ホワイトペーパー

Web 会議：安全なリアルタイムのコラボレーションを最大限に活用

本書は Cisco WebEx Meeting Center、Cisco WebEx Training Center、Cisco WebEx Support Center、および Cisco WebEx Event Center のセキュリティ情報に焦点を当てています。

概要

Cisco WebEx® オンラインソリューションは、世界中の従業員と仮想チームが同じ部屋で作業を行っているかのような、リアルタイムのコラボレーションを実現します。実際、オンラインコラボレーションは、移動時間やコスト、さらに会議室のスペースの問題さえもなくすという点で、従来のフェイスツーフェイスのコラボレーションより優れています。世界中の企業、組織、政府機関が、ビジネス プロセスを簡素化し、営業、マーケティング、トレーニング、プロジェクト管理、およびサポート チームの成果を向上させるべく、Cisco WebEx® ソリューションを活用しています。

このような企業や組織のすべてにおいて、セキュリティは基本的な関心事項となっており、 オンラインコラボレーションでは、ミーティングのスケジュール設定から参加者の認証、ドキュメントの共有にいたるまで、複数のレベルのセキュリティを備える必要があります。

シスコは、セキュリティをネットワーク、プラットフォーム、およびアプリケーションの設計、導入、メンテナンスにおける最優先事項に位置付けており、 最も厳しいセキュリティ要件が設けられている場合でも、WebEx® ソリューションなら自信を持ってビジネス プロセスに組み込むことができます。

Cisco WebEx オンラインアプリケーション、およびその基盤となるコミュニケーションインフラストラクチャである Cisco WebEx Cloud のセキュリティ機能を理解することは、投資決定を行ううえで重要となります。

Cisco WebEx Cloud インフラストラクチャ

Cisco WebEx Meetings は、業界をリードするパフォーマンス、統合性、柔軟性、拡張性、および可用性を備えた非常に安全なサービス配信プラットフォームである Cisco WebEx Cloud を通じて配信される Software as a Service（SaaS）ソリューションです。Cisco WebEx Cloud は、導入とアプリケーションの配信を容易にし、総所有コストを抑える一方、最高レベルのエンタープライズセキュリティを実現します。

スイッチドアーキテクチャ

シスコは、高速のミーティングスイッチを配置した専用の分散ネットワークを世界中に展開しています。これにより、プレゼンタのコンピュータから発信され、参加者のコンピュータに届くミーティングセッションのデータは、Cisco WebEx Cloud で切り替えられ、保存され続けることはありません。[1]

[1] ユーザーがネットワークベース記録（NBR）を有効にすると、ミーティングの内容が記録および保存されます。また、NBR に加えて、WebEx はユーザープロファイル データとユーザーファイルも保存します。

データセンター

Cisco WebEx Cloud は、リアルタイムの Web コミュニケーション専用のコミュニケーションインフラストラクチャです。WebEx ミーティングセッションは、世界中の複数のデータセンターにあるスイッチング機器を使用します。これらのデータセンターは、主要なインターネットアクセスポイントの近くに戦略的に配置され、専用の高帯域幅ファイバを使用して世界中のトラフィックをルーティングします。シスコは、Cisco WebEx Cloud 内でインフラストラクチャ全体を運用しており、米国内のデータは米国地域に、ヨーロッパ内のデータはヨーロッパ地域にとどまります。

さらに、シスコはバックボーン接続、インターネットピアリング、グローバル サイトのバックアップ、およびエンドユーザーのパフォーマンスと可用性を向上させるためのキャッシング技術を支える、ネットワークのポイントオブプレゼンス（PoP）ロケーションを運用しています。また、シスコのスタッフが 24 時間 365 日体制で、ロジスティック上からセキュリティ、運用、および変更管理を支援しています。

安全性に優れた WebEx ミーティングのエクスペリエンスの概要

WebEx ミーティングは、次のようなエクスペリエンスを提供します。

- ミーティングサイトの構成
- スケジュール設定のセキュリティ オプション
- WebEx ミーティングの開始と参加のためのオプション
- 暗号化技術
- Transport Layer Security
- ファイアウォールの互換性
- ミーティングデータのプライバシ
- ミーティング中のセキュリティ
- シングルサインオン
- サードパーティの認定（独立監査により Cisco WebEx のセキュリティを検証）

「WebEx ミーティング」と「Cisco WebEx ミーティングセッション」とは、すべての Cisco WebEx オンライン製品で使用される統合音声会議、インターネット音声会議、シングルおよびマルチポイントビデオ会議を指します。これらの製品には、次のものが含まれます。

