資料1－4

www.pwc.com/jp/advisory

総務省
公衆無線LANセキュリティ分科会

公衆無線LANへの攻撃手法

2017/11/24

PwCサイバーサービス合同会社
サイバーセキュリティ研究所 所長
神薗 雅紀

pwc

攻撃の分類

情報セキュリティの定義における下記の特性のいずれを侵害するかによって、公衆無線LANに対する攻撃手法を整理する。

可用性（Availability）

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

機密性（Confidentiality）

認可されていない個人，エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。

完全性（Integrity）

正確さ、および完全さの特性。

※JIS Q 27000より

無線LANの動作・認証方式

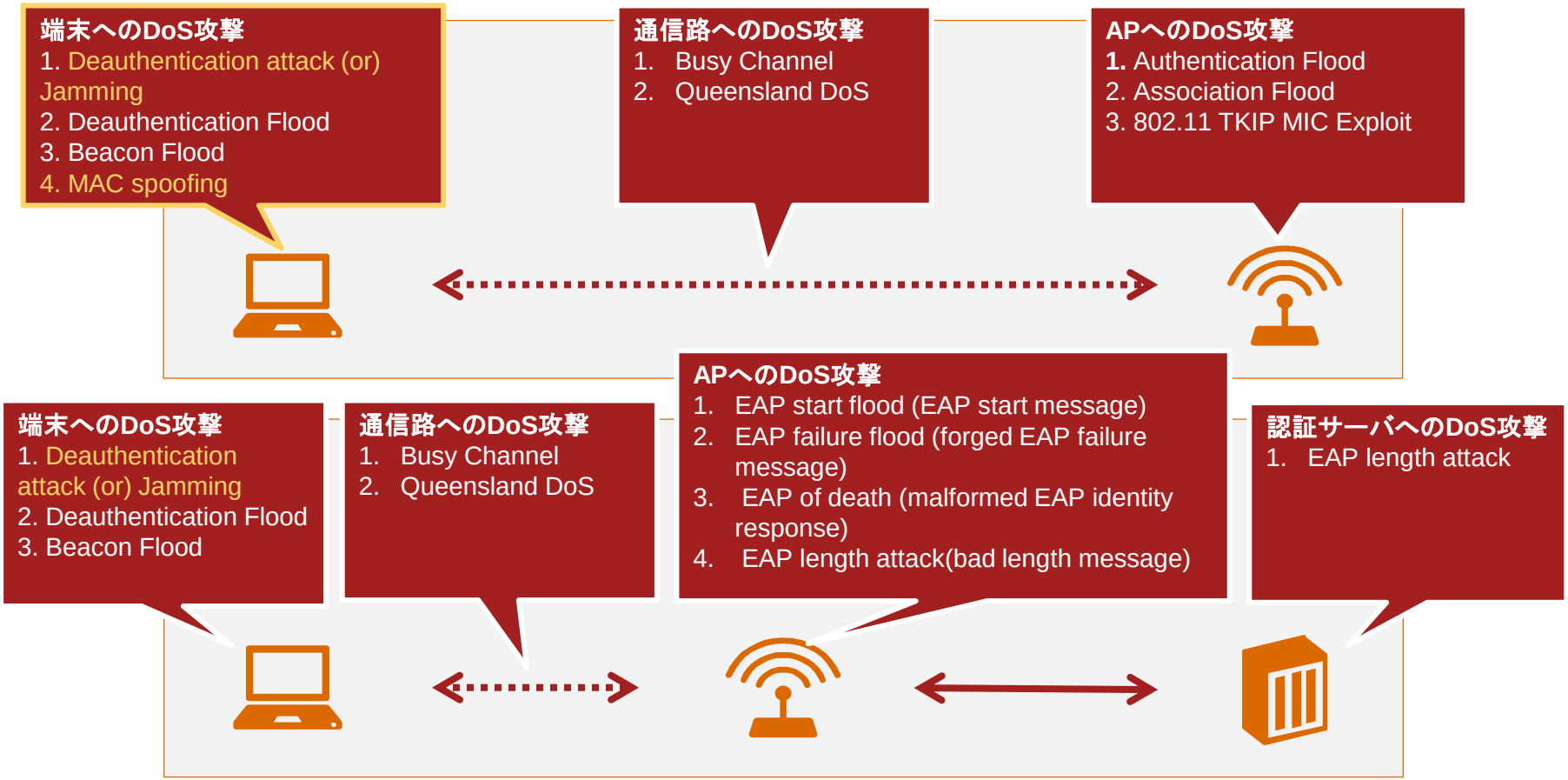
無線LAN通信の動作・認証方式には下図のように複数のモードがあり、動作・認証方式と攻撃目的によって接続端末、アクセスポイント(AP)、通信路など、攻撃者が介入する位置が変化する。

