NET ASSIST
24/7 Guardian Deity

2023.8 #28

NEWS LETTER

TOPICS

＊ TOPICSの各タイトルをクリックすると該当の記事へ飛びます

#1 いよいよ1年を切ったCentOS 7のサポート期限（EOL）

CentOS 7 のサポート期限

過去の記事でも何度かご紹介しておりましたが、いよいよCentOS 7のサポート終了まで1年を切りました！

サポート期限（EOL） 2024年6月30日

※EOL＝End Of Lifeの略。
サポート期限終了を意味する

CentOS 7をご利用頂いているお客様は非常に多いため、今回は改めてサポート期限終了に向けて、CentOS 7ユーザーが対応すべき内容を整理してご紹介いたします。

OSサポート終了の影響

そもそも、OSのサポートが終了すると、一体何が問題となるのでしょうか？お客様の中には、サポート終了でサーバーが使えなくなるのか？といったお問合せを頂くことも多いですが、結論から言うとサーバーは使い続けることができます。では、何が問題となるか。ポイントは以下2つです。

①セキュリティリスクが高くなる

すべてのOS・ソフトウェアには、セキュリティ上の弱点「脆弱性」が潜んでいます。通常、提供元はサポート期間中に「脆弱性」が発見された場合は、修正プログラムを提供しますが、サポート終了後に新たな「脆弱性」が発見された場合は、修正プログラムは提供されません。つまり、セキュリティ上の弱点を残したままの状態となり、サイバー攻撃などの対象となりやすくなるのです。

②安定性が低くなる

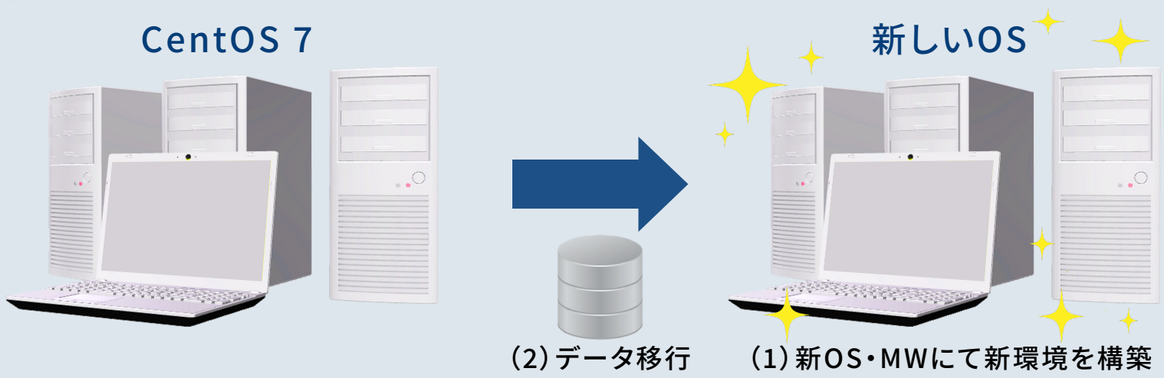
1でもお伝えした通り、提供元はサポート期間が終わると修正や機能のアップグレードを行う事はありません。不具合がおこったとしても対処がされないためOSの安定性は低くなり、場合によっては不具合を許容しながら使い続けることになりかねません。また、ソフトウェアやアプリケーションが推奨するOSからも外れることが多く、利用しているソフトウェアやアプリケーションの動作に問題が生じる可能性もあります。

サポート終了に向けて何をすればいいのか？

サポート期限が切れるとセキュリティリスクが高くなり、安定性が低くなることはわかりました。ではCentOS 7を利用しているユーザーは、一体何をすればいいのでしょうか？
対処法としては、以下が挙げられます。

①新しいOSへ移行する

WindowsOSの場合は、そのままWindowsのアップグレードを行う事で対処できることもありますが、CentOSの場合はそうはいきません。CentOSを始めとするLinux系OSの場合、PHPを始めとする導入パッケージのバージョンが変更されるなど、そのままのサーバーでアップグレードを行うと大抵は不具合が発生するため、新しいOSで構築したサーバー環境に「移行」をしなければなりません。



