

セキュリティとコンプライアンス経営：第1回 LSMAP 導入部

2020年10月28日
常葉大学法学部教授 大久保紀彦

1. はじめに

LSMAP 導入として、藤岡先生「サイバーセキュリティ法制（第1回）」の内容と、それへの皆様の反応を受け、法的問題を扱う上での基礎的な知識を確認する講義とする。

・私の研究について：

<https://researchmap.jp/n-okubo>

<https://ci.nii.ac.jp/nrid/9000403296790>

・企業の中で法律を担当することの意味：企業法務とビジネス法務の違いについて

・技術専門家として、企業のなかで法務部に「任せる」のなにかということに任せるのか知っておく必要。

問題発生・拡大前に報告相談しておくことは自らの責任でもある。



2. 法律問題とは何か？

(1) 自分にとっての「権利」と「義務」

結局のところ関係者との問題：ステークホルダーとの関係性が重要

経営学との共通の課題がある：マイケルポーター「Creating shared value」

(2) 「契約」に着目してみる

まず企業の中と外とを考えると、まずは企業の外との関係

①お客様との関係、②経営資源調達先（サプライヤー）との関係

・お客様との契約は事業内容に応じて売買だったり請負だったりもする。

・サプライヤーはさまざまな相手、ひとつだけではない。部品、原材料、通信サービス、電力、金融、システム、情報（ヒト・モノ・カネ・情報）

・さまざまな経営資源を集めて企業内で処理をしてアウトプットを顧客に送り出す。それが企業。

「お客様」「サプライヤー」との間には「契約」がある。

・「お客様」「サプライヤー」とは「取引関係」にあるステークホルダーだということができる。

(3) 「契約自由の原則」と「民法」

契約自由の原則：契約書はなくてもよい。諾成主義（意思表示が一致していれば契約。

521条）

⇒自分の意思で自由に契約を成立させた以上、それを守られなければならない。

⇒トラブルがあったときにどうなるか？

⇒（契約書はない場合もあるし、あっても全ては書き込めない。）そのときに登場するのが民法である。

3. 契約と民法

(1) 契約主体

3条：「人」権利能力

33条：「法人」法律にもとづいて設立されたものに限る

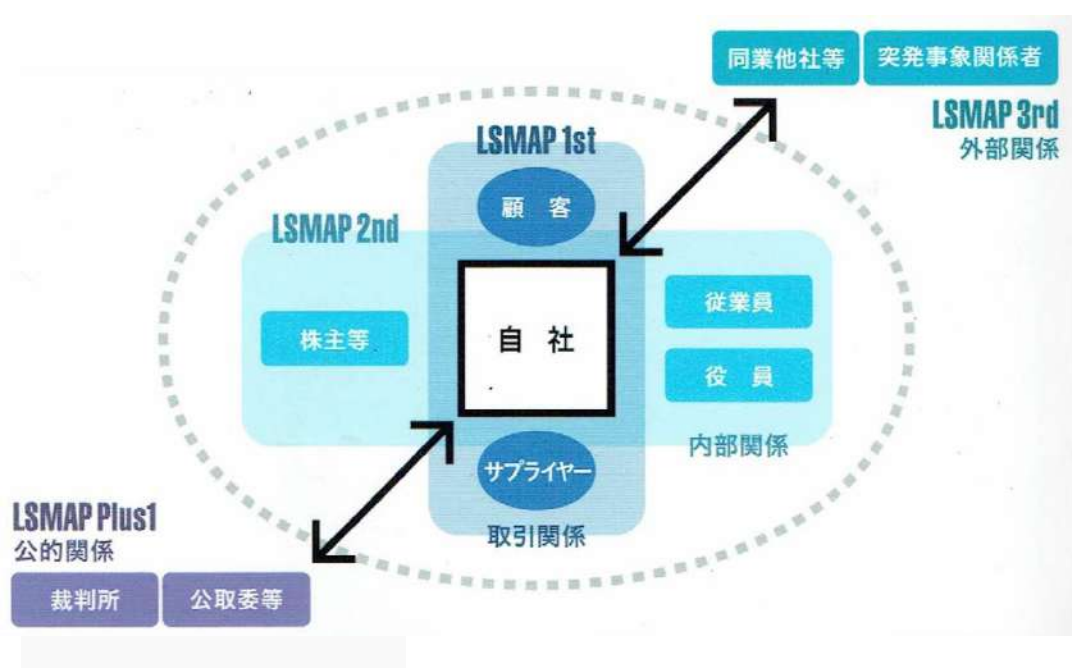
(2) 守らねばならない契約を守れなかったどうなるか？

損害賠償責任（415条）：相手が契約を守らなかった場合、損害賠償請求できる。



4. 不法行為

「お客様」「サプライヤー」以外の企業の外部者とは⇒競争相手。事業運営上たまたま遭遇する相手（業務車両の交通事故相手）。⇒民法 709 条 不法行為による損害賠償
基本にお金で解決する。（民法上は「差止請求」の条文はない。）



