（8月6日発表）

デジタル時代のビジネスリスクマネジメント
～企業経営者が取り組むべき課題～

ビジネスリスクマネジメント委員会
（2018年度）
委員長
遠山 敬史

デジタル化の急速な進展の中でサイバー脅威への対応が企業経営者にとって喫緊の課題となっている。本委員会では、サイバーセキュリティを取り上げ、特にあらゆるモノがインターネットでつながるIoTの急速な進展に注目し、サイバー攻撃の現状把握とともに、企業経営者はどのようなリスクマネジメントに取り組むべきかという視点を持って活動してきた。本報告書は、企業経営者にサイバーセキュリティへの理解をあらためて促すため、最低限取り組むべきことを整理して、取りまとめたものである。

Ⅰ サイバーセキュリティ

1.企業が直面するサイバー脅威 ──IoTの進展、グローバルにサプライチェーンが展開する中で

・デジタル化が急速に進展する現在、あらゆる情報がデータ化され、インターネットを通じて、グローバルに海外子会社や委託先、取引先などとつながっている。また、クラウドコンピューティングも普及し、今やITシステムなしの企業経営は想定することができない。
・こうした中で、ITシステムは、日々刻々と高度化・巧妙化するサイバー脅威にさらされており、機密情報や個人情報の漏洩（ろうえい）やデータ改ざんのほか、システムの稼働停止による事業活動全体の停滞といった企業経営にとって極めて重大な影響を及ぼすおそれがある。
・また、ここ数年、IoTが進展し、ターゲットとなるIoT機器の増加によって、ウェブカメラが乗っ取られるなどサイバー攻撃の件数も急増している。委託先のネットワークがサイバー攻撃を受けたり、製品に組み込むために委託先から購入した部品がマルウェアに感染していたりするなど、ビジネス全体に多大な影響を及ぼすサプライチェーンリスクも企業経営における喫緊の課題である。
・われわれ企業経営者は、こうしたサイバー攻撃を企業価値や企業の存立への重大な脅威として捉え、常に対峙していく必要がある。

2.企業経営者はサイバーセキュリティにどうコミットしていくべきか

(1) 企業経営者のマインドセットを直ちに変革すべき

・サイバー攻撃は、長年にわたって創造してきた企業価値やブランド、信頼を一瞬で破壊しかねない、企業の存立や持続可能性への重大な脅威である。企業経営者はこの重大な脅威に対して危機感を持つべきである。
・サイバーセキュリティは、BCP（事業継続計画）やリスクマネジメントの一環であることを超えて、将来に向けた積極的な企業の成長戦略への投資として喫緊に取り組むべきである。

(2) サイバーセキュリティへのアプローチの転換を

・機密性を重視した「情報セキュリティ」とともに、システムが継続的に稼働できる可用性をも重視した「サイバーセキュリティ」を意識した対策を講じるべきである。
・サイバー攻撃に対しては、100%完璧なセキュリティ対策はあり得ないことを前提として、不正侵入の早期発見と被害の最小化に向けて、直ちに復旧させるレジリエンスの考え方を採るべきである。

(3) 全社挙げての横断的な取り組みを

・「ITシステムはテクノロジー特有の分野にかかわる」「IT部門に任せておけばよい」という先入観や部門任せの考えを捨て、全社挙げての横断的な組織体制を構築するべきである。

3.IoTにかかわるサイバーセキュリティ

(1) 製品サイバーセキュリティ：ライフサイクルに応じた対策を

・現在、ネットワークにつながった膨大な数の製品を踏み台にして、サイバー脅威が拡散していく事態が生じていることから、製品開発、製造、市場運用というライフサイクルに応じた対策を講じる必要がある。

●製品開発・設計段階：セキュリティ・バイ・デザインの発想を

想定されるサイバー脅威を分析した上で、製品にはどのような機能を持たせるべきか、その機能を持たせるためにはどのような設計をするべきかというアプローチを採る必要がある。

●製造段階：サプライチェーン全体を挙げての対策を

自社だけでなく、外注先などを含めたサプライチェーン全体で、IoTにおけるサイバーセキュリティに対する感度を高め、全体で取り組むことができる実効性がある対策を講じなければならない。

●市場運用段階：平時からの対応検討を

製品が市場に出荷された後に第三者から製品の脆弱(ぜいじゃく)性を指摘された場合に、平時からどのように対応をするべきかを考えておく必要がある。その際、特に製品製造部門や品質管理部門と連携しながら、製造や販売する製品の脆弱性に対応するためのチーム（PSIRT：Product Security Incident Response Team）の構築が有効である。

(2) 制御システムセキュリティ：可用性を重視した対策を

・特に制御システムでは可用性が重視され、システム停止の回避と安定稼働が最優先となる。そのため、制御システムに関するサイバーセキュリティを考える上では、想定される脅威とその脅威が顕在化するシナリオとしてどのようなものが考えられるか、どの段階で検知できるかを分析することが重要である その上で、早期にサイバー攻撃を検知できる体制を構築するとともに、検知後の対応が重要となるため、平時から訓練や研修を行い、対応能力を高めていかなければならない。

4.社会全体としてのサイバーセキュリティへの取り組みを

・サイバー攻撃が社会全体に対する脅威であり、積極的にセキュリティ対策に取り組んでいくためにも、企業同士でサイバー攻撃に関する情報共有や分析を行い、セキュリティ対応の向上に取り組んでいくISAC（Information Sharing and Analysis Center）のような組織を活用し、自社の対策を検討する際に他社事例を参考にしていくことが有用かつ重要である。

Ⅱ IoTの進展に伴った国境を越えた個人データの移転
― GDPRなどのグローバル・ルールへの対応

・IoTの進展に伴い、モノが個人情報を含むさまざまなデータを収集し、そのデータが国境を越えて移転していく時代が到来している。その中で、世界では個人データの越境移転規制に関するルールの制定が急速に進んでおり、グローバルに展開する日本企業もその対応を迫られている現状を企業経営者は当然把握していなければならない。

・EUの一般データ保護規則（GDPR）やeプライバシー規則案、中国のサイバーセキュリティ法、カリフォルニア州の消費者プライバシー法など、企業経営者は、個人データ保護法制を含むデータ法制に関する動向を絶えず注視し、対応していかなければならない。

Ⅲ デジタル化、AI化、IoTの進展の中でのビジネスリスクマネジメント
― ITを活用した「コンプライアンスの実現を」

・デジタル化、AI化、さらにはIoTが急速に進展する現在、ITを活用したコンプライアンスの実現を目指すことが急務である。

・こうした最新の技術を活用したモニタリングや分析手法は、不正に対して　極めて強い抑止力を有し、仮に不正が発生した場合でも、異常値の検出などを捉えることによって、早期に発見され、財産的な損害のほか、企業のブランドや信頼の低下など、被害の最小化に大きく貢献するはずである。

・一方、モニタリングが行き過ぎると、プライバシーや個人の尊厳の侵害につながる可能性もあることも認識する必要がある。企業経営者は技術の進展に伴って生じる倫理の問題を常に真摯(しんし)に考え続け、人間中心の社会の構築につながる価値創造に挑むとともに、透明性を高めたコンプライアンス体制の構築・運用に努めていくべきである。

詳しくはコチラ