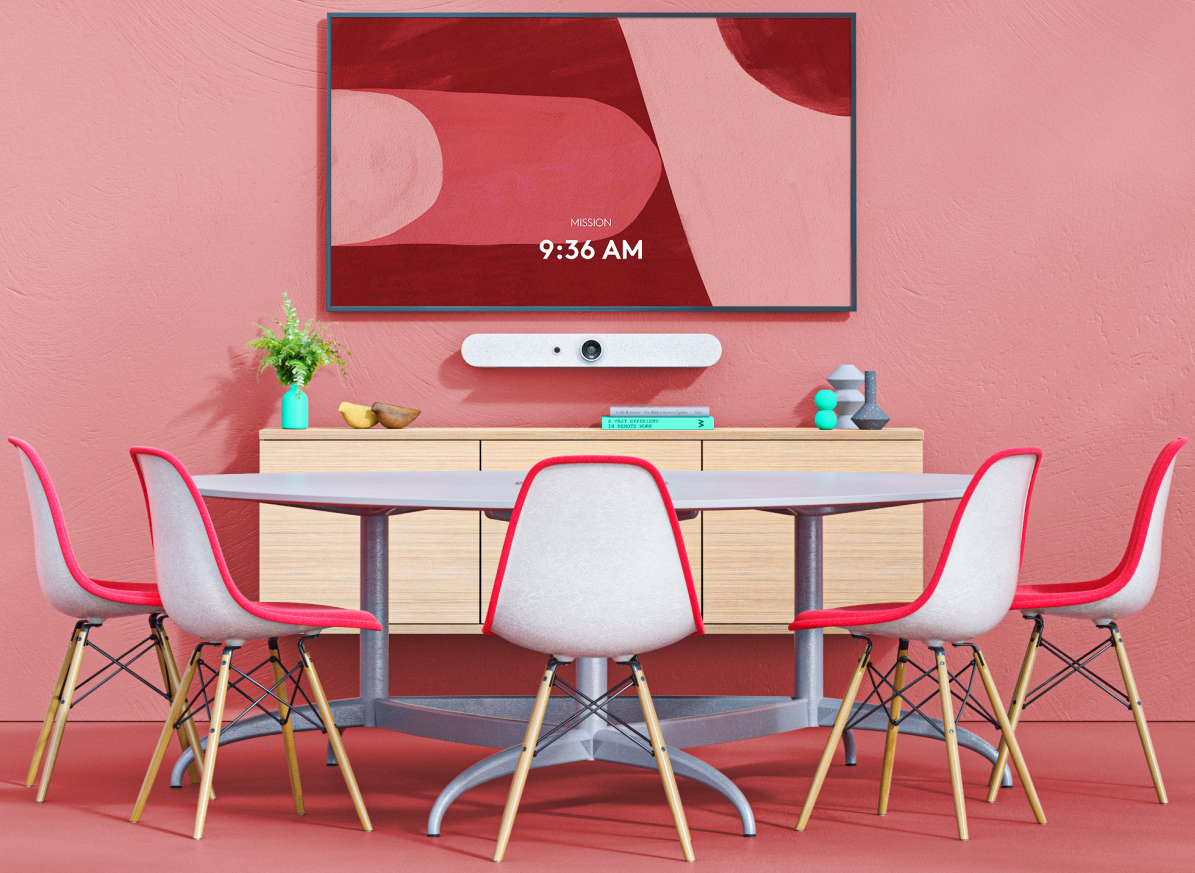
ロジクール ビデオコラボレーションのセキュリティとプライバシー



はじめに

サイバー攻撃は世界中で頻度を増しており、また手口も巧妙になっています。これは、ますます分散化とオンライン化が進むハイブリッドワーク環境において、組織に重大なリスクをもたらします。

今日のサイバー犯罪は、いつどこで発生してもおかしくありません。ハッカーはソフトウェアとハードウェア両方の脆弱性を狙っています。カメラやヘッドセットなどのデバイスも標的になるのです。

