

事例から学ぶ！  
ウェブ改ざんの実態とその対策

クラウド事業者からみた実態とジレンマ

製品ベンダーの立場でみた最近の改ざんの実態



Profit from the cloud™

パラレルズ株式会社

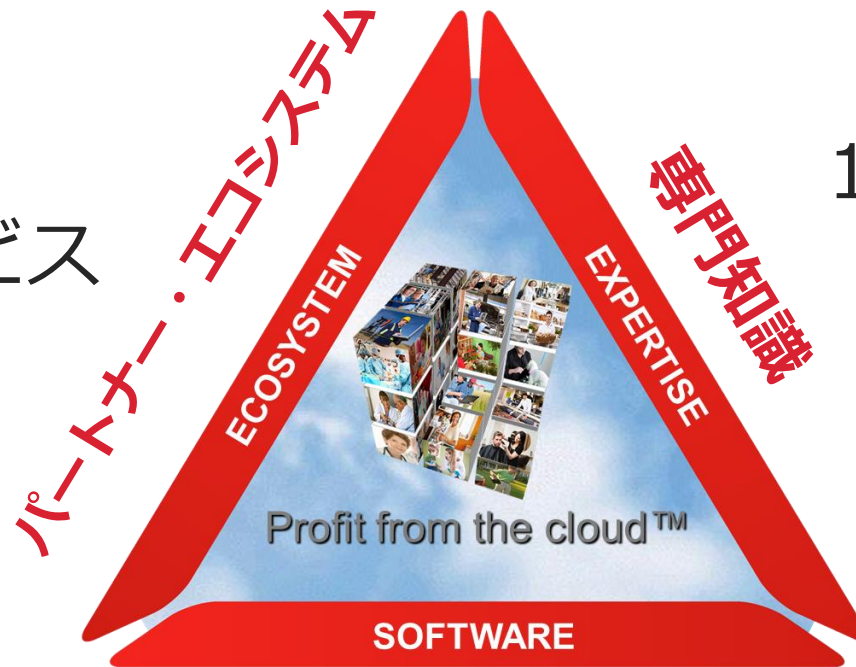
サービスプロバイダビジネス事業部

セールスエンジニア 鈴木隆之

# Parallels = クラウドのパートナー

SMBクラウド市場において成長および収益をあげるように支援

400+ ISVs、  
9,000 サービス  
プロバイダ



13年のクラウド  
ビジネス経験

ソフトウェア

先進のクラウドサービス提供  
プラットフォーム

# Parallels Plesk Panel とは？

- サーバ、ウェブサイト、アプリケーションを管理するウェブデザイナー、ウェブマスター、ウェブオーナーのためのプロフェッショナルなコントロールパネル
  - ウェブホスティングを便利にそして容易にする非常に優れたツール
- 多数のホスティング/クラウドサービス事業者様で採用
  - 専用サーバ
  - VPS/クラウド
  - シェアードホスティング
  - SaaS
- ソフトウェアの提供方法・サービス内容・提供範囲
  - 事業者によってさまざま
    - 例：マネージド、セルフ



# コントロールパネルの表と裏



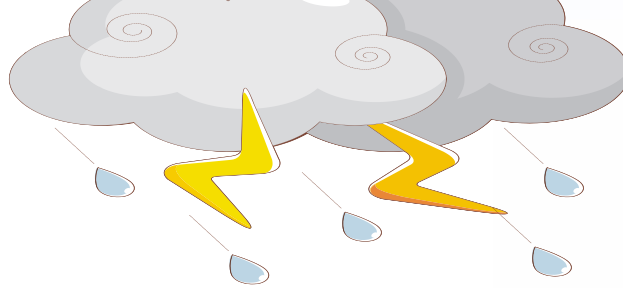
- ボタンを押すだけで様々な飲み物が出てくる！
- 飲み物の専門知識不要！
- 簡単・便利！

- 中身は複雑
  - メンテナンスは必須
    - 怠ると様々な問題が発生！
- 認識が異なると空白が発生  
= リスク発生**

どこまで自分でやるか？

空白

どこまで任せているか？



> **こんな使い方は危険！  
不適切な利用方法**

# 1. パネルのアップデートを適用せずに利用

## Parallels Plesk Panel 10.1.1 MU #15 [09-June-2011]

[-] phpMyAdmin XSS vulnerability <http://www.securityfocus.com/bid/47945/info>.

[-] SQL injection at subscription's owner changing in Plesk Panel.

[-] Horde XSS injection.

[-] Multiple XSS vulnerabilities in Plesk Panel.

[-] sw-cp-server can be crashed by client certificate.

## Parallels Plesk Panel 10.0.1 MU #7 [09-June-2011]

[-] phpMyAdmin XSS vulnerability <http://www.securityfocus.com/bid/47945/info>.

[-] SQL injection at subscription's owner changing in Plesk Panel.

[-] Horde XSS injection.

