情報セキュリティの動向

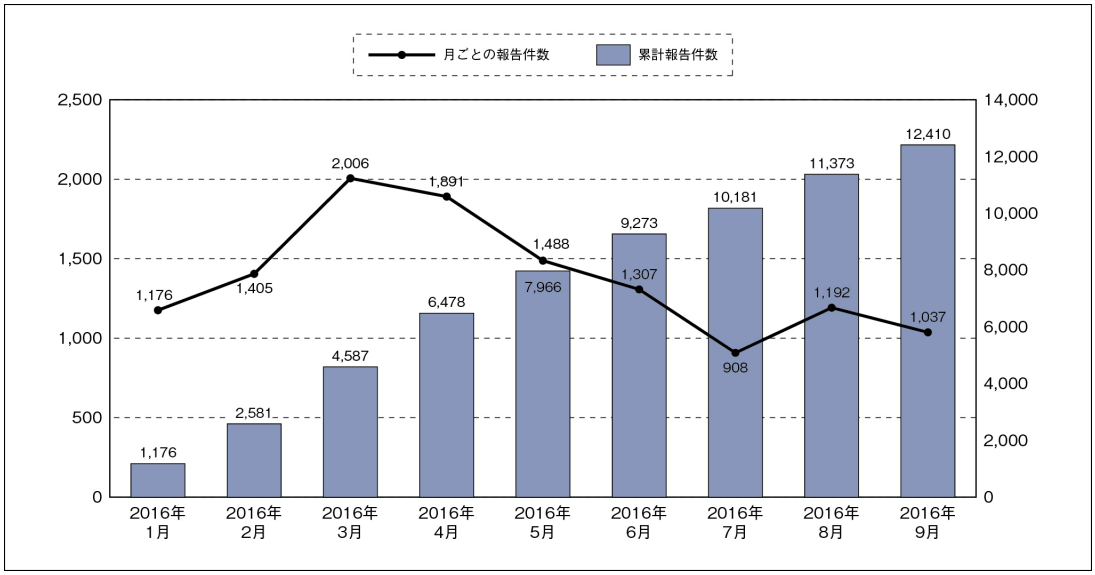
青木 翔 ●一般社団法人JPCERTコーディネーションセンター 早期警戒グループ 情報分析ライン 情報セキュリティアナリスト

組織において高度サイバー攻撃への対策は進んでいるものの、多様な攻撃集団の台頭や攻撃手段の巧妙化によって、被害が継続して発生している。DDoS攻撃や金銭窃取を目的とした攻撃についても攻撃の規模が拡大しており、有事に備えた事業継続計画が必要となりつつある。

■セキュリティインシデントの報告件数

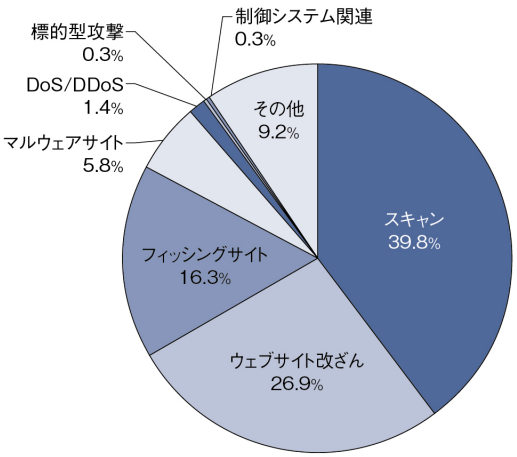
2016年1～9月にJPCERTコーディネーションセンター（JPCERT/CC）に報告された情報セキュリティインシデント（以下、インシデント）件数は、1万2410件となった（資料4-1-1）[1]。DoS/DDoSについては151件と、2013～2015年における報告件数（120件前後）に比べて増加傾向となった（資料4-1-2）。

