2015年の情報セキュリティ動向

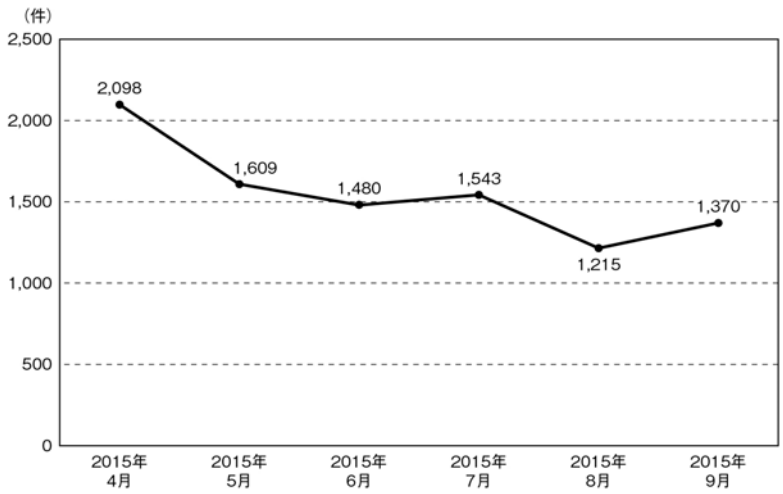
塩田 修一 ●一般社団法人JPCERTコーディネーションセンター 早期警戒グループ 情報分析ライン 情報セキュリティアナリスト

金銭を狙うマルウェアの一種であるランサムウェアは、各言語に対応したりLinuxを狙ったりなど多様化を見せながら世界的に流行した。インシデントとしては、高度サイバー攻撃が特徴的だった。

JPCERTコーディネーションセンター（JPCERT/CC）では、国内外で発生した情報セキュリティインシデント（以下、インシデント）に関する対応依頼と報告を受け付けている[1]。2015年4月から9月までに報告されたインシデント件数は9315件となり、2015年初夏ごろから報道された、いわゆるAPT（Advanced Persistent Threat）とも呼ばれる標的型攻撃の報告件数は、同期間内で119件となった（資料3-6-1、3-6-2）[2]。