[-] Multiple XSS vulnerabilities in Plesk Panel.

[-] sw-cp-server can be crashed by client certificate.

## Parallels Plesk Panel 10.2.0 MU #7 [03-June-2011]

[-] phpMyAdmin XSS vulnerability <http://www.securityfocus.com/bid/47945/info>.

[-] SQL injection at subscription's owner changing in Plesk Panel.

[-] Panel removes current key on cleanKeyHistory command from Key Administrator server.

## Parallels Plesk Panel 10.2.0 MU #12 [28-Nov-2011]

[-] Security fix: ProFTPD Response Pool Use-After-Free Vulnerability.

## Parallels Plesk Panel 10.3.1 MU #16 [24-Nov-2011]

[-] Security fix: ProFTPD Response Pool Use-After-Free Vulnerability.

## Parallels Plesk Panel 10.4.4 MU #4 [23-Nov-2011]

[-] Spam filter sensitivity error.

[-] Security fix: ProFTPD Response Pool Use-After-Free Vulnerability.

[-] Can not issue several SSL certificates via OpenSRS module.

[-] SQL injection vulnerability that allows anonymous attacker remotely compromise Plesk server has been fixed.

## Parallels Plesk Panel 10.1.1 MU #22 [14-Feb-2012]

[-] SQL injection vulnerability that allows anonymous attacker remotely compromise Plesk server has been fixed.

## Parallels Plesk Panel 10.0.1 MU #13 [14-Feb-2012]

[-] SQL injection vulnerability that allows anonymous attacker remotely compromise Plesk server has been fixed.

## Parallels Plesk Panel 10.4.4 MU #16 [10-Feb-2012]

[-] /usr/local/psa/bin/repair -r throwing error "Argument 1 passed to Service\_Dns\_Zone::\_\_construct() must be an instance of DNSZone, instance of Db\_Table\_Row given".

## [フィックス] 旧バージョンの Plesk - Plesk Panel のリモート脆弱性、

### 対象製品:

- Parallels Plesk Panel 10.3 for Linux/Unix
- Parallels Plesk Panel 10.2 for Linux/Unix
- Parallels Plesk Panel 10.1 for Linux/Unix
- Parallels Plesk Panel 10.0.x for Linux/Unix
- Parallels Plesk Panel 9.x for Linux/Unix

## 脆弱性に関する問題 VU#310500、CVE-2013-0132、CVE-2013-013

### 対象製品:

- Parallels Plesk Panel 11.x for Linux
- Parallels Plesk Panel 10.x for Linux
- Parallels Plesk Panel 9.x for Linux/Unix
- Parallels Plesk Panel 8.x for Linux/Unix
- Parallels Plesk Panel 7.x for Linux/Unix

### 背景

Parallels Plesk Panel

CVE-2013-0132

明されています。

脆弱性が確認

んが、Parallels

### 対象製品:

- Parallels Plesk Panel 9.2 for Linux/Unix
- Parallels Plesk Panel 9.0 for Linux/Unix

### 情報

2012年5月3日、PHP-CGIにコードのリモート実行の脆弱性があることが公開されました (CVE-2012-1823)。

これは重大な脆弱性

PHP-FastCGIはこ

Parallels Plesk Pa

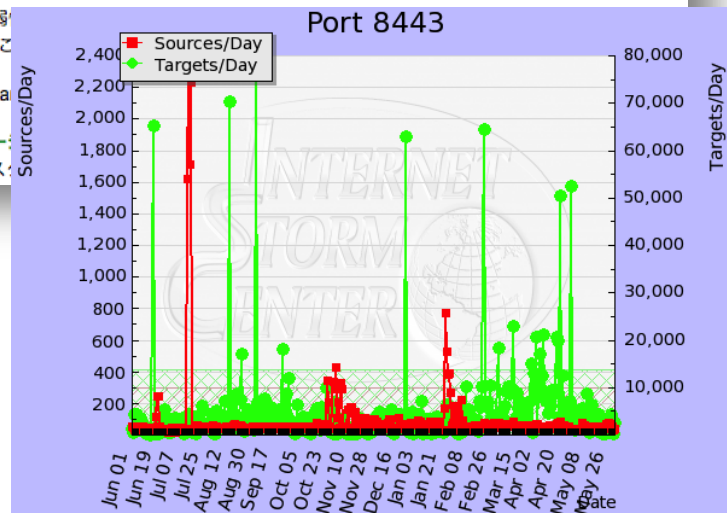
PP for Linux パー

cgi\_wrapper ス

Port 8443

Sources/Day

Targets/Day





# 2. (サポートなしの) 旧バージョンを使い続ける

The screenshot shows the Parallels website's support page for Parallels Plesk Panel. The page title is "Parallels Plesk Panel ライフサイクルポリシー". It contains several sections: "Parallels Plesk Panel バージョン", "現在サポートされている Parallels Plesk Panel バージョン", "ライフサイクルポリシー", and a table of lifecycle dates.