②延長サポートをうける

弊社ではご提供しておりませんが、コミュニティによるサポートが終了した後の「延長サポート」をサービスとして提供しているベンダーもあります。1のように新しいOSの環境へ移行を行うと、対象サーバーで運用されているコンテンツやシステムの改修も必要となるため、サポート期限までに移行を完了することができないケースもあるかと思います。そんなユーザー向けに、各社延長サポートのサービスを提供しておりますので、どうしてもサポート期限終了までに移行が間に合わないという方は、延長サポートを検討してみてください。

次ページへ

前ページより

新しいOSは何を選択すればいいのか？

過去の記事でもご紹介しましたが、CentOS 7の後継OSであったCentOS 8はすでにサポートが終了（2021年12月31日）しており、CentOS 9はリリースされていないためCentOS LinuxのプロジェクトはCentOS 7とともに終了いたします。
CentOSは無償のOSでRHELと高い互換性を持ち、有償OS並みの長期サポートがあったため日本国内では広く利用されているOSでしたが、今回のプロジェクト終了に伴い無償のOSを使い続けることのリスクもユーザー側は考えねばなりません。
とはいえ、CentOS 8の突然のサポート終了のタイミングで、新たにCentOSの代わりとなる「AlmaLinux」や「RockyLinux」というRHEL互換のクローンOSも登場してきています。（2023年6月26日に、これらのクローンOSをRed Hat社が非難するというニュースもありましたが・・・）以下にて、リプレイス先候補のOSとその比較表をご紹介いたします。移行先環境に何を重視するのかにもより、適切なOSをご選択ください

ディストリビューション	Red Hat Enterprise Linux（RHEL）	AlmaLinux	Ubuntu	Amazon Linux
費用有無	有償	無償	無償	無償（AWS環境の場合のみ）
サポート期間 EOL	RHEL8：2029年5月 RHEL9：2032年5月	AlmaLinux8：2029年3月 AlmaLinux9：2032年5月	Ubuntu22.04LTS：2027年4月	Amazon Linux2023：2028年3月
安定性・継続性	高	中	高	高
移行元CentOSとの互換性	高	高	低	低
特徴	Red Hat社が提供する有償OSのため、プロジェクト終了の心配がなく安定して長期サポートが受けられる	RHELのクローンOSのため、CentOSとの互換性は高いがコミュニティ主動で開発しているため、長期的に安定してサポートが受けられる保証はない	Debian派生のOSのため、RHEL互換であるCentOSからの移行となると互換性は低いが、世界的に見るとUbuntuのシェアが大きい。リリースを行うスピードも早く、LTS版のサポート期間は5年となっている	AWS環境で利用可能。今までのAmazon Linuxと違い、Fedoraをベースに構築されるためCentOSとの互換性は低め。Ubuntuと同様2年ごとのリリースかつサポート期間は5年間。AWS提供のため安定した長期サポートが受けられる

移行のご検討はお早めに！

弊社では、新しいOSへの移行のお手伝いを承っております。一部のお客様にはすでに移行のご提案も実施しておりますが、冒頭で述べたようにCentOS 7を利用しているサーバーは非常に多く、年明けからは多くのお客様からご依頼を頂くことが予想されます。ご依頼頂くタイミングによっては、サポート終了までに対応できないという可能性もございますので、余裕をもったスケジュールで移行が進められるよう、なるべく今年中にご依頼頂くことをお勧めしております！
なお、移行についてのご相談は下記にて承りますのでお気軽にご連絡ください。
株式会社ネットアシスト営業部　sales@netassist.ne.jp

#2 情報セキュリティ白書2023を見てみよう（前編）

情報セキュリティ白書2023とは

独立行政法人情報処理推進機構（IPA）により2023年7月25日（火）に刊行された書籍です。
2022年度の情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生状況、被害実態など定番トピックの他、その年ならではの象徴的なトピックを取り上げています。
国内外の官民の各種データ、資料を数多く引用しトピックを解説しており、情報セキュリティ分野の全体把握が容易です。
書籍として購入するだけでなく、アンケートの回答に協力することでPDF版の入手も可能です。

独立行政法人情報処理推進機構(IPA)「情報セキュリティ白書2023」
https://www.ipa.go.jp/publish/wp-security/2023.html

