2013年の情報セキュリティ動向

中谷 昌幸 ●JPCERTコーディネーションセンター 早期警戒グループマネージャ 情報セキュリティアナリスト

Web改ざんが多発し、パスワードリスト使う不正アクセスやネットバンクの不正送金、政府や企業狙う標的型攻撃も増加。不足するセキュリティ人材の育成が新たな課題に。

インターネットを取り巻く脅威は増加の一途をたどっており、2013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、2013年に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）のうち、主要なものや特徴的なものについて取り上げる。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と情報セキュリティに関する人材育成についても触れたい。

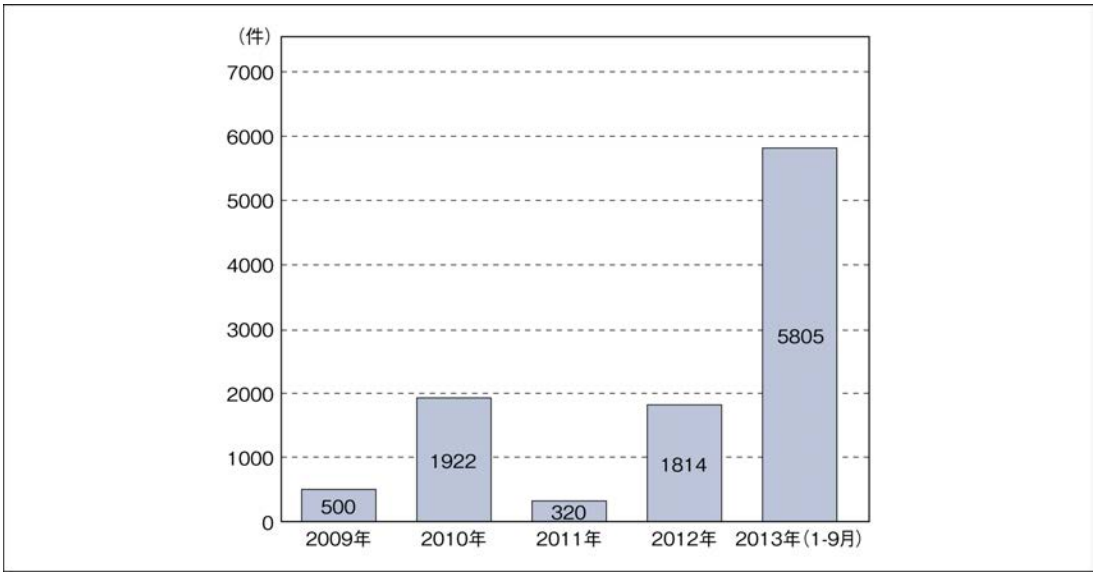
■Web改ざんの多発

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]（資料5-4-1）。このうち、Webサイトの改ざんに関する2013年のインシデント報告は、9月時点ですでに前年の3.2倍となっている[*2]。

「不審なiframe」や「難読化されたJavaScript」が挿入されるタイプの改ざんが多く、それらのWebサイトは一見しただけでは改ざんされているとは分からない。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、利用者のパソコンが脆弱性を持っていた場合にはマルウエアに感染してしまう可能性がある。多くの場合、マルウエアがユーザーのパソコンに感染するために使用する脆弱性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ぐことができる。したがって、ユーザーは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。

これらWebサイトの改ざんの手口について、詳細は分かっていないが、攻撃者はWebサイトの管理者用のID・パスワードを何らかの方法で盗み出し、それを使用して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使用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。

資料 5-4-1 Web 改ざんインシデント報告件数



出典：JPCERT/CC インシデント報告対応レポート [2013 年 7 月 1 日～2013 年 9 月 30 日]

次に、2013 年に発生した Web 改ざんに関して特徴的な事例をいくつか紹介する。

● CMS で管理されているサイトの改ざん

昨今、Web サイトを容易に管理できるようにして管理・運用コストを低減するために、CMS(Content Management System) が利用されている。CMS は、ホスティング事業者などのサービスを中心に広く利用されるようになり、一説には全 Web サイトの 3 分の 1 は CMS を使用したものだと言われている。CMS の普及が進む一方で、CMS で管理された Web サイトに固有のインシデントが増加している。

複数のインシデント事例を総合すると、次のようなシナリオで改ざんが行われていると考えられる。既知の脆弱性を内在した 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、CMS の脆弱性を利用して当該 Web サイトを攻撃する。攻撃者はログイン権限を奪取し、機密情報を窃取したり、ファイルの改ざんや閲覧者を感染させるためのマルウエアを設置したりする。

