

## ユニファイド コミュニケーション対応エンタープライズのセキュリティ

統合されたコミュニケーション システムは本質的に、従来の独立した電話やメッセージング システムよりも安全です。

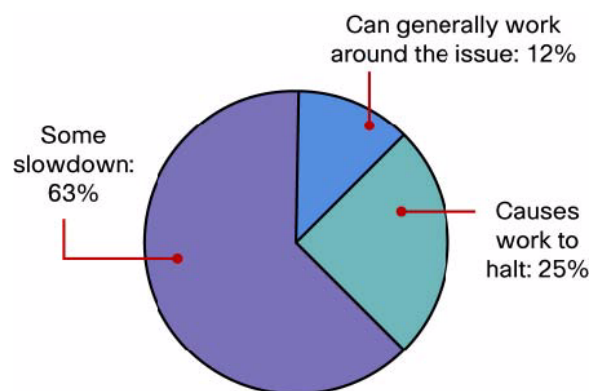
### ビジネス コミュニケーションの課題

今日のグローバル経済では、以前と異なり時間的および地理的な境界は消滅しつつあります。顧客の場所やタイムゾーンを問わずサービスを提供できるように、多くの企業が 24 時間の顧客対応体制を取っています。

企業、行政機関、学術機関がこのダイナミックな市場で生き延びていくには、他の職員や顧客といつでも連絡が取れるようにしておく必要があります。顧客と同じく、従業員も地理的に分散し、絶えず移動しているため、組織が競争において優位に立つには、従業員がどこからでも安全に情報を取り出せるようなくみが必要です。

現実には、主要意思決定者への連絡に時間がかかるとビジネスに多大な影響が及ぶことが調査で明らかになっています (図 1)。それぞれ独立したシステムをいくつも運営している組織の場合は、さまざまなコミュニケーション形態を一括して安全に管理する方法がなければ、さらに遅延は悪化します。

図 1 主要意思決定者への連絡の遅れがビジネスに与える影響



Source: Forrester Research, March 2005 Next-Generation Communications Study

### シスコ ユニファイド コミュニケーションはどのように役立つか

さまざまな種類のコミュニケーション方法を一つにまとめれば、連絡の取りやすさの向上というグローバルな組織のニーズに対応できます。テレフォニーに特化した製品とテクノロジーで構成されるシスコ ユニファイド コミュニケーションは、このニーズに応えるために、音声、ビデオ、データ、およびコラボレーションの各アプリケーションを安全に統合してデスクトップやモバイル デバイスで利用できるようにするソリューションです。シスコ ユニファイド コミュニケーションを構成しているのは、シスコおよびパートナーが提供する統合 IP テレフォニー、メッセージング、プレゼンス (ユーザの場所の情報と応答可能かどうかを

示すステータス)、モビリティ、ホワイトボード、音声/ビデオ会議などの製品とテクノロジーです。これらのコラボレーション機能を組み合わせると、従業員どうしの連絡が取りやすくなり、顧客サービスの向上につながります。

#### 意思決定の時間短縮

いくつもの機能を組み合わせて連携させることは、社内コミュニケーションのスピードアップに大きく貢献します。たとえば、電子化された名簿の名前を一つずつクリックするだけで自動的に電話会議が生成できれば、情報交換や意思決定の時間が短縮されます。そうでなければ、参加者の名前と電話番号をいくつもの名簿から探し出して、全員に電話をかけ、相手が不在ならば折り返し電話をかけてもらうようにメッセージを残さなければなりません。電話がかかってきたときに携帯電話とデスクトップ電話の両方で呼び出し音が鳴るようにしておけば、ほぼどこからでも電話に出られるので、非生産的な「テレフォン タグ」(電話を掛け合うが相手が見つからない状態)はなくなります。連絡が取りやすくなれば、ビジネスプロセスがスムーズに進行します。

#### コール センターとカスタマー サービスの質の向上

テレフォニーに顧客データを統合すれば、コール センターなどの組織全体で最新の顧客履歴へのアクセスができるようになります。この最新の顧客情報へのアクセスに加えて、チャットとインスタント メッセージを利用した他の従業員や専門家へのすばやい問い合わせが可能になれば、全体的なカスタマー エクスペリエンスの向上が期待できます。

