情シスだってラクしたい！
Amazon EC2 を守る、Trend Micro Cloud One – Workload Security

トレンドマイクロ株式会社

クラウドセキュリティ普及のための取り組み

トレンドマイクロはアマゾン ウェブ サービス ジャパン社（AWS）と ともに
クラウド環境のセキュリティ啓蒙活動に取り組んでいます

★ クラウド環境の脅威に関する情報発信･学習機会の提供

★ クラウドセキュリティのベストプラクティス・考え方を発信

トレンドマイクロは法人組織のセキュリティイノベーション推進を支援する
組織を設立し、セキュリティの啓蒙に努めています

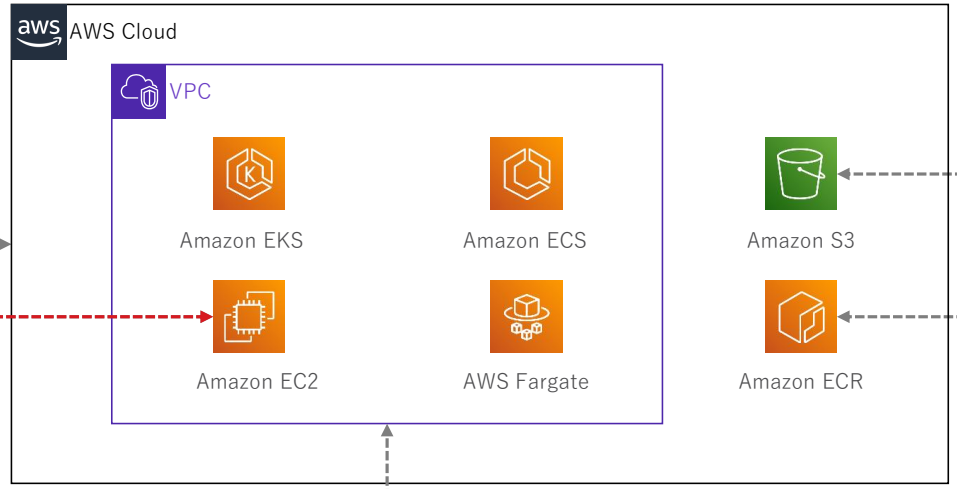
★ サイバーセキュリティ・イノベーション研究所設立

- トレンドマイクロ製品･サービスの安全性評価
- 役割に適したセキュリティ教育の提供
- 専門性の高い脅威分析と、その結果の公開

トレンドマイクロは多様なクラウド環境にセキュリティを提供

AWS上の設定不備を可視化、
コンプライアンス対応支援

Trend Micro Cloud One –
Conformity



Amazon S3の
不正プログラムスキャン

Trend Micro Cloud One –
File Storage Security

クラウドワークロード、
およびコンテナの保護

Trend Micro Cloud One –
Workload Security

AWS環境向け
ネットワーク型IPS

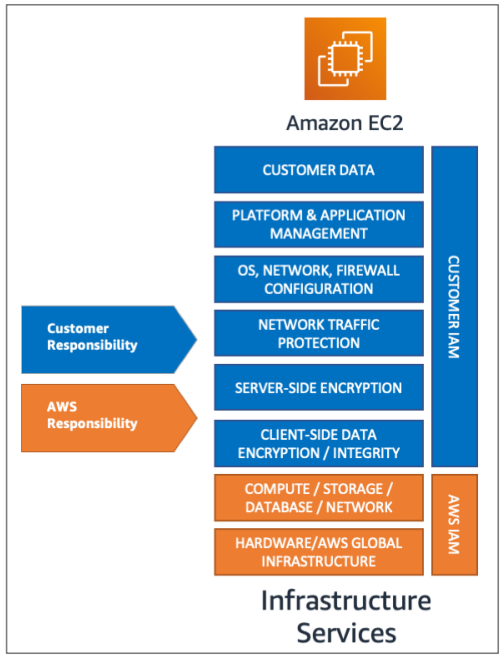
Trend Micro Cloud One –
Network Security

コンテナイメージのスキャンと
ランタイム保護

Trend Micro Cloud One –
Container Security

AWS環境のセキュリティ検討時に責任共有モデルの理解は必須

利用するサービスによって、ユーザ側の責任範囲は変動
Amazon EC2の場合、ゲストOSに対する脆弱性管理もユーザの責任範囲



インスタンスへのネットワークアクセスの制御

インスタンスへの接続に使用する認証情報の管理

ゲストOSとゲストOS上にデプロイされたソフトウェアの管理（脆弱性へのパッチ適用など）

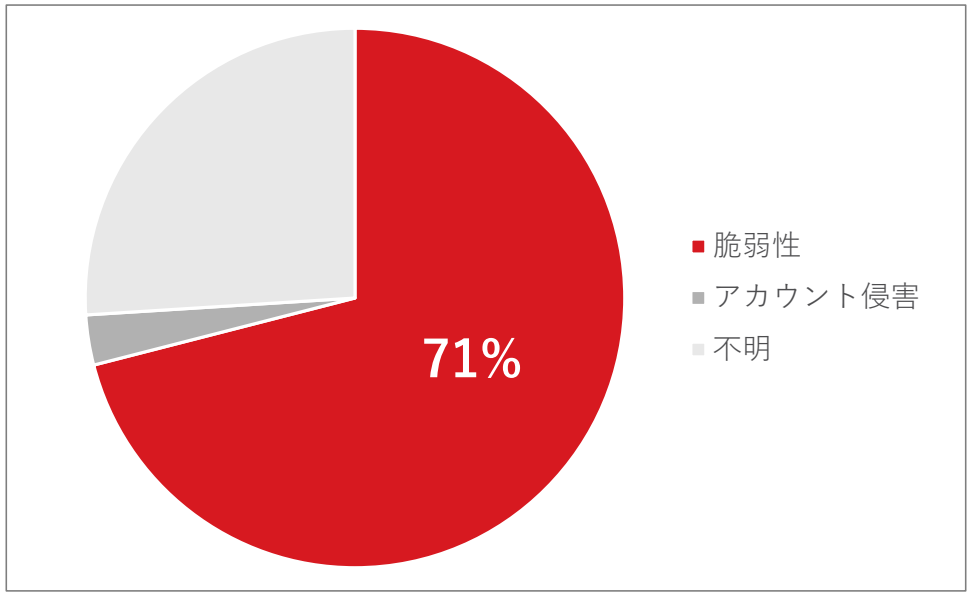
インスタンスにアタッチされたIAMロールと、それらのロールに関連付けられたアクセス許可の設定

