Cisco DNA Center ランダム化 MAC アドレスに関する Q&A

改訂：2022 年 3 月 29 日

MAC ランダム化

モバイル エンドポイント デバイスへのランダム MAC アドレスの割り当ては新しいものではありませんが、MAC ランダム化の使用方法は時間の経過とともに変化してきました。当初、デバイスはMAC ランダム化を利用して既知のワイヤレスネットワークをプローブしていました。プローブ要求フレームで、デバイスは、一定のプライバシーを確保するため、MAC アドレスをランダム化して実際の MAC アドレスを隠していました。時間の経過とともに、デバイスは、ランダム MAC アドレスを使用してワイヤレスネットワークと連動するようになりました。現在、このランダム化は、エンドポイントデバイスまたはエンドポイントデバイスの背後のユーザーを一意に識別するためにMAC アドレスに依存するネットワーク要素に問題を引き起こしています。各ハードウェアベンダーは導入プロセスで固有のアルゴリズムを使用するため、MAC ランダム化はデバイスごとに異なる方法で導入されます。続くセクション（「Microsoft Windows 10」ー「Apple iOS 14」）では、各モバイル オペレーティング システムに MAC ランダム化がどのように組み込まれるかについて説明します。

Microsoft Windows 10

次の箇条書きには、MAC ランダム化と Microsoft Windows 10 に関する重要な詳細情報が記載されています。

- ランダム化は、すべてのワイヤレス接続に対してグローバルに、またはサービスセット識別子（SSID）とも呼ばれるネットワークプロファイルごとに設定できます。
- ランダム化は、工場出荷時のプリセットにより、デフォルトで無効になっています。
- ネットワークプロファイルでは、毎日異なるランダム MAC アドレスを生成するように Windows 10 を設定できます。
- ランダム MAC アドレスが特定のネットワークプロファイルに使用されると、そのアドレスはネットワークプロファイルを削除しない限り保持されます。
- ネットワークプロファイルを削除すると、次回ネットワークに接続したときに別のランダム MAC アドレスが生成されます。
- Microsoft Windows 10 での MAC ランダム化と設定の詳細については、こちらをクリックしてください。

Google Android 10/11

次の箇条書きには、MAC ランダム化と Google Android 10/11 に関する重要な詳細情報が記載されています。

- ランダム化は、SSID とも呼ばれるネットワークプロファイルごとに設定できます。
- ランダム化は、工場出荷時のプリセットにより、クライアントモード、SoftAp、および Wi-Fi Direct に対してデフォルトで有効になっています。
- ランダム MAC アドレスが特定のネットワークプロファイルに使用されると、そのネットワークプロファイルを削除して再作成した後も、デバイスは同じランダム MAC アドレスを使用し続けます。

- Google Android 10/11 での MAC ランダム化と設定の詳細については、こちらをクリックしてください。

Apple iOS 14、iPadOS 14、watchOS7

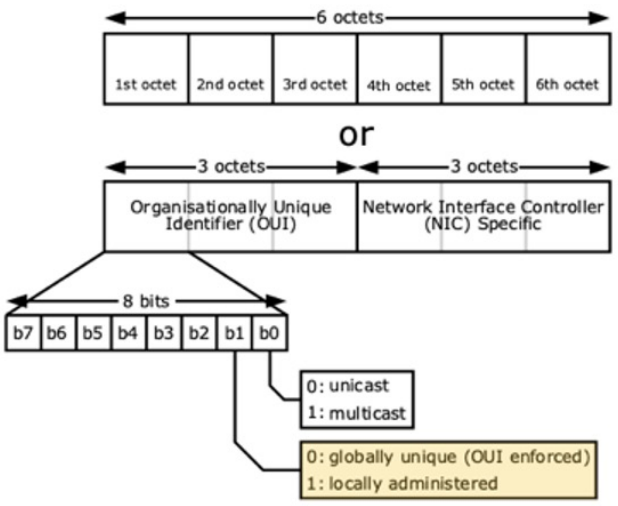
次の箇条書きには、MAC ランダム化と Apple iOS 14、iPadOS 14、および watchOS7 に関する重要な詳細情報が記載されています。