#### 生産性の向上

同様に、セキュリティが確保されたただ一つのメールボックスに複数の電話機、電子メールシステム、および FAX 機からのメッセージが収集されれば、いくつものメッセージング システムの確認と管理にかかる時間と労力の無駄がなくなります。メールボックスを一本化すれば、すばやい応答が可能になり、メッセージの見落としや返信の遅れが減るため、個人の生産性が向上します。見落としや返信の遅れは、ビジネスに手痛い影響を及ぼす可能性があります。

2005 年に The Radicati Group, Inc. が実施した調査によれば、統合メッセージングだけで労働者 1 人あたり 1 日最大 40 分の生産的な時間の増加が可能です。シスコの委託を受けて Sage Research が 2005 年に実施した調査では、200 を超える組織へのインタビューが行われ、完全な機能を備えたユニファイド コミュニケーション システムにアクセスできる労働者は 1 日あたり平均 55 分の生産性向上を達成していることが報告されています。

集約による資本コストおよび運用コストの節約という基本的な効果の他にも、シスコ ユニファイド コミュニケーションには多数の利点があり、生産性を向上させると共に、企業のカスタマー サービス改善を通して競争力を高めるのに役立ちます。しかし、これらの利点を最大限に活かすには、ユニファイド コミュニケーション ネットワークのセキュリティが保証されていなければなりません。ユニファイド コミュニケーションには、企業の音声ネットワークのセキュリティに関するさまざまな新しい課題が伴いますが、実際には、会話とメッセージの機密性は従来のテレフォニー ネットワークよりも優れています。

#### セキュリティに関する機能と考慮事項

セキュリティ面での懸念事項と解決策のいくつかは、電話料金詐欺のように、ユニファイド コミュニケーション環境においても従来の電話網と変わりません。ただし、今日では会話のプライバシー、メッセージの機密性、およびユーザとデバイスの認証に関する法規制がますます厳しくなっています。したがって、ユニファイド コミュニケーション導入の計画を立て

るときは、グローバル組織に直接影響を与える米国の SOX (Sarbanes-Oxley) 法、GLB (Gramm-Leach-Bliley) 法、HIPAA (Health Insurance Portability and Accountability Act)、PCI (Payment Card Industry) データ セキュリティ基準、ヨーロッパの Basel II などの規定におけるセキュリティ要件に対処する必要があります。

セキュリティをインフラストラクチャの中に統合すれば、DoS (サービス拒絶) 攻撃やワームのような、通常はデータ ネットワークを標的にしているものの、攻撃に成功すれば音声 ネットワークにも影響を及ぼす可能性のある悪質な活動を未然に防ぐことができます。

シスコ ユニファイド コミュニケーションへのセキュリティの統合による保護の概要を次に示します。

#### 会話のプライバシー

前述のように、電話機能および関連アプリケーション (ディレクトリ、メッセージング システム、予定表など) を社内データ ネットワークに追加する場合は、会話のプライバシーを保護しなければなりません。音声会話のセキュリティの点では、シスコ ユニファイド コミュニケーション ネットワーク環境の方が従来の電話システムよりも優れています。

このようなセキュリティを実現できるのは、シスコ ユニファイド コミュニケーション システムでは音声会話の暗号化が可能となっているからです。この暗号化は電話機と電話機の間で行われるので、会話のセキュリティはエンドツーエンドで維持されます。したがって、暗号化された電話での会話に盗聴者が侵入してきたとしても、会話の内容は判別不可能です。

#### メッセージの機密性

同様に、今日の統合ボイスメール システムでは、プライバシーのレベルを高めることが可能です。会社の電話内線番号に制約を設けて、何ができ、何ができないかを定めるルールを指定できるようになっています。たとえば、特定のメッセージの転送を許可する一方で、「プライベート」のマーク付きのメッセージは転送しないようにボイスメール システムを設定します。同様に、特定の個人には第三者からのボイス メッセージを電子メールで受信することを許可し、他の従業員には禁止するように電話システムを設定することもできます。

