

# End-to-End セキュリティを担保する 1

## セキュリティエンジニアリング特論 第3回

栗原 淳

兵庫県立大学大学院

2021-10-21

はじめに

# はじめに

第3回からは、「安全なシステム・プロトコル」を組む雰囲気を知るため

- End-to-End (E2E) セキュリティの原則と必要性
- Web サイトでの E2E セキュリティ実践のため、ブラウザ側<sup>1</sup>&サーバ<sup>2</sup>側で、標準技術を選定して組み合わせる方法
  - 選定した暗号化モードでの共通鍵・公開鍵暗号化において「Forward Secrecy」を担保する？
  - AES 暗号化の「鍵導出」はどうやったらいい？
  - RSA 署名のパディング・運用方法の標準はどうなっているのか？

等を学んでいく。

まず今回は、その「さわり」を解説・体験してみる。

---

<sup>1</sup> 「フロントエンド」と呼ぶ

<sup>2</sup> 「バックエンド」と呼ぶ

# 事前準備

\*nix (Linux, Mac, ...) 前提だが、以下の通り.

- Bash/Zsh, Git が利用可能
- Node.js LTS (ver.14 以上), npm, yarn が利用可能
- Google Chrome 系ブラウザ and/or Firefox が利用可能

※ 必須ではないが、準備は強く推奨.

※ Windows 環境ならば VM で

(Windows10 環境ならば WSL2 と PowerShell でも)

# 今後の予定 (暫定)

- 1 導入&とりあえず暗号化コードを触ってみる ← 今日はココ
- 2 共通鍵暗号化によるデータ秘匿を組み上げる
- 3 公開鍵暗号化による鍵秘匿を組み上げる
- 4 ハッシュ・MAC・署名, それぞれの使い所と使い方
- 5 全てをまとめて End-to-End セキュリティを担保する

# モダン Web サイトと End-to-End セキュリティ

# Web サイトにおける昨今の情勢

- EU における General Data Protection Regulation (GDPR) の施行 (2018 年)
- GDPR に続いて、カリフォルニア、南米、オセアニアで類似の法律の制定の動き
- 日本においても、2020 年に個人情報保護法の改正法案提出の見通し



企業にとって、「正しく」「強固」に  
ユーザデータ、ユーザプライバシーを保護することは必須の事項

# 最近流行りの Web システム

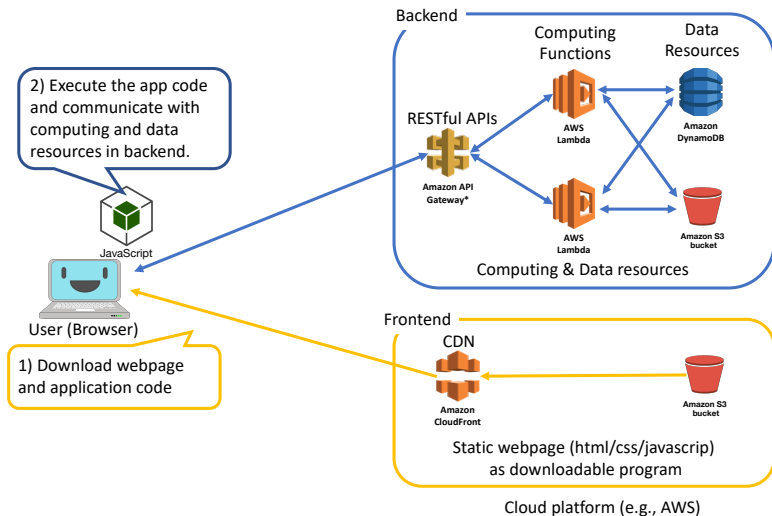
- クラウドプラットフォーム上で構築
- 「サーバ」のない (サーバレス) 構成
- JavaScript のフレームワーク (ReactJS/Vue など) を多用した, Single Page Application 構成