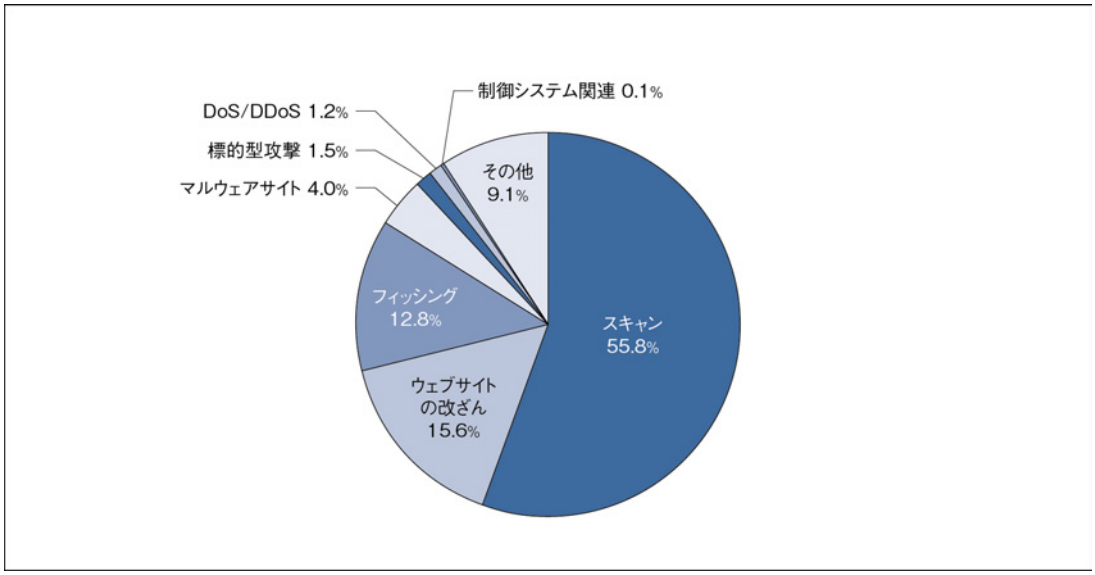
2015年の特徴的な事象を、以下に述べる。

資料3-6-1 インシデント報告件数の推移（2015年4〜9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3-6-2　インシデントカテゴリー別割合（2015年4〜9月）



出典：「JPCERT/CC インシデント報告対応レポート」を基に作成

■継続して確認されているサイバー攻撃の傾向

●ウェブサイト改ざんの傾向

ウェブサイト改ざんの報告件数は1241件と、前年同期間（2091件）よりも減少傾向に見えるが、ウェブサイトへの脅威が減少したわけではない。2015年1月には、Content Management System（CMS）へのブルートフォース攻撃が多数報告された。

ウェブサイトのコンテンツが改ざんされたことによってアクセス元のユーザーのパソコンが攻撃サイト（Exploit Kit）に誘導される攻撃についても、年間を通して報告を受けている。なお、攻撃サイトでは複数のアプリケーション（Internet ExplorerやAdobe Flash Playerなど）の脆弱性への攻撃が行われ、脆弱性が存在した場合はランサムウェアなどマルウェアへの感染被害につながることも継続して確認している。

管理するウェブサイトを改ざんから防ぐためには、利用しているCMSなどの脆弱性情報を収集し、速やかに修正プログラムを適用するほか、システム管理用パスワードを適切に管理するなどの対策がウェブサイト管理者に引き続き求められる。

●2015年のDDoS攻撃の特徴

JPCERT/CCでは、2015年6月に、金銭（Bitcoin）を要求する脅迫を伴うDDoS攻撃を国内で確認している。DD4BC（DDoS for Bitcoin）[3]と呼ばれる攻撃者は、小規模なDDoS攻撃を行った後に金銭（Bitcoin）の支払いに応じない場合はDDoS攻撃を再度行うと脅迫し、無視すると標的とした組織に対して10G〜40Gbps程度[4]のトラフィックを送りつけた。10月には、同様の手法でArmada Collective[5]と名乗る攻撃者も現れている。

また、日本で行われている捕鯨に反対するアノニマスが国内複数組織にDDoS攻撃を行い、国内外に報道されたことも注目された事案の一つといえる。

■マルウェアを使って金銭を狙う攻撃

2014年に流行したVAWTRAKやGameover Zeusのようなインターネットバンキング利用者を狙うマルウェアのほか、2015年にはパソコンのファイルをマルウェアで暗号化し、復号鍵と引き換えに金銭を要求するランサムウェアが世界的に流行した。国内外を問わず多数の事例や被害が確認されており、インシデントが国内でも報告された。いずれのマルウェアも、感染した利用者から金銭をせしめることを狙っている。

●国内でのランサムウェアの感染被害

ランサムウェアは各地域の言語に対応し、さらには亜種が生み出されて多様化しつつ、世界中で猛威を振るっている。たとえば、米連邦捜査局（FBI）によれば、ランサムウェアであるCryptoWallの被害総額（復旧費）は2014年4月から2015年6月までの期間で1800万ドルに達しているという[6]。

ランサムウェアは、利用者の金銭を狙ったマルウェアとして、サイバー犯罪の脅威の一つに数えられるほどに至っている。2015年4月には、攻撃者からの脅迫メッセージが日本語で表示される亜種が確認されている。11月には、Linuxシステムの管理者アカウントを狙ったランサムウェア[7]が確認されるなど、多様化も進んでいる。

