**親子の会話から学ぶクラウドセキュリティ（2）：1人では大変だなあ――クラウド上で安全なネットワークを構築・管理するために必要な基礎知識**

<https://www.atmarkit.co.jp/ait/articles/2008/04/news002.html>　　[[PDF出力]](https://id.itmedia.jp/isentry?return_url=https://ids.itmedia.jp/pdf/ait/200804_news002.pdf&article_url=https://www.atmarkit.co.jp/ait/articles/2008/04/news002.html&encoding=shiftjis&ac=e8cb9106baa7e37eb9feb877b9f0a27ddaf48b95ba02da49cbb3a8247ee7fec4)

**親子の会話で出てくるような素朴な疑問点から、クラウド環境における情報セキュリティの技術を学習する連載。今回は、クラウド上で安全なネットワークを構築・管理するために必要な基礎知識について。**

**2020年08月04日 05時00分 更新**

**[**青山桃子，**株式会社日立ソリューションズ]**

　親子の会話で出てくるような素朴な疑問点から、クラウド環境における情報セキュリティの技術を学習する本連載「親子の会話から学ぶクラウドセキュリティ」。[初回](https://www.atmarkit.co.jp/ait/articles/2007/02/news006.html" \t "_blank)は、クラウドを始める前に覚えておきたいセキュリティの基礎知識について解説しました。今回は、クラウド上で安全なネットワークを構築・管理するために必要な基礎知識についてです。

**安全なネットワーク構成って、どうやって考えるの？**



おかあさん、Webアプリケーションの設計ができたよ！



よくできたわね。構築する前に、安全なネットワーク構成も設計しておきましょうね。



安全なネットワーク構成ってどうやって考えるの？



まずは、必要なセキュリティレベルに応じてゾーンを分けましょうね。例えば、インターネットからアクセスできるサーバと、そうではないサーバというようにね。



クラウドにあるのに、アクセスできないサーバもあるの？



おもちゃ屋さんで、値段の高いおもちゃの売り場に空箱が置いてあることがあるでしょ？　悪い人に盗まれないように、本物（大事なデータ）はお店の人にしか取れない（アクセスできない）ところにあるのよ。

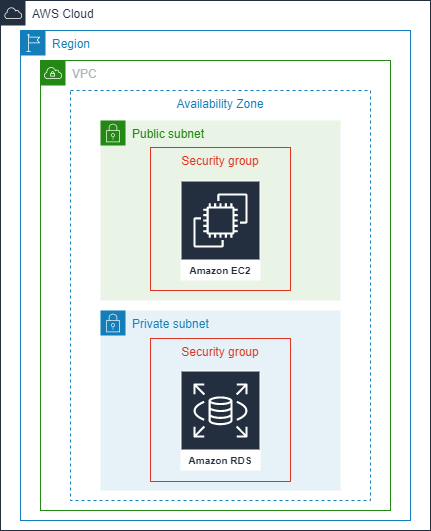
　ネットワークにおいてセキュリティを考えるべきポイントには、アクセス制御、攻撃検知・防御、ログによるトレーサビリティー（いつ、どこで、何が起きたかを追跡すること）の確保、可用性の確保などがあります。

　ネットワーク構成を考えるとき、求められているセキュリティレベルごとにゾーンを分けておくとセキュリティ対策を講じやすくなります。

　ゾーン分けは、アクセス制御を行う単位として使える他、セキュリティ対策の優先度を検討するのに役立ちます。ゾーンを分けておけば、例えば「インターネットから直接アクセスできるサーバはサイバー攻撃を受けるリスクが高いため、優先的にセキュリティ対策を施す」ことが可能になります。同じゾーン内に異なるセキュリティ対策状況の機器が混在すると、セキュリティホールになり、横展開による攻撃の被害に遭いやすくなるというリスクがあります。

　Amazon Web Services（AWS）の場合、「Amazon Elastic Compute Cloud（EC2）」などのインスタンスは、「Amazon Virtual Private Cloud（VPC）」という、クラウド上の論理的にプライベートな領域に配置します。これは仮想的な1つのネットワークのようなイメージです。各インスタンスへのアクセス制御は、セキュリティグループの設定により行えます。

　また、インターネットとの通信可否はサブネットを使って区別することができます。Webサーバのようにインターネットから直接アクセスしたいものはPublic Subnetに、DBサーバのようにインターネットから直接アクセスできないようにしたいものはPrivate Subnetに配置します。

  
AWS上のネットワーク構成イメージ（アイコン：AWS）

**サーバ以外にも必要なものがあるの？**



Webサービスなら、WAF（Web Application Firewall）もあった方がよさそうね。



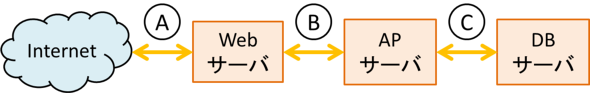
サーバ以外にも必要なものがあるの？



ネットワークのセキュリティ対策は、ネットワーク構成を考えるときに決めておいた方がいいよ。後からでも付けられるけど、手間がかかる場合があるからね。

　オンプレミスの場合、必要なセキュリティ対策を導入するために物理的な機器を設置することが多かったと思います。クラウドの場合、サービス・機能を追加することでセキュリティ対策を実施するのが主な考え方になります。