ユーザの手元で計算を実行する機会の増加

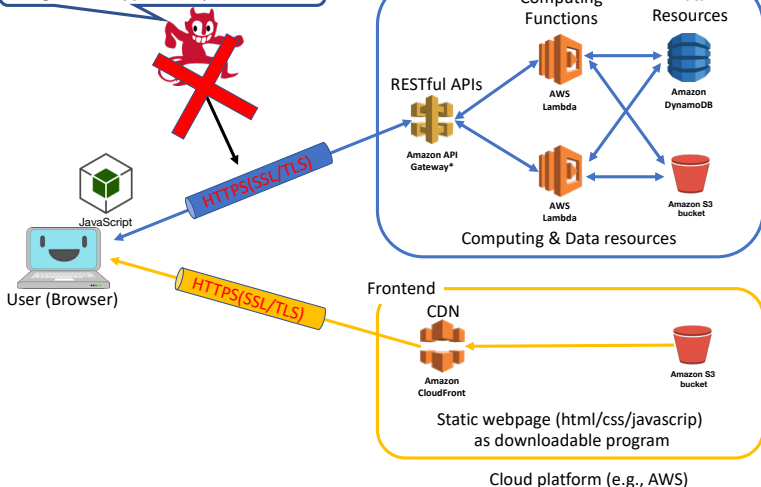


## AWS を例にした典型的な構成:



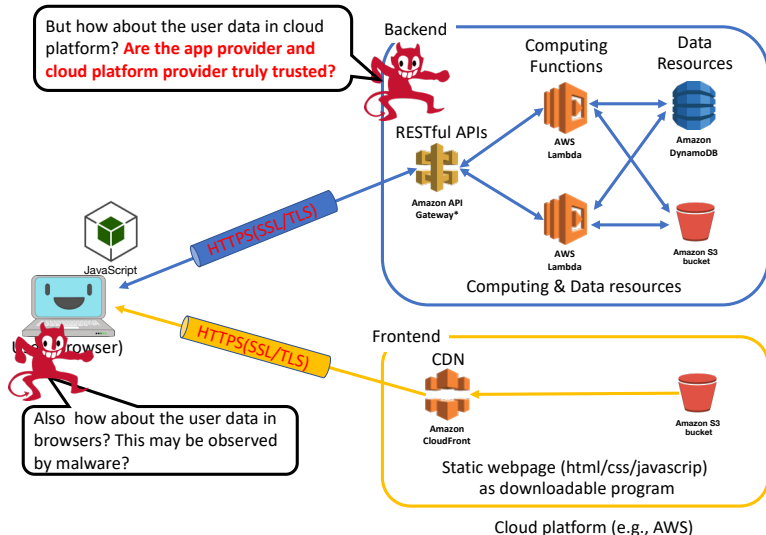
# AWS を例にした典型的な構成:

SSL/TLS prevent protect user data from being eavesdropped on a public channel



通常、ユーザ・クラウド間の HTTP 通信路は SSL/TLS で保護  
⇒ HTTP 通信路から外部の盗聴者へのユーザデータ漏洩を防止

# AWS を例にした典型的な構成:



しかし、クラウド PF 内・ブラウザ内のデータ保護は……？

# 「暗号化しているから安全です」という叙述トリック

(Web とはちょっと違いますが…) 某クラウドストレージ事業者の例

従来の暗号化を凌駕

□ は、□ アプリとサーバー間で転送中のファイル、および保管中のファイルを保護します。各ファイルは不連続のブロックに分割され、強力な暗号を使用して暗号化されます。変更されたブロックのみが同期の対象になります。 [詳しくはこちら](#)

クラウドベースの (Web) サービスでよくある文言：

- (SSL/TLS で) 転送中のデータを暗号化して保護
- ストレージに保存されるデータは暗号化して保護

- (SSL/TLS で) 転送中のデータを暗号化して保護  
⇒ 公開通信路の盗聴からデータを保護
- ストレージに保存されるデータを暗号化して保護  
⇒ ストレージ自体が盗まれた時や，第三者のストレージを使っている場合のデータ漏洩を防止

いずれも事業者に対しての秘匿性を担保しているわけではない<sup>3</sup>



(望む・望まないにしろ) 事業者はユーザデータを不必要に取得

---

<sup>3</sup>事業者はデータを見放題ということ。

このようなクラウドサービス・Web App を作ることは：

- ユーザにとって：共有不要な相手とデータを共有している
- 事業者にとって：昨今のプライバシー・セキュリティ要求の高まりから，**無用なリスクを背負いこむ可能性が大**

今後，Web App を作っていくにあたって

「必要な相手とだけ」確実に・正しく，データを共有できるように，適切なデータ秘匿が必要 (不必要にデータ取得しない)

