CL-007

無線 LAN 暗号化の阻害を可能とする新たな攻撃法の提案とその効果 -WPA2 に対する暗号化無効攻撃の新たな提案-

Proposal of a new attack method that can block wireless LAN encryption and its effect -A new proposal for an encryption invalidation attack against WPA2-

井上 雄登† 中嶋 祥吾† 西井 大智† 白石 善明† 森井 昌克†
Taketo Inoue Shogo Nakajima Daichi Nishii Yoshiaki Shiraishi Masakatu Morii

1 はじめに

今日，ネットワーク接続のために利用される無線 LAN のほとんどが Wi-Fi 機器によるものである．自宅ではもちろんのこと，ホテルやカフェなどの商業施設，図書館や空港といった公共施設においてでさえ Wi-Fi を利用することが当たり前となっているが，データの送受信に電波を利用する Wi-Fi は盗聴が容易であるため，通信内容の暗号化は必要不可欠である．そこで，Wi-Fi では標準暗号方式として WPA2，もしくはその後継としての WPA3 が利用されている．しかしながら，それらの暗号方式が必ずしも安全であるとは言い切れず，実際に KRACK[5] あるいは Dragonblood[6] をはじめとする，WPA2/3 の脆弱性を利用した攻撃法が過去に提案されている．また，2020 年には Kr00k と呼ばれる WPA2 の脆弱性を利用した攻撃が発表されている [1]．Kr00k を実行すると一部の Wi-Fi 端末では送信バッファにあるパケットがすべて 0 の暗号鍵で暗号化されたうえで送信されてしまうため，攻撃者はチャネルを盗聴することで容易にそれらのパケットを復号することが可能となり，重要な情報が漏洩してしまう恐れがある．しかし，実際の利用環境を想定した場合，送信バッファにパケットがたまっている状況というのは一瞬しかないため，攻撃が成功する確率は限りなく低く，現実的な影響はないとされている [3].

そこで，我々は実環境においてもパケットを復号することができるような新たな攻撃法を提案する．本攻撃では DoS 攻撃を用いることにより，クライアントのデータ送信を停止させ，Wi-Fi 端末の送信バッファにパケットをためさせる．その後 Kr00k を実行することで，クライアントにすべて 0 の暗号鍵で暗号化したパケットを送信させる．そして，それらのパケットをキャプチャ，復号することで端末のアクセス先の情報等を盗み取る．本攻撃は KRACK とは異なり，中間者となることや攻撃対象のクライアント端末と同じ Wi-Fi に接続している必要はなく，電波の届く範囲にいるだけでよいため比較的容易に実行することができる．

本論文の構成は以下のとおりである．まず第 2 章では Wi-Fi のセキュリティプロトコルについて説明する．次に第 3 章では Kr00k の概要と実現可能性について説明する．第 4 章では Kr00k と DoS 攻撃を組み合わせた新たな攻撃の流れについて述べ，第 5 章でその評価及び，対策について考察する．最後に第 6 章で全体の結論を述べる．

2 Wi-Fi セキュリティ

本章ではまず，Wi-Fi のセキュリティプロトコルについて説明する．

2.1 アクセスポイントとの接続

クライアントが Wi-Fi を利用して通信を開始するためにはまずアクセスポイントと接続する必要がある．本節ではクライアントとアクセスポイントの接続手順について説明する．

アクセスポイントは通常，1 秒に約 10 回の規則的な間隔でビーコンと呼ばれる短い無線メッセージを送信することで自身の存在を広告している．アクセスポイントに接続したいクライアントはまず，通信可能なアクセスポイントを見つけようとする．これには静的スキャンと動的スキャンの 2 つがある．静的スキャンではクライアントは次々に無線周波数 (チャネル) を切り替えながら，ビーコンメッセージを聞くことでアクセスポイントを見つける．動的スキャンではクライアントはプローブ要求と呼ばれるメッセージを送信する．プローブ要求を受信したアクセスポイントはそのクライアントに対して，ビーコンと同じような内容のプローブ応答を送信する．この方法により，クライアントはそのエリアのアクセスポイントを素早く把握することが可能となる．

次にクライアントは見つけたアクセスポイントの中から接続したいアクセスポイントを選択し認証手続きに入る．現在では認証手続きは形だけのものであり，情報などは特に交換されない．ただし，アクセスポイントとクライアントの双方が WPA3 に対応している場合には認証手続きの前に，SAE(Simultaneous Authentication of Equals) ハンドシェイクによって事前共有鍵から一時的なマスター鍵を生成する．認証手続きが終了すると，アソシエーション手続きに入る．クライアントはアクセスポイントにアソシエーション要求を送信する．要求を受信したアクセスポイントは，より詳細な通信方式の情報が含まれているアソシエーション応答を返す．

