企業のDXにおける新たなサイバーセキュリティ

アジャイル開発でのセキュリティ実装
インフラ担当者の役割

PwCコンサルティング合同会社　シニアマネージャー　山田 素久

本稿では、アジャイル開発におけるインフラ関連の技術動向に触れ、その中で大企業のインフラ担当者がアジャイル開発にどのように寄与していくのか、これまでの役割と何が変わっていくのかについて解説します。

アジャイル開発環境を支えるインフラ技術 ～ サーバーレスアーキテクチャやコンテナ技術の台頭

近年、クラウド上ではさまざまなサーバーレスアーキテクチャやサーバーレスコンテナ技術が登場しています。こうした環境では、利用企業が自分たちでOS環境をメンテナンスする必要がありません。こうした技術はDevOpsやアジャイル開発と相性がよく、コンテナ技術の進歩も相まって、OSレイヤーは実行環境の一部として、アプリケーションと一緒にデプロイされるようになりつつあります。さらにインフラ構成管理ツールにより、インフラのデプロイも自動化することが可能となっており、かつてのようにインフラ担当者のみがOSにログインできる特権を持ち、アプリケーション開発者の依頼に基づき作業を行う、という場面が徐々に減りつつあります。

存続し続ける既存システムとアジャイル環境を両立させるアーキテクチャ設計・導入を

アジャイル開発におけるインフラ担当者のセキュリティ上の役割は、主に以下の2点に集約されると考えます。

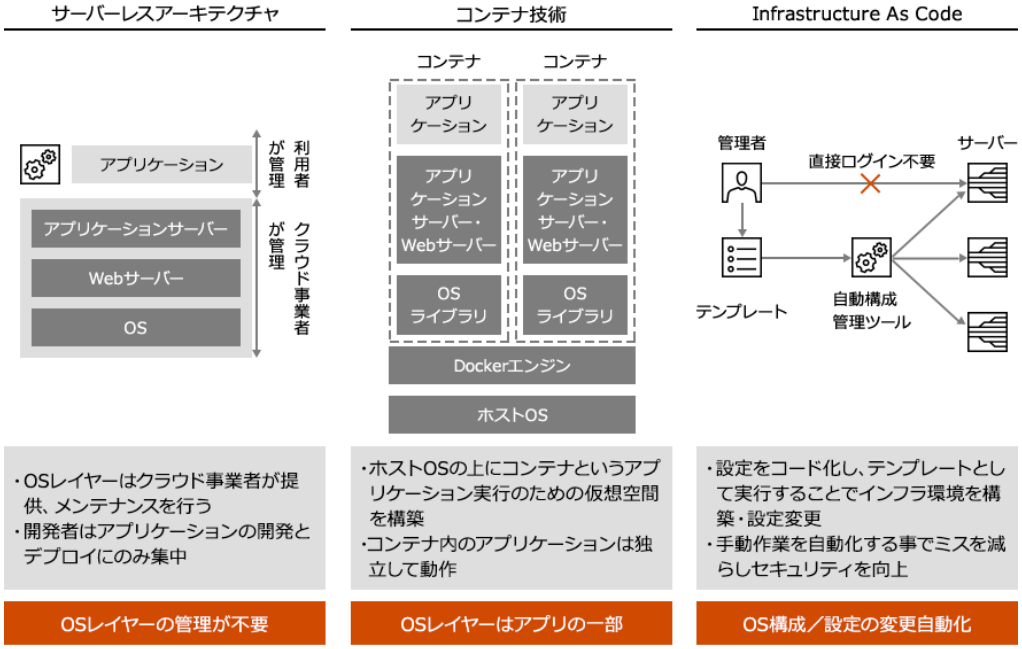
1. セキュリティを考慮したインフラアーキテクチャの設計と導入
2. 脆弱性の管理とセキュアな構成の提供

1. セキュリティを考慮したインフラアーキテクチャの設計と導入

セキュリティを考慮したインフラアーキテクチャの設計と導入において重要なのは、いきなり全ての環境がクラウドやコンテナに移行するわけではないということです。大企業においてはレガシーな基幹システムや既に構築されたプライベートクラウドが存在するため、そうした環境を併用しながら徐々に新しいアーキテクチャに移行していくのが常です。したがって、アプリケーション開発者が求めるアジャイルなインフラを導入するにあたり、既存環境との親和性やセキュリティを考慮したアーキテクチャを設計し、導入することが重要な役割となります。

図表1：アジャイル開発を支えるインフラ技術

・サーバーレスアーキテクチャやコンテナ技術などはアジャイル開発と相性がよく、
これまでのようなインフラ担当者とアプリケーション開発者の役割分担の垣根があいまいになりつつある。



