The Guaranteed Network
いちばん近くで、もっと先へ。

AX＆FortiGate
セキュア仮想ネットワークソリューション
システム構築ガイド

初 版

アラクサラネットワークス株式会社

はじめに

セキュア仮想ネットワークソリューションは、アラクサラ AX シリーズによるネットワークパーティションと、Fortinet 社 FortiGate シリーズによる仮想ファイアウォール(VDOM)とを組合せて構築できる、高度なセキュリティ管理を備えた仮想ネットワークのソリューションです。本ガイドは Fortinet,inc.およびフォーティネットジャパン(株)との共同評価など相互の協力のもと、セキュア仮想ネットワークソリューションの考え方や一例を紹介し、また同システム構築の際の一助となることを目的として書かれています。

関連資料

・AX シリーズ ネットワークパーティション ソリューションガイド［基本編］［認証編］［応用編］
・AXシリーズ製品マニュアル（ http://www.alaxala.com/jp/techinfo/manual/index.html ）

・Fortinet 各種資料のダウンロード(http://www.fortinet.co.jp/download/)
・Fortinet Technical Documentation (http://docs.fortinet.com/) (英文サイト)

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。弊社製品を用いたシステム構築の一助としていただくためのものとご理解いただけますようお願いいたします。

本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX シリーズ

AX6700S/AX6600S/AX6300S	Ver. 11.4.E
AX3600S,AX2400S	Ver. 11.5.A
AX1200S	Ver. 2.3

FortiGate シリーズ

FortiOS	Ver. 4.0 MR3

なお本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本資料を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

商標一覧

・アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
・Fotinet®、FortiGate®は Fortinet,inc.の登録商標、その他本書で記載されているフォーティネット製品はフォーティネットの商標です。
・Microsoft Excel は米 Microsoft 社の商標又は登録商標です。
・Ethernet は、米国 Xerox Corp.の商品名称です。
・イーサネットは、富士ゼロックス(株)の商品名称です。
・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

目次

1. 仮想ネットワークによるセキュリティレベルの向上

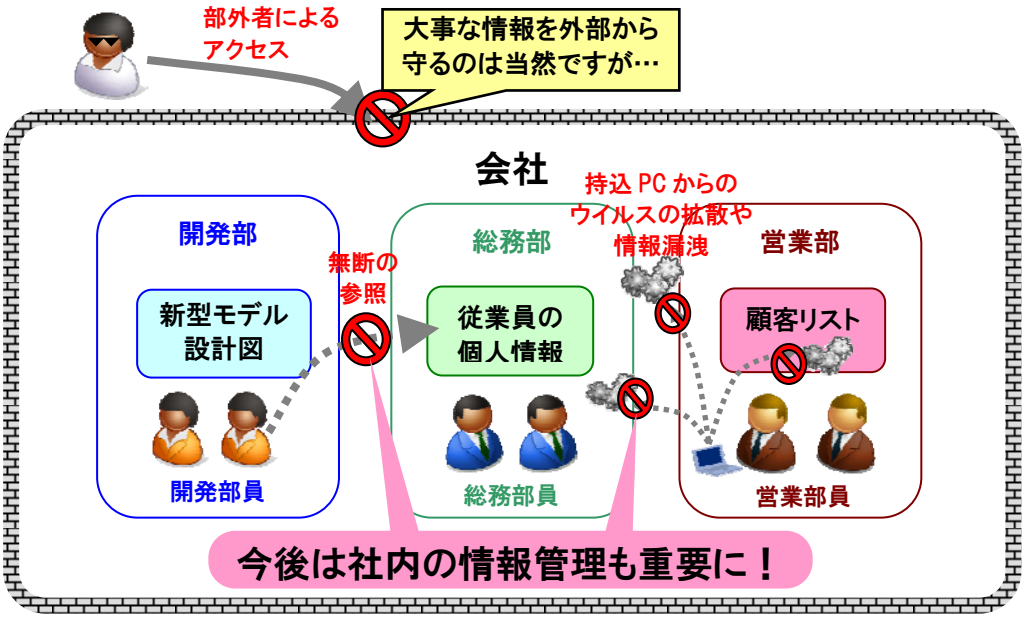
1.1 重要度を増すシステムのセキュリティ対策

昨今、企業の持つ個人情報の漏洩からそのユーザらに莫大な損害が発生したり、国家の機密情報の漏洩が世界的な社会問題になったりするなど、企業や行政団体、教育機関など社会組織において各種情報の取り扱いが厳しくなっています。

一方で、情報管理のためのツールとして一般的な存在となった IT システムですが、こちらもウイルス感染やスパムメール、インターネットからの攻撃などシステム外部からの要因以外にも、組織内に持ち込まれたPCからのウイルス感染、マルウェアによる情報漏洩、さらには悪意を持つユーザの組織内部からの意図的な攻撃や機密情報の漏洩操作など、守るべき情報に対する脅威の内容も高度かつ多種にわたっています。
また、ノート型 PC に加えタブレット端末やスマートフォンなど、個人が持てる情報端末に多様性が増していることも、各種情報にアクセスできる機会を増やしています。

このような背景から、これからのITシステムにおいては、組織内の各部門で持つさまざまな情報に対し、その情報をアクセスすべき権限を持つユーザーにのみ適切なアクセス権限を与え、またその情報に直接関係しないユーザには不必要にアクセスさせないような環境を作る必要があります。

つまり、IT システムにおけるセキュリティ管理は会社、行政団体、教育機関などといった単位から、部門や省庁、学部といった、より細かい単位でのセキュリティ(脅威)管理が重要となるでしょう。



1.2 システムに求められる課題と 2 つの「仮想化」がもたらす解決策

情報それぞれに適切なアクセス権限を与えることを考えると、以下の施策が考えられます。

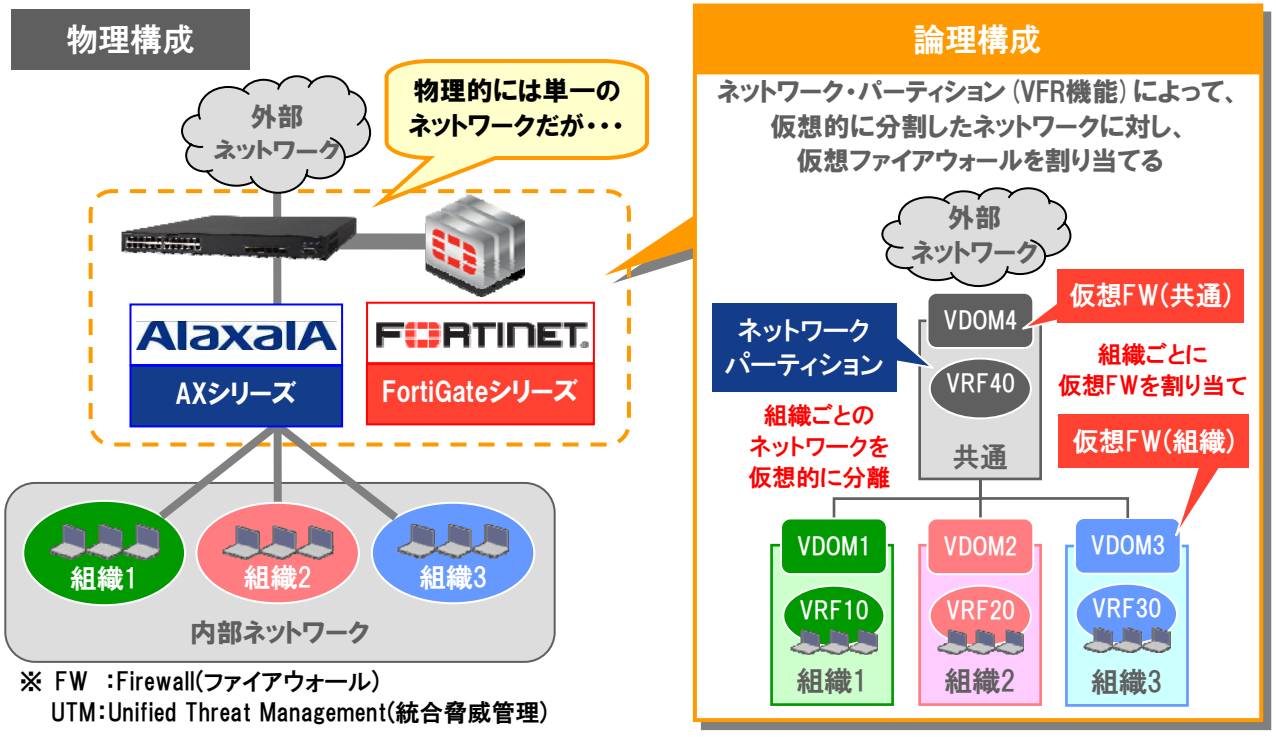
- **ネットワークの分離**
  ネットワークを組織単位で完全に分ける（物理的にアクセスできないようにする）。
- **ユーザ認証**
  認証機能を取り入れることで、不正なユーザを排除。
- **アクセス制御**
  URL、アプリケーションフィルタ等で必要な通信の許可、不要な通信の禁止を制御。
- **アクセスログの記録**
  サーバ、ネットワーク等への不正アクセス等を監視。

さらにセキュリティをより効果的なものとするには、システムと運用の両面から複数の対策を実施する必要があります。しかし以上のような施策を導入する場合、システムにおいてはネットワーク機器装置の増加や、それに伴う各種設定(フィルタ等)の追加が必要です。また運用においては運用・管理の煩雑化など初期投資や運用のためのコストが増加します。これらが大きな阻害要因となり現実にはなかなか導入に至らないケースが多いかと考えられます。

「ネットワークやアクセス制御は組織毎に細分化してセキュリティを強化したいが、それに伴う装置や運用の増加にかかるコストは抑えたい」－これらの相反する課題を解決するソリューションが、以下に示す 2 つの仮想化技術の組み合わせによるソリューションです。

- **ネットワークの仮想化**
  単一の物理ネットワークを複数の仮想ネットワークに分離することで組織間のセキュリティを確保
- **ファイアウォールの仮想化**
  仮想ネットワークごとに仮想ファイアウォール（FW）を割り当てることで組織単位に最適なセキュリティポリシーを運用

そしてこのソリューションをより現実的なものとするため、このたびアラクサラネットワークスと Fortinet が手を結び、「セキュア仮想ネットワークソリューション」として提案いたします。



1.3 セキュア仮想ネットワークソリューション概要

セキュア仮想ネットワークソリューションとは、2 つの仮想化技術の組み合わせによって、組織ごとに高度にセキュリティ管理されたネットワークシステムを必要最小限の機器で提供するソリューションです。

2 つの仮想化をどのように組み合わせて実現するのか、それぞれの仮想化の概念を踏まえながら、セキュア仮想ネットワークソリューションの概要を紹介します。

1.3.1 ネットワークの仮想化

組織間のセキュリティを確保するためには、それぞれの組織で独立したネットワークとしてしまうことが最もシンプルかつ簡単な方法です。そこでアラクサラのネットワーク・パーティションで組織ごとに独立したネットワーク構成を作ります。

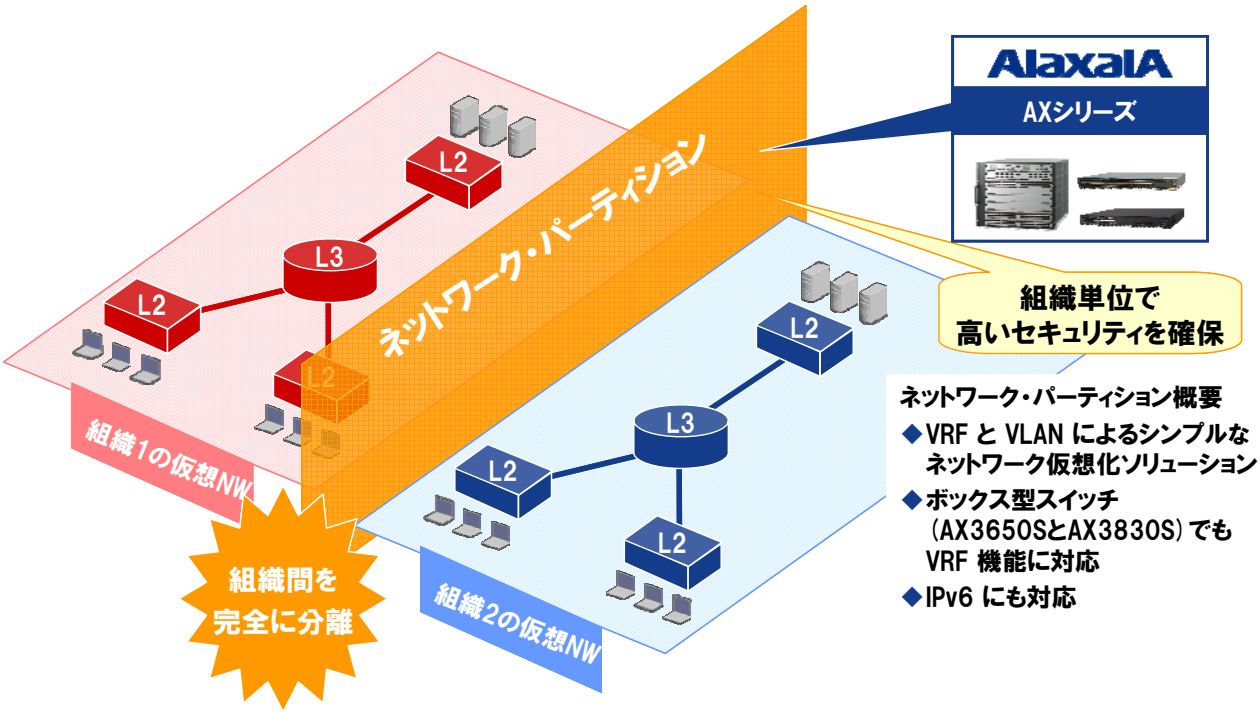


図 1.3-1 ネットワーク・パーティションによる仮想ネットワーク概念図

ネットワークごと組織単位に分離するため、組織間の通信を完全に遮断することができます。
しかし、ネットワーク自体はネットワーク・パーティションによる仮想ネットワークで構成されるため、実際のスイッチ機器は最少の構成で済み、機器や運用コストの増加を抑えます。

1.3.2 ファイアウォールの仮想化

ネットワーク・パーティションによって組織毎に分けられたネットワークそれぞれに対する、外部からの脅威の防御や内部からのアクセス制御、管理、監視については、やはりそれぞれのネットワークにファイアウォールを配するのがシンプルでわかりやすい構成でしょう。

そのネットワークそれぞれに渡るいくつものファイアウォールを、Fortinet の FortiGate シリーズによる仮想ファイアウォール(VDOM)が担います。

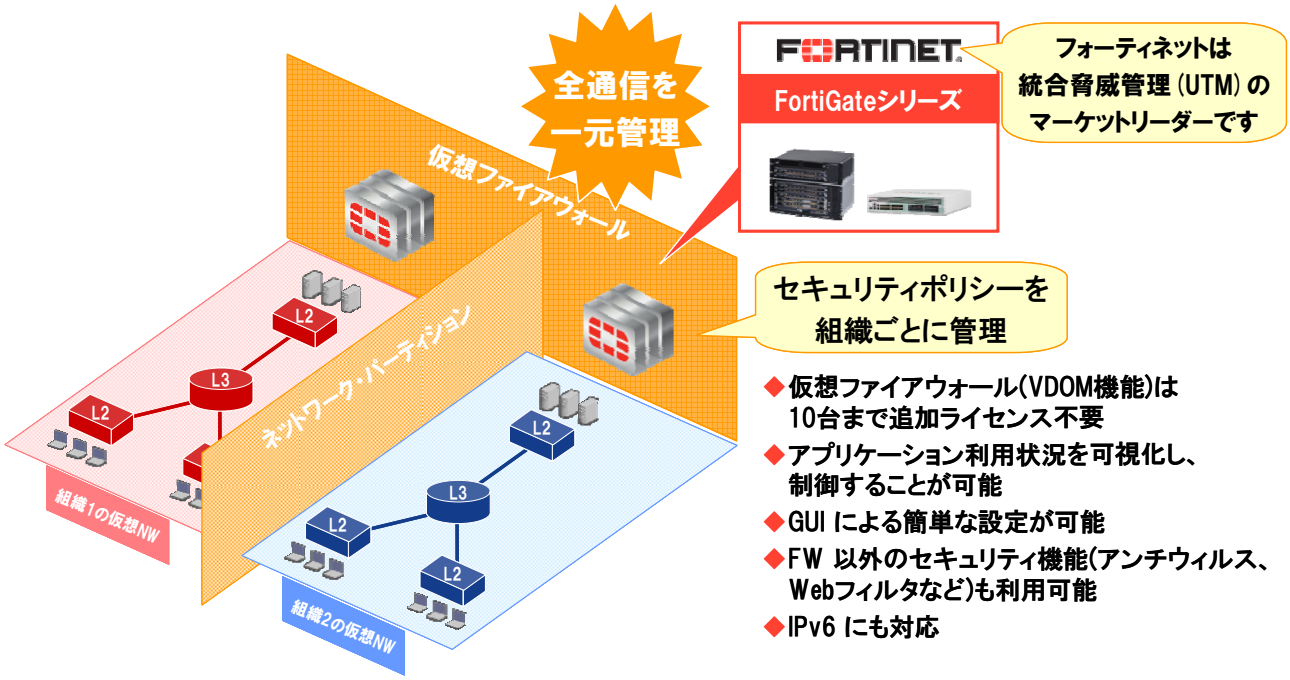


図 1.3-2 仮想ファイアウォール適用の概念図

ネットワーク・パーティションによる仮想ネットワークで構成された組織毎のネットワークそれぞれに対し、仮想ファイアウォール(VDOM)をそれぞれ配することで、組織毎のアクセス管理や監視を、同じく最小限の投資で済ませることが可能です。

また VDOM は単なるファイアウォールとしてだけではなく、URL フィルタや IPS 検知、ウイルスチェックなど、高度な脅威管理機能を備えています。このため組織毎の詳細なアクセス制御でその組織自体を守るだけでなく、万が一の組織内部からの攻撃やウイルス感染の脅威をその組織内など局所的に留め、他の組織への影響を防ぐ、といった高度なセキュリティを実現します。

このように、アラクサラのネットワーク・パーティションと、Fortinet FortiGate の VDOM の組み合わせにより、組織毎に独立して高度なセキュリティ管理をそなえたネットワークを最小限の装置機器構成で構築することができます。

システム全体として高度なセキュリティ環境を実現しながらも、機器の構成と運用管理コストについては最小化の両立を図ったシステムを作ることを可能にする。それが「セキュア仮想ネットワークソリューション」です。

2. キーテクノロジ

ここでは、先に述べた「2 つの仮想化」それぞれについて、より詳細に解説します。

2.1 ネットワーク・パーティション（VRF 機能）

アラクサラが提供する、ネットワークにおける仮想化技術がネットワーク・パーティションです。

ネットワーク・パーティションとは、レイヤ 3 機能を論理的に分割する『VRF(Virtual/VPN Routing and Forwarding)』と呼ばれる機能に、レイヤ 2 の論理ネットワーク技術である VLAN を組合せ、複数の論理的なネットワークをシンプルな物理構成によるシステムで実現する技術です。

