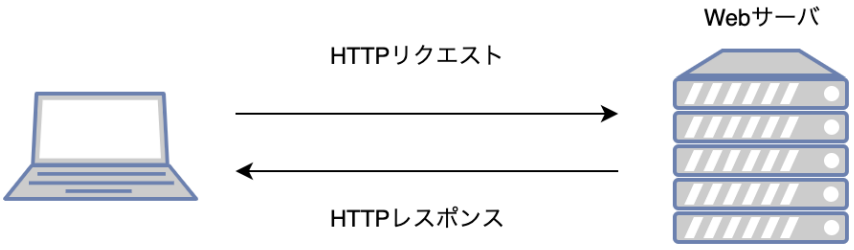
HTTPとセッション

HTTP(HyperText Transfer Protocol)通信の構成

HTTP通信は、HTTPリクエストとHTTPレスポンスで構成される。



リクエストメッセージ

クライアントからWebサーバへ送信されるメッセージのこと。リクエストライン、リクエストヘッダで構成される。

〈例〉Google Chromeでの確認（デベロッパーツール＞ネットワーク）

▼ Request Headers　☑ Raw

```
GET /~sec/http_session_2.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Connection: keep-alive
Cookie: PHPSESSID=mn65u2tbt40e3k7pjkav99f0ta
Host: 10.201.10.38
Referer: http://10.201.10.38/~sec/http_session_3.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.
0.0.0 Safari/537.36
```

1行目・・・リクエストライン、Webサーバへの命令。

＜例＞　**GET**　/~sec/http_session2.php　**HTTP/1.1**

メソッド　URL(URI)　**プロトコルバージョン**

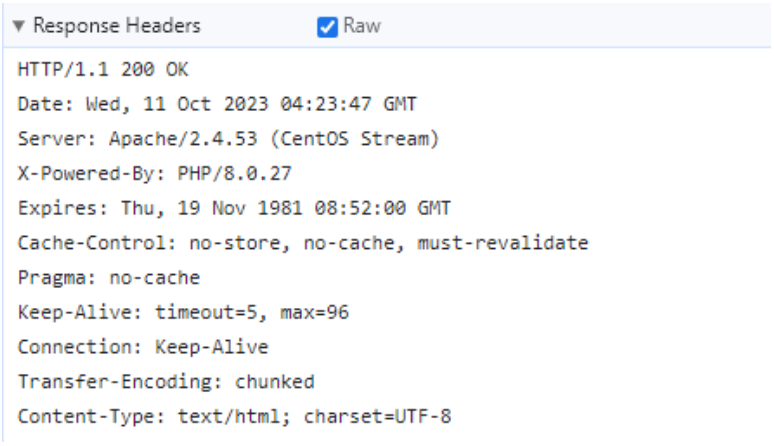
メソッド・・・POST、HEADなどもある。

2行目以降・・・ヘッダ、「**名前:値**」で区切った形式で記述される。

レスポンスメッセージ

Webサーバからクライアントへ送信されるメッセージのこと。ステータスライン、ヘッダ、ボディで構成される。

〈例〉Google Chromeでの確認（デベロッパーツール＞ネットワーク）



ステータスライン(1行目)　　**HTTP/1.1** (プロトコルバージョン) **200**(ステータスコード) **OK** (テキストフレーズ)

ヘッダ(2行目以降)　　Date : Wed , 11 Oct 2023 04:18.36 GMT

Server: Apache/2.4.53 (CentOS Stream)

:

Content-Type: text/html; charset=UTF-8

ヘッダは空白行が現れるまで続く

空行　　ヘッダとボディの区切り

ボディ　　<body>〜</body>

▼ 代表的なレスポンスヘッダ

Content-Length(ボディのバイト数)、Content-Type (MIMEタイプ)、text/html、text/css

▼ POSTメソッド

メッセージボディ

フォームに**入力されたデータ**のこと。POSTメソッドのリクエストメッセージのボディ部分にメッセージボディが含まれて送信される。

ヘッダとボディは空行で区切る。

<例>メッセージボディ　kosu=2&kakaku=400

パーセントエンコーディング

日本語などをURLに記述する場合に使用される。バイト単位、%××(16進数)で表現される。

＜例＞**%22**　・・・　”　**%27**　・・・　’

