



## Contents

### 5 第1部 暗号の基本を学ぶ

#### 6 第1章 暗号のはなし

- Part1 暗号の基本  
方式は2種類 鍵の数で決まる
- Part2 インターネット  
証明書を使って認証と鍵交換
- Part3 無線 LAN  
4回のやり取りで二つの鍵を共有

#### 22 第2章 暗号と認証を基礎から理解する

- Part1 暗号の基礎  
暗号と認証で安全な通信
- Part2 SLの実態  
整数の性質を使った暗号を利用

#### 38 第3章 安全の“鍵”を握る暗号化

#### 42 第4章 暗号化してデータを守る

48 いまさら聞けない定番技術：AES

### 49 第2部 暗号化通信を学ぶ

#### 50 第1章 もっと使おう！やさしく丸ごと VPN

- Part1 プロローグ  
VPN はまるで社内便 仮想的な専用線を作る
- Part2 拠点間 VPN  
品質異なる3タイプ NAT 越え技術がカギ
- Part3 リモートアクセス VPN  
セキュリティ対策が重要 用途はIoTにも拡大へ
- Part4 クラウドを生かす VPN  
クラウドと拠点を直結 運用業務でも不可欠に

#### 72 第2章 Q & A で納得！VPNの疑問 10

#### 82 第3章 VPNって何なの？

#### 88 第4章 狙われるセキュリティプロトコル

- Part1 トレンドを知る  
無線 LAN や Web が脅威にさらされる
- Part2 基礎を学ぶ  
実体は「暗号技術」と「手順」
- Part3 WPA2の脆弱性「KRACKs」  
攻撃者が偽のAPでヒントを集める
- Part4 SSLの脆弱性「POODLE」  
安全性が高い TLS への移行で解決

#### 106 第5章 SSLはもう古い TLSがおもしろい

- Q1 SSLはなぜ「もう古い」なの？
- Q2 TLSが必要なのは大事な通信だけ？
- Q3 なぜTLSで安全が守れるの？
- Q4 TLS通信のステップを教えて！
- Q5 TLSの安全性はどう決まる？
- Q6 サーバー証明書は本当に安全？
- Q7 TLSはWeb専用なの？
- Q8 SSLを使えなくしたい
- Q9 暗号と数学の関係は？

#### 126 第6章 AIスピーカーで重要な会話が外部に漏れないか調査せよ！

#### 132 第7章 IoTの通信を暗号化した場合の影響を調査せよ！

#### 138 第8章 FTPS

144 いまさら聞けない定番技術：TLS

### 145 第3部 認証の基本を学ぶ

#### 146 第1章 認証って何ですか？

#### 152 第2章 PKIって何だろう？

158 いまさら聞けない定番技術：Kerberos 認証

#### 159 第3章 PKI

#### 168 第4章 認証の順序

#### 174 第5章 サーバー認証

#### 180 第6章 無線LANの認証

#### 186 第7章 RADIUS 認証を利用して安全性を高める

192 索引



# 暗号と認証

最強の指南書



## 初出 一覧

### 第1部 暗号の基本を学ぶ

#### 第1章 暗号のはなし

日経 NETWORK 2018年6月号 特集1

#### 第2章 暗号と認証を基礎から理解する

日経 NETWORK 2014年2月号 特集1

#### 第3章 安全の“鍵”を握る暗号化

日経 NETWORK 2014年2月号  
ようこそ！ネットワーク村へ

#### 第4章 暗号化してデータを守る

日経 NETWORK 2017年8月号  
Windows ネットワーク攻略術

#### いまさら聞けない定番技術：AES

日経 NETWORK 2016年11月号

### 第2部 暗号化通信を学ぶ

#### 第1章 もっと使おう！やさしく丸ごとVPN

日経 NETWORK 2016年2月号 特集1

#### 第2章 Q & A で納得！VPNの疑問10

日経 NETWORK 2016年10月号 特集2

#### 第3章 VPNって何なの？

日経 NETWORK 2017年9月号  
スッキリわかる！ネットワーク技術解説

#### 第4章 狙われるセキュリティプロトコル

日経 NETWORK 2018年1月号 特集1

#### 第5章 SSLはもう古い TLSがおもしろい

日経 NETWORK 2015年9月号 特集1

#### 第6章 AIスピーカーで重要な会話が外部に漏れないか調査せよ！

日経 NETWORK 2018年6月号  
ネットワークなんでも実験室

#### 第7章 IoTの通信を暗号化した場合の影響を調査せよ！

日経 NETWORK 2018年8月号  
ネットワークなんでも実験室

### 第8章 FTPS

日経 NETWORK 2016年1月号  
ネットワーク達人の知恵

#### いまさら聞けない定番技術：TLS

日経 NETWORK 2016年2月号

### 第3部 認証の基本を学ぶ

#### 第1章 認証って何ですか？

日経 NETWORK 2018年5月号  
スッキリわかる！ネットワーク技術解説

#### 第2章 PKIって何だろう？

日経 NETWORK 2017年10月号  
スッキリわかる！ネットワーク技術解説

#### いまさら聞けない定番技術：Kerberos 認証

日経 NETWORK 2014年1月号

### 第3章 PKI

日経 NETWORK 2016年10月号  
図解で学ぶネットワークの基礎

### 第4章 認証の順序

日経 NETWORK 2015年12月号  
ネットワーク達人の知恵

### 第5章 サーバー認証

日経 NETWORK 2016年3月号  
ネットワーク達人の知恵

### 第6章 無線LANの認証

日経 NETWORK 2017年5月号  
ネットワーク達人の知恵

### 第7章 RADIUS 認証を利用して安全性を高める

日経 NETWORK 2017年10月号  
Windows ネットワーク攻略術

※本書は、日経 NETWORK に掲載した記事を基に加筆・修正したものです。記事の内容や記事中に登場する会社名・人物・その所属・コメントなどは、掲載当時のものであることをご了承ください。