

# マンション証明書と一戸建て証明書

🔒 保護された通信 | <https://www.ij.ad.jp/>



Internet Initiative Japan



wizSafe

セキュリティ本部セキュリティ情報統括室

須賀祐治

2018-10-18

Ongoing Innovation

# 最初の「お作法」

---

- 本発表について  
開示すべき利益相反状態はありません。
- 本発表はすべて筆者の個人的見解であって  
所属組織とは無関係です。

# 自己紹介代わりに <https://www.ijj.ad.jp/news/ijjnews/>

- 今日発行されました！

## 仮想通貨と暗号技術

大きな可能性を持つがゆえに、さまざまなリスクを内包しているのが仮想通貨の仕組みと言える。  
本稿では、暗号技術の観点から、仮想通貨の課題を考えてみたい。

IJセキュリティ本部  
セキュリティ情報統括室  
須賀 祐治



当初、ビットコインは、主として行なわれたプロジェクト名性確保というモチベーション層が変化したと考えられ通信方式であるTor (The C

仮想通貨としてよく知らは、P2Pネットワークと暗の匿名性を確保しながらビットコインは、匿名の研究による論文のなかで、その八年一月に公開され、今ええます。二〇〇九年一月にThe Cryptography Mailing ました。コンセプトに続き、ビットコインは徐々に認知ニテイで利用されるように、ン黎明期に、実際に利用されの交換事例が知られていまソのものに「仮想的な」価狭い範囲の閉じた世界でンでしたが、二〇一一年一月になる通販サイトの決済方りました。匿名で決済でき注目され、ほぼ同時期にビットが急騰していることが報告

**仮想通貨を取り巻く**

# IJJ. news

IJJ was founded in 1992 as a pioneer in the commercial Internet market in Japan. Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry. The history of IJJ is indeed the history of the Internet in Japan.

October 2018

VOL.

# 148



東京オリンピック・パラリンピック競技大会  
組織委員会 会長

特別対談 人となり **森 喜朗** 氏

特集 **デジタル通貨と  
ディーカレット**



# 須賀執筆のIIRネタ(抜粋)

<https://www.ij.ad.jp/dev/report/iir/>

- Vol.39 (2018-06) ROCA(RSA実装問題)
- Vol.33 (2016-12) TLS1.3
- Vol.31 (2016-06) 耐量子暗号
- Vol.30 (2016-03) Let's Encrypt
- Vol.26 (2015-02) ID管理技術
- Vol.25 (2014-11) POODLE attack
- Vol.21 (2013-11) 仮想通貨 Bitcoin
- Vol.18 (2013-02)