資料4-1-1 インシデント報告件数の推移（2016年1～9月）



出典：「JPCERT/CC インシデント報告対応レポート」を基に作成

資料4-1-2　インシデントカテゴリー別割合（2016年1〜9月）



スキャン	4,272件（−3,135件）	↘
ウェブサイト改ざん	2,887件（＋　854件）	↗
フィッシングサイト	1,754件（＋　275件）	→
マルウェアサイト	618件（＋　42件）	→
DoS/DDoS	151件（＋　27件）	↗
標的型攻撃	31件（−　88件）	↘
制御システム関連	31件（＋　22件）	↗
その他	991件（−　683件）	↘

※（）内の数値は前年同期間からの変動値

出典：「JPCERT/CCインシデント報告対応レポート」を基に作成

■主なインシデントカテゴリーの傾向

●ウェブサイトの改ざん

ウェブサイト改ざんについて2016年1〜9月に報告された件数は2877件と、前年同期間（2033件）よりも増加した。

2016年11月には、JPCERT/CCや警察庁がウェブサイト改ざんに関する注意喚起[2]を公開した。その注意喚起では、ウェブサイトのコンテンツが改ざんされ、ウェブサーバー上に不正に設置されたファイルへアクセスするよう誘導される事例を挙げ、対策を呼び掛けた。

ウェブサイト管理者は、管理するウェブサイトやウェブサーバーを守るため、使用している製品やソフトウェアの脆弱性情報を収集して速やかに修正プログラムを適用し、システム管理用のパスワードを適切に管理するほか、意図しないファイルの設置やコンテンツの改ざんなどにいち早く気付くため頻繁にマスターファイルとの差分を比較するといった対策が引き続き求められる。

●DDoS攻撃

2016年は、アノニマス（Anonymous）と呼ばれる攻撃者集団によって国内のウェブサイトのサービスが停止する事例が数多く見られた。攻撃の目的は、捕鯨などへの抗議活動のためにサービスを停止させて攻撃者の威力を誇示することにあるといわれている。攻撃を避けるための計画的なサービス停止であっても、サービスを止めさせたとして攻撃者を勢いづかせた事例も見られ、慎重な対応が求められた。

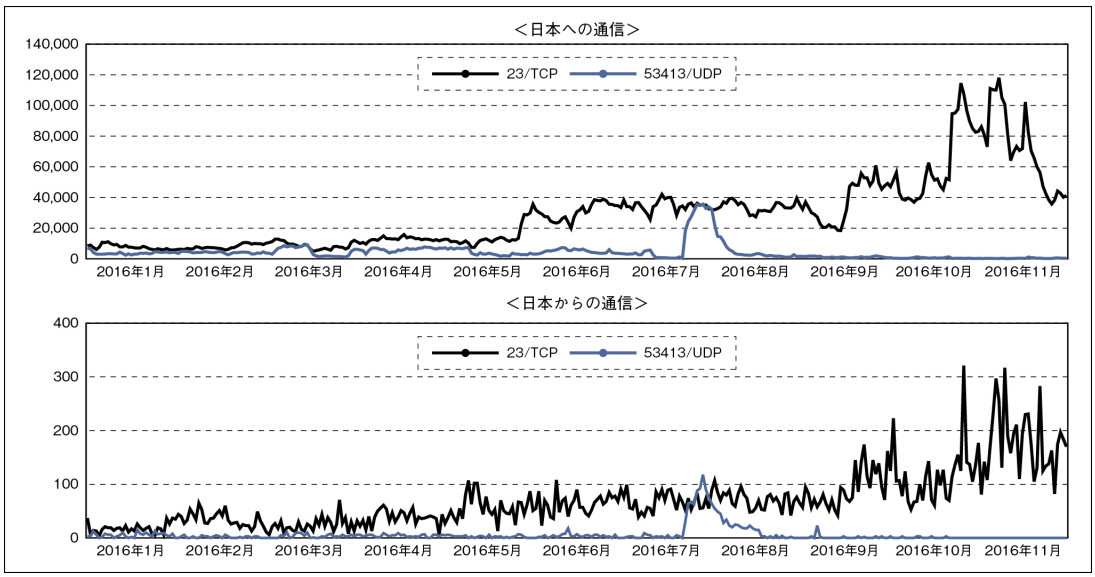
世界的にも、マルウェア「Mirai」などに感染した機器がBotnetを形成して行われた大規模なDDoS攻撃が大きな話題となった。このマルウェアは、Telnetポート（23/TCP）など端末を遠隔操作できるサービス機能を対象としており、監視カメラや特定産業向けの組み込み通信機器、ルーター、サーバーなどが狙われた。この攻撃は、脆弱な認証情報に対し辞書攻撃を行ったり、任意のコードが実行可能な脆弱性を悪用したりして、機器をマルウェアに感染させBot化する。

