



セキュアなWeb会議

Webex MeetingsとDuo Security連携によるセキュアな会議の実施

Ver.1.0

ネットワンシステムズ株式会社

ビジネス開発本部 第1応用技術部

2021年10月1日

目次

1	はじめに
2	本ドキュメントについて
2-1	目的と背景
2-2	対象製品とサービス
2-3	機能と注意事項
3	WebexとDuoの連携構成
3-1	本環境と構成図
4	検証結果
4-1	検証内容と結果
5	考察とまとめ
5-1	検証結果からの考察
5-2	まとめ
6	著者紹介

1 はじめに

本ドキュメントでは、Cisco Systems社がサービス提供するクラウドコラボレーション製品（Webex）とCisco Duoの認証サービス連携について解説します。複数のクラウドサービスの利用が主流となり、ID/Passwordの管理の重要性が増していること、またパスワードのみだけでなくMFA（Multi-Factor Authentication）の重要性も高まっています。今回はWebexを安全に利用するためのCisco Duoを利用した多要認証機能および信頼されたデバイスのみで該当のサービスを利用するためのTrusted Endpointsの機能を利用したアクセス制御方法について解説するものとなります。

2 本ドキュメントについて

2-1 目的と背景

COVID-19の脅威によりWeb会議の需要がここ1、2年で増大しました。クラウドサービスを利用する機会が増え、自宅、会社と場所を問わずに利用できるようになりました。近年ではインターネットのある環境さえあれば直接社内ネットワークを介すことなく、クラウドサービスを利用できるため、リモートワークの利便性を追求した環境を整えることを優先し、セキュリティについては後回しになりがちです。

最近ではゼロトラストセキュリティが主流となり、さまざまなデバイスや場所からのアクセスに対して、検疫などの仕組みを整えなくてはならなくなったこともあり、アクセス元をどのように信頼するか、またその手法を検討しなくてはならなくなりました。その一つがゼロトラストの基本であるIdentity管理の仕組みです。利用するクラウドサービスが多岐にわたり、IDパスワードをサービス毎に設定して運用しているケースも少なくありませんし、その情報が流出してしまった場合のリスクを考えると最適ではありません。

本ホワイトペーパーで説明するソリューションでは、Cisco社の提供するコラボレーション製品Cisco Webexとゼロトラストセキュリティを実現するCisco Duoを利用し、Web会議を安全に利用するための仕組みについての検証内容や検証結果についての説明を行います。

2-2 対象製品とサービス

■コラボレーション製品

Cisco Webex Meetings
Cisco Webex Meetings App
Cisco Webex Teams App

■セキュリティ製品

Cisco Secure Access by Duo（以下Cisco Duoと表記）
Cisco Secure Endpoints（以下AMP for Endpointsと表記）

2-3 機能と注意事項

・ Cisco Duo利用時の注意事項

本ドキュメントでは、Cisco Duoの多要素認証の機能を利用し、Webexを利用するための安全な仕組みを検証しております。現在利用されるデバイスは、スマートフォン、PCなどさまざまですが、Duoのみを契約するだけでは、すべての機能は利用できません。

たとえば、マルウェア感染した端末などのデバイスからの利用を拒否する場合は、AMP for Endpointsの機能が必要になりますが、現時点で対応している端末のOSは、Windows やMACのみとなっております。よって、スマートフォンでのマルウェアからの脅威を守るためには別のプロダクトの検討が必要です。

