トレンドマイクロ ホワイトペーパー

AWS 環境の公開サーバに対するセキュリティ検討ガイド

Version 1.1

» 本ガイドは、AWS 上でサーバを構築済み、あるいは構築を予定・検討しているユーザが、
AWS 上に公開サーバを構築する上で知っておくべきセキュリティ対策のポイントと
トレンドマイクロが推奨する対策方法についてご紹介します。
なお、本ガイド内の解説では、公開サーバの構築に Amazon EC 2[1] を利用することを前提としています。

目次

1 はじめに

近年ではクラウドを利用して公開サーバを構築するだけでなく、人事・会計等の業務システム用のサーバをクラウドで構築する企業も増えてきました。

サーバをクラウドで構築するためのサービスである IaaS（Infrastructure as a Service）市場においては、特にアマゾン ウェブ サービス（以下、AWS）が市場のシェアを大きく占めております。ユーザは AWS を利用することで、数分で手軽にサーバを立ち上げることが可能となりました。しかし、その手軽さ故に、セキュリティに関して十分な検討・対策が施されないまま、公開サーバが構築されてしまうことがあります。

本ガイドは、AWS 上でサーバを構築済み、あるいは構築を予定・検討しているユーザが、AWS 上に公開サーバを構築する上で知っておくべきセキュリティ対策のポイントとトレンドマイクロが推奨する対策方法についてご紹介します。なお、本ガイド内の解説では、公開サーバの構築に Amazon Elastic Compute Cloud (以下、Amazon EC2) [1]を利用することを前提としています。

2 AWS が提供するセキュリティモデル

AWS が提供するクラウドサービスは、AWS とユーザそれぞれの責任範囲を明確に分けた「責任共有モデル [2]」が基になっています。まずは、この責任共有モデルと AWS 上に公開サーバを構築する場合のセキュリティ対策ポイントについて解説します。

2.1 責任共有モデルとセキュリティについて

AWS の提唱する、責任共有モデルとは、AWS とお客様がセキュリティとコンプライアンスに関して共同で責任を持つという考え方です。
AWS は、AWS クラウドで提供されるインフラストラクチャの保護について責任を負います。このインフラストラクチャはハードウェア、ソフトウェア、ネットワーキング、AWS クラウドのサービスを実行する施設などが挙げられます。対して、お客様の責任は、選択した AWS クラウドのサービスに応じて異なります。本ホワイトペーパーで取り上げる、Amazon EC2 などのサービスは Infrastructure as a Service (IaaS) に分類されているため、必要なすべてのセキュリティ構成および管理のタスクをお客様が実行する必要があります。

AWS 上で公開サーバを構築する場合を、この責任共有モデルに照らし合わせ、レイヤ毎に考えると、ネットワーク、仮想インフラ等の公開サーバが動くための基本的なインフラレイヤに対しては AWS が責任を持ち、そうしたインフラ上で動くゲスト OS、ミドルウェア、Web アプリケーションについては全てユーザが責任を持つことになります。

[1] https://aws.amazon.com/jp/ec2/
[2] https://aws.amazon.com/jp/compliance/shared-responsibility-model/

図１： AWS の責任共有モデル

このようにレイヤごとに見ると、AWS の責任範囲、ユーザの責任範囲ははっきりと分かれています。しかし、セキュリティの観点から気を付けなければいけないのは、AWS の責任範囲の中で提供されているセキュリティ機能に関しても、その“設定”はユーザ自身が実施しなければならない点です。この点を考慮して、AWS とユーザの責任範囲におけるセキュリティをそれぞれ見ていきましょう。

AWS の責任範囲におけるセキュリティ

レイヤで見ると AWS の責任範囲は、「ネットワークインフラ」、「仮想化基盤」です。この範囲に該当するネットワークセキュリティはとても重要です。AWS はネットワークセキュリティを実現する機能として、例えば、ファイアウォール機能である「セキュリティグループ」というサービスを提供しています。セキュリティグループを利用することで、関連付けられた Amazon EC2 インスタンスのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をインスタンスレベルでコントロールすることが可能となります。しかし、こうした“設定”はユーザがしなければならず、ユーザが誤って不要なポートを空けた設定をした場合などは、セキュリティレベルが保てなくなってしまうため注意が必要です。

