JavaScript による End-to-End セキュリティ

AES はどうやって使えばいいのか？ (共通鍵暗号の使い方) 編

栗原 淳

August 21, 2019

はじめに

はじめに

前回 (第 1 回) は

- 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、JavaScript での暗号 (AES) の利用のさわり

を話した。

E2E セキュリティの重要性はわかったし、AES を使ってみることもできた。

でも、実際の App で正しく・安全に AES を使うにはどうすべきなのか？

今回は正しく・安全に AES を使ってみる方法、についてのお話。

この講義で最終的に理解できること

- パスワードを使って AES を暗号化するのってどうすればいいか？
- バイナリ鍵を使って AES を暗号化するにはどうすればいいか？

「たったこれだけ」のことでも、気をつけなければならない「重要なお作法」がある。
この作法を守る・守らないで安全性は大違いなので本当に注意[1]。

[1] 世の中のソフトウェアのコード見ると、全くセオリー守ってないのがあって…本当危険…

この講義の対象と事前準備

対象:

- 暗号・セキュリティ技術に興味がある初学者
- Web に暗号技術を導入したい Web 系のエンジニア

必須ではないが触って楽しむのには必要な事前準備:

- Git が使えるようになっていること
- Node.js が使えるようになっていること
- Google Chrome 系ブラウザ and/or Firefox が利用可能なこと

AESの使い方 事始め

AES を使う際に気をつけることは、ざっと 3 点。

- AES に入れる「鍵」のランダム具合
- AES に入れる「鍵」を総当りする際の大変さ
- AES の「暗号化モード」の安全性

pbkdf2, hkdf, cbc/ctr/cfb...

AESの使い方: とりあえず暗号化してみよう

パスワードで暗号化してみる

pbkdf 使え

バイナリ鍵で暗号化してみる

hkdf 使え

危ない暗号化モードで暗号化してみる

ecb とか論外だから ctr とか使え

AESの使い方: 細かめの解説

PBKDF2ってなに？

jscu なら動くよ

HKDFってなに？

暗号化モードの種類

ctr 云々。
js でのサポート具合を列挙

まとめ

まとめ

お疲れ様でした。

-

次回以降…リクエスト次第ですが、

- 公開鍵暗号とその使い方
- 「情報が改ざんされてない」ことを保証するために（電子署名と MAC）
- RFC とアルゴリズム・フォーマット

などを予定。

宣伝 1

E2E 暗号化ファイル転送サービス「iTransfy」を提供しています。

宣伝 2

Zettant ではイケイケの仲間を募集しています。

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

Appendix

This page is not counted.