#### 認証と検証

ネットワーク上のユーザ、デバイス、およびトラフィックの認証と検証は、どの企業のセキュリティ戦略にも不可欠です。セキュリティが万全ではない音声システムは、組織のビジネス プロセス中断を狙ったデータ ネットワーク攻撃のアクセス ポイントとして利用されることもあります。このような攻撃を企てる者は、悪意のあるデータを音声トラフィックに見せかけて送り込もうとします。この偽装した音声トラフィックが従来のデータ セキュリティ システムを通過して標的に到達することを狙っているのです。

しかし、シスコ ユニファイド コミュニケーション システムではこのようなことは起こりません。ネットワーク上のすべてのトラフィックが検査され、音声トラフィックとデータトラフィックが分離され、音声トラフィックに見えるトラフィックが本当に音声かどうかの確認が行われます。

同様に、ネットワークに接続されたパーソナル コンピュータをハッカーが操り、プリンタ、FAX 機、あるいは電話機に見せかけて攻撃をしかけることも考えられます。このデバイス スプーフィングは、不正なデバイスの検出と検出後の除去を回避する手段としても使われることがあります。このような攻撃を防ぐために、シスコ ユニファイド コミュニケーション ネットワークでは、すべての電話機 (有線とワイヤレスの両方) およびその他のテレフォニー関

連機器の認証が行われ、ネットワーク上での使用を許可されたデバイスかどうかの検証が行われます。企業、ワークグループ、および個人の生産性に不可欠なコミュニケーションの完全性は、このようにして守られます。

最も単純でありながら最もありふれた脅威の一つに、攻撃者が他の人物になりすまして電話をかけ、機密情報へのアクセスを狙うというものがあります。企業の中には、顧客サービス自動化を目的として発信者識別情報を利用しているところもあります。この情報は、着信電話の番号と発信元の名前を組み合わせると発信者を識別するものです。攻撃者はこれに対処するために、偽の発信者識別情報を送信して正当な発信者を装います。

しかし、最近承認された国際的セキュリティテクノロジー基準が採用されているユニファイド コミュニケーション システムでは、発信側デバイスに追加のクレデンシャルを要求して、そのクレデンシャルをネットワークによって検証するようになっています。この検査によって、デバイスの正当性が確認され、識別情報偽装のリスクが軽減されます。

### 電話料金詐欺の防止

電話料金詐欺とは、企業の電話システムに電話をかけて長距離ネットワークにつながることで、企業の許可なく電話を使うことです。この種の攻撃は、外線発信可能な内線番号への転送を禁止するだけで防止できます。

ユニファイド コミュニケーションには、電話の転送やメッセージ通知の送信などの機能を使用できる電話番号を制御する機能が統合されています。ポリシーとシステムを適切に設定すれば、長距離用電話番号へのアクセスを防止できるだけでなく、電話料金詐欺に一般的に使われる番号、たとえば国際電話番号を制限することもできます。

### 分散型 DoS 攻撃の防止

ユニファイド コミュニケーションに対する最大の脅威はおそらく、コンピュータ データ ネットワーク内のオペレーティング システムとアプリケーションを狙った分散型 DoS (DDoS) 攻撃によるものでしょう。基盤となるデータ ネットワークを保護するように設計された適切なセキュリティ対策が講じられていれば、本質的にユニファイド コミュニケーション システムは DDoS 攻撃から守られるので、偽のメッセージが大量にネットワークに送りつけられたために発生するダウンタイムも回避できます。

ネットワーク全域の戦略上重要な場所に展開される、シスコ ユニファイド コミュニケーションのセキュリティ ソリューションは、DDoS 攻撃の検出だけでなく、悪質なトラフィックの識別とブロックをリアルタイムで、正当なビジネス クリティカル トランザクションの流れに影響を与えることなく実行することができます。最大規模の攻撃を受けてもシスコの DDoS 対策製品がすみやかにその影響を緩和し、コミュニケーション トラフィックの継続性を維持すると共に、重要な資産を常に確実に保護します。

