経営者の喫緊の課題

新たなサイバーリスクへの向き合い方

法律事務所クロス
弁護士　山岡裕明

セキュリティインシデントが次々と発生しており，サイバーリスクはどの企業においても看過できない事業リスクとなっている。

このサイバーリスクへの取組みとして，サイバーセキュリティに関する法律，ガイドライン，サービス・インフラの整備が進んでおり，また，予防策および事後対応策についての経験・知見が集積しつつある。そうしたなか，セキュリティインシデントに関する平時・有事の法務対応の重要性が増している。

本稿では，法務として押さえるべきサイバーセキュリティに関する近時の動向を紹介する。

Ⅰ 新たなサイバーリスクとサイバーセキュリティの重要性

サイバー攻撃が多様化し，新たなセキュリティインシデント[1]が次々と発生している。

典型的なセキュリティインシデントとしては，2014年６月に発生した株式会社ベネッセコーポレーションにおける個人情報の漏えい事案（以下「ベネッセ事件」という）に代表される，内部者による情報の持出し事案である。

ところが，近年のセキュリティインシデントの多くは，外部者によるサイバー攻撃を原因としており，その被害の内容は，情報[2]の毀損および漏えいから，不正アクセスによる仮想通貨の流出やインターネットバンキングに係る不正送金といった経済的価値そのものの損害へと広がっている。さらに，ネットワークおよび電子データを前提にますます多くのサービスが構成されていくことを考えると，サービス・インフラの機能障害や，IoT機器の誤作動といった社会経済機能への障害へと被害が拡大することが想定される（**【図表】**参照）。

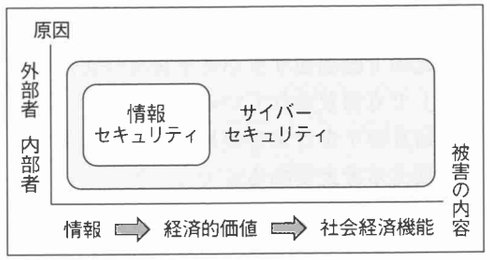
こうした新たなサイバーリスクを受けて，企業が確保すべきセキュリティの範囲は情報セキュリティからサイバーセキュリティへと拡大しており，サイバーセキュリティ体制を整備する重要性はますます増加している。

本稿では，本特集の総論として，サイバーセキュリティを取り巻く近時の法制度の動向を概観するとともに，サイバーリスクに係る企業のリスクマネジメントについて紹介する。

[1]「インシデント」とは，「中断・阻害，損失，緊急事態又は危機になり得る又はそれらを引き起こし得る状況」と定義される（ISO22300：2012）。

[2] 個人情報，営業秘密，それら以外の価値のあるデータを含む。

【図表】原因と被害の内容にみるセキュリティの必要性



Ⅱ 近時の法規制・法改正の動向

サイバーリスクの高まりを受け，近年サイバーセキュリティに関する法改正が積極的に行われている。詳細は別稿「サイバーセキュリティ関連法の改正動向」を参照いただくとして，以下には直近に成立した法改正の概要を紹介する[3]。

1　電気通信事業法及び国立研究開発法人情報通信研究機構法の改正

平成30年５月16日に電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律が成立した。

電気通信事業法に係る改正は，IoT機器を悪用したサイバー攻撃対策として，電気通信事業者間で，第三者機関を通して，サイバー攻撃の指令を出す悪質な機器などの情報を共有することを可能とするものである。

国立研究開発法人情報通信研究機構法（通称「NICT法」という）に係る改正は，国立研究開発法人情報通信研究機構の業務に，パスワード設定に不備のあるIoT機器の調査を含めるもので，この調査によりパスワード設定に不備のある機器（その機器に係るIPアドレス）を特定のうえ，当該IPアドレスを管理する電気通信事業者において，利用者に対して注意喚起等を行わせるものである。

2　著作権法改正

平成30年５月18日に著作権法の一部を改正する法律が成立した。

サイバーセキュリティに関する部分としては，サイバーセキュリティ確保のためのソフトウェアの調査解析（リバースエンジニアリング）を，著作権制限の対象とした（30条の４）。

かかる著作権法の改正は，NICT法の改正とともに，セキュリティ確保の目的であっても従来はその適法性に疑義があった調査行為について，適法に行わしめることを可能とするものである。

