



READY FOR ANYTHING

レジリエントなデータセンターの構築

—— ゲール・メレディス・オットeson (Gail Meredith Otteson) による報告

レジリエンスは、ITインフラの心臓部であるデータセンターでは特に重要な要素となる。アプリケーション、サーバ、およびストレージをデータセンターに統合する現在のトレンドは、ビジネスのレジリエンスを増強する絶好のチャンスだ。IT組織は統合プロジェクトの着手と同時に、現在から将来にわたるアプリケーションやテクノロジーのために、安全でレジリエントな基盤が構築されていることを確認する必要がある。データセンターにレジリエントなアーキテクチャを採用するITマネージャは、新たなアプリケーションの要求に迅速に対応することができるサービス志向のインフラのメリットが何であるのかを認識しているので、ビジネスの機敏性を拡大させることもできるのだ。

ネットワークのレジリエンス

Cisco Business Ready Data Centerは、レジリエンスの高いネットワークアーキテクチャを提供している。IP、ストレージおよびオブティカルコンポーネントを備えたデータセンターを適切に展開すれば、最適なアプリケーションサービスレベルの基盤を創造することになる。このアプローチのおかげで、ややもするとIT予算の浪費を招く可能性を抱えているデータセンター運用に対して大幅な経費削減をもたらすことも可能になる。

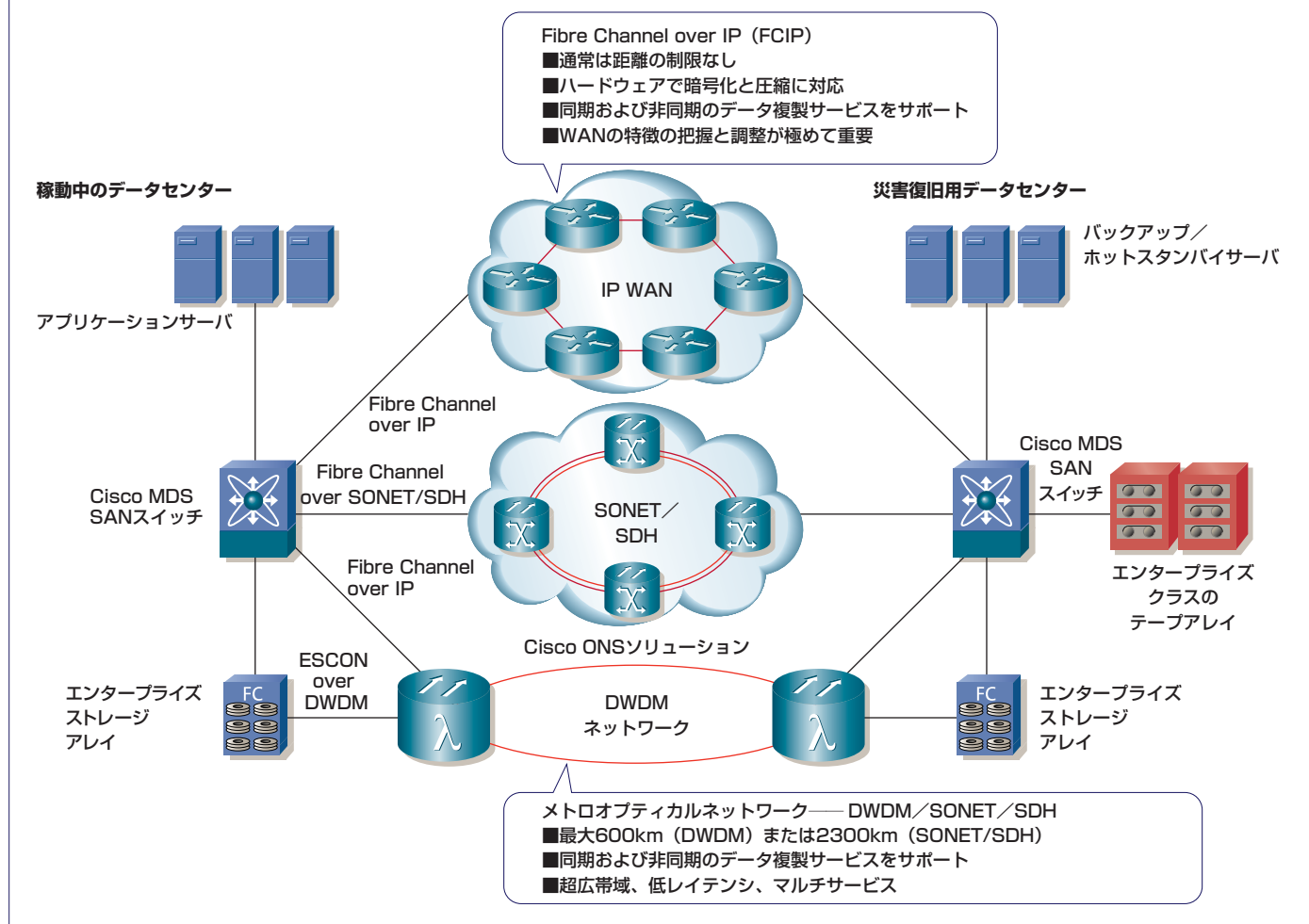
ネットワークのレジリエンスに不可欠なものとして、将来のキャパシティの増大やサービスの成長に備えた