　オンプレミスのWebサービスの例として、Web／AP／DBサーバの3つが動いているものを考えてみましょう。ここに加えるべきセキュリティ対策機器としては何が考えられるでしょうか。また、それに対応するAWSのサービスを考えてみましょう。



**（1）ファイアウォール（主な設置箇所：A、B）**

　境界防御の最も基本的なセキュリティ機器といえるファイアウォール。IPアドレス、TCP/UDPポート番号などでのアクセス制御を得意としています。IPv6通信の設定も適切に行うようにしましょう。インターネットとの境界にはもちろんですが、Webサーバを設置するDMZ（DeMilitarized Zone）とAP／DBサーバを設置する内部ネットワークとの境界にも置く必要があります。

　AWSの場合、サブネットのネットワークACL（アクセス制御リスト）や、セキュリティグループの設定により同様のアクセス制御を行えます。セキュリティグループのルールはIPアドレス、ポートによる制御はもちろん、送信元（ソース）のセキュリティグループも指定できます。

**（2）ロードバランサー（負荷分散装置）（主な設置箇所：A、B、C）**

　可用性確保のために、各サーバの前段にロードバランサーを置きます。複数のサーバを設置し、トラフィックを適切に振り分けるようにします。また、障害が発生して、1つのサーバがダウンした場合もサービスを継続できます。

　AWSの場合、「AWS Elastic Load Balancing（ELB）」を使用して、負荷分散を行えます。

　また、「AWS Auto Scaling」を利用して、使用するリソースを最適化できます。障害発生時には自動的にインスタンスを終了し、新しいインスタンスを起動することも可能です。

**（3）リバースプロキシ（主な設置箇所：A）**

　データをキャッシュしWebサーバの負荷を軽減したり、内部のWebサーバを隠蔽（いんぺい）したりすることができます。ロードバランサーやSSLアクセラレータと一緒に提供されることもあります。コンテンツ配信ネットワークが同様の役割を果たす場合もあります。

　AWSの場合、「Amazon CloudFront」というコンテンツ配信ネットワークが利用可能です。

**（4）SSLアクセラレータ（主な設置箇所：A）**

　SSL/TLS通信（HTTPS）の暗号化・復号を行う機器です。インターネット側へ送るときは暗号化し、Webサーバ側へ送るときは復号します。平文のHTTPリクエストを見る必要があるような機器（WAFなど）に組み込まれている場合もあります。

　AWSの場合、AWS ELBでSSL/TLSの終端が可能です。

**（5）WAF（主な設置箇所：A）**

　Webアプリケーション特有の攻撃を検知・防御します。Webアプリケーション特有の攻撃の例としては、クロスサイトスクリプティングやSQLインジェクションなどがあります。WAFはHTTPリクエストの中身（ヘッダ・ボディー）を見てこれらの攻撃を検知・防御できます。Webアプリケーション自体に脆弱（ぜいじゃく）性がなければ不要ともいえますが、新しく発見された脆弱性に対処したい場合や、Webアプリケーション自体の修正が難しい場合などに有効です。また、PCI DSS（Payment Card Industry Data Security Standard）などの基準に準拠するため、といった目的で導入を検討する場合もあります。

　ただし、正常な通信と攻撃を正確に区別するにはルールをチューニングする必要があるため、導入・運用に手間がかかるといわれています。

　AWSの場合、「AWS WAF」があります。用意されたAWS WAF用のマネージドルールを使用することで、チューニングの手間を軽減できます。

**（6）IDS／IPS（主な設置箇所：A）**

　ネットワークベースのIDS（Intrusion Detection System）／IPS（Intrusion Prevention System）と、ホストベースのIDS／IPSが存在します。通信を監視し、攻撃を検知・防御します。WAFで検知するようなアプリケーション特有の攻撃検知は得意ではない場合があります。

　AWSの場合、「Amazon GuardDuty」を利用することで、悪意のある操作や不正な動作を継続的にモニタリングし、脅威を検出できます。

**（7）DoS・DDoS攻撃対策（主な設置箇所：A）**

　DoS／DDoS攻撃とは、大量の通信を送り付けたり、不正な通信を送り付けたりすることでサービスを提供不可能な状態にする攻撃です。

　DDoS攻撃対策専用機を導入する他、大量の通信についてはファイアウォールの機能で対策したり、不正な通信についてはIDS／IPSなどで対策したりすることもできます。

