



サーバ公開勘所

-自分はどうしてます編-

今回のお題は？

- 誰もが気にするセキュリティー周り
- 特にOSやミドルウェアの話を共有したい！

こんなことを考えてます

- 2W1Hを明確に
- 最新版を追いかける
- 登場人物と役割を決める
- ソフトを知ってさらに固める

2W1Hを明確に

誰が何処からどう使うか

- サーバの最小構成が決まる
- 「やってはいけない事」がハッキリする



我が家の要望は . . .

- 誰

- 自分と他友人2人くらい

- 何処

- 日本国内のどこからでも

- どう使う

- 作ったサイトの実験場が欲しい！
- ファイルの共有場所あったら便利だね！
- 専用wikiとかどうですか！
- Minecraftしたい！

そんな我が家のサーバ構成



Minecrafut



PHP - FPM

NGINX



FreeBSD®

サーバの構成が決まったらインストールしていく

最新版を追いかける

最初はOSについて

- 特別な理由がない限り、
できるだけ最新のものがよいです。
- パッチもどんどん出るので
インストール直後は最新化する。

我が家のOSはバージョン何？

BSDは `uname -a` で確認。

```
[gh123or456@kuma_da_kuma ~]$ uname -a
FreeBSD kuma_da_kuma 9.3-RELEASE-p30
usr/obj/usr/src/sys/GENERIC amd64
```

サポートが終了したリリース

これまでのリリースのリリース日、分類、保守終了日 (End-Of-Life (EOL)) の完全な情報は、[FreeBSD セキュリティ情報](#) の [サポートが終了したリリース](#) にまとめられています。

- **11.0** (2016 年 10 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [Readme](#): [Errata](#) (正誤表): [チェックサム](#)
- **10.2** (2015 年 8 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [Readme](#): [Errata](#) (正誤表)
- **10.1** (2014 年 11 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [Readme](#): [Errata](#) (正誤表)
- **10.0** (2014 年 1 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [Readme](#): [Errata](#) (正誤表)
- **9.3** (2014 年 7 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [README](#): [Errata](#) (正誤表)
- **9.2** (2013 年 9 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [README](#): [Errata](#) (正誤表)
- **9.1** (2012 年 12 月) [アナウンス](#): [リリースノート](#): [インストールガイド](#): [ハードウェアノート](#): [README](#): [Errata](#) (正誤表)

んんー？

OS最新化とパッチ充て

基本的に公式サイトに載っている通りにやる

- OSのメジャーアップデート

```
freebsd-update -r 11.1-RELEASE upgrade
```

- セキュリティパッチの適用

```
freebsd-update install
```

```
[gh123or456@kuma_da_kuma ~]$ freebsd-version  
11.1-RELEASE-p7  
[gh123or456@kuma_da_kuma ~]$
```

コマンドごと変わった

ソフトのインストール

パッケージ管理ソフトに頼る

- 管理ツールのDB更新

```
pkg update -f
```

- ソフトをインストールする

```
pkg install nginx
```

ここで構成管理ツール(Ansibleとか)を使うのもあり

古いソフトの更新

- 管理ツールから最新版があるか確認できる

```
pkg version -l '<'
```

- まとめて更新

```
pkg upgrade
```

手動でソースからインストールしていたりすると
管理ツールの監視から外れるので
難易度が跳ね上がる。上級者向け。

登場人物と役割を決める

各ユーザの使い方を明確にすること

- 管理者、作業者、システムユーザ、など
各ユーザのできることは明確にする。

`cat /etc/passwd` でユーザの一覧確認

- `sdudo`を使ってコマンド単位で委任するのが定石
-> ありがちなのは、すべてのコマンドを`sudo`できる影の管理者

`visudo` で管理

登場人物と役割を決める

不要なユーザはnologinにしてしまいか削除する。

- ありがちなのは、
「guest」「test」「admin」「tomcat」とか？

`rmuser -p admin` で対話式にadminの削除

- 参考
[不要なデフォルト・ユーザー・アカウントの除去
\(IBMの記事\)](#)

ソフトを知ってさらに固める

メジャーなソフトのメジャーな対応

ソフトによってはセキュリティを高められる機能があるので活用していく。

- sshd
 - ポート変更
 - rootログインの拒否
 - 鍵認証
 - パスワードログインの拒否



ソフトを知ってさらに固める

- nginx
 - 応答に余計な情報を載せないようにする
`server_tokens off` などなど
 - ファイルの公開決定
 - SSL対応
 - etc etc etc.....

