2014年の情報セキュリティ動向

松本 悦宜 ●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

Web改ざん、パスワードリスト攻撃が継続発生し、ネットバンキング不正送金が過去最悪を更新。標的型攻撃が深刻化し、新たな脆弱性や制御システムの脅威も注目された。対策として国際連携や、情報共有作戦が成果を上げつつある。

インターネット上の脅威は増加の一途をたどっており、2014年もさまざまな情報セキュリティインシデントが発生した。ここでは、2014年に発生した情報セキュリティインシデントのうち、注目された事例や特徴的な事例について述べる。また、昨今注目を浴びつつある制御システムのセキュリティ動向についても触れたい。

■Web改ざんの継続的な発生

一般社団法人JPCERTコーディネーションセンター（以下、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]。このうち、Webサイトの改ざんに関するインシデント報告は、2013年に大きく増加し、2014年も9月現在で3500件を超える報告を受領している[2]。

報告を受けたWebサイトの改ざんでは、不審なiframeや難読化されたJavaScriptが挿入されていて、一見しただけでは改ざんされているとは分からないケースが多い。気付かないまま利用者がアクセスすると、攻撃ツール(Exploit Kit)が設置されたサイトに転送され、利用者のパソコンに脆弱性があればマルウエアに感染してしまう可能性がある。マルウエアが利用者のパソコンを感染させるために使用する脆弱性の多くは既知のものであり、OSやアプリケーションを最新の状態に保つことで、マルウエア感染を防げることが多い。このような基本的なセキュリティ対策を徹底することが重要である。

Webサイトを改ざんする手口の詳細は分かっていないが、何らかの方法で盗み出したWebサイトの管理者用のID・パスワードでコンテンツ管理システムに不正にログインしたり、システムに内在する脆弱性を悪用するなどして、ファイルの書き換えを行ったりしていると考えられる。

●CMS利用サイトの改ざん

最近では、Webサイトの管理・運用コストを低減するために、CMS(Content Management System)が利用される。CMSは、ホスティング事業者などの契約者向けサービスとして普及しているばかりでなく、企業の自営サイトなどにおいても広く使用されている。CMSの普及が進むにつれ、特定のCMSで管理されたWebサイトに共通したインシデントが発生するケースも増加している。

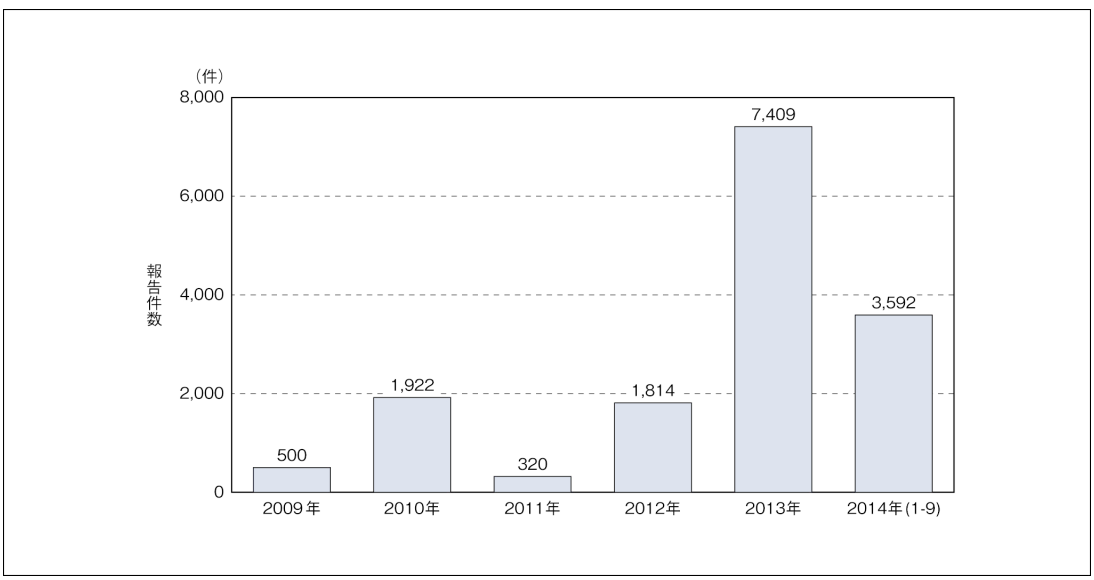
個々のインシデントで判明した断片的な事実を総合すると、次のようなシナリオで大規模に改ざ