出典：Amazon Web Services ブログ、2021年、アマゾン ウェブ サービス、 https://aws.amazon.com/jp/blogs/news/applying-the-aws-shared-responsibility-model-to-your-gxp-solution/
参考：Amazon EC2におけるセキュリティ、アマゾン ウェブ サービス、 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-security.html

脆弱性って、そんなに危ないんですか…？

情報漏えい事例のうち、71%は脆弱性が原因

前年度と比較すると、事例1件あたりの漏えいした情報量は約13倍に増加
脆弱性を放置すると、情報漏えいをはじめとする深刻な被害をもたらす可能性も…

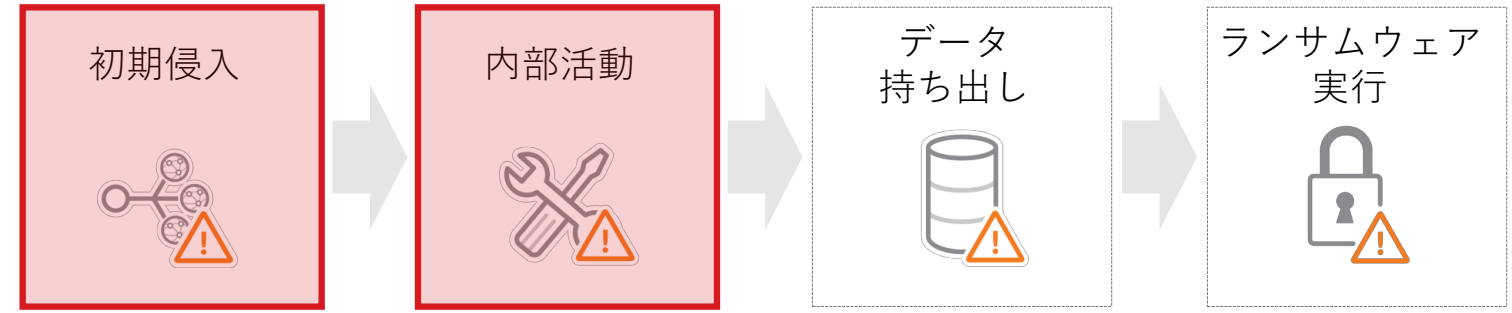


Web/クラウドからの情報漏えい事例における事故原因割合(2022/1 – 2022/6)(n=38件)

出典：2022年上半期サイバーセキュリティレポート、2022年、トレンドマイクロ、
https://resources.trendmicro.com/rs/945-CXD-062/images/m506-2022年上半期サイバーセキュリティレポート.pdf