ユーザの責任範囲におけるセキュリティ

AWS 上で動くゲスト OS、その OS 上で動くミドルウェアや Web アプリケーションといった仮想マシンのセキュリティはユーザの責任です。ゲスト OS のファイアウォール設定、OS やミドルウェアのパッチ適用、アクセス管理等全てを実施しなければなりません。また、それだけでなく、ウイルス対策、Web アプリケーションファイアウォール（WAF）、IPS（侵入防御）といった対策によるセキュリティ強化も必要となるでしょう。こうしたセキュリティ強化に対して、AWS からは Web アプリケーションファイアウォール「AWS WAF[3]」が提供されています。AWS 上で公開サーバを構築する場合は、「AWS WAF」の導入を検討することをお勧めします。

[3] https://aws.amazon.com/jp/waf/

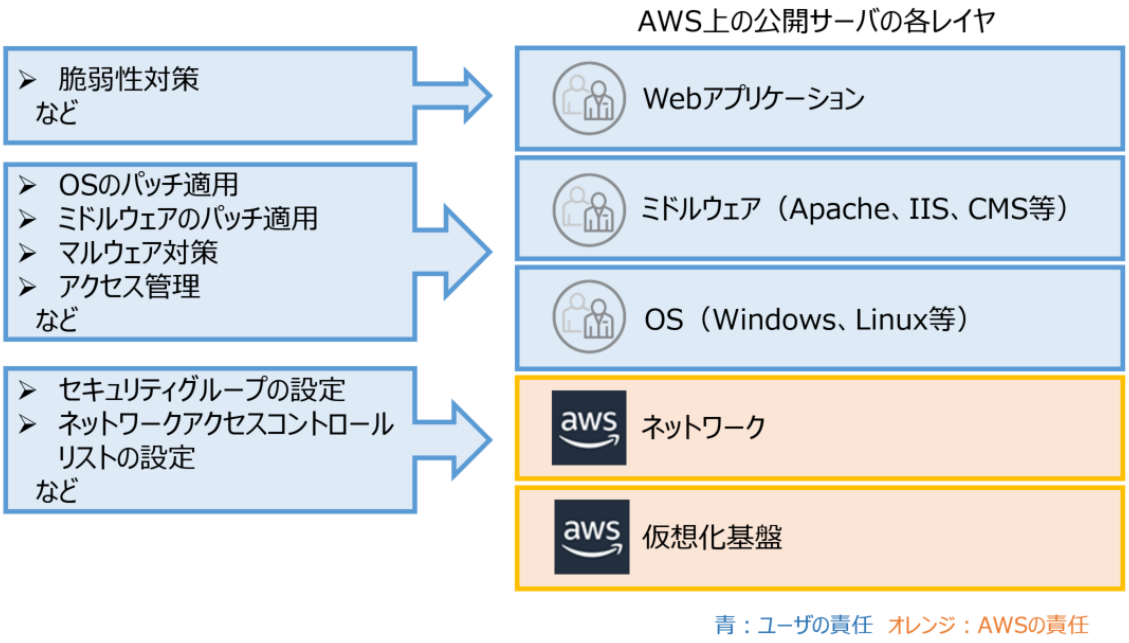

図２：ユーザが対応しなければならないポイント

2.2 検討すべきセキュリティ対策のポイント

AWS の責任共有モデルからも分かるとおり、AWS が提供するセキュリティ機能を導入したとしても、ユーザがセキュリティに対して負うべき責任がゼロになることはありません。よりシンプルに見ていくため、AWS 上の公開サーバを 4 つのレイヤで考えてみましょう。

