HTML5プロフェッショナル認定試験
レベル1ポイント解説無料セミナー

株式会社クリーク・アンド・リバー社 認定講師

高井 歩

本日の概要

ネットワーク・サーバ関連技術
- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

試験範囲
- 試験概要
- 試験範囲

Web関連技術
- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

試験範囲
- 試験概要
- 試験範囲

ネットワーク・サーバ関連技術
- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

Web関連技術
- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

HTML5プロフェッショナル認定資格とは

- 次世代のWebプロフェッショナルのスキルの向上に貢献するために、
  HTML5を活用したWebページやWebアプリケーションなどのデザイン、
  設計、構築に関する体系だった知識とスキルを備えたHTML5のプロフェッ
  ショナルを中立的な立場で公平かつ厳正に認定する資格制度です。

- Webデザイナー、Webプログラマー、スマートフォンアプリ開発者、
  サーバーサイドエンジニアなどの、Web開発プロジェクトやWebサービス
  に関わるあらゆるプロフェッショナルが対象です。

- 多くの企業が推進する次世代Web言語の認定資格として、
  HTML5のプロフェッショナルのスキルの向上に役立ちます。
  また、企業内や研修機関での『技術力を担保する客観的基準』としても
  活用できます。

二つのレベル

HTML5 Level.1

マルチデバイスに対応した静的なWebコンテンツをHTML5を使ってデザイン・作成できる。

対象

- Webデザイナー/HTMLコーダー
- Webディレクター/グラフィックデザイナー
- フロントエンドプログラマー
- Webシステム開発者
- スマートフォンアプリ開発者
- サーバーサイドエンジニア

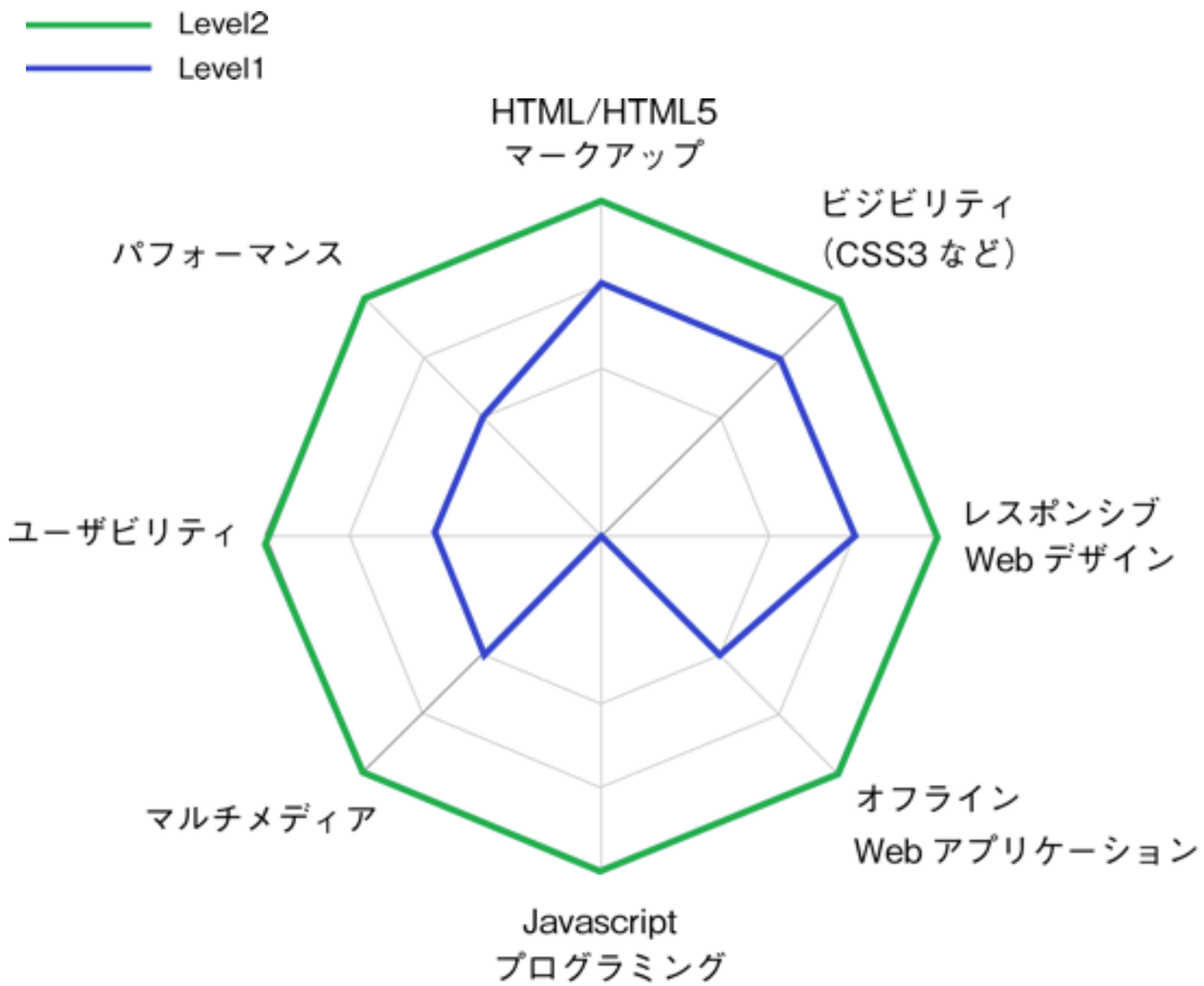
HTML5 Level.2

システム間連携や最新のマルチメディア技術に対応したWebアプリケーションや動的Webコンテンツの開発・設計ができる。

対象

- Webシステム開発者
- スマートフォンアプリ開発者
- フロントエンドプログラマー
- Webディレクター
- サーバーサイドエンジニア
- Webデザイナー/HTMLコーダー

レベル1とレベル2の資格体系



HTML/HTML5マークアップ
HTML5に関するタグの用途、構造の組み立て方に関する技術

ビジビリティ
JavascriptやCSS3などを用いて、デザイン仕様に沿った見やすい表示を行うための技術

レスポンシブWebデザイン
一つのソースで、スマートフォンなどの様々なデバイスの画面サイズに対応させるための技術

オフラインWebアプリケーション
通信が常時接続状態ではない環境でも、効率的にWebコンテンツを動作させるための技術

Javascriptプログラミング
Javascriptを使って、動的なWebコンテンツを作成する技術

マルチメディア
３D・動画・音声ファイルなどのマルチメディアコンテンツの表示・再生に関する技術

ユーザビリティ
ナビゲーション、地図表示など操作しやすいコンテンツを作成するための技術

パフォーマンス
データベースや、並列処理を使ってコンテンツを効率良く高速に動作させるための技術

レベル1とレベル2の資格体系

ベーシックレベル
HTML5プロフェッショナル向け

所要時間：90分
試験問題数：約60問
受験料：\15,000 （税抜）
認定条件： HTML5 レベル1試験に合格すること
認定の有意性の期限：5年間

認定名： HTML5 Level1 (Markup Professional)
試験名： HTML5 Level1 Exam

この資格の認定者は、下記のスキルと知識を持つWebプロフェッショナルであることを証明できます。

- **HTML5を使って静的なWebコンテンツを作成することができる。**
- **ユーザビリティ・ビジビリティの高いWEBコンテンツを設計・作成することができる。**
- **スマートフォンや車載システムなど、様々なデバイスに対応したコンテンツ作成ができる。**

アドバンストレベル
HTML5プロフェッショナル向け

所要時間：90分
試験問題数：未定
受験料：未定
認定条件：HTML5 レベル2試験に合格し、かつ有意なHTML5レベル1認定を保有していること。
認定の有意性の期限：5年間

認定名： HTML5 Level2 (Application Development Professional)
試験名： HTML5 Level2 Exam

この資格の認定者は、下記のスキルと知識を持つWebプロフェッショナルであることを証明できます。

- **動的に動作させて高いユーザビリティを実現するリッチユーザインターフェイスアプリケーションを作成することができる。**
- **マルチデバイスに対応し高パフォーマンスで動作する動的コンテンツを作成することができる。**
- **システム間連携を行いリアルタイムな情報を提供するアプリケーションを作成することができる。**

レベル1の出題構成

主題	割合	項目
Webの基礎知識	*30%*	・*HTTP,HTTPSプロトコル* ・*HTMLの書式* ・ネットワーク・サーバ関連技術の概要 ・*Web*関連技術の概要
CSS3	20%	・スタイルシートの基本 ・CSSデザイン ・カスケード（優先順位）
要素	*37%*	・*HTML4.01*以前の要素および属性 ・*HTML5*で新しく加わった要素および属性
レスポンシブWebデザイン	10%	・マルチデバイス対応ページの作成 ・メディアクエリ ・スマートフォンサイト最適化
オフライン*Web*アプリケーション	*3%*	・オフライン*Web*アプリケーション

ネットワーク・サーバ関連技術

ネットワーク・サーバ関連技術
- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

試験範囲
- 試験概要
- 試験範囲

Web関連技術
- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

ネットワーク・サーバ関連技術

- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

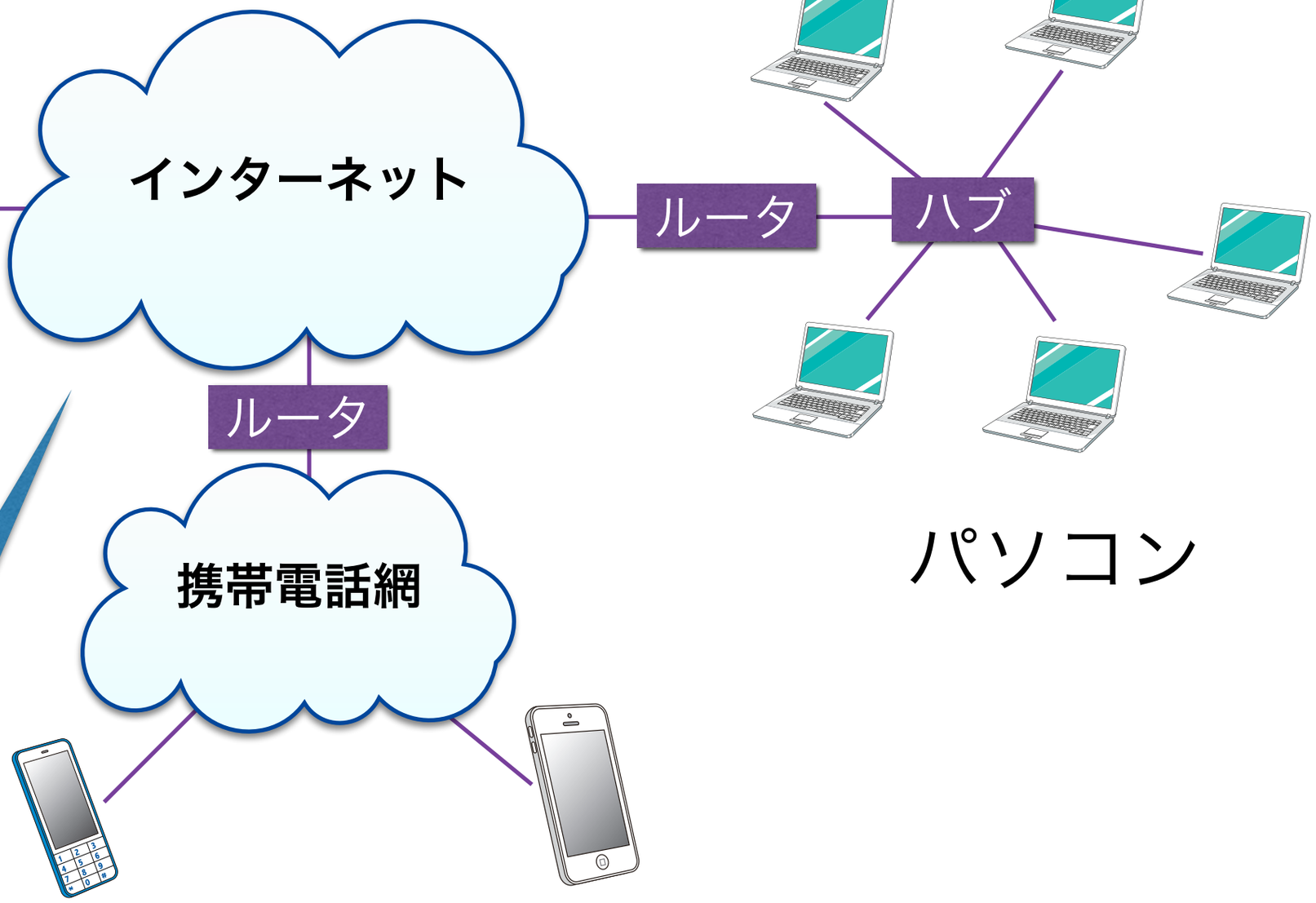
- TCP/IPの概要
- IP
- TCP
- UDP

インターネット

Webサーバ

インターネットを通じて通信を行なうために使用される規格(通信方法)が

TCP/IP



パソコン

TCP/IPによる通信の例

Webブラウザ

Webサーバ

HTTP

HTTP

TCP

TCP

IP

IP

無線LAN

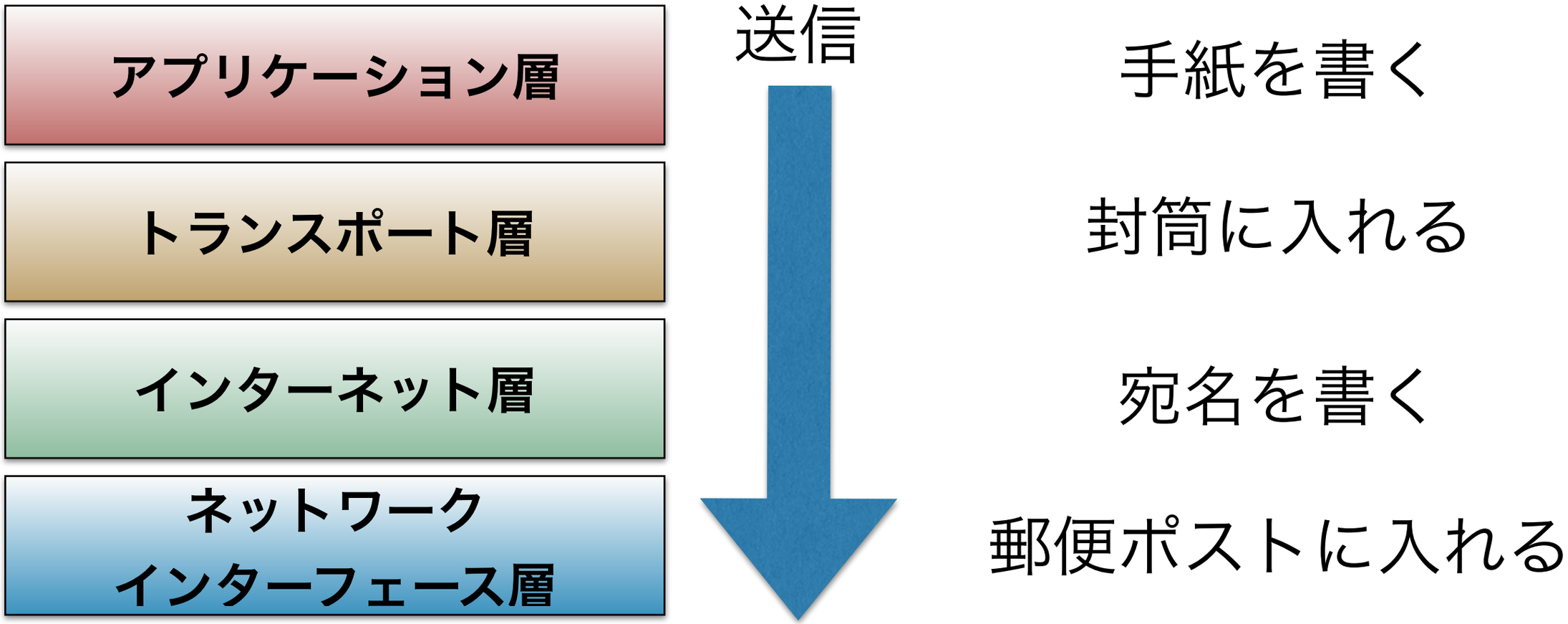
有線LAN

インターネット

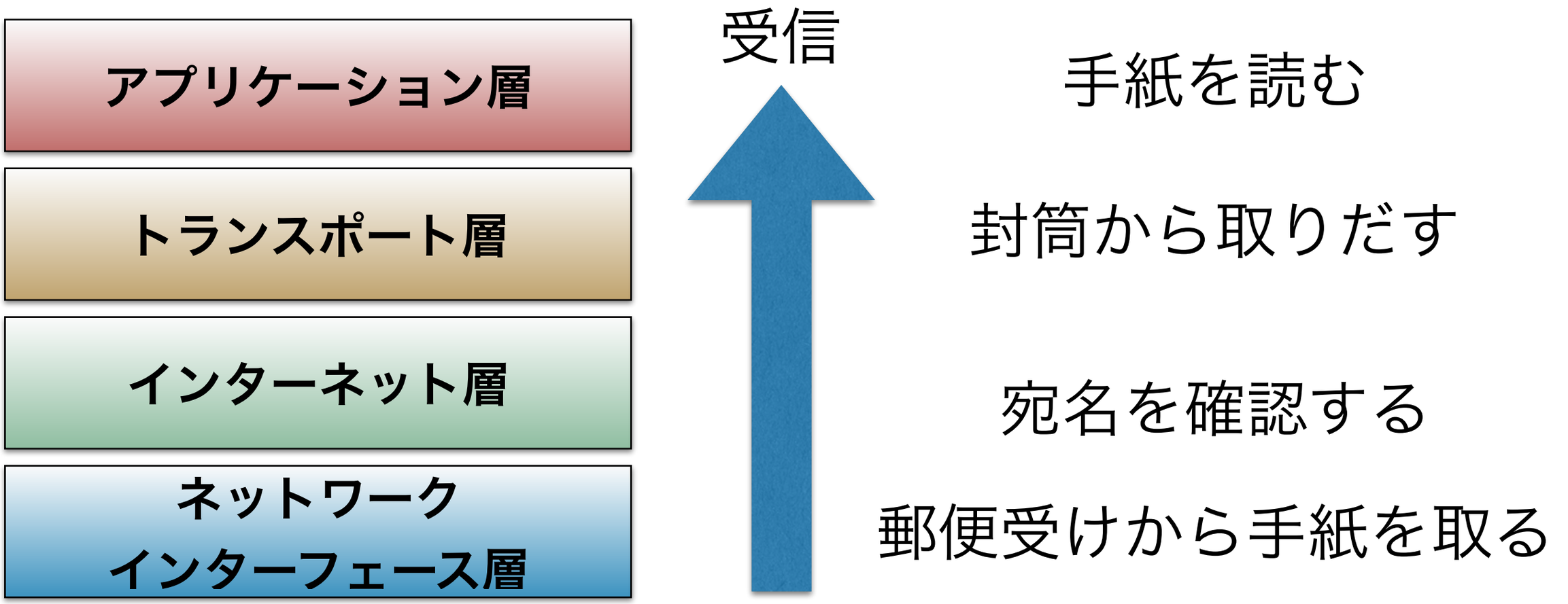
TCP/IP階層図(1)

