ISOG-J 日本セキュリティオペレーション事業者協議会

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

Parallels

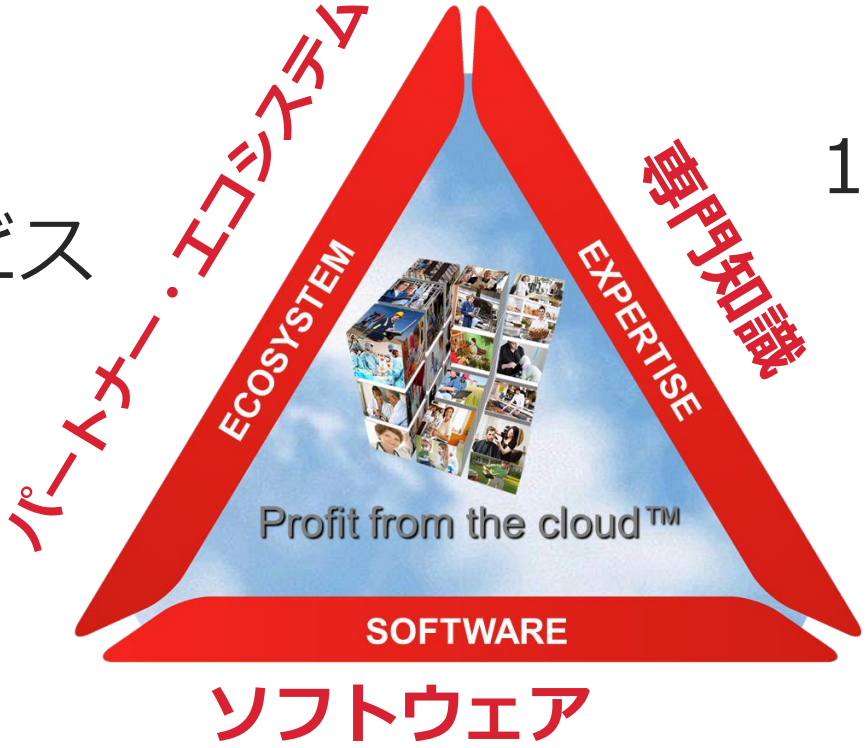
Profit from the cloud™

パラレルス株式会社
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

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 cleanKeysHistory 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
- Parallels Ple
- Plesk 7.5.x F
- Plesk 7.1.x F
- Plesk 7.0.x
- Parallels Ple
- Parallels Ple
- Parallels Ple
- Parallels Ple
- Parallels Ple
- Parallels Ple
- Plesk 7.x for

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

背景

Parallels Ples
CVE-2013-01
明されていま

脆弱性が確認
んが、Paralle

Parallels Plesk Panel：PHP-CGI にコードのリモート実行の脆弱性

対象製品:

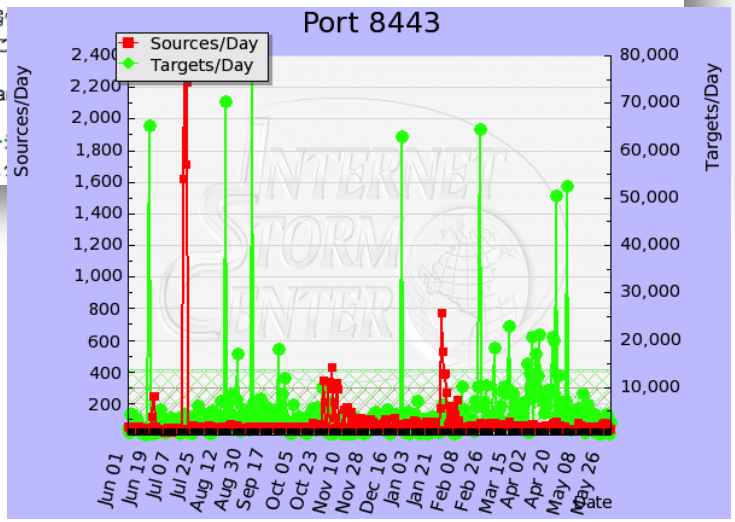
- Parallels Plesk Panel 9.2 for Linux/Unix
- Parallels Plesk Panel 9.0 for Linux/Unix

