西村あさひ法律事務所
NISHIMURA & ASAHI
危機管理ニューズレター

2017 年
1 月号

Ⅰ. TEVA 事件

執筆者:木目田 裕、平尾 覚、吉本 祐介

イスラエルの世界最大の後発医薬品製造会社である TEVA は、2016 年 12 月 22 日、ロシアなどにおける Foreign Corrupt Practices Act(以下「FCPA」といいます。)違反に関して、米国司法省(以下「DOJ」といいます。)との間で 283 百万ドルを支払う旨の訴追延期合意(Deferred Prosecution Agreement、以下「DPA」といいます。)を締結すると共に、同日、米国証券取引監視委員会(以下「SEC」といいます。)との間でも 519 百万ドルを支払う旨の和解に合意しました。また、TEVA の子会社であるロシア企業の TEVA LLC(以下「TEVA ロシア」といいます。)は、ロシアにおける FCPA 違反に関して、DOJ との間で有罪答弁合意(Plea Agreement、以下「PA」といいます。)を締結しました。

TEVA に対して科された罰金額は、史上 4 番目に高い罰金額であるとともに、製薬業界に限っていえば、最も高い罰金が科された事案となります。

また、TEVA 事件において、注目に値するのは、TEVA ロシアが贈賄を行った方法です。TEVA ロシアは、ロシア政府による薬の調達に影響力を有するロシア公務員が実質的に支配しているロシア企業を TEVA 製の薬の販売会社とした上で、通常以上に値引きした価格で薬を当該ロシア企業に販売しており、この値引き販売によって当該ロシア企業が得た利益が賄賂と認定されました。

販売代理店等を起用する際に、いわゆる贈賄デューデリジェンスを行う企業は増えつつあります。贈賄デューデリジェンスを行う際の視点の 1 つは、当該販売代理店等が公務員と関係を有するか否かというものです。仮に当該販売代理店等が企業のビジネスに影響力を有する公務員により支配されている企業であった場合、当該販売代理店等に対する有利な取り計らいが公務員に対する賄賂であると認定されるリスクがあります。TEVA 事件は、販売代理店等を起用する際の贈賄デューデリジェンスの必要性を改めて教えてくれる事件であるといえます。

また、TEVA 事件では、米国上場企業である TEVA だけでなく、TEVA ロシアも FCPA による摘発の対象となりました。外国企業や外国人が外国公務員贈賄に及んだ場合の処罰について規定した 15 U.S.C. 78dd-3 は、外国企業や外国人が FCPA の適用対象となるためには、「while in the territory of the United States」すなわち米国の領域内で違反行為に及ぶことを要求しています。しかし、本件では、DOJ は、15 U.S.C. 78dd-3 を適用するのではなく、TEVA ロシアは、米国上場企業である TEVA の Agent として FCPA 違反に及んだとして、米国上場企業による外国公務員贈賄行為を規制する 15 U.S.C. 78dd-1 を適用しました。

単に、親子関係にあるからといって、子会社が親会社の Agent となるわけではありません。子会社が親会社の Agent に該当する場合、親会社は、Agent である子会社の債務も負担することになり、部分的には、法人格否認が認められたのと同様の効果が生じます。そのため、法人格否認が通常認められないのと同様に、子会社が親会社の Agent に該当するのも、親会社が子会社を過度に支配した場合など例外的な場合に限られるというのが一般的な理解です。DOJ も「A Resource Guide to the U.S. Foreign Corrupt Practices Act」において、問題となっている取引について、親会社が子会社に対してどの程度の影響力を有しているか、たとえば、親会社が子会社の活動をどの程度把握し、子会社の活動を指揮する力を有しているか否かを勘案の上、子会社が親会社の Agent に当たるか否かを判断するとしています。この点、簡易起訴状の記載からは、TEVA と TEVA ロシアとの間に、TEVA ロシアが TEVA の Agent であることを認めるに足る事情が記載されているとはいえません。

もっとも、本件では、TEVA は DOJ と DPA を締結することができています。TEVA ロシアが TEVA の Agent であることを認め、FCPA の域外適用を受け入れ PA に応じたのは、TEVA が DPA を締結できずに有罪答弁をし、そのビジネスに重大な悪影響が及ぶ事態を回避するという戦略上の判断からである可能性があります。したがって、本件で TEVA ロシアが Agent であることを受け入れた事実を過大に捉える必要はないかもしれません。