**Parallels Plesk Panel バージョン**

現在サポートされている Parallels Plesk Panel バージョン :

- Parallels Plesk Panel 11.x
- Parallels Plesk Panel 10.4.4

**ライフサイクルポリシー :**

- メジャーバージョンとは、バージョン番号の先頭の数字が更新されたバージョンです。たとえば、Plesk 9 と Plesk 10 ではメジャーバージョンが異なりますが、Plesk 10.2 と 10.3 では同じです。
- Parallels は、Parallels Plesk Panel の最新の (およびその直前の) メジャーバージョンを対象にソフトウェアパッチを提供し、技術サポートリクエストを受け付けます。
- それぞれのメジャーバージョンは、リリース後少なくとも 4 年間は完全にサポートされます。
  - 延長サポート : この 4 年間に経過した後は製品を新たに購入することはできなくなり、その後 6 ヶ月は重大な問題に限ってパッチが提供されます。
  - サポート終了 (EOL) : 延長サポート期間が終了すると、パッチの開発は終了し、技術サポートリクエストの受付も終了します。
- 安定したオペレーションを維持するには、各メジャーバージョンに対して提供されている最新のアップデート/パッチを適用する必要があります。たとえば、Plesk 9 シリーズの場合は最新の 9.5.x バージョン、Plesk 10 シリーズの場合は最新の 10.4.x バージョン、Plesk 11 シリーズの場合は最新の 11.x バージョンです。
- また、特定のインスタンスに対するサポートは、現在サポートされている OS を使用していることが条件となります。このポリシーについては後で詳しく説明します。
- サポート対象外のインスタンスであっても、サポートされるバージョンまたは環境への更新に関連するテクニカルサポートのリクエストについては引き続き受け付けます。

以下の表は、Parallels Plesk Panel 各バージョンの延長サポート期間の開始日と、パッチサポートの提供終了日を示します。これらの日付が同じに迫っているお客様は、最新の Parallels Plesk Panel バージョンにアップグレードすることをお勧めします。

各バージョンのライフサイクル関連日付 :

製品	リリース日	サポート終了 (EOL) 延長サポート期間の開始日	延長サポート期間の終了日
Parallels Plesk Panel 11	2012 年 6 月 13 日	2016 年 6 月 13 日	2016 年 12 月 13 日
Parallels Plesk Panel 10	2010 年 11 月 3 日	2014 年 11 月 3 日	2015 年 5 月 3 日
Parallels Plesk Panel 9	2008 年 12 月 9 日	2012 年 12 月 9 日	2013 年 6 月 9 日
Parallels Plesk Panel 8	2006 年 9 月 20 日	2012 年 3 月 1 日	2012 年 9 月 1 日
Parallels Small Business Panel*	2009 年 11 月 3 日	2011 年 8 月 1 日	2012 年 7 月 1 日
Parallels Plesk Panel 7 およびそれ以前	2004 年 2 月 10 日	n/a	2012 年 1 月 1 日

## Parallels Plesk Panel ライフサイクルポリシー

<http://www.parallels.com/jp/support/policy/plesk-lifecycle/>

## 旧バージョンの Parallels Plesk Panel の利用に関する注意喚起

各位

JPCERT-AT-2013-0018

JPCERT/CC

2013-04-08

<<< JPCERT/CC Alert 2013-04-08 >>>

旧バージョンの Parallels Plesk Panel の利用に関する注意喚起

<https://www.jpCERT.or.jp/at/2013/at130018.html>

### I. 概要

JPCERT/CC では、サーバ上に不正な Apache モジュールが設置されたことにより、Web サイト閲覧時に意図しない JavaScript が挿入される Web 改ざんに関する報告を多数受けています。改ざんされたサイトを閲覧した場合、結果としてユーザの PC がマルウェアに感染する可能性があります。

弊センターにて入手した情報によると、これらのサイトでは、サポート期限切れのバージョンを含む旧バージョンの Parallels Plesk Panel が多く使われているとのことです。Parallels Plesk Panel が稼働しているサーバには、付随する様々なソフトウェア(MySQL、BIND、phpMyAdmin 等)がインストールされている可能性があり、ユーザはこれらのソフトウェアを使用している認識が薄いため、脆弱性を内在した古いバージョンで稼働している場合が多くあります。

## JPCERTコーディネーションセンターウェブサイト

<http://www.jpCERT.or.jp/at/2013/at130018.html>

サーバ上に不正な Apache モジュールが設置、サイトの改ざん、マルウェア配布

### 3. 適切にパスワード管理をしてない

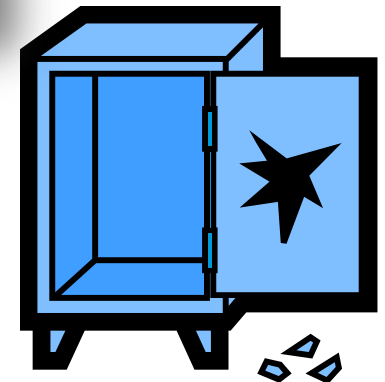
- 簡単な文字列 – 辞書攻撃
- 長期間変更しない
- 同じパスワードを使い回す

管理者パスワードとメールパスワードが同じ！

パスワード  最弱 (?)

