機先を制し機密情報の漏えいを未然に阻止するダークウェブの調査

情報漏えいやフィッシングサイトによる詐欺行為といったセキュリティ上の脅威に、企業は先手を打って対処することはできないのだろうか。そうしたニーズに応えるものが、富士通が提供する「ダークウェブ調査サービス」だ。最新のテクノロジーと、セキュリティに関する高度なスキルと知見を備えた人材が一体となり、企業に様々な被害をもたらす「脅威情報」をいち早く発見、対処に繋げることを支援している。

攻撃ツールや盗まれた機密情報が闇取引されるダークウェブ

近年、サイバーセキュリティに対する意識の向上とともに、「ダークウェブ」という言葉が広く耳目を集めるようになってきた。一般にダークウェブと言えば、「サイバー犯罪者によって窃取された機密情報が売買される、サイバー犯罪の温床」というイメージを抱く人も多いと思われるが、そもそも、ダークウェブとは、どのようなインターネット空間を指すのか。

現状のインターネットは大きく「クリアウェブ（サーフェイスウェブ）」と「ディープウェブ」の領域に二分されると言われている（図1）。クリアウェブとは、一般的なウェブブラウザを用い、一般的な検索エンジンで調べて、不特定多数の人々が情報を探して到達できるインターネット空間を指す。公開されている企業や個人のウェブサイト、SNSなどがその代表例だ。

一方、ディープウェブとは、通常の検索エンジンではたどり着けないようなインターネット空間であり、ID/パスワードでアクセスが制限された企業の社内サイトなどがその一例となる。そのディープウェブ内の一部であり、アクセスに専用のツールやブラウザが必要なウェブサイトがダークウェブと呼ばれている。

ダークウェブは匿名性が高く、情報の発信者やアクセスする人も特定が難しいと言われている。本来、ダークウェブは高度なセキュリティ技術により、個人情報を秘匿しながら機密情報をやり取りするために開発されたものだ。だが、その性質上、サイバー攻撃や犯罪の温床と