暗号技術を用いたプロトコル・実装に  
多発している問題の整理とあるべき姿



# マンション証明書と一戸建て証明書

🔒 保護された通信 | <https://www.ij.ad.jp/>



Internet Initiative Japan



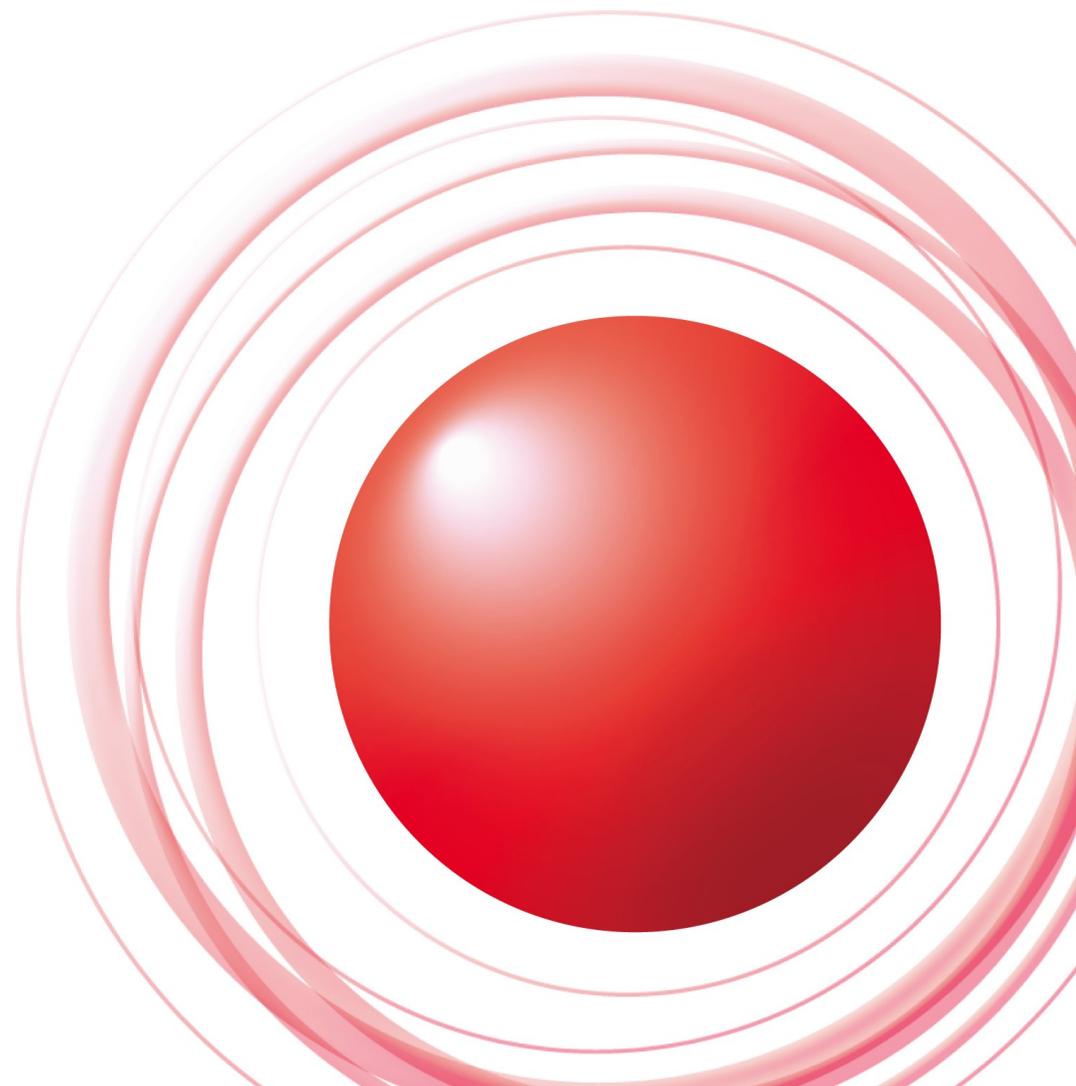
wizSafe

セキュリティ本部セキュリティ情報統括室

須賀祐治

2018-10-18

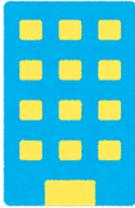
Ongoing Innovation



# タイトルからはこういうイメージ？



# 今回の発表方針とか

- Terminology 思いついたので言ってみる
  - 「一番先言うたで」というスナップショット
- VPS等でのサーバ証明書配備を調査してみるとある観点での分類ができそうなことに気がつく
  - マンション証明書  一戸建て証明書 
- メリットとかリスクとかの分析はまだできていない
  - 議論のきっかけになればいいなと
  - 忌憚なきご意見お待ちしております

# マンション証明書

Subject Alternative Name

- 異なるドメイン名がSANに共存している証明書

**Subject DN** OU=Domain Control Validated, OU=PositiveSSL Multi-Domain, CN=sni178105.cloudflaressl.com

**Issuer DN** C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2

**Serial** 37496200757866105856235991347100563408

**Validity** 2018-02-22 00:00:00 to 2018-08-31 23:59:59 (190 days, 23:59:59)

**Names**

- \*.angrycpu.com
- \*.baeb71i.ga
- \*.blockcoiners.com
- \*.cediplus.org
- \*.cellos-consortium.org
- \*.choinkidomacyno.gq
- \*.deuz39i.cf
- \*.faab52i.cf
- \*.game2cloud.com
- \*.genesequencing.gq
- \*.hellosmooth.com
- \*.jiez97i.cf
- \*.kentonchamber.org
- \*.lanicchiadelsole.altervista.org
- \*.leav11i.cf
- \*.leiq89i.ga
- \*.manhoodlose.ga
- \*.multansultan.com.pk
- \*.noem25i.ga
- \*.qwpfilmink.ga
- \*.ratanfire.in
- \*.softwarebombde.tk
- \*.sotrue.cc
- \*.soulbible.ga



VPSでお隣のVMに入居してる人の顔を知らない状況とよく似てる

<https://censys.io/certificates/2843400699468ff9439c3ec89c3ee475d8d6ae9d1ca4107cad94d54b112c5e8f>

