ビジネスインテリジェンス

改めて確認しておきたい雇用法とサイバー・セキュリティーの分野における留意事項

増田・舟井・アイファート&ミッチェル法律事務所

所長/弁護士
小林　城治

弁護士
フランク・デルバルト

インターナショナル・
リーガル・アドバイザー
田原　直

本稿では、雇用法とサイバー・セキュリティーの各分野から、近年の動きを踏まえつつ、特にご留意いただきたい2つのトピックを取り上げて概説します。

1. フィールドサービス・エンジニアの割増賃金の受給資格

機械等の販売業者を中心に、製品の販売先に赴いて、販売した製品の設置・保守・修理などを行う、フィールドサービス・エンジニア（Field Service Engineers/Technicians）と呼ばれる技術者を雇用している会社は少なくありません。このようなフィールドサービス・エンジニアに対して給与を支払う際に、1週間のうち40時間を超える労働時間に対して、割増賃金（Overtime Pay）を支払っていないケースが多く散見されます。限られた例外を除き、フィールドサービス・エンジニアに割増賃金を支払わないのは、連邦や各州における賃金時間法（Wage and Hour Law）に違反し、賃金の不払いに対して大きな法的責任を負うことにもなりかねません。

もっとも、連邦レベルでは、公正労働基準法（Fair Labor Standards Act）において、一定の要件を満たす管理職（Executive Employee）や専門職（Professional Employee）、運営職（Administrative Employee）など、限られたタイプの従業員に対しては、割増賃金に関する規則の適用が除外されています。

しかしながら、米国労働省（Department of Labor）は、いくつかのオピニオン・レターの中で、フィールドサービス・エンジニアの主な職務は、「専門的な知的指導や学習による長期にわたる過程を通じて慣習的に習得されるような、科学その他の学問の発展的な分野の知識を必要とするものではない」として、割増賃金に関する規則の適用除外になっている専門職には当たらないとの見解を示しています。また、米国労働省は、サービス従業員や、フィールドサービス・エンジニアのような修理技術者は、適用除外の対象となる運営職にも当たらないとの立場を長期にわたって採用しています。その理由の一つとして、フィールドサービス・エンジニアは、機械を設置・修理するために（適用除外と

増田・舟井・アイファート＆ミッチェル法律事務所
米国でビジネスを展開する日系企業及びその他国際企業を代理する法人向け総合法律事務所。日英バイリンガルの弁護士とスタッフが複数所属しており、米国進出から米国事業の運営・拡大まで、全米規模でのリーガル・サービスをワンストップで提供している。

筆者紹介

小林　城治 所長 / 弁護士
M&A、ジョイント・ベンチャー及び戦略的アライアンスを含むクロスボーダー案件、並びに販売・流通契約等の商取引についてアドバイスする。また、商標、著作権、データプライバシー問題及び複雑なライセンス取引等の知的財産案件も手掛けている。代理するクライアントは、自動車、工作機械、情報テクノロジー、ソフトウェア、食品及びバイオファーマ等、多岐の業界にわたる。日本の大手法律事務所であるTMI総合法律事務所にてインターンとして勤務した経験を有する。

フランク・デルバルト 弁護士
従業員の雇用から、従業員福利制度、退職プランまで、雇用・労働法・福利厚生に係るあらゆる問題について経営幹部及び人事担当マネージャーにアドバイスする。雇用差別や従業員の誤分類に関する紛争・訴訟にも対応している。当事務所に入所する前は、14年間保険会社に勤務し、フォーチュン500に選ばれた企業や有名大学など幅広い分野の顧客層を相手に保険業務を行っていた。

田原　直 インターナショナル・リーガル・アドバイザー
主要取扱分野は、クロスボーダー及び国内取引に関する企業法務、M&Aにおけるデューデリジェンス、融資契約や株式購入・株主間契約の作成等の各種サポート。商品、サービスまたはテクノロジーの開発・製造・販売、生産・供給配置に係る販売代理店や販売店との取引等、商事取引に関する案件に関与した経験を有する。当事務所に入所する前は、東京の法律事務所で6年間、日本の弁護士として勤務していた。米国ではニューヨーク州弁護士資格のみを保持。

連絡先

徳吉　史子
ディレクター（グローバル・クライアント・サービス）
Tel: 312-245-7439
E-mail: ftokuyoshi@masudafunai.com
www.masudafunai.com

なる運営職の要件の一つである)「裁量的かつ独立した判断を行う」ものではないとの見解も示しています。

そして、米国労働省によれば、フィールドサービス・エンジニアは、割増賃金の受給対象である高度な技能を有する技術者(Highly Skilled Technicians)の特徴に最もよく当てはまるとの見解を示しています。

