DNSの動向

森下 泰宏 ●株式会社日本レジストリサービス（JPRS）広報宣伝室 技術広報担当

IPフラグメンテーションの排除を目的とした「DNS flag day 2020」が計画中。「DNS over HTTPS（DoH）」も普及し始めたが、運用への影響に対する懸念も。

本稿ではDNSに関する動向として、ルートゾーンKSKロールオーバーの状況、DNS flag dayの状況、DNS over HTTPS（DoH）の状況、DNSサーバーソフトウェアの脆弱性の状況について、順に報告する。

■ルートゾーンKSKロールオーバーの状況

●ルートゾーンKSKロールオーバーとは

ルートゾーンKSKロールオーバーとは、ルートゾーンのDNSSECで使われている鍵署名鍵（KSK）を複数の作業ステップを経て、新しい鍵に更新する作業である。ルートゾーンKSKロールオーバーそのものの概要と必要な作業については、インターネット白書2018「DNSの動向」（p.255）で解説しているので、そちらを参照されたい。

●作業の状況

2017年から実施されてきた、DNSSECの運用開始後初となるルートゾーンKSKロールオーバーに関する作業は、すべて終了した。

2019年1月11日から3月22日にかけて、使われなくなった旧KSK（KSK-2010）を失効させる作業が実施された。これにより、今回のルートゾーンKSKロールオーバーにおいて、ルートサーバーの設定に影響する一連の作業ステップが完了した。上記を含め、2018年10月11日に実施された新KSK（KSK-2017）における署名開始から現在まで、本件に起因する大きな問題の発生は報告されていない。

なお、ルートサーバーの運用者の一部から、ルートゾーンの運用に影響を及ぼさない程度ではあるが、旧KSKの失効期間中にDNSKEYリソースレコードの問い合わせ数が増加したことが報告されている。

●ルートゾーンKSKロールオーバーの今後

現在行われている作業は今回の作業状況の振り返りと、次回に向けた手順の整備である。

2019年3月4日、ICANNが今回のルートゾーンKSKロールオーバーの全体状況をまとめた文書を公開した[1]。この文書は今回のルートゾーンKSKロールオーバーのすべての作業ステップとその状況についてまとめたものであり、次回以降のルートゾーンKSKロールオーバーの計画作成に役立てることを目的としている。その後、2019年11月1日にICANNがルートゾーンKSKロールオーバーの今後の実施方法に関する提案をまとめた文書を公開した[2]。

この文書における主要なポイントとして、以下

インターネット白書／ ©1996-2020 Impress R&D

の項目が挙げられる。

・KSKのライフサイクルを定義（資料3-5-1、資料3-5-2）
　スタンバイ期間を2年、アクティブ期間を3年とする
・KSKの鍵長・アルゴリズムの変更については、本文書の対象としない
　それらを実施する際には、計画を別途作成する

　本文書に関するパブリックコメントが、2019年11月11日から2020年2月21日まで実施されている[3]。今後、パブリックコメントへの対応・メーリングリストでの議論などを経て、次回以降のルートゾーンKSKロールオーバーの計画がまとめられる予定である。

■DNS flag dayの状況

●DNS flag dayとは

　DNS flag day[4]とは、DNSに関する重要な変更について、歩調を合わせて実施する日として準備を進めている関係者により名付けられたものである。

●DNS flag day 2019の状況

　2019年のDNS flag dayは当初「DNS flag day」として実施され、その後に「DNS flag day 2019」という名称に改められた[5]。DNS flag day 2019では、2019年2月1日以降にリリースされる主要なDNSソフトウェアにおけるEDNS0[6]に関する動作が変更された。DNS flag day 2019が実施された背景とその影響については、インターネット白書2019「DNSの動向」（p.204-208）で解説しているので、そちらを参照されたい。

