50

## 【 0 1 4 9 】

第3実施例において、運用サーバ211の障害が検出された場合のフェイルオーバー処理（図42）について考える。まず、フェイルオーバー処理部160は、障害切替経路データベース181のうち、監視IDフィールドの値が「50」のエントリを検索する（ステップS701）。そして、フェイルオーバー処理部160は、切替対象VRF「1」と、切替対象経路「10.1.1.1」と、切替先出力インタフェース「132」とを読み出す。

## 【 0 1 5 0 】

次に、フェイルオーバー処理部160は、切替対象VRF「1」に対応するVRF1ルーティングテーブル121を、切替対象経路「10.1.1.1」をキーとして検索する。そして、フェイルオーバー処理部160は、一致するエントリE31の出力インタフェース「131」を一時的に記憶した上で、出力インタフェースフィールドの値を、読み出された切替先出力インタフェース「132」へと更新する。

10

## 【 0 1 5 1 】

フェイルオーバー処理部160は、インタフェースデータベース140を、読み出された切替先出力インタフェース「132」をキーとして検索する（ステップS702）。そして、一致するエントリのVRF番号「2」を取得する。

## 【 0 1 5 2 】

フェイルオーバー処理部160は、i)ステップS701で読み出された切替対象VRF「1」に対応するVRF1ルーティングテーブル121に登録されているエントリについてのあて先IPアドレスが、ii)ステップS702で取得したVRF番号「2」に対応するVRF2ルーティングテーブル122に存在するか否かを判定する。そして、フェイルオーバー処理部160は、上記i)に存在し、かつ、上記ii)に存在しないあて先IPアドレスの経路情報を、VRF2ルーティングテーブル122にコピーする（ステップS703、S704）。

20

## 【 0 1 5 3 】

図43は、図42のステップS701において更新された後のVRF1ルーティングテーブル121を示す説明図である。障害検出前のVRF1ルーティングテーブル121を示す図37との違いは、エントリE31の出力インタフェースフィールドの値が更新されている点である。

## 【 0 1 5 4 】

図44は、図42のステップS703、S704において更新された後のVRF2ルーティングテーブル122を示す説明図である。障害検出前のVRF2ルーティングテーブル122を示す図38との違いは、エントリE34～E37が追加されている点である。追加されているエントリE34～E37は、障害検出前のVRF1ルーティングテーブル121に存在し、かつ、障害検出前のVRF2ルーティングテーブル122に存在しないあて先IPアドレスの経路情報である。

30

## 【 0 1 5 5 】

図45は、図42のステップS706において更新された後の障害切替経路データベース181を示す説明図である。障害検出前の障害切替経路データベース181を示す図40との違いは、監視ID50の監視情報を示すエントリE31の切替先出力インタフェースフィールドの値が「131」へと更新されている点である。

40

## 【 0 1 5 6 】

（C-4）第3実施例における障害検出後の動作：

図46は、第3実施例において運用サーバ211の障害が検出された場合の第1のサービス提供時の動作を示す説明図である。図46に示すように、ホスト301は、第1のサービスを提供するサーバ（運用サーバ211もしくは予備サーバ212）にアクセスするため、あて先IPアドレスを10.1.1.1とする要求パケットを送信する。

## 【 0 1 5 7 】

ネットワーク装置100aは、ホスト301から送信されたパケットをインタフェース133において受信する（図13：ステップS11）。次に、パケット転送処理部150

50

は、図6に示したインタフェースデータベース140を検索し、インタフェースの識別子133に一致するエントリのVRFフィールドの値「1」を取得する(図13:ステップS12)。VRFが1であるため、パケット転送処理部150は、図43に示したVRF1ルーティングテーブル121を検索する(図13:ステップS13)。このようにして、パケット転送処理部150は、ステップS13で求めたインタフェース132からパケットを出力する。

【0158】

上述のようにして、ホスト301からの要求パケットは、予備サーバ212へ転送される。予備サーバ212は、ホスト301から受信したパケットを元にしてサービスを行った後、ホスト301に対して応答パケットを送信する。この応答パケットのあて先IPアドレスは、ホスト301のIPアドレス20.1.1.1である。

10

【0159】

ネットワーク装置100aは、予備サーバ212から送信されたパケットをインタフェース132において受信する。その後、パケット転送処理部150は、当該受信パケットについて、上述と同様の処理を行う。この際、インタフェースデータベース140のインタフェースの識別子132に一致するエントリのVRFフィールドの値は「2」であるため、パケット転送処理部150は、VRF2ルーティングテーブル122を検索する。この結果、予備サーバ212からの応答パケットはホスト301へ転送される。なお、ホスト302についてもホスト301と同様の動作となる。

【0160】

20

以上のように、第1のサービスを提供する運用サーバ211の障害検出後においては、予備サーバ212が第1のサービスを提供する運用系サーバとして機能することがわかる。

【0161】

図47は、第3実施例において運用サーバ211の障害が検出された場合の第2のサービス提供時の動作を示す説明図である。図47に示すように、ホスト301は、第2のサービスを提供するサーバ(運用サーバ221もしくは予備サーバ222)にアクセスするため、あて先IPアドレスを10.1.1.2とする要求パケットを送信する。

【0162】

ネットワーク装置100aは、ホスト301から送信されたパケットをインタフェース133において受信する(図13:ステップS11)。図46の場合と同様に、パケット転送処理部150は、図6に示したインタフェースデータベース140を検索し、インタフェースの識別子133に一致するエントリのVRFフィールドの値「1」を取得する(図13:ステップS12)。VRFが1であるため、パケット転送処理部150は、図43に示したVRF1ルーティングテーブル121を検索する(図13:ステップS13)。このようにして、パケット転送処理部150は、ステップS13で求めたインタフェース131からパケットを出力する。

30

【0163】

上述のようにして、ホスト301からの要求パケットは、運用サーバ221へ転送される。運用サーバ221は、ホスト301から受信したパケットを元にしてサービスを行った後、ホスト301に対して応答パケットを送信する。この応答パケットのあて先IPアドレスは、ホスト301のIPアドレス20.1.1.1である。

40

【0164】

ネットワーク装置100aは、運用サーバ221から送信されたパケットをインタフェース131において受信する。その後、パケット転送処理部150は、当該受信パケットについて、図13で説明したものと同様の処理を行う。この際、インタフェースデータベース140のインタフェースの識別子131に一致するエントリのVRFフィールドの値は「1」となるため、パケット転送処理部150は、VRF1ルーティングテーブル121を検索する。この結果、運用サーバ221からの応答パケットはホスト301へ転送される。なお、ホスト302についてもホスト301と同様の動作となる。

50

## 【 0 1 6 5 】

以上のように、第 1 のサービスを提供する運用サーバ 2 1 1 の障害検出後においても、障害が発生していない運用サーバ 2 2 1 は、運用サーバ 2 1 1 の障害の影響を受けることなく継続して第 2 のサービスを提供する運用系サーバとして機能することがわかる。

## 【 0 1 6 6 】

( C - 5 ) 第 3 実施例における状態監視処理 ( 2 ) :

図 3 9 で説明した通り、監視 ID 5 0 の監視対象の装置は、監視先 IP アドレスフィールドの値が 1 0 . 1 . 1 . 1、かつ、監視先 V R F フィールドの値が第 1 の V R F である。これは、すなわち、運用サーバ 2 1 1 の障害検出前においては運用サーバ 2 1 1 であった。

10

## 【 0 1 6 7 】

第 3 実施例において、運用サーバ 2 1 1 の障害が検出された場合の状態監視処理について考える。まず、状態監視処理によってサーバの障害が検出され ( 図 1 4 : ステップ S 5 0 4 : なし )、フェイルオーバー処理 ( 図 1 4 : ステップ S 5 0 8 ) が行われる。フェイルオーバー処理 ( 図 4 2 ) によって、図 4 0 に示した状態の障害切替経路データベース 1 8 1 をもとに、V R F 1 ルーティングテーブル 1 2 1 は図 4 3 に示す状態に、V R F 2 ルーティングテーブル 1 2 2 は図 4 4 に示す状態に、それぞれ更新される。

## 【 0 1 6 8 】

その後の状態監視処理は次のようになる。状態監視データベース 1 7 0 が図 3 9 に示した状態の場合、エン트리 E 3 1 ( 監視 ID : 5 0 ) の例では、監視先 V R F フィールドの値は「 1 」である。このため、状態監視処理 ( 図 1 4 : ステップ S 5 0 2 ) においてフェイルオーバー処理部 1 6 0 は、図 4 3 に示した V R F 1 ルーティングテーブル 1 2 1 を検索する。このとき、監視先 IP アドレスフィールドの値「 1 0 . 1 . 1 . 1 」をキーとして、V R F 1 ルーティングテーブル 1 2 1 のあて先 IP アドレスフィールドに一致するエント리를検索する。すると、ネクストホップ IP アドレスは「 1 0 . 1 . 1 . 1」、出力インタフェースは「 1 3 2 」 ( 図 4 3 : エン트리 E 3 1 ) であることが分かる。

20

## 【 0 1 6 9 】

従って、フェイルオーバー処理部 1 6 0 は、インタフェース 1 3 2 から予備サーバ 2 1 2 へ向けてパケットを送信する。すなわち、このことは、図 3 9 のエン트리 E 3 1 に示した監視 ID 5 0 の監視対象の装置が、運用サーバ 2 1 1 から予備サーバ 2 1 2 へ変更されたことを示している。

30

## 【 0 1 7 0 】

新たな監視対象である予備サーバ 2 1 2 は正常に動作している。このため、状態監視処理 ( 図 1 4 : ステップ S 5 0 3 ) においてフェイルオーバー処理部 1 6 0 は、応答パケットを受信する。応答パケットを受信するため、フェイルオーバー処理部 1 6 0 は、状態監視データベース 1 7 0 の監視状態フィールドの値を「通信可」へと更新し、復旧検出時処理 ( 図 1 4 : ステップ S 5 0 6 ) を行う。しかし、第 3 実施例における復旧切替データベース 1 9 0 には何も情報が登録されていないため、フェイルオーバー処理部 1 6 0 は、復旧検出時処理では何も行わない。上述の状態監視処理の動作を行った後の状態監視データベース 1 7 0 は、図 3 9 で示した状態となる。

40

## 【 0 1 7 1 】

( C - 6 ) 第 3 実施例におけるフェイルオーバー処理 ( 2 ) :

次に、予備サーバ 2 1 2 の障害が検出された場合のフェイルオーバー処理について考える。まず、状態監視処理によってサーバの障害が検出され ( 図 1 4 : ステップ S 5 0 4 : なし )、フェイルオーバー処理 ( 図 1 4 : ステップ S 5 0 8 ) が行われる。フェイルオーバー処理 ( 図 4 2 ) では、フェイルオーバー処理部 1 6 0 は、図 4 5 に示した障害切替経路データベース 1 8 1 のうち、監視 ID フィールドの値が「 5 0 」のエント리를検索し、切替対象 V R F 「 1 」と、切替対象経路「 1 0 . 1 . 1 . 1 」と、切替先出力インタフェース「 1 3 1 」を読み出す ( ステップ S 7 0 1 )。

## 【 0 1 7 2 】

50

フェイルオーバー処理部 160 は、VRF 1 ルーティングテーブル 121 を、切替対象経路「10.1.1.1」をキーとして検索する。そして、フェイルオーバー処理部 160 は、一致するエントリの出力インタフェース「132」を一時的に記憶した上で、出力インタフェースフィールドの値を、上記で読み出された「131」へと更新する。

【0173】

フェイルオーバー処理部 160 は、図 6 に示したインタフェースデータベース 140 を、読み出された切替先出力インタフェース「131」をキーとして検索する（ステップ S702）。そして、一致するエントリの VRF 番号「1」を取得する。

