2017年のコンピューターセキュリティ動向

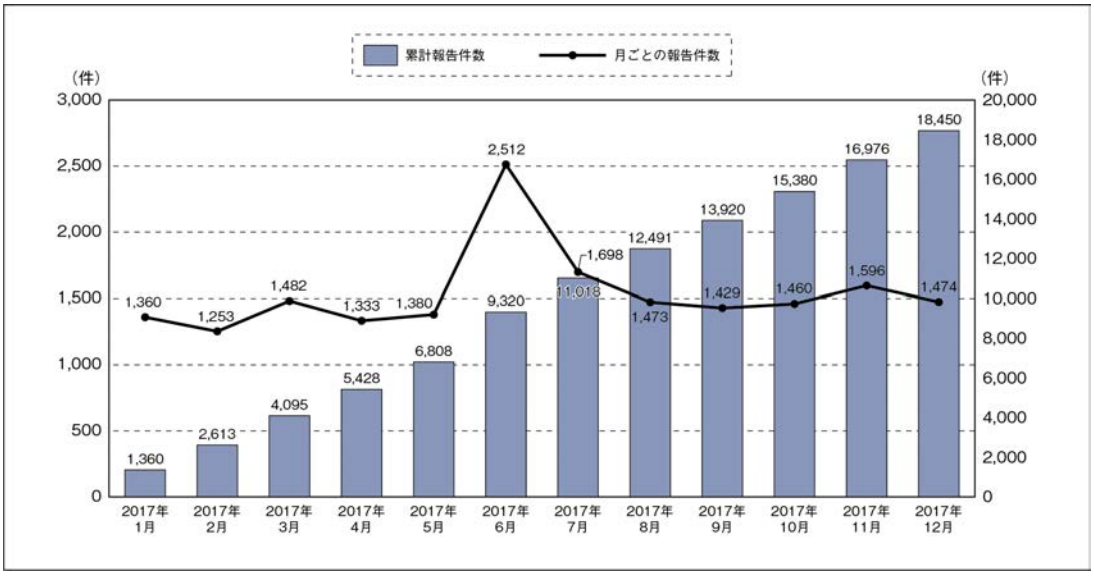
清水 友基 ●一般社団法人JPCERTコーディネーションセンター 早期警戒グループ 情報分析ライン 情報セキュリティアナリスト

脆弱性を悪用して感染を拡大するランサムウェアによる攻撃が高度化。世界で同時多発したWannaCryは大きな被害をもたらし、11月以降はIoT機器に感染するマルウェアMiraiの亜種が国内で感染拡大。

