SAKURA Internet

www.sakura.ad.jp

VPSはじめの一歩

さくらインターネット株式会社　研究所所長　鷲北 賢

2013年1月26日

自己紹介

SAKURA Internet

- 鷲北 賢（わしきた けん）
  - 1998年4月入社
  - バックボーンのお守りからサービス開発まで
    - 初期の専用サーバ、データセンター構築
    - オンラインゲームプロジェクト
    - CTO兼取締役などなど
  - 2009年より、さくらインターネット研究所 所長
    - 仮想化技術の研究（Linux KVM）
    - さくらのVPS開発ヘルプ
  - 2011年さくらのクラウド 開発チームリーダー兼務
  - @ken_washikita

目次

SAKURA Internet

はじめに

SAKURA Internet

- 本セッションは講義ではありません
  - メモを取るほどではありません
- 細かい設定は後でゆっくり調べてください
  - 「VPS セキュリティ」でググった方が早くて確実
- CentOS 6.3をベースにしています
  - 一番ポピュラーなんです…
- 構えずに、気楽に聞いていただければ幸いです

1. VPSについて

VPSとは

SAKURA Internet

- Virtual Private Server
  - 仮想化技術を活用し、ホストサーバ上に専用サーバと同等の機能を実装して提供するサーバサービス
  - ユーザはroot権限もしくは同等の権限を持ち、サーバを管理／運用することができる

- 安価でありながら高い自由度が得られる
  - 必要なソフトウェアをインストールできる
  - 自由に設定変更できる
  - 他のユーザを気にしなくて済む

さくらのVPS

SAKURA Internet

	1G	2G	4G	8G	NEW SSD 1G	NEW SSD 2G
月額料金	980円	1,480円	3,980円	7,980円	1,780円	3,680円
年間一括料金 (1ヶ月分お得)	10,780円	16,280円	43,780円	87,780円	19,580円	40,480円
初期費用	0円	1,980円 キャンペーンにつき 0円 ※	5,980円	9,980円	1,780円	3,680円
メモリ	1GB	2GB	4GB	8GB	1GB	2GB
ディスク容量	100GB	200GB	400GB	800GB	50GB	100GB
CPU	仮想2コア	仮想3コア	仮想4コア	仮想6コア	仮想2コア	仮想3コア
ネームサーバ	5ゾーン		10ゾーン		5ゾーン	
リージョン	石狩 / 大阪		大阪		石狩	

2013年1月25日現在

気になるセキュリティ

SAKURA Internet

- 管理／運用の責任
  - クラックされたら困る
  - 何か問題が起こるのが怖い

- どうやったら安全に使えるの？

ご説明いたします。

2. ログインに関する設定

rootログインとパスワード

SAKURA Internet

- VPSを始めたら最初にやるべきこと
  - パスワードを変える
  - システムはユーザにパスワードを送らなければならない → 平文でパスワードを持っている
    → **なんかイヤ**
  - とにかく最初に変更する

- ちなみに
  - さくらのVPSは初期状態では「停止」しています
  - コンパネから起動するまでは安全です

参考：ログイン直後のコンパネ

SAKURA Internet

さくらインターネット
VPSコントロールパネル

SAKURA Internet

SAKURA Internet VPS Control Panel　　会員メニュー | パスワード変更 | 操作履歴 | ログアウト

- VPSホーム
- リモートコンソール
- OS再インストール
- ネームサーバ登録
- お知らせ
- マニュアル
- お問い合わせ

VPS ホーム

VPSホームは、仮想サーバの操作、現在の稼動状態、リソース情報といった情報を確認することができます。

仮想サーバ情報	
IPアドレス	[redacted]
ホスト名 変更	[redacted].sakura.ne.jp (標準)
メモリ	1GB
ディスク	100GB
ステータス 更新	停止
仮想サーバ操作	起動 停止 再起動