Referer

Refererとは、閲覧中のWebページを見る前にアクセスした参照ページのこと。

＜例＞GoogleからECCコンピュータ専門学校へアクセス・・・GoogleがReferer

1. Refererヘッダ

   リクエストメッセージにつくことがある。リンク元のURL、意図した**遷移を経ている**か確認できる。**form,a**によるリンクなどでもつく。

2. セキュリティ問題

   URLに機密情報やセッションIDが含まれている場合、Referer経由で外部に漏洩して、なりすましに悪用される可能性がある。

GETとPOSTの使い分け

- GETメソッドは**参照のみ**用いる
- GETメソッドは副作用がないことが期待される
- **機密情報**の送信はPOSTを使用する。

▼GETの問題点

パラメータがReferer経由で外部に漏れる。

パラメータがアクセスログに残る。

パラメータがブラウザのアドレスバーに表示されて他人に覗かれる。

パラメータ付きURLを利用者がSNSなどで共有してしまう。

hiddenパラメータ

表示されないが、HTMLソース上で確認できる。

HTTPのステートレス性

クライアントの状態を記憶しておく機能。HTMLのレスポンスにパラメータの状態を記録しておく。

ブラウザから送信される値は、書き換えることができる。**hidden、radioボタンの選択値が該当**する。

HTTP認証

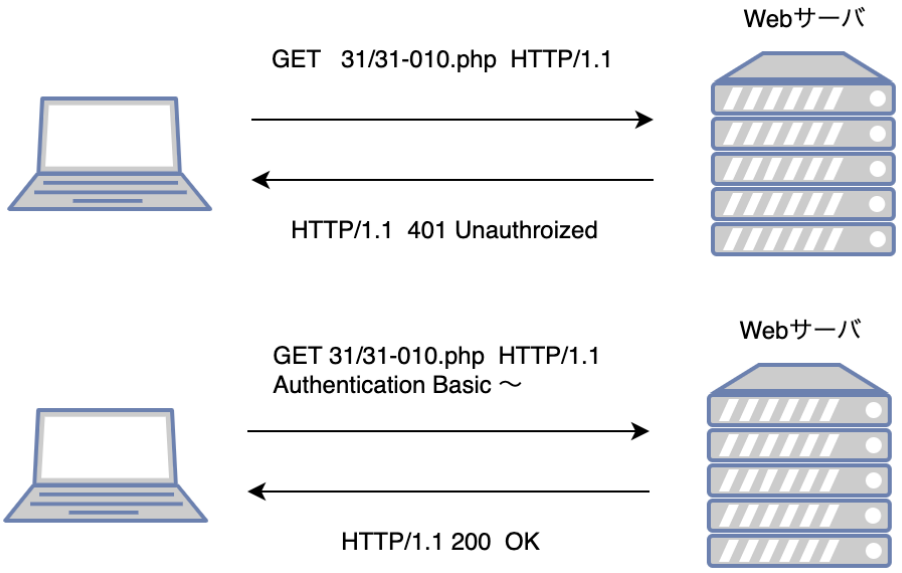
HTTPの認証にはBasic認証、NTLM認証、Digest認証がある。

1. Basic認証

   ユーザID、パスワードを使用して認証を行う。認証に使用されるデータは暗号化はされない。

   認証が必要なページにリクエストがあると、いったん「401 Unauthroized」ステータスを返す。ブラウザはこのステータスを受け

   て、IDとパスワードの入力画面を表示し、入力されたIDとパスワードをサーバへ送信する。



Authentication: Basic ～

～の部分は**ID :パスワードをBase 64**でエンコードしたものが入る。Base64でデコードするとIDとパスワードがわかる。

AAA

AAAとはセキュリティの基本概念、Authentication(認証)、Authorization(認可)、Accouting(課金)で構成される。

Authentication(認証)　・・・　ユーザID、パスワードを使用して許可されたものか確認すること。

Authorization(認可)　・・・　認証されたユーザが許可された権限のこと。

Accounting(課金)　・・・　ログの管理。

セッション管理

Cookie(クッキー)

サーバ側がブラウザに対して記憶させている情報のこと。「**名前=変数**」の形式のデータ。

レスポンスヘッダの「**Set-Cookie:**」により保存される。

セッションID

クッキー値(**PHPSESSID=・・・**)、ブラウザからサーバ側へアクセスする際に送信される。**Cookie:PHPSESSID=・・・で設定リクエストヘッダに設定される。**

クッキーの値について

クッキーで保持できる**値の個数や文字数には制限**がある。

値は利用者本人から参照・変更ができるため機密情報は保存しない方がよい。

セッションIDの乗っ取り

セッションIDが他人乗っ取られると、なりすましにあってしまう。

セッションIDの漏洩に注意する必要がある。

1. セッションIDの漏えい原因

   クッキーの属性に不備があるため、セッションIDが盗聴される。XSSなどアプリケーションの脆弱性により漏えいする。プラットフォームの脆弱性により漏えいする。Refererのヘッダにより漏えいする。

2. クッキーの属性

   クッキーの属性には次のようなものがある。

   Domain (クッキーをセットしたサーバのドメイン)、**Path (クッキーを送信するURLのディレクトリ)**、**Expire (クッキーの有効期限)**、

   Secure (HTTPSのクッキーを送信する)、**HttpOnly (クッキー値へJavaScriptからアクセスできない)**

   Domain属性・・・指定していない場合は、クッキーをセットしたサーバのドメインになる。Domain=ドメイン名(例Domain=ecc.ac.jp)、ただし設定すると漏えいにもつながる。comp.ecc.ac.jp以外にもクッキー情報が漏えいしてしまうことがある。

   ＊Domain属性は原則として指定しない。

   HttpOnly属性・・・JavaScriptからアクセスできないようにするため、XSSなどによるクッキーの漏えいを防ぐことができる。session.cookei_httponly = on