ホワイトペーパー

# SAVI 7300 OFFICE シリーズ DECT™ セキュリティ

## ワイヤレス ヘッドセットでハンズフリーの自由を実現

従業員が音声通話やビデオ通話でのコラボレーションに、より多くの時間を費やすようになり、ワイヤレス ヘッドセットの生産性と健康面におけるメリットは、さらに大きなものとなっています。
特定の業界では、セキュリティ面での懸念からワイヤレス ヘッドセットが選択肢から除外されることも珍しくありませんでした。
しかし、Poly Savi 7300 Office シリーズは、軍事レベルの暗号化を搭載することで、DECT™ Forum の最高のセキュリティレベルを上回る設計になっており、あらゆる組織でワイヤレスヘッドセットのメリットを得ることができます。

## サイバーセキュリティ: 5 大脅威のうちの一つ

サイバーセキュリティの脅威は、World Economic Forum (WEF) の Global Risk Report (2019 年)[1] で示されている、世界が直面している主なリスクの上位 5 つのうちの一つです。
この報告書は、公共機関、民間部門、学会、および市民社会の意思決定者による回答の結果を表しています。
Cybersecurity Ventures 社によると、ランサムウェアによる被害額は 2021 年までに 20 兆ドルに達する見込みで、企業がサイバー攻撃の被害を受けた場合に莫大な経済的費用がかかることになります [2]。
Gartner 社によると、増加し続けるサイバーセキュリティの脅威に対処するため、情報およびセキュリティ リスク マネジメントの市場におけるエンドユーザーの支出は、2019 年 ～ 2024 年の間に 8.3%の年平均成長率で増加し、恒常通貨で 2,114 億ドルに達すると予測されています [3]。

## 最新世代の POLY DECT™ ヘッドセットで セキュアなコミュニケーションを確保

Digitally Enhanced Cordless Telecommunication (DECT) は、1.9Ghz* で確立されるテクノロジーです。最大 180m (見通し距離) の通信範囲で、ワイヤレス スペクトラムの一部を専用に使用することで、企業のオフィスや自宅環境に高度なセキュリティと音質を提供します。DECT™ テクノロジーは、Wi-Fi ネットワークなどの他のテクノロジーとスペクトラムを共有しないため、よく「干渉がない」と言われます。

セキュリティは、増加する脅威に対抗するために時間とともに進化してきた、DECT™ テクノロジーの多くの長所のうちの一つです。DECT™ ヘッドセット システムは、ヘッドセットとベースで構成されており、Time Division Multiple Access (TDMA) デジタル無線通信、6 のキャリア周波数 (日本での DECT™ 実装)、10 のキャリア周波数 (ヨーロッパでの DECT™ 実装) および 5 のキャリア周波数 (米国での DECT™実装) からの動的チャネル選択、24 のタイム スロットに加え、マルチレイヤー セキュリティ システムを使用しています。この多層構造のシステムには、サブスクリプション、暗号化、および認証が含まれ、盗聴に対する非常に高度な保護を確保します。
医療や金融などの特定の業界では、最大限のセキュリティと機密性を確保するため、DECT™ ベースのワイヤレス通信が必要とされます。

## DECT™ セキュリティ チェーンの 3 つのステップ

DECT™ セキュリティ チェーンは、以下に示したとおりの 3 つのステップで構成されています。

### ペアリング

プロセスの最初の重要なステップは、ヘッドセットとベースを紐付けることです。ペアリングは無線でも行えますが、ヘッドセットをベースに物理的にドッキングさせる方法では、より高いセキュリティを確保できます。
これにより、プロセスの間に共有される秘密鍵（シークレットキー）が、無線ではなく充電の接点を介して交換されます。

### 認証

通話ごとに、ペアリングのプロセスで共有された秘密鍵を使用して、サブスクライブされたヘッドセットとベースの間の認証が確立されます。ペアリングされていないヘッドセットは、ベースで使用することはできません。