図３： AWS 上の公開サーバの４レイヤ

この 4 レイヤでユーザがセキュリティ対策を検討すべきポイントは、「Web アプリケーション」、「ミドルウェア」、「OS」の 3 レイヤです。この 3 レイヤのうち、「Web アプリケーション」に対して AWS からは WAF のサービス「AWS WAF」が提供されており、このサービスを利用することで SQL インジェクションやクロスサイトスクリプティングのような一般的な攻撃に対する対策は可能になります。しかし、それだけでは「ミドルウェア」、「OS」の 2 レイヤに対するセキュリティ対策が不十分となるため、ユーザは別途セキュリティ対策の導入を検討する必要があります。

公開サーバのレイヤ	各レイヤへのセキュリティ対策
Web アプリケーション	AWS WAF を導入し、セキュリティルールを作成する必要がある。また、Amazon Cloud Front[4] を導入していない等、構築環境によっては AWS WAF を利用できない可能性がある
ミドルウェア	別途対策を導入する必要がある
OS	別途対策を導入する必要がある
ネットワーク	セキュリティグループなどによるアクセス制御

表 1 ： AWS 上の公開サーバに対するセキュリティ対策

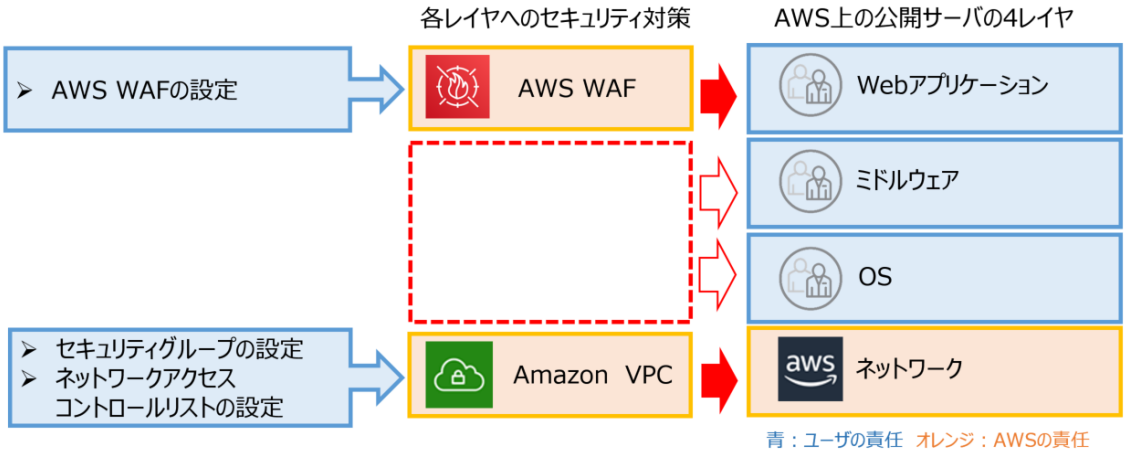

図 4 ： 検討すべきセキュリティ対策のポイント

[4] https://aws.amazon.com/jp/cloudfront

3 ミドルウェアの脆弱性と公開サーバに対する脅威

「ミドルウェア」や「OS」の対策については、別途ユーザが実施する必要があるのは前述のとおりですが、これらのレイヤにおいてはどのような脅威が存在するのでしょうか。

オンプレミス環境や AWS 環境を問わず、過去に公開サーバ上で動くミドルウェア等の脆弱性がサイバー犯罪者に狙われる事例が実際に確認されています。ここでは、ミドルウェアに着目して過去に見つかった深刻な脆弱性とその脆弱性を悪用した攻撃の活動について紹介します。

3.1 ミドルウェアで見つかる深刻な脆弱性

ミドルウェアにおいても、時に深刻な脆弱性が発見されています。実際に 2018 年～2019 年の 2 年間を振り返っても、Web アプリケーションフレームワークの Apache struts 2 や Word Press 等の CMS（コンテンツマネジメントシステム）を始めとする多くの Web サーバで利用されているミドルウェアの深刻な脆弱性が発見されています。ここでは、これまでに見つかった深刻な脆弱性とその脆弱性を悪用した攻撃の活動についてご紹介します。