ランサムウェアの感染経路は、改ざんされたウェブサイトからが主流である[8]。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去することや、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推奨される。ランサムウェアによって暗号化されたファイルは、要求された金銭を払って鍵を得ても完全には復号できない場合もある。そのため、重要なデータについては定期的にバックアップを取っておくことが望ましい。

●国内のインターネットバンキング利用者を狙う不正送金マルウェア

警察庁が2015年9月に発表したデータによると、インターネットバンキングに係る不正送金による2015年上半期（1〜6月）の被害は、15億4400万円に上っている[9]。マルウェアなどを使ってインターネットバンキングのID・パスワード情報を窃取し、それを悪用して被害者の預貯金を別の口座に不正に送金して引き出すのが、多くの不正送金の手口である。

2015年4月には、WERDLOD[10]と呼ばれるマルウェアが話題になった。WERDLODは大手通販サービスの請求書を偽装した日本語のメールに添付され、広範囲に配布された。WERDLODに感染すると、インターネットバンキングにアクセスしたときに不正なプロキシサーバーを経由するようになり、そこで利用者の認証情報が窃取される。8月には、利用者の認証情報や電子証明書を窃取するSHIZ[11]と呼ばれるマルウェアが話題になった。これらのほかにも、官庁を装ったフィッシングサイトに誘導し、標的とした利用者の認証情報を窃取するBrolux[12]や、信用金庫の利用者を標的としたTinba[13]などのマルウェアも確認されている。

2015年10月に観測された、不正送金のマルウェアに感染させるばらまき型メール攻撃（スパムメール）は巧妙で、攻撃当初にはウイルス対策ソフトでも検知できない場合があった。情報処理推進機構（IPA）やJPCERT/CCでは、注意喚起[14]や、早期警戒情報[15]を発行して注意を呼び掛けた。

不正送金に関連したマルウェアに対しては、使用しているソフトウェアを常に最新の状態に保つことやウイルス対策ソフトを最新化して定期的に

ウイルススキャンをするなどの対策で効果が期待できる。全国銀行協会からも対策[16]などを紹介した資料が公開されているので、参考にしていただきたい。

■高度サイバー攻撃の状況

2015年を代表する特徴的なインシデントとしては、高度サイバー攻撃が挙げられる[17]。高度サイバー攻撃は、長期間にわたり攻撃が続くとともに、攻撃されていることに気付くことが難しく、気付くまでに攻撃が2年半以上続いていた事例[18]も報告されている。

●高度サイバー攻撃で用いられたマルウェア

JPCERT/CCは2015年4月から9月までの間に、延べ133組織に、高度サイバー攻撃について調査を促す通知を行った。その結果、96組織でEmdiviと呼ばれる遠隔操作マルウェアが使用されていたことが分かったほか、PlugXと呼ばれる遠隔操作マルウェアも確認している。これらは、標的とした組織のパソコンに何らかの方法で感染させることで侵入を果たし、Command & Control（C2）サーバーからの指示を受けて動作するもので、攻撃者はマルウェアに感染した組織のパソコンを遠隔操作し、組織の機密情報を盗もうと試みる。

これらのマルウェアの感染経路は複数あることを確認している。主な感染経路は、標的型メールにして、日常業務に密接したメールにマルウェアを添付して送りつける方法である。文章やファイル名などが巧妙に偽装されているため受信者が意図せずに開いてしまい、感染へと誘導される。

その他の感染手段として、Adobe Flash Playerの脆弱性を悪用したウェブサイト経由の攻撃も確認している。これは、2015年7月に公開されたAdobe Flash Playerの脆弱性（CVE-2015-5119、CVE-2015-5122）を悪用した攻撃であった。この脆弱性においては検証コードなども流出したため、流出後すぐにマルウェア感染への悪用が始まってしまった。これにより、攻撃者が積極的に新しい脆弱性を用いていることが分かる。