いずれにせよ、DOJ が比較的緩やかに Agent 性を認定する傾向があることには留意が必要です。

木目田 裕（きめだ ひろし）　西村あさひ法律事務所　弁護士
h_kimeda@jurists.co.jp

主たる業務分野は、企業の危機管理・争訟。危機管理の観点からは、決算訂正問題やインサイダー取引事案、役職員不祥事、情報漏洩案件、海外公務員贈賄案件、独禁法違反案件の対応等について種々の案件でアドバイスしている。争訟の観点からは、税務争訟や証券訴訟、会社争訟(責任追及訴訟、敵対的買収防衛)、独禁法関係争訟等を手がけている。なお、法令案・政策案の立案案件にも従事。

平尾 覚（ひらお かく）　西村あさひ法律事務所　弁護士
k_hirao@jurists.co.jp

公正取引委員会、証券取引等監視委員会をはじめとする国内当局対応、行政機関との紛争対応、企業不祥事対応、訴訟対応のほか、国際カルテルや FCPA 事案等への対応その他海外当局による捜査/調査対応などを手がける。

吉本 祐介（よしもと ゆうすけ）　西村あさひ法律事務所　弁護士
y_yoshimoto@jurists.co.jp

2002 年弁護士登録。三井物産株式会社法務部及び米国三井物産株式会社ニューヨーク本店出向後、2012 年ジャカルタの Ali Budiardjo, Nugroho,Reksodiputro 法律事務所出向。海外各国におけるコンプライアンス問題や日本企業のアジア進出などを幅広く手掛ける。

Ⅱ. 企業不祥事における個人責任の追及についての日米の温度感の差異とその変化の芽

執筆者:木目田 裕

最近、広く知られるようになっていると思いますが、企業不祥事において、違法行為を行った役職員個人の刑事責任を含む個人責任をどのように捉えるか、日米で大きな温度差があります。

日本ですと、横領や背任のような個人が不正に利得した事案は別にして、企業不祥事について、役職員個人が私腹を肥やしたのではなく、あくまで会社のために違法行為を行ったに過ぎないのだから、役職員個人を厳しく処罰したり、その個人責任をあまり厳しく追及するべきでない、むしろ組織としての会社を厳しく処罰すべきだ、という感覚が一般的だと思われます。例えば、カルテルであれば、橋梁談合のころは一時的に企業も社会も個人の責任を特に厳しく問題にしていましたが(個人の逮捕・勾留、懲戒解雇など)、そうした一時の例外を別にすると、「刑事責任が問われるとしても在宅起訴で済む」、「刑事事件にでもならない限りは懲戒解雇まではせず、本社又は関係会社等で雇用を継続する」、「国際カルテルで米国に服役した個人について、服役中はもとより服役後も解雇はしないで関係会社等で雇用を継続する」という対応が少なくありません(むしろ一般的と言ってもよいと思います)。これは、企業が役職員に甘いというだけでなく、日本社会の一般的な感覚ではないかと思います。例えば、カルテルにより米国で数十人の日本人が服役しているという新聞報道等があれば、少なからぬ日本人が本人や家族のことを同情する気持ちを抱いたと思います。また、いわゆる日本版司法取引をめぐる議論でも、日本の当局や実務家、研究者の間では、「上司が部下の犯罪関

与を明らかにすることで寛大な処分を得るなんて、あり得ない」、「企業不祥事で役職員個人が具体的に利得しているわけでもないのに、企業が当局に積極的に違法行為を自主申告して捜査協力したからといって、個人を厳しく処罰して、企業を処罰しないという対応はとれない」という感覚が強いと思います。これは、ある意味で、第二次世界大戦後の日本企業社会における団結性・帰属意識の強さの現れなのだろうと思います。というのも、役職員が自分個人にとっては出世とか社内の評価くらいしかメリットがないのに、会社のために自分の人生を棒に振るようなリスクを進んでとっているからであり、米国の法曹等からはなかなか理解して貰えない行動様式です。