登録時期	脆弱性	ソフトウェア	脆弱性の詳細
2019 年 5 月	CVE-2019-0232	Apache Tomcat	攻撃者は OS コマンドインジェクションを利用することで、任意のコマンドを実行することが可能となる。[※5]
2019 年 4 月	CVE-2019-8942 CVE-2019-8943	WordPress	これらの脆弱性を併用することで、「author（投稿者）」以上の権限を持った攻撃者が任意の PHP コードを実行しシステムを管理できるようになる。[※6]
2019 年 4 月	CVE-2019-0192	Apache Solr	安全でないデシリアライゼーションに関する深刻度“critical”の脆弱性。攻撃者はこの脆弱性を利用することで、Apache Solr サーバで遠隔から任意のコードを実行することが可能になる。[※7]

[5] https://blog.trendmicro.co.jp/archives/21195
[6] https://blog.trendmicro.co.jp/archives/20487
[7] https://blog.trendmicro.co.jp/archives/20755

2019 年 4 月	CVE-2019-6340	Drupal	Drupal のセキュリティチームが定義した 5 段階の中で最高の「Highly critical」に分類された。攻撃者はこの脆弱性を利用することで、認証無しに遠隔から任意のコードを実行することが可能となる。※8
2019 年 4 月	CVE-2019-2725	Oracle WebLogic Server	攻撃者はサーバの実行権限を利用することで任意のコードを実行することが可能となる。**パッチ公開前に攻撃コードが公開されたためゼロデイ攻撃が可能であったことに加えて、実際の攻撃の可能性を探索する活動も報告された。**※9
2018 年 6 月	CVE-2018-7602	Drupal	攻撃者はこの脆弱性を利用することで、遠隔から任意のコードを実行することが可能となる。**本脆弱性を利用した攻撃が実際に確認された。**※10
2018 年 8 月	CVE-2018-11776	Apache Struts2	深刻度“critical”の脆弱性。攻撃者はこの脆弱性を利用することで、遠隔から任意のコードを実行することが可能となる。また、**本脆弱性を利用した攻撃コードが公開されている。**※11

表 2 ： 2018 年から 2019 年に発見された公開サーバに関連するミドルウェアの脆弱性の例

上記の通り様々なミドルウェアにおいて深刻な脆弱性が発見されていることに加えて、攻撃コードの公開に留まらず脆弱性を悪用した攻撃が確認されている例もあることから、実際にこれらを悪用する脅威が存在していることがわかります。

こうした脆弱性は例年発見されており、脆弱性に対してベンダからリリースされるパッチを迅速に適用することが重要です。しかし、他のアプリケーション等の互換性によってパッチが適用できない場合や使用中のミドルウェアのサポートが終了し、ソフトウェアベンダからパッチが公開されなくなった場合には、そうしたセキュリティリスクを残したまま公開サーバを運用しなければなりません。そうしたセキュリティリスクを残した場合、公開サーバを攻撃されて情報漏えい等の深刻なセキュリティインシデントにつながる可能性があるため、IPS（侵入防御システム） などのセキュリティ対策を検討することをお勧めします。

[8] https://blog.trendmicro.co.jp/archives/20517
[9] https://www.ipa.go.jp/security/ciadr/vul/20190428_WebLogicServer.html
[10] https://blog.trendmicro.co.jp/archives/19266
[11] https://www.ipa.go.jp/security/ciadr/vul/20180823-struts.html

3.2 公開サーバを狙うサイバー攻撃

公開サーバを攻撃された事例は数多く報告されています。公開サーバを攻撃された結果、サイトを改ざんされ、自組織の Web サイトが脆弱性攻撃サイトへの誘導や不正プログラムの配布に意図せず加担してしまうケースや、顧客情報やクレジットカード情報等の漏えいといった大きな被害につながる可能性があります。実際にサイバー犯罪者は外部に露出している公開サーバを標的にしており、2019 年の 1 年間で公開サーバが攻撃を受けた被害の公表事例が 86 件公表されています。ここで注目すべきは、2019 年における事例のうち、約 52% が公開サーバにおけるシステムの脆弱性を悪用されていることです。他の割合では未公表または不明としている事例が大半を占めることから、多くのケースにおいて脆弱性が原因となり攻撃が成功していることが推測されます。