Ⅲ 企業・役員の責任

セキュリティインシデントが発生した場合，サイバーセキュリティの確保を怠ったことを理由に企業およびその役員の法的責任が問われることとなる。

かつては，情報漏えい事案において，主に情報漏えいを招いた企業の法的責任が問題となってきたが[4]，近年のセキュリティインシ

[3] サイバーセキュリティ基本法の一部を改正する法律案が平成30年３月９日に第196回通常国会に提出されたが，本稿執筆時点において成立に至っていないので，本稿では割愛する。改正の詳細は，別稿「サイバーセキュリティ関連法の改正動向」を参照されたい。

[4] 情報漏えい事案において法人の責任が問題となった主な裁判例については，拙稿「サイバーセキュリティと企業法務」ビジネス法務2017年10月号～2018年１月号を参照されたい。また，役員の法的責任の根拠については，同じく拙稿「情報漏えいと取締役の情報セキュリティ体制整備義務」中央ロー・ジャーナル14巻３号を参照されたい。

デントの事案では，企業のみならずその役員も，損害賠償請求事件の被告として法的責任が問われるようになっている[5]。

他方で，経済産業省が公開するサイバーセキュリティ経営ガイドラインにおいて，サイバーセキュリティへの意識の高まりが明確に表れている。すなわち，そのVer1.0（平成27年12月28日公開）は，「サイバー攻撃により，個人情報や安全保障上の機微な技術の流出，インフラの供給停止など社会に対して損害を与えてしまった場合，社会から経営者のリスク対応の是非，さらには経営責任が問われることもある」という内容であったところ，Ver2.0（平成29年11月16日公開）では，「サイバー攻撃が避けられないリスクとなっている現状において，経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である」と言及され，経営者の責任についてより踏み込んだ内容となっている。

また，一般社団法人日本経済団体連合会は，平成30年３月16日付けで「経団連サイバーセキュリティ経営宣言」を行い，そのなかで「いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている」とする。

これらのガイドラインや宣言は，セキュリティインシデントが発生した場合の役員の法的責任の根拠となるものではないが，セキュリティインシデントを可及的に防止するためには，役員・経営層が責任を持ってサイバーセキュリティの整備を推進することが極めて重要であるとの社会的なコンセンサスが浸透しつつあることの表れといえる。

Ⅳ セキュリティインシデントに対するリスクマジネジメント

前記の「経団連サイバーセキュリティ経営宣言」でも言及されているとおり，サイバーセキュリティをリスクマネジメントの１つとして捉える考えがある。

一般的にリスクマネジメントとは，リスクについて組織を指揮統制するための調整された活動をいう。企業経営の文脈では，企業経営に伴うさまざまなリスク（自然災害リスク，交通事故や労災事故等）が顕在化すると経済的損失が発生する可能性があり，事業継続に影響を与えかねないので，これらのリスクを適切に管理するための活動をいう。会社法においても，リスクマネジメントは「内部統制のフレームワークを示すもの」と考えられており[6]，リスクマネジメント（リスク管理）体制は，内部統制システムのうち「損失の危険の管理に関する規程その他の体制」（会社法施行規則100条１項２号）に位置づけられる[7]。

ここでいうリスクに，サイバーセキュリティ上のリスクを含めるというものである。

リスクマネジメントの代表的なフレームワークとして，リスクアセスメント→リスク対応というステップがある。リスクアセスメントとは，リスクの特定，分析，評価を行うものであり，このリスクアセスメントをふまえ，リスク対応がとられる。そしてリスク対応には，リスクの低減（最適化），移転，保有（受容），回避という４つの対応方法がある[8]。

以下，サイバーセキュリティを４つのリスク対応に分けて紹介する。

[5] ベネッセ事件において，ベネッセの役員に対して株主代表訴訟が提起されている。また，2018年１月28日に国内仮想通貨取引所コインチェック社から大量の仮想通貨が流出した事件において，複数の訴訟において，同社の役員も被告となっている。

[6] 2003年６月付経済産業省「リスク新時代の内部統制」報告書。

[7] 平成28年８月２日付内閣官房内閣サイバーセキュリティセンター「企業経営のためのサイバーセキュリティの考え方」１頁は，サイバーセキュリティについて「セキュリティリスクの管理も，会社法において取締役会の決議事項になっている『内部統制システム構築の基本方針』の中に含まれると考えられる」とする。

1　リスクの低減（最適化）

リスクの低減（最適化）とは，リスクが顕在化する可能性を減らしたり，実際に顕在化した場合の影響を少なくしようとすることをいう。

サイバーセキュリティについていえば，セキュリティインシデントが発生しないよう人的・技術的・物理的な対応策を講じること，および発生した場合の対応策を事前に定めておくことである。サイバーセキュリティにおいて，最も重要なリスクマネジメントの１つである。