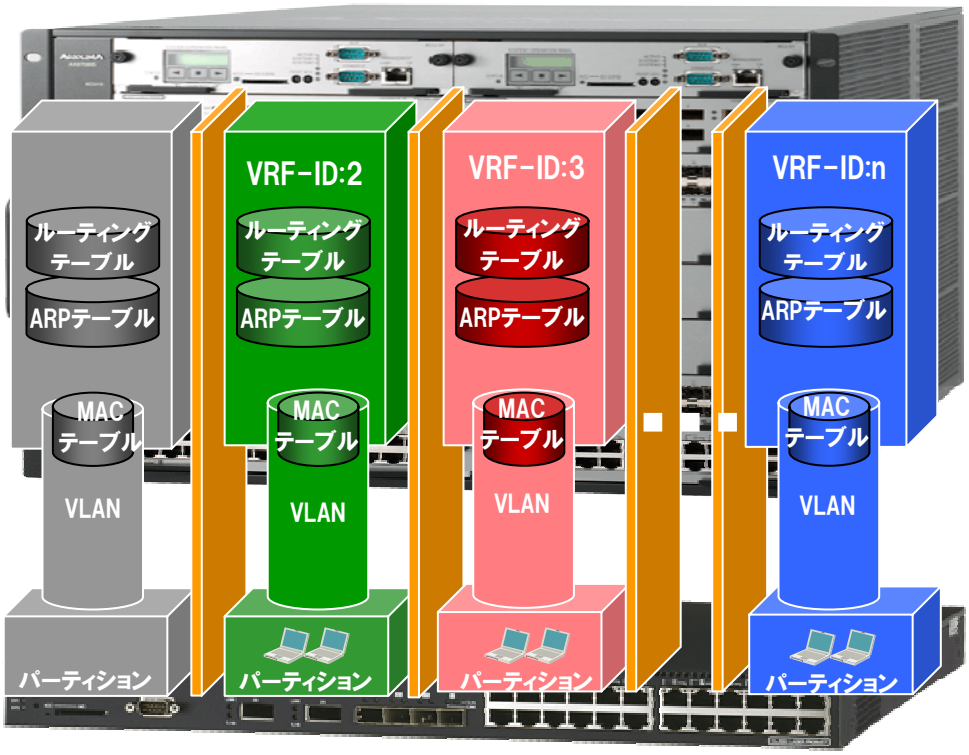


図 2.1-1 ネットワーク・パーティション概念図

VRF では、レイヤ 3 ネットワークでの基本情報であるルーティングテーブルや ARP テーブルなどを、扱う複数のネットワークそれぞれで独立して制御および管理をおこないます。この VRF によって分けられた論理的なレイヤ 3 ネットワークと VLAN によって分けられた論理的なレイヤ 2 ネットワークを、分割されたネットワーク単位でまとめたものを「パーティション」と呼びます。

これにより、レイヤ 3 のネットワークが論理的にいくつもあるようなシステムを 1 台で構成することが可能となるため、組織単位で独立したネットワーク構成とすることも簡単にできます。

ただし、VLAN およびルーティングテーブルや ARP テーブルは、装置の持つ全体のリソースを各 VRF で分けあって使用します。従って VRF によって装置の収容条件等が拡張されるものではありません。

VRF を扱う装置内では、VRF-ID と呼ぶ VRF 毎にユニークな識別子を各パーティション内の VRF や VLAN に付与して区別しますが、システム全体の管理用などに VRF-ID を持たないパーティションによるネットワークも存在します。これをグローバルネットワークと呼び、グローバルネットワークでは telnet や FTP、syslog などシステム管理に関する機能が一般の VRF より広くサポートされます。

AX シリーズにおいて VRF 機能をサポートする機種および設定可能な VRF 数は以下の通りです。

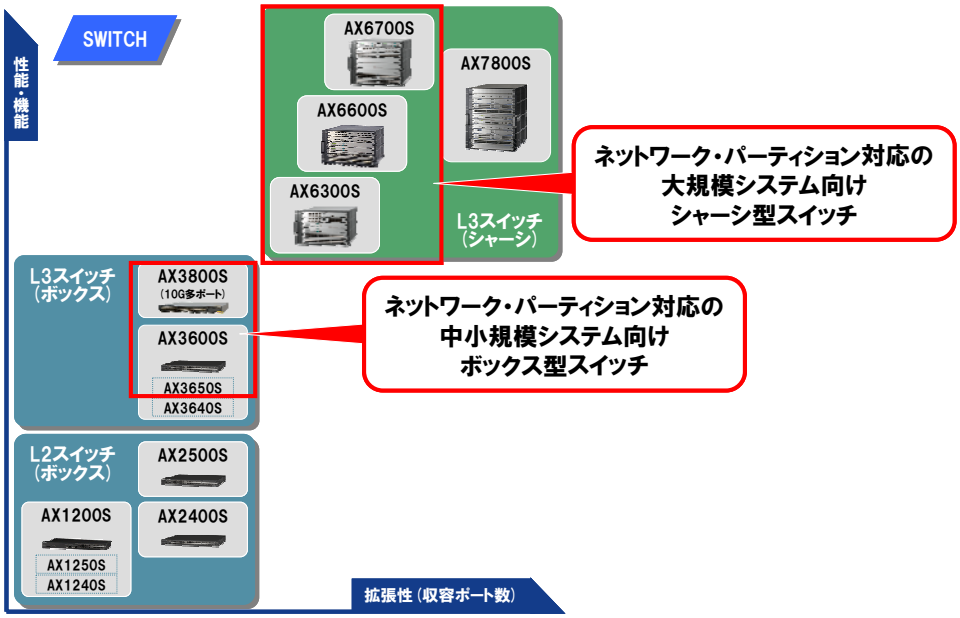


図 2.1-2 ネットワーク・パーティション対応の AX シリーズ

表 2-1 VRFサポート状況

VRF サポート機種	シャーシ型			ボックス型	
	AX6700S	AX6600S	AX6300S	AX3830S	AX3650S
VRF 設定可能数 （グローバル含まず）	63/124/249 (*1)	63/124/249 (*1)	63/124/249 (*1)	31	31

(*1)同時に使用する L2 冗長プロトコルの有無や種類によります。

ネットワーク・パーティションのさらに詳しい内容については、「AX シリーズ ネットワークパーティション ソリューションガイド [基本編] [認証編] [応用編]」に記載しています。こちらも合わせてご利用ください。

2.2 仮想ファイアウォール(VDOM)と FortiGate シリーズ

FortiGate がそなえる仮想ドメイン（VDOM）は、物理的な FortiGate 装置を複数の仮想装置（セキュリティドメイン）に分割する機能です。各 VDOM は、ネットワークやファイアウォール、セキュリティなど各種の設定を個別に設定でき、また管理者も個別に分けることが可能など、各々が全く独立した FortiGate 装置として振る舞います。以下に概念図を示します。

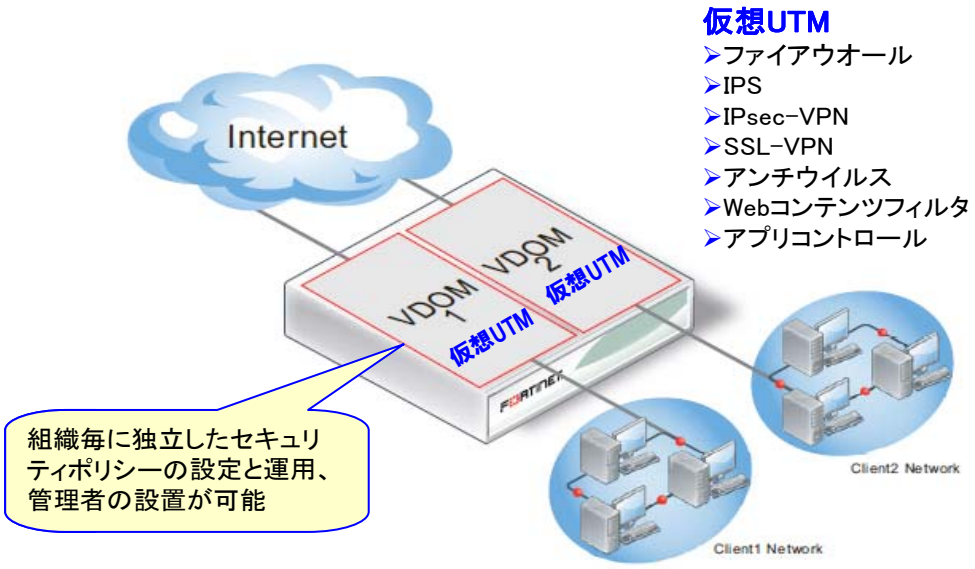


図 2.2-1 仮想ドメイン(VDOM)の概念図

この VDOM では、ファイアウォールとしての機能も充実しています。一般的なファイアウォールの機能(アドレス/ポートによるフィルタ、NAT 等)から、VPN、IPS 検知、アンチウイルス、Web コンテンツフィルタ、アプリケーションコントロールなどの統合的なセキュリティ機能（UTM）までを備え、またそれらは各 VDOM 個別に設定することが可能です。

またネットワークに VDOM を加える場合、各 VDOM は以下の 2 つの動作モードのいずれかで構成することができます。これらのモードについても各 VDOM 毎に独立して設定が可能です。

- TP(トランスペアレント)モード:
  同一ネットワークセグメント(VLAN)内でファイアウォールとして機能します。
- RT(ルータ)モード:
  異なるネットワークセグメント(VLAN)にまたがりゲートウェイ的に動作可能です。
  NAT などを使う場合はこちらのモードで使用することが前提となります。

このように省スペース、省消費電力、柔軟性と簡素な管理を提供し、FortiGate の根幹をなす VDOM は以下のような用途で広く利用されています。

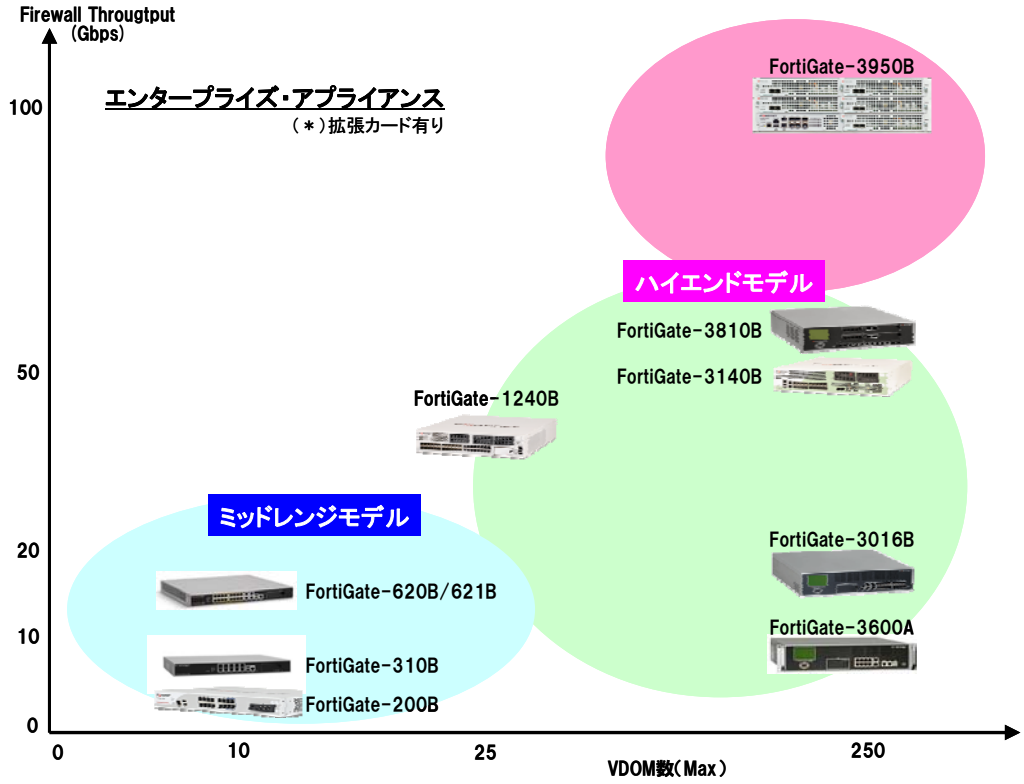
➢データセンタにおける、顧客別の独立したネットワークセキュリティサービス。

➢事務、教員、学生などセキュリティレベルの異なるネットワークそれぞれに対する、独立したネットワークセキュリティゲートウェイの提供。

➢プライベートクラウドサービスにて、独立したネットワークセキュリティゲートウェイオプションサービス。

➢同じプライベートアドレスを持つネットワーク同士のアドレスの変更を伴わない統合。

また、FortiGate シリーズはシステムの用途や規模に合わせ、豊富にラインアップを揃えています。



FortiGate-50B シリーズ以上の FortiGate では、オプションライセンス等の追加無しに最大 10 の仮想ドメインを構成できます。FortiGate-1240B ではオプションを追加することで最大 25 まで、FortiGate-3000 シリーズ以上では同様にオプションの追加で最大 250 まで拡張することができます。より上位の大規模エンタープライズシステムに対応するシャーシ型製品の FortiGate-5140 なら 14 枚の FortiGate ブレードを使用することにより最大 3,500 個の VDOM が構築できます。

また、FortiGate-3000 シリーズ以上では 10Gbps のインタフェースを備えており、大規模かつ大容量なスループットが要求される構成にも耐ええる構成となっております。

2.3 仮想化テクノロジーの組み合わせによるメリット

以上、アラクサラのネットワーク・パーティションと、Fortinet の仮想ドメイン(VDOM)を組み合わせることで、次のようなメリットが得られます。

➢ミニマムな物理的制約

物理構成(装置台数)の最小化により、導入コストや電力/スペースなどを低減。また管理対象も少なくなり、運用コストも低減。

➢自在な論理構成

論理構成は自在なので物理構成はシンプルなまま、高度なネットワークを構成することが可能。

➢システム変更への柔軟な対応

仮想ネットワークは他への影響無しに追加削除が自由。組織の統合や部署の新設など、柔軟な対応が可能。

➢IPv6 Ready

AX シリーズ、FortiGate シリーズとも IPv6 Ready Logo 取得済み。IPv6 マイグレーションにも対応可能。

➢ネットワーク認証とも連携

AX シリーズのネットワーク認証機能と連携することで、ロケーションに縛られずに自分のリソース(仮想システム)へアクセスすることが可能。

2.4 セキュア仮想ネットワークの具体化イメージ

以上、2 つの仮想化技術によって提唱されるセキュア仮想ネットワークソリューションを、実際のシステムとして適用し構築するとどのようになるのか、どのようなメリットがあるのかについて解説します。

まず、会社などで使われるネットワークは、一般的には以下のようなイメージで考えられます。

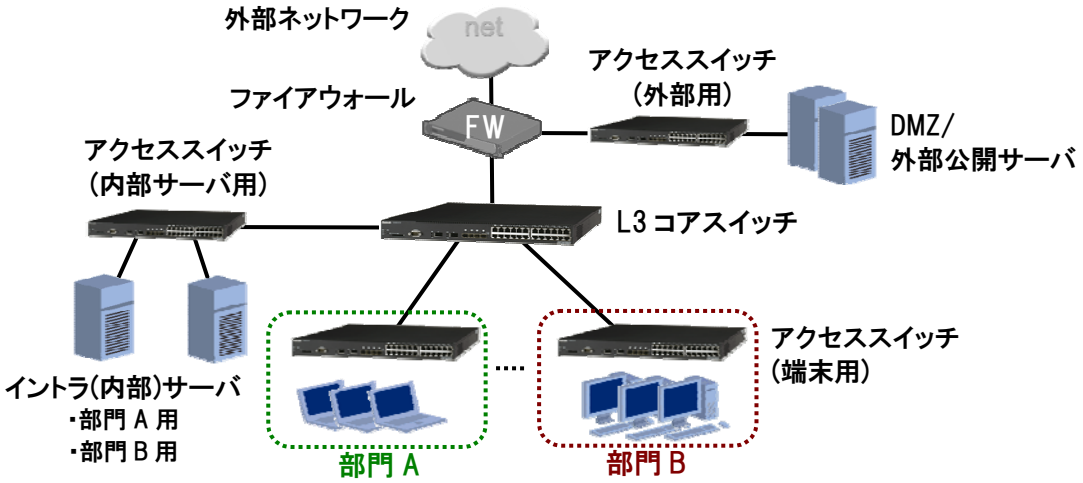


図 2.4-1 一般的なネットワーク構成

このような会社ネットワークを、アラクサラと Fortinet の仮想化技術を用いたセキュア仮想ネットワークとして再構成すると、

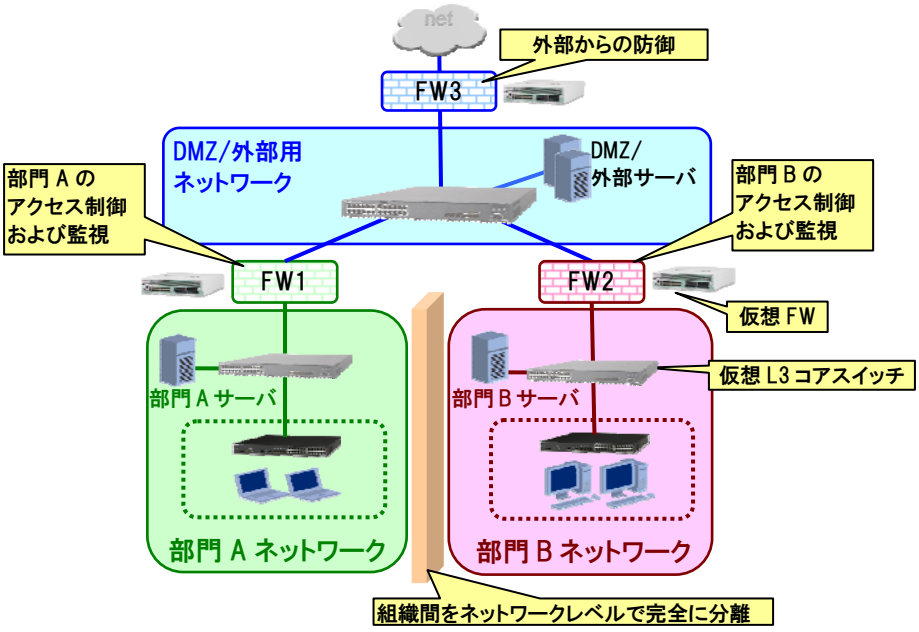
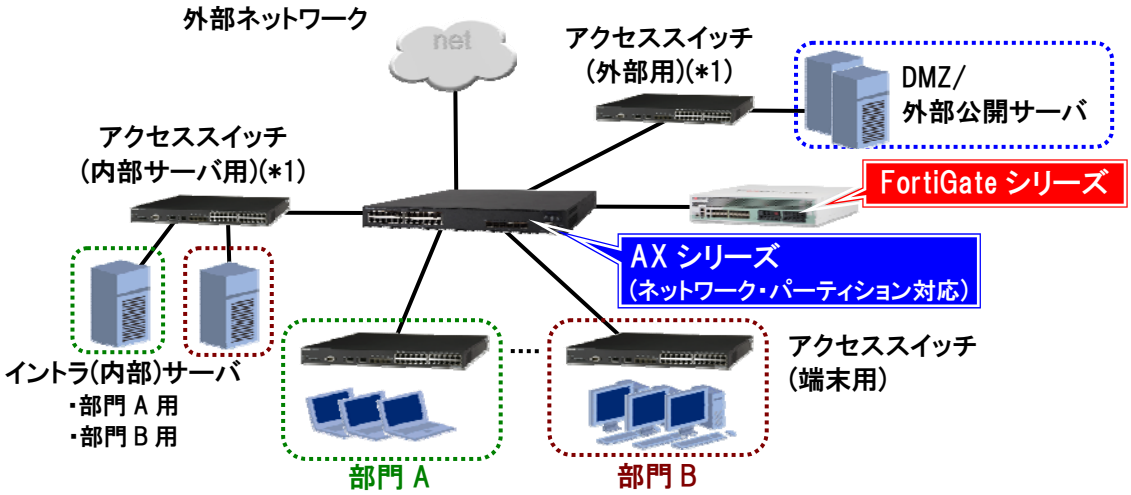


図 2.4-2 セキュア仮想ネットワークの論理構成

図 2.4-2 セキュア仮想ネットワークの論理構成のように、組織ごとにネットワークとアクセス制御が分離された、高度なセキュリティを備えるネットワークとすることができます。

しかしながら、このネットワークを実現する装置の構成は以下図 2.4-3の通りとなり、最初に提示した図 2.4-1の単一ネットワーク構成とほとんど変わらない構成となります。このように両社の仮想化技術によって、最小限の装置機器およびその管理でネットワークを運用できることがわかります。



