サイバーセキュリティとコーポレート・ガバナンス

＜ 目 次 ＞

サイバーセキュリティとコーポレート・ガバナンス

<< 要 旨 >>

◎「サイバーセキュリティ」とは、「電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること」をいい、「サイバーセキュリティリスク」とは、「サイバーセキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと」をいいます。

◎ 企業のサイバー分野での情報・技術の利活用が拡大する中、サイバー攻撃の増加や巧妙化などにより、サイバーセキュリティリスクが発現した「サイバーセキュリティインシデント」の発生は増加が続き、その影響が深刻化しています。

◎ 企業のセキュリティ対策の柱は、基本方針である「セキュリティポリシー」と、それを具現化し、実行していく組織の仕組みである「セキュリティマネジメントシステム」です。また、セキュリティ対策は、リスクアセスメントやリスクコントロールといったリスクマネジメントのプロセスに沿って行われ、PDCA サイクルを廻すことが重要です。

◎ 情報漏えいやシステムの機能停止などのサイバー事故は、企業経営と社会全体に大きな影響を与えます。サイバーセキュリティは経営者がリーダーシップを発揮し、企業全体として取り組まねばならない経営問題です。また、サイバー事故を防ぐことは、社会に対する責務であり、企業には、サイバーセキュリティに関するコーポレート・ガバナンス体制の整備・確立が求められています。

◎ リスクの低減などを図るセキュリティ対策を講じても、リスクはゼロにはなりません。こうした残存リスクに関しては、リスク移転の手法として、「サイバー保険」の活用が選択肢のひとつとなります。わが国では、認知度、加入率ともにまだ低い状況ですが、最近は、インシデント対応のサポート機能など、付随サービスも拡充されてきており、サイバー保険市場は今後拡大していくものと思われます。

１．はじめに

グローバルベースで経済・社会のデジタル化やネットワーク化が進展する中、企業にとって IT、AI やビッグデータの活用など、サイバー分野での情報や技術の利活用は、企業価値や国際競争力の維持・強化のために必要不可欠なものとなってきました。そして、それと同時に、企業の事業の成長や継続性を確保するために、経営資源である情報・データ等の情報資産を守るサイバーセキュリティ体制の構築も必須の条件となっています。

また、サイバーセキュリティは個々の企業だけの問題ではありません。企業は、そのステークホルダーをはじめ、広く社会と関わりを持ちながら、事業を展開していますので、サイバー事故が発生した場合、その影響は当該企業内にととどまらず、社会全体に及ぶことになります。年々高度化・巧妙化するサイバー攻撃は、社会全体に対する脅威であると認識されるようになり、国も社会も企業に対するセキュリティ体制確立への要請を強めてきています。企業にとって、サイバーセキュリティは重要な経営課題であるだけではなく、社会全体に対する責務として、コーポレート・ガバナンスの問題ともなっているのです。

今回は、サイバー分野でのリスクとリスクマネジメントの要点を踏まえながら、企業が経営課題およびコーポレート・ガバナンスの問題として取り組まなければならない**「サイバーセキュリティ」**についてレポートします。

２．サイバーセキュリティとサイバーセキュリティリスク

（１）サイバーセキュリティ

① サイバーセキュリティとは

一般的に、企業におけるセキュリティとは、「経営資源を脅威から守り、安全に経営を行うための活動全般」をいいます。では、**「サイバーセキュリティ」**において想定される「守るべき経営資源」とは何でしょうか。「サイバーセキュリティ」とは、「電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること」と定義されます（平成 29 年 11 月公開、 経済産業省／独立行政法人 情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver2.0」、以下、「経営ガイドライン」といいます）。この定義からわかるように、サイバーセキュリティにおいて守るべき経営資源は、電子データやそれらをコントロールする各種システムといった、**「情報資産」**（詳細は後述します）となります。守るべき対象が情報資産であるという意味では、サイバーセキュリティは**「情報セキュリティ」**に包括されており、「情報セキュリティ」の中のサイバー分野に焦点をあてたものと考えていいでしょう。本レポートでは、サイバー関連の論点に重点を置きながらも、可能な限り広く情報セキュリティ上の論点についてもレポートします。

② 情報セキュリティの３要素

では、守られるべき情報の価値とは何でしょうか。情報は**「機密性」**、**「完全性」**、**「可用性」**という３つの要素を備えてはじめてその価値を有するといわれています。情報セキュリティとは、情報が価値を有するためのこの３つの要素を維持すること[1]です。リスクの顕在化によって、このいずれかが損なわれると、情報は価値を失い、企業に損害が発生します。情報セキュリティの３要素については、セキュリティ対策やセキュリティマネジメントの基本として理解しておく必要があります。

ｉ）機密性（Confidentiality）

機密性とは、情報に対するアクセス権限の保護・管理が徹底されている状態にあることをいいます。権限を与えられていない者が情報にアクセスできたり、情報の書き換えができたりすると、機密情報の漏えいや改ざんにつながり、情報の価値が失われることになります。機密性を維持するためには、ウイルス対策や個人認証によるアクセス制御、暗号の利用などの技術的対策、オフィスへの入退室管理などの物理的対策に加え、情報の取り扱いに関する権限規定やルールの徹底といった人的対策も重要になってきます。

ⅱ）完全性（Integrity）

完全性とは、情報が正確かつ完全な状態に保たれていることをいいます。例えば、マルウェア（参照　コラム１：サイバー攻撃の種類）によって情報が改ざんや破壊されると、企業はその情報を利用することができなくなるので、その情報はもはや価値を持ちません。さらに、取引先等に誤ったデータを送信することなどにより、他社に損害を与えるような事態も起こりえます。また、不正アクセスがなくても、情報やソフトウェアが適宜更新されず、古いままで放置されていると、完全性が損なわれている状態になりかねないということにも注意が必要です。

ⅲ）可用性（Availability）

可用性とは、権限を有する者がアクセスしたときに、情報がいつでも使える状態にあることをいいます。サーバーが停止するなど、システムにトラブルが発生すると、この可用性が損なわれることになります。可用性を維持するには、サイバー攻撃などへの備えといった技術的対策の他に、災害時の電源対策などの物理的対策も講じておく必要があります。

③ その他付加的要素

最近では、上記の３要素に、「**真正性**（利用者や情報そのものが本物であること）」、「**信頼性**（システムが不具合なく意図するとおりに稼働すること）」、「**責任追跡性**（利用者の行動が記録され、誰によって行なわれた動作かが後から確認できること）と**否認防止**（利用者がその動作記録を否認できないようにすること）」を加えて、情報セキュリティの６要素（あるいは責任追跡性と否認防止を分けて７要素）とすることもあります[2]。

---

[1] 日本産業規格の JIS Q 27000:2019 の 3.28 に「情報セキュリティ」が定義されています。また、これら３つの要素は英語の頭文字から、情報セキュリティの CIA ともいわれています。

[2] JIS Q 27000:2019 3.28 注記

（２）サイバーセキュリティリスク

① サイバーセキュリティリスクとは

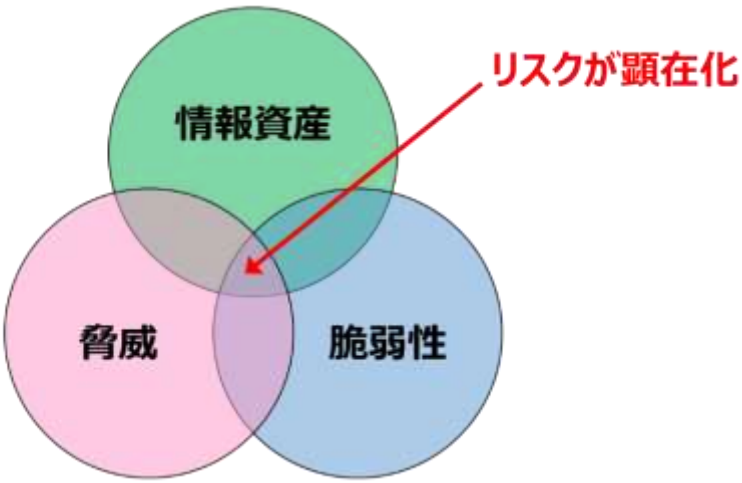
サイバーセキュリティを確立するために、マネジメントされなければならないのが**「サイバーセキュリティリスク」**です。経営ガイドラインではサイバーセキュリティリスクは「サイバーセキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと」と定義されています。リスクを理解することがリスクマネジメントの出発点です。以下では、サイバーセキュリティリスクの理解のために、より広い概念である**「情報セキュリティリスク」**について、その特性を整理していきます。