2.2 4way handshake

接続しようとしているアクセスポイントがセキュリティプロトコルとして WPA2 を採用している場合，アソシエーション手続きの後に，4way handshake と呼ばれる鍵生成・共有プロトコルに従って暗号鍵の生成と共有を行う．4way handshake では PTK(Pairwise Transient Key) と GTK(Group Temporal Key) という 2 種類の鍵をインストールする．ここで，PTK はユニキャスト通信を暗号・復号化するための鍵であり，アクセスポイントとクライアント 1 つに対して共通のものが 1 つできる．GTK はマルチキャスト，ブロードキャスト通信を暗号・復号化するための鍵であり，アクセスポイントに接続しているすべてのクライアントで共通のものとなる．

まず PTK であるが，これはアクセスポイントのパスフレーズと MAC アドレスから事前に計算さ

† 神戸大学
Kobe University

れる PMK(Pairwise Master Key)，クライアントとアクセスポイントの MAC アドレス，そして 2 つの乱数 ANonce(Authenticator Nonce) と SNonce(Supplicant Nonce) から生成される．PTK はアクセスポイントがクライアントに GTK を送信する際の暗号化に用いる KEK(Key Encryption Key)，クライアントがアクセスポイントから送られた GTK を復号するために使用される KCK(Key Confirmation Key)，そして，実際にデータを送信する際の暗号化に使う TK(Temporary Key) の 3 つからなる．図 1 に 4way handshake の流れを示す．

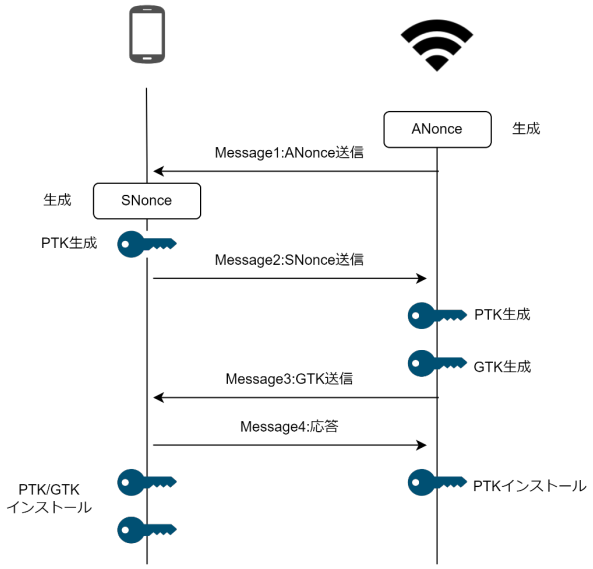

図 1　4way handshake

(1)メッセージ 1 でアクセスポイントはクライアントに ANonce を送信する．
(2)メッセージ 1 を受け取ったクライアントは SNonce と PTK を生成し，メッセージ 2 として SNonce を送信する．
(3)SNonce を受け取ったアクセスポイントは PTK と GTK を生成し，メッセージ 3 として GTK を KEK で暗号化して送信する．
(4)クライアントは KCK を使って GTK を復号した後，メッセージ 4 を送信し，4way handshake の完了を通知する．

このようにしてアクセスポイントとクライアントの接続が完了する．

2.3　WPA2-CCMP

WPA2 は標準では暗号化プロトコルとして AES(Advanced Encryption Standard) を用いた CCMP(Counter mode with CBC-MAC Protocol) を採用している．CCMP では暗号化したいデータを直接暗号化するのではなく，カウンターと呼ばれる一定の値を暗号化して，その結果とデータの XOR(排他的論理和) をとることで暗号文を生成する (図 2)．また，カウンターを AES で暗号化する際に用いられる暗号鍵が前節で述べた TK である．

WPA2 ではクライアントとアクセスポイントが接続するたびに 4way handshake が行われるため，同じ鍵が 2 度利用されることはない．この仕様を実現するため，多くのクライアントではアクセスポイントと切断されるたびに暗号鍵をクリアしている．