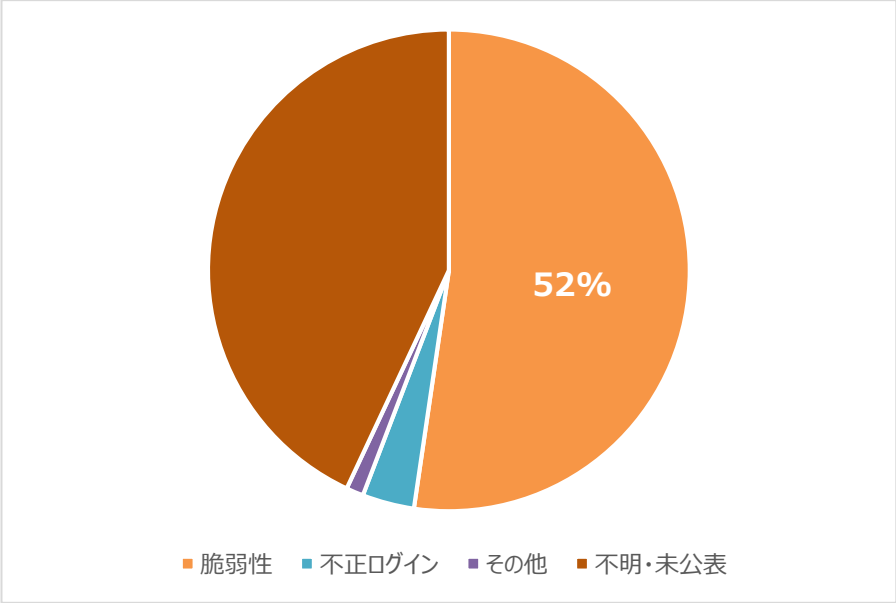

図 5 ： 2019 年の 1 年間における公開サーバへの攻撃被害事例の原因別割合
（ 2020 年 トレンドマイクロ調べ）

4 AWS 上の公開サーバに対するセキュリティ強化

ミドルウェアの深刻な脆弱性や公開サーバの脆弱性を狙われた事例からも、公開サーバにおけるミドルウェアや OS のセキュリティ対策が重要だということが分かります。このような公開サーバにおけるセキュリティ対策の重要性は、オンプレミス環境とクラウド環境で違いがあるわけではなく、AWS 上の公開サーバにも同様に対策の検討が必要です。トレンドマイクロでは、こうしたセキュリティリスクを解決するために、総合サーバセキュリティソリューション「Trend Micro Deep Security™（ 以下、「Deep Security」）」を活用したセキュリティ強化をお勧めします。
Deep Security は、Amazon EC 2 インスタンス上にインストールするソフトウェア型（ ホスト型） のセキュリティ対策製品です。サーバのセキュリティ対策に必要な 7 つの機能を 1 つの製品に実装しています。具体的には、ウイルスの侵入を防ぐ「不正プログラム対策」、OS やアプリケーション、ミドルウェアの脆弱

性を突いた攻撃を OS のネットワーク層でブロックする「IPS/IDS（ 侵入防御/検知）」、外部の不正な URL への通信をブロックする「Web レピュテーション機能」、ファイルやレジストリに改ざんが発生した際に管理者に通知する「変更監視」、OS への不正なログイン試行などを監視する「セキュリティログ監視」、アプリケーションの実行をホワイトリスト/ブラックリストで管理できる「アプリケーションコントロール機能」また、「ファイアウォール」の 7 つのセキュリティ機能が実装されています [12]。こうした Deep Security の機能を活用することで、AWS 上の公開サーバのセキュリティ対策を強化することができます。