階層	主な役割
アプリケーション層	送信内容を準備する 受信内容を処理する
トランスポート層	間違いの無い通信を行なう
インターネット層	通信相手を選択する
ネットワーク インターフェース層	物理的にネットワークに接続して データを送受信する

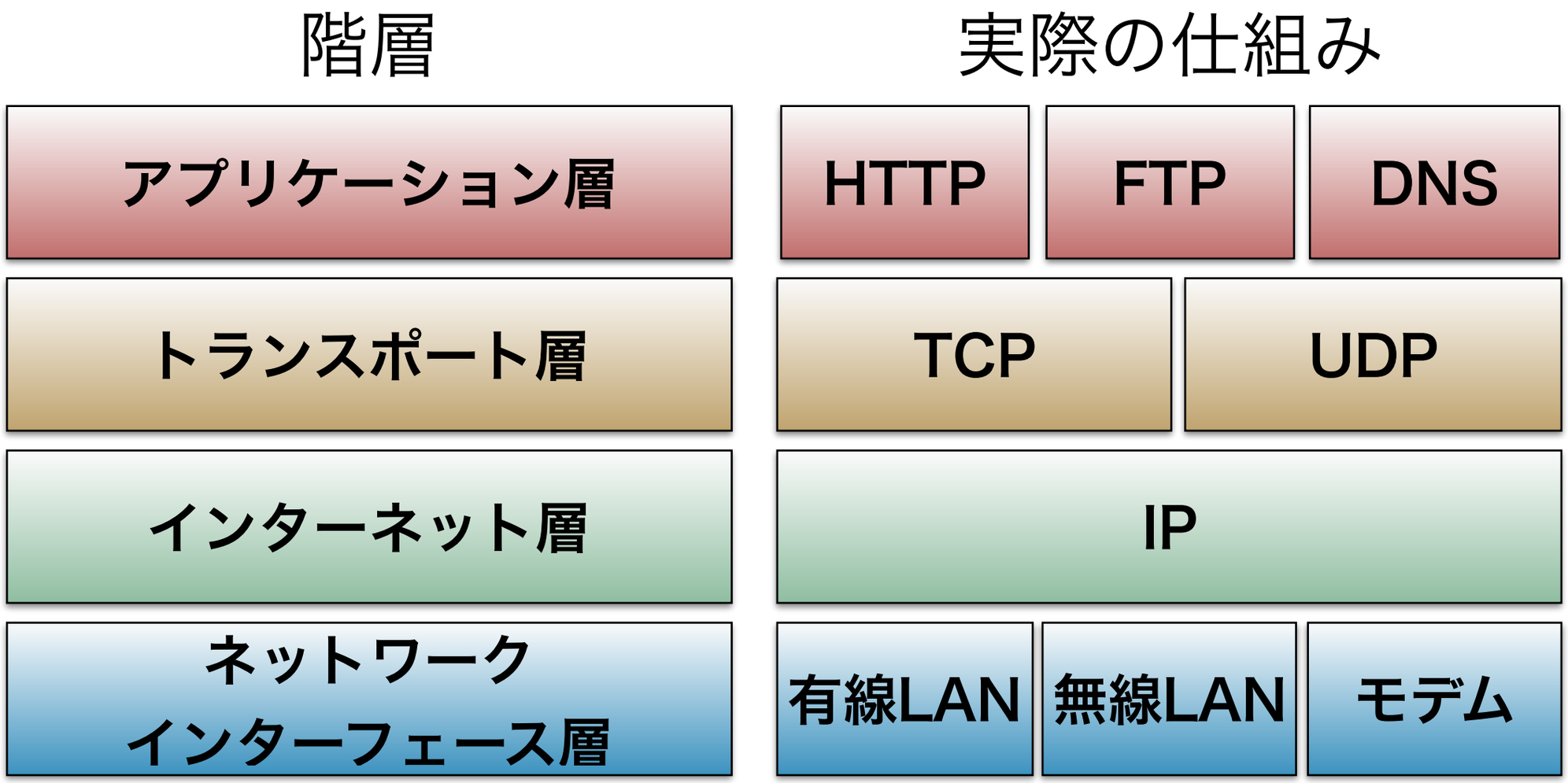
TCP/IP階層図(2)



TCP/IP階層図(3)



TCP/IP階層図(3)



問題1

TCP/IPの階層に含まれないものをひとつ選びなさい

A. ネットワークインターフェース層

B. インターネット層

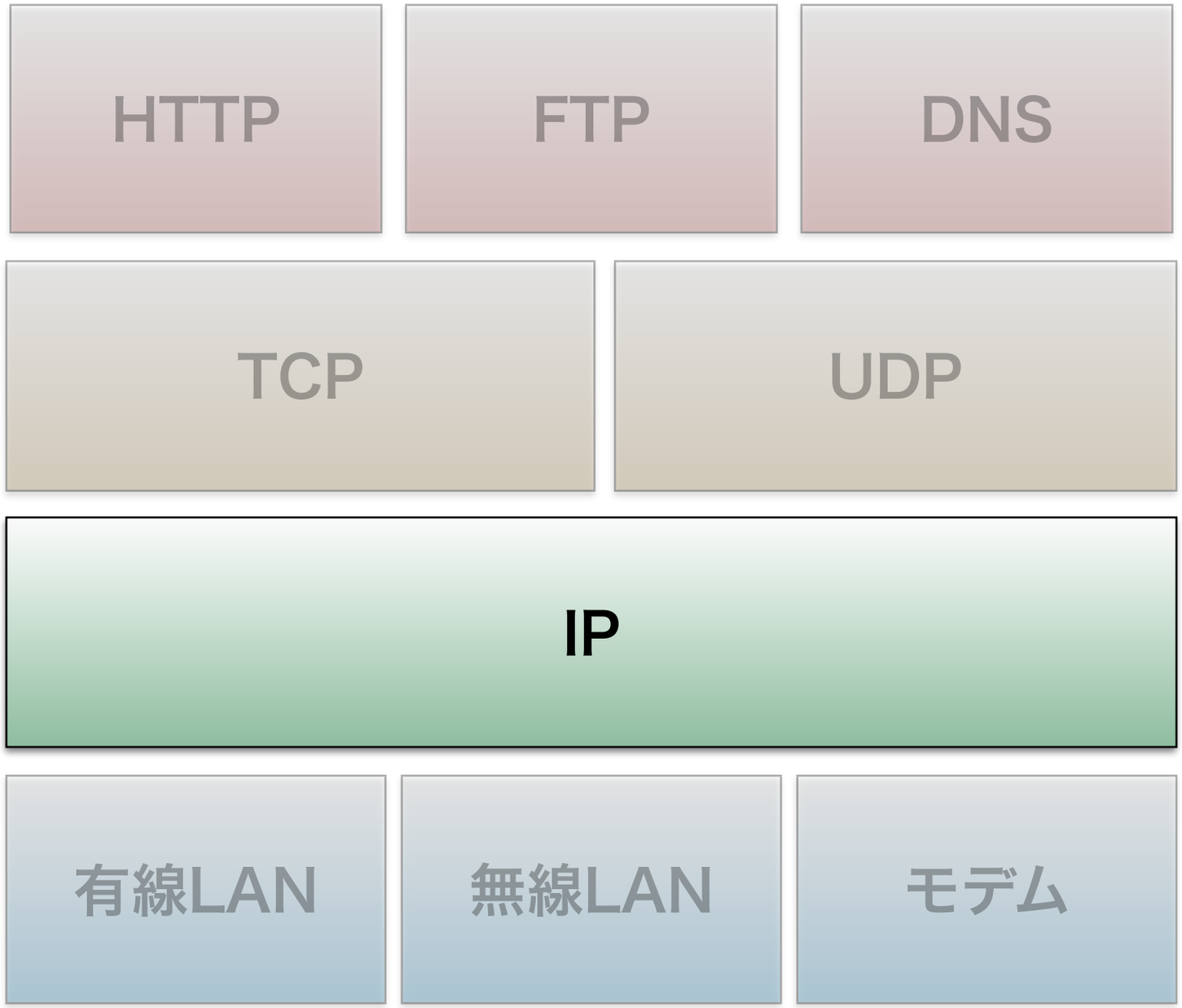
C. トランスポート層

D. アプリケーション層

E. データリンク層

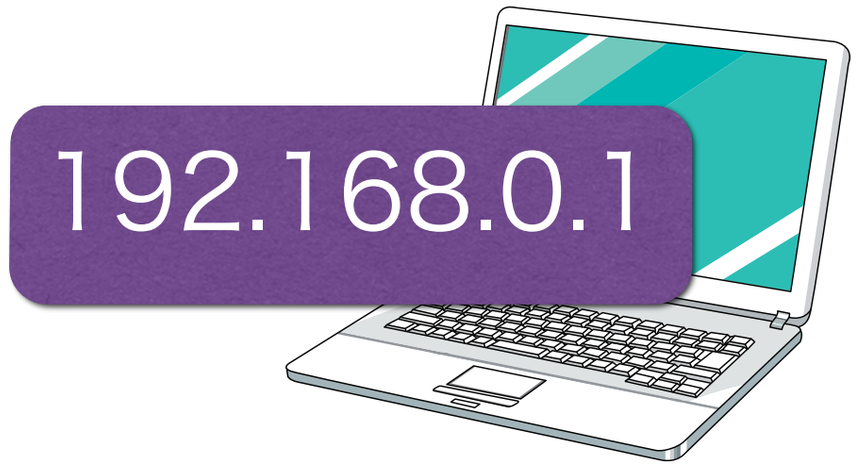
IP

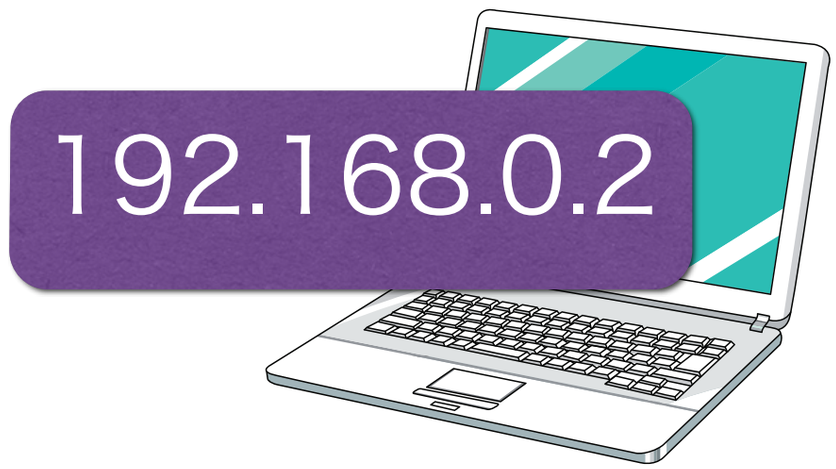
Internet Protocol

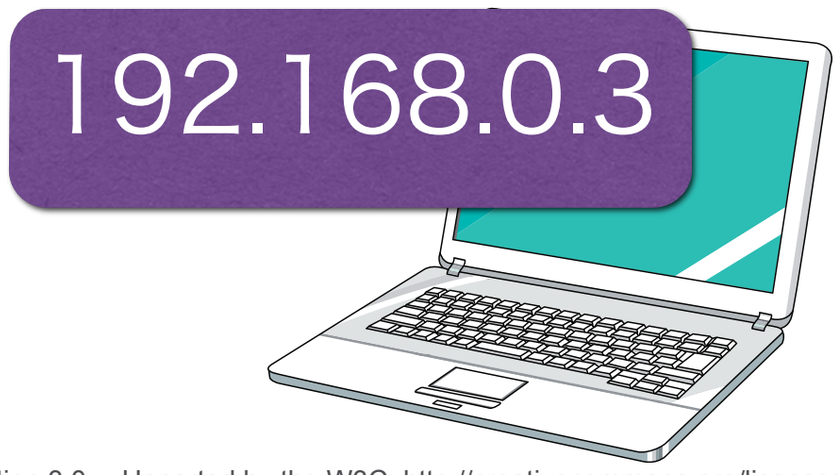


IPアドレス

1番
のPCにデータを送るよ







192.168.0.1

4つのブロックに分かれる

ひとつのブロックは0〜255の数

256の4乗で約42億通り

IP(2)

192.168.100.1

宛先IPアドレス
を見て、経路を選択

IPパケット
宛先 192.168.100.1

192.168.300.1

IPパケット
宛先 192.168.100.1

ゲートウェイ

ゲートウェイ

問題2

IPについての説明で正しいものをひとつ選びなさい

A. IPアドレスをつかって送信先、送信元のホストを識別する

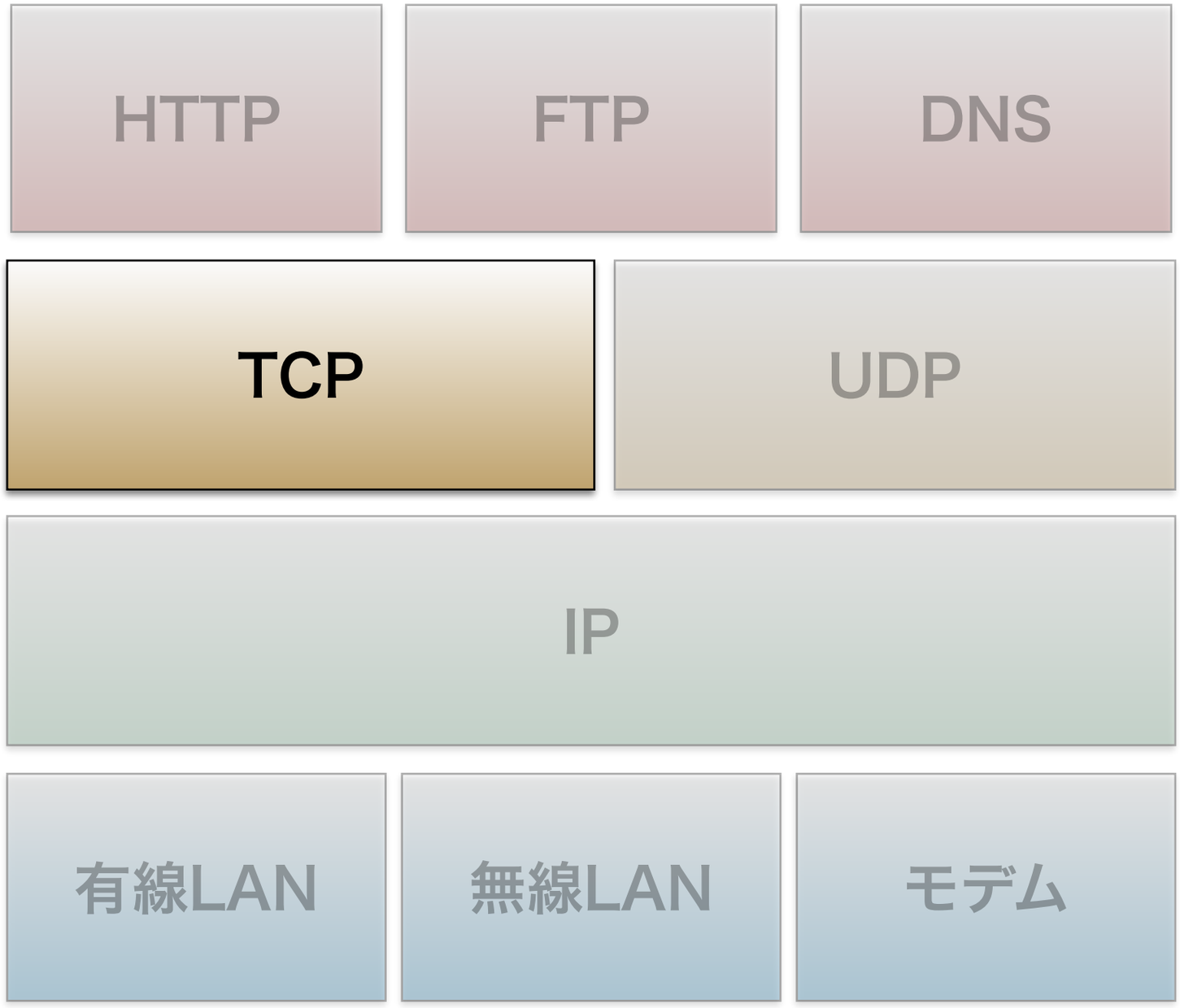
B. IPアドレスのひとつのブロックは1から256までの数字で表す

C. IPの転送の形式は、IPセグメントである

D. IPには順序制御や再送がある

TCP

Transmission Control Protocol



TCP(1)

- 確実に通信することが重要、ただしちょっと遅い
  - コネクション確立
  - データを小分け(セグメント)にして送受信
  - セグメントの順番は保証される
  - 受けとりが確認できなければセグメントを再送

TCP (2)

通信可能ですか?

