June 2, 2020

2020 年 6 月 2 日

CONFIDENTIALITY AND VIDEO-CONFERENCING

秘密保持とテレビ会議

There is no doubt that the current global COVID-19 pandemic and resulting work-from-home rules, restriction of travel, and other preventative measures have caused a major shift in the way that we all work and interact with our colleagues, business partners, and customers. While the inconvenience and isolation caused by the current situation may certainly not be ideal, it must also be said that video-conferencing and similar technologies have been vital in allowing our businesses to continue to operate as we all work through this challenging period. Along with the benefits of these video-conferencing technologies, however, there naturally also are certain risks primarily relating to security. According to IT security experts, there is always a trade-off and balance between ease of use and security associated with these technologies, and those using them should be aware of their vulnerabilities.

As an attorney, the question I most often receive is what level of care or vigilance is legally required when discussing confidential information, personal information, or trade secrets using the various video-conferencing technologies which currently exist. In addition, there is the issue of how to legally protect both companies and individuals from hacking or inadvertent leaks of confidential information in the course of tele-working or video-conferencing.

The fact is that, while certain video-conferencing applications and systems have been proven to be more secure that others, no system appears to be completely hack-proof. Moreover, from a legal perspective, it is not required that a video-conferencing system be entirely hack-proof, but rather that the system's security features and other measures taken to ensure confidentiality are reasonable both in light of the relevant technology being used as well as the level of sensitivity of the information being discussed.

In advising clients regarding their legal obligations to protect confidential information and establish internal controls, I focus on the three following areas:

現在、世界的に流行中の新型コロナウィルス（COVID-19）により、在宅勤務や移動制限などの予防措置がとられていますが、これにより私たちの働き方や、同僚・取引先・顧客との関わり方に大きな変化が生じています。現状の不便さや孤立は決して理想的なものではないかもしれませんが、この困難な時期を乗り越えて事業を続けていくためには、テレビ会議などの技術が不可欠であるとも言わなければなりません。しかしながら、こういったテレビ会議技術には、利点に加えて、主にセキュリティに関連する特定のリスクも当然のことながら存在します。IT セキュリティの専門家によると、これらのテクノロジーの使いやすさとセキュリティとの間には、常にトレードオフとバランスがあるとされており、ユーザーはその脆弱性を認識しておく必要があります。

弁護士として私が最もよく受ける質問は、今あるさまざまなテレビ会議技術を利用して機密情報、個人情報、又は企業秘密について議論する際に、どの程度の注意又は警戒が法的に要求されるかというものです。また、テレワークやテレビ会議に絡むハッキングや機密情報の不注意による漏洩から、企業と個人の双方をどのように法的に保護するかという問題もあります。

実際のところ、一部のテレビ会議アプリやシステムは、他のものよりも安全であることが証明されていますが、どのシステムであれ、ハッキングを完全に防ぐことは出来ないようです。法的には、完全なハッキング対策が求められるのではなく、使用されている関連技術や扱われている情報の機密性のレベルに照らして、テレビ会議システムのセキュリティ機能や機密性を確保するために講じられるその他の措置が合理的であることが求められます。

機密情報を保護し、内部統制を確立するための法的義務についてクライアントに助言するにあたり、私は、以下の 3 つの分野を重視しています。

1) 技術的・物理的セキュリティ

2) 契約及び方針

1) Technological/Physical Security

2) Contracts and Written Policies

3) Education of Employees

The key from a legal perspective with respect to these issues is to ensure that a company has all three aspects covered. Doing so allows the company to not only prevent the hacking or unauthorized disclosure of trade secrets or other confidential information, but can also protect the company from claims of negligence in the event such hacking or unauthorized disclosure occurs.

1. Technological/Physical Security

The technological and physical security aspects of tele-working or video-conferencing relate to the effective use of encryption, passwords, waiting rooms, firewalls, requiring the host to confirm the identity of all participants, and other security measures. There have recently been numerous news reports identifying very serious security issues associated with certain widely used video-conferencing systems, such as allowing outside third parties to participate in, eavesdrop on, and even disrupt confidential corporate video-conferences. Therefore, in order to avoid the unauthorized disclosure of confidential information as well as future liability, it is incumbent upon companies, individual managers, and employees to be aware of the security risks associated with the video-conferencing software and other systems they are using, and in the event such systems are inadequate in light of the sensitivity of the information being discussed, utilize other systems or find alternative means of communicating such highly sensitive information.

2. Contracts and Written Policies

The current COVID-19 pandemic has caused many companies and other organizations to develop official written policies addressing issues related to work from home, video-conferencing, and corporate communications. One of the main purposes of these types of official policies is to provide important rules with which employees must comply in order to avoid the unauthorized disclosure of company trade secrets, confidential information, and personal information. Such policies can also become part of the contract between the employee and the company. In addition, employment contracts which contain appropriate confidentiality provisions also serve this purpose and create a legal obligation to protect these

3) 従業員教育

これらの論点を法的観点から見た場合、企業が 3 つの側面すべてを確実にカバーできるようにすることが重要になってきます。そうすることで、企業は、企業秘密やその他の機密情報のハッキングや不正開示を防止できるだけでなく、ハッキングや不正開示が発生した場合の過失の主張からも自社を守ることができるのです。

