企業情報を守るために

～情報漏洩防止の一環として～

株式会社メルク

目次

１．誰が貴社の情報を盗むのか

☆競合他社

☆産業スパイ

☆各国の諜報機関

☆不満のある社員

☆派閥争いのライバル側

☆労使紛争の相手側

☆寂しい秘書

☆低収入の出入り業者

☆マスコミ

☆名簿業者

２．どのような情報を盗むのか

☆顧客名簿

☆技術開発情報や新製品情報

☆インサイダー情報

☆キーパーソンの個人情報

☆役員の行動予定、立ち寄り先、個人情報

☆ライバル側の戦略、弱み

☆入札情報　…etc.

３．どのように盗むのか

☆オシント

(OSINT:Open source intelligence)

公開されている資料を集め分析

☆シギント

(SIGINT:signals intelligence)

通信、電磁波、信号等の傍受及び盗聴を利用した諜報活動

（代表例　エシュロン（Echelon）、盗聴）

☆ヒューミント

(HUMINT:Human intelligence)

人間を媒介とした諜報

☆イミント

(IMINT:Imagery intelligence)

偵察衛星や偵察機によって撮影された画像を継続的に分析

４．情報漏洩による被害

☆損害賠償の発生

企業の管理している個人情報や機密情報が漏洩した場合、多くのケースで損害賠償が発生します。事案の規模にもよりますが、損害賠償額は非常に高額になることが想定されます。また、企業ではなく個人単位で管理している情報が漏洩した場合でも、クレジットカードの不正利用などで金銭的な被害が発生する恐れがあります。

個人情報漏洩による平均損害賠償額

6億3,767万円

(NPO日本ネットワークセキュリティ協会)
2018年度

☆社会的信用の低下

情報漏洩の事案や事件がニュースなどで大きく報道されると、その企業は「情報漏洩を起こした会社」として認知されてしまい、企業イメージが悪化します。それによって社会的な信用が低下し、長期的な顧客離れなどにつながってしまうことも考えられます。

☆研究開発費の霧散

今まで掛けてきた新製品などへの研究開発費が全く回収できず、多大な損失となる恐れがあります。

☆失脚や敗北

派閥争いによる脱落や労使交渉の敗北を招きます。

５．最新事例

　2020年1月、ソフトバンク社員が在日ロシア通商代表部幹部職員に対して、不正に機密を漏洩し、不正競争防止法違反容疑で警視庁公安部に逮捕されました。
　7月9日に判決があり、懲役2年、執行猶予1年、罰金80万円の判決が言い渡されました。
　この事件に関しては、ご記憶の方も多いのではないかと存じます。

　少し内容を掘り下げてみます。

　逮捕された社員は当時通信設備構築担当の統括部長で、漏洩したものは「基地局づくりの手順書」でした。持参したノートパソコンの画面に表示し、写真を撮らせたと供述しています。

　出会いは東京・新橋の路上、偶然を装って一杯誘い、数回会食したのちに後任担当者に引き継いだ。
　2～3か月に一度会って、日露の霍光名所など当たり障りのない話をするうちに仲良くなり、徐々に機密情報を提供し、１回あたり20万円の現金を手渡しされるようになった。
　本人は「ただロシアの友人の役に立ってあげたかった、渡した情報もそれほど機密の情報とは思わなかった」と供述している反面、「連絡先どころか名前も教えてもらえず、次回の会合場所と日時を伝えられた。スパイかもしれないと思ったが後戻りできない状況だった。」と供述しています。

　ここで漏洩した資料が本人は大した内容ではないと言っていますが、導入されている装置のメーカー、型番や設置場所の情報が含まれていた場合、攻撃と諜報に非常に役立つものではないかと存じます。