このパスワードは、メールボックスへのアクセスと、Panel へのログインに使用されます（アドレスが補助ユーザに関連付けられている場合）。

パスワード確認





## 4. アクセス制限の不在・不備

- “便利だから”という理由だけでユーザへの適切な権限の付与が出来ていない

例

- 社員全員が管理者権限でアクセスできる
  - 複数人で1ユーザ情報、パスワードを使い回し
  - 開発会社に渡したパスワードをそのままにしておく
- 
- 利用しないユーザ情報が削除されないまま
  - IPアドレスなどによるアクセス元の制限が不在



## 5. サーバの基本的な設定を行っていない

### パネルだけアップデートすればOKだと思っている

- OS、アプリケーションも適宜アップデートしていない
- 知らない、不要なアプリケーションを起動したまま
- 公開を必要としないネットワークポートを開けたまま
- ...

### うっかりミスはつきもの

- 設定を変えたら動作確認を..

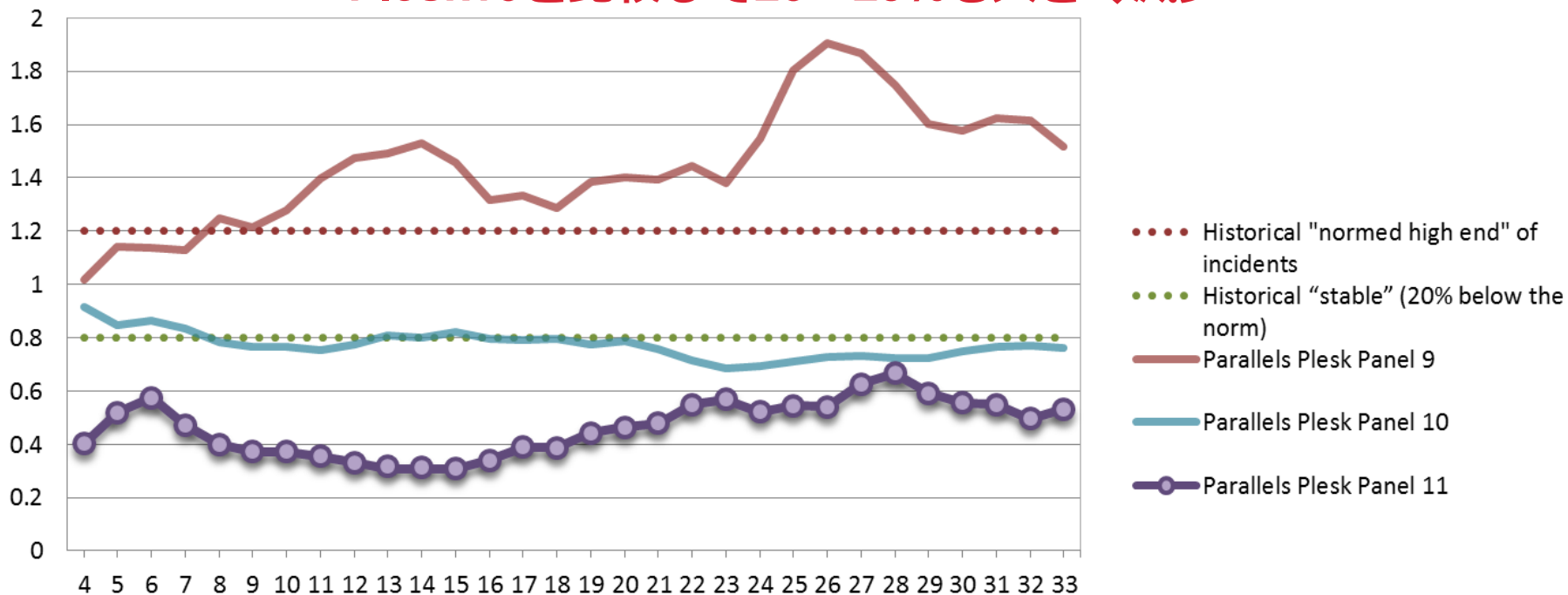
**サービス事業者とあなたの責任範囲を  
理解してますか？**

# > 最新版Parallels Plesk Panel における セキュリティ対策

# よりよい品質と安定性を求めたPlesk 11.5

- Plesk 11.5は、正式リリース前の9か月間に多くのユーザの目に触れるパブリックプレビュープログラムを実施
- Plesk11.5から、公開前だけのテストだけでなく、リリース後も継続して品質テスト実施体制を導入

**結果： サポート問い合わせ数が Plesk9と比較で70%、  
Plesk10と比較して20~25%も大きく減少**



# 自動アップデート機能 (V10~)

Parallels® Panel

ログインユーザ: 鈴木隆之 ログアウト ヘルプ

Powered by

ホーム

ホスティングサービス

- 顧客
- リセラー
- ドメイン
- 契約
- サービスプラン

サーバ管理

- ツールと設定**
- ヘルスマニタリング
- 拡張

マイ・プロフィール

- プロフィールとプリファレンス
- パスワードを変更

アイデアを提案

当社の Facebook ページ

Like

© 1999-2013. Parallels IP Holdings GmbH. All rights reserved.

