InterRisk Thai Report ＜2022 No.01＞

タイにおけるサイバーリスク

[概要]

- 2021 年にタイでサイバー攻撃を受けたユーザーの割合は約 21% であり、全世界平均の約 29%と比べて低い水準になっているものの、2021 年の損害額は前年と比較して 144%増加しており、220 万ドル（約 7, 260 万バーツ）におよびます。
- サイバー攻撃の手口が多様化しており、海外子会社を踏み台にして本社のシステムに侵入するケースもあります。
- サイバー攻撃の対策のためには役割分担を事前に明確化しておくことと、定期的な訓練が重要です。

近年、コンピュータやネットワークを使用したサイバー攻撃のリスクが顕在化しています。サイバー攻撃には詐欺や ID・パスワードの盗み取りや、不正アクセス等があり、コンピューターウイルスも含まれます。コンピュータシステムがウイルスに感染した場合、ファイルを破損させたり、全体の機能の設定を変更したり、他のデバイスやシステムを自己複製する等の恐れがあります。ウイルスはマルウェアの一種で、悪意のあるソフトウェアにより攻撃者が被害者から情報を盗んだり金銭を得たりするためのツールとして使用されています。近年、急増しているランサムウェアもウイルスの一種であり、このウイルスで攻撃された場合はファイルがロックされてしまうため、ファイルを元に戻すことと引き換えに身代金を要求されるものです。

情報テクノロジーが日々進化を遂げる一方で、サイバー犯罪の問題も日々深刻化しています。セキュリティー対策がサイバー犯罪に追い付いていない傾向にあり、サイバー犯罪発生頻度が増加しています。

世界有数の調査会社 Cybersecurity Ventures は、世界のサイバー犯罪による被害額はこの 5 年間で毎年 15%ずつ増加し、2025 年の年間被害額は 10 兆 5000 億ドルに到達、2015 年と比較して 3 兆ドル増加すると予測しています。これは 1 年間の自然災害による被害額よりも大きい数字になっています。

本稿ではタイにおけるサイバーリスクの事例等をご紹介するとともに、海外拠点における有事の際の対応を「初動」に焦点を当てて説明します。

タイのサイバーリスク

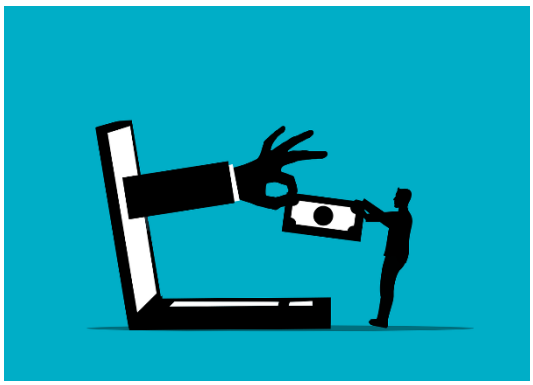
世界的なセキュリティ会社であるKaspersky社の調査をもとに、タイと他国とのサイバーリスク状況を比較すると、2021 年にタイでサイバー攻撃を受けたユーザーの割合は約21% であり、全世界平均の約29% と比べて低い水準になっています。

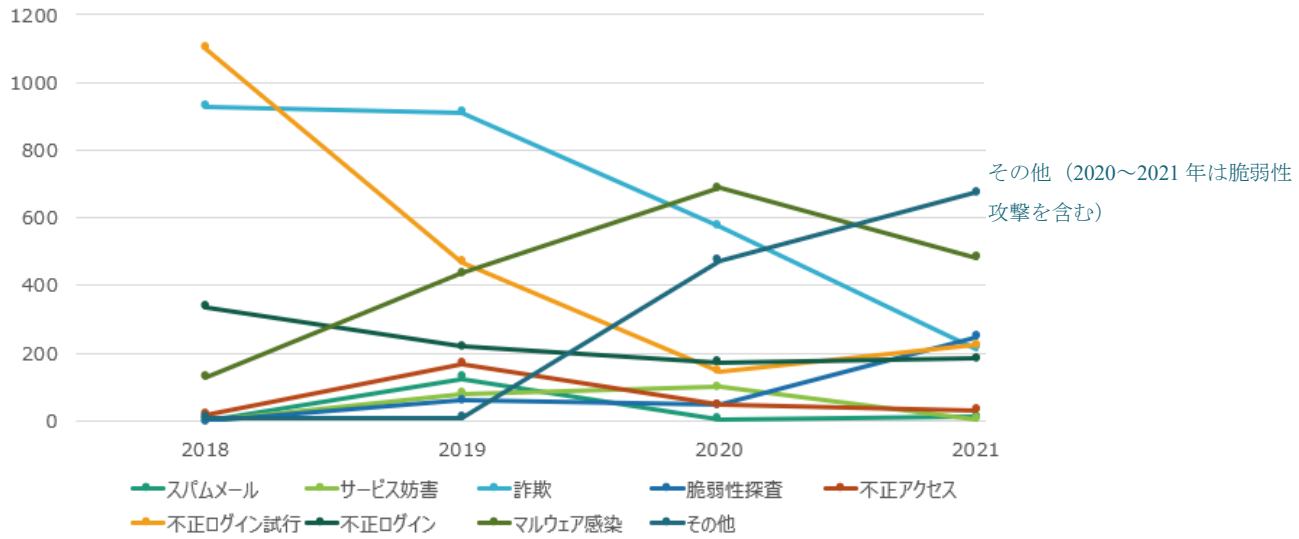
タイ科学技術省が管轄するThaiCERT(Thailand Computer Emergency ResponseTeam) は、サイバー攻撃を下表の9つに分別し、2011 年以降の月次発生件数を公表しています。