本ホワイトペーパーでは、CollabOSで動作するデバイスのセキュリティとプライバシーに当社がどのように取り組んでいるかをご紹介します。現在これに該当するデバイスとしては、Rally Bar、Rally Bar Mini、RoomMate、ロジクール Tap Scheduler、Tap IPが挙げられます。

COLLABOSとは？

CollabOSは、一部のロジクール ビデオコラボレーションデバイスに搭載されている統合型オペレーティングシステムです。CollabOSを使用することで、これらのデバイスがシームレスに連携し、継続的に改善され、導入と管理がこれまで以上に容易になり、高品質で公平な会議体験をすべての人に提供できるようになります。

CollabOSでは、Microsoft Teams、Zoom、Robinなど、サードパーティのアプリケーションおよびスケジューリングサービスをロジクールのハードウェアと連携させることができるため、ビデオ会議の導入と管理がより容易になります。

また、ビデオ会議の参加者のユーザー体験を継続的に改善すると同時に、投資したビデオ会議用機器をより長く利用できます。新機能、拡張機能、セキュリティ対策を含むファームウェアのアップデートは、追加費用がかかることなく、無線で自動的にデバイスに送信されます。

COLLABOS搭載デバイス

- **Rally Bar**と**Rally Bar Mini**はロジクールの一体型高機能ビデオバーで、大、中、小すべての規模の会議室をこの2つでカバーできます。独自仕様の光学カメラ、同時双方向音声、AI搭載の専用サブカメラを備えています。どちらもUSBモードとアプライアンスモードの導入に対応しており、卓越した柔軟性と使いやすさを備えています。

  Rally BarとRally Bar Miniの詳細

- **RoomMate**は会議用カメラおよび周辺機器向けのビデオ会議アプライアンスです。Rally SystemやMeetUpのほか、対応するサードパーティ製オーディオシステムも接続できます。Microsoft Teams® Rooms on AndroidやZoom Rooms（アプライアンス版）など、主要なビデオ会議サービスを簡単に導入できます。

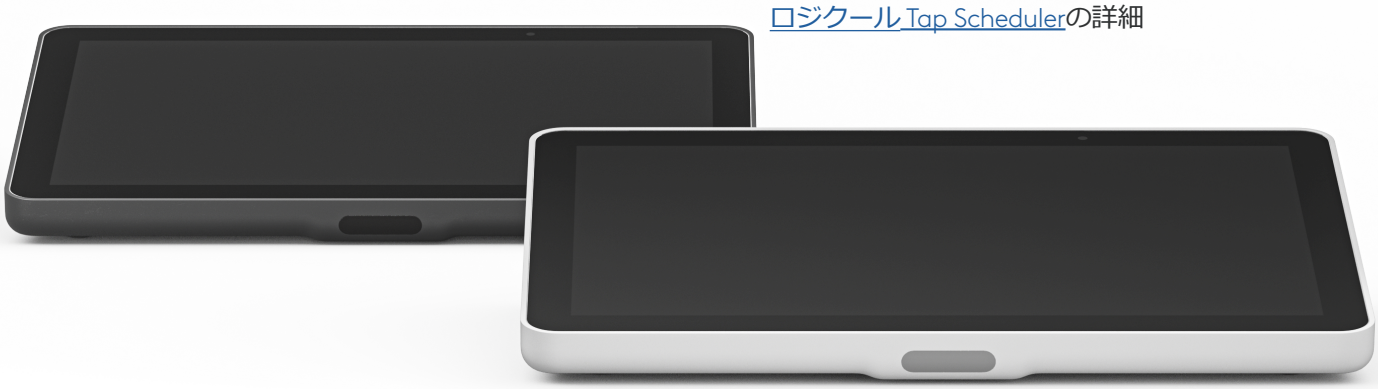
  RoomMateの詳細

- **Tap IP**は、ネットワークに接続して使用するタッチコントローラです。利用するプラットフォームとアプリケーションを問わず、ビデオ会議に簡単に参加できます。Tap IPは、薄型の筐体に10.1インチの大型ディスプレイ、常時オンの状態を維持するモーションセンサーを備えています。コンテンツの共有も簡単で、あらゆる会議室で一貫した会議体験を提供することができます。

