

ポリシー ベースのコラボレーション： セキュアな業務とコミュニケーションを約束する、 エンタープライズ規模のフレームワークへの移行

このホワイトペーパーの内容

ビジネス環境は急速に変化しています。多くの孤立した地域経済から、相互接続された1つのグローバルな経済へと移行するにつれて、スピードと俊敏性が重要になってきています。組織では、物理的な会議から仮想会議への急速な切り替えが進んでおり、豊富なオンライン ツールを使用して従業員が地域やタイムゾーンを超えてコミュニケーションできるようになってきています。そういった同僚、パートナー、サプライヤ、顧客とのコラボレーションの緊密化により、コストの削減、迅速な意志決定、生産性の向上、革新のスピードアップ、開発期間の短縮などが達成されています。ブロードバンドの普及に伴い、このような移行の背景に欠かせない要素としてテクノロジーは進化してきました。モバイル機能を備えたデバイスやネットワークが利用可能になったことで、業務のモバイル化が進んでいます。サービス指向アーキテクチャ (SOA) の増加は、ソフトウェア革新のスピードを短縮します。また、サービスとしてのソフトウェア (SaaS) の導入が増えることで、これらのソリューションを使用できる世界中のナレッジ ワーカーの数が大幅に増加します。

このように、すべてをより迅速に、適切に、低コストで実現することが常に求められていることから、すべての業界、あらゆる規模の企業が、社の内外を問わずすべての利害関係者を結ぶコラボレーション機能を、ビジネスプロセスおよびワークフローに組み入れようとしています。顧客、パートナー、サプライヤ、製造業者、およびその他の外部関係者をプロセスに効果的に含めることができれば、企業では市場への投入期間を短縮し、販売サイクルを短縮し、ワークフロー全体の生産性を上げ、顧客の忠誠心や満足度を高めることができることと認識されています。しかし、これらのメリットにはリスクが伴います。インターネットによって、データやリソースは広く分散したグループ間でも透過的に共有することが可能になった一方で、ハッカーが同じデータを送信中に傍受したり、コラボレーション チャネルの脆弱性を悪用して機密性の高いデータやネットワーク リソースに不正アクセスすることも可能になりました。ほとんどの組織にとって情報は最も貴重な資産であり、ビジネスのライフラインとなるため、オンラインでのコラボレーションを望む誰もがこの問題について関心を持っているに違いありません。

本当の意味での効果的なポリシー ベースのコラボレーション ソリューションは、いつ誰とでもリアルタイムでコラボレーションでき、構造化コンテンツも非構造化コンテンツも、その保存場所を問わずに非同期で共有できるという自由を実現します。優れたポリシー フレームワークを使用することによって、さまざまなユーザとリソースの接続状況を効果的に識別し、ユーザがアクセスできる情報やオンラインのコラボレーション ワークスペースへの参加方法を、それに応じて適切に定義することができるようになります。

このドキュメントでは、コラボレーションの進化、オンプレミスおよびオンデマンドへの対応の現状、会社間のコミュニケーションをセキュリティで保護し、規制遵守要件を満たすためにはポリシー ベースのアプローチが鍵となる理由について説明します。また、シスコが

業界の中でどれほど独自のポジショニングを行っているか、お客様のためにどのような方法でこの課題に対処し、あらゆるネットワークやデバイスで信頼性を持って行えるコラボレーションを実現しているかについても詳しく説明します。ポリシー ベースのコラボレーションによるこのビジョンは、2 つの環境のそれぞれの長所を、双方とも兼ね備えています。すなわち、最も厳格な IT セキュリティおよび遵守要件を満たす一方で、ユーザは Web 上の個人用スペースやソーシャル スペースで行ってきたのとまったく同じようにワークスペースをカスタマイズできるのです。