セキュリティとコンプライアンス経営：第2回 LSMAP の全容

2020年11月8日

常葉大学法学部教授 大久保紀彦

1. 関係的契約とステークホルダーマネジメント

契約とは、法律的には両者の「権利」「義務」に帰着するが、英米法的には「関係」を重視する視点がある。1980年代から、アメリカでは経営学的にはポーターの「Creating shared value」、法律学ではマクニールの「Relational Contract Theory: 関係的契約理論」が主張された。

⇒企業法務としてもステークホルダーマネジメントの視点が必要である。

2. LSMAP 1st.

企業にとってお金のやりとりがあり事業活動におけるステークホルダー「顧客」「サプライヤー」との契約関係(=取引関係)である。契約が守られないときには、415条の「債務不履行」による損害賠償が問題となる。

3. LSMAP 3rd.

企業と外部との法的関係は、上記 1st.だけでなく、見ず知らずの相手、との間でトラブルが発生した場合にも生ずる。1st.の「取引関係」に対して「外部関係」と考えてみるとよい。

民法 709 条の「不法行為」に基づく損害賠償の問題である。また、競合他社との間でのトラブルについては特別法として独禁法や不正競争防止法なども存在する。

4. LSMAP 2nd.

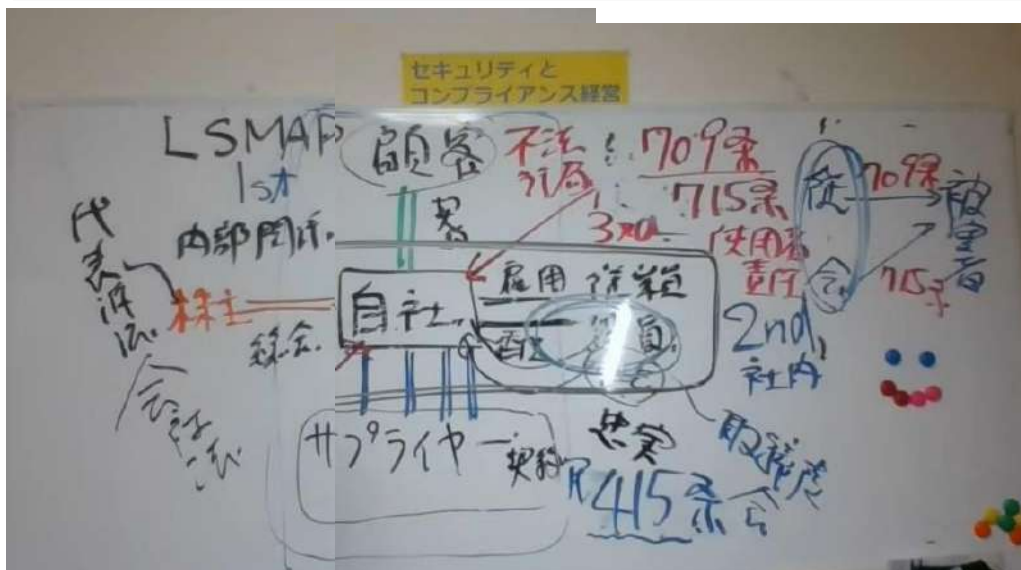
今日あたらしく説明するのは、「内部関係」の 2nd.となる。

(1) 従業員

企業の「内部」における契約関係である。企業と「従業員」との「雇用契約」が存在する。企業には、契約内容にとどまらず従業員に対する安全配慮義務があることに注意を要する。なお、労働者側保護視点を含む労働契約法など労働関係の特別法が存在する。

(2) 役員

企業において業務に従事しているのは、従業員だけでなく取締役等の役員もある。企業と「役員（取締役等）」と関係は「委任契約」と捉えられている。取締役には善管注意義務、忠実義務があり、会社に損害を与えた場合には、会社に対して損害賠償責任が発生する。



(3) 株主

さらに言えば、出資をしている「株主」もいわば企業にとって内部者と言える。株主は会社の持ち主なのであって、株主総会は企業の最高の意思決定機関であり、取締役の任免権がある。「役員」「株主」との間は、会社法によって規律されており、役員が会社に損害賠償責任が発生する行為を行った場合、株主は会社に代わって「役員から会社に対する損害賠償」を請求する「株主代表訴訟」を提起することができる。

(4) 取締役会の活用

株主総会は最高意思決定機関だが、役員任免・配当・計算書類・合併・再編などを除く通常的意思決定は、会社法上、取締役会に委ねられている。株主も閲覧できる議事録の作成義務がある取締役会においてオープンな議論を行うことは、内部関係である株主を重視する株主経営の視点から極めて重要である。

情報・サイバーセキュリティの専門家であるみなさんが、その徹底を図るうえで取締役会をどのように活用していくか、ということは、本科目における重要課題である。5回シリーズの後半で考えていきたい。

(5) 使用者責任：LSMAP2nd. 3rd.にまたがる問題

従業員が業務遂行にあたって「故意・過失」によって外部者に損害を与えた場合、従業員自身が損害賠償責任を負うのであって、みなさん個人の責任となることに注意していただく必要がある。たとえば、タクシー会社の運転手が交通事故を起こせば本人に民法 709 条の不法行為責任が生じるし、それは情報セキュリティ上の業務でも同様となる。