### 暗号化

通話ごとに、ヘッドセットとベースの間の音声は暗号化されるため、侵入者が読み取ることはできません。この暗号キーは 60 秒ごとに再生成されます。

## DECT™ セキュリティの進化

ワイヤレスでの会話の秘密性の保護は、常に最優先事項となっています。というのも、2009 に、DeDECTed Group と呼ばれるホワイトハットハッカーのグループが、基本的な DECT™ 製品に関するセキュリティの弱点の概要を述べたレポートを発表し、DECT™ 標準の強化の必要性が明らかになったためです。この中で、このハッカー グループは、DECT™製品が ETSI 標準で定められた標準の認証および暗号化を使用していないことによる、データ侵害の脅威を明らかにしました。Poly DECT™ ヘッドセット製品では、常に認証と暗号化を使用してきました。

Poly (Plantronics) もその会員である DECT™ Forum では、DeDECTed Group の報告を精査し、DECT™ のセキュリティロードマップを公開しました。最初の段階は Step A と呼ばれ、4 つの強化された DECT™ セキュリティ機能が追加されました。これにより、盗聴のリスクを低減し、会話の安全性を維持することができます (以下の表を参照)。

## STEP A
## 強化された DECT™ セキュリティ機能

**#1**
**新しい乱数生成器**
連続した試行で乱数を推測し、それをキーの生成に使用することは、事実上不可能です。

**#2**
**ピア側の動作の評価**
ヘッドセットからベースへの通信が予測パターンを外れると接続が中断されるため、ハッキング攻撃は、毎回あらゆる面で完璧でなければ成功しないでしょう。

**#3**
**即時の暗号化**
接続が確立された直後に、暗号化が有効化されるので、有用な情報が漏れることはありません。

**#4**
**鍵の再発行の手順**
通話中に新しく発行された暗号解読鍵を使用 – 暗号化エンジンにより使用される暗号解読鍵は、少なくとも 60 秒に 1 回は更新されるので、無差別にパスワードを組み合わせてログインを試みるブルートフォース攻撃などを阻止することが可能です。

公式の DECT™ Security Certification Program が 2013 年に公開され、承認された試験所で製品が個別に試験および検証されるようになりました。
Poly は、ワイヤレス製品業界の中で、DECT™ Forum で定められたセキュリティ標準を完全に満たした最初のプロバイダーです。2013 年 10 月に強化されたセキュリティ機能を搭載した Poly (Plantronics) CS500 シリーズが出荷され、その他の Poly 製品がすぐ後に続きました。
さらに先の段階も Step B および Step C として定義されており、各段階で、前のステップのセキュリティをより強化していきます。

## STEP B
DECT™ Standard Authentication Algorithm 2 (DSAA2) と呼ばれる AES 128 ビット暗号化に基づいた認証アルゴリズムの改良点を定義するもので、2012 年に公開されました。

## STEP C
DECT™ Standard Cypher 2 (DSC2) と呼ばれる AES 128 ビットキーに基づいた暗号化アルゴリズムの改良点を定義するもので、さらにセキュリティを強化するための真性乱数生成器が含まれています。ETSI がこの標準を定め、公開しています。

## DECT™ セキュリティの STEP C を上回るよう設計された POLY SAVI 7300 OFFICE シリーズ

Poly の Savi 7300 Office シリーズは、DECT™ セキュリティの Step C の要件を満たすよう設計されています。さらに、Step C で AES 128 ビットと定義されているところを、AES 256 ビット暗号化を使用することで、実際にはこの要件を上回る設計になっています。AES 256 ビット暗号化は、FIPS140-2 に準拠した承認済みのセキュリティ機能の一つであり、アメリカ合衆国連邦政府で必須とされているだけでなく、世界中の銀行や金融会社で使用されています。

また、Savi 7300 Office シリーズは、Bluetooth® 無線通信を使用しない設計のため、スマートフォンに接続することはできません。このため、Bluetooth 接続が禁止されていたり、録音や法令遵守の目的で企業の通信ネットワークを経由して通話する必要がある場合に最適です。