# 一戸建て証明書

- 同組織のFQDNのみが同居する証明書

– 居候とか内縁とかヤヤコシイツッコミはやめてね

```
-----
Subject DN  C=US, ST=California, L=Mountain View, O=Google LLC, CN=*.google.com
Issuer DN   C=US, O=Google Trust Services, CN=Google Internet Authority G3
Serial      1721922324728960956
Validity    2018-10-09 13:09:00 to 2019-01-01 13:09:00 (84 days, 0:00:00)
-----
Names      *.android.com
           *.appengine.google.com
           *.cloud.google.com
           *.g.co
           *.gcp.gvt2.com
           *.ggpht.cn
           *.google-analytics.com
           *.google.ca
           *.google.cl
           *.google.co.in
           *.google.co.jp
           *.google.co.uk
           *.google.com
           *.google.com.ar
-----
```

<https://censys.io/certificates/2b51048cefd7a7aee614d2c2f90cf4121384ab63986787bac37737185f01e768>

# 一戸建て証明書(表札が一つの姓)

- 同じドメイン名のFQDNのみ同居する証明書  
– 異なるサブドメインがたくさん並ぶ

**Subject DN** C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=amazon-smtp.amazon.com

**Issuer DN** C=US, O=DigiCert Inc, CN=DigiCert Global CA G2

**Serial** 20851302682428253890987339823177204813

**Validity** 2018-04-09 00:00:00 to 2019-05-07 12:00:00 (393 days, 12:00:00)

**Names** amazon-smtp.amazon.com

smtp-fw-0101.amazon.com

smtp-fw-0102.amazon.com

smtp-fw-0103.amazon.com

smtp-fw-2101.amazon.com

smtp-fw-33001.amazon.com

smtp-fw-36001.amazon.com

smtp-fw-36002.amazon.com

smtp-fw-4101.amazon.com

smtp-fw-52001.amazon.com

smtp-fw-52002.amazon.com

smtp-fw-52003.amazon.com

smtp-fw-52004.amazon.com

smtp-fw-6001.amazon.com

smtp-fw-6002.amazon.com

<https://censys.io/certificates/31f39c4ea054b1dbbec53171dcc729f6ad6bb55ae338096c74afe5df88248d02>

smtp-fw-7002.amazon.com

# ぼっち証明書

- たったひとつのFQDNだけに対応した証明書



Certificates

692bcd68738efa3d0b92df89164c409533d17855a6ce6e21bb3b04aca5297f82



www.iij.ad.jp

SANs



www.iij.ad.jp

Certificate Trust CT ZLint 1 PEM

## Basic Information

**Subject DN** C=JP, ST=Tokyo, L=Chiyoda-ku, O=Internet Initiative Japan Inc., OU=Business Infrastructure Reformation Department, CN=www.iij.ad.jp

**Issuer DN** C=JP, O=Cybertrust Japan Co., Ltd., CN=Cybertrust Japan Public CA G3

**Serial** 470599878672442502249933270129020491131009928235

**Validity** 2017-01-25 08:19:08 to 2020-02-28 14:59:00 (1129 days, 6:39:52)

**Names** www.iij.ad.jp

Bro

<https://censys.io/certificates/692bcd68738efa3d0b92df89164c409533d17855a6ce6e21bb3b04aca5297f82>

# ぼっち証明書 (C-1戸建て証明書) の功罪

- CTの仕組みにより証明書発行するとFQDNがバレる
  - JANOG40でご紹介した Censys 等で簡単に
    - 事後資料出していないことに今頃気がつく
  - 特にごく最近発行されたものだけをピックアップすると次頁のようなことが判明してしまう

– <https://censys.io/certificates?q=>

念のため自主規制

念のため自主規制

**parsed.validity.start**

念のため自主規制

**2018-09-01**

念のため自主規制

念のため自主規制

**ev**

念のため自主規制

# よゐこのみんなは やっちゃダメよ

Apache Tomcat/8.5.29

Home Documentation Configuration Examples

## Apache Tomcat/8.5.29

If you're seeing this, you've



**Recommended Reading:**  
[Security Considerations HOW-TO](#)  
[Manager Application HOW-TO](#)  
[Clustering/Session Replication](#)

**Developer Quick Start**

[Tomcat Setup](#)      [Realms & AAA](#)  
[First Web Application](#)      [JDBC Data Sources](#)

**Managing Tomcat**

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.5 access to the manager application is split between different users.  
[Read more...](#)