もっとも 715 条にもとづいて会社が連帯責任として同時に被害者に賠償責任を負うことになって、現実的には会社がいったんは賠償を行うことが多い。しかし、判決としては従業員本人と会社との連帯責任となる。会社は、従業員に対して求償を行うことができるが、従業員に負担力があるかどうか。企業としての信用度も落ちてしま。

企業としては、従業員による行為で結果として会社の責任・損失が際限なく拡がる可能性があるのだから、コンプライアンスを徹底させておく必要がある。

715 条の使用者責任には、企業側が「選任・監督に相当の注意をしており、それによっても損害が発生したよ場合」の免責条項があるが、適用ほとんど適用はない。企業として結果として外部に損害を与えないよう、コンプライアンス経営を徹底させなければならない。

5. LSMAP plus 1

最後に「公的關係」である。

(1) 行政機関

許認可、日常の行政指導を受ける省庁、地方自治体とオープンかつ正しい関係を築き、社会経済の発展・顧客の利益実現といった共通目標を見出し、公正な競争を行わねばならない。そこにおける法律は、各業界ごとの「業法」であり、各省庁によって規制を受ける。また全業界に適用のある「独禁法」を運用する公正取引委員会の存在もある。

企業にとっても、不正競争を行う企業が存在して、そのような企業が不当な利益を得たり、業界の評判が落ちるのであれば、みずからの事業に悪影響が及ぶ。その意味で「企業」と「行政」とは価値観を共有できるといえる。

(2) 司法機関

いざ訴訟となれば、迅速な裁判という共通目標に向けて、問題解決を図っていく必要がある。

セキュリティとコンプライアンス経営：第3回 三つの責任、損害賠償

2020年12月6日

常葉大学法学部教授 大久保紀彦

1. 三つの責任

ある行為は、三つの法的責任を発生させる。①民事責任、②刑事責任、③行政責任である。

(1) 交通事故を例とする個人の責任

ある人が交通事故を起こしてしまった場合を想定してもらえるとわかるであろうが、①民事責任とは、事故被害者への損害賠償責任である。民法などの民事法上の責任となり、交通事故で相手を死亡させてしまうと1億円を超える賠償金額は稀ではない。②刑事責任は、刑法などに基づく懲役刑・罰金刑などである。③行政責任も法に基づくが、行政機関から課される責任であり、交通事故の場合には行政機関（警察・公安委員会）が発行する運転免許停止、反則金などである。

②と③の違いは、②裁判によって責任のありなしが決まるという点で。三つの責任が全て課されることもあるであろうし、一つだけ、あるいは二つとなることもある。

(2) 情報セキュリティにおける企業の責任

企業として、情報セキュリティ上の事故、たとえば個人情報の漏洩を起こした際にはどうなるのか。まず、①民事責任として、漏洩してしまった個人への損害賠償責任がある。次に、②刑事責任として、個人情報保護法上の罰金刑がある。そして、③行政責任として、個人情報保護法上の情報取扱事業者としての登録取消し、さらに監督官庁から、各業法上の責任を問われる。たとえば、勧告や業務停止、事業免許停止などである。

企業として、三つの責任について考えていく必要があり、かならずしも情報関連、セキュリティ関連の法律だけでなく、民法、刑法をはじめとするさまざまな一般的な法律が関連してくることを意識しておいていただきたい。

2. LSMAP1st. と LSMAP 3rd.における企業責任のちがい

(1) LSMAP1st.

社外であってもLSMAP1st.における「顧客」「サプライヤー」とは契約関係にあり、企業として契約を守れなかった場合には、契約上の責任が発生する。損害賠償については、個々の契約内容が重要になるが、基本的に民法415条に従うことになる。契約自由の原則のもとで契約をした以上、契約を守れなかったのであれば、損害賠償責任を負うことが基本となる。ただし、免責事由があれば賠償責任を免れるということになる。責任を問われる側が免責を求めるのであれば免責事由を立証しなければならない。

契約が重要となる

(2) LSMAP 3rd.

同じ社外であってもLSMAP 3rd.では、相手とは契約関係がなく、民法709条の不法行為責任が問題となる。709条は基本的に事後的な金銭賠償でしかなく、差止請求はできない。損害賠償にあたっては、請求する側が相手の故意・過失を立証しなければならない。