② 情報セキュリティリスクの３要素

情報セキュリティリスクには、**「情報資産」**、**「脅威」**、**「脆弱性」**という、これらがすべて揃うと「リスクが顕在化」するとされている３つの要素があります（図表１）。したがって、この３つの要素のいずれかを減じさせる方策を講じることが、セキュリティ対策の基本になります。リスクマネジメントの出発点であるリスクアセスメント（３．で解説します）においても、この３つの要素ごとに整理して行われることが、効果的なセキュリティ対策を講じるために大変重要なことです。

＜図表１＞　情報セキュリティリスクの３要素

「情報資産」、「脅威」、「脆弱性」の３要素が揃うと「リスクが顕在化」します。



ｉ）情報資産（Asset）

情報資産とは、情報・データ、ソフトウェア、ハードウェアなど企業経営に必要な資産（経営資源）のことです。なぜ資産がリスクの要素になるのでしょうか。それは、守るべきものがあるということ自体が、それを失うリスクを抱えることになるからです。だからといって、リスクを減らそうと、大事な資産をむやみに処分してばかりでは、企業経営は成り立ちません。まずは、資産管理台帳を作成するなど、自社の保有するすべての「情報資産」を把握することから始める必要があります。そのうえで、自社の事業や事業戦略に必要な情報資産かどうかを整理していくことが重要です。

情報資産には、情報・データやシステム（ハードウェア、ソフトウェア）の他にも、サービス、信用、ブランドなど、有形・無形の保護すべき価値を有するものがすべて含まれますので、これらすべてに同等レベルのセキュリティ対策を講じていくのは現実的には無理があります。そこで、実際のリスクアセスメントにおいては、各情報資産の金銭的な価値に加え、情報の機密性・完全性・可用性などが損なわれた場合に、どれだけの影響を受けるのか、どの程度の損害を被るのかによって、事業運営・継続における優先順位を設けておくことも必要となってきます。

ⅱ）脅威（Threat）

脅威とは、情報資産に事故を発生させる要因のことです。脅威に対応するには、存在する脅威を漏れなく認識しておかねばなりません。その際には、脅威には情報資産の種類ごとに様々なものがあることや、同じ情報資産でも時期や場所によって何が脅威となるかが変わってくることにも注意が必要です。網羅的かつ体系的に脅威を認識するために、脅威を**物理的脅威**、**技術的脅威**、**人的脅威**の３つに分類・整理することが多くみられます。

- **物理的脅威**

  地震や火災、落雷などの自然災害やハードウェアの破損などに起因する脅威を指します。

- **技術的脅威**

  マルウェアの侵入やネットワークへの不正アクセスといった「サイバー攻撃」、これらによるプログラムの不具合の発生などの脅威を指します。

- **人的脅威**

  入力ミス、誤操作、メール誤送信などに起因する脅威を指します。社員などの内部関係者の不正による情報漏えいなども含みます。なお、外部からのサイバー攻撃も人による脅威であるとして、人的脅威とする考え方もありますが、本レポートでは、サイバー攻撃は、オペレーションのミスや内部不正とは異なり、社内教育やルールの徹底・管理といった人的対策だけでは対応が極めて難しいものであるため、技術的脅威に分類しています。

ⅲ）脆弱性（Vulnerability）

脆弱性とは、脅威につけ込まれやすい弱点のことです。情報セキュリティリスクの３要素のうち、情報資産は事業経営において持たねばならず、脅威は自らの努力だけではなかなか減じることが難しいものです。したがって、

情報セキュリティ対策は、この脆弱性をいかにカバーしていくかということが中心になります。脆弱性は情報資産が脅威に耐えうるかどうかの問題ですので、脅威の種類に対応する形で存在します。そのため、脆弱性も脅威の種類に対比させて、**物理的脆弱性**、**技術的脆弱性**、**人的脆弱性**の３つに分類されるのが一般的です。

- **物理的脆弱性**
  建物の耐震耐火構造の不備やオフィスの入退室管理の不備などが該当します。

- **技術的脆弱性**
  アクセス制御の不備、OS やソフトウェアのセキュリティホール（欠陥）の放置などが該当します。

- **人的脆弱性**
  不十分なセキュリティ教育、アクセス権限ルールの不徹底や管理体制の不備などが該当します。

③ サイバー攻撃

サイバー攻撃とは

サイバー攻撃とは、「コンピュータシステムやネットワークに悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと」をいいます（経営ガイドラインより）。情報セキュリティに対する様々な脅威のうちのひとつですが、脅威といえばこのサイバー攻撃を思い浮かべる人も多いのではないでしょうか。情報化社会の進展に伴い、サイバー攻撃は年々高度化、巧妙化してきており、企業経営に深刻な被害をもたらす事件も発生するなど、その脅威は増大するばかりです。わが国のサイバーセキュリティの基本理念を謳った**「サイバーセキュリティ基本法」**（平成 26 年 11 月成立、平成 27 年１月施行）やそれを具体化させた経営ガイドライン等の各方針・施策なども、サイバー攻撃に対する防衛力の向上を主たる軸として、そのためのセキュリティ投資を各組織・企業の責務と位置付けています。

サイバー攻撃の最近の動向

かつては、不特定多数を相手に、それぞれの脆弱性につけ込むマルウェアによる攻撃が主流でしたが、近年ではピンポイントで特定の企業、団体、個人をターゲットにする、不正アクセス、ランサムウェア、DDos 攻撃などによる標的型攻撃（参照 コラム１ ：サイバー攻撃の種類）が継続的に発生しています。手口が複雑化・巧妙化し、攻撃を検知すること自体が難しいものも登場してきており、標的を長期にわたり執拗に追跡する傾向も明らかになってきています。また、特に最近の傾向として、セキュリティレベルが比較的低い海外拠点やリモートワークが広がる中での VPN 製品を侵入経路とする例など、物理的、技術的あるいは人的にセキュリティ対策が手薄となった箇所を狙った攻撃も報告されています。

◆ コラム１：サイバー攻撃の種類 ◆

サイバー攻撃の手法は実に多岐にわたるので、そのすべてを網羅することはできませんが、よく耳にする主なものをあげてみました（体系立てた分類ではありません）。

● マルウェア

コンピュータやネットワークに被害を与えることを目的に作られた不正なソフトウェアの総称です。代表的なマルウェアに以下のものがあります。

・ウイルス

コンピュータに侵入する不正プログラム。利用者がメールの添付ファイルを開いたり、Web サイトを閲覧したりすることで感染します。自己増殖し、宿主となるプログラムを機能不全に陥れます。

・トロイの木馬

正規プログラムを偽装し、利用者にダウンロードさせ、コンピュータに侵入するマルウェアです。

・ワーム

ウイルスと違って、寄生先なしで単体で活動できるので、利用者の動作がなくとも、コンピュータに侵入し、有害な働きをするマルウェアです。また、自己複製により、感染元から被害が拡散する可能性があります。

・スパイウェア

感染したコンピュータの情報を（利用者の意思に反して）収集し、外部へ送信します。

・ランサムウェア

コンピュータに不正に侵入し、機能をロックする、あるいはデータを暗号化するなどした後で、制限や暗号を解除することの引き換えに「身代金」を要求してくるものです。最近では、機密情報を窃取しておいて、身代金が支払われなければ、外部へ流出させるという**「二重の脅迫」**という手口も現れました。