表：ThaiCERTが月次発生件数を公表している攻撃の種類

項目	内容
1. スパムメール	誹謗中傷、様々な商品の広告、受信者が希望していない情報（SPAM）等、個人や企業の信頼性を損なう不正なコンテンツを電子メールによって流布する攻撃。
2. サービス妨害	システムに対する攻撃を行い、通常通りに使用できないようにする攻撃。ウェブサービスを稼働しているサーバやネットワーク等に過剰な負荷をかけて（Dos 攻撃 /DDoS 攻撃）直接妨害する場合や、ウェブサービスをサポートする建物や電力系統、空調設備等のインフラを攻撃し間接的に妨害する場合がある。
3. 詐欺	偽の WEB サイトからユーザーの ID やパスワードを盗むフィッシング攻撃、または著作権を侵害する製品やソフトウェアの不正販売等。
4. 脆弱性探査	OS 情報、インストールされているソフトウェア情報、アカウント情報等、システム上で利用可能なサービスを利用して、攻撃者の脆弱性に関する情報を収集しようとする攻撃。システム内の重要な情報を明かすため、ネットワークのトラフィックの情報を収集する（Sniffing）。
5. 不正アクセス	機密情報への不正アクセスや、情報の改ざんを行う攻撃。
6. 不正ログイン試行	認証情報（ID、PW) を取得するために、システムのハッキング、アカウント認証方法の推測、総当たり攻撃等を行う攻撃。
7. 不正ログイン	認証情報（ID、PW）が取得され、不正ログインが成功したケース。
8. マルウェア感染	ユーザーやシステムに望ましくない結果をもたらすプログラムやソフトウェア（ウイルス、ワーム、トロイの木馬、スパイウェア等）によってシステムの誤作動を発生させたり、システムを破壊する攻撃。
9. Other （その他）	上記以外全ての新規や未分類される脅威。上記以外の脅威による被害が増えた場合、攻撃の種類が新たに分類される。

過去４年間の総数は 2,520 件(2018)、 2,470 件(2019)、2,250 件(2020)、2,069 件(2021) と大きく変わりませんが、不正ログインが減少する一方でマルウェア感染と、その他の攻撃（脆弱性攻撃等）の増加が目立ちます。2021 年のサイバー攻撃による損害金額は 144%増加し、220 万ドル（7,260 万バーツ）となっており、法律サービス、建設、卸売と小売、ヘルスケアと不動産業界が多くの被害を受けています。また、タイの被害額は東南アジアで第 6 位となっています。





図：タイにおけるサイバー攻撃件数の推移（過去 4 年）

次にタイで発生した大規模なサイバーインシデントの事例は以下のとおりです。経営に大きな影響を与える深刻なサイバーインシデントが発生しています。

表：タイで近年発生したサイバーインシデントの事例

事件発生日	業種	内容
2016 年 8 月	銀行	ATM がマルウェアに感染し、合計 1,200 万バーツ以上が窃取。犯人は、21 台の ATM から計 300 回以上に渡って毎回 4 万バーツずつ引き出し。
2017 年 7 月	銀行	保証状を発行するオンラインサービスから法人顧客 3,000 社分の社名が流出。他の銀行でも住宅・個人ローン等、小口融資のオンライン不正申請で 12 万人分の口座情報が流出。
2018 年 3 月	通信会社	大手通信会社から 1 万 1,400 人分の顧客情報が流出。
2020 年 5 月	通信会社	タイ最大手の通信会社で 80 億件以上のネット利用記録が流出。同社は「ログはインターネット利用の全体像を示すものであり、顧客の個人情報や機密情報を示すものではない」と釈明。
2020 年 9 月	病院	コンピュータシステムがランサムウェアに感染。システム全体が操作不能となり、医療サービスに支障をきたした。犯人は 20 万ビットコイン（約 630 億バーツ）の身代金を要求。
2021 年 5 月	保険会社	大手保険グループがハッカーグループ「Avaddon」によるサイバー攻撃を受け、顧客の医療報告書（センシティブデータ）、銀行口座のスキャン文書、国民 ID カード情報を含む 3 テラバイトの情報が流出。