4.1 AWS WAF と Trend Micro Deep Security の組合せ

既に AWS WAF を導入しているユーザは、あらためて「OS」、「ミドルウェア」のレイヤに残るセキュリティリスクを見直し、対策を検討することをお勧めします。トレンドマイクロが提供する Deep Security の「IPS（ 侵入防御）」機能であれば、OS やミドルウェアを狙った攻撃をブロックすることができるため、AWS WAF と組み合わせて導入することで、公開サーバの全レイヤのセキュリティリスクに対応することができます。

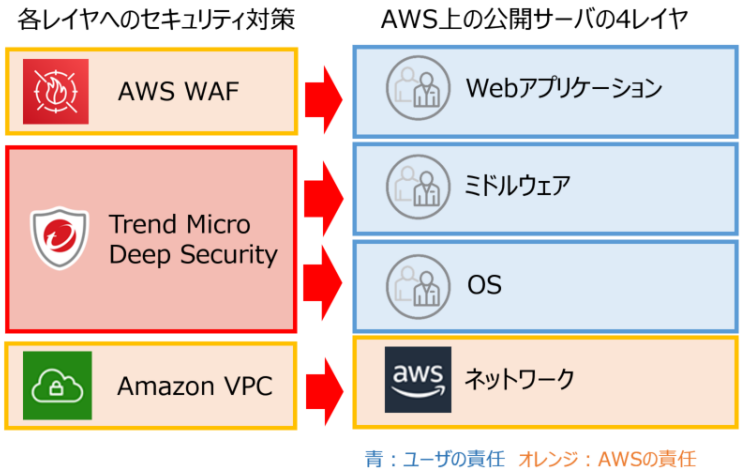

図 6 ： AWS WAF+ Deep Security の組み合わせによるセキュリティ強化

4.2 Trend Micro Deep Security 単体でのセキュリティ強化

AWS WAF を導入していないユーザまたは、構築環境上 AWS WAF が導入できないユーザは、「Web アプリケーション」のレイヤを含めた Deep Security の活用をお勧めします。ミドルウェアの脆弱性に有効な Deep Security の「IPS（侵入防御）」機能は、SQL インジェクションやクロスサイトスクリプティング等の一般的な Web アプリケーションに対する攻撃も検知・ブロックすることができます。そのため、Deep Security を導入することで、ユーザの責任範囲である「Web アプリケーション」、「ミドルウェア」、「OS」の 3 レイヤに対するセキュリティを一括で強化できます。

[12] http://www.trendmicro.co.jp/jp/business/products/tmds/index.html#functio

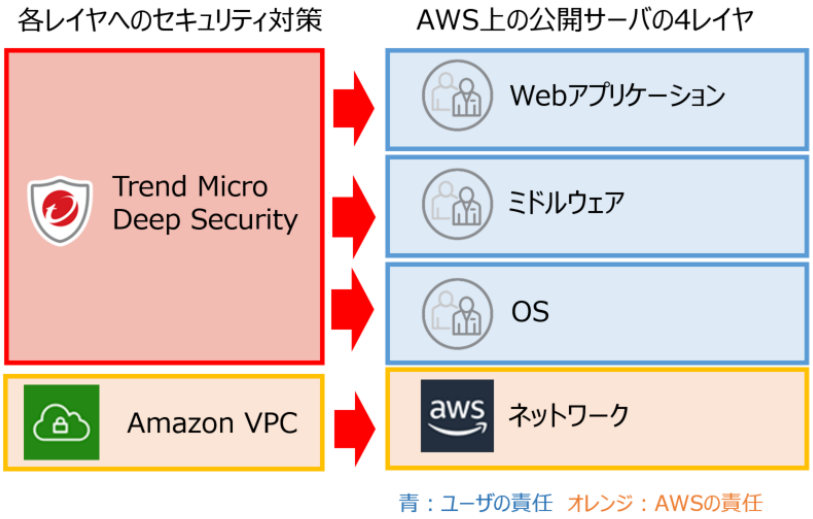

図 7 ：Deep Security 単体で実現するセキュリティ強化

4.3 Trend Micro Deep Security を活用したセキュリティ対策

Deep Security で強化できるのは、「Web アプリケーション」、「ミドルウェア」、「OS」の脆弱性対策だけではありません。最後に公開サーバに Deep Security を導入することで実現できるセキュリティ対策をまとめて解説します。