■セキュリティインシデントの報告件数

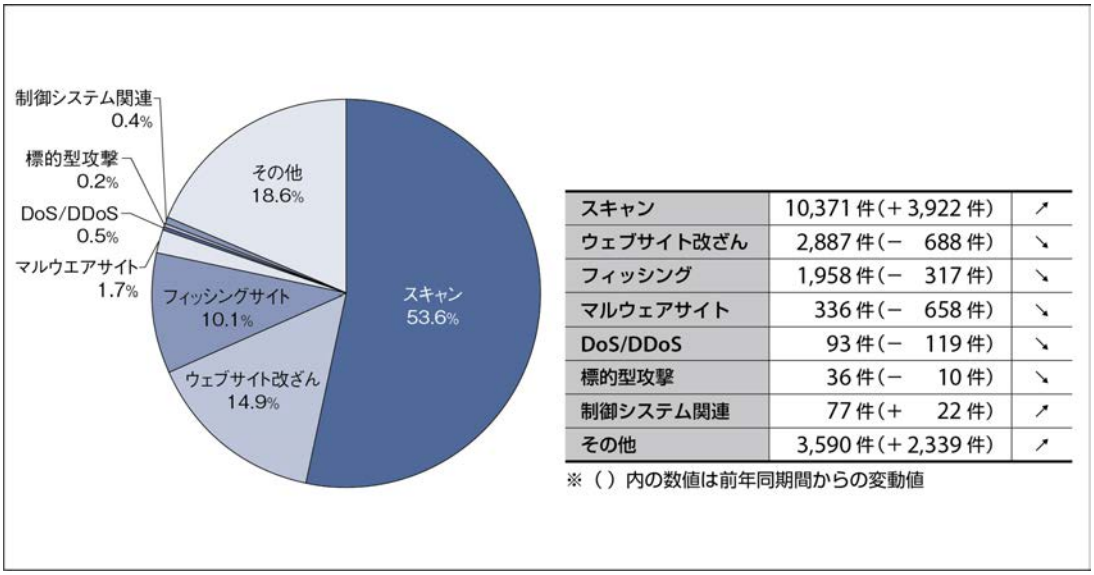
2017年1月から12月までにJPCERTコーディネーションセンター（JPCERT/CC）に報告されたコンピューターセキュリティインシデント（以下、インシデント）の件数は1万8450件（前年は1万4,857件）であった（資料4-1-1）。前年と比較して、「スキャン」の報告件数が特に増加した（資料4-1-2）。スキャンの報告件数が増加した主因は、6月頃に脆弱性（CVE-2017-10845）を悪用されマルウェアに感染した国内の機器からのスキャンによるものと考えられる。なお、コメントスパム（ブログのコメント欄に関係のないメッセージや広告などを書き込む行為）は、これまでインシデントとしては扱ってこなかったが、多数の報告が続いていることを考慮し、2017年から「その他」のインシデントとした。

資料4-1-1　インシデント報告件数の推移（2017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（2017年1〜12月）



スキャン	10,371件（+3,922件）	↗
ウェブサイト改ざん	2,887件（−　688件）	↘
フィッシング	1,958件（−　317件）	↘
マルウェアサイト	336件（−　658件）	↘
DoS/DDoS	93件（−　119件）	↘
標的型攻撃	36件（−　10件）	↘
制御システム関連	77件（+　22件）	↗
その他	3,590件（+2,339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

■サイバー攻撃の主な動向

●ランサムウェア

WannaCryをはじめとするさまざまな種類のランサムウェアによる感染が世界中で同時多発的に発生し、日本国内でも感染が確認された。これまでのランサムウェアは自己増殖性を持たず、メー

ルや改ざんされたウェブサイトを通じて攻撃サイトへ誘導されるなどして感染していたが、2017年には、脆弱性を悪用して感染範囲を拡大させるランサムウェアが登場した。

特にWannaCryは、5月に世界的な感染が確認され、話題となった。WannaCryは次の2点で従来のランサムウェアと大きく異なっていた。動作を制御する機能としてKillSwitchと呼ばれるものが実装されていた点、SMB v1の脆弱性（MS17-010）を悪用して感染を拡大するワームのように自己増殖する機能を備えていた点である。なお、WannaCryの約1か月後に登場したNotPetyaでもSMBv1の脆弱性を悪用した自己増殖性が確認されている。NotPetyaについては、メモリー上から認証情報を抽出するツールmimikatzを利用して認証情報を取得してPsExecやWMICによってネットワーク内で自己増殖して感染を広げる手法によって、組織内ネットワーク上を横断的に侵害することが確認されている。

ネットワーク経由でアクセス可能なコンピューターに対し、Remote Desktop Protocol（RDP）経由で総当たり攻撃やリスト型攻撃、脆弱な認証情報を悪用した侵入も確認された。また、ランサムウェアを使用した標的型攻撃と見られる攻撃や、攻撃の痕跡を隠すために攻撃の最終段階でランサムウェアを使った事例も確認されている[1]。

ランサムウェアに対しては、アプリケーションソフトウェアやウイルス対策ソフトの定義ファイルやOSの更新といった基本的なセキュリティ対策が重要である。さらに、ランサムウェアで暗号化される以前のバックアップデータを暗号化されたデータで上書きしないよう、バックアップデータを世代管理することも重要である。