1. 技術的・物理的セキュリティ

テレワークやテレビ会議の技術的及び物理的セキュリティは、暗号化、パスワード、待機室、ファイアウォール、ホストによる全参加者の身元確認、及びその他のセキュリティ対策の効果的な使用が関係します。最近、広く利用されているあるテレビ会議システムに関して、非常に深刻なセキュリティ上の問題を明らかにするニュースが多数報道されました。例えば、企業の内部のテレビ会議に、外部の第三者が参加する、会議を盗聴する、さらには妨害するといったものです。したがって、機密情報の不正開示や将来的な損害賠償責任を回避するためには、利用しているテレビ会議ソフトやその他のシステムに関連するセキュリティ上のリスクを認識するとともに、扱っている情報の機密性に照らしてそのシステムが不十分である場合には、他のシステムを利用するか、又はそのような機密性の高い情報をやり取りするための代替手段を見つけることが、企業、個々の管理者及び従業員の義務となります。

2. 契約及び方針

現在の新型コロナウィルスの世界的流行により、多くの企業やその他の組織で、在宅勤務、テレビ会議及びコーポレート・コミュニケーションに関連する課題に対処するための文書による公式方針の策定が進んでいます。こういった公式方針の主な目的の 1 つは、会社の企業秘密、機密情報、及び個人情報の不正開示を回避するために従業員が遵守しなければならない重要なルールを定めることにあります。このような方針は、従業員と会社との間の契約の一部となることもあり得ます。また、適切な秘密保持条項を含む雇用契約もこの目的に資するものであり、この種の機密性の高い情報を保護する法的義務を生じさせます。契約や会社の公式方針は、個人の法的義務を生み出すだけでなく、以下に述べるような個人の責任に関する教育という目的にも適うものです。

3. 従業員教育

types of highly sensitive information. Not only do contracts and official company policies create legal obligations for individuals, they also serve the purpose of educating them regarding their responsibilities as discussed below.

3. Education of Employees

By far the most cost-effective means of avoiding the unauthorized disclosure or hacking of confidential video-conference communications, and also legally protecting one's company in the event of such unauthorized disclosure, is educating employees beforehand as to the limitations of the relevant technology as well as their obligations to maintain confidentiality. The vast majority of leaks of company trade secrets and other confidential information are inadvertent and can be avoided by educating employees through job orientation training, seminars, internal webinars, one-on-one guidance, exit interviews, and written policies and contracts regarding the importance of confidentiality as well as concrete rules and actions which employees should take. It is far less expensive to engage in these types of educational activities as a preventative measure than to have to initiate, or defend against, formal legal action after a leak or unauthorized disclosure of confidential information has occurred. At the same time, education of employees also protects a company against claims resulting from intentional trade secret theft or economic espionage by providing evidence that the company did indeed provide the relevant bad actor with confidentiality training and was not negligent.

The above are all essential elements of an effective Trade Secrets Program which companies should implement in order to protect their confidential information during this challenging time requiring the widespread use of tele-working and video-conferencing. Moreover, the current global pandemic promises to change the ways in which we work well into the future, meaning that these technologies will likely become permanent and more prominent fixtures of the workplace going forward. Therefore, it is important to understand that these technologies, while vital and convenient, are also unfortunately associated with certain security and other risks which could expose companies and individuals to legal liability if not properly managed.

Finally, it must be emphasized that any Trade Secrets Program must address and be tailored to the specific needs and unique characteristics of each company or other organization based upon the above three pillars. Therefore, in order to create and

秘密のテレビ会議通信の不正開示やハッキングを回避し、不正開示があった場合にも自社を法的に保護するために最も費用対効果の高い方法は、なんといっても、従業員に関連技術の限界と秘密保持義務について事前に教育することです。企業秘密やその他の機密情報の漏洩の大部分は、不注意によるものであり、機密保持の重要性並びに従業員が従うべき具体的な規則及び行動に関して、入社時の研修、セミナー、社内ウェビナー、1 対 1 の指導、退職時の面接、それに明文化された方針や契約などを通じて従業員を教育することで回避することが可能です。こういった教育活動を予防策として行う方が、機密情報の漏洩や不正開示が発生した後に正式な法的措置を開始したり、法的措置に対して防御したりするよりも、はるかに費用が少なくて済みます。同時に、従業員を教育することで、企業は、意図的な企業秘密の窃盗又は経済スパイ行為に起因する請求を受けた場合も、当該行為を行った者に機密保持のための研修を実際に提供しており、同社に過失がなかったことの証拠を提示することで保護されます。

上述した事項はすべて、テレワークやテレビ会議の幅広い利用が求められるこの困難な時期に、企業が機密情報を保護するために実施すべき、効果的な「企業秘密プログラム」の必須要素です。現在の世界的な大流行が将来的に私たちの働き方を変えるとも言われており、それはすなわち、今後、これらの技術が恒久的かつより重要な職場設備になるだろうということです。よって、これらの技術は、便利で不可欠ではあるものの、適切に管理されない場合には、企業や個人を法的責任にさらす可能性のある特定のセキュリティ上のリスクやその他のリスクとも不幸にも結び付いているということを理解しておくことが重要です。

最後に、「企業秘密プログラム」は、上記の 3 つの柱に基づいて、各企業やその他の組織の具体的なニーズと独自の特徴に対応し、それらに適合するものでなくてはならないということを強調しておかなければなりません。したがって、効果的な企業秘密プログラムを作成し、実施するためには、適切な技術的・物理的セキュリティ対策に関連した資格を有する IT セキュリティの専門家と緊密に協力することが重要であり、また、上述の契約、方針及び教育上の措置を実施するために、資格を有する弁護士とも緊密に協力することが重要です。

北浜法律事務所・外国法共同事業

ジェリー・メステッキー（パートナー）
JMestecky@kitahama.or.jp

implement an effective Trade Secrets Program, it is important to work closely with qualified IT security professionals regarding appropriate technological/physical security measures, and also to work closely with qualified attorneys in order to implement the contractual, policy, and educational measures discussed above.

KITAHAMA PARTNERS

Jiri Mestecky (Partner)
JMestecky@kitahama.or.jp