(*1)実際は VLAN でわけられているため、サーバ用スイッチは外部用/内部用でまとめても良い。

図 2.4-3 セキュア仮想ネットワークの物理構成

2.5 装置の冗長化

さらに、実際に運用されるシステムでは、装置機器や回線の障害などに対応できるよう可用性を考慮した構成とするケースが一般的ですが、複数のネットワークが同一の装置上に構成される仮想ネットワークでは、より高い信頼性が要求されるため、システムとして冗長構成は必須です。

アラクサラの AX シリーズでは、FT スイッチ（AX6700S/AX6600S/AX6300S）や、リング、GSRP 等に代表される高信頼、高可用を実現する機能の他、STP/VRRP 等の標準化された装置冗長プロトコルも利用可能です。
こちらについても、構成に応じて当社 Web ページ等にて各種構築ガイドを揃えていますのでご活用ください。

一方、Fortinet の FortiGate シリーズにおいても、HA（High Availability：冗長化構成）機能により、冗長構成のシステムを構築することができます。FortiGate の HA 機能は、独自のプロトコル FGCP（FotiGate Clustering Protocol）により、装置の2重化を実現し、Active－Active、Active－Passive の各モードに対応します。

（1）Active－Passive モード動作概要
ホットスタンドバイ・フェイルオーバ保護機能を提供。

- トラフィックを処理する Primary Unit と Subordinate unit から構成。
- Subordinate unit はネットワークと Primary Unit に接続されるが、トラフィックは処理しない。
- Subordinate unit は通常スタンドバイ状態で待機。
- Primary Unit が故障等により、“Cluster State Information”メッセージを受信すると、スタンドバイ状態から Active 状態に移行し、トラフィックを処理。
- リンクのフェイルオーバ保護機能を提供。

（2）Active－Active モード動作概要

ロードバランシングならびにフェールオーバ保護機能を提供。

- すべてのクラスタユニット間でネットワークトラフィックを負荷分散。
- トラフィックを処理する Primary Unit と1台以上の Subordinate unit で構成されます。
- Primary Unit は、全トラフィックを受信し、処理します。
- Primary Unit は、ウイルススキャンのトラフィック、またはオプションで全 TCP およびウイルススキャンのトラフィックを複数のクラスタユニット間で負荷分散します。
- Active－Passive クラスタ同様にリンクのフェイルオーバ保護機能を提供。
- Primary Unitに障害が発生した場合、Subordinate unitがPrimary Unitになり、残りのすべてのクラスタユニット間でTCPセッションを再配布します。
- Subordinate unitに障害が発生した場合、Primary Unitは残りのすべてのクラスタユニット間で全TCPセッションを再配布します。

この他、詳細につきましては、FortiOS Handbook v3 - High Availability 等を参照願います。

以下、2.4節で紹介したセキュア仮想ネットワークの物理構成を冗長構成とした例を以下に示します。論理的な構成は「図 2.4-2 セキュア仮想ネットワークの論理構成」と変わりません。

（1） FT スイッチコア＋FortiGate HA

比較的大規模なシステムで、L3 コアのスイッチが AX6700S シリーズ等のシャーシ型となる場合、FT 構成として、シンプルに高信頼なシステムを構成することができます。

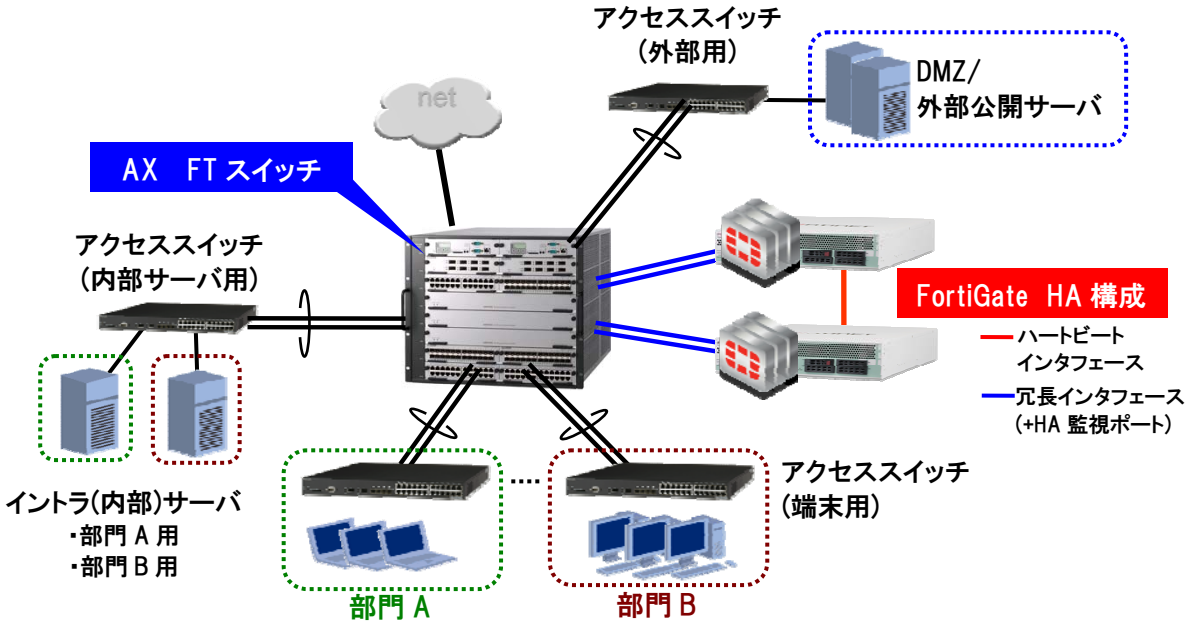


図 2.5-1 FT スイッチ＋FortiGate 冗長構成

FT スイッチと周辺スイッチの接続はリンクアグリゲーションでの接続が基本ですが、FortiGate との接続においては、LACP モードのリンクアグリゲーションまたは FortiGate でサポートされる冗長インタフェース機能による接続となります。回線の帯域を有効に使いたい場合はリンクアグリゲーション(LACP)による接続を、回線障害時の系切替時間を優先させる場合は冗長インタフェースによる接続とすることを推奨します。

(2) STP+VRRP ＋FortiGate HA

中小規模のシステムで、L3 コアスイッチを AX3650S 等のボックス型で構成するといった場合は、一般的な STP+VRRP 構成と組み合わせ、以下のような構成とすることもできます。

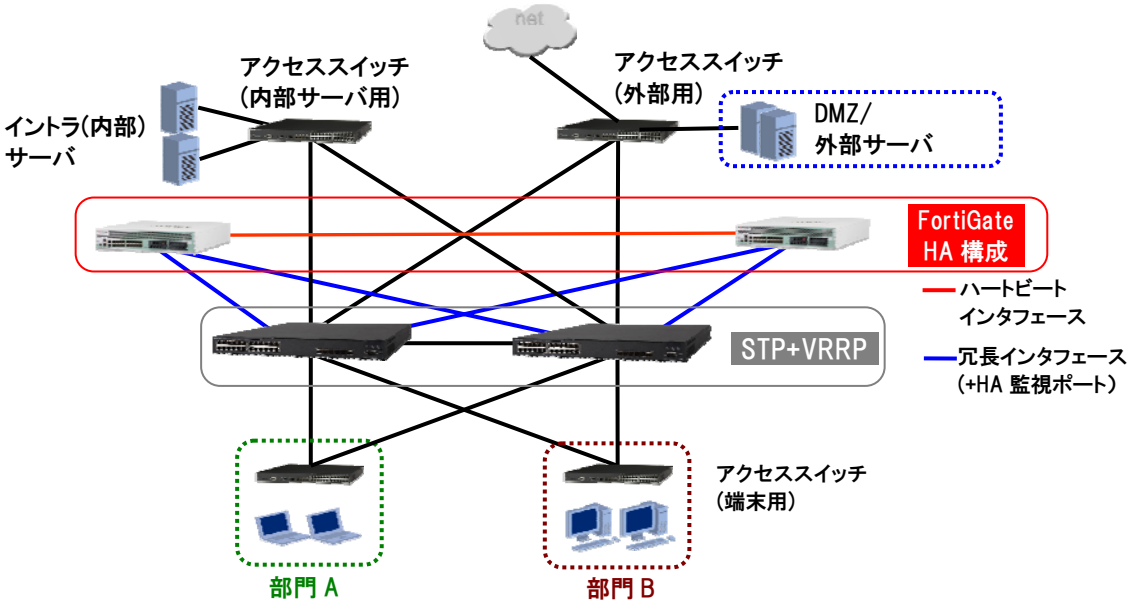


図 2.5-2 STP/VRRP 構成 + FortiGate 冗長構成

この構成においても、FortiGate との接続は FortiGate の冗長インタフェースを基本として接続することを推奨します。なおその際、スイッチ側で FortiGate と接続するポートに対しては STP の設定は不要です。

3. システム構築例

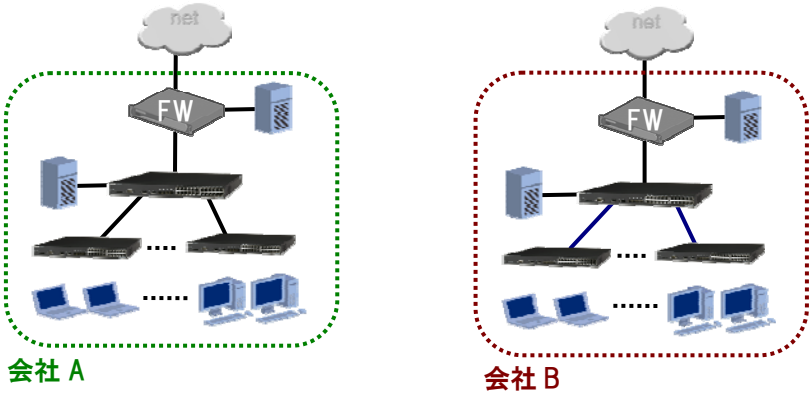
これまでの解説の通り、アラクサラのネットワーク・パーティションによる仮想ネットワークとFortiGateのVDOMによる仮想ファイアウォールを使うと、最小限の装置機器の運用で複数のネットワークとアクセス制御による高度なセキュリティを持つネットワークを構成できます。本章では、2.4節で紹介した構成をもとに、

- FT スイッチと FortiGate　HA 構成での構成例
- ボックス型スイッチによる STP+VRRP 構成と FortiGate HA 構成での構成例

それぞれを構築する場合について解説します。

3.1　完全システム分離構成の適用例（FT スイッチコア+FortiGate HA）

仮想ネットワークは全く独立した複数のシステムを収容できます。以下に、既に稼動中の複数ネットワークを仮想ネットワークとして扱う場合の構築例について示します。仮想ネットワークにてまったく独立分離したネットワークを扱うため、端末やサーバの設定はこれまでのネットワークと設定を変更することなく利用することが可能です。



用途	VLAN ID	IP アドレス
会社 A 外部接続用	1000	10.10.1.0/24（外部）
会社 A サーバ用	10	172.16.0.0/16
会社 A PC 用	100-101	192.168.0-1.0/24
会社 B 外部接続用	1000	10.20.2.0/24（外部）
会社 B サーバ用	10	172.16.0.0/16
会社 B 端末 PC 用	100-101	192.168.0-1.0/24

図 3.1-1 2 つの独立したネットワーク

ここでは、以上のように 2 つの会社の全く独立したネットワークを例に考えます。この会社 A と会社 B のネットワークをまとめて扱うネットワークの再構築を図ると、もともとが互いに独立したネットワークであるため使用している IP アドレスが重複するなど、そのままでは再構築は困難かと思われます。

このようなケースにおいて、セキュア仮想ネットワークソリューションが最適です。

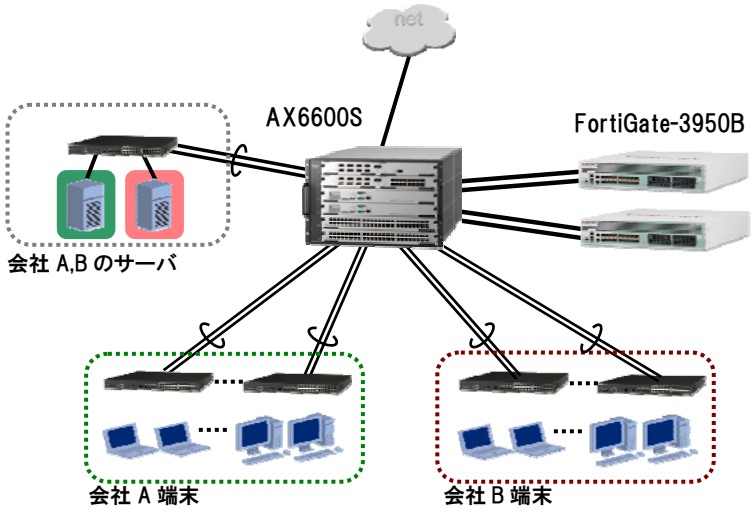


図 3.1-2 仮想ネットワークによる会社 A,B 統合システムの物理構成

物理構成は以上のように単一のネットワークとほとんど変わらない構成となります。ファイアウォールについては、FortiGate を冗長構成で使用しネットワークのコア部分に組み込む形となります。

しかしながら、仮想ネットワークと仮想ファイアウォールによる論理的なネットワーク構成は以下の通りとなり、会社 A、会社 B それぞれのネットワークは完全に独立分離した形で以上のネットワーク構成に収容する形となります。

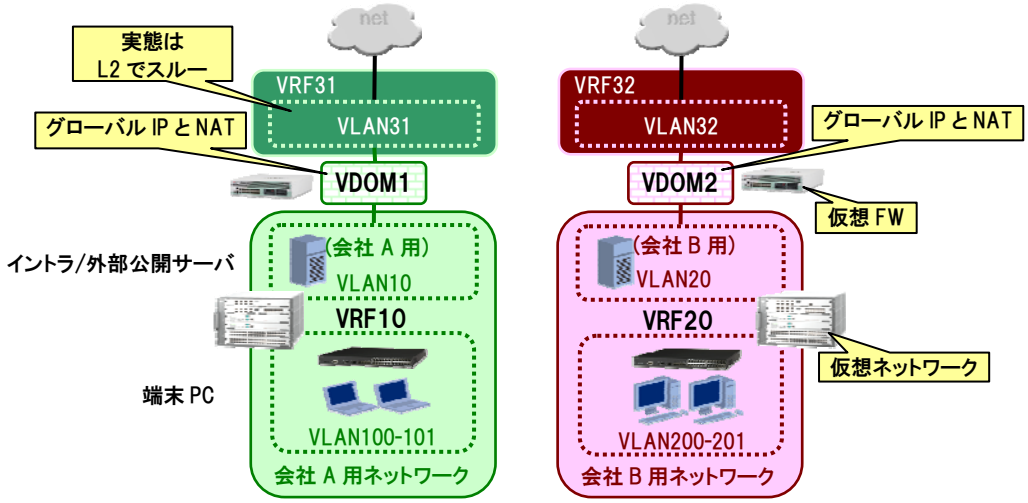
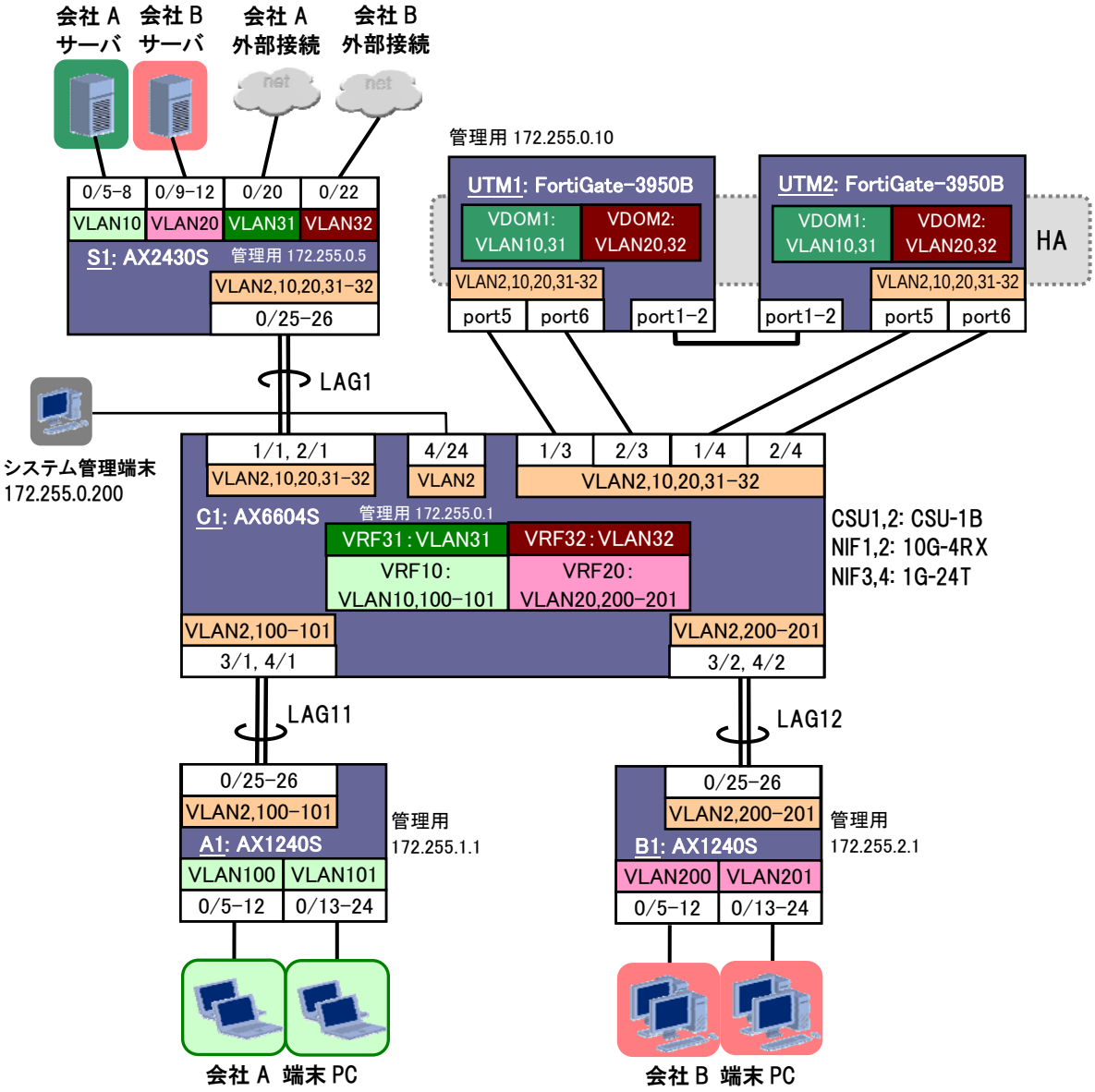


図 3.1-3 会社 A,B システムの論理構成

具体的には、ネットワーク・パーティション(VRF)による仮想ネットワークにて会社 A、会社 B の内部ネットワークそれぞれを収容し、また外部ネットワークとのファイアウォールについても、仮想ファイアウォール(VDOM)にてそれぞれのネットワークの外部接続用ファイアウォールとして機能するように構成します。

これにより、会社 A,会社 B から見ると今まで同様なネットワーク環境が、物理的な一つのネットワークに収容することができます。

このネットワークにおける、各装置ごとでの論理構成は以下のようになります。



用途	VDOM	VRF ID	VLAN ID	IP アドレス
会社 A 外部接続用	VDOM1	31	31	10.10.1.0/24 (外部)
会社 A サーバ/Uplink 用		10	10	172.16.0.0/16
会社 A 端末 PC 用	–		100-101	192.168.0-1.0/24
会社 B 外部接続用	VDOM2	32	32	10.20.2.0/24 (外部)
会社 B サーバ/Uplink 用		20	20	172.16.0.0/16
会社 B 端末 PC 用	–		200-201	192.168.0-1.0/24
システム総合管理用	–	global	2	172.255.0.0/16

