新連載　サイバーセキュリティと企業法務

《第1回》

サイバーセキュリティを取り巻く法制度の基本

法律事務所クロス
弁護士 山岡裕明

本年５月中旬発生した世界同時サイバー攻撃は記憶に久しい。報道によると[1]，サイバー攻撃はランサムウェアというコンピュータウイルスを利用したもので，ランサムウエアに感染するとパソコンやサーバー内のデータ（情報）が暗号化されて使えなくなり，元に戻す見返りに金銭を要求するという攻撃である。その結果，英国の病院では手術の中止が相次いだとされ，国内でも被害が確認されている。

とかく技術的な側面が強いサイバーセキュリティの分野であるが，法務の役割も極めて重要である。そこで，本稿では，企業法務の視点から，サイバーセキュリティを取り巻く法制度および法的問題点を紹介するとともに，サイバーセキュリティに関する企業の法的責任を紹介していく予定である。

Ⅰ はじめに

今回のサイバー攻撃による被害の特徴は情報の暗号化というものであったが，サイバー攻撃に関連してこれまで多かった被害は情報の漏えいであろう。

耳目を集めた国内の情報漏えい事案としては，日本年金機構や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があげられる。特に，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（株式会社ベネッセコーポーションおよび同社のグループ会社を総称して，以下「ベネッセ」という）における情報漏えい事案では，情報漏えいに伴う情報セキュリティ対策費として260億円が特別損失として計上されたほか，個人情報が漏えいしたとされる顧客からベネッセに対して損害賠償請求訴訟およびベネッセの役員６人に対して総額260億円をベネッセに賠償するよう求める株主代表訴訟が提起されている[2]。

こうしたサイバーセキュリティを巡る昨今の状況をふまえると，国内外を問わず，またその規模に関係なく，あらゆる企業がサイバー攻撃の脅威に晒されている。また，サイバー攻撃の多様化や被害の甚大さに鑑みると，サイバーセキュリティは全社的に対策を講じなければ到底対応しきれない問題，すなわち，経営判断が要求されるレベルの問題である。

経済産業省は，平成27年12月に初めて「サイバーセキュリティ経営ガイドライン」を公表し，その中で「ビジネスを脅かすサイバー攻撃は避けられないリスクとなっている。そ

[1] 日本経済新聞東京本社版2017年５月16日朝刊３頁。

[2] サイバー攻撃の一義的な定義はないものの，インターネットを経由した外部からの脅威と理解する限りにおいては，ベネッセにおける情報漏えいの原因が再委託先企業の派遣社員による持ち出しであるため，サイバー攻撃によるものではない。しかしながら，広くサイバーセキュリティまたは情報セキュリティに対する脅威という意味においては，看過できないケースであるため，ここに紹介した次第である。

の防衛策には，セキュリティへの投資が必要となる。つまり，企業戦略として，……経営判断が求められる」とし，「サイバーセキュリティは経営問題」と位置づける。

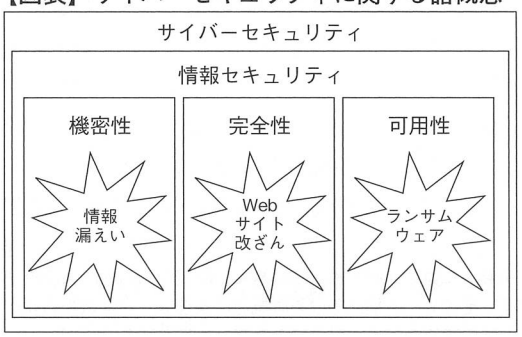
また，内閣官房サイバーセキュリティセンターも，平成28年８月２日付で「企業経営のためのサイバーセキュリティの考え方の策定について」を公表し，その中で「サイバーセキュリティの確保は，企業の経営層が果たすべき責任の一つである」とする。

とかく技術的な側面が強く，企業法務との関連性が乏しく思われがちなサイバーセキュリティの分野であるが，サイバーセキュリティの確保を怠った場合，サイバー攻撃を受けた企業がその法的責任を追及されかねない状況にある。特にサイバーセキュリティの確保が経営判断事項であれば，経営判断にかかわる取締役もその責任を問われかねない。そうだとすれば，企業法務に携わる者としても，サイバーセキュリティは決して無縁なものではない。

Ⅱ サイバーセキュリティに関する諸概念の整理

サイバーセキュリティに関する諸概念を整理してみると，【図表】のようになる。

【図表】サイバーセキュリティに関する諸概念



1　サイバーセキュリティと情報セキュリティとの関係

まず，「セキュリティ」を直訳するとすれば，「安全」である。昨今のサイバー攻撃を始めとする不正行為に関する文脈でいえば，「攻撃や不正行為からの安全を確保するための措置または体制」という意味合いになろう[3]。

次に，サイバーセキュリティの定義についてみると，サイバーセキュリティ基本法は，「……①情報の漏えい，滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに②情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置……が講じられ，その状態が適切に維持管理されていること」（数字については筆者による）と定義する。①はもっぱら「情報」自体に着目したものであるのに対して，②は情報システムや情報ネットワークといったいわゆる情報インフラに着目したものとなっている。

