

X ヘッダーの挿入と暗号化

- 機能の概要と変更履歴 （1 ページ）
- 機能説明 （2 ページ）
- 機能の仕組み （2 ページ）
- X-Header の挿入と暗号化の設定 （4 ページ）
- X-Header の挿入および暗号化構成をモニタリングして障害対応する （6 ページ）
- アンチスプーフィングのサポート （6 ページ）

機能の概要と変更履歴

要約データ

表 *1*: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
X-Header エンリッチメントによるアンチスプーフィング機能のサポートを追加しました。	2023.02.0
最初の導入。	2020.02.x

機能説明

X-Header の挿入および X-Header 暗号化のプロセスは、総称してヘッダーエンリッチメント（HE）と呼ばれます。UPF は HE をサポートし、URL リクエストの HTTP ヘッダー内の既存の X-Header フィールドを削除および変更できます。

この機能により、HTTP、WSP GET および POST 要求パケットおよび、モバイルアドバタイズメントの挿入（MSISDN、IMSI、IP アドレス、ユーザーによるカスタマイズが可能、など）としてエンドアプリケーションが使用する HTTP 応答にヘッダーを追加できます。

機能の仕組み

HE には次の 2 つの動作が含まれます。

1. ヘッダーの挿入
2. ヘッダーの暗号化

X-Header の挿入

拡張ヘッダー（X-Header）フィールドは、ユーザーID、デバイスの検出などの特定の目的でプロトコルヘッダーに追加されるフィールドです。X-Header メカニズムでは、プロトコルを変更せずに追加の entity-header フィールドを定義できます。ただし、これらのフィールドは、受信者が認識できないものとします。

X-Header の挿入機能を使用すると、HTTP または WSP の GET および POST 要求パケットと HTTP 応答パケットに X-Header を挿入できます。HTTP または WSP 要求および HTTP 応答パケットに X-Header を挿入するようにルールを構成できます。ルールに関連付けられた課金アクションには、パケットに挿入される X-Header のリストが含まれます。

（注）

- パケットに X-Header が挿入されているフローはオフロードされません。
- X-Header 設定では、transmit order CLI に関係なく、すべての TCP OOO パケットがバッファされ、順序変更後に送信されます。

X-Header の暗号化

X-Header の暗号化により、挿入前に X-Header フィールドを暗号化できます。IP フローに対して（いずれかの X-Header フォーマットにより）すでに X-Header が挿入されていて、かつ現在の charging-action に [first-request-only] フラグが設定されている場合、そのフォーマットによる X-Header の挿入は行われません。charging-action に [first-request-only] フラグが設定されていな

い場合、該当する IP フローの他の適切なパケットでは、その X-Header フォーマットによる挿入が続行されます。

X-Header のフォーマット構成を変更しても、既存のコールの再暗号化はトリガーされません。ただし、新しいコールには変更された設定が適用されます。変更された構成は、次の再暗号化時に、再暗号化タイムアウトが指定されている既存のコールに対して適用されます。データのフロー中にパラメータの暗号化が有効になった場合、暗号化された値が使用できなくなるため、そのパラメータの挿入は停止します。

（注） この機能では、フローのリカバリはサポートされません。

制限事項

ここでは、現在のリリースに存在する制限について説明します。

- 応答パケットへの X-Header 挿入はサポートされません。
- RSA および RC4MD5 による X-Header の暗号化はサポートされていますが、AES による X-Header の暗号化はサポートされていません。
- X-Header のモニタープロトコルはサポートされていません。
- パケットでは、次の X-Header フィールドの挿入は、されていません。
  - QoS
  - UIDH
  - カスタマー ID
  - Hash Value
  - 時刻
  - RADIUS 文字列
  - Session-Id
  - 輻輳レベル
  - ユーザープロファイル
- HTTP ヘッダーの解析とバッファリングは、rulebase に明示的に delete-existing と設定されている x-header フィールドで構成された x-header フォーマットがある場合にのみ実行されます。x-header delete-existing を使用しないオペレータの場合、解析またはバッファリングによるオーバーヘッドは発生しません。

X-Header の挿入と暗号化の設定

X ヘッダーの挿入の設定

ステップ 1	X-Header を挿入する必要がある HTTP パケットを識別するための ruledef を作成または設定します。
ステップ 2	rulebase を作成または設定し、charging-action を設定します。これにより、HTTP パケットに X-headerフィールドが挿入されます。
ステップ 3 :	「*X-Header* フォーマットの作成」の説明に従って、X-Header フォーマットを作成します。
ステップ 4	「*X-Header* フォーマットを構成する」の説明に従って、課金アクションのメッセージタイプに基づいて、X-Header フォーマットを構成します。

X-Header フォーマットの作成

X-Header フォーマットを作成するには、次の構成を使用します。

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
    end
```

X-Header フォーマットの設定

X-Header フォーマットを構成するには、次の構成を使用します。

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
      insert xheader_field_name string-constant xheader_field_value | variable
 { bearer { 3gpp { apn | charging-characteristics | charging-id | imei
 | imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id
 | ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] [ delete-existing ] |
http { host | url } }
       end
```

X ヘッダーの暗号化の設定

ステップ 1	「*X-Header* の挿入を構成」で説明されているように、X-Header の挿入を構成します。

ステップ 2	「*X-Header* の暗号化を構成」で説明されているように、rulebase を作成または構成し、使用する暗号化証明書と再暗号化パラメータを構成します。
ステップ 3	「暗号化証明書の設定」の説明に従って、使用する暗号化証明書を設定します。