情報

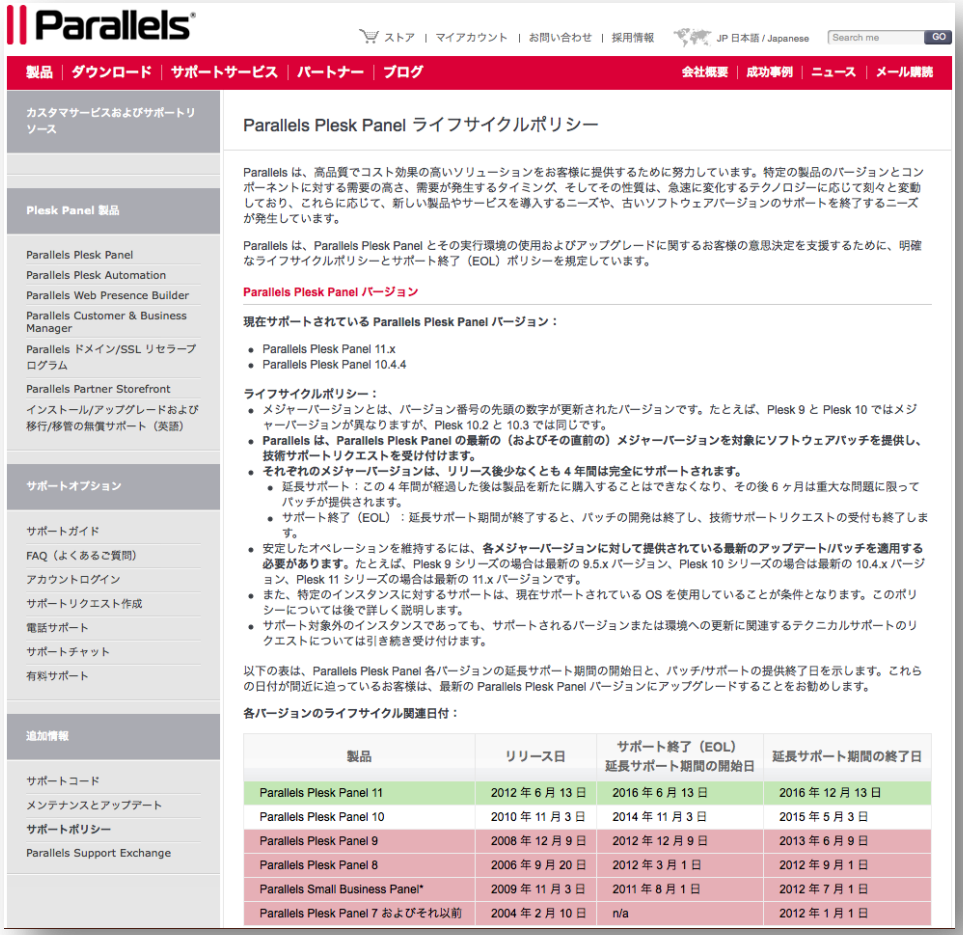
2012 年 5 月 3 日、PHP-CGI にコードのリモート実行の脆弱性があることが公開されました（CVE-2012-1823）。
これは重大な脆弱
PHP-FastCGI はこ