・マクロウイルス

文章作成ソフトや表計算ソフトなどのマクロ機能を悪用して作成されたウイルスです。近年、猛威を振るった emotet（エモテット）もマクロウイルスの一種です。

● 標的型攻撃

主に機密情報を入手することを目的に、特定の企業・組織を狙うサイバー攻撃の総称です。対象の端末をマルウェアに感染させるため、有害ファイルを添付したメールを送り付ける**標的型メール攻撃**や対象先が頻繁にアクセスする Web サイトを改ざんして待ち伏せする**水飲み場攻撃**といった手口があります。

● Dos 攻撃／DDos 攻撃

Dos 攻撃とは標的のサーバーなどに対して、大量のデータを送り付け、標的に膨大な負荷をかけることで、機能を停止させようとする攻撃です。送るデータ自体には不正がないため、受け取る側で正当なデータ送信と峻別して撃退するのが難しいとされています。このうち、より対策を講じにくくするため、攻撃対象を直接攻撃せず、複数の他のサーバーや PC などを中継させて複数拠点から標的を攻撃するのが、**DDos 攻撃**です。

（３）サイバー（情報）セキュリティインシデントの現状

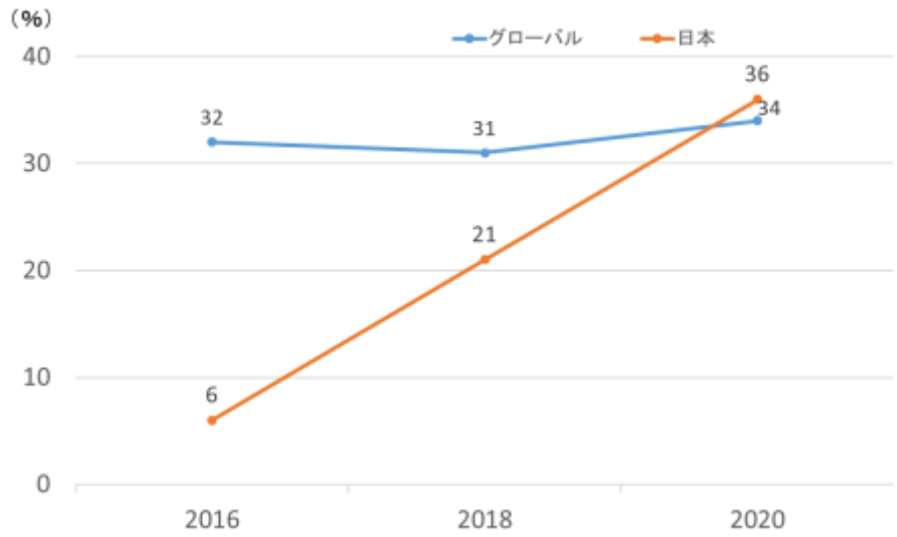
これまで見てきたサイバーセキュリティリスクが発現・現実化した事象のことを**サイバーセキュリティインシデント**[3]といいます。サイバーセキュリティインンシデントは、企業の IT 活用や IoT の拡大、そして、それらを対象としたサイバー攻撃手法の巧妙化や新たな脅威の出現等により、増加の傾向が続いています。統計や調査結果を基に、サイバーセキュリティインシデントの現状を見てみると、サイバーセキュリティリスクが増大し、その影響が深刻化していることがわかります。

① 増加するサイバー攻撃

PwC 社が２年に一度、グローバル規模で行うオンラインアンケート調査によれば、グローバル、日本ともにサイバー攻撃（サイバー犯罪）が増加してきています。特に最近では、日本においてサイバー攻撃が急増しており、2020 年の調査では、調査対象全体の３６%の企業がサイバー犯罪の被害にあったと回答しています。これは２年前より 15 ポイントの大幅な増加となっています。

＜図表２＞「サイバー 犯罪」の被害にあったと回答した組織の比率

（有効回答数 グローバル 5,018社 うち、日本企業 172社）



（出所） PwC Japanグループ「経済犯罪実態調査2020 日本分析版」

[3] 経営ガイドラインの定義より。わが国では、事故と事故につながる可能性がある事象の両方をまとめて、また、偶発的か意図的かを問わずインシデントと呼ぶことが多くなっています。

② 新たなランサムウェア

独立行政法人 情報処理推進機構（IPA）は、毎年、前年に発生したセキュリティインシデントやサイバー攻撃の状況等から、脅威を選出し、専門家等の投票により順位付けした「情報セキュリティ 10 大脅威」を発表しています。それによれば、2020 年において、組織向け脅威のトップは「ランサムウェアによる被害」で、前年の第 5 位から大きく順位を上げています。「二重の脅迫」（参照 コラム 1 ：サイバー攻撃の種類）という新しい手口も顕在化しました。また、個別に感染経路をみてみると、テレワークの普及に伴い、社外からのアクセス手段である VPN 製品の脆弱性を攻撃する事例も多く報告されており、初登場ながら第 3 位の脅威としてランク付けされています（図表 3）。サイバー攻撃は、時代の潮流に乗じ、常に進化し続けているといえるでしょう。

＜図表 3＞ ２０２０年 情報セキュリティ １０大脅威

「個人」向け脅威	順位	「組織」向け脅威	前年順位
スマホ決済の不正利用	1	ランサムウェアによる被害	5
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取	1
ネット上の誹謗・中傷・デマ	3	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
メールやＳＭＳ等を使った脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃	4
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害	3
インターネットバンキングの不正利用	6	内部不正による情報漏えい	2
インターネット上のサービスからの個人情報の詐取	7	予期せぬIT基盤の障害に伴う業務停止	6
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン	16
不正アプリによるスマートフォン利用者への被害	9	不注意による情報漏えい等の被害	7
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加	14

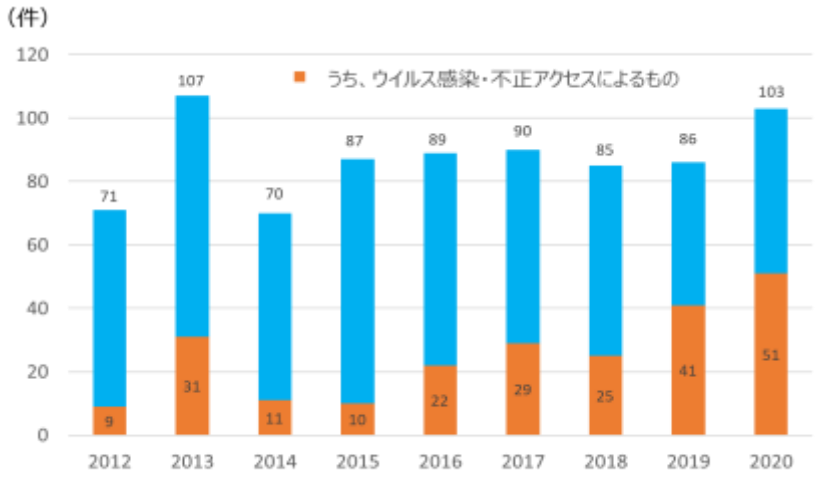
（出所） 情報処理推進機構（IPA）「情報セキュリティ１０大脅威 ２０２１」

③ 情報漏えい・紛失事故

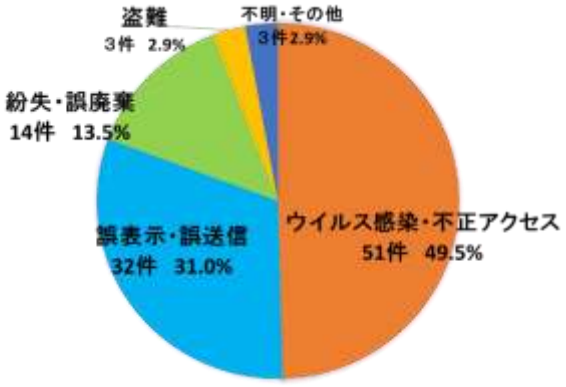
企業へ極めて大きな被害を与えかねない、サイバーセキュリティインシデントの典型的事例が、「個人情報の漏えい・紛失」です。東京商工リサーチ社の調査によれば、2020 年に上場企業（約 3,800 社）とその子会社における、個人情報の漏えい・紛失事故件数（公表ベース）は 103 件（社数 88 社）、漏えいした個人情報は 2,515 万人分となっています。103 件という事故件数は、調査を開始した 2012 年以降で、2013 年の 107 件に次いで 2 番目の多さです。このうち、近年増加の一途を辿っている「ウイルス感染・不正アクセス」などのサイバー攻撃が原因である事故が、51 件（45 社）発生しており、全体の 49.5%を占め最多となっています。質・量ともに増大し続けるサイバー攻撃に対するセキュリティ対策の重要性が、ますます高まっています。

