レジリエンスの方策

キャンパス、ブランチオフィス、および遠隔勤務者のITシステムにレジリエンスを構築する

―― ゲール・メレディス・オッテソン（Gail Meredith Otteson）による報告

RECIPE FOR RESILIENCE

コンセプトと実施の間には大きな隔たりがある。有効なビジネスレジリエンス戦略の策定とレジリエンスを備えたITシステムの構築には、多額の投資と熟考された集中力が求められる。シスコはビジネスの機敏性を向上し、障害に耐えるレジリエンスに優れたITシステムを構築するための総合的なアプローチで企業を支援している。このアプローチは組織全体をカバーするものとして、ネットワーク、アプリケーション、コミュニケーション、さらに労働力にわたるレジリエンスに注力するものである。

最初に、レジリエンスを測定する

レジリエンスはネットワークのアップタイムなど数値化可能な統計的要素と、顧客満足度のように顕在化しにくい要素の両面がある。したがって、その測定は決して容易ではない。

「ITの観点からレジリエンスの測定が最も容易な項目はサービスの可用性です。サービスのレジリエンスレベルを理解するためには、IT組織全体がそのシステムをビジネスのプロセスに適合させるように努めなければなりません」

シスコのエンタプライズ・マーケティングのシニア・ソリューション・マーケティング・マネージャであるボビー・グハサルカー（Bobby Guhasarkar）はそう語る。

「多くの組織はサービスの可用性を測定するのではなく、各構成要素を見ているだけなのです。しかし、ビジネスのレジリエンスはアプリケーション、サーバ、およびネットワークの可用性をビジネスのプロセスと組み合わせた総体として測定されるものです」

企業はアップタイムの測定によって、ITシステムのレジリエンスへの理解をスタートさせることができる。サービスプロバイダは、長年“ファイブナイン（99.999%）”の概念でダウンタイムの想定を進めてきた。しかし、停止が実際のビジネスに与える影響が考慮されていない点において、この測定基準は可用性に関する数字遊びでしかない。ITグループは、統計的な解釈によって設定SLA（Service-Level Agreement）の正当性を確認することができる。たとえば、99.5%が可用性の目標だとすると、週に50分間のサービス停止が容認されることになる。企業のビジネスクリティカルなアプリケーションのある月の停止時間が100分間だったとしよう。その場合、ITグループは目標SLA値の範囲内であると主張することができる。しかし、ビジネスにとっては短期的な収益喪失や顧客の不満、あるいは法規制違反や訴訟の恐れを招くことになるかも知れないのだ。

エンドユーザーの観点から見たITシステムのレジリエンスの測定はさらに有益である。サービスレベルでユーザーに対する可用性を測定する基準には以下が含まれている。

■MTBF（Mean Time Between Failure：平均障害間隔）

障害が発生するまでにサービスが稼動していた時間の長さを指す。最長MTBFは最もレジリエンスが低いサービスコンポーネントのMTBFによって影響を受ける。

■MTTR（Mean Time To Repair：平均修理時間）

障害が発生してからサービスの復旧までにかかった時間の長さを指す。最短MTTRは、最もレジリエンスが低いサービスコンポーネントのMTTRの影響を受ける。

ネットワークのレジリエンス

高可用性ネットワークはサービスのレジリエンスの基礎である。グハサルカーによれば、ネットワークのレジリエンスを短期的なコスト低減の視点でしかとらえていない企業は、災害というものを軽視しているという。彼らはエンド・ツー・エンドのネットワークインテリジェンスにより実現される先端的サービスの機敏性という利点を失うだけではない。障害箇所を確認してトラブルシューティングを行うのに何時間も苦闘し、そのうえ問題解決のために何社ものベンダーと交渉することになるであろう。

ガートナー社が「リアルタイム・エンタープライズ（The Real-Time Enterprise）」に関するレポートの中で提言しているように、確かに高可用性ネットワークの構築戦略には設備投資と運用経費面でかなり多額の投資が必要になる。しかし、アップタイムの大幅増、顧客満足度の向上、収益の増加、規制違反による罰則金支出の削減などによって、それを補う十分な効果が得られることも事実である。