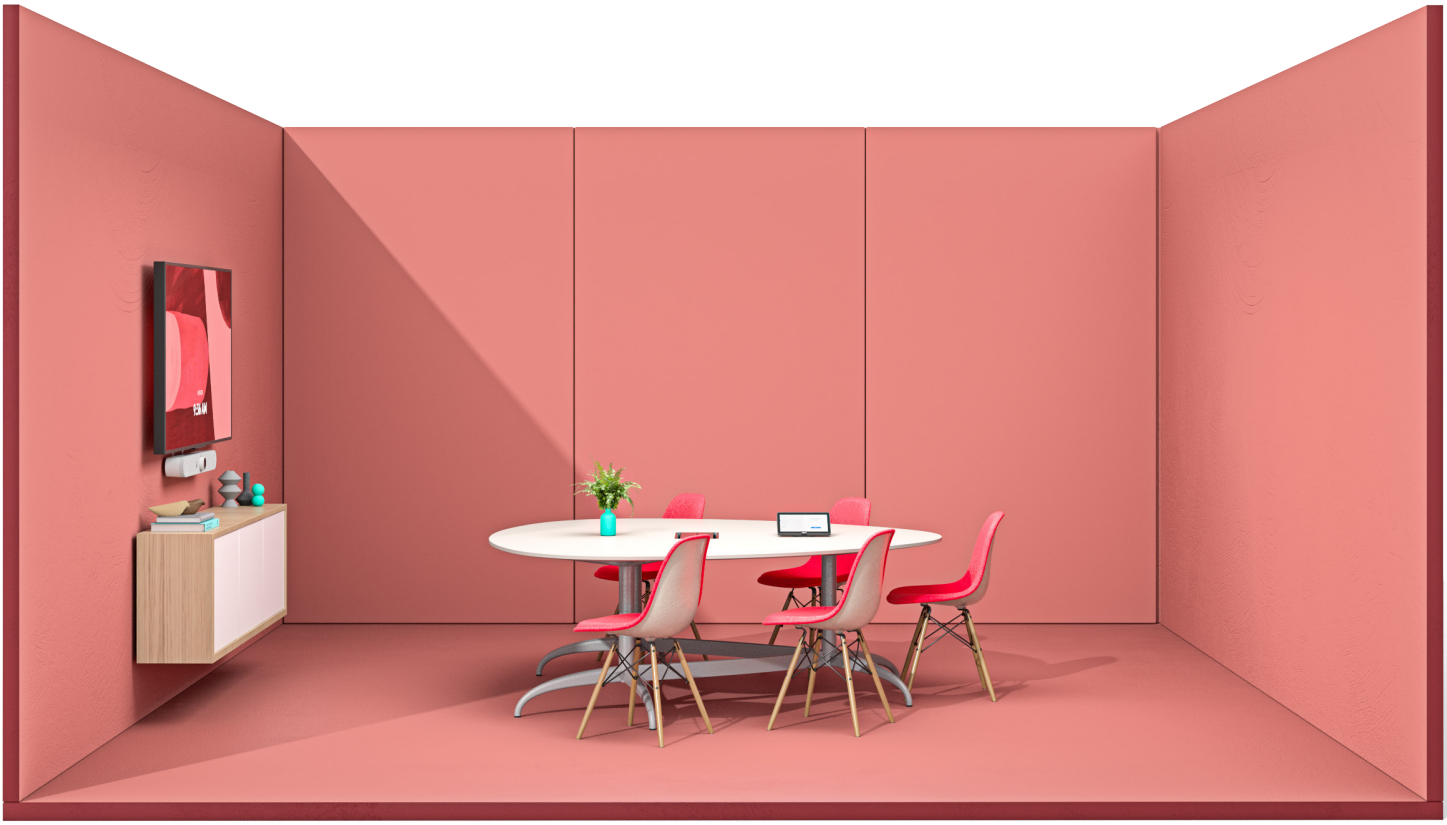
  Tap IPの詳細

- **ロジクール Tap Scheduler**は会議室専用のスケジューリングパネルで、オフィスでの会議室の利用を効率化できるよう設計されています。ロジクール Tap Schedulerを使えば、会議の詳細情報を確認したり、臨時の会議や予定された会議のために会議室を予約したりすることが簡単に行えます。使用中かどうかを色で示すLEDライトを備えているため、離れた場所からでも空き会議室をすぐに見つけることができます。

  ロジクール Tap Schedulerの詳細



セキュリティとプライバシー



ロジクールは、すべてのビデオ会議用製品の設計においてセキュリティとプライバシーを非常に重要視しています。CollabOSはAndroid 10上で動作し、業界トップレベルのセキュリティ、プライバシー、パフォーマンスを提供します。

ロジクール製品は、製品の設計、開発、商品化における業界のベストプラクティスに従った安全な開発ライフサイクルのもとで開発されています。設計の初期段階からセキュリティを考慮しているため、セキュリティ面の要求に十分以上に応えることができています。

例を挙げると、セキュリティの専門家を組織全体から集めてセキュリティレビュー委員会を組織し、製品設計レビューを実施しています。また、開発中およびテスト中に、システムとソフトウェアのセキュリティを厳密に検証することや、セキュリティの脅威を分類する業界標準であるSTRIDEに準拠することもこの一環です。