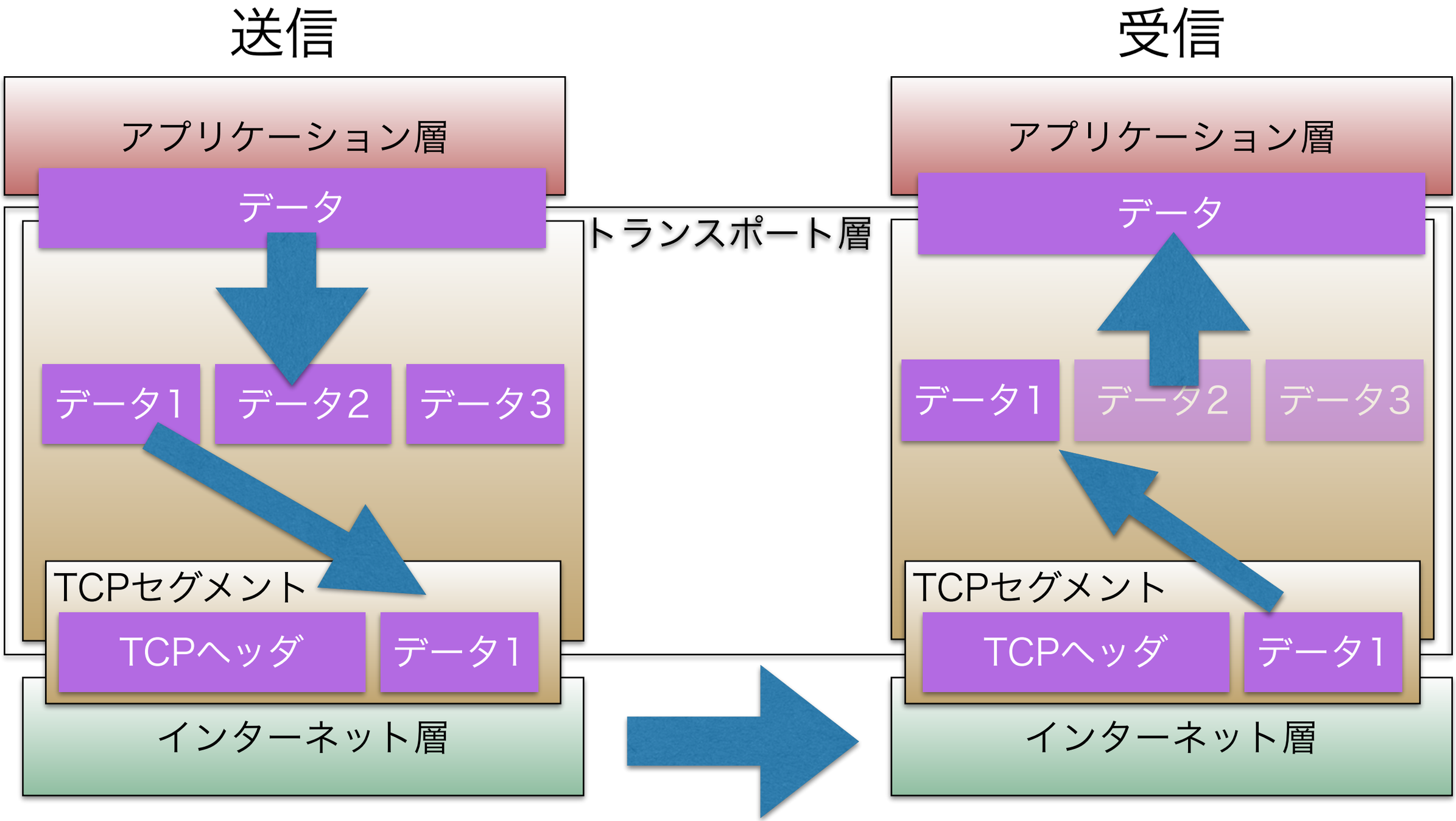
はい、通信可能です

コネクション確立

では、データを送ります

データ

TCP (3)



TCP (4)

データその1を送ります

データその1を受けとりました

受けとりが
確認できない
場合は再送

データその2を送ります

トラブル発生

もう一度データその2を送ります

データその2を受けとりました

問題3

TCPの特徴として間違っているものをひとつ選びなさい

A. 送信に失敗すると再送信する

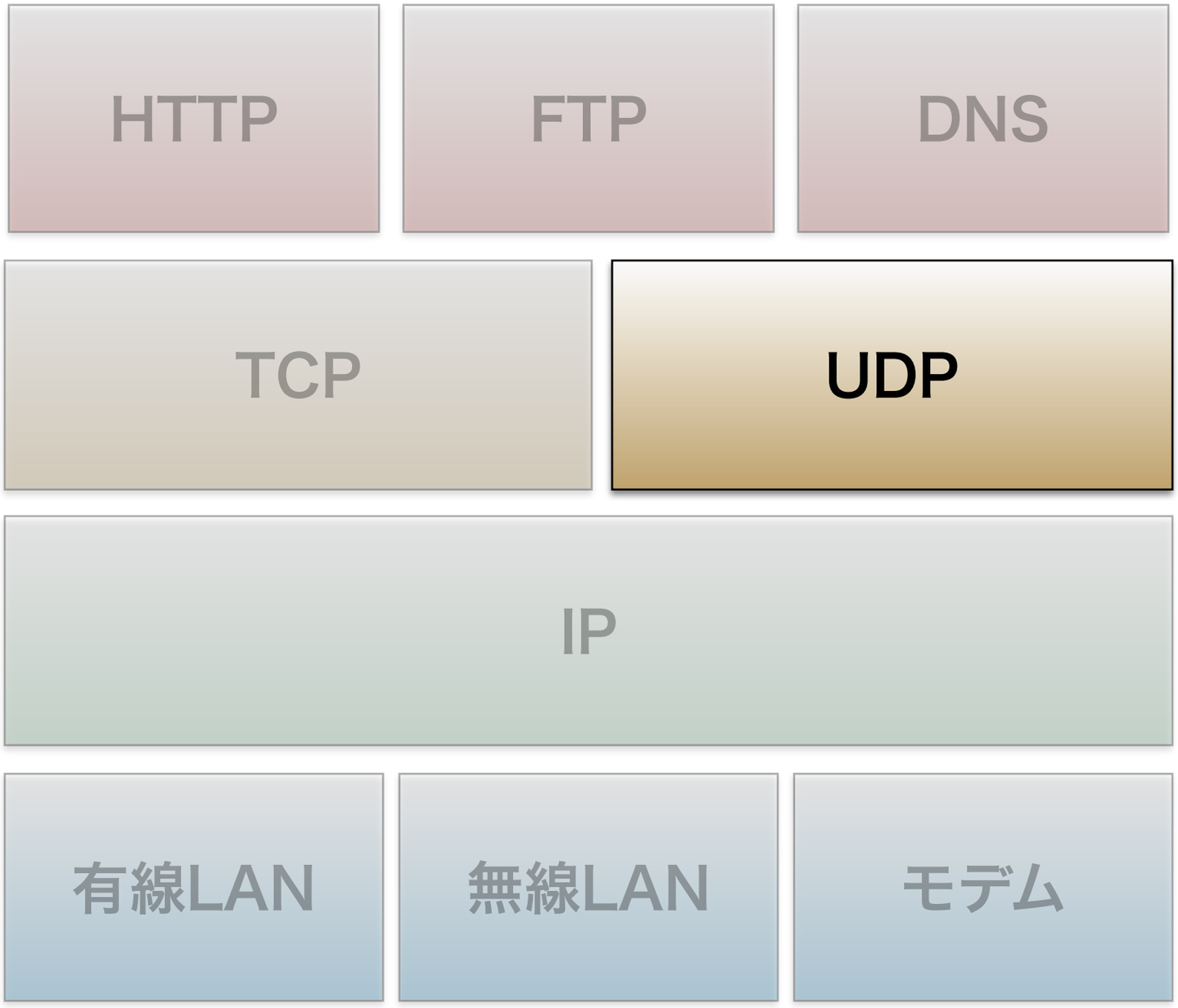
B. 信頼性が低い

C. 送信された順序が保たれる

D. アプリケーション層のデータは分割される

UDP

User Datagram Protocol



UDP(1)

- 高速なデータ転送が重要。ただし信頼性に欠ける。
  - コネクションなし
  - 順序制御なし
  - 再送なし

UDP (2)

データその1を送ります

トラブル発生

データその2を送ります

トラブルがあっても気にせず送信

データその3を送ります

経路が違えば、順番が変わることも

データその4を送ります

問題4

UDPの特徴として間違っているものをひとつ選びなさい

A. 送信に失敗すると再送信する

B. TCPよりも信頼性が低い

C. TCPよりも高速である

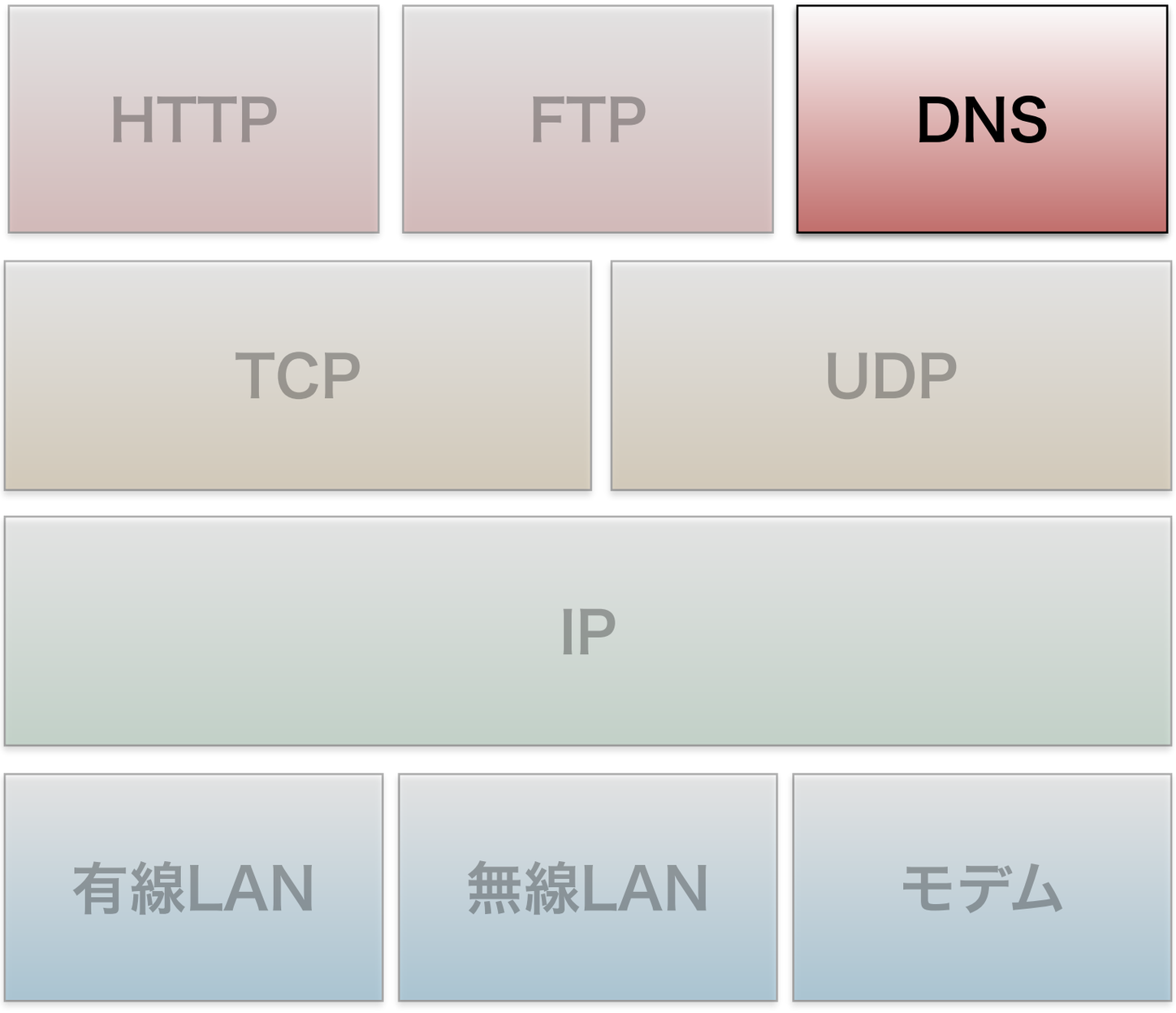
D. アプリケーション層のデータは分割される

ネットワーク・サーバ関連技術

- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

- URL(URI)
- DNS
- DNSレコード
- whois情報

DNS



URL(URI)

http://www.example.com/index.html

http　　スキーム名

www.example.com　　ホスト名

index.html　　パス

スキーム名などに使用できる文字

0～9,A～Z,a～z,-,.,_,~

使用できない文字(スペースや日本語)を使う場合には、

URLエンコードする(スペース->%20)

DNS(1)

DNSはホスト名をIPアドレスに変換(またはその逆)する。

DNSサーバ

www.example.com
のIPアドレスは?

93.184.216.119です。

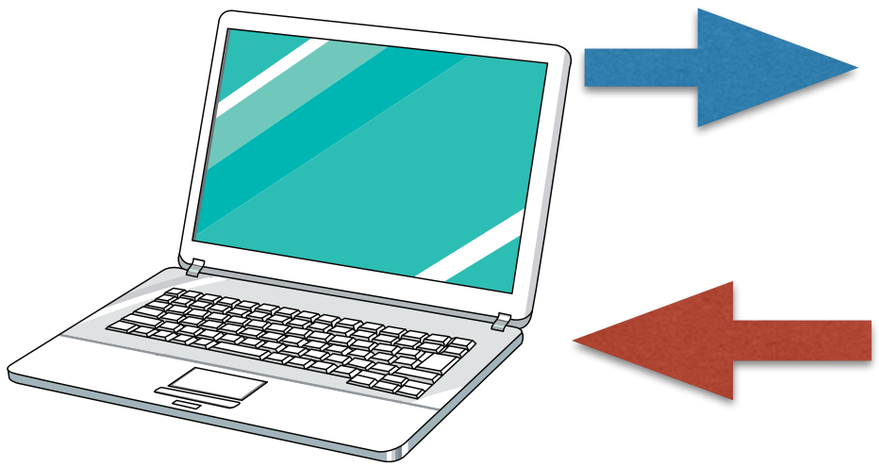
DNS(2)

www.example.com.

.(最後のドット)	ルート(省略可)
com	トップレベルドメイン
example	セカンドレベルドメイン
www	ホスト

DNS(4)

www.example.com.
のIPアドレスは?



93.184.216.119です。

DNSサーバ

ルートドメイン

comドメイン

exampleドメイン

再帰問い合わせ

DNSレコード

DNSサーバはドメイン内の様々な情報を持っている。
その情報をDNSレコードと言う。

A	ドメイン内のホスト名と そのIPアドレス
CNAME	ホスト名の別名
MX	ドメインのメールサーバの ホスト名
NS	ドメインのDNSサーバの ホスト名
TXT	ホストへのテキスト情報 (コメントや追加機能など)

whois情報

ドメインの管理責任者の情報を公開している

```
[Domain Name]                           HTML5EXAM.JP

   … 中略 …

Contact Information: [公開連絡窓口]
[名前]                                  特定非営利活動法人エルピーアイジャパン
[Name]                                  Linux Professional Institute Japan
[Email]                                 kimura@lpi.or.jp
[Web Page]
[郵便番号]                              106-0041
[住所]                                  東京都港区
                                        麻布台　1-11-9
                                        CR神谷町ビル　7F
[Postal Address]                        Minato-ku
                                        1-11-9 Azabudai
                                        7F CR Kamiya-cho Bldg.
[電話番号]                              03-3568-4482
[FAX番号]                               03-3568-4483
```

問題5

DNSについての説明で間違っているものをひとつ選びなさい

A. ルートドメインのDNSサーバは全てのドメインの情報を持っている

B. ホスト名とIPアドレスを紐付けるのはAレコードである

C. DNSサーバは自分が知らないドメインについては、他のDNSサーバに問い合わせる

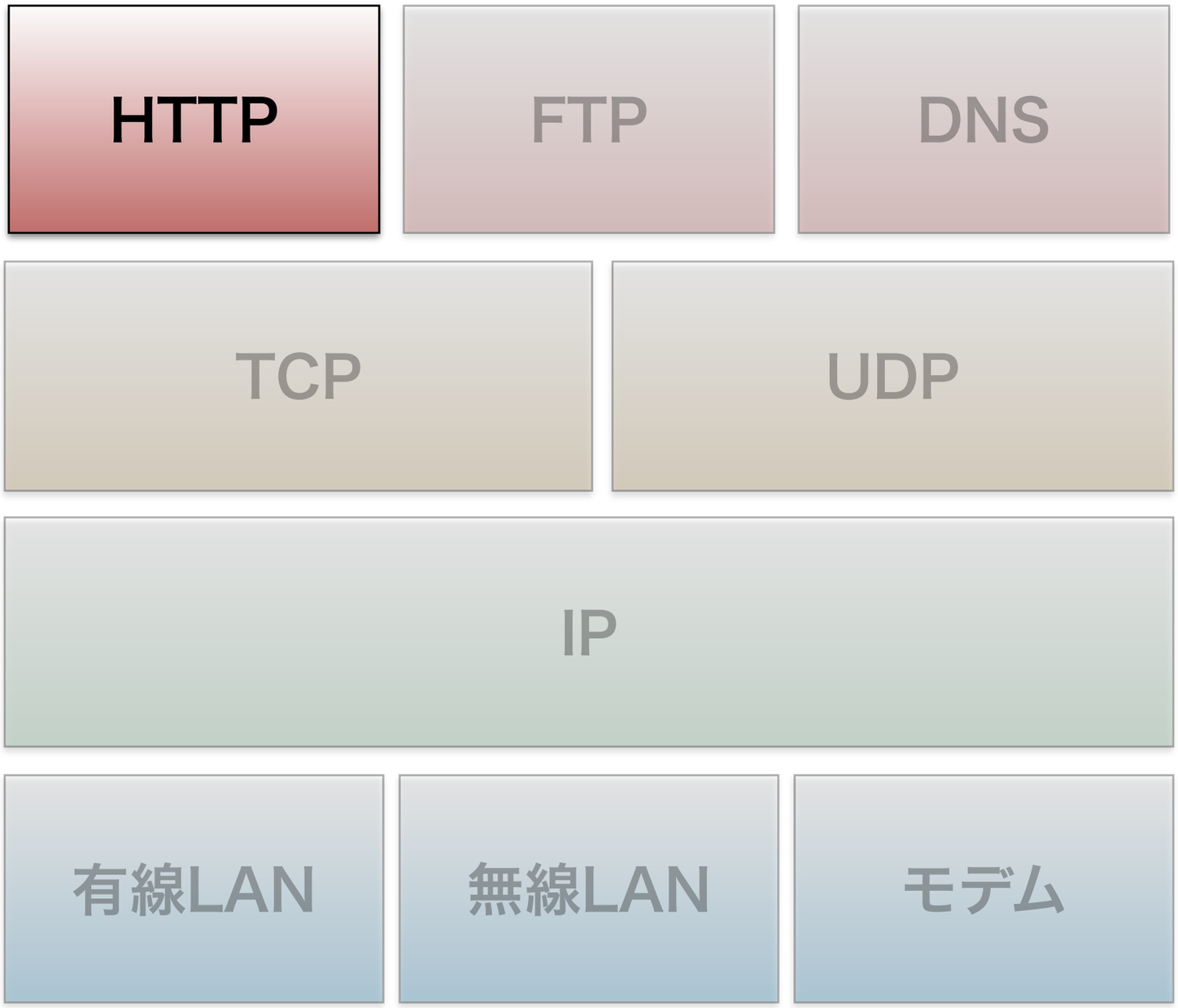
D. example.comのcomはトップレベルドメインである

ネットワーク・サーバ関連技術

- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- リバースプロキシ
- データベース

- HTTP
- DNS
- DNSレコード
- whois情報

HTTP



HTTPの通信手順(1)

リクエスト

GET **/index.html** HTTP/1.1

Accept: image/gif, image/jpeg, */*

Accept-Language: ja

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (Compatible; MSIE 6.0; Windows NT

Host: **www.example.com**

Connection: Keep-Alive

<空行>

<メッセージボディ>

リクエスト行

リクエストメソッドとHTTPのバージョン

ヘッダ

ブラウザ情報や接続情報など

メッセージボディ

POSTメソッドの場合などに使用

レスポンス

HTTPの通信手順(2)