はじめに

インターネットと高帯域幅によって常時接続のオンデマンド環境が実現され、グローバルに共同作業できるコミュニケーション環境の基盤が築かれました。しかし、ほとんどのビジネス コラボレーションは、個人で、または同じ部屋にいる人々の間で行われているわけではありません。ますます高度化する IP ネットワーク、アプリケーション、およびエンドポイントのおかげで、Voice over IP (VoIP)、Web およびオーディオ会議、E メール、インスタント メッセージング、モバイル、ビデオなどを使用して実施されています。この仮想化された共同作業の機能により、ビジネスのスピードが加速しただけでなく、多様な労働力をつなぎ、モビリティと革新を強化し、生産性を高め、コストを削減し、市場投入期間を短縮し、利益率を上げるなどの大きなビジネス上のメリットが生まれました。

コラボレーションによって、グローバルな競争の勢力図が完全に再定義されたのです。特に中規模企業では、重要なビジネス パートナーと対話するツールを持つことで、迅速な意思決定と行動ができないことが場合によっては障害となる大規模なグローバル企業に対して、競争力において優位に立てる可能性があります。

さらに、企業の成長はこれまで以上に新しい顧客へのアクセスを増やし、既存の関係を改善し、新しい市場を確立し、新しいビジネス モデルを引き出すことにかかっています。企業が競争する必要がある場所が増え、ますますモバイル化した多様な労働力を活用することが、グローバリゼーションの意味になってきています。リモート コラボレーション用のツールは普及しつつあるものの、共有情報を保護するために必要なセキュリティ ポリシーおよびテクノロジーが必ずしも適切に実装されているわけではなく、企業は定量化可能な法的および金銭的リスクにさらされています。

エンタープライズの成功にコラボレーションが不可欠な理由

さまざまな労働力をつなぎ、重要なビジネス パートナーと対話するためのツールを提供することにより、急速な成長と競争力の維持を望む企業にとっては、コラボレーションが不可欠なものとなりました。たとえば、営業担当者は既存の顧客の売上を増やし、新しい顧客を獲得し、新しいチャネルを開拓し、より大きな取引をより迅速にまとめることで業績を伸ばします。営業チームでは顧客を獲得するために利用できるあらゆるツールを使用する必要があり、企業がコラボレーション プロセスを完成させるまで待つことはできません。コミュニケーションをセキュリティで保護できない場合には、とにかく情報を共有し、うまくいくよう願うしかありません。このような現実問題には、ポリシーベースのコラボレーションで対応できます。重要なデータが侵害されるまで待つのではなく、組織でネットワークとデバイス上の情報を制御および管理するためのポリシーを適用することができるようになります。

Web 上でビジネスを行う企業もコラボレーションを活用しています。競合する商品やサービスを販売する多くの Web ベースの組織では、顧客サービスが第一の差別化要因になることがよくあります。顧客サービスの問題が発生したとき、ビジネスの維持には状況解決までのスピードが重要とな

ります。不満を感じる顧客に対しては、互換性のないポリシーを設定した従業員がいたために、ファイアウォールがファイアウォールを超えることができなかったなどということは理由になりません。顧客サービスでは、知的財産を保護するだけでなく、ビジネスを実行可能にするコラボレーションにセキュリティ対策が必要であることが明白です。コラボレーションにセキュリティ対策が施されていない場合、セキュリティ対策によって解決されるよりも多くの問題が発生することにもなってしまいます。

現在では、企業コミュニケーション ツール セットの中でも、これらの課題を満たすツールがますます一般的なコンポーネントとなってきています。リアルタイムのコラボレーションを戦略的に使用することにより、生産性の向上、意思決定の迅速化、市場投入時間の短縮、いつでもどこでも専門家にアクセスできる、顧客とサプライヤの忠誠心の向上といったメリットを実現できます。これらすべての要因が成長率と利益率の向上に結び付き、ポリシー ベースのコラボレーションは、グローバル経済の基盤として位置付けられるようになります。

ネットワークが物理的な組織を超えて拡張し続けるにつれ、ビジネスとそのエコシステムの安全なコラボレーションを実現可能にするうえで、セキュリティとプライバシー、情報の整合性、サービス品質 (QoS)、アクセス性、および信頼性が、ますます重要な役割を果たすようになってきます。

