2018年の情報セキュリティ動向

森崎 樹弥 ●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

金銭窃取を目的としたスパムメールやSMSを利用した偽サイトへの誘導などの攻撃、不正アクセスによる個人情報漏えい被害発生のほか、国内初となる日本語ビジネスメール詐欺が確認された。

■セキュリティインシデントの報告件数

2018年1月から12月までにJPCERTコーディネーションセンター（JPCERT/CC）に報告されたコンピューターセキュリティインシデント（以下、インシデント）の件数は1万5751件（前年は1万8450件）であった（資料4-1-1）。前年と比較して、「スキャン」および「ウェブサイト改ざん」の報告件数が減少した一方で、「フィッシングサイト」の報告が増加した（資料4-1-2）。フィッシングサイトの報告件数は前年比50％の増加になっており、中でも、国内ブランドを装ったフィッシングサイトの増加が顕著だった。

■ユーザー個人を対象とした攻撃

●実在する組織からのメッセージを装った偽サイトへの誘導

2018年は、実在する組織からのメッセージを装ったメールやSMSを送りつけ、偽サイトへ誘導する攻撃が多数報告された。特に、宅配業者をかたる不審なSMSが2018年7月の中旬から急増し、注意が呼びかけられている[1]。 SMS本文中に記載されたリンク先をタップすると、攻撃者によって準備された偽のサイトへ誘導される。偽サイト内では、画面のどの領域をタップしても、マルウエアのダウンロードが開始される。このマルウエアは、連絡先などスマートフォン内に保存された情報の窃取や端末の遠隔操作を試みるものであった。

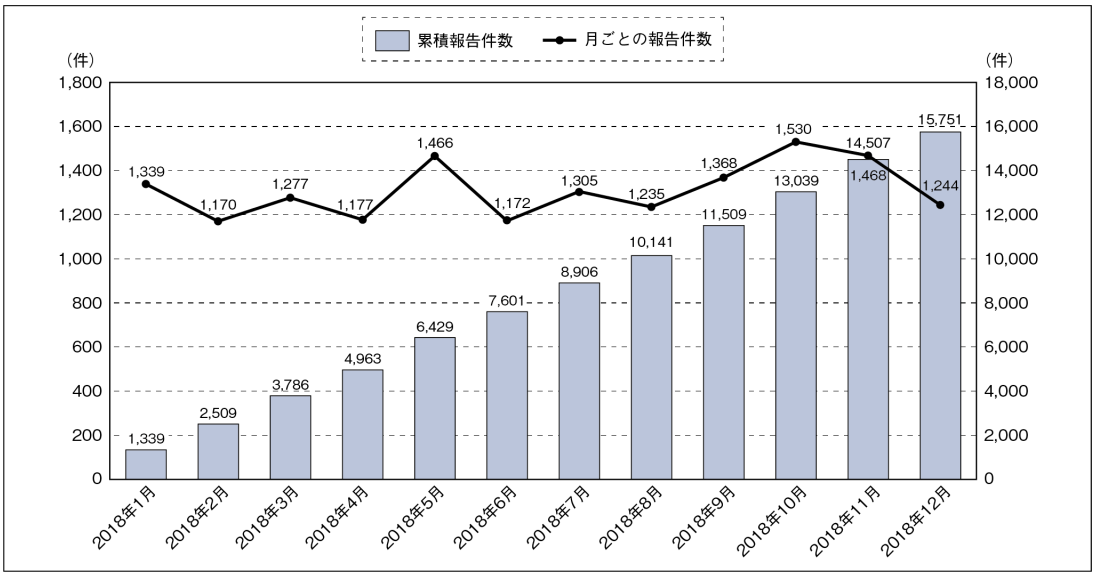
これらの攻撃に遭わないためには、身に覚えのないメールやSMSなどの受信時に、不用意にURLをクリックしないことや、送信元の組織や個人に電話など別の手段で受信したメールやSMSが正当な送り主によるものか確認することが重要である。また、ソフトウエアをインストールする際には信頼のできるサイトからに限り、利用するソフトウエアを最新のものに維持するなど、PCやスマートフォンのセキュリティ対策を心がけたい。