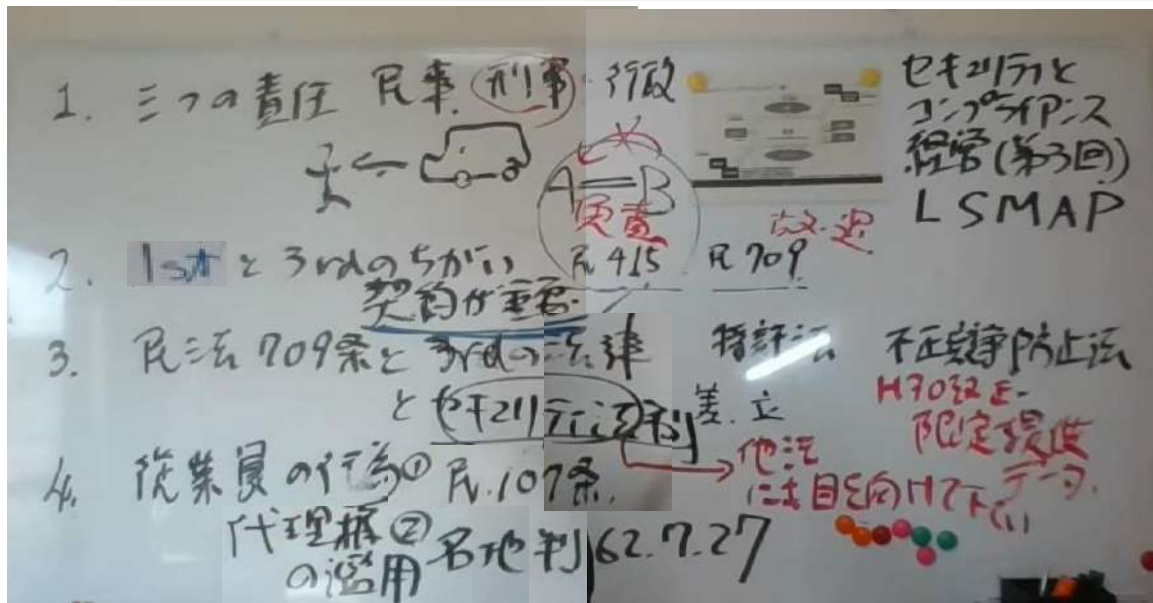
不法行為の問題となり、法律が重要となる

3. 民法 709 条と 3rd.の法律

知的財産が侵害された場合に適用される特許法などの知的財産法や、企業が秘密として管理している営業秘密が侵害された場合に適用される不正競争防止法においては、損害賠償だけでなく差止請求も認められ得る。また損害賠償における損害額の立証責任が軽減されてもいる。

また、情報セキュリティ関連で外部との法律問題が発生したときには、情報セキュリティ法制でまなんだ情報関連の法律だけではなく、民法など・刑法など・各業法が適用され、民事責任、刑事責任、行政責任が発生してくる。

3rd.における情報セキュリティの法律問題では、情報関連・セキュリティ関連の法律だけでなく、民事・刑事・行政関連の一般法が重要となってくる



4. 従業員の業務としての行為結果を従業員が負うことがあるか？

(1) 代理権の濫用

従業員は会社の代理行為を行っており、その効果は会社に帰属することが原則だが、自己または第三者の利益を図る目的で行った行為について相手方がそのことについて悪意または有過失であればその効果は従業員に帰属する。

たとえば、ある従業員が会社の名で融資を受けその契約自体には何の問題もないが、金員を自己の口座に振り込ませ、そのことを融資側が知っていた場合には、その融資契約の当事者は会社ではなく従業員個人ということになる。

第107条 代理人が自己又は第三者の利益を図る目的で代理権の範囲内の行為をした場合において、相手方がその目的を知り、又は知ることができたときは、その行為は、代理権を有しない者がした行為とみなす。

(2) 労働者が重過失によって使用者に損害を与えた場合

「労働者がその業務遂行中、重大な過失（深夜勤中の居眠り）によって使用者に損害を与えた場合、使用者は労働者に債務不履行による損害賠償を請求することができ、その賠償額については、雇用関係における信義則及び公平の見地から損害発生に至る諸事情を斟酌して決すべきである」（大隈鉄工居眠り事故事件）（名古屋地判昭和62年7月27日判タ655号126頁）

セキュリティとコンプライアンス経営

第4回 情報セキュリティ業務をLSMAPのフレームワークで分析してみる

2021年1月11日

常葉大学法学部教授 大久保紀彦

1. はじめに

これまでの講義の振返ってみたい。

企業・個人にとっての法律の意味は、権利・義務である。コンプライアンス経営という視点ではまず「義務」を重視する。それはステークホルダーひいては社会に対する企業の責任でもある。また義務を知ることで、相手の法的義務を理解でき、正当な権利主張を行うこともできるのだ。

そして、従業員、役員が行う行為によって、企業がいかなる責任を負うのかということを「モレなく、ダブリなく」確認していくことができるのが「LSMAP(Legal Stakeholders MAP)」なのである。LSMAPのうえで、従業員や役員の問題となった（問題となりうる）行為が企業によってどのような責任をもたらすことになるのかを確認してもらいたい。

つぎに、一つの責任を見出して、安心してはならない。①民事責任、②刑事責任、③行政責任、と三つの責任があるのだから、次にはそのチェックを行う必要がある。

2. 課題

さて、上記のフレームワークを、みなさんの日常業務にあてはめて考えていただきたい、というのが課題であった。

- (1) 「サイバーセキュリティ法制」その他みなさんが受講されてきた科目で学んできておられるセキュリティ法とみなさんの日常業務を照らし合わせしてください。
- (2) セキュリティ関連諸法のなかでも、みなさんの職務上最も注意すべき法律を一つ選んでください。
- (3) その法律のコンプライアンスが徹底されないとき、どのような事故・インシデントが発生し、それはLSMAPにおけるどのステークホルダーとの関係において、企業が民事責任を負うでしょうか。また、企業が刑事責任、行政責任も併せて負うことはないでしょうか。