Parallels Plesk Pa

PP for Linux バー
cgi_wrapper ス



2. （サポートなしの）旧バージョンを使い続ける



Parallels

ストア | マイアカウント | お問い合わせ | 採用情報 | JP 日本語 / Japanese | Search me | GO

製品 | ダウンロード | サポートサービス | パートナー | ブログ | 会社概要 | 成功事例 | ニュース | メール購読

カスタマサービスおよびサポートリソース

Plesk Panel 製品

- Parallels Plesk Panel
- Parallels Plesk Automation
- Parallels Web Presence Builder
- Parallels Customer & Business Manager
- Parallels ドメイン/SSL リセラープログラム
- Parallels Partner Storefront
- インストール/アップグレードおよび移行/移管の無償サポート（英語）

サポートオプション

- サポートガイド
- FAQ（よくあるご質問）
- アカウントログイン
- サポートリクエスト作成
- 電話サポート
- サポートチャット
- 有料サポート

追加情報

- サポートコード
- メンテナンスとアップデート
- **サポートポリシー**
- Parallels Support Exchange

Parallels Plesk Panel ライフサイクルポリシー

Parallels は、高品質でコスト効果の高いソリューションをお客様に提供するために努力しています。特定の製品のバージョンとコンポーネントに対する需要の高さ、需要が発生するタイミング、そしてその性質は、急速に変化するテクノロジーに応じて刻々と変動しており、これらに応じて、新しい製品やサービスを導入するニーズや、古いソフトウェアバージョンのサポートを終了するニーズが発生しています。

Parallels は、Parallels Plesk Panel とその実行環境の使用およびアップグレードに関するお客様の意思決定を支援するために、明確なライフサイクルポリシーとサポート終了（EOL）ポリシーを規定しています。

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：

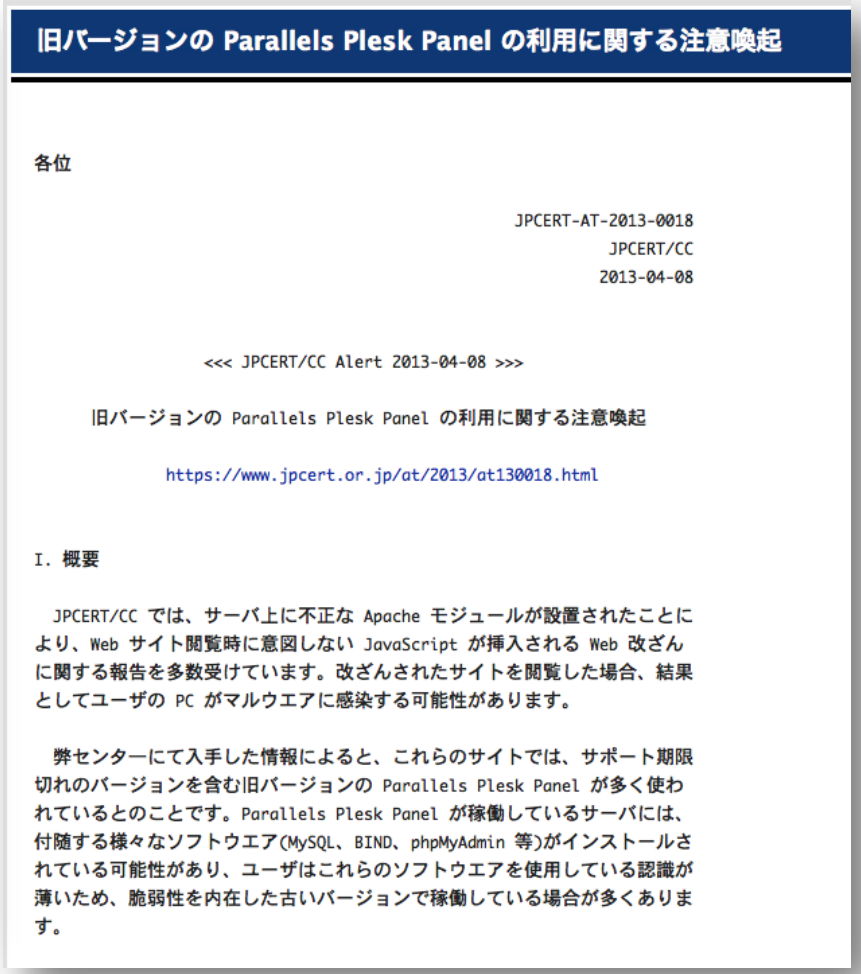
- メジャーバージョンとは、バージョン番号の先頭の数字が更新されたバージョンです。たとえば、Plesk 9 と Plesk 10 ではメジャーバージョンが異なりますが、Plesk 10.2 と 10.3 では同じです。
- **Parallels は、Parallels Plesk Panel の最新の（およびその直前の）メジャーバージョンを対象にソフトウェアパッチを提供し、技術サポートリクエストを受け付けます。**
- **それぞれのメジャーバージョンは、リリース後少なくとも 4 年間は完全にサポートされます。**
  - 延長サポート：この 4 年間が経過した後は製品を新たに購入することはできなくなり、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。これらの日付が間近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 がマルウエ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エア(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エ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。