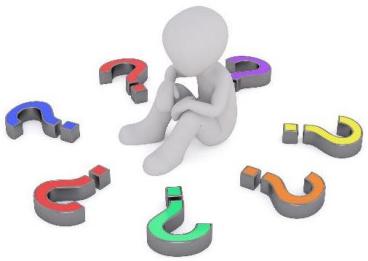
サイバーセキュリティ対策のポイント

タイを含む海外拠点においては、本社と比べてリソース（人・時間・費用等）が限られているため、本社からの全面的な支援が得られる場合等を除き、一般にセキュリティレベルは本社に比べて低い傾向にあります。攻撃者はこうした状況を認識しており、まず海外拠点に侵入し、海外拠点を「踏み台」にして本丸の本社への侵入を試みるケースが見られます。

サイバー攻撃は近年手口が多様化しており、発生時の対応にも柔軟性が求められます。事前に詳細な対応策を持っていても、必ずしもそのとおりに対応できるとは限らず、またインシデント発生後の対応は自社単独で完結することは難しいため、「インシデント発生時にまず何をしないといけないのか」、本社や外部ベンダーとの役割分担を事前に明確にしておくこと（役割を担ってもらうこと）がなにより重要です。このような観点から、本記事では「異常の検知」から「初動対応」に至る過程で、以下の対応策を最低限の準備として整備し、どんなインシデントが発生するか具体例を設定し、定期的に訓練しておくことを推奨します。

～　検知から初動対応まで　～　「気づけるか」、「報告し動きだせるか」

「気づけるか」 （異常の検知）	インシデントの兆候（サイバー攻撃の発生）に素早く気づき、被害を最小化できるか。（平時からの社員教育、訓練を定期的に実施し、実施記録を文書で保持する。）
「報告し動きだせるか」 （初動対応）	**情報共有全般** □サイバー攻撃の第一発見者は誰に相談、報告するか？ ※基本対応は何によって定められているか □誰が責任者としてインシデント事案（またはおそれのある事案）を認識するのか、その後責任者として対応すべきことが明確になっているか？ □監督官庁への報告義務はないか？ ※未報告の際には行政罰が課される等の制約はないか **本社への報告** □本社の報告・連絡先は明確か？ ※マルウェア感染、情報漏洩が確認されたら速やかに本社報告を行う（特に本社とネットワークがつながっている場合には、被害が本社に及ぶ可能性あり急を要する） **封じ込め・原因調査・影響分析** □担当部門・外部ベンダーの連絡先・連携体制・役割分担は明確か？ ※自社および本社では判断・対応が難しい領域も多いため、外部ベンダーとの連携がポイントとなる。特に初動の連絡体制が重要



保険および付帯サービスによる早期復旧への支援

ここではサイバー保険について解説します。インシデントが発生した場合、前述のとおり自社における初動対応が被害最小化の観点においてなにより重要ですが、その対応には緊急性と同時に高度な技術対応も必要となります。海外拠点というリソースが限られた環境の下、自社ですべてを対応できる企業はそう多くないでしょう。常日頃から訓練し、外部ベンダーと速やかに連携をとれる状態にしておくことを強くお勧めします。

サイバー保険に加入している場合、保険会社はサイバーインシデントの専門業者と連携し、速やかに対応を開始し、早期復旧を目指します。また、お客さまがＩＴ業務を委託している外部ベンダーとも積極的に連携することで、事態の早期解決に繋がります。前述の訓練実施に向けた標的型攻撃メール訓練サービス（下図）等を提供している保険会社もあります。

前述のとおりランサムウェア被害に伴う巨額な金銭的負担等、サイバー攻撃の手法が巧妙化し、サイバーリスクは年々高まっています。また直接的な損害に加えて、二次災害、三次災害と拡大するケースも増えており、自社だけではなく取引先、お客様、株主、場合によっては市場や社会へも影響を及ぼしかねません。保険を有効活用することにより、限られたリソースでも緊急性と高度な技術対応をもって事態解決にあたるという選択肢もあるということを知っておくことも重要です。

