株式会社クララオンライン

セキュリティアップデート for linux

Ver1.0

株式会社クララオンライン

2014/11/17

目次

1 サービス概要 3
2 サービス詳細 3
2.1 セキュリティアップデート実施の有無の判断基準 3
2.2 サービスプラン 5
2.2-1 セキュリティアップデートサービス for Linux 5
3 サービス契約 7
3.1 契約について 7
3.1-1 契約単位 7
3.1-2 申し込み方法 7
3.2 利用開始について 7
3.2-1 リードタイム 7
3.2-2 利用開始までの流れ 7
3.3 解約について 7
3.4 注意事項 7
3.4-1 パスワードの変更について 8
3.4-2 本仕様書について 8
4 免責 8

改訂履歴

バージョン	変更日	変更概要	変更者
Ver1.0	2014/11/17	初版	CLARA

1　サービス概要

Linux のセキュリティアップデートをお客様の代わりに行います。
クララオンライン「**セキュリティアップデートサービス for Linux**」はクララオンラインの実績と経験に基づくサーバインフラの運用ノウハウをもとに、セキュリティ情報のご案内とアップデート作業を代行、最新の状態を保ちます。

2　サービス詳細

クララオンラインが定めた定義にもとづいて、サービス対象項目に関して、アナウンス、対策を行うサービスです。サービス対象項目は下記の通りとなります。

クララオンラインにて必要と判断した場合にセキュリティアップデートを行います。

2.1　セキュリティアップデート実施の有無の判断基準

クララオンラインによるセキュリティレベルの判断基準は以下のとおりとし、セキュリティレベル「中」に分類される脆弱性に対し、セキュリティアップデートを提供します。

セキュリティレベル	対象脆弱性タイプ	適用対象サーバ
高 (標準提供)	リモートから任意のコマンドの実行が可能（サーバの乗っ取りなどの危険性がある）な脆弱性がある場合	全サーバを対象にセキュリティアップデートを実施
中	リモートから DoS 攻撃や、情報漏洩の可能性のある脆弱性がある場合	セキュリティアップデートサービスをご契約のお客様のみ実施

表1. サービス対象項目一覧

攻撃タイプ	概要	セキュリティレベル
リモートコード実行攻撃	リモートから任意のコマンドの実行をする攻撃です	高
DoS 攻撃	DoS はネット上のトラフィック（通信量）を増大させるなどして、通信を処理している回線やサーバの処理能力（リソース）を占有することによって、システムを使用困難にしたり、ダウンさせたり、過負荷によってサーバの機材そのものを誤動作させたり停止させたりすることです。	中
情報漏洩	情報の漏えいとは、当該情報にアクセスするため権限を明示的に受けていない者に対して、情報が意図的にあるいは意図せずに開示されることです。	中
SQL インジェクション	ソフトウェアが外部からの入力内容を、上位コンポーネントを通じて使用し、その内容から SQL コマンドを構築している場合において、意図	中

	している SQL コマンドを改ざんできてしまう特殊な要素を、適切に無効化せずに下位コンポーネントに送信する際に発生する脆弱性です。	
不適切な認証	ユーザが与えられた識別を所持していることを主張した際に、ソフトウェアにおいてその主張が正しいことを適切に証明しないという問題です。	中
暗号の問題	このカテゴリの脆弱性は暗号の利用に関するものです。	中
リソース管理の問題 (メモリリーク等)	このカテゴリの脆弱性は、システムリソースの不適切な管理に関連するものです。	中

2.2　サービスプラン

2.2-1 セキュリティアップデートサービス for Linux

2.2-1-1 サービス内容

対象は Linux サーバで、サーバにインストールされたソフトウェアの深刻な脆弱性が公開された際に、当該ソフトウェアの脆弱性公開の通知、および、アップデート作業を提供するサービスです。