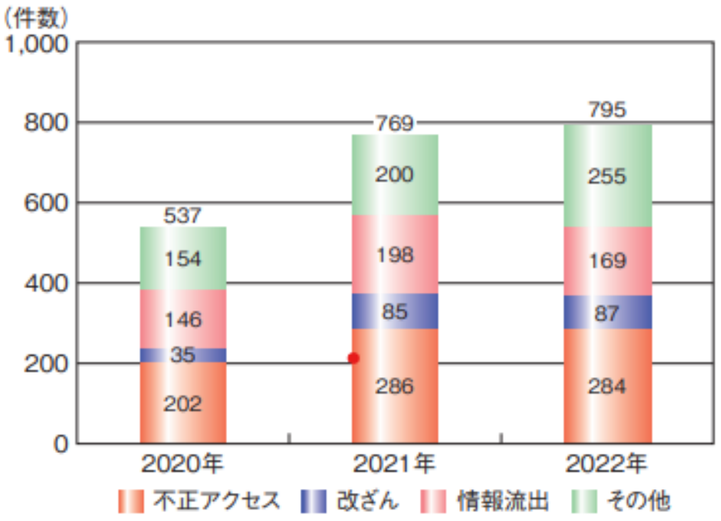
約250ページにも及ぶ内容のため、インフラ面に関連の高い部分を抜粋し、前編（8月）・後編（9月）の2回に分けてお届けします。

次ページへ

前ページより

国内における情報セキュリティインシデントの発生状況

三井物産セキュアディレクション株式会社（以下、MBSD社）によれば、2022年の情報セキュリティインシデントの種類別報道件数は全体で795件となり、2021年に対し3.4%増でした。不正アクセス、改ざんがほぼ横ばいで、「情報流出」は前年比14.6%減、「その他」が27.5%増でした（図1）



※セキュリティ白書2023　図1　情報セキュリティインシデントの種類別報道件数
（出典）MBSD 社による集計情報を基に IPA が作成

(1)ランサムウェアの被害

とりわけ大きく被害数を伸ばしたのはランサムウェアによる被害です。
ランサムウェア（ransomware）とは、「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語であり、パソコンやサーバー等のシステムをロックすることや、システムに保存されているファイルを暗号化することにより使用不能にして金銭を要求するウイルスの総称です。

2022年中に警察庁に報告された国内のランサムウェアによる被害は230件で、前年比57.5%増でした（図2）。
被害対象として、中小企業の被害件数が前年比53.2%増、団体等の被害件数が前年比155.6%増となっており、企業、団体等の規模を問わず広範に及んでいることがうかがえます。

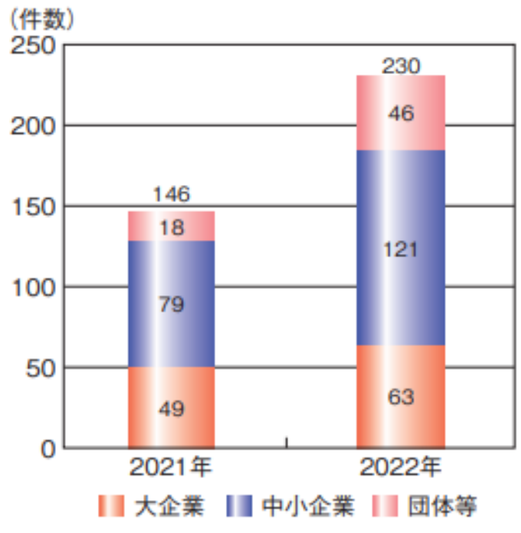


図2　国内のランサムウェアによる被害件数（2021～2022年）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等に ついて」
「令和4年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

攻撃の手口では、窃取したデータを暴露する「二重の脅迫」に加え、被害組織へのDDoS攻撃や、被害の事実を被害組織の顧客や利害関係者に連絡する等の脅迫手法も確認されています。ここ数年で被害が急増している要因として、ランサムウェア攻撃をサービスとして提供する「RaaS（Ransomware as a Service）」の普及や、攻撃者の組織化・分業化が挙げられます。

感染経路としては、2021年に引き続きインターネットに公開されたVPN機器等の脆弱性や、強度の弱い認証情報等を悪用し、ランサムウェアに感染させる手口が多く見られました。
侵入経路とされる機器のセキュリティパッチの適用状況について、得られた119件の回答のうち、「最新のセキュリティパッチを適用済み」は29.4%（35件）、「未適用のセキュリティパッチがあった」は54.6%（65件）でした。