【0174】

フェイルオーバー処理部 160 は、i) ステップ S701 で読み出された切替対象 VRF 「1」に対応する VRF 1 ルーティングテーブル 121 に登録されているエントリについて、あて先 IP アドレスが、ii) ステップ S702 で取得した VRF 番号「1」に対応する VRF 1 ルーティングテーブル 121 に存在するかどうかを判定する。上記 i)、ii) 共に、VRF 1 ルーティングテーブル 121 を参照しているため、ステップ S703 の判定は必ず「YES」となる。すなわち、ステップ S704 の IP アドレスの経路情報のコピーは実行されない。

10

【0175】

ステップ S706 において、フェイルオーバー処理部 160 は、障害切替経路データベース 181 の切替先出力インタフェースの値を、上記で一時的に記憶した出力インタフェースの値「132」へ更新する。ステップ S707 においてフェイルオーバー処理部 160 は、全ての切替対象について処理を行ったと判断し、フェイルオーバー処理を終了する。

20

【0176】

なお、ステップ S701 において更新された後の VRF 1 ルーティングテーブル 121 は、図 37 に示す状態となる。ステップ S704 は実行されないため、VRF 2 ルーティングテーブル 122 は図 44 に示す状態のままである。また、ステップ S706 において更新された後の障害切替経路データベース 181 は、図 40 に示す状態となる。

【0177】

(C-7) 第 3 実施例における状態監視処理(3)：

図 39 で説明した通り、監視 ID 50 の監視対象の装置は、監視先 IP アドレスフィールドの値が 10.1.1.1、かつ、監視先 VRF フィールドの値が第 1 の VRF である。状態監視処理(図 14：ステップ S502)においてフェイルオーバー処理部 160 は、図 37 に示した VRF 1 ルーティングテーブル 121 を検索する。このとき、監視先 IP アドレスフィールドの値「10.1.1.1」に一致するエントリから、出力インタフェースは「131」(図 37：エントリ E31)であることが分かる。従って、フェイルオーバー処理部 160 は、インタフェース 131 から運用サーバ 211 へ向けてパケットを送信する。すなわち、このことは、図 39 のエントリ E31 に示した監視 ID 50 の監視対象の装置が、予備サーバ 212 から運用サーバ 211 へ戻ったことを示している。

30

【0178】

(C-8) 第 3 実施例における予備サーバの障害検出後の動作：

図 48 は、第 3 実施例において予備サーバ 212 の障害が検出された場合の第 1 のサービス提供時の動作を示す説明図である。図 48 に示すように、ホスト 301 は、第 1 のサービスを提供するサーバ(運用サーバ 211 もしくは予備サーバ 212)にアクセスするため、あて先 IP アドレスを 10.1.1.1 とする要求パケットを送信する。

40

【0179】

ネットワーク装置 100a のパケット転送処理部 150 は、図 6 に示したインタフェースデータベース 140 を検索し、インタフェースの識別子 133 に一致するエントリの VRF フィールドの値「1」を取得する(図 13：ステップ S12)。VRF が 1 であるため、パケット転送処理部 150 は、図 37 に示した VRF 1 ルーティングテーブル 121 を検索し(図 13：ステップ S13)、インタフェース 131 からパケットを出力する。

【0180】

50

上述のようにして、ホスト301からの要求パケットは、運用サーバ211へ転送される。運用サーバ211は、ホスト301から受信したパケットを元にしてサービスを行った後、ホスト301に対して応答パケットを送信する。この応答パケットのあて先IPアドレスは、ホスト301のIPアドレス20.1.1.1である。

#### 【0181】

ネットワーク装置100aは、運用サーバ211から送信されたパケットをインタフェース131において受信する。その後、パケット転送処理部150は、当該受信パケットについて、上述と同様の処理を行う。この際、インタフェースデータベース140のインタフェースの識別子131に一致するエントリのVRFフィールドの値は「1」であるため、パケット転送処理部150は、VRF1ルーティングテーブル121を検索する。この結果、運用サーバ211からの応答パケットはホスト301へ転送される。なお、ホスト302についてもホスト301と同様の動作となる。

10

#### 【0182】

以上のように、第1のサービスを提供する予備サーバ212の障害検出後においては、運用サーバ211が第1のサービスを提供する運用系サーバとして機能することがわかる。なお、第3実施例において予備サーバ212の障害が検出された場合の第2のサービス提供時の動作は、図47で説明したものと同様である。

#### 【0183】

図49は、ルーティングテーブルの内容を消去するためのコマンドの一例を示す説明図である。ネットワーク装置100aの管理者が、図49に示す運用コマンドをネットワーク装置100aの管理端末(図示省略)より実行することで、ネットワーク装置100aは、VRF2ルーティングテーブル122のエントリを全て消去する。その後、ネットワーク装置100aの学習処理部(図示省略)は、インタフェースデータベース140のVRF番号フィールドの値が「2」であるインタフェースと、当該インタフェースに回線や他のネットワークを介して接続されている装置とのIPアドレスを再学習する。そして、学習処理部は、学習した装置等の情報をVRF2ルーティングテーブル122へ格納する。

20

#### 【0184】

上述の通り、一旦予備サーバ212を運用系サーバとして機能させた場合、運用系サーバが予備サーバ212から運用サーバ211へと戻った場合であっても、VRF2ルーティングテーブル122には、VRF1ルーティングテーブル121の情報がコピーされたままである。すなわち、VRF2ルーティングテーブル122は、図44に示した状態のままであり、不要なエントリE34~E37が存在する。このようにすれば、上記のような不要なエントリを、ルーティングテーブルから削除することができ、ルーティングテーブルの不要なリソース消費を抑制することができる。

30

#### 【0185】

図50は、ルーティングテーブルから任意の経路情報を消去するためのコマンドの一例を示す説明図である。ネットワーク装置100aの管理者が、図50に示す運用コマンドをネットワーク装置100aの管理端末(図示省略)より実行することで、ネットワーク装置100aは、VRF1ルーティングテーブル121のあて先IPアドレスが「10.1.1.1」であるエントリを消去する。その後、ネットワーク装置100aの学習処理部(図示省略)は、インタフェースデータベース140のVRF番号フィールドの値が「1」であるインタフェースのうち、IPアドレスが「10.1.1.1」である情報を再学習する。そして、学習処理部は、学習した装置等の情報をVRF1ルーティングテーブル121へ格納する。

40

#### 【0186】

上述の通り、一旦予備サーバ212を運用系サーバとして機能させた場合、予備サーバ212の障害を検出するまでは、予備サーバ212が運用系サーバとして機能する。しかし、図50に示した運用コマンドを実行することによって、VRF1ルーティングテーブル121は図37に示す状態となる。このため、強制的に運用サーバ211を運用系サー

50

バとして機能させることができる。

【0187】

このように、第3実施例では、状態監視部としてのフェイルオーバ処理部160は、クライアント装置(ホスト301、ホスト302)に所定のサービスを提供する第1の仮想ネットワーク(VRF1)に所属する処理装置(運用サーバ211および運用サーバ221)の状態を監視する。そして、フェイルオーバ処理部160は、当該処理装置がサービスを提供することができない障害状態であると判定された場合に、第2の仮想ネットワークの経路情報であるVRF2ルーティングテーブル122に、第1の仮想ネットワークの経路情報であるVRF1ルーティングテーブル121中の、クライアント装置に関する経路情報をコピーする。また、VRF1ルーティングテーブル121中の、第1の処理装置(運用サーバ211または運用サーバ221)のレイヤ3アドレスをあて先アドレスとするエントリの出力先インタフェースを、第2の処理装置(予備サーバ212または予備サーバ222)が接続されているインタフェースへと更新する。

10

【0188】

この結果、例えば、ネットワーク装置100aの1つのインタフェースに対して、レイヤ3アドレスの異なる複数の処理装置(運用サーバ211、運用サーバ221)が接続されている場合であっても、互いの処理装置の状態に影響されないフェイルオーバ処理が可能となる。

【0189】

D. 第4実施例：

20

本発明の第4実施例では、運用系サーバと、待機系サーバとの両方を用いてサービスを行いつつ、フェイルオーバを実現する構成を説明する。

【0190】

(D-1) 第4実施例におけるシステム構成：

図51は、第4実施例におけるネットワークシステム10bの概略構成を示す説明図である。図1で示した第1実施例との違いは、障害切替データベース180の代わりにロードバランス切替データベース182を備える点と、VRF定義情報としてのVRFロードバランスデータベース141を備える点と、復旧切替データベース190を備えない点であり、他の構成については第1実施例と同様である。なお、以下では、第1実施例と異なる構成および動作を有する部分についてのみ説明する。

30

【0191】

運用サーバ201および予備サーバ202は、例えば、WEBサービス等のサービスを提供するためのサーバコンピュータである。本実施例においては、2台のサーバは共にホットスタンバイ状態でサービスを行う、いわゆる運用系サーバである。

【0192】

VRFロードバランスデータベース141は、運用サーバ201と、予備サーバ202とのどちらを選択して通信を行うかを判断するための基礎となるデータベースである。ロードバランス切替データベース182は、フェイルオーバ処理に用いられる情報を保持するためのデータベースである。

【0193】

40

図52は、第4実施例におけるネットワーク装置100bの構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。図5に示した第1実施例との違いは、行C10、C11、C14、C15が削除されている点と、行C401~C404が追加されている点であり、他の構成については第1実施例と同様である。

【0194】

行C401は、次のi)~l)のことを定義している。

i) インタフェース133が第1のVRFのネットワークに所属すること。

j) 行C402で定義する第2のVRFのネットワークとロードバランスすること。

k) 状態監視ルール50により運用サーバ201の障害を検出した際に、インタフェース133で受信したパケットのロードバランス先として第1のVRFを対象外にすること

50

。 1) 状態監視ルール50により運用サーバ201の復旧を検出した際に、インタフェース133で受信したパケットのロードバランス先として第1のVRFを対象外にしたままにする(ロックする)こと。

【0195】

行C402は、次のm)、n)のことを定義している。

m) インタフェース133が第2のVRFのネットワークに所属すること。

n) インタフェース133が行C401で定義する第1のVRFのネットワークとロードバランスすること。

【0196】

行C403は、次のo)~r)のことを定義している。

o) インタフェース134が第1のVRFのネットワークに所属すること。

p) 行C404で定義する第2のVRFのネットワークとロードバランスすること。

q) 状態監視ルール50により運用サーバ201の障害を検出した際に、インタフェース134で受信したパケットのロードバランス先として第1のVRFを対象外にすること。

r) 状態監視ルール50により運用サーバ201の復旧を検出した際に、インタフェース134で受信したパケットのロードバランス先として第1のVRFを対象にする(リカバリする)こと。

【0197】

行C404は、次のs)、t)のことを定義している。

s) インタフェース134が第2のVRFのネットワークに所属すること。

t) インタフェース134が行C403で定義する第1のVRFのネットワークとロードバランスすること。

【0198】

図53は、第4実施例におけるインタフェースデータベース140の一例を示す説明図である。図6に示した第1実施例との違いは、インタフェースデータベース140に格納されているエントリの内容のみである。エントリE43およびエントリE44のVRF番号フィールドには「LB」という値が格納されている。これは、インタフェース133およびインタフェース134からパケットを受信した際に、予め定められた規則に従ってロードバランス処理を行うことを意味している。ロードバランス処理についての詳細は後述する。

【0199】

図54は、第4実施例におけるVRFロードバランスデータベース141の一例を示す説明図である。VRFロードバランスデータベース141は、インタフェース番号フィールドと、ロードバランス種別フィールドと、VRF番号フィールドとを含んでいる。インタフェース番号フィールドには、パケットを受信したインタフェースの識別子が格納される。ロードバランス種別フィールドには、ネットワーク装置100bがパケットを転送する際に検索するルーティングテーブルのVRF番号を特定するための検索方法を示す情報が格納される。VRF番号フィールドには、ロードバランス処理の対象となるVRFネットワークの識別子が複数格納される。