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。

レジリエンス向上のための Cisco IOS Software設計

Cisco IOS Software開発チームは、ネットワークのダウンタイムを削減させる機能の開発に体系的なエンド・ツー・エンドのアプローチをとっている。この戦略には、下記の3つの方向性が含まれている。

システムレベルの冗長性（System-level redundancy）には、システム障害のMTTRとダウンタイムを減らし、リモート機器を守る冗長なハードウェアコンポーネントとレジリエンスの高いプロトコルを組み合わせている。これらの機能にはNSF with SSO（Nonstop Forwarding with Stateful Switchover）、Hot Standby Router Protocol（HSRP）、Gateway Load Balancing Protocol（GLBP）、IPSec（IP Security）ステートフルフェールオーバー、ステートフルNAT（Network Address Translation：ネットワークアドレス変換）、ウォームリロード、およびウォームアップグレードが含まれている。

ネットワークレベルの冗長性（Network-level redundancy）は、ネットワークコンバージェンスの加速、保護、およびネットワークが停止した場合の復旧を提供する。ここに組み込まれたCisco NSF認知機能（Embedded Cisco NSF Awareness）は、インテリジェントプロトコルファブリックを作成する一方で、Intermediate System-to-Intermediate System（IS-IS）、Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）などのコンバージェンス、および自己修復ルーティングのプロトコルがリンクの障害を回避するためにトラフィックが動的にリルートされる。その他の機能として、IP Event DumpingやマルチキャストのSSM高速コンバージェンス（subsecond convergence）がある。

Embedded managementは、CiscoWorks内の自動化された機能や検証済みのサードパーティーの管理ツールと対話することによって、障害やイベントの管理、構成管理、および可用性の測定を先見的に提供する。Cisco IOS Embedded Event ManagerやCisco IOSのサービスに含まれているソフトウェアアップグレード機能は、このような機能の一例である。

高可用性ネットワーキングのためのシスコの戦略には、下記の要素が含まれている。

- ネットワークインフラの強化
- 現実世界のネットワークデザイン
- ネットワーク運用の再調整
- リアルタイムネットワーク管理
- 絶え間ないネットワークサポート

ネットワークインフラの強化

可用性の高いネットワークインフラを構築するためには、機器レベルのレジリエンス、ネットワークレベルのレジリエンス、管理能力および自己防衛力という4つの柱がある。企業が最適レベルの機器のレジリエンスを実現するためには、MTBFが長いハードウェアプラットフォームとMTTRの短縮を実現するソフトウェア技術を選択しなければならない。ハードウェアは電源、監視エンジン、ルーティングエンジンなど、冗長度の高いコンポーネントが含まれているほどレジリエンスに優れているということになる。

ネットワークレベルのレジリエンスは、特にキャンパスコアにあるクリティカルな機器間に複数のリンクを提供することである。ブランチオフィスには、本社のデータセンターへの二次的なアクセス、すなわちバックアップ用のWAN接続が必要だ。Cisco IOS Softwareの機能は、機器またはネットワークのレベルで障害が発生した場合、切迫した箇所や特定の停止箇所を検出し、自動的にホットスタンバイのコンポーネントに切り換えたり、故障したリンクを迂回させたりすることによってMTTRを短縮する。「今では、12万5000以上の独自ルートを持つルーティングテーブルに対するネットワークコンバージェンスでも1秒とかかりません。これは、実に驚くべき数値的な成果です」とグハサルカーは語った。

Cisco IOS Softwareには管理能力と自己防衛力の機能も組み込まれている（コラム『レジリエンス向上のためのCisco IOS Software設計』を参照）。

現実的なネットワークデザイン

レジリエンスに優れたハードウェアやソフトウェアと同等に重要なのは、現実世界のシナリオで実証され、さらに何回もテストを重ねたネットワークデザインである。シスコのエンジニアの専門チームは、広範な用途や産業分野に向けて高可用性デザインのベストプラクティスの開発とテストを行い、キャンパス、ブランチオフィス、データセンター、および遠隔勤務者など企業のネットワークドメインのためのレファレンスデザインガイドを公開している（cisco.com/packet/171_6b1 and cisco.com/packet/171_6b2を参照）。シスコは、そのデザイン推奨事項の有効性を検証し、製品設計グループにフィードバックするためにサードパーティーの研究機関とも協力している。