多くの CMS には、多様なプラグインが提供されており、プラグインが脆弱性を持つ場合もある。CMS 本体についてはパッチの適用などで脆弱性を修正していても、プラグインの脆弱性が放置されていることがあり、それを狙った攻撃事例も少なくない。

CMS およびプラグインの脆弱性情報を収集し、修正プログラムの公開後速やかに適用することで、Web サイト改ざんなどの被害の可能性を大きく低減できる。Web サイトの管理者は、CMS に関しても脆弱性対策のための体制を構築、維持することが重要である。なお、一部の Web ホスティングサービスでは、顧客に Web サイトの管理者権限が与えられているが、その場合には、顧客が脆弱性対策を行わなければならない。

● Darkleech による Web サイト改ざん

2013 年 3 月、「Darkleech」または「Darkleech

Apache Module」と呼ばれる新たなマルウエアが確認された。このマルウエアは、サーバー上のコンテンツファイルを書き換えることはしないが、Web サーバーソフトウエアである Apache に何らかの手段で不正なモジュールを埋め込み、それを用いて Apache から Web ブラウザへ応答メッセージとして送られる段階で、Web コンテンツを動的に書き換える。

この Web サイト改ざんでは、サーバー上に存在するコンテンツファイル自体は書き換えられないため、サーバー上のコンテンツファイルを監視していても改ざんを見つけることはできない。このため、改ざんに管理者が気付くまでに相当の時間が経過してしまう危険性がある。

「Darkleech」による Web サイト改ざんは、2013 年夏以降減少しているようであるが、これは何かしらの対策が功を奏したというわけではなく、一時的に攻撃者が攻撃を抑制したり、より見えにくい攻撃に手口が変わったりした可能性があるため、引き続き注意が必要である。

■パスワードリストを使用した不正アクセス

2013 年 3 月ごろから、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が発生している。これは、別の事業者から漏洩した ID とパスワードの対のリストを使用して不正ログインを試みるもので、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の成功確率は、ユーザー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高まる。公表された被害状況を見ると、数万件から数百万件のアカウントに不正なログインが試行され、その 1% 前後で不正なログインが成功したとされているケースが多い。

攻撃者はログインに成功した場合、アカウントの個人情報やクレジットカード情報を窃取しており、一部では盗み取られたクレジットカード情報の不正利用といった被害も発生している。

ユーザーの対策としてパスワードの使い回しをしないことが求められるが、サービスごとに異なるパスワードを設定することをユーザーに徹底させるのは、現実には難しい。さらに今後も攻撃の継続が推察されることから、クレジットカード情報などの機微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の提供が望まれる。

■金融系マルウエア ― Zeus(Citadel)

ここ数年、インターネットバンキングユーザーを対象とした、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 2013 年 10 月 18 日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被害は 2013 年 1 月から 10 月中旬で 7 億 6 千万円に上り、過去最悪を更新している。これらの被害は、主にマルウエア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することで発生している。

この金融口座情報の窃取に使用されるマルウエアとしては、Zeus が有名であり、被害の多くは Zeus の亜種である Citadel によって引き起こされていると言われている。

これら不正送金に使用されるマルウエアへの対策は特別なものではなく、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。

■ DNS Amp による DDoS 攻撃

2013 年 3 月、海外のクラウド事業者が大規模

なDDoS攻撃を受けたと発表した。DNS Amp攻撃[*3]は、DNSの「再帰的な問い合わせ」を悪用したものだ。インターネットからの再帰的な問い合わせを許可しているDNSキャッシュサーバー(以下、オープンリゾルバ)に、攻撃対象サーバーのIPアドレスを送信元IPアドレスとして設定した再帰的な問い合わせパケットを多数送りつける。これにより、攻撃対象のサーバーに多量の、しかも比較的サイズの大きな応答パケットを送りつける攻撃である。

DNS Amp攻撃を受けたサーバーは、回線帯域を埋め尽くされたり、システムのリソースが枯渇したりして、サービスが維持できなくなるなどの状態に陥ってしまう。この攻撃は多数の一般のDNSサーバーを経由して行われるため、攻撃者の特定が難しい。送信元のIPアドレスも広範囲に及ぶため、IPアドレスによるフィルタでは対策が難しい。

3月に発生したDDoS攻撃は5月に犯人が逮捕されたが、同様の手口を使用したと思われるDDoS攻撃はその後も発生している。各国のCSIRTやISP事業者が、オープンリゾルバとなっているサーバーへの注意喚起を行ったり、オープンリゾルバとなっているDNSサーバーを確認するサイト[*4]を公開したりするなどして、攻撃のプラットフォームとなるオープンリゾルバの削減に努めている。

■標的型攻撃(主にAPT)

