脱IT初心者「社長の疑問・用語解説」（第65回）

闇のお悩み「ダークウェブ」

2023.05.24

ビジネスにIT活用が欠かせないことは理解しているつもりだが、次から次へと登場する難解なIT用語がよく分からない。そんなIT初心者の社長にも理解できるようにITキーワードを解説する本連載。今回は、万一、会社の機密情報が公開されたら信用が失墜し、お先真っ暗になりかねない「ダークウェブ」だ。

「社長、ダークウェブで同業の機密情報が売買されているようです。うちも何か対策を考えましょう」（総務兼IT担当者）

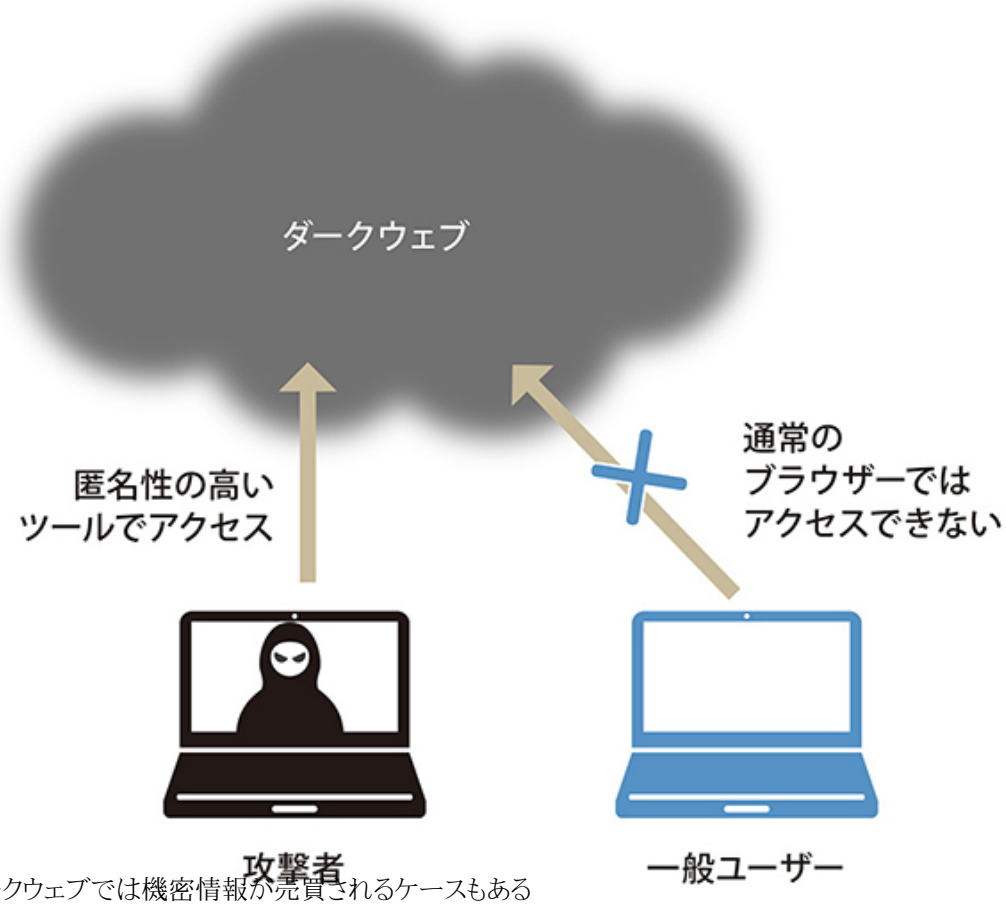
「ダーク……。宇宙映画の新作でもやるのか。見に行きたいな」（社長）

「暗黒面があるのは似ていますが、映画とはまったく関係ありません。ダークウェブは闇のウェブサイトのことで、違法な取引にも使われているんです」

「もしかしてワシのダークな情報が漏れているんじゃないだろうな。すぐに対策を考えなさい」

盗まれた顧客情報などが闇取引の温床に

ダークウェブはインターネットの住所であるIPアドレスを隠した闇サイトで、Microsoft EdgeやGoogle Chromeなどの一般的なウェブブラウザーからはアクセスできません。匿名性が高く、アクセス元の特定が困難なことから、違法ドラッグなどの闇取引の温床になったり、攻撃者が盗み取った企業の機密情報やクレジットカード番号などの個人情報が売買されたりするなど実被害も広がっています。ランサムウエア感染や不正アクセスなどによって顧客データなどの機密情報が流出すると、ダークウェブで売買されるケースもあります。中小企業も早急にセキュリティ対策を強化しなければなりません。



ダークウェブでは機密情報が売買されるケースもある

Q ダークウェブを悪用されると何が起こるのでしょうか

攻撃者が盗み取った企業の機密情報を売買目的にダークウェブに掲載すると、別の攻撃者が機密情報を買い取り、再び企業を攻撃するといったように被害が広がる恐れもあります。違法な売買は仮想通貨で決済されるので犯罪者を見つけにくいと言われます。

Q ダークウェブの悪用手口を教えてください

攻撃者が企業のデータを暗号化して身代金を要求するランサムウエアの感染被害が広がっています。近年は「二重の脅迫」の手口が知られ、第一の脅迫である身代金の支払いに応じなかった場合、第二の脅迫として、盗み取った機密情報をウェブに公開すると脅すものです。その公開先として、ダークウェブのリークサイトが悪用される事例があります。

Q ダークウェブの被害を防ぐにはどうすればいいですか

興味本位でダークウェブのサイトにアクセスしないことです。攻撃者に身元を突き止められて従業員の個人情報や会社のメールアドレスなどが悪用される恐れがあります。また、ダークウェブに情報を公開されないよう、ランサムウエアや標的型攻撃などから企業の情報を守るセキュリティ対策を強化します。セキュリティ対策に不備がないかを最新動向に詳しいITサービス事業者に相談するといいでしょう。

お先真っ暗にならないために対策が必須

「社長、ダークウェブがどんなものか、分かっていただけましたか」（総務兼IT担当者）

「ダークウェブが危ないサイトであるのは何となく分かった。ワシの闇が公開されたら、それこそお先真っ暗になりかねんな」（社長）

「えっ、社長に隠しておきたい闇なんてあるんですか。まさか、こっそりためたヘソクリなんて言わないでくださいね」

「そう、ヘソクリなんじゃが、会社の情報と違ってセキュリティ対策で守れないことが一番な闇（悩み）だ」