# データの秘匿性・プライバシーを謳うサービス

## ■ Tresorit<sup>4</sup>:

事業者・サーバに情報が漏れないことを謳ったクラウドストレージサービス。Dropbox に近い。

## ■ KeyBase<sup>5</sup>:

事業者・サーバに情報を漏らさず、メッセージ・ファイル共有（クラウドストレージ）が可能な SNS。2020 年春に Zoom に買収された。

## ■ Signal<sup>6</sup>:

事業者・サーバに情報を漏らさないメッセージング・通話アプリケーション。「最も安全な」チャットサービスと呼ばれており、各類似サービス (WhatsApp など) にプロトコルを提供。

北米・EU 共に、スノーデンの事件以降、事業者にも情報を与えない  
**End-to-End 暗号化**を謳ったサービスが強く注目を浴びている。

<sup>4</sup><https://tresorit.com/>

<sup>5</sup><https://keybase.io/>

<sup>6</sup><https://signal.org/>

# End-to-End セキュリティとは

## End-to-End (E2E) Principle<sup>7</sup>

The end-to-end principle is a network design method in which **application-specific features are kept at communication end points.**

(アプリケーションの機能はネットワークシステムの**終端**で実装されるべきという原則)

---

<sup>7</sup>J. H. Saltzer et al., “End-to-End Arguments in System Design”, in Proc. ICDCS 1981, pp. 509–512, Apr. 1981.



アプリケーションのセキュリティについての E2E Principle:

## End-to-End (E2E) セキュリティ

情報を共有する主体同士 (End-to-End) について、セキュリティ 3 原則を担保する。

- 情報の秘匿性 (主体のみで情報を共有可能) ⇒ E2E 暗号化
- 主体・情報の真正性 (主体が生成した情報であることを証明)
- 情報の可用性 (主体同士が正しく情報を利用可能)

ポイント：アプリケーションにおいて「情報を共有する主体」は一体何か．

- アプリケーションを利用するユーザ同士？
- サーバ・クライアントアプリ同士？
- 他？

では、Web アプリケーションにおけるエンドポイントとは？

- ユーザ側エンド:

⇒ JavaScript/HTML/CSS など「ブラウザ内で実行・レンダリングされる」Web フロントエンド要素<sup>8</sup>

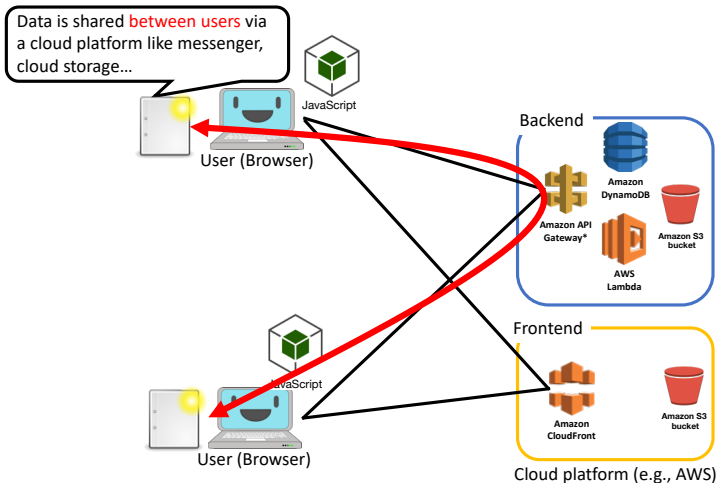
- もう一方のエンド:

⇒ Web アプリケーション次第で変化

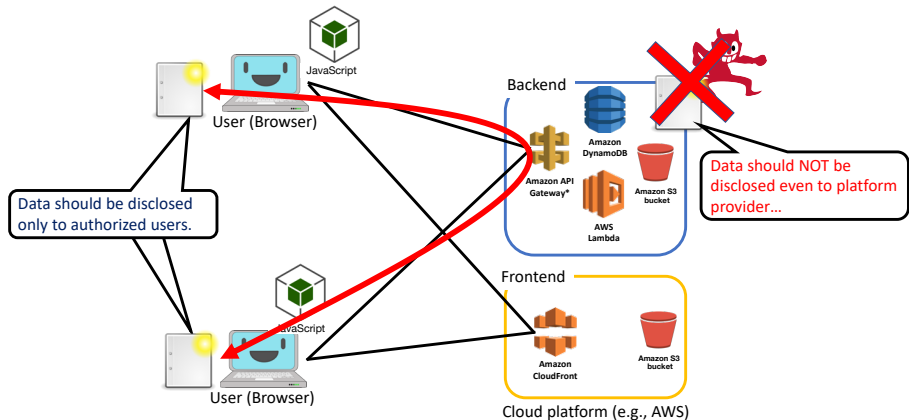
---

<sup>8</sup>実際にユーザが触れる要素がエンドポイントであって、Web サービスにおいては、端末やブラウザはエンドポイントにならない

例: クラウドプラットフォームを介し、**ユーザ同士が情報を共有する主体**の場合 = ユーザのブラウザ同士が両エンド

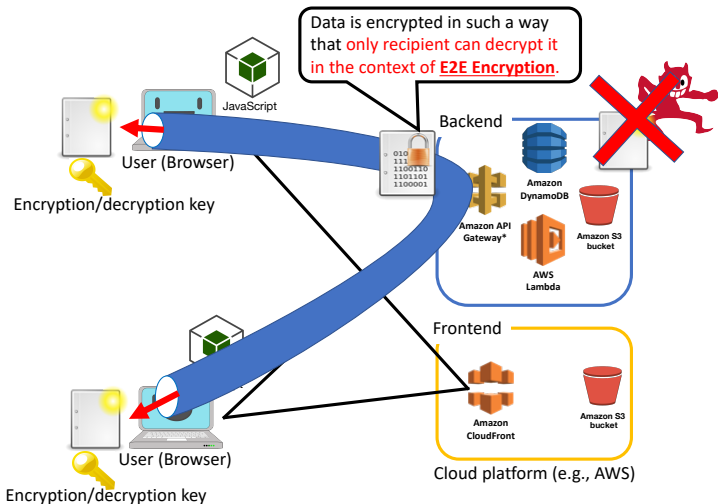


E2E セキュリティの観点からは、クラウドプラットフォーム自身ですら情報を取得可能であるべきではない



※ユーザがサーバとのみやり取りする場合，一方の主体 (End) はサーバとなる。

この例の場合、E2E セキュリティのためには、情報を共有する主体同士のみが復号可能なよう、やり取りするデータを全て暗号化する (E2E 暗号化)



E2E セキュリティを実現するには、構築するアプリケーション毎に「情報を共有する主体」を正しく定義する必要.

E2E セキュリティを実現しつつ、「事業者にとってリスクとなるような情報はなるべく不用意に取得しない」ことも重要.

# Web App における End-to-End セキュリティ

改めて…

サービスで E2E セキュリティを考える意味

- ユーザプライバシーの保護
- 事業者側のリスクの低減

Web アプリケーションにおける E2E セキュリティ

少なくとも片方のエンドは Web フロントエンド要素

⇒ Web フロントエンドでセキュリティを担保する方法が必要



と，いうわけで，今回は「Web のための E2E セキュリティ」として Web ブラウザ内でのデータの暗号化 (E2E 暗号化) の「さわり」を紹介する．

# JavaScriptで暗号を使ってみよう [基礎編]

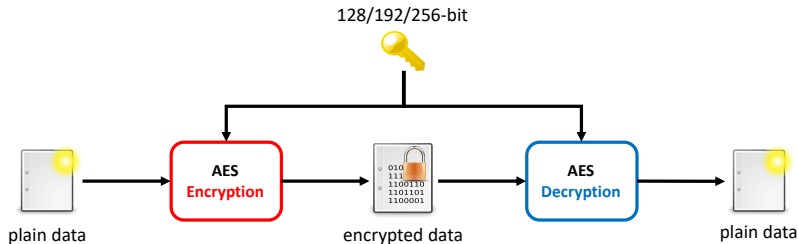
–お試しで AES–

# AES (Advanced Encryption Standard) とは？

## AES

米国 NIST の標準<sup>9</sup> 暗号アルゴリズム (※共通鍵暗号)

- 鍵長は 3 種類: 128-bit, 192-bit, 256-bit
- 欧州 NESSIE, 日本 CRYPTREC などの標準規格としても採択
- 現在まで致命的な欠陥の発見のない, 安全性の高いアルゴリズム



<sup>9</sup> NIST FIPS 197 <https://www.nist.gov/publications/advanced-encryption-standard-aes>

AES はアルゴリズム自体がまずもって標準規格

しかし、AES 暗号化における「暗号の利用モード」は元より、

- 入力する鍵の生成方法、
- パスワードベース暗号化の際の暗号化手順、
- etc....