リソース情報
CPU

パスワードの変え方

1. 初期パスワードでrootログイン
2. passwdコマンドで変更
3. ログアウトして、再ログインできるか試す

- 万が一に備えてコンソールで変更し、sshでログインを試すことをお勧めします
- 最悪の場合、さくらのVPSでは「OS再インストール」機能があります

参考：パスワードの変更

SAKURA Internet

リモートコンソール

リモートコンソール画面より、仮想サーバのシリアルポートを介した操作を行うことができます。

VNCコンソールを開く

```
Starting acpi daemon: [  OK  ]
Starting sshd: [  OK  ]
ntpdate: Synchronizing with time server: [  OK  ]
Syncing hardware clock to system time [  OK  ]
Starting ntpd: [  OK  ]
Starting postfix: [  OK  ]
Starting crond: [  OK  ]
Starting atd: [  OK  ]

CentOS release 6.3 (Final)
Kernel 2.6.32-279.19.1.el6.x86_64 on an x86_64

[redacted].sakura.ne.jp login: root
Password:
Last login: Mon Jan 21 17:59:43 on ttyS0

SAKURA Internet [Virtual Private Server SERVICE]

[root@[redacted] ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@[redacted] ~]#
```

注意事項

⚠ リモートコンソール機能は、仮想サーバのシリアルポ
っており、仮想サーバ上の設定ファイルの一部内容を
を利用できなくなりますので、十分ご注意ください。
ださい。

[redacted]:22 - VT

File Edit Setup Control Window Help

```
Last login: Mon Jan 21 18:00:38 2013 from [redacted]

SAKURA Internet [Virtual Private Server SERVICE]

[root@[redacted] ~]#
```

sshのセキュリティを見直す

SAKURA Internet

- sshはよく攻撃される
  - sshは暗号化されていて安全な通信手段だが、しょせんログイン名とパスワードで保護されているだけ

1. sshでrootログインできないようにする
2. sshのポート番号を変更する
3. パスワードログインをやめ、公開鍵認証にする

sshでrootログインできないようにする

SAKURA Internet

- 一般ユーザでログインしてからsudoを使う
  - wheelグループに所属するユーザでsudoする
  - ユーザならばrootよりも狙われにくい

- 1台のサーバをみんなで共有したいときも有効
  - root権限を与えたい人だけwheelに所属させる
  - ログを見れば誰が何をしたかも分かる

設定方法

1. 一般ユーザを作成
   $　useradd *username* –G wheel
2. パスワードを設定
   $　passwd *username*
3. sudoの設定を変更する
   $　visudo
   　%wheel　ALL=(ALL)　ALL　　←コメントアウトを消す
4. sshでrootログインを禁止する
   $　vi /etc/ssh/sshd_config
   　PermitRootLogin no　　←yesをnoに変える
5. sshdを再起動
   $　service sshd restart