ランサムウェアの攻撃でも脆弱性の悪用を確認

最近はクラウド環境でもランサムウェアの被害が発生
初期侵入やシステム内部での探索・拡散に脆弱性が悪用されるケースも存在



ターゲットの組織情報を
事前に調べて
脆弱な箇所から侵入

ネットワーク内部の
情報を掌握し
高い権限を獲得

奪取した権限で
脅迫用のデータを
持ち出し

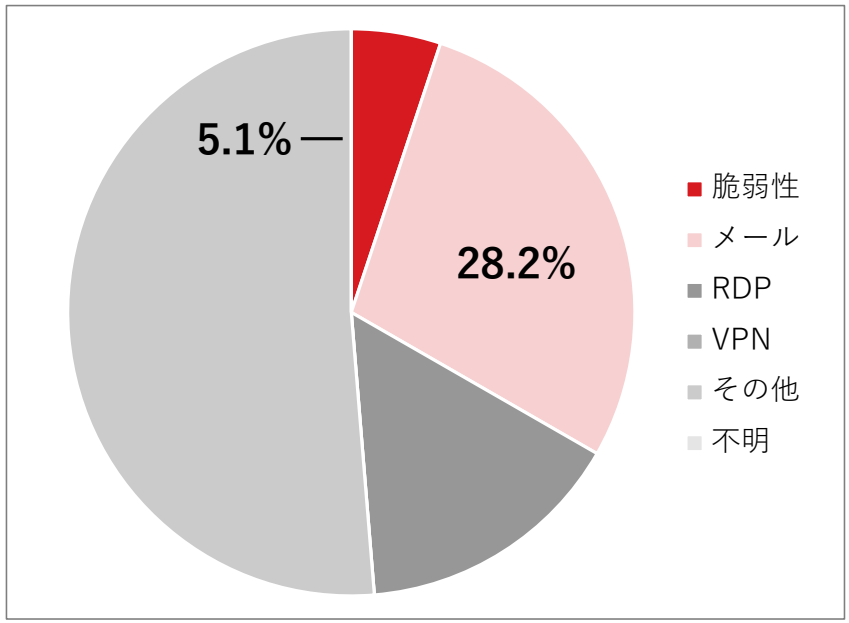
セキュリティ製品を
停止後に組織内に
ランサムウェアを展開

ターゲットの環境へ侵入後、様々な攻撃手法を駆使して対話的に侵害範囲を拡大

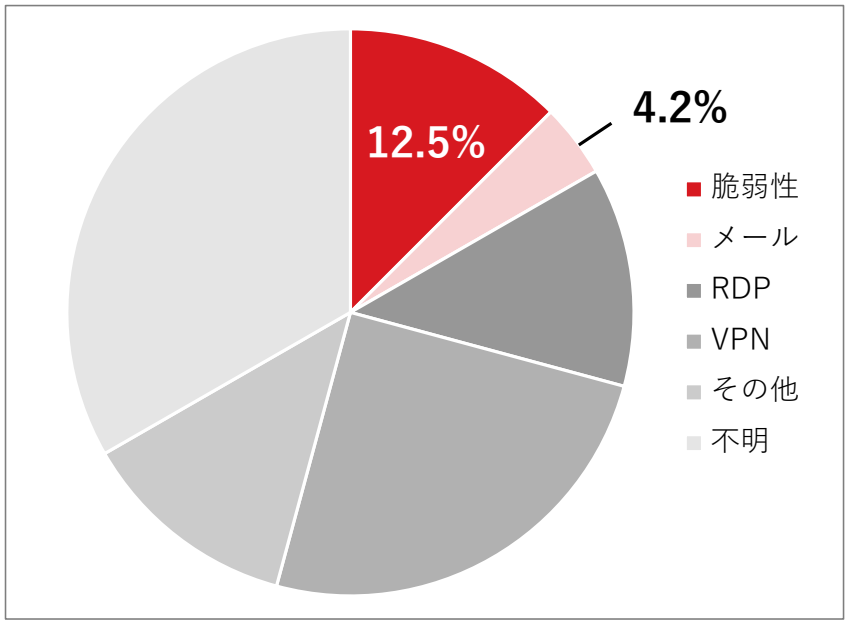
出典：最新の被害事例の傾向から学ぶ「ランサムウェアの攻撃パターン」、2022年、トレンドマイクロ、
https://www.trendmicro.com/ja_jp/jp-security/22/g/securitytrend-20220701-01.html

初期侵入における脆弱性の悪用が増加

脆弱性を悪用して侵入するケースは5.1%→12.5%に増加
逆にメールを悪用した侵入は28.2%→4.2%に減少



トレンドマイクロのインシデント対応支援で確認された侵入経路の割合
(2019/1 – 2020/12)

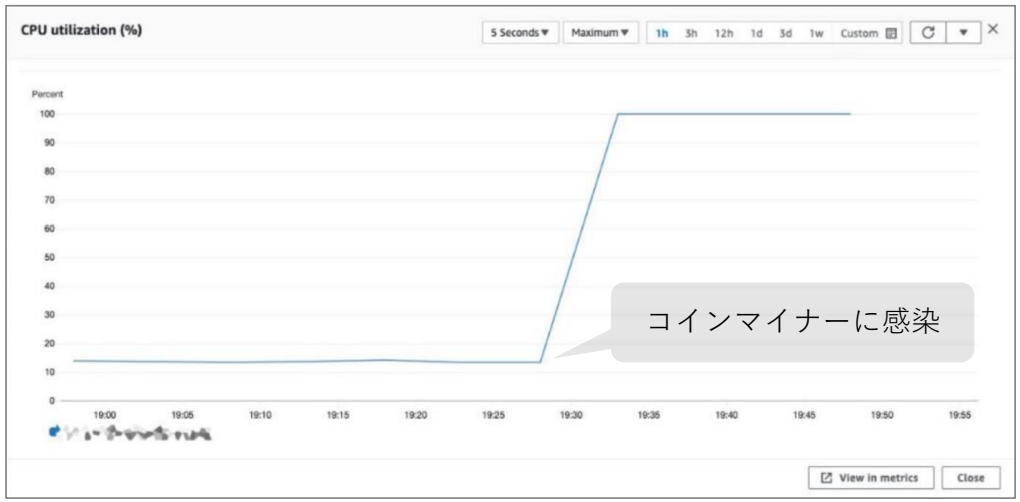


トレンドマイクロのインシデント対応支援で確認された侵入経路の割合
(2021/1 – 2022/6)

出典：トレンドマイクロのインシデント対応支援情報をもとに作成

コインマイナーの攻撃でも脆弱性の悪用を確認

企業のクラウド利用に合わせてクラウド環境でのコインマイナーの被害も増加
脆弱性を抱えた端末からシステム内に感染が拡散



CPU 使用率の急上昇を示すダッシュボード画面

CPUの負荷高騰による
ダウンタイムの発生
(調査用端末では13%→100%)

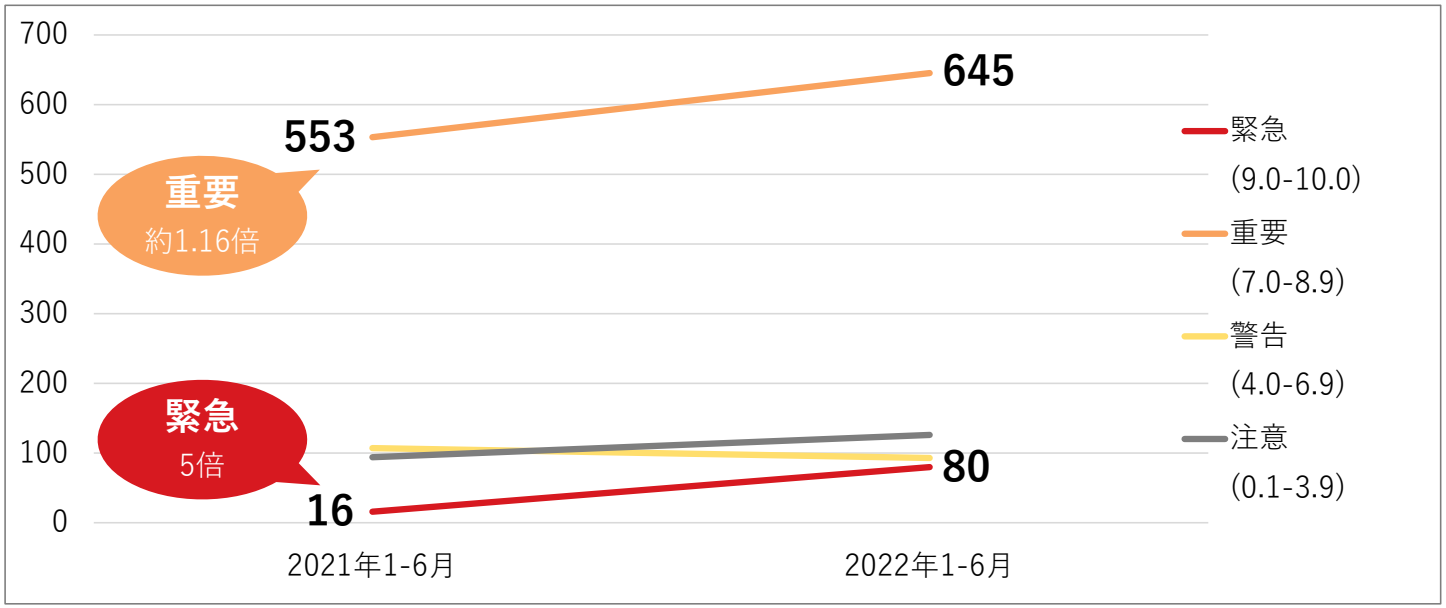
インスタンスの稼働率上昇による
運用コスト増
(調査用端末では$20→$130)