▼DNS flag day 2019の影響に関する注意点

　現在まで、DNS flag day 2019に起因する大きな問題の発生は報告されておらず、公式サイトには「非常に成功したイベントであった」旨が記載されている（『was a very successful event』）」。しかし、DNS flag day 2019で動作が変更されたフルリゾルバーの実装は最新のメジャーバージョンのみであり、BINDでは9.14.0以降、Unboundでは1.9.0以降となっている。そのため、今後フルリゾルバーの新しい実装の普及に従い、DNS flag day 2019に起因する問題が顕在化する可能性が残されていることに留意する必要がある。

●DNS flag day 2020

　DNS flag day 2019の「成功」を受け、DNS関係者の間でDNS flag day 2020の実施が計画されている[7]。

▼DNS flag day 2020の背景／理由

　DNS flag day 2020では、DNSからのIPフラグメンテーションの排除を主な目的としている。IPフラグメンテーションはIPパケットを中継する際、通過するリンクまたはネットワークで扱える最大転送単位（MTU：Maximum Transmission Unit）に従って、大きなIPパケットを分割することである。IPフラグメンテーションは、サイズの大きなIPパケットを、そのIPパケットのサイズより小さなMTUを持つネットワークを通して中継する際に必要になる。

　しかし、インターネット上にはIPフラグメンテーションを正しく扱えない機器・環境が数多く存在することが報告されている[8][9]。またDNS応答がIPフラグメンテーションによって断片化されることに起因する、セキュリティ上の問題も指摘されている[10]。

　こうした状況から、DNS flag day 2020ではDNSからのIPフラグメンテーションの排除に

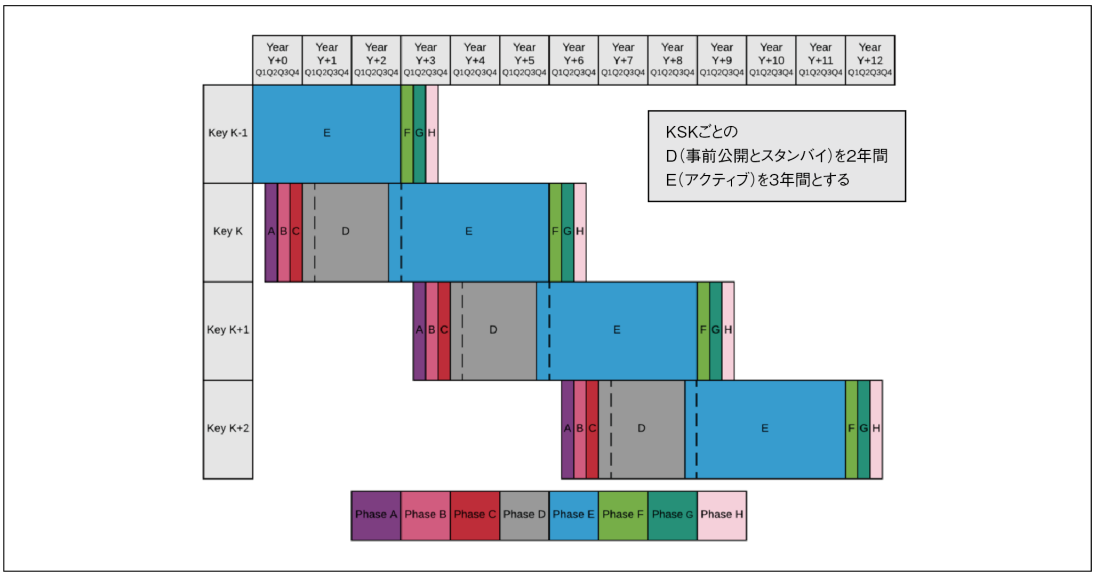
インターネット白書／ ©1996-2020 Impress R&D

資料3-5-1　KSKロールオーバーにおける各フェーズとその説明

フェーズ	説明
A：生成	新しいKSKを生成、1番目のKMF（鍵管理のための設備）で管理
B：複製	新しいKSKを2番目のKMFに複製
C：最初の鍵セット署名	新しいKSK公開鍵を含む最初の鍵セットを、公開準備のために署名
D：事前公開とスタンバイ	新しいKSKを、DNSKEY RRsetの一部としてルートゾーンで事前公開
E：ロールオーバーとアクティブ	新しいKSKで、DNSKEY RRsetを署名（新しいKSKをアクティブに）
F：失効	以前のKSKに失効ビットを設定、失効完了後にルートゾーンから削除
G：最初の削除	以前のKSKを1番目のKMFから削除
H：最後の削除	以前のKSKを2番目のKMFから削除（以前のKSKは完全に消滅）