図 3.1-4 会社 A,B 統合システム 論理設定詳細

3.1.1 システム構築時のポイント

本例の構成を設計する際におけるポイントを以下に示します。

(1) コアスイッチ、UTM の要求性能や収容条件は元システムを集約した分が必要。

複数のネットワークをそれぞれ仮想ネットワークとして扱い物理的にはひとつの構成に集約する場合、もとのネットワークで必要な性能や収容条件の和を超える性能や収容能力が必要となります。
従って使用する装置の選定に関しては、もとのネットワークそれぞれで使用していた装置の必要性能や収容条件の総和を目安とすれば良いでしょう。

(2) 可用性の確保はフォールト・トレラント(FT)構成で。UTM(FortiGate)は HA 構成で。

本例のようにコアに AX6700S/AX6600S/AX6300S といったシャーシ型のスイッチを用いる場合では、装置の可用性確保にはフォールト・トレラント構成(装置内モジュールを冗長とした構成)を推奨します。また UTM については HA 構成とします。

(3) コアスイッチと UTM 間は FortiGate の冗長インタフェースを使用する。

コアスイッチと UTM(FortiGate)間の接続については、回線帯域が許すのであればリンクアグリゲーションではなく FortiGate の持つ機能である冗長インタフェースを用いて回線の可用性を確保します。

回線の帯域もリンクアグリゲーションで確保したい、という場合は LACP によるリンクアグリゲーションを使用します。

(4) 各仮想ネットワークの VDOM をそれぞれ外部とのファイアウォールとして構成する。

既存のネットワークを収容する場合、もとのネットワークで持っていたグローバル IP アドレスをそのまま引き継ぐケースが多いと思われます。

従ってそれぞれのネットワークでの外部への接続はそれぞれのネットワークの持つ VDOM を用いて直接外部と接続するように設定します。VDOM では IP アドレス重複の許容はもちろん、NAT も VDOM ごとに独立して機能します。

(5) FortiGate はインターネットと接続できるパスを設ける。

FortiGate のライセンス管理や各種フィルタ機能で使用されるパターンファイル、シグネチャ等の更新などは外部にある Fortinet の専用サーバを通しておこないます。従って FortiGate はインターネット接続できる環境下に置く必要があります。

3.1.2 スイッチ機器(AX シリーズ)設定時のポイント

コンフィグなど、機器の設定の際のポイントを以下に示します。

(1) シャーシ型スイッチ(AX6700S/AX6600S/AX6300S)で VRF を使用する場合、モードを設定する。 AX Serise

シャーシ型のモデル(AX6700S/AX6600S/AX6300S)でネットワーク・パーティション(VRF)を使用する場合、VRF の動作モードを設定する必要があります。また本設定の際にはスイッチング機構(BSU、CSU、MSU)が再起動されます。

(2) VLAN インタフェースでの設定は最初に所属 VRF の設定からおこなう。 AX Serise

VLAN インタフェースでは、所属 VRF の設定と IP アドレスの設定が必要ですが、所属 VRF の設定は IP アドレスの設定前におこなう必要があります。(IP アドレスが設定されている状態では所属 VRF の設定はできません。)
ですので、VLAN インタフェースの設定では所属 VRF の設定を最初におこなってください。

(3) ForiGate と接続するポートについては特に設定不要。(リンクアグリゲーションしない) AX Serise

FortiGate との接続は、FortiGate の冗長インタフェースを通じておこないます。このため AX スイッチ側では、FortiGate と接続するポートでの冗長設定等は不要です。

3.1.3 UTM 機器(FortiGate)設定時のポイント

(1) 物理インタフェースの設計や設定を最初におこなう。 FortiGate

論理インタフェース(VLAN)や VLAN に関連する設定は、物理インタフェースと紐づいており、論理インタフェースを設定した後に物理インタフェースのみの設定変更はできません。(VLAN の設定を残したまま、その VLAN を割り付ける物理インタフェースを変更するということはできません。一旦その物理インタフェース上の VLAN 設定を全て削除してから、変更先の物理インタフェースを定義し、その上に再度 VLAN を設定しなおすことになります。)

このため、FortiGate に関する構成設計や設定は、まず最初に物理インタフェースの仕様を決めてからおこなうことを推奨します。

(2) HA(冗長クラスタ)のマスタとする装置は、プライオリティ設定値をデフォルトより大きな値とする。 FortiGate

装置を 2 台以上用意して、HA(装置冗長クラスタ)を構成する場合、マスタ/バックアップとなる装置の優先付けとしてプライオリティを設定します。プライオリティは設定値の大きい方が優先されます。

また、プライオリティの低い装置(=バックアップとなる装置)を HA 構成に加えた場合、その装置の設定は自動的にプライオリティのもっとも高い装置(=マスタ)のものと同じに同期されます。このため、マスタとしたい装置のプライオリティはデフォルトの値(=128)より大きく設定することを推奨します。
これにより、新規に装置を HA 構成に加えた場合の設定内容の消失を防げます。

(3) コンフィグ他、各種機能等の設定作業はマスタ装置のみに対しておこなえば良い。 FortiGate

上述の通り、バックアップとする装置(=プライオリティの低い装置)を HA に加えると、その装置の設定内容はマスタの装置と同じものに自動的に設定変更され、マスタ装置において各種機能の設定変更が発生しても同期して同時に設定変更がおこなわれます。

従って、複数台の装置で HA を構成しているケースでも、各種設定の変更作業はマスタ装置に対してのみおこなえば良いです。

(4) HA で監視ポートを使用する際は HA の構成が正しく済んでから設定すること。 FortiGate

HA ではポートのリンク状態でマスタを切り替えることも可能であり、その際の HA 系交替の監視対象となるポートを HA 監視ポートと呼びます。装置交換時など、マスタ以外の装置でこの監視ポートを設定する際は下記のいずれかの方法で設定してください。

- 新規に HA を構築するときは、HA クラスタの構築をし、HA が正しく動作していることを確認してから HA 監視ポートの設定をする。
- 追加する装置に、少なくともマスタ装置と同じ監視ポート設定をしてからマスタ装置に接続する。(予めバックアップしておいた設定を、追加する装置にリストアした後に、HA クラスタへ参加させる)
- マスタ装置に接続する前に、マスタ装置の HA 監視ポートがすべてアップ状態であることを確認する。

5 章の留意事項でも解説していますが、装置交換時などで方法を誤ると最悪の場合、現在運用中のコンフィグが消失してしまうおそれがあります。

(5) AX と接続するポート(物理インタフェース)は冗長インタフェースとする。 FortiGate

FortiGate の持つ機能として、物理ポート(物理インタフェース)に対する冗長機能があり、冗長インタフェースと呼ばれます。AX シリーズスイッチへの接続は、この冗長インタフェースによりおこなう設定とします。

なお冗長インタフェースでアクティブとなるポートのプライオリティは変更できず、番号が若いポートが常に上位のプライオリティとなります。

(6) 必要に応じて管理 VDOM を変更する。 FortiGate

シグネチャのアップデートや snmp trap の送出など、FortiGate 全体の管理に関わる VDOM を管理 VDOM と呼び、デフォルトでは root バーチャルドメインが管理 VDOM となっています。
今回の例では、システム全体の管理用は個別の VRF と独立したネットワーク構成(グローバル VRF を使用)としており、FortiGate 本体の管理もその中でおこなうようにしているため、root バーチャルドメインはグローバル VRF 内にある設定としています。

ですが管理 VDOM を変更すれば、root 以外の VDOM でも FortiGate 全体の管理に関わる役割を持たせることもできます。例えば、VDOM1 の管理者=システム全体の管理者、などであったりする場合は、管理 VDOM を VDOM1 とすることも可能です。

3.1.4 コンフィグレーション例

本構成のコンフィグレーションの例を下記に示します。

(1) コアスイッチ（AX6600S)の設定

C1 (AX6604S)の設定	
スパニングツリーの抑止	
(config)# spanning-tree disable	AX シリーズではデフォルトで PVST+が有効になっており、FT 構成とする場合にはこれを抑止します。
VRF の設定	
(config)# vrf mode l2protocol-disable All CSU will be restarted automatically when the selected mode differs from current mode. Do you wish to change mode (y/n): y (config)# vrf definition 10 (config)# vrf definition 20 (config)# vrf definition 30	VRFをL2 プロトコル併用無しで設定します。(構築ポイント(1)) (CSU 再起動を確認されますので、OK なら'y'を入力) VRF10 を使用することを設定します。 VRF20 を使用することを設定します。 VRF30 を使用することを設定します。
VLAN の設定	
(config)# vlan 2,10,20,31-32,100-101,200-201	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.1 255.255.0.0 (config)# interface vlan 10 (config-if)# vrf forwarding 10 (config-if)# ip address 172.16.0.1 255.255.0.0 (config)# interface vlan 20 (config-if)# vrf forwarding 20 (config-if)# ip address 172.16.0.1 255.255.0.0 (config)# interface vlan 31 (config-if)# vrf forwarding 30 (config)# interface vlan 32 (config-if)# vrf forwarding 30 (config)# interface vlan 100 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.0.1 255.255.255.0 (config)# interface vlan 101 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.1.1 255.255.255.0 (config)# interface vlan 200 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.0.1 255.255.255.0 (config)# interface vlan 201 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.1.1 255.255.255.0	VLAN2 はシステム管理用に global で使用します。 VLAN2 に IP アドレスを設定します。 VLAN10 はVRF10 で使用します。(構築ポイント(2)) VLAN10 に IP アドレスを設定します。 VLAN20 はVRF20 で使用します。(構築ポイント(2)) VLAN20 に IP アドレスを設定します。 VLAN31,VLAN32 は VRF30 で使用しますが、IP アドレスは設定しません。 VLAN100 はVRF10 で使用します。(構築ポイント(2)) VLAN100 に IP アドレスを設定します。 VLAN101 はVRF10 で使用します。(構築ポイント(2)) VLAN101 に IP アドレスを設定します。 VLAN200 はVRF20 で使用します。(構築ポイント(2)) VLAN200 に IP アドレスを設定します。 VLAN201 はVRF20 で使用します。(構築ポイント(2)) VLAN200 に IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface gigabitethernet 4/24 (config-if)# switchport access vlan 2 (config)# interface range tengigabitethernet 1/1, tengigabitethernet 2/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on	ポート 4/24 はシステム管理用に VLAN2 のアクセスポートとします。 ポート 1/1,2/1 は装置 S1 接続用にチャネルグループ 1 を構成します。

C1 (AX6604S)の設定	
(config)# interface range tengigabitethernet 1/3, tengigabitethernet 2/3 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,10,20,31-32	ポート 1/3,2/3 は UTM1 接続用に VLAN2,10,20,31-32 のトランクポートとします。
(config)# interface range tengigabitethernet 1/4, tengigabitethernet 2/4 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,10,20,31-32	ポート 1/4,2/4 は UTM2 接続用に VLAN2,10,20,31-32 のトランクポートとします。
(config)# interface1 range gigabitethernet 3/1, gigabitethernet 4/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 11 mode on	ポート 3/1,4/1 は装置 A1 接続用にチャネルグループ 11 を構成します。
(config)# interface range gigabitethernet 3/2, gigabitethernet 4/2 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 12 mode on	ポート 3/2,4/2 は装置 A2 接続用にチャネルグループ 12 を構成します。
ポートチャネルの設定	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,31-32	ポートチャネル 1 はトランクポートとし VLAN2,10,20,31-32 の転送を許可します。
(config)# interface port-channel 11 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,100-101	ポートチャネル 11 はトランクポートとし VLAN2,100-101 の転送を許可します。
(config)# interface port-channel 12 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,200-201	ポートチャネル 12 はトランクポートとし VLAN2,200-201 の転送を許可します。
デフォルトルートの設定	
(config)# ip route vrf10 0.0.0.0 0.0.0.0 172.16.0.254	VRF10 でのデフォルトルートを設定します。
(config)# ip route vrf20 0.0.0.0 0.0.0.0 172.16.0.254	VRF20 でのデフォルトルートを設定します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

(2) サーバ用アクセススイッチ (AX2430S)の設定

S1 (AX2430S-24T2X)の設定	
スパニングツリーの抑止	
(config)# spanning-tree disable	AXシリーズではデフォルトでPVST+が有効になっており、FT構成とする場合にはこれを抑止します。(構築ポイント(2))
VLAN の設定	
(config)# vlan 2,10,20,31-32	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.5 255.255.0.0	VLAN2 はシステム管理用に global で使用します。 VLAN2 に IP アドレスを設定します。

S1 (AX2430S-24T2X)の設定	
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range tengigabitethernet 0/25-26 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on (config)# interface range gigabitethernet 0/5-8 (config-if-range)# switchport access vlan 10 (config)# interface range gigabitethernet 0/9-12 (config-if-range)# switchport access vlan 20 (config)# interface gigabitethernet 0/20 (config-if)# switchport access vlan 31 (config)# interface gigabitethernet 0/22 (config-if)# switchport access vlan 32	ポート 0/25-26 は装置 C1 接続用にチャネルグループ 1 を構成します。 ポート 0/5-8 は会社 A サーバ接続用に VLAN10 のアクセスポートとして構成します。 ポート 0/9-12 は会社 B サーバ接続用に VLAN20 のアクセスポートとして構成します。 ポート 0/20 は会社 A 外部接続用に VLAN31 のアクセスポートとして構成します。 ポート 0/22 は会社 B 外部接続用に VLAN32 のアクセスポートとして構成します。
ポートチャネルの設定	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,31-32	ポートチャネル 1 はトランクポートとし VLAN2,10,20,31-32 の転送を許可します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

(3) 端末 PC 用アクセススイッチ (AX1240S)の設定

A1 (AX1240S-24T2C)の設定	
スパニングツリーの抑止	
(config)# spanning-tree disable	AX シリーズではデフォルトで PVST+が有効となっていますが、FT 構成とする場合はこれを抑止します。
VLAN の設定	
(config)# vlan 2,100-101	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.1.1 255.255.0.0	VLAN2 をシステム管理用に使用するため、装置の IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range gigabitethernet 0/25-26 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 11 mode on (config)# interface range fastethernet 0/1-12 (config-if-range)# switchport access vlan 100 (config)# interface fastethernet 0/13-24 (config-if-range)# switchport access vlan 101	ポート 0/25-26 は装置 C1,C2 接続用にチャネルグループ 11 を構成します。 VLAN2,100-101 のトランクポートとして構成します。 ポート 0/1-12 は会社 A 端末 PC のセグメント 1 接続用に VLAN100 のアクセスポートとして構成します。 ポート 0/13-24 は会社 A 端末 PC のセグメント 2 接続用に VLAN101 のアクセスポートとして構成します。
ポートチャネルの設定	
(config)# interface port-channel 11 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,100-101	ポートチャネル 11 はトランクポートとし VLAN2,100-101 の転送を許可します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

装置 B1 の設定は使用する VLAN ID と装置アドレスが異なる以外は装置 A1 の設定と同様です。
(VLAN：100-101→200-201、装置アドレス：172.255.1.1→172.255.2.1)

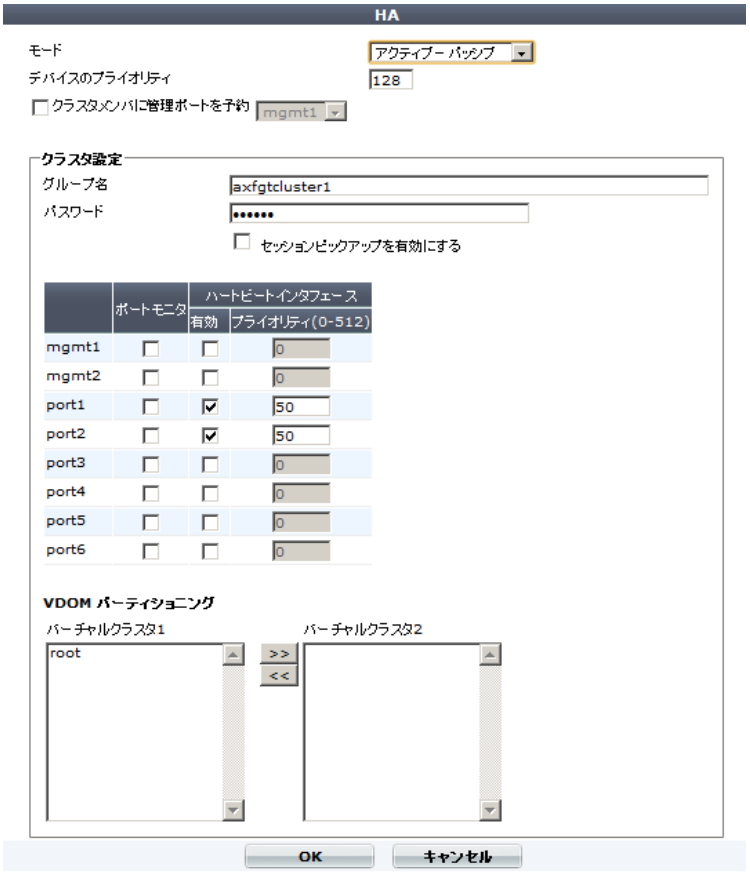
(4) UTM (FortiGate)の設定

FortiGate にて HA 構成を組む場合、マスタとする装置にて基本的な設定をおこなっておきます。

UTM1 (FortiGate-3950B)の設定

HA(冗長)クラスタの設定

CLI	GUI

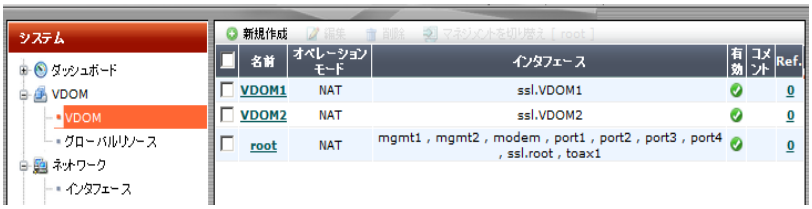
config system ha
  set mode a-p
  set group-name axfgcluster1
  set password secret123
  set hbdev port1 50 port2 50
  set priority 130
end
	システム＞設定＞HA
	[モード] アクティブ-パッシブ
	[デバイスのプライオリティ] 130　*装置のプライオリティ(大きい方が高優先)*
	[グループ名] axfgcluster1　*任意のグループ名*
	[パスワード] secret123　*任意の推察されにくいパスワード*
	[ハートビートインタフェース]
	[port1] 有効をチェック [プライオリティ] 50
	[port2] 有効をチェック [プライオリティ] 50
	<OK>
	 

VDOM の作成

config system global set vdom-admin enable end You will be logged out for the operation to take effect Do you want to continue? (y/n)y	システム＞ダッシュボード＞Status [システムステータスウィジェット] バーチャルドメイン [有効]をクリック 

```
config vdom
  edit VDOM1
  next
  edit VDOM2
end
```

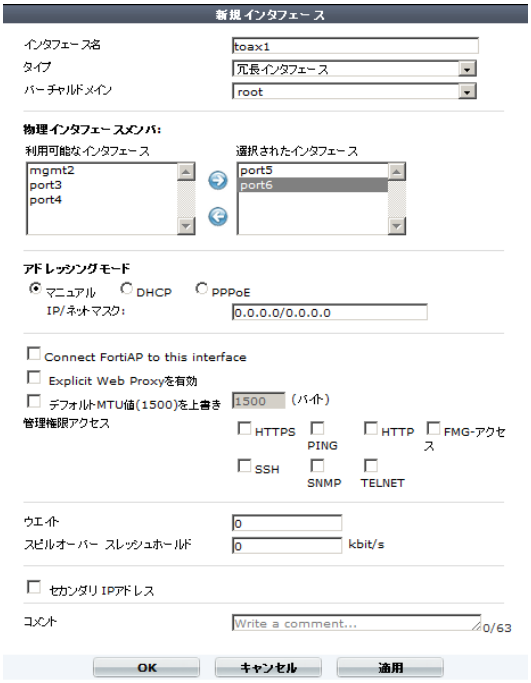
システム＞VDOM＞VDOM＞新規作成
[名前] VDOM1
[オペレーションモード] NAT
〈OK〉
同様に VDOM2 を作成する。