3. 視点

みなさんのレポートを読ませていただき、

- ① どのようなインシデントを想定したか？
 - ② その際にどのような法律の適用がありうるか？
 - ③ LSMAP上で考えるとどのようなステークホルダーとの関係が法的問題となるのか？
- という視点で私の方で整理して、とくに指摘が多かった点について説明をしていきたい。

4. 情報漏洩の二つのタイプと適用される法律

「漏洩」してしまう情報には二つのタイプがある。「個人情報」と「営業秘密」である。

(1) 個人情報の漏洩

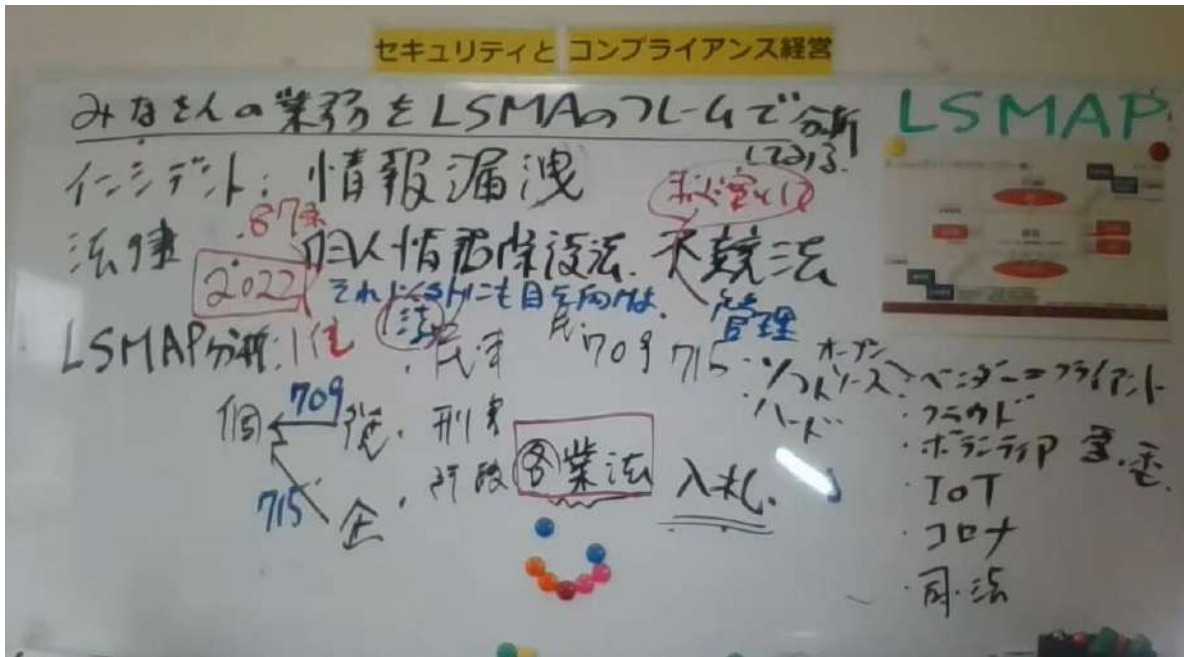
もちろん、個人情報保護法が適用される。「個人情報取扱事業者」の定義として以前は5000件であったが1件でも取扱事業者となる。

注意いただきたいのは、クラウド事業者である。情報の中身にはあずかりしらぬクラウド事業者は、経済産業省ガイドラインによって「個人情報取扱事業者」とされているがそれで安心してはならない。もしクラウド事業者の過失によって、また従業員の不正行為によって情報が漏洩してしまったらどうであろうか。個人情報保護法に抵触せずとも、企業として民事上の損害賠償責任(709条または715条)を負うことになってしまう。また、例えば電気通信事業法などの業法によって事業上の勧告を受けたり、行政から入札停止とされたりするなど、事業に大きなダメージが起こりうるのである。個人情報取扱事業者かどうかに関わらず、情報漏洩は企業にとって命取りとなりかねない。

(2) 営業秘密の流出・侵害

これについては、会社が損害を受ける局面である。不正競争防止法に基づき、相手企業に対して損害賠償請求また差止請求が可能となる。

しかし気をつけていなければならないのは、「営業秘密」として企業内で管理されているかどうかである。パスワードもかかっていないとなると、秘密として管理されておらず、不正競争防止法上の保護対象とはならない。企業にとって有用な顧客情報であっても、差止め、損害賠償の対象とはなかったという裁判例もある。「秘密としての管理」するうえでは、ソフトとしての従業員規則などのルールと、ハードとしての秘密管理・アクセス不可状態にすること、このソフトとハードの両面での対策が不可欠である。現在の技術水準においては、PW だけでは不十分ということになるであろう。



(3) 個人情報保護法の改正

改正個人情報保護法が 2022 年より施行される。重要点を説明しておく。

① 法人刑事罰の強化

情報漏洩を起こした個人への刑事罰は 1 年以下の懲役、50 万円以下の罰金とかわらないが、法人への罰金が 50 万円から 1 億円となる（87 条）。個人情報取扱事業者であれば規模に関わりなく小規模のベンチャー企業にも適用される。必ず意識しておいていただきたい。