ネットワーク運用の再調整

意図的ではないにしろ、人的な過失によるダウンタイムの原因の多さについて、企業は決して過少評価してはならない。ガートナー社によれば、想定外に発生したネットワークのダウンタイムのうち、3分の1は人的

エラーが原因であるとしている。さらにSage Research社は、この数字は全体の3分の2に近いとしている。高品質の製品と優秀なネットワークデザインによって最高のサービスを達成するためには、秩序だった運用プロセスを開発し、厳密にそれを実行することのできる十分に訓練された運用チームが必要だ。このようなプロセスの1つは、機器のアクセスと管理のためのセキュリティポリシーを徹底的に文書化し、一貫して実行することである。

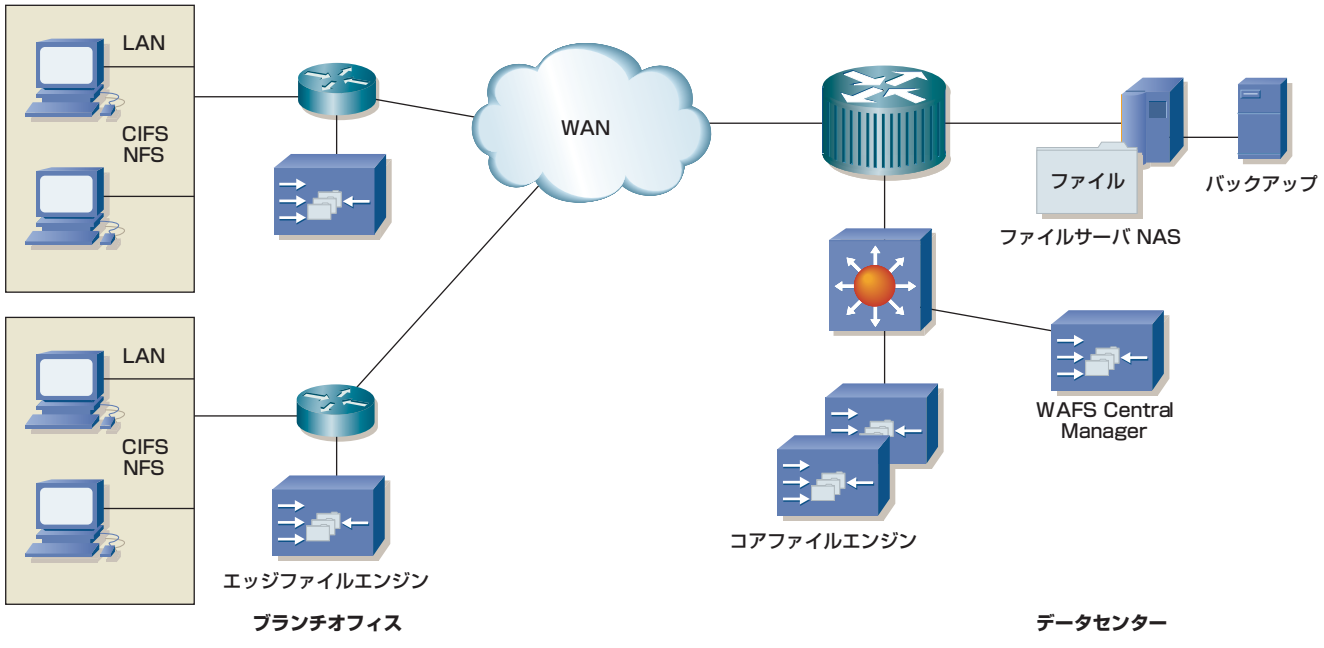
シスコのアドバンストサービスは、ソフトウェアのライフサイクル、変更管理、およびサービスレベルの管理に関して、運用上のベストプラクティスと評価のガイドラインを公開している(コラム『レジリエンスのための参考資料』を参照)。シスコは企画、設計、実施、運用、および最適化にいたるネットワークのライフサイクル全体にわたるハイアベイラビリティネットワーキングサービスのポートフォリオによる実践経験も提供している。