出典：https://www.icann.org/en/system/files/files/proposal-future-rz-ksk-rollovers-01nov19-en.pdf の記述を翻訳

資料3-5-2　KSKのロールオーバーサイクル



出典：https://www.icann.org/en/system/files/files/proposal-future-rz-ksk-rollovers-01nov19-en.pdf

焦点が当てられることとなった。IPフラグメンテーションを発生させないようにUDPで取り扱うDNSメッセージのサイズを制限し、大きなサイズのDNSメッセージをTCPで取り扱うようにすることで、IPフラグメンテーションに起因する問題の回避を図っている。

▼DNSメッセージサイズに関する考察

DNS flag day 2020に際し、IPフラグメンテーションを発生させないようにするためのDNSメッセージサイズの推奨値が、関係者の間で検討された[11]。その結果、現在のほぼすべてのネットワークにおいてIPフラグメンテーションの発生を回避可能な値として、IPv6における最小MTUである1280バイトからIPv6ヘッダー40バイトとUDPヘッダー8バイトを引いた、1232バイトが選択された。

●DNS flag day 2020における推奨項目

DNS flag day 2020に対応するための権威DNS

インターネット白書／©1996-2020 Impress R&D

サーバー・フルリゾルバー（キャッシュDNSサーバー）・DNSソフトウェアにおける推奨項目が、公式サイトで公開されている。

・UDPにおけるDNSメッセージサイズの最大値を1232バイトに設定する
・DNSメッセージをUDPとTCPの双方で適切に取り扱えるようにする

いずれも、IPフラグメンテーションを発生させないようにするためのものである。

▼権威DNSサーバーにおける推奨項目
権威DNSサーバーにおける推奨項目は、以下の3つである。

①UDP/53とTCP/53の双方でサービスを提供すること
②EDNSバッファサイズとして、1232バイトを設定すること
③EDNSバッファサイズより大きなDNS応答をUDPで送信しないこと

▼フルリゾルバーにおける推奨項目
フルリゾルバーにおける推奨項目は、以下の3つである。なお、①と②は、権威DNSサーバーとフルリゾルバーの双方で共通に推奨されている。

①UDP/53とTCP/53の双方でサービスを提供すること
②EDNSバッファサイズとして、1232バイトを設定すること
③権威DNSサーバーからのDNS応答が切り詰められていた場合、同じ問い合わせをTCPで再送すること

▼DNSソフトウェアにおける推奨項目
DNSソフトウェアにおける推奨項目は、以下の2つである。

①DNSの標準仕様に合致していること
②EDNSバッファサイズのデフォルト値を1232とすること

●DNS flag day 2020への対応

▼各組織における対応が必要
DNS flag day 2020では、各組織が運用する権威DNSサーバー／フルリゾルバーにおける対応・必要に応じた設定変更が必要になる。DNS flag dayの公式サイトにおいて、権威DNSサーバー・フルリゾルバーにおける対応状況の確認方法と、主要なDNSソフトウェアにおけるENDSバッファサイズを設定する方法が紹介されているので参考にされたい（資料3-5-3）。
▼DNS flag day 2020の実施時期
2020年1月現在、DNS flag day 2020の実施日は未定であり、コミュニティによる検討が進められている。議論はオープンな場で進められており[12]、誰でも参加できる。