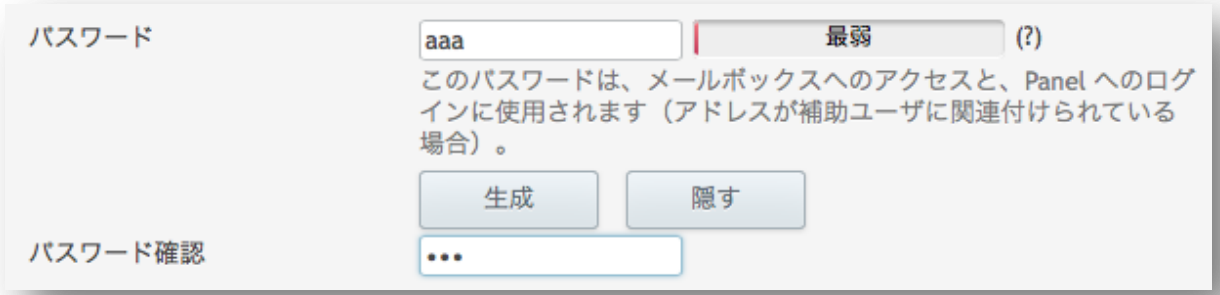
JPCERTコーディネーションセンターウェブサイト
http://www.jpcert.or.jp/at/2013/at130018.html

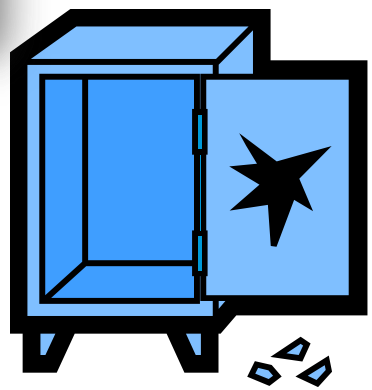
サーバ上に不正な Apache モジュールが設置、サイトの改ざん、マルウェア配布

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！





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..

