AWSでFirebox Cloudを活用する

ウォッチガードのセキュリティ機能をAWSのビジネスクリティカルなIT資産にまで拡張

AWS（Amazon Web Services）とは

AWS は、パブリッククラウドへ迅速かつ容易なリソースの展開を可能にするプラットフォームです。AWS は、コンピューティング、ストレージ、コンテンツ配信などの機能を
備えたホスティング環境に、IaaS（Infrastructure-as-a-Service）としてシステムを展開できます。中堅中小企業であっても、初期コスト不要の従量制課金モデルで AWS を利用し、オンプレミスのデータセンターに代わる魅力的なプラットフォームとして、パブリッククラウドを活用することができます。RightScale の「2016 State of the Cloud（2016 年クラウドの現状）」レポートによると、71%の SMB（中堅中小企業）がパブリッククラウド環境で 1 つのアプリケーションを運用しています。しかしながら、自社で制御できるオンプレミスのデータセンター外に企業の IT インフラを移動することで、セキュリティダイナミックが変化し、重要な資産を保護するために追加のセキュリティソリューションが必要となります。

パブリッククラウドにおけるセキュリティ

パブリッククラウドは、あらゆる規模の企業に無限の新たなビジネスチャンスをもたらしました。その一方で、ハッカーもまた、その成長に注目するようになり、最近では、パブリッククラウドサービスで運用されているサーバや、AWS の仮想化コンピューティング環境である Amazon EC2 で運用されているサーバを標的にする攻撃も見つかっています。

> セキュリティという観点では、AWS などのパブリッククラウド環境にサーバを移動しても、自社のデータセンターで運用する場合と変わりません。ファイアウォールやアクセス制御のルールを設定せずにポートをオープンにしたままにしておくと、物理サーバと同様にハッカーからの攻撃を受けてしまいます。

パブリッククラウド上のサーバにおいても、セキュリティ対策が不十分であれば、オンプレミスと同様に攻撃を許してしまうことになります。IaaS サーバへのデータの移行が進める企業が増えれば、そのデータを追いかける犯罪も増加します。AWS はその対策として、クラウドインフラストラクチャのセキュリティ確保に努めてきましたが、パブリッククラウドの機密情報保護については、双方がセキュリティに対する責任を共有する事とされています。

セキュリティとAWSの責任共有モデル

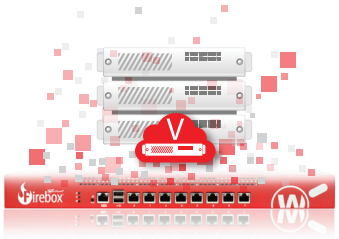
Amazon Web Services は、クラウドインフラストラクチャのセキュリティ対策は万全だとしていますが、クラウド上の企業の情報資産のセキュリティ対策は、ユーザ側の責任であると明記されています。AWS の責任共有モデルでは、AWS によって、次のように責任が区別され、規定されています。

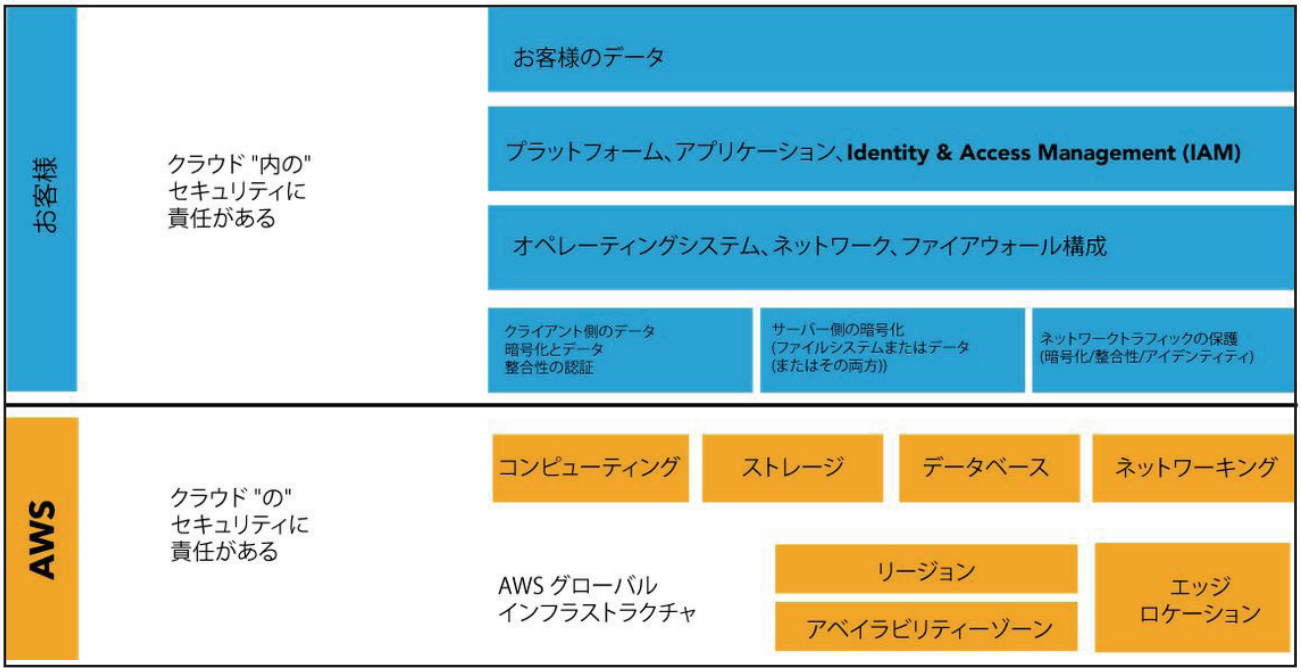
- クラウドサービスプロバイダ（AWS）が実装・運用するセキュリティ対策 -「クラウドのセキュリティ」
- AWS サービスを利用する顧客のコンテンツとアプリケーションのセキュリティを確保するために顧客が実装・運用するセキュリティ対策 -「クラウド内のセキュリティ」