- ランダム化は、SSID とも呼ばれるネットワークプロファイルごとに設定できます。
- ランダム化は、工場出荷時のプリセットにより、デフォルトで有効になっています。
- 以前の iOS バージョンでは、iOS 14 に更新すると、既存の SSID の MAC ランダム化が有効になります。
- ランダム MAC アドレスが特定のネットワークプロファイルに使用されると、そのネットワークプロファイルを削除して再作成した後も、デバイスは同じランダム MAC アドレスを使用し続けます。
- Apple iOS 14、iPadOS 14、および watchOS7 での MAC ランダム化と設定の詳細については、こちらをクリックしてください。

MAC ランダム化の動作

この MAC ランダム化の生成は、IEEE によって設定されたルールに従って実行されます。次の図は、IEEE のルールを理解するための基礎的な情報を示しています。図 1 に、MAC アドレスの 48 ビット構造が示されています。さらに、この図では、MAC アドレスがユニキャストかマルチキャストかを b0 ビットで識別し、MAC アドレスがグローバルに管理されているか、それともローカルに管理されているかを b1 ビットで識別する方式が示されています。MAC アドレスをランダム MAC アドレスと見なすには、MAC アドレスをローカルに管理し（b1 ビットを 1 に設定）、ユニキャストアドレスにする必要があります（b0 ビットを 0 に設定）。

図 *1 : MAC* アドレスの構成要素



By Inductiveload, modified/corrected by Kju - SVG drawing based on PNG uploaded by User:Vtraveller. This can be found on Wikipedia here., CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=1852032

図 1 に、MAC アドレスの構成要素を示します。コンポーネントには、オクテット、ビット、OUI、NIC が含まれます。b1 ビットは、MAC アドレスがグローバルに管理されるか、それともローカルに管理されるかを決定し、b0 ビットは、MAC アドレスがユニキャストアドレスかマルチキャストアドレスかを決定します。

IEEE によると、ランダム MAC アドレスとして判定されるには、最初のオクテット（16 進表記）が 2、6、A、または E で終わる必要があります。たとえば、32:8c:27:26:72:34 の第 1 オクテットの 2 は、これがランダム MAC アドレスであることを示しています。

次の箇条書きには、MAC ランダム化がクライアントデバイスに及ぼす影響を明確に示す情報が記載されています。

- エンドユーザーデバイスの場合、SSID ごとに MAC アドレスが保持されます。クライアントデバイスが SSID に初めて参加すると、新しいランダム MAC アドレスが生成されます。クライアントが同じ SSID に再参加すると、クライアントは以前と同じ MAC アドレスを割り当てられます。
- クライアントデバイスがネットワークを削除して SSID をクリアした後、同じ SSID に再参加すると、クライアントは同じ MAC アドレスを割り当てられます。
- クライアントデバイスには、最大でネットワーク内の SSID の数に等しい数の MAC アドレスを指定できます。
- MAC アドレスの重複は可能です。
- 2 つの異なるクライアントに同じ MAC アドレスを割り当てることができます。この動作はデバイス側で処理されますが、まれに重複する MAC アドレスが割り当てられる場合があります。

ブリッジ型ネットワークについての一般的な考慮事項

ブリッジ型ネットワーク（レイヤ 2）では、特定の VLAN に対して MAC アドレスが一意の識別子として使用され、この同じ MAC アドレスが異なる VLAN に存在することがあります。レイヤ 2 ネットワークは MAC アドレスの複製では動作できないため、ネットワークデバイスとコントローラは複製を管理する必要があります。

一般的なネットワークでは、制御ノードが MAC アドレス重複検出の役割をファーストホップセキュリティ（FHS）機能に委任できます。この事後対応策は、MAC アドレス攻撃者のアクセスを検知して阻止するために役立ちます。

