WebCryptoから始める  
暗号化生活

株式会社ムラサメ研究所  
みやたけ　ゆき

# まえがき

# はじめに

目次

目次

[WebCryptoから始める 暗号化生活 1](#_Toc22147501)

[まえがき 2](#_Toc22147502)

[はじめに 3](#_Toc22147503)

[1 基礎知識 6](#_Toc22147504)

[1.1. 暗号化概要 6](#_Toc22147505)

[1.1.1. 暗号化の目的 6](#_Toc22147506)

[1.1.2. 暗号化の方式 6](#_Toc22147507)

[1.1.3. PKI(Public Key Infrastructure)基盤 7](#_Toc22147508)

[1.1.4. 認証局（CA） 7](#_Toc22147509)

[1.1.5. データ形式 7](#_Toc22147510)

[1.1.6. PKCS 8](#_Toc22147511)

[1.2. WebCryptoとは 8](#_Toc22147512)

[1.3. ブラウザ対応状況 8](#_Toc22147513)

[2. ツールの使い方 9](#_Toc22147514)

[2.1. OpenSSH、Puttyのインストール 9](#_Toc22147515)

[2.2. OpenSSH、Puttyの使い方 9](#_Toc22147516)

[2.3. PKI.js 9](#_Toc22147517)

[3. WebCryptoお試し 9](#_Toc22147518)

[3.1. RSAキーを作成 9](#_Toc22147519)

[3.2. RSAキーの読み込み 9](#_Toc22147520)

[3.3. 作成したキーを外部サービスで使う 9](#_Toc22147521)

1. 基礎知識
   1. 暗号化概要
      1. 暗号化の目的

我々は知らず知らずのうちに暗号化を利用しています。

無線LAN、SSH、HTTPS、パスワードの保存、クラウドストレージ

数え上げるときりがありません。

暗号化や認証により下記の問題を解決します

* 盗聴  
  アリスがボブに送った秘密のメッセージをイブに読まれること  
  データの暗号化で防ぐ事ができます
* 改ざん  
  アリスがボブに好き（はぁと）って送ったメッセージを  
  ボブに思いをよせていたマロリーに 嫌いと改ざんされること  
  デジタル署名により防ぐ事ができます
* なりすまし  
  イブがボブに、アリスの名を語って嘘のメッセージを送ること  
  信頼性の高い認証局を使う事で防ぐ事ができます
  + 1. 暗号化の方式
* ハッシュ  
  可変の文字列から固定長の文字列を生成する  
  メッセージダイジェストとも呼ばれる  
  ハッシュ化された文字列から元には戻せない  
  処理速度は速い  
  データの改ざんを調べる事ができる  
  MD5、SHA-1、SHA-256等が有名
* 共通鍵方式  
  暗号化、複合化に同じ鍵を使う  
  相手毎に鍵を作るので鍵の管理が大変  
  速度は比較的速い  
  鍵を相手に安全に渡す事が難しいため、下記の公開鍵方式で鍵を暗号化して送る事がある  
  暗号方式はDES、AESなどがある
* 公開鍵方式  
  暗号化に公開鍵、複合化に秘密鍵と対になる2つの鍵を使う  
  秘密鍵がなければ複合化できないので、公開鍵は漏れても問題がない  
  計算に時間がかかるため、共通鍵方式と併用されることが多い  
  RSA、DSA、楕円曲線暗号が使われる  
  + 1. データ形式

データを表す形式は ASN.1にて定義されています

* BER (Basic Encoding Rules)  
  日本語に訳すと、基本的な符号化規則

バイナリ形式の基本的なデータエンコーディングルール

1つのデータをコンテナにして連結させた形式です  
コンテナは、コンテナ種類、サイズ、データで構成されます  
  
ただし、符号化において複数の表現が可能なため、署名において問題が発生します  
そのため、暗号化においては厳密なDERやCERが使われます

* DER (Distinguished Encoding Rules)  
  日本語に訳すと、優れた符号化規則？  
  BERのサブセットでより厳密に正規化された規格です  
  固定長のデータを扱う時に使われます
* CER (Canonical Encoding Rules)  
  日本語に訳すと、正規化された符号化規則？  
  BERのサブセットでより厳密に正規化された規格です  
  可変長データの時に使われます
* PEM (Privacy Enhanced Mail)  
  日本語だと、匿名性を負荷した電子メール？  
  DERやCERはバイナリデータで、そのままでは人間が扱いにくく  
  メールやHTTPにおいて扱いが難しくなるので  
  Base64でバイナリデータをエンコーディングし、ヘッダとフッタを付与したものをPEMと呼びます  
  + 1. PKI(Public Key Infrastructure)基盤

公開鍵方式を利用したセキュリティインフラの事をさします

* X.509  
  証明書や失効リストに関する取り決め
* TLS  
  トランスポート層で暗号化しセキュリティーを付与します  
  SSHやHTTPSなどに使われています
  + 1. 認証局（CA）

公開鍵が改ざんされた場合、悪意のある人にデータが盗まれる可能性がある  
第三者により公開鍵を証明する仕組み

CAの役割は２つ。公開鍵を登録する事と、失効させること。

（図が必要）

アリスがボブに暗号化メッセージを送る時を考えてみます

ボブはアリスに自分の公開鍵を渡します  
アリスはボブの公開鍵を使いメッセージを暗号化しボブに送ります  
秘密鍵はボブしか持っていないため、ボブ以外にはメッセージが解読できません  
  