ホーム > ツールと設定 >

## アップデートおよびアップグレードの設定

Panel のアップデートおよびアップグレードポリシーをセットアップできます。「アップデート」に含まれるのは軽微な修正ですが、「アップグレード」には Panel 機能のより複雑な変更が含まれるため、長時間のダウンタイムが必要になる場合があります。自動更新をオンにして、今後のアップグレードの対象とする Panel リリース階層を選択しておくことをお勧めします。リリース階層は各 Panel バージョンに対して定められており、Panel の開発段階を示します。当然ながら、より上位のリリース階層のバージョンでは、初期のバージョンと比べて機能が向上しています。Panel のリリース (General Availability) より前に新機能をお試しになりたい場合は、アーリーアダプタリリースへのアップグレードをご検討ください。一方、すべてのメジャーアップデートが含まれ、多数のサービスプロバイダによって安定的に利用されているソリューションをご利用になりたい場合は、Panel が「レイトアダプタリリース」のステータスになるまでお待ちください (通常はジェネラルリリースの 2、3 ヶ月後となります)。選択した Panel リリース階層へのアップグレードが提供されると、Panel の [ホーム] ページに通知が表示されます。 [Panel のリリース階層についてさらに詳しく。](#)

以下の Panel リリースのアップグレードが提供されたら通知を受け取る:

- アーリーアダプタリリース  
アーリーアダプタリリースには、予定されたすべての機能が含まれ、旧バージョンからこのバージョンに正常にアップグレードすることができます。このバージョンでは、アップデートを重ねて徐々に機能が向上します。このバージョンを選択することにより、新機能をいち早く利用して、最新のアップデートを受け取ることができます。
- (推奨) ジェネラルリリース  
ジェネラルリリースは、すべての品質テストに合格しています。軽微な問題は、アップデートによって速やかに修正されます。Panel を常にジェネラルリリースにアップグレードするようお勧めします。
- レイトアダプタリリース  
レイトアダプタリリースには、現在の Panel バージョンに対して発行されたすべてのメジャーアップデートが含まれており、多数のサービスプロバイダが一定期間にわたって安定して使用しています。

アップデート

- 現在インストールされている Panel バージョンのアップデートを自動インストールする (推奨)
  - サードパーティコンポーネント (MySQL、PHPMyAdmin など) のアップデートを自動インストール
- アップデートについて通知を受け取るが、自動インストールは行わない  
重大なセキュリティアップデートは引き続き自動インストールされます。

# 安易なパスワード入力の拒否 (V10~)

## パスワード強度

ユーザがシステムでパスワードを新たに設定（パスワードを新規作成または変更）する場合、このページで指示されたパスワード強度の要件に従う必要があります。パスワードの強度は、複雑さと長さによって決まります。パスワードの強化をユーザに徹底させることをお勧めします。

パスワードの最低限の強度に関する  非常に弱い  
要件

大文字、小文字、または数字のいずれかのみを使用する 5 文字以上のパスワードです。このセキュリティレベルでは、最も簡単なパスワード推測攻撃を防御できます。

弱い

小文字と、大文字（2 文字）、数字（1 のいずれかを組み合わせた 5 文字以上のパスワードの推測に対する基本的な防御を実現し

平均的

大文字と小文字、特殊文字を組み合わせたパスワードです。パスワード盗難を狙う攻撃を確実

強い

大文字と小文字、数字、特殊文字を組み合わせたパスワードです。ブルートフォース攻撃を強

非常に強い

大文字と小文字、数字、特殊文字を組み合わせたパスワードです。最もセキュリティの高い防  
ぐという短所があります。

## 管理者パネル

ウェブサイトとドメイン   メール   アプリケーション   ファイル   統計   ユーザ   アカウント

### 顧客、ユーザパネル

#### メールアドレスを作成

全般   転送   メールエイリアス   自動応答   スпамフィルタ

このメールアカウントに補助ユーザが関連付けられている場合(コントロールパネルへのアクセスが有効)、このメールアドレスとパスワードを変更すると、補助ユーザのログイン名とパスワードが新しい値に変わります。

メールアドレス \*  @ sasaki-build.com

コントロールパネルへのアクセス(ユーザ名:)

パスワード  強 (?)