上記を踏まえると、多くのフィールドサービス・エンジニアは、割増賃金に関する規制の適用除外となる従業員には該当せず、1週間のうち40時間を超える労働時間に対して、割増賃金を支給する必要がある場合がほとんどであると考えられます。

2. ビジネスメール詐欺

ビジネスメール詐欺(Business Email Compromise(BEC))とは、電子メールを用いて、企業の経営者や従業員などになりすまし、金銭の支払いを要求したり、不正に情報にアクセスしたりする詐欺行為をいいます。企業の電子メールシステムへのアクセス権を不正に得たり、ソーシャル・エンジニアリングの手法(特に、不注意に情報を手渡してしまうように心理的に操作する手法をいいます。)を用いることで、従業員を欺き、金銭や機密情報を入手することが一般的です。このビジネスメール詐欺は、ここ数年で、非常に増加し、規模の大小を問わず、あらゆる企業にとって大きな脅威となっています。

その中でも特に典型的なビジネスメール詐欺の手法として、ある従業員の上席や取引先になりすまし、その従業員に対して、送金を指示したり、機密情報を送付するように指示するものがあります。このビジネスメール詐欺に用いられる電子メールの内容は、あたかも正規のものであるかのように非常に巧妙に作られ、正規のドメインと非常に類似している偽のドメインを利用していることも多くあります。例えば、正規のドメインが「abc.com」である場合、「ab-c.com」や「a6c.com」といったように、しっかり確認しないと見誤ってしまうように作られている場合があります。

米国連邦捜査局のインターネット犯罪苦情センター(Internet Crime Complaint Center(IC3))の2021年インターネット犯罪報告書によれば、ビジネスメール詐欺に関して、2021年だけで、同センターに報告された苦情件数が19,000件以上、被害の調整済損失額も24億ドル近くにまで上っています。

例えば、近年の事例では、日本企業の米国子会社において、何者かが、日本企業の経営幹部になりすまし、米国子会社の従業員に対して、虚偽の情報を用いて3000万ドル近くの送金を指示し、流出させた例がありました。また、別の例では、米国の防衛関連企業において、何者かが、同企業の正規の取引先になりすまし、虚偽の発注書を用いて軍事関連機器の送付を求め、実際に送付されたとされる事例もありました。

さらに、最近では、金銭や機密情報のほかに、物品を要求するものも増え始め、特に食糧・農業分野における企業等に対して、米国連邦捜査局、米国食品医薬品局および米国農務省が共同で注意喚起をしています。

このようにビジネスメール詐欺が横行することになった一つの理由として、技術的な専門性がそれほど必要なく、比較的簡単に遂行できることが挙げられます。簡単に入手可能なツールだけでも、信ぴょう性のある巧妙な内容のフィッシング・メールやなりすましドメインを作成することができます。

ビジネスメール詐欺の被害を防ぐためには、各企業において、従業員に対してビジネスメール詐欺によるリスク等に関する研修を行い、強力な電子メールのセキュリティー・プロトコルを導入することが考えられます。これには、二段階認証の使用や定期的なパスワードの変更、疑わしい電子メールをブロックするための電子メールフィルターの導入などが含まれます。

また、機密情報や会社資金などの取扱いに関するプロトコルを導入することも重要です。例えば、取引先に対して送金をする場合に数段階の承認プロセスを設けることが考えられます。また、取引先(と思われるところ)から支払先口座に変更があった旨の電子メールを受け取った場合には、(仮に電子メールの送信元が正規のものであったとしても、不正に入手されたものである可能性もあるため、)実際に振り込む前に、電話で取引先に確認することも必要となってきます。

さらに、フィッシング・メールやその他の疑わしい行為を事前に検知し、ブロックするために、人工知能や機械学習の技術を利用した、より高度な電子メールのセキュリティー・ソリューションを導入することも考えられます。

もっとも、上記のような対策を行ったとしても、ビジネスメール詐欺のリスクを完全に排除することはできません。万が一、被害にあったときに備えて、サイバー保険に加入しておくことも、被害を最小化するためには検討に値します。ただし、ビジネスメール詐欺については保険の対象となっていなかったり、別途特約を付ける必要があったりすることもあるので、注意が必要です。

以上のように、ビジネスメール詐欺は、非常に巧妙な手法で会社の資金や機密情報を盗み取り、さまざまな企業に対する大きな脅威となっています。強力な電子メールのセキュリティー・プロトコルの導入や従業員にそのリスク等に関する研修を行うことによって、ビジネスメール詐欺の被害を未然に防ぎ、財政的な損失を最小化することが可能となります。