

電子メールにおける リスクマネジメントの必要性

社員のメールにともなう企業責任の重大性

他人の権利に対する侵害や違法な内容を含むメールを社員が企業のシステムを使って発信した場合、企業が責任を問われる可能性があります。それが企業名による広告メール等であれば、企業自身の行為として責任を負うことになります。

また、メール発信自体は社員の行為と評価される場合でも、社員が「事業の執行」につき行った不法行為については、企業は使用者として被害者に対する損害賠償責任を負うことがあります(民法715条1項)。この場合、判例では、厳密に事業の執行の範囲内でも業務執行と同一の外形があればよいとされますので、使用者責任成立の範囲が拡張されています。また、使用者は被用者の選任、監督に過失がなかったことを立証すれば免責されます(同条項但書)が、判例上企業はほとんど免責を認められないのが実情です。

さらに、社員の違法メール発信が外形上も業務執行の範囲外であり、使用者責任が否定される場合でも、社員の不法行為(違法メール発信行為)を助長したり、放置したことについての過失を認定され、企業が損害賠償責任(民法709条や415条)を問われる可能性もあります。

そのほか、社内メールでセクハラが行われた場合、加害社員本人に不法行為責任が生じるのは当然ですが、その社員を雇用する企業についても、使用者責任(民法715条)や労働契約上の安全配慮義務違反の責任(民法415条)を問われる可能性があります。



速水法律事務所
弁護士・MBA

速水 幹由 様

はやみ・みきよし

1984年弁護士登録。速水法律事務所主宰。東京弁護士会所属。1992～1994年米国に留学し、MBA(経営学修士)取得。積極的に取り組んでいる分野はビジネス法務戦略、無体財産権(著作権・商標・意匠)、インターネット関連問題、企業を原告または被告とする製造物責任、損害賠償(契約違反・不法行為)。著書に「インターネット時代の企業防衛 eポリシー」(日本語版追加部分)「インターネット法学会内」(共著)「裁判実務体系30 製造物責任関係訴訟法」(共著)などがある。
hayami@law.ne.jp

セキュリティポリシーと プライバシー侵害の危険

これらメールを使った非違行為や企業秘密の漏洩等を防止するためには、社員教育だけでは心許ないものがあり、企業としては社内メールを監視するの一方策です。しかし、それには社員のプライバシーを侵害するリスクをともないます。

この問題に関しては、企業が事前に従業員の承諾を得ない限り不法行為になるとする説(違法説)、事前に従業員に告知しておけば従業員の承諾を得なくても不法行為にならないとする説(折衷説)および事前の告知も従業員の承諾もなく不法行為にならないとする説(合法説)に分類できます。

そのうち、モニタリングを知らさず秘かに社

員のメールを読むことは盗聴と変わりがないため、合法説はとりにくく考えます。残り説のうち、折衷説が合理的でしょう。企業設備の社内ネットワークについて、社員に使用を命じたり、禁止したり、使用方法等の条件をつけることも、労務指揮権、業務命令権の一環として許されるはずですが、他方、社員の側からしても、あらかじめモニタリングの可能性の告知があれば、それなりの対処ができるからです。ただし、学説も流動的で法的リスク(法の変動性)が大きいので、企業としては書面で社員の事前承諾を得ておく方がベターでしょう。

その反面、モニタリングによるリスクもあります。たとえば、セクハラ・メールをモニターした企業が適切な措置を講じなければ、社員の不法行為を放置した責任を問われかね

ません。そのうえ、実際にはメールを見ていなくても、企業がモニタリングによって社内メールの内容を管理できる立場にある以上、そのチェックを怠ったことの管理責任を問われる可能性すらあります。