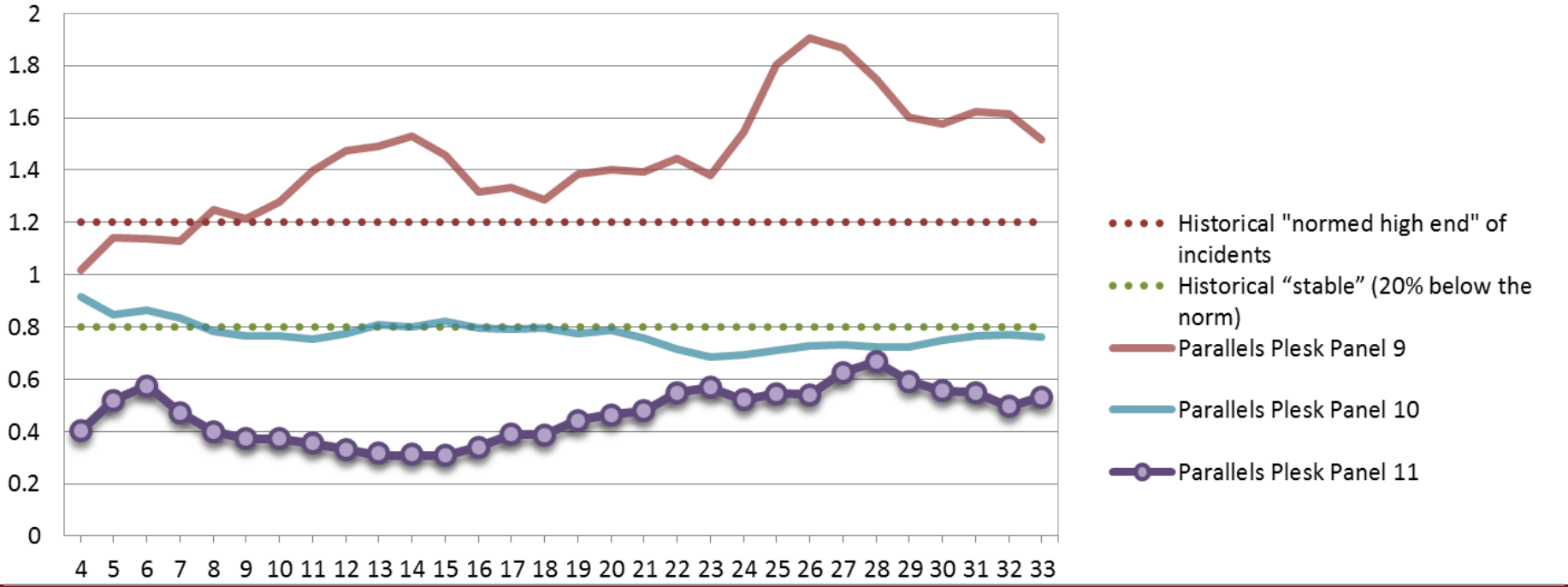
サービス事業者とあなたの責任範囲を理解してますか？

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～）