AWS は、AWS のエンドポイントの保護、保存されるデータの暗号化、および顧客の仮想ネットワークとアプリケーションのセグメンテーションのための一連のセキュリティツールによって、「クラウドのセキュリティ」を実現します。責任共有モデルにおいては、顧客のコンテンツ、プラットフォーム、アプリケーション、およびネットワークに対するセキュリティ対策はユーザ側に任されます。

ネットワークセキュリティでAWSのセキュリティを強化する

AWS には、インスタンスと VPC（仮想パブリッククラウド）へのアクセスを制御するための仮想ファイアウォールの組み込み機能が提供されています。ネットワークアクセス ACL（制御リスト）と呼ばれるこのセキュリティレイヤが、1 つ以上のサブネットの送受信トラフィックを制御するファイアウォールとして機能します。しかしながら、アクセス制御だけでは、セキュリティの課題の一部分しか解決されません。AWS での十分なセキュリティ対策には、インバウンド／アウトバウンドトラフィックの検査機能を備え、最新のサイバー攻撃を検知・防止できる強力なセキュリティツールを使用する必要があります。





AWS責任共有モデルのセキュリティ対策をFirebox Cloudで補完する

WatchGuard Firebox® Cloud により、ウォッチガードの先進の Firebox® アプライアンスをパブリッククラウドに適用することができます。Firebox Cloud for AWS は、従来型の不正侵入検知、ゲートウェイウイルス対策、アプリケーション制御、URL フィルタリングの他、最新のマルウェア、ランサムウェア対策などの高度なセキュリティ機能も含む、包括的なセキュリティサービスポートフォリオによって、AWS 環境を保護します。各セキュリティサービスは、容易な管理と費用対効果の高い仮想 Firebox によるセキュリティソリューションとして提供されます。

さらに、Firebox Cloud の管理には、クラウド対応のネットワークセキュリティ可視化ソリューション「WatchGuard Dimension」を利用することが可能です。WatchGuard Dimension は、ビッグデータの可視化、およびレポートツールを提供し、セキュリティに関する重要な問題や傾向を迅速に特定・抽出し、システム環境全般の最適なセキュリティポリシーを設定する上で重要なインサイトを提供します。これにより、AWS 環境のセキュリティを容易に管理できるようになります。

Firebox Cloudの主な活用事例

- AWS に展開したサーバの保護　Firebox Cloud インスタンスをインストールし、インターネットへのアクセスが可能な複数の仮想サーバを保護できます。Firebox Cloud インスタンスが、インターネットからサーバへのインバウンド接続のゲートウェイとなります。Firebox Cloud インスタンスにポリシーやセキュリティサービスを設定して、仮想サーバへのトラフィックを制御します。
- ブランチオフィス VPN ゲートウェイ　BOVPN（ブランチオフィス仮想プライベートネットワーク）によって、離れたオフィス間での暗号化されたセキュアな接続が実現します。本社、分散拠点、リモートユーザ、在宅勤務者が、BOVPN トンネルのネットワークとホストとなります。企業のファイアウォール内での重要なデータの送受信などの通信に、この方法が利用されます。　この方法では、BOVPN によってオフィス間のセキュア接続が提供されるため、専用回線のコスト削減が可能になり、エンドポイントのセキュリティが確保されます。Firebox Cloud を BOVPN（ブランチオフィス VPN）ゲートウェイのエンドポイントとして構成することで、AWS ネットワークのリソースと Firebox または互換 VPN ゲートウェイのエンドポイントで保護された他のネットワークの間のセキュア VPN 接続が実現します。
- モバイル VPN ゲートウェイ　SSL、IPSec、L2TP のモバイル VPN クライアントからの VPN 接続を Firebox Cloud で受け取り、AWS ネットワークの保護リソースへのユーザやグループのアクセスを制御するポリシーを構成することもできます。

ウォッチガードについて

WatchGuard® Technologies, Inc. は、ネットワークセキュリティ、セキュアWi-Fi、ネットワークインテリジェンス製品、セキュリティサービスの世界的なリーダー企業であり、世界各国の75,000社以上のお客様にサービスを提供しています。ウォッチガードのミッションは、中堅中小企業や多拠点をもつ分散型企業向けの理想的なセキュリティソリューションを提供し、すべての企業がエンタープライズグレードのセキュリティを容易に利用できるようにすることです。ウォッチガードの本社は、米国ワシントン州のシアトルにあり、北米、欧州、日本、アジア太平洋地域、および南米にオフィス展開しています。詳しくは、WatchGuard.co.jpをご覧ください。

 Part No WGJPAWS_032817