アドホック・モード

インフラストラクチャ・モード

可用性を侵害する攻撃

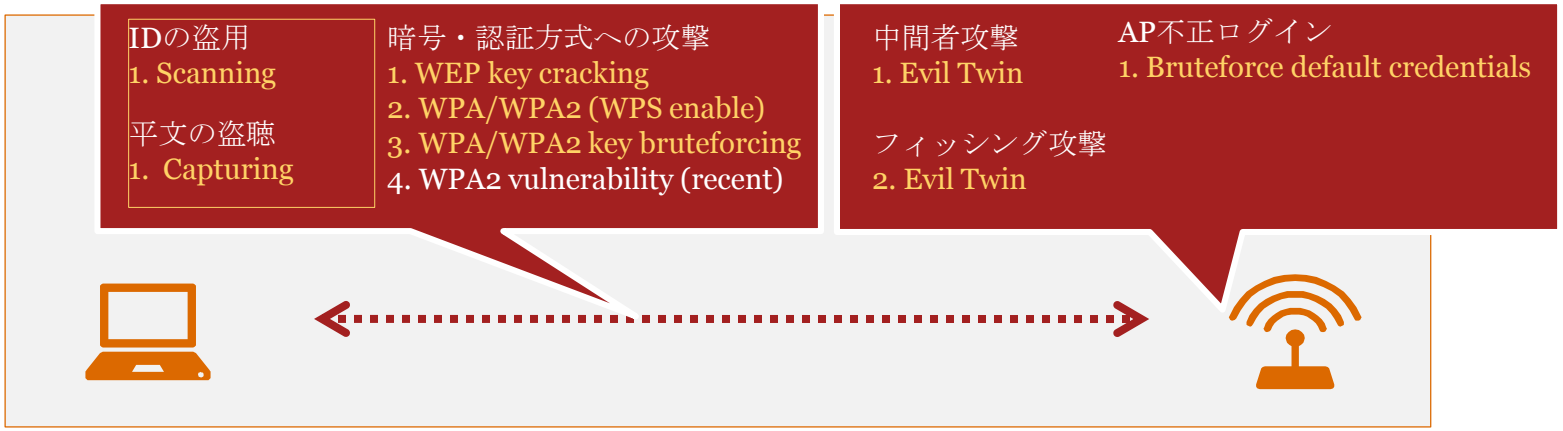
主に**DoS攻撃**や**Jamming攻撃**によって標的を通信不可能な状態に追いやる手法となる。代表的なものとして強制的に標的端末の認証を解除する攻撃や、電磁的なノイズで通信をジャミングする攻撃が存在する。