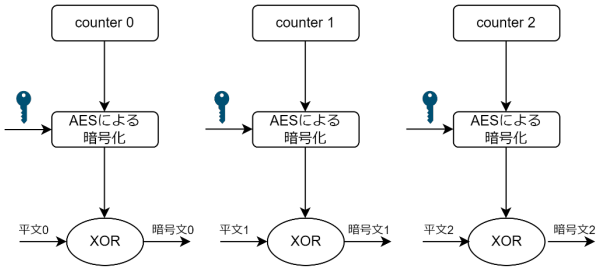

図 2　CCMP の暗号化処理

2.4　アクセスポイントとの切断

クライアント端末がアクセスポイントの電波が届く範囲の外に出たときや，ユーザが Wi-Fi をオフにした時など，アクセスポイントとクライアントが接続を切断する場合は，Management フレームと呼ばれるものの一種である Deauthentication フレームや Disassociation フレームなどが利用される．クライアントがこれらのフレームをアクセスポイントから受信した場合，切断に向けた処理に入る．処理の 1 つとして前節でも述べた暗号鍵のクリアがある．重要なことはこれらの切断フレームはセキュリティプロトコルとして WPA2 を採用している場合，認証及び暗号化が必須となっていない，ということである．したがって，切断フレームが認証及び暗号化されていない Wi-Fi 接続では，攻撃者はこれらのフレームを容易に偽造することができ，そのフレームをクライアントに向けて送信し続けることで，クライアントが Wi-Fi アクセスポイントに接続できないようにする DoS 攻撃を行うことができる．

3　Kr00k

本章では Kr00k の概要とその実現可能性について述べる．

3.1　Kr00k の概要

2020 年に一部の Wi-Fi チップの脆弱性を悪用し，通信内容を容易に復号することを可能とする Kr00k と呼ばれる攻撃が ESET によって発表された [1]．2.4 節で述べた通り，アクセスポイントがクライアントとの接続を切断するとき，アクセスポイントはクライアント宛てに特定のパケットを送信する．パケットを受け取ったクライアントは切断に向けた処理に入り暗号鍵のクリアを行う．ここまでは正常な動作である．しかし，一部の Wi-Fi チップでは暗号鍵をクリアし，すべて 0 の鍵がセットされた状態であったとしても，送信バッファにたまっているパケットをその鍵で暗号化した上で送信してしまう．

結果として，クライアントはアクセスポイントから切断される際に，送信バッファ内にあるパケットをすべて 0 の鍵で暗号化したうえで送信する．これが Kr00k で述べられている脆弱性であり，攻撃者はチャネルを盗聴することで容易に通信内容を復号することが可能である．攻撃者は任意のタイミングで切断フレームを送るだけでよく，また WPA2 では切断フレームの認証及び暗号化が

されていない場合が多いため，攻撃者はこれらのフレームを簡単に偽造することができ，Wi-Fi のパスワードを知っていなくとも容易に攻撃を行うことが可能である．

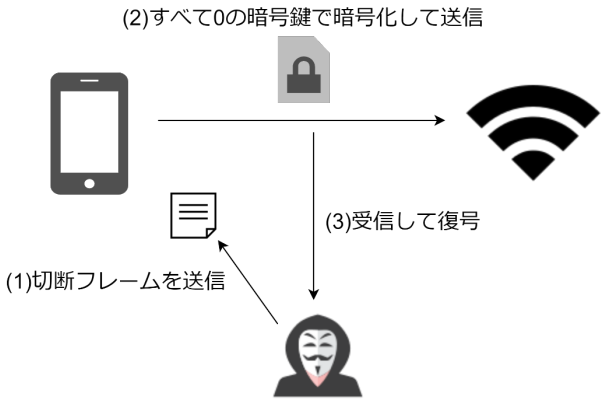

図 3　Kr00k の攻撃概要

Kr00k の攻撃概要を図 3 に示す．攻撃は以下の手順で行われる．

(1)攻撃者はクライアントに向けて Disassociation フレームを偽造して送信.
(2)クライアントは Wi-Fi から切断され，バッファに残ったパケットをすべて 0 の暗号鍵で暗号化して送信.
(3)攻撃者はクライアントが送信したパケットを受信し，復号.

3.2　実現可能性

まず，クライアントからアクセスポイントに向けて多くのパケットが連続的に送信されているような環境での Kr00k の実現可能性については，平均 2,3 個のパケットがすべて 0 の暗号鍵で暗号化されて送信されることがわかっている [3]．クライアントからアクセスポイントに向けて連続的にパケットが送信されている場合は図 4 に示すように，送信バッファにパケットがある程度たまっているような状態が一定時間存在し，そのタイミングで切断フレームを送信することで攻撃者はパケットを復号することが可能となる．

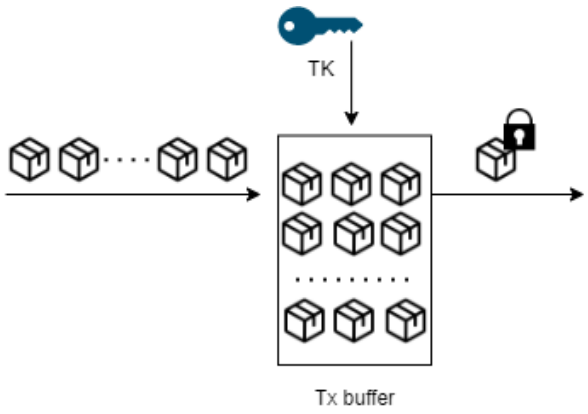

図 4　連続的にパケット送信している場合

しかし，より実環境に近い環境，例えばクライアントがネットサーフィンなどをしているような環境では攻撃が成功しないことがわかっている [3]．通常の通信時においてはクライアント側からアクセスポイント側に多くのパケットを送信する状況があまり多くなく，送信するパケットが存在しない時間というのが存在する．クライアントがアクセスポイントにパケットを連続的に送信していない場合，図 5 に示すように，送信バッファに入ったパケットは即座に通信路に流される．したがって，パケットがバッファ内にとどまっているような状態というのは一瞬の間しかなく，そのタイミングを狙って切断フレームを送信するのは現実的に不可能である．

