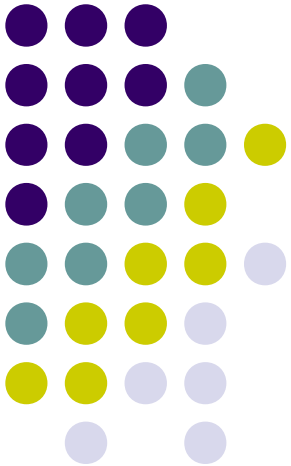
サーバー構築とハッキング対策

オビタスター株式会社
前田　学



オビタスター株式会社とは？

業務内容：ホームページ制作・作成、Web制作・作成。デザイン代行。SEO、SEM代行。ドメイン取得代行。レンタルサーバー。アクセス解析。サポート・保守メンテナンス。オープンソースセミナー・講習会・勉強会。ネットワーク構築。PCサポート。NTTフレンドリーショップ テレポケット（販売代理店）。NTTコミュニケーションズ　バリューパートナー（販売代理店）。PCPOS（ポスレジ販売）。各種ハード・ソフトウェア販売。SSL取得代行。カード、コンビニ決済代行などなど。

設立：2004年（平成16年）10月
本社所在地：大阪市天王寺区上本町6-4-13
代表：代表取締役　高畑和子
資本金：1000万

1783年　滋賀県にて初代高畑吉兵衛が海鮮問屋を設立。
1968年11月　まつかわや創業開始
1997年11月　大阪府優良店舗知事賞受賞
2002年4月　インターネット事業発足、オンラインきもの見本市をオープン。
2003年1月　楽天市場よりショップ・オブ・ザ・イヤー新人賞受賞
2004年10月　オビタスター株式会社設立
2005年7月　オンラインきもの見本市！自社サイトオープン。
2005年10月　自社サイトのショッピングモールオープン。
2006年11月　自社でサーバーを構築。

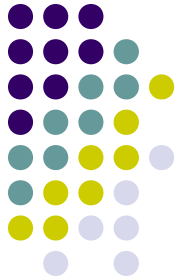
ハッキング事例①-CMSの脆弱性をついた攻撃

ハッキング発見数:	多い（ほとんどがこの原因）
ハッキング方法:	CMSの画像アップロード機能や、ファイルアップロード機能、自動バージョンアップ機能などのWeb画面からファイルをアップロードできる機能の脆弱性をついた攻撃が多い。
ハッキング目的:	ハッキングの目的のほとんどは何かしらのプログラムを埋め込むこと。 埋め込んだ後は、恐らく、このサイトを利用して〇〇ができるという形で情報を販売して、購入や、情報を手に入れた別の人が埋め込まれたそのプログラムを利用して、メールを一斉送信したり、他のサーバーに攻撃を仕掛けたり、自分たちが足がつかないようにしながら、踏み台として利用されることが多い。
ハッキング発見方法:	基本的に攻撃の方法は、ブラウザで脆弱性のあるファイルに「POST」として直接アップロードするような方法がほとんどになるため、アクセスログを見て確認するのが、発見しやすく分かりやすい。自分たちのIPアドレス以外にて、例えば管理画面の画像アップするようなファイルに直接POSTしていたりするような場合は、怪しいと考えることができる。 ファイルを改ざんした際、ファイルに数字と英語の羅列の暗号化されたような、MD5、base64などにて戻すとURLになるような形で埋め込んで、バックリンクや、自社サイトへの誘導などを行うようなケースも多く、そのような場合は、ウィルスソフトにて検索した際に、改ざんされたファイルがウィルスソフトに検知される場合があるので、それを元に探すことができる。
ハッキング対策:	一番は利用しているCMSは常に最新版に保つようにしておくこと。 開発の止まっているモジュールやプラグインなどによっては、脆弱性が放置されているケースがあるので、開発が続いているものを利用すること。 便利ということだけで、ファイルやフォルダに無闇にWebからのアップロード権限、変更権限を与えないこと。 ベーシック認証、IP制限などを利用したりして、管理画面のアドレスには直接アクセスできないようにすること。