このパスワードは、メールボックスへのアクセスと、Panel へのログインに使用されます(アドレスが補助ユーザに関連付けられている場合)。

パスワード確認

メールボックス

デフォルトサイズ(無制限)

別サイズ  KB

最大サイズはデフォルトサイズより大きくできません。

パネルログイン用ユーザアカウント、FTP  
アカウントのパスワードに対しても同様の  
制限あり





# 複数の管理者毎のアカウント作成 (V11.5~)

同時に1つの管理者アカウントを複数の管理者が共有することを避ける

[ホーム](#) > [ツールと設定](#) >



## 追加管理者アカウント

テクニカルサポートエンジニア用に追加の管理者アカウントを作成し、これらのエンジニアに様々なことができます。

 管理者アカウントを追加 |  削除 | その他 ▾

合計 2 件

1 ページあたりのエントリの数

<input type="checkbox"/>	担当者名 ^	ユーザ名
<input type="checkbox"/>	 <a href="#">Ken Yamazaki</a>	yamazaki-admin
<input type="checkbox"/>	 <a href="#">Kozo Kato</a>	kato-admin

合計 2 件

メール

[ホーム](#) > [ツールと設定](#) > [追加管理者アカウント](#) >

## 管理者アカウントを追加

ユーザ名 \*

パスワード \*  強 (?)

パスワードの確認 \*

メール \*

担当者名 \*

コメント

\* 必須フィールド

# Plesk DB内の各種パスワードの暗号化 (V11~)

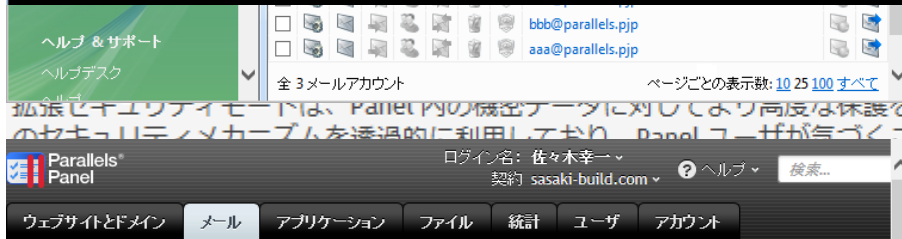


Plesk 9, Plesk 10は生パスワードを格納

```
mysql> select concat_ws('@', mail.mail_name, domains.name), accounts.password from domains, mail, accounts where domains.id=mail.dom_id and accounts.id=mail.account_id order by domains.name ASC, mail.mail_name ASC;
```

concat_ws('@', mail.mail_name, domains.name)	password
aaa@parallels.pjp	mmmnSW@
bbb@parallels.pjp	mmmnSW@
ccc@parallels.pjp	mmmnSW@

3 rows in set (0.00 sec)



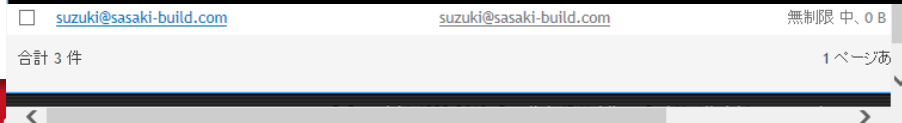
適用します。このモードで、Panel は複数のセキュリティメカニズムを透過的に利用しており、Panel ユーザーが気づくことはありません。Panel のセキュリティを

Plesk 11から暗号化パスワードを格納

```
mysql> select concat_ws('@', mail.mail_name, domains.name), accounts.password from domains, mail, accounts where domains.id=mail.dom_id and accounts.id=mail.account_id order by domains.name ASC, mail.mail_name ASC;
```

concat_ws('@', mail.mail_name, domains.name)	password
kato@sasaki-build.com	\$AES-128-CBC\$6Bbn80BYw/CvP7ryPyaKuQ==\$XxjhYENIWLtdzx9ZyktqAw==
sasaki@sasaki-build.com	\$AES-128-CBC\$dKrotG0mLupHwmzRz6MUiw==\$TCTYzeJ6mgHn/QgbPM+lyg==
suzuki@sasaki-build.com	\$AES-128-CBC\$NFzeqy1e/cJW8WXSkoWrDw==\$+EyhGohAak3EeSiAqSr5qA==

3 rows in set (0.15 sec)




# APSパッケージの自動更新 (V11.5~)

ウェブサイトとドメイン メール アプリケーション ファイル 統計 ユーザ アカウント

## ウェブサイトとドメイン

ウェブサイトの設定と管理を行います。他の契約に切り替えることができません。

 **ウェブホスティングアクセス**  
IP アドレス: 10.37.130.230  
FTP ログイン: sasaki-build

 **スケジュール済みタスク**

## 顧客パネル



Wordpress

Administrative interface



更新可能 [3.7.1-22 に更新する](#)

新しいドメインを追加

新しいサブドメインを追加

新し

[sasaki-build.com](#) [ホスティング設定](#)