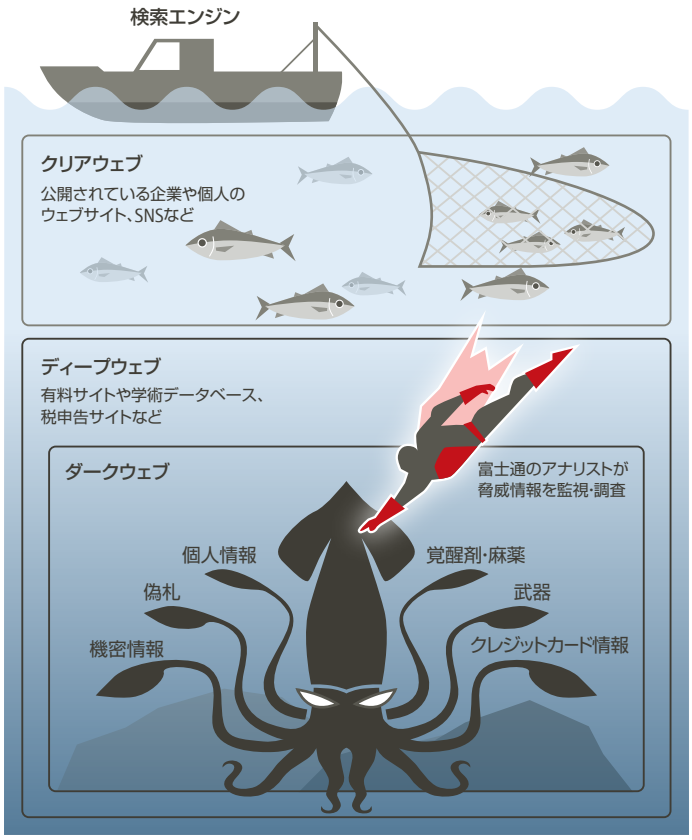


図1 インターネットの2つの領域とダークウェブのイメージ

なっているのも実情である。

実際、ダークウェブ上では、ありとあらゆる違法な取引が行われている。偽造パスポートをはじめ、偽札や盗難品、時には軍事兵器の売買さえやり取りされることもある。

また、サイバー攻撃の観点から着目すると、ハッキングツールや世に公開される前の脆弱性情報をはじめ、企業の社内サイトに侵入するためのID/パスワード情報や、多種多様な機密情報も存在している。さらに、盗まれた個人情報も数多く売買されており、実際の企業における個人メールアドレスはもとより、氏名、生年月日、住所やセキュリティコードまでを含めたクレジットカード情報の販売も確認されている。そうした個人情報は販売用のサンプルとして、一部のデータにマスクをかけた状態で公開されているケースも多い。

特に最近では、標的型ランサムウェア攻撃に遭遇した企業の機密情報が公開されていることが、多数報告されている。

このほかにも、サイバー攻撃に際して共犯者を募集するような書き込みも行われている。いわゆるショッピングサイトや掲示板、フォーラムなどをイメージすれば分かりやすいだろう。

高度な知見で脅威情報を探し出す「ダークウェブ調査サービス」

サイバー攻撃によるセキュリティインシデントを防ぐためには、自社にとって脅威となる情報がダークウェブ上にも存在していないか、定期的に調査を行うことが必須となる。攻撃者が攻撃を行う際に利用するIDやパスワード、個人情報といった機密情報、フィッシング詐欺での利用が疑われる、自社と類似したドメイン名を有したウェブサイト、または自社の名前やブランド名を無断利用したウェブサイトやSNSアカウントなどが例として挙げられるだろう。そうした自社にとって脅威となりかねない情報をいち早く見つけ出すことでサイバー攻撃の予兆を捉え、被害が生じる前に適切な防御策を講じることが可能になる。

だが、先に述べたように一般的な検索エンジンやツールでダークウェブにアクセスすることは難しく、また、機密情報がやり取りされるページも摘発を逃れるため、頻繁に変更される。そうしたことから、自社にとって脅威となる情報がダークウェブ上でやり取りされているかどうかを調べ出すのは多くの労苦を強いられる。クリアウェブも含めた膨大な情報の中から「本当にセキュリティリスクとなるものはどれなのか」正しく分析するのは至難の業だ。また、脅威になりそうな情報を見つけ出せたとしても「どう対処していいか分からない」という声も少なくない。そもそも、社内にダークウェブの調査が可能なスキルを有した人員を確保したり、維持したりするのが困難であるのも実情ではないか。

そうした課題に応えるものが、富士通の「サイバー脅威プロアクティブ分析 ダークウェブ調査サービス」(以下、ダークウェブ調査サービス)である。これは、富士通のセキュリティマイスターがクリアウェブからダークウェブまでを網羅した継続的な監視と脅威情報の抽出を行うとともに、情報流出の事実や攻撃の予兆などがないか、調査・報告することで、攻撃者の狙いや侵入経路などを想定した事前/ピンポイントの防御強化を支援するものだ。

すなわち、サイバー攻撃者がターゲットとする企業へと侵入するための事前調査を行う「偵察」、および、入手した機密情報を用いて効果的な攻撃を仕掛けるためのツールを作成する「武器化」といった脅威に対応する、多層防御の初期段階をカバーするサービスとも言える。

効果的な調査キーワード設定をはじめ脅威の度合いに応じた対策も提言

それでは、ダークウェブ調査サービスの特長と、もたらされるメリットについて説明していこう。

具体的なサービス提供の流れであるが、はじめに調査方針を策定した上で調査キーワードを設定し、クリアウェブからダークウェブまでに至るインターネット上から脅威情報を収集。さらに、富士通の高度なセキュリティに関する知見を有したアナリストが「発見された脅威情報が、自社にとってどの程度の脅威となるものなのか」調査・分析を行ったのちに、結果をとりまとめ報告書として提供する(図2)。

インターネット上にある膨大なデータの中から、脅威情報を効果的に収集するためには適切な調査キーワードの設定が不可欠となる。それに対して富士通は、豊富な知見とノウハウに基づいたキーワードの選定が可能だ。例えば、金融機関であれば、フィッシングサイトの存在を危惧されているケースが多い。そこで、似たようなドメイン名が登録されていた場合はその疑いが高いため、調査キーワードにドメイン名を設定する。同様に商品のブランド名などでも、関連性の高いドメイン名が