sshのポート番号を変更する

SAKURA Internet

- 22番ポートは常に狙われている
- 変更するだけで大半のアタックはなくなる

1. ポート番号を変更する

   $ sudo vi /etc/ssh/sshd_config
   Port *10022*

2. sshdを再起動

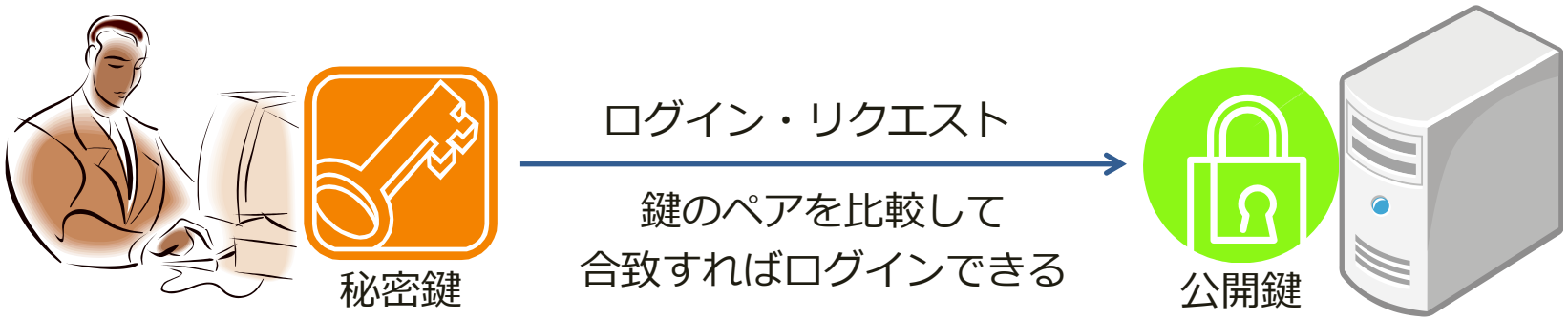
   $ sudo service sshd restart

10022番ポートも使い古されています

公開鍵認証を使う

SAKURA Internet

- パスワードをやめて、秘密鍵・公開鍵を使う
- VPSに公開鍵を設置
  - 秘密鍵を使ってアクセスするとログインできる
  - 秘密鍵を盗まれない限り安全
  - 公開鍵を解析しても秘密鍵は再現できない



公開鍵・秘密鍵の作り方

SAKURA Internet

- Linuxでssh-keygenと入力
- いくつか質問されるが全部空リターンでOK
- ホームに「.ssh」ディレクトリができる
  - id_rsa　　秘密鍵。厳重に保管
  - id_rsa.pub 公開鍵。サーバに設置
- ファイルのパーミッションにも注意

公開鍵をVPSに置く

SAKURA Internet

1. サーバにログイン
2. sshdの設定変更

   $ sudo vi /etc/ssh/sshd_config
   PubkeyAuthentication yes ← 公開鍵認証有効
   PasswordAuthentication no ← パスワード認証無効
   $ sudo service sshd restart
3. ホームに.sshディレクトリを作成、パーミッション設定

   $ cd ; mkdir .ssh
   $ chmod 700 .ssh
4. .sshにauthorized_keysファイルを作成
   公開鍵を保存

   $ cd .ssh
   $ cat >authorized_keys
   $ chmod 600 authorized_keys

秘密鍵を使ってログインする

SAKURA Internet

- 他のLinuxサーバからログインする
  - 秘密鍵がホームの.sshにid_rsaという名前で保管されていれば、sshコマンドでログインできる
  - scpやほかのssh系コマンドが自由に使える
- TeraTermやPuttyなどのターミナルソフトから
  - 秘密鍵をPCに移し、ソフトから指定してログイン
  - 指定方法はそれぞれのソフトに従って行う
- ファイル転送はWinSCPがお勧め
  - 公開鍵認証でFTPライクなファイル転送が可能
  - Windows/Macintoshクライアントがある

公開鍵認証の注意点

SAKURA Internet

- 秘密鍵の管理に注意
  - 秘密鍵を持ち歩かねばならず、リスクになり得る
  - 秘密鍵を入れたPCの管理は結局パスワードで…
  - 秘密鍵をなくしたら直ちに公開鍵を削除・更新する

- 秘密鍵がないときにログインする手段がない
  - パスワード認証を無効化するのは一長一短
  - よく考えて設定するべき

3. iptablesによるパケットフィルタ

iptablesとは

SAKURA Internet

- サーバのポートで、パケットを通したり拒否するフィルタを設定する
- 必要なものだけを通し、不要なものを拒否することで、アタックを避け、セキュリティを上げることができる
- サーバで設定できるファイア・ウォール

- 「設定さえすれば安全」ではない
- 無用なアタックを避け、リスクを低減するもの

iptablesの設定方法

SAKURA Internet

1. 定義ファイルを書く
   - /etc/sysconfig/iptablesに記述する
   - 記述例は次ページに紹介します
2. iptablesサービスを再起動

