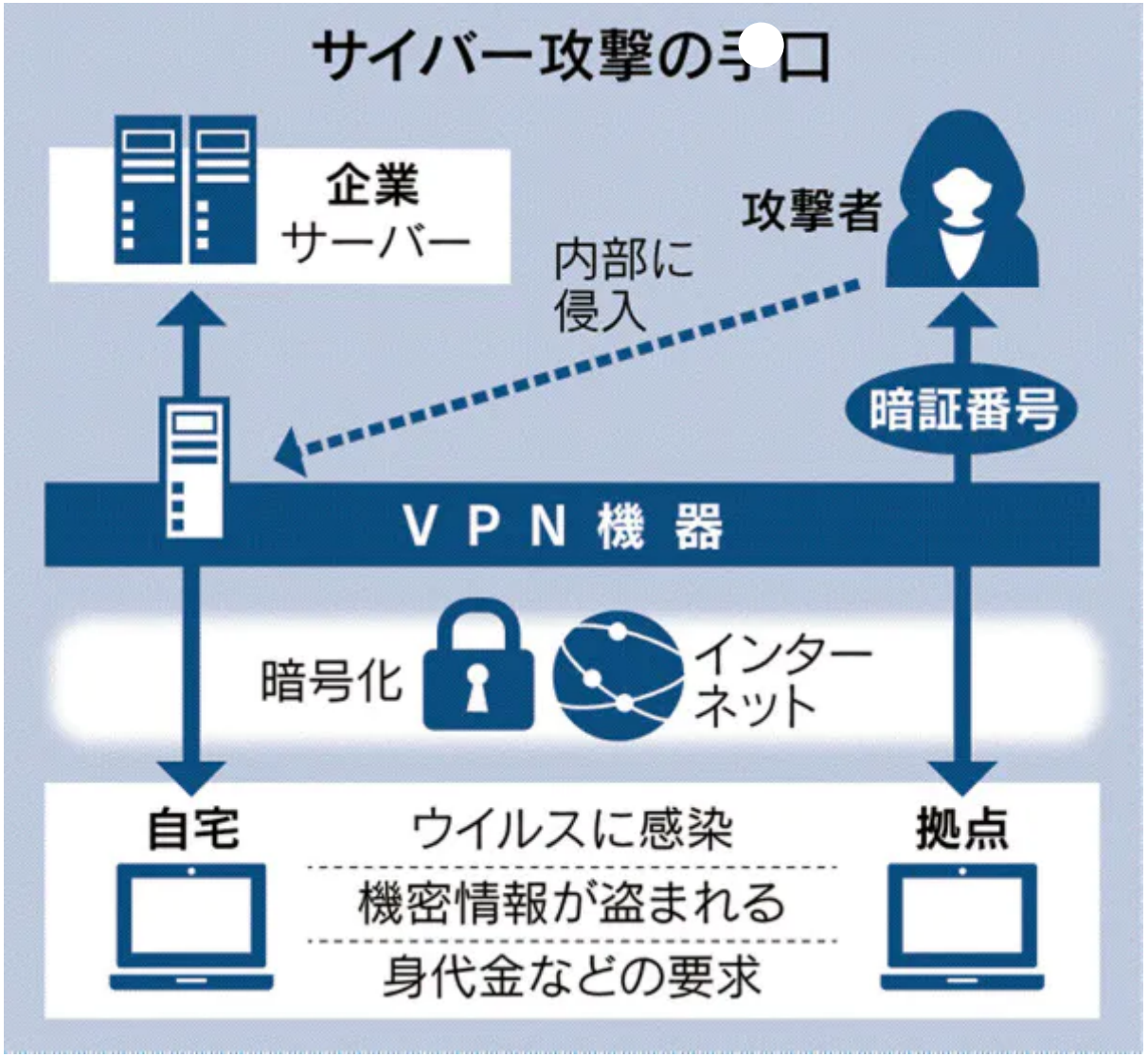
日本経済新聞

テレワーク、VPN暗証番号流出　国内38社に不正接続

2020/8/24 20:00 (2020/8/25 5:33更新) | 日本経済新聞　電子版



日立化成や住友林業など国内の38社が不正アクセスを受け、テレワークに欠かせない社外接続の暗証番号が流出した恐れがあることが分かった。第三者が機密情報を抜き取ったり、ウイルスをばらまいたりする2次被害が予想される。事態を重く見た内閣サイバーセキュリティセンター（NISC）も調査に乗り出しており、企業は対策が急務となっている。

【関連記事】
VPN脆弱性、修正遅れ突く 「ゼロトラスト」不可欠
ウェブ会議「私だけ遅い」　社内の怪奇現象の正体

新型コロナウイルスの流行で、日本企業の大半が本社と社員の自宅をつなぐテレワーク対応を迫られている。今回流出が判明した中には、こうした在宅勤務を推進する企業も多く含まれている。ソフトや機器の更新を怠っていたとみられる例も散見され、リモート時代の情報リスクが改めて浮き彫りになった形だ。

漏洩したのは、VPN（仮想私設網）と呼ばれる接続サービスの利用情報だ。VPNは通信データを暗号化し、社外から業務システムに接続する際などに使う。実際の専用線を敷設するより導入コストが安いため、多くの企業が社員の在宅勤務などに役立てている。

NISCによると、8月中旬に犯罪サイト上で、世界900社超のVPN情報がやり取りされていることを確認。詳細を調べたところ、このうち38社は日本企業だったことが分かった。

日本経済新聞が入手した被害企業リストには、日立化成や住友林業、ゼンショーホールディングス、オンキヨーの名前が挙がっている。医薬品製造の全薬工業、エネルギー関連の岩谷産業、電力機器のダイヘン、自動車総連も含まれていた。

ロシア語を使うハッカーが各社に不正アクセスして情報を入手したとみられる。VPNを使う際のユーザー名やパスワード、ネット上の住所を示すIPアドレスが流通していた可能性がある。

悪意ある第三者に情報が渡れば、VPNを伝って各社の基幹システムへの侵入が可能となる。各社は「社員情報の流出などの被害は確認していない」（住友林業）と口をそろえる。だが特別な対策を取らないと、社員を装って社内情報を盗み見したり、内部からサイバー攻撃を仕

掛けたりできる状態だという。

今回情報が流出した企業は、米専門企業パルスセキュアのVPNサービスを使っていた。パルスセキュアは世界で2万社以上の顧客を持つ業界大手だが、同社のVPNを巡っては2019年4月に自ら脆弱性についての情報を公表。修正プログラムも公開していた。

日本でも民間団体JPCERTコーディネーションセンターが注意を喚起していた。しかし必要な対策を取っていない企業が多く残っており、情報漏洩の危険性が問題視されていた。一部企業は安全性に問題があるままVPNを使い続けていたもようで、ハッカーはこの弱点を突いて情報を盗み取ったとみられる。

今後は38社を「踏み台」にして各社の取引先などへ不正アクセスを試みる動きも予想される。サイバーセキュリティー会社サイファーマ（東京・千代田）の山田正弘氏は「IDや暗証番号だけでなく、2要素認証などを導入し、監視を強化することが重要だ」と話す。

被害企業の多くは「当該装置は停止した」（日立化成）「必要な対応を取った」（全薬工業）とする。社員ごとにアクセス制限を設けるなど追加対策も欠かせない。

新型コロナの感染拡大を受け、企業はテレワークの体制拡充を急いでいる。NISCは緊急事態宣言が発令された4月以降、企業の安全対策の遅れが目立つと指摘。「混乱に乗じたサイバー攻撃の兆候がみられる」と警鐘を鳴らしていた。