ポリコムジャパン株式会社

PGSJ201300062
2013 年 7 月 3 日

ビデオ会議のセキュリティの確保について
~ セキュリティ攻撃からポリコム製品を守るために~

企業、政府機関、教育機関、医療機関、金融機関など、多くの組織は、生産性および業務効率を高めるために日々努力を重ねています。ビデオ会議は、これらの目標を達成する上で不可欠なツールとなっています。そのため、ビデオ会議のセキュリティを確保し、ビデオ通話で会議参加者が安心して機密情報を共有できるようにする必要があります。

ポリコムでは、セキュアなビデオ会議を提供することを重視しており、ポリコムソリューションの全ラインアップにはセキュリティ機能が導入されています。会議端末からインフラストラクチャまで、ポリコムのすべてのソリューションには、厳格な業界標準を満たすセキュリティ機能が搭載されています。
ベストプラクティスに従ってビデオ会議システムを使用することにより、これらの機能を活用し、ネットワーク上の音声、映像、およびデータトラフィックのセキュリティを確保することができます。

一部の業界では、セキュリティ規制への準拠が義務付けられています。ポリコムは、それらの業界団体や組織と緊密に連携し、セキュリティ規制に準拠し、かつお客様にとって使いやすいソリューションの開発に取り組んでいます。

インターネットを介した PC、タブレットなどと同様に弊社の製品も快適にお使いいただくためには、セキュリティ対策に十分準備が必要です。ポリコムは、システムの脆弱性を診断するために、定期的に監査を実施することをお客様に推奨しています。

<よくある質問 (FAQ) - Polycom® HDX® セキュリティアップデートについて>
以下に、Polycom® HDX® シリーズ バージョン 3.1.1.3 より前の Polycom HDX ソフトウェアバージョンのセキュリティリスクの概要、ご使用のシステムに脆弱性があるかどうかを判断するための情報、救済措置、および追加情報の入手方法について説明します。

HDX ソフトウェアのバージョンと脆弱性の関連性は?
3.1.1.3 をお使いであれば、現在までに報告されている不正アクセスへの脆弱性は対処されています。
- 3.0.x をお使いの方は、3.1.1.3 同様セキュリティー対策されている、3.0.6 をインストール
またはサービス契約をされている方は、ソフトウェアのアップグレードをして、3.1.1.3 をインストール
することもできます。
- 3.1.x をお使いの方は、3.1.1.3 をインストールできます。
- 3.0 または、それ以前のバージョンをお使いの方は、最新のソフトウェアをご購入いただく、または、サービス契約をしていただいている方は、バージョンアップして 3.1.1.3 をインストールすることができます。
諸事情で 3.1.1.3 に挙げられない場合は、下記推奨事項（ベストプラクティス）をご参照ください。
3.0.6 は 3.0.5 にセキュリティー機能部分のみを搭載したバージョンになります。
3.0.5 にホットフィックスが適用されている場合は、サポート窓口にご相談ください。

VSX シリーズとの本件脆弱性の対象となりますか？
本件の脆弱性は VSX シリーズについては関係ありません。
ベストプラクティスに従ってビデオ会議システムを使用することにより、VSX の機能を活用し、ネットワーク上の音声、映像、およびデータトラフィックのセキュリティを確保することができます。
下記推奨事項（ベストプラクティス）をご参照ください。

現在も攻撃の可能性はありますか?
企業・組織のセキュリティを脅かす新しい脅威は次々に登場しています。どのようなセキュリティ対策をしていても、悪質なサイバー攻撃、不正アクセスの可能性がないとはいいきれるものではありません。
常に最新のセキュリティ対策は必要です。

使用中の HDX システムが攻撃されたかどうかを判断する方法は?