ウェブサイトの場所: [httpdocs/](#) IP アドレス: 10.37.130.230 システムユーザ: sa

 [開く](#)  [プレビュー](#)  [一時停止](#)  [無効化](#)



Wordpress

Administrative interface



更新可能 [3.7.1-22 に更新する](#)



EC-CUBE (PLESK ONLY)

## 管理者パネル

ホーム > ツールと設定 > インストール済みアプリケーション >  
**アップデート設定**

- インストールされたすべてのアプリケーションを強制的に更新  
アップデートが公開されると、すべての顧客のアプリケーションが自動更新されます。顧客が自動更新を無効化することはできません。警告：このオプションを使用する場合、更新によってアプリケーションの機能が著しく影響を受ける可能性があるため、注意が必要です。例えば、異なるバージョンのアプリケーションではアプリケーション拡張が機能しない場合があります。
- 「アップデートの公開後、このアプリケーションを自動更新」オプションをデフォルトでオンにする  
新規インストールされたアプリケーションに対し、アプリケーションの設定で「このアプリケーションを自動更新」オプションはオンに設定されます。

OK

キャンセル

# FTPS – FTP over SSL サポート (V11.5~)

FTPによるファイル転送が暗号化され、パケットからの情報漏洩を防止

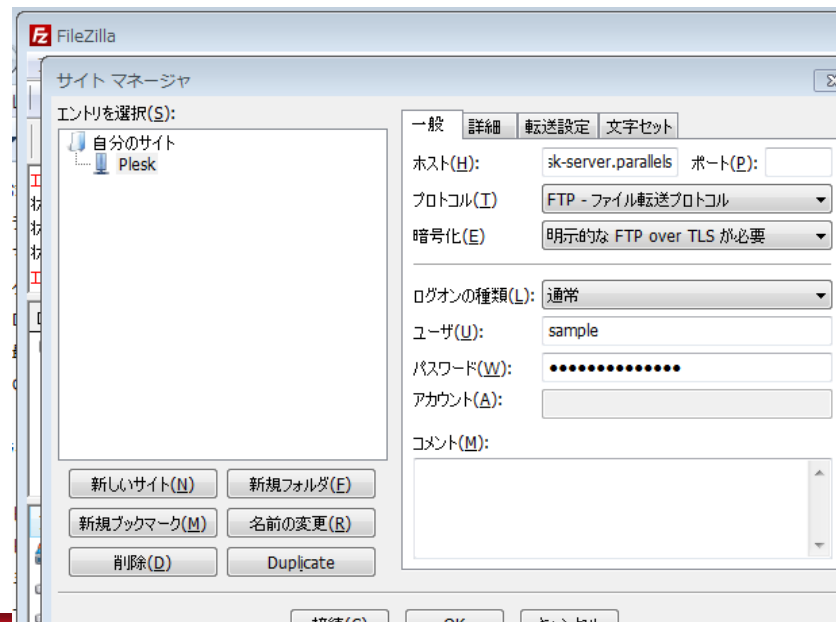
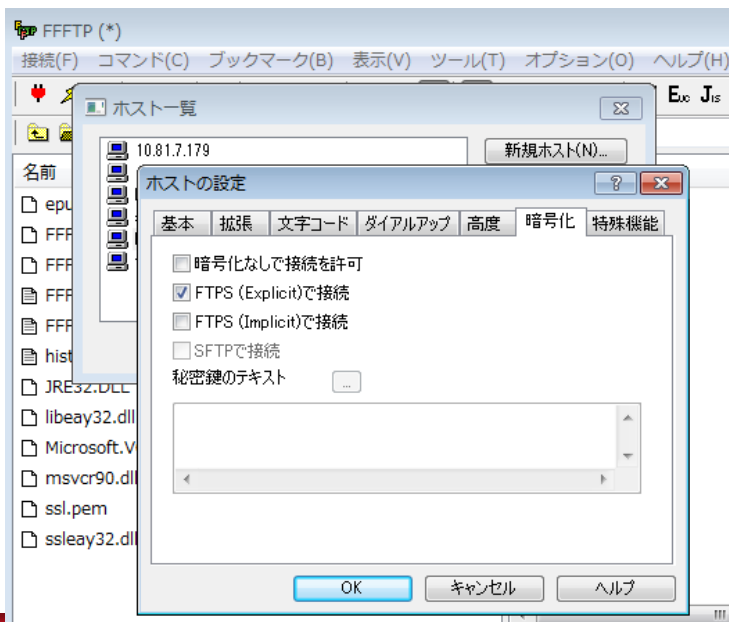
## セキュア FTP

FTPS は、FTP サーバと外部 FTP クライアントとの間の SSL 通信および TLS 通信を保護するために使用されます。ここで、許可する接続の種類を選択できます。