Linux環境を標的にした
コインマイナーが増加
(Linuxにおける検出数は8,240→13,228)

出典：浮遊する戦場―クラウドを狙う暗号資産マイニング活動の脅威、2022年、トレンドマイクロ、
https://resources.trendmicro.com/rs/945-CXD-062/images/浮遊する戦場―クラウドを狙う暗号資産マイニング活動の脅威.pdf
出典：2022年年間サイバーセキュリティレポート、2023年、トレンドマイクロ、
https://resources.trendmicro.com/rs/945-CXD-062/images/ m558-2022年年間サイバーセキュリティレポート.pdf

脆弱性の発見数は増加傾向

新たに発見される緊急/重要/注意レベルの脆弱性が増加
脆弱性の放置はリスクを伴うため、早期対処が必要

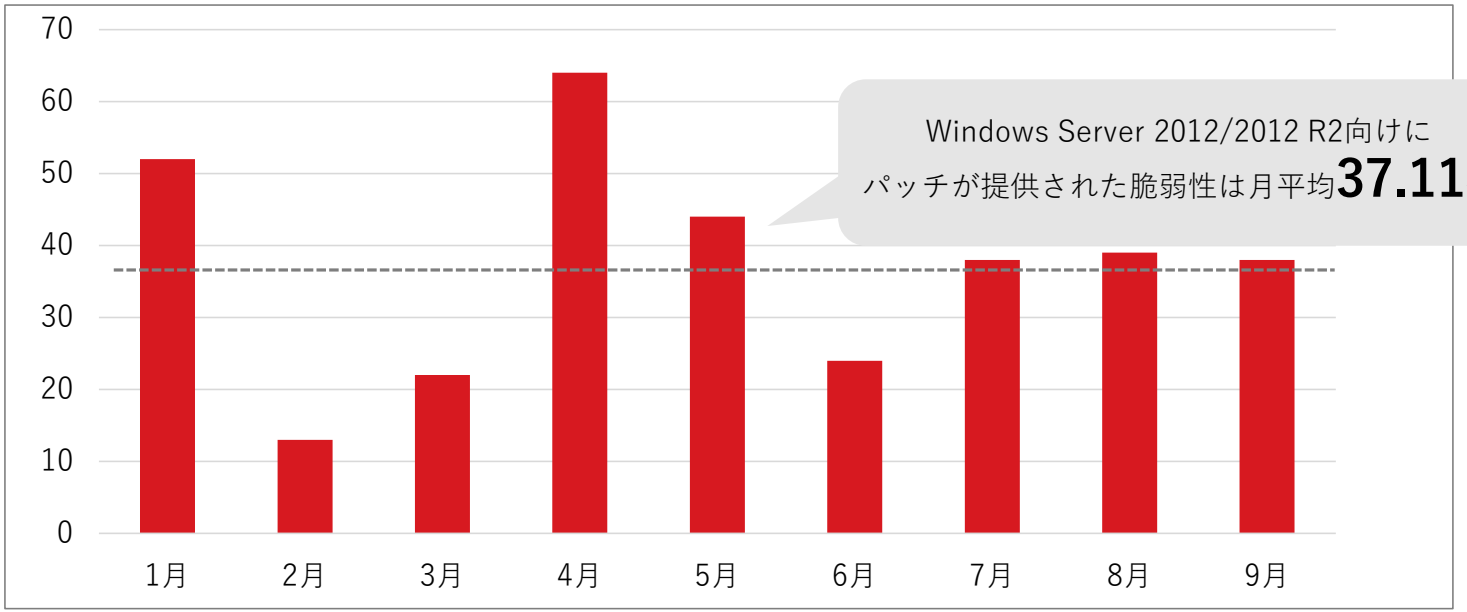


2021 年上半期と2022 年上半期にZDIより公表された脆弱性のCVSSに基づく深刻度別内訳

出典：2022年上半期サイバーセキュリティレポート、2022年、トレンドマイクロ、
https://resources.trendmicro.com/rs/945-CXD-062/images/m506-2023年上半期サイバーセキュリティレポート.pdf