脆弱性を悪用してマルウェアに感染させる攻撃に対しては、OSやアプリケーションを最新の状態に保つことが基本的な対策である。しかしながら、攻撃された時点では脆弱性が公表されておらず、対策も提供されていないことが多い。対策プログラムが提供されていない期間に脆弱性を悪用されてマルウェア感染に至ることを防ぐには、信頼していないウェブサイトにおいてAdobe Flash Playerがウェブブラウザーで実行されないようにインターネットゾーンの設定を行うことや、米MicrosoftのEMET（Enhanced Mitigation Experience Toolkit）を導入して脆弱性の影響を緩和する対策を取ることも効果がある。

●マルウェア感染後の組織内の横断的侵害

高度サイバー攻撃では、マルウェアに感染させた後、攻撃者からの遠隔操作に従って組織内の他のパソコンやサーバーを監視し感染範囲を広げていく活動が行われる。JPCERT/CCでは、このようなネットワーク内で感染範囲を拡大する活動を「横断的侵害」と呼んでいる。JPCERT/CCが対処を支援したインシデントにおいては、横断的侵害が行われた形跡がある事例を複数確認している。

横断的侵害は攻撃者にとって有益な情報を探索するために行われ、特に認証サーバー（Active Directory）が攻撃の対象となることが多い。Active Directoryは組織ネットワーク内の認証を一元的に管理しているので、同サーバーからドメイン管理者権限を有するユーザーアカウントを窃取できれば、それを悪用して他のパソコンやサーバーに侵入したり、当該管理者に許された

ファイルへアクセスしたりすることができる。

ドメイン管理者権限を不正に利用された例のうち、セキュリティ更新プログラムMS14-068で修正されたKerberos KDCの脆弱性が悪用されている事例も確認された。JPCERT/CCでも緊急性があると判断したため、2014年にこの脆弱性に関する注意喚起を行っている。

そのほか、ローカル管理者のアカウントを悪用した横断的侵害も確認されている。横断的侵害を防ぎ早期に検知するためには、アクセスログやイベントログを適切に管理し、ログに不審な形跡が残されていないかを定期的に調査することが求められる[19]。