リアルタイムのネットワーク管理

FCAPS(Fault, Configuration, Accounting, Performance, and Security:障害、構成、アカウンティング、プロビジョニング、およびセキュリティ)管理のスピードと精度向上を目指して、シスコのネットワークシステムとの対話を可能にするように設計された総合的なネットワーク管理ツールによって、非常に効率のよいネットワーク運用が実現する。CiscoWorksツールにある自動化機能は、ネットワークマネージャの時間の使い方を大幅に改善する。ルーチンの日常業務に費やす時間が削減され、ビジネスのレジリエンスを増すプロジェクトにもっと多くの労力を使うことができるようになるのである。

一貫した設定によって、ネットワークの可用性が強化される。Cisco Smartportsは、Cisco Catalystスイッチのためのソリューションであり、イーサネットネットワークで非常に重要な機能の設定を簡素化するものだ。Smartportsは最低限の手間と専門知識だけで、シスコのベストプラクティスに基づいて検証されたスイッチポートの設定を実行する。Macrosは、Cisco Business Readyキャンパスソリューション用に推奨されている基本的なセキュリティ、可用性、QoS(Quality of

シスコの広域ファイルサービス



近隣: シスコのファイルエンジンは、WAFSテクノロジーを利用してリモートロケーションから中央のファイルにアクセスするのにエンタープライズLANに近いパフォーマンスを発揮する

レジリエンスのための参考資料

高可用性ネットワーキング、総合的なセキュリティ、そしてネットワーク、アプリケーション、コミュニケーション、および労働力に対するレジリエンスの構築についてさらに詳しく学ぶために、シスコは下記のオンラインリソースを推奨する。

■Cisco Business Readyアーキテクチャ
cisco.com/go/businessready

■高可用性ネットワーキング
高可用性ネットワーキングのためのシスコのベストプラクティス（Cisco Best Practices for High Availability Networking）：
cisco.com/packet/171_6b4
IPジャーナル『IPルーティングにおける高可用性』（IP Journal：“High Availability in IP Routing”）：
cisco.com/packet/171_6b5
PACKET『24時間アップタイム』（Packet：“Around-the-Clock Uptime”）：
cisco.com/packet/171_6b6
PACKET『可用性の高いネットワークの構築』（Packet：“High Availability Networking”）：
cisco.com/packet/171_6b7
PACKET『キャンパスネットワークのための高可用性』（Packet：“High Availability for Campus Networks”）：
cisco.com/packet/171_6b8
PACKET『新しいルート計算を加速する』（Packet：“Calculating New Routes Faster”）：
cisco.com/packet/171_6b9
Cisco Smartports
cisco.com/go/smartports

■総合的なセキュリティ
Cisco SAFE：
cisco.com/go/safe
Cisco AutoSecure：
cisco.com/packet/171_6b10
Cisco Guard DDoS緩和アプライアンス（Cisco Guard DDoS Mitigation Appliances）：
cisco.com/packet/171_6b11
ネットワークセキュリティのためのプラニングサービス（Planning Services for Network Security）：
cisco.com/packet/171_6b12

■コミュニケーションのレジリエンス
Cisco AutoQoS：
cisco.com/packet/171_6b19
Cisco 3800シリーズのISR（Cisco 3800 Series ISR）：
cisco.com/packet/171_6b20
Cisco 2800シリーズのISR（Cisco 2800 Series ISR）：
cisco.com/packet/171_6b21
Cisco CallManager Express：
cisco.com/packet/171_6b22
Cisco Survivable Remote Site Telephony：
cisco.com/packet/171_6b23
Cisco Unity Express：
cisco.com/packet/171_6b24
IPコミュニケーションのためのセキュリティ強化（Enhanced Security for IP Communications）：
cisco.com/packet/171_6b25

■アプリケーションのレジリエンス
データセンター／ビジネス継続のためのSAN拡張の概要（Data Center：SAN Extension for Business Continuance Overview）：
cisco.com/packet/171_6b13
SAN拡張の代替案を理解する（Understanding the Alternatives for Extending SANs）：
cisco.com/packet/171_6b14
Cisco WAFSとCisco ファイルエンジン（Cisco WAFS and Cisco File Engines）：
cisco.com/packet/171_6b15
ブランチオフィスルータ・ベースのコンテンツキャッシング（Branch office router-based content caching）：
cisco.com/packet/171_6b16
ブランチオフィスルータ・ベースの圧縮（Branch office router-based compression）：
cisco.com/packet/171_6b17
cisco.com/packet/171_6b18
ビジネス継続のための光ネットワーキングソリューション（Optical Networking Solutions for Business Continuance）：
cisco.com/packet/171_6b27