脆弱性を修復するためのパッチの提供数も増加傾向

リリースから10年以上経過したWindows Server 2012/2012 R2向けのパッチに絞っても
パッチが提供されない月は存在しない



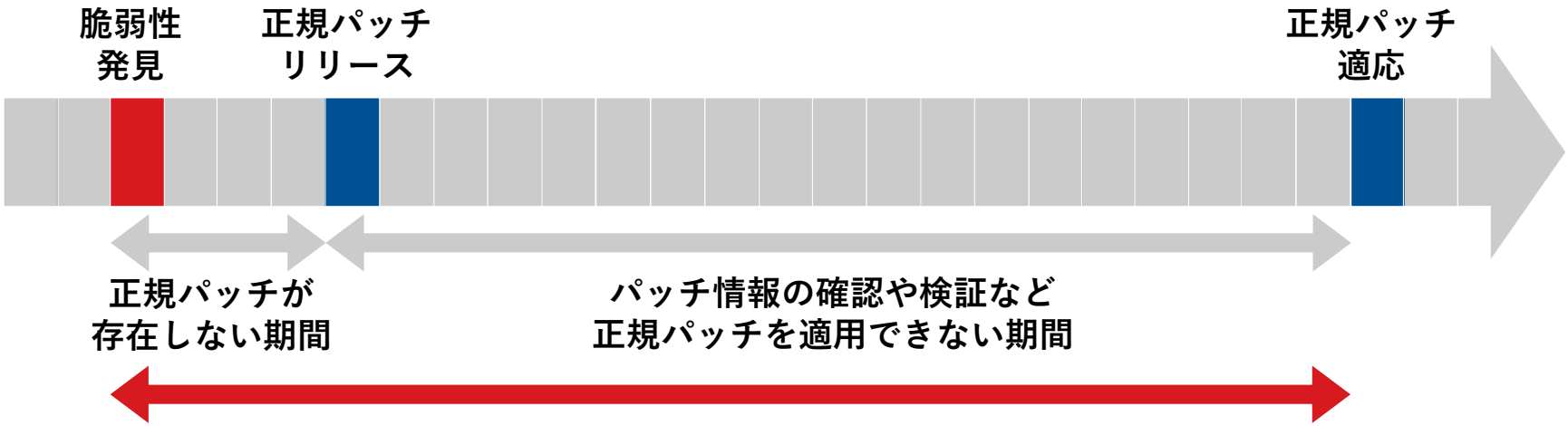
セキュリティ更新プログラム内で
Windows Server 2012/2012 R2向けにパッチが提供された脆弱性件数(2022/1 – 2022/9)

参考：セキュリティ更新プログラム ガイド、2022年、マイクロソフト株式会社、https://msrc.microsoft.com/update-guide/ja-jp