安易なパスワード入力の拒否（V10～）

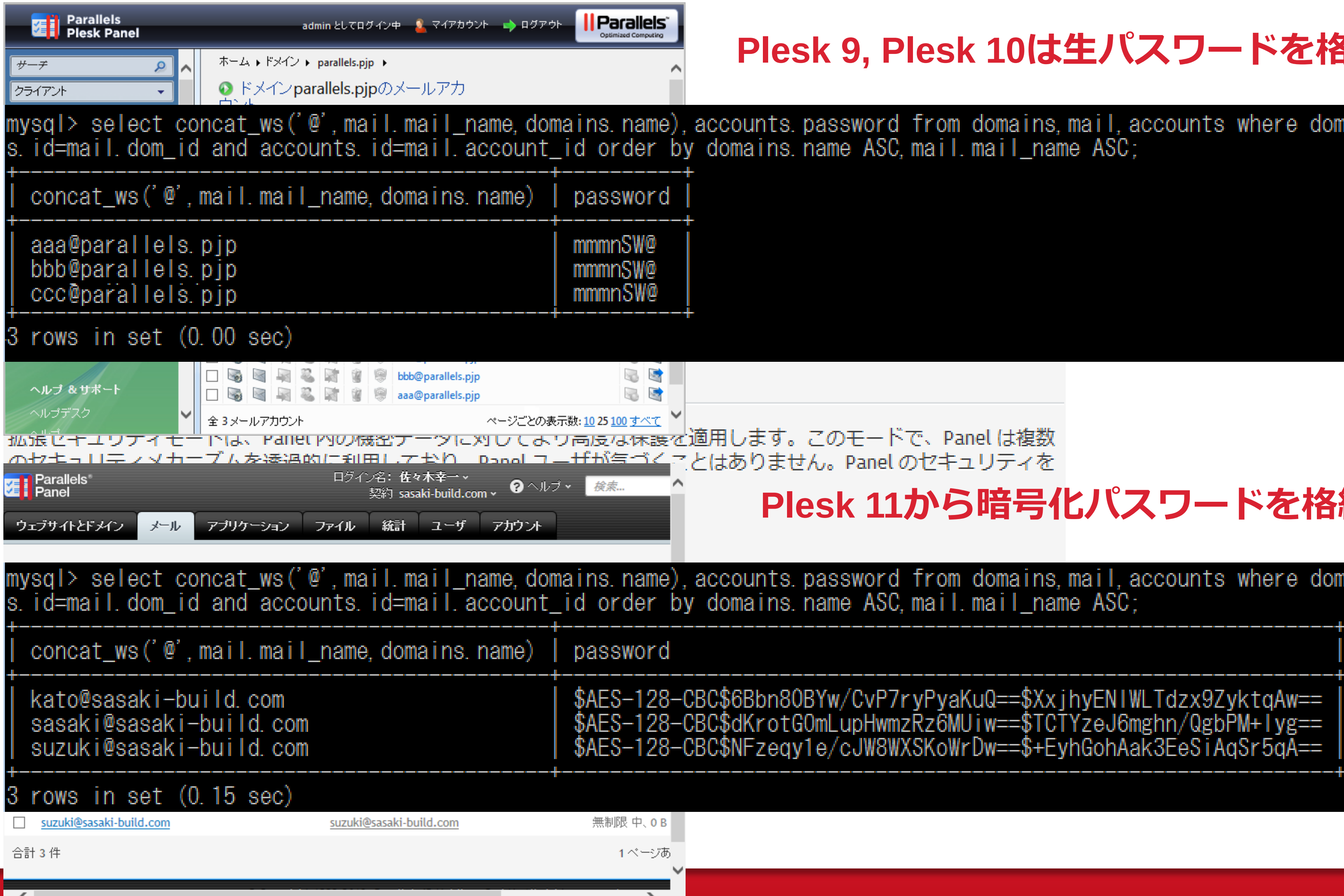
パネルログイン用ユーザアカウント、FTPアカウントのパスワードに対しても同様の制限あり