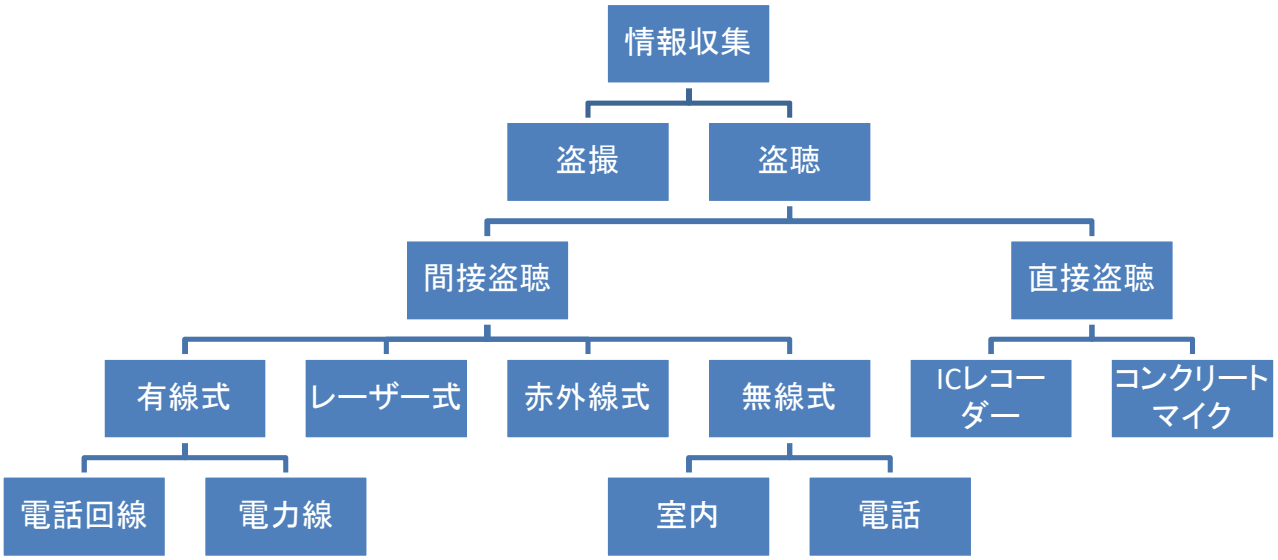
　裁判で明らかになった内容はこの1件ですが、本人は2回現金を受け取っていることを認めていますので、他にも漏洩した情報があることは間違いありません。また、ターゲットになったのが1人だけとは限りません。他にも表に出ないものもあるかもしれません。

　今回のケースはロシアが昔から使用している伝統的なヒューミントの手法ですが、一般の方には馴染みがなかったのかもしれません。

　明らかになっていない点としては、ロシア側はどのようにして彼を見つけターゲットにしたかです。
　ソフトバンクの公開情報の中にあったのか、内部に協力者がいたのか、電話をかけてききだしたのかなど様々な可能性があります。もしかすると盗聴器が設置されていたかもしれません。

　そして、次は貴社の誰かがターゲットになる可能性もあります。
　ロシア以外にも多くの国が日本の情報を今も狙っています。

６．情報収集装置の種類



市販されている盗聴器／盗撮器

					
コンセント型	コンセント型	ケーブルタップ型	ブラックボックス型	ACコンセント内部型	電卓偽装型
					
HDMIケーブル偽装型	電話回線用	カールコード偽装型	モジュラーコネクタ型	ペン型ICレコーダー	USBメモリー型ICレコーダー

					
ACアダプター型	マウス型	USBチャージャー型	デジタルクロック型	TVリモコン型	リモコンキー型
					
バインダー型	スマホ充電スタンド偽装型	スマホカバー型	ドリンキングリッド型	ヘッドホン型	スマホホルダー型

7．どこに設置されるのか

☆役員室

☆役員会議室／ボードルーム

☆応接室

☆経営企画部署

☆秘書室

☆新規事業部署

☆先端技術部署

☆研究施設

☆営業部署

☆経理部署

☆法務部署　…etc.

　これらの場所では机の上下、ペン立て、コンセント内部、延長ケーブル、応接テーブル裏、ソファ裏／クッション下、絵画裏、置物内部、キャビネット上部／裏、観葉植物、天井裏、壁内部などを定期的に盗聴器の有無を点検する必要があります。
　特にコンセントに差し込むだけで発見されるまで永遠に盗聴されてしまう延長ケーブルなどのコンセント型は短時間で交換できてしまうので、設置前に電波が出ていないか確認し封印シールを貼ってから設置することが重要です。
　定期的に盗聴点検を実施されていらっしゃらない企業様は一度現状を確認されてみてはいかがでしょうか。もしかすると既に盗聴器入りのものが設置されているかもしれません。
　また、経営会議など重要な会議の前にはタイムリーな実施が必要です。
　これらの場所以外でも役員様のご自宅や社用車なども定期的な盗聴点検をお勧めします。(実際に実施されていらっしゃる企業様もございます)