### ベスト プラクティス

ユニファイド コミュニケーションのセキュリティを確立するには、組織のネットワーク インフラストラクチャにすでに組み込まれている、データ保護のためのセキュリティ機能を活用します。基盤となるデータ ネットワーク インフラストラクチャをウイルス、不正アクセス、および盗聴から守るためのベスト プラクティスに従うことは、音声会話と関連アプリケーションを保護するうえで重要です。

ユニファイド コミュニケーション ネットワークのセキュリティを確保するには、音声、データ、およびビデオのコミュニケーションを一つのシステムとしてとらえ、このシステムを構成する次のようなコンポーネントをすべて保護する必要があります。

- ・ 基盤となるネットワークおよびアプリケーションのインフラストラクチャ
- ・ 電話スイッチ（コールサーバとも呼ばれる）
- ・ 個々の電話機
- ・ 各種のユニファイド アプリケーション

このようなコンポーネントのそれぞれを保護するには、組織全体のさまざまなスキル セットを集約し、音声、ネットワーク運用、セキュリティ運用、電話運用、およびビジネス上の意思決定者が一体となって協力する必要があります。

従業員の勤務地の地理的分散が進むにつれて、遠隔地からの冗長接続の構築も必要になります。冗長化しておけば、分散したユニファイド コミュニケーション機器と中央の電話スイッチとの間でのダウンタイムを防ぐのに役立ちます。音声コミュニケーション関連のすべてのネットワーク トラフィックを論理的にデータ トラフィックから分離させることができるので、音声トラフィック セグメントがデータ ネットワーク リソースに送信されることはなくなります。

### まとめ

シスコ ユニファイド コミュニケーションは、テレフォニーに特化した、データ ネットワーク上で実行されるアプリケーション、デバイス、およびシステムを統合したソリューションであり、次のように多数の利点があります。

- ・ 従業員の生産性と連絡の取りやすさの向上。これは最終的にカスタマー サービスレベルの向上につながります。地理的な境界やタイムゾーンを乗り越える今日のグローバル市場において、連絡の取りやすさはますます重要になっています。
- ・ セキュリティ レベルの向上。重要な音声サービスの継続性を維持すると共に、プライバシーに関する世界各国の規定に対応するのに役立ちます。
- ・ 従業員コミュニケーション管理に関連した時間の節約。
- ・ ネットワークの統合と集約に伴う資本コストおよび運用コストの節約。

テレフォニー コミュニケーションをネットワークに追加するときには発生する、セキュリティ面での懸念事項（特に DDoS）に対処するには、既存のデータ ネットワークにすでに組み込まれている保護機能を活用します。さらに、今日のシステムは暗号化と使用ポリシーのメカニズムも備えているので、ユニファイド コミュニケーションによる会話とメッセージングシステムのセキュリティは、従来のテレフォニー環境よりも強化されます。電話料金詐欺を回避するには、従来のテレフォニー環境と同様の対策を取ります。

ユニファイド コミュニケーション アプリケーションをネットワークに追加するときは、セキュリティに対して全体的なアプローチを取る必要があります。つまり、電話機、アプリケーション、および電話スイッチをはじめとする、ネットワーク インフラストラクチャのセキュリティのあらゆる面に対して対策を施す必要があります。また、ユニファイド コミュニケーションが常に利用可能であるように、遠隔地からの接続を冗長化することもセキュリティ対策の一つです。

ユニファイド コミュニケーションを安全に導入するには、組織のあらゆる機能の専門家が参加することと、包括的なコミュニケーション セキュリティ ポリシーの綿密な計画、開発、および実装が必要です。このことを支援するために、シスコでは、ユニファイド コミュニケーション ソリューションのセキュリティを万全にするための設計、テスト、および実装に関する広範なサービスを提供しています。

ビジネスに対するシスコ ユニファイド コミュニケーションの価値の詳細については、<http://www.cisco.com/jp/go/secureuc/> を参照してください。

©2008 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