トレンド

ガートナー・ジャパン

ビッグ・データ環境にはデータ中心型のセキュリティが必要であるとの見解を発表

本年6月、ガートナーは、昨今の複雑化するセキュリティ環境を単純化するために、情報セキュリティ最高責任者(CISO)はビッグ・データのセキュリティと従来のセキュリティを分けて考えるのではなく、すべてのセキュリティをカバーするポリシーを策定する必要があるとの見解を発表した。

データ中心型のセキュリティ

ガートナーは、2016年までの間に企業・組織の80%以上が、データ・サイロ横断型の統合データ・セキュリティ・ポリシーの策定に失敗し、結果として法令を遵守できず、セキュリティ違反、社会的責任の追及につながる恐れがあると予見している。

ガートナーの主席リサーチ・アナリスト、ブライアン・ローワンス氏は、「従来、企業はデータを、構造化サイロと非構造化サイロの枠内で管理してきましたが、これにはリレーショナル・データベース管理システム(RDBMS)、ファイル・ストレージ・システム、非構造化ファイルの共有などが不可欠でした。しかし、ビッグ・データとクラウド・ストレージ環境の登場によってデータの格納、アクセス、処理の方法が大きく変わりつつある今、CISOは『データ中心型のセキュリティ』を考える必要があります。残念ながら、現在このようなアプローチは一般的ではありません。また、データ・セキュリティ・ポリシーとその管理構造が確立されていないため、プランニングが欠かせません」と語っている。

CISOは信頼できるチーム・メンバーと連携し、企業全体を網羅したデータ・セキュリティ・ポリシーを策定し、データ・レジデンシの要件、各関係者の責任範囲、ビジネス・ニーズ、データ・プロセス・ニーズ、セキュリティ・コントロールを定義する必要がある。

管理構造を確立していく

ガートナーのリサーチ担当バイスプレジデント、アール・パーキンス氏は「データ・サイロ全体を通じてデータ・セキュリティのガバナンス(統制)ポリシーの重要性も大きく高まりつつありますが、現在のところ市場には、CISOが一貫性をもってすべてのサイロを管理するために必要な『データ中心型の監査と保護(DCAP: Data-Centric Audit and Protection)』を実現するソリューションがありません。このため、サイロごとに異なるツールが使用されており、これらのツールごとに機能、ネットワーク・アーキテクチャ、データ・リポジトリが異なるため、全社規模のデータ・セキュリティ・プランを実装することが難しくなっています」と語っている。

クラウド・サービス・プロバイダーやセキュリティ・ベンダーが利用するパブリック・クラウド・サービスとインフラ基盤も、このデータ・セキュリティ・プランをさらに複雑化させる要因となる。ベンダー各社は、オンプレミス(自社運用)環境とクラウド環境の双方を通じて異なるサイロ・リポジトリに適用できる製品の開発に取り組んでいるが、まだユーザー側がこのレベルにまで達していない。前出のブライアン・ローワンス氏は、「企業の各部門の責任者は、セキュリティ・チームと連携することに慣れていないかもしれません。そのため、CISOは各部門の責任者と信頼関係を構築し、データ・セキュリティの管理構造を確立し、各部門を横断した教育、研修の必要性を明確にする必要があります」と語っている。

●お問い合せ先●
ガートナー・ジャパン㈱　広報室
TEL：03-6430-1888
URL：http://www.gartner.co.jp/