高可用性デザインがある。ネットワーク投資がデータセンターのTCO (Total Cost of Ownership: 所有コスト) に占める割合はごくわずかだとしても、META Group (2004年4月) は、「中途半端に最適化されたネットワークデザインは可用性の高いデータセンターに重大な悪影響をもたらし、企業がその設計や実施に費やしたその他すべての投資を葬り去ってしまう可能性がある」と述べている。高可用性ネットワーク構築の基本については、本誌8ページの『レジリエンスの方策』を参照。

データセンターのレジリエンスに対する基本的要件は、MTBF (Mean Time Between Failure: 平均障害間隔) が長いレジリエントなネットワークエレメントである。一般に大規模なデータセンターでは、レジリエンスと拡張性に優れ、ビジネスクリティカルなアプリケーションへのアクセスを最適化し、安全を確保するインテリジェントなプラットフォームであるCisco Catalyst 6500シリーズのスイッチがシスコのIPネットワークのアプリケーション層の基礎になっている。その冗長度の高いスーパーバイザオプションがステートフルフェールオーバーを提供する一方で、特別なサービスモジュールによりファイアウォールの構築、暗号化、ロードバランシング、およびネットワーク分析などインテリジェントネットワークサービスを直接ネットワークファブリックに統合することができる。NSF with SSO (Nonstop

レジリエンス (耐障害性・障害回復力):

レジリエンスとは、障害を未然に予測して、システム障害に至る致命的なエラーを回避するとともに、万一障害に陥った場合でも早急にシステムを復帰させることができる能力を指している。



長距離SAN: シスコのSAN拡張により、町の両端にあるデータセンター間、2万kmも離れた所、あるいは地球を半周するほどの距離であっても透過的にSANの拡張が可能になる

Forwarding with Stateful Switchover)、IPSec (IP Security) のステートフルフェールオーバー、および HSRP (Hot Standby Router Protocol) などCisco IOS Softwareのレジリエンス機能は、コンポーネントやデバイスに障害が発生した場合の迅速な復旧とセッションの保護を確実なものにする。

ストレージのイノベーション

シスコのデータセンターストレージネットワークは、Cisco MDS 9000インテリジェントSAN (Storage Area

Network) スイッチ製品ファミリーを基礎にしている。無停止のソフトウェアアップグレードやステートフルフェールオーバーなどの高可用性機能は、MDS 9500シリーズの大きな特長である。さらにシスコは、MDS SANスイッチの全ファミリーにおいて、ネットワークのレジリエンスに対応したイノベティブなストレージネットワーク技術群を導入した。そんなイノベーションの1つであるバーチャルSAN (VSAN) は、最近ANSI (American National Standards Institute Inc.: 米国規格協会) のT.11ファイバチャネル委員会の規格にも採用された。VSANは、論理的に分離されているSANの可用性やセキュリティに影響を与えることなく、隔離されているストレージの“孤島 (islands)”を中央で集中管理され拡張性をもった単一の物理的ネットワークに統合する。さらに、シスコはルーティングの柔軟性にVSANの安定性や拡張性を組み合わせたイノベーション