インタフェースの設定（冗長インタフェース）

```
config global
  config system interface
    edit toax1
    set vdom root
    set type redundant
    set member port5 port6
  end
end
```

システム＞ネットワーク＞インタフェース＞新規作成
[インタフェース名] toax1
[タイプ] 冗長インタフェース
[バーチャルドメイン] root
[物理インタフェースメンバ][選択されたインタフェース] port5 port6
〈OK〉



VLAN の設定

```
config global
config system interface
  edit vlan10
    set vdom VDOM1
    set ip 172.16.0.254/16
    set allowaccess ping
    set interface toax1
    set vlanid 10
  next
  edit vlan20
    set vdom VDOM2
    set ip 172.16.0.254/16
    set allowaccess ping
    set interface toax1
    set vlanid 20
  next
  edit vlan31
    set vdom VDOM1
    set ip 10.10.1.254/24
(グローバルアドレスを 10.10.1.254、
10.20.2.254 として例示)
    set interface toax1
```

システム＞ネットワーク＞インタフェース＞新規作成
[インタフェース名] vlan10
[タイプ] VLAN
[インタフェース] toax1
[VLAN ID] 10
[バーチャルドメイン] VDOM1
[IP/ネットマスク] 172.16.0.254/16
[管理権限アクセス] PING にチェック

同様に VLAN20,VLAN31,VLAN32 を作成する。
(グローバルアドレスを 10.10.1.254、10.20.2.254 として例示)

```
    set vlanid 31
  next
  edit vlan32
    set vdom VDOM2
    set ip 10.20.2.254/24
    set interface "toax1"
    set vlanid 32
end
end
```

VDOM1 の設定

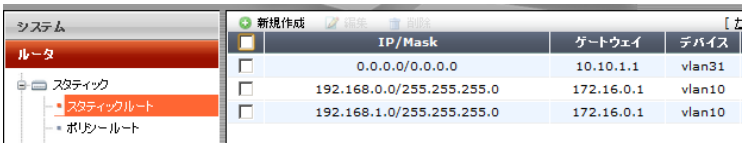
デフォルトルートとスタティックルートの設定

```
config vdom
edit VDOM1
config router static
  edit 0
    set device vlan31
    set gateway 10.10.1.1 グローバルアドレスを 10.10.1.1 として例示
  next
  edit 0
    set device vlan10
    set dst 192.168.0.0/24
    set gateway 172.16.0.1
  next
  edit 0
    set device vlan10
    set dst 192.168.1.0/24
    set gateway 172.16.0.1
end
end
```

現在の VDOM＞VDOM1
ルータ＞スタティック＞スタティックルート＞新規作成
[宛先 IP/ネットマスク] 0.0.0.0/0.0.0.0
[デバイス] vlan31
[ゲートウェイ] 10.10.1.1 *グローバルアドレスを 10.10.1.1 として例示*
<OK>

続いてもう一度
ルータ＞スタティック＞スタティックルート から 新規作成
[宛先 IP/ネットマスク] 192.168.0.0/24
[デバイス] vlan10
[ゲートウェイ] 172.16.0.1
<OK>

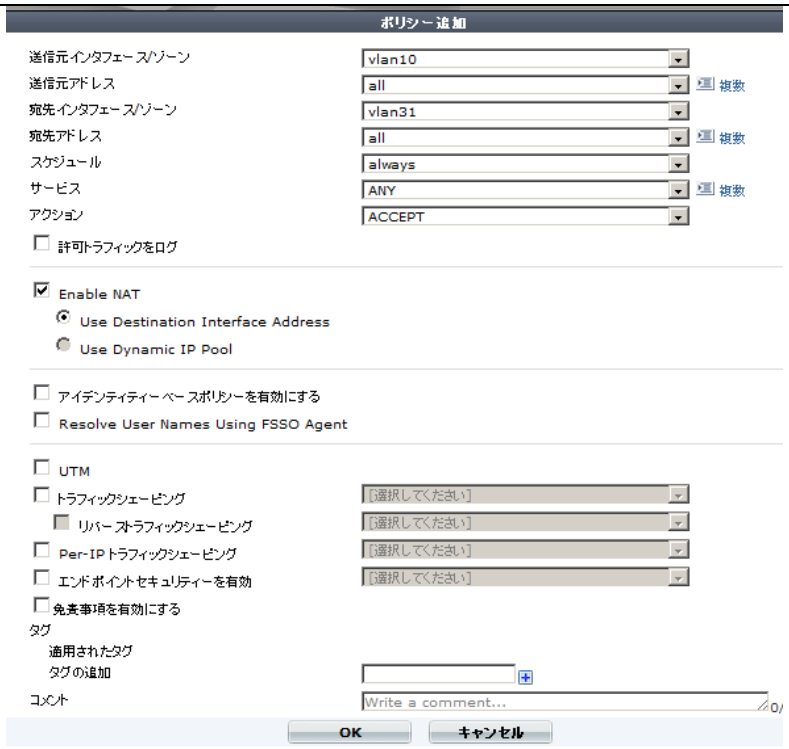
同様に、192.168.1.0/24 へのスタティックルートを追加する。



ファイアウォール設定例(NAT ポリシの追加)

```
config vdom
edit VDOM1
config firewall policy
edit 0
  set srcintf vlan10
  set dstintf vlan31
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
  set nat enable
end
end
```

現在の VDOM＞VDOM1
ファイアウォール＞ポリシー＞ポリシー＞新規作成
[送信元インタフェース/ゾーン] vlan10
[送信元アドレス] all
[宛先インタフェース/ゾーン] vlan31
[宛先アドレス] all
[スケジュール] always
[サービス] ANY
[アクション] ACCEPT
[Enable NAT] チェック [Use Destination Interface Address ラジオボタン] ON
<OK>



VDOM2 の設定

デフォルトルートとスタティックルートの設定

```
config vdom
edit VDOM2
config router static
  edit 0
    set device vlan32
    set gateway 10.20.2.1 グローバルアドレスを 10.20.2.1 として例示
  next
  edit 0
    set device vlan20
    set dst 192.168.0.0/24
    set gateway 172.16.0.1
  next
  edit 0
    set device vlan20
    set dst 192.168.1.0/24
    set gateway 172.16.0.1
end
end
```

現在の VDOM＞VDOM2
ルータ＞スタティック＞スタティックルート＞新規作成
[宛先 IP/ネットマスク] 0.0.0.0/0.0.0.0
[デバイス] vlan32
[ゲートウェイ] 10.20.2.1 *グローバルアドレスを 10.20.2.1 として例示*
<OK>

続いてもう一度
ルータ＞スタティック＞スタティックルート から 新規作成
[宛先 IP/ネットマスク] 192.168.0.0/24
[デバイス] vlan20
[ゲートウェイ] 172.16.0.1
<OK>

同様に、192.168.1.0/24 へのスタティックルートを追加する。

ファイアウォール設定例(NAT ポリシの追加)

```
config vdom
edit VDOM2
config firewall policy
edit 0
  set srcintf vlan20
  set dstintf vlan32
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
  set nat enable
end
end
```

現在の VDOM＞VDOM2
ファイアウォール＞ポリシー＞ポリシー＞新規作成
[送信元インタフェース/ゾーン] vlan20
[送信元アドレス] all
[宛先インタフェース/ゾーン] vlan32
[宛先アドレス] all
[スケジュール] always
[サービス] ANY
[アクション] ACCEPT
[Enable NAT] チェック [Use Destination Interface Address ラジオボタン] ON
<OK>

管理 VDOM の変更（必要に応じて）	
config global config system global set management-vdom *VDOM 名* end end	現在の VDOM＞グローバル システム＞VDOM＞ 管理 VDOM にしたい VDOM 名左隅のチェックボックスをチェック [マネジメントを切り替え]アイコンをクリック
設定のバックアップ	
config global exec backup config ftp master.conf *サーバ IP アドレス ユーザー ID パスワード*	現在の VDOM＞グローバル システム＞ダッシュボード＞Status>システムステータスウィジェット [システムコンフィグレーション]の[バックアップ]をクリック

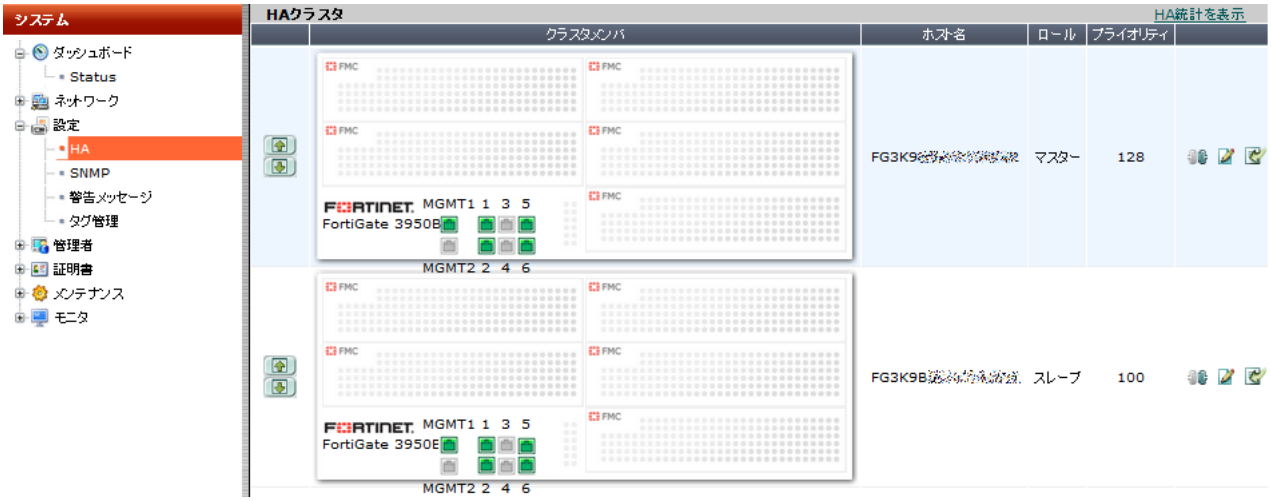
続いて、バックアップとして使用する装置の設定をマスタ装置と接続する前に以下のように設定します。

UTM2 (FortiGate-3950B)の設定	
HA(冗長)クラスタの設定	
CLI	**GUI**
config system ha set mode a-p set group-name axfgcluster1 set password secret123 set hbdev port1 50 port2 50 set priority 100 end	システム＞設定＞HA [モード] アクティブ-パッシブ [デバイスのプライオリティ] 100 *UTM1 に設定した値より小さく* [グループ名] axfgcluster1 *UTM1 に設定したグループ名と同じもの* [パスワード] secret123 *UTM1 に設定したパスワードと同じもの* [ハートビートインタフェース] [port1] 有効をチェック [プライオリティ] 50 *port1 と* [port2] 有効をチェック [プライオリティ] 50 *port2 を使用* <OK>

バックアップ装置での以上の設定終了後、マスタ装置へ接続、続いてネットワークに接続します。

HA の確認は以下の通りです。
正しく動作している場合、マスタ側、バックアップ側、どちらの装置でも同じ結果が得られます。

GUI の場合
システム＞設定＞HA



CLI の場合

```
# config global
(global) # get system ha status
Model: 3950
Mode: a-p
Group: 32
Debug: 0
ses_pickup: disable
Master:128 FG3K9B3X00000001 FG3K9B3X00000001 0
Slave :100 FG3K9B3X00000002 FG3K9B3X00000002 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG3K9B3X00000001
Slave :1 FG3K9B3X00000002
```

バックアップ側の装置については、マスタ側の装置でおこなった設定をおこなう必要はありません。HA のバックアップと認識された時点で、マスタで設定した内容がそのままバックアップ側にコピーされます。

続いて、マスタ側の装置に接続し、HA 監視ポートの設定をします。設定はバックアップ側に同期されます。

HA監視ポート設定 （構築ポイント(4)）

```
config global
config system ha
  set monitor toax1
end
end
```

システム＞設定＞HA

マスタ状態の装置の編集 アイコンクリック

[ポートモニタ] toax1 をチェック

<OK>をクリック

3.2 組織単位に分割管理する場合の適用例（STP+VRRP + FortiGate HA）

企業など、既にネットワークを一つの大きな単位で使用しているケースで、1 章での解説のようにセキュリティ管理を強化するために、ネットワークの単位を組織ごとに細分化する例について解説します。

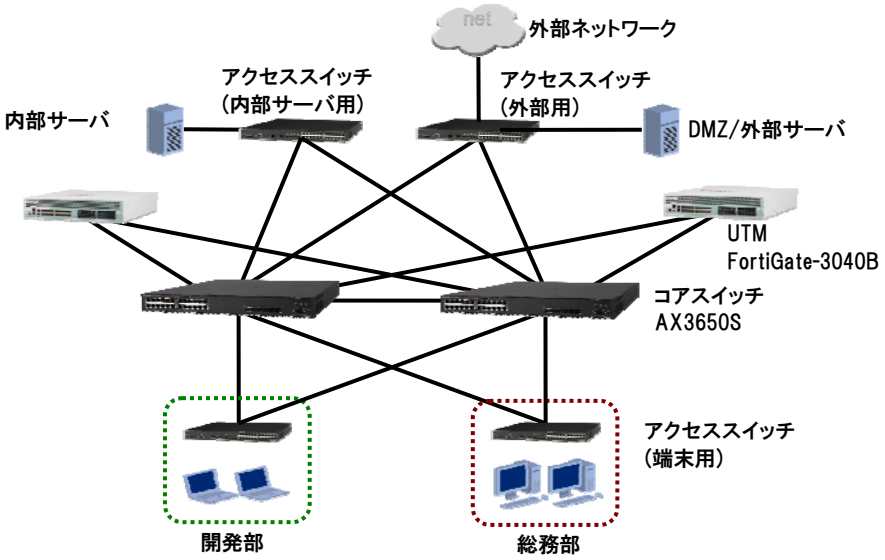


図 3.2-1 部門別仮想ネットワーク物理構成

物理構成は以上のように単一のシステムを構成した場合とほとんど変わらない構成となります。しかしながら、仮想ネットワークを含めた論理的なネットワーク構成は以下の通りとなります。ファイアウォールについては、FortiGate を冗長構成で使用しネットワークのコア部分に組み込む形となります。

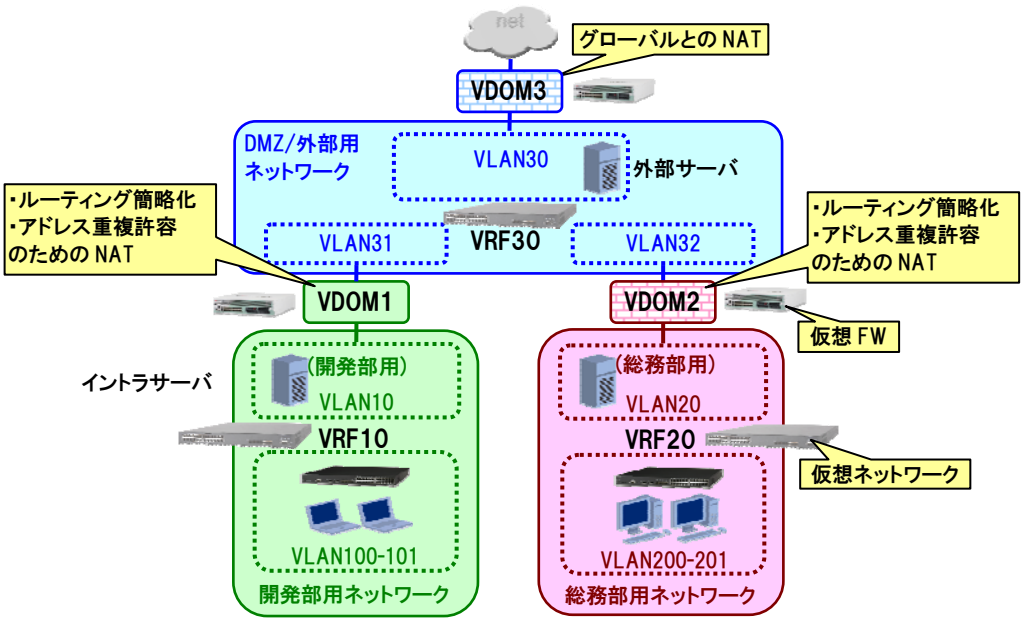
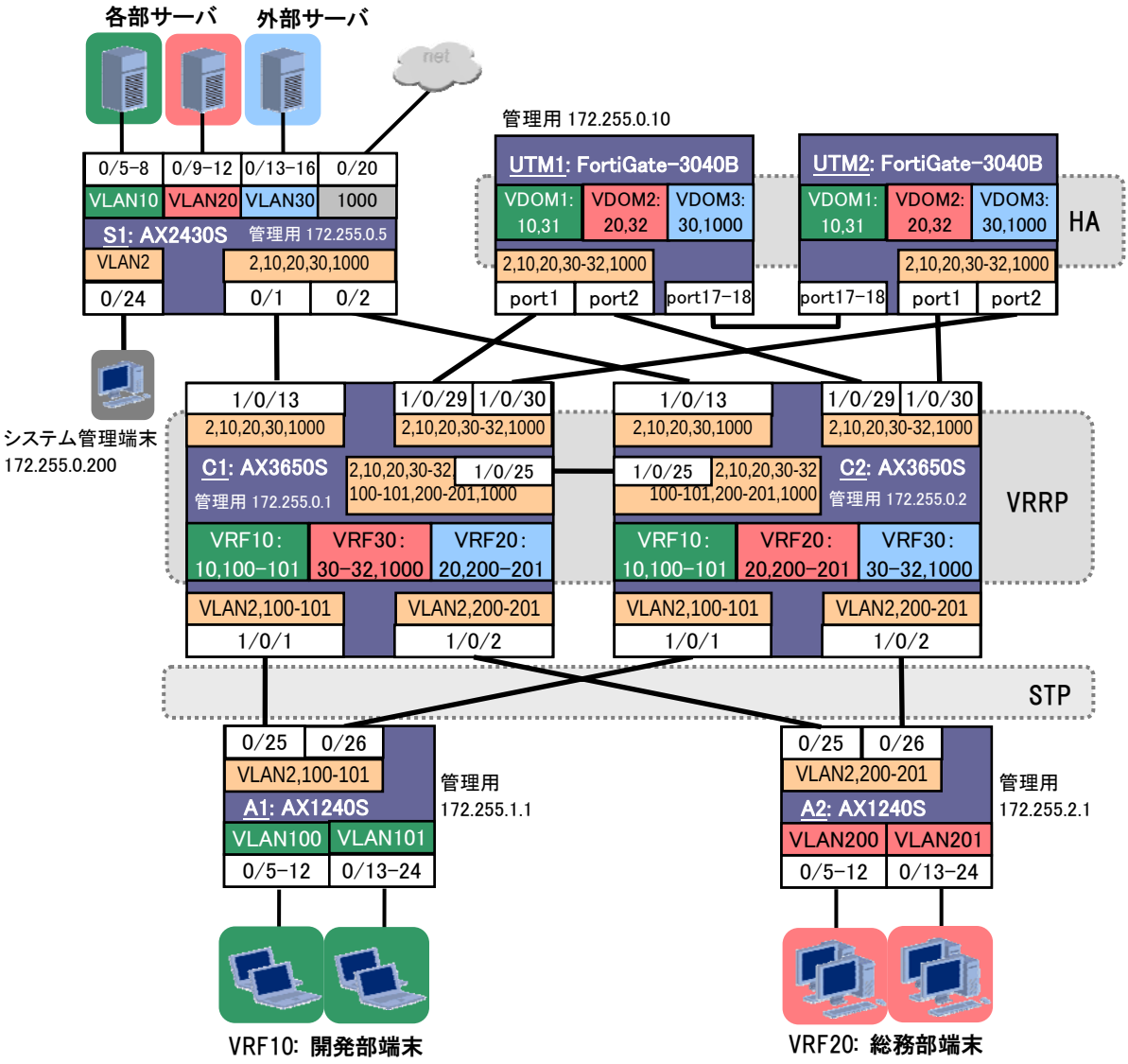


