Press Release
報道関係者各位

2024 年 11 月 6 日
SUSE ソフトウェアソリューションズジャパン株式会社

SUSE、「クラウドのセキュリティレポート」の日本語版を発表
AI 時代のクラウドセキュリティの課題に関する重要な洞察を明らかに

- 調査対象のアジア太平洋地域の IT リーダーの 64%が過去 12 か月間に少なくとも 1 件のクラウドセキュリティインシデントを経験し、62%が同じ期間にエッジセキュリティインシデントも経験
- アジア太平洋地域ではクラウドの導入が広まっているものの、セキュリティ上の懸念がクラウド導入の増加を妨げており、アジア太平洋地域の IT プロフェッショナルの 84%が、データの安全性が保証されれば、より多くのワークロードをクラウドとエッジに移行すると回答しているが日本は 53%と他国と異なる結果に

東京（日本）- 2024 年 11 月 6 日 - 革新的でオープンかつセキュアなエンタープライズグレードのソリューションで世界をリードする SUSE®(日本法人:SUSE ソフトウエアソリューションズジャパン株式会社 カントリーマネージャー　村上督)は本日、初の「Securing the Cloud(クラウドのセキュリティ)」に関するアジア太平洋地域レポートを発表しました。このレポートでは、生成 AI(Gen AI)とエッジコンピューティングがクラウドセキュリティに与える影響に焦点を当て、日本を含む中国、シンガポール、インド、韓国、インドネシア、オーストラリアのいわゆるアジア太平洋地域におけるクラウドセキュリティの課題について 900 名の IT エンジニア、プロフェッショナル、意思決定者などの回答をもとにしています。

2024 年アジア太平洋地域版のレポートでは、ますます複雑化するクラウドおよびエッジ環境のセキュリティ確保において IT チームが直面している差し迫った課題を明らかにし、クラウド導入における主な課題を特定しています。このレポートでは、アジア太平洋地域の IT 意思決定者が独自の機会と課題に直面していることを特定し、アジア太平洋地域諸国間で優先事項と懸念事項に大きな違いがあることが浮き彫りになりました。

SUSE による「Securing the Cloud」トレンドレポート全文は、こちらからご覧いただけます。

調査概要

調査期間：2024 年 9 月 3 日から 12 日

調査対象者属性：IT マネジメント層（IT プロフェッショナル、IT に関する意思決定者等）

人数：900 名（内訳：日本、中国、インド、韓国、インドネシア　各国 150 名、オーストラリア　100 名、シンガポール 50 名）

主な調査結果（日本）

- 調査対象となった全地域の中で、日本の意思決定者がクラウドに移行していないと回答した割合は APAC で最も高い（ワークロードの 36%がクラウドに移行していないと回答）： 全体的なクラウド移行に対するアプローチがまだ保守的であることを示唆している
- 日本の IT 意思決定者にとって、生成 AI への脅威に関してはセキュリティが最重要課題となっている：内訳は AI を利用したサイバー攻撃（39%）と AI サプライチェーンにおける脆弱性（31%）と回答
- エッジコンピューティングに関して、データは日本の IT 意思決定者にとっても重要な懸念事項である： データ・プライバシーの確保と規制遵守（27%）、データ損失とデータ流出（29%）、信頼できる接続性とデータ転送の確保（23%）と回答。

主な調査結果（アジア太平洋地域）

- **生成 AI に関するプライバシーとデータセキュリティの懸念:** IT 意思決定者の 57%が、生成 AI クラウドセキュリティにおけるプライバシーとデータ セキュリティに対して懸念を抱いています。
- **クラウドおよびエッジセキュリティインシデントの多発:** 過去 12 か月間に 64%のチームがクラウド、62%がエッジのセキュリティインシデントを確認しており、APAC 地域におけるセキュリティの課題が広範であることが浮き彫りになっています。
- **クラウド移行に対する条件付き意欲:**データの安全性が保証されれば、より多くのワークロードをクラウドまたはエッジに移行する意欲が高く、特に中国（97%）、インドネシア（94%）、インド（93%）、シンガポール（90%）の回答者がクラウド、およびエッジ以降に意欲を示しています。しかし、この意欲は強力なセキュリティ対策が条件となっており、セキュリティがこの地域でのクラウド採用拡大における重要な課題であることが明らかです。なお、日本（53%）はアジア太平洋地域内で明らかに例外的な回答となり、同地域でのクラウド移行は保守的である傾向が見られます。

- **ランサムウェア攻撃に関する最大の懸念:** 回答者の 34%が、セキュリティ上の最大の懸念としてランサムウェア攻撃を挙げており、次いでゼロデイ脆弱性を悪用した攻撃(27%)、クラウド内での機密データのアクセスに対する可視性管理（23%）が続いています。
- **サプライチェーンセキュリティに注力：**IT 意思決定者の 4 人に 1 人（24%）が、ソフトウェア部品表（SBOM）の深さ／品質／セキュリティ（24%）が、今後 1 年間で優先度を増すと考えています。IT 意思決定者の 33%が、セキュリティを強化するためにソフトウェアサプライチェーンの見直しを検討しています。

SUSE Japan のカントリーマネージャーである村上督（むらかみただし）は、このレポート結果について次のようにコメントしています：日本政府は、世界で最も AI フレンドリーな国になるという考えを表明し、AI テクノロジーで起きている急速な変化に非常に敏感に反応しています。しかし、SUSE の最新レポートが浮き彫りにしているように、生成 AI やエッジコンピューティングなどの新しいテクノロジーは、日本の企業にとって、特にデータとサプライチェーンの実証に関する新たなセキュリティ上の課題を生み出しています。多くの業界で AI が大きな影響を与える可能性がある中、SUSE は、このような状況におけるセキュリティについて、インシデントが「いつ」起こり得るかではなく、「どのように」起こり得るかという問題として再考することを推奨します。SUSE は、この新しいデジタル環境における回復力を確保するために、カスタマイズされたオープンソースソリューションで企業をサポートすることに引き続き注力します。オープンソースを活用することで、企業は、イノベーションを促進するダイナミックな新技術を取り入れながら、クラウドセキュリティの実践を保護し、前進させるための最前線に立つことができます。

トレンドレポートの結果は、ランサムウェア攻撃の脅威、生成 AI に関連するプライバシーとデータの問題、AI を活用したサイバー攻撃など、クラウドおよびエッジ テクノロジーの導入において APAC 諸国が直面している独特で多様なセキュリティ上の課題を明らかにしています。

SUSE による「Securing the Cloud」トレンドレポート全文は、こちらからご覧いただけます。

SUSE について：

SUSE は、SUSE Linux Enterprise、Rancher、NeuVector など、革新的で信頼性が高く、セキュアなエンタープライズオープンソースソリューションのグローバルリーダーです。Fortune 500 企業の 60%以上が、ミッションクリティカルなワークロードの構築に SUSE を利用しており、データセンターからクラウド、エッジ、そしてその先に至るまで、SUSE はあらゆる場所でのイノベーションを可能にします。SUSE は、オープンソースに "オープン "を取り戻し、パートナーやコミュニティと協力して、お客様がイノベーションの課題に取り組むための俊敏性と、戦略やソリューションを進化させるための自由を提供します。詳細については、www.suse.com でご確認ください。

【本件に関する報道関係お問い合わせ先】

株式会社ビーコミ SUSE 広報担当：石井・加藤

携帯：090-8844-9057 Email：pr[at]b-comi.co.jp