AWS セキュリティ対策のキホン①

はじめに

皆さんは AWS への攻撃と聞いて何を思い浮かべますか？

- AWS アカウント情報の漏洩
- AWS リソースの不正利用
- システムへの不正ログイン
- アプリケーションの不正操作
- etc

一般的な対策や、AWS 特有の対策について考慮し検討を実施していく必要があります。

今回は AWS セキュリティ対策のキホンという形で何回かに分けてポイント毎に気を付ける箇所を記載してみたいと思います。

ヒデンのタレにならないために

セキュリティ対策といっても範囲が広いです。

実施できるところから進めるでも良いですが、根拠となる指針がないと後で振り返った際に抜け漏れがでてしまっていたなどの可能性があります。そのため、最初の検討段階で何かしらの指針に基づいて進めていく形を推奨します。

AWS では 2019 年 1 月に以下ホワイトペーパーを公開しています。今回はこちらのフレームワークを指針とする形で進めていきます。

[NIST サイバーセキュリティフレームワーク（CSF） - AWS クラウドにおける NIST CSF への準拠]
https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/NIST_Cybersecurity_Framework_CSF_JP.pdf

[IPA - セキュリティ関連 NIST 文書]
https://www.ipa.go.jp/security/publications/nist/

CSF（CYBER SECURITY FRAMEWORK）とは

CSF では以下 5 つのコアを中心とし、実施すべき対策をまとめています。

AWS のどのサービスを利用して、何に対するセキュリティを守っていくのかが重要となります。

AWS のセキュリティ関連の資料でも CSF の考え方で説明しています。AWS サービスの組み合わせで一連フローにしているものもありますので興味がわいた方は探してみてください。

まとめ

今回は AWS セキュリティ対策の全体的な考え方について CSF を用いて検討していく流れを記載しました。

次回はもう少し具体的に特定 AWS サービスを利用した場合のセキュリティ対策について投稿する予定です。

さいごに

CTC では上記フレームワークと過去実績を基にお客様にセキュリティに特化した AWS のセキュリティコンサルサービスを提供しております。