できることが多すぎるので、外部の評価ツールに頼るのがよいかと思う

ソフトを知ってさらに固める

メジャーな脆弱性対応

話題になるような奴は適宜対応する
自分が当てにするのは以下

- 脆弱性の特設サイト
- IPA先生のアナウンス
- OSの公式サイト(セキュリティパッチ)
- ソフトのサイト
- VPSを借りてるサイトのアナウンス(さくら)
- CVE/JNV

我が家はこんな状況でした

脆弱性	状況
POODLE	SSL3.0は無効にした
ShellShock	bashは更新済み
Heartbleed	OpenSSL更新済み
GHOST	我が家はBSD 危険性低め
Dirty COW	我が家はBSD
KRACKs	VPSなのでついてない
BlueBorne	VPSなのでついてない
MELTDOWN	アップデートして祈る
SPECTRE	アップデートして祈る

ソフトを知ってさらに固める

通信の制限

ファイアウォールによるポート、プロトコル制限

- iptable
- pf

ウェブサーバなら受信拒否

- IP やMacアドレスではじく
- クライアント認証

ソフトを知ってさらに固める

定期的なログ確認

外部とやり取りするソフトはアクセスログを残せることが多いので定期的を確認する。

- sshdなど -> auth.log
- nginx -> access.log
- pf -> pflog



ソフトを知ってさらに固める

access.log

```
67.106.248.198 - - [20/Mar/2018:21:05:09 +0900] "GET /pmd/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:09 +0900] "GET /pma/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:09 +0900] "GET /PMA/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:10 +0900] "GET /PMA2/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:10 +0900] "GET /pmamy/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:11 +0900] "GET /pmamy2/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:11 +0900] "GET /mysql/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:11 +0900] "GET /admin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:12 +0900] "GET /db/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:12 +0900] "GET /dbadmin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:13 +0900] "GET /web/phpMyAdmin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:13 +0900] "GET /admin/pma/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:13 +0900] "GET /admin/PMA/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:14 +0900] "GET /admin/mysql/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:14 +0900] "GET /admin/mysql2/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:15 +0900] "GET /admin/phpmyadmin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:15 +0900] "GET /admin/phpMyAdmin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:16 +0900] "GET /admin/phpmyadmin2/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:16 +0900] "GET /mysqladmin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:16 +0900] "GET /mysql-admin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
67.106.248.198 - - [20/Mar/2018:21:05:17 +0900] "GET /phpadmin/index.php HTTP/1.0" 404 16 "-" "Mozilla/5.0"
```

ソフトを知ってさらに固める

auth.log

```
input_userauth_request: invalid user deploy [preauth]
input_userauth_request: invalid user user [preauth]
input_userauth_request: invalid user user [preauth]
input_userauth_request: invalid user miner [preauth]
input_userauth_request: invalid user test [preauth]
input_userauth_request: invalid user ethos [preauth]
input_userauth_request: invalid user ethos [preauth]
input_userauth_request: invalid user miner [preauth]
input_userauth_request: invalid user ethos [preauth]
input_userauth_request: invalid user ethos [preauth]
input_userauth_request: invalid user ansible [preauth]
input_userauth_request: invalid user rig [preauth]
input_userauth_request: invalid user rig [preauth]
input_userauth_request: invalid user test [preauth]
input_userauth_request: invalid user user [preauth]
input_userauth_request: invalid user support [preauth]
input_userauth_request: invalid user PlcmSpIp [preauth]
input_userauth_request: invalid user ftpuser [preauth]
input_userauth_request: invalid user ubuntu [preauth]
input_userauth_request: invalid user tomcat [preauth]
```

ソフトを知ってさらに固める

auth.log

```
input_userauth_request: invalid user radio [preauth]
input_userauth_request: invalid user radio [preauth]
input_userauth_request: invalid user radio [preauth]
input_userauth_request: invalid user bot1 [preauth]
input_userauth_request: invalid user bot1 [preauth]
input_userauth_request: invalid user bot1 [preauth]
input_userauth_request: invalid user user [preauth]
input_userauth_request: invalid user bot1 [preauth]
input_userauth_request: invalid user deploy [preauth]
input_userauth_request: invalid user deploy [preauth]
input_userauth_request: invalid user deploy [preauth]
input_userauth_request: invalid user deploy [preauth]
input_userauth_request: invalid user deploy [preauth]
input_userauth_request: invalid user minecraft [preauth]
input_userauth_request: invalid user hive [preauth]
input_userauth_request: invalid user minecraft [preauth]
input_userauth_request: invalid user minecraft [preauth]
input_userauth_request: invalid user minecraft [preauth]
input_userauth_request: invalid user minecraft [preauth]
input_userauth_request: invalid user minecraft [preauth]
```

まとめ

- 結局コツコツ当たり前の事をやるしかない
- 気づける仕組みを知っておくことが大切

最後に

Q.今の時代、サーバ持つ意味あるんですかね・・・？

A. ないです。ないけど魅力はあるので、是非。