「サイバーセキュリティリスクへの法的対応～事前準備の重要性～」

Smith Gambrell Russel（SGR）法律事務所

2022 年 2 月 現在

タイトル

サイバーセキュリティリスクへの法的対応～事前準備の重要性～

概要

昨今日本でも大きな話題となっている企業に対する「サイバー攻撃」。顧客や従業員等の個人情報の漏洩は企業の社会的評価を含め甚大な損害をもたらします。本稿では、法的観点から、サイバーセキュリティリスクに企業はどのように向き合っていくべきかにつき解説します。

はじめに

2021 年夏に開催された東京オリンピック・パラリンピックの期間中、大会運営に関わるシステムやネットワークに対して合計 4 億回を超えるサイバー攻撃が行われたことが大きな話題となりました（実害は発生せず）。また、大企業がいわゆるランサムウェア攻撃[1]を受け、ハッカーに対して身代金を支払ったという事案[2]も決して珍しいものではなくなりました。

このように、サイバー攻撃への備え、すなわちサイバーセキュリティの構築はいまや企業にとって喫緊の課題となっているといえます。しかしながら、自社サーバーのセキュリティを強化するといった技術的な対応策は思いつくとしても、法的に企業が（ひいては善管注意義務を負う役員が）どのような行動を取ることが必要か、という点については必ずしも明確に把握していない企業関係者の方も多いのではないでしょうか。

[1] 悪意あるソフトウェア／コードを指すマルウェアの一つであり、感染したコンピュータの利用者のシステムへのアクセスを制限する。利用者のアクセスを制限したうえで、解除のために（個人情報の公開を交渉材料にする場合もあり）身代金の支払いを要求するパターンが典型的です。

[2] 米国では 2021 年だけでも、コロニアル・パイプライン社や JBS Foods の米国子会社に対するランサムウェア攻撃の結果、当該企業が数百～数千万ドル規模の「身代金」を支払うに至ったという事件が発生しています。

今回は、サイバーセキュリティリスクへの企業としてのあるべき対応策について、法的観点からご紹介します。なお、サイバー攻撃の手法については、日々複雑化、変化を重ねており、企業として求められる対応の内容や程度もリスクの大きさに伴って日々変動するため、（以下にも述べるとおり）常に最新の状況に応じた対策を講じることが必要となってくる点にご留意ください。

サイバーセキュリティリスクと役員責任の関係性

まず前提として、サイバーセキュリティ体制の構築が役員の善管注意義務との関係でどのような意味を持つかを簡単に説明します。

役員が企業／ステークホルダーに対して負う義務（すなわち善管注意義務）は、「企業活動に内包されるリスク」の存在を前提に、「当該リスクを避ける」点にあるといえます。サイバーセキュリティとの関係では、企業活動との関係でサイバー攻撃を無視することはもはやできない昨今の状況に照らすと、具体的にどのようなリスクが存在し、いかにしてそのようなリスクを回避し企業価値を守るかという点の検討及び実行が、役員の善管注意義務の一端として要求されているといえます。

なお、企業活動が内包するリスクに関して、サイバーセキュリティについては、企業活動のグローバル化に伴い、本国のみでなく海外におけるセキュリティも注視する必要がある点に留意が必要です。例えば、海外子会社と日本の親会社が共通のサーバーを使用している場合、海外子会社サイドに対するハッカー攻撃が発生すると、親会社の保有する日本サイドの情報までもが漏洩対象となる、といった具合であり、海外子会社、場合によってはサプライチェーン上に存在する他社のセキュリティ状況の確認までも必要となってくるのです。

サイバーセキュリティ体制構築の重要性

上記のとおり、役員の善管注意義務の観点からも、サイバーセキュリティ体制を構築することは重要な企業課題となります。具体的には、①サイバーセキュリティ事案の発生防止を志向した危機管理体制、②有事を想定した事前準備、及び③迅速かつ適格な有事対応の整備がサイバーセキュリティ体制の要になるといえます。

サイバー攻撃の内容が複雑化・多様化している現在、完全なセキュリティを敷くことは著しく困難です。一方で、企業として、万が一の事象が発生したとしても、事前に尽くせるだけの合理的措置は尽くしていたと主張できること、また、事態発生後に迅速かつ適格な対応を行ったと主張できることが、被害を最低限に食い止める上で極めて重要であることから、「事前準備」がサイバーセキュリティリスクに対峙する企業にとって何よりも重要なポイントであることを意識することが必要です。