**Documentation**

[Tomcat](#)  
[Tomcat](#)  
[Tomcat Wiki](#)

Find additional important configuration information in:

[tomcat-announce](#)  
 Important announcements, rele-  
 vulnerability notifications. (Low  
 tomcat-users

証明書

全般 詳細 証明のパス

 証明書の情報

この証明書の目的:

- リモート コンピューターの ID を保証する
- リモート コンピューターに ID を証明する
- 2.16.840.1.114412.2.1
- 2.23.140.1.1

\*詳細は、証明機関のステートメントを参照してください。

発行先: ██████████.go.jp

発行者: DigiCert SHA2 Extended Validation Server CA

有効期間 2018/██████████

発行者のステートメント(S)

OK

# 実はもう一枚同日発行されてる

The screenshot shows a web browser window displaying the Apache Tomcat/8.5.29 homepage. Overlaid on the browser are two windows titled '証明書' (Certificate). The top window shows the '証明書の情報' (Certificate Information) tab, listing the purpose of the certificate and the IP addresses it is intended for: 2.16.840.1.114412.2.1 and 2.23.140.1.1. The bottom window shows the '全般' (General) tab, displaying a table of certificate fields and values for two different certificates.

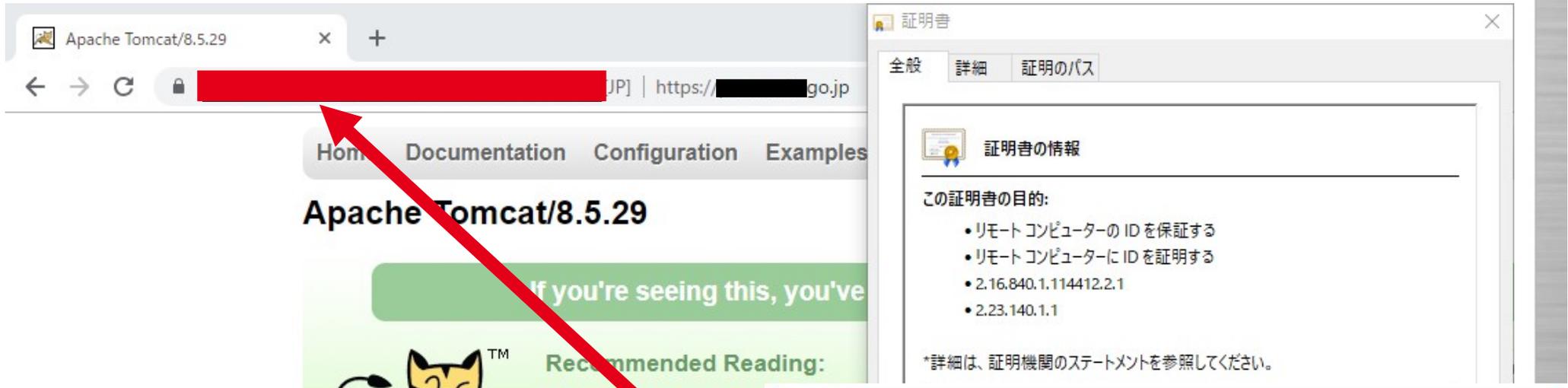
フィールド	値
バージョン	V3
シリアル番号	08232627a292757402b18aba...
署名アルゴリズム	sha256RSA
署名ハッシュアルゴリズム	sha256
発行者	DigiCert SHA2 Extended Vali...
有効期間の開始	2018年 日 9:00:00
有効期間の終了	2019年 日 21:00:00
サブジェクト	.go.jp