一方で、「誤表示・誤送信」が 32 件（構成比 31.0%）、「紛失・誤廃棄」が 14 件（同 13.5%）と内部関係者の人為的ミスも情報漏えいの主な原因となっていることから、人的脅威および人的脆弱性に対する基本的なセキュリティ対策も大変重要であることがわかります（図表 4、5）。

＜図表 4＞　上場企業グループの個人情報漏えい・紛失事故件数



＜図表 5＞　2020年　個人情報漏えい・紛失事故（計103件）の原因別件数



（出所）　図表 4、5 ともに、東京商工リサーチ社 「『上場企業の個人情報漏えい・紛失事故』調査（2020年）」を基に弊社が編集

３．サイバーセキュリティ対策～セキュリティ体制の構築

サイバーセキュリティとサイバーセキュリティリスクについての基本概念とインシデントの現状を踏まえたうえで、次に「企業において、どのようにサイバーセキュリティ対策を講じ、セキュリティマネジメント体制を確立・整備していけばいいのか」について見ていきましょう。

（１）セキュリティポリシーとセキュリティマネジメントシステム

セキュイリティ対策の推進の柱となるのが、基本方針である**「セキュリティポリシー」**と、それを具現化し、実行していく組織の仕組みや枠組みである**「セキュリティマネジメントシステム」**です。

① セキュリティポリシー

セキュリティポリシーとは

経営ガイドラインにおいて、セキュリティポリシーとは、「企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したもの」で、「セキュリティポリシーに沿って、組織内セキュリティ対策が規定される」とされています。つまり、セキュリティに関する基本方針や行動指針を示し、セキュリティ対策の実施の拠りどころとなるのがセキュリティポリシーなのです。セキュリティポリシーでは、どの情報資産を、どのような脅威から、どのように守るのかといった基本的な考え方をまずは明らかにします。そのうえで、セキュリティを確保するための体制、運用規定などを具体的に記載していきます。ポリシーといえども狭義の基本方針にとどまらず、それが確実に実践されるための具体的な対策基準なども同時に規定されることが必要です。

経営者が表明するセキュリティポリシー

セキュリティポリシーの策定は、単にセキュリティ対策の基本となるだけではなく、社員の意識の向上や取引先、顧客、株主などのステークホルダーからの信頼性の向上につながるものですから、担当部門・部署に任せきりにせず、経営者自らが取り組むべきものです。経営ガイドラインが「経営者」が正式に表明したものと規定している理由も、セキュリティ対策は経営者にとっての重要課題であるとの考え方によります。

② セキュリティマネジメントシステム

セキュリティマネジメントシステムとは

セキュリティポリシーを実行・具現化するための組織の仕組みが、セキュリティマネジメントシステムです。セキュリティポリシーをより具体化させたルール・マニュアルの策定、情報セキュリティに関する委員会や会議など組織の整備、セキュリティ投資計画の策定と実行、社内のセキュリティ教育など、目標とするセキュリティ水準を達成するための、ヒト、モノ、カネのすべてに関する企業全体の仕組みがセキュリティマネジメントシステムであるといえます。

PDCA サイクルの重要性

セキュリティポリシーとセキュリティマネジメントシステムは、セキュリティ対策を推進していくための、いわば車の両輪です。対策の効果の検証、企業を取り巻くリスク環境の変化などを踏まえ、マネジメントシステムは常に実効性の高いものを維持する努力が必要ですが、時には根本であるポリシーに立ち返った見直しも大切です。セキュリティマネジメントの活動に終点はなく、リスクマネジメントの基本ともいえる **PDCA サイクル**（計画：Plan→実行：Do→検証：Check→是正：Action）を廻し続けることが求められます。情報セキュリティマネジメントに関する国際標準[4]においても、この PDCA サイクルは大変重要視されていますし、経営ガイドラインにおいても、サイバーセキュリティ経営の重要 10 項目のひとつに掲げられています。

③ 国際規格やフレームワークの活用

事業内容、規模、経営戦略などが企業によって様々であるように、リスクの 3 要素（情報資産・脅威・脆弱性）やリスクの受容水準などのサイバーセキュリティに関する事情も企業ごとに違います。セキュリティポリシーもセキュリティマネジメントシステムもそれぞれの企業が自社に適したものを作り上げていくことが重要です。

しかし、企業にとって、これらをすべてゼロから構築していくことは並大抵のことではありません。そこで、企業にとって参考になるのが、**国際標準化機構（ISO）**が定めた**ISO/IEC27000 シリーズ**などの国際規格です。高度な情報化社会において、サイバーセキュリティは社会全体の問題ですから、個々の企業の枠を超えて整備されていかねばなりません。また、企業間のコミュニケーションを円滑にする意味でも、一定程度共通の基準が必要となります。こうした観点からサイバー（情報）セキュリティの分野においても、国際標準化の活動が進められてきました。これら国際規格には、セキュリティポリシーの策定やセキュリティマネジメントシステムを構築するにあたってのルール（「要求基準」）が定められていますので、企業のセキュリティ体制の構築に大いに役立つものと思われます。また、ISO 以外でも、米国立標準技術研究所（NIST）[5]など、国際的に認知されたセキュリティマネジメントに関する専門機関等が作成したフレームワークを活用することも体系的なアプローチに有効な方法です。

（２）サイバーセキュリティにおけるリスクマネジメントのプロセス

本項では、リスクアセスメントからリスク対応（リスクコントロールとリスクファイナンシング）というリスクマネジメントの基本的なプロセスに照らしながら、サイバーセキュリティマネジメントのプロセスを説明します。[6]

---

4 国際標準化機構の ISO/IEC 27001（その和訳版 JIS Q 27001）等

5 米国立標準技術研究所（NIST：National Institute of Standards and Technology）。米国商務省配下の計量標準研究所で、標準規格や産業技術の進歩によって技術革新の促進と産業競争力の向上を目的としています。

6 経営ガイドラインでは、リスク対応の各プロセスについて具体例を挙げながら用語解説をしています。本レポートでは用語の定義と具体例について一部を引用しています。

① リスクアセスメント

リスクアセスメントのプロセスは、大きく以下の３つに分けられます。

ｉ）リスクの特定

リスクを洗い出し、企業にとっての包括的なリスクの一覧を作成するプロセスを指します。情報資産の管理台帳を作成し、それぞれの情報資産に対する脅威とその情報資産の脆弱性を明らかにしていきます。

ii）リスクの分析

洗い出したリスクごとにその特質を理解し、それがどの程度のリスクなのかという**リスクレベル**を決定するプロセスを指します。他のリスク分析と同様に、サイバーセキュリティリスクにおいても、事象（リスクの顕在化）の起こりやすさと起きた場合の損害や損失の規模の組み合わせから、当該リスクの大きさ（＝発生確率×発生時の影響の大きさ）を見える化していきます。しかし、サイバー攻撃の頻度や、被害の大きさなど、サイバーの分野では、過去のデータや実績があまり蓄積されてはおらず、サイバーセキュリティリスクの分析は大変難しいプロセスであるといえます。日頃から、社内外のインシデントの発生や被害状況などセキュイリティリスクに関する最新の情報を収集しておくことが必要です。

iii）リスクの評価

リスクの大きさが受容可能かまたは許容可能かを決定するために、リスク分析の結果（リスクレベル）を（あらかじめ定めた）リスクの評価や受容の基準（**＝リスク基準）**と比較するプロセスを指します。リスク基準は自社の経営戦略や外部および内部環境に基づいて総合的に判断され、決定されるものです。たとえば、情報資産が損なわれたとき、それ自体の金銭的損失よりも、その後の顧客や取引先への損害賠償や社会的信用の失墜などによる影響の方が大きくなる可能性もあります。自社がどれだけのリスクを許容できるかは時間軸も含めて慎重に判断されなければなりません。