   $ sudo /etc/rc.d/init.d/iptables restart

- ルールを間違えると悲惨
  - コンソールで設定、sshでテストをお勧めします
  - 最悪の場合、さくらのVPSでは「OS再イン(r

/etc/sysconfig/iptables

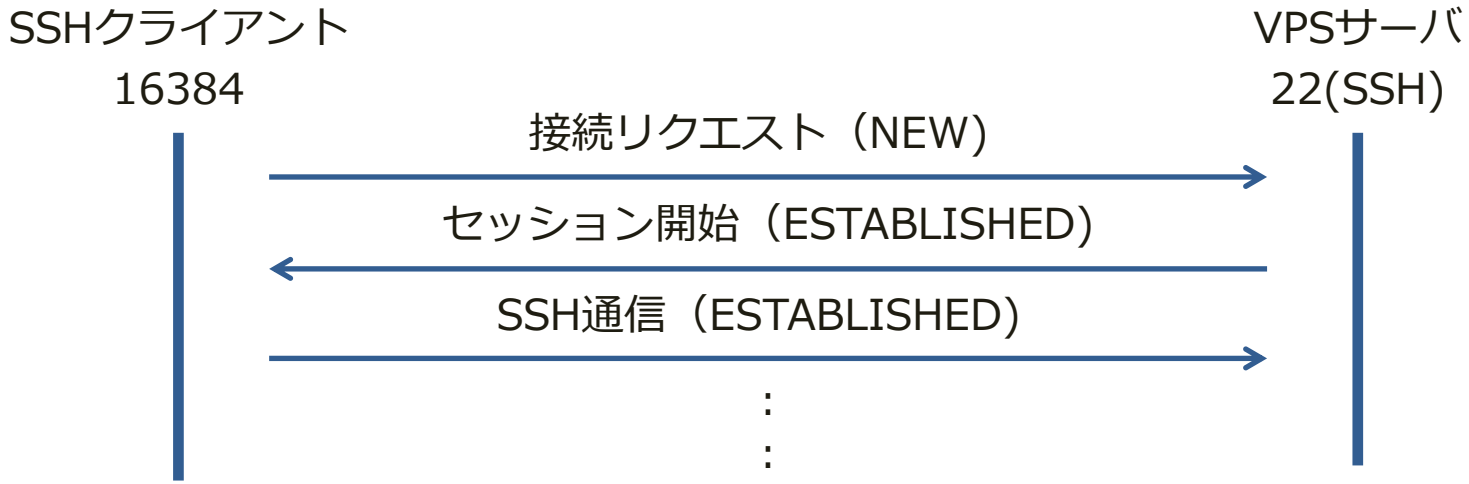
SAKURA Internet

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
#
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
#
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
#
COMMIT
```

参考：stateについて

SAKURA Internet

-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT



1. 22番ポートへの新規パケット（NEW）はACCEPT
2. OUTPUTはACCEPT
3. ESTABLISHEDなINPUTはACCEPT

→ SSHが可能

4. ソフトウェアのセキュリティ

VPSにおけるソフトウェア

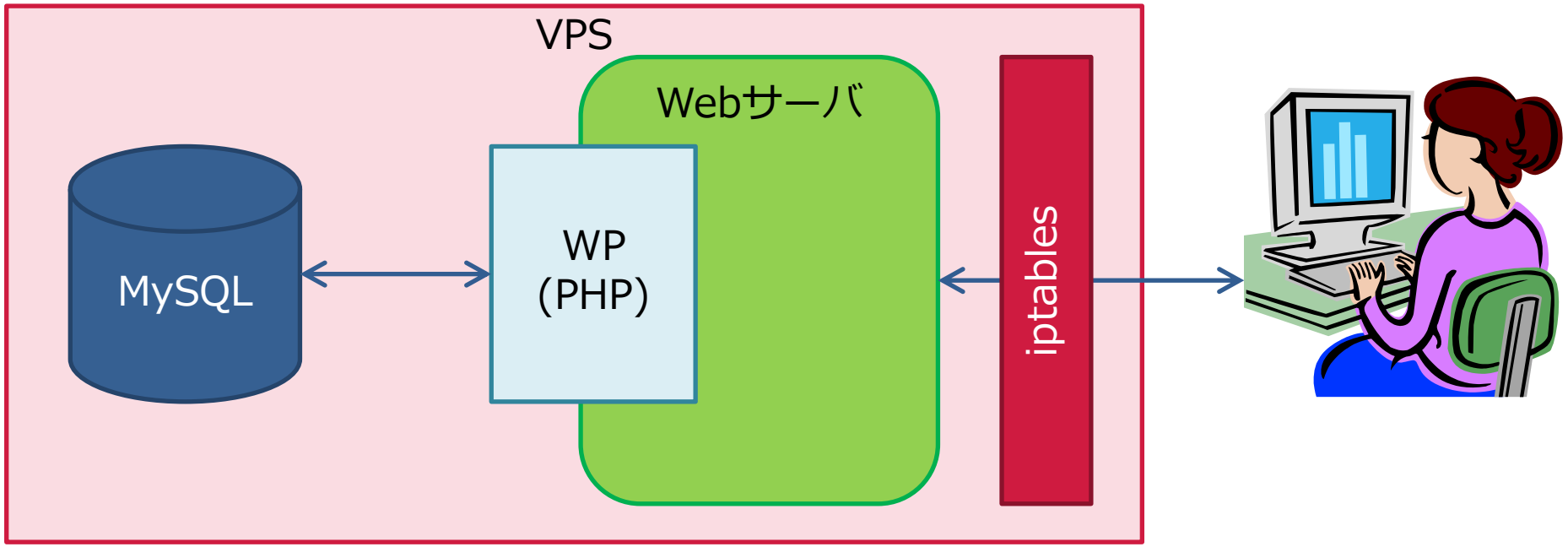
SAKURA Internet

- ゲストOS（Linuxカーネル）
  - 比較的安定していて深刻な問題は少ない
  - セキュリティ問題が発生しても速やかにパッチされる
- サーバ（Web、メール、DNS…）