■DNS over HTTPS（DoH）の状況

●DoHとは

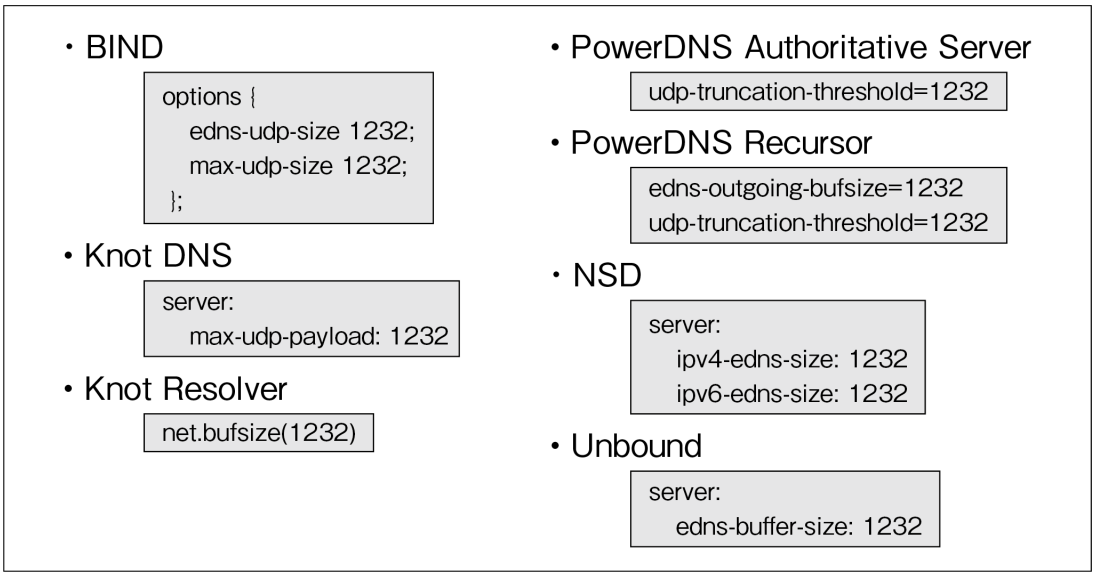
DNS over HTTPS（DoH）は、DNSの通信にWebの通信で使われるHTTPSを使って、通信路の保護／暗号化を実現するためのプロトコルである。DoHの概要については、インターネット白書2019「DNSの動向」（p.210）で解説しているので、そちらを参照されたい。

●DoHのサポート状況

プライバシー保護に対する意識の高まりを受け、DNSの実装・サービスにおけるDoHのサポー

インターネット白書／ ©1996-2020 Impress R&D

資料3-5-3　主要なDNSソフトウェアにおけるEDNSバッファサイズの設定方法



出典：https://dnsflagday.net/2020/#how-to-test から引用

トが急速に進んでいる。

▼フルリゾルバーにおけるサポート

Google Public DNSをはじめとする主要なパブリックDNSサービスにおけるサポートに加え、国内の事業者では2019年5月にIIJが、「IIJ Public DNS」の試験サービスを開始した[13]。

▼アプリケーション・OSにおけるサポート

WebブラウザーではFirefox 62以降、Chrome 78以降のバージョンでDoHが標準サポートされており、利用可能である。AndroidではGoogleの持株会社Alphabetの子会社であるJigsawが開発した、Intraをインストールすることで、DoHの利用が可能になる[14]。また、Microsoftも将来のWindowsにおいて、DoHを標準サポートする旨を発表している[15]。

●DoHに対する懸念事項

実装やサービスへの急速な展開が進む一方、一部の識者からはDoHの普及に対する懸念を示す声も挙がっている。以下、現在挙がっている主な懸念点について説明する。

▼各組織の管理ポリシーをバイパスされるリスク

組織内ネットワークや家庭内ネットワークにおいて、ポリシー上特定のサイトやサービスへのアクセスを制限する際の手段の一つとしてDNSブロッキング[16]が利用されている。組織内の利用者がDoHで外部のDNSサービスを使うようになることで、DNSブロッキングで実現されている組織内ネットワークにおけるアクセス制限や家庭内ネットワークにおけるペアレンタルコントロールといった、各組織の管理ポリシーをバイパスされるおそれがある。