② リスクコントロール

リスク顕在化による損失の発生頻度と影響の大きさを削減するリスク対応方法を**リスクコントロール**といいます。

ｉ）リスクの回避

リスク回避とは「脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去ること」と定義されます。抜本的な対策となる可能性は高いものの、極端なリスク回避策は、利益の喪失や企業としての成長、イノベーションの阻害につながるという本末転倒した事態を招く可能性があります。リスクとリターンのバランスをとることが極めて重要です。

（例）「インターネットからの不正侵入」という脅威に対し、外部との接続を断ち、Web 上での公開を停止する。

◆ コラム２：サイバーリスクの定量化モデル ◆

リスクを評価する際には、経済的損失の規模を把握するために、どうしても定量的な分析が必要になってきます。それは、サイバーリスクでも同じことです。近年、サイバーリスクの数値化の研究が進められており、保険会社などでは、自らの保険の引受判断にも不可欠なものとして、リスク分析会社と提携するなどして、サイバーリスクの定量化モデルを導入しています。

しかし、サイバーリスクは、災害や自動車事故等に比べれば、まだまだ過去データが公的なものとしては蓄積されておらず、データ収集や複雑な計算処理にリソースを割けない一般の企業において、リスクを数値化することは相当に大変難しいことと思われます。

そこで、一般社団法人 日本サイバーセキュリティ・イノベーション委員会（JCIC）では、**最大予想損害額***の考え方や同業種の平均値といった**ベンチマーク値**（独立行政法人 情報処理推進機構（IPA）による「情報セキュリティ対策ベンチマーク」より算出）を用いたサイバーリスクの数値化モデルを作成しました。このモデルでは、個人情報漏えいによる金銭被害については、NPO 日本ネットワークセキュリティ協会（JNSA）が公開している**損害賠償算定式****を用い、ビジネス停止による機会損失については、社内ヒアリングに基づいて計算するなどして、想定損失額を算定しています。そして、JCIC は取締役会等でのこのモデルの活用を通じて、経営者層がサイバーリスクを共通で理解できる体制が必要であると提唱しています（JCIC シンクタンクレポート 19 Sep.2018 「取締役会で議論するためのサイバーリスクの数値化モデル」）。

重要なことは、経営者がサイバーリスクを概念としてだけではなく、いかに具体的数値で表された経営の指標として理解するかということなのです。

＊ 最大予想損害額（ＰＭＬ：Probable Maximum Loss）とは、発生しうる一事故による最大の予想損害額（ワーストシナリオに基づく予想損害額）をいいます。

＊＊ JNSA の損害賠償算定式（JNSA「情報セキュリティインシデントに関する調査報告書 別紙」より）
想定損害賠償額＝漏えい個人情報価値×情報漏えい元組織の社会的責任度×事後対応評価
（各項にもそれぞれ定量化の算定式、または判定基準があります）

ii）リスクの低減

リスク低減とは「脆弱性に対してセキュリティ対策を講じることにより、脅威発生の可能性を下げること」と定義されます。リスク回避とは対照的に、積極的にリスクと対峙するリスクコントロール方法であるといえます。セキュリティ対策の多くはこれに分類されます。

（例）・セキュリティソフトの導入、情報の紛失、漏えいなどに備えて行なう情報の暗号化や社員に対するデータへのアクセス制御などの技術的対策。
・サーバー室への入退室管理の強化といった物理的対策。
・社員に対するセキュリティ教育、訓練の実施や社内ルールの策定・徹底などの人的対策。

③ リスクファイナンシング

リスクが顕在化した場合の損失に対する財務的手当てを行うリスク対応方法が**リスクファイナンシング**です。

ⅰ）リスクの移転

リスク移転とは、「リスクを他社などに移すこと」をいいます。

（例）・サイバー保険による損失のカバー。
・IT システムの運用を外部へ委託する際、不正侵入やマルウェア感染などの被害について委託先へ損害賠償請求が可能な契約を締結。

ⅱ）リスクの保有

リスク保有とは、リスク移転をせずに、「ある特定のリスクにより、起こりうる損失の負担を受容すること」です。まさに自社でリスクを抱えるということですから、事業展開やリスク環境の変化に応じて、リスクアセスメントを継続し、リスクレベル（リスクの大きさ）とリスク基準（受容水準）の見直しを続けていくことが必要です。

（３）サイバーセキュリティ対策に関する考え方の変化

情報システムやネットワークの高度化・複雑化はとどまることはありません。一方、サイバー攻撃の手口がますます巧妙化するなど、脅威も増大するばかりです。こうした状況の変化に伴い、当然のように、サイバーセキュリティに関する考え方も変化・進歩してきています。サイバーセキュリティ対策の策定・実践において考慮すべきと思われる考え方の変化の例を２つ紹介します。

① インシデント対応重視型へのシフト

かつてのセキュリティ対策は脅威から情報資産を守るという「防御」を中心に考えられてきました。確かに、防御を固め、できるだけ脅威の侵入を防ぐことは大切なことです。しかし、近年は「防御も重要だが、完全な防御は不可能で、脅威の侵入は不可避である」という前提に立ち、発生したインシデントへの対応プロセスを重視する考え方が主流となってきています。「国際規格やフレームワークの活用」で取り上げた米国立標準技術研究所（NIST）は、この考え方を取り入れ、2014 年に「サイバーセキュリティフレームワーク」を公表しています。この NIST のフレームワークでは、セキュリティ対策のプロセスが、「特定」、「防御」、「検知」、「対応」、「復旧」の 5 つに分けて整理されています。平常時には、「特定」、「防御」を進めておき、サイバー攻撃などのインシデントが発生した非常時には、速やかに**「検知」**、**「対応」**、**「復旧」**にあたることができるような体制を整備することが推奨されています。

しかし、非常時には社内の情報伝達がうまくいかないことも多く、また平常時と同じ業務体制でインシデントに対応するのは容易なことではありません。そこで、**CSIRT**（Computer Security Incident Response Team）[7]と呼ばれる、非常時に稼働するインシデント対応の実働部隊を設置する企業も増えてきています。

② ゼロトラストセキュリティの考え方

脅威の侵入を外部と内部の境界で防ごうとする「境界防御」を主としたセキュリティモデルを「境界線モデル」といいます。従来のセキュリティ対策は「内部は安全で、脅威は外部からやってくる」という前提に立った、この境界線モデルが中心でした。しかし、最近は、この境界線モデルの限界が指摘されるようになってきました。クラウド型情報システムの発展やネットワークの複雑化、リモートワークの普及など、内外の境界線があいまいになり、もはや「内部は安全」とは言い切れなくなってきたのです。

こうした状況を受けて、「ネットワークの中に信頼できるところはどこにもない」とする**「ゼロトラスト」**という考え方が広まってきました。ゼロトラストでは文字通り、内部さえも信頼しないので、サイバー攻撃などの外部からの脅威だけではなく、内部不正の問題への対策にも活用できる考え方となります。しかし、境界線を集中的に守る境界線モデルより、ゼロトラストセキュリティモデルの方が、セキュリティ対策を講じる対象や範囲が格段に増大し、複雑化せざるを得ません。管理・運用コストが大きく膨らむ可能性もあります。現実的には、全てをゼロトラストセキュリティに移行するというより、境界線モデルとの併用や、複数の境界線を引く**「多層防御」**[8]の一部として実装されていくものと思われます。

