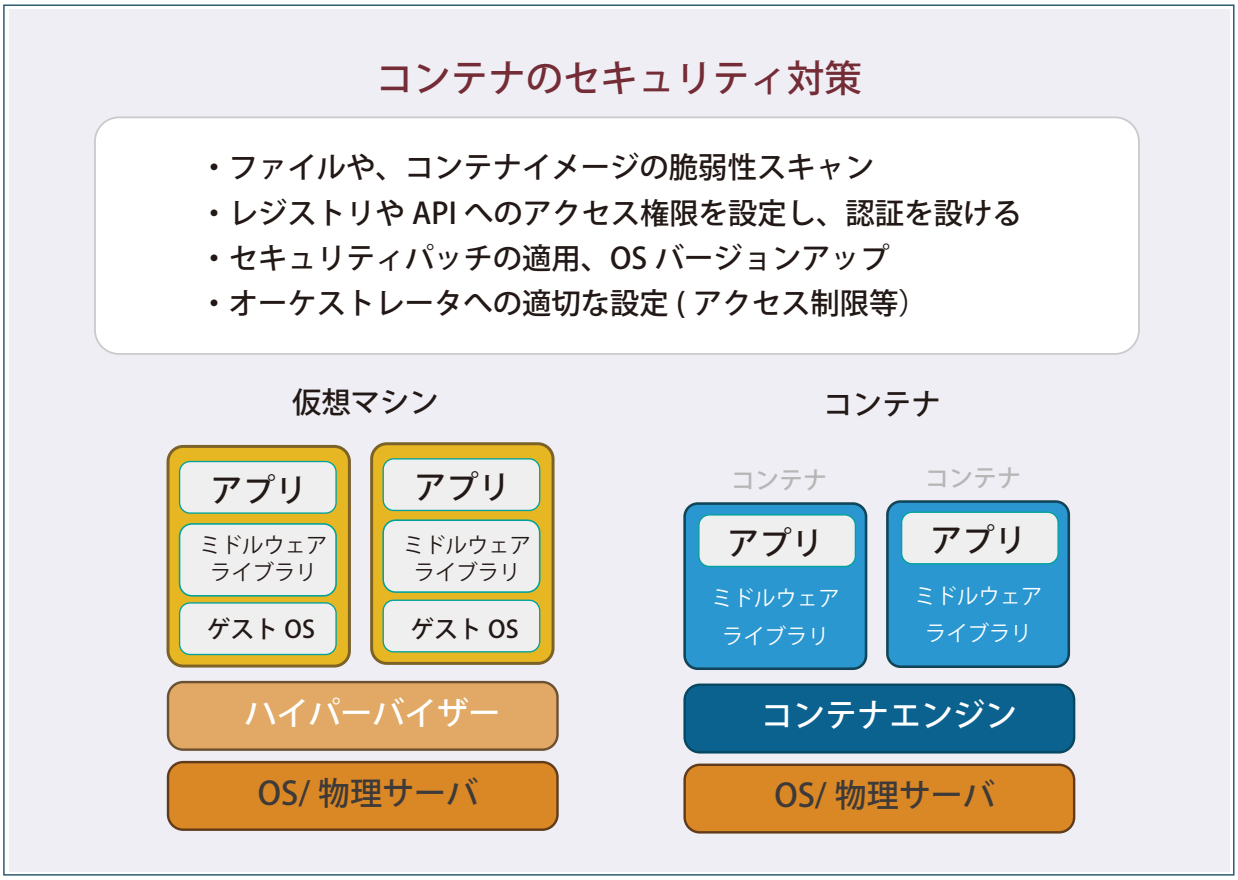
コンテナ利用のリスク対応



今や Gmail や YouTube などを代表に、多くの企業のアプリケーションがコンテナで実行されています。
コンテナは、VM などのサーバ仮想化に比べオーバーヘッドが少ないため、軽量で高速に動作するのが特徴で、近年 Web アプリの開発を中心に爆発的に利用されています。
コンテナといえば、オープンソフトウェアである Docker（ドッカー）が有名ですが、その Docker でさえ、初版のリリースが 2013 年であるため、最近になって採用され始めた技術です。よって一昔前には存在もしていなかったということで、こうした新しい技術をシステムに取り入れる場合には、企業は IT セキュリティ対策の見直しが必要です。
先日、Docker ホストを狙う、クリプトジャック ワームの「Graboid」がニュースになりました。攻撃者によって、セキュリティで保護されていない Docker デーモンが乗っ取られると、Docker イメージがインストールされ、それが実行されると、C&C サーバーからマルウェアがダウンロードされ、匿名性の高い仮想通貨 Monero をマイニングするために展開されるというワームです。ここで問題なのは、従来型のエンドポイントセキュリティの製品の多くはコンテナ内のデータや操作を検査対象にしていないため、このような種類のマルウェアを検出できないということです。
コンテナに対してのセキュリティ対策としては、コンテナ管理のためのオーケストレーションシステムである Kubernetes（クバネティス）等に適切な設定をすることがまず必要です。これは、コンテナのデプロイやスケーリング、管理などを司る部分であるため、セキュリティ対策が非常に重要なのです。コンテナが、実行後に破棄されてもログが残るように設定したり、認証やアクセス制限を追加するなどの対策を行うべきです。コンテナイメージの脆弱性スキャンを行うツールも存在するので、そうしたものを利用するのも有効です。
コンテナは、ホストとカーネルを共有しているため、定期的な OS のバージョンアップはもちろん、場合によっては OS 側でコンテナプロセスの動きや、コンテナが呼べるカーネルコールを制限したりすることも必要かもしれません。
定期的に行っているセキュリティリスクの見直しに際し、コンテナの仮想化は、ゲスト OS を起動せずにアプリを起動させる仕組みであるため、セキュリティ対策を主導するのはインフラ担当なのかアプリ開発の担当なのか分かりづらく、セキュリティ対策の対象から抜け落ちてしまっては困ります。
採用する企業は、VM 等の仮想化とコンテナの仮想化の仕組みの違いを理解し、適切なセキュリティ対策が望まれます。