DDoS攻撃の際に発生したトラフィックは1Tbps近くにも及んだといわれており、対策されたシステムでも耐えがたい攻撃規模となった[3]。

JPCERT/CCが運用する定点観測システム「TSUBAME」では、脆弱な機器の探索活動に用いられるとされている23/TCPや53413/UDPの通信量は国内向け／海外向け共に増加を確認している（資料4-1-3）。これらのうち、一定量はマルウェアの活動によるものと推測される。

Miraiは揮発メモリ上にしか存在しないことから、感染しても機器を再起動すれば除去できるものの、認証情報を変更しない限り再感染する恐れが高い。このように、保有する機器を正確に把握し適切に設定管理することが、機器の管理者に求められている。

資料4-1-3　特定ポート宛てのパケット数の推移（2016年1〜11月）



出典：JPCERT/CCのインターネット定点観測システム「TSUBAME」のデータを基に作成

●金銭搾取を目的とした攻撃

警察庁が発表したデータによると、2016年上半期（1〜6月）に発生したインターネットバンキング利用に係る不正送金の被害について、信用金庫や法人口座の被害額と被害件数は共に、大幅に減少した（被害額は2016年上半期が8億9800万円、2015年下半期が15億3000万円）[4]。しかし、個人口座においては平均すると2015年と同水準の被害額と被害件数であることから、今後も対策を続けることが重要である。

加えて、2016年もインターネットバンキングのID・パスワード情報を窃取するマルウェアが、日本語を含むスパムメールに添付されて国内に送付されていることが確認された。たとえばUrsnif（別名：Gozi、Snifula）[5]、Shiotob（別名：URLZone、Bebloh）[6]、KRBANKER[7]といった、海外で被害を引き起こしたマルウェアが、国内でも使われ始めていた。

ランサムウェアも、2015年に引き続き猛威を振るった。トレンドマイクロによると、2016年上半期にランサムウェアに感染した国内組織は1740組織に達し、2015年に比べて急増している[8]。同

社が英国で行った調査では、ランサムウェアで暗号化されたファイルの約半数は被害者が金銭を支払った場合でも復元できなかったとされていることから、定期的なバックアップなどの事前対策が重要である。

このような金銭窃取を目的とした攻撃では、マルウェアが添付されたスパムメールや、改ざんされたウェブサイト経由の感染が報告されている[9]。マルウェアの感染を防ぐために、OSやアプリケーションの修正プログラムを早急に適用して脆弱性を除くことや、ウイルス対策ソフトを最新の状態に維持し定期的にウイルススキャンを行うことが望ましい。

■高度サイバー攻撃に関する動向

2015年に大きな話題となった高度サイバー攻撃は、企業の規模や種類を問わず、2016年も多くの被害を発生させた。活発な攻撃グループやその手法、使用されるマルウェアは常に変化している。そのため、各組織が属する業界内で情報を共有することでサイバー攻撃の動向を迅速に入手し、組織内で攻撃を早期に検知するために実施している対策に反映させていくことが求められている。

●高度サイバー攻撃で用いられたマルウェア

JPCERT/CCは2016年1〜9月の期間に、31件の高度サイバー攻撃に関連したインシデント対応を行った。その結果、DaserfやAsurex、Elirksと呼ばれる遠隔操作マルウェアに関するインシデントが多く見られた。攻撃者は、これらのマルウェアを攻撃対象とした組織の端末に感染させることでその組織へ侵入して組織内のネットワーク構成を把握し、機密情報を窃取する。