オンライン専用PACKET

データセンターの災害復旧およびInterior Gateway Protocol (IGP)やBorder Gateway Protocol (BGP)を使った負荷分散に関するデザインガイドはcisco.com/packet/171_6c1で見ることができる。

ンであるVSAN間ルーティングによって、ネットワークのレジリエンスの増強をも実現した。VSAN間ルーティングによって、VSANの境界を超えたデバイス間のコネクティビティが確立される一方、VSANファブリックの分離も維持されるのである。このイノベーションは、複数のVSAN間で(テープバックアップシステムなど)のリソース共用を可能にするものであり、拡張可能なデータセンターの統合には不可欠な存在である。

データセンターの内部では、レジリエントなネットワークエレメントが重要だ。さらにビジネス継続の要求に対処するものとして、SAN拡張ソリューションに対する期待はますます高まっている。これらのソリューションは、データセンター内のSANと同じ水準の可用性とセキュリティを提供しなければならない。シスコのレジリエントなSAN拡張のオプションは、アプリケーションの要求と最もコスト効率のよい接続オプションを一致させる能力を提供している。このようなオプションには、既存のWANインフラ活用のためのFibre Channel over IP (FCIP)、DWDM (Dense Wavelength-Division Multiplexing: 高密度波長分割多重)などのオプティカルソリューション、および高いパフォーマンスと低レイテンシを要求するアプリケーションのためのFibre Channel over SONETまたはSDHが含まれている。

毎秒数百ギガビットのスループットと、50ミリ秒の復旧時間をサポートするオプティカルネットワークはビジネス継続の要求に対する魅力的なオプションであり、その価格もより手頃なものになってきた(本誌23ページの『レジリエンスの冒険』を参照)。Cisco ONS 15454のようなマルチサービスオプティカルソリューションは、音声、ビデオ、データ、およびストレージをサポートすることで、コストの高い冗長WANネットワークをより効率的な単一のソリューションに統合するものである。

想定されるあらゆる中断からネットワークやそこにつながれているサーバとストレージデバイスを確実に、迅速かつシームレスに復旧できるレジリエンスの高いネットワークデザインには、これらのネットワークエレメントがすべて組み込まれていなければならない。シスコはこのようなレベルのレジリエンスを達成するため

に、その有効性に対する十分な検証に基づくベストプラクティスのレファレンスデザインガイドを提供している。特に、データセンターのネットワークの高可用性を支えるテクニカルレファレンスガイドについてはcisco.com/go/datacenterで見ることができる。

ネットワークレジリエンスの最後の構成要素は、特に変更管理に際して、一貫して高可用性ネットワークのベストプラクティスに則って行動する、統制のとれた運用チームである。常に変化し続けるデータセンターの環境では、サーバ、アプリケーション、ストレージ、光伝送/セキュリティ、ビジネス継続、およびネットワークを担当するグループ間の協力体制が必要である。運用プロセスはプロセスを標準化し、説明責任を果たし、ルーチンプロセスを自動化する管理ツールを利用する必要がある。Sage Research社によれば、予定されていないネットワーク停止の原因を追跡したところ、その3分の2が管理エラーであり、それらはおおむねCiscoWorks Resource Manager Essentialsのようなツールを基盤とした厳密な変更管理システムを活用することで排除することができるのである。

アプリケーションのレジリエンス

データセンター統合にあたって最も大きな懸念課題は、統合されたインフラ上のアプリケーションのセキュリティや可用性、サービスレベルをいかに維持するかということである。ここにおいて、統合されていないサイロ型のアプリケーションは物理的に分離されているので、ダウンタイムやセキュリティ侵害のリスクを低減できるのではないかと……という誤った考えが蔓延している。

「サイロ型のアプリケーションやインフラは硬直していて効率が悪いので、データセンターマネージャはリソースを統合しなければなりません」とシスコのデータセンターネットワークのソリューション・マネージャであるジョナサン・ジラード(Jonathan Gilad)は語る。