４．サイバーセキュリティとコーポレート・ガバナンス

IT の利活用は今や企業にとって、企業価値や競争力を持ったビジネスを構築していく上での必須条件となっています。また、企業は顧客の個人情報や差別化を図るための技術情報など、様々な重要情報・機密情報を保有し、経営資源として利活用しています。そして、それぞれの企業は取引先や業界他社と、あるいはその枠を超えていくつものネットワークを構成し、さらにそれぞれのネットワークが相互に、あるいは複層的に連携しているのです。こうした高度ネットワーク社会において、企業は、自社の事業の安定的発展のためだけでなく、ステークホルダーやそして社会全体への責任を果たすために、サイバーセキュリティに取り組まなければなりません。サイバーセキュリティは、経営者がリーダーシップを発揮し、企業全体で取り組まねばならない「経営問題」であると同時に、社会に対する責務としてコーポレート・ガバナンスの問題でもあるのです。今、企業と企業経営者には、その体制の整備・確立が強く求められています。

---

7 CSIRT：1988 年、米国で発生した大規模なインターネット障害で、マルウェアに関する情報が共有されず、サービス復旧に時間がかかったことを反省し、インシデント対応の専門的実働部隊がカーネギーメロン大学内につくられたのが最初の事例です。

8 多層防御：システムやネットワーク内に複数のセキュリティ対策を講じること。物理層、ネットワーク層からデータ層まで多層防御を導入することで、単一の境界防御層による対策よりも、未知のサイバー攻撃等に突破されるリスクの軽減が期待されます。

（１）サイバーセキュリティは経営問題

① セキュリティ対策は将来の事業活動・成長に必須の「投資」

「サイバーセキュリティは経営問題である」というのは、国策の基本理念としても明確に打ち出されています。経営ガイドラインにおいては、サイバーセキュリティのための、「セキュリティ投資は必要不可欠かつ経営者の責務である」と明記されています。ここで、「投資」という表現を用いているのは、「セキュリティ対策の実施を『コスト』と捉えるのではなく、将来の事業活動・成長に必須なものと位置付けて『投資』と捉えることが重要である」との考え方に基づいています。サイバーセキュリティへの取り組みは、サイバー攻撃に対する防衛力の向上や事業継続性の確保にととどまらず、IT の利活用などにより、企業の収益を生み出す上でも重要な経営課題なのです。

② サイバーセキュリティ人材の育成と確保

サイバーセキュリティ人材の不足

当然ながら、サイバーセキュリティを推し進めるには、この分野に通じた人材が必要です。世界的にサイバーセキュリティ人材の不足が指摘されていますが、とりわけ、わが国における人材不足は深刻な状況です。NRI セキュアテクノロジーズ社の実態調査によれば、日本の企業の 86.2%（調査対象 1,222 社）が、セキュリティ人材が不足しているとしています[9]。さらに、内閣サイバーセキュリティセンター（NISC）のまとめ[10]によれば、セキュリティ技術の専門性を持った実務者・技術者層だけではなく、ビジネス戦略と一体になってサイバーセキュリティの企画・立案、実務者層の指揮と経営層への橋渡しができる戦略マネジメント層と呼ばれる、育成に相当の時間を要する高度人材が不足しているのです。今後、こうしたセキュリティ人材の需要はさらに高まるとみられ、人材の育成は喫緊の課題となっています。

経営の最重要課題

こうした認識に基づき、NISC、経済産業省や総務省など各関係省庁も、サイバーセキュリティ人材の育成・確保に向けたプログラムを展開させています。しかし、実際にセキュリティ人材を育成・確保するのは企業の役割です。そのための環境整備や投資はまさに経営者が正面から取り組まなければならない最重要の経営課題といえるでしょう。

③ 社会全体の発展のためのサイバーセキュリティ

NISC の「企業経営のためのサイバーセキュリティの考え方」（平成 28 年 8 月策定）では、企業経営においては、サイバーセキュリティは、ビジネス戦略の一環であると同時に、社会的な要求・要請であるとの基本的認識が必要であるとされています。IT が社会の基盤となり、IoT システムがさらに普及する、すべてがつながる社

[9] NRI Secure Insight 2020 （企業における情報セキュリティ実態調査）より

[10] NISC 令和３年１月「人材の確保、育成、活躍推進に向けた今後の検討の方向性について（全体像）」

会において、企業経営者には、企業は社会の中の存在であり、社会全体の発展に貢献することが企業の使命であるとの認識に立ち、サイバーセキュリティに取り組むことが求められているのです。より具体的には、適切な情報発信、提供する機能やサービスを全うするという観点からのリスクマネジメント、サプライチェーン全体でのサイバーセキュリティの確保などに努めなければならないとされています。

（２）サイバーセキュリティはコーポレート・ガバナンスの問題

① 情報セキュリティガバナンスという考え方

社会全体の発展に貢献する企業のあり方というのは、コーポレート・ガバナンスの問題として議論されるものです。つまり、各企業は、サイバーセキュリティを含む情報セキュリティに、社会の中での企業として取り組むという意識を持ち、コーポレート・ガバナンスとして取り組んでいくことが求められているのです。この**「情報セキュリティガバナンス」**という考え方は、2005 年 3 月に経済産業省より発表された「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」 において提唱されました。そこでは、「情報セキュリティガバナンス」を「社会的責任にも配慮した**コーポレート・ガバナンス**と、それを支えるメカニズムである**内部統制**の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義しています。企業経営者は、セキュリティ対策を、経営戦略・事業目的を組織として機能させていく活動（内部統制）に組み込み、社会的責任を踏まえた上で、自社を規律（コーポレート・ガバナンス）しながら、情報セキュリティに取り組むことが求められています。

② 経営層（取締役会）の関与

この情報セキュリティガバナンスの考え方は、**コーポレート・ガバナンス・コード**の策定（2015 年）や改訂（2021 年）を機に、上場企業を中心に浸透してきました。経済産業省が、2018 年 5 月に発表した「産業サイバーセキュリティ強化に向けたアクションプラン：サイバーセキュリティ経営強化パッケージ」では、企業にサイバーセキュリティ経営を求める仕組みを構築するために、コーポレート・ガバナンス・システム（CGS）に関するガイドラインの中にサイバーセキュリティを位置付けました。また、サイバーセキュリティへの経営層の関与を、上場企業で行われている**「取締役会の実効性評価」**の評価項目へ組み込むことや市場（投資家）に対するサイバーセキュリティ経営の可視化など、より具体的なコーポレート・ガバナンスの施策が提唱されています。サイバーセキュリティについて、取締役会にて実効性のある議論が行われているのか、そもそも企業としてサイバーセキュリティに取り組む姿勢があるのか、それをステークホルダーや社会に対してわかりやすく説明しようとしているのかが、より一層問われることになりました。

（３）企業や経営者の責任

サイバーセキュリティへの取り組みが、ステークホルダーや社会に対する責任である以上、もし、サイバーセキュリティに関する事故が発生し、社会に影響を与えた場合、企業はその責任を問われることになります。たとえば、個人情報が漏えいするなどの事故が発生した場合、損害を被った顧客などへの損害賠償責任を負う可能性があります。また、その場合、すべての顧客に対する連絡・謝罪といった各種事務対応、被害拡大防止のための事務プロセスの変更等、大きな費用と時間の負担を強いられることにもなるでしょう。さらに、こうした直接的な経済的損失に加え、企業の事業継続・発展に対する大きな阻害要因となる社会的信用の失墜も免れません。このように、サイバーセキュリティに関して企業が社会に対して負う責任は大変重いものなのです。本項では、企業や経営者が負う責任を、その法的な側面から整理していきます。

① 企業や経営者に対する法的責任

企業の法的責任が問われる代表的な場合

サイバー関連の事故に関して、契約上の規定があれば、当然に契約に基づく責任が問われることになります。それ以外でも、セキュリティ対策の不備を理由とした損害賠償責任（民法 709 条：不法行為）、従業員の不正、委託先・提携先のセキュリティ対策の不備を理由とした損害賠償責任（民法 715 条：使用者責任、同法 719 条：共同不法行為）などが企業の法的責任の根拠として挙げられます。