その米国ですが、よく指摘されるように、エンロン事件に際して、アーサー・アンダーセンを破たんさせて、多数の無辜の役職員を失業させるなどしたことを踏まえ、特に 2000 年以降は、「違法行為をした個人は厳しく処罰し、必ず刑務所に服役させて身をもって償ってもらい、一般予防を図る。企業については、違法行為による収益は罰金等として剥奪し、DPA(Deferred Prosecution Agreement)等を通じて再発防止策を図って貰えれば、それでよい。違法行為があったからといって企業を破たん等させるのは、無辜の役職員や株主・取引先等にいわば二重の損害を与えてしまうから、そこまで企業を追い込まない」という考え方が一般的であるように思われます。そのため、企業不祥事で DPA が多用されるようになったわけです(木目田＝山田「企業のコンプライアンス体制の確立と米国の訴追延期合意—Deferred Prosecution Agreement—」旬刊商事法務 1801 号 43 頁以下(2007 年))。また、こうした米国の考え方は、米国司法省の FCPA に係るいわゆるパイロットプログラム(https://www.justice.gov/opa/file/838386/download)からも明らかです。

以上のように、企業不祥事における個人責任(特に刑事責任)の追及についての日米の温度感の差異は非常に大きいものがあります。実際、米国司法省が関係する案件ですと、役職員個人の刑事責任追及に関係する点だけでなく、米国司法省の担当検察官から違法行為に関与した役職員の即時の解雇を求められ、日本企業が直ちにこれに応じないのは何故なのかについて米国司法省側に理解して貰うのは大変です。

ところが、最近、日本企業について、もしかしたら米国型発想の芽も出つつあるのではないか、と感じることがあります。企業不祥事があった場合の役職員個人の刑事処罰、懲戒解雇といった処分などの点で、日本企業にしてはドライだなと感じる場面が徐々に現れつつあると感じます。

数年前の年賀状に「敵対的買収防衛、ガバナンス改革、カルテル、刑事司法改革など、日本の法社会は、10 年、20 年という時間差で、米国を追いかけているように感じます。一般刑事事件でも、60 年代半ばのジョンソン大統領の下で設置された刑事司法改革委の報告書を読むと、まるで 90 年代から 2000 年前後の日本社会のことを論じているようで、非常に興味深く感じます」と書いたことがあります。

やはり、この点でも、日本社会は米国を追いかけることになるのか、数十年前の米国社会は、いかなる物の考え方をしていたのか、興味が尽きないところです。

木目田 裕(きめだ ひろし)
西村あさひ法律事務所 弁護士
h_kimeda@jurists.co.jp

主たる業務分野は、企業の危機管理・争訟。危機管理の観点からは、決算訂正問題やインサイダー取引事案、役職員不祥事、情報漏洩案件、海外公務員贈賄案件、独禁法違反案件の対応等について種々の案件でアドバイスしている。争訟の観点からは、税務争訟や証券訴訟、会社争訟(責任追及訴訟、敵対的買収防衛)、独禁法関係争訟等を手がけている。なお、法令案・政策案の立案案件にも従事。

Ⅲ. 高度化されたサイバー攻撃

執筆者:北條 孝佳

1. 最近のサイバー攻撃事例

毎週のように様々な組織等がサイバー攻撃を受け、被害に遭われたという報道を耳にしていると思います。最近の事例として、日本では 2016 年 11 月に日本経済出版社の端末が、業務上のやり取りを装った標的型メール攻撃によってマルウェアに感染し、攻撃者が用意した外部サーバと通信を行い、約 1,200 件の取引先の個人情報を窃取される事案が発生しました。

海外では 2016 年 2 月にバングラデシュ中央銀行において、大規模な不正送金事件が発生しました。バングラデシュ中央銀行をサイバー攻撃した攻撃者らは、同銀行のアメリカニューヨーク連邦準備銀行口座から他国の複数の口座に対して 9 億 5,100 万ドルの不正送金が試みられ、実際に 8,100 万ドルがフィリピンの口座へ送金されました。本件は、攻撃者らによる 5 回目の不正送

