JavaScript による End-to-End セキュリティ

第 4 回 データの真正性・本人確認のためのテクニック 編

栗原 淳

2019 年 10 月 3x 日

はじめに

はじめに

第 1,2,3 回では

- End-to-End (E2E) セキュリティの原則と必要性
- JavaScript で AES を正しく・安全に暗号化する方法
- JavaScript で RSA 暗号・楕円曲線暗号を使ってを正しく・安全に暗号化する方法

を勉強した。

今回は、第 3 回で懸案事項だった「データのやり取りしてる相手って本当に正しい相手？」を保証する方法を学んでいく。

この講義で最終的に学びたいこと

-

細かい話もするが、数式は使わない。
「イメージ」と「コードの流れ＆その流れの必要性」をつかめるようにする。

発表者紹介

栗原 淳 (Jun Kurihara)

- (株) ゼタント 主任研究員
  (株) 国際電気通信基礎技術研究所 (ATR) 連携研究員
- 博士 (工学),
  専門: セキュリティ、応用数学、システムアーキテクチャとか
- Web システム (フロントエンド・バックエンド) を作ったり、論文他のアルゴリズムを実装したり、研究して論文書いたり、セキュリティ技術中心に手広くやってます。
- GitHub: `https://github.com/junkurihara`
  LinkedIn: `https://www.linkedin.com/in/junkurihara`

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:

- Bash, Git が使えるようになっていること
- Node.js, npm, yarn 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

今後の予定 (暫定)

1. 導入&JS の暗号化コードを触ってみる
2. AES を正しく・安全に暗号化するには？
3. 公開鍵暗号はどうやって使う？その使い方のコツは？
4. ハッシュ・MAC・署名、それぞれの使い所と使い方は？← 今日はココ
5. RFC にまつわるあれこれ（証明書・鍵フォーマット・etc...)

「こういうのを知りたい」というリクエストがあれば是非。
マニアックすぎて最後の RFC の話題はやるかどうか不明…

セカンドシーズンも検討中。[1]

[1] 場所等変えてもっと来やすい場所へ。。。

まとめ

まとめ

お疲れ様でした。

次回は

宣伝: iTransfy by Zettant

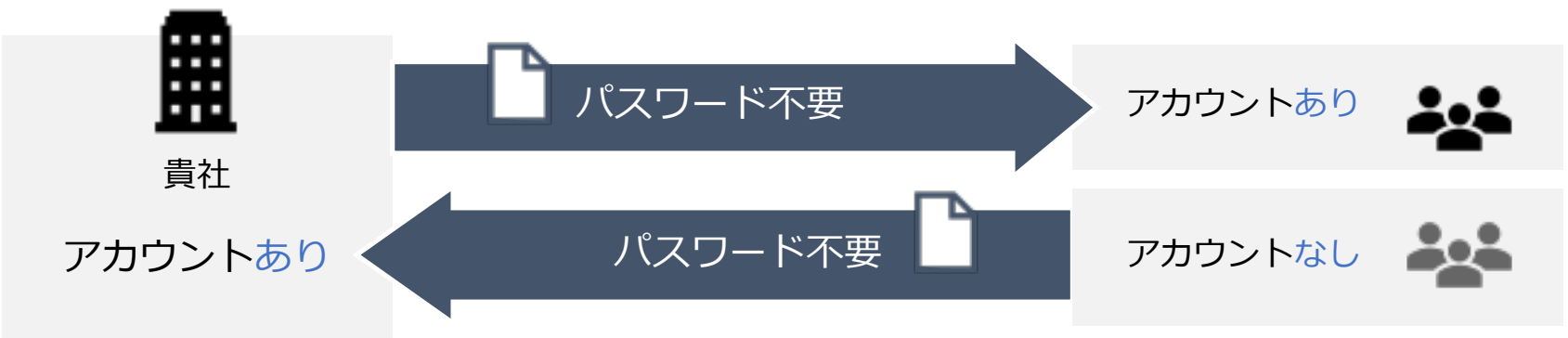
簡単・安全にファイル転送ができる

iTransfy for biz

https://www.itransfy.com

アカウント登録で、パスワード入力の手間が省けます

クライアント/協力会社等へファイルを送りたい、また送付してほしい時の手間を軽減



宣伝: 株式会社ゼタント

ゼタントはのミッションは、

「自分の身は自分で守ることができる世の中にする」

ことです。
共感してくれる仲間を募集しています！

問合せ先: recruit@zettant.com
会社 URL: https://www.zettant.com