レイヤ 2 ネットワークは、同じ事後対応策を使用してランダム MAC アドレスの重複を処理します。

レイヤ 2 ネットワークがランダム MAC アドレスの重複動作とその影響を処理する方法については、次の例を参照してください。

1. クライアントでランダム MAC アドレスを有効または無効にすると、SSID は変更されず、クライアントによって MAC アドレスが変更されます（ユニバーサル <> ランダム）。

   この場合、古いクライアントがネットワークを離れて、新しいクライアントが参加するかのように処理されます。古いクライアントは、通常のエージングの対象となります。またはプローブ応答の検出および削除の対象となりません。新しいクライアントでは、通常のオンボーディングプロセスが実行されます。

2. モビリティイベントでは、クライアントがネットワークを移動するときの SSID は同じです。

   このケースは、通常のモビリティとして管理されます。

3. ランダムアドレスの重複がある場合、ランダム MAC アドレスの重複が発生している可能性があります。次の箇条書きは、重複する可能性のある事項について説明しています。

   - 同じ VLAN 上の同じ SSID、または同じ VLAN への異なる SSID マッピング
   - 同じワイヤレス LAN コントローラ、または異なるワイヤレス LAN コントローラ
   - 同じノード、または異なるアクセスノード

Cisco スイッチへの影響

この挙動はワイヤレスクライアントで確認されるため、影響分析はワイヤレスクライアントに焦点を合わせています。有線クライアントの場合、MAC アドレスの重複は、Cisco FHS のコンポーネントであるスイッチ統合セキュリティ機能（SISF）によって管理されます。

クライアント オンボーディング

ワイヤレスインフラストラクチャは、MAC アドレスに基づいてワイヤレスクライアントを識別し、一意の識別子として扱います。MAC アドレスが変更されると、クライアントは新しいクライアントと見なされます。

クライアントは、許可/認証フェーズを経て IP アドレスを取得し、次にネイバー探索を実行します。その後、ネットワークでの通信が可能になります。

認証/許可

クライアントはアクセスポイント（AP）を介してネットワークに接続し、APはクライアントへのアクセスを許可する前にコントローラと通信します。ランダムアドレスやユニバーサルアドレスは、同じプロセスを通過します。

Q&A

ランダム MAC アドレスを使用したクライアントの認証にどのような影響がありますか。

一意の MAC アドレスはそれぞれ異なるクライアントとして管理されるため、影響はありません。

MAC アドレスの重複は可能ですか。

まれなケースですが、重複する MAC アドレスが表示されることがあります。

MAC アドレスの重複が発生するとどうなりますか。

MACアドレスの重複が同じコントローラまたはネットワークアクセスノードで発生した場合、クライアントはネットワークを離脱して再参加するかのように扱われます。MACアドレスの重複が別のコントローラまたはネットワークアクセスノードで発生した場合、クライアントはモビリティイベントとして扱われます。現時点では、コントローラによって MAC アドレスの重複は管理されません。

IP アドレスの取得

クライアントには、DHCP サーバーによって割り当てられた IP アドレス、静的 IP アドレス、または自動設定された IP アドレスを割り当てることができます。次の IP アドレスは、MAC ランダム化の影響を受けます。

- DHCP サーバーによって割り当てられた IP アドレスと自動設定された IP アドレスの場合、MAC アドレスが変更されると IP アドレスも変更されます。この変更は、それぞれのアドレスが別のクライアントであるかのように管理されます。そのため、ネイバー探索は IP アドレスが割り当てられた後に行われます。
- 静的 IP アドレスの場合、MAC アドレスが変更されても、同じ IP アドレスがネットワークインターフェイスで使用されると、ネイバー探索キャッシュが更新されるまでの間、トラフィックが影響を受けます。

Q&A

MAC ランダム化は DHCP プールにどのように影響しますか。

一意の MAC アドレスは、それぞれ異なるクライアントとして管理されます。各々の SSID が異なる DHCP プールを使用している場合、影響はありません。SSID が同じ DHCP プールを使用している場合、古い MAC アドレスに割り当てられた IP アドレスのリースが期限切れになるまでの間、一時的な影響があります。

