

# JavaScript による **End-to-End** セキュリティ

## 入門編

栗原 淳

August 14, 2019

はじめに

# はじめに

この講義では

- End-to-End (E2E) セキュリティの原則
- Web サイトでの E2E セキュリティ実践のため、JavaScript での実装方法
  - ブラウザ側
  - サーバ側 (Node.js)

のさわりを学ぶ。

# 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

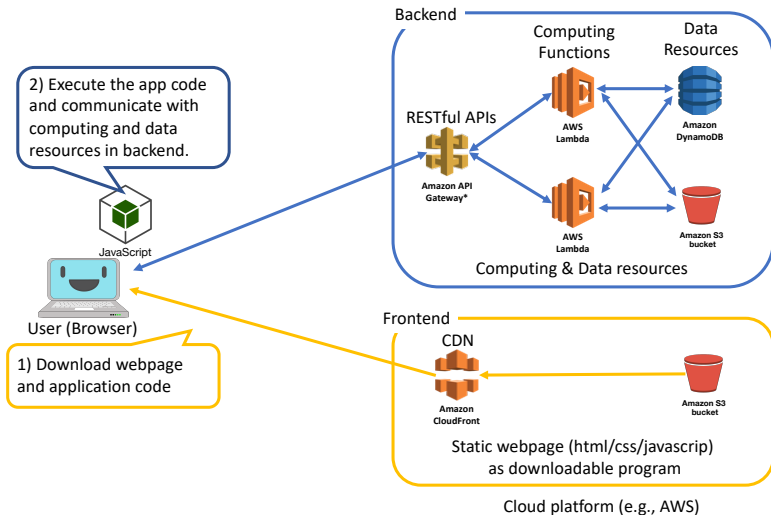
# 最近流行りの Web システム

- 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 (ReactJS など) を多用した、Single Page Application 構成