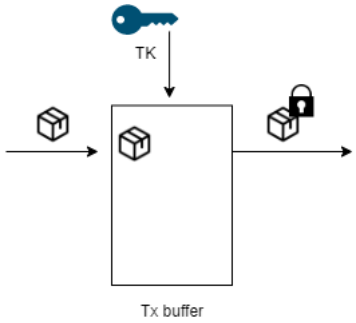

図 5　パケットを連続的に送信していない場合

以上のことから，実環境上での一般的な通信時に Kr00k を成功させるのは容易ではなく，実現可能性は極めて低い．

4　Kr00k を用いた新たな攻撃

3.2 節で述べた通り，実際の利用環境を想定した場合 Kr00k の実現可能性は非常に低いが，これはパケットがバッファにたまっている状態が極わずかな時間しかなく，そのタイミングで切断フレームを送信するのが非常に難易度の高いためであった．そこで，我々はクライアントのデータ送信を停止させる DoS 攻撃を Kr00k と組み合わせることを考えた．

4.1　Quiet

無線 LAN の規格である IEEE802.11(Institute of Electrical and Electronics Engineers) では，ルータやアクセスポイントなどのデバイスが 5GHz の電波帯域をレーダと共有することが許容されている．ここでのレーダとは気象観測・航空レーダなどのことである．レーダ信号は電波の干渉に対して脆弱であるため，アクセスポイントは 5GHz 帯域で動作している間，DFS(Dynamic Frequency Selection) によりレーダと干渉しないように周波数を自動的に変更する必要がある．

Quiet は通信に使用するチャネルがレーダなどと干渉を起こしてないか効率的に調査するため，データの送信を一時停止するようにアクセスポイントがクライアントに命じる信号である．Quiet はビーコンなどのいくつかのパケットに追加可能であり，ビーコンの場合にはオプション領域追加され，暗号化や改ざん検知は行われない．Quiet のフォーマットを図 6 に示す．

- Tag ID はオプション情報を識別するための ID であり，Quiet では 40 になる．

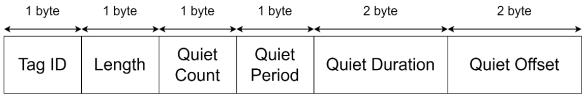

図 6　Quiet のフォーマット

- Length は Quiet の情報が入っている部分の長さであり，6 となる．
- Quiet Count は送信停止期間が始まるまでのビーコンの数を表している．なお，Quiet Count において 0 は予約されていて使えない．
- Quiet Period は送信停止期間が定期的かどうかを示している．0 がセットされている場合は以降，送信停止期間がないことを表し，0 以外の値がセットされている場合は 2 つの送信停止期間の間のビーコンの数を表している．
- Quiet Duration は送信停止期間の長さを単位 TU で表している．1[TU] が 1024[μs] であることと，領域が 2 バイト，つまり 0〜65535 が表現可能であることから，最大でおよそ 67 秒間クライアントがデータを送信するのを停止させることができる．
- Quiet Offset はビーコンを受信してから送信停止期間が始まるまでの長さを単位 TU で表している．

各要素の関係を表すと図 7 のようになる．

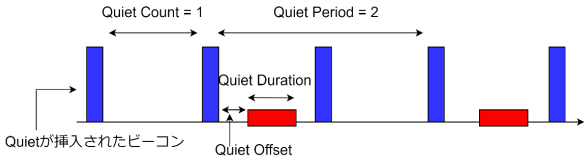

図 7　Quiet の各要素の関係

先に述べたように Quiet は 5GHz 帯で動作するアクセスポイントが使用しているチャネル上でレーダと干渉を起こしていないかを効率的に調べるために利用されるが，一部のクライアント端末では 2.4GHz 帯を使用していたとしても，Quiet が挿入されたビーコンを受信した際，データの送信を停止することが分かっている．また，Quiet を利用した DoS 攻撃である Quiet attack も提案されている [4].

