サイバーセキュリティーの対応

DX推進における勘所(3)

見澤 博樹（みさわ・ひろき）コンサルティング事業本部業務ITコンサルティング部 マネージャー

DX（デジタルトランスフォーメーション）推進の際、サイバーセキュリティーの対応は外せない。サイバーセキュリティー対応の最初のポイントは経営層によるサイバーセキュリティーの理解である。DXの推進に際して方が一サイバーセキュリティーに関する問題が発生してしまっては、DXによるデジタル化がかえって経営に悪影響をもたらすことになりかねないためである。

サイバー攻撃や内部犯行により、企業内の機密情報、個人情報、顧客情報の漏えいや、システムダウンなどによるサービス自体の停止がひとたび発生すれば、社内の混乱はもちろん、顧客や取引先からの信用喪失につながる。一方で、昨今ではさまざまな調査でサイバーセキュリティー上の脅威の増大が示されている。

今回は、DX化に向けたサイバーセキュリティー対応を行う上でポイントを三つに絞ってお伝えしたい。

①管理体制の構築・サイバーセキュリティー対策の検討や、日々のリスクを監視する体制を構築するには、まずサイバーセキュリティーを統括する責任者と組織を組成し、役割と責任を明確にすることが重要となる。対象となる人材確保や社内教育が難しい場合は、役割の一部を外部委託することも可能である。

②脅威の認識・サイバーセキュリティー対策を検討する際に、そもそも守るべき情報は何かを明確化したうえで、「社内外に存在する脅威は何か」を認識し、それぞれの脅威への対策を検討することが重要である。内部脅威の例としては、誤操作、デバイス紛失、管理ミスなどが挙げられ、外部脅威ではサイバー攻撃、不正アクセス、盗聴、自然災害など多岐にわたるが、把握した脅威ごとに、適切な対策を立てることが求められる。

③ゼロトラスト・最後に今後のサイバーセキュリティー対策を検討する上で参考にすべき「ゼロトラスト」という考え方を解説する。従来のサイバーセキュリティー対策は、社内ネットワークを社外から隔離し、ひとたびネットワークに入れば自由にアクセスできる反面、万が一不正に侵入された場合の情報漏えいリスクがある。「ゼロトラスト」は社内と社外の境界に囚われず、データにアクセスすることに対し認証を実施し、データそのもののセキュリティーを担保する。テレワークなどインターネット経由で業務をするのが当たり前な時代における新たなサイバーセキュリティーの考え方となる。

次回はDXを実現させるための経営のコミットメントについて解説をする。

（毎週木曜日に掲載）