コラボレーションの課題

真にボーダーレスなエンタープライズにポリシー ベースのコラボレーション プラットフォームがあれば、ビジネスのあらゆる側面を強化する、最高のユーザ エクスペリエンスを実現できます。集中型のネットワークでは、従来のネットワーク境界の内外にいるリモート ワーカーとの間で、また、独立系の請負業者、サプライチェーンと顧客、およびより大規模なパートナーによるエコシステムへと重要な情報を伝達できます。しかし、これらのコミュニケーション手段を 1 つの安全なプラットフォームへと集中させることは、今なお対処の難しい課題です。たとえば、さまざまなベンダーが使用する古い機器やアプリケーションをネットワーク接続し、隔離した場所にあるデータへとアクセスするようにし、ユーザのトレーニングをほとんど、またはまったく必要としないような使いやすいインターフェイスの背後にすべてを隠してしまう必要があります。

ただし、強力な企業ポリシーと包括的なポリシー管理ソリューションが実装されていなければ、組織の最も貴重な資産である情報が侵害されてしまう可能性があります。Identity Theft Resource Center (ITRC) によれば、2007 年には 1 億 2700 万のデータ レコードが脅威にさらされています。この種類の脅威は、エンタープライズに大きな金銭的被害をもたらす可能性があります。独立系のプライバシー管理調査会社、Ponemon Institute によって実施された調査では、2007 年に平均的なデータ侵害によって米国企業でデータ レコードあたり 197 ドルの損害が発生したことが報告されました。

オンプレミスと電子ネットワークの両方で非常に貴重なビジネス資産を保護し、単一障害ポイント (SPF) を回避するには、包括的なポリシー ベースのアーキテクチャが必要です。動作を動的にプロファイリングするソリューションがあれば、インフラストラクチャ全体でのきめ細かなアクセス制御も提供できます。

セキュリティ上の懸念事項に対する強力なポリシー アプローチ

現在のビジネス環境には、非常に複雑で裁判管轄権ごとに異なる多数の遵守要件があります。従来の境界セキュリティをコラボレーション テクノロジー用の複雑な戦略と統合することにより、組織では Sarbanes-Oxley、Gramm-Leach-Bliley (GLB)、Health Insurance Portability and Accountability Act (HIPAA)、Payment Card Industry (PCI) Data Security Standard、European Basel II、およびその他の規定に含まれるセキュリティ要件とプライバシー要件に効果的に対応できます。

境界セキュリティとコラボレーション テクノロジー用の戦略が実装されていても、ネットワークはまだ脆弱である可能性があります。たとえば、ユニファイド コミュニケーション インフラストラクチャ内で

最も脆弱なリンクを露呈させるクロスベクター攻撃が、ネットワーク接続された環境の他の部分に対して実行される場合があります。ハッカーは、よくモバイル ハンドヘルド デバイスをターゲットにして、ラップトップ コンピュータなどの他のコンピューティング デバイスに実装されている強力なセキュリティを迂回します。クロスベクター攻撃やその他の潜在的な脅威からモバイル デバイスを保護するには、組織では大規模なセキュリティ ポリシー戦略にワイヤレス セキュリティ ポリシーを統合する必要があります。

確実な遵守と貴重な企業資産の保護に役立つセキュリティ ポリシーの統合は、安全なコラボレーション戦略のほんの一部です。信頼性の高いコラボレーションを実現し、データの整合性とリソースの可用性を確保するには、組織はデータへのユーザ アクセスとデータ自体を効果的に管理する必要があります。ID 管理ツールは、組織がユーザ、グループ、役割、属性を管理するのに役立ちます。たとえば、ID 管理ツールを使用して、組織でのユーザの役割に基づいて特定のデータへのアクセスを制限できます。同様に、データ分類ツールを使用すると、エンタープライズの IT リーダーがコラボレーション チャンネル経由で移動する情報の種類と価値を理解できるため、どのユーザ、グループ、役割がデータにアクセスできるかを決定できます。ID 管理ツールとデータ分類ツールの両方を共に稼働させ、可能な場合にはポリシー管理インフラストラクチャに統合することによって、コラボレーション用の安全なプラットフォームとして機能するようにエンタープライズ ネットワークの機能を強化する必要があります。