【0200】

図55は、第4実施例におけるパケット転送処理の手順を示すフローチャートである。図13に示した第1実施例との違いは、ステップS21~S23が追加されている点だけであり、他の動作については第1実施例と同様である。ステップS21においてパケット転送処理部150は、インタフェースデータベース140のインタフェース番号フィールドの値と、パケットを受信したインタフェースの識別子とが一致するエントリのVRF番号フィールドの値が「LB」であるか否かを判定する。VRF番号フィールドの値が「LB」で無い場合、ステップS13へ遷移する。

【0201】

10

20

30

40

50

V R F 番号フィールドの値が「L B」である場合、ステップ S 2 2 においてパケット転送処理部 1 5 0 は、V R F ロードバランスデータベース 1 4 1 を検索する。具体的には、V R F ロードバランスデータベース 1 4 1 のインタフェース番号フィールドの値と、パケットを受信したインタフェースの識別子とが一致するエントリを検索する。そして、パケット転送処理部 1 5 0 は、当該一致したエントリのロードバランス種別フィールドの値と、V R F 番号フィールドの値とを取得する。

#### 【 0 2 0 2 】

ステップ S 2 3 においてパケット転送処理部 1 5 0 は、V R F 番号を決定する。パケット転送処理部 1 5 0 は、ステップ S 2 2 において取得したロードバランス種別フィールドの値が示す検索方法に従って V R F 番号を決定する。図 5 4 の例では、ロードバランス種別フィールドには「送信元 I P アドレス」という値が格納されている。このため、パケット転送処理部 1 5 0 は、送信元 I P アドレスをもとにして、所定のルールに基づいて V R F 番号を決定することとなる。所定のルールとは、例えば、次のようなルールを採用することができる。

- ・送信元 I P アドレスが「2 0 . 1 . 1 . 1」の場合は V R F 番号フィールドに格納されている複数の V R F ネットワークの識別子のうちの前者（すなわち、V R F 番号 1）を V R F 番号であると決定する。

- ・送信元 I P アドレスが「3 0 . 1 . 1 . 1」の場合は V R F 番号フィールドに格納されている複数の V R F ネットワークの識別子のうちの後者（すなわち、V R F 番号 2）を V R F 番号であると決定する。

#### 【 0 2 0 3 】

なお、このルールは、上記具体例に示した内容に限らず任意のものを採用することができる。例えば、送信元 I P アドレスに基づくハッシュ計算等により V R F 番号を求めるものとしても良い。また、V R F 番号を特定するための検索方法は、送信元 I P アドレス情報に基づくものに限られない。例えば、送信元 I P アドレス以外の情報（受信パケット中に含まれる種々の情報）に基づいて V R F 番号を決定しても良い。また、過去のパケット送信量の統計に基づいて、V R F 番号を特定することもできる。

#### 【 0 2 0 4 】

図 5 6 は、第 4 実施例における V R F 1 ルーティングテーブル 1 2 1 の一例を示す説明図である。第 4 実施例における V R F 1 ルーティングテーブル 1 2 1 は、図 7 に示した第 1 実施例と同様である。V R F 1 ルーティングテーブル 1 2 1 には、次のいずれかインタフェースの情報と、当該インタフェースに回線や他のネットワーク装置を介して接続されている装置の情報とが保持される。

- ・インタフェースデータベース 1 4 0（図 5 3）の V R F 番号フィールドの値が「1」であるインタフェース。

- ・インタフェースデータベース 1 4 0（図 5 3）の V R F 番号フィールドの値が「L B」であって、V R F ロードバランスデータベース 1 4 1の V R F 番号フィールドの値に「1」が含まれているインタフェース。

すなわち、インタフェース 1 3 1、1 3 3、1 3 4、および、運用サーバ 2 0 1、ホスト 3 0 1、ホスト 3 0 2 の情報が保持される。

#### 【 0 2 0 5 】

図 5 7 は、第 4 実施例における V R F 2 ルーティングテーブル 1 2 2 の一例を示す説明図である。図 8 に示した第 1 実施例との違いは、エントリ E 4 3 ~ E 4 6 が追加されている点だけである。V R F 2 ルーティングテーブル 1 2 2 には、次のいずれかインタフェースの情報と、当該インタフェースに回線や他のネットワーク装置を介して接続されている装置の情報とが保持される。

- ・インタフェースデータベース 1 4 0（図 5 3）の V R F 番号フィールドの値が「2」であるインタフェース。

- ・インタフェースデータベース 1 4 0（図 5 3）の V R F 番号フィールドの値が「L B」であって、V R F ロードバランスデータベース 1 4 1の V R F 番号フィールドの値に「

10

20

30

40

50

2」が含まれているインタフェース。

すなわち、インタフェース132、133、134、および、予備サーバ202、ホスト301、ホスト302の情報が保持される。

【0206】

図58は、第4実施例におけるロードバランス切替データベース182の一例を示す説明図である。ロードバランス切替データベース182は、監視IDフィールドと、切替対象インタフェースフィールドと、ロードバランス対象外VRFフィールドと、切替後状態フィールドとを含んでいる。監視IDフィールドと、切替対象インタフェースフィールドと、切替後状態フィールドに格納される情報は、図10で説明した通りである。ロードバランス対象外VRFフィールドには、監視IDにおける監視対象である装置が通信可状態から通信不可状態となった場合に、ロードバランス処理の対象となるVRFネットワーク群から除外する(換言すれば、VRFロードバランスデータベース141のVRF番号フィールドから除外する)VRF番号が格納されている。

10

【0207】

このロードバランス切替データベース182は、ネットワーク装置100bにおける構成情報を定義したコンフィギュレーションデータベース110(図52)に基づいて保持される。すなわち、ロードバランス切替データベース182のエントリE41には、図52で説明したコンフィギュレーション情報の行C401で定義された情報が格納される。同様に、エントリE42には行C403で定義された情報が格納される。

【0208】

20

(D-2)第4実施例における障害検出前の動作:

図59は、運用サーバ201と予備サーバ202とがサービスを提供し得る状態である場合の、ネットワークシステム10bの動作を示す説明図である。ホスト301からの要求パケットを受信したネットワーク装置100bは、図55に示したパケット転送処理に従ってパケットの出力先を決定する。具体的には、パケット転送処理部150は、図53に示すインタフェースデータベース140のインタフェースの識別子133に一致するエントリE43のVRF番号フィールドの値「LB」を取得する(ステップS12)。VRF番号が「LB」であるため、パケット転送処理部150はVRFロードバランスデータベース141を検索する(ステップS21、22)。

【0209】

30

次に、パケット転送処理部150は、送信元IPアドレス「20.1.1.1」を元にして、VRF番号「1」を決定する(ステップS23)。ステップS23で求めたVRF番号は「1」であるため、パケット転送処理部150は、VRFルーティングテーブル121を検索し、出力インタフェースフィールドの値「131」を取得する(ステップS13)。パケット転送処理部150は、ステップS13で求めた出力インタフェース131からパケットを出力する(ステップS14)。

【0210】

運用サーバ201は、ホスト301から受信したパケットをもとにしてサービスを行った後、ホスト301に対して応答パケットを送信する。この、応答パケット中継時には、第1のVRFネットワークが使用される(図53:エントリE41)。

40

【0211】

一方、ホスト302からの要求パケットを受信したネットワーク装置100bは、上述同様、図55に示したパケット転送処理に従ってパケットの出力先を決定する。具体的には、パケット転送処理部150は、インタフェースの識別子134に一致するエントリE44のVRF番号フィールドの値「LB」を取得する(ステップS12)。VRF番号が「LB」であるため、パケット転送処理部150はVRFロードバランスデータベース141を検索する(ステップS21、22)。

【0212】

次に、パケット転送処理部150は、送信元IPアドレス「30.1.1.1」を元にして、VRF番号「2」を決定する(ステップS23)。ステップS23で求めたVRF

50

番号は「2」であるため、パケット転送処理部150は、VRFルーティングテーブル122を検索し、出力インタフェースフィールドの値「132」を取得する(ステップS13)。パケット転送処理部150は、ステップS13で求めた出力インタフェース132からパケットを出力する(ステップS14)。

#### 【0213】

予備サーバ202は、ホスト302から受信したパケットをもとにしてサービスを行った後、ホスト302に対して応答パケットを送信する。この、応答パケット中継時には、第2のVRFネットワークが使用される(図53:エン트리E42)。

#### 【0214】

以上のように、運用サーバ201および予備サーバ202の障害検出前においては、これら2台のサーバにより分散して処理が行われる。すなわち、運用サーバ201と、予備サーバ202の両方が運用系サーバとして機能している。

10

#### 【0215】

(D-3)第4実施例における状態監視処理:

第4実施例における状態監視処理は、図14で説明した第1実施例と同じ手順により行う。

#### 【0216】

(D-4)第4実施例におけるフェイルオーバー処理:

図60は、第4実施例におけるフェイルオーバー処理(図14:ステップS508)の手順を示すフローチャートである。フェイルオーバー処理部160は、状態監視処理で障害を検出した監視IDと、図58で説明したロードバランス切替データベース182とを使用し、図60のフローチャートに従って、障害検出に伴うフェイルオーバー処理を行う。

20

#### 【0217】

まず、ステップS801においてフェイルオーバー処理部160は、VRFロードバランスデータベースのVRF番号からロードバランス対象外VRFを除外する。具体的には、フェイルオーバー処理部160は、ロードバランス切替データベース182(図58)のうち、監視IDフィールドの値が、状態監視処理において障害が検出された監視IDと同じエントリを検索する。そして、検索されたエントリについての、切替対象インタフェースフィールドと、ロードバランス対象外VRFフィールドと、切替後状態フィールドの値を読み出す。次に、フェイルオーバー処理部160は、VRFロードバランスデータベース141のインタフェース番号フィールドを、読み出された切替対象インタフェースフィールドの値をキーとして検索する。そして、該当するエントリについてのVRF番号フィールドの値から、読み出されたロードバランス対象外VRFフィールドを除外する。

30

#### 【0218】

ステップS802においてフェイルオーバー処理部160は、全ての切替対象について処理を行ったか否かを判定する。具体的には、ステップS801において検索されたエントリ(ロードバランス切替データベース182のうち、監視IDフィールドの値が状態監視処理において障害が検出された監視IDと同じエントリ)の切替対象インタフェースの全てについて、上述のステップの処理を行ったか否かを判定する。全ての切替対象について処理を行った場合、処理を終了する。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー処理部160は、ステップS801へ戻り、処理を継続する。

40

#### 【0219】

図61は、図60のステップS801において更新された後のVRFロードバランスデータベース141を示す説明図である。障害検出前のVRFロードバランスデータベース141を示す図54との違いは、インタフェース番号フィールドの値が「133」、「134」のエントリ(エン트리E41、E42)のVRF番号フィールドの値から「1」が除外され、「2」のみとなっている点である。

#### 【0220】

図62は、運用サーバ201に障害が検出された場合におけるネットワークシステム10bの動作を示す説明図である。ホスト301からの要求パケットを受信したネットワー

50

ク装置 100b は、図 55 に示したパケット転送処理に従ってパケットの出力先を決定する。具体的には、パケット転送処理部 150 は、図 53 に示すインタフェースデータベース 140 のインタフェースの識別子 133 に一致するエントリ E43 の VRF 番号フィールドの値「LB」を取得する（ステップ S12）。VRF 番号が「LB」であるため、パケット転送処理部 150 は図 61 に示した VRF ロードバランスデータベース 141 を検索する（ステップ S21、S22）。