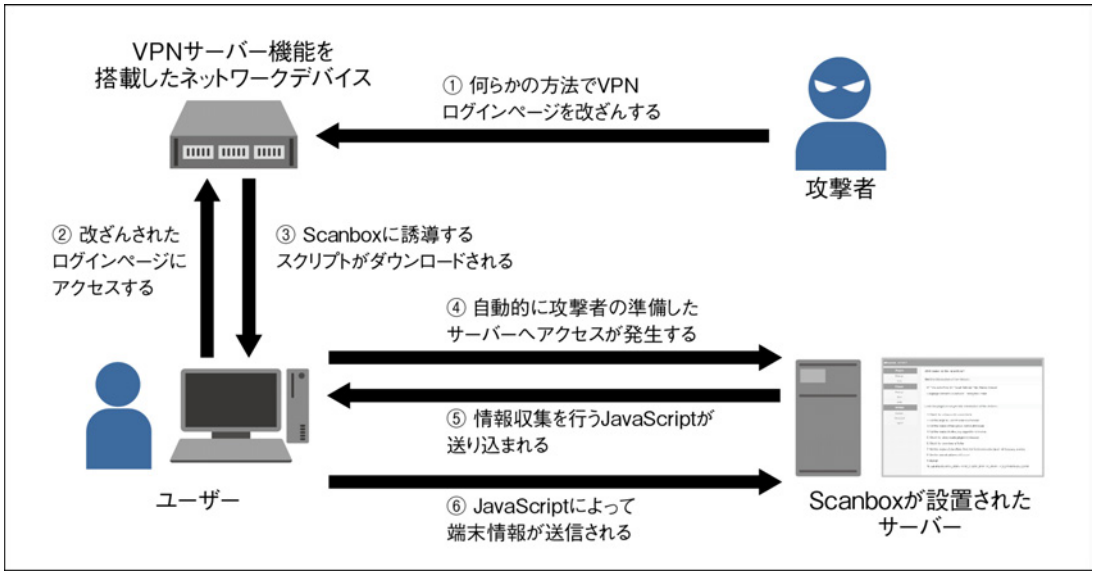
●情報窃取を目的としたツールの確認

JPCERT/CCでは、マルウェアを用いた攻撃以外に、情報窃取を目的とした、Scanboxと呼ばれる攻撃ツールを用いた攻撃を確認している。ScanboxはJavaScriptで構成された攻撃ツールで、Scanboxが仕込まれたウェブサイトにアクセスしたパソコンのウェブブラウザー上で動作し、パソコンの環境情報などを窃取する（資料3-6-3）。2015年には、VPN機器のVPN接続用ログインページが改ざんされ、Scanboxへ誘導する不正なコードを埋め込んだ攻撃[20]が確認された。

ScanboxはIPアドレスを含むパソコンの情報を収集し、VPNセッションでユーザーが入力した内容などを、ウェブブラウザーの実行が終わるまで窃取し続ける。つまり、Scanboxによる攻撃ではパソコンが継続的にマルウェア感染するわけではないが、パソコンの情報やウェブブラウザーへの入力情報が組織外にいる攻撃者に窃取されるのである。収集した情報を基に、攻撃者が次の段階の攻撃に移る可能性もある。

そのため、高度サイバー攻撃では早い段階での攻撃検知に努めるとともに、攻撃に気付いた場合は攻撃者の次の一手を勘案して防御を固める必要がある。Scanboxのような攻撃に備えるには、信頼していないウェブサイトからダウンロードしたJavaScriptがウェブブラウザーで実行されないようにインターネットゾーンの設定を行うことが推奨される。

資料3-6-3　Scanboxを使用した攻撃の流れ



出典：JPCERT/CC、「改ざんされた VPN サーバから攻撃ツール Scanbox に誘導」、『分析センターだより』、2015 年 8 月 20 日

●高度サイバー攻撃への対処

1つの高度サイバー攻撃事案に関連する機器のログを分析することにより、標的となっている他の組織を割り出せる場合がある。JPCERT/CCでは、被害の可能性がある組織に対して客観的事実を連絡するとともに、復旧に向けた対応方法も紹介している[21]。

また、攻撃の高度化に伴い、事前の対策だけですべての攻撃を防ぐことは困難になっている。そのため、侵入を受けたとしても、被害を局所化すべく迅速な検知と対応および事前の備えが重要である。サイバー攻撃を受けた組織が攻撃に少しでも早く気付けるように、JPCERT/CCでは2015年11月に、一般的な組織で利用される機器において高度サイバー攻撃の痕跡がシステムログに記録される様子と調査方法をまとめた資料「高度サイバー攻撃への対処におけるログの活用と分析方法」[22]を公開した。気が付きにくい高度サイバー攻撃を検出するための方策とともに、組織内でシステムログを活用することの重要性を記載した資料である。

JPCERT/CCだけではなく、セキュリティ関連組織などが提供している高度サイバー攻撃に関する有用な情報はさまざまある。それらの情報を参考にし、活用されることを推奨する。

■2015年に注目された脆弱性など

2015年には、glibcといった広く利用されているソフトウェアライブラリの脆弱性や、QEMUのような仮想マシン基盤に用いられるソフトウェアの脆弱性などが話題となった。ここでは、2015年に発見され注目された脆弱性と、脆弱性に関する動向を紹介する。

●glibcの脆弱性「GHOST」

2015年1月に、Linux GNU C library（glibc）の脆弱性をあるセキュリティ関連企業が報告し、「GHOST」と名付けた。悪用するとLinux OSが搭載されているパソコンで任意のコードを実行できるとして騒がれた。これは、glibcにおいて、ホ

