N ニュータニックスニュース!

役立つニュータニックス！ from「THE FORECAST by NUTANIX」

米・連邦政府機関、クラウドセキュリティに積極的に取り組む

カルヴァン・ヘニック */ フリーライター

パブリッククラウドは政府機関で数々の IT 目標の達成に寄与している。しかし、機密データの安全を確保するためには、適切なツールを選び、正しいプロセスを踏む必要がある。

パブリッククラウドの活用は、いまやあらゆる業界で増加しているといっても過言ではなく、米・連邦政府機関も例外ではない。IT リソースの使用率改善やデータセンターの統合を目指しているほか、変化し続ける需要に応じ、リソースの拡大や縮小を図っている。しかし、こうして政府機関がパブリッククラウドの利用を進める背景には、政策にからんだ理由も存在している。

クラウドサービスに対する信頼は、ここ数年で大きく前進を見せた。パブリッククラウドが登場した頃は、クラウドベンダーが機密情報を危険にさらすのではないかという疑念のもと、自社のデータセンターの外にワークロードを置くことなど、到底受け入れられないという考え方が一般的だった。

しかしそれ以降、クラウドベンダーが提供するサービスにインシデントが発生することはほとんどなく、多くのベンダーがセキュリティおよびコンプライアンス認証を取得した。初期の頃から数年かけて実績を築き上げ、当初の不安は大部分が無用であったと証明するに至ったのだ。

だからといって、政府機関がクラウドのセキュリティに目を光らせないというわけではない。GAO（米国会計検査院）で情報セキュリティの責任者を務めるグレゴリー・ウィルシェン氏は、こうした内容に言及する。

ウィルシェン氏 「業務にクラウドを利用する政府機関が増えるほど、クラウドサービスに預ける情報が適切に保護されるよう、留意することが極めて重要になります。データが目の前にないからといって、セキュリティに対しても盲目的になっていないでしょうか。セキュリティはクラウドサービスプロバイダーの責任だと思いがちですが、それは間違いです。政府機関の責任において、データを保護しなければなりません」

ウェルシェン氏が登壇し発言したこのウェビナーには、GAO の IT & サイバーセキュリティチーム次長、ラリー・クロスランド氏、そしてニュータニックスで政府向けシステムエンジニアリングを率いるシニアディレクター、ダン・ファーロンも参加した。

クラウド採用の理由とメリット

政府機関がパブリッククラウドを使う理由として、「政策による推進要因が多数ある」とクロスランド氏は指摘する。例えば、OMB（米国行政管理予算局）の「クラウドファースト」政策が挙げられる。この政策により、政府機関が新たな IT 投資を行う際、クラウドを考慮することが求められるようになった。

形式的に義務付けただけだろうと思うかもしれないが、リソースをクラウドに移行し、そのメリットを肌で感じる機会を創出することにこの政策の意図があるということだ。

「メリットの 1 つはもちろん、IT リソースの管理における効率性の向上です。IT 資産が十分に活用されていないというケースが、政府機関には多々あるのです」とウィルシェン氏。

リソースをパブリッククラウドへ移行すれば、データセンターの統合も加速する。近年は、これが連邦政府におけるクラウド利用推奨の主な理由となっている。コスト削減も重要な目的だ。

クロスランド氏とウェルシェン氏が引用した GAO の報告書では、2015 年以降にクラウドへの支出を増やした 16 機関は、2019 年 4 月の時点で総額で数億ドルものコスト削減を実現したとされている（カスタマーサービスの強化など、他のメリットについても言及している）。

そして多くの組織と同様、恐らくパブリッククラウドの利点として最もよく知られる要素、つまり敏捷性と柔軟性の実現について政府機関も模索しているとのことだ。

ウェルシェン氏 「需要の増加、あるいは急増が起こっても、クラウドサービスプロバイダーに依頼すれば、その分を容易に調達することができます。需要がなければ、受けるサービスを縮小することだってできるのです」

セキュリティへの懸念

パブリッククラウドに移行したデータは、政府機関の物理的なセキュリティ境界の外に置かれている。しかし、重要なセキュリティ課題、そして懸念事項の多くが消えたわけではない。ウェルシェン氏はこう指摘する。

