ワイヤレス設置の際に、事前検討事項

1) オフィスのレイアウトや空間　（広さ・仕切り方）
　下記の条件がある場合は、より慎重に検討する必要有
　　– 金属の遮蔽物や大きい設置物
　　– 大きな窓ガラス（特に金属でコーティングされているもの）

2) 設置台数
　何台設置したいのか？

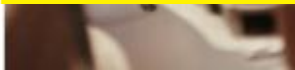
3) ヘッドセットの設置間隔
　　– 2 ～ 4m が理想

4) ワイヤレス製品無線通信規格
　DECT – 設置台数は、Wideband 時は、Narrowbandの1/2
　　出力を低くすれば、設置台数を増やせる可能性あり。

　Bluetooth – 使用時間が影響する。（1日中なのか、半日なのか）
　　WiFi (IEEE 802.11b,g,n)　に少なからず影響有

　DECT (1.9GHz) /Bluetooth (2.4GHz) は、共存可能

Jabra®
YOU'RE ON



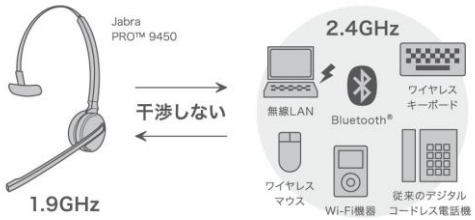
通信規格 – DECT

Jabra PRO 9450 は、DECT（Digital Enhanced Cordless Telecommunications ）**を通信規格として採用しております。**
1998年に欧州で開発された企画にて、現在欧米を含む、**世界の110ヶ国以上にて採用されており、民生使用の無線機器においては、最も“安全な”通信規格であると考えられております。**

日本国内においては、2010年10月26日省令改正、TELEC T-254発効。2011年 3月28日 ARIB STD-T101発効。
1,893~1,906 GHz の周波数帯域の5キャリアを使用しています。

- 欧州DECT: 1,880 ~ 1,900 GHz / 米国DECT: 1,920 ~ 1,930 GHz

国内のほとんどのワイヤレス製品は、2.4GHz 帯 を使用しており、1.9GHz 帯である DECT製品は、
2.4GHz 製品との電波の干渉は、皆無に等しいです。



DECT方式は、認証アルゴリズムと暗号化によりセキュリティーを保証しております。
認証アルゴリズム（DSAA – DECT Standard Authentication Algorithm）は、一般には公開されておらず、DECT 製品製造会社のみが知っているだけです。
ベースユニットが無作為に選定した信号をヘッドセットに送り続け通信します。

*GN Netcom A/S は、DECT Forum の正会員です。
そして、GN ネットコムジャパン は、DECT Forum Japan ワーキンググループの正会員です。

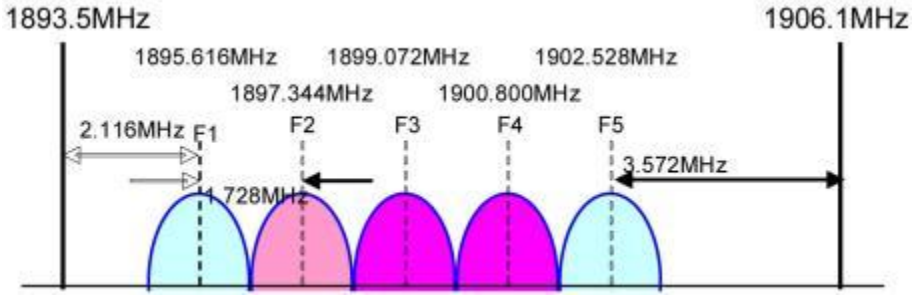
J-DECT

Jabra®
YOU'RE ON

同時使用台数：最大 18台

Jabra PRO 9450 は、DECT（Digital Enhanced Cordless Telecommunications ）**を通信規格として採用しております。**