注：特に記載のない限り、本ホワイトペーパーで取り上げるセキュリティとプライバシーに関する機能は、先述の5つのデバイスすべて（本ホワイトペーパーでは「*CollabOS* デバイス」と呼びます）に当てはまります。

情報セキュリティ

セキュア開発ライフサイクル（SDLC）

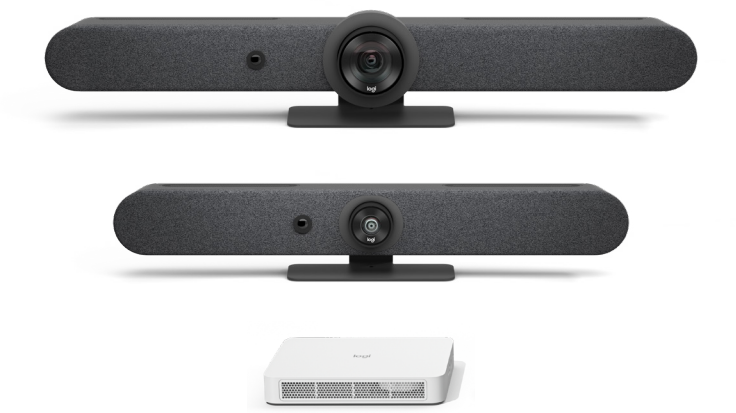
ロジクールのCollabOSデバイス用SDLCでは、システム開発の各段階（設計、実装、リリース）にセキュリティ審査のためのゲートを設けています。設計フェーズでは、すべての設計ドキュメントが社内外のセキュリティ専門家によってレビューされます。

実装フェーズでは、開発チームが作成したコードに対し、自動レビューと人間によるレビューの両方が行われます。すべてのソースコードに対して静的分析が行われます。結果に問題があった場合にはフラグが付けられ、開発チームとセキュリティ専門家によるレビューが行われます。

CollabOSデバイス用のソフトウェア開発はすべて以下を含む、ただし必ずしもこれに限定することのない業界標準に準拠しています。

- Android Secure Coding Standard
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT C++ Coding Standard

ソフトウェアのリリース前には、機能とセキュリティの両方について一連の徹底したテストが行われます。システムのアップデートや新規リリースもSDLCに従っており、現場で使うソフトウェアは、メジャーリリースまでの間に発見された問題に対処するセキュリティパッチを適用して保守、更新されます。