パッチ適用、大変じゃないですか…？

脆弱性対策の基本と課題

脆弱性対策の基本は、ベンダーが提供する正規の修正プログラム(=パッチ)の速やかな適用
ただし実際の運用では実現が難しいケースも存在



正規パッチを適用できない 「セキュリティの空白期間」

「セキュリティの空白期間」をいかに短くするかが重要

セキュリティの空白期間を守る『仮想パッチ』

暫定的なセキュリティを担保するためにソフトウェアベンダーが提供するセキュリティ機能
正規のパッチを早急に適用する事が難しい環境の一時的な保護を支援

脆弱性自体の
修正はできない

IPSルールで攻撃を
検知・ブロック

IPSルールで脆弱性を狙う攻撃パケットを
ネットワークレベルで検知・ブロック

ソフトウェアの脆弱性自体は残るが
ネットワーク経由の攻撃には対処可能

ネットワークレベルで対処するため
稼働中のサービスへの影響が少ない

要注意：仮想パッチは脆弱性そのものを修復する機能ではない

仮想パッチはあくまでも『暫定的な』脆弱性対策
ネットワーク経由の攻撃は対応可能だが、ローカル上で完結する攻撃をはじめ対応不可なものも存在

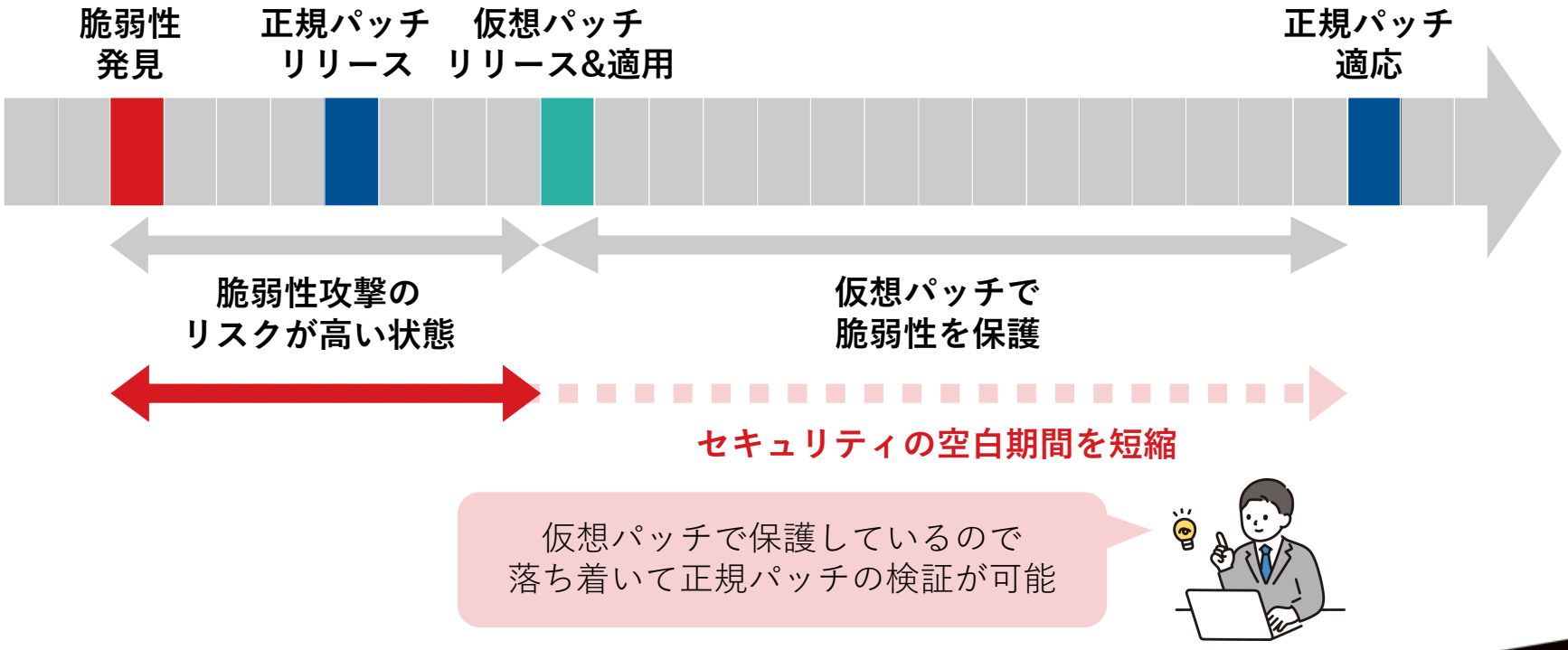
脆弱性を**放置**した状態

仮想パッチを適用した状態

正規パッチを適用した状態

『仮想パッチ』でセキュリティの空白期間を短縮

脆弱性対策の基本は、ベンダーが提供する正規の修正プログラム(=パッチ)の速やかな適用
正規パッチの適用まで、仮想パッチで脆弱性を狙う攻撃をブロック



仮想パッチで保護しているので
落ち着いて正規パッチの検証が可能

脆弱性対策・パッチ運用をラクにする
Trend Micro Cloud One – Workload Security™

クラウドセキュリティはまとめてシンプルに！ Trend Cloud One™

Trend Cloud One™

- Workload Security

クラウドワークロードおよびコンテナの保護


Amazon Elastic Compute Cloud (Amazon EC2)


Amazon Elastic Container Service (Amazon ECS)


Amazon Elastic Kubernetes Service (Amazon EKS)


AWS Elastic Beanstalk

- File Storage Security

クラウドストレージの不正プログラムスキャン


Amazon Simple Storage Service (Amazon S3)

- Conformity

クラウドの設定不備を可視化、コンプライアンス対応支援

AWS Cloud

- Network Security

クラウド向けネットワークIPS


Amazon Virtual Private Cloud (Amazon VPC)

- Container Security

コンテナイメージのスキャンとランタイム保護

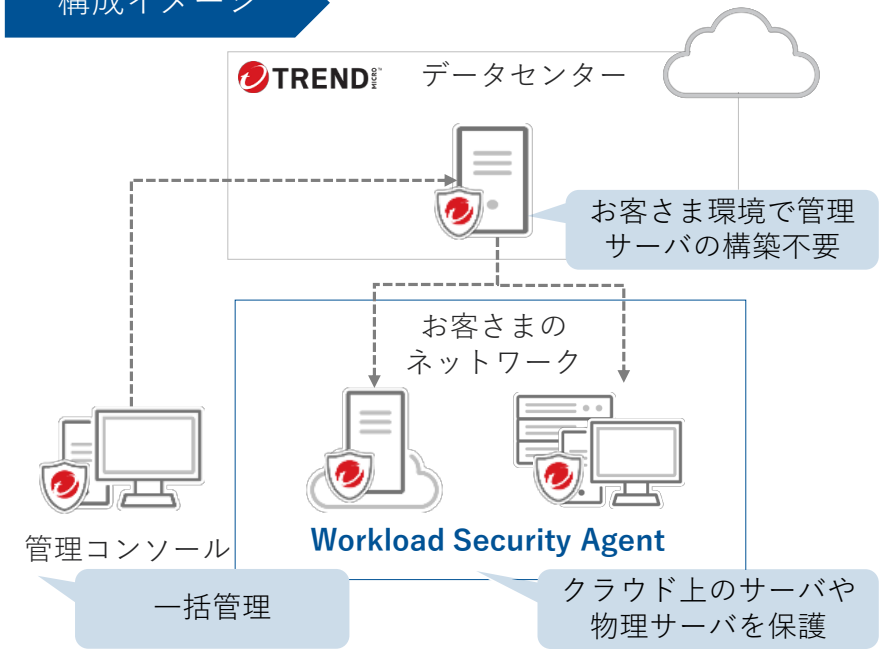

Amazon Elastic Container Registry (Amazon ECR)


Amazon Elastic Kubernetes Service (Amazon EKS)

Trend Micro Cloud One – Workload Security（以下、Workload Security）

クラウド上のサーバにAgentをインストールすることで脆弱性対策や多層防御を提供
トレンドマイクロが管理サーバは提供するため、お客さまの管理サーバ構築は不要

構成イメージ



特徴

- 管理サーバの構築・運用が不要
- サーバ保護に必要な複数の機能を単一Agentに搭載

提供機能

- Agentをインストールしたサーバに下記機能を提供、サーバの多層防御・脆弱性対策を実現
  - 不正プログラム対策
  - **IPS/IDS(侵入防御) ➡ 仮想パッチ**
  - Webレピュテーション
  - ファイアウォール
  - アプリケーションコントロール
  - 変更監視
  - セキュリティログ監視
    アクティビティ監視(EDR/XDR)

脆弱性対策・パッチ運用をラクにする『仮想パッチ』

トレンドマイクロは世界最大級の脆弱性発見コミュニティを運営
そのナレッジを活かして、Workload SecurityはAmazon EC2に対して仮想パッチを提供