リクエスト

レスポンス

レスポンス行
レスポンスコードとHTTPのバージョン

ヘッダ
サーバ情報や最終更新日時など

メッセージボディ
HTMLや画像などリソース本体

```
HTTP/1.1 200 OK
Date: Sun, 8 Aug 2015 12:34:56 GMT
Server: Apache/2.4.22 (Unix) (Red-Hat/Linux)
Last-Modified: Tue, 07 Jul 2015 12:34:18 GMT
ETag: "1dba6-131b-3fd31e4a"
Accept-Ranges: bytes
Content-Length: 4891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
<空行>
<html>
</html>
```

リクエストメソッド

HTTPクライアント(Webブラウザ)から、
Webサーバへのリクエスト(要求)の種類は複数ある。

GET	**リソースを取得**
POST	**リソースの作成、データの追加**
HEAD	ヘッダ情報のみ取得
PUT	ファイルを転送
OPTIONS	サーバで利用できる機能を取得
DELETE	リソース、データの削除
TRACE	通信経路の取得
CONNECT	SSL通信でトンネル接続する

Webブラウザのアドレスバーにurlを入力してWebページを表示する場合など

問い合わせフォームからの送信や、ログイン時のID/パスワード送信など

GET/POST以外のメソッドは現在ではほとんど使用されていない。
PUT,DELETEなどはPOSTで代用されることが多い。

ステータスコード

レスポンスに含まれる3桁のコード

まず大分類を覚える

1XX	情報
2XX	**成功**
3XX	リダイレクション
4XX	**クライアントエラー**
5XX	**サーバエラー**

次によく使われるコードを覚える

200	**OK**
301	恒久的に移動した
302	一時的な移動
401	認証が必要
403	アクセス権限なし
404	**リソースが存在しない**
500	**サーバ内部のエラー**
503	メンテナンスや過負荷

各Webブラウザのデベロッパーツール内のネットワーク(Firefox,Chrome),タイムライン(Safari)などで確認できる

問題6

HTTPのレスポンスコード500について正しい説明を選択してください。

A. 一時的な移動

B. OK

C. サーバ内部のエラー

D. リソースが存在しない

ネットワーク・サーバ関連技術

- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- リバースプロキシ
- データベース

- Webサーバ
- バーチャルホスト

Webサーバ(1)

http://www.example.com/index.html

を下さい

リクエスト

HTTP

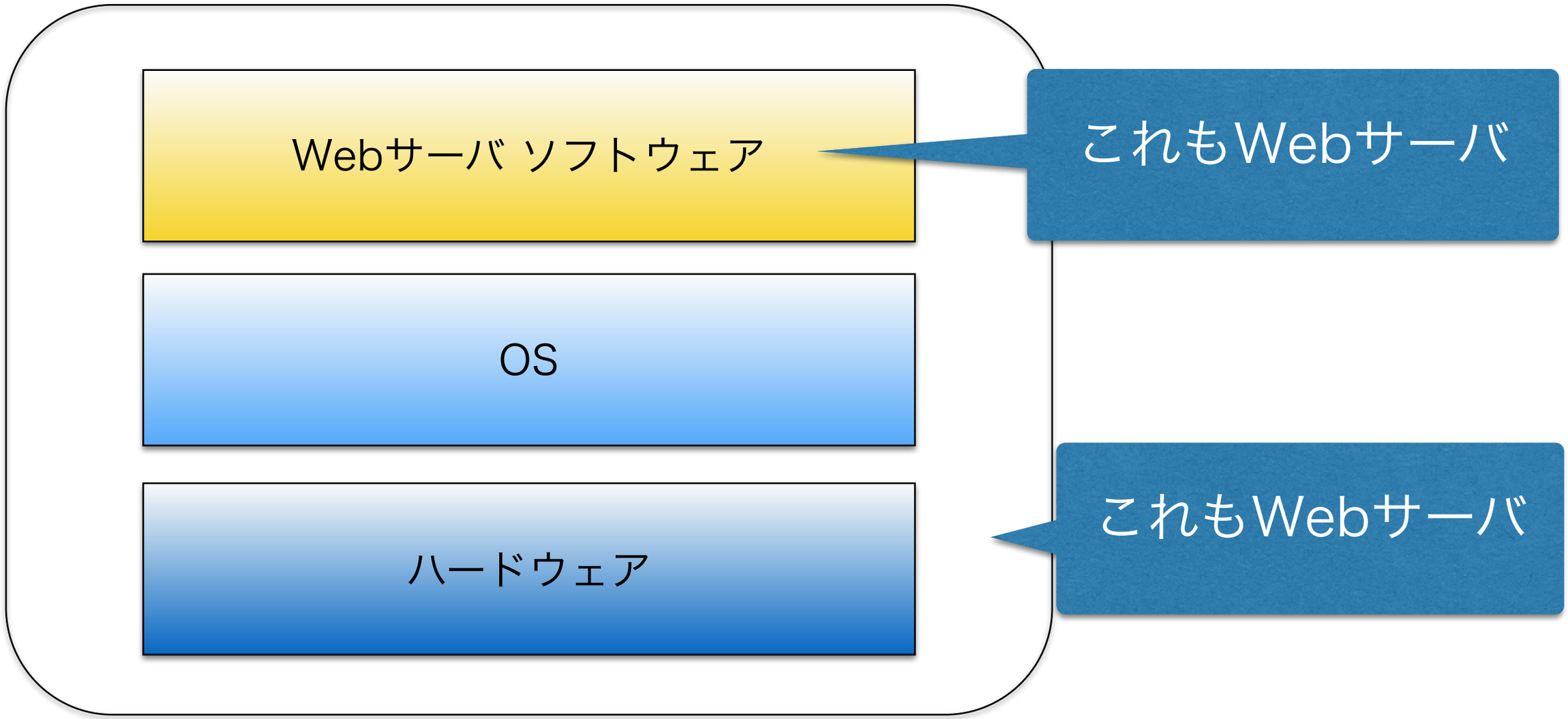
レスポンス

Webクライアント
(Webブラウザ)

index.html

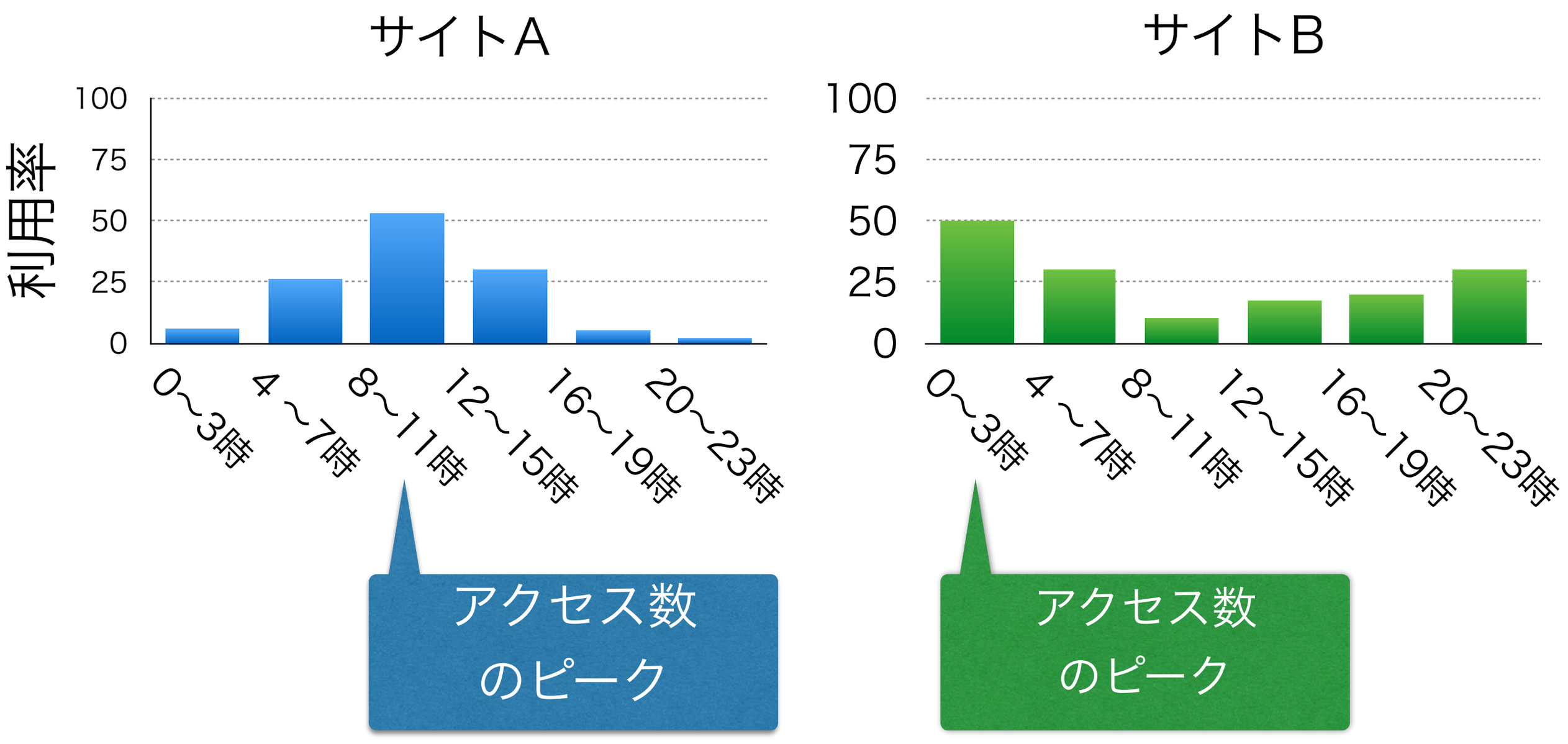
Webサーバ

Webサーバ(2)

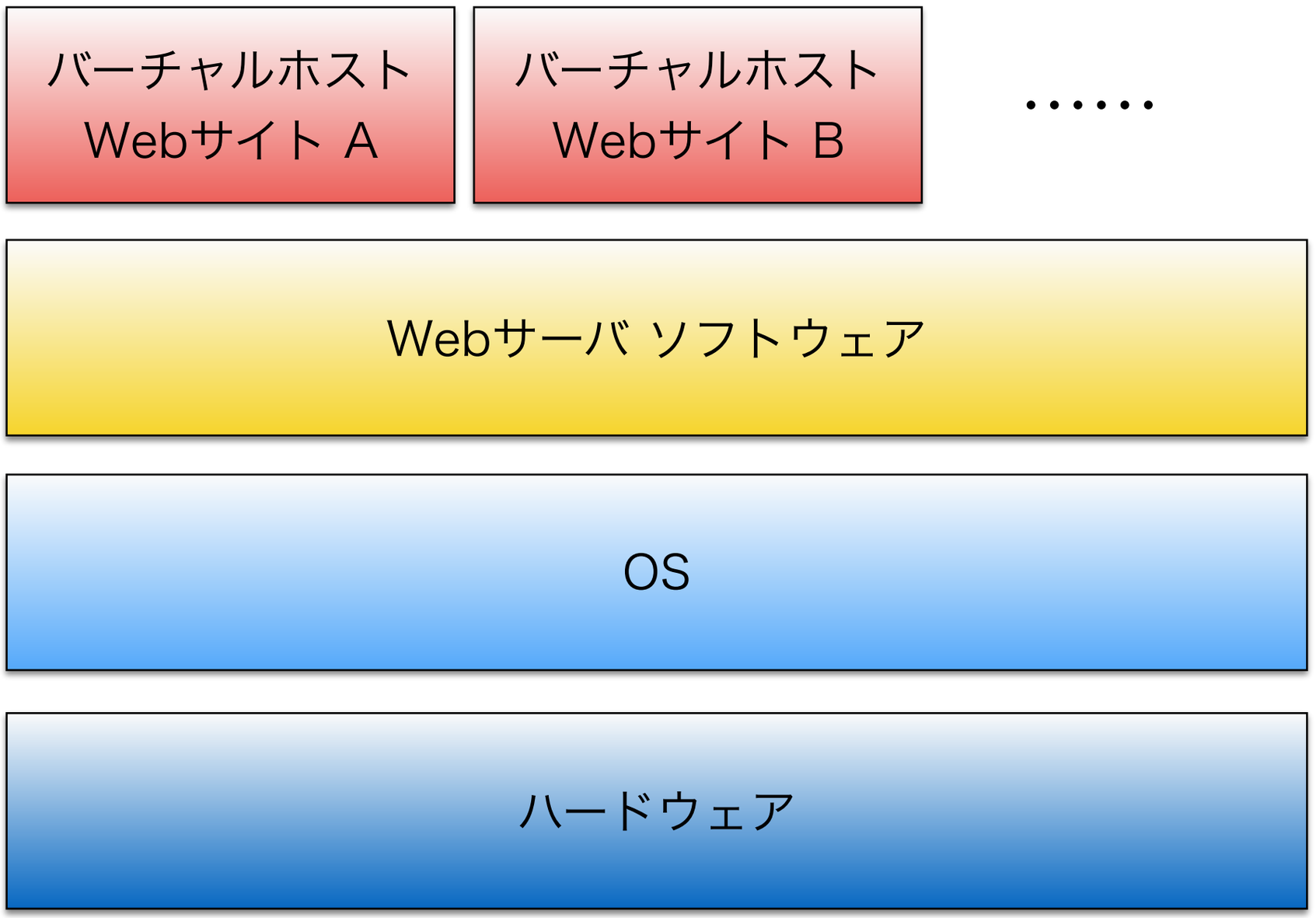


バーチャルホスト(1)

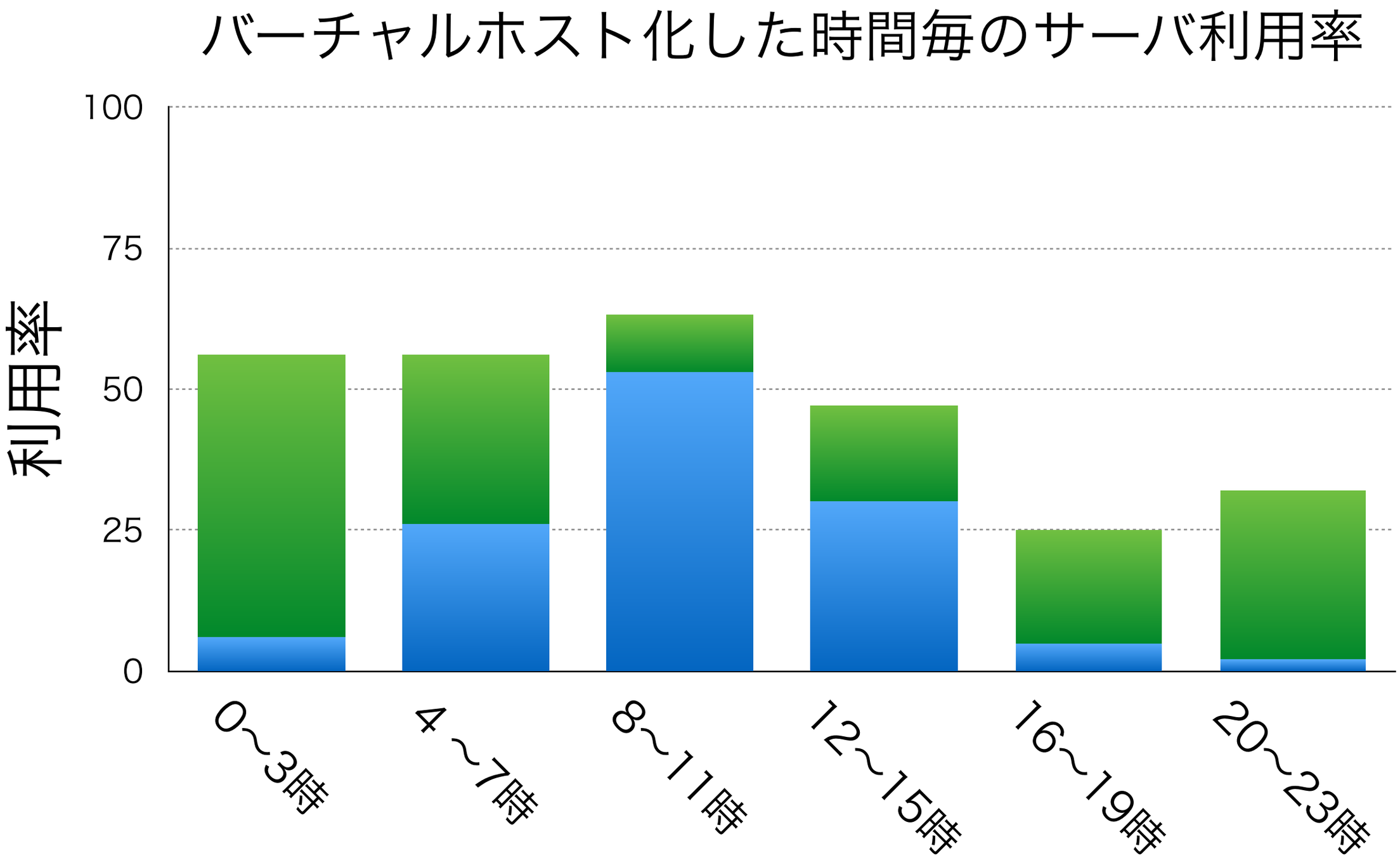
2台のサーバで2つのWebサイトを運用



バーチャルホスト(2)



バーチャルホスト(3)



バーチャルホスト(4)

バーチャルホスト
Webサイト A
siteA.example.com

バーチャルホスト
Webサイト B
siteB.example.com

Webサーバ ソフトウェア

URIやIPアドレスで
どのバーチャルホスト
に繋ぐか判断する

http://siteA.example.com/index.html

バーチャルホスト(5)