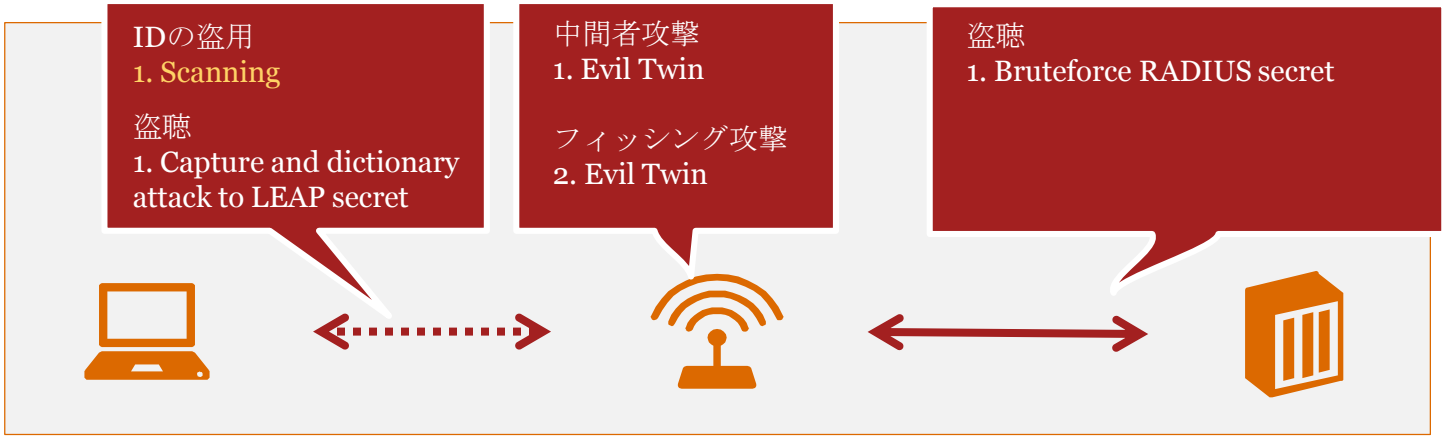


※上図のうち、黄色で表記されているものは実現が比較的容易な攻撃手法。

機密性を侵害する攻撃

無線電波を盗聴し、暗号化を解読するなどして標的の通信内容を不正に取得する。また正規のAPになりすまし、標的を悪意ある環境に誘い込むような攻撃も存在する。

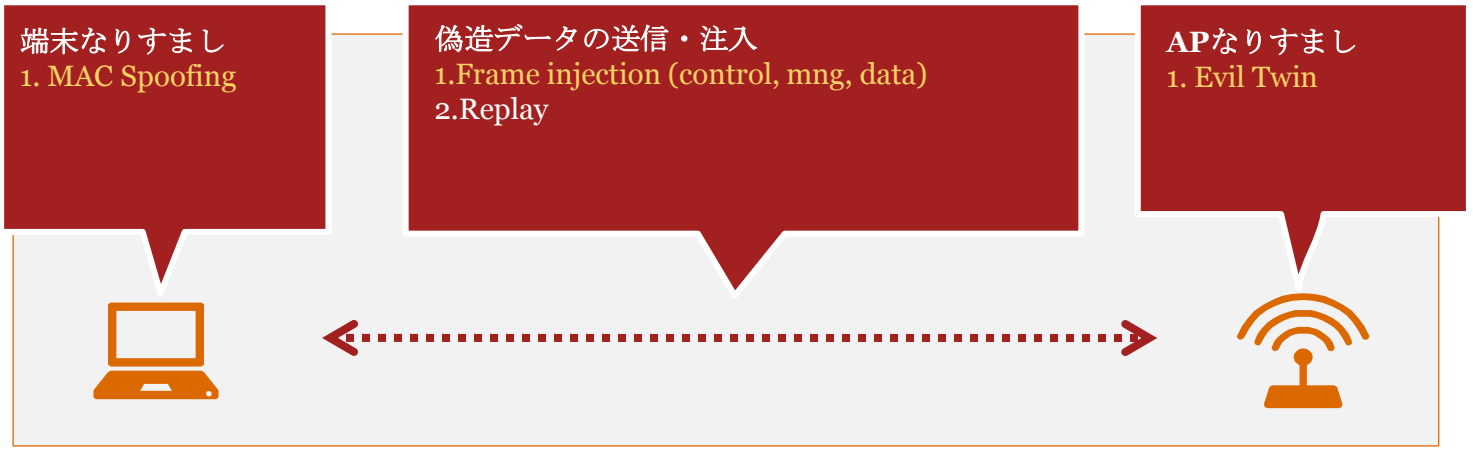