経営者（取締役）の責任が問われる場合

取締役は、会社との委任関係に基づき、会社に対して善良なる管理者の注意を払う義務（**善管注意義務**）を負うとされています（会社法 330 条、民法 644 条）。取締役がこの善管注意義務を怠った結果、会社や第三者が損害を被った場合、取締役はそれぞれに対して損害賠償責任を負います（会社法 423 条、同 429 条）。サイバーセキュリティ事故が適切な内部統制システムの構築[11]を怠った結果として起きたとされた場合、取締役は善管注意義務違反の責任を問われることになります。サイバーセキュリティへの取り組みはコーポレート・ガバナンスの一環であるとされる時代において、内部統制システムの構築の不備は経営者（取締役）の善管注意義務違反であるとされるようになってきています。

② 個人情報保護法

個人情報の有用性と個人の権利・利益の保護

サイバーセキュリティ対策で守られるべき情報資産として第一に挙げられるのが、個人情報でしょう。個人情報は企業の経済活動において大変有用なものですが、個人の人格尊重の理念のもとに適正かつ慎重に取り扱わ

11 会社法では、大会社以外の株式会社に、内部統制システムの構築を義務付けていません。また大会社も内部統制システムの構築を取締役会で決定しさえすればよいことになっています。そこで、内部統制システムの不備の問題は善管注意義務違反の問題として論じられることになります。

れることが強く求められています。私たちの社会を安全かつ快適に発展させるためには、不適切な個人情報の利用を防止しながら、適切な利用は促進するという難しい施策を両立させねばなりません。そのための核となる法律が**個人情報保護法**です。この法律では、個人情報を事業に使用する企業（個人情報取扱事業者）に対して、個人情報の取得、取り扱い、管理等に関し、様々な義務を課しています。これらに違反し、個人情報保護委員会からの改善命令にも従わない場合は罰則規定が適用されます。

情報漏えいと個人情報保護法

しかし、個人情報保護法には、情報漏えい自体を直接罰する規定はありません。また、損害賠償責任に関する規定もおかれていません（法律に規定された義務の違反があれば罰則規定が適用される可能性はあります）。一方、欧米では、欧州のＧＤＰＲ[12]や各消費者保護に関する法律に基づいて、情報漏えいに対して直接的に高額な制裁金や損害賠償を命じる例が多く見られます。わが国も、こうした国際的潮流を踏まえ、個人情報保護法において企業の対応義務や問題が起きた時の罰則が強化されていくものと思われます。

５．リスクマネジメントとしてのサイバー保険

サイバーセキュリティリスクの３つの要素は、「情報資産」、「脅威」、「脆弱性」です。事業を行う上では、このいずれもゼロにすることはできません。つまり、サイバーリスクは決してゼロにはならないのです。３． で述べたリスクを低減させるなどのリスクコントロール施策の後にも残存するリスクのうち、受容水準を超えると判断される部分については、リスクの移転を検討することになります。サイバーセキュリティの分野におけるリスク移転の代表的手法が**「サイバー保険」**です。

（１）サイバー保険とは

① サイバーセキュリティにおけるサイバー保険の位置づけ

サイバー保険とは、「サイバー事故により企業に生じた第三者に対する『損害賠償責任』のほか、事故時に必要となる『費用』や自社の『喪失利益』を包括的に補償する保険」です（一般社団法人 日本損害保険協会）。一般的に、保険は、リスクマネジメントの最終プロセスともいえる、リスク移転の手段のひとつですが、サイバー保険も考え方は同じです。したがって、サイバー保険を利用する場合は、サイバー攻撃対策など合理的なリスクコントロール策を講じてもなお、自社の受容基準を超えるリスクが残存する場合に、そのリスクが顕在化した際の損害を、一定の保険料を支払うことでカバーするものであるという基本原則を忘れてはなりません。リスクアセスメントやリスクコントロールといったリスクマネジメントのプロセスを踏まず、サイバー保険だけで、サイバーセキュリ

[12] ＧＤＰＲ：General Data Protection Regulation 「EU 一般データ保護規則」、2018 年施行。個人データの域外移転を原則禁止しており、行政罰規定があり、違反者には制裁金が課せられます。EU 域外の事業者にも適用される規則です。

ティ体制を構築することは、そもそもリスクマネジメントへの取り組み姿勢として誤っており、また、現実的にも、保険会社による引受けの拒絶や保険料の高額化などの問題により、困難なことなのです。

② サイバー保険の補償内容

補償内容

一般的なサイバー保険の補償内容は、**「損害賠償責任」**、**「事故対応費用」**、**「利益損害・営業継続費用」**の３つに大別されます。

ⅰ）損害賠償責任

情報漏えい等のサイバー事故により、法律上の賠償責任を負い、賠償金を支払うことになった場合、その経済的損失を補償するものです。賠償責任を巡って争訟となった場合の争訟費用も含まれます。

ⅱ）事故対応費用

サイバー事故に起因して、一定の期間内に生じた各種費用を補償します。具体的には以下のものがあります。

- インシデントの発生など事故が発生したおそれが生じた場合の調査・確認費用
- 事故が発生した場合の原因調査・被害状況調査費用
- 事故発生を対外公表する場合のメディア対応費用
- コールセンターの設置などのクレーム対応費用
- 消失データの復元、被改ざんウェブの復旧費用
- 被害者への見舞金の支払い
- 訴訟対応・法律相談費用
- 再発防止策の策定費用
- 情報漏えいされた個人のクレジット情報の不正使用監視費用　　など

ⅲ）利益損害・営業継続費用

ネットワークを構成する IT 機器等が機能を停止することによって生じた利益損害（逸失利益・収益減少防止のための費用）や通常の営業を継続するために要した臨時の費用などの営業継続費用を補償します。

保険金額（補償金額）の設定

では、保険金額はいくらに設定すればよいのでしょうか。それを適切に決定するためにも、リスクアセスメントのプロセスにおいて、自社のリスクを正確に評価しておかねばなりません。また、具体的な保険金額を設定するには、リスクの定量的な評価が必要です。これは簡単な作業ではありませんが、最近では、保険会社が保険の付帯サービスとして、サイバーリスクの定量評価サービスやそのツールを提供している場合もありますので、そうしたサービスの利用を検討してもいいかもしれません。

セキュリティ状況で変わる保険料率

保険料率は被保険者である会社の事業内容や規模に加えて、適切なセキュリティ対策が策定・実行されているかなども含めた、その会社のセキュリティ状況によって決まってきます。

補償されないもの

保険は金銭的な評価が可能なものしか補償されないことも忘れてはいけません。事故後の事業継続にいかに不可欠なものであっても、金銭的価値では評価しにくい企業の信用などは保険ではカバーされないのです。こうしたことからも、サイバー保険はあくまで備えのひとつに過ぎず、各種セキュリティ対策の策定とそれを実行する組織・仕組みづくりをサイバーセキュリティの中核に置かなければならないのです。

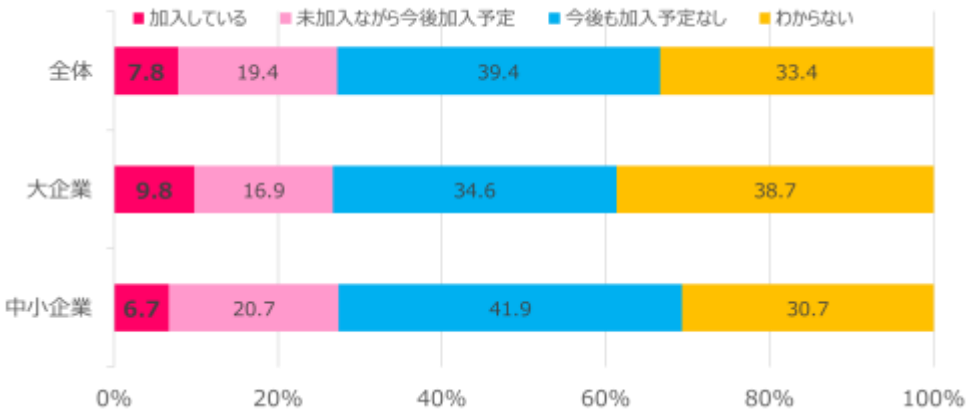
（２）サイバー保険の現状と今後

現在、サイバー保険はどれぐらい活用されているのでしょうか。今後はどうなっていくのでしょうか。関連団体の調査レポートなどから、サイバー保険の現状を踏まえ、今後を展望してみましょう。