4.2　Quiet attack と Kr00k を組み合わせる

Kr00k によりクライアントが送信したデータを復号するためには，クライアントデバイスの送信バッファにパケットがある程度たまっている状態で，切断フレームをクライアント宛てに送信しなければならない．しかし，通常の通信時 (例えばクライアントがネットサーフィンを行っている場合) にはバッファにパケットがたまっているタイミングでクライアントをアクセスポイントから切断させるのは非常に難しく，Kr00k の実現可能性は非常に低い [3]．そこで，我々は 4.1 節で述べた Quiet を利用した Quiet attack を Kr00k と組み合わせることで，通常の通信時でもクライアントが送信するデータを容易に復号できるような新たな攻撃法を提案する．攻撃の流れとしては次のようになる．

(1)攻撃者は攻撃対象のクライアントデバイスが接続しているアクセスポイントのビーコンをキャプチャする．
(2)キャプチャしたビーコンのオプション領域に Quiet を挿入し，さらに宛先をクライアントデバイスに書き換えて送信する (図 8).
(3)Quiet が挿入されたビーコンを受信したクライアントは Quiet Duration に記載されている時間だけデータ送信を停止しなければならないため，この間に送信しようとしたパケットは送信バッファにたまる (図 9).
(4)攻撃者は切断フレームを送ることでクライアントに送信バッファ内のパケットをすべて 0 の暗号鍵で暗号化させたうえで送信させ，それらのパケットを受信して復号する (図 10).

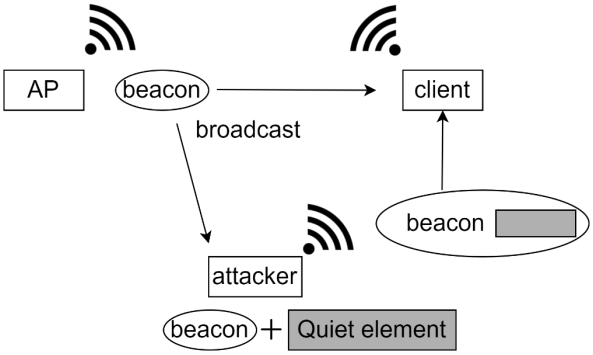

図 8　Quiet を挿入

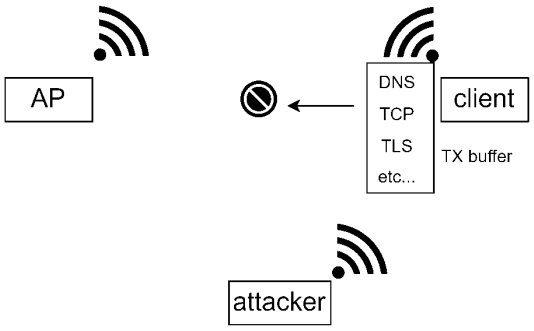

図 9　クライアントがデータの送信停止

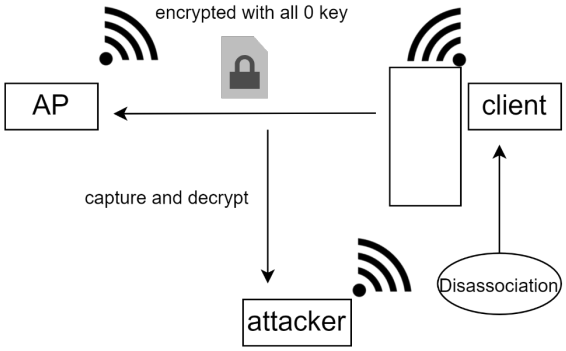

図 10　すべて 0 の暗号鍵で暗号化して送信

このようにすることで，攻撃者は通常の通信時であってもクライアントが送信するデータを容易に復号することが可能である．

5 攻撃の評価

我々は 4.2 節で述べた新たな攻撃法について，実環境上での影響を評価するために，攻撃を実装したうえで実験を行った．

5.1 実験方法

実験で使用した機器を以下に示す．

表 1 実験に使用した機器

攻撃者	Kali Linux(VMware) Wi-Fi アダプタ
アクセスポイント	BUFFALO WAPS-1266
クライアント	nexus5(Android versin:6.0.1)

また，アクセスポイントの無線モードとしては 802.11g とした．以下に攻撃した際の Quiet の各パラメータの値を示す．() 内は 16 進数表記である．

表 2 Quiet の各パラメータの値

Quiet Count	1(0x01)
Quiet Period	0(0x00)
Quiet Duration	10000(0x2710)
Quiet Offset	0(0x0000)

クライアントの動作としては Web ブラウザを使用し，Web ページ内にあるリンクを順に 10 回たどっていくようにした．ただし，Web ページ内のリンクを押すタイミングは攻撃者が Quiet を挿入したビーコンを送信した直後とした．攻撃者は VMware で立ち上げた Kali Linux であり，偽造したビーコン，切断フレームを送信するために USB 接続の Wi-Fi アダプタを接続した．また，パケットキャプチャツールである Wireshark を立ち上げ，[Edit]→[Preferences]→[Protocols]→[IEEE 802.11] で暗号鍵としてすべて 0 の鍵 (TK) を設定し，クライアントが送信するパケットを復号できるようにした．

