X ヘッダーの挿入と暗号化

マニュアルの変更履歴

改訂の詳細	リリース
xheader-format コマンドの **delete-existing** キーワードオプションを使用した、x-header フィールドのスプーフィング検出を有効にする CLI のサポートを追加。	21.28.m0
最初の導入。	21.25

機能説明

X-Header の挿入および X-Header 暗号化機能は、総称してヘッダーエンリッチメントと呼ばれます。この機能により、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ものなど）をはじめ、エンドアプリケーションで使用する HTTP または WSP の GET および POST 要求パケット、および HTTP レスポンスパケットにヘッダーを追加できます。

機能の仕組み

X-Header の挿入

この項では、X-Header の挿入機能の概要について説明します。

拡張ヘッダー（X-Header）フィールドは、RFC や標準規格では定義されていませんが、特定の目的でプロトコルヘッダーに追加できるフィールドです。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が、entity-header フィールドは受信者が認識できるフィールドとは想定されていません。認識されないヘッダーフィールドは、受信者によって無視されて、トランスペアレントプロキシによって転送される必要があります。

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 レスポンスパケットに X-Header を挿入できます。HTTP または WSP 要求および HTTP レスポンスパケットに X-Header を挿入するオペレータは、挿入ルールを設定できます。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。

X-Header の暗号化

ここでは、X-Header の暗号化機能の概要を説明します。

X-Header の暗号化により X-Header の挿入機能が強化され、X-Header に挿入できるフィールド数が増えるのに加え、フィールド挿入前の暗号化も可能になります。

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に対しては、その X-Header フォーマットによる挿入が続行されます。

X-Header フォーマットの設定を変更しても、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。

（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。

X-Header の挿入と暗号化の設定

この項では、X-Header の挿入および暗号化機能（総称して、ヘッダーの機能拡張）の設定方法について説明します。

X-Header の挿入

表 *1:* 手順

ステップ	説明
1	X-Header を挿入する必要がある HTTP/WSP パケットを識別するための ruledef を作成および設定します。
2	ルールベースを作成および設定し、HTTP/WSP パケットに X-Header フィールドを挿入する課金アクションを設定します。
3	X-Header 形式を作成および設定します。
4	課金アクションのメッセージタイプに基づいて X-Header フィールドの挿入を設定します。

X-Header の暗号化

表 *2:* 手順

ステップ	説明
1	X-Header の挿入、暗号化、および暗号化証明書は CLI で設定されます。
2	コールが接続されると、各再生成時間の後に、暗号化証明書を使用して文字列が暗号化されます。
3	課金アクションで X-Header 形式が設定されている ruledef にパケットがヒットすると、そのパケットへの X-Header の挿入は、指定された X-Header 形式を使用して行われます。
4	暗号化としてマークされているフィールドに対して X-Header を挿入する場合、以前に暗号化された値がそのフィールドに適宜入力されます。

X ヘッダーの挿入の設定

ここでは、X-Header の挿入機能の設定方法について説明します。

X-Header の挿入機能を設定するには、次の手順を実行します。

表 *3:* 手順

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* フォーマットの設定」の説明に従って、X-Header フォーマットを設定します。

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、次の設定を使用します。

```
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 フォーマットを設定するには、次の設定を使用します。

```
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

ここでは、X ヘッダーの暗号化機能を設定する方法について説明します。

表 *4:* 手順

ステップ 1	「*X* ヘッダーの挿入の設定」の説明に従って、X ヘッダーの挿入を設定します。

ステップ 2	「*X* ヘッダーの暗号化の設定」の説明に従って、ルールベースを作成または設定し、使用する暗号化証明書と再暗号化パラメータを設定します。
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 ヘッダーの暗号化を設定するには、次の設定例を参考にしてください。

```
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：

- この設定により、指定したルールベースに基づいて、すべてのサブスクライバに対して X ヘッダー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 の挿入と暗号化の設定の確認

Exec モードで次のコマンドを入力して設定を確認します。

xheader-format *xheader_format_name*

X-Header の挿入および暗号化機能のモニタリングとトラブルシューティング

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging charging-action statistics name

このコマンドの出力には、X-Header の統計情報が表示されます。

- XHeader 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

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。