中小企業のための

香港における サイバー犯罪

サイバー犯罪に対して香港の法律の現状

関連のある法律：

(1)刑事罪行条例（香港法律第200章）第161条：犯罪あるいは不誠実な目的でのパソコン使用罪

(2)刑事罪行条例第59条と60条：（他人の）財産に破壊や損傷を与える罪。59条により、「財産」の定義はパソコンデーターとプログラムにまで拡大された

(3)電気通信条例（香港法律第106章）第27A条：電気通信の手段でパソコンに無断侵入の罪

(4)窃盗罪条例（香港法律第210章）第11条：不法侵入罪の拡大解釈により、パソコンへの不法侵入もこれに該当する

(5)窃盗罪条例の第19条：不正経理（会計）罪の拡大解釈により、パソコン内の資料を破壊、損傷、隠す、偽造に関する罪

以上はサイバー犯罪に関連するわずかな法律です。正直なところ、今時のサイバー犯罪の前に無力な現状でしょう。これらの法律の本質は旧経済時代の法律であり、言い換えると、21世紀のサイバー犯罪は90年代の法律と思考のままで解決することは現実的ではありません。

問題点：

(1)サイバー犯罪は国境を越え、他国で発生する

当局（警察）は犯罪の新源地にさえ心当たりがありません。簡単に言うと、一般の犯罪は、犯罪が起こった国で発生するが、サイバーの世界（バーチャル世界）は他の国にいながら容易に対象国で犯罪を実行することができます。ほとんどの国の司法は国内で発生した犯罪に対しての司法権しか持ちませんが、オーストラリア、イギリスやシンガポールなどの国は海外で始動したサイバー犯罪を国内でも起訴することができます。つまり、海外から国内で被害を受けたサイバー犯罪は国内の法廷にも司法権があります。ただし、香港には国境外行為に関する司法権の立法は香港の立法会に拒否されました。

現在の法律では、海外で始動したサイバー犯罪を起訴することは無理であり、証拠・情報収取すら難しい状況です。

(2)「身元」への保護がほとんどない

多くのサイバー犯罪の特徴は身分が盗まれることです。ただし、香港の法律では、実際の「身元」は財産として見なされません。なおさら、バーチャルな身元は財産とみなされません。例えば、IDとパスワードが盗まれた時に、現在の香港法から見ると、被害者が自分のIDとパスワードが使用できれば、それは「盗まれてない」とみなされてしまいます。ただし、アメリカの法律は異なり、身元窃盗はかなり厳しい連邦法違反行為となります。

(3)重罰がない

現在の法律でハッキング、マルウェアなどの主要なサイバー犯罪に対して重罰がありません。すでに説明しましたが、法律が現在の状況に追いついておらず、香港当局が海外の証拠を取ることは制限されています。

結論：

万が一サイバー被害にあってしまった場合は、時間との戦いですので、警察への通報や弁護士への相談を含めすぐにでも動く必要があります。

サイバー犯罪の種類

—データーの窃盗

—お金の窃盗

—フィッシング（暗証番号の詐取）

—マルウェア（被害与えたり情報を盗み出したりする目的で開発された悪意のあるソフト）

—ハッキング（パソコン・ネットワーク侵入）

—身分の窃盗（IDとパスワードの窃盗）

—詐欺メール

など様々な種類があります。

サイバー犯罪者の特徴や本質

—集団的（国レベル、テロ、過激行動）

—高学歴・技術の所持者

—ハッキング設備は簡単に入手可能

—盗まれたデーターであるIDやパスワードは闇市場で巨大な需要がある

—国境を越え、他国で行動（黒幕は探しにくく、捕まえにくい）

筆者紹介

ANDY CHENG
弁護士　アンディチェン法律事務所代表
米系法律事務所から独立し開業。企業向けの法律相談・契約書作成を得意としている。香港大学法律学科卒業、慶應義塾大学へ留学後、在香港日本国総領事館勤務の経験もありジェトロ相談員も務めていた。日本語堪能
www.andysolicitor.com
info@andysolicitor.com