※上図のうち、黄色で表記されているものは実現が比較的容易な攻撃手法。

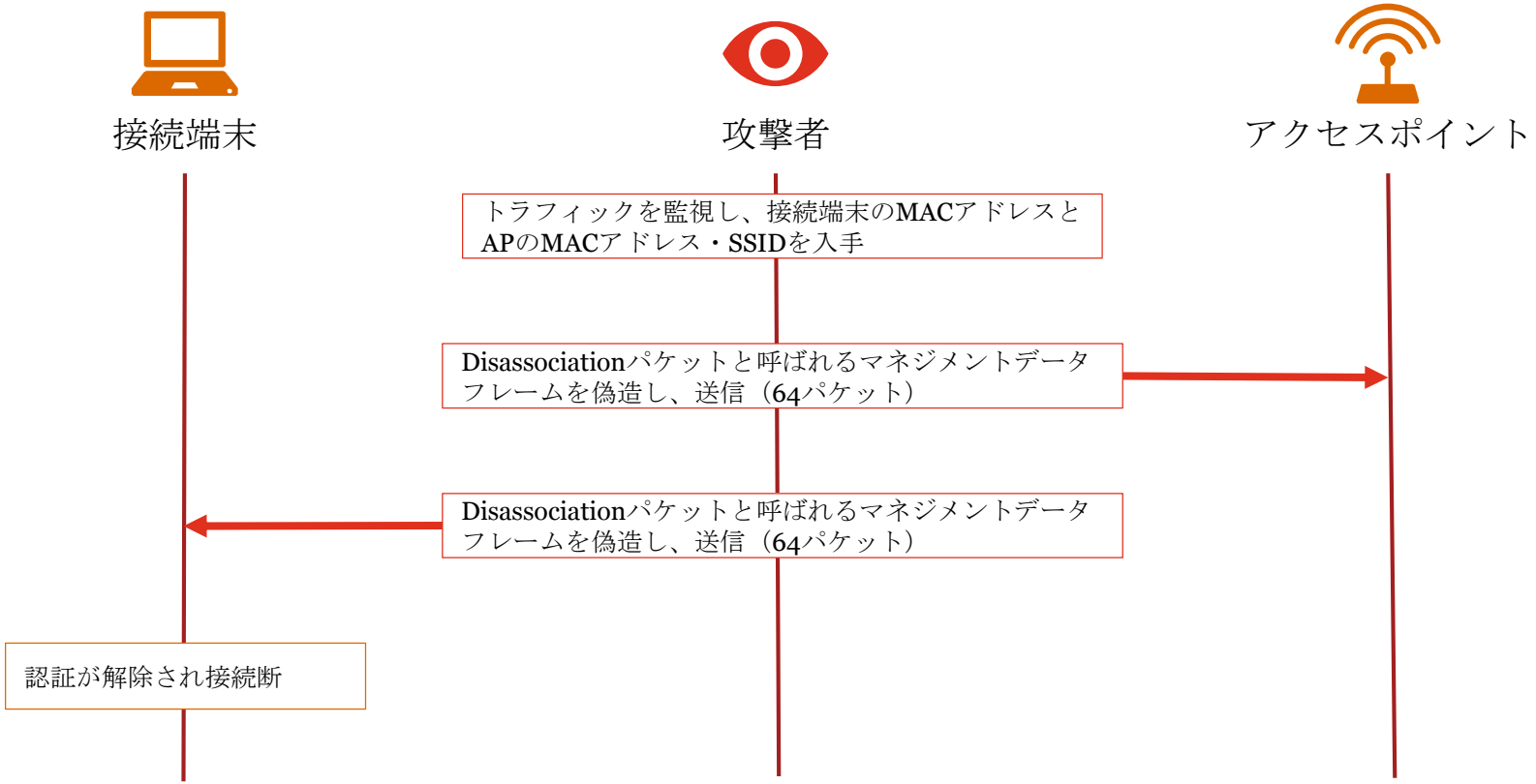
完全性を侵害する攻撃

他端末や正規のAPになりすまし、偽造した制御データフレームなどを注入するといった攻撃となる。



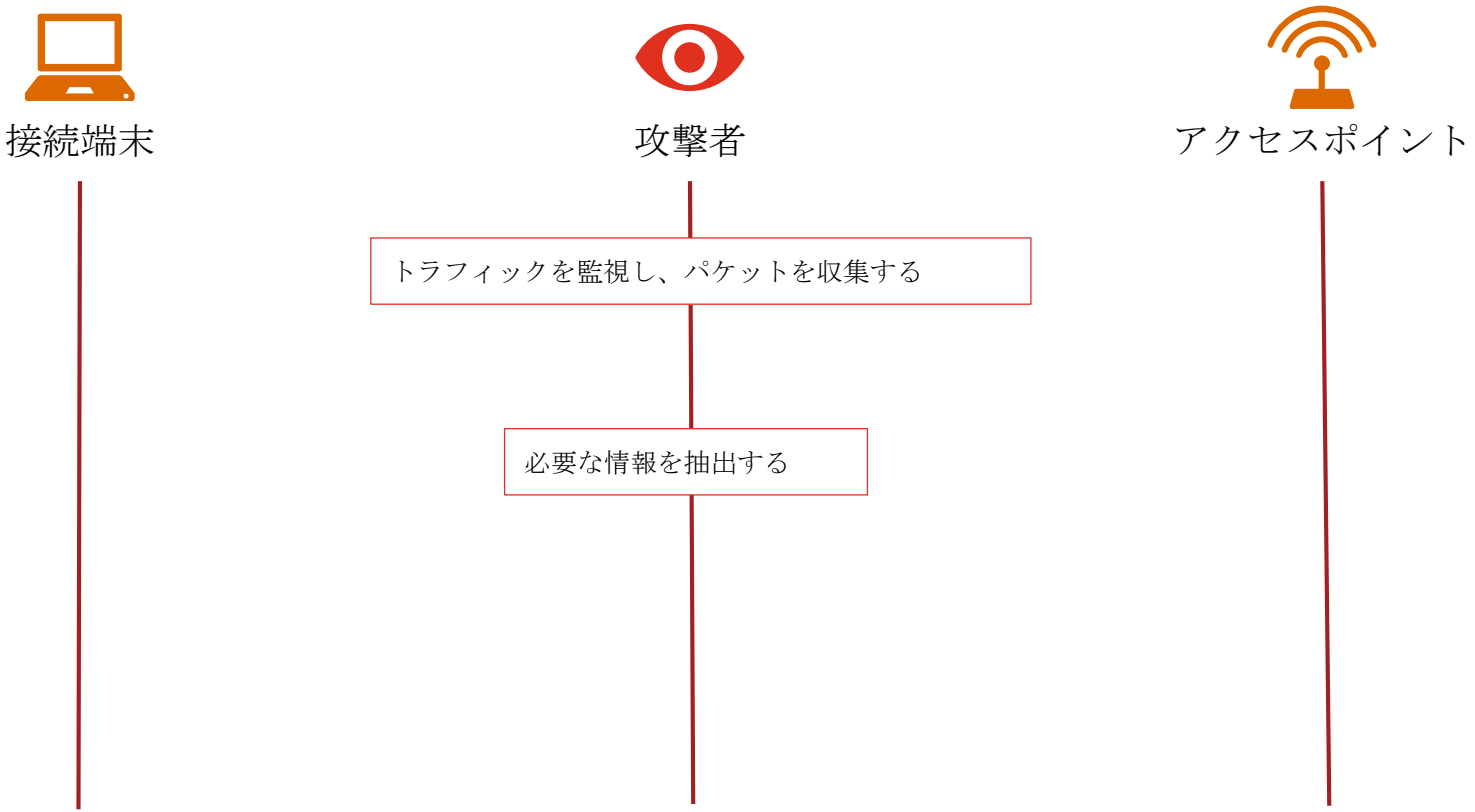
※上図のうち、黄色で表記されているものは実現が比較的容易な攻撃手法。