X ヘッダーの暗号化の設定

X-Header の暗号化を構成するには、次の構成を使用します。

```
configure
   active-charging service ecs_service_name
     rulebase rulebase_name
        xheader-encryption certificate-name certificate_name
        xheader-encryption re-encryption period re-encryption_period
        end
```

注：

- この構成により、指定した rulebase に基づいて、すべてのサブスクライバに対して X-Header の暗号化が有効になります。
- 証明書が削除されても、ECS ではそのコピーが引き続き使用されます。証明書名がルールベースから削除されると、コピーは解放されます。
- X ヘッダーのフォーマット設定を変更しても、既存のコールの再暗号化はトリガーされません。ただし、新しいコールには変更された設定が適用されます。変更された設定は、次の再暗号化のときに、再暗号化のタイムアウトが指定されている既存のコールにも適用されます。データのフロー中にパラメータの暗号化が有効になった場合、暗号化された値が使用できなくなるため、そのパラメータの挿入は停止します。

暗号化証明書の設定

暗号化証明書を設定するには、次の設定を使用してください。

```
configure
   certificate name certificate_name pem { { data pem_certificate_data
private-key pem [ encrypted ] data pem_pvt_key } | { url url private-key
pem { [ encrypted ] data pem_pvt_key | url url } }
   end
```

X-Header の挿入と暗号化の構成を確認する

Exec モードで次のコマンドを入力して構成を確認します。

xheader-format *xheader_format_name*

X-Header の挿入および暗号化構成をモニタリングして障害対応する

show active-charging charging-action statistics name

このコマンドの出力には、X-Header の統計が表示されます。

- X-Header 情報：
  - 挿入された XHeader のバイト数
  - 挿入された XHeader のパケット数
  - XHeader によって消費される IP フラグメント数
  - 削除された XHeader のバイト数
  - 削除された XHeader のパケット数

show active-charging rulebase statistics name

このコマンドの出力には、ヘッダーエンリッチメントの統計が表示されます。

- HTTP ヘッダーのバッファリング制限到達

アンチスプーフィングのサポート

機能説明

UPF は、ヘッダーエンリッチメントを使用したスプーフィング検出と緩和をサポートしています。アンチスプーフィング機能により、オペレータとそのサブスクライバは、悪意のある UE デバイスによって引き起こされるスプーフィング脅威を阻止します。この機能は、外部ポータルがサブスクライバまたはコンテンツの承認に使用されている場合に、不正行為を検出します。

アンチスプーフィング機能は、HTTP 要求に対してのみサポートされます。この機能により、URL 要求の HTTP ヘッダー内の既存の X-Header フィールドを削除および変更できます。

ユーザー生成のヘッダー名が X-Header フォーマットで使用されているヘッダー名と類似している場合、X-Header フィールドを検索、削除、変更できます。X-Header フィールド名では、大文字と小文字が区別されません。たとえば、x-MSISDN フィールドと x-msisdn フィールドが、受信 HTTP 要求に存在する場合、両方のフィールドが処理されます。

user HTTP ヘッダーに、挿入するフィールドがすでにある場合、それらのフィールドに対応する値は、ヘッダーの最後の部分にあるゲートウェイからの変更された値に置き換えられます。

ヘッダーにすでに存在する 1 つのフィールドに複数のエントリがある場合、フィールドの 1 つのインスタンスがゲートウェイから挿入された値とともに選択されます。

HTTP GET 要求が複数ある場合、パケットヘッダーを、すべての GET 要求の X-header フィールドに置き換えます。暗号化が有効になっている場合は、X-Header の挿入後に実行されます。

制限事項

次に、アンチスプーフィング機能の既知の制限事項を示します。

- HTTP の GET または POST ヘッダーが、3 つのパケットで完了していない場合、アンチスプーフィングは、ヘッダーが完了する最後のパケットに対してのみ実行されます。それ以外の場合、パケットは HE なしで送信されます。
- フィールド名に「x-」を含まないフィールドは許可されますが、x- で始まらない拡張ヘッダーフィールドは削除されません。

X-Header でのアンチスプーフィングを有効にする

X-Header でアンチスプーフィングを有効にするには、次の設定を使用します。

```
configure
   active-charging service acs_service_name
      xheader-format xheader_format_name
         insert xheader_field_name variable { bearer subscriber-ip-address
} [ encrypt ] [ delete-existing ]
         exit
```

注：

- **delete-existing**：このコマンドは、X-Header ファイルのスプーフィングの検出を有効にします。
- この機能はデフォルトで無効に設定されています。
- 最大 10 の X-Header フィールドを設定するには、**delete-existing** CLI キーワードを使用します。このキーワードには、X-Header 挿入用に設定されたフィールドも含まれます。

OAM のサポート

この項では、アンチスプーフィング機能の show コマンドとそれらの出力に関する情報を示します。

show user-plane-service statistics charging-action [name | all]

このコマンドの出力には、課金アクションに関するユーザープレーン統計が表示されます。

- X-Header 情報：
  - 挿入された XHeader のバイト数

- 挿入された XHeader のパケット数
- 削除された XHeader のバイト数
- 削除された XHeader のパケット数

show user-plane-service statistics rulebase [name | all]

このコマンドの出力には、rulebase のユーザープレーン統計が表示されます。

- ヘッダーの機能拡張統計
  - HTTP ヘッダーのバッファリング制限到達

翻訳について
このドキュメントは、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。

翻訳について
このドキュメントは、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。