んが行われていると考えられる。既知の脆弱性をもつCMSで管理されているWebサイトを、検索ツールなどを利用して探し出し、脆弱性を利用して攻撃する。ログイン権限を奪取して、機密情報を窃取したり、閲覧者をマルウエアに感染させるためにファイルを改ざんしたりする。

多くのCMSには、サードパーティから多様な拡張機能が提供されているが、これらの拡張機能の中にも脆弱性が存在しうる。そうした場合、CMS本体についてはパッチの適用などの脆弱性対策をしていても、拡張機能の脆弱性は放置されたままになっていることが多く、それを狙った攻撃事例が少なくない。

こうした攻撃によりWebサイトが改ざんされるなどの被害の可能性を低減するには、CMS本体だけでなく拡張機能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ための体制を構築、維持することが重要である。

資料4-6-1　Webサイトの改ざんに関するインシデントの報告件数



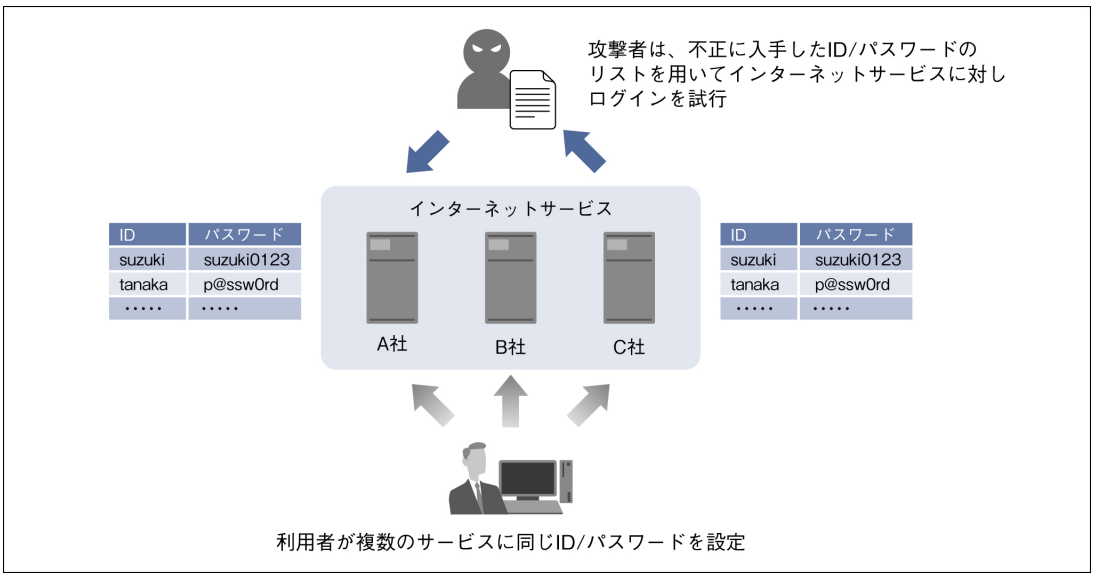
出典：JPCERT/CC インシデント報告対応レポート[3]（2009年～2014年）より作成

■パスワードリスト攻撃

●パスワードリスト攻撃とは

2013年3月ごろから始まった、国内の事業者が提供するWebサービスに対して大量の不正ログインを試みる攻撃は、2014年も継続的に発生した。別の事業者から漏えいしたIDとパスワードの対のリストを使用してログインを試みるこの手法は、一般に「パスワードリスト攻撃」と呼ばれている。パスワードリスト攻撃は、利用者が同じパスワードを複数のWebサイトで使い回していると成功確率が高まる。公表された被害状況報告によれば、数万件から数百万件のログインが試行され、その1%前後で不正なログインに成功したとされている。