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、特にAPT(Advanced Persistent Threat)による攻撃が深刻である。APTは通常、特定の企業や組織を執拗かつ効果的に攻撃する能力と意思を兼ね備えた集団を表す。

APTによる攻撃は、2000年代後半から始まったと言われている。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。

APT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、攻撃者は目的を達成するまで攻撃を繰り返してくるため、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、現在APTへの有効な対策として考えられているのは、事故前提でインシデントが発生した際に、攻撃の範囲を的確に把握し、被害を最小限にする運用体制作りと、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)を共有することによる未然防止の取り組みである。

攻撃を受けた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て情報共有の枠組み[*5]を運用しており、成果を上げ始めている。

■制御システムセキュリティ

電力、ガスなどのエネルギー生成や配送、各種製造工場などの設備の運用をオートメーション化し、稼働状態を遠隔監視・制御しているのが制御システムである。制御システムにも、広くTCP/IPなどのオープンシステム技術が取り入れられるとともに、制御システム用ネットワークと他のネットワークとの接続が急速に進んでいる。そのため、サイバーインシデントの脅威が制御システムでも高まっており、制御システムのセキュリティが注目されている。

制御システムにおけるインシデントは、人命に関わったり、大勢の市民に影響が及んだりする可能性がある。そのような深刻なインシデントの報告は少数の海外事例が報告されているのみで、

まだ国内ではマルウエア感染による不具合が散見されるにとどまっている。制御システム用製品は、攻撃のない環境で使われることを前提に、セキュリティへの配慮なしに開発されたものが多い。ところが、インターネットに接続された機器を検索するシステムを利用して調べた結果として、数十万台の制御システム用製品がインターネットに直結されていることが報告されている。また、脆弱性の報告件数も増加の一途をたどっている[*6]。

こういった状況から、国内でも制御システムのセキュリティ対策に向けた動きが本格化し始めている。各制御機器ベンダーがセキュリティソリューションの提供を始めたのに加え、「技術研究組合制御システムセキュリティセンター[*7]」(CSSC) が東北多賀城本部を開設してテストベッド環境を整備するとともに、制御機器（組み込み機器）のセキュリティ保証に関する認証制度であるEDSA(Embedded Device Security Assurance) の準備を進めている。また、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に関するマネジメントシステムの認証制度のパイロットプロジェクトに取り組んでいる。他方、JPCERT/CC においても、制御システムのインシデント報告を受け付け、対応の支援を行うための態勢整備を進めている。

■情報セキュリティ人材の育成

ここまで述べたように、インターネット上の脅威は増加し、企業や組織を取り巻く環境は悪化している。事故の発生を前提とした対策を行っていくために、各企業等がCSIRTのようなインシデントに対応できる専門組織をもつことが重要である。そのためのセキュリティに関して高いスキルをもつ人材が、日本全体として質量ともに大きく不足しているとされている。今般、政府がとりまとめた「サイバーセキュリティ戦略[*8]」(2013年6月10日情報セキュリティ政策会議決定) においては、「潜在的には約8万人のセキュリティ人材が不足している状態」に対応するため、さまざまな情報セキュリティ人材の育成に向けた取り組みを行うこととしている。

国内での人材育成の取り組みとしては、古くはIPAが2004年より実施している「セキュリティキャンプ[*9]」がある。2013年には、JNSAが学生を対象に実施した大会と経済産業省が社会人向けに実施した大会を融合したハッカー大会である「SECCON2013[*10]」や、5つの大学が連携して実施する「実践セキュリティ人材の育成コース（SecCap）[*11]」といった、新しい取り組みが行われている。

---

*1. インシデントの報告（JPCERT/CC）
https://www.jpcert.or.jp/form/
*2. 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
*3. DDoSにあなたのDNSが使われる〜DNS Ampの脅威と対策〜（JPRS）
http://jprs.jp/related-info/guide/003.pdf?
*4. オープンリゾルバ確認サイト（JPCERT/CC）
http://www.openresolver.jp/
*5. サイバー情報共有イニシアティブ（J-CSIP:ジェイシップ）（IPA）
http://www.ipa.go.jp/security/J-CSIP/
*6. ICS-CERT Year in Review – FY 2012
https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2012_Final.pdf
*7. 制御システムセキュリティセンター
http://www.css-center.or.jp/
*8. サイバーセキュリティ戦略（内閣官房情報セキュリティセンター）
http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf
*9. セキュリティキャンプ（IPA）
http://www.ipa.go.jp/jinzai/renkei/index_5.html
*10. SECCON2013
http://2013.seccon.jp/
*11. SecCap
http://www.seccap.jp

［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～2014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