他方，情報セキュリティとは，法令上の定義はないものの，情報処理技術分野においては，企業の情報システムを取り巻くさまざまな脅威から，情報の機密性・完全性・可用性の３要素を確保・維持すること，と定義されることが一般的である。

情報セキュリティがもっぱら情報自体に係る安全の確保・維持に着目した概念であることからすると，情報セキュリティは，サイバーセキュリティにおける①の要素に極めて近い概念といえる。換言すれば，サイバーセキュリティは，情報自体に加え，情報インフラを対象としている点で，情報セキュリティよりも広義の概念ということになる[4]。

2　情報セキュリティの三要素

続いて情報セキュリティの三要素の具体的

[3] 情報システム安全対策指針（国家公安委員会告示第19号）によると，「セキュリティ」とは「犯罪，不正行為，災害若しくは事故による被害を受けること又は情報システムが犯罪若しくは不正行為の用に供されることが防止されている状態をいう」とされる。

内容である。

(1) 機密性

機密性とは，アクセスを認められた者だけが情報にアクセスできることをいう。日本年金機構やベネッセにおける個人情報の漏えい事案は，この機密性にかかわる問題である。

(2) 完全性

完全性とは，情報および処理方法が正確かつ確実であることをいう。昨今度々報道されるWebサイトの改ざん事案は，Webサイト上の情報が改ざんされている点で，情報の正確性および確実性が損なわれているといえ，この完全性にかかわる問題である。

(3) 可用性

可用性とは，アクセスを認められた者が必要な時に情報を利用できることをいう。

先日の世界同時サイバー攻撃で使用されたランサムウェアは，感染した端末内にあるデータ（情報）を暗号化して利用できなくさせる点で，この可用性にかかわる問題である。

Ⅲ サイバーセキュリティに関する法令

サイバーセキュリティに関する法令としては，企業にサイバーセキュリティの体制整備を求める類型と，サイバーセキュリティを脅かす者に法的責任を課すことでサイバー攻撃を牽制・抑止する類型がある。

この２つの類型からわかるとおり，サイバーセキュリティにおいては，企業側のセキュリティ体制の整備と攻撃者への牽制・抑止とが両輪となっている。上記の「サイバーセキュリティ経営ガイドライン」および「企業経営のためのサイバーセキュリティの考え方の策定について」が相次いで公表されたことは，企業側として特に対策を講じなくとも法や捜査機関がサイバー攻撃から守ってくれるという時代ではないことの証左といえる。特にサイバー攻撃の巧妙化[5]により攻撃者の特定が日々困難になっていることを考慮すると，後者の効果は限定的となっており，前者，つまり企業自身による体制整備の重要性が増しているといえる。

以下，サイバーセキュリティに関する主な法令について類型別に紹介する。

1 企業に体制整備を求める類型

(1) サイバーセキュリティ基本法

サイバーセキュリティ基本法は，一部の事業者に対して「自主的かつ積極的にサイバーセキュリティの確保に努める」（同法６条，７条）として努力義務を課している。

(2) 会社法

会社法は，内部統制システムを取締役会・取締役の決議事項としており，大会社，指名委員会等設置会社および監査等委員会設置会社においては，内部統制システムについて決議することが義務づけられている。かかる内部統制システムにサイバーセキュリティに関する体制が含まれると考えられる[6]。

そして，内部統制システムを整備する義務

---

[4] サイバーセキュリティと情報セキュリティとの関係については，一義的な見解があるわけではなく，両概念の対象および機能並びにそれらが用いられる文脈によってさまざまな見解が存在する。そこで，本稿における両概念の整理は，企業法務の観点からサイバーセキュリティを論じるための便宜上の整理であることを付言する。

[5] たとえば，通信経路を匿名化する技術であるTor（The Onion Router）があげられる。

[6] 平成23年４月経済産業省「情報セキュリティ関連法令の要求事項集」６頁によれば，「会社における情報セキュリティに関する体制は，その会社の内部統制の一部といえる。取締役の内部統制構築義務には，適切な情報セキュリティを講じる義務が含まれ得る」とする。

の違反は，取締役の善管注意義務違反を構成すると考えられており，当該取締役個人は会社に対して任務懈怠による損害賠償責任を負い，その任務懈怠に悪意または重過失のあるときは第三者に対して損害賠償責任を負う。

上述のとおり，経済産業省は「サイバーセキュリティ経営ガイドライン」を公表しているところ，このガイドラインは法的拘束力を持つものではないものの，取締役の善管注意義務違反が検討されるうえで１つの重要な指針になる。

⑶ 不正アクセス行為の禁止等に関する法律

不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という）は，後記**2**⑵のとおり，不正アクセス行為を禁止するほか，アクセス管理者に対し，不正アクセス行為からの防御措置を講ずべき責務を定めている（同法８条）。