## POLY のリモートデバイス管理

Savi 7300 Office シリーズは、Poly のリモートデバイス管理ソリューションでサポートされているため、最新のファームウェアの修正およびパッチにより、デバイスを常に最新の状態に保つことができます。また、デバイスの設定をリモートで構成することもできます。ワイヤレスによるヘッドセットのサブスクライブ機能を無効化することで、さらにセキュリティを高めることができます。

## POLY DECT™ ヘッドセットのセキュリティ


| | |
|---|---|
| サブスクリプション方式 | 物理的または無線のいずれかで設定可能 |
| DECT™ セキュリティレベル | Step C を上回る |
| 認証 | 128 ビット DSAA2 (AES) |
| 暗号化 | 256 ビット AES Step C を上回る |
| BLUETOOTH 無線通信対応 | – |
| FIPS 140-2 準拠の機能 | ○<br>(256 ビット AES) |

## 用語集

**AES**
Advanced Encryption Standard の略。アメリカ合衆国連邦政府で採用されているだけでなく、世界中でデータの暗号化に使用されています。

**認証**
ヘッドセットとベースが相互に ID をアサートする動作。セキュリティ Step B において、DECT™ Standard Authentication Algorithm 2 (DSAA2) と呼ばれる、改良されたアルゴリズムの中で定義されています。これは、DECT™ セキュリティ標準 ETSI EN 300 175-7 で定義されている DSAA の最新版です。

**DECT™ FORUM**
DECT™ 業界の提携環境を支援し、DECT™ ワイヤレステクノロジーの開発と改善のためのプログラムを促進しています。Poly (Plantronics) は DECT™ Forum の正会員です。

**DSAA**
DECT™ セキュリティ標準 ETSI EN 300 175-7 で定義されている、DECT™ Standard Authentication Algorithm。ベースとヘッドセットで使用され、ペアリングが成功するためには、これが一致する必要があります。

**DSAA2**
DECT™ Standard Authentication Algorithm 2。DECT™ セキュリティ Step B で使用される、改善されたアルゴリズム。

**DSC**
DECT™ セキュリティ標準 ETSI EN 300 175-7 で定義されている、DECT™ Standard Cypher。

**DSC2**
DECT™ Standard Cypher 2。DECT™ セキュリティ Step C で使用される、改善されたアルゴリズム。

**暗号化**
真の意味を隠すように、情報が秘密コードに変換されるプロセス。セキュリティ Step C において、DECT™ Standard Cypher 2 (DSC2) と呼ばれる改善された暗号化アルゴリズムの中で定義されています。
これは、DECT™ セキュリティ標準 ETSI EN 300 175-7 で定義されている DSC の最新版です。

**FIPS140-2**
米国 National Institute of Standards and Technology (NIST、アメリカ国立標準技術研究所) によって規定された暗号モジュールのセキュリティ要件。承認済みのセキュリティ機能が記載されており、AES はこのうちの一つです。
米国政府機関で必須となっています。

**STEP B**
DECT™ Standard Authentication Algorithm 2 (DSAA2) と呼ばれる AES 128 ビット暗号化に基づいた認証アルゴリズムの改良点を定義するもので、2012 年に公開されました。

**STEP C**
DECT™ Standard Cypher 2 (DSC2) と呼ばれる AES 128 ビットキーに基づいた暗号化アルゴリズムの改良点を定義します。この標準は ETSI によって定められ、公開されました。

**サブスクリプション**
ヘッドセットとベースがペアリングされるプロセス。このプロセスでは、一意の認証コードと暗号化コードが交換されます。ヘッドセットとベースは、工場出荷時にすでにペアリングされています。

*注: 使用される DECT™ の周波数は国や地域で異なるため、Poly では市場によって異なる SKU を提供しています。

[1]The Global Risks Report 2019 14th Edition、Wold Economic Forum http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[2]Cyber Security Ventures 社「Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021 (2021 年までに世界のランサムウェア被害額が 200 億ドルに達する見込み)」

[3]Gartner 社「Forecast: Information Security and Risk Management Worldwide, 2018-2024, 3Q20 Update (予測: 世界の情報セキュリティおよびリスク管理、2018 年 ～ 2024 年、3Q20 アップデート)」(2020 年 10 月 5 日出版)