### FTPS 使用ポリシー

- セキュア FTPS 接続のみを許可する
- セキュア FTPS と非セキュア FTP 接続の両方を許可する
- 非セキュア FTP 接続のみを許可する。FTPS を使用しない

一般的なFTP クライアントでも既にサポート



# バックアップファイル経由での情報漏えい防止 (V11~)

- パスワードによるバックアップファイルのプロテクト – FTPレポジトリにアップロードされるバックアップファイルにパスワードを適用
- バックアップファイルへのサイニング  
– バックアップファイルの改ざんチェック

## 個人用 FTP リポジトリの設定

### 設定

FTP サーバのホスト名またはIP *	<input type="text" value="ftp.plesk.parapara.jp"/>
バックアップファイルストレージ用ディレクトリ	<input type="text" value="/backups/"/> 例. /myfolder/mybackups/
FTP ログイン名 *	<input type="text" value="backupacc"/>
古い FTP パスワード	なし
FTP パスワード	<input type="password" value="....."/>
FTP パスワードの確認	<input type="password" value="....."/>
パッシブモードを利用する	<input type="checkbox"/>
FTPS を使用	<input checked="" type="checkbox"/>

### バックアップセキュリティ設定

バックアップセキュリティを強化するためには、バックアップに含まれる機密データ（特にパスワード）をパスワード保護することをお勧めします。これによって、バックアップストレージにセキュリティ侵害が発生しても、機密データが攻撃者の手に渡りません。バックアップ保護に使用したパスワードを忘れた場合、復元することはできません。そのため、パスワードとバックアップファイル名のリストを安全な場所に保管しておくことをお勧めします。

パスワード保護を使用する	<input checked="" type="checkbox"/>
旧パスワード	なし
パスワード *	<input type="password" value="....."/>
パスワード再入力 *	<input type="password" value="....."/>

## ローカルコンピュータからサーバリポジトリにバックアップファイルをアップロードする

### ファイルアップロード

Panel リポジトリにバックアップファイルをアップロードします。最大ファイルサイズは 2 GB までに制限されています。

ファイルパス  ファイルが選択されていません。

[ファイルをアップロードする](#)

### バックアップのセキュリティ設定

Panel checks backup files for a valid structure and signature. Files that were modified, corrupted, or created on another server are distrusted. The option below enables you to restore data from such files. Select this option only if you trust the backup source because uploading such a file may compromise security or disrupt the operation of the server. Note: Backup files made in Panel versions prior to 11.5 are considered as distrusted because they lack signatures. Be sure to restore such files if you trust their source.

Upload backup files without a valid signature

このバックアップに対してパスワード保護を適用した場合、下のフィールドにパスワードを入力してください。パスワードを誤入力すると、Panel が警告を表示しますが、サーバへのバックアップファイルのアップロードは実行されません。バックアップの復元中に、このパスワードを再入力することを求められます。

このバックアップはパスワード保護されています。

パスワード \*

パスワード再入力 \*

# Chroot環境を前提とするSSH接続設定

範囲外のファイル参照、意図しないプログラム実行を禁止

The screenshot shows the control panel for sasaki-build.com. The main heading is "契約 sasaki-build.com をカスタマイズ". Below it, there's a warning about changing plans. A navigation bar includes "リソース", "パーミッション", "ホスティングパラメータ", "PHP 設定", and "アプリケーション". The "ホスティングパラメータ" tab is active, showing "SSH 経由のサーバアクセスの管理". The settings are:

- 許可しない
- Chrooted 環境へのアクセスのみ許可する
- すべてのタイプのシェルへのアクセスを許可する

Below these is a note: "ホスティングパラメータ「契約のシステムユーザとしてサーバシェルへ SSH アクセス」をプリセットにします." At the bottom, there are checkboxes for "プロバイダのポリシーを上書きする潜在的に安全ではないウェブスクリプトオプションのセットアップ" and "ホスティングパフォーマンス設定管理".



## その他の機能強化 (V11.5~)

- XML RPC APIアクセスに対するIP Address制限  
特定のIP Address に限った API利用制限
- Web Mail - RoundCubeサポート  
AtMail は除かれ、RoundCubeがデフォルトWebMailとしてサポート
- Web Mail - Horde IMP5サポート  
既にEOLに達しているHorde IMP 3.xからのアップデート
- Chroot環境前提の各種プログラム実行  
各種Pleskツールから呼び出されるwget, zip, unzip, gzip/gunzip, tar, curl  
プログラムがchroot環境下で実行
- Parallels Premium AntivirusのウィルスチェックエンジンがVersion 5か  
ら6へ更新

# まとめ

パネル（サーバ）を脅威から保護するためには：

- 最新版Parallels Plesk Panelの利用を
- サーバ全体のセキュリティー対策も忘れず
  - 適切なユーザ権限、パスワード管理と正しいサーバ運用を



**現在ご利用サービスの保守提供範囲の確認と、ご自身ができる作業範囲を正しく理解しましょう**

# Thank You