など、**運用方法にも多くの標準規格が存在している**。

それら標準規格を読み解き、さらに共通鍵暗号・公開鍵暗号・ハッシュを組み合わせた上で、安全に使っていく必要がある。

が、今回は、まずは慣れるために「**とにかく AES を使ってデータを暗号化してみる**こと」から始め、E2E 暗号化の雰囲気を知る。

# JavaScript における暗号の利用環境

一般的な統合ライブラリは C で書かれた OpenSSL だが、JavaScript から直接呼び出すことができない。

JavaScript から利用可能な暗号の統合ライブラリ:

- **WebCrypto API** (ブラウザ)<sup>10</sup>:  
W3C にて標準化が進む Web API (ブラウザのネイティブ API)。
- **Crypto** (Node.js)<sup>11</sup>:  
Node.js 環境にて利用可能な暗号ライブラリ (Node.js のネイティブ API)。OpenSSL のラッパー。
- **sjcl** (Node.js/ブラウザ)<sup>12</sup>:  
Stanford 大学暗号研究室で開発された pure JS なライブラリ。

---

<sup>10</sup><https://www.w3.org/TR/WebCryptoAPI/>

<sup>11</sup><https://nodejs.org/api/crypto.html>

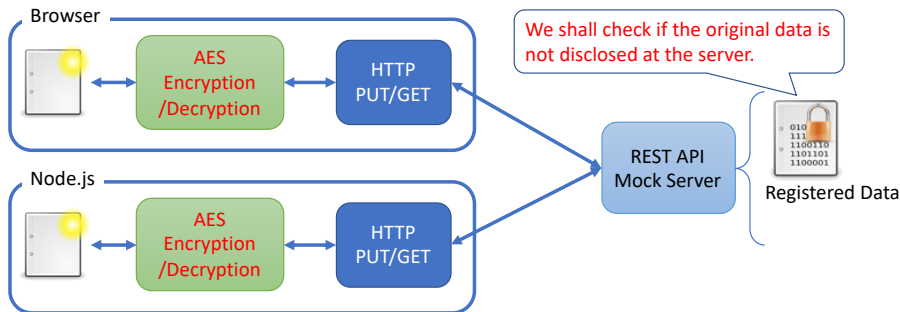
<sup>12</sup><http://bitwiseshiftleft.github.io/sjcl/>

今回は、高速動作が期待されるネイティブ実装な統合ライブラリ 2 つを例にとる．

- WebCrypto API → ブラウザ向け
- Node Crypto → サーバ/スタンドアロン S/W (Node.js) 向け

# 今回やってみること

ブラウザのJS 実行エンジン・Node.js をエンドとし、REST API で暗号化データを登録してみる。



単なるデータの HTTP PUT/GET の前段・後段に AES 暗号化・復号部分を組み込んでみる。

※モックサーバはローカルホストで立ち上げ。

# JavaScript プロジェクトの準備

- プロジェクトの GitHub リポジトリ<sup>13</sup>を Clone

```
$ git clone  
https://github.com/junkurihara/lecture-security_engineering.git  
$ cd sample-03
```

- 依存パッケージのインストール

```
$ yarn install
```

- ライブラリのビルド

```
$ yarn build
```

---

<sup>13</sup>[https://github.com/junkurihara/lecture-security\\_engineering](https://github.com/junkurihara/lecture-security_engineering)



# REST API モックサーバの準備

今回は SSL 接続可能な共有サーバを準備済  
(<https://e2e.secarchlab.net/>)<sup>14</sup>.

別途、検証用のモックサーバをローカルで立ち上げ可能.

## モックサーバの立ち上げ

```
$ yarn start
```

起動すると、localhost の 3000 番ポートで HTTP リクエストを待ち受け開始する.

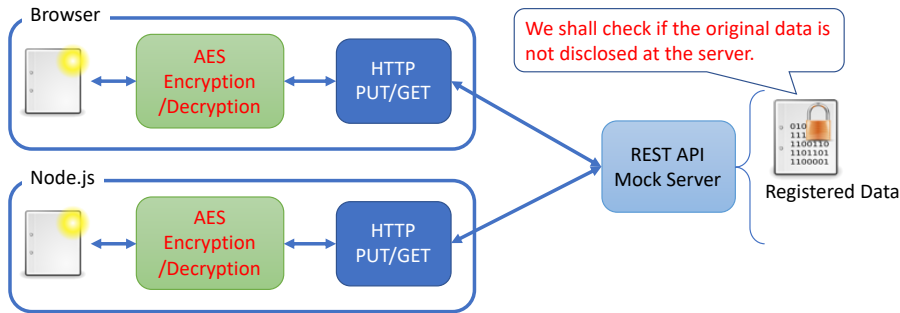
---

<sup>14</sup>2021/10/22 以降はサーバ停止. ローカルモックサーバを利用のこと.