MAC ランダム化は自動設定されたアドレスにどのように影響しますか。

新しい MAC アドレスは別のクライアントとして管理されます。古い IP アドレスをキャッシュしている転送関連テーブルがエージングメカニズムによって削除されるまでの間、スイッチに影響が及びます。

MAC ランダム化は、静的 IP アドレスを割り当てられたクライアントにどのように影響しますか。

クライアントが MAC アドレスを変更した後も同じ IP アドレスを使用し続けると、Address Resolution Protocol（ARP）キャッシュが更新されるまで、トラフィックが中断されることが予想されます。

ネイバー探索

ネットワークデバイスがレイヤ 3 で通信する場合、ネットワーク内のデバイスは、ARP などのネイバー探索プロトコル（NDP）を使用して、宛先 MAC アドレスへのネクストホップを検出します。

Q&A

MAC ランダム化は NDP と ARP にどのように影響しますか。

MAC アドレスが変更されるため、ネイバーデバイスは、MAC アドレスが変更された後に ARP キャッシュと NDP キャッシュを更新する必要があります。更新しないと、この情報に依存するトラフィックが中断されます。

Cisco DNA Center への影響

保証

Wireless Clients 360

- アシュアランスは、MAC アドレスに基づいてワイヤレスクライアントを識別し、一意の識別子として扱います。MAC アドレスが変更されると、クライアントは新しいクライアントと見なされます。異なる MAC アドレスベースのクライアント履歴は、同じユーザーデバイスの場合でもマージされません。ユーザーデバイスは、個々の MAC アドレスを検索して詳細とメトリックを取得する必要があります。
- アシュアランスでは、同時使用クライアント数は最新のテレメトリデータに基づいて計算されます。ランダム MAC アドレスが有効になっているクライアントが別の SSID に参加すると、5 分間で、その SSID の重複クライアントが作成され、クライアント数が増加します。次の 5 分間で、新しいテレメトリデータに基づいてクライアント数が修正されます。
- イベントビューアとメトリックは MAC アドレスに限定されます。

Q&A

MAC ランダム化は、一意のクライアントの数やクライアント総数にどのように影響しますか。

クライアントがネットワークに参加した SSID の数に基づいて、履歴中のクライアント数が増加します。

MAC アドレスの重複は可能ですか。

まれなケースですが、重複する MAC アドレスが表示されることがあります。

クライアントがドロップアウトしていないのに、[Client 360] のウィンドウにギャップがあるのはなぜですか。

デバイスが別の SSID に参加して MAC アドレスを変更した場合、新しい MAC アドレスに応じてデータがプロットされることはありません。同じデバイスが同じ SSID に再参加して古い MAC アドレスを取得すると、データがプロットされます。そのため、ギャップが生じることが予想されます。他の MAC アドレスの [Client 360] ウィンドウに移動して、該当するデータを表示できます。

ネットワークに重複する MAC アドレスがある場合、MAC ランダム化は Cisco DNA Center にどのように影響しますか。

Cisco DNA Center は、予期しない動作と不正確なメトリックを示します。

イベントビューアにどのように影響しますか。

クライアントが SSID を変更すると、イベントビューアが別の MAC アドレスのイベントをキャプチャすることはできなくなります。イベント履歴を表示するには、MAC アドレスに基づいてそれぞれのクライアントに移動します。

すべてのイベントと他のメトリックを 1 つの場所に表示できますか。

特定のイベントや他の重要なパフォーマンスインジケータを表示するには、それぞれの MAC アドレスに移動する必要があります。

アプリケーション エクスペリエンス

全般的なアプリケーション エクスペリエンスは MAC ランダム化の影響を受けませんが、クライアントベースおよびユーザーベースのアプリケーションメトリックは MAC アドレスに限定されます。

Q&A

MAC ランダム化はアプリケーション エクスペリエンスにどのように影響しますか。

[Overall Application Experience] トレンドウィンドウでは、クライアントの使用状況は、デバイスの MAC アドレスの数に基づいて分割されます。