つまり、個別具体的事情の下で両リスクを天秤にかけ、モニターするかしないかを判断する必要があります。

ただ、一般論としては、モニタリングの可能性をあらかじめ社員に告知し、かつ社内メールを業務用だけに限定する内容の社内規則を制定するのがよいといえるでしょう。

社内メールが組織秩序を損なうサブカルチャーに支配された場合、その損失ははかりしれません。かといって、モニタリングが私生活の盗聴類似の効果をもたらせば、法的に問題なだけでなく、職場の雰囲気や却って阻害することになります。これを避ける意味からも、社内メールの使用目的を業務に限定し、初めから私的な会話が対象にならないようにするのがよいでしょう。また、その方が、公序良俗違反(民法90条)を理由にモニタリング規則が無効とされるリスクも低くなります。もっとも、第一次的チェックにはモニタリングソフトを使い、対象となったメールだけを人の目でチェックするのが穏当でしょう。

メールにともなうその他のリスク

その他にも、たとえば誤って顧客のメールアドレスを漏洩してしまう事故もあります(2001年11月8日付日本経済新聞朝刊で、法務省メールサービス登録者に関するメールアドレス情報誤配信の事例が報じられた)。ちなみに、個人情報保護法案における個人情報は、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)(2条1項)をいってされています。

メールアドレス自体が個人情報に当たる可

能性は低いにしても、住所、氏名等のCRM (Customer Relationship Management) データと結合すれば、個人情報に該当し得ます。同法案制定の場合における規制違反とプライバシー侵害とは必ずしも重なり合うわけではありませんが、規制逸脱行為には違法性が認められ、プライバシー侵害の損害をともなうときは、不法行為が成立すると考えておいた方がよいでしょう。

あるいは、知らずにウィルスをまきちらすこともあります。この場合、少なくとも市販のウィルス対策ソフトを使えば防げたのに使っていなかったようなときは、企業として過失責任を問われる可能性を否定しがたいといえます。

そのほか、なりすましや文書内容の改ざんを防止するための制度活用も検討すべきです。電子署名を行った利用者の作成した情報であること、およびその情報の改変が行われていないことを、民間の第三者機関が確認する電子認証に関しては、一定の基準に適合し特定認証業務を行う認定認証事業者を認定する制度(電子署名法)があります。また、公証人による電子私署証書認証、電子確定日付付与等を受けられる電子公証制度(公証人法)および商業登記制度に基づく登記所の証明を受けられる電子認証制度(商業登記法)もあります。民間業者のうち認定を受けた者と受けない者を含め、これらのどれを利用するかは、目的とコストに応じ使い分けるようにします。

いずれにせよ、リスクヘッジを考える場合、

ゼロか100かではなく、コスト・ベネフィットを考慮しつつ自己に有利な武器を増やすという姿勢で臨むべきです。

また、法解釈の変動リスク(法的リスク)を管理するためには、ビジネスマンと弁護士との協働によって、その変動方向を予測した上で対応ポジションを選択する“ビジネス法務戦略”の手法が有効です。

“ビジネス法務戦略”の意味

ちなみに、私のいう“ビジネス法務戦略”とは、流動する法状況の方向を予測し、それを踏まえてビジネス戦略を検討することであり、“法と経済の総合”という視点に立って対応策を組み込んだ戦略を構築することです。その根底にあるのは、「法は決してスタティックなものではなく、立法論はもちろん法解釈も、時代のトレンドとともにダイナミックに変遷するものである」という認識です。

換言すると、上部構造たる法は下部構造たる経済によって規定され、法解釈も経済的合理性に導かれて変遷するという認識にもとづいて、判例等の法解釈や法改正に関する将来の動向を見通し、その予測を前提にビジネスマンと(顧問)弁護士との協働でビジネス戦略を構築しようとする手法です。

(速水氏のサイト

<http://www.asahi-net.or.jp/~nf5m-hym/>中の「私の“ビジネス法務戦略”論」参照)

メールによるリスクと、メールにともなうその他リスクの可能性例

- 社員が他人の権利に対する侵害や違法な内容を含むメールを企業のシステムを使って発信した場合のリスク
- 社内メールでセクハラが行われた場合のリスク
- モニタリングによって社員のプライバシーを侵害するリスク
- モニタリングのために責任を問われやすくなるリスク
- 誤って顧客情報等を漏洩するリスク
- 知らずにウィルスをまきちらすリスク
- なりすましや文書内容の改ざんのリスク