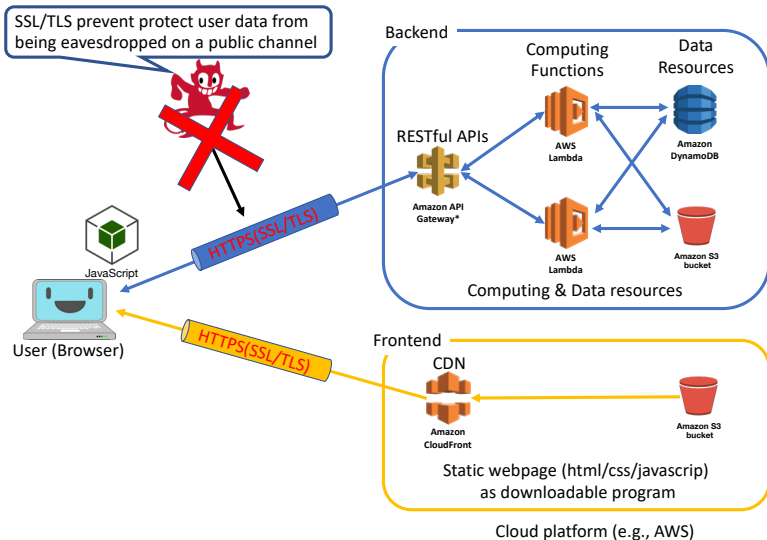


ユーザの手元で計算を実行する機会の増加

## AWS を例にした典型的な構成:



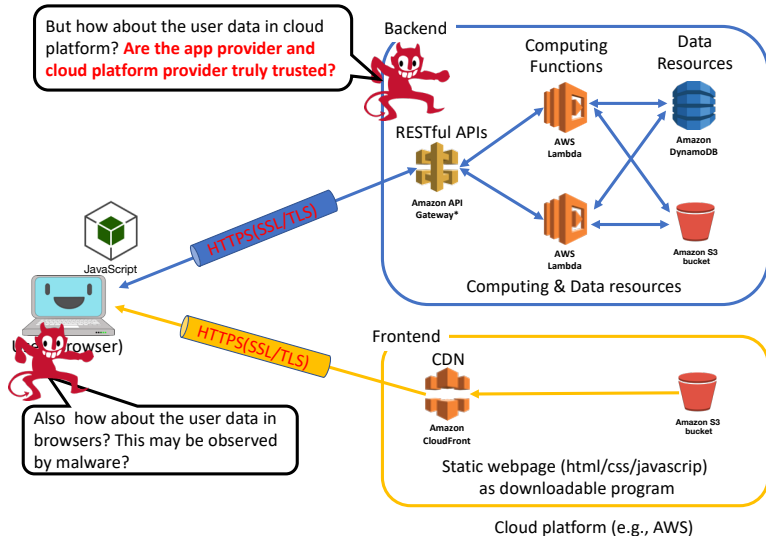
# AWS を例にした典型的な構成:



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>1</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>1</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>2</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>3</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。

## ■ Signal<sup>4</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>2</sup><https://tresorit.com/>

<sup>3</sup><https://keybase.io/>

<sup>4</sup><https://signal.org/>

# End-to-End セキュリティとは

## End-to-End (E2E) Principle<sup>5</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>5</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>6</sup>

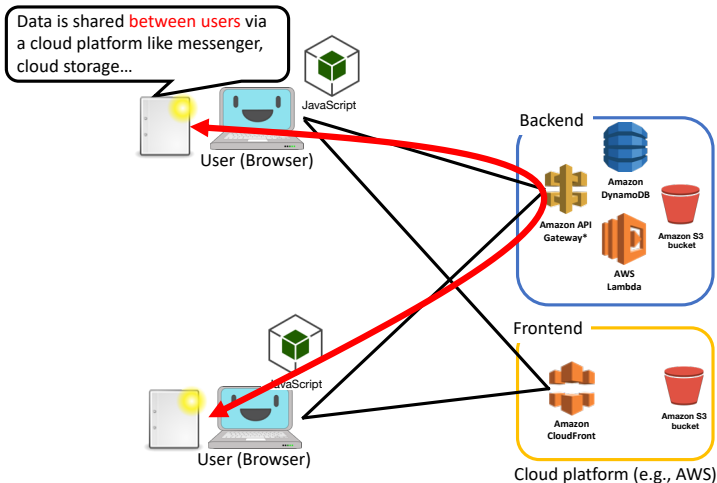
- もう一方のエンド:

⇒ Web アプリケーション次第で変化

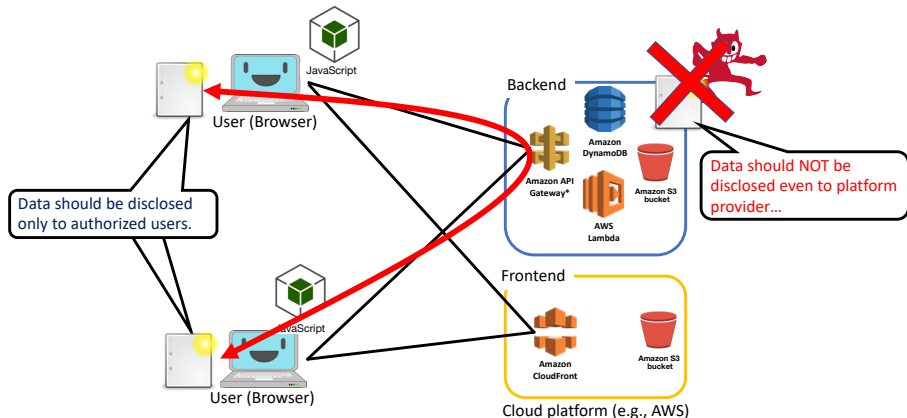
---

<sup>6</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

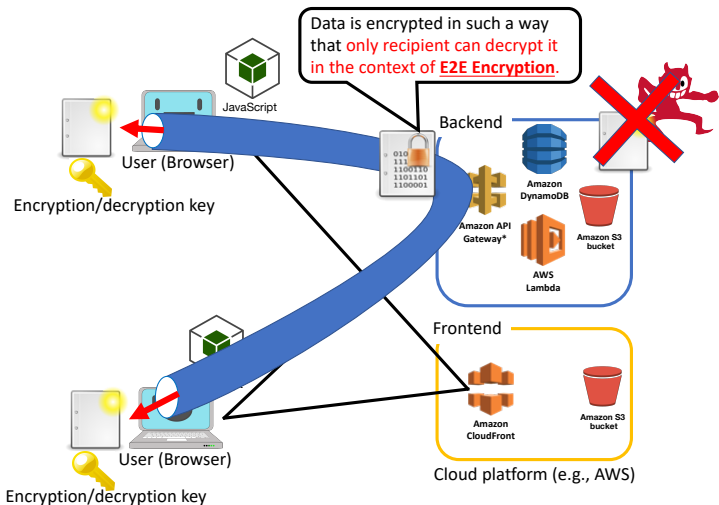


E2Eセキュリティの観点からは、クラウドプラットフォーム自身ですら情報を取得可能であるべきではない



※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JavaScriptにおけるデータの暗号化(E2E暗号化)の「さわり」を紹介します。

# JavaScript で暗号を試みよう [基礎編]

—今回はお試しで AES—

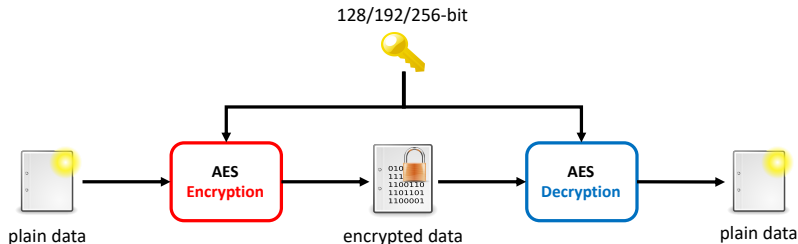


# AES (Advanced Encryption Standard) とは？

## AES

米国 NIST の標準暗号アルゴリズム (※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は見つかっていない、安全性の高い**デファクトスタンダード**のアルゴリズム



共通鍵暗号・公開鍵暗号・ハッシュがどうのとか、それらを組み合わせ安全に使うためにはどうするかとか、そういう話は今回はしない。

とりあえず「AES という暗号アルゴリズムがあるんだ」くらいで十分。今回、まずは「とにかく JS で AES を使ってデータを暗号化してみることに」から始める。

# 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>7</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>8</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>9</sup>:  
Stanford 大学暗号研究室で開発された pure JS なライブラリ。

---

<sup>7</sup><https://www.w3.org/TR/WebCryptoAPI/>

<sup>8</sup><https://nodejs.org/api/crypto.html>

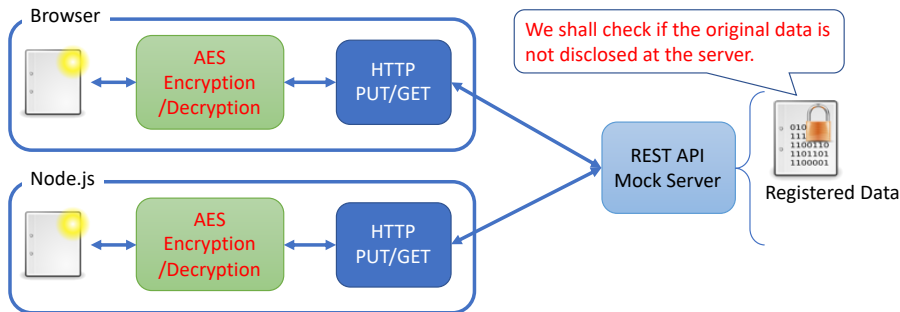
<sup>9</sup><http://bitwiseshiftleft.github.io/sjcl/>

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
- Node Crypto

# 今回やってみること

ブラウザ・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。

# 環境

以下の環境が前提:

- Node.js (> v10) がインストール済<sup>10</sup>
- ブラウザとして、Google Chrome (系ブラウザ)、もしくは Firefox がインストール済み
- Visual Studio Code や WebStorm などの統合開発環境がセットアップ済みだとなお良い。

---

<sup>10</sup>npm に加えて yarn も使えるとなお良い (インストールコマンド: `npm i -g yarn`)

# JavaScript プロジェクトの準備

- プロジェクトの GitHub リポジトリ<sup>11</sup> を Check Out

```
$ git clone https://github.com/zettant/e2e-security-class  
$ cd e2e-security-class/sample
```

- 依存パッケージのインストール

```
$ yarn install or npm install
```

---

<sup>11</sup><https://github.com/junkurihara/e2e-security-class>

# 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.zettant.com/>)。

別途、検証用の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

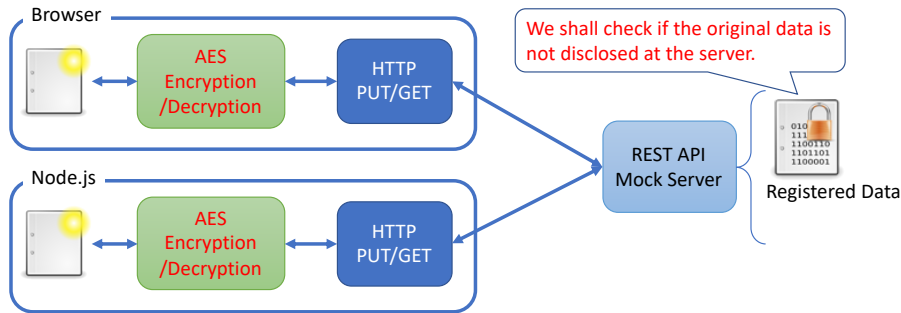
```
$ yarn start
```

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。



## とりあえず試してみる: コマンドライン編

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
.../e2e-security-class/sample ←場所を確認

$ yarn execute post -r 'hello my secret world!!!' ← 登録12
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>12</sup>-r を抜くとローカルのモックサーバに接続

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 という鍵で暗号化  
-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=13  
Registered id: 2 ← id=2 番として登録したというメッセージ
```

---

<sup>13</sup>実際に使う AES 鍵のバイナリ表現 (base64)

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>14</sup>

---

<sup>14</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>15</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>15</sup>key が間違っていると失敗する

<https://e2e.zettant.com/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>16</sup>

```
[
  {
    "data": "hello my secret world!!!",
    "id": 1
  },
  {
    "data": "EoeSsv5BFR6sljZh3iMMlPxa+wA4UxQnM30J2027kJU=",
    "iv": "zuwTPW7nrWon6nEhryzzxA==",
    "salt": "jbfL016yS9RUb8Sf+6m+Pm2L1Io7ulSpqHsr+R6RTu4=",
    "id": 2
  }
]
```

生のまま登録されているデータ (=事業者は中身を見放題)

暗号化して登録されているデータ (=事業者は中身を見られない)

<sup>16</sup> ローカルホストに立てた場合は <http://localhost:3000/data>

# とりあえず試してみる: ブラウザ編

- 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>17</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>17</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.zettant.com/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！

# Node.js での暗号化・復号の中身

Node.js Crypto ライブラリを使った AES-CBC 暗号化

# ブラウザでの暗号化・復号の中身

WebCrypto APIを使った AES-CBC 暗号化

補足: **API** が違うのがめんどくさい…

手前味噌だが、統合 **API** を使って楽をすると良い

# ブラウザ同士での相互接続性の確認

API を通じて暗号化データをやり取りしてみる。

E2E Security!

JSON の表示を出す



- 1 今回は共通鍵暗号
- 2 公開鍵暗号& Hybrid Encryption
- 3 ハッシュ・署名と HMAC
- 4 超マニアック講座：RFC とアルゴリズム・フォーマット

# 引用文献

# Appendix

This page is not counted.