図 3.2-2 部門別仮想ネットワーク論理構成

ネットワーク・パーティション(VRF)による仮想ネットワークにて、開発部、総務部それぞれを独立した L3 ネットワークとし、また DMZ として使用する外部接続用のセグメントも仮想ネットワークとして、独立したネットワークとします。そしてそれぞれを仮想ファイアウォール(VDOM)にて橋渡しするように構成します。

これにより、開発部および総務部それぞれ独立したネットワークでの構成となり、また各部門の脅威管理(アンチウイルス、IPS、各種フィルタ)を含めたアクセス管理も各 VDOM で独立しておこなうことが可能となります。

また、装置個別の設定を反映した論理構成は以下の通りとなります。



用途	VDOM	VRF ID	VLAN ID	IP アドレス
外部接続用	VDOM3	30	1000	10.10.1.0/24 (外部)
			30	172.16.30.0/24
開発-外部接続用	VDOM1		31	172.16.31.0/24
開発部サーバ/Uplink 用		10	10	172.16.10.0/24
開発部端末 PC 用	-		100-101	192.168.0-1.0/24
総務-外部接続用	VDOM2	30	32	172.16.32.0/24
総務部サーバ/Uplink 用		20	20	172.16.20.0/24
総務部端末 PC 用	-		200-201	192.169.0-1.0/24
システム総合管理用	-	global	2	172.255.0.0/16

図 3.2-3 部門別仮想ネットワーク 論理設定詳細

3.2.1 システム構築時のポイント

本例の構成を設計する際におけるポイントを以下に示します。

(1) コアスイッチ、UTM 各装置の要求性能や収容条件は、もとのシステムで使用の装置と同等で良い。

今回の構成のように、もととなるネットワークで VLAN にてセグメント分けしていた部分を、仮想ネットワークで置き換えるといった構成とする場合、ネットワーク全体の収容条件はもとのネットワークとほとんど変わらないこととなります。従って使用する装置の選定に関しては、もとのネットワークで使用していた装置の収容条件と同等と考えることができます。

(2) 可用性の確保は STP+VRRP 構成を基本とするが、UTM(FortiGate)は HA(冗長クラスタ)構成。

コアスイッチが AX3650S などボックス型である場合、障害などに対する可用性の確保のために 2 台使用してスパニングツリーと VRRP を組み合わせた構成を基本として構築します。FortiGate も同様に 2 台以上を用意しますがこちらは同装置の持つ装置冗長構成の機能である HA を用います。

(3) コアスイッチと UTM 間は FortiGate の冗長インタフェースを使用。

コアスイッチと UTM(FortiGate)間の接続については、スパニングツリーではなく FortiGate の持つ機能である冗長インタフェースを用いて回線の可用性を確保します。

(4) 各 VDOM で NAT を使用すれば、IP アドレスの重複も可能。

VDOM は仮想のファイアウォールとして機能しますが、VDOM では NAT も独立して機能します。このため、各部門で使用する IP アドレスを重複させることが可能です。

また、部門ごとの仮想ネットワークが接続される外部接続用の仮想ネットワーク内でのルーティングテーブルも簡略化することが可能です。

ただし、同じ FortiGate で NAT を複数回繰り返すことになり、システムでの転送性能の上限値が小さくなるとかレイテンシが大きくなるなど、システム全体のパフォーマンスに影響するので注意が必要です。

(5) FortiGate はインターネットと接続できるパスを設ける。

FortiGate のライセンス管理や各種フィルタ機能で使用されるパターンファイル、シグネチャ等の更新などは外部にある Fortinet の専用サーバを通しておこないます。従って FortiGate はインターネット接続できる環境下に置く必要があります。

3.2.2 スイッチ機器(AX シリーズ)設定時のポイント

コンフィグなど、機器の設定の際のポイントを以下に示します。

(1) ボックス型(AX3650S)で VRF を使用する場合、モードの設定は不要 AX Serise

AX3650S で VRF 機能を使用する場合、VRF モードの設定は不要です。また VRF モード設定に伴うスイッチング機構の再起動等もありません。

(2) STP は rapid-pvst を使用する。 AX Serise

AX シリーズのスイッチでは、デフォルトで PVST+の STP が動作していますが、障害時の系切替が高速な Rapid PVST+での使用を推奨します。

(3) VLAN インタフェースでの設定は最初に所属 VRF の設定からおこなう。 AX Serise

VLAN インタフェースでは、所属 VRF の設定と IP アドレスの設定が必要ですが、所属 VRF の設定は IP アドレスの設定前におこなう必要があります。(IP アドレスが設定されている状態では所属 VRF の設定はできません。)
ですので、VLAN インタフェースの設定では所属 VRF の設定を最初におこなってください。

(4) FortiGate と接続するポートは STP 対象外とする。PC やサーバを接続するポートについても同様 AX Serise

FortiGate と接続する回線の可用性確保には、FortiGate の機能である冗長インタフェースを使用するため、FortiGate と接続する AX スイッチ側のポートに対しては STP 対象外の設定(portfast 設定)とします。

(5) PC やサーバを接続するポートについても STP 対象外とする。 AX Serise

PC やサーバなど、STP に関与しない装置を接続するポートについても、STP 対象外の設定(portfast 設定)とします。タグ付き VLAN を扱うトランクポートの場合は trunk 指定を忘れないようにしてください。

3.2.3 UTM 機器(FortiGate)設定時のポイント

同様に、FortiGate の設定におけるポイントを以下に示します。

(1) 物理インタフェースの設計や設定を最初におこなう。 FortiGate

論理インタフェース(VLAN)や VLAN に関連する設定は、物理インタフェースと紐づいており、論理インタフェースを設定した後に物理インタフェースのみの設定変更はできません。(VLAN の設定を残したまま、その VLAN を割り付ける物理インタフェースを変更するということはできません。一旦その物理インタフェース上の VLAN 設定を全て削除してから、変更先の物理インタフェースを定義し、その上に再度 VLAN を設定しなおすことになります。)

このため、FortiGate に関する構成設計や設定は、まず最初に物理インタフェースの仕様を決めてからおこなうことを推奨します。

(2) HA のマスタとする装置は、プライオリティ設定値をデフォルトより大きな値とする。 FortiGate

FortiGate を 2 台以上用意して、HA(装置冗長クラスタ)を構成する場合、マスタ/バックアップとなる装置の優先付けとしてプライオリティを設定します。プライオリティは設定値の大きい方が優先されます。

また、プライオリティの低い装置(=バックアップとなる装置)を HA 構成に加えた場合、その装置の設定は自動的にプライオリティのもっとも高い装置(=マスタ)のものと同じに同期されます。このため、マスタとしたい装置のプライオリティはデフォルトの値(=128)より大きく設定することを推奨します。
これにより、新規に装置を HA 構成に加えた場合の設定内容の消失を防げます。

(3) コンフィグ他、各種機能等の設定作業はマスタ装置のみに対しておこなえば良い。 FortiGate

上述の通り、バックアップとする装置(=プライオリティの低い装置)を HA に加えると、その装置の設定内容はマスタの装置と同じものに自動的に設定変更され、マスタの装置において各種機能の設定変更が発生しても同期して同時に設定変更がおこなわれます。

従って、複数台の装置で HA を構成しているケースでも、各種設定の変更作業はマスタの装置に対してのみおこなえば良いです。

(4) HA で監視ポートを使用する際は HA の構成が正しく済んでから設定すること。 FortiGate

HA ではポートのリンク状態でマスタを切り替えることも可能であり、その際の HA 系交替の監視対象となるポートを HA 監視ポートと呼びます。装置交換時など、マスタ以外の装置でこの監視ポートを設定する際は下記のいずれかの方法で設定してください。

- 新規に HA を構築するときは、HA クラスタの構築をし、HA が正しく動作していることを確認してから HA 監視ポートの設定をする。
- 追加する装置に、少なくともマスタ装置と同じ監視ポート設定をしてからマスタ装置に接続する。(予めバックアップしておいた設定を、追加する装置にリストアした後に、HA クラスタへ参加させる)
- マスタ装置に接続する前に、マスタ装置の HA 監視ポートがすべてアップ状態であることを確認する。

5 章 留意事項でも解説していますが、装置交換時などで方法を誤ると最悪の場合、現在運用中のコンフィグが消失してしまうおそれがあります。

(5) AX と接続するポート(物理インタフェース)は冗長インタフェースとする。 FortiGate

FortiGate の持つ機能として、物理ポート(物理インタフェース)に対する冗長機能があり、冗長インタフェースと呼ばれます。AX シリーズスイッチへの接続は、この冗長インタフェースによりおこなう設定とします。

なお冗長インタフェースでアクティブとなるポートのプライオリティは変更できず、番号が若いポートが常に上位のプライオリティとなります。

(6) 必要に応じて管理 VDOM の変更も可能 FortiGate

シグネチャのアップデートや snmp trap の送出など、FortiGate 全体の管理に関わる VDOM を管理 VDOM と呼び、デフォルトでは root バーチャルドメインが管理 VDOM となっています。
今回の例では、システム全体の管理用は個別の VRF と独立したネットワーク構成(グローバル VRF を使用)としており、FortiGate 本体の管理もその中でおこなうようにしているため、root バーチャルドメインはグローバル VRF 内にある設定としています。

ですが管理 VDOM を変更すれば、root 以外の VDOM でも FortiGate 全体の管理に関わる役割を持たせることもできます。例えば、VDOM1 の管理者=システム全体の管理者、などであったりする場合は、管理 VDOM を VDOM1 とすることも可能です。

3.2.4 コンフィグレーション例

本構成のコンフィグレーションの例を下記に示します。

(1) コアスイッチ（AX3650S)の設定

C1 (AX3650S-24T6XW)の設定

スパニングツリーの設定

```
(config)# spanning-tree mode rapid-pvst
```

スパニングツリーのモードを Rapid PVST+に設定します。
(構築ポイント(2))

VRF の設定

```
(config)# vrf definition 10
(config)# vrf definition 20
(config)# vrf definition 30
```

VRF10,20,30 を使用することを設定します。(構築ポイント(1))

VLAN の設定

```
(config)# vlan 2,10,20,30-32,100-101,200-201,1000
```

使用する VLAN の設定をおこないます。

VLAN インタフェースの設定

```
(config)# interface vlan 2
(config-if)# ip address 172.255.0.1 255.255.0.0
```

VLAN2 はシステム管理用に VRF を設定せず使用します。
VLAN2 に装置の IP アドレスを設定します。

```
(config)# interface vlan 10
(config-if)# vrf forwarding 10
(config-if)# ip address 172.16.10.1 255.255.255.0
(config-if)# vrrp 10 ip 172.16.10.1
```

VLAN10 はVRF10 で使用します。(構築ポイント(3))
VLAN10 に IP アドレスを設定します。
VLAN10 に VRRP の仮想 IP アドレスを設定します。

```
(config)# interface vlan 20
(config-if)# vrf forwarding 20
(config-if)# ip address 172.16.20.1 255.255.255.0
(config-if)# vrrp 20 ip 172.16.20.1
```

VLAN20 はVRF20 で使用します。(構築ポイント(3))
VLAN20 に IP アドレスを設定します。
VLAN20 に VRRP の仮想 IP アドレスを設定します。

```
(config)# interface vlan 30
(config-if)# vrf forwarding 30
(config-if)# ip address 172.16.30.1 255.255.255.0
(config-if)# vrrp 30 ip 172.16.30.1
```

VLAN100 はVRF10 で使用します。(構築ポイント(3))
VLAN100 に IP アドレスを設定します。
VLAN100 に VRRP の仮想 IP アドレスを設定します。

```
(config)# interface vlan 31
(config-if)# vrf forwarding 30
(config-if)# ip address 172.16.31.1 255.255.255.0
(config-if)# vrrp 31 ip 172.16.31.1
```

VLAN101 はVRF10 で使用します。(構築ポイント(3))
VLAN101 に IP アドレスを設定します。
VLAN101 に VRRP の仮想 IP アドレスを設定します。

```
(config)# interface vlan 32
(config-if)# vrf forwarding 30
(config-if)# ip address 172.16.32.1 255.255.255.0
(config-if)# vrrp 32 ip 172.16.32.1
```

VLAN200 はVRF20 で使用します。(構築ポイント(3))
VLAN200 に IP アドレスを設定します。
VLAN200 に VRRP の仮想 IP アドレスを設定します。

```
(config)# interface vlan 100
(config-if)# vrf forwarding 10
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# vrrp 100 ip 192.168.0.1
```

VLAN201 はVRF20 で使用します。(構築ポイント(3))
VLAN201 に IP アドレスを設定します。
VLAN201 に VRRP の仮想 IP アドレスを設定します。

```
(config)# interface vlan 101
(config-if)# vrf forwarding 10
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# vrrp 101 ip 192.168.1.1
```

VLAN1000 は VRF30 で使用しますが、IP アドレスは設定しません。

```
(config)# interface vlan 200
(config-if)# vrf forwarding 20
(config-if)# ip address 192.169.0.1 255.255.255.0
(config-if)# vrrp 200 ip 192.169.0.1

(config)# interface vlan 201
(config-if)# vrf forwarding 20
(config-if)# ip address 192.169.1.1 255.255.255.0
(config-if)# vrrp 201 ip 192.169.1.1

(config)# interface vlan 1000
(config-if)# vrf forwarding 30
```

C1 (AX3650S-24T6XW)の設定	
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface gigabitethernet 1/0/1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,100-101 (config)# interface gigabitethernet 1/0/2 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,200-201 (config)# interface gigabitethernet 1/0/13 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,30,1000 (config)# interface tengigabitethernet 1/0/25 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,30-32,100-101,200-201,1000 (config)# interface range tengigabitethernet 1/0/29-30 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,10,20,30-32,1000 (config-if-range)# spanning-tree portfast trunk	ポート 2/24 はシステム管理用に VLAN2 のアクセスポートとします。 ポート 1/0/1 は装置 A1 接続用に VLAN2,100-101 を扱うトランクポート(タグ付 VLAN を扱うポート)を構成します。 ポート 1/0/2 は装置 A2 接続用に VLAN2,200-201 を扱うトランクポート(タグ付 VLAN を扱うポート)を構成します。 ポート 1/0/13 は装置 S1 接続用に VLAN2,10,20,30,1000 を扱うトランクポート(タグ付 VLAN を扱うポート)を構成します。 ポート 1/0/25 は装置 C2 との接続用に VLAN2,10,20,30-32,100-101,200-201,1000 を扱うトランクポート(タグ付 VLAN を扱うポート)を構成します。 ポート 1/0/29 と 1/0/30 は UTM の接続用に VLAN2,10,20,30-32,1000 を扱うトランクポート(タグ付 VLAN を扱うポート)を構成します。 但しスパニングツリーの対象外ポートとするため、portfast設定としておきます。(構築ポイント(4))
デフォルトルートの設定	
(config)# ip route vrf10 0.0.0.0 0.0.0.0 172.16.10.254 (config)# ip route vrf20 0.0.0.0 0.0.0.0 172.16.20.254 (config)# ip route vrf30 0.0.0.0 0.0.0.0 172.16.30.254	VRF10 でのデフォルトルートを設定します。 VRF20 でのデフォルトルートを設定します。 VRF30 でのデフォルトルートを設定します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

装置 C2 は、VLAN に与える IP アドレスが異なる以外は装置 C1 での設定と同様です。

C2 (AX3650S-24T6XW)の設定（装置 C1 との相違点のみ）	
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.2 255.255.0.0	VLAN2 はシステム管理用に VRF を設定せず使用します。 VLAN2 に装置の IP アドレスを設定します。
(config)# interface vlan 10 (config-if)# vrf forwarding 10 (config-if)# ip address 172.16.10.2 255.255.255.0 (config-if)# vrrp 10 ip 172.16.10.1	VLAN10 はVRF10 で使用します。(構築ポイント(3)) VLAN10 に IP アドレスを設定します。 VLAN10 に VRRP の仮想 IP アドレスを設定します。
(config)# interface vlan 20 (config-if)# vrf forwarding 20 (config-if)# ip address 172.16.20.2 255.255.255.0 (config-if)# vrrp 20 ip 172.16.20.1	VLAN20 はVRF20 で使用します。(構築ポイント(3)) VLAN20 に IP アドレスを設定します。 VLAN20 に VRRP の仮想 IP アドレスを設定します。
(config)# interface vlan 30 (config-if)# vrf forwarding 30 (config-if)# ip address 172.16.30.2 255.255.255.0 (config-if)# vrrp 30 ip 172.16.30.1	VLAN100 はVRF10 で使用します。(構築ポイント(3)) VLAN100 に IP アドレスを設定します。 VLAN100 に VRRP の仮想 IP アドレスを設定します。
(config)# interface vlan 31 (config-if)# vrf forwarding 30 (config-if)# ip address 172.16.31.2 255.255.255.0 (config-if)# vrrp 31 ip 172.16.31.1	VLAN101 はVRF10 で使用します。(構築ポイント(3)) VLAN101 に IP アドレスを設定します。 VLAN101 に VRRP の仮想 IP アドレスを設定します。
(config)# interface vlan 32 (config-if)# vrf forwarding 30 (config-if)# ip address 172.16.32.2 255.255.255.0 (config-if)# vrrp 32 ip 172.16.32.1	VLAN200 はVRF20 で使用します。(構築ポイント(3)) VLAN200 に IP アドレスを設定します。 VLAN200 に VRRP の仮想 IP アドレスを設定します。
(config)# interface vlan 100 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.0.2 255.255.255.0 (config-if)# vrrp 100 ip 192.168.0.1	VLAN201 はVRF20 で使用します。(構築ポイント(3)) VLAN201 に IP アドレスを設定します。 VLAN201 に VRRP の仮想 IP アドレスを設定します。
(config)# interface vlan 101 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.1.2 255.255.255.0 (config-if)# vrrp 101 ip 192.168.1.1	VLAN1000 は VRF30 で使用しますが、IP アドレスは設定しません。
(config)# interface vlan 200 (config-if)# vrf forwarding 20 (config-if)# ip address 192.169.0.2 255.255.255.0 (config-if)# vrrp 200 ip 192.169.0.1	
(config)# interface vlan 201 (config-if)# vrf forwarding 20 (config-if)# ip address 192.169.1.2 255.255.255.0 (config-if)# vrrp 201 ip 192.169.1.1	
(config)# interface vlan 1000 (config-if)# vrf forwarding 30	

(2) サーバ用アクセススイッチ（AX2430S)の設定

S1 (AX2430S-24T)の設定	
スパニングツリーの設定	
(config)# spanning-tree mode rapid-pvst	スパニングツリーのモードを rapid-pvst に設定します。
VLAN の設定	
(config)# vlan 2,10,20,30,1000	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.5 255.255.0.0	VLAN2 はシステム管理用に global で使用します。 VLAN2 に IP アドレスを設定します。