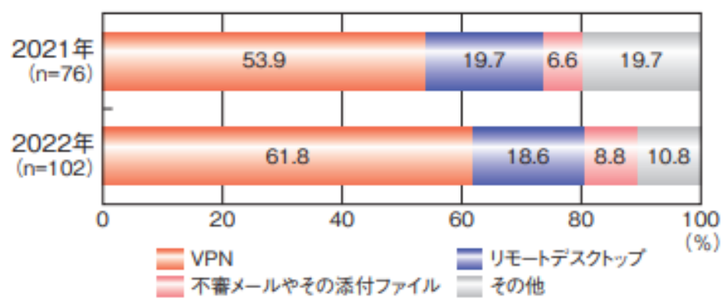
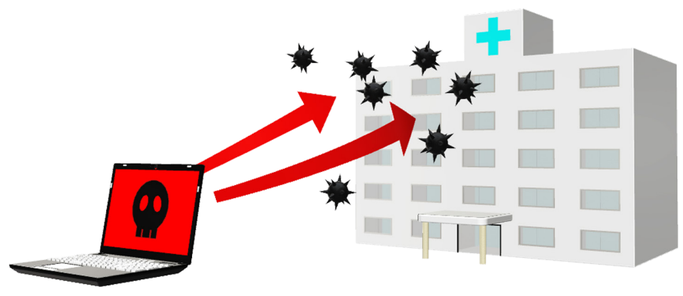


図3　ランサムウェアの感染経路（2021～2022年）
（出典）警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等に ついて」
「令和4年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成

脆弱性をついた攻撃がメインとなる中、6割以上の企業が、対策が不十分だったという事実は重く受け止める必要がありそうです。



(2)不正アクセスによる情報漏洩被害

不正アクセスの手口は年々巧妙化しており、システムの脆弱性を悪用したものや、サプライチェーンを含む対策が不十分な取引先や委託先、システムへの侵入等、様々な原因から不正アクセスが発生しています。
金銭的被害も確認された事例があり、一層深刻な事態となっています。
2022年10月に公表された、入力フォーム支援サービスを提供する株式会社ショーケースの事例では、同社が提供するサービスにおいて、第三者による不正アクセスでソースコードが書き換えられ、サービス利用企業のWebサイトで入力された情報が外部へ流出するといった被害も確認されています。

最後に

各種セキュリティサービスを導入することで被害を未然に防ぎ、被害拡大を抑える効果が考えられます。

弊社では、アプリケーション層を守る「WAF」や、サーバーへの悪意ある第三者のアクセスや侵入を検知・防御も行える「IDS/IPS」といったセキュリティサービスの取り扱いがございます。
ご検討の際は担当営業までご相談ください。

来月の後編では、国内の情報セキュリティ政策について抜粋してお伝えいたします。お楽しみに！

#3 【9月14日(木)】脆弱性診断に関するセミナーを開催!

この度、Webサイト制作会社様や自社サイトの管理や運営をされている企業のご担当者様を対象に、『丸わかり!WEBサイト運用に必要な「脆弱性診断」を徹底解説!～診断の様子もお見せします!～』と題してセミナーを開催いたします。

日　程	2023年9月14日(木) 14:00～15:00
費　用	無料
開催場所	Zoom(事前登録制)

セミナー概要

Webサイトを安全に運用するためには、脆弱性が潜んでいないかを定期的に確認することが重要です。
今回のセミナーでは、脆弱性を確認できる「脆弱性診断」に関して、診断の概要や診断項目、
Webサイトに合わせた診断種類の選び方など、具体的に解説いたします。
また、実際に脆弱性診断を検討しているものの、イメージが湧かない!という方に向けて、
今回は実際に自動診断を行う様子もお見せいたします。
ご興味のある方はぜひご参加ください!

詳細の確認・お申込みは下記URLからお願いいたします。

https://www.netassist.ne.jp/0914_security_webinar/

NET ASSIST 24/7 Guardian Deity
株式会社 ネットアシスト

TEL 03-3985-6780
mail sales@netassist.ne.jp
web https://www.netassist.ne.jp