ポリシー ベースの戦略がメリットとなる業界共通のシナリオ

ビジネスにとってコラボレーションとネットワークレベルでのセキュリティが重要な場合には、ネットワーク ファブリックの一部としてのポリシー管理および適用も重要になってきます。現実的な観点から、セキュリティ機能は、標準ベースで管理がしやすく、コラボレーション プラットフォームに透過的に統合されていて、導入と管理のコスト効率が高く、テクノロジーとプラットフォームの間で協調し、各企業固有のニーズに適合できる拡張性を備えている必要があります。同時に組織では、データ、VoIP、インスタント メッセージングとプレゼンス、Web、コラボレーション ワークスペース、オーディオ会議とビデオ会議を含め、すべてのアプリケーションで目標、役割、使用パターンを定義して、ビジネスの観点からポリシー管理を適用する必要があります。

以下のシナリオ例では、ポリシー ベースの戦略の実装が具体的なビジネス メリットの実現にどのように役立つかを示しています。また、包括的なポリシーが備わっていないことが原因となり、不慮のセキュリティ違反によって発生してしまう、深刻な影響の可能性についても説明しています。

金融サービス

投資銀行業務では、正式な完成文書を構成していくプロセスの中で、追加する情報を専門家が同僚とよく共有します。このシナリオでは、金融アナリストが、医薬品業界に関するリサーチ レポート草案を共有して、フィードバックを集め、事実に対する正確さを確保します。彼女は同僚に電話してレポートの草稿のレビューを依頼しようとして、彼女の知らない間に、同僚は最近仕事が変わって同じ会社のブローカーになっており、医薬品業界の株を機関投資家に販売しています。同僚の職務が変わったため、組織の強力なポリシー管理フレームワークによって電話は自動的にブロックされます。彼女は E メールとインスタント メッセージで同僚と連絡を取ろうとしますが、これらもブロックされます。ポリシーが適用されていないと、会社は倫理的な壁を規定する重大な SEC 規則に違反し、多額の罰金を科せられていたことでしょう。この例は、倫理的な従業員でも、悪意なしに非常に深刻なポリシー違反を犯す可能性があることを明確に示しています。幸い、強力なポリシーおよび管理フレームワークによって、この不慮のコミュニケーションは防止され、会社は数百万ドルの罰金を払わずに済みました。

石油とガス

石油探査は非常に高コストでリスクを伴うため、企業ではよく共同事業を作ることで新しい油田掘削コストを分担します。各参加者は、掘削場所、掘削方法、およびその他の技術ノウハウに関する知的財産を提供する場合があります。関与する企業も互いに競争しているため、共同事業に関与し、厳格な秘密保持契約に署名した、権限を持つ人物だけがコラボレーション サイトへのアクセスを許可されることが重要です。これらの機密文書およびコンテンツへのアクセスまたは権限を管理するポリシー システムがないと、このパートナーシップは失敗してしまう可能性があります。各企業が、競争上の懸念から知識の大半を共有するのを拒否する可能性が高いためです。ただし、強力なポリシー ベースのアーキテクチャがあれば、業務上の適切な役割を持つ人物だけが、適切な状況および条件下でのみ機密データにアクセス可能になるようにできます。たとえば、ポリシー システムでは、ユーザが公共の Wi-Fi ネットワーク経由でアクセスしている場合、コラボレーション サイトへのアクセスをブロックすることができます。このようなポリシー制御が実装されていれば、プロジェクトを進めていくことができます。

政府

国や州政府では、信頼できて同じ国籍の少数の人物にのみ、情報を公開する必要が生じることがあります。このシナリオで、米国政府は選ばれた他の国々と共有するテロ警戒データベースを構築しています。最近発生した爆撃の後、インド政府は自国の諜報レポートと比較するために、このデータベースへのアクセスを要求しています。情報は非常に機密性が高く、国家の安全保障を侵害する可能性があるため、米国政府はその共有について危惧しています。しかし、インドは同盟国であるため、米国政府は選択されたレコードを一定期間、インドの最高諜報機関の指名された数人のみに提供することを決定します。ポリシー管理システムでは、情報にアクセスできる人物、情報の使用方法、および情報を利用可能な期間に関するアクセス制御を適用することで、この情報開示とアクセスを非常に限定的なものにすることができます。