■労働力のレジリエンス
Cisco Business Readyテレワーカー（Cisco Business Ready Teleworker）：
cisco.com/packet/171_6b26

Service）、および管理機能に対して一貫性があり信頼性の高い設定を実現することができる。

シスコは最も優秀なマネジメント会社と協力し、各企業の多様な予算やレジリエンスのゴールに合った問題点の管理、根本原因の分析、および変更管理システムのポートフォリオを提供している。シスコとサードパーティーのパートナーのツールは運用面の対応時間を改善し、ネットワークのダウンタイムを削減するのに役立つ。たとえば、OPNETのNetDoctorおよびIT Sentinel製品は設定変更を検証し、設定の監査を自動化するのである。

徹底したネットワークサポート

シスコは、サポートのドキュメンテーションやリソースのオンライン利用に対して継続的に注力している。またネットワーク専門の認定やトレーニング、スペアリ

ング戦略、SMARTNetへの対応、さらに400人のCCIE認定者を含む1600人以上のサポートエンジニアが常時活動するテクニカルアシスタンスセンター（TAC：Technical Assistance Center）を世界各地で提供している。

広範囲にわたるセキュリティ

レジリエンスを備えたITインフラを構築する企業は、エンド・ツー・エンドのセキュリティに投資しなければならない。チェックを逃れたたった1つのウィルスやワームが、基本的なビジネス活動（たとえばEメールなど）を何日間も停止させることがあり得るからだ。そして、サービス拒否攻撃（DOS：Denial-Of-Service）はビジネスクリティカルなアプリケーションを使用不能にし、情報の盗難は、企業を顧客の信頼の失墜や法規制への違反の危機に晒す危険性を秘めているのである。

潜在的な脆弱性を生み出してしまう背景には、ワイヤレスネットワークの構築、そして専用回線の代わりにインターネットを利用してWANサービスを実施する最近の傾向が含まれている。企業は、従業員のモビリティがもたらすメリットと、これらの脆弱性に対処するセキュリティポリシーやシステムに関連するコストのバランスをとらなければならない。

Cisco SAFEブループリントは、個々のネットワークドメインに対する脅威と脆弱性に関する詳細な情報に加え、多層化したセキュリティソリューションによってそれを緩和するためのレファレンスアーキテクチャを提供している（cisco.com/go/safe）。

ますます複雑になるIT環境の中で、たとえ前触れのない突然の攻撃の間でもビジネスがレジリエンスを保ち続けるためには、かつてないまでの強力なセキュリティポリシーが求められている。シスコはITシステムのセキュリティの現状を評価し、そこで認識された課題へのセキュリティソリューションと運用のベストプラクティスを開発することによって、企業を支援するエキスパートセキュリティ評価サービスを提供している。この評価サービスに関してさらに詳しくは、cisco.com/packet/171_6b3で見ることができる。

Cisco Network Admission Control（NAC：ネットワークアドミッション制御）は、ルータ、アクセスサーバ、エンドポイント、およびウィルス保護ソフトを包括したキャンパスおよびブランチオフィスのネットワーク全体にわたるシステムレベルの防衛ソリューションだ。これは、Cisco NACによってネットワークがユーザーと機器のアクセスに対して識別や制限を行い、無認可や悪影響をおよぼすコンポーネントを論理的に隔離し、ポリシーのガイドラインに従い脅威に迅速に対処できるようにするものである。

キャンパスとブランチオフィス全体に張り巡らされたファイアウォールや侵入検知・防止機器は、DoS攻撃を感知して防ぎ、意図的なハッキングや妨害を阻止するのに役立つ。

CiscoWorksのSecurity Information Management System（SIMS）は、数百あるこれらの機器が作成する膨大なセキュリティデータを収集し、相互を関連づけて分析。進行中の攻撃を識別して、有効な対応ガイダンスをまとめる。Cisco Guard DDoS緩和アプライアンスは、Cisco Traffic Anomaly Detectorとの組み合わせで、DoSのトラフィックをフローからフィルタリングし、適正なトラフィックの継続を確保し、DoS攻撃下でも通常の運用の継続を実現する。キャンパスワイヤレスLANでは、Cisco AironetソリューションがIEEE 802.1x認証と無線暗号化に加え、新しいワイヤレスLAN侵入検知を提供している。

