2019.03.19

InterRisk Thai Report ＜2019 No.07＞

東南アジアのサイバーリスク

【要旨】
- **東南アジアなどの中進国、発展途上国は多くのサイバー攻撃の対象となっています。**
- **セキュリティレベルの低い海外拠点を踏み台にして本社の情報が狙われるおそれがあります。**

1. 東南アジアのサイバーリスク

Kaspersky 社の 2017 年調査によれば、同社のウイルス対策ソフトを利用しているユーザーの中でウィルスを検知した割合が高い国ワースト 20 は下表の通りです。ワースト 20 のうち東南アジアの国が 5 カ国ランクインしています。また、下図の分布図からアジア、アフリカ、南アメリカといった発展途上国、中進国で多くのユーザーがサイバー攻撃を受けていることが分かります。

表　悪意あるプログラムによる攻撃を受けたユーザーの割合ワースト 20[*1]

順位	国	割合	順位	国	割合
1	ベトナム	67.41%	11	ソマリア	57.78%
2	アフガニスタン	63.03%	12	ネパール	57.60%
3	アルジェリア	61.36%	13	モザンビーク	56.12%
4	ラオス	61.08%	14	リビア	55.85%
5	モンゴル	60.67%	15	カンボジア	55.79%
6	ウズベキスタン	58.86%	16	カザフスタン	54.87%
7	ルワンダ	58.42%	17	スーダン	54.76%
8	イラク	58.39%	18	ミャンマー	54.73%
9	エチオピア	58.35%	19	インドネシア	53.92%
10	バングラデシュ	58.09%	20	モロッコ	53.48%

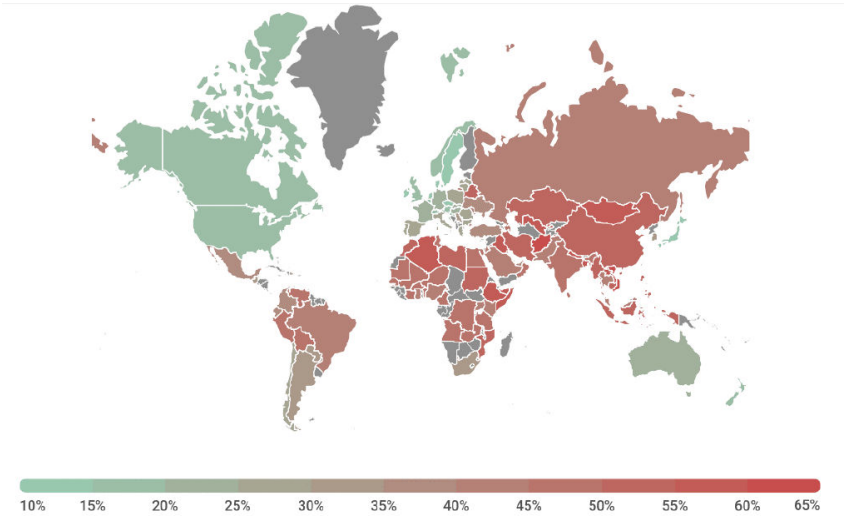


図　悪意あるプログラムによる攻撃を受けたユーザーの割合[*1]

次に、同じく Kaspersky 社が 2017 年に調査した「ランサムウェアによる攻撃を受けたユーザーの割合が高い国」ワースト 10 を下表に示します。最も割合が高い国は日本であり、東南アジアではベトナム、カンボジア、インドネシアがランクインしています。

表　ランサムウェアによる攻撃を受けたユーザーの割合ワースト 10[*1]

順位	国	割合	順位	国	割合
1	日本	2.83%	6	カンボジア	1.53%
2	イタリア	2.37%	7	クロアチア	1.48%
3	ベトナム	1.85%	8	レバノン	1.44%
4	ブルガリア	1.68%	9	ブラジル	1.42%
5	台湾	1.59%	10	インドネシア	1.35%