#### 【0221】

次に、パケット転送処理部 150 は、送信元 IP アドレス「20.1.1.1」を元にして、VRF 番号を決定する（ステップ S23）。なお、このとき、図 61 に示した VRF ロードバランスデータベース 141 の、VRF 番号フィールドの値（すなわち、ロード  
10  
バランス処理の対象となる VRF ネットワークの識別子）は「2」のみしかないので、パケット転送処理部 150 は、送信元 IP アドレスによらず VRF 番号「2」を選択する。その後、パケット転送処理部 150 は、VRF ルーティングテーブル 122 を検索し、出力インタフェースフィールドの値「132」を取得する（ステップ S13）。パケット転送処理部 150 ステップ S13 で求めた出力インタフェース 132 からパケットを出力する（ステップ S14）。

#### 【0222】

予備サーバ 202 は、ホスト 301 から受信したパケットをもとにしてサービスを行った後、ホスト 301 に対して応答パケットを送信する。この、応答パケット中継時には、  
20  
第 2 の VRF ネットワークが使用される（図 53：エントリ E42）。

#### 【0223】

一方、ホスト 302 からの要求パケットを受信したネットワーク装置 100b の動作は、図 59 で説明したものと同様である。

#### 【0224】

以上のように、運用サーバ 201 の障害検出後においては、障害が検出されたサーバ以外のサーバ（上述の例では、予備サーバ 202）によって処理が行われる。すなわち、障害が検出されたサーバ以外のサーバが運用系サーバとして機能する。なお、例えば、3 台のサーバ（第 1～第 3 のサーバ）によってロードバランス処理を行っていた場合は、第 1 のサーバの障害検出後は、第 2 のサーバと、第 3 のサーバとの 2 台で分散して処理を行う  
30

#### 【0225】

（D-5）第 4 実施例における復旧検出時処理：

図 63 は、第 4 実施例における復旧検出時処理（図 14：ステップ S506）の手順を示すフローチャートである。フェイルオーバ処理部 160 は、状態監視処理で復旧を検出した監視 ID と、図 58 で説明したロードバランス切替データベース 182 とを使用し、図 63 のフローチャートに従って、復旧検出に伴う復旧検出時処理を行う。

#### 【0226】

まず、ステップ S851 においてフェイルオーバ処理部 160 は、切替後動作がロックか否かを判定する。具体的には、フェイルオーバ処理部 160 は、図 58 に示したロード  
40  
バランス切替データベース 182 のうち、監視 ID フィールドの値が、状態監視処理において復旧を検出した監視 ID と同じエントリを検索する。そして、検索されたエントリについての、切替対象インタフェースフィールドと、ロードバランス対象外 VRF フィールドと、切替後状態フィールドの値を読み出す。読み出された切替後状態フィールドの値が「ロック」である場合、フェイルオーバ処理部 160 は、ステップ S853 へ遷移する。

#### 【0227】

一方、読み出された切替後状態フィールドの値が「ロック」で無い場合、フェイルオーバ処理部 160 は、ステップ S852 において、VRF ロードバランスデータベースの VRF 番号にロードバランス対象外 VRF を追加する。具体的には、フェイルオーバ処理部 160 は、図 61 に示した VRF ロードバランスデータベース 141 のインタフェース番号フィールドを、読み出された切替対象インタフェースフィールドの値をキーとして検索  
50

する。そして、該当するエントリについてのVRF番号フィールドに、読み出された切替対象インタフェースフィールドの値を追加する。

【0228】

ステップS853においてフェイルオーバー処理部160は、全ての切替対象の処理を行ったかを判定する。具体的には、ステップS851において検索されたエントリ（ロードバランス切替データベース182のうち、監視IDフィールドの値が状態監視処理において復旧を検出した監視IDと同じエントリ）の切替対象インタフェースの全てについて、ステップS852、S852の処理を行ったか否かを判定する。全ての切替対象について処理を行った場合、フェイルオーバー処理部160は、処理を終了する。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー処理部160は、ステップS851へ戻って処理を継続する。

10

【0229】

図64は、運用サーバ201の復旧が検出された場合における、ステップS852（図63）で更新された後のVRFロードバランスデータベース141を示す説明図である。復旧検出前のVRFロードバランスデータベース141を示す図61との違いは、インタフェース番号フィールドの値が「134」のエントリ（エントリE42）のVRF番号フィールドの値に「1」が追加されている点である。

【0230】

前述の通り、VRFロードバランスデータベース141のVRF番号フィールドには、ロードバランス処理の対象となるVRFネットワークの識別子が格納される。すなわち、復旧検出時処理終了後のVRFロードバランスデータベース141（図64）の下では、インタフェース133から入力されたパケットは第2のVRFネットワークの下で処理され、インタフェース134から入力されたパケットは第1または第2のVRFネットワークの下で処理される。これは、図58に示したロードバランス切替データベース182に従って、インタフェース133についてはロック動作が、インタフェース134についてはリカバリ動作が行われたことを示している。

20

【0231】

図65は、コマンドの一例を示す説明図である。このような運用コマンドを実行することにより、VRFロードバランスデータベース141のインタフェース133に関する情報を初期化（図54に示した状態）することができる。このため、ネットワークシステム10bを、運用サーバ201に障害が発生する前の状態へ復元することが可能となる。

30

【0232】

このように、第4実施例では、パケット転送処理部150は、クライアント装置（ホスト301、ホスト302）からパケットを受信した際に、予め定められた規則に従ってパケットの送信元である装置毎（ホスト301、ホスト302）に、第1の仮想ネットワークの経路情報であるVRF1ルーティングテーブル121および第2の仮想ネットワークの経路情報であるVRF2ルーティングテーブル122のいずれか一方を用いて経路探索を行う。このため、2台の処理装置（運用サーバ201、予備サーバ202）の両方を、サービスの提供に使用することができる。従って、設備投資の観点から、効率の良いネットワークシステムを提供することができる。

40

【0233】

さらに、状態監視部としてのフェイルオーバー処理部160は、第1の仮想ネットワーク（VRF1）に所属する第1の処理装置（運用サーバ201）と、第2の仮想ネットワーク（VRF2）に所属する第2の処理装置（予備サーバ202）の両方の状態を監視する。そして、フェイルオーバー処理部160は、監視対象であるいずれか一方の処理装置が障害状態であると判定された場合に、第1の仮想ネットワークおよび第2の仮想ネットワークの両方に所属していたクライアント装置（ホスト301、ホスト302）を、障害状態であると判定された一方の処理装置が所属する仮想ネットワークから除外するように、VRF定義情報であるVRFロードバランスデータベース141を更新する。このため、適用例1と同様の効果を得ることができる。

50

## 【0234】

E. 第5実施例：

本発明の第5実施例では、サービスを提供するサーバの運用状態を監視する管理用のサーバを備える構成を説明する。

## 【0235】

(E-1) 第5実施例におけるシステム構成：

図66は、第5実施例におけるネットワークシステム10cの概略構成を示す説明図である。図1で示した第1実施例との違いは、管理装置としての管理サーバ250を備える点と、ネットワーク装置100cが、インタフェース135を備え、状態監視データベース170と、障害切替データベース180と、復旧切替データベース190とを備えない点であり、他の構成については第1実施例と同様である。なお、以下では、第1実施例と異なる構成および効果を有する部分についてのみ説明する。

10

## 【0236】

管理サーバ250は、インタフェース135を介してネットワーク装置100cと接続されている外部装置である。管理サーバ250は、運用サーバ201および予備サーバ202の状態監視を行い、ネットワーク装置100cにフェイルオーバー処理を指示する機能を有する。

## 【0237】

管理サーバ250は、フェイルオーバー管理部251と、状態監視データベース254と、障害切替データベース253と、復旧切替データベース252とを備えている。フェイルオーバー管理部251についての詳細は後述する。状態監視データベース254の構成は、状態監視データベース170(図9)と同様である。障害切替データベース253の構成は、障害切替データベース180(図10)と同様である。復旧切替データベース252の構成は、復旧切替データベース190(図11)と同様である。

20

## 【0238】

本実施例におけるネットワーク装置100cのフェイルオーバー処理部160は、管理サーバ250からの指示を受け付け、フェイルオーバー処理を実行する処理部である。なお、管理サーバ250に設定されるIPアドレス、サブネットマスク長、デフォルトゲートウェイは、以後の説明には不要であるため説明を省略する。

## 【0239】

図67は、第5実施例におけるネットワーク装置100cの構成情報を規定するコンフィギュレーション情報の一例を示す説明図である。図5に示した第1実施例との違いは、行C11、C15が削除されている点と、行C501~C503が追加されている点であり、他の構成については第1実施例と同様である。

30

## 【0240】

行C501は、インタフェース135を定義している。インタフェースの種類はイーサネット(登録商標)である。行C502は、インタフェース135のIPアドレスと、サブネットマスク長とを定義している。行C503は、フェイルオーバーを指示するサーバが管理サーバ250であることを定義している。この行C503の定義は省略可能である。しかし、意図しない外部装置からのフェイルオーバー指示に基づいてネットワーク装置100cが動作することを抑制するためには、行C503の定義を省略しない方が好ましい。

40

## 【0241】

なお、インタフェース131~134とは異なり、インタフェース135には所属するVRFネットワークの定義がされていない。これは、インタフェース135はどのVRFネットワークにも所属しないインタフェースであることを意味している。

## 【0242】

図68は、第5実施例におけるインタフェースデータベース140の一例を示す説明図である。図6に示した第1実施例との違いは、エントリE55が追加されている点のみである。エントリE55は、図67で説明したコンフィギュレーション情報の行C501、C502で定義された情報が格納される。

50

## 【 0 2 4 3 】

( E - 2 ) 第 5 実施例における状態監視処理 :

図 6 9 は、第 5 実施例における状態監視処理の手順を示すフローチャートである。管理サーバ 2 5 0 のフェイルオーバ管理部 2 5 1 は、状態監視データベース 2 5 4 を使用し、図 6 9 のフローチャートに従ってサーバ ( 運用サーバ 2 0 1、予備サーバ 2 0 2 ) の運用状態を監視する。まず、ステップ S 9 0 1 においてフェイルオーバ管理部 2 5 1 は、状態監視データベース 2 5 4 に基づいて、サーバの監視を行う。この監視における障害 ( または復旧 ) 有無の判断は、例えば、定期的に監視対象となるサーバに対してパケットを送信し、当該パケットに対する応答パケットの有無により行うことができる。また、他の方法 ( 例えば、ネットワーク装置 1 0 0 c が障害および復旧の監視を行い、その結果を管理サーバ 2 5 0 へ定期的に送信するような方法 ) を採用することもできる。

10

## 【 0 2 4 4 】

ステップ S 9 0 2 においてフェイルオーバ管理部 2 5 1 は、状態監視の結果を判定する。監視対象の障害が検出された場合、ステップ S 9 0 3 においてフェイルオーバ管理部 2 5 1 は、状態監視データベース 2 5 4 の該当するエントリを「通信不可」へと更新する ( 詳細は、図 1 4 のステップ S 5 0 7 と同様 )。その後、ステップ S 9 0 4 においてフェイルオーバ管理部 2 5 1 は、フェイルオーバ処理 ( 詳細は後述 ) を行う。

## 【 0 2 4 5 】

一方、ステップ S 9 0 2 において監視対象の復旧が検出された場合、ステップ S 9 0 5 においてフェイルオーバ管理部 2 5 1 は、状態監視データベース 2 5 4 の該当するエントリを「通信可」へと更新する ( 詳細は、図 1 4 のステップ S 5 0 5 と同様 )。その後、ステップ S 9 0 6 においてフェイルオーバ管理部 2 5 1 は、復旧検出時処理 ( 詳細は後述 ) を行う。