評価方法としては 10 回のアクセスのうち，何回宛先情報を含んだパケットを復号できるかをカウントした．宛先情報とは IP アドレスやドメイン名のことであり，言い換えると，10 回のアクセスの内で何回 TCP パケットや DNS パケットを復号できたかということである．注意点としては，1 回のアクセスでクライアントが送信するパケットのうち，できるだけ多くを復号するというのが目的ではない．1 回のアクセスにつき 1 つでも宛先情報を含んだパケットを復号できればカウントする．

5.2 実験結果

本実験は Web ブラウザとして Chrome を使用した．

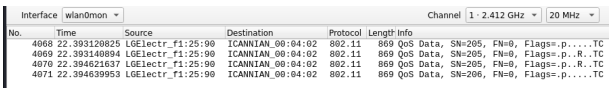

図 11 キャプチャしたパケットの例

表 3 実験結果 1

Chrome	復号
1 回目	×
2 回目	成功
3 回目	成功
4 回目	×
5 回目	×
6 回目	×
7 回目	×
8 回目	成功
9 回目	×
10 回目	×

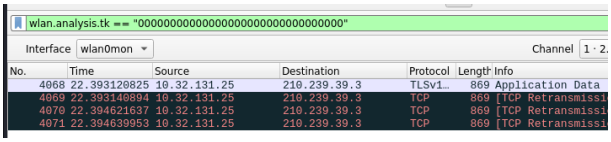

図 12 復号したパケットの例

表 3 から分かる通り，パケットの復号に成功した回数は非常に少なかった．また，攻撃者が切断フレームをクライアント宛てに送信しても，クライアントは Wi-Fi 接続を即座に切断しなかった．図 11 はクライアントが送信したパケットを Wireshark でキャプチャした時の画像で，図 12 はキャプチャしたパケットを Wireshark の機能で復号した時の画像である．復号前は送信元，送信先ともに MAC アドレスとなっており，これらは LAN 内の機器のアドレスであるため，クライアントがどこの Web ページにアクセスしているかはわからない．しかし，復号することで，ペイロード部分が解読可能な形となり，宛先情報が IP アドレスとして取得可能となった．

5.2.1 切断フレームと確認応答

パケットの復号に成功した回数が少なかったのは，攻撃者が切断フレームを送信してもクライアントが Wi-Fi から即座に切断されなかったことが原因であると考えられる．そこで，クライアントが即座に切断されなかった理由について考える．切断フレームを受信したクライアントデバイスは送信元に確認応答を返す必要がある．しかし，クライアントは切断フレームを受信する前に Quiet が挿入されたビーコンを受信しており，データの送信が一時的に禁止されている状態である．そのため，クライアントは確認応答を返すことができず，切断フレームを受信しても即座に Wi-Fi から切断されなかったのだと考えることができる．

また，実験で用いた android 端末は Quiet が挿入されたビーコンを受信し，一定時間データの送信ができない状態となると Wi-Fi から自動的に切断されてしまうことがあった．すなわち，攻撃者が送信した切断フレームによってではなく，クライアントデバイスが自らアクセスポイントとの接続を切ってしまうがために，復号に成功する回数が非常に少ない結果となってしまったと考えられる．そこで，次項では切断フレームを送るタイミングを見直した攻撃法について述べる．

5.2.2 切断フレームの送るタイミング変更

これまでに述べた攻撃法では攻撃者が切断フレームを送信してもクライアントが Wi-Fi 接続を即座に切らな

いため，パケットを復号できる回数が非常に少ないといった問題があった．そこで，本項では切断フレームを送信するタイミグを変更した場合の結果について述べる．変更点としては，攻撃者は Quiet が挿入されたビーコンを送信してから一定時間待ったのち，切断フレームを送信するのではなく，ビーコンを送信してから Quiet Duration に設定した時間だけ待機した後，切断フレームを送信するというものである．このようにすることで，クライアントはデータの送信が一時的に停止されている期間の後に切断フレームを受信することになるため，確認応答を返すことができ，Wi-Fi 接続を即座に切ることになる．結果を以下に示す．

表 4　実験結果 2

Chrome	復号
1 回目	成功
2 回目	×
3 回目	成功
4 回目	成功
5 回目	×
6 回目	×
7 回目	×
8 回目	×
9 回目	成功
10 回目	×