① サイバー保険加入状況

一般社団法人 日本損害保険協会の調査（対象企業数 1,535 社、うち大企業 520 社、中小企業 1,015 社）によれば、サイバー保険に加入している企業は全体の 7.8%（大企業 9.8%、中小企業 6.7%）となっています。全体の２割程度の企業は、「今後加入予定」としているものの、現段階において、わが国では、サイバー保険に加入している企業は決して多くないというのが実態のようです（図表６）。

＜図表６＞ サイバー保険加入状況



（出所） 日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020」

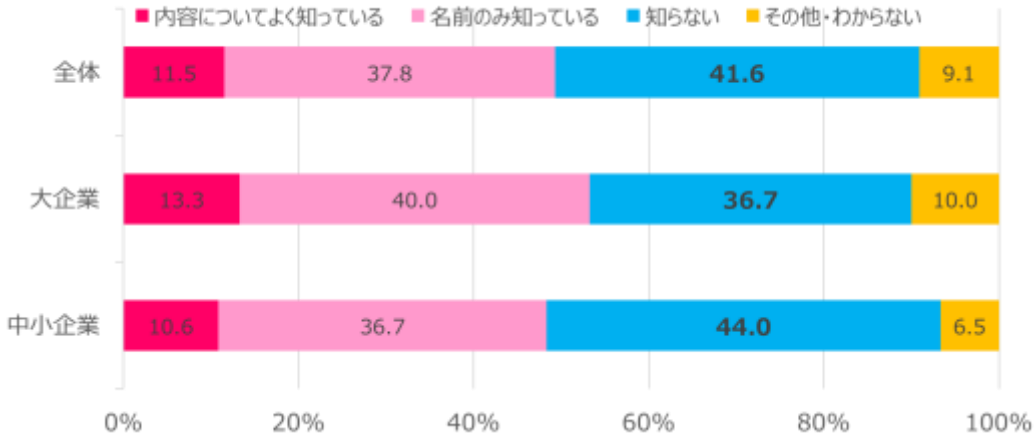
② 今後拡大が見込まれるサイバー保険市場

しかし、今後を展望すると、わが国のサイバー保険市場は、相当程度に拡大する可能性があると思われます。

低いサイバー保険の認知度

そもそも、わが国では、サイバー保険の認知度自体がまだ低いようです。日本損害保険協会の調べでは、大企業、中小企業ともに、約４割の企業が、サイバー保険を「知らない」と回答しています（図表７）。
その一方で、同じ調査でも、９割以上の企業が、何らかのサイバーセキュリティ対策を行っており、サイバーリスクに対する意識はすでに多くの企業が持っていることがわかります。サイバーインシデントが増加し続けるリスク環境、国や経済団体・関連団体によるサイバーセキュリティに関する基盤づくりや啓発活動の推進などを受け、企業（経営者）のサイバーセキュリティに対する意識は、今後さらに高まってくるものと思われます[13]。現段階でのサイバー保険の認知度の低さは、サイバー保険市場の潜在的な成長力を意味しているかもしれません。

＜図表７＞ サイバー保険の認知度



（出所） 日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020」

拡充される付随サービス

近年、保険会社は、サイバー保険に付随したサービスの拡充を図るなど、企業のサイバーセキュリティの取り組みの支援に注力しています。先に述べた、サイバーリスクの定量評価サービスのほか、セキュリティ状況の診断やクラウドを利用した異常の検出・初期対応サービス、弁護士の紹介や外部への広報活動に関するコンサルティング、さらには、セミナーの開催などの社員教育のサポート等、様々なサービスが提供されるようになってきました。

[13] 経理の電子化による生産性の向上を目指した「電子帳簿保存法」の改正（令和４年１月施行）などにみられるように、サイバー分野での情報・技術の利活用は、企業の規模を問わない、通常業務においても必須のこととなっています。

インシデント対応のサポート機能を求めて

一方、企業側もサイバー保険に関し、リスク移転の機能だけではなく、こうした付随サービスを重要視するようになってきました。「セキュリティ対策に関する考え方の変化」として、セキュリティ対策のインシデント対応重視型へのシフトについて述べましたが、最近では、企業が、一定のリスク顕在化、つまりインシデントの発生が不可避に近い状態にあると判断した上で、その発生の初動からの一連のインシデント対応（調査対応、弁護士対応、ステークホルダー対応等）におけるサポート機能を、サイバー保険に求めるケースが見られるようになってきています。まさに、セキュリティ対策の手段としてのサイバー保険の活用です。

先行して拡大する海外の市場

調査・統計ごとにばらつきはありますが、サイバーセキュリティの分野で先行する欧米では、全体のおよそ 3 割の企業がサイバー保険に加入しており、業種や企業の規模によっては、加入率は 6 割以上に上るようです[14]。さらに、多くの専門家が、不確実な面もあるものの、今後、数年間で世界のサイバー保険市場が急拡大するとみています[15]。

6．最後に

今回は、「サイバーセキュリティ」についてレポートしました。その定義やリスクマネジメントの基本も取り上げましたので、サイバーセキュリティやその対策を講じるうえでの、基本的な考え方はご理解いただけたと思います。繰り返しになりますが、サイバーセキュリティは、経営問題として、コーポレート・ガバナンスの問題として、経営者が率先し、企業全体が取り組まなければならない、重要かつ喫緊の課題です。本レポートが、その取り組みにおいて、少しでも参考になれば幸いです。

以　上

---

14 OECD「Enhancing the Role of Insurance in Cyber Risk Management（2017.12）、
公益財団法人 損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向 2019 年 9 月」、
NRI セキュアテクノロジーズ社「NRI Secure Insight 2020」 他

15 日本経済新聞 電子版 2020/2/28 「サイバー保険が世界で拡大　5 年後、200 億ドル市場に」より

銀泉リスクソリューションズ株式会社

■ 設立　：1997年6月
■登録番号　関東財務局長　第１８号
■ 代表者　：代表取締役社長　瀬古　義久
■ 資本金　：1億円
■ 株主　：銀泉株式会社（100%）
■ 取引銀行　：三井住友銀行
■ 役職員　：21名
■ 事業所　：東京都千代田区九段南3-7-14
TEL 03-5226-2212（代）

■ 保険仲立人業務
・顧客ニーズに即した保険契約の設計と契約締結の媒介
・リスク対応の各種サービスの斡旋・提供

■ リスクマネジメントコンサルティング業務
・リスク実態の調査に基づく最適な保険仕様の設計
・グローバル取引信用保険等の設計・構築
・キャプティブを活用したリスクファイナンスの提供
・国内プロジェクトファイナンスの保険コンサルティング業務

2021年6月末時点

●弊社の親会社である銀泉株式会社は保険代理店であり、保険仲立人である弊社とは立場が異なります。
●銀泉株式会社と弊社が共同して、お客様の同一の保険契約を募集することはいたしません。
●本レポートは情報提供を目的としており、保険の募集、弊社の商品・サービスの販売・勧奨をするものではありません。
●ご不明点や詳細につきましては、以下銀泉リスクソリューションズ株式会社までお問合せください。

本レポートに関するお問い合わせ先
銀泉リスクソリューションズ株式会社　業務企画部
TEL/ 03-5226-2212　　FAX/03-5226-2609
E-mail / grs@ginsen-gr.co.jp

なお、「サイバーリスクへの対応」については弊社ＨＰでもご紹介しております
サイバーリスクへの対応 Response to cyber risk | 銀泉リスクソリューションズ（ginsen-risk.com）