▼セキュリティ上のリスク

インターネット白書／©1996-2020 Impress R&D

以前から、DNS通信を利用した遠隔操作ウイルスの制御や情報の抜き取りを図るマルウェアの活動が報告されている。こうしたマルウェアがDoHに対応することで、通信内容の判別や不正な通信のブロックといった対策が困難になるおそれがある[17]。

▼サービス提供者への情報の集中化

DoHの普及により、特定の大手パブリックDNSサービス事業者に利用者のアクセス情報が集中するおそれがある。こうした、いわゆる「DNSの中央集権化」に対し、DNSの技術的な面・メタデータの取り扱いの面の双方から、懸念の声が上がっている[18]。

●今後の展望

DoHはIETFにおけるプロトコルの標準化と実装／サービスにおけるサポートが先行し、各組織における取り扱いや運用の仕組み作り、事業者が提供するサービスの仕様、取得する情報の透明化など、課題の解決が後手に回っている状況である。IETFの場でもこうした課題は認識されており、2019年11月に開催されたIETF 106において、アプリケーションにおけるDNSの取り扱いについて議論するためのApplication Behavior Considering DNS (abcd) BoFが開催されている[19]。

■DNSサーバーソフトウェアの脆弱性の状況

●BINDの脆弱性の状況

資料3-5-4に、2019年中にJPRSが注意喚起したBINDの脆弱性の一覧を示した。

2019年のBINDの脆弱性の報告件数は9件と、昨年の6件に比べ、再び増加傾向となった。その原因の一つとして、IETFにおけるDNSに関する活発な標準化活動と、それを受けたBINDへの機能追加が挙げられる。BINDは以前からRFCのリファレンス実装の役割を果たしており、標準化活動の進行に伴い、実装される機能が増加することになる[20]。

すなわち、

・標準化された機能が実装され、BINDの内部構造やロジックが複雑化する
・複雑化することで、脆弱性が含まれるリスクが増大する

という状況が発生することになる。

そのため、本件は「DNS Camel」として、IETFの場で問題提起された[21]。こうした状況は開発元のISCも認識しており、BINDの複雑なコードを単純化してメンテナンスコストと脆弱性のリスクを下げる、リファクタリングが進められている[22]。

●BIND以外のDNSソフトウェアの状況

資料3-5-5に、2019年中にJPRSが注意喚起したBIND以外のDNSソフトウェアの脆弱性の一覧を示した。

利用可能なDNSソフトウェアの多様化に伴い、BIND以外のDNSソフトウェアの脆弱性がコンスタントに報告されるようになっている。

DNSにはプロトコル・実装・運用の三つの要素があるが、運用が特に重要である。そのため、運用に関する動向に注意し、各組織において必要に応じた対応をとることが肝要である。

インターネット白書／ ©1996-2020 Impress R&D

資料3-5-4　2019年にJPRSが注意喚起したBINDの脆弱性

公開・更新日	タイトル
2019/11/21	（緊急）BIND 9.xの脆弱性（システムリソースの過度な消費）について（CVE-2019-6477）
2019/10/17	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2019-6476）
2019/10/17	BIND 9.xの脆弱性（mirror zones機能におけるDNSSEC検証のバイパス）について（CVE-2019-6475）
2019/6/20	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2019-6471）
2019/4/25	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2019-6467）
2019/4/25	（緊急）BIND 9.xの脆弱性（ファイル記述子の過度な消費）について（CVE-2018-5743）
2019/2/22	（緊急）BIND 9.xの脆弱性（メモリリークの発生）について（CVE-2018-5744）
2019/2/22	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2018-5745）
2019/2/22	BIND 9.xの脆弱性（アクセス制限の不具合によるゾーンデータの流出）について（CVE-2019-6465）