ブランチオフィスは、キャンパスネットワークとデータセンターをバックドア攻撃に晒している。しかし、セキュリティオペレータはCisco VPN、IPSec、および暗号化テクノロジーを使ってブランチオフィス接続の安全を確保することができる。ここにおいて、オペレータにはブランチオフィスのルータを迅速に封鎖する能力が必要になってくる。Cisco IOS Softwareの機能であるCisco AutoSecureは、“ワンタッチ（one touch）”のリモート機器ロックダウンプロセスを提供している。これは、ルータをスキャンして攻撃を受けているポートを閉鎖。その脆弱性を見つけて、将来の攻撃を防ぐための設定変更を提案するのである。

レジリエントなアプリケーション

ビジネスアプリケーションが常に利用可能で、いつでもアクセスできることを確認する段階にきたら、デー

タセンターが注目の中心になってくる。シスコはCisco ONS 15000光ネットワーキングソリューションやCisco MDS 9000ファミリのマルチレイヤディレクタとファブリックスイッチを使って、さまざまな媒体に対してあらゆるタイプの光およびIP SAN（Storage Area Networking）を提供している。同期および非同期のレプリケーションに対応するためには、データセンター内にあるテクノロジーの中でも、ローカルおよびグローバルなロードバランシング、バーチャルSAN（VSAN）などのインテリジェントストレージネットワーク、セキュリティ（たとえば、侵入検知とファイアウォールのセキュリティ）、およびビジネスの継続性が重要である。データセンター内のアプリケーションのレジリエンス提供に非常に重要な役割を果たすこれらのソリューション群に関しては、本誌17ページの『レジリエントなデータセンターの構築』にさらに詳しく掲載されている。

シスコは世界中の企業やサービスプロバイダへのデータセンターソリューションの提供だけでなく、ブランチオフィスのデータのためにNetwork-Attached Storage（NAS）に関連するエンド・ツー・エンドのストレージ統合ソリューションをも提供するための努力を重ねている。今までこの作業は、主にリモートロケーションから中央のファイルにアクセスする際に、エンタープライズLANに近いパフォーマンスを発揮するシスコの広域ファイルサービス（WAFS：Cisco Wide Area File Services）テクノロジーを中心に進められてきた。Cisco WAFSは、高度なプロトコルレベルのキャッシング、圧縮、ネットワーク最適化技術などを駆使して、WANを通じたファイルサーバへのアクセスに伴うレイテンシを最低限に抑える。

ブランチオフィスのユーザーは、アプリケーションのパフォーマンスが許容範囲にあることが確認できるのだ。ブランチオフィス内のCisco WAFSエッジファイルエンジンは、このテクノロジーを使ってデータセンターにある部門別サーバにつながるWAFSコアファイルエンジンに連絡する。WAFS Central Managerは、社内全体に分散しているファイルエンジン全部の管理、構成、監視、およびメンテナンスを中央集中的に行うWebベースの装備を提供する管理モジュールである（11ページの図を参照）。

ブランチオフィスのクライアントファイルサーバのリクエストは、ファイルシステムキャッシュを使ってローカルで管理するのか、リモートファイルサーバへの転送を図るのかを決定するローカルファイルエンジンに送られる。後者の場合、エッジファイルエンジンはCommon Internet File Server（CIFS）またはNetwork File System（NFS）のリクエストをカプセル化。Cisco WAFSトランスポートプロトコルを使って、WAN経由でコアファイルエンジンへ送る。このプロトコルは、WAN上のCIFSおよびNFSプロトコルの対話（chattiness）を制限し、エンドユーザーのデータ検索のための帯域利用を保護している。

コアファイルエンジンはCisco WAFSのリクエストをCIFSまたはNFSにデコードし、そのリクエストをファイルサーバに送り、応答をブランチオフィスエッジのファイルサーバを経由してクライアントへと伝送するためにCisco WAFSプロトコルにカプセル化する。エッジファイルエンジンは、実際のファイルサーバとは逆にリモートファイルサーバに対する純粋なキャッシングおよびアクセラレーションシステムとして動作する。この特性のおかげでユーザーや許可の定義と管理が不要になり、あるいはキャッシュ容量の管理も必要なくなることから、WAFSの運用とメンテナンスが簡素化される。ここでは、クライアントソフトウェアやローカルストレージも必要ない。