メリット

- サーバを無駄なく使用することが出来る
- 新規サイトの立ち上げが簡単

デメリット

- ハードウェア,OSなどにトラブルがおきると一連托生
- 一部のサイトにアクセスが集中すると、他のサイトに影響が出る

問題7

バーチャルホストの特徴として正しいものを選びなさい

A. サーバの運用コストが増大する

B. TCPベースと名前ベースがある

C. 一部のサイトへのアクセス集中が他サイトに影響を与える

D. ハードウェアのトラブルの影響は受けない

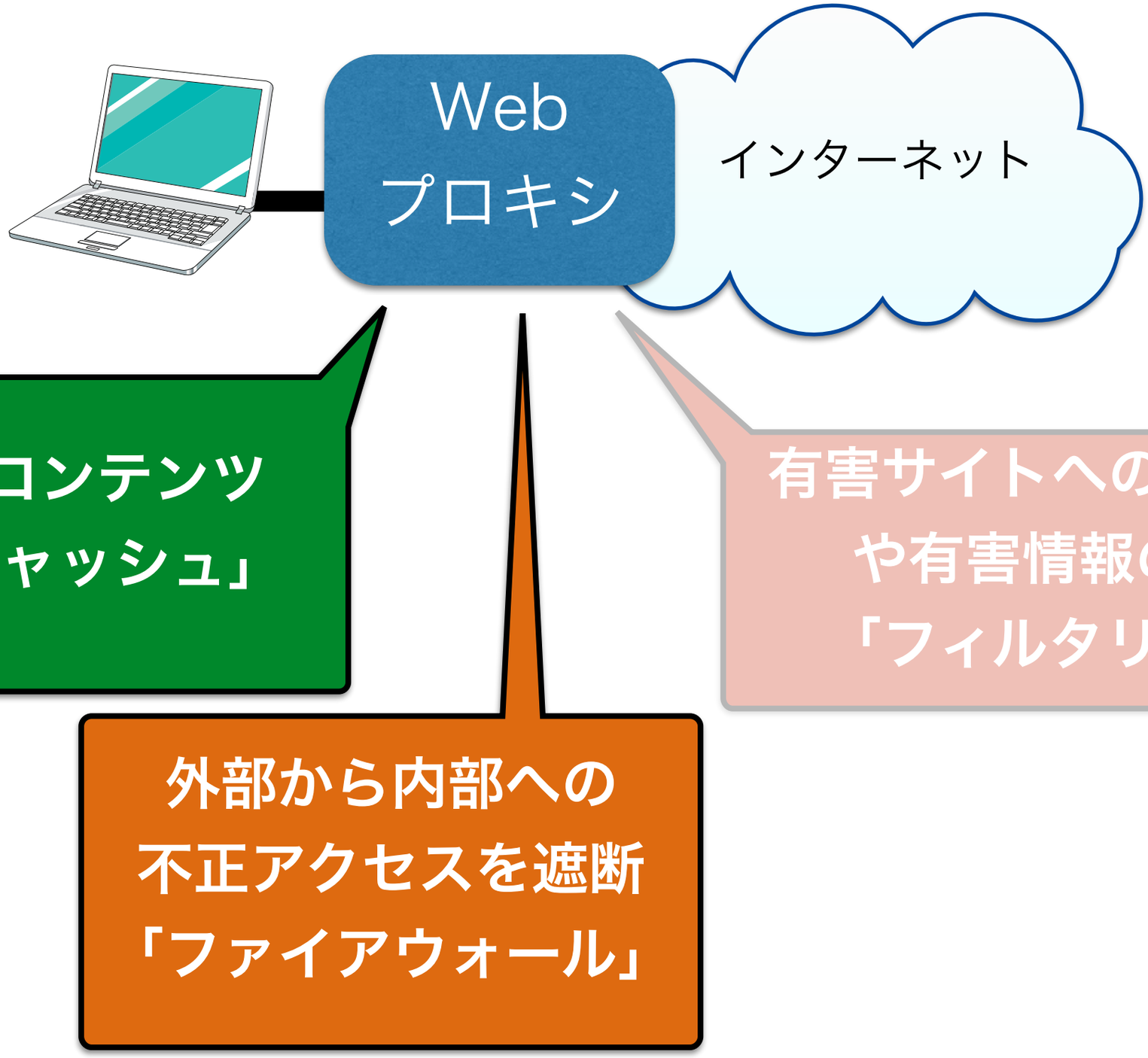
ネットワーク・サーバ関連技術

- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

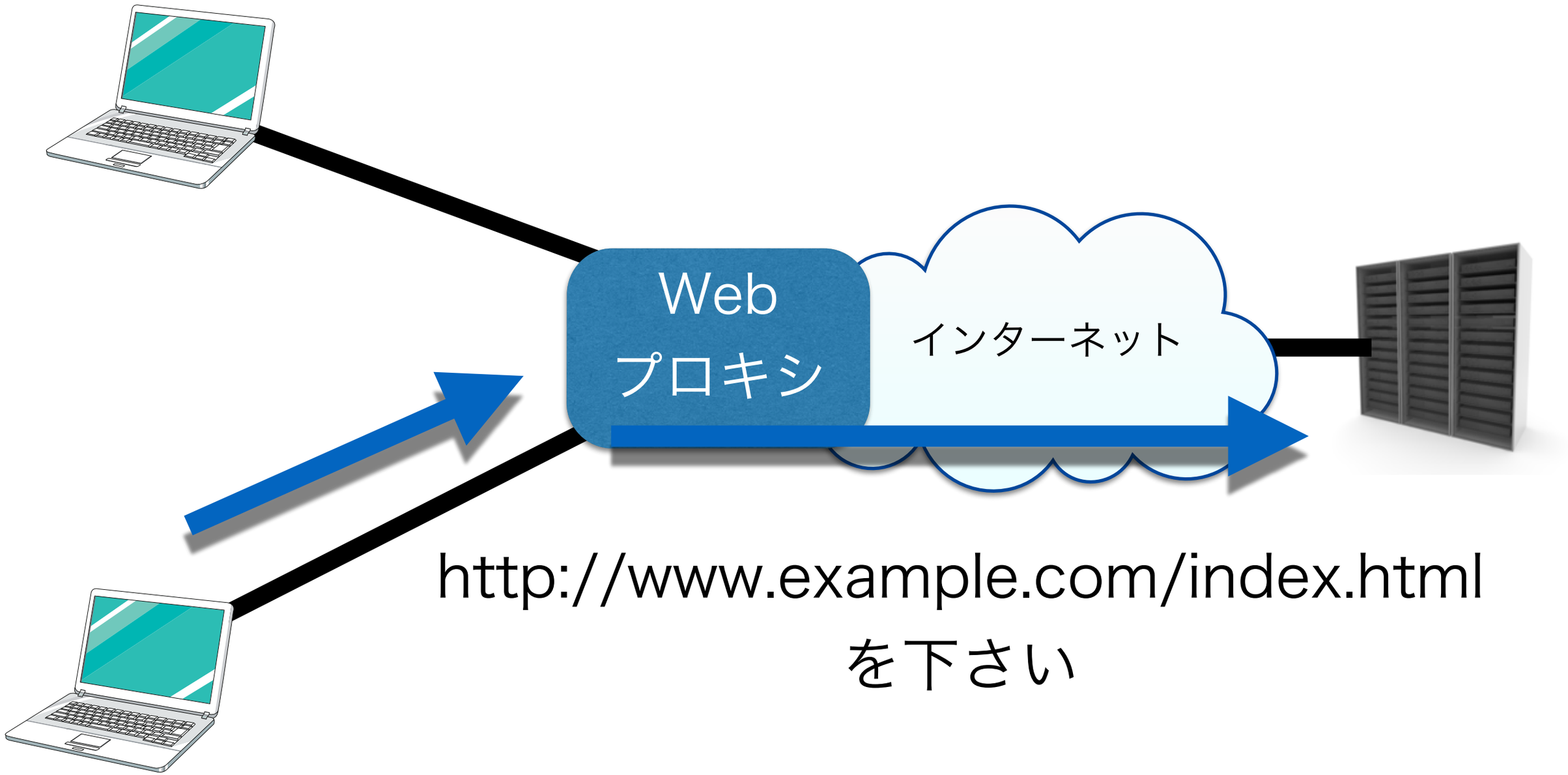
- プロキシ
- キャッシュ
- ファイアウォール
- リバースプロキシ
- 負荷分散

プロキシ

Webプロキシ

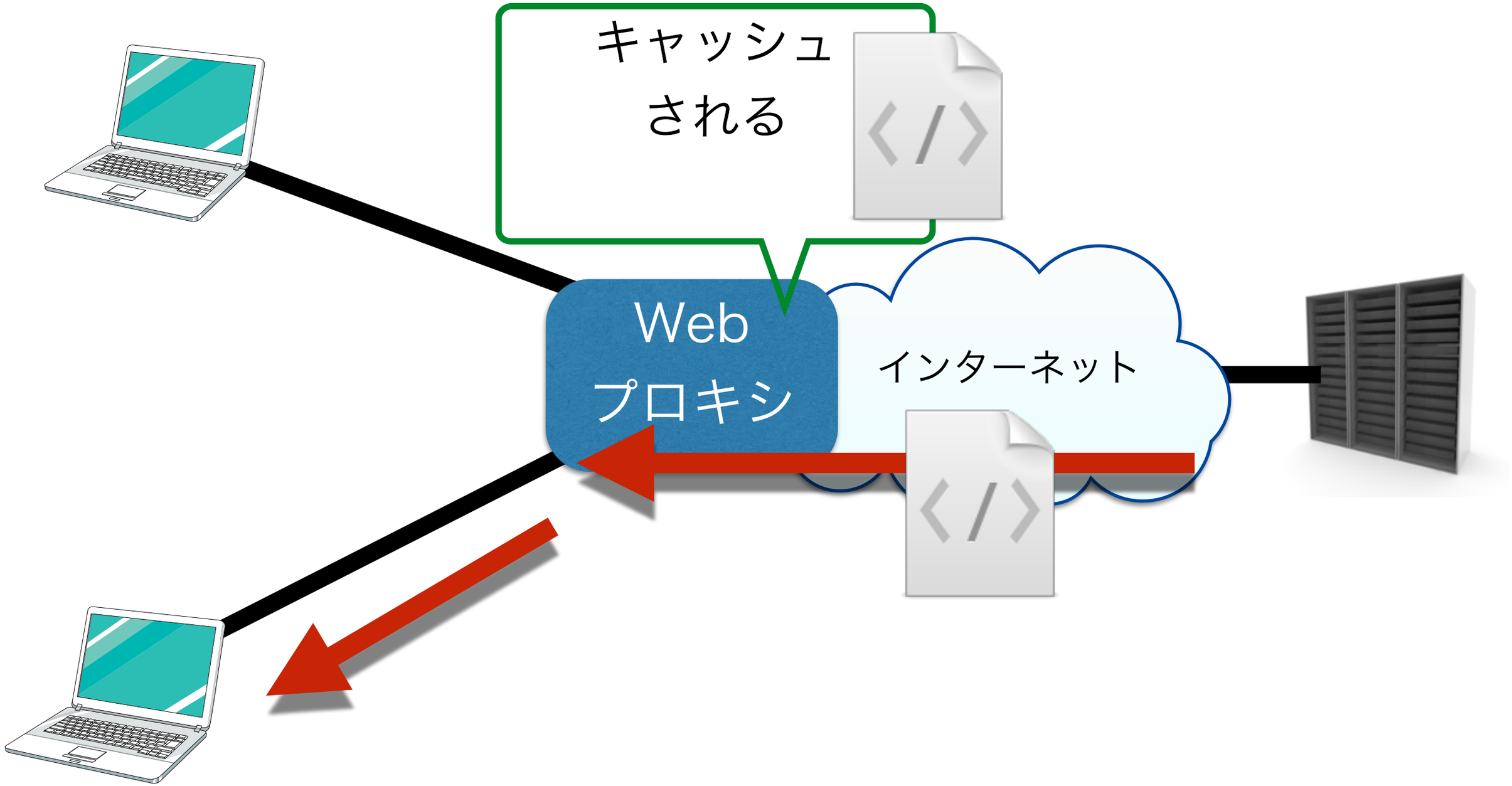


キャッシュ(1)

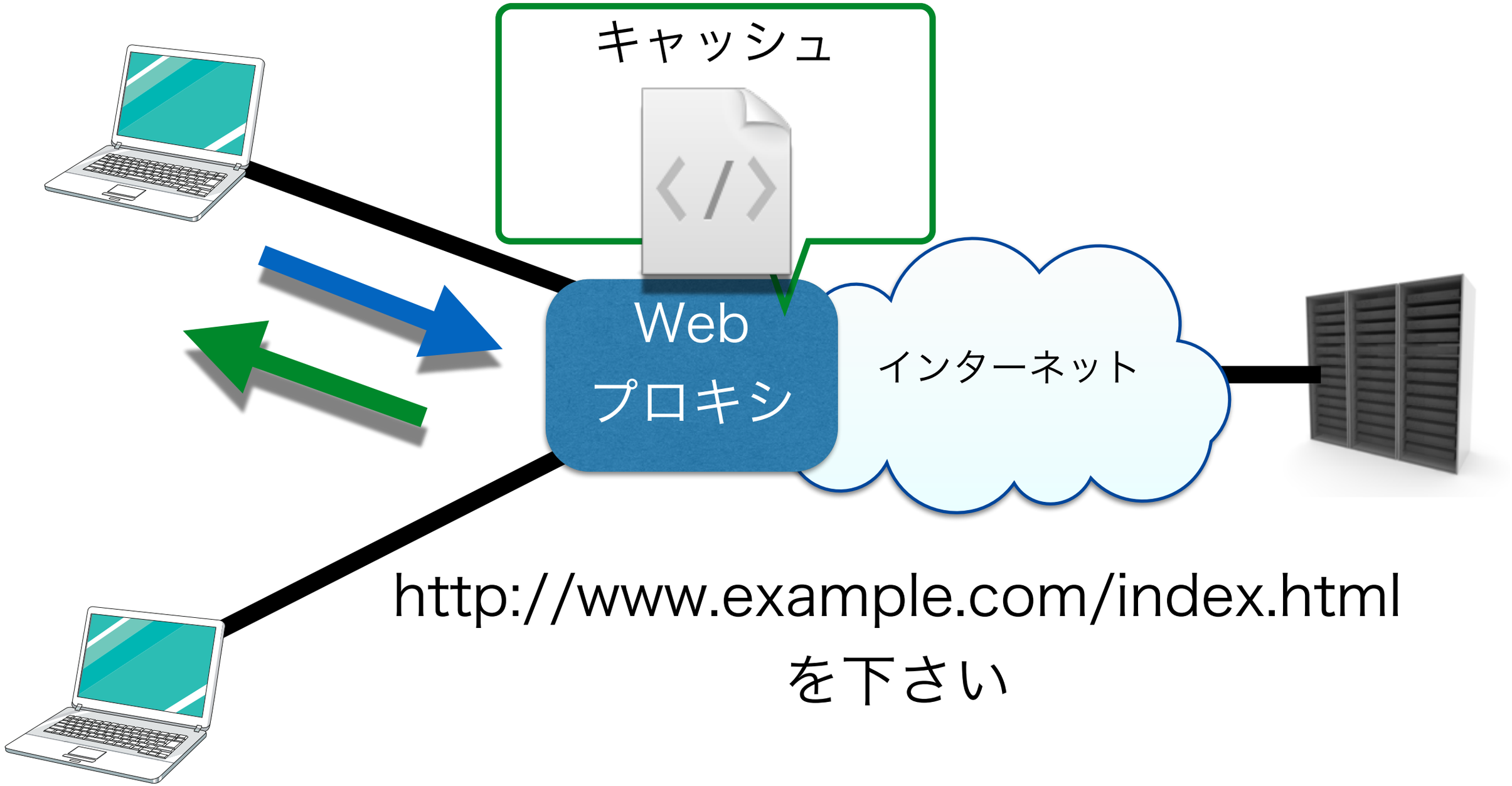


http://www.example.com/index.html
を下さい

キャッシュ(2)

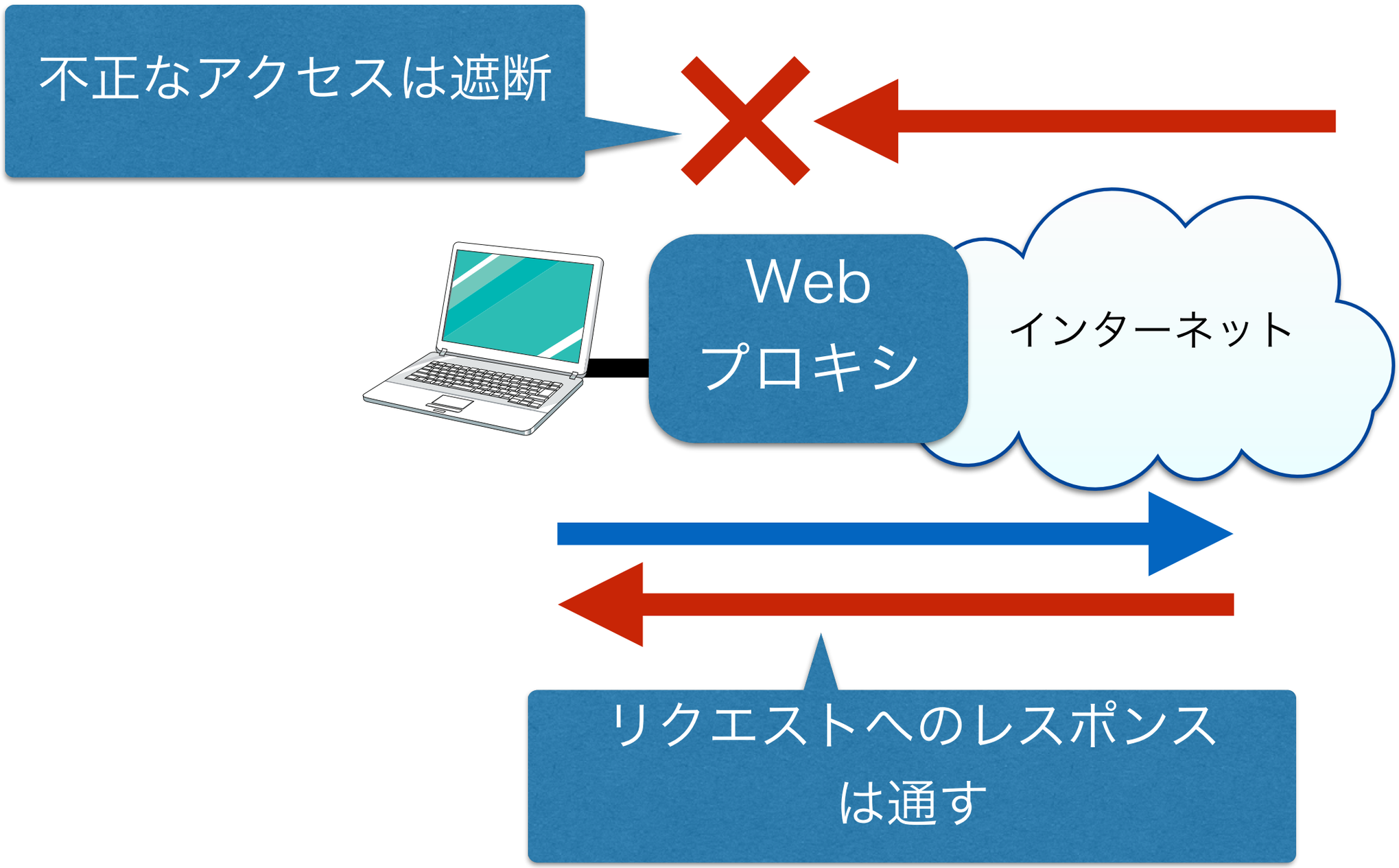


キャッシュ(3)