# コマンドラインで暗号化 (スタンドアロンアプリ・サーバ)

# コマンドラインで暗号化

JavaScript (Node.js) をコマンドラインから実行してみて、動作イメージを確認してみる。



まずは生データを POST してサーバに登録してみる。

```
$ pwd
...../sample-03 ←場所を確認

$ yarn execute post -r 'hello my secret world!!!' ← 登録15
Register plaintext data to remote server
Data: hello my secret world!!!
Registered id: 1 ← id=1 番として登録したというメッセージ
```

登録したデータを生のまま取得してみる。

```
$ yarn execute get -r 1 ← id=1 番の登録データを取得
Retrieve plaintext data to remote server
Registered Id: 1
Retrieved data: hello my secret world!!! ← 取得した 1 番のデータ
```

---

<sup>15</sup> ローカルモックサーバに接続する場合は -r を抜く

データを AES 暗号化したあと POST してサーバに登録してみる.

```
$ yarn execute post \  
-e -k 'my secret key' \ ← my secret key という PW で暗号化  
-r 'hello my super secret world!!!'  
Register encrypted data to remote server  
Data: hello my super secret world!!!  
Key: my secret key  
Note: Derived key binary in base64:  
o12da4tawTjHd4woS+DeexcCR9E0yVKml6g0zZkGzDc=16  
Registered id: 2 ← id=2 番として登録したというメッセージ
```

AES 自体は, AES256-CBC モード (RFC3602 他で標準化) を利用

---

<sup>16</sup>実際に使う AES 鍵のバイナリ表現 (base64), 標準規格 PBKDF2 (RFC8018, PKCS #5 v2.1) にて導出

暗号化して登録したデータを生のまま取得してみて、暗号化されていることを確認する.

```
$ yarn execute get -r 2 ← id=2 番の登録データを取得
Retrieve plaintext data to remote server
Registered Id: 2
Retrieved data: EoeSsv5BFR6s1jZh3iMM1Pxa+wA4UxQnM30J2027kJU= ←
取得した 2 番のデータ
```

Base64 エンコードされているが、暗号化されており中身はまったくわからない.<sup>17</sup>

---

<sup>17</sup>Mac/Linux の場合、ターミナルで “echo [base64str] | base64 -D -” と実行してみると訳のわからないデータにデコードされることが確認できる.

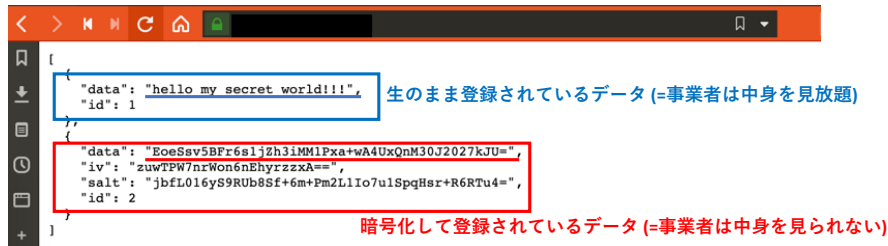
取得した後、復号してみる<sup>18</sup>

```
$ yarn execute get \  
-d -k 'my secret key' \ ← my secret key という鍵で復号  
-r 2 ← id=2 の鍵を取得  
Retrieve encrypted data to remote server  
Id: 2  
Key: my secret key  
Note: Derived key binary in base64:  
o12da4tawTjHd4woS+DeexcCR9E0yVKml6g0zZkGzDc=  
Decrypted data: hello my super secret world!!! ← 正しく復号された
```

---

<sup>18</sup>key が間違っていると失敗する

<https://e2e.secarchlab.net/data> にアクセスすると、サーバでの登録状況が一覧できる。<sup>19</sup>



<sup>19</sup> ローカルホストに立てた場合は <http://localhost:3000/data>



# ブラウザで暗号化 (ユーザエンド)

# ブラウザで暗号化

- 1 samples/src/post-get-browser.html をブラウザで開く。
- 2 真っ白な画面で「開発者ツール」を起動<sup>20</sup>，Web コンソールを表示する。

コマンドラインでやった「暗号化して登録→取得して復号」の一連の流れが初期設定のデータ・鍵を使って実行される。



<sup>20</sup>Chrome: Ctrl(Cmd)+Alt(Opt)+i

以下の2パターンで色々試すことができる.