ところが、悪意を持ったマロリーがボブの公開鍵ではなく自分の公開鍵をアリスに送りました

それを知らないアリスは、マロリーの公開鍵で暗号化してしまいました  
秘密鍵を持っているマロリーはメッセージを手に入れました  
  
上記の問題の解決に、認証局（キャロル）が必要です

ボブはキャロルに公開鍵を登録します  
アリスはキャロルからキャロルが署名したボブの公開鍵をもらいます  
アリスは署名が正しい事を確認し、ボブの公開鍵で暗号化しボブに送ります

たとえマロリーが自分の公開鍵をアリスに渡したとしても、署名でなりすましがバレます

* + 1. PKCS

１～１５？

* 1. WebCryptoとは

Webブラウザで暗号化を行うAPI  
<https://webrtc.org/>

* 1. ブラウザ対応状況

図

1. ツールの使い方
   1. OpenSSH、Puttyのインストール
   2. OpenSSH、Puttyの使い方
   3. PKI.js
2. WebCryptoを試す
   1. RSAキーを作成

まず手始めにRSAキーを作って表示してみましょう  
コードは下記にPushしているので適宜見てください

<https://github.com/YukiMiyatake/WebApiTest/tree/master/WebCrypto/src/sample3.1>

* WebCryptoライブラリの呼び出し

|  |
| --- |
| // WebCryptoのライブラリ  let crypto = window.crypto || window.msCrypto;  let subtle = crypto.subtle;  // アルゴリズム  const signAlg = "RSASSA-PKCS1-v1\_5";  const hashAlg = "SHA-256"; |

WebCryptoのライブラリはwindowから取得します

widnow.crypto、IE 11の場合は window.msCryptoで取得します

アルゴリズムはとりあえず上記を設定しておきます  
crypto.subtleで実際のインタフェースを取得します

* KeyPairの作成

|  |
| --- |
| function createCryptoKeys() {  return( Promise.resolve()  .then(() => {  // アルゴリズムを選びKeyPairを作る  let algorithm = {  name: signAlg,  modulusLength: 2048,  publicExponent: new Uint8Array([0x01, 0x00, 0x01]),  hash: {  name: hashAlg  }  };  return subtle.generateKey(algorithm, true, ["sign", "verify"]);  },  error => Promise.reject((`Error during generateKey: ${error}`))  ) |

Htmlから呼ばれる関数を作ります

WebCryptoは非同期ライブラリになっていて、Promiseを使います

Algorithmにはアルゴリズム等を指定します  
RSA以外にもECDSAやHMACなども指定する事ができます

usagesには["sign", "verify"]を指定しておきます  
Algorithmに公開鍵方式を指定した場合はCryptoKeyPair、共通鍵方式の場合はCryptoKeyを返却するPromiseが返ってきます

* キーのエクスポート

|  |
| --- |
| .then(keyPair => {  // PrivateKeyをpkcs#8(秘密鍵)形式にExportする  return (subtle.exportKey(  "pkcs8",  keyPair.privateKey  ));  },  error => Promise.reject((`Error during exportkey: ${error}`))  ) |

generateKeyで作成したCryptoKeyPairよりprivateKeyを使います

それを秘密鍵の標準形式 PKCS#8にExportします

PKCS#8にExportされた値を返すPromiseが生成されます

* 文字列型へ変換しTextareaに表示する

|  |
| --- |
| .then(pkcs8 => {  // ArrayBufferを文字列にし  const pkcs8str = ab2str(pkcs8);  // Base64エンコードを行い64文字毎に改行を行い  const base64 = pac64(btoa(pkcs8str));  // ヘッダとフッタを追加  const pem = `-----BEGIN PRIVATE KEY-----\n${base64}\n-----END PRIVATE KEY-----`;  // Textareaに表示  document.getElementById("pem-text").value = pem;  return (pem);  })  );  } |

ExportしたデータはArrayBufferなので、ab2strでStringに変換する  
次に組み込み関数btoaでBase64にエンコードする  
そしてpac64で64バイト毎に改行を行い  
最後にヘッダ度フッタを追加すればPEM形式の出来上がりです

* ライブラリコード

|  |
| --- |
| // 64文字ごとに改行を入れる  function pac64(pemString)  {  const stringLength = pemString.length;  let resultString = "";  for(let i = 0, count = 0; i < stringLength; i++, count++) {  if( count > 63 ) {  resultString = `${resultString}\r\n`;  count = 0;  }  resultString += pemString[i];  }  return resultString;  }  // ArrayBufferをStringに  function ab2str(buf) {  return String.fromCharCode.apply(null, new Uint8Array(buf));  } |

64バイト毎に改行を入れる関数とArrayBufferをStringにする関数は上記になります

* HTMLコード

|  |
| --- |
| <!DOCTYPE html>  <html lang="en" xmlns="http://www.w3.org/1999/xhtml">  <head>  <script lang="text/javascript" src="mycrypto.js" ></script>  <title>Sample1</title>  </head>  <body>  <div class="container">  <label >PrivateKey Generate</label><br>  <textarea id="pem-text" cols="70" rows="10"></textarea><br>  <button type="button" onclick="createCryptoKeys();">Create</button>  </div>  </body>  </html> |

mycrypto.js（先ほど作ったJavaScript）を読み込み  
createCryptoKeys()を呼ぶだけの簡単なHTMLです

* 実行結果

|  |
| --- |
| テキスト が含まれている画像  自動的に生成された説明 |

* 1. RSAキーの読み込み
  2. 作成したキーを外部サービスで使う