# JavaScript による End-to-End セキュリティ

## 入門編

栗原 淳

July 24, 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

# 最近流行りの **Web** システム

# 「SSL/TLS で暗号化しているから安全です」の嘘

# End-to-End セキュリティの原則とは

# Web システムにおける End-to-End セキュリティ

導入する意味

# JavaScript で暗号を使ってみよう [基礎編]

# ブラウザでの暗号化: **WebCrypto API**

# サーバでの暗号化: **Node.js Crypto**

# ブラウザ・サーバ間での相互接続性の確認

# 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

# 引用文献

# Appendix

This page is not counted.