金の際、送金先の口座名を「foundation」と記載すべきところを誤って「fandation」と記載したことによって偶然に発覚したものであり、このミスがなければさらなる被害が発生した可能性がありました。バングラデシュ中央銀行のシステムにはファイアウォールと呼ばれる不要な通信を遮断する機器が導入されていなかったことも起因して、同銀行の端末がマルウェアに感染し、攻撃者はバングラデシュ中央銀行内のシステム等を詳細に把握した後に不正送金が行われました。また、このような世界中の銀行や金融機関との取引においては、SWIFT(Society for Worldwide Interbank Financial Telecommunication:国際銀行間通信協会)が提供しているシステムが利用されていますが、マルウェアによってバングラデシュ中央銀行の端末が利用するこのシステムに対しても攻撃が行われ、不正な取引が発覚しないように改ざんされていました。

バングラディシュ中央銀行に対する攻撃の他にも、2016 年 11 月には、アメリカ海軍において、委託先業者の社員が使用していた端末が攻撃され、アメリカ海軍の現役及び退役兵士ら 13 万人以上の社会保障番号を含む重要情報が窃取される事案が発生し、さらに、同年 12 月には、韓国軍において、外部ネットワークと内部ネットワークの両方に接続されていたサーバを介して多数の端末がマルウェアに感染し、軍内部ネットワークに保存されていた軍事情報が窃取される事案が発生しています。

2. 標的型攻撃

これらのサイバー攻撃は、いずれも標的型攻撃と呼ばれる特定の組織や企業等を狙って組織等が保有する機密情報や金銭を窃取することが目的の攻撃と考えられます。標的型攻撃の主な手法は、①攻撃者が用意した Web サイトに対し、攻撃対象組織の端末から接続された場合にはマルウェアに感染させ、それ以外の組織から接続された場合には通常の Web サイトを閲覧させる「水飲み場攻撃」や、②マルウェアが添付されたメールを受信した人が、マルウェアと気付かずに添付ファイルを実行して感染してしまう「標的型メール攻撃」の 2 種類があります。いずれも標的となった組織等の人たちは、攻撃に気付くことなくマルウェアに感染させられてしまい、機密情報を含む組織等の様々な内部情報を窃取されてしまいます。

標的型攻撃に使用されるマルウェアは、過去にも別の組織等で使用されたことのある既知のマルウェアがほとんどですが、通常のウイルス対策ソフトではまず検知できません。それは、通常のウイルス対策ソフトは、マルウェアの核となる実行コードに着目し、コードが一致していればマルウェアであると判定しますが、この核となる実行コードが隠ぺいされたり、暗号化・難読化されたり、分割されたりした場合には、マルウェアではないと判定してしまうからです。実際に、あるマルウェアは核となる実行コードを難読化した上で 3 つのファイルに分割し、実行時に結合して動作させるという複数の仕組みを実装し、ウイルス対策ソフトでは検知できないようにしている例もありました。さらに、攻撃者は作成したマルウェアを予め様々なウイルス対策ソフトで検知されないことを確認した上で送信していますので、検知されないことは実証済みです。

ウイルス対策ソフトを開発している企業もこのようなマルウェアに対抗するために、マルウェアの挙動に着目した検知技術を開発したり、最近では AI(Artificial Intelligence:人工知能)を用いた検知技術を開発したりしていますが、完成度はそれほど高くなく、完成して一般的に普及するにはまだまだ時間がかかると考えられます。

標的型攻撃に用いられるマルウェアに感染すると、マルウェア自身が発見されないようにマルウェア本体を通常の OS(Windows 等のオペレーティングシステム)上で動作している正規のプログラムに偽装したり、不正なコードのみを注入(インジェクション)したりします。また、外部との通信を行う場合も、他の外部通信に紛れ込ませるために端末の使用者がブラウザで Web サイトを閲覧しているときにだけバックグラウンドで外部と通信を行ったり、特定の時間や特定の期間のみ動作するように設定されていたりします。さらに、感染した端末の電源を切っても、再度電源が入ればマルウェアが実行されるように仕組まれていたりするため、完全に除去しない限り半永久的に動作するものも存在します。

窃取した情報を外部に送信する場合は、収集したファイル群にパスワードを付けて暗号化し圧縮して外部に送信し、ファイルサイズが大きくなる場合には、ファイルを分割して一定期間の間隔を空けて送信します。このようにすることで、外部との通信量が増加しないように工夫しており、また、仮に管理者や解析業者に圧縮ファイルの断片を発見されたとしてもパスワードを知らなければ開くことができないように対策をしています。