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center（Cisco WebEx Remote Support および Cisco WebEx Remote Access を含む）

特に記載がない限り、本書で説明するセキュリティ機能は、上記の WebEx アプリケーションのすべてに等しく備えられています。

WebEx ミーティングのロール

WebEx ミーティングには、主催者、代理主催者、プレゼンタ、および参加者の 4 つのロールがあります。次の項で、各ロールのセキュリティ権限について説明します。

主催者

WebEx ミーティングのスケジュールを設定し、ミーティングを開始します。主催者は、ミーティング中のエクスペリエンスを制御します。セキュリティ面については、主催者は参加者にプレゼンタの権限を付与できます。また、ミーティングを停止したり、参加者を退席させたりすることも可能です。

代理主催者

主催者は、予定されている WebEx ミーティングを主催者に代わって開始できる代理主催者を指名します。セキュリティ面については、代理主催者には、主催者と同じ権限が付与されます。

プレゼンタ

プレゼンタは、プレゼンテーション、特定のアプリケーション、またはデスクトップ全体を共有し、注釈ツールを制御します。セキュリティ面については、プレゼンタは各参加者に共有アプリケーションおよびデスクトップのリモート制御を許可したり、許可を取り消したりできます。

参加者

参加者は、セキュリティに関する責任や権限を持ちません。

WebEx サイト管理モジュール

WebEx サイト管理モジュールにより、権限を持つ管理者は、主催者とプレゼンタの権限に関して、ミーティングごとにセキュリティポリシーを管理し、適用することができます。たとえば、セッション構成をカスタマイズして、アプリケーションを共有したり、サイトまたはユーザー単位でファイルを転送したりするといった、プレゼンタの機能を無効にすることが可能です。

WebEx サイト管理モジュールでは、次のセキュリティ関連の機能が管理されます。

アカウント管理

- 制限回数を超えてログインに失敗すると、アカウントをロックする（制限回数は設定により変更可能）。
- 指定された時間が経過した後、アカウントのロックを自動的に解除する。
- 定義した期間使用されなかったアカウントを非アクティブ化する。

特定のユーザー アカウントの操作

- 次回ログイン時にユーザーにパスワードの変更を要求する。
- ユーザー アカウントをロックまたはロック解除する。
- ユーザー アカウントをアクティブ化または非アクティブ化する。

アカウントの作成

- 新規アカウントの要求時にセキュリティテキストを求める。
- 電子メールによる新規アカウントの確認を要求する。
- 新規アカウントの自己登録（サインアップ）を許可する。
- 新規アカウントの自己登録の規則を設定する。

アカウントのパスワード

次のような強力なアカウントパスワードの基準を適用する。

- 大文字と小文字の両方を含む
- 最小長
- 数字の最低必要数
- 英文字の最低必要数
- 特殊文字の最低必要数
- 同じ文字を 3 回以上使用することは不可

- 以前使用した所定数のパスワードは再使用不可
- ダイナミックテキスト（サイト名、主催者名、ユーザー名）は使用不可
- 設定可能なリストのパスワードは使用不可（「password」など）
- パスワードを変更するまでの間隔の最短期間
- 主催者による、設定可能な時間間隔でのアカウントパスワードの変更
- すべてのユーザーによる、次回ログイン時のアカウントパスワードの変更

パーソナルミーティングルーム

パーソナルミーティングルームには、個人用の URL とパスワードでアクセスできます。これらのルームで、主催者は開催予定のミーティングと進行中のミーティングの公開、ミーティングの開始とミーティングへの参加、およびミーティング参加者とのファイルの共有が可能です。管理者は、次のようなパーソナルミーティングルームのセキュリティ関連機能を設定できます。

- パーソナルミーティングルームのファイル共有オプション
- パーソナルミーティングルームのファイルのパスワード要件

WebEx サイト管理で実現するその他のセキュリティ関連機能

- 主催者または参加者は、名前と電子メールアドレスを保存することで、新しいミーティングの設定や新しいミーティングへの参加がより簡単に行えます。
- 主催者は、他の主催者に記録を再譲渡できます。
- 主催者と参加者のすべてのアクセスに認証を求めることで、サイトへのアクセスを制限できます。認証は、公開されているミーティングなどのサイト情報だけでなく、サイト上のミーティングへのアクセスの際にも要求することが可能です。
- WebEx Access Anywhere に強力なパスワードの規則を適用できます。
- すべてのミーティングを非公開にできます。
- 「パスワードを忘れた場合」の承認を要求できます。
- アカウントのパスワードをユーザーの代わりに再入力するのではなく、リセットするよう要求できます。