脆弱性自体の
修正はできない

IPSルールで攻撃を
検知・ブロック

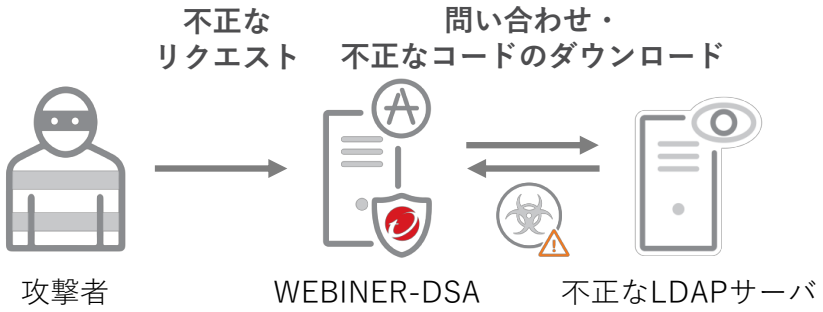
IPSルールで脆弱性を狙う攻撃パケットを
ネットワークレベルで検知・ブロック

ソフトウェアの脆弱性自体は残るが
ネットワーク経由の攻撃には対処可能

ネットワークレベルで対処するため
稼働中のサービスへの影響が少ない

仮想パッチのデモ

デモ環境のイメージ



Log4jがリクエストに対してログ出力
JNDI Lookup機能がリクエストを処理

Cloud One – Workload Securityを
「WEBINER-DSA」にインストール済み

IPS/IDS機能の利用あり/なしの
両パターンで不正なリクエストを送信

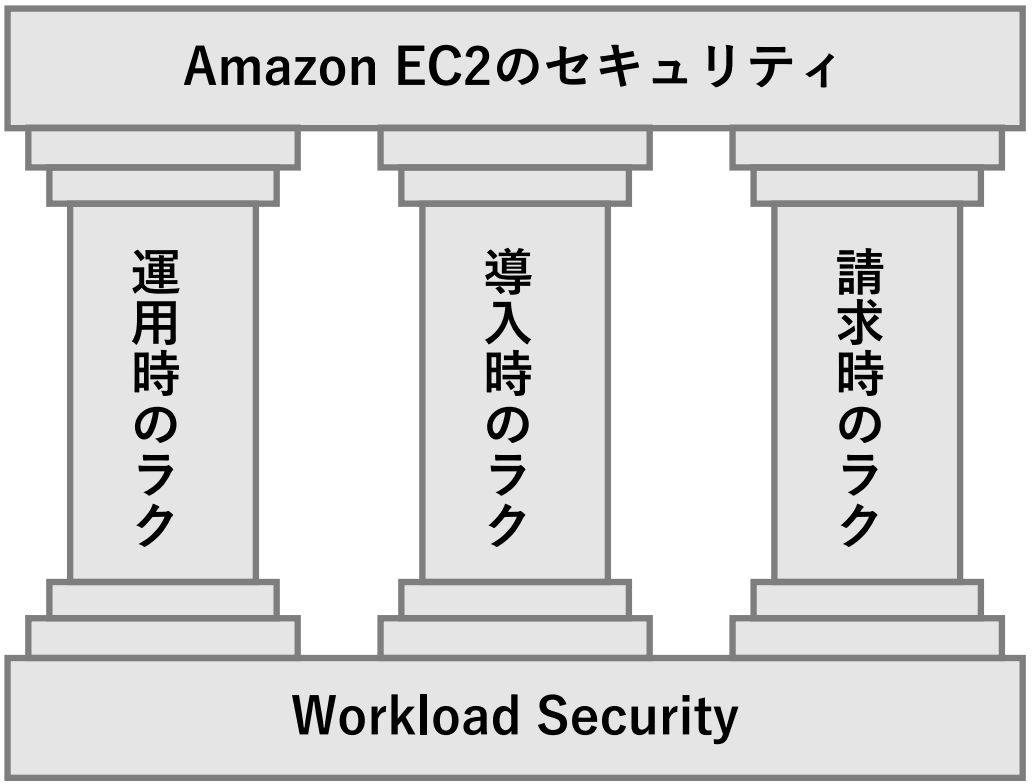
不正なリクエストは
難読化したものを利用

デモの流れ

設定内容の確認 → 不審なリクエスト送信 → IPS有効化 → 不審なリクエスト送信

※イベント当日はデモを実施しました

Workload Securityは仮想パッチ以外の『ラク』も提供



セキュリティ製品の運用をラクにする『多層防御』

Workload Securityはサーバに必要な複数のセキュリティを機能を1製品で提供
複数のセキュリティ製品を運用する負荷の軽減を支援

ランサムウェアの
攻撃の流れ

社外公開された脆弱性の悪用	Workload Security
システム内部の探索	Workload Security
システム内部の脆弱性の悪用	Workload Security
不正プログラムの持ち込み	Workload Security
不正プログラムの実行	Workload Security
データの持ち出し	Workload Security
ランサムウェアの実行	Workload Security

**攻撃手法ごとに
セキュリティ製品を導入すると
管理や運用負荷が増加する**

**1製品で複数の
セキュリティ機能を提供する
「多層防御」が有効**

Agentインストールをラクにする『Auto-Scaling対応』

Workload SecurityはAuto-Scalingで増加したインスタンスに対して
Agentのインストールとあらかじめ設定されたセキュリティポリシーを自動的に適用

インストールスクリプトで
ポリシー適用まで自動化

Auto-Scalingで増加したインスタンスも
自動で保護

管理マネージャ

常時起動分

Auto-Scaling後の増加分

クラウド環境の柔軟性の例：オートスケーリング機能

クラウドリソースの稼働状況や設定に応じて、自動的にクラウドリソースを増減し、
アプリケーションのパフォーマンスを最適化する機能

請求をラクにする『支払方法の統合』

Workload Securityはライセンス購入以外にAWS Marketplace経由の従量課金でも利用可能
AWS Marketplace経由の場合、Workload Securityの請求はAWSの請求に統合

従量課金

<課金条件>
インスタンスサイズ×利用機能×
Agentの稼働時間

<支払いサイクル>
月払い
(請求はAWSやAzureの請求に一本化)

<お奨めの利用シーン>
リソースの増減が想定されるシステム
(例：ECサイト用サーバ/サービス基盤のサーバ)