●金銭窃取を目的とした攻撃

2018年も国内外によらず、継続して世界的にスパムメールが確認されており、その中にはマルウエア拡散を狙ったものも含まれている。そのようなマルウエア拡散を狙ったメールには日本語で記述されたものも確認されている。トレンドマイクロの調査[2]によると、マルウエア拡散を狙ったスパムメールのうち、日本語で記述されたメールの約95％はバンキングトロジャン拡散目的だった。

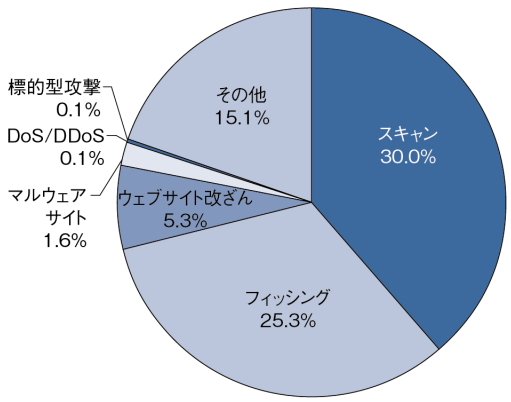
2018年に国内で確認された日本語で記述されたマルウエア拡散メール攻撃の特徴の1つとして、CUTWAILと呼ばれるボットネットを

資料4-1-1　インシデント報告件数の推移（2018年1～12月）



出典：「JPCERT/CC インシデント報告対応レポート」をもとに作成（インシデント報告対応レポート（JPCERT/CC、https://www.jpcert.or.jp/ir/report.html）

資料4-1-2　インシデント報告件数のカテゴリ別内訳（2018年1～12月）



スキャン	5,939件（–4,432件）	↘
ウェブサイト改ざん	1,055件（–　903件）	↘
フィッシング	5,000件（+1,694件）	↗
マルウェアサイト	326件（–　10件）	↘
DoS/DDoS	18件（–　75件）	↘
標的型攻撃	26件（–　10件）	↘
制御システム関連	7件（–　70件）	↘
その他	2,978件（–　612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」をもとに作成

攻撃インフラとして利用している点が挙げられる。CUTWAILは2007年頃から確認されており[3]、2018年上半期の6か月においても、2018年8月上旬のInternet Query（IQY）ファイルを不正利用する攻撃や[4]、2018年10月下旬のステガノグラフィを用いた攻撃においても[5]利用が確認されている。

一方で、仮想通貨を要求する脅迫メールが2018

年7月下旬頃から世界中で確認され[6]、9月中旬頃からは日本語で記述されたものも散見された[7]。これらのメールには「入手した受信者に関する情報を削除する代わりに仮想通貨を要求する」との内容が記載されており、受信者自身に関係する情報を侵害したと不安をあおることで金銭の獲得を狙う手法が使われていた。また、海外では、このような脅迫メールにマルウエアを忍ばせているケースも確認されている[8][9]。

このような攻撃の被害に遭わないためには、添付ファイルやメール本文中のリンクを不用意に開かないことや受信したメールに関して、不審な点がないかなどを確認したうえで冷静に対応することが重要である。

■法人組織を対象とした攻撃

●仮想通貨マイニングマルウエア

2018年でも、仮想通貨マイニングマルウエアが継続して確認されている。これは、設置者が自らの意思でウェブサイトに Coinhive を埋め込み利用するものではなく、組織のウェブサイトなどにウェブサイト改ざんを通じて埋め込まれていたり、何らかの方法で不正にアクセスしたサーバーにプログラムが設置されたりするケースだと想定される。特に、Oracle WebLogic Server の脆弱性（CVE-2017-10271）[10]やDrupal の脆弱性（CVE-2018-7600）[11]および（CVE-2018-7602）[12]など、ソフトウエアの脆弱性を悪用した攻撃が、複数の組織で確認されている。これらのマルウエアの感染を防ぎ、早期に感染を検知するためには、サーバーや、ウェブコンテンツにおいて、不審なファイルが設置されていないかの確認や、可能ならばウイルス対策ソフトによる定期的なスキャンを行うことが望ましい。また、サーバーで用いるアプリケーションだけでなく、OSやサーバーで用いるライブラリやフレームワークなどのソフトウエア基盤についても最新の状態に維持することが重要である。