1. サービス提供時間

   営業時間内(平日 10:00−18:00)でのご提供となります。

   営業時間外 (休日(全日)、平日 18:00～10:00)に作業をご希望の場合、別途有償での作業も可能となります。

2. 対象 OS・ソフトウェア

   対象 OS は、別表 1 をご参照ください。

   対象ソフトウェアは、OS ベンダから提供されたソフトウェア、または、クララオンラインから提供されたソフトウェアとなります。詳細は、別表 1 をご参照ください。

   お客様がソースコードからインストールしたソフトウェアの場合は、対象ソフトウェアであっても本サービスの対象外となります。

3. セキュリティアナウンス

   対象 OS・ソフトウェアに脆弱性が公表された場合、ご契約のお客様に対して概要・対応方針についてアナウンスを実施いたします。

   OS 単位で管理する為、対象ソフトウェアを導入されていないお客様へも通知いたします。

4. 対策の実施

   アナウンスを実施後、ご依頼のあった対策について実施させて頂きます。

   原則として、お客様より作業依頼をいただいていない対策作業は実施されませんのでご注意ください。

   対策作業は営業時間内(平日 10:00−18:00)での実施となります。

   営業時間外 (休日(全日)、平日 18:00～翌 10:00)に作業をご希望の場合、別途有償でのお見積もりも可能です。

表 2. 対応フロー

項番	対応内容	作業者
1	脆弱性確認	クララオンライン
2	お客様への通知	クララオンライン
3	お客様からの依頼 依頼があったもの　→ 項番 4 へ 依頼が無かったもの → 項番 5 へ	お客様
4	対策の実施 → 項番 5 へ	クララオンライン
5	対応完了	

5. 価格について

別表 2 をご参照ください。

2.2-1-2 サポート範囲

セキュリティアップデート作業に関するご質問をお受けいたします。原則として、メール・電話でのサポートとなります。

お客様で作業を行う場合の具体的なアップデート方法等の質問はサポート対象外となります。

3　サービス契約

3.1　契約について

3.1-1 契約単位

本サービスは、Linux サーバを対象とし、仮想サーバ、物理サーバを問わず OS 単位でお申込み頂けます。

3.1-2 申し込み方法

クララオンライン指定の Web フォーム・注文書といたします。

3.2　利用開始について

3.2-1 リードタイム

お申込み受付完了後、1 営業日

3.2-2 利用開始までの流れ

I. お申込み（お客様）
II. 1 営業日で「**セキュリティアップデートサービス for Linux**」サービス開始(クララオンライン)
※ご利用開始日以降に確認された脆弱性が対象となります。

3.3　解約について

解約をされる場合は、解約希望日の前月末日までに解約申込書をお送り下さい。

3.4　注意事項

- ウェブサーバ起動時の SSL パスフレーズを設定されている場合は、クララオンラインへの通知が必要です。
- アップデート対応時間は弊社営業時間内(平日 10:00～18:00)となります。
※営業時間外に作業をご希望のお客様は、お見積もりさせていただきますので別途ご相談下さい。
- 本オプションサービスの最低利用期間は 1 ヶ月となります。
- 対策後はお客様による動作確認をおこなって頂きます。
- 本サービスは対象パッケージのアップデートを行うサービスです。システムへの攻撃・不正侵入防止等を保証するサービスではございません。

・　OS 提供ベンダの保守が終了した時点で、本サービスの提供も終了となります。

3.4-1 パスワードの変更について

お客様にてパスワードを変更される場合、必ずクララオンラインまでお知らせください。
お知らせがない場合、本サービスが提供できない場合がございます。

3.4-2 本仕様書について

本仕様書に定めの無いことは、サービス約款に従います。本仕様書は、最新版を有効とします。

4　免責

・　対策作業の前までに、発生した事象については免責とさせていただきます。
・　対策（アップデートパッチ適用等）後の動作を保証するものではございません。
・　OS ベンダより提供されるアップデートパッケージは、その安全性、信頼性、適時性、および性能は保証されるものではありません。
・