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

Plesk DB内の各種パスワードの暗号化（V11～）

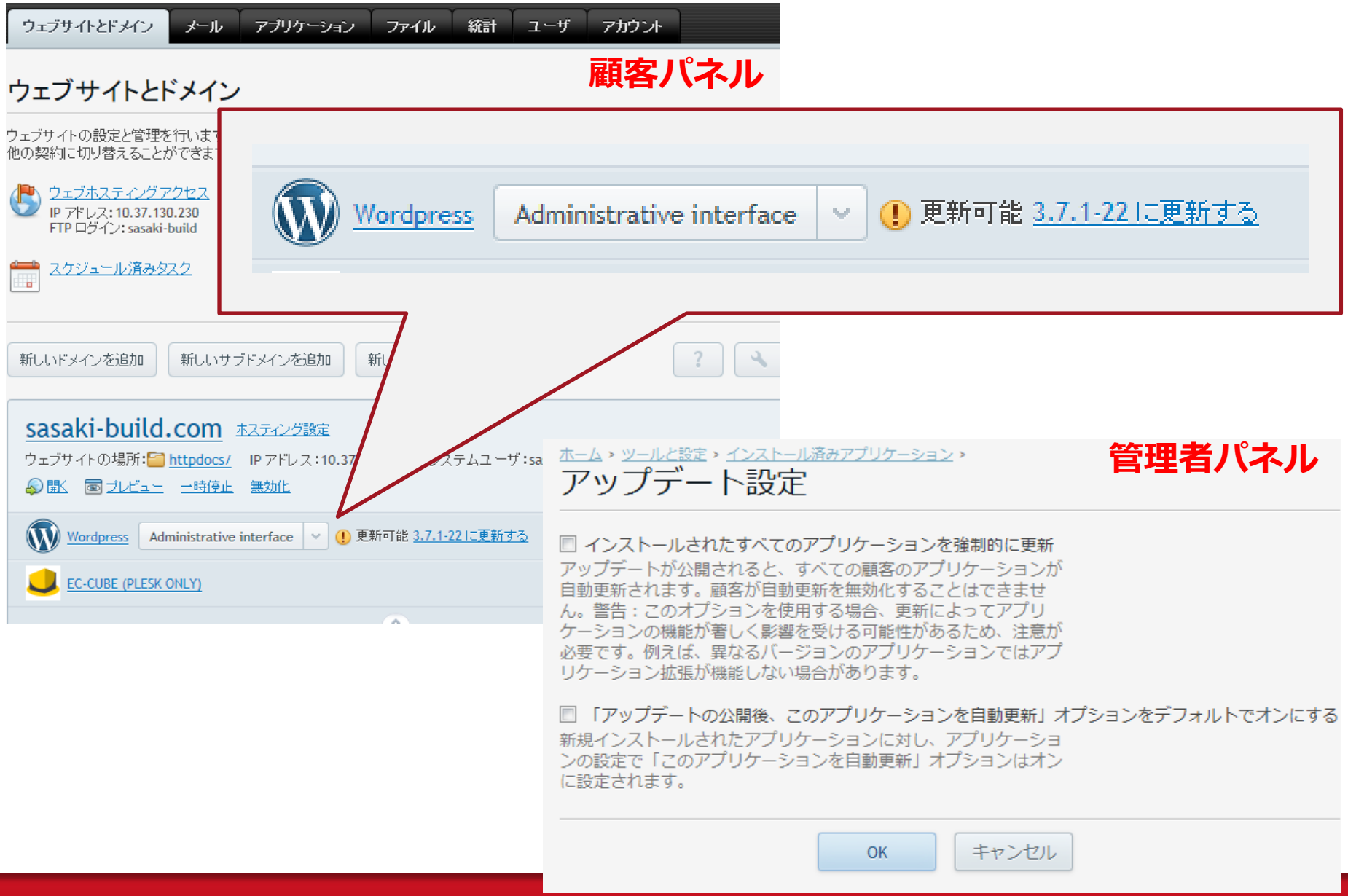
Plesk 9, Plesk 10は生パスワードを格納



拡張セキュリティモードは、Panel 内の機密データに対してより高度な保護を適用します。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