単一のユーザーデバイスに関して、集約された使用状況またはスループットメトリックを表示できますか。

集約された使用状況またはスループットメトリック情報を直接表示する方法はありません。ただし、ユーザーのすべての MAC アドレスを把握している場合は、各 MAC アドレスの個々のアプリケーションメトリックを取得して追加できます。

ヘルス スコア

MAC ランダム化は正常性スコアに影響しません。

Q&A

MAC ランダム化はクライアントの正常性スコアに影響しますか。

クライアントの正常性スコアには影響しません。クライアントが別の MAC アドレスでネットワークに参加すると、ユーザーは新しいクライアントとして扱われ、そのユーザーセッションの正常性スコアが計算されます。

グローバル検索

MAC ランダム化が有効になっているクライアントが複数の SSID に参加している場合、ユーザーまたはデバイス名のグローバル検索を実行すると、多数のクライアントデバイスが表示されることがあります。

Q&A

特定のデバイスホスト名を検索すると、多数のデバイスエントリが表示されるのはなぜですか。

あるデバイスで MAC ランダム化が有効になっているときに、そのデバイスが複数の SSID に参加すると、Cisco DNA Center は複数の一意のクライアントエントリを収集します。検索結果には、MAC アドレスに基づくすべてのクライアントエントリが表示されます。

ユーザー検索に問題がありますか。

ユーザー検索はMACランダム化の影響を受けません。検索では、関連するすべてのデバイスエントリが引き続き表示されます。クライアントが異なるSSIDに参加すると、さらに多くのデバイスが表示されます。

インテリジェントキャプチャ

クライアントキャプチャはMACアドレスに基づいてスケジュールされます。クライアントがMACアドレスを変更すると、そのイベントはクライアントの切断として扱われ、パケットキャプチャは停止します。

Q&A

MACランダム化は、既存のスケジュールのクライアントキャプチャに影響しますか。

クライアントがiOS 14にアップグレードされる前にクライアントキャプチャがスケジュールされている場合、MAC IDは絶対的な値です。既存のスケジュールを削除し、現在のMACアドレスで新しいスケジュールを再作成する必要があります。

クライアントがSSIDを変更した場合、この変更はクライアントキャプチャに影響しますか。

影響します。クライアントが別のSSIDに切り替えられると、クライアントキャプチャが停止します。

MACランダム化は、クライアントキャプチャをスケジュールできるデバイスの規模または数に影響しますか。

Cisco DNA Centerでは、部分キャプチャの場合は16のMACアドレス、完全キャプチャの場合は1つのMACアドレスに制限されています。クライアントが複数のSSIDに参加した場合、同じデバイスに複数のMACアドレスが存在することになります。単一ユーザーに対して、複数のクライアントキャプチャをスケジュールする必要があるかもしれません。この状況では、異なるユーザーに対して同時に複数のキャプチャをスケジュールすることが制限されます。

AIネットワーク分析

次の箇条書きは、MACランダム化がAIネットワーク分析に与える影響を示しています。対象となるのは、ネットワークヒートマップ、サイト比較、およびAI問題の発生です。

- ネットワークヒートマップの場合、クライアント数がMACアドレスに基づいて大きな数値になります。
- サイトの比較の場合、影響はありません。
- AI問題の発生の場合、SSIDレベルで集約されます。集約されない場合、影響はありません。

Wi-Fi 6

クライアントが異なるSSID間を移動した場合、クライアント機能数が最大5分間増加します。次の5分間に、ワイヤレスLANコントローラから取得された更新済みのテレメトリデータに基づいて数が修正されます。

Q&A

MACランダム化はWi-Fi 6の履歴メトリックに影響しますか。

Cisco DNA Centerの固有クライアントMACアドレス数に基づいて、クライアントがネットワークに参加したSSIDの数に基づく履歴中のクライアント数の値が増加する場合があります。