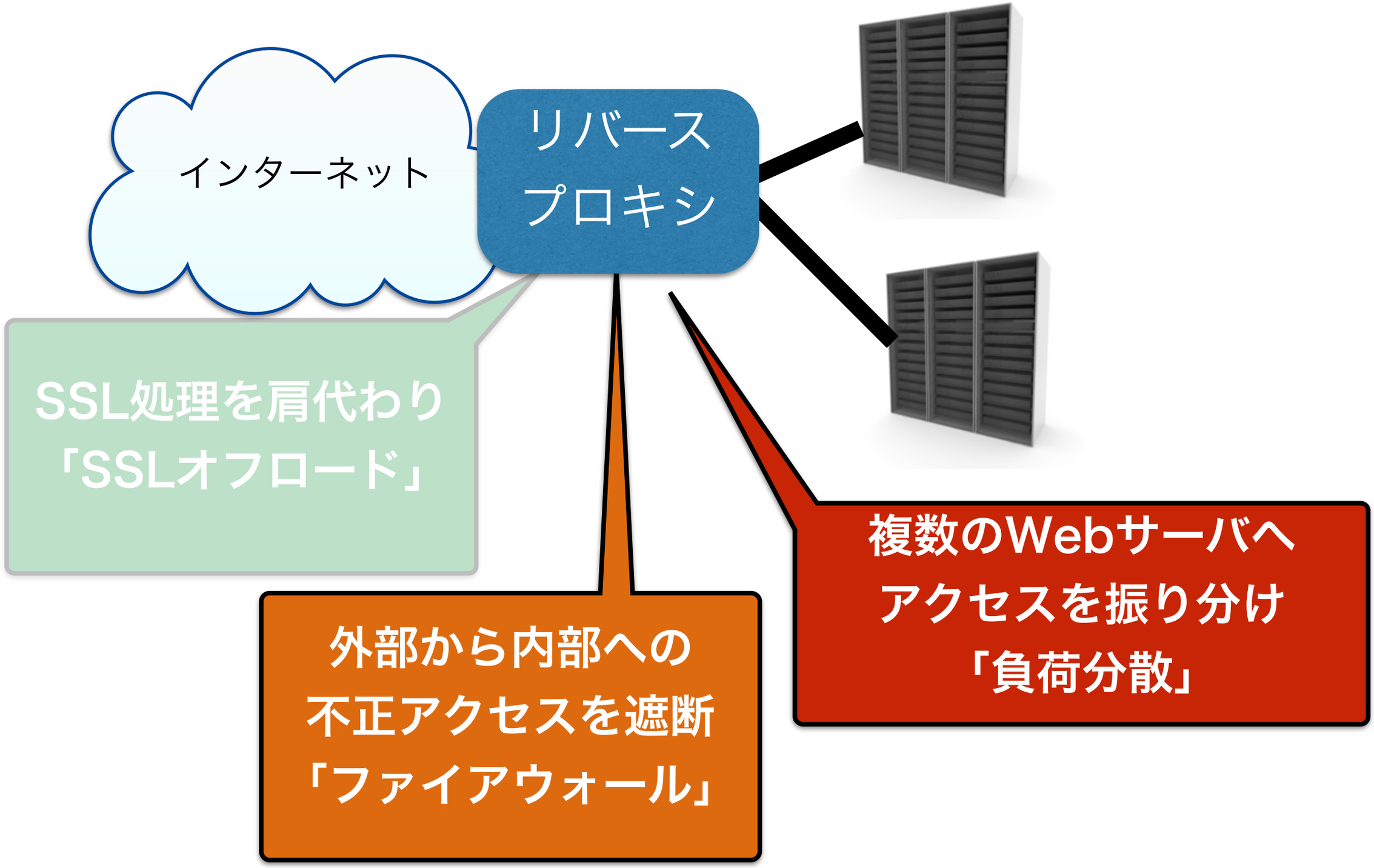


http://www.example.com/index.html
を下さい

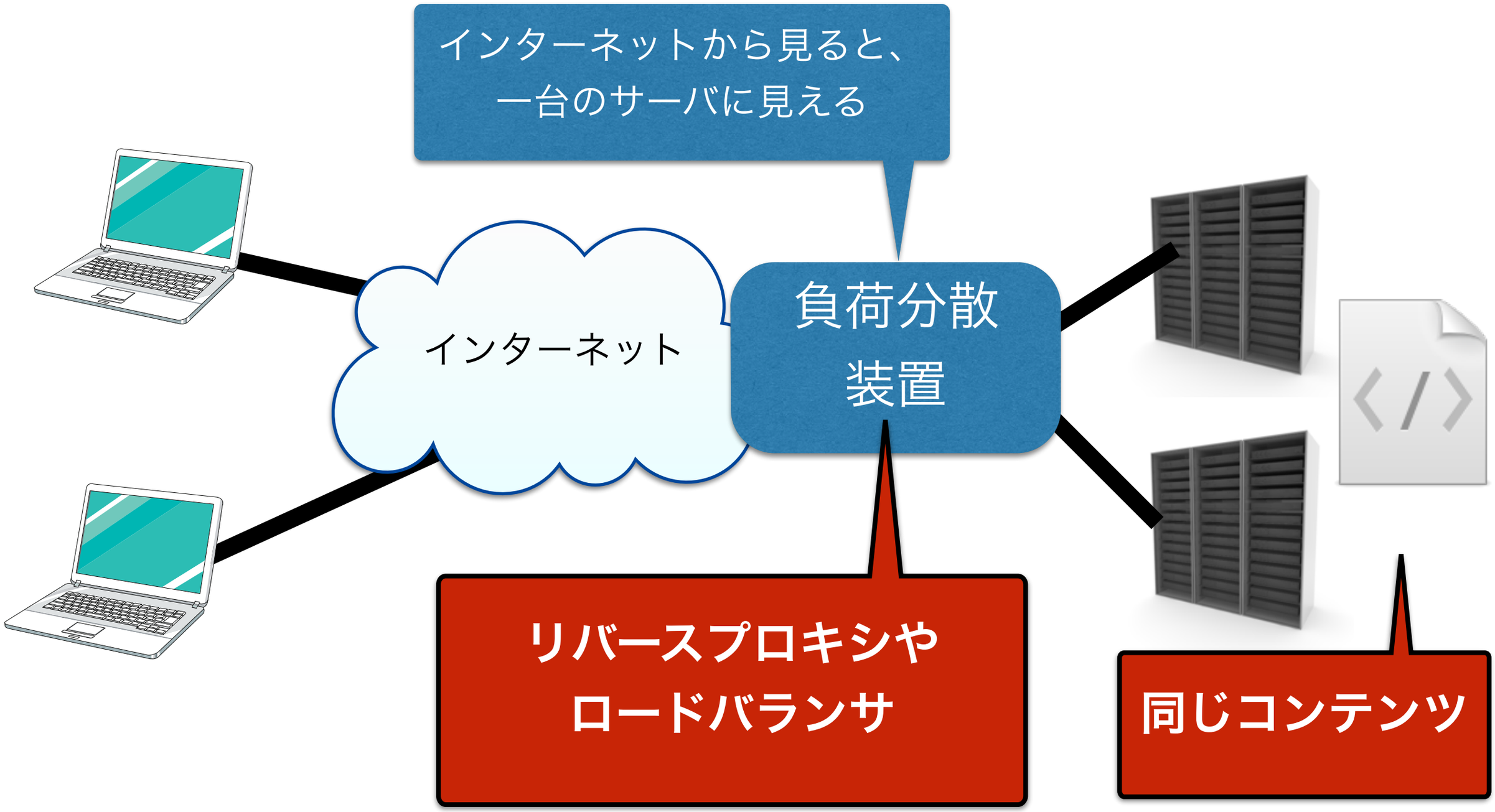
ファイアウォール



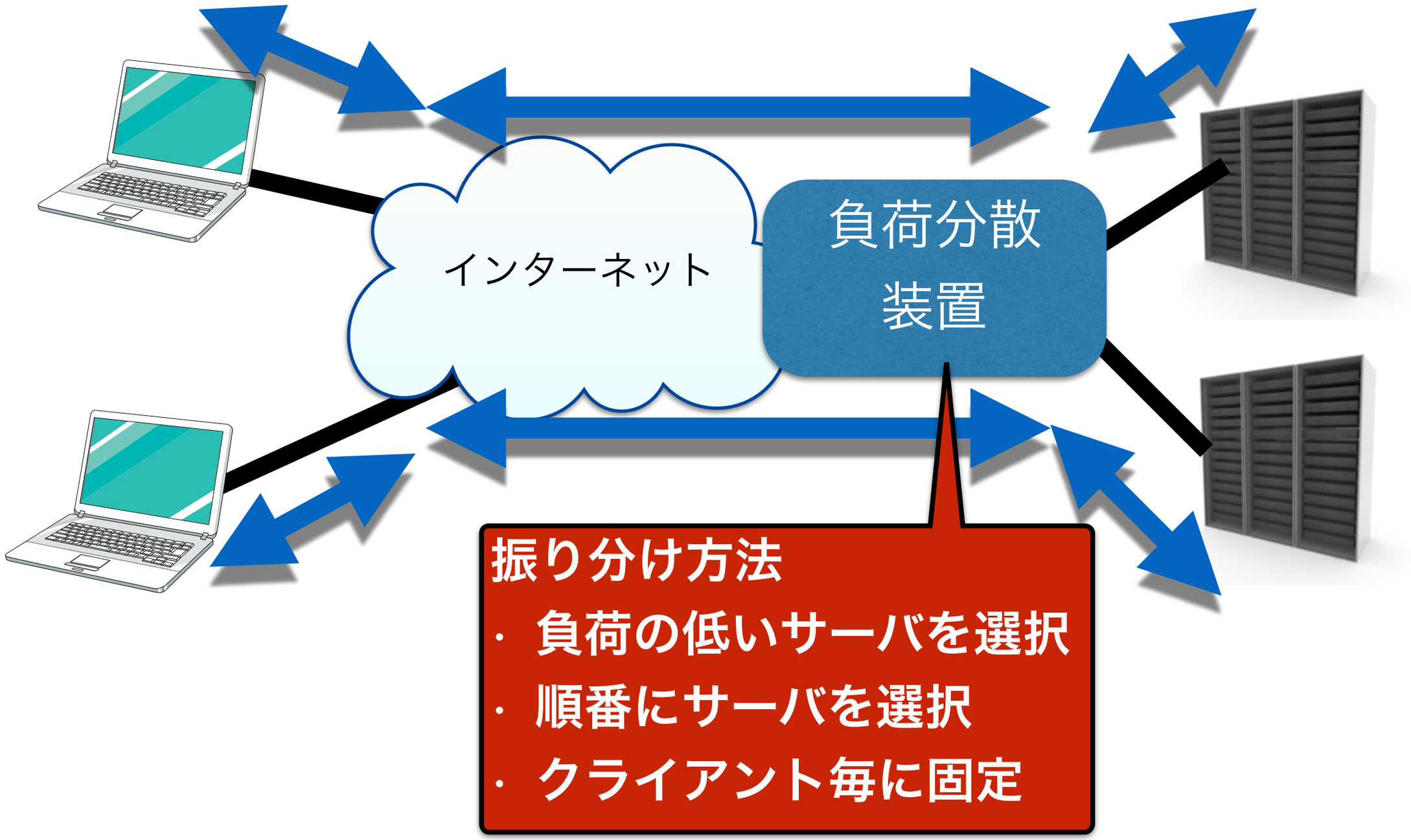
リバースプロキシ



負荷分散(1)



負荷分散(2)



問題8

負荷分散の特徴で間違っているものを選びなさい

A. 外部からは1台のサーバに見える

B. 不正なアクセスを遮断する

C. 順番にサーバを選択する方法をラウンドロビンと言う

D. リバースプロキシが使用されることもある

ネットワーク・サーバ関連技術

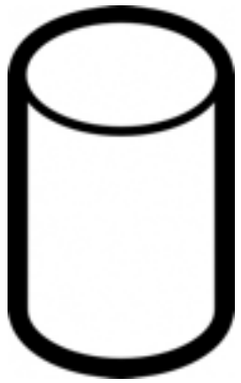
- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

- データベース
- SQL
- CMS
- MVCアーキテクチャ

データベース

Data Base Management System

データの蓄積　を管理する仕組み　略してDBMS



システム構成図などでは、
筒状のアイコンで表されます

- たくさんのデータを効率的に管理する
- データの整合性などを保証する
- データの処理を抽象的に扱う方法を提供する

リレーショナルデータベース

- DBMSのうち、関係代数を元に作られたものをリレーショナルデータベース(RDBMS)と言う

- データは表の形式で扱われる

カラム名(列名)

テーブル(表)

member (会員テーブル)

id	name	sex	age	type
1	Suzuki	M	75	1
2	Ohnuma	F	30	2
3	Nojima	M	64	3
4	Shimada	M	47	2
5	Komine	F	63	1

カラム(列)

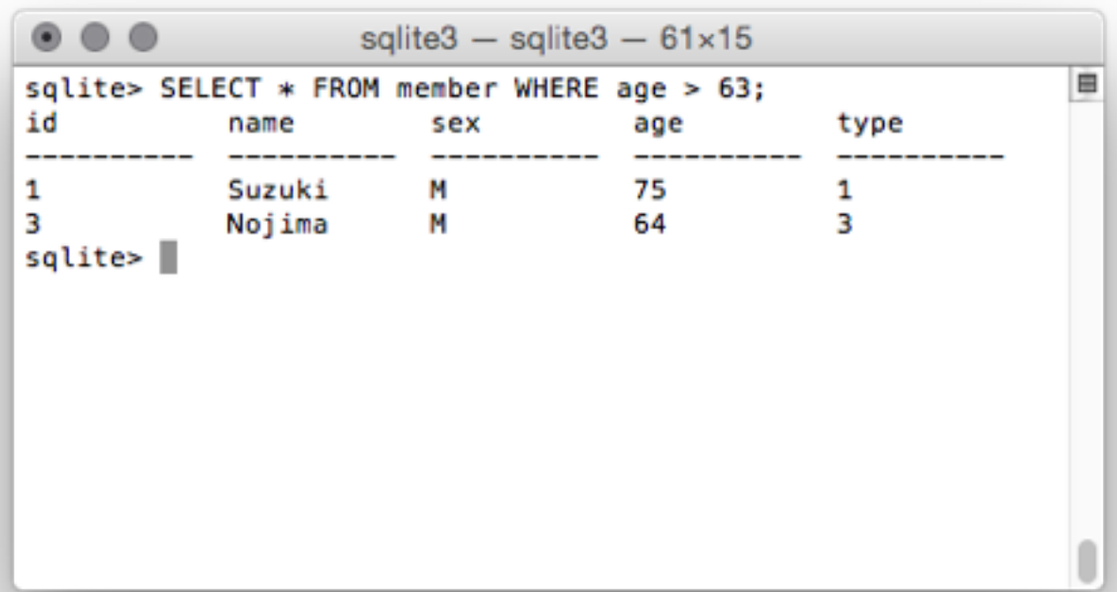
レコード(行)

ＳＱＬ

- リレーショナルデータベースを操作するための言語
- 結果を得るための条件を記述する
- ISOで規格化されているため、RDBMS製品間である程度互換性がある

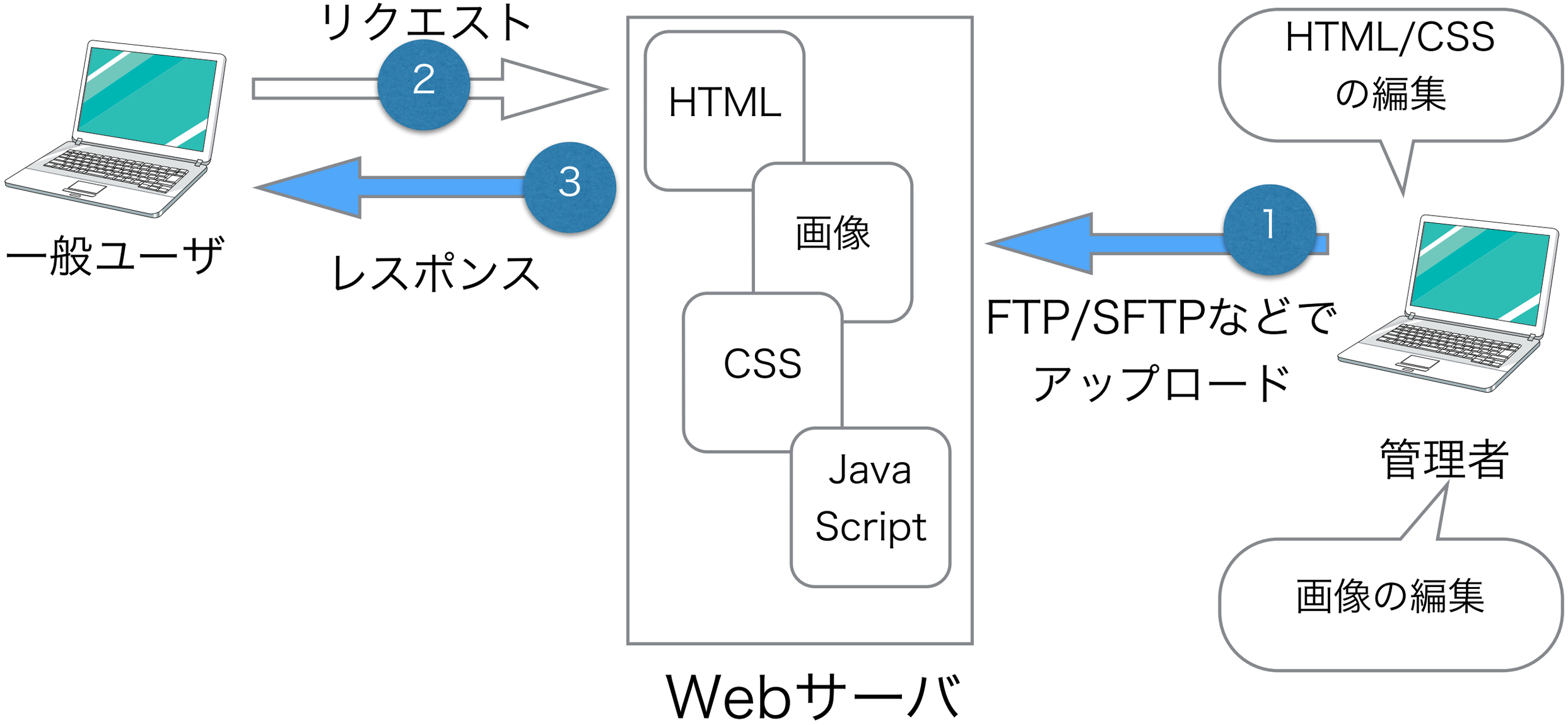
例) 63歳より年上のレコードだけを選択する

SELECT * FROM member WHERE age > 63;



CMS(Contents Manage System)

一般的なWebページの更新方法



CMS(Contents Manage System)