●ウェブサイトの改ざん

2017年2月にWordPressの脆弱性（CVE-2017-5611）を悪用したウェブサイトの改ざんが世界中で確認された。JPCERT/CCでも、本脆弱性を悪用した国内のウェブサイトの改ざんを確認したため、注意喚起を公開し対策を呼びかけた[2]。資料4-1-3において、2月にウェブサイト改ざんの件数が増えた主因は、本脆弱性を狙った攻撃の増加にあると考えられる。

資料4-1-3　カテゴリ別インシデント件数（2017年1〜3月）

インシデント	1月	2月	3月	合計	前四半期合計
フィッシングサイト	191	246	270	707	521
Webサイト改ざん	143	590	234	967	688
マルウエアサイト	35	24	32	91	376
スキャン	869	682	840	2391	2177
DoS/DDoS	16	58	1	75	61
制御システム関連	3	0	1	4	24
標的型攻撃	4	6	1	11	15
その他	144	242	224	610	260

出典：「JPCERT/CCインシデント報告対応レポート」をもとに作成

ウェブサイトが改ざんされた場合、表示される見かけ上のウェブページは変わらなくとも、攻撃サイトへ誘導するためのスクリプトなどを仕込まれ、ウェブサイトを閲覧したユーザーがマルウェアに感染させるサイトへ誘導される場合もある。ウェブサイト改ざんの対策として、ウェブサー

バーで使用しているOSやアプリケーションソフトウェアを最新の状態に維持すること、ウェブサイトのコンテンツを更新するために使うPCを限定しアクセス制限を適切に設定することが重要である。また、ウェブサイトの改ざんを早期に検知するために、定期的にコンテンツの完全性を確認することも推奨される。

●DDoS攻撃

上半期（2017年1〜6月）は、アノニマス（Anonymous）と呼ばれる匿名の攻撃者集団によるDDoS攻撃が国内組織で複数確認された。JPCERT/CCが確認した事例では、Slow HTTP POST Attackを実装した攻撃ツールが悪用されたと見られるケースが複数あった。こうした攻撃ツールは、インターネット上に公開されており、入手が容易な状況にある。Slow HTTP POST Attack対策を考慮したウェブサイトの設定が望まれる[3]。

2017年6月には、銀行や証券会社などを対象としたArmada Collectiveを名乗る攻撃者による、脅迫を伴うDDoS攻撃が世界中で確認された。使われた脅迫メールは、2015年の同攻撃者によるDDoS攻撃の際に使われている文面と類似していたことから、JPCERT/CCは情報を公開している[4]。また、こうした攻撃に便乗したと考えられるPhantom Squadを名乗る攻撃者集団からの脅迫メールも確認された。9月には、国内のFX事業者などへの脅迫を伴うDDoS攻撃が確認されており、JPCERT/CCは情報を公開した[5]。

DDoS攻撃の影響を軽減するために、攻撃を受けた際の対応の確認など、事前に体制を整備することが望ましい。

●金銭窃取を目的とした攻撃

警察庁によれば、上半期（2017年1〜6月）に発生したインターネットバンキング利用に関わる不正送金の事犯の発生件数は214件（前年同期比▲645件）、被害額約5億6400万円（前年同期比▲3億3300万円）と、件数・被害額ともに減少した[6]。しかし、バンキングマルウェアDreamBotに感染し、インターネットバンキングのユーザーIDやパスワードなどが不正に窃取された事犯が増加しているとの情報もあり、引き続き注意が必要である[7]。DreamBotや類似マルウェアへの感染を目的とした不審メールによる攻撃が2015年10月から継続している。

これらは、怪しげなメール文面で送られてくるのではなく、実在する組織を騙り自然なメール文面で送られてくるなど、内容は日々変化している。マルウェアの感染を防ぐためには、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、ウイルス対策ソフトを更新して定期的にウイルススキャンを行うこと、さらに脆弱性を悪用して感染させるケースも確認されているためOSやアプリケーションソフトウェアを最新の状態に維持することが重要である。