WebEx ミーティングのスケジュール設定のセキュリティオプション

- 各主催者に、（無効にできないサイト管理レベルで設定されるパラメータ内で）ミーティングのアクセスセキュリティを指定する権限を付与できます。
- 確認可能な予定表に表示されないよう、ミーティングを非公開にできます。
- 主催者がミーティングに参加する前に、参加者の参加を許可できます。
- 参加者は、主催者が参加する前に音声にアクセスできます。
- WebEx サイトのアカウントを持つ参加者のみの参加を許可できます。
- ミーティング中に電話会議の情報を表示できます。
- 残りの参加者が 1 名のみになった場合、設定可能な時間でミーティングを自動的に終了できます。
- ミーティングへの参加時に、参加者に対して電子メールアドレスの入力を求めることができます。

ミーティングの公開または非公開

主催者は、カスタマイズした WebEx サイトに公開されているミーティング予定表にミーティングを公開するか、ミーティングのスケジュールを非公開で設定し、ミーティング予定表に表示されないようにするかを選択できます。非公開のミーティングについては、主催者が電子メールによる招待プロセスで参加者にリンクを送信するか、参加者に [ミーティングに参加（Join Meeting）] ページで指定のミーティング番号を入力するよう求めることにより、参加者に対して、ミーティングの開催を明示的に通知する必要があります。

内部または外部ミーティング

主催者は、ミーティングの参加者をカスタマイズした WebEx サイトのアカウントを持つ人物に制限できます。主催者はその際、各参加者がミーティングに参加するサイトにログインできるかどうかを確認します。

ミーティングのパスワード

主催者はミーティングのパスワードを設定してから、ミーティングの招待メールにパスワードを含めるか含めないかを選択できます。

登録

- 主催者は、登録機能によりミーティングへのアクセスを制限できます。主催者は、自身が登録し、明示的に承認した招待者のみを許可する「アクセスコントロールリスト」を作成します。
- WebEx Training Center および WebEx Event Center における登録 ID の再使用を認めないことで、ミーティングのセキュリティを確保できます。すでに使用されている登録 ID の再使用を試みた参加者は、ミーティングに参加できなくなります。これにより、複数の参加者間の ID の共有を防ぐことができます。
- さらに、主催者はアクセスを制限し、参加者を退席させることで、ミーティングのセキュリティを維持できます。

これらのスケジュール設定オプションの組み合わせを微調整することにより、セキュリティポリシーに対応できます。

WebEx ミーティングの開始とWebEx ミーティングへの参加

WebEx ミーティングは、カスタマイズした WebEx サイトで主催者のユーザー ID とパスワードの認証が行われた後に開始されます。主催者は、最初にミーティングを制御する権限を持つ、最初のプレゼンタとなります。主催者は、任意の参加者に主催者またはプレゼンタの権限を付与したり、付与した権限を取り消したり、特定の参加者を退席させたり、いつでもセッションを終了したりできます。

主催者がミーティングに参加できないか、ミーティングに接続できなくなった場合、主催者はミーティングの開始と制御を担当する代理主催者を指名することが可能です。これにより、主催者のロールが想定外の参加者や権限を持たない参加者に割り当てられる可能性がなくなり、ミーティングのセキュリティがより高い状態に維持されます。

カスタマイズした WebEx サイトは、参加者が主催者より先に音声などのミーティングに参加できるように、また、先に参加した人物が使用できる機能をチャットと音声に制限するように設定可能です。

参加者が WebEx ミーティングに初めて参加する場合、その参加者のコンピュータに WebEx クライアントソフトウェアが自動的にダウンロードされ、インストールされます。WebEx クライアントソフトウェアは、VeriSign が発行した証明書を使用してデジタル署名されます。その後のミーティングでは、WebEx アプリケーションにより、変更や更新を含むファイルのみがダウンロードおよびインストールされます。参加者は、コンピュータのオペレーティングシステムのアンインストール機能を使用して、WebEx のファイルを簡単に削除できます。