  - サーバ本体は安定しているが運用は色々難しい
  - アプリケーションやプラグインには要注意
  - 管理用パスワードや認証システムは出来の悪いものもある → アプリを踏み台にシステムを破られるケースも
- データベース（MySQL、PostgreSQL…）
  - アクセス権限をきちんと設定し、iptablesでしっかり保護
  - 複数サーバ構成でない限りアクセスポートは開けない

ソフトウェアの例：WordPress

SAKURA Internet

- WordPressを構成するソフトウェア
  - Webサーバ（Apache）
  - PHP
  - MySQL



- **最新版を使うことが重要**

- yum updateなど、簡単にチェック・アップデートが行えるので積極的に実施する
  - 面倒な人には自動ツールyum-cronがオススメ

- アプリケーションはこまめにチェック
  - アップデートはセキュリティ・パッチがほとんどなので面倒がらずに必ずインストールする

5. リモートコンソールのセキュリティ

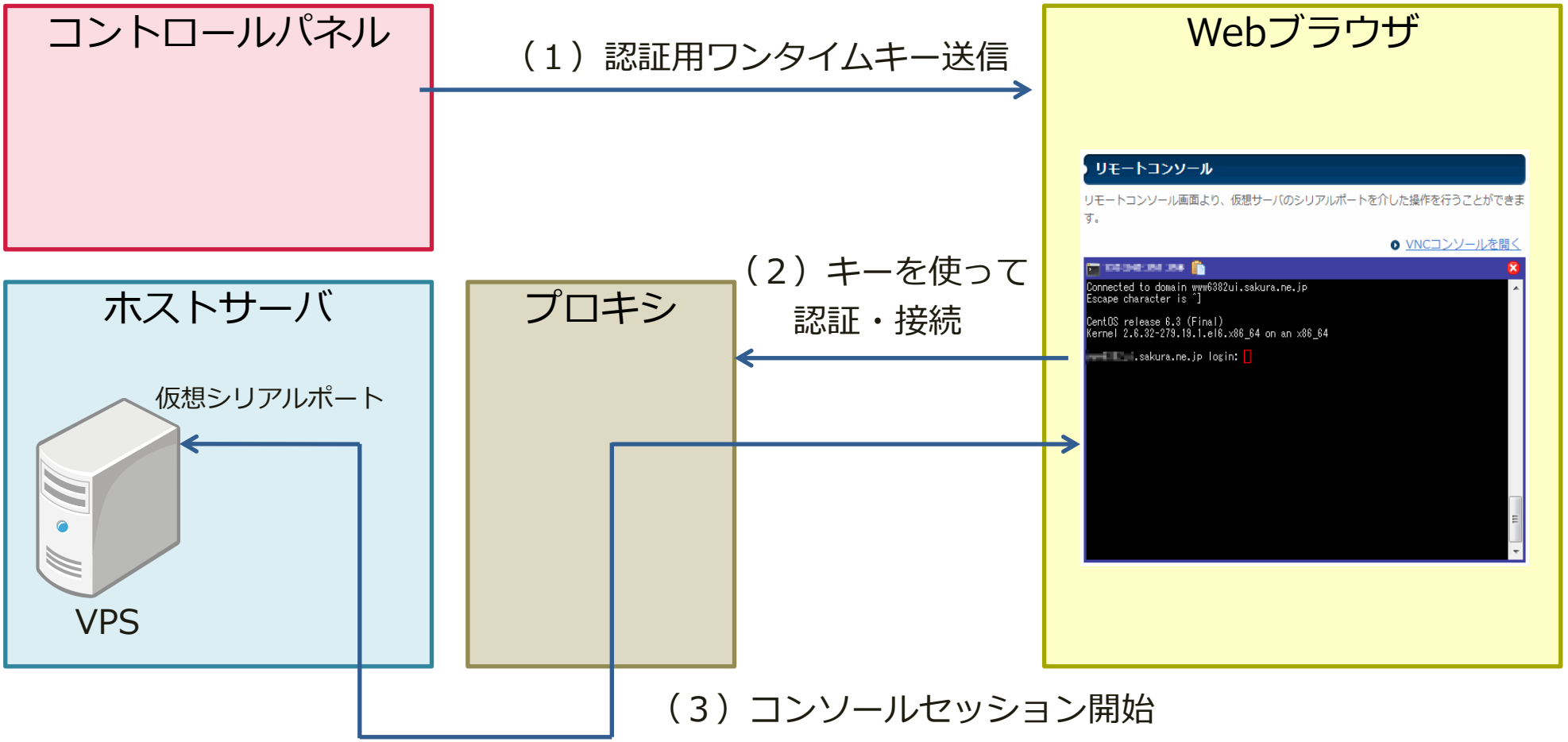
VPSのリモートコンソールは大丈夫か？

SAKURA Internet

- リモートコンソール機能
  - VPSのシリアルポートを介してディスプレイ／キーボードを直接Webコンソール上に表示し、操作を可能にしたもの
  - VNCコンソールを使えばCTL+ALT＋DELも送れる
  - リセットしたあとシングルモードでブート可能
  - うっかりするとシステム乗っ取りも簡単

セキュリティは大丈夫？

