NET ASSIST
24/7 Guardian Deity

News Letter

2021.5

#01

【目次】

主にメールにて、ネットアシストのニュースやＩＴ関連トピックスをお届けします。
今回が記念すべき第１回目の配信です。

感想などの反響は、メールでも担当営業にお伝えいただくのでも大歓迎です。
自社の新サービス紹介や、取り上げて欲しい題材などあればご連絡ください。

今後毎月発行予定となりますので、ぜひご一読いただければと思います。
これからもネットアシストをよろしくお願いいたします！

迫るＣｅｎｔＯＳ８のサポート期間終了に対する今後の対応

CentOS8の代替OSについて

去る2020年12月9日(日本時間)、CentOS公式からの発表によりIT業界に衝撃が走りました。
CentOS8のサポート期限が「2029年6月30日」から「2021年12月30日」に7年半も短縮するという発表です。
CentOS8ユーザーは有償OSであるRHEL、テスト用OSであるCentOS stream、または他ディストリビューションのOSへのリプレイスが必要でした。それから半年、有志の手により代替OSであるAlma Linux、Rocky Linuxが発表されました。

代替OSについて

前提としてCentOS8はRHEL8のソースコードを元に組まれた無償OSです。
RHEL8自体は有償ですがそのソフトウェアのソースコードはオープンソースライセンスに基づき無償で公開されております。
CentOS8はこれをもとに商標や商用パッケージ等を除去したものです。
代替OSのAlma Linux、Rocky LinuxはCent OS8と同じく、公開されているソースコードを元に組まれたOS となります。

Alma Linuxについて

2021年3月30日にCloud Linux社より公開されたOSです。
2029年までの長期サポートとCent OS8と同じ使用感を備えた無償のOSです。CentOS8の環境に最も近い運用が可能です。
一部のクラウドベンダーでもリリースが予定されており、現在CentOS8を利用しているお客様は、このOSのリリースを待つのが良さそうです。

Rocky Linuxについて

5月にリリース予定のOSです。
CentOSプロジェクトの創設者であるグレゴリー・クルツァー氏が率いて開発しています。
サポート期間は2029年5月のため、リリース後には商用可能な無償OSとして利用が検討されています。

PICK UP!

不正アクセス事例

慶応義塾大学 湘南藤沢キャンパス（SFC）

2021年5月7日、慶応義塾大学は、SFCの会議室予約へ不正アクセスを検知し、個人情報6507件の漏洩の可能性を発表しました。
今回漏洩したデータは、会議室を利用した学生・教職員などの氏名・電話番号・メールアドレスとみられます。
トップページの表示が乱れていることを確認したことから詳細を調査した結果、サイバー攻撃を受けていたことが判明しました。
同大学は今回被害を受けたシステム以外にも、情報ネットワークシステムや授業支援システムなどの複数のシステムを保有しており、昨年から断続的なサイバー攻撃を確認していました。2020年11月にもSFCキャンパスのサーバーへの不正アクセスによって、30,000件の学生の個人情報が漏洩した可能性からCSIRT（情報セキュリティーインシデント対策チーム）を発足したばかりでした。

このような不正アクセスを防ぐには・・・

・Webアプリケーションやシステムの脆弱性診断の実施
・Webアプリケーションファイアウォール（WAF）の導入 がおすすめ！

脆弱性を含んだままのコードを利用していると、その脆弱性を突かれて不正アクセスは発生します。また、長く稼働しているシステムには、開発時には発見されていなかった脆弱性が含まれている場合もあり、安定的に利用できているシステムでも、Webシステム自体の脆弱性を定期的に診断し、セキュリティリスクをつぶしておくことが必要です。
また、未知の攻撃や脆弱性などは日々発見されていますが、そのたびに診断＋改修を行うことはまず不可能です。そのため、速やかに新たな脆弱性やゼロデイ攻撃に対応するためには、Webアプリケーションレベルでの攻撃を防御してくれる「WAF」の導入も必須となります。

ネットアシストで提供可能なサービス

脆弱性診断：自動ツールでの診断やエンジニアによる手動診断など
WAF：主に、クラウド型のWAFサービスを販売。

攻撃遮断くん　クラウド型WAFサービス Scutum　WafCharm

★サービスの詳細や費用などは直接お問合せください

Vulnerability 今月の脆弱性

※今月、公式から発表された脆弱性の一部をご紹介しています。

・概要

・脆弱性が存在するプロダクトおよびバージョン

【Exchange Server】
権限を持たない攻撃者が遠隔地からカーネルモードでコードの実行が可能等

Exchange Server 2013 / 2016 / 2019

【WordPress】
攻撃者による影響を受けたシステムの制御権が乗っ取られる危険性

・WordPress 3.7から5.7.1までのバージョン

【EC-CUBE】
クロスサイトスクリプティングの危険性

・EC-CUBE 4.0.0から4.0.5までのバージョン

【Google Chrome】
攻撃者よる影響を受けたシステムの制御権が乗っ取られる危険性

・Google Chrome version 90.0.4430.212 よりも前のバージョン
（※for Windows・for Mac・for Linux　共通）

【Firefox】
ユニバーサルクロスサイトスクリプティングの危険性　等

・Firefox 88.0.1よりも前のバージョン
・Firefox for Android 88.1.3よりも前のバージョン

【Samba】
攻撃者によって影響を受けたシステムの制御権が乗っ取られる危険性

・Samba 3.6.0以降のすべてのサポートされているバージョン

お問い合わせ
株式会社ネットアシスト
0120-941-670
sales@netassist.ne.jp
https://www.netassist.ne.jp/