ハッキング事例②-FTPを盗んでの攻撃

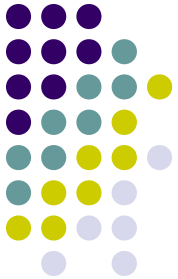
ハッキング発見数:	多い
ハッキング方法:	FTPのIDとパスワードを何かしらの方法で盗み、プログラムのファイルをアップロードする方法。FTPの設定されたパソコンを直接操作している場合もある。プログラムにてランダムに総当たりでログインできるか試して、当たったら利用するということも多いため、パスワードを分かりやすい簡単なIDやパスワードにしていると、簡単に盗まれてしまうことが多い。
ハッキング目的:	ハッキングの目的のほとんどは何かしらのプログラムを埋め込むこと。 埋め込んだ後は、恐らく、このサイトを利用して〇〇ができるという形で情報を販売して、購入や、情報を手に入れた別の人が埋め込まれたそのプログラムを利用して、メールを一斉送信したり、他のサーバーに攻撃を仕掛けたり、自分たちが足がつかないようにしながら、踏み台として利用されることが多い。
ハッキング発見方法:	FTPのログを確認し、自分以外のIPにてログインされていたり、ファイルを変更されていれば間違いなくそれが原因。パソコンを直接操作の場合は、記憶がない時間に自分のIPでファイルが変更されているログがあればそれが原因。 比較的発見しやすいハッキング。
ハッキング対策:	FTPを利用しないという方法が一番ベストではありますが、サーバーが提供している場合は、必要のないFTPアカウントは削除しておくといいかも。 FTPのIDやパスワードを簡単なものにしないこと。定期的に変更することも重要。 .ftpaccessが設定できるサーバーでは、これを上手く利用し、自分以外のIPではアクセスができないようにすることも大切。 パソコンが乗っ取られないように、ファイヤーウォールやウィルスソフトを導入し、常に最新版にしておくことが重要。

ハッキング事例③-サーバーデフォルト導入ソフトの脆弱性をついたハッキング(phpmyadminやftpソフトなど)



ハッキング発見数:	場合による
ハッキング方法:	サーバにデフォルトで導入されているmysqlの管理ソフトphpmyadminや、webにてftpができるftpソフト、webメールソフト、簡単にCMSをインストールできるソフト、簡単にCMSを設定するための各種CMSのファイルなどは、放置しておくとバージョンアップがされず、脆弱性が出てきて、攻撃される元となる場合がある。
ハッキング目的:	ハッキングの目的のほとんどは何かしらのプログラムを埋め込むこと。 埋め込んだ後は、恐らく、このサイトを利用して〇〇ができるという形で情報を販売して、購入や、情報を手に入れた別の人が埋め込まれたそのプログラムを利用して、メールを一斉送信したり、他のサーバーに攻撃を仕掛けたり、自分たちが足がつかないようにしながら、踏み台として利用されることが多い。
ハッキング発見方法:	Apacheのログを見て、自分ではないIPにて利用している様子があると、それが原因。
ハッキング対策:	サーバー側が提供していて自分たちでは触れない場合は、常にアップデートしてくれるサーバーを利用する。 自分の公開領域に置かれている場合は、自分たちで常に最新になるように管理する。 利用しないソフトは、削除する。 ベーシック認証や、IP制限をかけて、自分たちのみが利用できるようにする。

ハッキング事例④-サーバー本体の脆弱性をついた攻撃



ハッキング発見数:	少ないがある
ハッキング方法:	先日有名になったbashを仕込む攻撃や、tmp(temp)フォルダを利用した攻撃など、サーバー本体のソフトの脆弱性をついた攻撃。致命的になることが多い。
ハッキング目的:	ハッキングの目的のほとんどは何かしらのプログラムを埋め込むこと。 埋め込んだ後は、恐らく、このサイトを利用して〇〇ができるという形で情報を販売して、購入や、情報を手に入れた別の人が埋め込まれたそのプログラムを利用して、メールを一斉送信したり、他のサーバーに攻撃を仕掛けたり、自分たちが足がつかないようにしながら、踏み台として利用されることが多い。
ハッキング発見方法:	見つけにくい。サーバー管理の権限がないと見つけられないこともほとんど。
ハッキング対策:	常にサーバー自体を最新版にバージョンアップしてもらうことが重要。 管理権限がある場合は、自分たちで常に最新にしておくことが重要。 tmp(temp)などを利用できないようなサーバー設計をしている、Webにてサーバー情報などを閲覧できないようにして、脆弱性になりそうなプログラムの利用ができないようにしているサーバーを選択、構築することも重要。 共有サーバーや、仮想化などの場合は、自分たちの領域だけしっかりと最新にしていても、他の影響にて攻撃されてしまうことがあるため、その辺りの対応も確認しておくことが重要。

その他

よくある例として、古いプログラムがあるため、それが動作しなくなるからサーバーのバージョンアップも行わないという事例をよく聞くが、どちらも大きな脆弱性になるため、どこでどう攻撃されるか分からないので、必ずバージョンアップしていくことが重要。

サーバーを常にバージョンアップしていくというのは大変な作業。
どういった脆弱性が現在出ていて、どのような攻撃が流行っているのかも調べていく必要がある。

大きなサイトに関わらず、小さなサイトでも、今の時代は、あくまでもそのサイトや、サーバーは踏み台になるだけで利用されるもののため、サイトの規模の大小、有名・無名に関わらず狙われ、脆弱性があればそこに付け込んで攻撃される。
サイトは作って終わりではなく、作ったところがようやくスタート地点のため、そこからきちんとメンテナンスを行うことがサイトを公開している人の義務で、必ずやらないといけないことになる。自分のサイトやサーバーが踏み台となり、他の多くの人に迷惑をかけないようにしていくことが重要。

ご清聴ありがとうございました。