「インフラが優れたデザインに基づいて正しく統合された場合には、決してセキュリティやアプリケーションサービスのレベルが犠牲になることはありません。むしろ、実際にはアプリケーションのレジリエンスが改善されることになるのです」

データセンターの統合を加速するテクノロジーの1つに、シスコのワイドエリアファイルサービス(WAFS: Wide Area File Services)がある。これはすべてのファイルを可用性と安全性が高いデータセンターに移しながらも、ブランチオフィスの従業員がパフォーマンスの低下などに煩わされることのないよう、ブランチオフィスに大容量のファイルサービスを提供してくれる。

アプリケーションのレジリエンスを、統合されたデータセンターに組み込むのがトレンドだ。ここでは、利用可能なサーバとストレージリソースを、セキュリティと管理のための論理構成として表現するためにネットワークを活用するといった仮想化に焦点が当てられている。

Cisco Business Ready Data Centerは、IPとストレージの両者に対してネットワーク仮想化ソリューションを提供している。IPネットワークでは、Cisco IOS SoftwareによってバーチャルLAN (VLAN)を使ってアプリケーションの隔離が可能となる。トラフィックは論理的な分離が保たれるので、ブロードキャストストームなどにおけるアプリケーションの誤動作が他のアプリケーションに波及することはない。ファイアウォールは、セキュリティ侵害あるいはウイルスやワームの感染の拡大や影響を最低限に留めるためにリソースを分離している。また、統合されたCisco Firewall Services Module (FWSM)は各VLANに1つずつ複数のバーチャルファイアウォールとして構成することができるので、複雑度と経費の軽減に貢献してくれる。各セキュリティゾーン内では、Cisco Content Switching Moduleがサーバの正常な動きを監視し、併せてロードバランシングを行うことによって、サーバクラス全体にわたって上位レイヤのアプリケーションパフォーマンスが最適化される。

シスコは、Cisco MDS 9000ファミリのSANスイッチを通じて、インテリジェントSAN仮想化サービスを可能にした。「ストレージの仮想化をネットワークに移すことによって、アプリケーションのレジリエンスが増します」とシスコのストレージ・パーチャライゼーション・グループのシニア・テクニカル・マーケティング・エンジニアであるジェイソン・ワーナー (Jason Warner)は言う。

「アプリケーションは、データが実際に存在している地理的な位置を意識する必要はありません。確実に欲しいデータにアクセスできればいいのです。データセンター統合プロジェクトや合併・買収に伴うプラットフォームの移行中には、ベンダーの違いに縛られない1つのインターフェイスによってストレージリソースがオンラインに保たれます」

Cisco MDS 9000ファミリは、複数のパートナーからのインテリジェントストレージサービスのホストとなり、中央で管理するためのオープンなプラットフォームを提供する。これらのインテリジェントファブリックアプリケーションには、ネットワークホスト型の仮想化、データの移行、バックアップなどが含まれている。このようなオープンプラットフォームのアプローチによって、ストレージマネージャは最適化されたストレージの仮想化と管理アプリケーションを選ぶことができるのである。シスコはFabric Application Interface Specification (FAIS)ドラフトスタンダードのテクニカル・エディターとして、この分野における業界標準も推進している。

ビジネスの継続

現在の“24時間×7日間”稼働の世界の中で、企業にはいかなる場合にもビジネスプロセスを支援するITインフラが必要である。ビジネスの継続性は、万一の中断時にもIT資産を守り、復旧させるための技と科学の結晶である。ビジネスに与える影響の分析は、ノンストップのサービスが必要なアプリケーションと、ある程度のダウンタイムならばビジネスに悪影響を与えることなく耐えられるアプリケーションとを識別するものである。企業そのものを守り、コストをコントロールするのに必要なビジネス継続システムの規模は、これらのパラメータによって決定される。