その際には、採用する技術の特性を踏まえた、これまでとは異なる運用面での考慮が必要です。例えば、既存環境では踏み台サーバーを経由してホストOSに管理者アカウントでログインして実行していた作業を、インフラ構成管理ツールを使って自動デプロイさせることで管理者アカウントの使用を禁止するなど、これまでとは違った考え方が必要になります。こうしたアーキテクチャを導入することで、アプリケーション開発者はインフラの構成に頭を悩ますことなく、開発に集中することができます。

2. 継続的なセキュリティを実現する「脆弱性の管理」と「セキュアな構成の提供」

これまではOSやミドルウェア層の脆弱性についてはインフラ担当者が情報を収集し、パッチを適用することで管理がなされてきました。先ほど述べたように、アジャイル環境と既存環境の併用が続く以上、既存環境向けのこうしたセキュリティ運用が無くなることはありません。さらに実装形態によっては、コンテナはホストOSの上にデプロイされることもあるため、ホストOSの管理は引き続きインフラ担当者の業務範囲に含まれると考えられます。

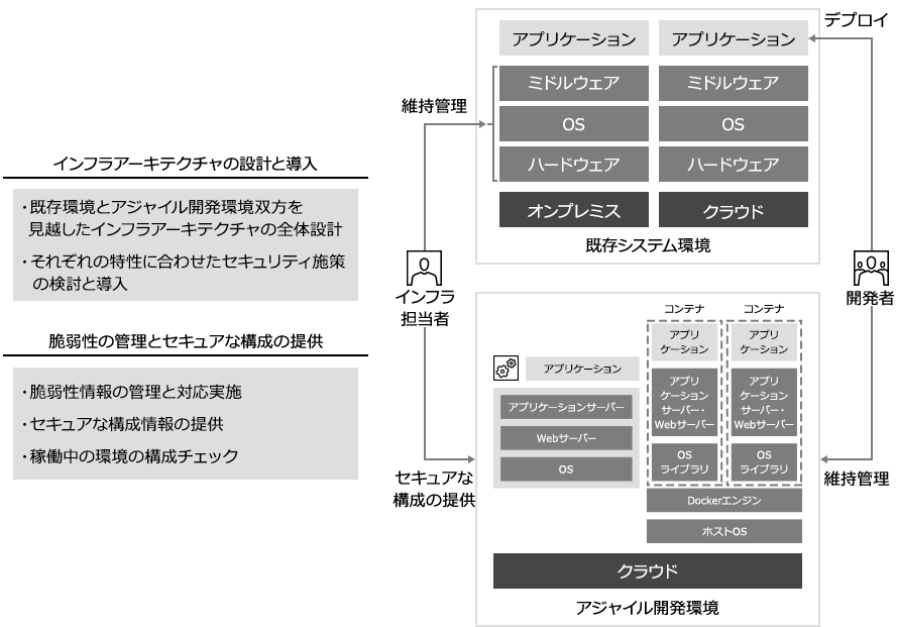
こうした環境においては、インフラ担当者とアプリケーション開発者の役割分担が曖昧になってしまうため、たとえインフラ層がアプリケーションの一部としてデプロイされるとしても、その構成や設定に不備がないかをインフラ担当者がチェックすることを推奨します。脆弱性が発見されればアプリケーション開発者と情報を共有して対応することが重要ですし、セキュリティが確保されたセキュアな構成情報を提供することが必要になります。また、アプリケーション開発者がデプロイしたコンテナの設定を確認することも重要になります。たとえアプリケーション開発者により維持・管理されるとしても、開発したアプリケーション・コード以外の部分でインフラ担当者が担う役割は依然として大きいのです。

本稿ではアジャイル開発におけるセキュリティ担当者とインフラ担当者の役割の変化について述べてきました。アジャイル開発では、アプリケーション開発者が主役でセキュリティ担当者とインフラ担当者は蚊帳の外もしくはスピードを阻害する抵抗勢力と見なされてしまう事例も散見されます。しかし、いかにアジャイルなアプリケーション開発ができようともセキュリティは無視してはいけない要素であり、それに対するセキュリティ担当者とインフラ担当者の役割は、変化こそすれ不要となるものではありません。

大企業においては役割分担が進んでおり、全ての領域を1人の開発者がカバーすることは不可能です。ぜひ変化を取り込み、自らの役割を再認識した上で、協力してアジャイル開発におけるセキュリティを向上させていただきたいと思います。

図表2：インフラ担当者の役割の変化

・存続する既存システムと新しい技術を取り込んだアジャイル開発環境を両立させるアーキテクチャ設計と、継続的なセキュリティを実現する脆弱性管理およびセキュアな構成の提供が主な役割となる。



お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com