② 報告義務

情報漏洩を起こしたさいの総務省（委員会）への報告義務は、これまでは、総務省告知にもとづくガイドライン上の義務であったが、個人情報保護法 22 条の 2 に明文化され、速やかに報告すべき法律上の義務となった。報告しない場合には行政処分として勧告を受ける。

③ 第三者への提供が制限される情報

これまでは個人情報でなければ他者に提供可能であったが、提供先に何らかの情報がありそれと併せると個人を特定できる「個人情報」になってしまう場合には、個人の許可なく提供ができなくなった。この点は注意しておいていただきたい。

5. 取締役の責任

CISOとして取締役あるいは近い将来、取締役となる方々、また企業経営者の方もいらっしゃると思う。取締役会の活用というテーマに進むうえでも、まず会社法によって規律されている取締役の責任について説明をしておきたい。

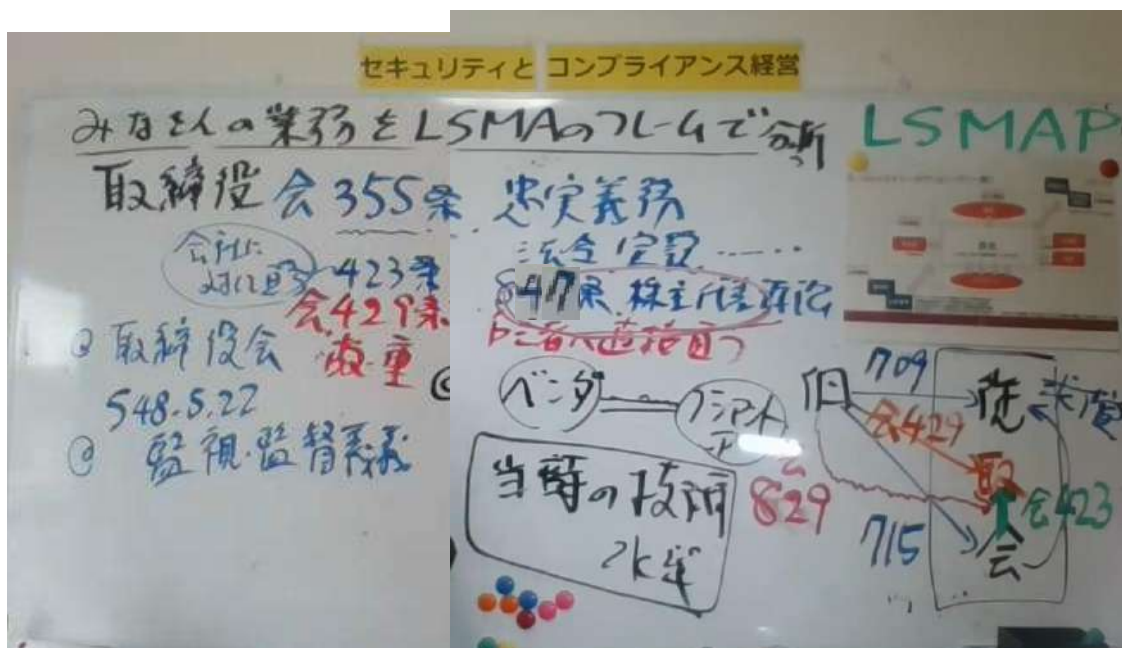
(1) 善管注意義務・忠実義務

取締役は経営の専門家として会社と「委任」契約による関係にあり（330条）善管注意義務を負う（民法643条）。また、法令、定款、株主総会決議を遵守し、会社に対して忠実に職務を行う義務（355条）を負うことになる。

(2) 会社に対する損害賠償責任

取締役上記の義務を果たせず会社に対して損害を与えた場合には、会社に対して損害賠償責任を負う（423条：任務懈怠責任）。⇒損害を受けた会社は、取締役に対して損害賠償請求を行うことができる。

■株主代表訴訟（責任追及の訴え）847条：株主は、会社に代わって取締役の責任を追及する訴えを提起できる。



(3) 第三者に対する損害賠償責任

ケースとして従業員の故意による情報漏洩があれば、従業員が被害者に対する損害賠償責任が生じる（709条）。会社も使用者責任（715条）が生じて損害賠償を行わねばならない。なお、従業員とは社員、アルバイト、派遣会社の社員、さらに子会社社員なども含む。

その際に、取締役としてCISOが職務を行うにつき悪意・重過失があって、結果として第三者に損害を与えたのであればどうか。取締役は第三者に対して直接、損害賠償責任を負うことになる（429条）。取締役であるCISOの職務遂行にあたって重過失があった結果、情報漏洩があって第三者が被害を受ければ、取締役本人が賠償請求を受ける可能性があることになる。

取締役の責任は大きい

6. 取締役会の活用へ

CISOとして取締役は、個人としてもこのように重い責任を負う。ならば、取締役会に情報セキュリティに関わる問題をあげてしまい、議論しておくべきである。他の取締役にも自分の担当任務以外で適正に職務が行われているかの監視・監督義務があるのだから、他の取締役を巻き込み、会社全体で取り組んでいくという考え方だ。次回は最終回となるが改めてこの点についてかんがえていきたい。