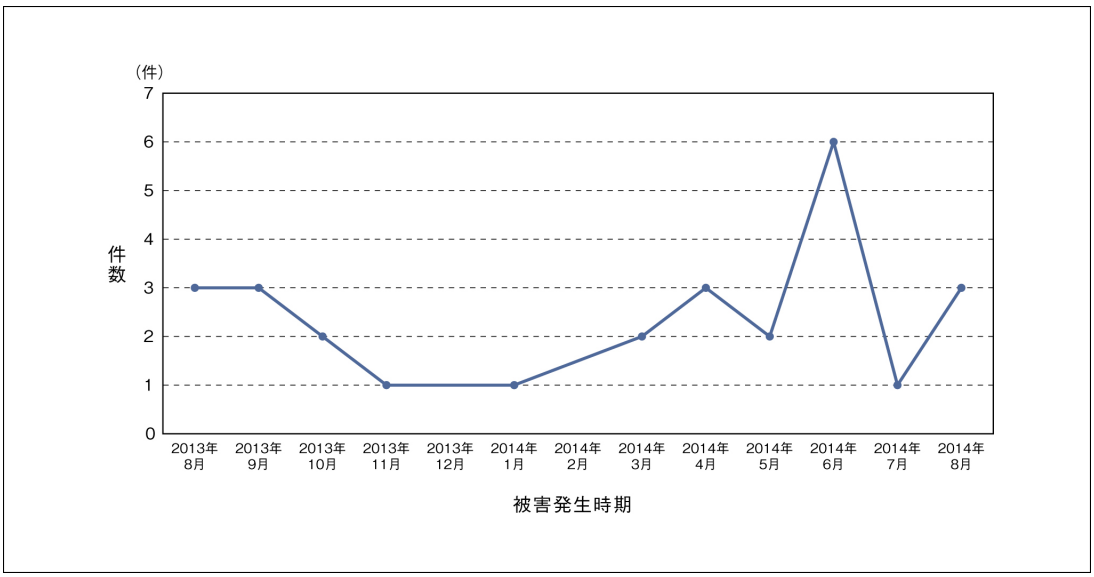
資料4-6-2　パスワードリスト攻撃の概要



出典：STOP!! パスワード使い回し!! パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ[4]（JPCERT/CC および IPA、2014 年 9 月）

不正ログインに成功した場合、アカウント保有者の個人情報やクレジットカード情報が窃取されている。一部では、クレジットカードを不正に利用されたり、アカウント保有者になりすましてその知人にプリペイドカードを購入して送らせたりするなど、金銭被害も発生している。対策はパスワードの使い回しをしないことだが、サービスごとに異なるパスワードを設定し覚えていることは、多くの利用者にとって現実には難しい。それを狙って今後も攻撃が継続すると推察されることから、クレジットカード情報などの機微な情報を管理するサービスにおいては、「二要素認証」などのより安全な認証方式への切り替えが望まれる。

資料4-6-3　パスワードリスト攻撃による被害を受けた企業数の推移



出典：STOP!!パスワード使い回し!! パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ（JPCERT/CC および IPA、2014 年 9 月）

●パスワードの使い回しストップを呼びかけ

パスワードリスト攻撃による不正ログインの被害が後を絶たないことから、独立行政法人情報処理推進機構 (IPA) および JPCERT/CC は、2014年9月に「パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」[5] を公開し、複数のサービスにおいて同じパスワードを使い回さないよう、インターネットサービス利用者に注意を促した。

■金融機関を狙うマルウエア

ここ数年、インターネットバンキング利用者を対象としたフィッシングやマルウエアによる被害が増加傾向にある。警察庁が2014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の不正送金による2014年上半期の被害は18億5200万円に上り、過去最悪を更新した。被害は、マルウエ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た攻撃者が、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ことで発生している。

●マルウエア「VAWTRAK」について

インターネットバンキングのID・パスワード情報の窃取に使用されるマルウエアとして、VAWTRAKと呼ばれるマルウエアが2014年5月ごろから話題になった。VAWTRAKはブラウザに侵入し、利用者がインターネットバンキングサイトにアクセスした時に、自動的に不正送金などを行う一方で、それを画面上では利用者に見せないようにしていると言われる。

従来、このようなマルウエアが動作するのは、主に大手銀行のインターネットバンキングにアクセスした時のみであったが、最近では国内のカード会社にアクセスした時にID・パスワード情報が窃取され、その後の不正なカード利用に使われる可能性があることがセキュリティベンダーの調べで確認された。