シリアル番号が違うのが確認できますか？

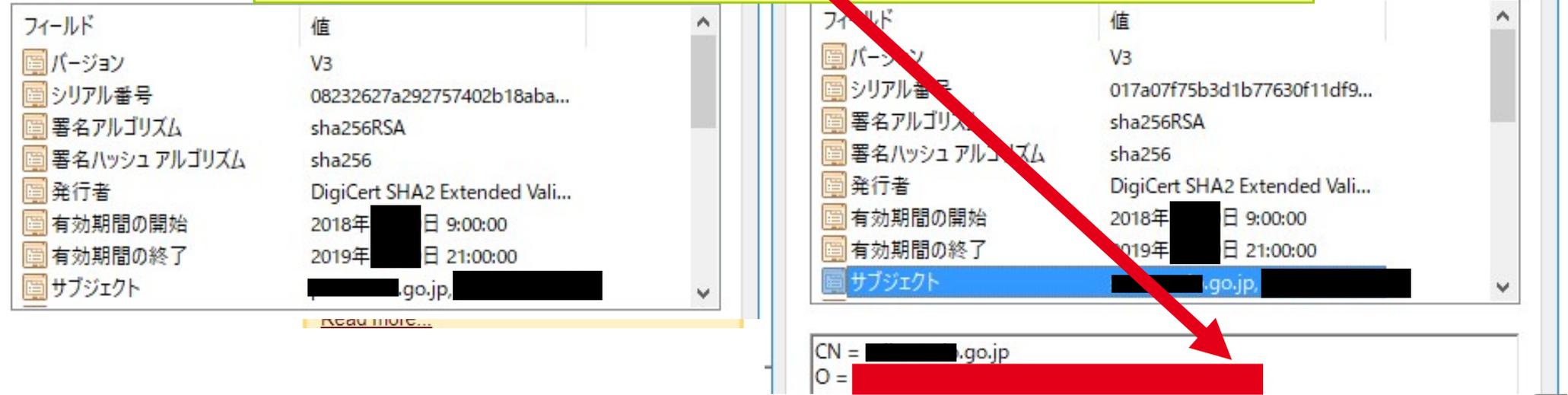
バージョン	V3
シリアル番号	017a07f75b3d1b77630f11df9...
署名アルゴリズム	sha256RSA
署名ハッシュアルゴリズム	sha256
発行者	DigiCert SHA2 Extended Vali...
有効期間の開始	2018年 日 9:00:00
有効期間の終了	2019年 日 21:00:00
サブジェクト	.go.jp

CN = .go.jp  
O =

# しかもEV証明書がアレゲ



そしてブラウザ表記は**Slerベンダー名**が記載  
これはこれまでも紹介してきたあの業界と一緒に



# ここから見えてくること

- 案外ワイルドカード証明書もアリなのかな？
- 参考情報：FAMGA

ワイルドカード証明書	<b>F</b> acebook
一戸建て証明書	<b>A</b> pple 2人同居=新婚？ <b>A</b> mazon 4人同居 <b>M</b> icrosoft 7人同居=2世帯くらい <b>G</b> oogle えらいたくさん しかも多国籍
ぼっち証明書	<b>G</b> oogle (www.google.com)

# マンション証明書のリスク

- 異なる組織が同じ鍵ペアを利用している
  - 理論的にはお隣さんのTLSトラフィック読める？
    - SNIの仕組みとかVMの独立性に依存しそう
  - (そもそも)VPSベンダーが鍵生成してるから...
  - go.jp でもマンション証明書を保持してるFQDNあり
- 自分で調べたサービスは秘密鍵が  
ぶっこ抜けなくなった
  - (いや,そこは本質じゃない)

# リモート鍵とかHSMとかで解決？

- ネットワークトポロジで分類できそう
- リモート: 鍵が必要になった時点で問い合わせ  
– レスponsできる？  
– そもそもVPS借りてる意味は？
- 物理的なHSMを預ければいいのかい？  
– コスト高いわ, 物理配送が必要で即時開通できん

# そのほか関連情報

- Chrome URL表記 www 端折る問題
  - “Trivial Subdomains” でgggrks
- TLS1.0/TLS1.1 死亡のお知らせ
  - [https://twitter.com/agl\\_/status/1051933087699881984](https://twitter.com/agl_/status/1051933087699881984)
- 2日前のChrome70でレガシー証明書死亡
  - <https://www.websecurity.symantec.com/ja/jp/blog/replace-your-symantec-ssl-tls-certificates>
- IPアドレス証明書はどう考える？
  - SANに含めた証明書事例: 1.1.1.1
    - [http://blog.livedoor.jp/k\\_urushima/archives/cat\\_30545.html](http://blog.livedoor.jp/k_urushima/archives/cat_30545.html)
- GPKIのてんmせdれfrrtgyふじこ

## Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ

---

IIJはいつもはじまりであり、未来です。

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ, Internet Initiative Japan は、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。©2016 Internet Initiative Japan Inc. All rights reserved. <http://www.iij.ad.jp/>

お問い合わせ先 IIJインフォメーションセンター  
TEL: 03-5205-4466 (9:30~17:30 土/日/祝日除く)  
info@iij.ad.jp

本書に掲載されている事柄は、将来予告なしに変更することがあります。