以上、述べてきましたように、標的型攻撃に用いられるマルウェアは、端末の使用者やシステムの管理者等に気付かれないように、かつ、継続的に動作するように高度に設計されています。そのため、このような高度化されたマルウェアを発見・駆除することは非常に困難になってきています。

3. サイバー攻撃への対応

自組織が、高度に設計されたマルウェアに感染した端末を発見することは困難になってきており、第三者や外部に委託している業者からの報告により発見されることが多くなってきています。そのような報告に対し、組織として適切に対応しなければ、顧客や製品開発等の機密情報が攻撃者らに窃取されたり、場合によっては攻撃者らの遠隔操作によって同端末から顧客等を攻撃したりして、感染した組織等は被害者のみならず、加害者になる可能性もあります。添付ファイルを実行してしまいマルウェアに感染したり、端末が再起動を繰り返して業務が停止したりするだけであれば被害は少ないですが、さらに攻撃者に遠隔操作され、機密情報が漏えいしたり、不正送金されたりしてさらなる被害が発生すれば、これはインシデント(事案)に発展します。外部からの報告にはインシデントに発展してからのものもありますので、そのような場合は被害も甚大になりかねないため、早急に対処する必要があります。

外部から報告を受けて、不審な通信の存在を認識したのであれば、感染した端末を早急に特定し、対応しなければなりません。しかし、不審な通信先を遮断したりウイルス対策ソフトを最新にして全端末をスキャンしたりするだけでは適切な対応とはいえません。前述のように標的型攻撃に使用されるマルウェアは、そのような方法では発見できないように高度に設計されているからです。そのため、外部と通信を行った一般的なログを全て収集して分析したり、外部と通信を行う生のデータを数日間保存し、マルウェアではない通信データを一つずつ確認して除外するホワイトリスト方式などにより、感染している端末を特定する方法が考えられます。そして、感染した端末を特定できた場合には、前述しましたように高度に設計されたマルウェアである可能性があるため、専門の業者に対応を依頼することを推奨します。解析の専門部隊を有する警察に相談することも選択肢の一つとして考慮することも推奨します。また、感染端末は、無害化するまでは業務では絶対に使用しないでください。業務で使用し続ければ、キーボードの打込みデータやメールのやり取り、ブラウザにて閲覧した履歴等、当該端末で行われている活動は全て攻撃者らに監視・窃取される可能性があるからです。

標的型攻撃の主な目的は情報窃取にありますが、このようなマルウェアにはシステムを破壊する機能を有しているものもあるため、最悪の場合は組織内の全ての端末が一斉に停止させられる危険性をも秘めています。実際に、韓国では、2013 年 3 月 20 日、放送局及び銀行の 6 組織のシステムに使用されていた端末がマルウェアに感染し、破壊され、システムが使用できなくなった事例が報告されています。

4. 結び

サイバー攻撃によって、情報が漏えいしたり、システムが停止したりしますと、情報元の被害者らから損害賠償請求をされたり、企業等のセキュリティ対策に不備があったとして評価が下がり株価に影響したりすることも考えられます。今やサイバー攻撃対策は情報システムを管理する方々だけの責任ではなく、経営者らによる適切な管理体制を構築し、インシデントが発生した場合には、適切かつ迅速な対応ができるように準備しておかなければならないという経営責任になっています。また、サイバーセキュリティは日々進化しているため、どのような管理体制を構築し、どのような対処をすれば経営者らの善管注意義務が果たされたといえるかは、明白ではありません。適宜見直しを行い、時勢に沿った管理、対応をすることが求められているといえるでしょう。

ほうじょう　たかよし
北條　孝佳　　西村あさひ法律事務所　弁護士
ta_hojo@jurists.co.jp
危機管理、社内不祥事などの企業法務に従事。特に情報漏洩をはじめとする様々なサイバーセキュリティ事案の調査・法的措置・再発防止策に関するアドバイスを行っている。2000 年、警察庁入庁。元警察庁技官。NTT 情報流通プラットフォーム研究所出向、警察大学校警察情報通信研究センター、東京大学生産技術研究所との共同研究等に従事し、数多くのサイバー攻撃事案を経験。2015 年弁護士登録(東京弁護士会)、2016 年当事務所入所。