Blogの例

一般ユーザ

リクエスト

5

8

ブログページの
HTML

PHPなどで書かれたプログラム

HTMLを生成

PHPなどで書かれた管理画面のプログラム

SQLで検索

6

7

記事の
コンテンツ

データベース

管理者

管理画面の
HTML

1

2

Blogの記事
を投稿

SQLで追加

3

4

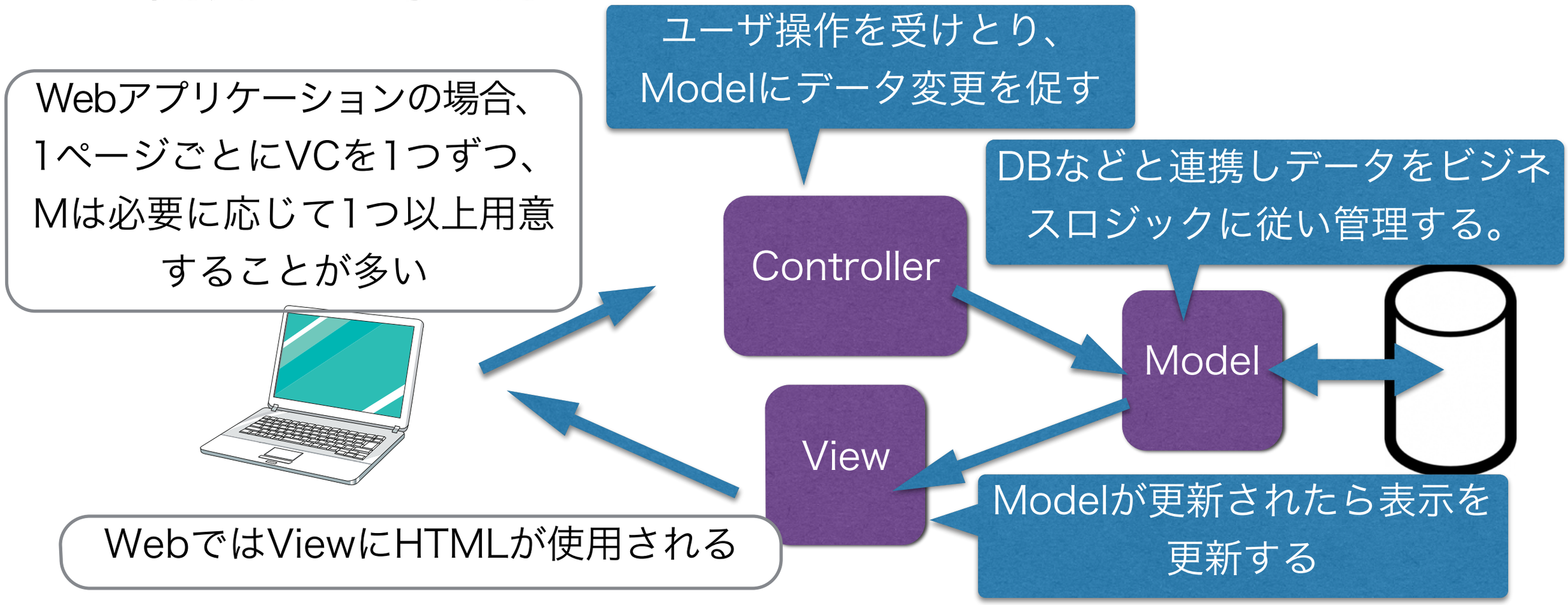
追加した結果

Webサーバ

Webブラウザ上の管理画面で、記事や画像などの**コンテンツ**を編集/管理できる。

MVCアーキテクチャ

- アプリケーションをM(**モデル**)V(**ビュー**)C(**コントローラ**)の3タイプのモジュールに分割して、アプリケーションの変更や応用に強いアプリケーションを開発する考え方



問題9

SQLに関する説明で間違っているものを選びなさい

A. データベースを操作するための言語である

B. 各データベース製品間で互換性は全くない

C. 機能によってDML,DDL,DCLなどに分類される

D. 検索機能はSELECTを使用する

Web関連技術

ネットワーク・サーバ関連技術
- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

試験範囲、頻出ポイント
- 試験概要
- 試験範囲
- 頻出ポイント

Web関連技術
- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

Web関連技術

- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

- JavaScript
- Ajax
- DOM

JavaScriptとは

- JavaScriptとは、通常Webブラウザ上で動作する**プログラム言語**です。
- HTML+CSSだけのWebページと、HTML+CSS+JavaScriptを使ったWebページの最大の違いは、**ユーザ操作や状況に応じて**表示を変えられる点にあります。

ECMA Script

- JavaScriptはWebブラウザごとに異なる実装が採用されています。なので微妙な差異があります。

- 国際的な規格としてはECMAという標準化団体が**ECMAScript**という名称で規格化しています。

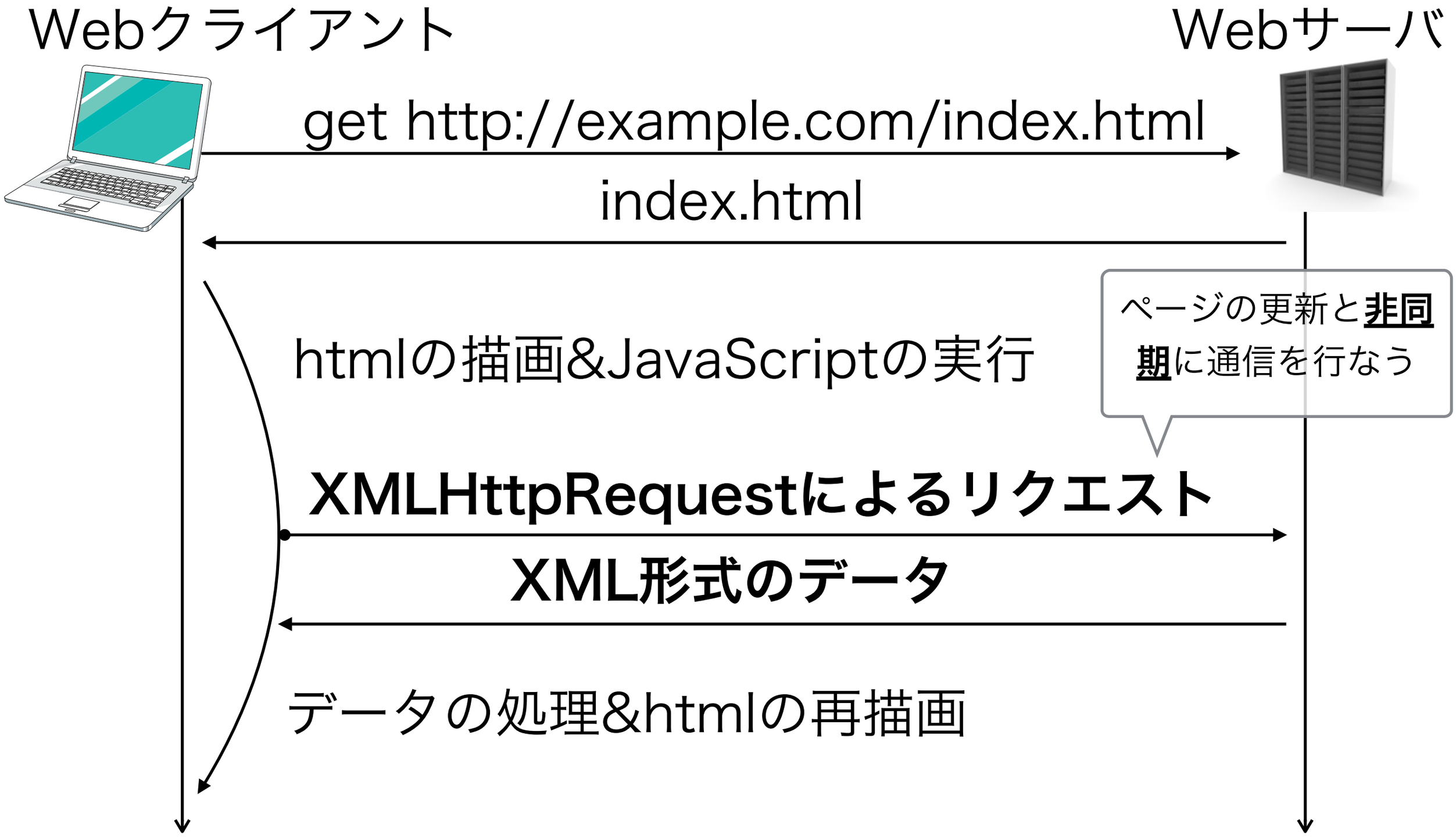
- 試験には出ませんが、現在の最新規格はバージョン5.1で、バージョン6が策定中です。

- Adobe Flashで使用されているActionScriptもECMA Scriptの派生的なプログラム言語です。

Ajax

- JavaScriptは公開されて約20年程経ちますが、現在のように注目される切っ掛けとなったのが、2005年頃に出てきたAjaxという概念です。
- Asynchronous JavaScript + XMLの頭文字を取って、Ajaxと名付けられました。
- Asynchronous = **非同期**の
- XML = HTMLと似たデータ記述方法

Ajaxの流れ



問題10

Ajaxの特徴として正しくない選択肢を選んでください

A. ページの表示と非同期にサーバと通信を行なう

B. 必ずページ全体をリロードする

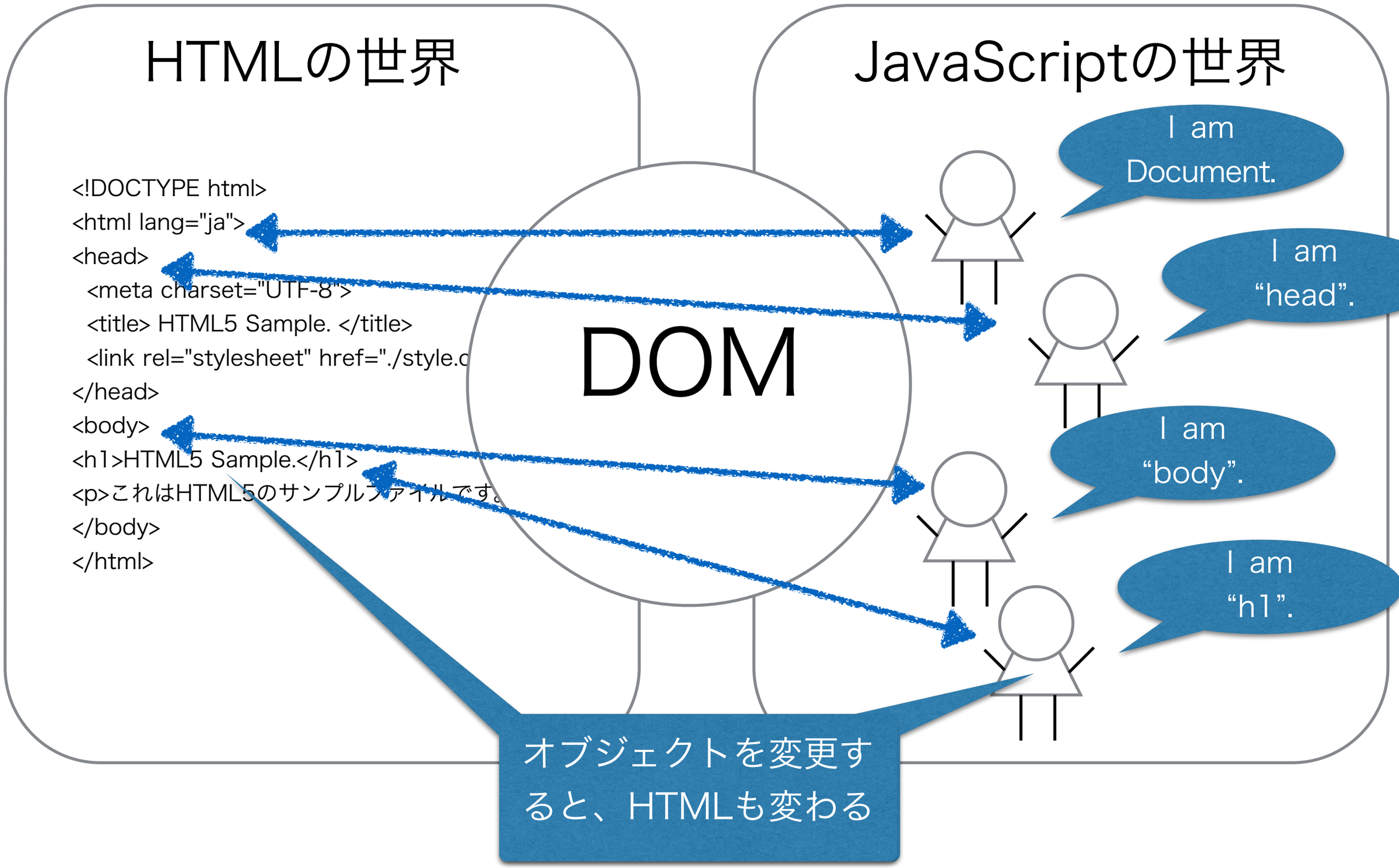
C. サーバとの通信データフォーマットはXMLである

D. JavaScriptを使用してHTML要素を変更する

DOM

- Document Object Model
  - Document = Webページ
  - Object = JavaScriptで処理を行なう単位
  - Model = 考え方、仕組み
- Webページをオブジェクトという単位に分割して JavaScriptから扱う仕組み

DOMは2つの世界の橋渡し



問題11

DOMについての説明で間違っている選択肢を2つ選んでください。

A. 基本的にHTML要素とオブジェクトは1対1で対応する

B. W3Cで策定され、標準化番号はMS-09である

C. DOMに対する変更はリロードしなくても反映される

D. DOMのオブジェクトの親オブジェクトは多くても1つである

Web関連技術

- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

- BMP
- PNG
- JPEG
- GIF
- インタレース

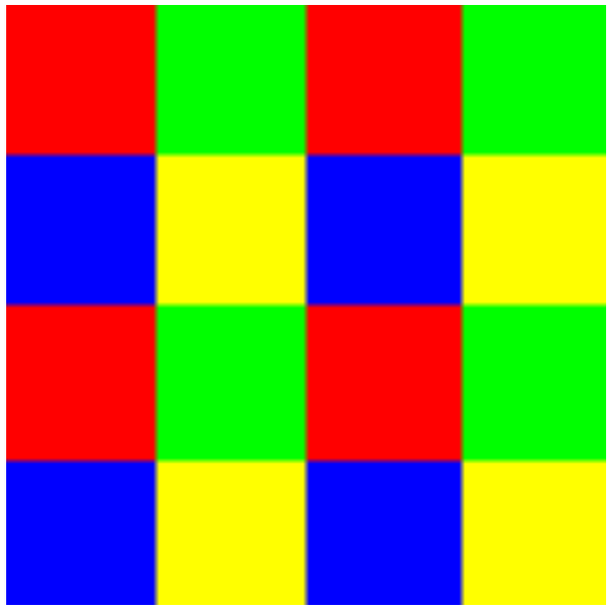
画像の保存形式

各保存形式の特徴となる要素

- 扱える色の数
- 圧縮方式
- 透明処理
- アニメーション
- インタレース

扱える色の数

フルカラー



#FF0000,#00FF00,#FF0000,#00FF00
#0000FF,#FFFF00,#0000FF,#FFFF00
#FF0000,#00FF00,#FF0000,#00FF00
#0000FF,#FFFF00,#0000FF,#FFFF00
ピクセル毎にRGB(A)値を持つ

インデックスカラー

1,2,1,2
3,4,3,4
1,2,1,2
3,4,3,4
ピクセル毎にパレットの
インデックス値を持つ

パレット

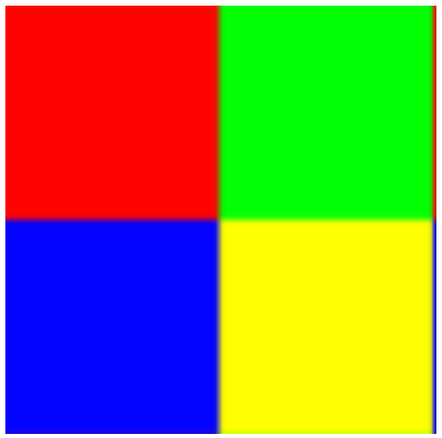
1	#FF0000
2	#00FF00
3	#0000FF
4	#FFFF00

パレットの数が
最大色数

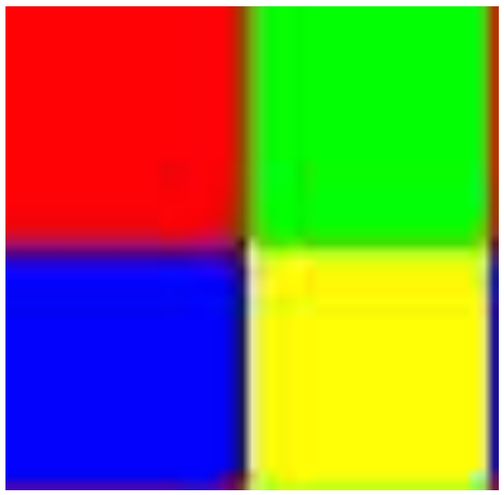
圧縮方法

- 元データを細ぎれにして、同じ部分をまとめることで、データ量を減らす。

- 圧縮を復元(伸長)すると、元のデータと同じデータになる可逆圧縮と、元のデータと等しくならない非可逆圧縮(データを間引くことでデータを減らす)がある。



元データ



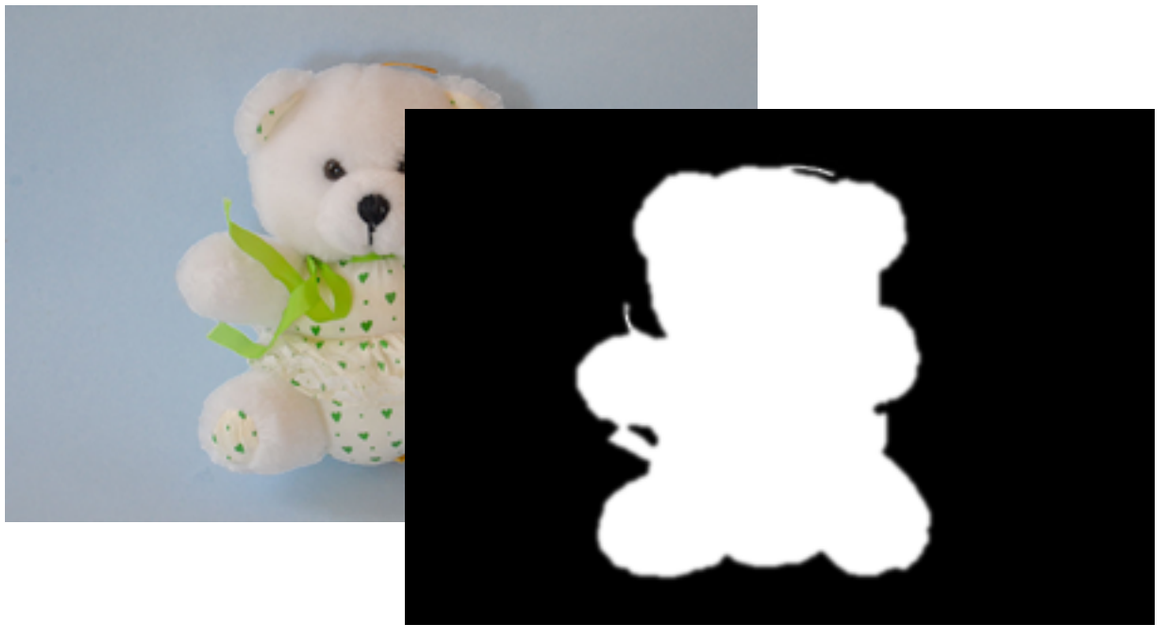
非可逆圧縮の復元データ

透明処理(1)