適用可能なポリシー管理によるコラボレーションの最適化

前述の金融サービス、石油とガス、および政府のシナリオで要求されるポリシー主導のテクノロジーはすでに存在します。あとはこれらを包括的なプラットフォームに統合するだけです。シスコのビジョンは、内部と外部のデータ ソースを含め、エンタープライズ全体を網羅するソリューションによってコラボレーションを最適化することです。このソリューションは、セキュリティおよび管理ポリシーを自動的に適用する一方で、データ センターからデスクトップまで、それぞれに応じた価値を提供する企業間のコラボレーションを可能にします。

企業の IT 管理者がコラボレーション環境のセキュリティ課題を満たすことができるよう、シスコは最高水準の安全性と整合性を備えるようにコラボレーション プラットフォームを設計しています。以下の Cisco® の安全なコラボレーション ソリューションは、多種多様なアプリケーション、デバイス、ネットワーク、およびオペレーティング システム全体でビジネスの生産性と俊敏性を高めます。

Cisco TrustSec および Cisco IOS Software による安全なインフラストラクチャ

安全なインフラストラクチャは、安全なコラボレーション環境の基盤となる構築ブロックです。高可用性の維持 (QoS など) と動的なアクセス管理 (VLAN など) によって安全なコラボレーションが可能になり、デバイスとデータ パケットの動的なタグ付けによって、ネットワーク全体にセキュリティ ポリシーを確実に適用するのに役立ちます。組織の既存の IT 投資を利用し、スケーラブルなスイッチセキュリティ サービスを提供する新しいアーキテクチャである Cisco TrustSec を導入することで、以下の方法によってこれらのメリットを実現できます。

- 安全なキャンパス アクセス制御: 重要なアプリケーションおよびリソースへ一貫した役割ベースの ID と管理アクセスを提供します

- 集中型のポリシー フレームワーク:さまざまな役割、サーバ、およびアクセス定義を集中化し、ID ポリシーの管理を簡素化します
 - 広範囲の整合性と機密性保持:規制要件に対応するためにデータ漏えいを防止します
- また、シスコのルーターは、ネットワーク インフラストラクチャへのサービス拒否 (DoS) 攻撃やその他の脅威を防止するのに役立ち、堅牢で適応性のあるセキュリティ ソリューションを提供します。ルーターの Cisco IOS® Software は、Cisco IOS Firewall、Intrusion Prevention System (IPS)、IP Security (IPsec)、Secure Sockets Layer (SSL) VPN などの包括的な[セキュリティテクノロジースイート](#)を提供します。これらのテクノロジーのメリットは、次のとおりです。
- 新しいハードウェアを導入せずに保護を追加: Cisco IOS Software を使用して既存のルーター上で新しいセキュリティ機能を有効にします。
 - 企業が最も必要とする場所でセキュリティを強化:遠隔地の支店を含め、ネットワーク内のあらゆる場所にファイアウォールや IPS などのセキュリティ機能、および集中管理型デバイスやポリシー管理を適用します。
 - 時間とコストの節約:ネットワーク内のデバイスの総数が削減されるため、継続的なサポートおよび管理コストが削減されます。

シスコのデータ損失防止ソリューション

コラボレーションに関連する重大な懸念事項は、ネットワーク境界を通過するトラフィック量が増加することです。シスコのデータ損失防止ソリューションは、以下の方法によって規制遵守とデータの整合性を維持するように設計されています。

- ネットワーク アクセスを許可する前にユーザとデバイスを認証する (Cisco Network Admission Control [NAC] を使用)
- エンドポイントのデバイスに保存されている機密情報のリアルタイム インベントリを提供し、情報が誤って権限のないユーザに送信されたり、リムーバブル メディアにロードされたりするのを防ぐためのセキュリティを提供する (Cisco Security Agent を使用)
- E メールをフィルタリングして機密情報が E メール経由で転送されないようにする (Cisco IronPort® テクノロジーを使用)