スト名からIPアドレスを取得する関数にバッファオーバーフローの脆弱性があるというものだったが、2013年5月に修正されており、攻撃も非常に難しいことが判明した。

●HTTP.sysの脆弱性

2015年4月には、Microsoftからセキュリティ更新プログラムMS15-034が公開された。この脆弱性は、細工されたHTTPリクエストを送り付けると、HTTPプロトコルスタック（HTTP.sys）における解析処理で誤動作が起き、リモートから任意のコードを実行できる可能性があるというものである。たとえば、Windows に検証コードを使用してアクセスするとサービスを停止させることが可能だった。MS15-034が公開された直後に、脆弱性の検証コードが公開された。

●QEMUの脆弱性「VENOM」

2015年5月に、オープンソースのプロセッサーエミュレーターであるQEMUのフロッピー・ディスク・コントローラ（FDC）実装にバッファオーバーフローの脆弱性が見つかり、「VENOM」と名付けられた。これは、仮想マシンからホストシステムを攻撃する手法として注目を集めた。XenやVirtualBoxなどもこの脆弱性を継承していて、クラウドサーバーのVPS（Virtual Private Server）サービスが攻撃リスクにさらされた。

●Diffie-Hellman（DH）鍵交換の脆弱性

OpenSSLなど複数のソフトウェアにおけるDiffie-Hellman（DH）鍵交換の脆弱性が、セキュリティ研究者の合同チームによって2015年5月に公表された。これはTLSプロトコルの鍵交換における脆弱性で、攻撃者がTLS接続時に暗号化方式を格下げすることが可能であることが指摘された。結果として、攻撃者は通信の内容を傍受したり、改ざんしたりできる可能性がある。この攻撃手法は「Logjam Attack」と名付けられた。

●共通脆弱性評価システム（CVSS）v3の公表

ソフトウェアなどの脆弱性の深刻度を評価する尺度の一つが、共通脆弱性評価システム（CVSS）である。これを用いると脆弱性の深刻度や性質を、オープンで汎用的な基準の下で定量的に表現し比較することができる。それまで使用されてきたCVSS v2は2007年6月に公開されたが、CVSS v3が開発され、2015年6月に公表された。

CVSS v3では、攻撃の難易度と影響を分けて評価できるように評価項目が整理され、攻撃の影響範囲の広がりを加味するなどの改善が施されている。IPAとJPCERT/CCが共同運営している脆弱性対策情報ポータルサイト「Japan Vulnerability Notes（JVN）」[23]でも12月からCVSS v3を導入し、CVSS v2とCVSS v3による評価を併記した。

■制御システムセキュリティの動向

産業用制御システム関連では、制御ネットワークとイントラネットが相互に接続されるケースが増えており、中には制御機器がインターネットに接続され稼働していることもある。離れた場所からの遠隔操作や情報系システムとのデータ連携などが可能になることで利便性が高まるためである。

一方で、制御システムはセキュリティパッチを適用していなかったり、適切なアクセス制御が行われていなかったりするケースが多く、多数の脆弱性が潜在しているとみられている。目立ったインシデント事例は公表されていないものの、攻撃が行われるとシステムの停止など、可用性に大きな影響を及ぼしかねない。さらには、インターネットに接続された機器を検索するサービスであるSHODAN[24]においても制御システム特有のプ

ロトコルへの対応が進んでおり、脆弱な制御システムが探索され攻撃される可能性があることから、潜在的な危険性は高まっている。

JPCERT/CCではインシデントの未然防止活動として、インターネットから直接アクセス可能な制御機器を調査し、インシデントにつながり得るものについては関連組織に通知を行っている。加えて、制御システムセキュリティに関する普及啓発やセキュリティ自己評価ツールの展開を継続的に行っている。