- `samples/src/post-get-browser.html` の中身を編集→リロード
- `samples/src/post-get-browser.html` を開いたまま, 開発者ツールの Web コンソールから POST 関数と GET 関数を実行.

ここでは後者を試してみる.

## Web コンソールから暗号化・登録してみる。

```
> e2eTest.postMyData(  
  {data: 'hello world!',  
    key: 'my browser key',  
    remote: true,  
    encrypt: true})  
.then( (result) => console.log(result) );
```

この部分を入力

◀ ▶ Promise {<pending>}

Note: Derived key binary in base64: J5SHI8TcJRGDdy9WQH9yqI2szxpyCsG8pirVjyzI0yQ=

post-get.js:25

▶ {id: 5}

VM486:6

id=5で登録された

```
e2eTest.postMyData(  
  {data: 'hello world!', ← 暗号化するデータ  
    key: 'my browser key', ← 鍵  
    remote: true, ← リモートサーバの場合 true  
    encrypt: true}) ← 暗号化する場合 true  
.then( (result) => console.log(result) );
```

～中略～

VM486:6 {id: 5}

コマンドラインと同じく，<https://e2e.secarchlab.net/data>を表示すると暗号化されて登録されていることがわかる．

今度は Web コンソールから取得・復号してみる。

```
> e2etest.getMyData(  
  {id: 5,  
    key: 'my browser key',  
    remote: true,  
    decrypt: true})  
  .then( (result) => console.log(result) );
```

この部分を入力

< ▶ Promise {<pending>}

Note: Derived key binary in base64: J5SHI8TcJRGDdy9WQH9yqI2szxpyCsG8pirVjyzI0yQ= [post-get.js:75](#)

▶ {data: "hello world!"}

[VM841:6](#)

取得して正しく復号  
できた

```
e2etest.getMyData(  
  {id: 5, ← id=5 のデータを取得  
    key: 'my browser key', ← 鍵  
    remote: true, ← リモートサーバの場合 true  
    decrypt: true}) ← 復号する場合 true  
  .then( (result) => console.log(result) );
```

～中略～

data: "hello world!"

もちろん，ブラウザ (WebCrypto) とコマンドラインで相互接続可能．

- ブラウザで暗号化・登録したデータを，コマンドラインで取得・復号
- コマンドラインで暗号化・登録したデータを，ブラウザで取得・復号

今まで登録したデータで試してみよう！

# 暗号化・復号の中身



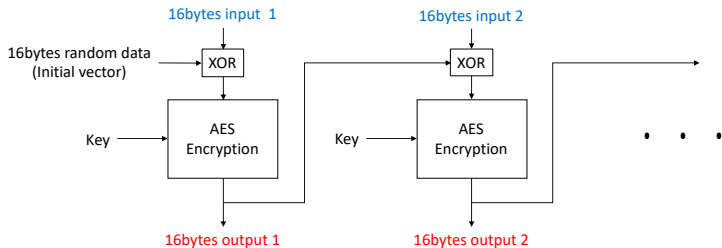
# 今回の事例でのモード設定

## AES の「利用モード」

AES の処理 1 回で暗号化できるのはたった 16bytes にすぎない。  
長いデータを連続で暗号化するために、**暗号化処理を連続して組み合わせる方法**が利用モード。

安全性向上のため、一般的に

- 「先頭の 16 バイトはランダムな初期化ベクトルと混ぜる」
  - 「前の 16 バイトのデータを継承して次の 16 バイトを処理」
- などの工夫を入れた利用モードを用いる。



まず、暗号の利用モードとして 256 ビット鍵 AES の CBC モードを採用 (ISO/IEC, FIPS PUB 197, RFC3602,...)