出典：JPRS DNS関連技術情報（https://jprs.jp/tech/）

資料3-5-5　2019年にJPRSが注意喚起したBIND以外のDNSソフトウェアの脆弱性

公開・更新日	タイトル
2019/12/6	Knot Resolverの脆弱性情報が公開されました（CVE-2019-19331）
2019/11/20	Unboundの脆弱性情報が公開されました（CVE-2019-18934）
2019/10/4	Unboundの脆弱性情報が公開されました（CVE-2019-16866）
2019/8/22	NSDの脆弱性情報が公開されました（CVE-2019-13207）
2019/8/8	PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2019-10203）（更新）
2019/7/12	Windows DNS Serverの脆弱性情報が公開されました（CVE-2019-0811）
2019/7/12	Windows DNSキャッシュリゾルバーサービスの脆弱性情報が公開されました（CVE-2019-1090）
2019/7/12	Knot Resolverの脆弱性情報が公開されました（CVE-2019-10190、CVE-2019-10191）
2019/6/24	PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2019-10162、CVE-2019-10163）
2019/3/20	PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2019-3871）
2019/1/23	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2019-3806、CVE-2019-3807）

出典：JPRS DNS関連技術情報（https://jprs.jp/tech/）

1. Review of the 2018 DNSSEC KSK Rollover
https://www.icann.org/review-2018-dnssec-ksk-rollover.pdf
2. Proposal for Future Root Zone KSK Rollovers - ICANN
https://www.icann.org/news/announcement-2-2019-11-01-en
3. Proposal for Future Root Zone KSK Rollovers - ICANN
https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en
4. 「flag day」は国旗の制定のような、歴史的な出来事を祝うために確保された祝日のことである。
5. 2019 | DNS flag day
https://dnsflagday.net/2019/
6. RFC 6891で定義されるDNSの拡張方式。512バイトよりも大きなメッセージサイズを通信コストの低いUDPで扱えるようにし、応答のフラグや応答コードも拡張する。
7. 2020 | DNS flag day
https://dnsflagday.net/2020/index-ja.html
8. draft-ietf-intarea-frag-fragile - IP Fragmentation Considered Fragile
https://tools.ietf.org/html/draft-ietf-intarea-frag-fragile
9. IPv6, Large UDP Packets and the DNS
https://www.potaroo.net/ispcol/2017-08/xtn-hdrs.html
10. Measures against cache poisoning attacks using IP fragmentation in DNS
https://indico.dns-oarc.net/event/31/contributions/692/
11. flag day 2020: Recommended EDNS buffer size ・Issue #125
https://github.com/dns-violations/dnsflagday/issues/125
12. Flag Day 2020: The date ・Issue #139
https://github.com/dns-violations/dnsflagday/issues/139
13. IIJ Public DNSサービス

インターネット白書／©1996-2020 Impress R&D

https://public.dns.iij.jp/

14. Intra
https://getintra.org/

15. Windows will improve user privacy with DNS over HTTPS
https://techcommunity.microsoft.com/t5/Networking-Blog/Windows-will-improve-user-privacy-with-DNS-over-HTTPS/ba-p/1014229

16. JPRS 用語辞典｜ DNS ブロッキング
https://jprs.jp/glossary/index.php?ID=0189

17.「DNS Queries over HTTPS」（DoH）プロトコルを悪用するマルウェアが出現- ZDNet Japan
https://japan.zdnet.com/article/35139444/

18. インターネットをより安全にする技術「DoH」に対して大手 ISP が抱える懸念とは？- GIGAZINE
https://gigazine.net/news/20191002-concern-dns-over-https/

19. 第 106 回 IETF Meeting（シンガポール）報告| 2019 年| ドメイン名関連会議報告| ドメイン名関連情報| JPRS
https://jprs.jp/related-info/event/2019/1225IETF.html
注：12 月 25 日公開を前提とした仮の URI

20. The Development of BIND, Tracking the Growth of the DNS and DNS
Standards Over 30 Years | Presentation - ICANN
https://www.icann.org/resources/files/1217015-2018-07-13-en

21. The DNS Camel, Or How many features can we add to this protocol
before it breaks?
https://datatracker.ietf.org/meeting/101/materials/slides-101-dnsop-sessa-the-dns-camel-01

22. BIND 9 Refactoring - Internet Systems Consortium
https://www.isc.org/blogs/bind-9-refactoring/

インターネット白書／ ©1996-2020 Impress R&D

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2020年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp

©1996-2021 Impress R&D