設計によるセキュリティとプライバシー

CollabOSデバイスには、製品開発の開始から実装、リリース、更新に至るまで、セキュリティとプライバシーが設計に組み込まれています。

以下に、これらのデバイスのセキュリティを強化するためにロジクールが実施している手順の一部を紹介します。

- **強固な基盤で構築：**プラットフォームは、優れたセキュリティと安定性を備えたAndroid 10をベースに構築されています。
- **デフォルトのユニバーサルパスワードの使用を回避：**ロジクールCollabOSデバイスには、デフォルトのユニバーサルパスワードの設定をしない業界のベストプラクティスおよびカリフォルニア州法に従い、デフォルトパスワードは設定していません。
- **ソフトウェアを常に最新の状態に：** CollabOSデバイスを常に最新の状態に保つため、無線でファームウェア更新を行います。
- **ソフトウェアの完全性を維持：**ソフトウェアイメージはすべて製造段階でデジタル署名され、安全な通信リンクを経由して配布されます。CollabOSデバイスは、ソフトウェアをインストールまたはアップグレードする前に、各ソフトウェアイメージの署名を検証することで、その完全性と信頼性を維持します。
- **セキュアな通信：**CollabOSバージョン1.7以降では、CollabOSデバイスとクラウド間のすべての通信にトランスポート レイヤー セキュリティ（TLS）バージョン1.2および1.3を使用します。TLS 1.1および1.0はCollabOSデバイスでは無効になり、セキュリティスキャンで検出されなくなりました。プラットフォーム上で実行されるアプリケーションでは、同様の形式を使用するか、別の形式の通信を追加で使用する場合があります。セキュリティプロトコルについては、アプリケーションのサービスプロバイダーに確認することをお勧めします。
- **個人データの保護：**CollabOSデバイスは、個人を特定できる情報（PII）をデバイス内に格納または保存することはありません。ただし、ビデオサービスプロバイダーは、アプリ内に個人を特定できる情報を保存する場合があります。PIIポリシーについては、サービスプロバイダーに確認することをお勧めします。

情報セキュリティ

デバイスアプリケーションのセキュリティ

CollabOSデバイスには、日々の業務で使用するアプリケーションがいくつか含まれています。デバイスを保護するために、ロジクールはデバイス上に存在するアプリケーションを注意深く管理しなければなりません。

アプリケーションをホワイトリストに登録するプロセスを通じて、使用を許可するアプリケーションを正確に制御できます。出荷前にソフトウェアを保護する一環として、当社では必須ではないアプリ、サービス、デバイスドライバーを削除または無効にすることで、攻撃対象領域を減らしています。すべてのCollabOSデバイスは、Androidシステムのコンポーネントである組み込みのSELinuxポリシーを利用しています。

アンチロールバック機能

CollabOS対応デバイスは、ソフトウェアの更新が適用されたシステムが、より安全ではないかも知れない以前のバージョンのソフトウェアに、戻されることを防ぐ機能を備えています。

ハードウェアのセキュリティ

すべてのCollabOS対応デバイスは、デバイスのセキュリティを強化する機能を複数備えています。デバイスに必要なシークレットやキーを保護するために、信頼性の高いエンクレーブを使用しています。ハードウェアは、製造時に署名されたブートソフトウェアとシステムファームウェアの有効性を検証するために、セキュアブートを利用します。

セキュリティ検証

当社の品質保証プロセスは、ソフトウェアコンポーネントのセキュリティテストスイートを使用して、各ソフトウェアリリースのセキュリティ上の脆弱性をチェックしています。テストスイートのゲートをクリアするまで、ソフトウェアをリリースすることはありません。

ファイアウォールのルール - ポートのフィルタリング/ブロック

すべてのCollabOS対応デバイスは、ポートのフィルタリングとブロックに関する独自のファイアウォールルールを実装し、ネットワークにさらされる攻撃対象領域を低減しています。