暗号化技術

WebEx ミーティングは、WebEx ミーティングセッション内の各参加者にリアルタイムのリッチメディアコンテンツを安全に配信できる設計となっており、プレゼンタがドキュメントやプレゼンテーションを共有する際は、データを最適化して共有できるようにする、シスコ® 独自の技術である Universal Communications Format（UCF）によりエンコードが行われます。iPad、iPhone、BlackBerry などのモバイル デバイス上の WebEx ミーティングアプリケーションでも、PC クライアントと同じ暗号化メカニズムが使用されます。

WebEx ミーティングは、次の暗号化メカニズムを備えています。

- PC やモバイルデバイスで WebEx ミーティングを行う場合、データは 128 ビット Secure Socket Layer（SSL）により、クライアントから Cisco WebEx Cloud に転送されます。
- Cisco WebEx Meeting Center のオプションとして、エンドツーエンド（E2E）暗号化が提供されます。ミーティング参加者間のミーティングコンテンツはすべて、Advanced Encryption Standard（AES）を使用してエンドツーエンドで暗号化されます。このとき、主催者のコンピュータでランダムに生成される 256 ビットキーが、公開キーベースのメカニズムにより参加者に配布されます。Cisco WebEx Cloud 側で終端する SSL 暗号化とは異なり、E2E 暗号化では Cisco WebEx Cloud インフラストラクチャ内のすべてのミーティングコンテンツが暗号化されます。クリアテキストのミーティングコンテンツのデータは、ミーティング参加者のコンピュータのメモリにのみ提示されます。[2]
- ユーザーが関連する「記憶する」オプションを選択した場合、そのユーザーの WebEx ミーティング用のログイン ID とパスワードが PC やモバイルデバイスに保存され、128 ビット AES で暗号化されます。

サイト管理者と主催者は、「ミーティングタイプ」オプションを使用して、E2E 暗号化を選択できます。ミーティングの主催者と参加者のみにキーが知らされるため、E2E ソリューションのセキュリティは、AES 単独の場合より強力です（ただし、E2E 暗号化では、ペイロード暗号化にも AES を使用します）。

正規ユーザーのみが特定のミーティングに参加できるよう、WebEx ミーティングクライアントから WebEx クラウドへの接続はすべて、暗号化トークンで認証されます。

Transport Layer Security

アプリケーション層での保護に加え、すべてのミーティングデータは 128 ビット SSL で転送されます。SSL は、（標準的な HTTP インターネットトラフィックに使用する）ファイアウォールポート 80 を使用してファイアウォールを通過するのではなく、（HTTPS トラフィックに使用する）ファイアウォールポート 443 を使用します。

WebEx ミーティングの参加者は、アプリケーション、プレゼンテーション、およびセッション層での論理接続を使用して Cisco WebEx Cloud に接続します。参加者のコンピュータ間のピアツーピア接続はありません。

ファイアウォールの互換性

WebEx ミーティングアプリケーションは、Cisco WebEx Cloud と通信し、HTTPS（ポート 443）を使用して信頼性と安全性に優れた接続を確立します。そのため、ファイアウォールを特別に設定して WebEx ミーティングを有効にする必要はありません。

[2] E2E 暗号化が有効になっている場合、NBR は使用できないため注意してください。このオプションは、WebEx Meeting Center でのみ使用できます。

ミーティングデータのプライバシ

すべての WebEx ミーティングのコンテンツ（チャット、音声、ビデオ、デスクトップ、またはドキュメント共有）は一時的なものです（ミーティング中にのみ存在します）。ミーティングのコンテンツは、デフォルトではシスコのクラウドにも参加者のコンピュータにも保存されません。シスコが保持するミーティング情報は、次の 2 種類のみです。

- **イベント詳細レコード（EDR）**：シスコは EDR を使用して請求と報告を行います。主催者の ID でログインすると、カスタマイズした WebEx サイトでイベントの詳細情報を確認できます。認証を受けると、WebEx サイトからこのデータをダウンロードするか、WebEx API を通じてデータにアクセスすることも可能です。EDR には、誰（ユーザー一名と電子メールアドレス）がどのミーティング（ミーティング ID）に参加し、いつどうしたか（参加時刻と退席時刻）など、ミーティングの参加に関する基本的な情報が含まれます。
- **ネットワークベース記録（NBR）ファイル**：主催者が WebEx ミーティングセッションを記録する場合、記録は Cisco WebEx Cloud 内に保存され、カスタマイズした WebEx サイトの MyRecordings エリアでアクセスできます。ミーティング中に主催者が NBR を有効にするか、すべてミーティングを記録するためのサイト全体のオプションを選択した場合にのみ、このファイルが作成されます。NBR は URL リンクからアクセス可能で、各リンクには、予測不能なトークンが含まれます。主催者は、NBR ファイルへのアクセスに関してフルコントロールを持ち、ファイルの削除や共有、ファイルを保護するためのパスワードの追加などを行うことができます。NBR 機能はオプションで、管理者が無効にできます。