スプラッシュスクリーンの表示中に HDX システムがハング (フリーズ) し、ブートプロセスを完了できず、ポリコム ビデオ アプリケーションを開くことができなくなります。

HDX システムが攻撃された場合、復元する方法は?
上記のような状態になった場合は、お使いのポリコム製品のシリアル番号を明記の上、ポリコムサポート(asiasupport@polycom.com)宛、ご連絡ください。

使用中の HDX システムへの攻撃を防ぐには？
ポリコムは、この脆弱性問題を HDX バージョン 3.1.1.3 で解決しました。
HDX バージョン 3.1.1.3 に直ちにアップグレードすることをお勧めします。

ポリコム製品の保守に加入されている方は、弊社サポートサイト http://support.polycom.com から最新版ソフトウェアバージョンのダウンロードが可能です。
その他事情でバージョンコントロールされている方は、下記の推奨事項１）～４）への対応をご検討ください。

セキュリティに関するポリコムの推奨事項は?
ポリコムでは、セキュアなビデオ会議を提供することを重視しているため、ポリコムソリューションの全ラインアップにはセキュリティ機能が導入されています。会議端末からインフラストラクチャまで、ポリコムのすべてのソリューションには、厳格な業界標準を満たすセキュリティ機能が搭載されています。ベストプラクティスに従ってビデオ会議システムを使用することにより、これらの機能を活用し、ネットワーク上の音声、映像、およびデータトラフィックのセキュリティを確保することができます。

ポリコム製品のセキュリティに関する最新情報については、弊社のセキュリティ情報ウェブサイト www.polyom.com/security (英語) を参照してください。このウェブページには、セキュリティに関する推奨事項やベストプラクティス、セキュリティ警告を提供するセキュリティセンターへのリンクがなど掲載されています。

以下の推奨事項（ベストプラクティス）に対応されることを強くお勧めします。
1) デフォルトのパスワードを変更
ビデオ会議システムに対して、常に管理者用パスワードを設定
パスワードは容易に推測されない、長く、複雑なものにし、定期的に変更するなど攻撃から守るようにします。Administrator's Guide for Polycom HDX Systems を参照ください。

2) 組織内ネットワークにファイヤーウォール
不正アクセスから守るためには、どんな場合でも、組織内のネットワークにファイヤーウォールを設置します。

3) telnet などを含む未使用のプロトコルやインターフェースを無効化にする
システムの Telnet 利用については、細心の注意を払い、必要なとき以外は Telnet アクセスをオフにし、特に、企業のファイヤーウォールを外からのアクセスを無効にしてください。
以下のような技術を使うこともご検討ください。
Telnet 利用が必要な下記機能の使用:
- Polycom SmartPairing™
- Converged Management Application™ (CMA®) システムを使用したスケジュール管理
- telnet-based Integrator API applications

4) リモート関係のオプション設定を無効化
会議室に参加者が集まったときにのみビデオ会議システムを使用する場合は、自動的に着信する「自動応答」機能を無効にし、ローカルカメラの遠隔操作を無効化することをお勧めします。
システムが会議室を利用されている方だけの場合は、システム＞管理者設定＞一般設定＞システム設定＞コール設定＞自動応答　を無効にする、ローカルカメラのリモートコントロールをオフにします。

ポリコム製品セキュリティに関する お問い合わせ先
受付時間：平日 9 時 30 分～17 時 30 分（土日祝日、年末年始を除く）
TEL：03-5213-2540

MAIL：JPInfo-S@polycom.com

製品に関する技術的なお問合せは、ご使用のポリコム製品のシリアル番号を明記の上、ポリコムサポート(asiasupport@polycom.com)宛、メールにてご連絡ください。

以上

上記の日本語による情報は、以下 2 つの文書/Web サイト記載内容を抄訳・抜粋したもので、英語原文の非公式な補足であり、英語原文との間で内容の齟齬のある場合は、英語原文を優先します。

http://www.polycom.com/products-services/resources/telepresence-video-education-center/secure-video-conferencing.html (Date: 6/30/2013)

http://www.polycom.com/content/dam/polycom/www/documents/faqs/polycom-hdx-security-update-faq-enus.pdf (Date: 5/16/2013)