シスコは、データセンター間のビジネス継続のために複数のIPおよびファイバチャネルのSAN拡張オプションをサポートしている。短距離から中距離(200~600km)では、広帯域と低レイテンシをサポートしているので、一般にはファイバチャネルをDWDMまたはSONET/SDH上に直結するのが最適である。Cisco ONS 15000は、大手ストレージベンダーやマネージドサービスプロバイダから、レプリケーションおよびミラ

ーリングアプリケーションに関する最も多くの認定を受けている製品ラインである。FCIPでは、企業が現在のWANインフラを活用し、コストをコントロールすることができる。これは、実際の伝送距離を制限するバッファクレジットを使うファイバチャネルとは異なり、伝送制御にTCPを使って最大2万kmまで海を越えた伝送や大陸間の伝送を可能にする。ストレージ中心に最適化されたTCPのバージョンは、最大32MBまでのウィンドウサイズをサポートしている。

SANの拡張

Cisco MDSファミリー用のSAN-OS 2.0の導入により、パフォーマンスとセキュリティが向上するだけでなくハードウェアベースの圧縮もサポートし、SAN拡張サービスが強化されている。Cisco MDS SANスイッチは、サイト間の距離を越えたレプリケーションをサポートするために、テープだけでなくディスク書き込みの加速をも支援。どちらの場合も、エクステンジへの報告を待つことなく、リモートのテープバックアップやディスクアレイへの交換を促進する。そして、伝送レートを向上させ、アプリケーションのパフォーマンスに対する影響を最大100%まで軽減するのである。

SAN拡張ソリューションアーキテクチャは「レプリケーションモードか？ 同期か／非同期か？」によって決定される。高可用性ソリューションにおいては、各リンク上に1つ以上のVSANを備え、両端に2台のスイッチが用いられる。また、アレイ内のクライアント保護機能によって、エラーリカバリとデータ妥当性の検証が実行されることになる。Cisco MDS 9000は、PortChannelテクノロジーによって、この保護機能をさらに強化してくれる。このPortChannelは、イーサネットスイッチングにおけるイーサネットチャネルと同様に、ロードバランスと容量拡大の目的で最大16のファイバチャネルまたはFCIPリンクの論理上のグループを形成する。また、各PortChannelは複数のVSANをトランクし、ファイバチャネル接続の伝送速度を2Gbpsから32Gbpsにまで押し上げることができる。

FCIPは書き込みのアクセラレーションとの組み合わせによって、同期および非同期のレプリケーションをFibre Channel over Opticalに匹敵するパフォーマンス

で提供することができる。SAN-OSバージョン2の新しいSAN Extension Tuner機能によって、ストレージマネージャは利用可能な帯域と往復時間に応じて、最低および最高の可用性やその他のパラメータを設定することができるようになるのである。

データセンターのセキュリティ

データセンターは、悪意ある行為の対象として最も狙いたがるターゲットだ。センターに適切な安全措置が施されていない場合には、ハッカー、ワーム、DDoS (Distributed Denial-Of-Service：分散型サービス拒否) 攻撃などにより大規模な破壊と多額の損失を招く可能性がある。データセンターマネージャは、サーバ、ストレージ、ネットワーク、アプリケーションなどのリソースを統合する場合、その変化がセキュリティ体制やアプリケーションのレジリエンスにどんな影響を与えるかを考慮しなければならない。セキュリティ担当とネットワーク担当のマネージャは、会社全体への波及もあり得る脅威に対して、防御を固めるネットワークセキュリティアーキテクチャを開発することができるように、データセンターのリソースに固有の脆弱性や脅威の理解に尽力しなければならない。シスコのセキュリティソリューションは、安全なコネクティビティの多層展開、脅威に対する防衛、そしてアクセス者の信頼性と特定に対するソリューションを通じて総合的な保護を提供するものである。

Cisco Business Ready Data Centerは、セキュリティを直接ネットワークインフラに統合することによって、エンド・ツー・エンドのセキュリティ、パフォーマンスおよび管理能力の最適化を達成している。これは、Cisco CatalystスイッチおよびCisco MDS 9000インテリジェントSANスイッチの統合された先端的セキュリティ機能のメリットを活かしたものだ。Cisco Catalyst 6500プラットフォームの統合されたセキュリティソフトウェアとサービスモジュールは、ファイアウォール、侵入検知システム(IDS：Intrusion Detection System)、SSL (Secure Sockets Layer)、DDoSプロテクション、およびIPSec VPN (IP Security Virtual Private Network)を提供し、帯域重視のデータセンター環境で要求されるさらに高いレベルのパフォーマンスを実