3 WebexとCisco Duo連携構成

3-1 本環境の構成図

本ホワイトペーパーでは、Webexを利用する際の多要素認証およびTrusted Endpointsの機能を利用した構成で試験を行います

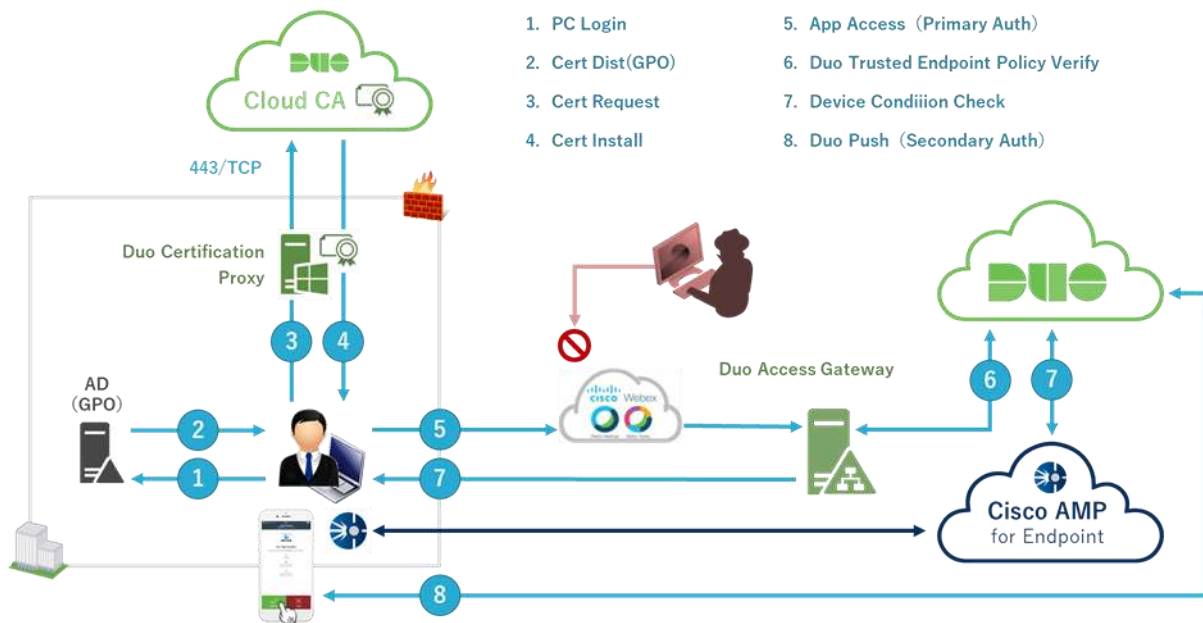


図1:WebexとCisco Duo検証構成

4 検証結果

4-1 検証内容と結果

Webex と Cisco Duo の検証については以下の観点で行いました。

- ・ Cisco Duo の Trusted Endpoints 機能によって、会社支給端末(証明書の入っている端末) に制限できるか検証する。
- ・ Cisco Duo の Trusted Endpoints + AMP for Endpoints 連携によってマルウェアに感染した端末からの Webex ログインをブロックできるかを検証する。

表 1:Webex と Cisco Duo における多要素認証検証項目

検証項目	結果
Webex ログイン時に Cisco Duo による多要素認証が可能なこと	○
Cisco Duo のポリシー条件外の際に多要素認証が拒否されること	○

表 2:Webex と Cisco Duo Trusted Endpoints における多要素認証検証項目

検証項目	結果
端末に証明書がない場合 Webex にログインできないこと	○
端末に証明書が配布されている場合 Webex にログインできること	○
端末がマルウェアなどに感染している場合、Webex にログインできないこと	○



図2:Cisco Duo認証時の成功ログ



図3:Cisco Duo認証時のエラーログ (AMP For Endpointsで脅威検知)

5 考察とまとめ

5-1 検証結果からの考察

試験結果より、Webexを利用する際にID/Passwordのみだけでなく、多要素認証も正常に機能しWeb会議を利用することができました。これにより昨今課題となっている不正アクセスやなりすましなどのリスクを軽減することができます。また、なりすましではなく本人であったとしても、そのデバイスの状態を可視化、管理を行うことで例えばマルウェアに感染している場合は不正にログインさせないことで情報漏洩を防ぐことができます。

一方で、アプリをログインした状態で利用し続ける場合、Webexアプリには自動的にサインアウトされる機能がないため、AMP for Endpointsでのマルウェア感染のチェック機能が省略されることもあり一部では課題が残る結果となりました。

5-2 まとめ

今回検証した結果を踏まえると、Webex とCisco Duoを利用した構成はゼロトラスト時代に即したWeb会議の利用を提供いたします。またCisco DuoはWebexに限らず様々なクラウドサービスとも連携することが可能です。

今回は、コラボレーション製品におけるWebexとCisco Duoの連携検証を行いました。Cisco Duoはコラボレーションに特化したものではなく、利用するクラウドサービスやネットワークの管理等全体を見据えたプロダクトとなります。本資料が導入する顧客においての一助になればと思います。

6 著者紹介

ネットワンシステムズ株式会社
ビジネス開発本部 第1応用技術部 セキュリティチーム
尾山 和宏

ネットワン入社以来、セキュリティ製品の担当として、ベン
ダー製品の評価・検証・技術サポート業務に従事
CISSP#502642、CCIE Security#64214
第3回 シスコテクノロジー論文コンテスト 最優秀賞

ネットワンシステムズ株式会社
ビジネス開発本部 第1応用技術部 セキュリティチーム
片岡 武義

ネットワンシステムズに入社以来、セキュリティ製品担当とし
て、主にCisco製品の評価・検証・技術サポート業務に従事。

ネットワンシステムズ株式会社
ビジネス開発本部 第1応用技術部 クラウドインフラチーム
小田中 俊博

ネットワンシステムズに入社以来、コラボレーション製品担当
として、顧客へのコミュニケーション環境の構築などに従事。