サイバー保険の主な有効性は大きく分けて以下の 3 点です。

① サイバー攻撃訓練サポート

社員向け標的型攻撃メール訓練実施に向けたツール提供等

② サイバーインシデント発生時の緊急対応サポート

専門業者と連携し、早期システム復旧対応を支援

③ サイバーインシデント復旧費用およびステークホルダー（取引先等）への費用を補償

緊急時対応を行った結果発生した費用や、個人情報漏洩等に伴う個人への賠償や取引先の機密情報漏洩に伴う賠償等

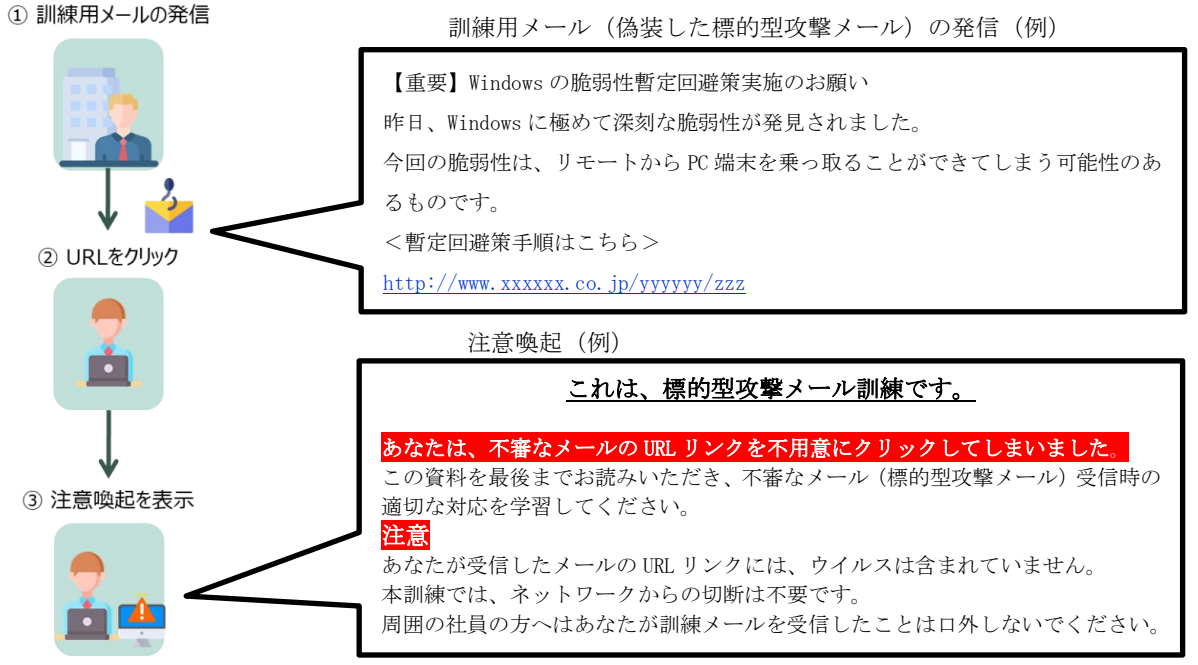


図　標的型メール訓練の例

参照

- https://www.avast.com/c-cybercrime
- https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx
- Kaspersky Security Bulletin Overall Statistics for 2020
- https://www.itday.in.th/kaspersky-reveals-a-30-45-percent-increase-in-web-threats-targeting-thai-users-in-q1-64/
- https://www.newsdirectory3.com/top-5-cyber-threats-to-attack-asean-thai-big-target-and-ransomware-that-hopes-more-than-money/
- https://www.terranovasecurity.com/what-is-ransomware/
- https://www.thairath.co.th/news/tech/2375175
- https://www.trendmicro.com/vinfo/us/security/definition/ransomware

画像の出典

- https://www.pixabay.com/photos/hacker-silhouette-hack-anonymous-3342696/
- https://www.pixabay.com/photos/regulation-gdpr-data-protection-3246979/
- https://www.pixabay.com/illustrations/question-mark-think-question-2318030/
- https://www.pixabay.com/vectors/scam-phishing-fraud-money-6922102/

MS&AD インターリスク総研株式会社は、MS&AD インシュアランスグループに属する、リスクマネジメントに関する調査研究およびコンサルティングを行う専門会社です。タイ進出企業さま向けのコンサルティング・セミナー等についてのお問い合わせ・お申込み等はお近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
MS&AD インターリスク総研（株）　総合管理部　国際業務グループ
TEL.03-5296-8920
https://www.irric.co.jp/

インターリスクアジアタイランドは、タイに設立された MS&AD インシュアランスグループに属するリスクマネジメント会社であり、お客様の工場・倉庫等における火災リスク調査や洪水リスク評価、ならびに交通リスク、サイバーリスク等に関する各種リスクコンサルティングサービスを提供しております。お問い合わせ・お申し込み等は、下記の弊社お問い合わせ先までお気軽にお寄せ下さい。

お問い合わせ先
InterRisk Asia(Thailand) Co., Ltd.
175 Sathorn City Tower. South Sathorn Road.Thungmahamek. Sathorn. Bangkok 10120. Thailand
TEL: +66-(0)-2679-5276
FAX: +66-(0)-2679-5278
https://www.interriskthai.co.th/