●標的型攻撃

2018年3月中旬頃、国内の報道機関において報道された事例が代表するように、2018年も国内の特定組織に向けた標的型攻撃は継続している。2018年1月から12月までの期間中、JPCERT/CCにおいても、国内の組織を標的とした標的型攻撃に関連したインシデント報告が合計26件寄せられた。標的に送られたメールに添付されたマクロ付きの文書ファイルを開かせることによってRedLeavesやANEL と呼ばれるボットに感染させたり、メールの本文中に記載されたURLをクリックさせることでTSCookieと呼ばれるダウンローダーをインストールさせたりする攻撃手法が確認された。また、メールに添付されたマクロ付きの文書ファイルを開かせることによって、最終的に、Cobalt Strikeのペイロード（Cobalt Strike Beacon）を実行する攻撃も確認された[13]。

標的型攻撃では、用いられるマルウエアや侵入手口が標的組織ごとにカスタマイズされているので、攻撃を完全に見破って防ぐことが難しい。そのため、すでに侵入されている可能性を念頭に、早期検知に配慮した日頃からの備えが重要だ。具体的には、まずは自組織における各種ログ（ProxyやFirewall、Active Directoryなど）の定期的な調査や端末の管理状態の確認など、運用状況の把握が重要である。

JPCERT/CCでは、ブログ記事として、2017年11月に「イベントログを可視化して不正使用されたアカウントを調査 ～LogonTracer～」[14]、2018年9月に「Sysmonログを可視化して端末の不審な挙動を調査~SysmonSearch~」[15]を公開した。これらの記事では、サイバー攻撃の調査時に活用できるツールを紹介している。また、2018年12

月には、「CSIRT構築および運用における実態調査」[16]を公開した。本調査結果などを参考にしつつ、CSIRT構築などをはじめとした社内体制の整備を行い、サイバー攻撃への備えを進めていただきたい。

●ビジネスメール詐欺（BEC: Business E-mail Compromise）

巧妙なメールなどのやりとりにより、企業の担当者を騙して、攻撃者が用意した口座へ送金させる、ビジネスメール詐欺の被害が世界各国で報告されている。

米国連邦捜査局（FBI）によると2013年10月から 2018年5月の約4年半の期間に、米国インターネット犯罪苦情センター（IC3）を含む複数の機関に報告されたビジネスメール詐欺の件数は7万8617件で、被害総額は約120億米ドルに上った。1件あたりの平均被害額は約16万米ドル、日本円換算で約1800万円になる[17]。

情報処理推進機構（IPA）によると、2018年7月に国内でも初めて日本語のビジネスメール詐欺が報告され、その後も被害事例の報告が継続しているとのことだ。[18]JPCERT/CCにおいても、ビジネスメール詐欺と思われるメールを受信したとの報告を国内組織から受けている。 トレンドマイクロは2018年6月、国内の法人組織における情報セキュリティ・社内IT責任者515人、経理責任者515人名を対象にアンケートを実施した。回答した1030名の約4割にあたる406名が組織内でビジネスメール詐欺と思われるメールを受信した経験を持ち、うち22名が所属するそれぞれの組織では実際に送金したとのことだ[19]。

全国銀行協会[20]や日本貿易振興協会（JETRO）[21]などでは事例を交えながら注意喚起を行っている。これらの注意喚起に記載があるとおり、ビジネスメール詐欺においては、それぞれが所属する業界の商慣習に応じて、冷静に対応することが重要である。

詐欺の手口を把握し、社内に注意喚起を行うだけではなく、通常の取引と異なる対応を求めるメールを受け取った際に、電話や対面など、メール以外の手段を用いて確認することなど、社内における手続きの整備などを推奨する。

●不正アクセス

2018年もサイトに保存された個人情報が不正アクセスによって大量に外部に漏洩するなどの事案が、様々な組織から公表された。

2018年4月、国内アウトレットモールの会員サイトにおいて会員情報が流出した可能性があると、同社ウェブサイト上で公表された。調査によりSQLインジェクションの脆弱性を悪用した不正アクセスによるものだったことが明らかになった。同社を含む複数組織から流出したとみられるユーザーのIDやパスワードがダークウェブなどで公開されていた。