マルウェアへの感染は、関係者を装った標的型メールに添付されているファイルの開封や、ウェブサイトを経由した攻撃（水飲み場型攻撃）などで試みられる。関係者を装った標的型攻撃では、組織内の人間とSNSなどで日常業務に関するやりとりを行って添付ファイルの開封を誘導するなど、手口が巧妙なものも確認された。

●遠隔操作に関する攻撃手法の巧妙化

攻撃者は、組織内の端末をマルウェアに感染させると、次に、インターネット上のCommand & Control（C2）サーバーを経由して端末を遠隔操作し、情報窃取を試みる。2015年に話題となったEmdiviを用いた攻撃活動ではC2サーバーなどの攻撃インフラを複数組織への攻撃活動に用いていたが、2016年のDaserfを用いた攻撃活動では攻撃対象組織ごとに異なるC2サーバーを用いるだけでなく、同一組織の感染端末ごとにC2サーバーを使い分けていた。そのため、ドメインやURLなどを用いたブラックリスト型での対策が難しく、攻撃者が組織内に潜伏し、長期にわたって情報が収集され続ける恐れがある。

また、Elirksでは、Windowsの起動時に特定のブログやSNSにアクセスし、そこからC2サーバーの情報を取得する手法が用いられている[10]。これは、セキュリティ対策製品の振る舞い検知を回避するためとみられる。さらに、ブログやSNSに投稿されている記事の内容を攻撃者が変更することでC2サーバーを切り替えられるため、ブラックリストによる遮断も回避できる。

こうしたマルウェアを用いた攻撃を早期に発見するためには、プロキシやファイアウォールなどのログを定期的に確認することが重要である。加えて、端末の使用時間や組織内で使用しているソフトウェアなどを把握し、ログと実際の使用状況が想定と異なった通信に着目して調査を進めていくことをお勧めする。

●ADのドメイン管理者権限の悪用

組織内の端末を遠隔操作できるようにした後、多くの攻撃者は、より有益な情報を窃取するために権限が高いユーザーのアカウントの乗っ取りを試みる。なかでも、組織ネットワーク内のユーザー端末の認証機能やサービスを利用するためのチケット管理機能を有するActive Directory（以下、AD）のドメイン管理者権限を不正に利用するケースが多く見受けられる。

たとえば、ADのドメイン管理者権限を窃取するために、Kerberos認証の仕組みを悪用したチケットを不正に生成し使用したと推測される事例が確認された。この場合、攻撃者は半永久的にリソースへのアクセスが可能となる。不正なチケットの生成には、ADのドメインコントローラを含む組織ネットワーク内のリソースの管理者権限が必要となるため、それらのリソースおよびリソースを管理するアカウントと端末を限定し認証情報を適切に管理することが、こうした事態を防ぐための対策である。

さらに、セキュリティパッチの適用やWindowsのバージョンアップを適切に実施することにより、セキュリティ強化を図ることも推奨される。

●対応体制の整備

高度サイバー攻撃など複雑化するインシデントの発生を早期に検知し被害を局所化するため、組織内CSIRTの構築整備も活発に進められた。「サイバーセキュリティ経営ガイドライン」[11]が公開された影響もあって、組織内CSIRT間の連携や情報共有を目的とした日本シーサート協議会の参加組織数は2016年12月1日の段階で198組織と、2015年の106組織からほぼ倍増し、今後もCSIRT構築の動きが広がると見込まれている。

JPCERT/CCは2016年3月に「高度サイバー攻撃（APT）への備えと対応ガイド〜企業や組織に進める一連のプロセスについて」を公開し、高度サイバー攻撃に備え、対応する際の戦略やポリシー、手順について記載した参考文書を公開した。同年6月には「CSIRT構築および運用における実態調査」として、国内のCSIRTの組織体制やポリシーなどについて調査し、集計・分析を行った結果も公開している。情報処理推進機構（IPA）では「企業のCISOやCSIRTに関する実態調査2016」と題して、企業経営者の情報セキュリティ対策に対する関与や組織的な対策状況に関する調査結果を公開している。このような資料を参考にして、自組織のセキュリティ対応体制づくりの整備に努めていただきたい。

