2022 年 1 月 8 日

Venture Solution

コラム記事

昨今のサイバー攻撃への対応力については、企業間で差が広がりつつあります。
自社だけではなく、関連企業や取引先企業へも影響を及ぼすサイバー攻撃の被害事例も多く報告されているいま、
サイバー攻撃への対応力を高めることが必要になっていると感じております。
そんな中で、サイバーセキュリティ対策が企業信頼度につながり、取引可否につながるとの記事が掲載されておりましたのでご紹介いたします。

サイバー防衛力の格付け広がる　「落第企業」取引停止も

（日経電子版 2022/1/8(土) 20:28 配信 より引用）

■サイバー防衛力の格付け広がる　「落第企業」取引停止も

サイバー攻撃への防衛力を格付けするサービスを導入する企業が増えている。欧米企業が先行し、**日本でも資生堂などがグループ会社のチェックに使い始めた。取引先の状況を検証し、「落第点」なら取引停止を検討する例も出ている。**各社でばらつきのあるサイバー防衛力を客観評価することが重要になっており、信用格付けのように普及する可能性もある。

■脆弱性をチェック

「御社の海外拠点のシステムに重大な脆弱性を発見した。すぐに是正しないと取引は続けられない」。国内の部品製造企業の IT 担当者は 2021 年 10 月、米国の取引先からのメールに驚いた。慌てて調べると、自社で存在すら把握していなかった海外の古いサーバーに、指摘通りの脆弱な点がみつかった。

（日経電子版より引用）

検知に使われたのは、米スタートアップのセキュリティ・スコアカード（SSC）のツールだ。ソフトに頻繁に修正プログラム（パッチ）を当てているかや、サイトが真正かを示す「SSL サーバー証明書」の有無、社内にマルウエア（悪意のあるプログラム）はないかなどをチェックする。その企業の機密が、ハッカーなどが情報交換する闇ウェブ上に流れていないかも分析する。

これらの分析のうえで対策レベルを A～F で格付けする。SSC によると、最低の F 評価を受けた企業のサイバー攻撃の被害リ

スクは、A 評価より 7.8 倍高いという。対象企業の調査協力は必要ないため、気づかないうちに調査されている企業も多い。21 年だけで 1000 万社以上が調査対象になったという。

SSC によると、仏アクサやフィンランドのノキアなどが同ツールを利用。決済サービスの英モジュアは取引先を調べ「低評価なら取引の打ち切りも検討する」としている。

増える身代金を問題視し、米政府は支払いに制限をかけ始めた。米財務省の外国資産管理局（OFAC）は 20 年 10 月、ロシアや北朝鮮、シリアなどとの関係が疑われる組織への支払いが制裁対象になり得ると表明した。とりわけロシアやその周辺国とみられる集団による攻撃が急増しており、何らかの追加措置が取られる可能性がある。

日本も経済産業省が 20 年 12 月に発行した経営者向けの文書で、ランサムウエアについて「金銭の支払いは厳に慎むべきだ」とした。

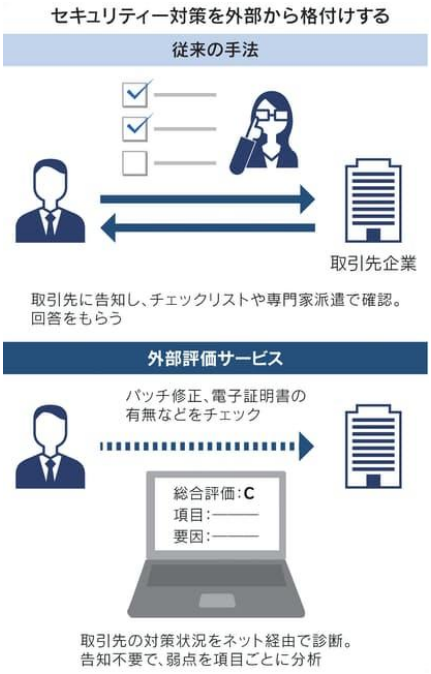
サイバー犯罪者の脅迫行為は違法となる一方、被害企業側の支払いを禁じる法律はない。企業の身代金支払いをすべて禁じるのは容易ではない。米連邦捜査局（FBI）は「ビジネスが機能障害に陥った場合、経営陣があらゆる選択肢を評価することは理解する」と指摘する。

■グループ会社も調査対象

日本では資生堂が、グループ企業のチェックなどに利用。トヨタ自動車など完成車や部品のメーカーでつくる「Japan Automotive ISAC（J-Auto-ISAC）」は 21 年 8 月以降、約 70 ある加盟社の診断に使った。中島一樹サポートセンター長は「今後も定期的に実施し、業界全体の防衛力底上げを図る」と話す。東京海上日動はサイバー保険を引き受ける際の保険料の算定に使う。

サイバー防衛力の「格付け」には、老舗の信用格付け会社も関心を強める。21 年 4 月には米フィッチ・レーティングスが SSC への出資を表明。米ムーディーズ・インベスターズ・サービスは 9 月、別のサイバー評価大手の米ビットサイト・テクノロジーズに 2 億 5000 万ドル（約 290 億円）を出資して業務提携すると発表した。

従来は取引先のセキュリティ対策を評価する手法として、チェックリストに記入してもらうなどの自己申告型が主流だった。ただ、こうした「性善説」に基づく調査は信頼性が乏しいとされる。デロイトトーマツグループの佐藤功陛パートナーは「日本企業はグループ内ですら海外拠点の方が、力関係が上になりがち。外部の供給網全体の状態を把握するのは困難だ」と指摘する。



（日経電子版より引用）

■信用格付け並みの普及予測も

海外拠点や供給網を通じたサイバー被害は後を絶たない。21 年には、日産自動車の北米子会社で、アプリ開発ツールなどのソフトウエアの設計図にあたる「ソースコード」がネット上に流出。米アップルの「MacBook（マックブック）」の設計図とみられるデータが、台湾メーカーへのサイバー攻撃を通じて盗まれてネット上で公開されたと報じられた。取引先のセキュリティを客観的に評価する重要性が高まっている。

SOMPO リスクマネジメント（東京・新宿）の熱海徹上席フェローは「米国では合併や買収を検討する企業の調査にも使われ始め、サイバー対策の格付けが成約を左右する状況だ」と話す。

米調査会社のガートナーはセキュリティー評価サービスについて、ビジネス関係のリスクを評価する際に「22 年中に既存の企業の信用格付けと同じレベルまで重要になる」と予測している。

（サイバーセキュリティーエディター　岩沢明信）

日本では海外企業との取引が多い企業も多く存在しています。
日本国内であれば、セキュリティ対策をどれほど講じているのかが取引基準になることは多くないと
言われておりますが、海外企業が対象となれば別問題だと考えております。
世界各国の先進国は日本と比較してもサイバーセキュリティ対策に重きを置いている企業も多いと言われており、
取引をする以上、対象の国のレベルに合わせていくことが喫緊の課題となると感じております。
日本レベルではなく、世界レベルでのセキュリティ対策を取っていくためにも、新しい情報を常に取り入れていく
必要があると考えています。