切断フレームを送るタイミングを変更しても，変更前と復号できる回数はほとんど同じであった．原因としては次のようなことが考えられる．

- 切断フレームを送る前に android 端末の仕様により Wi-Fi 接続が自動で切れる．
- 切断フレーム受信するタイミングと送信停止期間が終わるタイミングに差があり，その間にバッファ内のパケットを正規の暗号鍵で暗号化した上で送信する．

5.2.3　ブラウザ上でのエラーメッセージ

今回の攻撃は Quiet が挿入されたビーコンをクライアントに送信し，送信停止期間中にクライアントが送信しようとするパケットを送信バッファにためさせた状態で切断フレームを送り，すべて 0 の暗号鍵で暗号化させて送信させる，というものであった．したがって，クライアント側から見ると，ある Web ページのリンクを押した際に，すぐにそのページに遷移するのではなく，何秒かローディング状態が続くことになる．さらに，その後攻撃者によって切断フレームが送られてくるが，その切断フレームがユニキャスト通信であった場合，ブラウザ上でネットワーク接続エラーが毎回表示された (図 13)．そのため，攻撃が利用者に検出されやすく，実用的な攻撃であるとは言えない．そこで，我々はブラウザ上でエラーが表示されないようにする方法はないか模索し，切断フレームをユニキャストではなく，ブロードキャストするという結論に至った．さらに，攻撃の流れについても一部変更を加えた．新しい攻撃の流れは以下のとおり

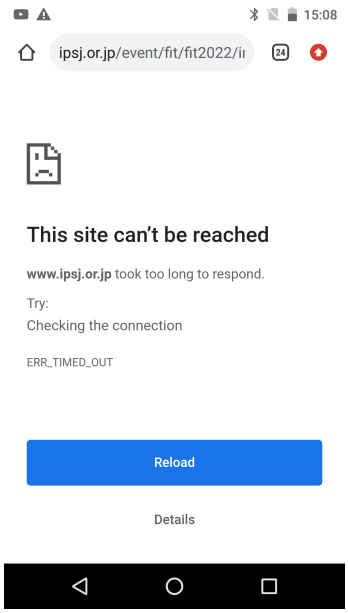

図 13　エラーメッセージ

である．

(1)攻撃者は攻撃対象のクライアントデバイスが接続しているアクセスポイントのビーコンをキャプチャする．

(2)キャプチャしたビーコンのオプション領域に Quiet を挿入し，さらに宛先をクライアントデバイスに書き換えて送信する．

(3)Quiet が挿入されたビーコンを受信したクライアントは Quiet Duration に記載されている時間だけデータ送信を停止しなければならないため，この間に送信しようとしたデータは送信バッファにたまる．

(4)攻撃者は Quiet を挿入したビーコンをクライアント宛てに送信してから一定時間待ったのち，切断フレームをブロードキャストする (変更) ことでクライアントに送信バッファ内のパケットをすべて 0 の暗号鍵で暗号化させたうえで送信させる．

(5)(追加) 攻撃者はクライアント宛てに切断フレームを送信する．

変更点は切断フレームをブロードキャストする点と，攻撃を行った後に再度切断フレームを送信する点である．(5) で切断フレームを送らずに，再び攻撃を行うと高い確率でブラウザ上でエラーメッセージが表示されてしまう．しかし，(5) で切断フレームを送信し，クライアントの Wi-Fi 接続を一度切断してから再び攻撃を行うことでエラーが表示される確率を下げることができた．

結果を表 5,6,7 に示す．ここで，エラーメッセージの表示はブラウザの仕様によるものであるため，Chrome だけでなく Edge や Firefox についても同様の実験を行った．エラー列において ✓ はエラーが表示されなかったことを，× はエラーが表示されたことを示す．

切断フレームをブロードキャストした場合，ブラウザ上でエラーが表示された回数はブラウザの種類に関係なく，ユニキャスト時に比べかなり少なくなった．さらに，復号が可能であった回数についても，切断フレームをユニキャストした場合によりもブロードキャストした場合のほうが多かった．

表 5　Chrome

	復号	エラー
1 回目	×	×
2 回目	成功	✓
3 回目	成功	✓
4 回目	成功	✓
5 回目	成功	×
6 回目	×	✓
7 回目	成功	✓
8 回目	×	✓
9 回目	成功	✓
10 回目	×	✓

表 6　Edge

	復号	エラー
1 回目	×	✓
2 回目	成功	✓
3 回目	成功	✓
4 回目	成功	✓
5 回目	×	✓
6 回目	成功	✓
7 回目	成功	✓
8 回目	成功	✓
9 回目	成功	×
10 回目	×	×

表 7　Firefox

	復号	エラー
1 回目	×	×
2 回目	成功	✓
3 回目	×	×
4 回目	成功	✓
5 回目	成功	✓
6 回目	×	✓
7 回目	成功	✓
8 回目	成功	✓
9 回目	成功	×
10 回目	×	×