リモートコンソールの仕組み



リモートコンソールのセキュリティ

SAKURA Internet

- 認証キーのやり取りはHTTPS
- ワンタイムキーで有効期限が短い
- ブラウザ／プロキシ間はSSHトンネル
- VNCプロキシ／ホストサーバ間はネットワークセキュリティにより安全を確保
  - ユーザは直接ホストにアクセスしていない
  - iptablesとは無関係（全部DROPでも動作する）
  - シリアルコンソールの設定を変えると動かなくなるので注意が必要

おわりに

その他のトピック

SAKURA Internet

- ログのチェック
  - ログには重要な情報が記録される
  - 記録期間を延ばすなど、初期設定から変えておくとよい項目もある
- リソース情報の確認
  - CPUやトラフィックの推移で性能やセキュリティ問題の発見につながることもある
- 監視ツール
  - ツールを使ってラクをしましょう

おまけ

SAKURA Internet

- ゲヒルン株式会社／Security.GS in 北海道
  - ウェブセキュリティ勉強会（参加無料）
  - 2013/2/17 15:30～17:30
  - 札幌市中央区 株式会社インフィニットループ 会議室
- 初級～中級者を対象とした講座
  - Webサービスの開発を始めた方
  - サービスのセキュリティを強化したいエンジニア
  - 最近VPSに触り始めた方など
- 講座内容
  - クラッカーの心理
  - XSSの話
  - JavaScriptの話

  ※ 講座内容は変更する場合がございます

http://atnd.org/events/36277