Cisco WebEx Connect

Cisco WebEx® Connect によるセキュリティ機能の要素とレイヤの多くは、企業データと個人データを保護し、不正アクセスを防止し、ビジネス上の機密情報を守るように設計されています。シスコは、物理サイト、アプリケーション、ネットワーク セキュリティにおいて業界標準のベスト プラクティスを採用することで、Cisco WebEx Connect のお客様に対して最高レベルのセキュリティを実現しています。また、Cisco WebEx Connect では、シスコが 2007 年後期に Securent を買収したことで取得した優れた権限およびポリシー管理製品である Cisco Enterprise Policy Manager も使用できます。

Cisco WebEx Connect コラボレーション プラットフォームは、正確なポリシー決定を行うためのユーザの役割、リソース、時刻、ネットワークの場所、デバイスの状態、プロジェクト ID など、さまざまな属性と任意の数の属性に対応できる優れたポリシー エンジンを提供することで、本当の意味で効果的なポリシー ベースのコラボレーション ソリューションの要件を満たします。また、Cisco WebEx Connect では適切な管理者が柔軟なポリシー モデリングおよび委任を行うことができるように、ビジネス プロセスに対応付けられたセキュリティ ポリシーを設定することで、ネットワークとコンテンツへのアクセスを厳重に管理できます。さらに、Cisco WebEx Connect では以下のことが実現できます。

- 異なるエンタープライズ コラボレーションおよびメッセージング製品の統合。これは、生産性を向上するために不可欠なことでありますが、追加のサードパーティ製品は必要ありません
- 堅牢なパフォーマンスと信頼性。このためには、マルチレイヤ型のアプローチとすべてのシステム コンポーネントを完全に冗長化することによって、すべての単一障害ポイントを除去することが必要です
- エンド ユーザの操作や管理者のトランザクションを含めた、すべてのイベントの詳細なログ。これはセキュリティと遵守を確実にするために不可欠です
- インスタント メッセージングとオーディオ、ビデオ、Web 会議を統合する拡張可能なプラットフォーム。非同期のコラボレーションを強化し、企業では、変化するユーザのビジネス ニーズに対応できるようになります

Cisco Enterprise Policy Manager

このホワイト ペーパーに記載されている目標を実現するには、ユニファイド コミュニケーションおよびコラボレーション ソリューションと統合された堅牢なエンタープライズ ポリシー管理プラットフォームを各組織で導入する必要があります。Cisco Enterprise Policy Manager (EPM) は、シスコ ユニファイド コミュニケーション製品と Cisco WebEx Connect を含め、さまざまなエンタープライズ アプリケーションおよびデータ ストアに対して豊富できめ細かな権限管理機能を提供します。Cisco EPM を使用して、ユーザによるドキュメントへのアクセス、レポートの表示、トランザクションの実行、チャット セッションへの参加、別のユーザとのコミュニケーションを制御するポリシーを管理できます。各アプリケーション サイロの外部にポリシーを配置し、外部で権限を管理することにより、組織ではこれらのポリシーを異種アプリケーション間で一貫して適用し、集中的に管理と監査を行うことができるようになります。

クライアントレス SSL VPN

クライアントレス SSL VPN を使用すると、移動中でも展示会用のキオスクでも、リモート ユーザは基本的にすべての場所またはデバイスから企業リソースにアクセスできます。また、クライアントレス SSL VPN は、ユーザ認証に基づいて動的にアクセスを制限できます。このため、ネットワーク アクセスを必要としてもクライアントをインストールできず、あらかじめ決められたアプリケーションまたはリソース セットのみアクセスする必要がある、請負業者またはゲスト ユーザに最適なソリューションになります。

Cisco Secure Desktop

Cisco Secure Desktop は、SSL VPN ソリューションと連携してエンドポイントのマシンに仮想デスクトップを作成します。数千もの HTML 以外のアプリケーションをすぐに変換できるため、HTML Web ブラウザ内で動作し、遅延の影響を受けやすいアプリケーションをサポートでき、完全に安全な作業環境内で LAN のようなエクスペリエンスを実現します。