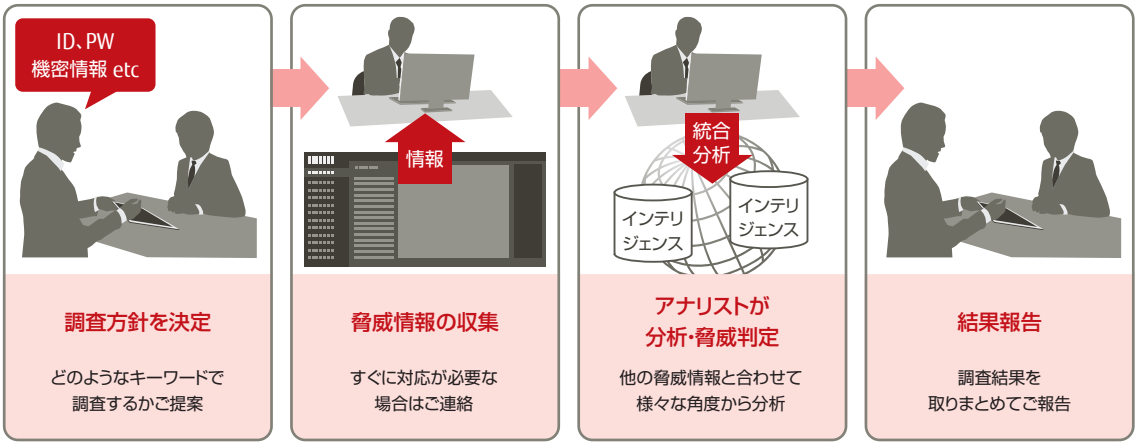


図2 ダークウェブ調査サービスのフロー

取得されている可能性があるのでそれらを調査キーワードに設定する。これらはほんの一例であり、それぞれの企業の要望や状況に応じて、効果的な調査キーワードの提案、策定を行っている。

続く脅威情報の収集については、イスラエルのセキュリティに関する新鋭企業、IntSights社との協働による、AI（人工知能）を用いた広範囲な調査の実施に加え、富士通のアナリストによる深堀も行っている。例えば、「どのような場所に、どういった脅威情報が存在しているのか」をアナリストは、日常的に監視している。そこから特定のフォーラムでやり取りされている内容に着目し、探りを入れていくことも少なくない。また、サイバー犯罪が行われている可能性が高いフォーラムが突然閉鎖されることもあるが、ダークウェブでは、どこからともなく同様のフォーラムが新たに出現することが往々にしてある。それをいかに早く見つけ出すかが肝要となるが、アナリストは他のコミュニティでの話題もウォッチしながら足取りを追っていくなど、様々な手立てを駆使して対処にあたっている。

そして、AIなどを駆使し、広範囲かつ深部にまで至るキーワードに関連する調査を行った結果、脅威情報が抽出されるが、その中には脅威度が低いものも少なからず存在する。前述したIntSights社でも脅威分析を実施し、脅威度の低いものはふるいにかけられ、さらに、高度なセキュリティ分析を行う富士通の専門機関「A3L（エーキューブラボ）:FUJITSU Advanced Artifact Analysis Laboratory」が調査結果に対して、企業にとってどの程度その情報が脅威となるのか分析を行う（図3）。そして、脅威の度合いに応じてスコア付けを行い、優先的に対応が必要な情報であることが分かる形でレポートを提出する。なお、誤情報なども「脅威に該当しない」、または「脅威が低い」ものとして報告する。

これにより、現状の把握に加え、危険度の高いものから優先的に対処することが可能となる。脅威のスコア付けは、「早急な対処が必要」「対処することが望ましい」「対処は不要だが経過観察が必要」「脅威なし」の4段階に分類。例えば、「迅速な対処が必要」なものには、「社員のID/パスワードが平文のままで漏えいしているのが発見された」などが挙げられる。このほかにも、発売される前の新製品の名称が確認された場合にも、脅威情報としてすぐに対処しなければならないだろう。