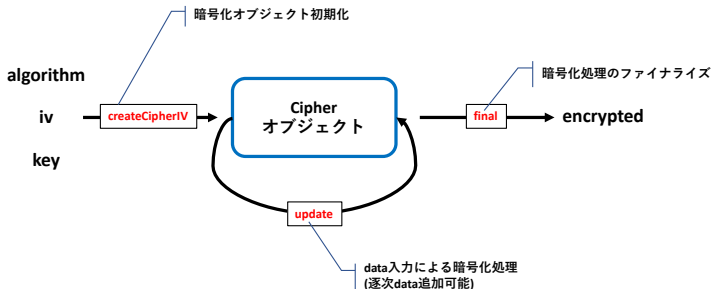
# Node.js Crypto ライブラリでの AES-CBC 暗号化・復号

## sample/src/encrypt-node.js: encrypt 関数

```
const crypto = require('crypto'); // crypto モジュールの読み出し
const algorithm = 'aes-256-cbc'; // AES-256-CBC モード

const iv = crypto.randomBytes(16); // Initial Vector の生成

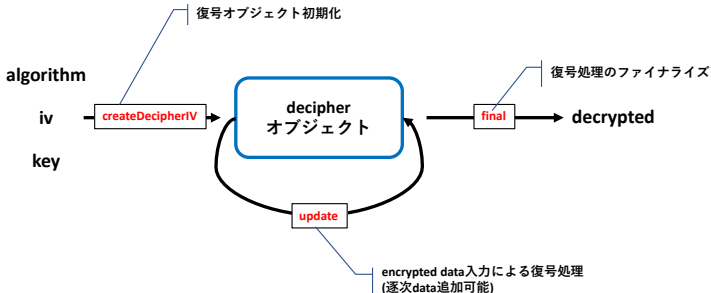
const cipher = crypto.createCipheriv(algorithm, key, iv); // 暗号化 Object 初期化
let encrypted = cipher.update(uint8data, 'utf8', 'base64'); // 暗号化
encrypted += cipher.final('base64'); // 暗号化完了
```



## sample/src/encrypt-node.js: decrypt 関数

```
const crypto = require('crypto'); // crypto モジュールの読み出し
const algorithm = 'aes-256-cbc'; // AES-256-CBC モード
```

```
const decipher = crypto.createDecipheriv(algorithm, key, iv); // 復号 Object 初期化
let decrypted = decipher.update(encrypted, 'base64', 'utf8'); // 復号
decrypted += decipher.final(); // 復号完了
```



# ブラウザ WebCrypto API での AES-CBC 暗号化・復号

## sample/src/encrypt-browser.js: encrypt 関数

```
const crypto = window.crypto; // WebCrypto API
const iv = crypto.getRandomValues(new Uint8Array(16)); // IV の生成

const importedKey = await crypto.subtle.importKey( // key オブジェクトの生成
  'raw', // バイナリ鍵のインポート指定
  key,
  { name: 'AES-CBC' }, // CBC モードに利用
  false, // key オブジェクトからの生鍵エクスポート可否
  ['encrypt', 'decrypt'] // 暗号化・復号に利用
);

const encrypted = await crypto.subtle.encrypt( // 暗号化を実行
  { name: 'AES-CBC', iv: uint8iv }, // CBC モードで暗号化
  importedKey,
  data
);
```

## sample/src/encrypt-browser.js: decrypt 関数

```
const crypto = window.crypto; // WebCrypto API

const importedKey = await crypto.subtle.importKey( // key オブジェクトの生成
  'raw', // バイナリ鍵のインポート指定
  key,
  { name: 'AES-CBC' }, // CBC モードに利用
  false, // key オブジェクトからの生鍵エクスポート可否
  ['encrypt', 'decrypt'] // 暗号化・復号に利用
);

const decrypted = await crypto.subtle.decrypt( // 暗号化を実行
  { name: 'AES-CBC', iv: uint8iv }, // CBC モードで暗号化
  importedKey,
  encrypted
);
```

# 鍵の導出はどうすればいいのか

今回は「パスワード」を用いて暗号化をした。

では、暗号化の鍵はどうやって導出していたのか？

⇒ **標準規格 PBKDF2 (RFC8018) を利用してパスワードを鍵へ変換**

sample-03/src/common/key.js (PBKDF2 の導出関数は栗原が実装)

```
// derive key from password
if(!salt){ salt = jscu.random.getRandomBytes(32); }
else { salt = jseu.encoder.decodeBase64(salt); }

const iterationCount = 2048; // must be shared with receiver
const hash = 'SHA-256'; // SHA-384, SHA-512, etc.

const key = await jscu.pbkdf.pbkdf2(
  str,
  salt,
  iterationCount,
  len,
  hash
).catch( (e) => {
  throw new Error('failed to derive binary key from string key: ${e.message}');
});
```

詳細は次回.

# まとめ



# まとめ

今回は、

- E2E セキュリティの概念・重要性の紹介
- Web における E2E セキュリティ実現の雰囲気を紹介

次回は、

- AES を「正しく」「安全に」使うために、鍵導出などで標準技術の使い所を紹介