メールの巧妙なやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる手口、ビジネスメール詐欺（BEC: Business E-mail Compromise）も確認されている。米連邦捜査局（FBI）によれば、2013年10月から2016年12月におけるBECの被害総額は約53億米ドルに上る[8]。国内でも、2017年4月に情報処理推進機構（IPA）から注意喚起が公表され[9]、12月には国内組織が「BECによる大規模な被害を受けた」と発表している[10]。

BEC対策として、まずはこのような手口があることを認識することが重要である。その上で、普段とは異なるメールに注意すること、取引先との連絡にメール以外の手段を用いることなどの対策が推奨される。

●高度サイバー攻撃（標的型攻撃）

2017年1月から12月までの期間中、JPCERT/CCには国内の組織を標的とした高度サイバー攻撃に関連したインシデント報告36件が寄せられた。ChChes、RedLeavesと呼ばれるマルウェアを用いた攻撃、Daserfと呼ばれるマルウェアに関連した攻撃（攻撃名：Tick、BRONZE BUTLERなど）が確認された。

前者の攻撃は、標的とする組織に対しメールを用いて侵入することから始まっていた。後者の攻撃では、Adobe Flash Playerの脆弱性を悪用した水飲み場攻撃などの従来からの手法を用いて侵入する事例もあれば、国内組織で使用される資産管理ソフトの脆弱性を悪用した事例もあった[11]。また、システムクリーナーソフトCCleanerの配布先のファイルに挿入された不正なコードによりマルウェアに感染させられた事例もあった[12]。このように、標的とする組織への侵入を試みるため、攻撃者は実にさまざまな攻撃手法を用いている。

高度サイバー攻撃では、用いられるマルウェアや侵入手口が標的組織ごとにカスタマイズされており、攻撃を完全に防ぐことが難しい。そのため、すでに侵入されている可能性を前提に、日頃から早期検知に配慮した備えが重要である。そのために、まずは自組織における各種ログ（ProxyやFirewall、Active Directoryなど）の定期的な確認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、サイバー攻撃の調査時に活用できる資料として、2017年3月に「ログを活用したActive Directoryに対する攻撃の検知と対策」[13]、11月に「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書（第2版）」[14]を公開した。こうしたログの調査に加え、外部の関係組織などとも連携し、攻撃動向や被害事例、対策ノウハウなどの情報収集に努めることも重要である。

■脆弱性の動向

2017年においても、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やマイクロソフト 製品の脆弱性が公表され、これらを悪用した攻撃が複数発生した。これらの脆弱性の詳細を紹介する。

●Apache Struts 2の脆弱性

2016年に引き続き、Apache Struts 2の脆弱性が複数公表され、JPCERT/CCからも注意喚起を公開した[15]。

特に、2017年3月に公表されたS2-045（CVE-2017-5638）は、公表の翌日に攻撃の実証コードが公開され、ほぼ同日に脆弱性を悪用した攻撃が始まっていたことが確認されている。複数の組織が被害を受け、クレジットカード情報を含む個人情報などが漏えいする被害が発生した。この脆弱性は、Apache Struts 2のデフォルトで使用されるパーサー（Jakarta Multipart parser）の処理に起因しており、使用するパーサーをApache Struts 2の設定ファイルで明示的に変更していない場合に影響を受ける。多くのサイトがこの脆弱性を悪用した攻撃の影響を受けやすい状況にあった。

上述の脆弱性のように、脆弱性情報の公表とほぼ同時に攻撃が始まり、被害が発生する場合がある。脆弱性への対策の基本はセキュリティアップデートだが、アップデートを適用する前に検証を行うなど、時間を要することもある。そのため、根本的な対策であるセキュリティアップデートを適用する前に、暫定的な回避策を講じることも望ましい。たとえば、Web Application Firewall（WAF）が導入されていれば、ルール（シグネチャ）を追加して攻撃を検知し被害を軽減で