⑷ 個人情報保護法

個人情報の保護に関する法律（以下「個人情報保護法」という）20条は，個人情報取扱業者に対し，個人データの漏えい，滅失，き損等について安全管理措置を義務づけており，また同法21条は従業者の監督，同法22条は委託先の監督を義務づけ，これらに違反した場合には個人情報保護委員会からの勧告（同法42条１項），さらにその勧告に従わない場合には命令を受ける場合がある（同法42条２項，３項）。この命令に違反した者に対する罰則も規定されている（同法84条）。

⑸ マイナンバー法

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「マイナンバー法」という）は，個人番号関係事務実施者（同法２条13号）に対して，「個人番号の漏えい，滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない」（同法12条）として，個人番号の適切な管理措置を義務付けている。

⑹ 不正競争防止法

不正競争防止法は，後記**2**⑶のとおり，営業秘密を侵害する行為について刑事罰を定めるところ，ある情報が営業秘密に該当するための要件の１つとして，当該情報を保有する企業に対して，「秘密として管理」していることを求めている（同法２条６項）。

2 サイバーセキュリティを脅かす者に法的責任を課すことで牽制・抑止する類型

⑴ 刑 法

刑法は，サイバーセキュリティを脅かす行為を類型化して規定する。なお，以下で登場する構成要件のうち「電子計算機」は「コンピュータ」と，「電磁的記録」はコンピュータによって処理される「電子データ」と表記する。

㋐ 電磁的記録不正作出罪（刑法161条の２）

同罪は，人の事務処理を誤らせる目的で，その事務処理の用に供する権利，義務または事実証明に関する電子データを不正に作る行為を処罰の対象とする。

たとえば，インターネットを介した会員登録において，虚偽の情報を送信し，顧客データベースの顧客データを勝手に作出・変更する行為がある[7]。情報セキュリティの三要素でいえば完全性に関するものである。

㋑ 電子計算機使用詐欺罪（刑法246条の２）

同罪は，コンピュータに虚偽の情報もくは不正の指令を与えて，財産権の得喪・変更に係る不実の電子データを作出する行為等を処罰の対象とする。

[7] 京都地判平９.５.９判時1613号157頁参照。

たとえば，盗んだクレジットカードの番号を悪用して，インターネットを介したクレジットカード決済をする行為がある[8]。情報セキュリティの三要素でいえば完全性に関するものである。

㈢ 電磁的記録毀棄罪（刑法258条，同法259条）

同罪は，電子データを毀棄する行為を処罰の対象とする。

たとえば，不正アクセスを行って，アクセス先のサーバー内の電子データを消去する行為がある。情報セキュリティの三要素でいえば可用性に関するものである。

㈣ 電子計算機損壊等業務妨害罪（刑法234条の２）

同罪は，コンピュータまたはそれに使用される電子データの機能を阻害して人の業務を妨害する行為を処罰の対象とする。

たとえば，DDos攻撃[9]や，上述のとおりランサムウェアに感染させる行為は同罪に該当する。情報セキュリティの三要素でいえば可用性に関するものである。

㈤ 不正指令電磁的記録作成等罪（いわゆるウイルス作成罪。刑法168条の２）

コンピュータに実行させる目的で不正指令電磁的記録（主にウイルス）を作成し，または提供する行為を処罰の対象とする。

ウイルスの機能によっては，情報の漏えい，情報の改ざん，コンピュータの使用不能化といった被害が出ることから，情報セキュリティの三要素でいえば機密性，完全性，可用性のすべてに関するものである。

⑵ 不正アクセス禁止法

ネットワークを利用した不正アクセスを防止するため，同法３条は，他人の識別符号（ID，パスワード等）を悪用する行為（同法２条４項１号）やコンピュータプログラムの不備を突く行為（同法２条４項２号，３号）といった「不正アクセス行為」を禁止し，情報の不正取得の付随行為を処罰すると規定する（同法11条）。

⑶ 個人情報保護法

個人情報データベース等を不正な利益を図る目的で盗用する行為は「個人情報データベース等不正提供罪」として処罰の対象となる（同法83条）。

⑷ マイナンバー法

不正アクセス行為を含む一定の不正な手段により個人番号を取得する行為は処罰の対象となる（同法51条）。

⑸ 不正競争防止法

営業秘密に対する一定類型の侵害行為（同法２条１項４号ないし10号）について，営業秘密の保有者に対し，差止請求権（同法３条）および損害賠償請求権（同法４条）を与えている。さらに，営業秘密侵害罪を犯した者には刑事罰（同法21条）を定め，犯罪行為者が法人の従業員である場合等にはその法人も処罰の対象となることがある（同法22条）。

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，知財紛争，システム紛争，ドメイン紛争，企業の情報管理対応を中心に扱う。

[8] 最決平18.2.14刑集60巻２号165頁参照。

[9] DDos攻撃（Destributed（分散型）DoS攻撃）とは，コンピュータやネットワークに過負荷をかける等によって本来のサービスが提供できなくなることを狙った攻撃であるDoS（Denial of Service）攻撃の一種である。たとえば，過負荷によりサーバーに障害が発生し，Webサイトへのアクセスができなくなるといった被害が発生する。