20

## 【 0 2 4 6 】

( E - 3 ) 第 5 実施例におけるフェイルオーバ処理 :

図 7 0 は、フェイルオーバ処理 ( 図 6 9 : ステップ S 9 0 4 ) の手順を示すフローチャートである。本フローチャートの左欄には、管理サーバ 2 5 0 のフェイルオーバ管理部 2 5 1 が行う処理を記載している。また、右欄にネットワーク装置 1 0 0 c のフェイルオーバ処理部 1 6 0 が行う処理を記載している。また、このことは後述する図 7 1 についても同様である。

30

## 【 0 2 4 7 】

まず、ステップ S 9 1 1 においてフェイルオーバ管理部 2 5 1 は、V R F 番号の切替指示を行う。具体的には、障害切替データベース 2 5 3 のうち、監視 I D フィールドの値が、状態監視処理において障害が検出された監視 I D と同じエントリを検索する。そして、検索されたエントリについての、切替対象インタフェースフィールドと、切替先 V R F フィールドと、切替後動作フィールドの値を読み出す。そして、読み出された値をもとにインタフェースデータベース 1 4 0 の更新を行うための指示を、ネットワーク装置 1 0 0 c のフェイルオーバ処理部 1 6 0 に対して送信する。

## 【 0 2 4 8 】

これを受信したフェイルオーバ処理部 1 6 0 は、ステップ S 9 1 2 において、示された内容に基づくインタフェースデータベース 1 4 0 の書換えを行う。その後のルーティングテーブルの書換え ( ステップ S 6 0 2 ) についても、第 1 実施例と同様である。

40

## 【 0 2 4 9 】

ステップ S 9 1 3 においてフェイルオーバ管理部 2 5 1 は、切替後動作がロックか否かを判定する。この判定は、ステップ S 9 1 1 で読み出された切替後動作フィールドの値を元に行う。切替後動作フィールドの値が「ロック」である場合、ステップ S 9 1 5 へ遷移する。一方、切替後動作フィールドの値が「ロック」で無い場合は、フェイルオーバ管理部 2 5 1 は、復旧切替データベース 2 5 2 へ監視対象となるエントリの情報を登録する ( ステップ S 9 1 4 )。ステップ S 9 1 5 においてフェイルオーバ管理部 2 5 1 は、全ての切替対象について処理を行ったか否かを判定する。全ての切替対象について処理を行った

50

場合、処理を終了する。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー管理部 251 は、ステップ S 9 1 1 へ戻り、処理を継続する。

【 0 2 5 0 】

( E - 4 ) 第 5 実施例における復旧検出時処理 :

図 7 1 は、復旧検出時処理 ( 図 6 9 : ステップ S 9 0 6 ) の手順を示すフローチャートである。まず、ステップ S 9 2 1 においてフェイルオーバー管理部 251 は、V R F 番号の切替指示を行う。具体的には、復旧切替データベース 252 のうち、監視 I D フィールドの値が、状態監視処理において復旧を検出した監視 I D と同じエントリを検索する。そして、検索されたエントリについての、切替対象インタフェースフィールドと、切替先 V R F フィールドの値を読み出す。そして、読み出された値をもとにインタフェースデータベ

10

【 0 2 5 1 】

これを受信したフェイルオーバー処理部 160 は、ステップ S 9 2 2 において、示された内容に基づくインタフェースデータベース 140 の書換えを行う。その後のルーティングテーブルの書換え ( ステップ S 6 5 2 ) についても、第 1 実施例と同様である。ステップ S 9 2 3 においてフェイルオーバー管理部 251 は、復旧切替データベース 252 から、ステップ S 9 2 1 ~ S 6 5 2 において処理を行った切替対象インタフェースを削除する。

【 0 2 5 2 】

ステップ S 9 2 4 においてフェイルオーバー管理部 251 は、全ての切替対象の処理を行ったかを判定する。全ての切替対象について処理を行った場合、フェイルオーバー管理部 251 は、復旧切替データベース 252 から、状態監視処理において復旧を検出した監視 I D そのものを削除し、処理を終了する。一方、全ての切替対象について処理を行っていない場合、フェイルオーバー管理部 251 は、ステップ S 9 2 1 へ戻り、処理を継続する。

20

【 0 2 5 3 】

本実施例では、管理サーバ 250 のフェイルオーバー管理部 251 が、第 1 実施例のフェイルオーバー処理部 160 が実施していた機能の一部を実施している。その他の点 ( 例えば、フェイルオーバー処理や、復旧検出時処理の実体的な処理内容 ) については、第 1 実施例と同様である。

【 0 2 5 4 】

このように、第 5 実施例では、管理装置 ( 管理サーバ 250 ) のフェイルオーバー管理部 251 は、ネットワーク装置 100 c のフェイルオーバー処理部 160 に対して、経路情報および V R F 定義情報の少なくともいずれか一方を更新するためのフェイルオーバー指示を送信する。このため、ネットワーク中継装置の管理装置が予め外部に設けられているような構成においても、適用例 1 と同様の効果を得ることができる。

30

【 0 2 5 5 】

また、管理サーバ 250 は、ネットワーク装置 100 c よりも高度な処理能力を有する場合が多い。従って、例えば、状態監視処理において、障害状態であるか否かの判定以外のより高度な判定 ( 例えば、処理装置の C P U 利用率等 ) を行うこともできる。

【 0 2 5 6 】

F . 変形例 :

なお、この発明は上記の実施例や実施形態に限られるものではなく、その要旨を逸脱しない範囲において種々の態様において実施することが可能であり、例えば次のような変形も可能である。

40

【 0 2 5 7 】

F 1 . 変形例 1 :

上記実施例では、説明を簡単にするため、2つの V R F を使用する構成について説明した。しかし、ネットワーク装置が備える V R F の個数は任意に定めることができる。また、ネットワーク装置は、V R F 属性を持たないグローバルネットワークを含むものとしても良い。この場合、当該グローバルネットワークは、V R F 属性を持たない一種の V R F

50

として考えることも可能である。

【0258】

F2．変形例2：

上記実施例では、ネットワークシステム構成の一例を示した。しかし、ネットワークシステム構成は、上述した態様に限らず、本発明の要旨を逸脱しない範囲において任意に定めることができる。具体的には、例えば、ネットワークシステムを構成するサーバやホストの台数は任意に決定することができる。また、サーバやホストは、ネットワーク装置と他のネットワーク装置を介して間接的に接続されるものとしても良い。

【0259】

F3．変形例3：

上記実施例では、ネットワーク装置の構成の一例を示した。しかし、ネットワーク装置の構成は、上述した態様に限らず、本発明の要旨を逸脱しない範囲において任意に定めることができる。具体的には、例えば、ネットワーク装置が有するインタフェースを、VLAN (Virtual Local Area Network) で多重化する論理的なインタフェースであるものとするすることができる。また、リンクアグリゲーションや、トンネルインタフェースや、MPLS (Multi-Protocol Label Switching) のLSP (Label Switched Path) といった仮想的なインタフェースを用いても良い。

【0260】

F4．変形例4：

上記実施例では、ネットワーク装置が備える各テーブルについて、その構成の一例を示した。しかし、これらのテーブルが備えるフィールドは、その発明の要旨を逸脱しない範囲において任意に定めることができる。例えば、上記に例示したフィールド以外のフィールドを備えるものとしても良い。また、各テーブルには、ダイレクトマップ方式を用いることも可能である。

【0261】

F5．変形例5：

上記実施例では、状態監視処理における監視対象は、サービスを提供している運用サーバであるものとした。しかし、状態監視処理における監視対象は、任意に定めることができる。例えば、直接サービスを行わないサーバ装置を監視対象とすることもできる。具体的には、サービスを提供するために必要なデータベースサーバや、記憶装置を監視対象としてもよい。このようにすれば、監視対象の装置を、ネットワークシステムの構成によって柔軟に設定することが可能となる。

【0262】

F6．変形例6：

上記実施例では、状態監視処理の一例を示した。しかし、状態監視処理は、上記実施例において例示した方法に限らず、任意の方法を採用することができる。例えば、ネットワーク装置とサーバとの間にTCP (Transmission Control Protocol) セッションを確立させておき、前記TCPセッションの切断をもって障害の検出としてもよく、TCPセッションが未確立な状態から、確立した状態になったことをもって、障害からの復旧を検出したとしてもよい。また、サーバの状態を検出するためのセッションは、TCPセッションに限定する必要もなく、BFDセッションなどのその他のセッションを利用してもよい。また、ネットワーク装置は、サーバが提供しているサービスにアクセスすることでサーバの運用状態を監視してもよい。

【0263】

F7．変形例7：

上記第5実施例では、管理サーバのフェイルオーバー管理部が、第1実施例のフェイルオーバー処理部が実施していた機能の一部を担うものとして記載した。しかし、このような構成は、第1実施例に限られない。例えば、ネットワーク装置の外部に設けられた管理サーバが、第2～第5実施例で説明したフェイルオーバー処理部の機能の一部を実施するものと

10

20

30

40

50

して構成することもできる。例えば、管理サーバ250が、第4実施例で説明したロードバランス処理を行う構成とすれば、さらに高度なロードバランス（例えば、サーバのCPU利用率に応じたロードバランス）を実現することが可能である。

【0264】

F8．変形例8：

上記第2～5実施例は、上記第1実施例からの構成変更であるものとして記載した。しかし、上記第2～5実施例は、第1実施例以外の実施例からの構成変更として適用することも可能である。またこれら上記第1～5実施例を組み合わせることも適用することもできる。

【符号の説明】

【0265】

10、10a～c…ネットワークシステム

50…状態監視ルール

51…状態監視ルール

100、100a～c…ネットワーク装置

110…コンフィギュレーションデータベース

121…VRF1ルーティングテーブル

122…VRF2ルーティングテーブル

131…インタフェース

132…インタフェース

133…インタフェース

134…インタフェース

135…インタフェース

140…インタフェースデータベース

141…VRFロードバランスデータベース

150…パケット転送処理部

160…フェイルオーバ処理部

170…状態監視データベース

180…障害切替データベース

181…障害切替経路データベース

182…ロードバランス切替データベース

190…復旧切替データベース

201…運用サーバ

202…予備サーバ

211…運用サーバ

212…予備サーバ

221…運用サーバ

222…予備サーバ

250…管理サーバ

251…フェイルオーバ管理部

252…復旧切替データベース

253…障害切替データベース

254…状態監視データベース

301…ホスト

302…ホスト

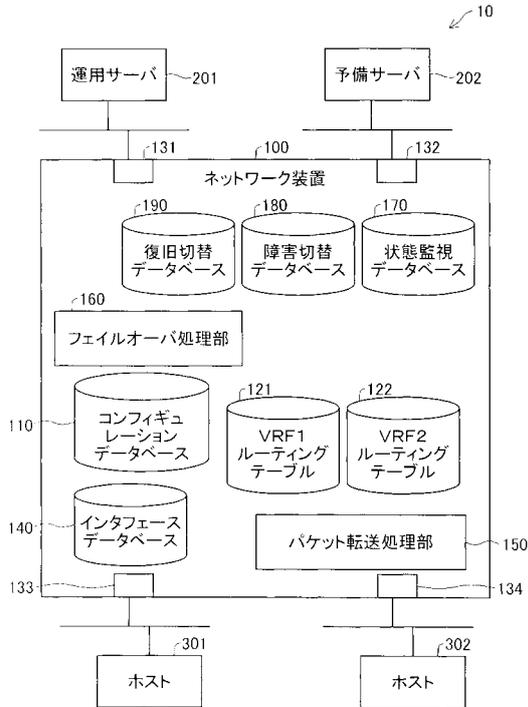
10

20

30

40

【図1】



【図2】

IPアドレス	サブネットマスク長	デフォルトゲートウェイ
10.1.1.1	24	10.1.1.254

【図6】

インタフェース番号	VRF番号	IPアドレス	サブネットマスク長
E1	1	10.1.1.254	24
E2	2	10.1.1.254	24
E3	1	20.1.1.254	24
E4	1	30.1.1.254	24

