ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●アカウントへの不正アクセス収まらず、IPAパスワードを使いまわさないよう注意喚起

http://news.mynavi.jp/news/2014/09/18/036/
http://internet.watch.impress.co.jp/docs/news/20140912_666654.html
http://www.itmedia.co.jp/enterprise/articles/1409/26/news170.html
http://www.ipa.go.jp/about/press/20140917.html

このニュースをザックリ言うと・・・

-国内Webサービスに対する不正ログイン攻撃が依然として発生しています。

- 9月12日、JR東日本が「My JR-EAST」に対し約21,000アカウントへの不正ログインがあったことを発表し、また26日には、ヤマト運輸の「クロネコメンバーズ」に対し10,589アカウントへの不正ログインがあったことが発表されています。

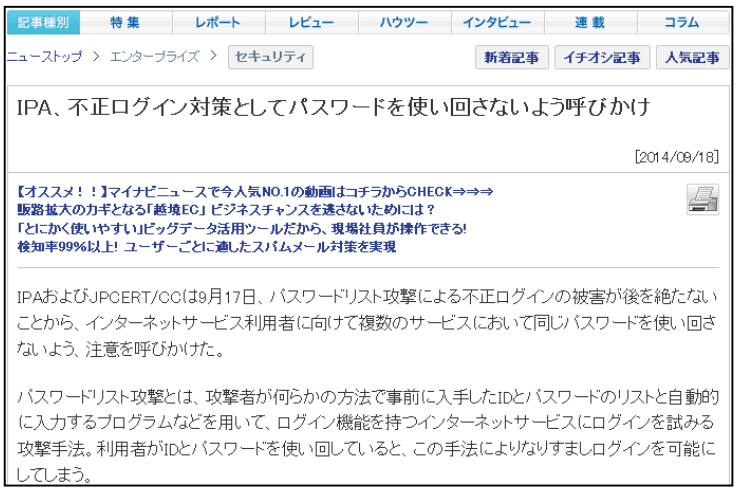
- これと前後して、17日、IPAが「パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」と題したプレスリリースを発表し、複数のサービスでパスワードを使い回さないよう啓発しています。

AUS便りからの所感等

- パスワード管理に関するセオリーとしては長年議論がなされ、有効とされる対策も時代とともに徐々に変化しており、これまでは批判も多かった「メモに書き留める」というものも、実際に設定するパスワードが比較的複雑で、かつメモ等を厳密に管理している限り、有効とされるようになっています。

- IPAのプレスリリースでは、安全でないとされる管理方法や推奨される対策等がまとまっていますので、今回のプレスリリースを叩き台にパスワードの設定・管理方法を検討すると良いでしょう。

- なお、推測されやすいような短い・簡単なパスワードを使わないことにも十分注意しましょう。


記事種別 | 特集 | レポート | レビュー | ハウツー | インタビュー | 連載 | コラム

ニューストップ > エンタープライズ > セキュリティ　新着記事 イチオシ記事 人気記事

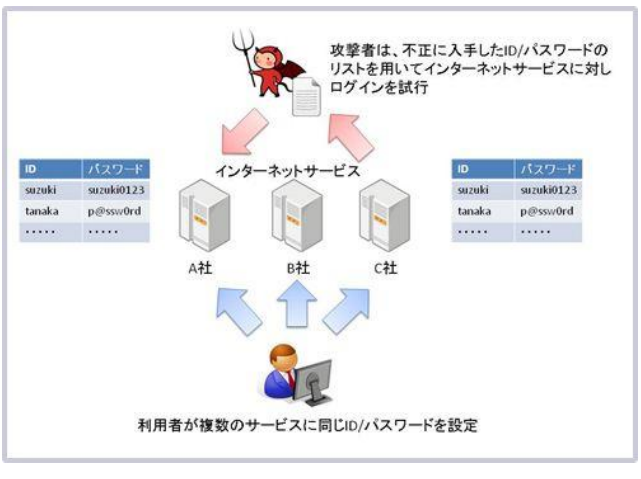
IPA、不正ログイン対策としてパスワードを使い回さないよう呼びかけ

[2014/09/18]

【オススメ！！】マイナビニュースで今人気NO.1の動画はコチラからCHECK⇒⇒⇒
販路拡大のカギとなる「越境EC」ビジネスチャンスを逃さないためには？
「とにかく使いやすい」ビッグデータ活用ツールだから、現場社員が操作できる！
検知率99%以上！ ユーザーごとに適したスパムメール対策を実現