Jamming / deauthentication attack



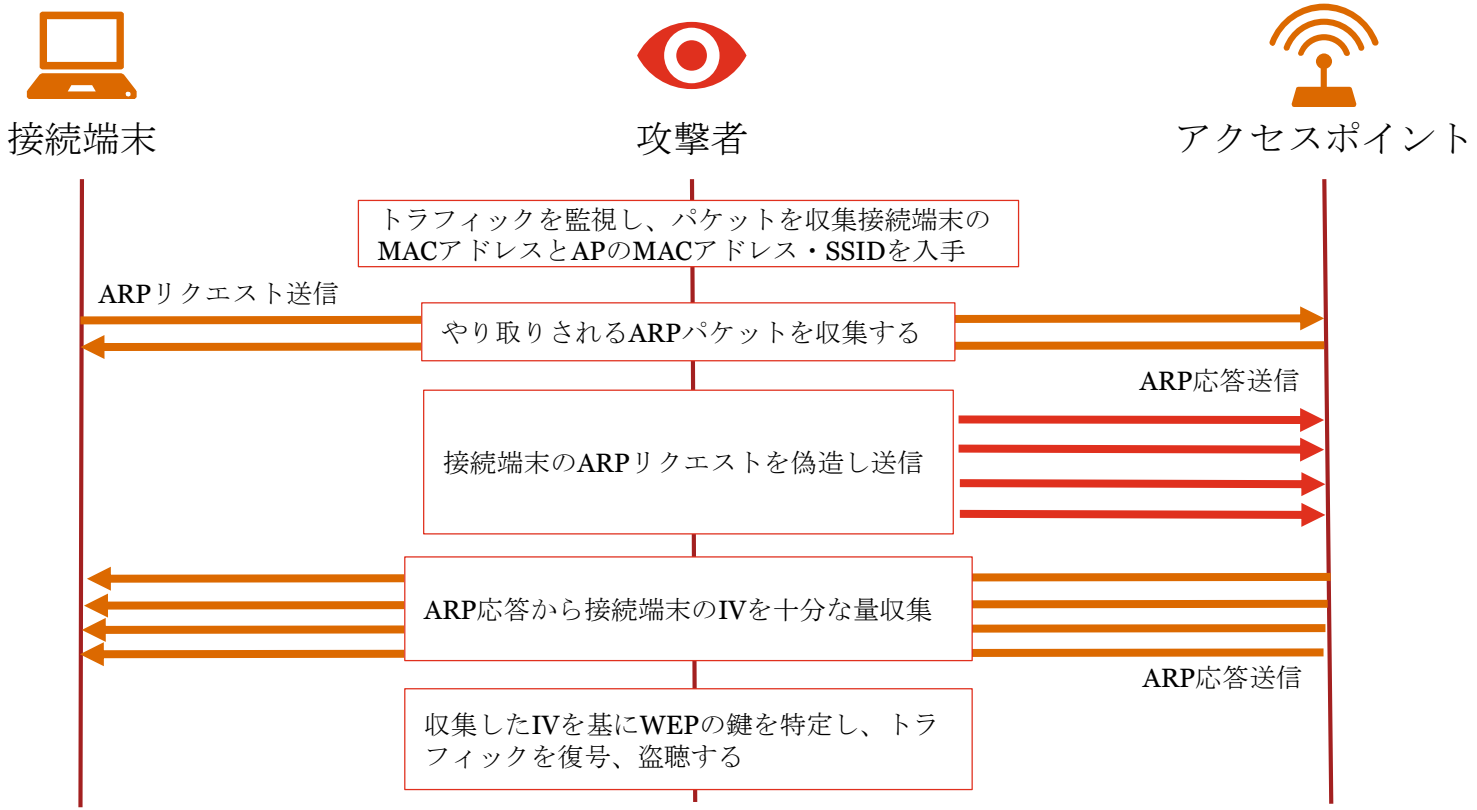
目的	脆弱性	対策	影響範囲
DoS	802.11規格においてマネジメントデータフレームが認証なしで送信される仕様	802.11wを利用する	すべてのクライアント端末

Eavesdropping Plain Text (open network)