詳細は，別稿「従業員による情報漏えいを防ぐポイント」および「インシデント発生から再発防止までの対応」を参照されたい。

セキュリティインシデントが発生した場合，特にその初動対応段階において社内でかなりの混乱が生じる。技術的な理由から原因の正確な特定が容易でなく，被害実態の把握にも時間を要することに加え[9]，被害関係者，捜査機関，個人情報保護委員会その他の規制当局への報告および対応など，対応事項が複雑多岐にわたるからである。こうした状況下において，誰（どの部門）が，いつ，何をすべきかが明確に定められていないと，混乱が深まり，被害が拡大することとなる。

したがって，リスクを低減（最適化）させるべく，平時から十分に対策を用意しておくことが肝要となる。

2　リスクの移転

リスクの移転とは，リスクの全部または一部を外部に移すことで，リスクが顕在化した場合の影響を抑えることをいい，最も典型的なものは，保険である。保険料を支払うことにより，リスクが顕在化した場合の金銭的損害を保険会社に負担させることで，リスクを移転するというものである。

サイバーセキュリティ分野においても，サイバー保険がある。セキュリティインシデントが発生した場合，対策に要する諸費用（主に調査費用，弁護士費用）および損害額が高額となることが少なくないため，サイバー保険によるリスクの移転は有効なリスクマネジメントの手段となる[10]。

そして，サイバーセキュリティにおいては，リスクの低減（最適化）とサイバー保険によるリスクの移転との間には相互に密接な関係が認められる。

すなわち，サイバー保険の内容によっては，リスクの低減（最適化）を図ることで，サイバー保険の保険料が安くなる（リスクの移転がしやすくなる）[11]とともに，一方で，サイバー保険に加入することで，それに付随したセキュリティサービスの提供やノウハウの共有を受けることが可能となり，結果として，リスクの低減（最適化）につながるという関係[12]にある。

したがって，セキュリティインシデントに

[8] JIS Q 31000：2010（ISO31000：2009）では，リスク対応として，①リスクを生じさせる活動を，開始または継続しないと決定することによって，リスクを回避すること，②ある機会を追求するために，リスクをとるまたは増加させること，③リスク源を除去すること，④起こりやすさを変えること，⑤結果を変えること，⑥１つ以上の他者とリスクを共有すること（契約およびリスクファイナンシングを含む），⑦情報に基づいた意思決定によって，リスクを保有すること，の７つが示されているが，①は回避，②～⑤は低減（最適化），⑥は移転，⑦は保有に分類することもできる。

[9] セキュリティインシデントの原因を調査するフォレンジック調査には数週間から数カ月間を要する。また，被害については，たとえば，漏えいしたクレジットカード情報の不正使用の報告が各カード会社から個別または段階的に届くなど，ただちに被害全体を把握することは困難なケースが多い。

[10] 米国では，証券取引委員会（SEC）が，サイバーリスク戦略の一環としてサイバー保険への加入を推奨している。

[11] たとえば，損害保険ジャパン日本興亜株式会社の2015年12月24日付プレスリリースによると，セキュリティ強化によるISMS認証の取得により，サイバー保険について最大約40%の割引が適用されることとなる（https://www.sjnk.co.jp/~/media/SJNK/files/news/2015/20151224_1.pdf）。

おけるリスクマネジメントにおいては，リスクの低減（最適化）とリスクの移転とが相乗効果をもたらすこととなるのである。

3　リスクの保有（受容）

リスクの持つ影響力が小さいため，特にリスクを低減するための対策を行わず，許容範囲内として受容することをいう。リスクが顕在化した場合の損失が，リスクに対処する費用よりも少ない場合には，リスクを保有（受容）することも経営判断として合理性を有することとなる。

セキュリティ体制の整備にはコストを伴うことから，どこまでセキュリティ体制を整備すべきかを決定するにあたっては，セキュリティインシデントが発生した場合の費用・損失との比較が重要となる。たとえば，B to Bのビジネスモデルのため保有する顧客情報の量が少なかったり，Webサービスを提供していないためセキュリティインデントが発生した場合の営業損害が限定的な企業まで，高度なセキュリティ体制の整備をすることは，必ずしも合理的ではない。そうした場合は，リスクマネジメントとして，セキュリティ対策を行わずにサイバーリスクを保有（受容）することも経営判断として合理性を有することとなるのである。