Cisco ASA Adaptive Security Appliances Phone Proxy

Cisco ASA Adaptive Security Appliances Phone Proxy を使用すると、臨時のテレワーカーが Cisco IP Phone を自宅のネットワークに差し込み、ネイティブの電話暗号化機能を使用して企業ネットワークへの安全な接続を作成することができます。この機能は、テレワーカーの生産性とコラボレーションを強化する統合コミュニケーション ツールを提供することで、オフィス内のエクスペリエンスをリモート ワーカーへと拡張します。Cisco ASA Phone Proxy では、デバイスを認証し、暗号化された接続を終了し、電話を内部の電話ネットワークに関連付け、暗号化されたリモート電話と内部ネットワーク内の暗号化されていない電話ネットワークとの間の接続を暗号化および復号化できます。これらの処理は、音声接続に必須となる、遅延の影響を受けやすい帯域幅を維持するために必要とされる QoS を提供しながら実行されます。さらに、Cisco ASA Phone Proxy は、ネット

ワーク内のサービスおよび生産性をリモート ユーザに提供します。これには、追加のルーターまたは VPN デバイスを自宅オフィスに導入する必要はありません。

Cisco ASA Presence Federation

Cisco ASA Presence Federation は、シスコおよび Microsoft の Presence Server 間で安全な接続を作成して、企業間のコラボレーションをセキュリティで保護します。

Cisco ASA Mobility Proxy

Cisco ASA Mobility Proxy により、さまざまなモバイル デバイスを内部ネットワークに安全に接続することができます。

Cisco Virtual Office

リモート ワーカーが使用できるツールを拡張すると、リモート ワーカーと一元管理されるワーカーとの間のコラボレーションがより強化されます。Cisco Virtual Office ソリューションは、製品、テクノロジー、サービスを組み合わせて、テレワーカーや遠隔地にいる従業員に、安全で充実した管理可能なネットワーク サービスを提供します。ソリューションのコンポーネントには、リモート サイトのプレゼンス、ヘッドエンドのプレゼンス、管理機能のセット、および導入と継続的な保守を容易にするサービスがあります。

Cisco Virtual Office は、オフィス リソースのデータ、ワイヤレス、音声、ビデオ、および TelePresence サービスを提供することで、自宅またはリモート オフィスにいるユーザの柔軟性と生産性を高めます。これらの機能を堅牢なセキュリティと共に実現することで、シスコでは、自宅から作業しながらスケジュールを管理する柔軟性をユーザに提供しています。このソリューションは、自動化されたゼロタッチの導入モデルを通じて保守されます。これによって時間とコストが削減され、IT 部門の効率性が大幅に向上します。Cisco Virtual Office ソリューションは、居場所を問わずにワーカーを強化することで、ビジネスの生産性を高めます。

信頼性の高いコラボレーション

コラボレーションによって、組織は生産性を高め、革新を加速し、競争上の強みを得るチャンスを獲得できます。組織、コミュニケーションの方式、およびネットワークが進化し続けるにしたがって、コラボレーションを可能にする、より動的で安全なインフラストラクチャを作成するニーズが急速に増えていきます。このことを念頭に置いて、シスコでは、組織が内部および外部の利害関係者と信頼性の高いコラボレーションを実行するための主なステップを明確にしています。

ステップ 1. コラボレーション エコシステムの明確化

信頼性の高いコラボレーションを実現するには、任意の場所の間で対話を可能にし、オンプレミス グループをインターネット経由で他者と接続するコラボレーション エコシステムがエンタープライズに必要です。このステップによって企業間のコラボレーションが強化され、ファイアウォールの両側にいるユーザは、セキュリティ違反や遵守について心配せずにコミュニケーションできるようになります。組織ではまず、ソリューションおよびサポートされるテクノロジーの範囲を含めたコラボレーションの目的だけでなく、ニーズやテクノロジーの進化に応じた改良と拡張を可能にする、将来に目を向けた柔軟な戦略を明確に定義する必要があります。このアプローチによって、組織は競争力を維持できると同時に、将来のセキュリティおよびコラボレーション要件を満たすことができない高価なデバイスまたはソリューションを置き換える必要性を回避することができます。