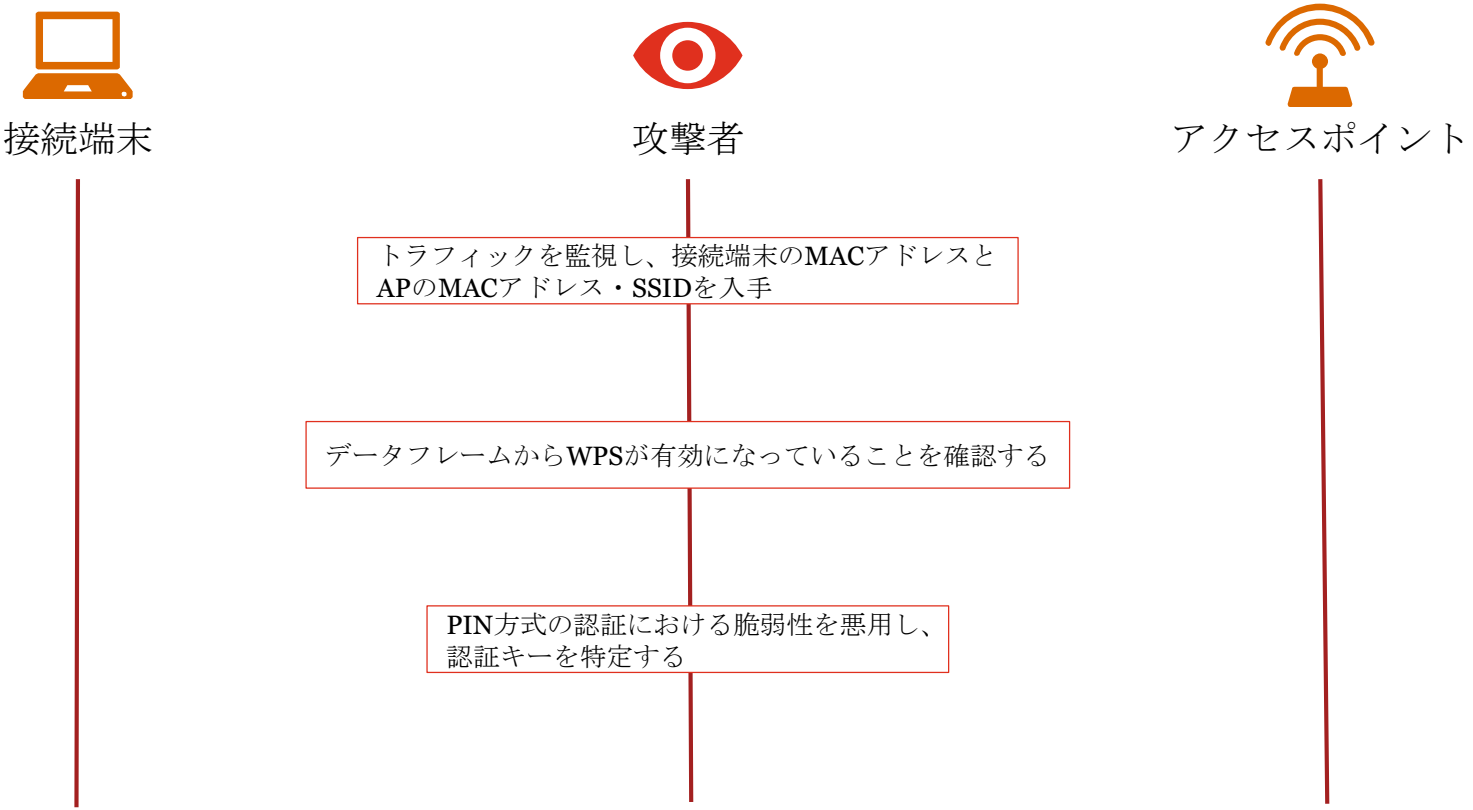
目的	脆弱性	対策	影響範囲
盗聴	オープン認証ネットワークでは通信が暗号化されていない点	アクセスポイントに暗号化と認証を設定する	すべてのクライアント端末とアクセスポイント

WEP Key Cracking (arp replay)



目的	脆弱性	対策	影響範囲
盗聴	WEPの鍵管理における暗号理論的な脆弱性	WPA2を利用する	すべてのクライアント端末とAP

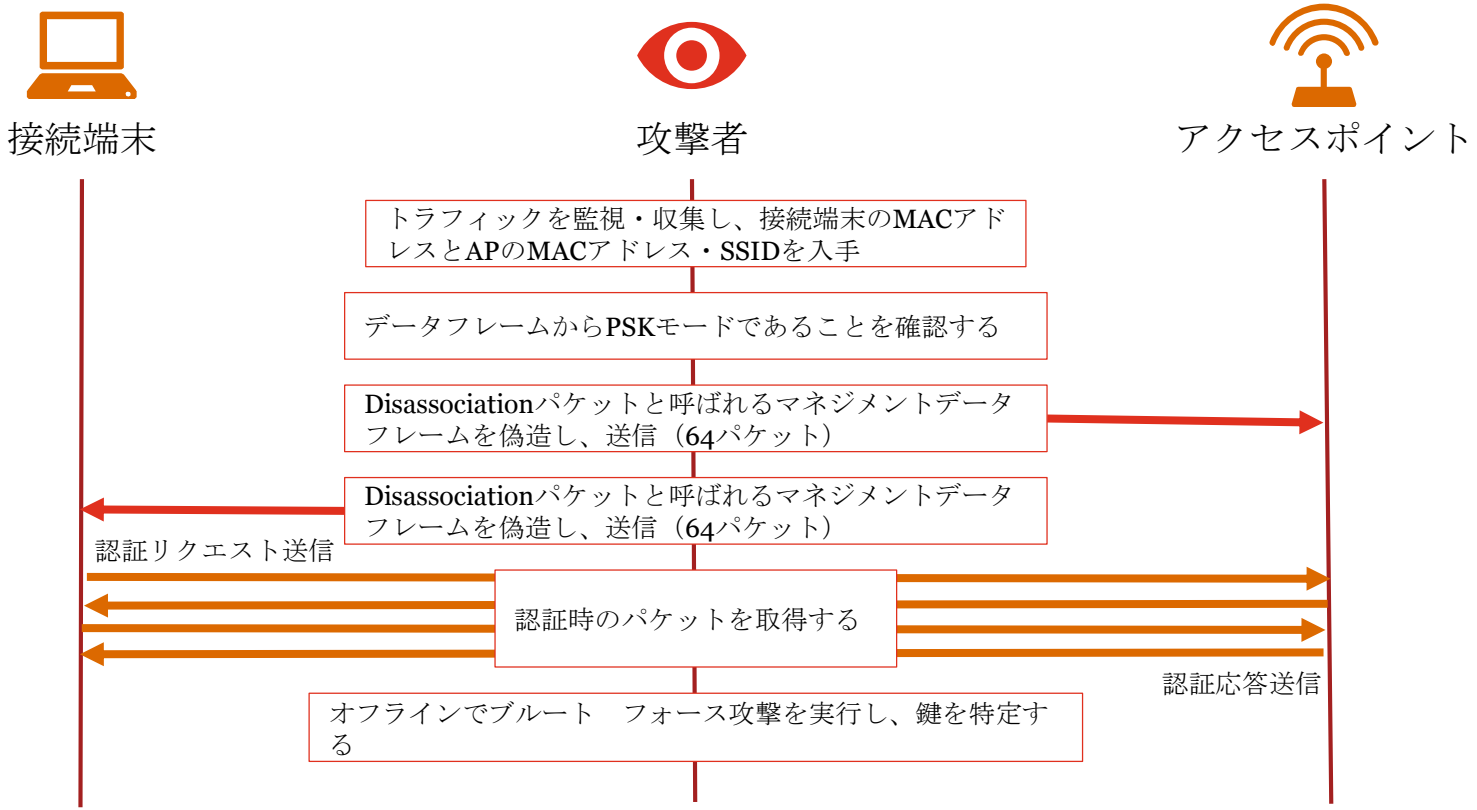
WPA/WPA2 - (WPS enabled AP)



