西村あさひ法律事務所

タイにおけるサイバー攻撃への対応

危機管理・アジア ニューズレター　2022 年 4 月 28 日号

執筆者:
E-mail 勝部 純
E-mail Vira Kammee
E-mail Vullope Techakasin
E-mail Pasayu Israsena Nah Ayudhaya

新型コロナウイルスの感染拡大はソーシャルディスタンスを余儀なくし、その結果、政府や民間事業者はインターネットベースの経済的取組みへと移行し、従業員はリモートワークを行い、取引に関するコミュニケーションや承認がインターネットを介して行われるようになりました。インターネットベースのコミュニケーションは、各種のサイバー犯罪を容易にしており、サイバー犯罪はタイでもグローバルでも増加しています。本ニューズレターでは、タイにおいて企業がサイバー攻撃を受けた場合にどのように対応すべきかについて紹介いたします。

1. タイにおけるサイバー攻撃

(1) タイ法における「サイバー攻撃」の定義

2019 年サイバーセキュリティ法において、「サイバー攻撃」とは、コンピューターシステム、コンピューターデータ又はその他の関連データに被害又は損害を生じさせることを意図した、コンピューター、コンピューターシステム又はプログラムの利用による行為又は違法な事業と定義されています。

(2) タイにおける典型的なサイバー攻撃の種類

✓ ランサムウェア

「ランサムウェア」は、情報を人質として利用するものであり、ファイルが文書形式、オーディオ形式、画像形式のいずれかにかかわらず、様々な種類のユーザーデータファイルをロック又は暗号化する目的で作成されたマルウェアの一種です。これにより、ユーザーは影響を受けたファイルにアクセスすることができなくなります。サイバー犯罪者は、ユーザーのデータベースに侵入し、ファイルを暗号化することにより、ユーザーによるアクセスを妨げ、一方、ファイルを回復するために一定の金額を支払うことを要求する身代金メモを残します。身代金の支払を行わなければ、影響を受けたファイルは回復されません。

また、サイバー犯罪者は、データ暗号化のみならずデータ侵害に及ぶランサムウェア攻撃を行っており、サイバー犯罪者は交渉力を高めるためにファイルに含まれる情報を盗みます。伝統的には、「身代金」は、データを復号する約束と引き換えに支払われる金銭であり、事業者が直ちに「人質」のデータを利用する必要がない場合は、身代金の支払について交渉したり、遅延させたりすることができる場合もあります。しかし、盗まれたデータが失われたり、著しく損傷を受けるリスクもあるため、そのようなリスクを軽減するために、事業者が直ちに身代金を支払う傾向があります。

✓ フィッシング

「フィッシング」においては、サイバー犯罪者は、一般的に、金融口座に関連するログイン情報(ユーザー名及びパスワード)などの重要な情報を取得するために、フィッシングメールをユーザーに送信します。例えば、サイバー犯罪者は、金融サービス提供者を装った電子メールを作成し、偽造されたファイルを添付したり、金融サービス提供者の本物のウェブサイトに類似

したウェブページを表示している詐欺ウェブサイトの URL を記載したりします。アクセスすると、ユーザーはログイン情報を入力するよう求められ、サイバー犯罪者は、そのようなログイン情報を利用して、ユーザーの金融情報にアクセスします。

(3) サイバー攻撃に関するタイの法律

✓ コンピューター関係犯罪法

2017 年コンピューター関係犯罪法は、コンピューターシステム又はデータへの不正アクセス等、各種のコンピューターの関係する犯罪を規律しており、通常、犯罪が行われた後に執行されます。

✓ 電子取引法

2001 年電子取引法は、「電子情報」を裁判で証拠として用いることを認めています。そのため、サイバー犯罪者に対して法的手続を開始するために弁護士によって収集され、電子データの形で裁判所に提出されたコンピューター関係犯罪に関する情報は、当該手続において証拠として用いることができます。

✓ サイバーセキュリティ法

2019 年サイバーセキュリティ法は、予防措置について規定しています。同法 49 条は、重要情報インフラ組織について、下記の目的を持つ又はサービスを行う組織であるとしています。

- 国家安全保障
- 公共サービス
- 銀行・金融(銀行や証券取引所など)
- IT・通信
- 輸送・物流
- エネルギー・公益事業
- 公衆衛生(病院など)
- その他、サイバーセキュリティ委員会(National Cybersecurity Committee)の定めるもの

重要情報インフラ組織は、サイバー攻撃を防止するため、最低限のサイバーセキュリティスタンダードを維持する義務を負っています。そのため、タイの重要情報インフラ組織と取引を行っている外国企業は、直接的であるか合弁事業を通じてであるかを問わず、サイバーセキュリティを重視する必要があるといえます。