ただし，前記のとおり，サイバーセキュリティ経営ガイドラインVer2.0において「経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である」という認識が浸透しつつあるなかでは，セキュリティ対策を一切行わずにすべてのリスクを保有（受容）するというよりは，可能な限りリスクの低減（最適化）としてのセキュリティ対策を行い，それでもなお残るリスクを受容するという文脈において考慮されることが多くなると考えられる[13]。

4　リスクの回避

リスクの回避とは，リスクの原因となる活動を行わないことをいう。リスクを保有（受容）することによって得られる利益に対して，保有（受容）することによるリスクのほうが極端に大きな場合に合理性を有する。

たとえば，あるECサイトを運営しているものの，当該サイトによる売上が想定ほど大きくない反面，インターネットを通じたWebサーバーへの不正アクセスによる損失リスクが極めて大きいことが見込まれる場合には，ECサイトの運営を停止するというものである。

山岡裕明（やまおか　ひろあき）
法律事務所クロス，弁護士。2010年弁護士登録。情報セキュリティスペシャリスト。情報法を専門とし，企業のサイバーセキュリティ対応，知財紛争，システム紛争，ドメイン紛争を中心に扱う。

[12] 中沢潔「米国におけるサイバー保険の現状」（JETROニューヨークだより2017年11月）20頁「サイバー保険に加入する大きなメリットは，様々なサイバー被害・被害の補償にとどまらず，保険会社によるリスク管理プロセスにおけるセキュリティ向上計画の策定や従業員に対するデータセキュリティに関する研修サービス，詳細にわたるセキュリティの脆弱性評価などを通じて企業がセキュリティ対策を包括的に見直しサイバーセキュリティ対策や規制コンプライアンスを強化できることにあり，（サイバー保険に加入することで）結果的に企業は将来起こり得るセキュリティインシデントに伴うリスクを最小限に抑制できるとみる声もある」という。

[13] 東京地判平25.3.19判例集未登載は，「いかなる程度のセキュリティ対策を取るかについては，当該セキュリティ対策を取るために必要となる費用や当該サイトで取り扱っている情報の内容とそれに応じた秘密保護の必要性等の程度を勘案して，適切な程度のセキュリティ対策を取ることが必要というべき」と判示し，あらゆるリスク低減策を取ることまでを要求するものではなく，あくまでコストとの比較において，「適切な程度のセキュリティ対策を取ることが必要」とする。逆にいえば，「適切な程度のセキュリティ対策を取った」うえで顕在化したリスクについては，受容することも経営判断として許容されると考えることが可能である。

官民の多様な主体における情報共有の促進を
サイバーセキュリティ関連法の改正動向

内閣官房　内閣サイバーセキュリティセンター
上席サイバーセキュリティ分析官　蔦　大輔

近年，サイバーセキュリティに関する情報を共有する動きが一層活発化しており，近時の法改正においても，情報共有を行うものが見受けられる。このため，それらを中心に近時の法改正の概要を解説するとともに，今後の取組みについて述べる。なお，意見にわたる部分は筆者の私見である。

Ⅰ 情報共有活動の活発化

近年，サイバー攻撃がますます複雑化・巧妙化するなか，サイバーセキュリティに関する情報を一定のコミュニティで共有する動きが一層活発化している。サイバーセキュリティは，本来，各々の組織において取り組むべきものであるが，攻撃が複雑化し，脅威の変化が早い現状においては，一組織の対応では限界があるため，情報を相互に共有することで自組織の取組みを一層高度化したいといった意識が背景にあると考えられる。

サイバーセキュリティに関する情報共有のための体制は，現時点においても複数存在しているところ，代表的なものをいくつか紹介する[1]。

1　J-CSIP（ジェイシップ）

独立行政法人情報処理推進機構（IPA）は，平成23年，サイバー情報共有イニシアティブ「J-CSIP[2]」を発足し，重工や重電等，重要インフラで利用される機器の製造業者を中心として，標的型メール攻撃に関する情報共有を実施している。

2　セプターおよびセプターカウンシル

内閣官房内閣サイバーセキュリティセンター（以下「NISC」という）は，重要インフラ事業者等の情報共有・分析機能を担う組織である「CEPTOAR（セプター）[3]」および各セプターの代表で構成された協議体である「セプターカウンシル」の運営および活動を支援している。

3　ISAC（アイザック）

民間の各業界において，自主的な情報共有

[1] 他にも，一般財団法人日本サイバー犯罪対策センター（JC3）による情報の共有や，一般社団法人JPCERTコーディネーションセンター（JPCERT／CC）による早期警戒情報の提供等がある。

[2] Initiative for Cyber Security Information sharing Partnership of Japan の略。

[3] Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略，平成30年3月末時点において，13分野18セプターが存在している。