目的	脆弱性	対策	影響範囲
盗聴	WPS※のPIN方式では容易にブルートフォース攻撃が実行できる	WPS機能を無効にする	すべてのクライアント端末とAP

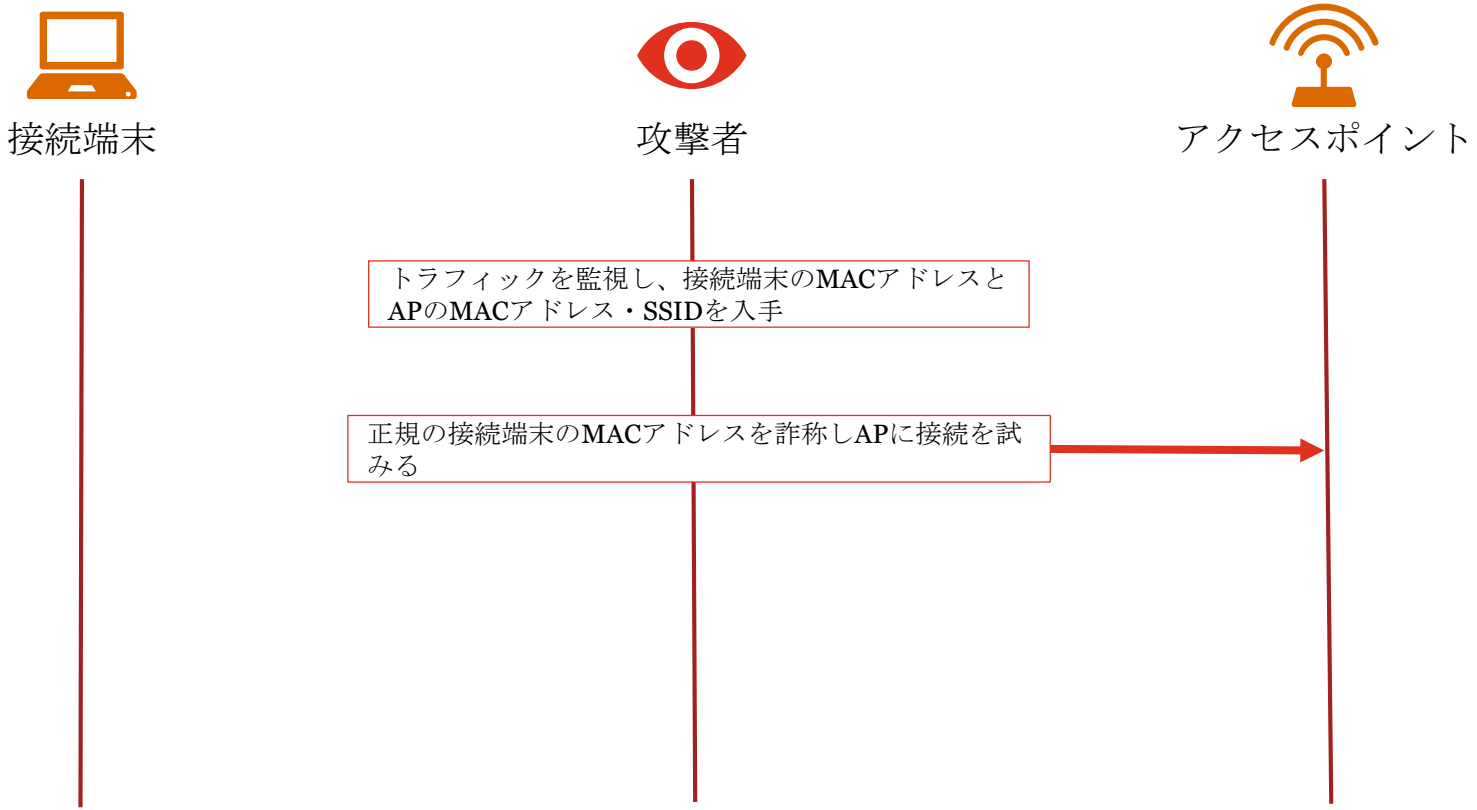
※WPS:Wi-Fi Protected Setupとは、無線LAN機器同士の暗号化設定を容易に行えるようにするための規格。