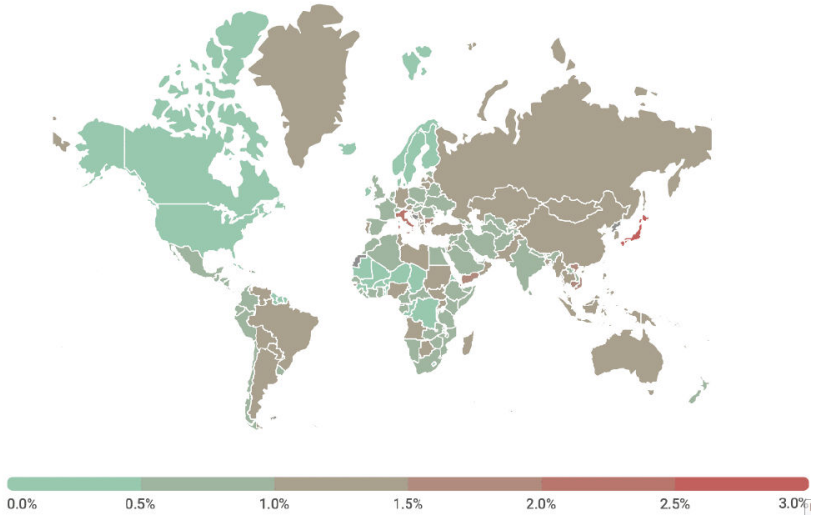


図　ランサムウェアによる攻撃を受けたユーザーの割合[*1]

2. 海外拠点のサイバーリスク

海外拠点ではそれぞれの拠点でイントラネットやメールシステムを構築しているケースが多く、これは国による規制、コスト、通信インフラの整備状況が大きく影響しています。海外拠点と日本の本社のシステムは一般的に様々なネットワークで接続されています。

セキュリティが弱い海外拠点でサイバー攻撃によりネットワークシステムのログイン ID、パスワードが不正に取得され、当該海外拠点のサーバーや端末を踏み台にして本社のシステムに不正アクセスされる可能性があります。海外拠点は、万一この方法で攻撃されて本社に損害を与えた場合、大きな責任を負うことになります。

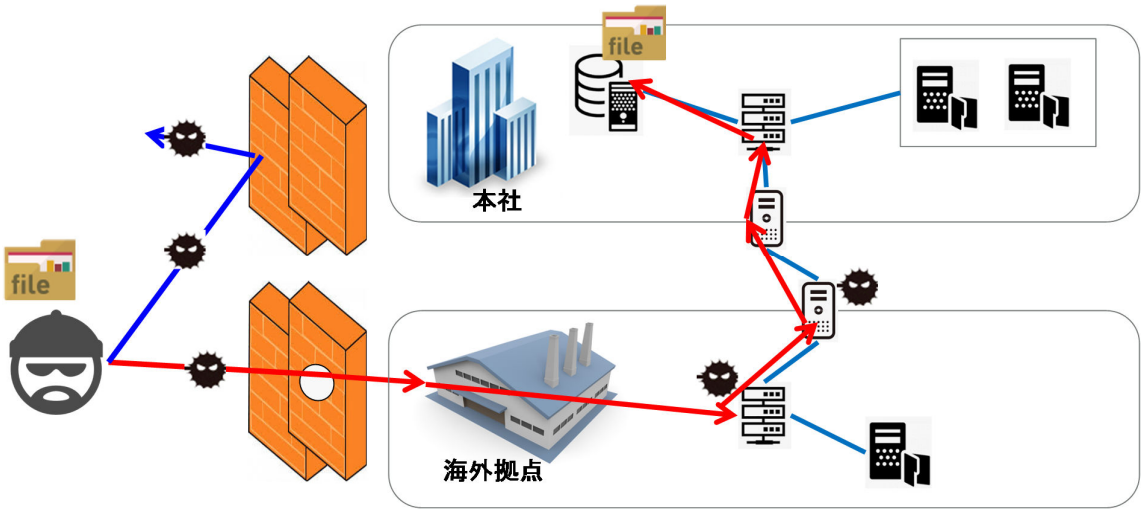


図　海外拠点を踏み台にして本社を攻撃するケース

特に東南アジア等では、各国の通信速度、規制、コストの問題で海外拠点のセキュリティレベルが本社を下回っているケースがあります。攻撃者が本社のデータベースに保存されている情報を狙う際、まず最初にセキュリティレベルの低い海外拠点が攻撃される可能性があります。

表　海外拠点と本社のセキュリティレベル（例）

海外拠点	対象	本社
外部提供サービス	メールシステム	自社システム部門管理
パッチ配信は外部に委託	マルウェア対策(パッチ配信)	自社システム部門管理
外部委託	ネットワーク監視(トラフィック等)	外部委託(365 日 24 時間)
なし	セキュリティ監視	外部委託(365 日 24 時間)
固定(本社と同じ)	ID	固定
強制自動更新	PW 管理	強制自動更新
ルール化→不適合は拒否	PW 強度	ルール化→不適合は拒否
WEB アクセス制限なし	WEB 閲覧	WEB アクセス制限サーバー
アクセス制限なし	データベース	アクセス制限
VPN、端末認識	リモートアクセス	VPN、端末認識