シスコは、WANを通じてストレージの統合に最適化されたソリューションの提供を図ってきた。さらに最近では、CiscoファイルエンジンとともにEMC NS500およびNS700シリーズの統合されたNASソリューションの販売とサポートの提供を巡ってEMCと合意した。IT管理者は、この総合的な商品によってブランチオフィスのデータのバックアップと災害時の復旧に、中央のリソースを活用できるようになる。この統合されたEMC/Ciscoソリューションの販売とサポートは、シスコの直販体制および世界中のパートナーのチャンネルを通じて実行される。

シスコは、Cisco 2600および3700シリーズのルータと新しいCisco 2800および3800シリーズのIntegrated Services Routers用のネットワークモジュールによって、ブランチオフィスの高速化およびWANコンプレッ

ション機能も提供している。Content Engineネットワークモジュールは、Real Windows Media Technologies（WMT）、Darwin、HTTP、PDF、Flash、Shockwave、FTP、およびMultimedia Messaging Service（MMS）のコンテンツを含む非常に多くの種類のファイルをCisco Application and Content Networking（ACNS）ソフトウェアが提供しているデマンドプルキャッシング（demand-pull caching）やプレポジショニング（事前配信）テクノロジーを使って配信する。このソリューションは、ソフトウェアファイル、セキュリティパッチ、業務用ビデオ、HTMLコンテンツなど多くのものの配信を高速化し、企業のアプリケーションとWAN帯域のパフォーマンス向上に貢献する。Ciscoのマルチサービスおよび総合的サービスのルータで利用できるWANコンプレッションモジュールは、フレームサイズを縮小。これにより、リンク上でさらに多くのデータを送ることを可能にし、スループットを犠牲にすることなく帯域利用を最適化する。

ネットワーク管理者はこのモジュールによってコストの高いインフラをアップグレードすることなく、アプリケーションのパフォーマンスとサービスの可用性を向上させることができるのである。

レジリエントなコミュニケーション

ビジネスのレジリエンス戦略で最も重要な要素は、レジリエントなコミュニケーションであり、それだけでも高可用性ネットワークが必要であることの正当性を実証するものとなる。企業は、各種ITアプリケーションにおける限定的な中断には耐えられるが、常時継続に近いコミュニケーションシステムの場合には、それが中断している最中やその直後を考えると、従業員の安全とビジネスフローにとって致命的なダメージとなる。

IPテレフォニー、ビデオ、およびユニファイドメッセージングのトラフィックを運ぶ高可用性ネットワークは、時間が厳しく問われる音声とビデオのトラフィックに優先順位をつけ、早く送るQoSメカニズムを利用している。Cisco Catalystスイッチでは、Cisco AutoQoSが大規模なQoS展開の割り当てと管理をするために、付加価値の高いインテリジェンスをCisco IOS SoftwareとCatalyst OS（CatOS）Softwareに組み込む。ここにおける実際の展開に基づくベストプラクティスには、シスコの専門的知識や経験がつめ込まれている。Cisco AutoQoSは、手作業による方法に比べて運用コストと時間を最大で3分の2も削減することができる。Cisco AutoQoSの最初の段階で、IPテレフォニーを展開したいがIP QoSの計画や展開の経験が足りない、あるいはそのために割り当てるスタッフの時間がないという企業のためにVoIP（Voice over IP）展開が自動化されるのである。

シスコはIPコミュニケーションのレジリエンス向上のために、その対極にある公共の電話網と同様に一から設計を始めた。CallManagersのクラスタリング、二次的データセンターの冗長クラスタリング、そしてIP電話用Power over Ethernet（PoE）、エクステンションモビリティ、911（緊急通報）ロケータのサポート、およびコールセンターの職員のためのリモートエージェント能力などの機能を長年にわたって提供してきたのである。