WPA/WPA2 - (key bruteforcing)



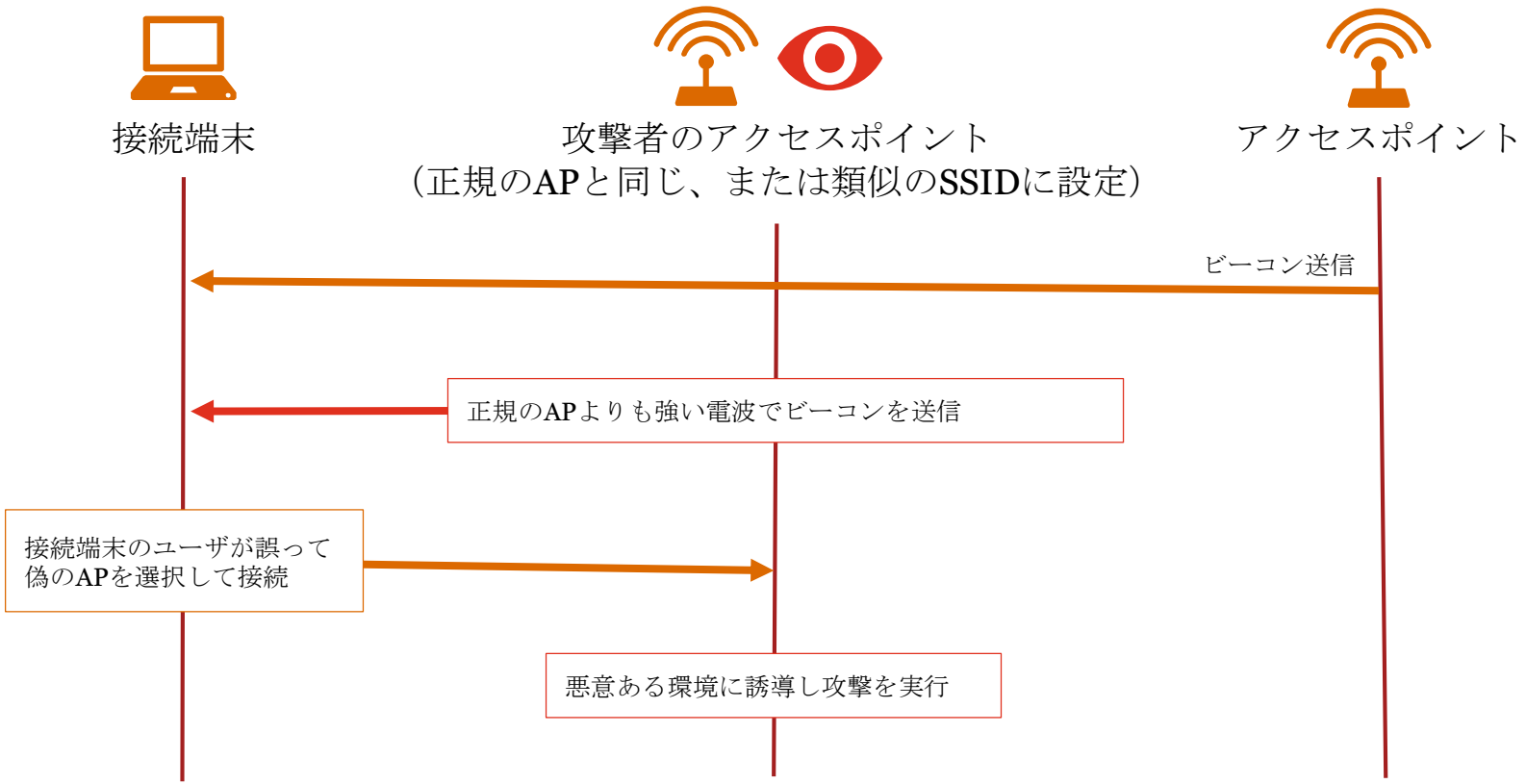
目的	脆弱性	対策	影響範囲
盗聴	PSK方式または8から63文字のASCIIコードのパスワードの利用	強固なパスワードを設定する	すべてのクライアント端末とAP

MAC Spoofing



目的	脆弱性	対策	影響範囲
DoS なりすまし	802.11規格においてコントロールフレームが保護されていない仕様	802.11wを利用する IPSを利用する	すべてのクライアント端末

Evil Twin



目的	脆弱性	対策	影響範囲
盗聴	ソーシャルエンジニアリング	不用意に不特定多数が利用する環境のアクセスポイントに接続しない	すべてのクライアント端末