5.3　考察

本章では実験結果の考察と提案する攻撃の対策法について述べる．

5.3.1　現実的脅威

切断フレームをブロードキャストする攻撃法の現実的脅威について述べる．ブロードキャストされた切断フレームを受信したクライアントは確認応答を送信元に返す必要がなく，受信したタイミングで即座に Wi-Fi 接続を切る．その後，アクセスポイントとの再接続のための処理に入る．この際，ブラウザではエラーが表示される確率は低く，利用者は攻撃の検出が困難であると考えられる．ここで，切断フレームをブロードキャストするためアクセスポイントに接続している攻撃対象のクライアントデバイス以外の端末も切断されてしまうが，すぐに再接続が完了するため，やはり攻撃が検出される可能性は低いと考えらる．また，攻撃者によって復号されるパケットには DNS や TCP パケットが含まれており，DNS で問い合わせているドメイン名や TCP パケットの宛先 IP アドレスを見ることで，クライアントのアクセス先の情報を得ることができ，現実的脅威のある攻撃であると言える．

5.3.2　対策法

まず，ユーザができる対策法として以下のようなことが挙げられる．

- Kr00k に対するパッチを適用する．
- Wi-Fi 暗号方式を WPA3 に変更する．
- WPA2 において PMF(Protected Management Frames) を有効にする．

Kr00k に対するパッチを適用するのがユーザが行える対策として一番重要なことである．また，本攻撃は攻撃者が偽造した切断フレームをクライアントが正規のアクセスポイントからのものであると誤認し，実際に Wi-Fi 接続を切断してしまうことを利用している．暗号方式を WPA3 に変更，WPA2 において PMF を有効にすることで切断フレームは暗号化及び認証されるようになる．したがって，攻撃者が切断フレームを偽造することが不可能となり，攻撃を防ぐことができるようになる．

パケットの復号とまではいかなくても，Quiet を用いることでクライアントの通信を停止させる DoS 攻撃が可能である．この DoS 攻撃は最新の iOS 搭載の iPhone に対しても有効であった．本来 Quiet は 5GHz 帯において，アクセスポイントの使用するチャネルが衛星などの他の電波と干渉していないかを効率的に調査するために用いられるものであり，2.4GHz 帯では不要のはずである．したがって，メーカーができる対策法としては 2.4GHz 帯において Quiet を無効にするということが挙げられる．

6　むすび

本論文では始めに，WPA2 の脆弱性を利用した攻撃である Kr00k についてその概要と実環境上での影響について述べた．次に，Kr00k を利用した新たな攻撃法の提案とその効果について述べた．まず，Quiet を用いてクライアントのデータ送信を停止させた後，クライアント宛てに切断フレームを送ったところ，ブラウザ上でネットワークの接続エラーが表示され，さらにパケットを復

号できる回数も少なかった．そこで，切断フレームをブロードキャストしたところ，ブラウザがエラーを表示する回数が減り，パケットを復号できる回数については増えた．そして復号したパケットからクライアントがアクセスしているサイトの情報を取得することができた．また，切断フレームをブロードキャストしたとしても他のクライアントについては，パケットを送受信している場合でない限り，エラーは表示されず，攻撃の検出は困難であると考えられる．以上より，本攻撃は実環境においてもクライアントが送信するパケットを容易に復号することを可能とするため，現実的脅威のある攻撃であると言える．

謝辞

本研究は，総務省の「電波資源拡大のための研究開発 (JPJ000254)」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の成果の一部である．また，本研究の一部は JSPS 科研費 20K11810 の助成を受けたものである．

参考文献

[1] Miloš Čermák，Štefan Svorenčík，Róbert Lipovský：”KR00K-CVE-2019-15126:SERIOUS VULNERABILITY DEEP INSIDE YOUR WI-FI ENCRYPTION”.
https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[2] 窪田恵人，五十部孝典，森井昌克：”無線 LAN 機器に対する DoS 攻撃の実装と評価”，コンピュータセキュリティシンポジウム 2019 論文集，pp.1079-1085(2019)

[3] 窪田恵人，白石善明，森井昌克：”実環境を想定した Kr00k の評価実験とその改良案”，コンピュータセキュリティシンポジウム 2020 論文集，pp.820-825(2020)

[4] Bastian Könings，Florian Schaub，Frank Kargl，Stefan Dietzel：”Channel Switch and Quiet attack: New DoS attacks exploiting the 802.11 standard”，2009 IEEE 34th Conference on Local Computer Networks，(2009)

[5] Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse.
https://www.krackattacks.com/

[6] DRAGONBLOOD: Analysing WPA3’s Dragonfly Handshake.
https://wpa3.mathyvanhoef.com/

[7] 802.11 Wireless Networks: The Definitive Guide, 2nd Edition by Matthew S. Gast.
https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html