きる。

●Microsoft製品に関する脆弱性

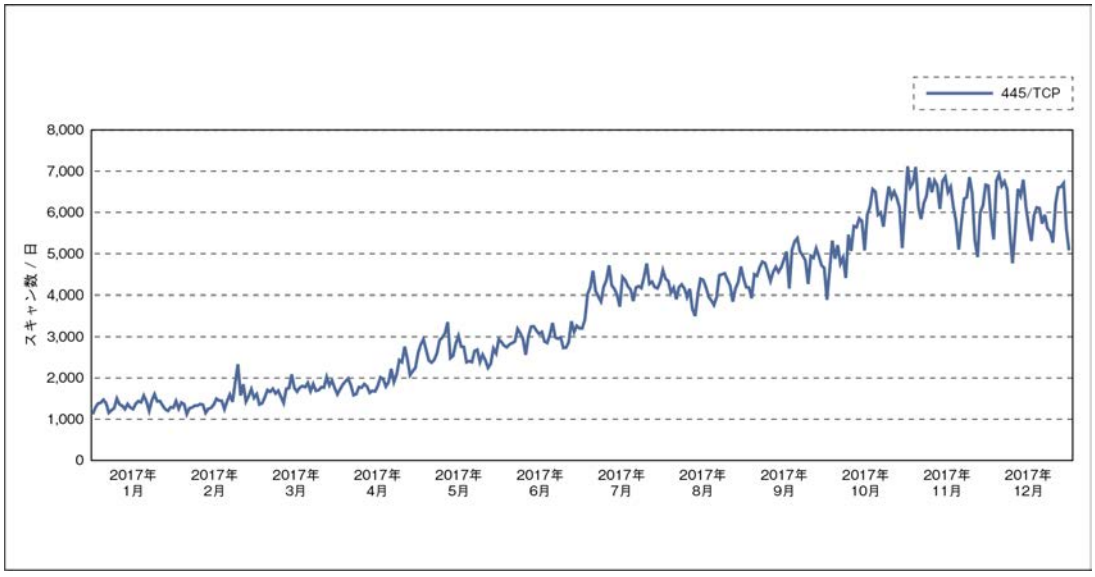
公表されたマイクロソフト製品の脆弱性にも悪用されたケースが複数確認された。特に、2017年4月に公開されたMicrosoft Office/WordPadの脆弱性（CVE-2017-0199）は、Microsoft OLEにおけるURL Monikerでの処理に起因し、悪用された場合、細工されたHTAコンテンツを処理することで任意のコードを実行される[16]。Kasperskyは、2017年4〜6月におけるMicrosoft Officeユーザーに対する攻撃の71%がこの脆弱性を悪用したものだったと報告している[17]。本脆弱性を悪用してDreamBotが拡散していたことはJPCERT/CCでも確認した。

2017年11月には、上述の脆弱性と同様に、細工されたファイルを開くことで任意のコードが実行されるMicrosoft Office/WordPadの脆弱性（CVE-2017-11882）が公表された。JPCERT/CCでは、本脆弱性を悪用したばらまき型メール攻撃を確認しており、脆弱性（CVE-2017-0199）のときと同様にさまざまなケースで悪用される可能性があるため、注意を呼びかけた[18]。

また、SMB v1サーバーが特定のリクエストを処理する際の不具合に起因する脆弱性（MS17-010）は、悪用された場合、遠隔から任意のコードを実行される。この脆弱性を悪用した攻撃も複数確認された。この脆弱性は、Shadow Brokersと名乗る攻撃者集団がハッキングにより米国家安全保障局（NSA）から入手したとされるツールの1つ、EternalBlueでも使われている。EternalBlueは、ランサムウェアWannaCryの感染拡大にも悪用されており、警察庁も当該ツールを悪用した攻撃によるものと考えられるアクセスを複数観測している[19]。JPCERT/CCのインターネット定点観測システムTSUBAMEでも、445/tcpポート宛てのパケットの増加を観測しており、当該脆弱性を狙った攻撃がされているものと見られる（資料4-1-4）。また、EternalBlueは、仮想通貨発掘マルウェアであるCOINMINERの感染拡大にも悪用されているため、今後もこの脆弱性を悪用した攻撃が続く可能性がある[20]。