プライバシー保護のため記録中であるかを示す外部デバイスインジケータ

ビデオや音声を記録するすべてのCollabOSデバイス（マイクやカメラなど）には動作中であることを明確に示すインジケータが搭載されています。Rally BarとRally Bar Miniには、会議用カメラに使用するレンズキャップが付属しています。

注：カメラとマイクを搭載しておらず、ビデオや音声を記録する機能を持たない*Tap IP*、ロジクール *Tap Scheduler*、*RoomMate*は該当しません。

アプリケーションのサンドボックス化

組み込まれたアプリケーションのサンドボックス化により、プラットフォーム上でのアプリケーションの相互干渉を防ぎます。各アプリケーションとそのデータには、作業用にそれぞれ専用のスペースが与えられます。データはアプリケーションごとのサンドボックスに保持されるため、動作中の他のアプリケーションからの、データの読み取りや書き込みを含めたデータへの通信や干渉が制限されます。

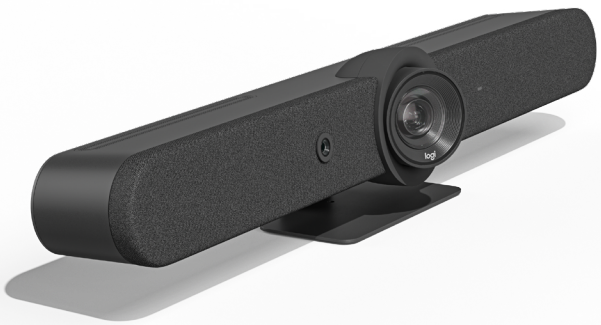
データの保護 - ストレージの暗号化

CollabOS対応デバイスでは、あらゆるデータの保存にハードウェアレベルのストレージ暗号化が使用されます。

バックエンドのデータセキュリティ

CollabOS対応デバイスと、デバイスをサポートするロジクール バックエンドシステム間の通信（無線アップデートなど）は、トランスポート レイヤー セキュリティ（TLS）で暗号化されたチャネルを介して実行されます。これにより、転送中のデータの暗号化と、デバイスが通信しているシステムの認証の両方を行えます。

AmazonのIoT（Internet of Things）フレームワークとインフラストラクチャを活用して、デバイスとバックエンド間の安全な通信を実現し、クラウドに保存されたデータを保護します。



脆弱性およびリスク管理

当社は製品のセキュリティを積極的に監視し、既知の脆弱性に対処するためにタイムリーな更新を提供します。

インシデント対応

ロジクールの製品に問題を見つけたお客様またはセキュリティ研究者の方は、ぜひ遠慮なくご報告ください。問題に現場で対処できるようサポートいたします。当社は、公開バグバウンティプログラムに参加しています。この制度は、参加している研究者が当社製品について問題を発見した場合に報告して報奨金を受け取ることができるもので、製品のセキュリティ向上を可能にする制度です。ロジクールは、報告されたセキュリティインシデントが有効かつ対処可能であることが判明した場合、その報告者に対して適切な報奨金を提供します。

さらに、インシデントを記録し、可能な限り迅速に対処します。その後、こうしたインシデントの報告は、責任ある情報開示として認められた手順通りに公表へとつながっていきます。

その他のリソース

CollabOS対応デバイスとしてご紹介したRally Bar、Rally Bar Mini、RoomMate、Tap IP、ロジクール Tap Scheduler について詳しくは、www.logicool.co.jp/ja-jp/video-collaboration.htmlをご覧ください。

お問い合わせ

ロジクール製品に関するセキュリティ上の懸案事項については、logitech.com / securityまでお知らせください。その他のご質問については、
logicool.co.jp/contactまでご連絡ください。

株式会社ロジクール
販売代理店または当社
(www.logicool.co.jp/ja-jp/vcsales)
までお問い合わせください

発行：2023年11月