セキュリティとコンプライアンス経営 第5回 取締役会の活用

2021年1月31日

常葉大学法学部教授 大久保紀彦

1. はじめに

本日の最終回では「取締役会の活用」を扱う。取締役としての CISO の視点で、あるいは担当取締役のもとで業務を行い、取締役を支える技術専門家の視点で聴いていただきたい。法律적으로는会社法の問題であるが、企業法務・コンプライアンス経営という意味では、経営学的な視点が必要な論点でもある。そのような学際的視点での講義を行ってまいりたい。

2. 所有と経営の分離

株式会社は、出資者である株主に所有される。しかし株主は資本を提供するが株主が経営するわけではない。経営は、経営の専門家として委任する取締役にまかせるのであって、「所有と経営」は分離される。

株式会社の意思決定最高機関は株主総会であり、取締役などの役員の任免、配当、M & A、計算書類、定款、などを扱うが、日常の経営は取締役に委任し、その決定は「取締役会」で行われることになる。

LSMAP2ndの内部関係における「株主」「取締役（役員）」「従業員（社員）」の関係を再確認していただきたい。



3. 取締役会のミッション

会社法 362 条 2 項にあるとおり、取締役会の権限は以下の三つである。

- ① 業務執行の決定：業務執行を行う取締役およびその内容を決めておく。各取締役はその範囲で個々に業務執行できるが、委任された業務内容を取締役会で決定することもできる。
- ② 取締役の職務執行の監督：各取締役が独断専行しないよう取締役間の相互チェックという考え。
- ③ 代表取締役（社長）の選任・解任

民法の世界ではフランス法、ドイツ法の影響、会社法の世界ではアメリカ法の影響があることは事実であり、それらの動向をということが頭にある。アメリカでは、取締役会といのは、取締役の業務執行を確認・チェックするモニタリングボードとしての性格が強いが、日本では取締役会において「経営事項の決定をする」というマネジメントボードとしての性格が強い。

指名委員会等設置会社などの新しいかたちの株式会社だけでなく、従来型の監査役設置会社であっても、情報セキュリティに関してはモニタリングボードとしての機能に目を向け、他の取締役が担当する業務にかかわるセキュリティ面を洗い出していくという姿勢も必要だといえよう。

4. 取締役自身の職務遂行

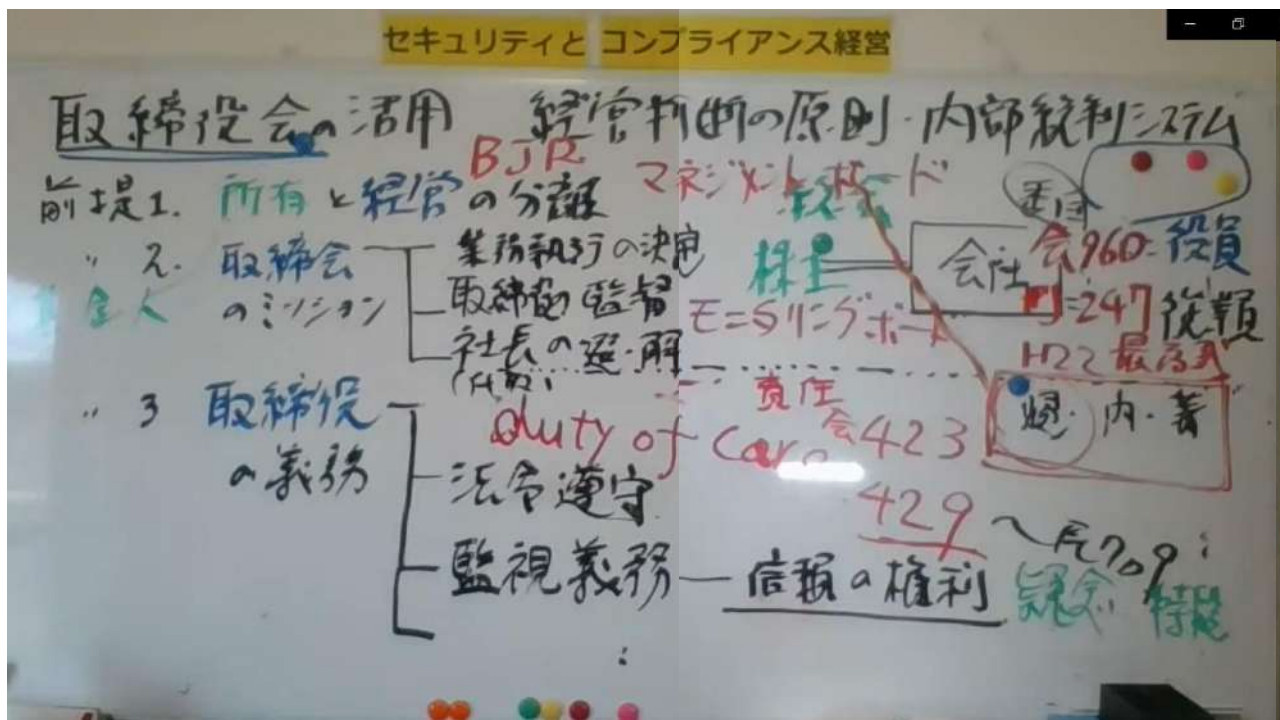
(1) 取締役の責任の根拠

取締役は会社から「委任」をされている（330 条）。請負ではないのであって、仕事が成功して完成できるかどうかは約束できないような高度な事項の委任を受ける。ただし、「善管注意義務」、つまり善良な管理者としてベストを尽くさなければならないのである。