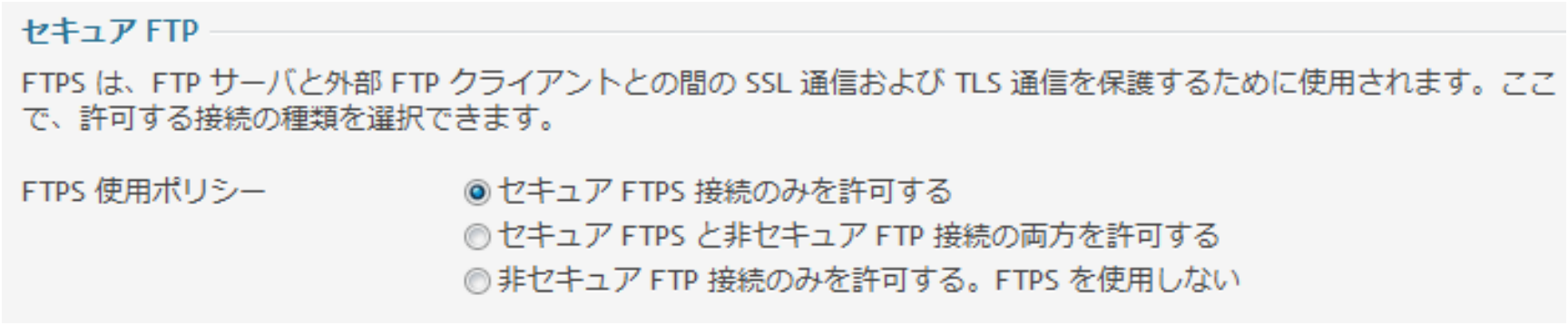
Plesk 11から暗号化パスワードを格納

APSパッケージの自動更新（V11.5～）

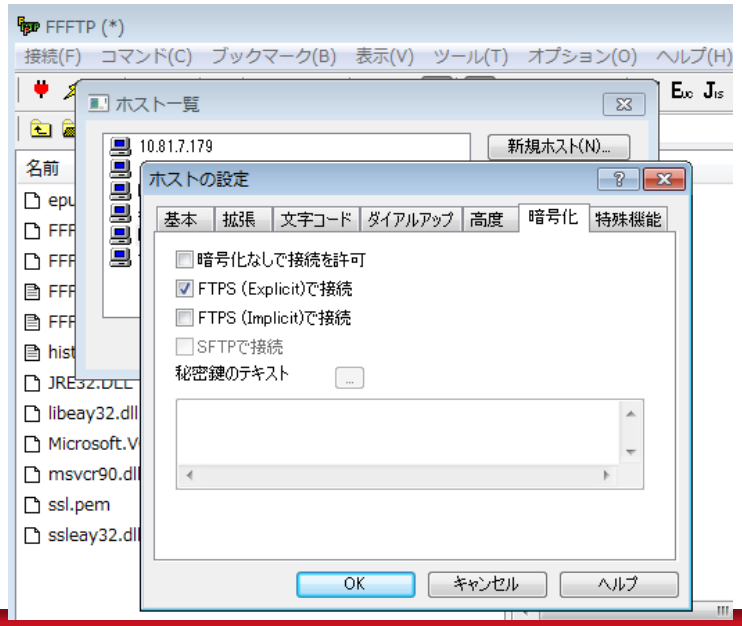


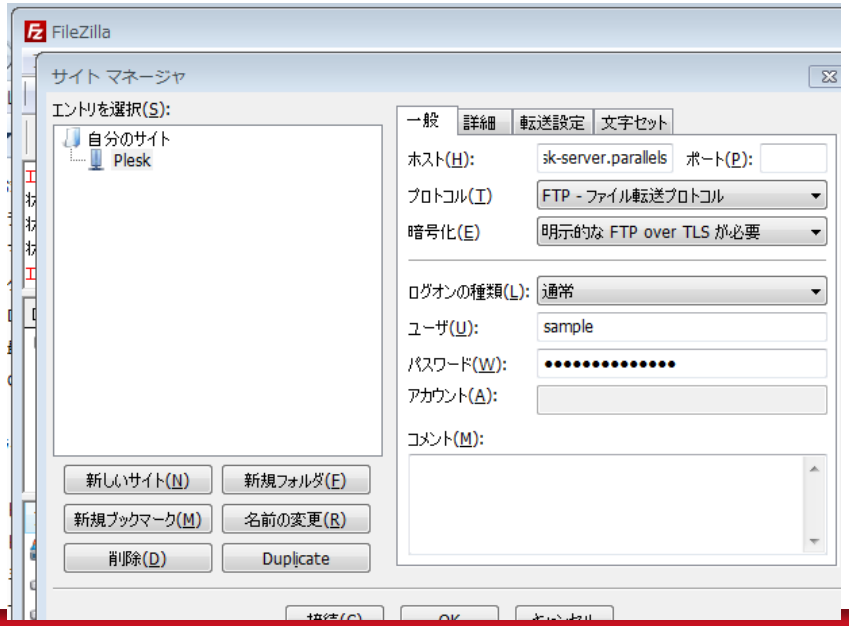
FTPS – FTP over SSL サポート（V11.5～）

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



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

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

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