S1 (AX2430S-24T)の設定	
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,10,20,30,1000 (config)# interface range gigabitethernet 0/5-8 (config-if-range)# switchport access vlan 10 (config-if-range)# spanning-tree portfast (config)# interface range gigabitethernet 0/9-12 (config-if-range)# switchport access vlan 20 (config-if-range)# spanning-tree portfast (config)# interface range gigabitethernet 0/13-16 (config-if-range)# switchport access vlan 30 (config-if-range)# spanning-tree portfast (config)# interface gigabitethernet 0/20 (config-if)# switchport access vlan 1000 (config-if)# spanning-tree portfast (config)# interface gigabitethernet 0/24 (config-if)# switchport access vlan 2 (config-if)# spanning-tree portfast	ポート 0/1-2 は装置 C1,C2 接続用に VLAN2,10,20,30,1000 のトランクポートとして構成します。 ポート 0/5-8 は開発部ローカルサーバ接続用に VLAN10 のアクセスポートとして構成します。 サーバ接続用のため、STP 対象外(portfast 設定)とします。 ポート 0/9-12 は総務部ローカルサーバ接続用に VLAN20 のアクセスポートとして構成します。 端末 PC 接続用のため STP 対象外(portfast 設定)とします。 ポート 0/13-16 は外部公開サーバ接続用に VLAN30 のアクセスポートとして構成します。 端末 PC 接続用のため STP 対象外(portfast 設定)とします。 ポート 0/20 は外部接続用に VLAN1000 のアクセスポートとして構成します。また STP 対象外(portfast 設定)とします。 ポート 0/24 はシステム管理 PC 接続用に VLAN2 のアクセスポートとして構成します。 端末 PC 接続用のため STP 対象外(portfast 設定)とします。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

(3) 端末 PC 用アクセススイッチ (AX1240S)の設定

A1 (AX1240S-24T2C)の設定	
スパニングツリーの設定	
(config)# spanning-tree mode rapid-pvst	スパニングツリーのモードを rapid-pvst に設定します。
VLAN の設定	
(config)# vlan 2,100-101	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.1.1 255.255.0.0	VLAN2 はシステム管理用に global で使用します。 VLAN2 に IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,100-101 (config)# interface range fastethernet 0/1-12 (config-if-range)# switchport access vlan 100 (config-if-range)# spanning-tree portfast (config)# interface fastethernet 0/13-24 (config-if-range)# switchport access vlan 101 (config-if-range)# spanning-tree portfast	ポート 0/25-26 は装置 C1,C2 接続用に VLAN2,100-101 のトランクポートとして構成します。 ポート 0/1-12 は開発部端末 PC のセグメント 1 接続用に VLAN100 のアクセスポートとして構成します。 PC 接続用のため、STP 対象外(portfast 設定)とします。 ポート 0/13-24 は開発部端末 PC のセグメント 2 接続用に VLAN101 のアクセスポートとして構成します。 PC 接続用のため、STP 対象外(portfast 設定)とします。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

装置 A2 の設定は使用する VLAN ID と装置アドレスが異なる以外は装置 A1 の設定と同様です。
(VLAN：100-101→200-201、装置アドレス：172.255.1.1→172.255.2.1)

(4) UTM (FortiGate)の設定

FortiGate にて HA 構成を組む場合、マスタとする装置にて基本的な設定をおこなっておきます。

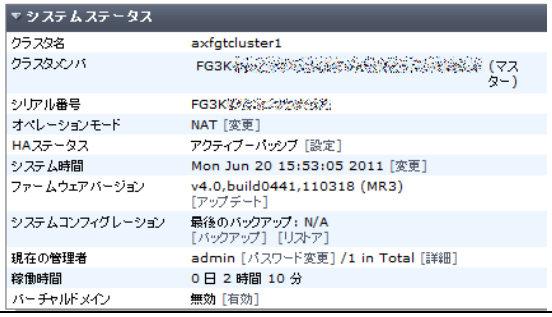
UTM1 (FortiGate-3040B)の設定

HA(冗長)クラスタの設定

CLI	GUI

config system ha
  set mode a-p
  set group-name axfgcluster1
  set password secret123
  set hbdev port17 50 port18 50
  set priority 130
end
	システム＞設定＞HA
	[モード] アクティブ-パッシブ
	[デバイスのプライオリティ] 130　*装置のプライオリティ(大きい方が高優先)*
	[グループ名] axfgcluster1　*任意のグループ名*
	[パスワード] secret123　*任意の推察されにくいパスワード*
	[ハートビートインタフェース]
	[port17] 有効をチェック [プライオリティ] 50
	[port18] 有効をチェック [プライオリティ] 50
	<OK>
	 

VDOM の作成

config system global set vdom-admin enable end You will be logged out for the operation to take effect Do you want to continue? (y/n)y	システム＞ダッシュボード＞Status [システムステータスウィジェット] バーチャルドメイン [有効]をクリック 

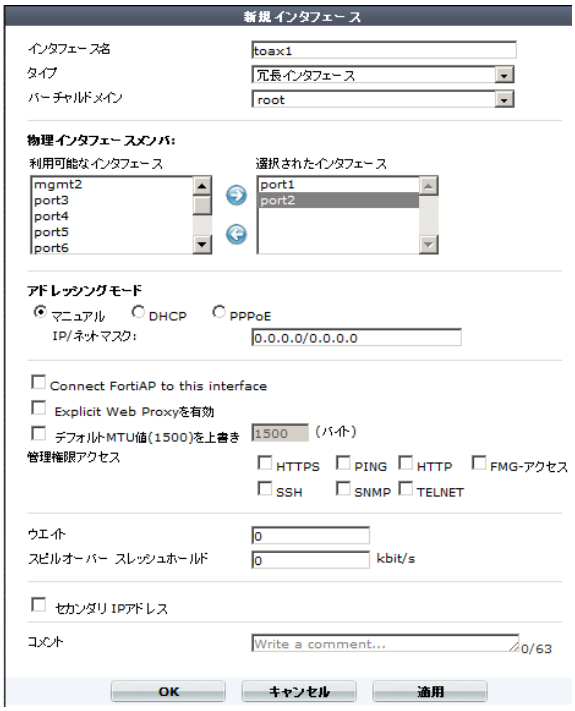
```
config vdom
  edit VDOM1
  next
  edit VDOM2
  next
  edit VDOM3
end
```

システム＞VDOM＞VDOM＞新規作成
[名前] VDOM1
[オペレーションモード] NAT
〈OK〉
同様に VDOM2、VDOM3 を作成する。

インタフェースの設定（冗長インタフェース）

```
config global
  config system interface
    edit toax1
    set vdom root
    set type redundant
    set member port1 port2
  end
end
```

システム＞ネットワーク＞インタフェース＞新規作成
[インタフェース名] toax1
[タイプ] 冗長インタフェース
[バーチャルドメイン] root
[物理インタフェースメンバ][選択されたインタフェース] port1 port2
〈OK〉

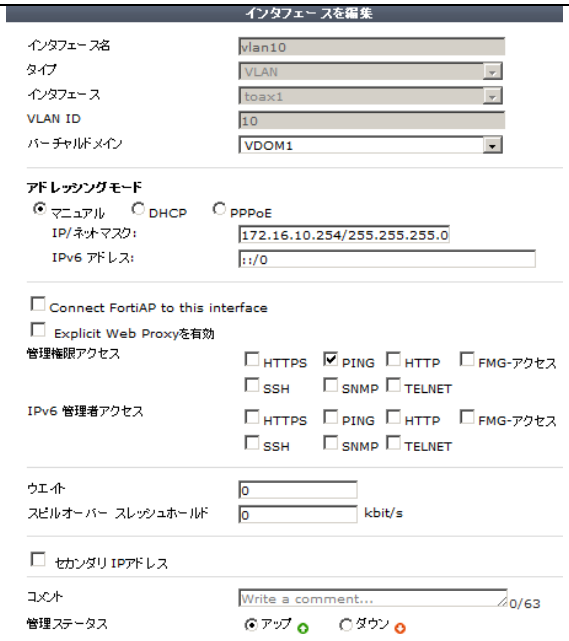


VLAN の設定

```
config global
config system interface
  edit vlan10
    set vdom VDOM1
    set ip 172.16.10.254/24
    set allowaccess ping
    set interface toax1
    set vlanid 10
  next
  edit vlan20
    set vdom VDOM2
    set ip 172.16.20.254/24
    set allowaccess ping
    set interface toax1
    set vlanid 20
  next
  edit vlan30
    set vdom VDOM3
    set ip 172.16.30.254/24
    set allowaccess ping
```

システム＞ネットワーク＞インタフェース＞新規作成
[インタフェース名] vlan10
[タイプ] VLAN
[インタフェース] toax1
[VLAN ID] 10
[バーチャルドメイン] VDOM1
[IP/ネットマスク] 172.16.10.254/24
[管理権限アクセス] PING にチェック

```
    set interface toax1
    set vlanid 30
  next
  edit vlan31
    set vdom VDOM1
    set ip 172.16.31.254/24
    set allowaccess ping
    set interface toax1
    set vlanid 31
  next
  edit vlan32
    set vdom VDOM2
    set ip 172.16.32.254/24
    set allowaccess ping
    set interface toax1
    set vlanid 32
  next
  edit vlan1000
    set vdom VDOM3
    set ip 10.10.1.254/24 グローバルアドレスを 10.10.1.254 として例示
    set allowaccess ping
    set interface toax1
    set vlanid 1000
  next
  edit vlan2
    set vdom root
    set ip 172.255.0.10/16
    set allowaccess ping https ssh
    set interface toax1
    set vlanid 2
end
end
```



同様に VLAN20,VLAN31,VLAN32,VLAN1000,VLAN2 を作成する。
グローバルアドレスを 10.10.1.254 として例示

toax1	root	0.0.0.0 / 0.0.0.0		
vlan2	root	172.255.0.10 / 255.255.0.0	HTTPS,PING,SSH	2
vlan10	VDOM1	172.16.10.254 / 255.255.255.0	PING	10
vlan20	VDOM2	172.16.20.254 / 255.255.255.0	PING	20
vlan30	VDOM3	172.16.30.254 / 255.255.255.0	PING	30
vlan31	VDOM1	172.16.31.254 / 255.255.255.0	PING	31
vlan32	VDOM2	172.16.32.254 / 255.255.255.0	PING	32
vlan1000	VDOM3	10.10.1.254 / 255.255.255.0	PING	1000

VDOM1 の設定

デフォルトルートとスタティックルートの設定

```
config vdom
edit VDOM1
config router static
  edit 0
    set device vlan31
    set gateway 172.16.31.1
  next
  edit 0
    set device vlan10
    set dst 192.168.0.0/24
    set gateway 172.16.10.1
  next
  edit 0
    set device vlan10
    set dst 192.168.1.0/24
    set gateway 172.16.10.1
end
end
```

現在の VDOM＞VDOM1
ルータ＞スタティック＞スタティックルート＞新規作成
[宛先 IP/ネットマスク] 0.0.0.0/0.0.0.0
[デバイス] vlan31
[ゲートウェイ] 172.16.31.1
<OK>

続いてもう一度
ルータ＞スタティック＞スタティックルート から 新規作成
[宛先 IP/ネットマスク] 192.168.0.0/24
[デバイス] vlan10
[ゲートウェイ] 172.16.10.1
<OK>
同様に、192.168.1.0/24 へのスタティックルートを追加する。

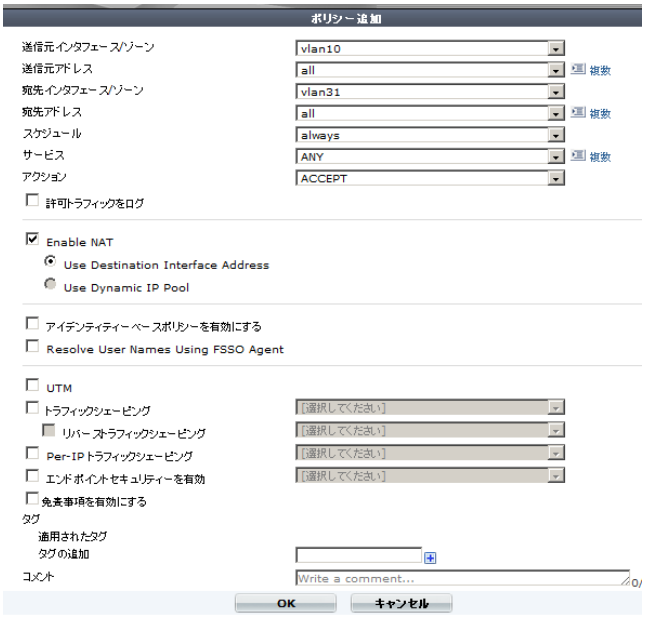
ファイアウォール設定例(NAT ポリシの追加)

```
config vdom
edit VDOM1
config firewall policy
edit 0
  set srcintf vlan10
  set dstintf vlan31
  set srcaddr all
  set dstaddr all
```

現在の VDOM＞VDOM1
ファイアウォール＞ポリシー＞ポリシー＞新規作成
[送信元インタフェース/ゾーン] vlan10
[送信元アドレス] all
[宛先インタフェース/ゾーン] vlan31
[宛先アドレス] all
[スケジュール] always

```
  set action accept
  set schedule always
  set service ANY
  set nat enable
end
end
```

[サービス] ANY
[アクション] ACCEPT
[Enable NAT] チェック [Use Destination Interface Address ラジオボタン] ON
<OK>



VDOM2 の設定

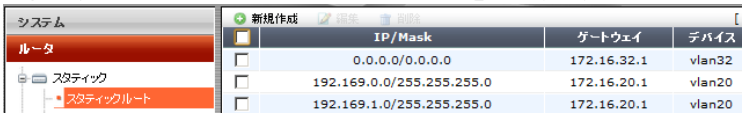
デフォルトルートとスタティックルートの設定

```
config vdom
edit VDOM2
config router static
  edit 0
    set device vlan32
    set gateway 172.16.32.1
  next
  edit 0
    set device vlan20
    set dst 192.169.0.0/24
    set gateway 172.16.20.1
  next
  edit 0
    set device vlan20
    set dst 192.169.1.0/24
    set gateway 172.16.20.1
end
end
```

現在の VDOM＞VDOM2
ルータ＞スタティック＞スタティックルート＞新規作成
[宛先 IP/ネットマスク] 0.0.0.0/0.0.0.0
[デバイス] vlan32
[ゲートウェイ] 172.16.32.1
<OK>

続いてもう一度
ルータ＞スタティック＞スタティックルート から 新規作成
[宛先 IP/ネットマスク] 192.169.0.0/24
[デバイス] vlan20
[ゲートウェイ] 172.16.20.1
<OK>

同様に、192.169.1.0/24 へのスタティックルートを追加する。



ファイアウォール設定例(NAT ポリシの追加)

```
config vdom
edit VDOM2
config firewall policy
edit 0
  set srcintf vlan20
  set dstintf vlan32
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
  set nat enable
end
end
```

現在の VDOM＞VDOM2
ファイアウォール＞ポリシー＞ポリシー＞新規作成
[送信元インタフェース/ゾーン] vlan20
[送信元アドレス] all
[宛先インタフェース/ゾーン] vlan32
[宛先アドレス] all
[スケジュール] always
[サービス] ANY
[アクション] ACCEPT
[Enable NAT] チェック [Use Destination Interface Address ラジオボタン] ON
<OK>

VDOM3 の設定

デフォルトルートとスタティックルートの設定

```
config vdom
edit VDOM3
config router static
  edit 0
    set device vlan1000
    set gateway 10.10.1.1 グローバルアドレスを 10.10.1.1 として例示
  next
  edit 0
    set device vlan30
    set dst 172.16.31.0/24
    set gateway 172.16.30.1
  next
  edit 0
    set device vlan30
    set dst 172.16.32.0/24
    set gateway 172.16.30.1
end
end
```

現在の VDOM＞VDOM3
ルータ＞スタティック＞スタティックルート＞新規作成
[宛先 IP/ネットマスク] 0.0.0.0/0.0.0.0
[デバイス] vlan1000
[ゲートウェイ] 10.10.1.1 *グローバルアドレスを 10.10.1.1 として例示*
<OK>

続いてもう一度
ルータ＞スタティック＞スタティックルート から 新規作成
[宛先 IP/ネットマスク] 172.16.31.0/24
[デバイス] vlan30
[ゲートウェイ] 172.16.30.1
<OK>

同様に、172.16.32.0/24 へのスタティックルートを追加する。

ファイアウォール設定例(NAT ポリシの追加)

```
config vdom
edit VDOM3
config firewall policy
edit 0
  set srcintf vlan30
  set dstintf vlan1000
  set srcaddr all
  set dstaddr all
  set action accept
  set schedule always
  set service ANY
  set nat enable
end
end
```

現在の VDOM＞VDOM3
ファイアウォール＞ポリシー＞ポリシー＞新規作成
[送信元インタフェース/ゾーン] vlan30
[送信元アドレス] all
[宛先インタフェース/ゾーン] vlan1000
[宛先アドレス] all
[スケジュール] always
[サービス] ANY
[アクション] ACCEPT
[Enable NAT] チェック [Use Destination Interface Address ラジオボタン] ON
<OK>

管理 VDOM の変更（必要に応じて）

```
config global
config system global
set management-vdom VDOM 名
end
end
```

現在の VDOM＞グローバル
システム＞VDOM＞
管理 VDOM にしたい VDOM 名左隅のチェックボックスをチェック
[マネジメントを切り替え]アイコンをクリック

設定のバックアップ

```
config global
exec backup config ftp
master.conf サーバ IP アドレス ユーザ ID パスワード
```

現在の VDOM＞グローバル
システム＞ダッシュボード＞Status>システムステータスウィジェット
[システムコンフィグレーション]の[バックアップ]をクリック

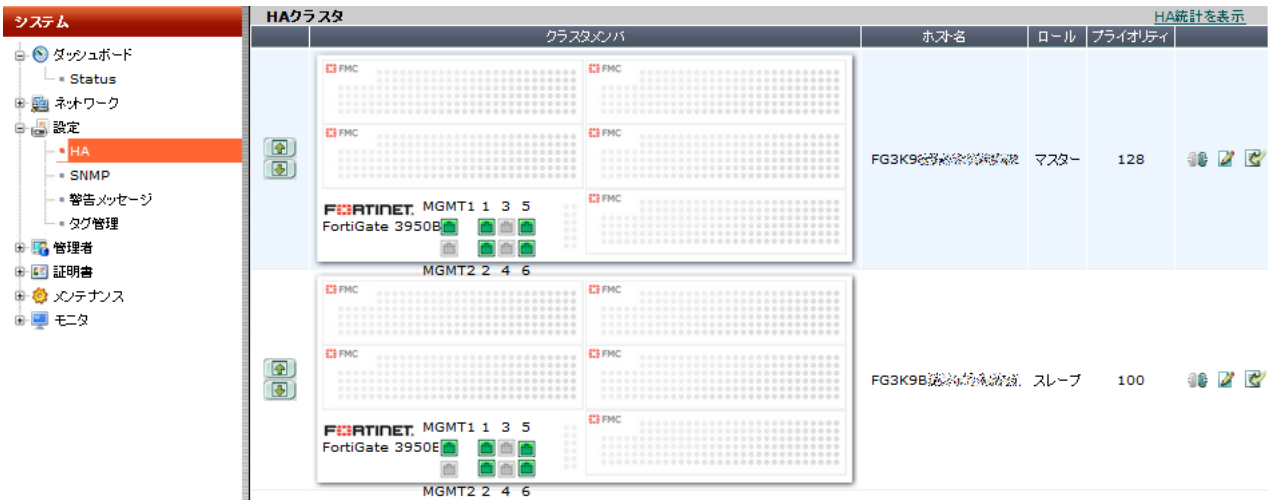
続いて、バックアップとして使用する装置の設定をマスタ装置と接続する前に以下のように設定します。

UTM2 (FortiGate-3040B)の設定	
HA(冗長)クラスタの設定	
CLI	**GUI**

`config system ha`
`  set mode a-p`
`  set group-name axfgcluster1`
`  set password secret123`
`  set hbdev port17 50 port18 50`
`  set priority 100`
`end`
	システム＞設定＞HA
	[モード] アクティブ-パッシブ
	[デバイスのプライオリティ] 100　*装置のプライオリティ(小さい方が優先度低)*
	[グループ名] axfgcluster1　*UTM1 に設定したグループ名と同じもの*
	[パスワード] secret123　*UTM1 に設定したパスワードと同じもの*
	[ハートビートインタフェース]
	[port17] 有効をチェック [プライオリティ] 50　*port17 と*
	[port18] 有効をチェック [プライオリティ] 50　*port18 を使用*
	<OK>

