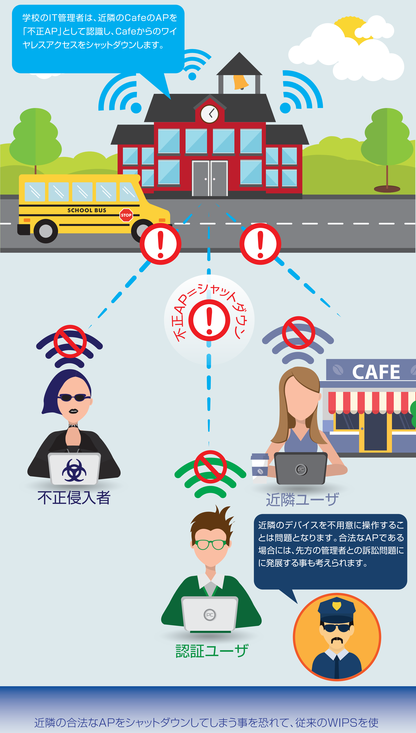
なぜ無線LANにWIPS機能が必要なのか?

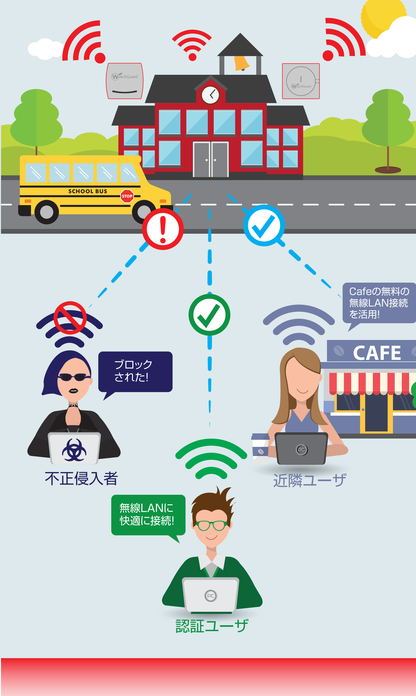
無線LANの急増は、利用者のインターネット接続に関する利便性が大幅に向上する一方、サイバー攻撃者にとっては、企業のネットワークやシステムへの侵入、探索、個人情報の搾取、マルウェアの感染・拡散などの不正行為のための機会が増加することにもなります。他社のWIPS(ワイヤレス侵入防御システム)では、アクセスポイントの規格によるフロー制御に依存するため、いくつかのセキュリティの課題を残しています。

一般的な他社のWIPSソリューションの場合には、ネットワークで認証されていない多くのAPを「不正AP」としての検知します。その検知結果により、管理者は合法な近隣のAPをシャットダウンしてしまう場合があります。



近隣の合法なAPをシャットダウンしてしまう事を恐れて、従来のWIPSを使用する管理者は不正APのアラートを無視するか、アラート機能を停止することを選ぶでしょう。また、この状況は、すべての無許可APを手動で調査するのに費やす管理者の負荷の増大と、実際の不正APによる脅威への対応といった課題を残します。

この課題はWatchGuard WIPSで解決できます。特許取得済みのMarker Packet 技術により、WatchGuard WIPS は自動的にワイヤレスクライアントを識別し、認定デバイス(Authorized)、ゲスト(Guest)、不正デバイス(Rogue)、外部(External)として分類します。
WIPSによる誤検知の排除により、管理者は重要な不正デバイスの排除のための作業のために時間を割り当てることが可能になります。



先進のWatchGuard WIPS(特許取得:ワイヤレス侵入防止システム)により、セキュリティを犠牲にしない、有益性の高い、ハイパフォーマンスな無線LAN環境を提供します。

Learn more at www.watchguard.co.jp

WatchGuard