■脆弱性に係る動向

2016年は、Javaのウェブアプリケーションを作成するためのソフトウェアフレームワークであるApache Strutsの脆弱性や、DNSサーバーのソフトウェアであるBINDの脆弱性のほか、デシリアライズ処理の実装に脆弱性を含むソフトウェアが複数発見されたことが話題となった。ここでは、特に注目された脆弱性や、脆弱性に関する動向を紹介する。

●シリアライズ／デシリアライズの処理に起因する脆弱性

シリアライズとは、状態をもつオブジェクトを送受信したりファイルに読み書きしたりするために、バイト列などに変換することである。デシリアライズとは、逆に、バイト列などからオブジェクトを復元することを表す。

2015年11月に米Apache Software Foundationから、Java言語のライブラリであるCommons Collectionsに存在する、デシリアライズ処置の実装に起因した脆弱性とその攻撃手法が公開された。本脆弱性は遠隔から任意の

コードを実行できるものであり、この脆弱性をもつサーバーを探索する活動が確認されたことが警察庁から報告された[12]。CMSのMagento 2やJoomla!でも、実装言語であるPHPのデシリアライズ処理に起因する脆弱性が報告されている。

これらの脆弱性は、シリアライズ／デシリアライズの処理において、信頼できない相手からのデータを検証せずに処理することに原因がある。そのため、JPCERT/CCが公開するセキュアコーディングガイドを参考に入力データの検証を行うことや、デシリアライズ時に自動的に実行される処理に注意して実装を行うことが推奨される[13]。

●Apache Struts 2の脆弱性

オープンソースのウェブアプリケーションの開発フレームワークであるApache Struts 2に、リクエストを適切に検証していないために遠隔から任意のコードを実行できる複数の脆弱性と、その実証コードが相次いで報告された[14]。脆弱性を悪用した攻撃ツールが公開されていることや、本脆弱性を標的としたアクセスを確認していることが警察庁からも報告され、脆弱性を修正したバージョンへのアップデートが急がれた[15]。

セキュリティアップデートが基本的な対策であるが、使用していない機能を無効化することも有効である。ウェブアプリケーションの脆弱性を狙った攻撃には通信に特徴的なパターンが見られるケースも多いので、Web Application Firewall（WAF）を導入して、そうした通信パターンを検知するためのルール（シグネチャ）を定義し、最小限のシステム変更で攻撃の被害を抑止する方法も回避策として有効である。

■制御システムセキュリティの動向

国内でも海外でも報道に至るような重大なサイバーインシデント事例は、2015年末のウクライナの発電所に対するサイバー攻撃以降、見られなかった。しかし、2016年8月に米FireEyeが報告した制御システム機器に関する統計資料によると、脆弱性の報告件数は増加傾向にあることが分かる[16]。2010年と2015年の脆弱性の報告件数を比較すると約7倍にもなっており、制御システムにおけるリスクが高まっていると言える。

IPAは、制御システムユーザー企業を対象としてセキュリティに対する意識や被害実績を調査し、2016年3月に調査報告書として公開した[17]。JPCERT/CCも、制御システムユーザー企業を対象として制御システムのネットワーク構成やセキュリティ対策、マルウェアの感染経験などに関するアンケート調査を行い、その調査結果を2016年11月に公表した[18]。さらに、同月には制御システムのセキュリティ対策状況を自己評価するためのチェックリストと解説がセットとなったセキュリティ自己評価ツール（J-CLICS）の日本語版を、12月にはその英語版を公開した[19]。

制御システムを利用している一部の業界に対しては、サイバーセキュリティ対策の実施を義務化する動きが見られた。たとえば、経済産業省は電気事業法に基づく省令と保安規定の内規を2016年9月に改正した。本改正では、電力設備などを狙ったサイバー攻撃に対するセキュリティ確保のために適切な措置を行うことが、電力事業者に義務化された。セキュリティ確保の具体的な方法については、日本電気技術規格委員会（JESC）が策定した「スマートメーターシステムセキュリティガイドライン」[20]と「電力制御システムセキュリティガイドライン」[21]に基づいて実施するよう指定されている。