ステップ 2. ポリシーの定義

次のステップは、ポリシーで定義されるボーダーレス エンタープライズの定義です。このボーダーレス エンタープライズでは、誰もが信頼性を持ってコラボレーションを

行い、状況に応じた情報を共有することでビジネスの革新を加速させることができます。この環境内のネットワークでは、基盤となるネットワーク セキュリティとコラボレーションに対応したセキュリティ アプライアンスとの密接な相互運用によって、安全で信頼できるコミュニティを実現します。このアプローチでは、動的でカスタマイズされた動作の定義を有効にする企業ポリシーを普遍的に導入することに加え、これらのポリシーの遵守を実施していくことが必要となります。このボーダーレス環境内にコラボレーション ツールを安全に導入するには、ポリシーを大規模な企業セキュリティ ポリシーおよびネットワーク ポリシーと統合する必要があります。この統合によって、新しいコラボレーション ソリューションを導入する機能を既存のポリシーが誤って制限することや、基盤となるセキュリティおよびネットワーク ポリシーが対応していない新しいリスクがこれらの新しいコラボレーション ツールによってエンタープライズにもたらされることが回避されます。

ステップ 3. コラボレーション カルチャーの創造

エンタープライズは変化し、在宅勤務者、リモート オフィス、出張を行うワーカーの数が増えました。より多くの従業員がより多くの場所に存在するようになり、サービスとストレージは必要な場所で必要なときに使用できることが求められています。この環境でのコラボレーションの場は、自宅や外出先へと移行していき、インテリジェントなリモートおよびネットワーク セキュリティ テクノロジーと広範なネットワークおよびコラボレーション サービスとの統合が必要になります。この統合アプローチによって、コミュニケーションの発信元となる場所や使用するデバイスまたはアクセス方式に関係なく、ポリシーによって管理されるアクセスと詳細なトラフィック検査の両方が可能になります。

このビジョンを可能にする主なテクノロジーの 1 つが、リソースの割り当てと管理です。これは、ネットワークで利用可能な帯域幅をすべて消費せずに、適切なユーザに対して優れたコラボレーションエクスペリエンスを確保するのに役立ちます。コラボレーション カルチャーをサポートする環境では、ポリシー ベースのソリューションがゲートキーパーとして機能し、アクセスを必要とするユーザに対してアクセスを拒否せずに、ユーザの動作を変更します。

結論

ユニファイド コミュニケーションは、それによって可能になるコラボレーションと並んで、単なる効率化ツール以上のものになりました。このため、エンタープライズの経営陣の主な懸案事項は、その戦略になってきています。これらのテクノロジーを最も効果的に導入して使用する組織は、より迅速に行動できるようになり、現在の競争環境において差別化を図っていくことができます。

このレベルでの安全なコラボレーションを実現する最適なソリューションには、動作を動的にプロファイリングし、ネットワーク レベルできめ細かなアクセス制御を提供する、包括的なポリシー ベースのアーキテクチャが必要です。このアプローチによって遵守に関する懸念が解消され、場所や時間を問わずに、誰とでもどのデバイスでも、ユーザとエンタープライズは信頼性を持ってコラボレーションを行うことができます。

シスコでは、企業の構内とリモートの両方でコラボレーションを行う従業員、およびホスティング型の Web ベースのプラットフォーム上で作業する従業員のニーズを理解しています。シスコの目的は、それぞれ固有のやりとりに対して、適切なレベルのセキュリティと QoS を提供する共通のプラットフォームを提供することです。安全なコラボレーション環境の構築を可能にすることによって、シスコはビジネスが実際に機能する速度を上げ、組織がリスクを負うことなく自由に共有、動機付け、革新、協力、すべてのトランザクションの実施を行えるようにすることで、信頼性の高い安全なコラボレーションを実現します。

©2009 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter>

お問い合わせ先