ウェルシェン氏 「政府機関は、組織の IT 環境におけるリスクを評価し、管理しなければなりません。クラウドコンピューティングでも同様、クラウド環境に関するリスクを評価、そして管理する必要があります。脅威を特定するのはもちろんのこと、クラウドプロバイダーによるセキュリティ管理が十分であるかどうか、精査することも重要です」

また、法令に基づきデータ保護規則を定義した上で、クラウドサービスプロバイダーのパフォーマンスを監視する必要もある。それは、データの可搬性や削除に係る方針が、要件を満たしていなければならないからだ。

クラウドのセキュリティ課題に向けた取り組み

クラウドのセキュリティ課題にいざ取り組むとなれば、政府機関は潤沢なリソースを持っているという。ウェルシェン氏によると、NIST（米国国立標準技術研究所）が様々な機関と協力し、データ保護基準の明確化とともに優先順位の整理を行った上で、政府の情報保護に向けたガイダンスを作成しているという。

この取り組みに、GSA（米国共通役務庁）も大きく貢献している。政府全体で共通となる調達方式を整備し、クラウドベースのソリューションを開発したのだ。そして DHS（米国国土安全保障省）は、連邦政府全体を見渡し、日々の業務においてセキュリティが保持されているかどうか、監視する役割を担っている。

クロスランド氏によると、こうした機関のうちいくつかが国防総省と協力し、FedRAMP を策定したという。FedRAMP とは、クラウドサービスのセキュリティ管理を評価、監視するにあたり、そのアプローチを標準化したものだ。

最終的には、クラウドスプロールの管理、クラウド環

境の監視、そしてセキュリティにおける脆弱性の検知をリアルタイムで行えるよう、これを可能にするツールの導入が必要となります。ニュータニックスに代表される SaaS ツールを導入すれば、セキュリティやコンプライアンスに係る業務の自動化が可能という。

理想的な SaaS ツールが持つ特長として、ニュータニックスのファーロンは次の点を挙げている。

●迅速な導入―― SaaS ツール自体がクラウドでホストされるため、実質的にも即座の導入が可能。
ファーロン 「監視ツールのためだけに、バックエンドインフラストラクチャ全体の構築はしたくないでしょう。仕事は増やしたくないものですよね」

●包括的なセキュリティとコンプライアンス――クラウドの目的はものごとをシンプルにすること。クラウドセキュリティツールも例外ではない。
ファーロン 「ガバナンスとオペレーションを、クラウド環境全体で標準化する必要があります。ですから、クラウド環境の監視を継続的かつリアルタイムに行わなければなりません。また、ハイブリッドアーキテクチャにおいては、オンプレミスからパブリッククラウドまで網羅するツールが必要です」

●リスクフリートライアル――SaaS ベースのセキュリティツールは、インフラストラクチャのサポートを必要としないため、ニュータニックスは無料でトライアルを提供している。
ファーロン 「SaaS プラットフォームの素晴らしい点は、ダウンロードや設定の手間がないことです。つまり、オンラインのトライアルを提供できるのです。実際には、パブリッククラウドの認証情報を入力すれば、セキュリティ管理だけでなく、コスト管理についても十分なサポートを受けることができます」

●レポートと修正の自動化――クラウドセキュリティツールは、変化し続ける環境に適応できなければならない。脅威を検知するだけでなく脆弱性をリアルタイムで修正するため、自動化の力を大いに活用する。
ファーロン 「インシデントに際してはレポートと修正が必要ですが、人間による操作はできる限り少ない方が望ましいと思います」

＊

ファーロンは続ける――「セキュリティは、クラウドプロバイダーと政府機関、双方の責任です。正しいツールセットを採用すれば、セキュリティコンプライアンスや監視など、政府機関側の負担軽減につながるでしょう」と話した。

（2020 年 3 月 23 日 , THE FORECAST by NUTANIX）
記事構成：ニュータニックス・ニュース！ 編集部 , Nutanix Japan

＊カルヴァン・ヘニック氏はフリーライター。BizTech、Engineering Inc.、Boston Globe Magazine などに寄稿している。

NUTANIX
YOUR ENTERPRISE CLOUD
お問い合わせ：03-4588-0520
info-jp@nutanix.com | www.nutanix.com/jp | @NutanixJapan
東京都千代田区大手町 1-1-1 大手町パークビルディング 7F