そして、法令順守により会社の利益を図る忠実義務がある（355 条）。アメリカ法的には、「Duty of care」であって、法律を守るとは当然ながら、いくつかの選択肢のなかから細心の注意をもって最善を尽くさねばならないのである。

(2) 経営判断の原則

そこで出てくるのが「経営判断の原則」である。何らかの条文に書かれているのではない。アメリカ法の Business Judgement Rule の考えに沿ったものであり、取締役の責任を判断するうえでの裁判所における判断基準である。下級審で積み重ねられ、最高裁の平成 22 年最高裁判決で考えが示された。



(3) 判例で示された考え方：

■平成 22 年最高裁判決（最判平成 22 年 7 月 15 日判時 2091 号 90 頁：アパマンショップ株主代表訴訟事件判決）

アパマンショップホールディングスが、子会社アパマンショップマンスリーの完全子会社化において、子会社株主である加盟店から株式を買取る際の価格を、出資時の価格（ただし、当時の市場価格の 5 倍）としたものであった。高裁判決の「破棄自判」であり、最高裁の一定の強い考えが示されていると言える。

① **意思決定過程**：意思決定の過程においてベストを尽くしているのか？ **取締役会**（当事案では、同一メンバーによる会議）**でしっかりと議論をしているのか？** 弁護士にも相談しているのか？ がチェックされている。

取締役会を活用すべき

② **意思決定の内容**：裁判所しく不合理ではなければ取締役の責任はないとされる。経営判断の結果が出るかどうかはわからないし、詳細な検証を行ってもそれは事後的な評価となってしまう。裁判所としてその内容の実質的当否には入り込まない、という考えである。

5. 他取締役の監視・監督

(1) 内容

取締役は、取締役会事項に限らず、代表取締役をはじめとする業務執行取締役の監視義務を負うことになる。あらゆることを監視する義務があり、それによる責任を負うという意味ではない。そもそも、そのようなことは不可能である。

ただし、少なくとも、取締役会に上程された問題については、意見を述べ他取締役の監視を行う必要がある。

(2) 信頼の原則

取締役会に上程されていないような他の取締役の業務については、「疑念を差し挟むべき特段の事情」がない限り、適正に行われていると信頼することが許され、監視義務違反の責任を問われることはない。このことは「信頼の原則」とされる。

取締役 CISO としては、他の取締役の業務（たとえば営業など）において情報セキュリティ上の問題が発生することを避けねばならない。場合によっては自らの責任を問われることになる。

ただし、信頼の原則を働かせるためには、会社組織として、情報収集・調査・検討等に関する体制やリスク管理等に関する体制が十分に整備されていることが前提となる。

(3) 内部統制システムの構築

内部統制システム：取締役の業務執行が法令や定款に適合することを確保するための体制、および当該企業やその子会社からなる企業集団の業務の適正を図るために必要なものとして法務省令で定める体制の整備（会社法第 362 条 4 項 6 号）

取締役会設置会社である大会社では、取締役会において内部統制システムの整備することが義務づけられている（362 条 5 項）。※大会社：資本金が 5 億円以上または負債の額が 200 億円以上（2 条 6 号）。

大会社に限らず CISO として内部統制システム構築を目指すべき

すぐに「内部統制システム」に至らずとも、たとえば個人情報漏洩対策として、まずは「プライバシーマーク」取得を目指した社内活動もちろん有効と考えられる。

6. おわりに

(1) CISO/取締役の責任

LSMAP をもう一度振り返っていただければ、CISO「取締役」として、情報セキュリティ・サイバーセキュリティの職務における任務懈怠によって「会社」に損害を与えれば会社に対して 423 条の賠償責任を負う。その賠償責任は、「株主」から株主代表訴訟によって問われることになる。その結果として「取引先」「顧客」「株主」に損害を与えてしまった場合に、悪意・重過失があれば、直接の損害賠償責任を負うことになる（429 条）

経営判断の原則が働くといっても、それは「法令遵守」が大前提となって、そのうえでの経営判断が一定の裁量に委ねられて責任を問われないという意味に過ぎない。現在の技術水準を前提とした情報セキュリティ・サイバーセキュリティ上の最新の法律上の義務を果たすことが最重要である。そのために、SECKUN で学んだ技術を活かしていただきたい。もちろん法的責任を問われることのないように、という意味にとどまらず、皆様の企業が競争優位を獲得するためにもである。

(2) 周りを巻き込む

本講義を最後まで受講していただいた皆様に感謝します。

優れた経営者・管理職とは、自らの行動変革だけでなく、周りの行動を変革できる人だといえるでしょう。本プログラム終了後、職場に戻ったみなさまは、取締役会も活用して周りを巻き込んで、各企業をさらに良き方向に導いていかれることを期待しています。