シングルサインオン

シスコは、Security Assertion Markup Language（SAML）1.1 と 2.0、および WS-Federation 1.0 プロトコルを使用して、ユーザのシングルサインオン（SSO）のフェデレーション認証をサポートしていますが、SAML 1.1 のサポートは終了する予定です。フェデレーション認証を使用するには、カスタマイズした WebEx サイトに公開キー X.509 証明書をアップロードする必要があり、アップロードすると、ユーザー属性を含む SAML アサーションを生成して、適合する秘密キーでアサーションのデジタル署名が行えます。WebEx では、ユーザー認証の前に、プリロードされた公開キーの証明書に対して SAML アサーションの署名を検証します。

サードパーティによる報告

独自に設けた厳しい社内手順だけでなく、WebEx のセキュリティ部門では、独立した複数のサードパーティに、シスコの社内ポリシー、手順、およびアプリケーションに対する厳格な監査の実施を依頼しています。これらの監査は、商用および政府機関向けのアプリケーションの両方について、ミッションクリティカルなセキュリティ要件を確認することを目的としています。

サードパーティによるセキュリティ評価

シスコはサードパーティベンダーを使用して、継続的かつ詳細な、コードによる侵入テストとサービス評価を実施しています。この取り組みの一環として、サードパーティは次のようなセキュリティ評価を行っています。

- 重要なアプリケーションとサービスの脆弱性の特定、およびソリューションの提案
- アーキテクチャの改善に関する一般的な分野の推奨
- コーディングのエラーの特定、およびコーディングのプラクティスの改善に関するアドバイスの提供
- WebEx のエンジニアリングスタッフとの直接的な連携による評価結果の説明、および改善策に関するアドバイスの提供

セーフハーバー認定

2012 年 3 月に、シスコはお客様とパートナ様のデータに関するセーフハーバー認定を取得しました（従業員データのセーフハーバー認定は、2011 年に取得）。シスコの包括的なプライバシ遵守プログラムに対する追加コンポーネントの役割を果たすこの認定は、政府機関や標準委員会から求められているものではありませんが、シスコは、多くのお客様がこの認定を重視していると認識しています。

EU データ保護指令では、プライバシ保護に関する EU の「適切性」を満たさない EU 諸国以外の国に、ヨーロッパ市民の個人データを転送することを禁じています。米国商務省は、米国の組織がセーフハーバーの一連のプライバシ原則に従うことでこの指令に準拠できる、セーフハーバーフレームワークを欧州委員会と共同で作成しました。企業は、米国商務省の Web サイトでこれらの原則に準拠していることを証明できます。2000 年に EU で承認されたこのフレームワークは、こうした原則に従う企業の慣行が、EU 市民に対する「適切な」プライバシ保護に相当すると EU が認めることを保証するものです。

SSAE16

PricewaterhouseCoopers は、米国公認会計士協会が定める基準に従い、Statement on Standards for Attestation Engagements No. 16（SSAE16）監査を毎年実施しています。SSAE16 の詳細については、http://www.ssae16.com [英語] を参照してください。

ISO 27001 および 27002

シスコは WebEx サービスに関して、2012 年 10 月に ISO 27001 を取得しました。認定は毎年の中間外部監査を経て、3 年ごとに更新されます。ISO 27001 は、情報セキュリティ管理システム（ISMS）の作成で推奨されるベストプラクティスを提供する、国際標準化機構（ISO）が公開している情報セキュリティ標準です。ISMS は、組織の情報リスク管理プロセスに関わるすべての法律、管理、物理、および技術面の制御を含む、ポリシーと手順のフレームワークです。ISMS の文書によると、ISO 27001 は、「情報セキュリティ管理システムを構築、実装、操作、監視、確認、保守、および改善するためのモデルを提供する」目的で開発されたものです。ISO 27001 および 27002 の詳細については、http://www.27000.org/ [英語] を参照してください。

詳細情報

Cisco WebEx ソリューションの詳細については、http://www.cisco.com/c/en/us/products/conferencing/web-conferencing/index.html [英語] を参照するか、営業担当者までお問い合わせください。

お問い合せ先

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

C11-709579-01JA 16.02