ウイルス対策

- 不正プログラム対策
  公開サーバ側のウイルス対策として、Deep Security の「不正プログラム対策」が有効です。

脆弱性対策

公開サーバ上に存在する脆弱性の対策として、Deep Security では、「IPS（ 侵入防御）の推奨設定」と「IPS（ 侵入防御）」の二つが有効です。

- IPS（侵入防御）
  公開サーバの脆弱性を狙った攻撃を検知・ブロックすることができます。
- IPS（侵入防御）の推奨設定
  公開サーバ内に存在する脆弱性をスキャンで見つけ、仮想パッチが適用できます。

自社で攻撃に気付ける対策

万が一、公開サーバが攻撃されてサイト改ざん、情報漏えいといった被害が発生した場合に備え、自社で早期に攻撃に気付ける仕組みづくりが重要です。ここでは、Deep Security が持つ以下の機能が有効です。

- システム上の変更監視
  公開サーバ上の Web サイト関連ファイルの改ざんを検知することができます。
- セキュリティログ監視
  公開サーバ上のセキュリティログを監視し、サーバの異常を検知することができます。
- IPS（侵入防御）
  公開サーバの脆弱性を狙った攻撃を検知・ブロックすることができます。
- ホスト型ファイアウォール
  公開サーバを狙った攻撃通信を検知・ブロックすることができます。
- Web レピュテーション機能
  サーバに設置された遠隔操作ツールの検知、不正サーバへのアクセスをブロックすることができます。

セキュリティ対策	対策項目	Deep Security 対応機能
ウイルス対策	公開サーバ側のウイルス感染防止	不正プログラム対策
脆弱性対策	脆弱性への攻撃を検知・ブロック	IPS（侵入防御）
	脆弱性の把握と修正パッチ適用	IPS（侵入防御）の推奨設定
自社で攻撃に気付く対策	サーバやシステムのファイル改ざん検知	システム上の変更監視
	セキュリティログによるサーバ異常の検知	セキュリティログ監視
	不正プログラムの侵入を検知・ブロック	不正プログラム対策
	サーバを狙った攻撃通信の検知	IPS（侵入防御） ホスト型ファイアウォール
	サーバに設置された遠隔操作ツールの検知	IPS（侵入防御） Web レピュテーション

表 3 ： Deep Security を活用したセキュリティ対策の一例

2020 年 4 月現在の情報をもとに作成されたものです。今後、仕様の変更、バージョンアップ等により、内容の全部もしくは一部に変更が生じる可能性があります。

サイバー犯罪者に公開サーバが狙われた事例は後を絶ちません。こうした事例の多くは、サイト改ざん、情報漏えい等、少なからず企業の資産やブランドイメージに影響を及ぼすようなものであり、公開サーバに対するセキュリティ対策の実施は必要不可欠となっています。本ガイドでは、AWS の責任共有モデルとセキュリティ対策のポイントについて解説してきました。AWS 上で公開サーバを構築するユーザは、AWS が提供するセキュリティ機能を上手く活用するだけでなく、こうした情報を基に追加のセキュリティ対策を検討することをお勧めします。

TREND MICRO

トレンドマイクロ株式会社

www.trendmicro.com

東京本社
〒151-0053 東京都渋谷区代々木2-1-1
新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口）
FAX.03-5334-3639

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13F
TEL.06-6350-0330　FAX.06-6350-0591

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7F
TEL.052-955-1221　FAX.052-963-6332

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7
シティ21ビル7F
TEL.092-471-0562　FAX.092-471-0563