◆ *Risk Solution NEWS TODAY No.31* （発行：平成３０年７月１７日）

「サイバー攻撃」に伴うリスク　～ 経営者に求められる責任 ～

2018 年 5 月、巨額の制裁金条項と広範な域外適用ルールを備えた GDPR（一般データ保護規則）が施行され、EU 諸国に拠点がある、または情報のやり取りがある域外の企業において、高い基準でのデータ保護の取り扱いが求められるようになった。しかしながら、グローバルに活躍する日本企業の多くが、2018 年 5 月の時点で GDPR への対応だけでなく、国内においてもデータ保護への十分な対応ができているとは言い難い。海外と比べ対応が後手に回っている日本企業において、サイバーリスクの影響と対応策を今一度考える必要がある。

１．新たなサイバー攻撃

IoT（Internet of Things）の拡大により、スマホ、タブレットなどの携帯端末の普及、SNS や AI 技術の革新などインターネットで出来ることが増え、取り扱う情報量が飛躍的に増大している。それは同時にサイバー攻撃の対象にさらされる情報や機会が増大していることを意味する。日本で通信教育大手企業から約 3,000 万件もの個人情報が流出し、米国では世界的な SNS の利用者情報約 8,700 万件が流出した事故が記憶に新しい。このような企業にとってのセキュリティの脅威の内容を見てみると、「標的型攻撃による被害」「ランサムウェアによる被害」が引き続き上位を占める一方、「ビジネスメール詐欺」や「脆弱性対策情報の悪用」※等、新しいサイバー攻撃の脅威が発生していることが分かる（下表参照）。これらの脅威に対する対応は事前に対応することには一定の限界があり、畢竟リスクの顕在後に対処せざるを得ないケースが多い。そこで事前のデータ保護やセキュリティ対策と同時に、ある程度被害を想定した事後の対応が重要である。

※「ビジネスメール詐欺」・・・・他社の担当者になりすまし、誤った口座にお金を振り込ませる手法
「脆弱性対策情報の悪用」・・・ソフトウェア販売会社が既存ソフトの脆弱性を公表の上、アップデートファイルを配布した後、端末でアップデートを実施されるまでの間に脆弱なポイントから攻撃を仕掛ける手法

■「情報セキュリティ１０大脅威 2018」

2018 年順位	「組織」向け脅威	2017 年順位	前年比
１位	標的型攻撃による被害	１位	-
２位	ランサムウェアによる被害	２位	-
３位	ビジネスメール詐欺による被害	ランク外	↑
４位	脆弱性対策情報の公開に伴う悪用増加	ランク外	↑
５位	脅威に対応するためのセキュリティ人材の不足	ランク外	↑
６位	ウェブサービスからの個人情報窃取	３位	↓
７位	IoT 危機の脆弱性の顕在化	８位	↑
８位	内部不正による情報漏えい	５位	↓
９位	サービス妨害攻撃によるサービスの停止	４位	↓
10 位	犯罪のビジネス化（アンダーグラウンドサービス）	９位	↓

出典：　独立行政法人情報処理推進機構「情報セキュリティ10大脅威2018」より　弊社作成

2．経営者が直面する新たなリスク

1）サイバー攻撃による被害

従来はサイバー攻撃を受けた場合の損害は、ウィルスの感染や個人情報の漏えい、ホームページの改ざん、サーバーダウン等の間接的な費用損害が主であったが、近年ではランサムウェアによる身代金請求や仮想通貨・電子決済システムへのハッキング等による不正送金など、直接的な経済損失をもたらすものが増えてきている。また、企業や個人の PC を踏み台として、なりすましによってウィルス感染や詐欺を行う等、その手口も巧妙化してきている。

■ サイバー攻撃による直接的損害の例

●2018 年 4 月	メキシコ銀行において電子決済システムの不正利用で 4 億ペソ（約 22 億円）が不正転送された。
●2018 年 1 月	利用者から預かっている約 580 億円相当の仮想通貨が不正アクセスにより消失。460 億円を手元資金で返金した。
●2017 年 9 月	金融会社の担当者になりすまして送付された偽の請求書により、3.6 億円を指示通り振込んだところ、回収不能となった。

2）役員に求められるサイバーセキュリティ

サイバー攻撃に対する役員の責任についても変化してきている。2014 年 11 月に制定された「サイバーセキュリティ基本法」において、国、公共団体、一部の重要基盤事業者に対しサイバーセキュリティに関する法整備をなされ明確な罰則が設けられた。更に 2017 年 11 月に経済産業省から公表された「サイバーセキュリティ経営ガイドライン ver2.0」においては、『サイバーセキュリティへの投資は必要不可欠、かつ経営者としての責務』と、サイバーセキュリティへの対応が経営者自身の義務であると明確化されている。

一般的な株式会社の場合、会社の運営に係る役員は「その任務を怠ったとき」かつ「故意・過失があり、損害との間に因果関係があるとき」に会社法第 423 条に則り、その法律上の賠償責任を追及される可能性がある。従来サイバーセキュリティについては、その責務が必ずしも明確ではなかったため、役員がサイバー対策に対する責任を負う可能性は低かったが、今後はその取り組みを怠ると民法第 644 条（善管注意義務）違反と判断とされる可能性が高くなった。そのため、サイバー攻撃に対する適切な対策を講じなかった場合には、役員個人に対しても、賠償責任が発生し求償される可能性があることに注意が必要である。併せて役員が十分な対応をしていたにも関わらず発生した損害による株主代表訴訟に対しては、万一の備えとして役員賠償責任保険（D&O 保険）へも加入を検討しておくことをお勧めしたい。

■ 関係法令一部抜粋

会社法第 423 条･･･	取締役、会計参与、監査役、執行役又は会計監査人は、その任務を怠ったときは、株式会社に対し、これによって生じた損害を賠償する責任を負う。
民法第 644 条･････	受任者は、委任の本旨に従い、善良な管理者の注意をもって、委任事務を処理する義務を負う。

【ニュースに関するお問い合わせ先】
銀泉リスクソリューションズ㈱　E-mail：　grs@ginsen-gr.co.jp
〒102-0074　東京都千代田区九段南 3-9-14　TEL03-5226-2301　FAX03-5226-2609