IPAおよびJPCERT/CCは9月17日、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、インターネットサービス利用者に向けて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、注意を呼びかけた。

パスワードリスト攻撃とは、攻撃者が何らかの方法で事前に入手したIDとパスワードのリストと自動的に入力するプログラムなどを用いて、ログイン機能を持つインターネットサービスにログインを試みる攻撃手法。利用者がIDとパスワードを使い回していると、この手法によりなりすましログインを可能にしてしまう。



●海外のサービスを利用、NTPサーバを悪用したDDoS攻撃

http://web.archive.org/web/20140919235124/http://www3.nhk.or.jp/news/html/20140918/k10014688641000.html
http://www.jiji.com/jc/zc?k=201409/2014091800340
http://www.yomiuri.co.jp/it/20140918-OYT1T50094.html

このニュースをザックリ言うと・・・

- 9月17日、全国初となるDDoS攻撃の容疑により、熊本市の少年が書類送検されました。
- 容疑者は、サイバー攻撃代行業とされる海外のサービス（報道によっては「サイバー攻撃への耐久力を調べる」サービスともされています）を利用し、3月19日から20日にかけてゲームオン社が運営する国内のオンラインゲームサーバへDDoS攻撃を行わせることにより、約9時間にわたりゲーム配信を妨害した疑いが持たれています。
- DDoS攻撃の内容は、NTP（PCの時計を調整するサービス）サーバの脆弱性を悪用し、多数のNTPサーバから第三者へパケットを送信させるというものであったとされています。

AUS便りからの所感等

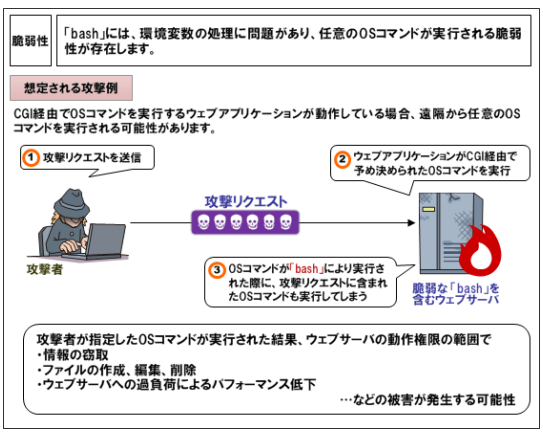
- NTPは、DNS等と同じUDPプロトコルが用いられるために、発信元IPアドレスを偽装する攻撃への悪用が指摘されており、サーバプログラム側で対策済みではあるものの、未対策のサーバ（ルータ等含む）が悪用されたと考えられます。
- このようなDDoS攻撃へ悪用されないよう、サーバソフトウェアへのパッチの適用等の対策、あるいはサーバの設定およびファイアウォール・UTMの設置による外部からのアクセス遮断等が重要となるでしょう。

●Bashにセキュリティホール、Webサーバ等で任意のコード実行の可能性

http://internet.watch.impress.co.jp/docs/news/20140926_668706.html
https://www.jpcert.or.jp/at/2014/at140037.html
https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html

このニュースをザックリ言うと・・・

- Linux（およびMac OS X等UNIX系OS）でコマンドラインおよびスクリプトで使用されるシェルプログラム「Bash」に、外部からの任意のコマンド実行につながり得る脆弱性「ShellShock」が確認されました。
- 脆弱性はBash実行時の環境変数の処理に起因するものであり、特にWebアプリケーションでBashを使用している場合、リクエストURL・ヘッダ等から不正な文字列を送り込むことにより、攻撃を受ける可能性があります。
- Bashを採用している各種Linuxディストリビューションより、Bashの修正バージョンがリリースされています。



AUS便りからの所感等

- Linuxを使用しているマシンには必ずと言っていいほどBashが入っており、PCサーバのみならずLinux OSを用いたアプライアンス等でも、今回の脆弱性の影響を受ける可能性があります。
- WebアプリケーションではBashスクリプトで作成したCGIはもちろんですが、他のスクリプト言語等で開発しているケースにおいても、メール送信時等サーバ上の外部プログラムを実行する際にBashが実行された場合に影響を受けます。
- 根本的な対策としてBashのアップデートは必要不可欠ですが、それまでの回避策としては、IPSないしUTMによる攻撃パターンの遮断も有効となる場合があるでしょう。