８．盗聴した情報の使用方法

☆M&A情報など企業で進行中の経営戦略を知ることができる

☆職場の人間関係を知り、利用する方法を考察する

☆誰と会ってどのような会話しているかを知り、企業の動向を考察する

☆職場に不満を持っている人物を特定し、協力者にする

☆偶然を装ってコンタクトする際の情報（出身地、興味、趣味など）を得る

☆行動予定を知り、生活のサイクルを把握する

☆特殊関係人がいないか把握し、利用方法を検討する

☆相手側の戦略を知り、対応策を検討することにより、先手を打つことができる

☆運がよければ弱みを握ることができる

☆運がよければ直接重要機密を知ることができる

９．日常的、定期的な盗聴点検のお勧め

以上のように盗聴は様々な方法で収集、利用され貴社を危機に陥れる可能性があります。

欧米では盗聴への対応をどのように実施しているかと申しますと、世界的な企業の場合、社内に専門のチーム（Sweeping Team）を持ち、HQや在外支店などを定期的に回って点検を行っています。

また、重要な場所には不審な電波の発信を自動的に検知する装置を天井に設置し、目に見えない電波を常時監視しています。（これは国内の企業でも実施されているところはあります）

しかも社員が出張する際には、簡易型の発見器を持参し、宿泊先で点検したり、場合によっては暗号電話機を持参したりしています。

また、世界的に有名な保険会社などは、専門業者と契約し、定期的に世界中で盗聴点検を実施しています。これは事実です。しかも最近始まったものではなく20年以上前から確認できている内容です。

国内に目を向けてみますと、何かおかしなことが起こってからの「盗聴調査」の時代が長らく続いておりましたが、ここ5年くらい前から定期的に「盗聴点検」を実施される企業様が増えてきました。

弊社が実施している上場企業様を中心に定期的に点検することにより安全を確認し安心を手に入れるという考え方が浸透してきたように思えます。

また、取引先の条件に定期的な盗聴点検を求める企業も出てきました。つまり、自分たちは情報漏洩防止対策を実施しているが、情報の提供先から漏れては困るということです。

盗聴点検は社内の一部の関係者しかその存在を知りません。例えば、総務部、社長室などです。ですので一般の社員の方はご存じありません。

また、対外的にも実施を秘匿される内容ですので、どこの会社が実施しているかも分かりません。
もちろん弊社も機密保持契約を締結しておりますので、ご説明の際に具体的な企業名を出すことはございません。
ただ、盗聴点検を実施し安心安全を担保されている企業様は確実に増えてきています。

他国では当たり前に攻撃と防御を実施している中、日本企業だけが盗聴に関して無策では勝ち抜いていくことは難しいとは思われませんか。

貴社がもしも定期的な盗聴点検を実施されていないのであれば、この機会にご検討をされることをお勧めいたします。

弊社がご提案している方法は、

①日常的な点検は弊社がやり方を社員の方にお教えし、社員の方が日常的／タイムリーに実施していただく。

②年1回の本格的な点検を弊社が担当させていただく。

この2本の柱で実施していただいております。

盗聴器はいつ仕掛けられるか分かりません。ですから少なくとも秋葉原で販売されている程度の誰でも簡単に入手でき仕掛けられる市販品は日常的に社員の方が点検するほうが良いと考えます。これだけでも盗聴のリスクは相当減ると思います。企業様によってはこれだけで良い場合もあります。

次に年1回弊社がEUの情報機関で使用されているのと同等の機材を使用しての点検を実施します。これは産業スパイや各国情報機関のターゲットになる可能性のあるグローバルに展開されている主に一部上場企業様で実施していただいております。

本当は3か月や半年に1回実施されると尚良いのですが、ご予算の関係と安全確認という意味合いから今のところ年1回の実施がほとんどです。

点検終了時にはご担当者様から、「今年も何もなくて安心しました」とのお言葉をいただいております。

貴社は何か事象がおこってから慌てて実施する「盗聴調査」、ネットワークセキュリティや入退室管理、防犯カメラなどと同様に常日頃から備え安全を確認する「盗聴点検」、どちらを選択されますか。　それとも何もせずに知らないうちに多大な損害を被ることを甘んじて受けますか。

ぜひご検討いただければ幸甚でございます。お問い合わせお待ちしております。

お問い合わせ先

株式会社メルク
新宿区西新宿6-10-1　日土地西新宿ビル8F

Tel:03-5288-5173
E-mail:csc@melc.co.jp

ご質問等ございましたらお気軽にお問い合わせください