バックアップ装置での以上の設定終了後、マスタ装置へ接続、続いてネットワークに接続します。

HA が正しく構成されているかの確認は以下の通りです。
GUI の場合
システム＞設定＞HA



CLI の場合

```
# config global
(global) # get system ha status
Model: 3950
Mode: a-p
Group: 32
Debug: 0
ses_pickup: disable
Master:128 FG3K9B3X00000001 FG3K9B3X00000001 0
Slave :100 FG3K9B3X00000002 FG3K9B3X00000002 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG3K9B3X00000001
Slave :1 FG3K9B3X00000002
```

バックアップ側の装置については、マスタ側の装置でおこなった設定をおこなう必要はありません。HA のバックアップと認識された時点で、マスタで設定した内容がそのままバックアップ側にコピーされます。

続いて、マスタ側の装置に接続し、HA 監視ポートの設定をします。設定はバックアップ側に同期されます。

HA監視ポート設定 （構築ポイント(4)）

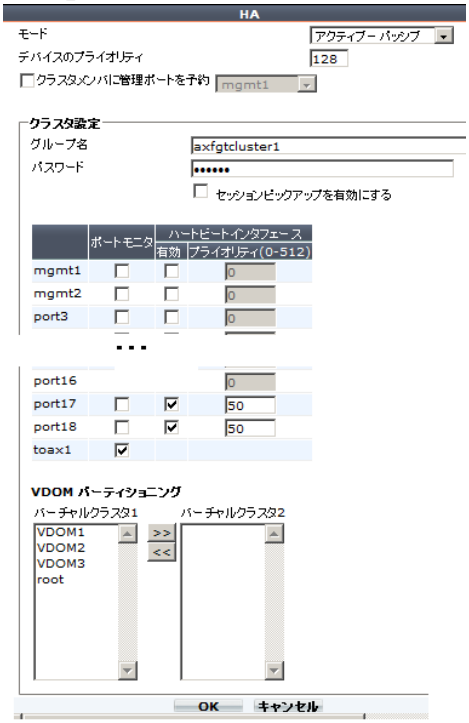
```
config global
config system ha
  set monitor toax1
end
end
```

システム＞設定＞HA

マスタ状態の装置の編集 アイコンクリック

[ポートモニタ] toax1 をチェック

<OK>をクリック



4. 効率的な運用ツール

ネットワークを仮想化すると、構成が物理的な構成、いわゆる見た目と異なることになるため、運用管理の面で負担が大きくなりがちです。

アラクサラのネットワーク・パーティションや FortiGate では、そういった仮想化されたネットワークの運用を手助けするツールも用意されています。

4.1 AX-Networker's Utility（仮想ネットワーク可視化ツール）

AX-Networker's-Utility（仮想ネットワーク可視化ツール）は，ネットワーク上に存在する装置の VRF/VLAN コンフィグレーションを集中的に収集，一覧表示し，その設定内容をチェックできるツールです。
また，ネットワーク上に存在する装置に接続された装置や端末の情報（以下，リソース情報）を集中的に収集，一覧表示し，検索できます。

- 装置の VRF/VLAN コンフィグレーションを収集し，装置間の VRF/VLAN コンフィグレーションを確認，検索および整合性チェックすることができます。

- 装置のリソース情報を収集し，その収集時点で装置に接続されている装置や端末の情報を確認できます。リソース情報としては，装置に接続している装置や端末の台数，装置や端末の MAC アドレス，Web 認証ログイン済み端末の IP アドレス，Web 認証ログイン済みユーザ名，論理名，Web/MAC 認証ログイン経過時間，Web/MAC 認証ログイン残時間，装置や端末が接続されている装置側のポート番号を一覧表示します。

- 装置の VRF/VLAN コンフィグレーションやリソース情報の収集を，GUI を利用して簡単に実施できます。広域・多拠点に分散する収集対象装置の台数が多い場合に，作業者の負荷を軽減できます。

これにより，装置の VRF/VLAN コンフィグレーションを更新する際に VRF/VLAN コンフィグレーションの整合性チェックを行ったり，装置のリソース情報を収集して，装置に接続されている装置や端末を VRF や VLAN 毎に接続されている台数として確認したり，特定のリソース情報のキーワードによる検索が容易に行えるようになります。

図 4.1-1 AX-Networker's Utility(仮想ネットワーク可視化ツール) 参照画面例

4.2 FortiManager と FortiAnalyzer

FortiGate に関しては、FortiGate における各種設定など装置そのものの管理と、FortiGate によるアクセス制御によって得られる各種ログ監視の両面を助けるアプライアンスがあります。

その前者にあたるのが FortiManager です。

FortiManager では、複数の FortiGate と、複数の仮想ドメイン（VDOM）を、集中管理するためのアプライアンス製品です。FortiManager を使うことで、共有できるセキュリティポリシを複数の FortiGate や VDOM に適用したり、FortiGate のファームェアの更新を集中的に効率よく実施できます。また、インターネットリーチャブルでない FortiGate に対して、アンチウイルスや IPS のシグネチャデータベースを更新することもできます。この他、設定履歴や差分の管理機能も備えています。FortiManager の XML API の利用で、自動化にも対応可能です。

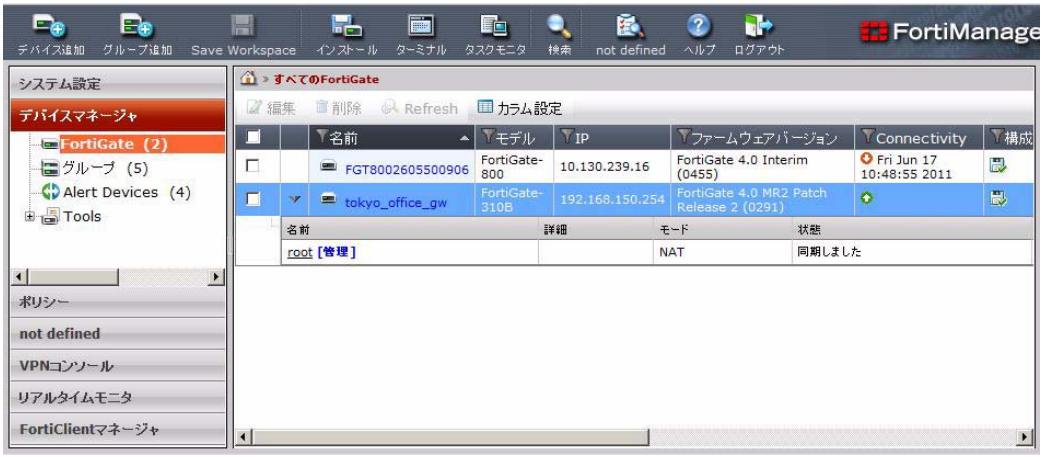


図 4.2-1 FortiManager 設定画面例

一方、ログ管理を助けるアプライアンスとして FortiAnalyzer があります。

FortiAnalyzer は、複数の FortiGate や複数の VDOM が記録するログを管理するためのアプライアンスであり、FortiAnalyzer を使うことで、ログの検索や、ログの集計、報告書作成と報告書の送付が簡単に行なえます。スケジューリング機能により、毎週月曜日8時に、VDOM 毎に PDF 形式の一週間の攻撃状況の報告書を作成し、VDOM 毎の管理者に報告書を電子メールで送付する、といったことが自動でできます。

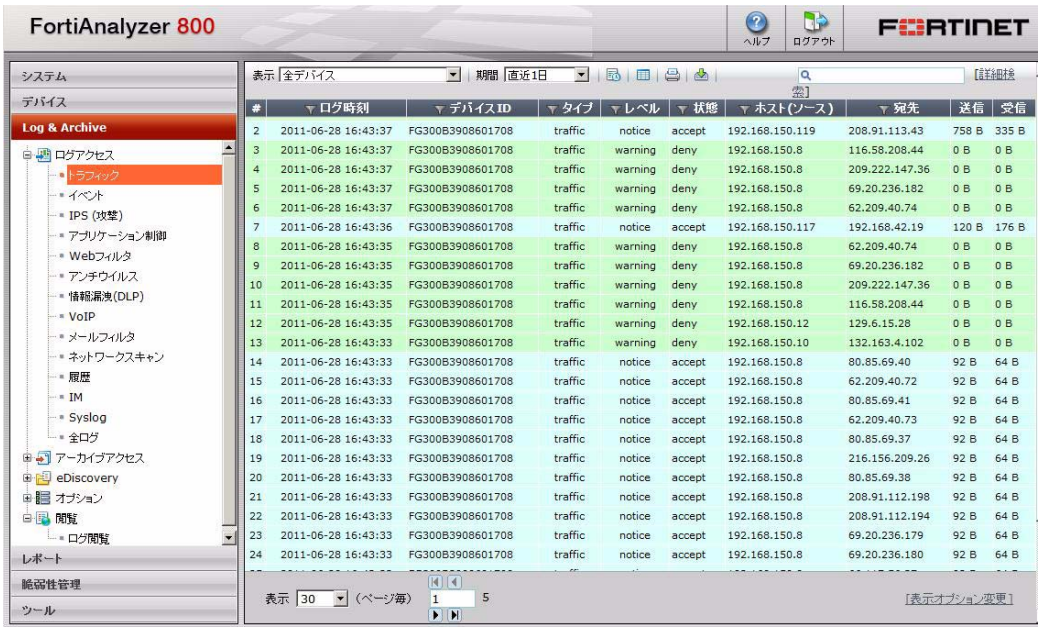


図 4.2-2 FortiAnalyzer 設定/ログ参照画面例

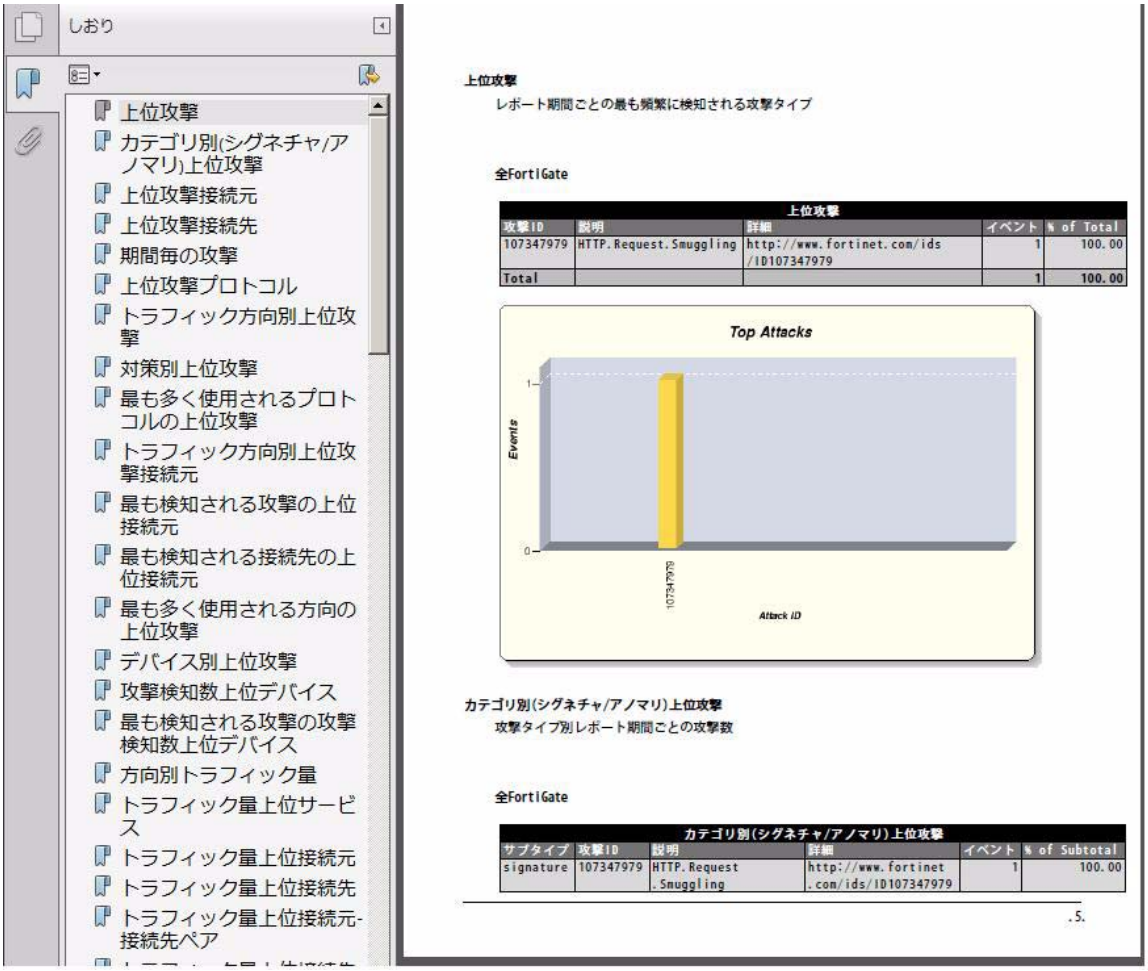


図 4.2-3　FortiAnalyzer 自動生成レポート例

5. 留意事項

(1) AX シリーズと FortiGate をリンクアグリゲーション接続する際は LACP を使用する。

FortiGate の物理インタフェースはリンクアグリゲーションによる冗長構成も可能ですが、いわゆるスタティックのモードはサポートされません。従って AX シリーズとリンクアグリゲーションを使って接続する必要がある場合は LACP モードを使用してください。

(2) FortiGate インタフェースでの DHCP クライアント使用について

FortiGate では、スタンドアロンで使用している場合に限りインタフェースでの IP アドレス指定に DHCP クライアントによる設定を使うことが可能ですが、HA 構成としている際はインタフェースへの DHCP クライアントによる IP アドレス設定はできません。

(3) FortiGate の HA 監視ポート設定の手順

HA の設定および監視ポートの設定がされた HA マスタ装置が監視ポートのダウンを検知している状態で、マスタと異なるコンフィグを持つ装置を監視ポートの設定なしに、マスタ装置に接続（HA クラスタへ参加）すると、マスタ側のコンフィグが消失します。追加された装置が新たなマスタとなり、コンフィグもあわせて追加された装置のものに同期するためです。(追加する装置では監視ポートの設定が無いと、監視ポートダウン検知無しとみなされます。)

マスタ装置に、工場出荷状態などマスタと異なる設定を持つ装置を接続するときの手順は下記のいずれかの方法を推奨します。

- 新規に HA を構築するときは、HA クラスタの構築をし、HA が正しく動作していることを確認してから HA 監視ポートの設定をする。
- 追加する装置に、少なくともマスタ装置と同じ監視ポート設定をしてからマスタ装置に接続する。
- マスタ装置に接続する前に、マスタ装置の HA 監視ポートがすべてアップ状態であることを確認する。

なお監視ポートのダウン検知状況は CLI で下記のように確認します。

```
FG3K9B3E00000001 (global) # dia sys ha dump 1
HA information.
vcluster id=1, nventry=2, state=work,
digest=4.3f.6e.62.a.40...
ventry  idx=0,id=1,FG3K9B3E00000001,prio=128,-50,claimed=0,override=0,
flag=1,time=0,mon=0
                                          ↑
                                    0       ポートダウン検知なし
                                    負の値  ポートダウン検知あり
                                    ※この例では、FG3K9B3E00000001 が監視ポートの
                                    いずれかのダウンを検知している状態を示します。
```

（※） ハードウェア障害の機器交換時は、予めバックアップしておいた設定を、新装置にリストアした後に、HA クラスタへ参加させることで、コンフィグの消失をさけることができます。

(4) FortiGate の HA 構成におけるマスタ装置交替について

HA 構成としている装置でマスタとなっていた装置がダウン後、再度復旧した場合に同じその装置がマスタ状態に戻る(切戻る)場合があります。

HA では override 設定(CLI でのみ設定可能。デフォルトでは disable)が disable であり、かつ HA 構成の装置同士の「安定稼働時間(※)」の差が 300 秒以上ある場合、メンバ追加時の系交替、いわゆる切戻りが抑止されます。HA での装置復旧ではほとんどの場合この条件に該当するため、一般的には切戻りが発生しませんが、override 設定が enable、もしくは安定稼動時間の差が 300 秒以下の場合は、プライオリティの高い装置がマスタになりますので、元マスタだった装置の復旧とともにマスタ交替も発生する(切戻る)状態が発生する場合があります。

(※)安定稼動時間：FortiGate が最後に経験した監視ポートのリンクダウンから、もしくは起動から監視ポートのリンクダウンが無ければ起動からの経過時間。HA 構成の装置間で安定稼動時間の差を確認するには、CLI にて以下のように行います。

```
FG50012205400050 # config global
FG50012205400050 (global) # diagnose sys ha dump 1
HA information.
vcluster id=1, nventry=2, state=work,
digest=fe.21.14.b3.e1.8d...
ventry idx=0,id=1,FG50012205400050,prio=128,0,override=0,
flag=1,time=0,mon=0.
mondev=port5,50
ventry idx=1,id=1,FG50012204400045,prio=128,0,override=0,
flag=0,time=194,mon=0.
```

コマンド実行した装置での値は常に'0'となる。

コマンド実行装置から見た、この相手装置に対する安定稼動時間の相対値。(単位 1/10 秒)
正の値であれば、安定稼動時間はコマンド実行した装置＞相手装置
負の値であれば、 〃 コマンド実行した装置＜相手装置
※この例ではコマンド実行した装置(FG50012205400050)の方が、19.4 秒長いことを示しています。

override 設定=disable であれば、相手装置に表示される time の値が
3000 以上である装置がマスタとなります。

付録

本ガイドにて紹介した構成のコンフィグレーション例です。

3 章の各ネットワーク構成における各装置の全コンフィグレーションについて、テキスト形式のファイルとして本ファイルに添付しております。(添付ファイルを抽出するには、Adobe Acrobat 5.0 以降もしくは Adobe Reader 6.0 以降が必要です。)

各コンフィグレーションについては、以下に示すファイル名と同じ名前の添付ファイルを参照下さい。

3.1 FTスイッチコア + FortiGate HA構成の例

	装置名と対象装置	対象ファイル
L3 コアスイッチ	C1 (AX6604S)	3-1_AXFG-guide_FT_C1.txt
UTM(*1)	UTM1(FortiGate-3950B)	3-1_AXFG-guide_FT_UTM1.conf
L2 アクセススイッチ	S1 (AX2430S-24T2X)	3-1_AXFG-guide_FT_S1.txt
	A1 (AX1240S-24T2C)	3-1_AXFG-guide_FT_A1.txt
	A2 (AX1240S-24T2C)	3-1_AXFG-guide_FT_A2.txt

(*1)UTM(FortiGate)のコンフィグは HA のマスタ分のみです。スレーブ側のコンフィグは HA 構成時にマスタと同期します。

3.2 STP+VRRP + FortiGate HA構成の例

	装置名と対象装置	対象ファイル
L3 コアスイッチ	C1 (AX3560S-24T6XW)	3-2_AXFG-guide_STP_C1.txt
	C2 (AX3560S-24T6XW)	3-2_AXFG-guide_STP_C2.txt
UTM(*1)	UTM1(FortiGate-3040B)	3-2_AXFG-guide_STP_UTM1.conf
L2 アクセススイッチ	S1 (AX2430S-24T)	3-2_AXFG-guide_STP_S1.txt
	A1 (AX1240S-24T2C)	3-2_AXFG-guide_STP_A1.txt
	A2 (AX1240S-24T2C)	3-2_AXFG-guide_STP_A2.txt

(*1)UTM(FortiGate)のコンフィグは HA のマスタ分のみです。スレーブ側のコンフィグは HA 構成時にマスタと同期します。

〈空白ページ〉

2011 年 7 月 5 日　初版発行

アラクサラネットワークス株式会社
ネットワークテクニカルサポート

〒212-0058
川崎市幸区鹿島田 890 番地 新川崎三井ビル西棟
http://www.alaxala.com/