DECT通信方式は、1キャリア（搬送波）に24スロット（12チャネル）を多重するTDMA/TDD方式を採用
国内DECTは、下記の通り 5 キャリアを使用しています。 しかしF2 ~ F4 は、既存 PHS（及び 開発中？Super PHS）にて占有されているため、既存PHSとの干渉を防ぐため、Jabra PRO 9450は下記 F1 または、F5 の 2キャリアのみ使用しております。



よって、同時使用できる台数にもかなりの制限があり、下記のような計算にて算定いたします。

机上にて、

1 キャリア： 24スロット ÷ 2（up link と down link）= 12 台

12 台 x 2 キャリア = 24 台

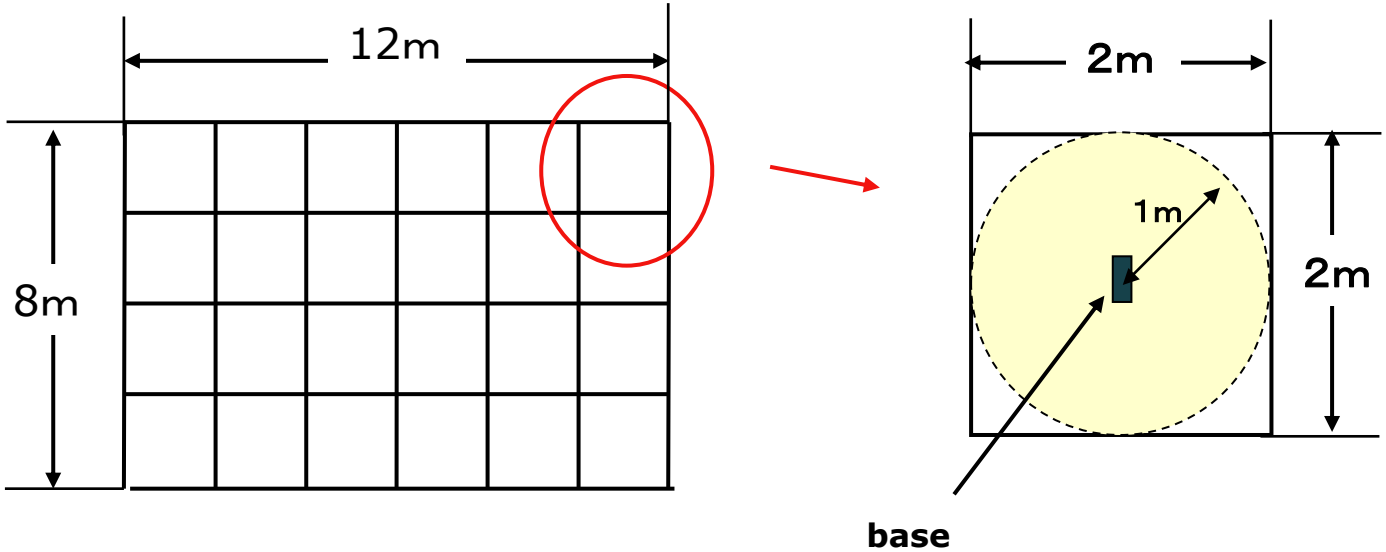
しかし DECT は、机上の計算通りには作動せず、実験及びいくつかのシュミレーションより、
弊社としては、計算の75% を 実作動と考えます。

24 台 x 75% = 18 台

もちろん、オフィスの環境・設置方法、Jabra PRO 9450 の 出力調整の組み合わせにて、左右される場合はあります。
狭いオフィスにて、適当な数のJabra PRO 9450 を使用する際は、出力をVery Lowに設定して使用することお奨めいたします。

推奨設置可能台数 （ １台／ ４㎡）

電波の衝突を軽くするため、バースユニットの設置間隔は、２ｍ
（間隔が広がれなそれだけ電波の衝突は防げます）**よって、**４ ㎡ となります。



例） 24 cell ／96㎡

Jabra®
YOU'RE ON

セキュリティ　– 認証と暗号化

DECT方式の通信のセキュリティでは、望ましくない第三者が電気通信の内容（ここでは音声通話）にアクセスできないようになっています。セキュリティには、主に2つの要素があります。認証アルゴリズムと暗号化によりセキュリティーを保証しております。