これらの脆弱性を悪用する攻撃への対策として、定期的なマイクロソフトアップデートの実施や、ファイアウォールの適切な設定、不要なサービスの無効化が重要である。

資料4-1-4　445/Tcpポート宛てのパケット数の推移（2017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

■制御システム、IoTセキュリティの動向

●制御システムの動向

制御システムを狙ったマルウェアとして、2016年12月のウクライナの電力網に対するサイバー攻撃に使用されたと見られるCRASHOVERRIDE（別名：Industroyer）と[21]、Schneider Electric社製の安全計装コントローラー Triconex を標的にした HatMan（別名：TRISIS またはTRITON）が新たに発見された[22]。CRASHOVERRIDEは、制御システム特有のプロトコルを用いて変電所のブレーカーを制御したとされる。HatManは、安全計装コントローラーのファームウェアを改ざんしてプログラムを追加し、ネットワーク経由の指令によりメモリー内容の読み取りやカスタムコードを実行できるようにする機能を持つ。中東の 1社でHatManの感染被害が確認されている[23]。また、米国エネルギー企業を中心に高度サイバー攻撃が観測された[24]。さらに、WannaCryやNotPetyaなどのランサムウェアにより、工場の操業にも影響を与える被害が国内外で報告された[25]。サイバー攻撃の影響が制御システムにも及ぶ事例が増加していると考えられる。

模擬プラントを用いた演習や攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析などを通じて、社会インフラや産業基盤へのサイバーセキュリティリスクに対応する人材・組織・システム・技術を生み出していくための組織としてIPA産業サイバーセキュリティセンターが2017年4月に発足した[26]。同センターでは、7月から産業サイバーセキュリティ人材育成事業として教育プログラムを開始している[27]。

●組み込み機器に関するIoTセキュリティの動向

2016年に引き続き、マルウェアに感染したIoT機器が多く確認された。これらのIoT機器は、認証情報が脆弱で、それを悪用されTelnetやSSHコンソール経由で制御を奪われて感染したと見られている。JPCERT/CCでは、2017年6月にマルウェアに感染した機器経由と見られるスキャンの増加をインターネット定点観測システム

TSUBAMEで確認し、観測結果についての情報および注意喚起を公開した[28]。

さらに、JPCERT/CCおよび情報通信研究機構(NICT)、警察庁などにおいて、11月頃よりMiraiの亜種による感染活動が確認された。この感染活動には、日本国内で普及しているルーターの既知の脆弱性が悪用されていることが判明した。感染した機器がボットネットに取り込まれ、攻撃者により遠隔から命令を受け、DDoS攻撃などに悪用される可能性があるため、JPCERT/CCでは注意喚起を公開した[29]。

IoT機器が感染するMiraiをはじめとするマルウェアの感染原因として、従来と同様の脆弱な認証情報の悪用ばかりでなく、IoTに対しても脆弱性が悪用される可能性を考慮しなければならない。実際に、BlueBorneと呼ばれるBluetoothの実装に関する脆弱性、KRACKと呼ばれるWPA2ハンドシェイクにおける問題など、IoTにも影響を及ぼす脆弱性が複数報告されている。今後は、IoT機器が感染する既知のマルウェアだけでなく、実装や仕様に関する問題や脆弱性を悪用した攻撃の可能性も考慮に入れ、開発者と利用者の双方が適切な対策を施すことが望まれる。被害を軽減するためには、IoT機器の脆弱性を修正したファームウェアの更新などが迅速に提供されること、それらの早期の適用が重要である。