攻撃者が何らかの方法で入手したIDやパスワードなどのリストを基に不正アクセスを試みる例もある。2018年7月末に検知された、国内企業に対するリスト型攻撃では、不正ログインの試行が大量に行われ、最終的に約1000台に上るスマートフォンの不正購入が確認された。

JPCERT/CCでは、ウェブサイトからの情報漏洩など、被害を防止するために、定期的な点検を行うよう呼びかけている。[22]利用しているソフトウエアのバージョン確認や取り扱うデータの利用方針を整理するだけでなく、セキュリティ診断を定期的に実施したり、管理や運用に利用しているログインID、パスワードの使いまわしや安易な設定が行われていないかを確認したりするなど、様々な観点からの点検が必要である。

■社会・インターネット基盤に影響をもたらす攻撃

●DDoS攻撃

JPCERT/CC では、11211/udpの通信ポートに対する探索活動が増加していることを、国内組織からの報告およびインターネット定点観測システム（TSUBAME）の観測データから2018年2月頃に把握し(資料4-1-3)、注意喚起を発行した[23]。これはmemcachedに対する探索活動だと考えられ、実際にmemcachedを悪用したとみられるDDoS攻撃を確認したとの報告もJPCERT/CCで受け取った。国内のホスティング事業者も注意喚起を発し[24][25]、memcached を利用しているユーザーに呼びかけた。

memcachedは、受け取ったデータを何倍にも増幅して送り返す機能を持つため、送信元IPアドレスを偽装したうえで、この機能を悪用し、標的となるサーバーに大量のデータを送りつけることができる[26]。DNSやSDP、NTP、CLDAPなど、これまで反射型のDDoSで用いられてきたプロトコルを悪用するよりはるかに大きな規模のDDoS攻撃になる恐れがある。実際に、今回の一連の攻撃は最大1Tbpsを超える過去最大規模のDDoS攻撃であったと報告されている[27]。

DDoS攻撃の標的にされた場合，それを逃れることは難しい。だが，事前にそうした事態に備えて、事業への影響を評価し、重大な影響があれば少しでもそれを軽減するために、顧客対応部門や広報部門などを巻き込んだ包括的な対応策を整備しておくことが望ましい。

●特定のネットワーク機器を狙った攻撃

2018 年 3 月下旬より、Cisco Smart Install Client が使用する 4786/tcp ポートに対するスキャンが増加していることがインターネット定点観測システム（TSUBAME）の観測データから確認された。増加の背景となったと考えられる脆弱性の情報として、シスコが2017年2月にCisco Smart Install Clientに関するアドバイザリを[28]、また、2018年3月には、Cisco Smart Install Clientの脆弱性（CVE-2018-0171）に関するアドバイザリを公開していた[29]。

実際に、当該スキャン活動以降、シスコ製スイッチを対象とした攻撃が確認され、それを受け、Cisco Talosが攻撃に関する情報を公開した[30]。攻撃を受けた際に、設定ファイルを持ちだされたり、設定などを変更されたりする被害が想定されるため、JPCERT/CCでも広く注意喚起を呼びかけた[31]。なお、注意喚起を行った4月以降も当該機器の探索活動の観測および攻撃に関する報告はJPCERT/CCにて確認しており、継続的に調査を続けている状況だ。