■CSIRT構築の動向

高度サイバー攻撃など複雑化するインシデントを完全に防ぐのは難しいことから、攻撃を早期に検知して対処する重要性が認識され、組織内CSIRT[25]を構築する動きが活発化している。組織内CSIRT間の連携や情報共有などを目的とした日本シーサート協議会[26]には2015年だけで37の組織が新たに加盟し、12月1日現在で加盟組織数が106となった。今後も国内のインシデント対応体制を整備する動きは継続し、日本シーサート協議会の加盟組織数の増加傾向も続くものとみられる。

1. JPCERT/CC インシデントの報告
   https://www.jpcert.or.jp/form/
2. 同期間に、インシデント報告対応レポートに「標的型攻撃」の項目を加えた。
3. Akamai Releases Findings of Increased Attacks and More Aggressive Tactics from DD4BC Extortionist Group
   https://www.akamai.com/us/en/about/news/press/2015-press/akamai-plxsert-releases-findings-on-dd4bc-bitcoin-attack-tactics.jsp
4. セキュリティ動向2015
   http://www.iij.ad.jp/company/development/tech/techweek/pdf/151112_1.pdf
5. Armada Collective
   https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html
6. Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes
   https://www.ic3.gov/media/2015/150623.aspx
7. Encryption ransomware threatens Linux users
   http://news.drweb.com/show/?i=9686&c=5&lng=en&p=0
8. IPA 2015年6月の呼びかけ
   https://www.ipa.go.jp/security/txt/2015/06outline.html
9. 平成27年上半期の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等について
   https://www.npa.go.jp/cyber/pdf/H270903_banking.pdf
10. 日本を標的とする新たなオンライン銀行詐欺ツール「WERDLOD」の手口を解説
    http://blog.trendmicro.co.jp/archives/11258
11. 「注文確認」、「複合機」2種の偽装メールを同時に確認、狙いはネットバンキング
    http://blog.trendmicro.co.jp/archives/12343
12. Brolux trojan targeting Japanese online bankers
    http://www.welivesecurity.com/2015/10/15/brolux-trojan-targeting-japanese-banks/
13. Tinba Banking Malware Also Targeting Financial Institutions in Japan and many other countries
    http://www.secureworks.com/resources/tips-and-articles/featured_articles/media-alert-banking-trojans-attack-russian-banks
14. 【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意
    https://www.ipa.go.jp/security/topics/alert271009.html
15. 早期警戒情報の提供について
    http://www.jpcert.or.jp/wwinfo/
16. 法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方について
    http://www.zenginkyo.or.jp/topic/detail/nid/3349/
17. 高度サイバー攻撃への対処におけるログの活用と分析
    https://www.jpcert.or.jp/research/APT-loganalysis_Report_20151117.pdf
18. サイバー情報共有イニシアティブ（J-CSIP）2014年度活動レポートの公開
    https://www.ipa.go.jp/about/press/20150527.html
19. 高度サイバー攻撃への対処におけるログの活用と分析方法
    https://www.jpcert.or.jp/research/apt-loganalysis.html
20. 改ざんされたVPNサーバから攻撃ツールScanboxに誘導
    https://www.jpcert.or.jp/magazine/acreport-scanbox.html
21. 第5回 JNSA記者懇談会 緊急時事ワークショップ ～他人事ではない、サイバー攻撃を受けた組織の選択肢～ においての講演資料
    https://www.jpcert.or.jp/present/2015/JNSAWG20150630-apt.pdf
22. 高度サイバー攻撃への対処におけるログの活用と分析方法
    https://www.jpcert.or.jp/research/apt-loganalysis.html
23. Japan Vulnerability Notes（JVN）
    https://jvn.jp/
24. SHODANを悪用した攻撃に備えてー制御システム編ー
    https://www.jpcert.or.jp/ics/20150609ICSR-shodan.pdf
25. CSIRT：Computer Security Incident Response Team。コンピューターセキュリティに係るインシデントに対処するための組

織の総称。

26. 日本シーサート協議会
http://www.nca.gr.jp/

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～2016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。

http://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