日本情報経済社会推進協会（JIPDEC）は2016年10月にCSMS認証基準を改定し、「CSMSシステムインテグレータ向けガイド」を公開した[22]。制御システムのシステムインテグレーターに対し

て開発・構築した制御システムのリスクアセスメントを実施するとともに、顧客に対して適切なセキュリティソリューションを提案し提供するように求めている。

1. インシデント報告対応四半期レポート（JPCERT/CC）
https://www.jpcert.or.jp/ir/report.html
2. Web サイト改ざんに関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2016/at160047.html
Web サイトの改ざんに関する注意喚起について（警察庁）
https://www.npa.go.jp/cyberpolice/detect/pdf/20161114.pdf
3. 仏 OVH, CEO の Octave Klaba 氏の Twitter での発言、2016 年 9 月 22 日.
4. 平成 28 年上半期におけるインターネットバンキングに係る不正送金事犯の発生状況について（警察庁）
https://www.npa.go.jp/cyber/pdf/H280908_banking.pdf
5. 国内ネットバンキングを狙う「URSNIF」が再び日本語メールで拡散（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/13560
6. バンキングトロージャン「Bebloh」感染狙う日本語スパムメールを相次いで確認（キヤノン IT ソリューションズ）
https://eset-info.canon-its.jp/malware_info/news/detail/160630_2.html
7.「金融監督庁」を偽装し国内 8 銀行のネットバンキングを狙う「KRBANKER」の新たな手口（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/13683
8. TrendLabs 2016 年上半期セキュリティラウンドアップ（トレンドマイクロ）
http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2016h1/
9.「ランサムウェア感染被害に備えて定期的なバックアップを」～組織における感染は組織全体に被害を及ぼす可能性も～（IPA）
https://www.ipa.go.jp/security/txt/2016/01outline.html
10. 標的型サイバー攻撃キャンペーン「BLACKGEAR」 日本も攻撃対象に（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/13990
11. サイバーセキュリティ経営ガイドライン（経済産業省）
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html
12.「WebLogic Server」の脆弱性探索が目的と考えられるアクセスの観測について（警察庁）
http://www.npa.go.jp/cyberpolice/detect/pdf/20151115.pdf
13. Java セキュアコーディング スタンダード（JPCERT/CC）
https://www.jpcert.or.jp/java-rules/ser12-j.html
https://www.jpcert.or.jp/java-rules/ser13-j.html
14. Apache Struts 2 Documentation S2-032
https://struts.apache.org/docs/s2-032.html
Apache Struts 2 Documentation S2-033
https://struts.apache.org/docs/s2-033.html
Apache Struts 2 Documentation S2-037
https://struts.apache.org/docs/s2-037.html
15. Apache Struts 2 の脆弱性を標的としたアクセスの観測について（警察庁）
http://www.npa.go.jp/cyberpolice/detect/pdf/20160427.pdf
16. Overload: Critical Lessons from 15 Years of ICS Vulnerabilities（FireEye）
17. 制御システム利用者のための脆弱性対応ガイド 第 2 版（IPA）
https://www.ipa.go.jp/files/000051552.pdf
制御システムユーザ企業の実態調査報告書（IPA）
https://www.ipa.go.jp/files/000051551.pdf
18. 制御システムセキュリティに関するアセットオーナ実態調査（JPCERT/CC）
https://www.jpcert.or.jp/ics/asset-owner-survey_2015.pdf
19. 制御システムセキュリティ自己評価ツール（J-CLICS）（JPCERT/CC）
https://www.jpcert.or.jp/ics/jclics.html
20. スマートメーターシステムセキュリティガイドライン（JESC）
https://www.denki.or.jp/wp-content/uploads/2016/07/s20160609.pdf
21. 電力制御システムセキュリティガイドライン（JESC）
https://www.denki.or.jp/wp-content/uploads/2016/07/d20160707.pdf
22. CSMS システムインテグレータ向けガイド ー CSMS 認証基準（IEC 62443-2- 1）対応ー Ver.1.0（JIPDEC）
https://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS112-10.pdf

［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～2017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