不正クライアント

MAC ランダム化に基づき、不正クライアントの数はデバイスの MAC アドレスの数に応じて変化します。それ以外の場合、侵入検知に影響はなく、MAC アドレスの衝突と署名は影響を受けません。

Q&A

MAC ランダム化が有効になっている場合、不正検出機能によって正しい攻撃 MAC アドレスが検出されますか。

攻撃 MAC アドレスは、物理 MAC アドレスではなく、ランダム MAC アドレスです。

マップと Cisco DNA Spaces

クライアントが別の SSID に参加すると、マップ上の重複クライアントが表示されます。

デバイスの分類

[Organizationally Unique Identifier（OUI）] フィールドが表示されない場合、デバイス タイプ ワークステーションと OS が正しくない可能性があります。

Cisco DNA Centerクライアントの問題

グローバルな問題は、同じクライアントが SSID で複数回失敗した場合でも、複数のクライアントの失敗として検出されるため、より迅速にトリガーされる可能性があります。SSID によって異なる問題は遅れてトリガーされる可能性があります。

Q&A

MAC ランダム化によって影響を受けるグローバルな問題の例を挙げてください。

認証の失敗、DHCP の失敗、ワイヤレス LAN コントローラ関連の失敗（範囲内の WLC、DHCP サーバー、AAA サーバー関連の失敗）といったクライアントの問題によって、グローバルな問題がより迅速に引き起こされる可能性があります。これらの障害が発生するのは、同じクライアントが SSID で複数回失敗した場合でも、複数のクライアントの失敗として検出されるためです。

MAC ランダム化のために Cisco DNA Center で遅れて発生する可能性のある問題はありますか。

「デュアルバンド対応クライアントは 5 GHz よりも 2.4 GHz を優先する」問題は、他の AP から最も近い 5 GHz プローブデータに依存しています。この問題は、異なる SSID でプローブするクライアントがカウントされないため、検出が遅くなる場合があります。Cisco DNA Center は、そのクライアントを新しいクライアントとして検出します。

一般的な Q&A

Q&A

Apple Analytics に影響はありますか。

Apple Analytics はワイヤレス LAN コントローラから取得されるため、Cisco DNA Center が Apple Analytics に影響を与えることはありません。

IP アドレスのリース時間が長く、古いセッションの期限が切れていない場合、重複クライアントは表示されますか。

VLAN が同じである場合、長いリース時間が設定されていると、DHCP サーバーの IP アドレスが不足します。VLAN が異なる場合、動作は現在と同じです。

こうした状況では、デバイス上のセッション数が制限されますか。

MAC-to-user マッピング制限を追加すると、クライアントセッション数に影響する可能性があります。

スケール

Q&A

MAC ランダム化は、Cisco DNA Center が監視するクライアントの数に影響しますか。

クライアントがランダム MAC アドレスを使用すると、履歴中のクライアント数が増加する可能性があります。最悪の場合、クライアント数が、実際のクライアント数に使用可能な SSID の数を掛けた数まで増加する可能性があります。このような増加は、すべてのクライアントがランダム MAC アドレスを使用している状況で、14 日以内に使用可能なすべての SSID に参加した場合にのみ発生し、顧客の規模と使用例に基づいて公開されている規模の制限を超えるおそれがあります。

MAC ランダム化は、インテリジェントキャプチャの規模に影響しますか。

直接的な影響はありませんが、Cisco DNA Center では、部分キャプチャの場合は 16 の MAC アドレス、完全キャプチャの場合は 1 つの MAC アドレスに制限されています。クライアントが複数の SSID に参加した場合、同じデバイスに複数の MAC アドレスが存在することになります。単一ユーザーに対して、複数のクライアントキャプチャをスケジュールする必要があるかもしれません。この状況では、異なるユーザーに対して同時に複数のキャプチャをスケジュールすることが制限されます。

SD-Access のプロビジョニング

MAC ランダム化による SD-Access プロビジョニングへの影響はありません。

回避策

回避策の 1 つは、クライアントで MAC ランダム化機能を無効にすることです。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/