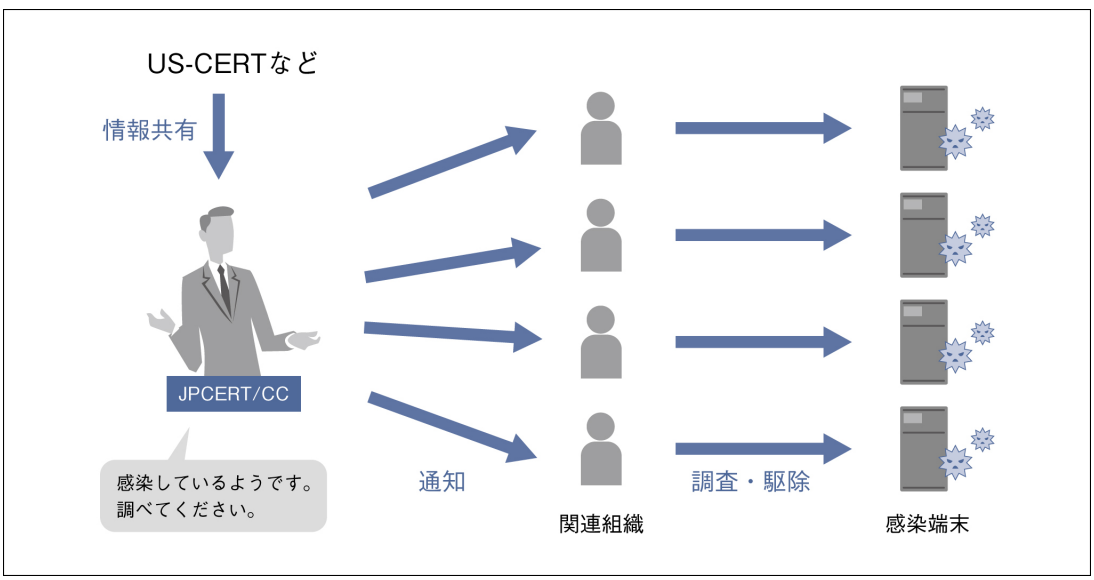
これら不正送金に関連したマルウエア感染の防止は、OSやアプリケーションの修正プログラムを

できるだけ早く適用するといった一般的なセキュリティ対策で十分な効果が期待できる。

●マルウエア「Game Over Zeus」について

不正送金などに使用されているマルウエア「Zeus」の亜種である「Game Over Zeus」が2011年ごろから継続的に確認されており、世界中で感染事例が確認されていた。海外では、米国連邦捜査局（FBI）および欧州刑事警察機構（ユーロポール）が中心となり、協力国の法執行機関、各国CSIRTと連携して、2014年5月から「国際的なボットネットのテイクダウン作戦」[6]を行った。国内では2014年7月からJPCERT/CCが、警察庁、総務省、一般社団法人日本データ通信協会テレコム・アイザック推進会議と協力し、国際連携活動の枠組みを通じて米国US-CERT等から提供された感染端末情報に基づいて、国内の感染端末利用者に対する通知と、不正プログラムの駆除等に関する情報提供を行った。

資料4-6-4　国際的なボットネットのテイクダウン作戦（JPCERT/CC の取り組み）



出典：JPCERT/CC

■2014年に発見され注目された脆弱性

2014年は、「OpenSSL」 や「bash」など多くのシステムで使用されているソフトウエアの深刻な脆弱性が発見された。これらの脆弱性は、攻撃に使うことが容易であったため、発表されてから1日足らずで悪用した攻撃が確認された。脆弱性対応が遅れたシステムの中には、被害が発生した事例もあった。以下、2014年に発見され注目された2つの脆弱性について紹介する。

●OpenSSLの脆弱性「Heartbleed」

暗号化通信などで広く使用されているオープンソースソフトウエアOpenSSLに情報漏えいの脆弱性があることが、2014年4月に公表された。この脆弱性を悪用するよう細工したパケットを送付する遠隔の第三者が、サーバーのメモリ内の情報を閲覧できる可能性があった。本脆弱性はOpenSSLのheartbeat拡張に関連していたため、Heartbleedと呼ばれている。OpenSSLはWebサーバーなど