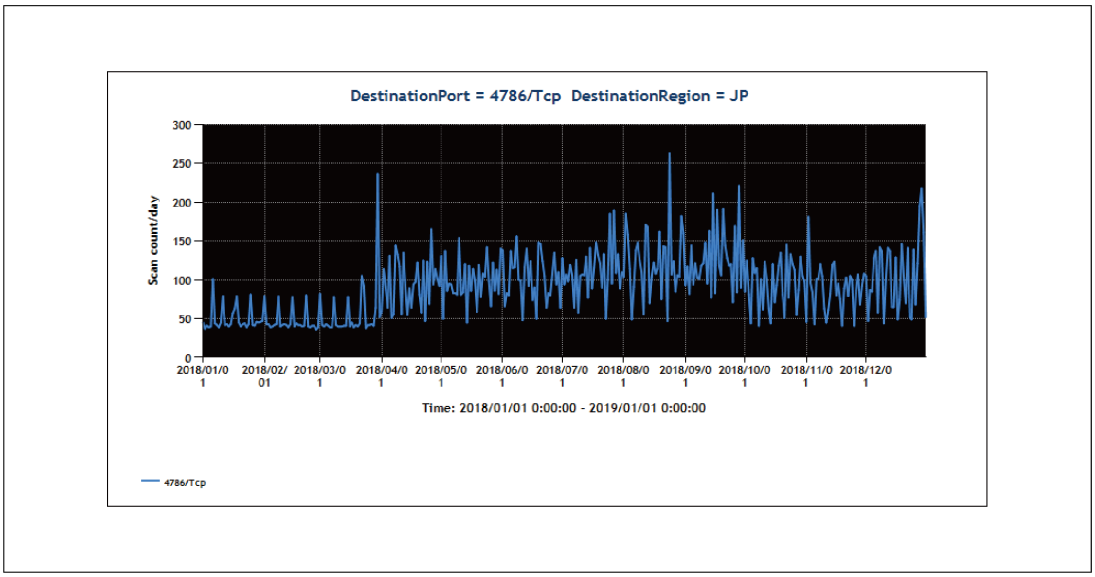
組織のネットワーク管理者は、自組織で利用している機器に関して、不必要な機能が有効になっているかどうかの確認を行うと同時に、利用していないポートが意図せず開放していないかの確認や外部からの通信の制限などを行い、できる限り機器のファームウエアを最新版にするよう心がけてほしい。

●MiraiおよびMirai亜種に関する攻撃

2016年に大規模なDDoS攻撃による被害をもたらしたIoT機器を狙うマルウエアMiraiやその亜種による機器の探知活動や感染活動を示すスキャンを2018年も継続して観測している。特に、2017年末から始まった、特定の機器の脆弱性を悪用してMirai亜種の感染を試みるような通信[32]も2018年も継続して観測し、脆弱性を狙った感染活動を確認している[33]。

こうした脆弱な IoT 機器に対して、法律による規制などの議論の進展がみられた。国内では、2018年11月に国立研究開発法人情報通信研究機

資料4-1-3　4786/tcp (Cisco Smart Install Client) へのスキャン（2018年1～12月）



出典：JPCERT/CC のインターネット定点観測システム TSUBAME のデータをもとに作成

構法（以降、NICT）が施行され、不正アクセスを防ぐための取り組みとして、パスワードの基準が定められた[34]。また、この一環として、インターネットに接続されたIoT機器の状況把握のため、NICTによる調査が行われる（2018年11月から2019年1月）[35]。

一方、米国のカリフォルニア州においても、2018年9月にIoTセキュリティ法が採択され、メーカーに対して、提供する製品が共通の初期パスワードを設定することを禁じるなど、機器のセキュリティ強化を図るための法律を明示した[36]。今後は、このような行政機関における指導の下、IoT機器のセキュリティを強化する取り組みが検討されることも予想できる。

1. 安心相談窓口だより- 宅配便業者をかたる偽ショートメッセージに関する相談が急増中
～誘導されるまま Android 端末にアプリをインストールしないように！～（情報処理推進機構（IPA））
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html
2. バンキングトロジャンのメール経由拡散を支える「スパムボット」（トレンドマイクロ）
https://blog.trendmicro.co.jp/archives/19346
3. CUTWAIL Spambot Leads to UPATRE-DYRE Infection（TRENDO MICRO）
https://blog.trendmicro.com/trendlabs-security-intelligence/cutwail-spambot-leads-to-upatre-dyre-infection/
4. IQY ファイルを利用するマルウェアスパム、日本のみを標的に50万通拡散（トレンドマイクロ）
https://blog.trendmicro.co.jp/archives/19506
5. Cutwail Spam Campaign Uses Steganography to Distribute URLZone（CROWD STRIKE）
https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/
6. 仮想通貨を要求する不審な脅迫メールについて（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2018080201.html
7. 仮想通貨を要求する日本語の脅迫メールについて（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2018091901.html
8. Sextortion with a side of ransomware（Proofpoint）
https://www.proofpoint.com/us/threat-insight/post/sextortion-side-ransomware
9. マルウエアへの感染を誘導し、仮想通貨を要求する脅迫メールについて https://www.jpcert.or.jp/newsflash/2018121101.html
10. Oracle WebLogic Server の脆弱性（CVE-2017-10271）に関

