安全に配慮したSaaSを提供するために考慮すべきエンジニアの役割の提案

Proposal of engineer roles to consider in order to provide safe SaaS

鈴木 優一・マネジメント分科会・情報セキュリティ大学院大学

Utilization of cloud services is a driving force and an indispensable part for changing business styles and lifestyles to new styles. The introduction by companies promoting DX (Digital Transformation) is increasing year by year, and while convenience is attracting attention, there is no end to damage such as information leakage and unauthorized access due to increasingly sophisticated and diversified cyber-attacks. Security incidents in businesses are constantly reported in the media on a daily basis. In order to deliver secure cloud services to users, it will be more important for service providers to improve security.

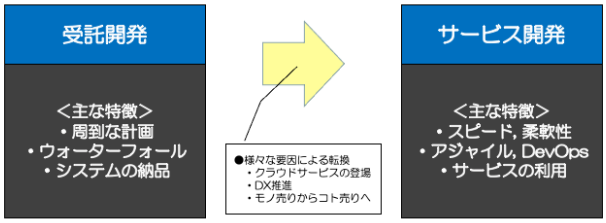
In this paper, as one of the options that contributes to the secure provision of cloud services, we will examine the function to enhance security by utilizing the resources provided by vendor companies. For vendor companies that are shifting from contract development to service development, we will propose a function to be implemented in the organization for the purpose of ensuring security in order to help the safe provision of cloud services.

1. 研究目的

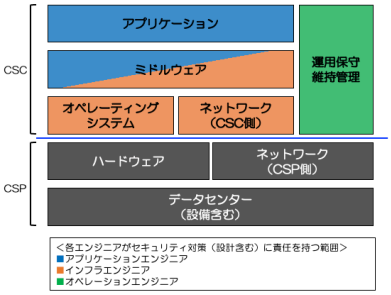
IT業界におけるベンダー企業とユーザ企業の関係を念頭に、クラウドサービスの安全な提供に貢献する選択肢の一つとして、ベンダー企業が「サービス開発組織」という新たな組織を作ることにより「セキュリティ確保がなされたクラウドサービス開発が可能になる」ことを明らかにする。

2. サービス開発

・クラウドサービスの登場によって、旧来の受託開発で提供されるシステムが、SaaS（Software as a Service）という形態でベンダー企業を介さずとも容易に利用が可能に。
・ベンダー企業は、世の中のあらゆるサービスを組み合わせ、自社の強みや価値を活かした開発をおこない提供するスタイル（サービス開発型）へシフト。



3. クラウドセキュリティ



・3種類のエンジニア（アプリケーションエンジニア、インフラエンジニア、オペレーションエンジニア）が所属し、業務上の機能役割を果たすことで、結果的にクラウドセキュリティを確保できる。

4. 検証

・2つ[*]の検証対象を用い、各セキュリティ要件や指示事項について、3種類のエンジニア（アプリケーションエンジニア、インフラエンジニア、オペレーションエンジニア）が所属し、機能役割を果たしていることが、どのようにセキュリティ確保に貢献しているかを議論し検証。

・セキュリティ確保が実現できる結果を得た。ただし、「インシデントレスポンス」の指示事項については、オペレーションエンジニアが業務上の役割のもとおこなう対応では、十分でないことが明らかとなった。

[*] Cloud Security Alliance（CSA）, ①「Top Threats to Cloud Computing The Egregious 11（クラウドの重大セキュリティ脅威11の悪質な脅威）,2019年」、②「Security Guidance for the Critical Areas of Focus in Cloud Computing v4.0（クラウドコンピューティングのためのセキュリティガイダンス v4.0）,2017年」

5. 提案

■STEP1
・サービス開発を担う専門組織を、新たに組成する。
■STEP2
・サービス開発組織には、3種類のエンジニア（アプリケーションエンジニア、インフラエンジニア、オペレーションエンジニア）を配置することで、技術的なセキュリティ確保を実現する。
■STEP3
・サービス開発組織における「インシデントレスポンス機能（NIST SP800-61のガイドをベースに、CSIRTまたはPSIRTに類似した機能を保有することが望ましいと想定）」の構築を目指す。

6. まとめ

安全なクラウドサービスを利用者へ届けるため、サービス提供者側（ベンダー企業）でセキュリティを高めることが、より重要になる。