さまざまなソフトウエアで使用されており、攻撃が容易である、本脆弱性を使用した攻撃はログに残らないなどの特徴で、システム管理者を戸惑わせた。

本脆弱性を使用した攻撃が一部のシステムで確認されており、警察庁の定点観測システムでは、本脆弱性の発表から数日後に、本脆弱性が存在するサーバー等の探索行為と考えられるパケットを観測したと発表した。また、国内の組織でも本脆弱性を使用した攻撃により、サーバーに不正アクセスが行われて個人情報が漏えいした事例も確認された。

●bash の脆弱性「ShellShock」

サーバーなどで広く使用されているオープンソースソフトウエアGNU bash の環境変数の処理に、ShellShockと呼ばれる脆弱性があることが、2014年9月に公表された。外部からの入力が環境変数に設定されるGNU bash の動作環境では、遠隔の第三者によってサーバーの任意のコマンドが実行される可能性があった。

本脆弱性はWebサーバーも影響を受け、細工したパラメータを遠隔の第三者がWebサーバーに送ることによって、サーバーの任意のコマンドを実行する可能性があった。本脆弱性の攻撃も一部のシステムで確認されており、本脆弱性を使用した攻撃を受けたサーバーがマルウエアに感染する事例も見られた。

■標的型攻撃

昨今、国内外で大きな問題となっているのが、政府や企業を対象として行われる標的型攻撃であり、中でも特定の企業や組織に対し執拗かつ効果的に攻撃を行うAPT（Advanced Persistent Threat）と呼ばれる脅威が深刻になっている。標的型攻撃は、2000年代後半から始まったと言われており、国内外の政府や企業を対象として、対象に特化した内容のマルウエア添付メールを送りつけ、マルウエアに感染させることで、企業や組織の機密情報を盗もうと試みる。

標的型攻撃の対策で特に難しいのは、一時的に攻撃を防ぐことができたとしても、目的を達成するまで攻撃が繰り返されるため、いつか攻撃が成功してしまう可能性が高いことである。このため、標的型攻撃への対策では、攻撃に使用された要素情報（IPアドレス、メールアドレス、URLなど）を基に、ネットワーク機器やIDS（侵入検知システム）などのセキュリティ製品などの未然防止の取り組みだけでなく、頻繁にログを確認するなどして、インシデントが発生した際に早期に検知するとともに攻撃の範囲を的確に把握し、被害を最小限にするための対処を迅速に実施できる運用体制作りを行うことが望ましい。

ともに類似した攻撃を受ける可能性がある組織同士で攻撃に関する情報を共有することで、より早い段階で攻撃を検知し攻撃の全体像を把握できる可能性があり、国内では情報処理推進機構（IPA）が参加組織間のハブとなった情報共有の枠組み「J-CSIP」[7]を運用しており、成果を上げ始めている。

また、各企業でもインシデントに備え、組織内にCSIRT（Computer Security Incident Response Team；コンピュータセキュリティにかかるインシデントに対処するための組織の総称）を構築する動きが活発になっている。組織間でのCSIRT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[8]には、2014の間に19もの組織が新たに加盟した。

●アップデートハイジャック

2014年ごろから、「アップデートハイジャック」とよばれる手法が国内で確認された。この手法は、まず攻撃対象となる組織が利用するソフトウエア

の正規のアップデートサーバーなどに侵入し、アップデート情報を改ざんする。利用者を不正なサーバーに誘導して改ざんされた悪意あるファイルをダウンロードさせ、アップデートされたソフトウエアだと勘違いさせて開かせることで、マルウエアに感染させる。

正規のソフトウエアにコード署名が付されていれば、攻撃者が署名した悪意あるファイルを用意していない限り、署名を確認することで悪意あるファイルか否かを判断できるはずが、アップデートのプロセスが自動化されている場合などは、確認する機会が事実上ない。また、攻撃者が正規のコードサイニング証明書を入手していた場合には、攻撃者が用意した悪意あるファイルと正規のファイルとをコード署名により区別することができない。