【図7】

あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E1	32	10.1.1.1	131
E2	32	-	-
E3	32	20.1.1.1	133
E4	32	-	-
E5	32	30.1.1.1	134
E6	32	-	-

【図3】

IPアドレス	サブネットマスク長	デフォルトゲートウェイ
20.1.1.1	24	20.1.1.254

【図4】

IPアドレス	サブネットマスク長	デフォルトゲートウェイ
30.1.1.1	24	30.1.1.254

【図5】

- C1: vrf definition 1
- C2: vrf definition 2
- C3: interface ethernet 131
- C4: vrf forwarding 1
- C5: ip address 10.1.1.254/24
- C6: interface ethernet 132
- C7: vrf forwarding 2
- C8: ip address 10.1.1.254/24
- C9: interface ethernet 133
- C10: vrf forwarding 1
- C11: vrf forwarding 2 redundant track 50 lock
- C12: ip address 20.1.1.254/24
- C13: interface ethernet 134
- C14: vrf forwarding 1
- C15: vrf forwarding 2 redundant track 50 recovery
- C16: ip address 30.1.1.254/24
- C17: track 50 ip route 10.1.1.1 vrf 1 reachability

【図8】

あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E1	32	10.1.1.1	132
E2	32	-	-

【図9】

監視ID	監視先IPアドレス	監視先VRF	監視状態
E1	10.1.1.1	1	通信可

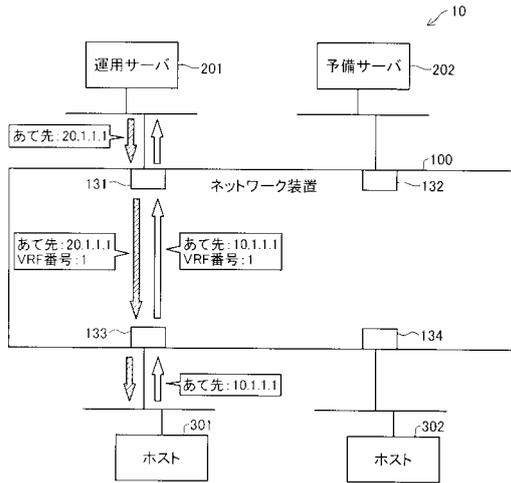
【図10】

監視ID	切替対象インタフェース	切替先VRF	切替後動作
E1	133	2	ロック
E2	134	2	リカバリー

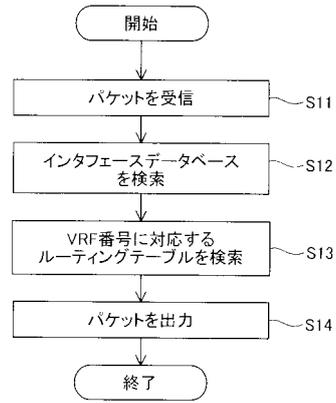
【図11】

監視ID	切替対象インタフェース	切替先VRF
50	134	1

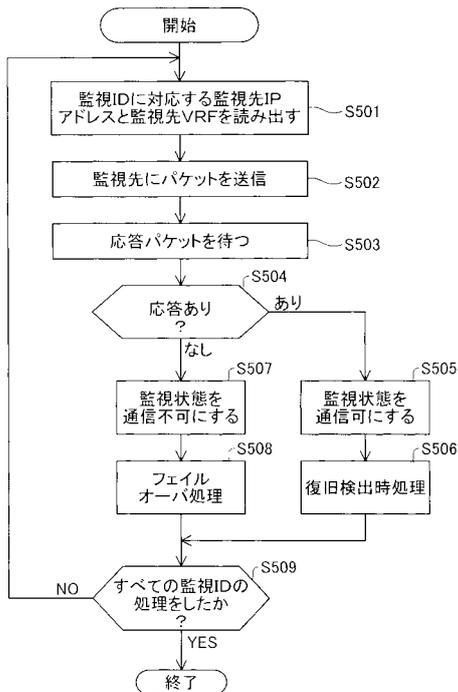
【図12】



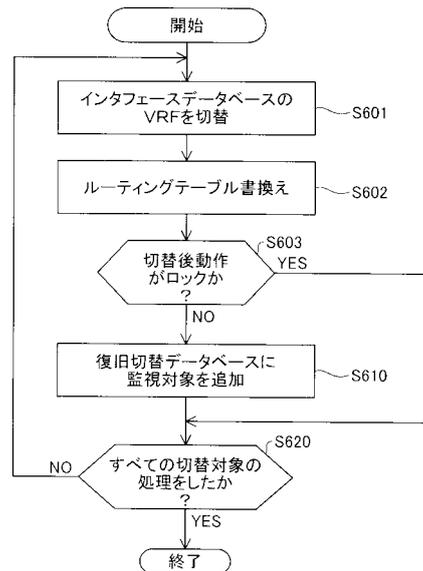
【図13】



【図14】



【図16】



【図15】

170

監視ID	監視先IPアドレス	監視先VRF	監視状態
50	10.1.1.1	1	通信不可

E1

【図17】

	インタフェース番号	VRF番号	IPアドレス	サブネットマスク長
E1	131	1	10.1.1.254	24
E2	132	2	10.1.1.254	24
E3	133	2	20.1.1.254	24
E4	134	2	30.1.1.254	24

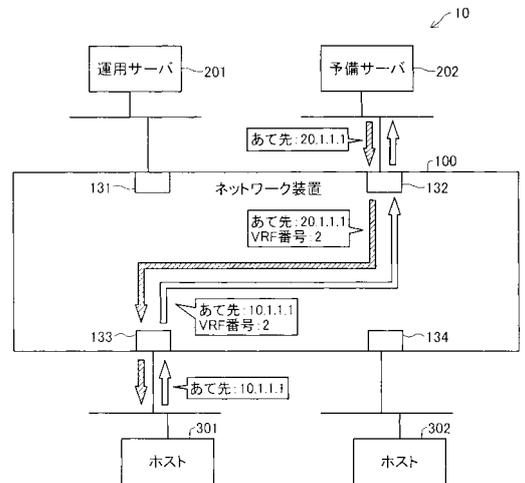
【図18】

あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
10.1.1.1	32	10.1.1.1	131
10.1.1.254	32	-	-

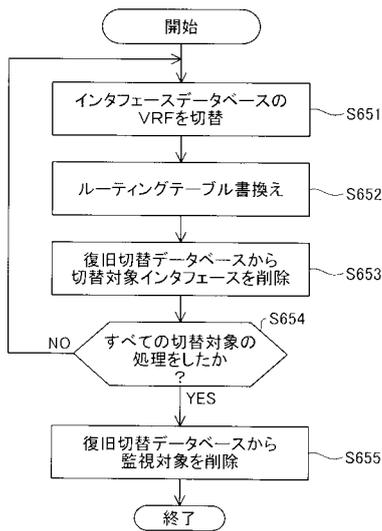
【図19】

	あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E1	10.1.1.1	32	10.1.1.1	132
E2	10.1.1.254	32	-	-
E3	20.1.1.1	32	20.1.1.1	133
E4	20.1.1.254	32	-	-
E5	30.1.1.1	32	30.1.1.1	134
E6	30.1.1.254	32	-	-

【図20】



【図21】



【図22】

	インタフェース番号	VRF番号	IPアドレス	サブネットマスク長
E1	131	1	10.1.1.254	24
E2	132	2	10.1.1.254	24
E3	133	2	20.1.1.254	24
E4	134	1	30.1.1.254	24

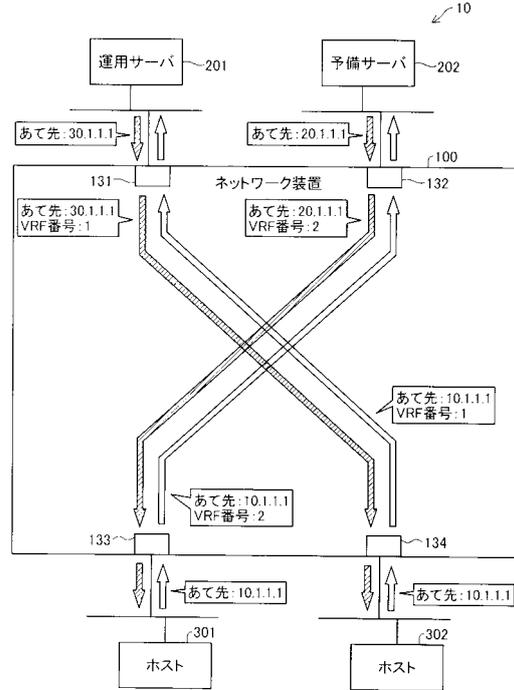
【図23】

	あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E1	10.1.1.1	32	10.1.1.1	131
E2	10.1.1.254	32	-	-
E3	30.1.1.1	32	30.1.1.1	134
E4	30.1.1.254	32	-	-

【図24】

	あて先 IPアドレス	サブ ネット マスク長	ネクストホップ IPアドレス	出カインタ フェース
E1	10.1.1.1	32	10.1.1.1	132
E2	10.1.1.254	32	-	-
E3	20.1.1.1	32	20.1.1.1	133
E4	20.1.1.254	32	-	-

【図25】



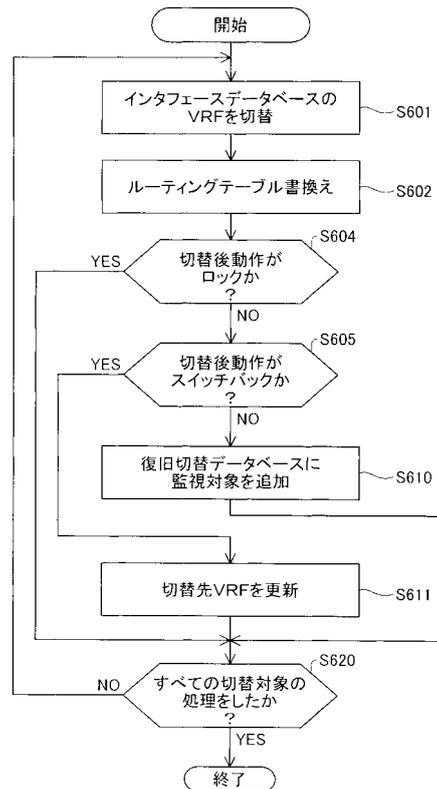
【図26】

Router# redundancy force-switchover interface 133 vrf 1

【図27】

- C1: vrf definition 1
- C2: vrf definition 2
- C3: interface ethernet 131
- C4: vrf forwarding 1
- C201: vrf forwarding 2 redundant track 50 switch-back
- C5: ip address 10.1.1.254/24
- C6: interface ethernet 132
- C202: vrf forwarding 1 redundant track 50 switch-back
- C7: vrf forwarding 2
- C8: ip address 10.1.1.254/24
- C9: interface ethernet 133
- C10: vrf forwarding 1
- C12: ip address 20.1.1.254/24
- C13: interface ethernet 134
- C14: vrf forwarding 1
- C16: ip address 30.1.1.254/24
- C203: track 50 ip route 10.1.1.1 vrf 1 reachability

【図29】



【図28】

	監視ID	切替対象インタフェース	切替先VRF	切替後動作
E21	50	131	2	スイッチバック
E22	50	132	1	スイッチバック

【図30】

	インタフェース番号	VRF番号	IPアドレス	サブネットマスク長
E21	131	2	10.1.1.254	24
E22	132	1	10.1.1.254	24
E23	133	1	20.1.1.254	24
E24	134	1	30.1.1.254	24