する注意喚起（JPCERT/CC）https://www.jpcert.or.jp/at/2018/at180004.html

11. Drupal の脆弱性（CVE-2018-7600）に関する注意喚起（JPCERT/CC）https://www.jpcert.or.jp/at/2018/at180012.html
12. Drupal の脆弱性（CVE-2018-7602）に関する注意喚起（JPCERT/CC）https://www.jpcert.or.jp/at/2018/at180019.html
13. インシデント報告対応レポート（JPCERT/CC）https://www.jpcert.or.jp/ir/report.html
14. イベントログを可視化して不正使用されたアカウントを調査～LogonTracer～（2017-11-28）（JPCERT/CC）https://blogs.jpcert.or.jp/ja/2017/11/logontracer.html
15. Sysmon ログを可視化して端末の不審な挙動を調査~Sysmon-Search~ （2018-09-06）（JPCERT/CC）https://blogs.jpcert.or.jp/ja/2018/09/SysmonSearch.html
16. 2017年度CSIRT構築および運用における実態調査（JPCERT/CC）https://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf
17. Business E-mail Compromise The 12 Billion Dollar Scam（IC3）https://www.ic3.gov/media/2018/180712.aspx
18. 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）（情報処理推進機構（IPA））https://www.ipa.go.jp/security/announce/201808-bec.html
19. 「ビジネスメール詐欺に関する実態調査2018」を発表（トレンドマイクロ）https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180814-01.html
20. 法人間の外国送金の資金をだまし取る詐欺にご注意！（BEC（Business E-mail Compromise）/ foreign remittance fraud）（全国銀行協会）https://www.zenginkyo.or.jp/topic/detail/nid/3561/
21. 国際的詐欺事件について（注意喚起）（日本貿易振興協会（JETRO））https://www.jetro.go.jp/contact/faq/419.html
22. Webサイトへのサイバー攻撃に備えて2018年7月（JPCERT/CC）https://www.jpcert.or.jp/newsflash/2018071801.html
23. memcached のアクセス制御に関する注意喚起（JPCERT/CC）https://www.jpcert.or.jp/at/2018/at180009.html
24. 【重要】memcached のアクセス制御に関する注意喚起（さくらインターネット）https://www.sakura.ad.jp/information/announcements/2018/02/27/1885/
25. 【注意喚起】memcached のアクセス制御に関する対応につきまして（GMO クラウド）https://help.gmocloud.com/app/answers/detail/a_id/3337
26. MEMCACHED リフレクション攻撃：DDoS 攻撃は新たな時代へ（アカマイ・テクノロジーズ）https://www.akamai.com/jp/ja/multimedia/documents/brochure/memcached-reflection-attacks-launch-a-new-era-for-ddos-brochure.pdf
27. GitHub に 1 TBps超の攻撃、「memcached」を利用する新たなDDoS 手法を解説（トレンドマイクロ）https://blog.trendmicro.co.jp/archives/17116
28. Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client（Cisco Talos）http://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html
29. Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability（Cisco Talos）https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
30. Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client（Cisco Talos）http://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html
31. Cisco Smart Install Client を悪用する攻撃に関する注意喚起（JPCERT/CC）https://www.jpcert.or.jp/at/2018/at180013.html
32. Mirai 亜種の感染活動に関する注意喚起（JPCERT/CC）http://www.jpcert.or.jp/at/2017/at170049.html
33. インターネット定点観測レポート（JPCERT/CC）https://www.jpcert.or.jp/tsubame/report/report201801-03.html
34. 新規制定・改正法令・告示　法律（総務省）http://www.soumu.go.jp/menu_hourei/s_houritsu.html
35. 日本国内でインターネットに接続された IoT 機器等に関する事前調査の実施について（国立研究開発法人情報通信研究機構）https://www.nict.go.jp/info/topics/2018/11/07-2.html
36. SB-327 Information privacy: connected devices.（カリフォルニア州議会）https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

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～2019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