なお、脅威の源となる、機密情報の漏えいが発生していた場合には、漏えい元となった可能性のあるシステムや部門にヒアリングを実施、もしマルウェア感染によって発生していたのならフォレンジックなどの対処を施す。また、従業員による情報の持ち出しが疑われる場合は、ユーザー行動監視/監査ツールの導入など、ソリューションを導入するといった手立てが必要となる。このほか、ID/パスワードの漏えいが確認されたのであれば、認証システムの見直しや強化を行わなければならない。

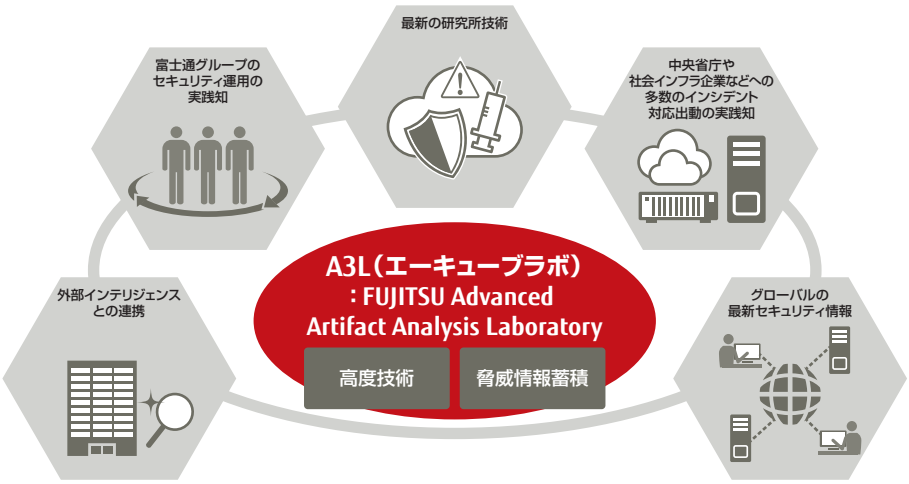
そうした脅威への対策立案・提案、導入についても、富士通はサポート可能だ。さらに、その場限りのスポット的な対処だけでなく、脅威に対する富士通の多彩なセキュリティソリューションを活用した恒久的な対策案の提示もできる。

高度な技術をもつセキュリティ人材と全方位のソリューション提供が強み

このような数々の優位性をもつダークウェブ調査サービスを支えているのが、セキュリティに関する高い知見と数多くの実績を積み重ねてきた富士通のアナリストの存在だ。アナリスト達は日常的に脅威に関する情報の収集、分析に努めているだけでなく、日進月歩のセキュリティ技術に対応するため、日々、自らのスキルや知識の研鑽を重ねている。

セキュリティに関する豊富な人材を擁していることに加え、エンドポイント対策からクラウドサービス管理に至る「ゼロトラストネットワーク」をトータルでサポートできることも大きな強みだ。さらに長年にわたり富士通が培ってきた、あらゆる業種業界におけるシステム構築・運用の知見を活かした、業種特化型のセキュリティ提案も行える。

冒頭でも述べたように、効果的な情報漏えい対策を実施するためには、攻撃者に先んじて防御策を講じることが不可欠だ。そのための有効な施策の1つとなるのが、ダークウェブ調査サービスであり、富士通では「お試し調査サービス」も提供しているので、ぜひ、その有効性を実際に確認して頂きたい。



※A3L:FUJITSU Advanced Artifact Analysis Laboratoryの略称であり高度なセキュリティ分析を行う専門機関

図3 A3Lで最新の脅威情報や研究技術を収集・解析してサービスに反映し、運用サービスの品質向上につなげる

お問い合わせ先
富士通コンタクトライン（総合窓口）　0120-933-200
受付時間 9:00～12:00および13:00～17:30（土曜・日曜・祝日・当社指定の休業日を除く）
富士通株式会社
https://www.fujitsu.com/jp/solutions/business-technology/security/secure/cyber-security/darkweb-research/