このような重要情報インフラ組織の予防措置の例としては、各組織のサイバーセキュリティの維持のための行動基準及びスタンダードフレームワークの策定(同法 44 条)、役員、運用スタッフ、所有者、コンピューター処理者の氏名、コンピューターシステムを監視する者の氏名をサイバーセキュリティ委員会事務局に通知すること(同法 46 条、52 条)、サイバーセキュリティの最低基準を検証し、サイバーセキュリティの維持に関するリスク評価を実施すること(同法 53 条、54 条)が挙げられます。サイバー攻撃が発生した場合、重要情報インフラ組織は、サイバーセキュリティ委員会事務局及びその監督当局又は規制当局に、当該サイバー攻撃を是正するために遅滞なく通知する責任を負います(同法 57 条)。サイバー攻撃を是正するため、管轄官庁は、関係者に対し、当該場所の所有者の同意を得て居所又は事業所への立入りを行うことや、情報又は文書の提供といった協力を求めるレターを発出する権限を有します(同法 62 条)。上記は現行法に定められた予備的な措置であり、サイバーセキュリティ委員会事務局は、同法 9 条に基づき、追加措置を規定する権限を有します。

✓ 個人情報保護法

2019 年個人データ保護法 4 条最終段落において、個人データ保護法の適用を免除されるデータ管理者は、所定の基準に従って個人データのセキュリティを維持する義務を負うと規定されています。当該基準に基づき、データ管理者は、データの

セキュリティ及び機密性を維持するものとされています。データ管理者は、不正に当該データを他人に開示し、又は当該データの修正を許可してはならず、また、当該データに関係のない者による当該データへのアクセスを防がなければなりません。

2. 最近のタイにおけるサイバー攻撃の事例

サイバーセキュリティに関する意識向上のためのセミナー、従業員のサイバーセキュリティの健全性チェック、フィッシングシミュレーション、組織全体のサイバーセキュリティの健全性評価の策定・実施など、通常、各事業者は独自にサイバーセキュリティ対策を講じていますが、それにもかかわらず、様々なサイバー攻撃に直面する可能性があります。最近の事例としては、2022 年 2 月 18 日にタイで携帯電話サービスを提供する通信会社がハッキングされた事例が挙げられます。これにより、約 10 万人のユーザーの情報がダークウェブ(ハッカーのオンラインコミュニティ)に流出しました。同社は、政府機関であるサイバーセキュリティ委員会及び放送・通信委員会、並びに影響を受けたユーザーに対して、サイバー攻撃について報告を行いました。また、サイバー攻撃後、当該通信会社は、検証を実施し、ソフトウェアやセキュリティシステムの更新を行うよう従業員に指示しました。さらに、当該通信会社は、同社のサービスはサイバー攻撃の影響を受けていないこと、法的手続を開始するために攻撃者及び情報漏洩者について調査していることを公表しました(なお、企業がサイバー攻撃について公表を行う法的義務はありません。)。

3. サイバー攻撃を受けた事業者の権利

事業者が被害・損害を被った場合、かかる事業者は、以下の手続を利用して、サイバー犯罪者を訴追するため、自ら刑事手続を開始し、又は警察官(タイ法において「inquiry official」と呼ばれます。)に対して申立てを行うことができます。

- ✓ 当該サイバー犯罪が発見されて以降の全ての段階について、攻撃を受けたコンピューターの検査報告書又はコンピューターの画面を印刷したものなどを収集した上、証拠として裁判所に提出し、又は警察官に対して提出する。被害を受けた事業者の従業員であって、当該サイバー攻撃に関する事実について知識を有する者は、裁判所又は警察において証言しなければならない。現在、タイの警察では、サイバー攻撃の被害者に対し、法的手続の申立てをオンライン上で行うサービスを提供している。
- ✓ 管轄を有する裁判所及び申立てを受理する権限を有する警察署は、犯罪地を管轄する裁判所及び警察署である。また、サイバー犯罪の専門当局であるテクノロジー犯罪監視局に対して申し立てることもできる。
- ✓ なお、インターネット上の情報は各サービスプロバイダーが管理しており、更なる法的手続を必要とするため、申立てを受理した裁判所及び警察官は、暗号化されたデータを直ちに復号化するなど、サイバー犯罪を直ちに是正することができない場合もある。

4. サイバー攻撃についての報告義務

2019 年サイバーセキュリティ法 58 条に基づき、重要情報インフラ組織のみが、通信システムへのサイバー攻撃又はそのおそれがある場合に政府当局に報告する義務を負っています。したがって、重要情報インフラ組織以外の事業者がサイバー攻撃を受けた場合、当該事業者が政府当局に報告する義務はありません。それにもかかわらず、顧客やユーザー等に影響を与えるサイバー攻撃が発生した場合、事業者は、サイバー攻撃を受けたことを当該顧客やユーザーに知らせ、その後の取引におけるセキュリティを向上させるべきであるといえます。さらに、事業者は、サイバーセキュリティ委員会事務局に対しても報告するのが望ましいといえます。

5. 終わりに

タイで事業を営む本邦企業は、重要インフラ組織との取引がある場合は、サイバーセキュリティについて特に重視する必要があり、また、サイバー攻撃に関する法的手続についてはタイ独自の内容も多いため、サイバー攻撃を受けた場合、サイバー犯罪を専門とする弁護士に助言を求め、速やかに対応することが望ましいといえます。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所　広報室　E-mail