　クラウドは通信量により従量課金されるサービスもあるため、お金を消費させるために大量のトラフィックを送る「Economic DoS（EDoS）」と呼ばれる攻撃が行われる場合もあります。

　AWSの場合、「AWS Shield」があります。無料で提供される「AWS Shield Standard」は、一般的なネットワーク層およびトランスポート層のDDoS攻撃を防御できます。より詳しい設定を行いたい場合や、アプリケーション層の対策を強化したい場合は「AWS Shield Advanced」も選択可能です。

　クラウドの環境では、そもそもWebサーバやAPサーバがサーバレスだったり、DBがマネージドサービスだったりして、ここで上げたような機能はサービス内で既に提供されているような場合も多くあります。逆に、個々のサービス特有の注意点がある可能性もあります。そういう時にも、基本的な対策の観点を押さえておけば、システムごとに応用できます。

　「この機器・サービスを使えばOK！　使わなきゃダメ！」ではなく、「こういう目的のセキュリティ対策は、このサービスで大丈夫か？」という考え方は、日々新しい技術が生み出されるITの環境変化に対応するための「セキュリティの基礎体力」といえるでしょう。「このサービスで大丈夫か？」という問題は、利用したいサービスのサポート窓口などで相談することをお勧めします。

**ネットワーク機器のセキュリティ対策は何をすればいいの？**



ネットワーク機器のセキュリティ対策は何をすればいいの？



通常のネットワーク機器同様、セキュリティパッチの適用が必要だよ。パッチ適用がベンダーとユーザーのどちらの責任になっているか確認しておこうね。ユーザーの責任になっている場合は、ちゃんと自分でやるのよ。



はあい。



あと、細かい設定は主にユーザーの責任になっている場合が多いから、設定ミスがないように気を付けてね。

　ネットワーク機器の主なセキュリティ対策は、セキュリティパッチの適用と設定の管理です。情報機器やソフトウェアは、最新のセキュリティパッチを適用しておくことで、既知の脆弱性を狙った攻撃による被害を防ぐことができます。サイバー攻撃の大部分は、この既知の脆弱性を狙った攻撃だといわれています。しかし、きちんとパッチを適用していても、設定ミスにより非公開のはずの情報にアクセスできたり、弱いパスワードを使っていたため不正アクセスされてしまったりという状況になっていてはいけません。

　AWSなどのクラウドサービスでは、こういったセキュリティ対策は「機器」ではなく「サービス」として提供されていることが多いと思います。その場合、ファームウェアに対するパッチ適用はクラウドベンダーの責任範囲に含まれるため、ユーザーは対応不要です。しかし、設定の不備などがあった場合はユーザーの責任になります。前回も書いた通り、AWSの場合は「責任共有モデル」により責任範囲が明示されています。

　特殊なパターンとして、「Amazon EC2でLinuxを構築して、ファイアウォールとして運用する」というような場合は、OSのセキュリティパッチの適用もユーザーの責任になるので、ご注意ください。

**1人では大変だなあ……。誰か手伝ってくれないかな？**



セキュリティ対策ってたくさんあるんだね。1人では大変だなあ……。誰か手伝ってくれないかな？



「サードパーティーのベンダーにお願いするのもいいんじゃないかしら。AWSには、サードパーティーのベンダーが自分の作ったものをAWS上でそのまま利用できる形で提供する仕組みがあるよ。



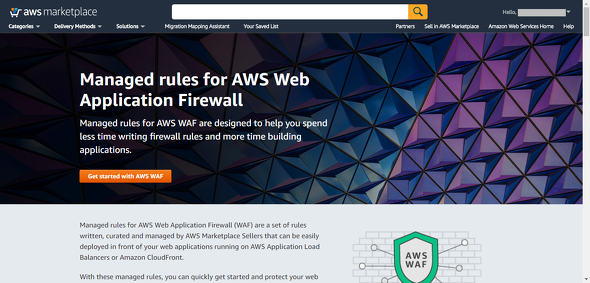
自分で構築しなくていいの？　楽できるね！



そうね。それだけじゃなくて、ユーザーのミスや環境によるエラーを防ぎやすく、問題が起きたときの対処もベンダーに相談できるから安心なのよ。

　「AWS Marketplace」を利用すると、サードパーティーのベンダーが提供するAWS上のサービスを購入できます。

　例えばAWS WAFには、AWSが提供するマネージドルール以外にも、サードパーティーが提供するマネージドルールも存在し、AWS Marketplaceで購入できます。そもそも、運用も自分でしたくない場合は、運用まで含まれているサービスもあるので、それも購入できます。

  
AWS WAFのマネージドルールもAWS Marketplaceで購入できる



もう構築してもいい？



いいわよ。実際にやってみるのが一番勉強になるね。

Copyright © ITmedia, Inc. All Rights Reserved.

[[ITmedia Inc.](https://corp.itmedia.co.jp/)](https://corp.itmedia.co.jp/)