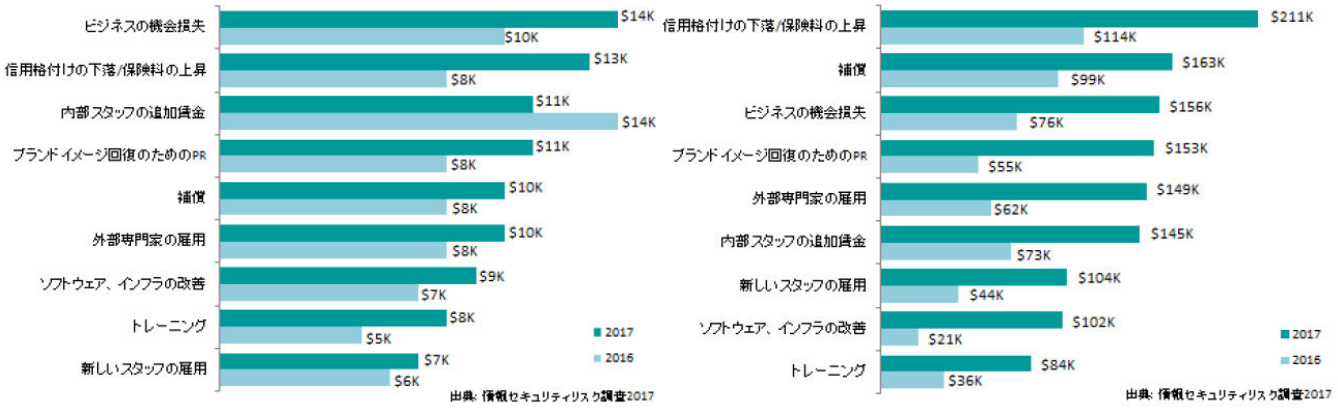
3. 情報漏洩による企業の被害

サイバー攻撃により情報が漏洩した場合、一般的に下表に示す損害が発生します。

表　情報漏洩による企業の損害

損害		概要
賠償責任	損害賠償金	漏洩により損害を与えてしまった人から請求される損害賠償金
	争訴費用	損害賠償に関する争訴費用、弁護士費用など
費用損害	法律相談費用	漏洩後の対応のために弁護士に対して支払う相談費用
	事故対応費用	漏洩後の対応として発生する費用 通信費用　→電話、FAX、郵便（文書作成、封筒代、送付費用など） 社外問合せ対応費用→コールセンター会社への委託費用 人件費→応援人員や残業代など 出張費や宿泊費→事故対応により生じる旅費等 事故原因調査費用→事故調査に要する費用（フォレンジック費用等）
	広告宣伝活動費用	謝罪広告（社告等）や再発防止策等の広報に要する費用
	コンサルティング費用	被害拡大防止策や原因調査、メディア対応、再発防止策の立案実施において外部専門家を起用した場合の費用
	見舞金	漏洩被害者に対して謝罪のために支払う見舞金や送付する見舞品の費用
逸失利益		本来得られるべきであるにもかかわらず、サイバー攻撃による事業中断等により、得られなくなった利益

情報漏洩の際に生じる損害額は大企業と中小企業で傾向が異なります。Kaspersky 社の調査によれば、データ侵害による平均的な財務的影響は、中小企業ではビジネス機会損失、信用格付け低下、スタッフ追加賃金、イメージ回復 PR が上位であるのに対し、大企業は信用格付け低下、補償が上位になっています。また、1 インシデントの財務的影響の平均は中小企業で 92,000 ドル(約 1040 万円)、大企業では 1,300,000 ドル(約 1 億 4700 万円)(1 ドル=113 円)と金額にも大きな差があることが分かります。



データ侵害における平均的な財務的影響（左：中小企業、右：大企業）*2

執筆者：InterRisk Asia (Thailand) Co., Ltd.　佐藤　公紀

参照

*1: Kaspersky Security Bulletin Overall Statistics for 2017

*2: Kaspersky Labo 「日本企業の情報セキュリティ予算の捉え方」

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）　総合企画部　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/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業の CSR 活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製／Copyright MS&AD インターリスク総研株式会社 2019