以下では、特に事前準備の側面に焦点を当てたうえで、それぞれの対応事項について実務的観点から紹

介していきます。

危機管理体制の構築：組織的な「心構え」の確立

取締役の役割としての明確化

上記のとおり、役員が負う善管注意義務の一端としてサイバーセキュリティ体制の構築・運用を位置付けることができるところ、このことを目に見える形で明確化すること（例：関連社内規定における取締役の管掌事項の一つとして、「サイバーセキュリティ体制の構築・運用」を挙げる等）が重要です。

また、既に欧米では多くの企業が導入しているとおり、取締役会や経営会議等の企業内の重要な意思決定機関における議題に自社のサイバーセキュリティに関する事項を加えることも重要です。なお、実際の検討内容や検討状況について議事録その他の記録を残すことも、万が一の事象が発生した場合の対応を見据える中で必要な対応といえます。

最後に、既に述べたとおり、企業活動の複雑化・グローバル化が進むなか、自社のみでなく関連会社におけるサイバーセキュリティ体制についても注視・監督できる体制を構築することがますます重要になってくるといえます[3]。

人材教育の重要性

この点、役員限りでサイバーセキュリティの重要性を認識するだけでは十分なサイバーセキュリティ体制の構築とはいえません。実務を担う各従業員が、サイバーセキュリティのなんたるか、どのような点に留意すべきかといった点を正確に理解していることが必要となります。

なお、人材教育に際して留意すべきは、管理部門の従業員／現場担当となる従業員それぞれが「各自の役割に応じた」十分な教育を受けられるようにする点です。この点、具体的な教育実施に際して、セキュリティの専門家や法律専門家の指導を仰ぐことも効果的であるといえます。

内部規定の整備

人材教育の点とも関連しますが、社内規定においてサイバーセキュリティに関する社内ルール・心構え

[3] なお、グループガバナンスとの関係では、海外子会社のガバナンス体制に対する過度な干渉は同時に法人格否認（Piercing Corporate Veil）という別途のイシューを生じさせることから、海外子会社の独立性は維持しつつグループ全体として万全のサイバーセキュリティ体制を構築するというバランス感覚に根ざした対応が要求される留意が必要です。

をポリシーとして明確化することは、見落とされがちですが非常に重要なポイントです[4]。具体的には、以下のような内容を規定することが必要となってきます。

・従業員／現場担当者の一般的責務
・規定の適用対象となる情報等の画定
・具体的なセキュリティ対策の内容（情報等の取扱方法や禁止事項の設定）
・有事対応（情報漏洩等発生時の対処手順等）
・社内教育その他の一般的事項等

具体的に社内規定を整備するに際しては、各企業が対面するサイバーセキュリティリスクの性質に応じた内容の検討が必要となってくるため、内部規定整備の重要性に照らすと、外部専門家の助言を仰ぐことも十分合理的な判断といえます。

具体的な対策の導入及び運用

社内研修や会議体、社内規定を通じた体制を整備したうえで、具体的な対策を講じることとなります。ここで具体的にどのような対策を講じるかは、企業の活動内容や取り扱う情報等の性質、既存のセキュリティ状況を踏まえ検討していくこととなります。

冒頭にも述べたとおり、企業／役員は自社の内包するリスクを正確に把握し、これに対処する義務を負うという前提に立ち返って検討を進めることが必要です。例えば、システムに脆弱性が発見されたのであれば直ちにそこへの対処を（更にいえばその前提となる脆弱性有無の確認を）、在宅勤務が増加するなかで従業員の使用 PC についてのルールが明確でないのであれば即刻ルールづくり及び周知徹底を、といった具合に、まずは現状認識、その次に迅速かつ適格な対応という形で対策の導入及び運用を進めることとなります。

その他の事前準備

上記各プロセスの他、自社のサイバーセキュリティリスクが実際のどの程度のインパクトを有するものか（＝金銭的評価／プライシング）を踏まえ、場合によっては、サイバーセキュリティ保険への加入やセキュリティ会社への外部委託等のリスク分散手法を採用することも一つの検討事項になってきます。

[4] この点、一般的に「サイバーセキュリティポリシー」というとウェブサイトに掲載される利用者・顧客向けのポリシーを思い浮かべがちですが、ここでは純粋な社内規定（例えば Information Privacy Policy 等）におけるサイバーセキュリティ関連の規定設定を想定しています。

事後対応について

事後対応については簡潔に述べるに留めますが、まずは状況の迅速な把握及び対策チームの組成（外部専門家への委任を含む）必要であり、これまで述べてきた諸々の事前準備は、有事対応の迅速性確保のためにも存在するといえます。とりわけ情報漏洩に関しては、時間の経過に比例して企業のダメージが拡大していくことから、担当者限りでの処理を試みるといった対応ではなく（そのような対応は却って証拠隠滅等のより不利な状況に企業を貶める恐れが高くなります）、内部共有・外部開示や原因究明その他の再発防止策の策定を含めた方針検討への迅速な移行が必要となります。