【図31】

	あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E21	10.1.1.1	32	10.1.1.1	132
E22	10.1.1.254	32	-	-
E23	20.1.1.1	32	20.1.1.1	133
E24	20.1.1.254	32	-	-
E25	30.1.1.1	32	30.1.1.1	134
E26	30.1.1.254	32	-	-

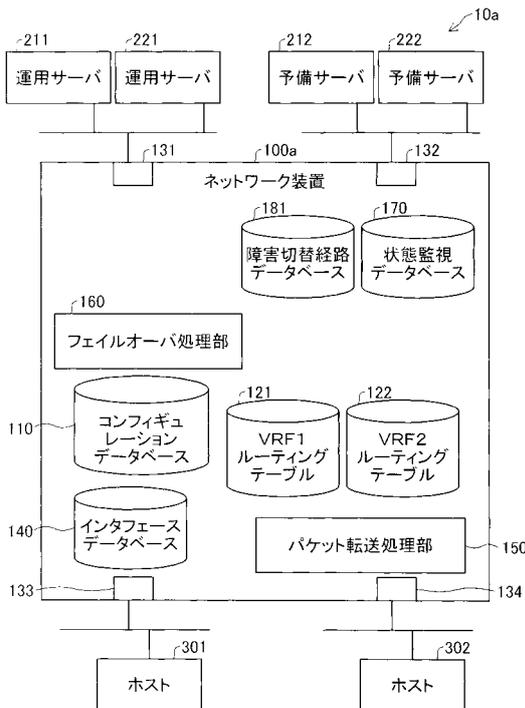
【図32】

	あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E21	10.1.1.1	32	10.1.1.1	131
E22	10.1.1.254	32	-	-

【図33】

	監視ID	切替対象インタフェース	切替先VRF	切替後動作
E21	50	131	1	スイッチバック
E22	50	132	2	スイッチバック

【図34】



【図35】

IPアドレス	サブネットマスク長	デフォルトゲートウェイ
10.1.1.2	24	10.1.1.254

【図36】

- C1: vrf definition 1
- C2: vrf definition 2
- C3: interface ethernet 131
- C4: vrf forwarding 1
- C5: ip address 10.1.1.254/24
- C6: interface ethernet 132
- C7: vrf forwarding 2
- C8: ip address 10.1.1.254/24
- C9: interface ethernet 133
- C10: vrf forwarding 1
- C12: ip address 20.1.1.254/24
- C13: interface ethernet 134
- C14: vrf forwarding 1
- C16: ip address 30.1.1.254/24
- C17: track 50 ip route 10.1.1.1 vrf 1 reachability
- C301: track 51 ip route 10.1.1.2 vrf 1 reachability
- C302: ip route 10.1.1.1 vrf 1 redundant track 50 out-interface 132
- C303: ip route 10.1.1.2 vrf 1 redundant track 51 out-interface 132

【図37】

	あて先IPアドレス	サブネットマスク長	ネクストホップIPアドレス	出力インタフェース
E31	10.1.1.1	32	10.1.1.1	131
E32	10.1.1.2	32	10.1.1.2	131
E33	10.1.1.254	32	-	-
E34	20.1.1.1	32	20.1.1.1	133
E35	20.1.1.254	32	-	-
E36	30.1.1.1	32	30.1.1.1	134
E37	30.1.1.254	32	-	-

【図38】

122

	あて先 IPアドレス	サブ ネット マスク長	ネクストホップ IPアドレス	出力 インタフェース
E31	10.1.1.1	32	10.1.1.1	132
E32	10.1.1.2	32	10.1.1.2	132
E33	10.1.1.254	32	-	-

【図39】

170

	監視ID	監視先 IPアドレス	監視先VRF	監視状態
E31	50	10.1.1.1	1	通信可
E32	51	10.1.1.2	1	通信可

【図40】

181

	監視ID	切替対象 VRF	切替対象 経路	切替先出力 インタフェース
E31	50	1	10.1.1.1	132
E32	51	1	10.1.1.2	132

【図41】

170

	監視ID	監視先 IPアドレス	監視先VRF	監視状態
E31	50	10.1.1.1	1	通信不可
E32	51	10.1.1.2	1	通信可

【図43】

121

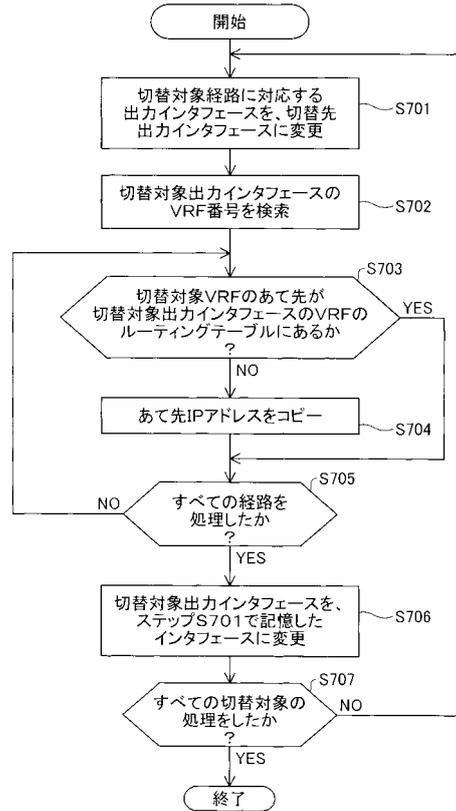
	あて先 IPアドレス	サブ ネット マスク長	ネクストホップ IPアドレス	出力 インタフェース
E31	10.1.1.1	32	10.1.1.1	132
E32	10.1.1.2	32	10.1.1.2	131
E33	10.1.1.254	32	-	-
E34	20.1.1.1	32	20.1.1.1	133
E35	20.1.1.254	32	-	-
E36	30.1.1.1	32	30.1.1.1	134
E37	30.1.1.254	32	-	-

【図44】

122

	あて先 IPアドレス	サブ ネット マスク長	ネクストホップ IPアドレス	出力 インタフェース
E31	10.1.1.1	32	10.1.1.1	132
E32	10.1.1.2	32	10.1.1.2	132
E33	10.1.1.254	32	-	-
E34	20.1.1.1	32	20.1.1.1	133
E35	20.1.1.254	32	-	-
E36	30.1.1.1	32	30.1.1.1	134
E37	30.1.1.254	32	-	-

【図42】

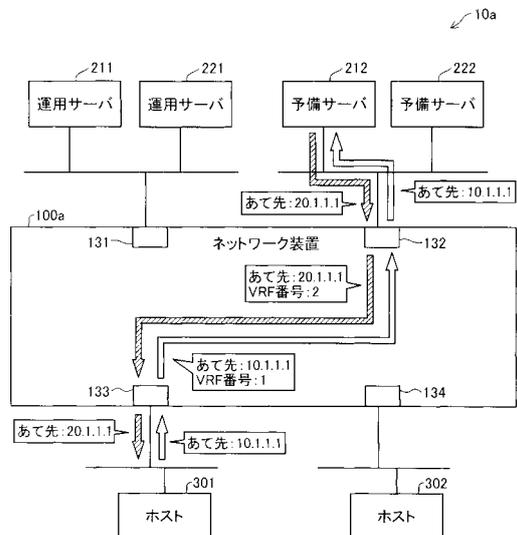


【図45】

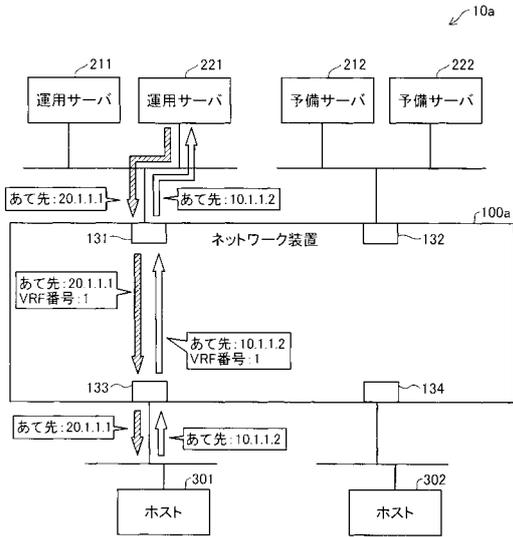
181

	監視ID	切替対象 VRF	切替対象 経路	切替先出力 インタフェース
E31	50	1	10.1.1.1	131
E32	51	1	10.1.1.2	132

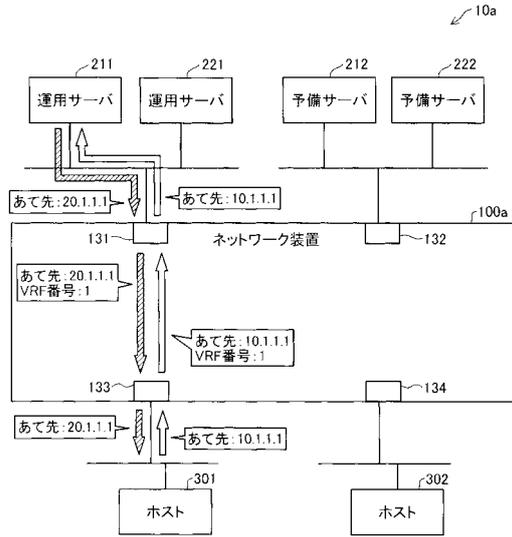
【図46】



【図 47】



【図 48】



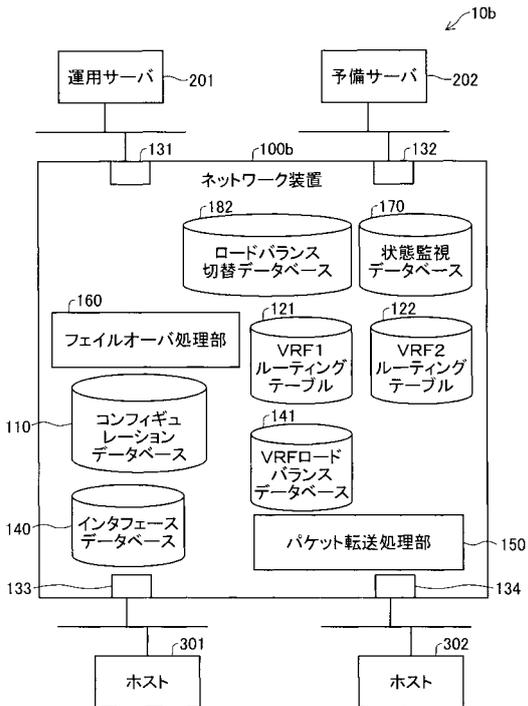
【図 49】

Router# clear ip route vrf 2

【図 50】

Router# clear ip route vrf 1 10.1.1.1

【図 51】



【図 52】

- C1: vrf definition 1
- C2: vrf definition 2
- C3: interface ethernet 131
- C4: vrf forwarding 1
- C5: ip address 10.1.1.254/24
- C6: interface ethernet 132
- C7: vrf forwarding 2
- C8: ip address 10.1.1.254/24
- C9: interface ethernet 133
- C401: vrf forwarding 1 load-balance track 50 lock
- C402: vrf forwarding 2 load-balance
- C12: ip address 20.1.1.254/24
- C13: interface ethernet 134
- C403: vrf forwarding 1 load-balance track 50 recovery
- C404: vrf forwarding 2 load-balance
- C16: ip address 30.1.1.254/24
- C17: track 50 ip route 10.1.1.1 vrf 1 reachability

