特集「サイバーセキュリティ」の発行に寄せて

宮　下　　尚

昨今，様々なものがデジタル化され，利用・共有されるデジタルトランスフォーメーションが急速に進展しており，大量のデータが企業システムやクラウドサービス上に蓄積されてきている．このようなデータは，インターネットにより相互に連携されることで大きな付加価値を生み出すための利活用が進んでおり，既存構造を覆すようなイノベーションを起こしている．

一方で，標的型攻撃による重要情報の窃取，仮想通貨のマイニング処理に代表されるコンピュータリソースの不正利用，特定企業をターゲットとしたサービス不能攻撃といった様々なセキュリティリスクを包含してもいる．このようなサイバーセキュリティリスクへの対応は，今やデータの利活用が自社ビジネスに必須となっている企業にとって，重要な経営課題であり，必要欠くべからざるものとなった．デジタルトランスフォーメーションによる新たなビジネスの創出展開とサイバーセキュリティリスクへの対応は表裏一体として取り組む必要がある．

また，サイバー攻撃は，年々その巧妙さを増しており，様々なサイバー空間の出入口から，企業ネットワークへの侵入を試みている．侵入後の活動についても，単純にデータを窃取するだけでなく，定常的にデータが攻撃者へ送付されるような仕組みを組み込むなど，より悪質なケースも見受けられる．侵入の手口が判明し，対応が取れるようになると，その対応を迂回するような新たな手口が出てくるなど，攻撃側と防御側でのイタチごっこ状態が継続している．更にクラウドサービスの利用拡大，働き方改革の推進等により，コンピュータリソースやデータの配置といった自社の ICT 環境に大きな変化が生じ，従来のセキュリティ対策の見直しも迫られている．

サイバー攻撃への対応については，完璧になるということはなく，日々，セキュリティ対策を怠るわけにはいかない状況である．多くの企業では，ISMS 認証等に代表されるセキュリティマネジメントシステムの構築やセキュリティソリューションの導入を中心とした技術的な防御対策が実施されてきたが，より早くサイバー攻撃の脅威やインシデントを検出し，被害を最小限にとどめるダメージコントロールの対応についても，その必要性が増してきている．これらのサイバーセキュリティ対応は，企業として事業を継続していくために，必要不可欠なものであり，具体化された戦略に基づくサイバーセキュリティ経営の確実な実践に加え，事故発生前提の考え方に基づく，サイバー BCP の確立が強く求められている．

弊社は，従来から実施してきたお客様システムの開発や運用保守業務に加え，ビジネスエコシステムを形成することで社会課題を解決するための新たなサービス型ビジネスの展開を図っており，それらの基盤となるサイバーセキュリティの重要性を強く認識している．そのため，経営レベルの取り組みとしてサイバーセキュリティ戦略を策定し，継続性を持って実行してきた．これまで弊社が取り組んできたサイバーセキュリティ戦略，およびその主要な活動内容を紹介し，弊社の活動から得られた知見や課題を共有することで，サイバーセキュリティの推進

に寄与できれば幸いである.

（執行役員　CRMO・CISO・CPO）