その画面、電磁波で“のぞかれて”いませんか？

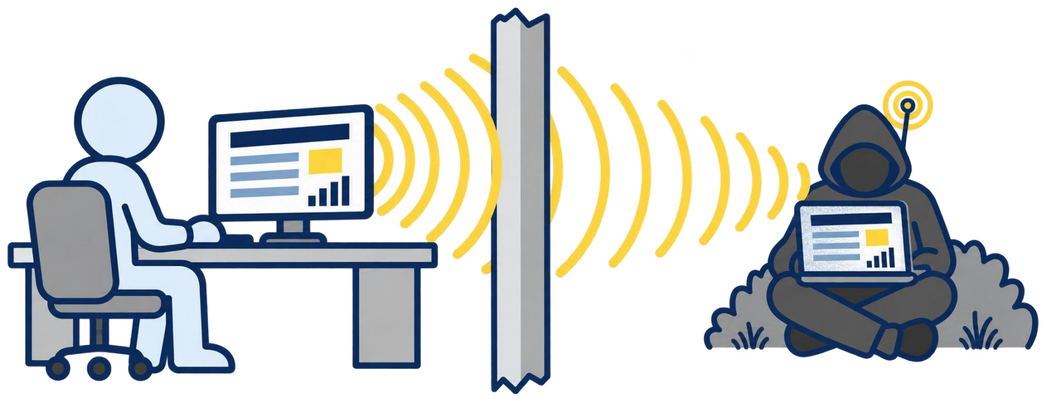
漏えい電磁波による情報窃取 ― パッシブTEMPESTの脅威とシールドによる対策

奈良先端科学技術大学院大学　情報セキュリティ工学研究室

■ TEMPEST（テンペスト）とは

パソコンやディスプレイ、キーボードなどの電子機器は、動作中に意図しない微弱な電磁波を出しています。この電磁波には、画面に表示された内容やキー入力の情報が含まれています。

離れた場所でこの電磁波をアンテナと受信機で捉え、信号処理を施すと、**画面の映像や入力した文字を再現できてしまいます。**これが「TEMPEST」と呼ばれる電磁波による情報漏えいです。



- ❑ 機器に触れる必要はなく、漏れてくる電磁波を「受信するだけ」で情報を盗める
- ❑ ネットワークを経由しないため、ファイアウォールやウイルス対策ソフトでは防げない
- ❑ 攻撃の痕跡（ログ）が残らず、盗まれたことに気づけない
- ❑ インターネットから切り離した端末（エアギャップ環境）からも情報が漏れる

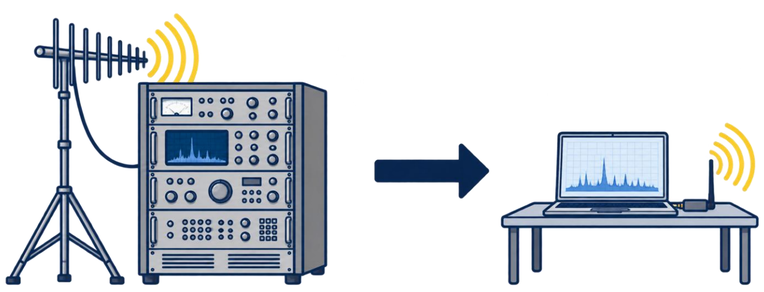
■ 何が盗まれるのか



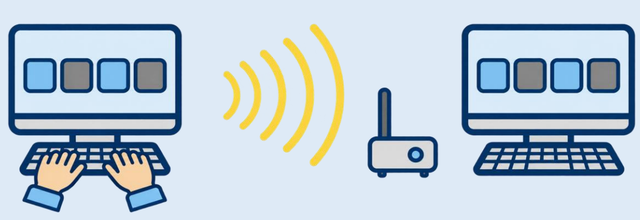
- ❑ ディスプレイの画面：文書、会議資料、設計図、個人情報など
- ❑ タブレット・スマホのタッチ入力：画面上のキーボードで押したキーが光るため、暗証番号やパスワードが読み取られる
- ❑ キーボードの打鍵：キーごとに電磁波のパターンが異なる
- ❑ プリンタやヘッドセットなどの周辺機器

※暗号化されたデータも、人が読むために画面に表示された時点で元の情報に戻っています。**暗号化では画面の情報は守れません。**

■ 誰でも攻撃できる時代に



- ❑ かつて：軍や政府機関だけが持つ、高価な専用装置が必要だった
- ❑ いま：市販の安価な受信機（ソフトウェア無線）と、公開されている解析プログラムで実行できる
- ❑ 我々の研究では、**持ち運べる小型の装置で、タブレットの画面と入力文字を離れた位置から再現・自動認識できる**ことを実証
- ❑ 海外では、80 m離れた場所から高精細ディスプレイの映像を再現した報告もある

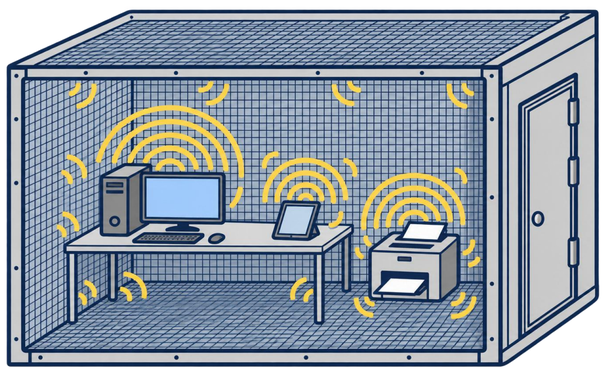


■ このブースの実演

入力用のPCに打ち込んだ数字を、離れた場所に置いたアンテナと受信機で電磁波から読み取り、別のPCの画面に表示します。**2台のPCはケーブルでもネットワークでもつながっていません。**

■ 対策の要は「シールド」

機器ごとの対策として、電磁波にノイズを重ねて情報を隠す方法（マスキング・ジャミング）や、ケーブルにフィルタを入れる方法もありますが、機器や漏えい経路ごとに個別の設計が必要です。シールドは、部屋や機器を導電性の材料ですき間なく覆い、内部の電磁波を外に出さない対策です。**守りたい機器の種類やメーカーに関係なく、空間ごとまとめて守れるのはシールドだけです。**





	機器ごとの対策	シールド
守れる範囲	対策した特定の機器だけ	**空間内のすべての機器**
新しい機器	その都度、対策が必要	**持ち込めばそのまま守られる**
未知の漏えい	想定外の経路は防げない	**経路を問わずまとめて遮へい**

- ❑ 扉・窓・換気口・ケーブルの貫通部のすき間が弱点 → シールド扉、シールドガラス、フィルタで処理
- ❑ 施設の重要度に応じて遮へい性能を設計し（例：60 dB＝電界強度を1/1000に）、施工後も定期的に測定

画面に映した瞬間、情報は暗号で守られていません。“電磁波を漏らさない空間”づくりが確実な第一歩です。