認証アルゴリズム（DSAA – DECT Standard Authentication Algorithm) は、一般には公開されておらず、DECT 製品製造会社のみが知っているだけです。 ベースユニットが無作為に選定した信号をヘッドセットに送り続け通信します。

DECT方式、DSC (DECT Standard Cipher)にて、この暗号化されています。 DSCは、35bit の初期化ベクター（IV)を用いたストリーム暗号と、そのキーとなるストリームとアクセスするためのキーとなる暗号の組み合わせです。DSCの仕様はもまた一切一般に公開はされておりません。

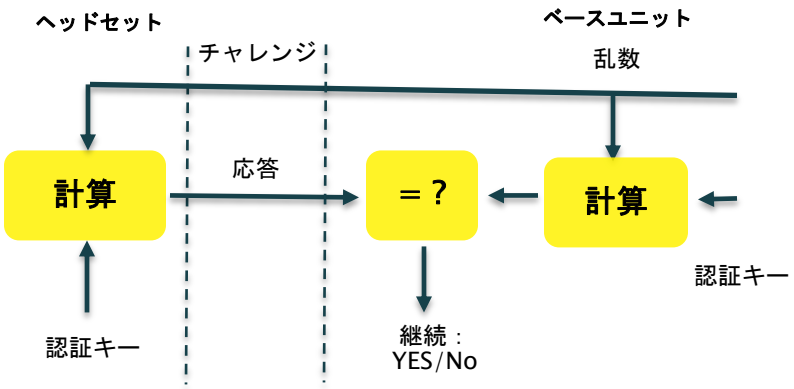
– 導出暗号キー:　ベースステーションとヘッドセット間の認証からの出力値。
各通話を成立させるために認証が実行されると、全てのデータに対して新しい暗号キーが使用されるようになります。

IVは、暗号化が行われるフレーム用のフレーム番号で初期化されます。フレームが送信されるたびに、IVはフレーム番号に応じて増えます。IVと暗号鍵を入力値として、キーストリームがDSCにより導出されます。その後、このキーストリームに対し、送信予定のデータフィールドとの排他的論理和（XOR）演算が行われます。

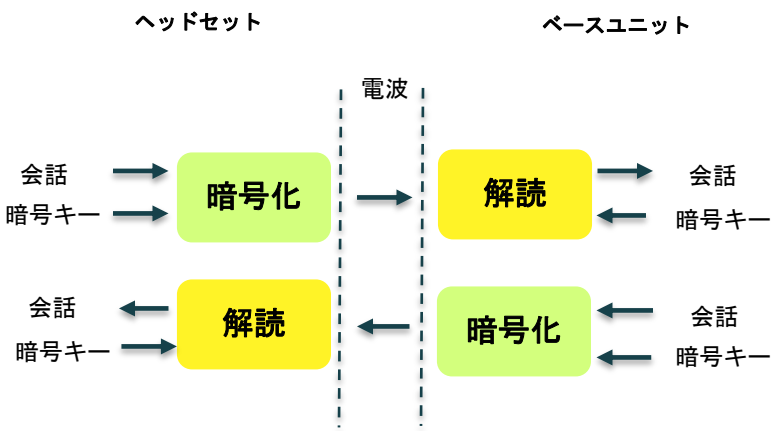
Jabra®
YOU'RE ON

セキュリティ　– 認証と暗号化

認証アルゴリズム



暗号化



今日DECT機器を盗聴・解析が可能なソフトウエア・ハードウエアは存在しないといわれております。もし通話内容が盗聴された場合は、回線元に対してなんらかの細工をされたか、通話データの保存場所に対し攻撃されたと見られます。または、社内の誰かが直接その機器に加工をする以外ありえません。

送信・受信するデータ毎に全ての異なる暗号キーとそれをとく解読キーが親機・子機にて生成され、通信を成立させます。よって、その異なるキーの組み合わせの及び生成するアルゴリズムを解析することは、限りなく不可能となりユーザーの通話の安全を保全します。