透明色

ピクセル毎に
透明にする/しないを選択する
半透明にはできない。
境界線がはっきりする。

アルファ値



ピクセル毎に透明度を指定できる。
境界を馴染ませられる。
Photoshopのレイヤマスクに似ている。

透明处理(2)

GIF

PNG

アニメーション

- パラパラマンガのような形で、簡易的なアニメーションを扱える。

- 試験範囲の形式の中では、GIFだけが可能。

- 一応、PNGを拡張したAPNGとMNGやJPEGに関連するMotionJPEGという規格がある。(Webではほとんど使われていない)

インタレース

- ファイル保存時にファイル先頭に飛び飛びの画素、後ろに残りの画素を保存する。

- Webブラウザは届いたデータを使って徐々に表示させることで、ユーザの体感速度を向上させる。

- JPEGには異なる仕組みで同様の効果が得られるプログレッシブJPEGという機能がある。

各形式のまとめ

	圧縮方法	色数	透明化	アニメ	インタレース
JPEG	**非可逆**	**フルカラー** モノクロ	なし	不可	可 (プログレッシブ)
GIF	可逆	**インデックス**	**透明色**	**可**	可
PNG	可逆	**フルカラー** **インデックス**	**アルファ値** **透明色**	不可	可
BMP	なし	フルカラー インデックス	なし	不可	不可

※上図は一般的な使用方法です。規格としては、
上図以外のものもあります。

問題12

イラストをアニメーションさせる場合、どの画像形式を使用すべきか選択してください。

A. PNG

B. Jpeg

C. GIF

D. BMP

Web関連技術

- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

- Base64
- DataURI

Base64(1)

- **バイナリデータ**を表示可能な**テキストデータに変換**する方法。

- ASCIIテキスト(半角英数字+記号)しか扱えないシステム(メールなど)がまだ沢山残っているため必要。

- メールに日本語や画像を含めるためには、ASCIIの印字可能文字の範囲にデータを変換する必要がある

- 変換には**変換表**を使用する。

Base64(2)

Base64 変換表

0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64 変換例

GIFファイルの場合、先頭に”GIF87a”という文字列が埋め込まれています。そのうちの”GIF”をBase64で変換してみましょう。

- “GIF”を2進数で表現 (ASCIIコード)
  →01000111 , 01001001 , 01000110
- 6bitずつに分割 (括弧内は10進表記)
  →010001(17),110100(52),100101(37),000110(6)
- 変換表で変換
  →R0lG

後述のData URIの章で
確認してみましょう

Data URI

- HTML/CSSが読み込む外部ファイルの代わりに、データ(画像、スタイルシート、JavaScriptなど)をHTMLに埋め込むことが出来る機能。

- HTMLに埋め込むことで全体のファイル数を減らし、サーバとの通信回数を少なくすることができる。

Data URIの書式

data:[<MIME-type>]
[;charset=<encoding>][;base64],<data>

使用例 画像を表示する→ ●

```
<img src="
C1hNUCBEYXRhWE1QCD94cGFja2V0ACwAAAAAEAA
QAAACHoQfGceo38CbilHq7jQa9w
+GYieNZZiRqRaxEbcxBQA7" >
```

問題13

Base64についての説明で間違っているものを選択してください。

A. 画像にしか使用できない

B. 64文字でデータを表現する

C. 元データに比べると、データ量は4/3倍になる

D. メール送信にも使用される

Web関連技術

- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ

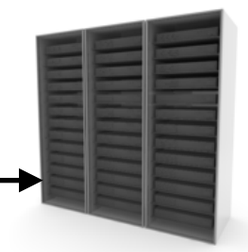
・ディレクトリ・トラバーサル
・SQLインジェクション
・クロスサイト・スクリプティング
・CSRF
・HTTPヘッダインジェクション

ディレクトリ・トラバーサル

Webクライアント

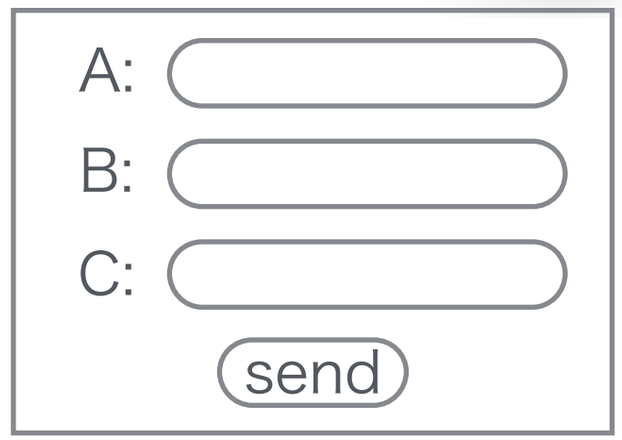
Webサーバ

http://省略/form.php?tmp=**form1.html**

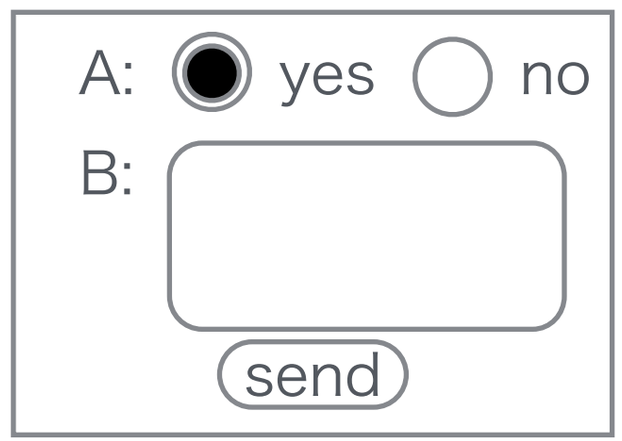


指定されたファイルを
埋め込み

form.php



form1.html



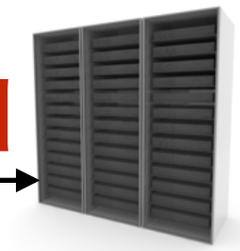
form2.html

ディレクトリ・トラバーサル

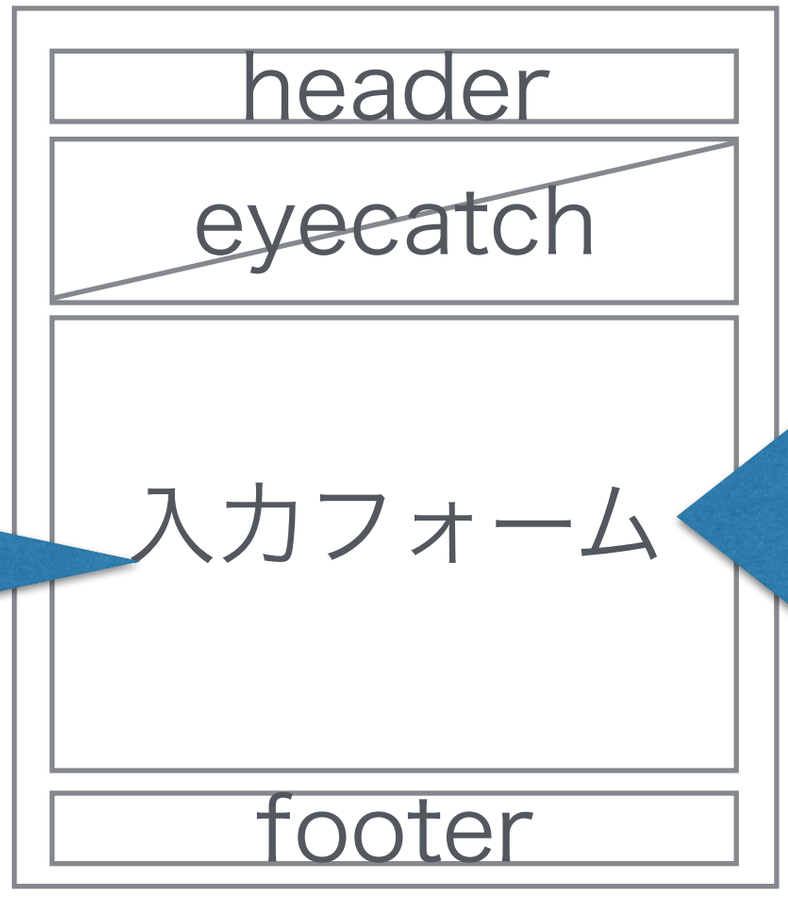
Webクライアント

Webサーバ

http://省略/form.php?tmp=**/etc/passwd**



非公開ファイルの内容が表示され、より悪質な攻撃に繋ってしまう。



form.php

サーバのユーザー一覧ファイル

root:x:0:0:root:/root:/bin/
bin:x:1:1:bin:/bin:/sbin/no
daemon:x:2:2:daemon:/sb

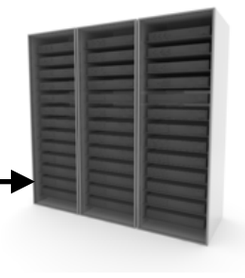
/etc/passwd

クロスサイトスクリプティング

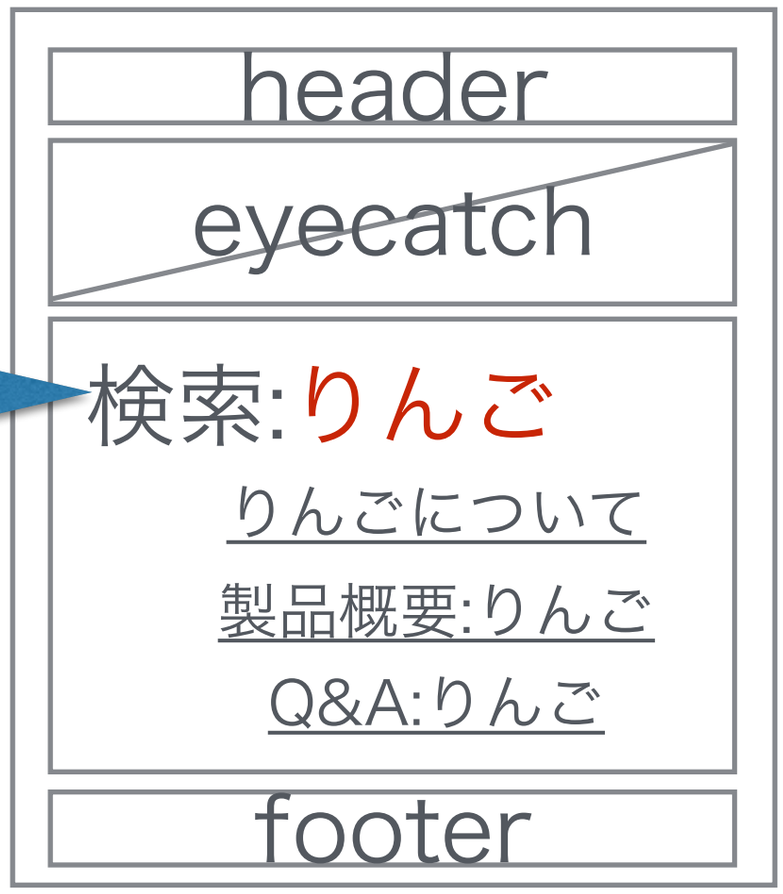
Webクライアント

Webサーバ

http://省略/search.php?key=**りんご**



指定されたキーワードを表示



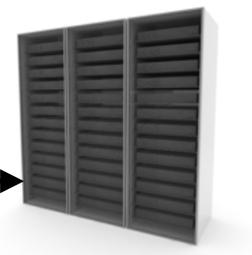
search.php

クロスサイトスクリプティング

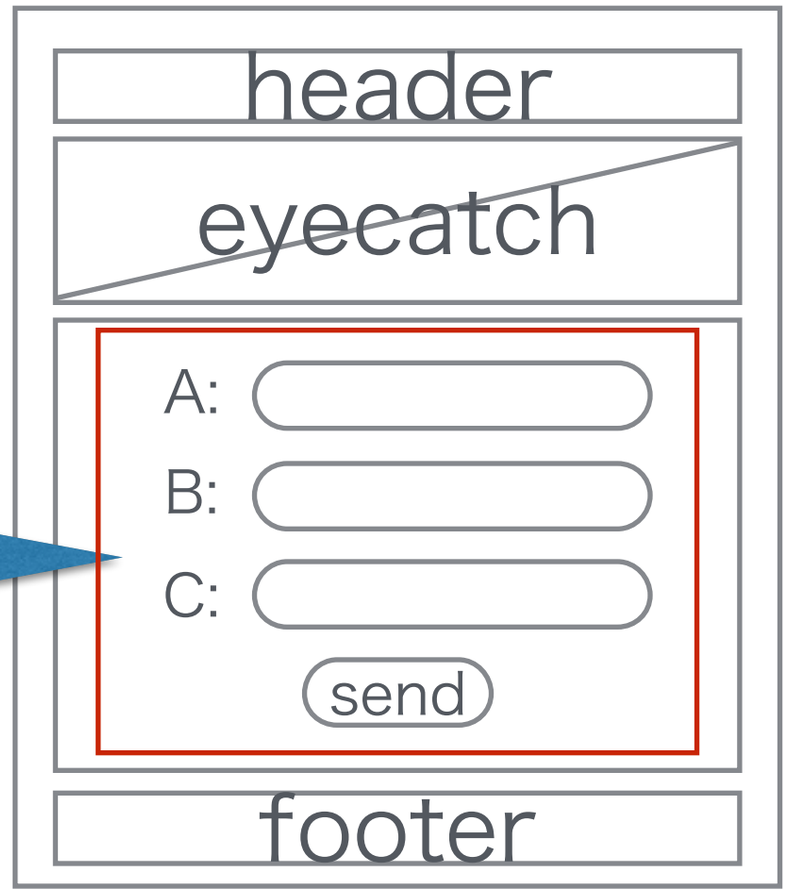
Webクライアント

Webサーバ

http://省略/search.php?key=<form…



指定された<form>タグを
そのまま表示してしまう
と、ニセの問い合わせ
フォームを表示してしまう
(スタイルを操作し、元の
内容を隠すこともできる)



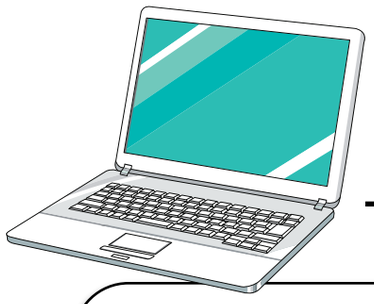
ニセの問い合わせフォームのタグを指定する。
入力データの送信先を、攻撃者のサイトにしておけば、情報は盗み放題。

search.php

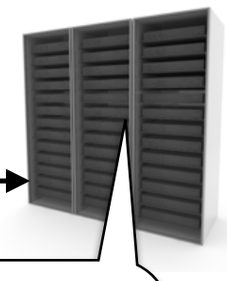
SQLインジェクション

Webクライアント

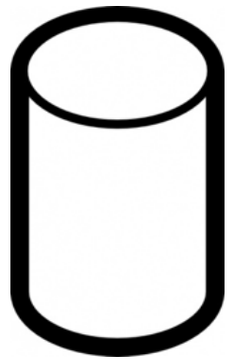
Webサーバ



http://省略/search.php?key=**りんご**



```
SELECT * FROM posts
WHERE text LIKE '%りんご%';
```



search.php

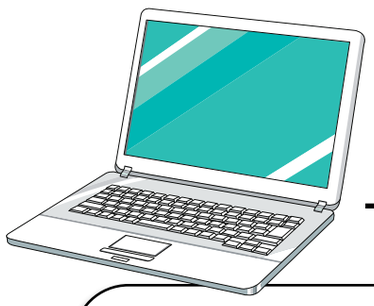
データベース

SQLを使用して、**データベース**から入力されたキーワードを検索

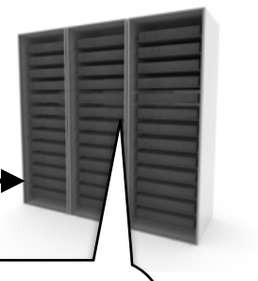
SQLインジェクション

Webクライアント

Webサーバ



http://省略/search.php?key=';DELETE…



SELECT * FROM posts
WHERE text LIKE '%'
;DELETE FROM posts;
SELECT * FROM posts '%%' ;

search.php

データベース

'; で一度命令を閉じて、別の命令を埋め込んでしまう。

HTTPヘッダインジェクション

攻撃者

攻撃用リンク

http://省略/redirect.php?url=**本来のリダイレクト先<改行>Location: htt...**

HTTPヘッダのLocationで転送先を指定。
複数ある場合は後の行が有効になる。

HTTP/1.1 302 Found
Location: http://本来のリダイレクト先**<改行>**
Location: http://攻撃用サイト

HTTP Header

Webクライアント

Webサーバ

```
<!DOCTYPE html>
<html>
<head>
        <meta charset="utf-8">
        <title>サンプル</title>
        <link rel="stylesheet" href="style.css">
</head>
<body>

</body>
</html>
```

HTTP Content

エスケープ処理による対処

クロスサイトスクリプティングの場合

- ユーザが入力したデータに含まれる記号などを置き替えることで安全なデータに変更する

- HTMLに埋め込む場合、< > ” ’ & といった記号があると入力されたデータがHTM Lのタグや属性として処理されてしまうため、記号を変換する。(PHPならhtmlentitiesなどを使用する)

ＳＱＬインジェクション、HTTPヘッダインジェクションでは対処すべき記号が異なる

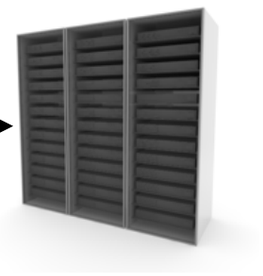
変換前	変換後
<	<
>	>
‘	'
“	"
&	&

<form> → **<**form**>**

Webブラウザの表示上は<form>と表示される

CSRF (Cross site request forgeries)

ログイン



ログアウトせずに
他のサイトを閲覧

攻撃者

攻撃用ページ

表示を隠された<form>など。
<form>のaction属性を正規のURLにしておく

ログイン情報と共に**意図しないデータを送信**して、**重要な操作を行なってしまう**

問題15

ユーザの入力をそのままHTMLに書き出してしまうことで発生する脆弱性の名称を選択してください。

A. CSRF

B. HTTPヘッダ・インジェクション

C. SQLインジェクション

D. クロスサイト・スクリプティング

質疑応答

本日の内容

ネットワーク・サーバ関連技術
- TCP/IP
- DNS
- HTTP
- Webサーバ
- プロキシ
- データベース

試験範囲
- 試験概要
- 試験範囲

Web関連技術
- JavaScript
- 画像ファイルフォーマット
- DataURI
- セキュリティ