1.ランサムウェア「ONI（鬼）」ランサムウェアを利用し、日本企業への侵入の痕跡を消去（サイバーリーズン・ジャパン）
https://www.cybereason.co.jp/blog/ransomware/1830/
2.WordPressの脆弱性に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170006.html
3.Slow HTTP DoS Attackに対する注意喚起について（警察庁）
https://www.npa.go.jp/cyberpolice/detect/pdf/20151216.pdf
4.Armada Collectiveを名乗る攻撃者からのDDoS攻撃に関する情報（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/20170062901.html
5.Phantom Squadを名乗る攻撃者からのDDoS攻撃に関する情報（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2017092101.html
6.平成29年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf
7.インターネットバンキングに係るコンピュータウイルスDreamBotに関する注意喚起（警察庁）
https://www.npa.go.jp/cyber/policy/20171211.html
8.Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam（FBI）
https://www.ic3.gov/media/2017/170504.aspx
9.ビジネスメール詐欺「BEC」に関する事例と注意喚起（IPA）
https://www.ipa.go.jp/files/000058478.pdf
10.JAL、詐欺被害3億8000万円777リース料や貨物委託料送金
http://www.aviationwire.jp/archives/136855
11.日本企業を狙う高度なサイバー攻撃の全貌 – BRONZE BUTLER（SecureWorks）
https://www.secureworks.jp/~/media/Files/JP/Reports/SecureWorksBronzeButlerReport.ashx
12.Additional information regarding the recent CCleaner APT security incident（Avast）
https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident
Security Notification for CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 for 32-bit Windows users（Piriform）
https://www.piriform.com/news/release-announcements/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users
13.ログを活用したActive Directoryに対する攻撃の検知と対策（JPCERT/CC）
https://www.jpcert.or.jp/research/AD.html
14.インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書（第2版）公開（2017-11-09）（JPCERT/CC）
https://www.jpcert.or.jp/magazine/acreport-ir_research2.html
15.Apache Struts 2の脆弱性(S2-045)に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170009.html
Apache Struts 2の脆弱性(S2-048)に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170025.html
Apache Struts 2の脆弱性(S2-052)に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170033.html
16.CVE-2017-0199 - 脆弱性調査レポート（ソフトバンク・テクノロジー）
https://www.softbanktech.jp/information/2017/20170428-01/
17.＜Kaspersky サイバー脅威レポート：2017年4月～6月＞ソフトウェアの脆弱性を悪用するエクスプロイトの公開に起因する攻撃は500万回以上に（Kaspersky）
https://www.kaspersky.co.jp/about/news/virus/2017/vir31082017
18.2017年11月マイクロソフトセキュリティ更新プログラムに関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170044.html
19.攻撃ツール「Eternalblue」を悪用した攻撃と考えられるアクセス

の観測について（警察庁）
https://www.npa.go.jp/cyberpolice/important/2017/20170511.html
20.「ファイルレス活動」を備えた仮想通貨発掘マルウェア「COINMINER」を確認、「EternalBlue」を利用して感染（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/15754
21.Alert (ICS-ALERT-17-206-01) CRASHOVERRIDE Malware（US-CERT）
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01
22.MAR-17-352-01 HatMan—Safety System Targeted Malware（US-CERT）https://ics-cert.us-cert.gov/MAR-17-352-01-HatMan—Safety-System-Targeted-Malware
23.Doragos Blog: TRISIS - Analyzing Safety System Targeted Malware（Doragos）
https://dragos.com/blog/trisis/
24.Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors
https://www.us-cert.gov/ncas/alerts/TA17-293A
25.Alert (ICS-ALERT-17-135-01I) Indicators Associated With WannaCry Ransomware (Update I)（US-CERT）
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01IAlert (ICS-ALERT-17-181-01C) Petya Malware Variant (Update C)（US-CERT）
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C
26.産業サイバーセキュリティセンター（IPA）
https://www.ipa.go.jp/icscoe/
27.プレス発表　産業サイバーセキュリティ人材育成施設７月始動、受講者を２月 20 日より募集開始（IPA）
https://www.ipa.go.jp/about/press/20170208.html
28.国内からの 22/TCP ポートへのアクセスの増加（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2017070701.html
NTT ドコモ Wi-Fi STATION L-02F の脆弱性に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170034.html
29.Mirai 亜種の感染活動に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2017/at170049.html

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～2018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