現する。

Cisco MDS 9000スイッチは、ストレージネットワークにおける無認可の管理アクセスに対してSecure Shell、Secure FTP、RADIUS、SNMPv3、およびRole-Based Access Control (RBAC: ロールベースアクセス制御) を適用する。さらにFibre Channel Security Protocol (FC-SP) は、ファイバチャネルファブリックに対してIPSecに似た機能を提供し、確実にスイッチ・ツー・スイッチの安全なコミュニケーションを確保する。シスコと共同で作成されたANSIのT11規格であるFC-SPは、機密性、データオリジンの認証、およびファブリック全体にわたるコネクションレスの整合性を提供する。VSANも、共通の物理的なSANインフラを別々のパーティシャルSANの孤島に分割することによりセキュリティを提供している。

データセンターのセキュリティのために選択肢はさまざまに存在するが、企業は以下の検討を進めるべきである。

- ハードウェアレトリミッタやコントロールプレーン保護などのツールによるインフラのセキュリティ。
- 統合されたシスコのファイアウォールによるステートフルセッション検査。
- 公開アクセスサーバにおけるCisco Security Agentによるエンドポイントの保護。
- すべてのデータセンタードメイン全体に展開したCisco Detectorまたは侵入検知デバイスおよびトラフィックをフィルタリングし、適正なセッションが継続できるようにするCisco GuardによるDDoSの緩和。
- ロールベースアクセス制御による信頼性と特定の徹底。
- ファイアウォールおよび侵入検知・防止デバイスによる周辺とドメインの保護。

コミュニケーションのレジリエンス

データセンターの統合には、しばしばシスコのIPコミュニケーションサービスとアプリケーションサーバが含まれている。レジリエントなコミュニケーションのためには、IPコミュニケーションサービスを備えたデータセンターの各ロケーションがPSTNへ直結するゲートウェイを持っていなければならない。シスコのサー

ビス統合型ルータは、広範なパケットテレフォニー・ベースの音声インターフェイスとシグナリングプロトコルを提供している。Cisco CallManagerは、クラスタ化によって高可用性を実現することができる。重大な中断の場合に迅速なIPテレフォニー復旧を実現するため、セカンダリデータセンター内にバックアップまたはホットスタンバイのクラスタを置くことができる。同様に、セカンダリデータセンター内にあるバックアップ用のCisco UnityユニファイドメッセージングおよびIPコンタクトセンターサーバがメッセージの整合性を保ち、コンタクトセンターサービスの継続を保証する。



十分に熟慮を重ねたデータセンター統合プロジェクトは、企業がレジリエンスを通じてビジネスの機敏性を一層向上するのに役立つ。シスコはデータセンターの技術的な複雑さと運用面での現実に取り組むソリューション、運用上のベストプラクティス、そしてレファレンスデザインによる企業の安全で総合的なデータセンターを計画、実施、運用への支援体制を整えている。

詳しい情報

- Cisco Business Ready Data Center : cisco.com/go/datacenter
- 可用性の高いデータセンターネットワーキングに関するホワイトペーパー (White paper on high availability data center networking) : cisco.com/packet/171_6c2
- シスコのストレージネットワーキング (Cisco storage networking) : cisco.com/packet/171_6c3
- SAN拡張に関するホワイトペーパー (White paper on extending SANs) : cisco.com/packet/171_6c4
- シスコのSAN拡張製品 (Cisco SAN extension products) : cisco.com/packet/171_6c5
- 「ビジネス継続のためにインテリジェントネットワーキングのインフラを構築する5つのステップ」 ("Five Steps to Building an Intelligent Networking Infrastructure for Business Continuation") : cisco.com/packet/171_6c6
- シスコの高可用性ネットワーキングサービス (Cisco High Availability Networking Services) : cisco.com/packet/171_6c7