なお、とりわけ米国においてはディスカバリー制度が存在し、関係者には証拠保持義務が課せられることから、情報漏えいが発生した場合、事態の把握に加え、関連する資料やコミュニケーションの破棄・改変が生じないように徹底すること（まずはそのような必要があることについての平時からの意識付け）が必要となる点、日本企業が見落としがちな留意点として申し添えておきます。

おわりに

本稿では、近年ますます重大な企業課題となってきているサイバーセキュリティ関連リスクについて、どのように対処すべきかという点について、法的側面から分析を行いました。

冒頭にも言及しているとおり、残念ながら「自社は絶対安全」と断言できるセキュリティ体制を構築することが難しいというのが、現在のハッカー等によるサイバー攻撃の状況を踏まえた客観的な評価になるかと思います。

しかしながら、だからこそ、実務上どこまでできるのか、どこまですべきなのかという点がより重要なポイントになってきており、外部専門家の助言も受けつつ、社内で適切な事前準備体制を構築していくことが、企業の保有する「情報」の価値がますます増大していく現代社会の中で重要な企業の取組事項となるのであり、本稿を踏まえ、企業の皆様が自社・自社グループ（ひいてはサプライチェーン）のサイバーセキュリティ体制について再考する契機となれば幸いです。

※免責事項：上記の内容は、一般的な説明にすぎません。具体的な状況に応じた法的助言または専門家意見として解釈しないようご留意ください。ご不明な点がございましたら、SGR 法律事務所までお問い合わせください。

米国弁護士 小島清顕 kkojima@sgrlaw.com
米国弁護士 猪子晶代 ahewett@sgrlaw.com
交換弁護士 佐賀洋之 hsaga@sgrlaw.com

Smith Gambrell Russel（SGR）法律事務所:

SGR 法律事務所は、1893 年に創設された創業 129 年のジョージア州アトランタ市発祥の米国総合法律事務所です。全米各地にオフィスを構え、約 300 人の弁護士が所属しています。取扱分野は、法人設立、各種契約、M&A・合弁・業務提携、雇用・労務、訴訟・紛争、企業誘致・助成金交渉、 貿易・通商関連、環境、建設、不動産、知財、倒産、税務、遺産相続計画、年金・福利厚生、海事、 サイバーセキュリティ・情報保護法、移民法・ビザ等、企業法務全般をカバーしています。全米法 律事務所ランキング・トップ 200（Am Law 200）にも継続して選出されています。日本チームは、 上記の総合法律サービスを日本語により提供しています。詳しくは、SGR 法律事務所の日本語ページをご参照ください。
https://www.sgrlaw.com/practices/japan-practice-team/

小島　清顕　Kiyo Kojima　パートナー　米国弁護士

日本出身（地元：神奈川県小田原市）、幼少期から米国在住。ロチェスター大学（NY 州）で政治・経済学を専攻。同時期に、イーストマン音楽学校にてファゴットも専攻・学位取得。学位取得後、インディアナ大学ロースクールと音学校に同時進学・卒業。JD 取得後、2003 年からホームタウンのジョージア州アトランタ市を拠点に米国各地で弁護士業務を営む。主に法人設立に伴うご相談、交渉・各種取引アドバイス、合併・合弁・共同開発・ライセンシング案件、雇用・労務案件、紛争防止・対応、知的財産管理・活用、企業誘致・土地選定・助成金交渉、そしてその他各種幅広い法務に対応しています。

猪子　晶代　Akiyo Inoko Hewett　米国弁護士

東京外国語大学外国語学部卒。慶応義塾大学ロースクール修了。

日本の司法試験に合格し、司法修習終了（66 期）。その後渡米し、エモリー大学ロースクールの LL.M.を経て、ジョージア司法試験合格。

現在は、日米の法曹資格を活かし、SGR 法律事務所アトランタ事務所において、契約書の作成・レビュー、M&A、雇用・労務、コンプライアンス、法人設立・維持、訴訟・紛争、ビザ等あらゆる案件で日本語による説明・サポートを提供している。

佐賀 洋之 Hiroyuki Saga　交換弁護士

2014 年東京大学法科大学院修了。2015 年弁護士登録。同年よりアンダーソン・毛利・友常法律事務所外国法共同事業にて執務。コーポレート（株主総会対応・M&A を含む業務提携・グローバル報酬プランの設計等）、国内外のベンチャー企業に対する投資案件、独占禁止法・下請法対応、国内外の訴訟対応等を主たる業務分野として活躍。2021 年米国コロンビア大学ロースクール(LL.M.)修了。2021 年 8 月から SGR 法律事務所にて交換弁護士として執務。