ライセンス購入

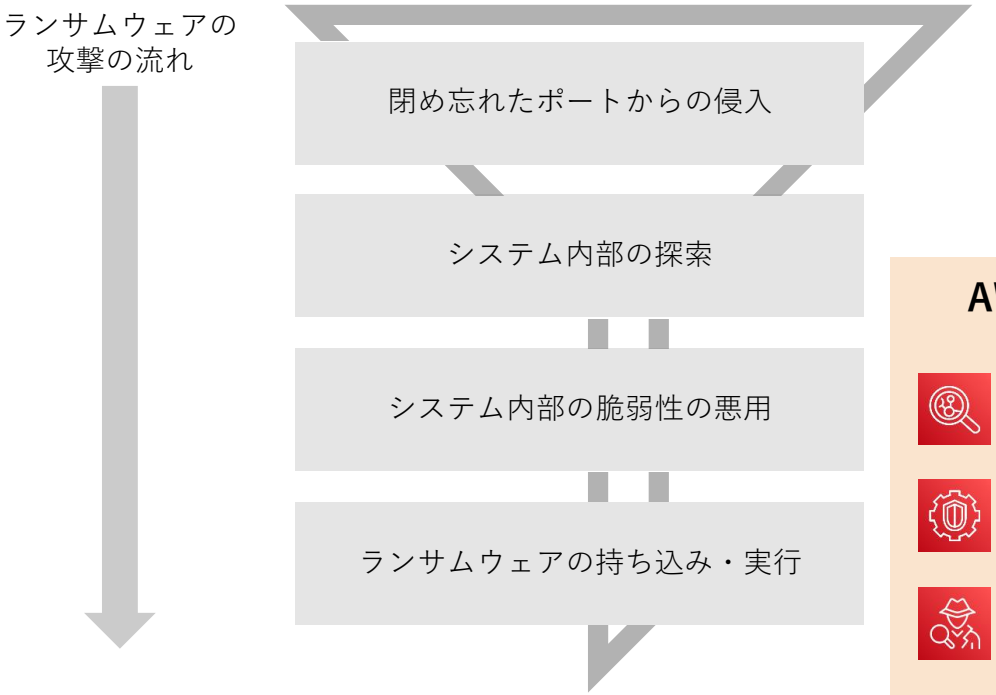
<課金条件>
利用機能×Agent数

<支払いサイクル>
年払い
(初年度はライセンス費用/2年目以降は更新費用)

<お奨めの利用シーン>
インスタンスの増減が少ないシステム
(例：社内業務用サーバ)

AWSサービスとWorkload Securityは併用が有効

AWSのセキュリティサービスを活用しつつ、
Workload Securityを組み合わせることでより効果的な対策を実現



AWSサービスは検知を提供

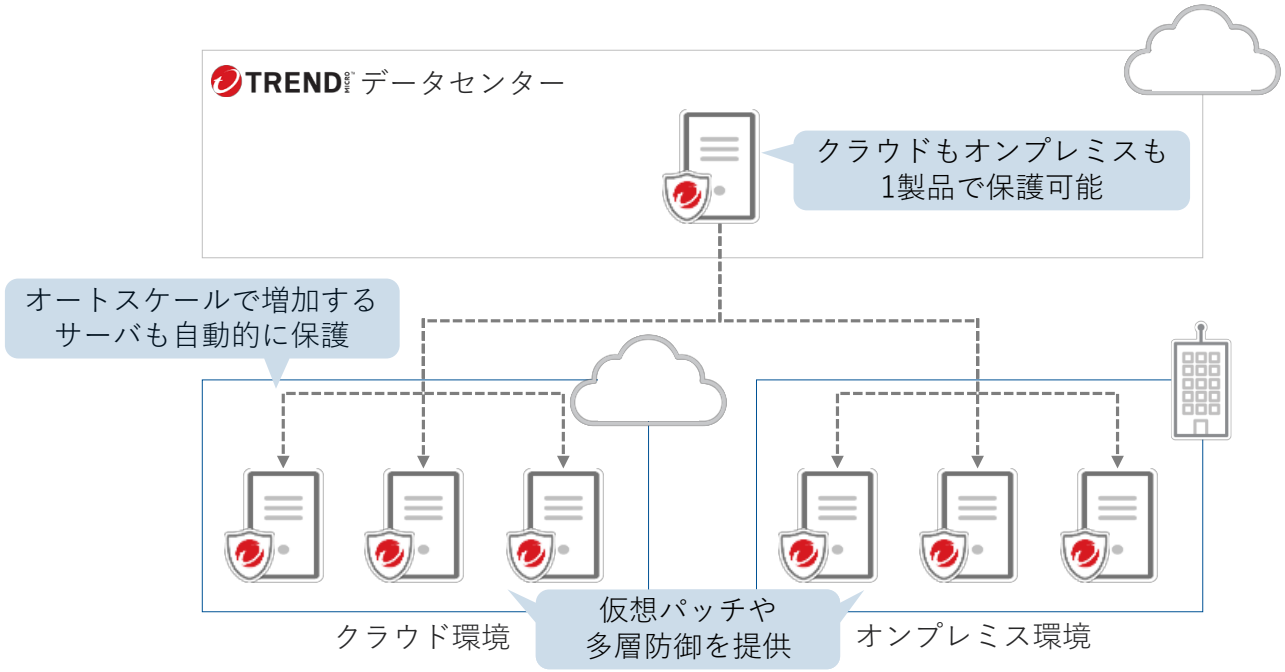
- Amazon Inspector
- Amazon GuardDuty
- Amazon Detective

Workload Securityは防御と検知を提供

- 不要ポートのブロック
- ログイン失敗の検知
- ポートスキャンの検知
- 脆弱性攻撃のブロック
- 不正プログラムの削除
- 一連の攻撃行動の可視化

おまけ：ハイブリッドクラウドのセキュリティをラクにする『オンプレミス対応』

Workload Securityはクラウド以外にオンプレミスの物理サーバや仮想サーバにも保護を提供
ハイブリッドクラウド環境のセキュリティレベルの統一や運用効率の向上を支援



まとめ：Amazon EC2のセキュリティをラクにするには？

クラウド環境であっても**脆弱性対策**は必須
ランサムウェアやコインマイナーも脆弱性を悪用

脆弱性対策には**仮想パッチ**
他に**クラウドの柔軟性を損ねない**ことも重要

クラウドの柔軟性を損わないセキュリティは
Trend Micro Cloud One – Workload Security

* 弊社製品、および他社製品に関する記載は、2023年6月時点の情報をもとに作成しています。
* 一部弊社環境での検証に基づく内容も記載していますが、お客様環境で同様の動作を保証するものではありません。