業界初のブランチオフィス用ルータのためのCisco Survivable Remote Site Telephony（SRST）は、本社のCallManagerクラスターにつながるWANサービスが万一中断された場合にも基本的な電話サービスを維持する。障害が発生した場合には、ローカルなCisco IOS Softwareで可能なSRSTルータが基本的なコール処理を提供し、Cisco CallManager 4.1を使ったCisco IP Phoneに対するシグナリングとメディア伝送において、認証および暗号化により安全確保をサポートするのだ。

WAN停止が頻発し、各ブランチオフィスの従業員数が240人以下の企業の場合、Cisco CallManager Expressが一般的に使われているキーシステムやローエンドのPBX（Private Branch Exchange：構内交換機）の機能をすべて提供する。そして、レジリエンスを強化するために2台のルータでCisco CallManager Expressを実行し、HSRPを使って即時フェールオーバー能力を提供する。あるいは、透過性を増すために1台のCallManager ExpressではHSRPを、もう1台ではSRSTを実行することも可能だ。Cisco Unity Expressは、ブランチのユーザーに統合されたローカルなボイスメールと自動応答システムの機能を提供する。

レジリエントな労働力

労働力のレジリエンス戦略を持たない企業は、「人財」という最も価値ある資産を浪費することになる。労働力のレジリエンスは、従業員に「いつでも、どこからでも会社のリソースにアクセスし、同じサービス下でアプリケーションの利用を強化。不測の中断に対処するパワー」を提供することである。場所と時間に縛られることなく、自由なアクセスを保証することによって、従業員が職務を遂行し、自分の生活を守るための柔軟性を確保する。すなわち、生産性と意欲を向上させることになるのだ。労働力のレジリエンスが優れた企業には、以下の要素が不可欠だ。

- 会議室、カフェテリア、ロビーの無線アクセスを通じて、Cisco AironetワイヤレスLANソリューション経由でキャンパスネットワーク全体のコネクティビティを提供するモビリティ機能。
- ユーザーが本社またはブランチオフィスのどのCisco IP Phoneにもログインでき、自分の机の電話と同じサービスを享受できる。特にボイスメールへのアクセスができるようにするIP電話のエクステンションモビリティ。
- ホテルの客室、会議場、空港のラウンジ、その他のホットスポットでブロードバンドやワイヤレスLANサービスを通じて移動中の従業員にリモートでデータと電話のサービスを提供するクライアントVPNサービスとCisco SoftPhone。
- 自宅のオフィスから安全なコネクティビティを可能にするルータ・ベースのブロードバンドVPNサービスと、Cisco IP PhoneまたはCisco SoftPhone。

企業のビジネス継続計画には、労働力のレジリエンスソリューションが含まれていなければならない。たとえば、万一、メインのデータセンターが火事や洪水で失われた場合にも、ITシステムは従業員のビジネスクリティカルなサービスへのアクセスを中断させることなく、スムーズな継続ができるように、アクティブなセッションを自動的に二次的なデータセンターへリルートしなければならない。

あるいは、悪天候で出社が危険な場合には、従業員は自宅でもオフィスと同様のサービスを使って、仕事ができる環境を築くのである。

これは極端な例だが――ホテルの客室で、にわか造りのワイヤレスLANを構築し、企業ネットワークへの安全なブロードバンド接続を確立したというシスコユーザーのケースもある。

労働力のレジリエンステクノロジーは、構成しやすく最低限の管理とユーザートレーニングで実現可能な特性を発揮するものでなければならない。たとえば、Cisco Business Readyテレワーカーは、社内ネットワークへのアクセスに、セキュリティが保証されたIPSec VPN上で音声とデータを暗号化して、PCとIP電話の単一ブロードバンド接続を活用している。リモート管理が可能なCisco 800シリーズのルータには、ユーザーには透過的な構成済みのVPN、セキュリティ、およびQoSの機能が装備されている。遠隔勤務者はテレビ会議や電話会議、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、IP電話内線サービスなど、会社の自席にいるのとまったく同じサービスを利用することができるのである。

◆ ◆ ◆

ハードウェアおよびソフトウェアの両面で非常に可用性の高いITシステムに貢献する要素、そしてネットワーク、アプリケーション、コミュニケーション、および労働力全体にわたって高いレジリエンスを構築するために適用されるリソースとソリューションに関しては慎重な検討が必要である。

それは、企業のビジネスのレジリエンス戦略をコンセプト段階から実践レベルへと転換させる、最も重要な第一歩となるはずである――。