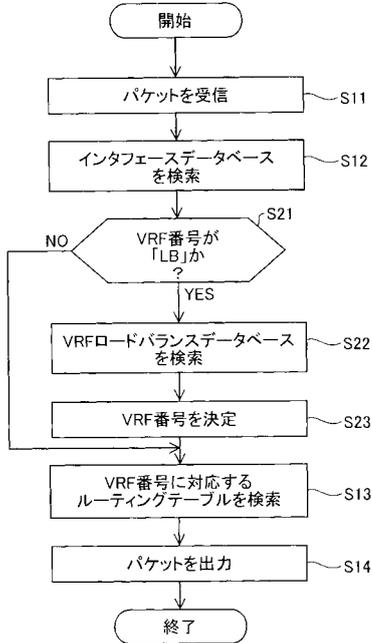
【図 53】

インタフェース番号	VRF番号	IPアドレス	サブネットマスク長
E41	131	10.1.1.254	24
E42	132	10.1.1.254	24
E43	133	20.1.1.254	24
E44	134	30.1.1.254	24

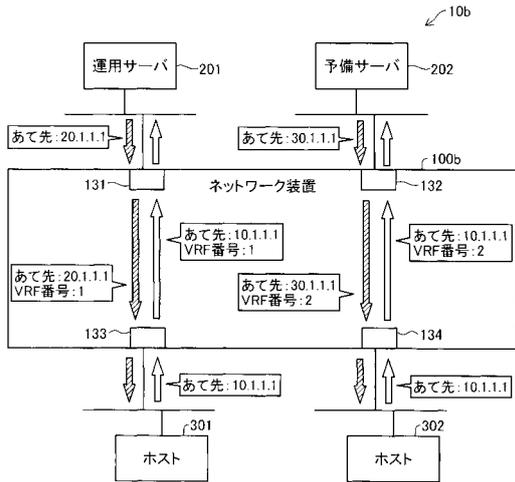
【図54】

	インタフェース番号	ロードバランス種別	VRF番号
E41	133	送信元IPアドレス	(1, 2)
E42	134	送信元IPアドレス	(1, 2)

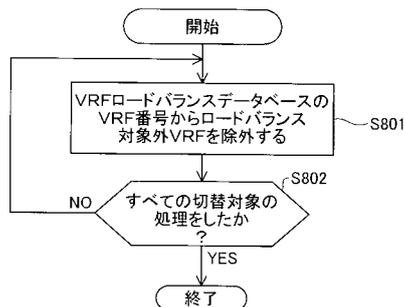
【図55】



【図59】



【図60】



【図56】

	あて先 IPアドレス	サブ ネット マスク長	ネクストホップ IPアドレス	出力 インタフェース
E41	10.1.1.1	32	10.1.1.1	131
E42	10.1.1.254	32	-	-
E43	20.1.1.1	32	20.1.1.1	133
E44	20.1.1.254	32	-	-
E45	30.1.1.1	32	30.1.1.1	134
E46	30.1.1.254	32	-	-

【図57】

	あて先 IPアドレス	サブ ネット マスク長	ネクストホップ IPアドレス	出力 インタフェース
E41	10.1.1.1	32	10.1.1.1	132
E42	10.1.1.254	32	-	-
E43	20.1.1.1	32	20.1.1.1	133
E44	20.1.1.254	32	-	-
E45	30.1.1.1	32	30.1.1.1	134
E46	30.1.1.254	32	-	-

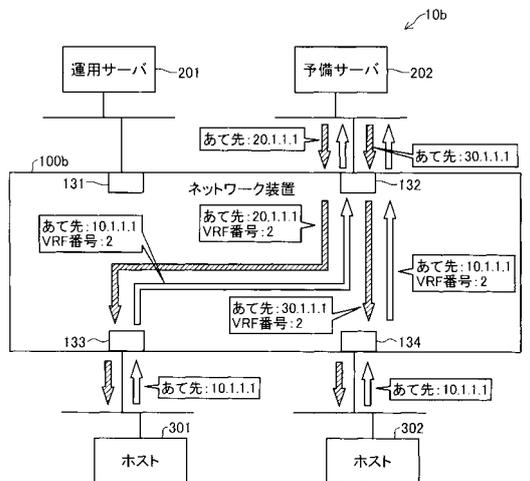
【図58】

	監視ID	切替対象 インタフェース	ロードバランス 対象外VRF	切替後状態
E41	50	133	1	ロック
E42	50	134	1	リカバリー

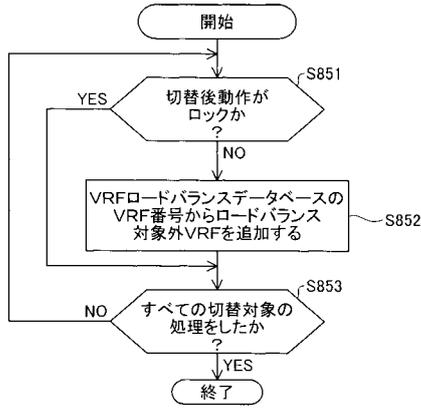
【図61】

	インタフェース番号	ロードバランス種別	VRF番号
E41	133	送信元IPアドレス	2
E42	134	送信元IPアドレス	2

【図62】



【図63】



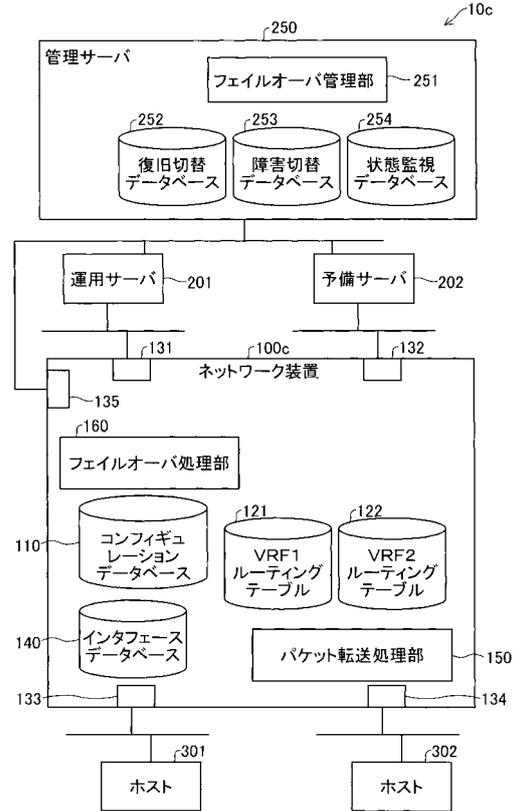
【図64】

	インタフェース番号	ロードバランス種別	VRF番号
E41	133	送信元IPアドレス	2
E42	134	送信元IPアドレス	(1, 2)

【図65】

Router# redundancy force-switchover interface 133 vrf 1,2

【図66】



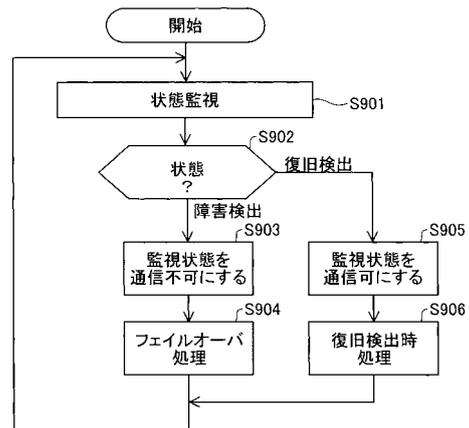
【図67】

- C1: vrf definition 1
- C2: vrf definition 2
- C3: interface ethernet 131
- C4: vrf forwarding 1
- C5: ip address 10.1.1.254/24
- C6: interface ethernet 132
- C7: vrf forwarding 2
- C8: ip address 10.1.1.254/24
- C9: interface ethernet 133
- C10: vrf forwarding 1
- C12: ip address 20.1.1.254/24
- C13: interface ethernet 134
- C14: vrf forwarding 1
- C16: ip address 30.1.1.254/24
- C501: interface ethernet 135
- C502: ip address 192.168.0.100/24
- C503: failover server 250

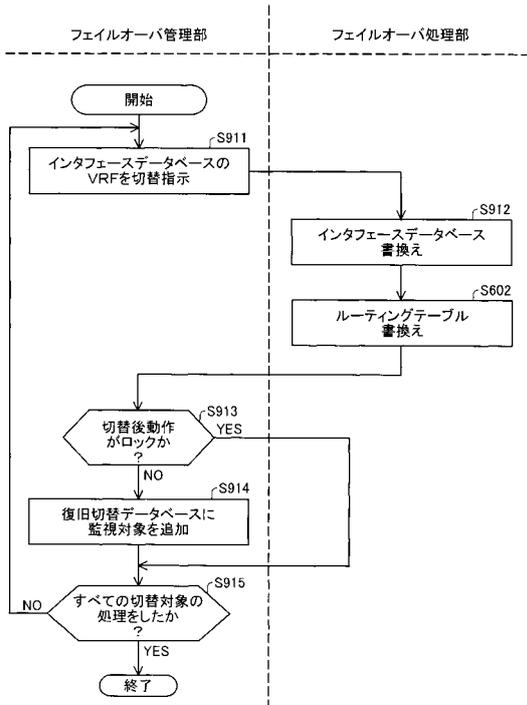
【図68】

	インタフェース番号	VRF番号	IPアドレス	サブネットマスク長
E51	131	1	10. 1. 1. 254	24
E52	132	2	10. 1. 1. 254	24
E53	133	1	20. 1. 1. 254	24
E54	134	1	30. 1. 1. 254	24
E55	135	-	192. 168. 0. 100	24

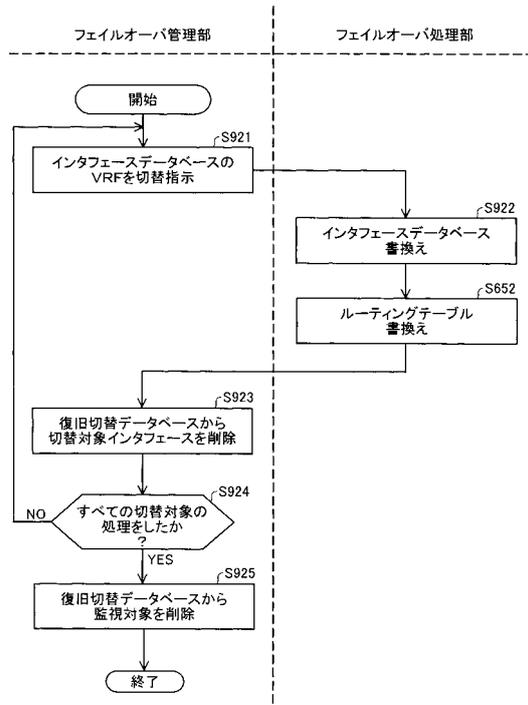
【図69】



【図70】



【図71】



## フロントページの続き

- (56)参考文献 特開2003-228527(JP,A)  
特開2008-193231(JP,A)  
特開2005-258847(JP,A)  
特開2005-056347(JP,A)  
特開2005-250626(JP,A)  
特開2002-261792(JP,A)  
国際公開第2009/045299(WO,A1)  
特表2010-541473(JP,A)  
特開2005-217933(JP,A)  
特開2006-215635(JP,A)  
米国特許出願公開第2007/0198710(US,A1)  
米国特許出願公開第2006/0209682(US,A1)  
立花 幸治, 浅井 保行, MiFにおける仮想化技術の利用, 技報 UNISYS TECHNOLOGY REVIEW, 日本, 日本ユニシス株式会社, 2009年 5月31日, 第29巻 第1号, pp. 35-44

## (58)調査した分野(Int.Cl., DB名)

G06F 11/16 - 11/20,  
G06F 13/00,  
G06F 15/16 - 15/177,  
H04L 12/00 - 12/28, 12/44 - 12/955