アップデートハイジャックは、ソフトウエアを使用する不特定多数の利用者を対象にできる攻撃であるが、標的型攻撃で使用される場合には、攻撃対象となる組織のIP アドレスからアクセスされた時は上述のような攻撃を行うが、他からアクセスされた時には何の悪さもしないなどの手法が併せて用いられた。

標的とされた組織が、この種の攻撃自体を防ぐことは困難だが、組織内で導入してよいソフトウエアを管理することや、ネットワーク機器やIPSなどのセキュリティ製品などのログを確認することにより、不正なファイルが配信された場合にも影響範囲を把握し、迅速に対応することが可能である。

●ドメイン名ハイジャック

JPCERT/CC は、国内組織が使用している .com ドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバーの情報が追加されるドメイン名ハイジャックのインシデント報告を、複数受領した。ドメイン名の登録情報 (以下、登録情報) の不正書換えによるドメイン名ハイジャックの影響により、一部の利用者が当該組織の Web サイトを閲覧する際の名前解決において、本来のサーバーとは異なる IP アドレスに誘導され、攻撃者が用意したサーバーに接続していたことを確認した。

ドメイン名を使用してサービスを提供している Web サイトなどのシステムは、登録情報の不正な書き換えによるドメイン名ハイジャックの影響を受ける可能性がある。現在も、報告を受けたインシデントの攻撃シナリオの全容を確認できてはいないが、ドメイン名登録者やドメイン名管理担当者は、登録情報を管理するための ID やパスワードなどの認証情報が第三者に不正に使用されないように適切に管理するとともに、早期検知による被害の軽減策として、whois などのコマンドを利用し、ネームサーバー情報などの登録情報が正しく設定されているか定期的に確認することが望ましい。

■制御システムセキュリティ

一般に、制御システムは最近までセキュリティに対する配慮を欠いたまま設計・構築されたものが多く、10年以上に及ぶライフタイムを通じてセキュリティパッチを適用する慣習が定着していないため、多数の脆弱性や弱点が潜在していると見られる。幸いにして国内では、これまでWindows PC一般を狙ったマルウエアに感染した制御システムが不具合を起こす事例が散見されるにとどまっている。しかしながら、海外では、制御システムに対するサイバー攻撃の事例が少しずつ積み上がってきており、対策が急がれている。

制御システムを狙うマルウエアは2010年に報告された「Stuxnet」だけとされてきたが、2014年には「Havex」および「Black Energy 2」と呼ばれるマルウエアの感染事例が海外で報告された。

いずれも制御システム向けに作り込まれた機能を備えているが、制御動作に影響を及ぼす機能はもたず、システムの内部情報の収集だけを目的に作られたマルウエアとされている。また、インターネットに接続された制御システム用機器が200万台以上見つかったとの報告もあった。

制御システムのインシデントは、人命や市民生活に影響を及ぼす事故を引き起こす可能性があり、セキュリティ対策が急がれている。技術研究組合制御システムセキュリティセンター（CSSC）[9]は、制御機器（組込み機器）のセキュリティ保証に関する認証制度EDSA(Embedded Device Security Assurance)の運用を開始し、一般財団法人日本情報経済社会推進協会（JIPDEC）では制御システムのセキュリティ管理システムの認証制度の運用を開始した。JPCERT/CCにおいても、制御システム用製品の脆弱性情報の取り扱いを主要ベンダーの協力を得て本格化し、インシデント対応の支援を行うための態勢整備を進めている。

1.JPCERT/CC インシデントの報告
https://www.jpcert.or.jp/form/
2.JPCERT/CC インシデント報告対応四半期レポート
https://www.jpcert.or.jp/ir/report.html
3. 脚注２参照
4.STOP!!パスワード使い回し!! パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ（JPCERT/CC およびIPA、2014年９月）
https://www.jpcert.or.jp/pr/2014/pr140004.html
5. 脚注４参照
6.JPCERT/CC、「インターネットバンキングに係わる不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について～国際的なボットネットのテイクダウン作戦～」に協力
https://www.jpcert.or.jp/pr/2014/pr140002.html
7. サイバー情報共有イニシアティブ（J-CSIP；ジェイシップ）
https://www.ipa.go.jp/security/J-CSIP/
8. 日本シーサート協議会
http://www.nca.gr.jp/
9. 制御システムセキュリティセンター
http://www.css-center.or.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～2015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