# ダークウェブ上から脅威情報を調査するサービス

## Service for Investigating Threat Information from Dark Web

河本　聡　　川原　勝広

**あらまし**

特殊なブラウザなどを使用しなければアクセスできないダークウェブでは，犯罪組織が違法な売買を目的として利用しているケースがある。そのため，ダークウェブ上でやり取りされている自組織の情報を把握し，脅威を未然もしくは早期に対処することが重要である。しかし，専門の調査官でない要員がダークウェブにアクセスして，調査することは技術的・心理的観点で困難である。このような状況を受け，富士通ではダークウェブを含むインターネット上から漏えいした機密情報，偽アカウント，攻撃の兆候などをお客様に代わって調査するFUJITSU Security Solution 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の提供を開始した。本サービスの特長は，ダークウェブを含むインターネットの深い階層までを調査対象とし，発見した脅威についてサイバーセキュリティ専門のアナリストが分析し，被害の発生可能性をスコア付けする点である。

本稿では，本サービスの背景，特長，調査実施の流れ，および検出できる内容について述べる。

**Abstract**

The dark web, which is inaccessible without using special browsers or other means, is used by criminal syndicates in some cases for the purpose of illegal trading. For that reason, it is important for organizations to keep tabs on their own information exchanged on the dark web to deal with any threat proactively or quickly. However, accessing and investigating the dark web is technically and psychologically difficult for personnel who are not specialist investigators. Given these circumstances, Fujitsu has started offering FUJITSU Security Solution Cyber Threat Proactive Analysis Dark Web Investigation Service, which investigates confidential information leaks, fake accounts, and signs of attacks over the Internet, including from the dark web, in place of customers. A feature of this service is that it examines deep layers of the Internet, including the dark web, and any threats detected are analyzed by analysts specialized in cyber security. These threats are then given scores to indicate the likelihood of damage. This paper presents the background and features of this service, the implemented investigation process, and what can be detected.

## 1. まえがき

デジタルテクノロジーの進化によって「つながるサービス」が次々に生み出され，社会のデジタル化が加速している。一方で，サイバー攻撃の脅威の数と種類が増え，その手口も複雑化・巧妙化してきている。

インターネット上には膨大なコンテンツが存在し，検索エンジンを活用することで必要な情報にたどり着ける。しかし，インターネットは以下の三つの領域で構成されており，その中には通常たどり着けない領域も存在する。

(1) クリアウェブ (表層ウェブ)

企業の公開サイトや個人サイトなど，誰でも閲覧できる領域である。

(2) ディープウェブ

検索エンジンでは見つけられない領域である。例えば，ID・パスワード（以下，アクセス情報）でアクセス制限されているサイトや，社内ネットワーク上のサイトが該当する。

(3) ダークウェブ

通常のブラウザではアクセスできない領域である。専用ソフトを利用してアクセスする。

昨今，ダークウェブを温床としたサイバー攻撃や犯罪が増加している。ダークウェブは，元々は個人情報や機密情報を高いセキュリティでやり取りするために開発されたものであり，特殊なブラウザなどを使用しなければアクセスできない。そのため，ダークウェブ上でやり取りされている自組織の情報を把握し，脅威を未然もしくは早期に対処することが重要である。しかし，専門の調査官でない要員がダークウェブにアクセスして，調査することは技術的・心理的観点で困難である。

そこで富士通は，上述の領域でお客様の情報が漏えいしていないか，またお客様のICT環境を攻撃する兆候がないかを調査するFUJITSU Security Solution 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の提供を開始した。

本稿では，本サービス提供の背景，調査の効果的な進め方，および検出できる内容について述べる。

## 2. 背景と現状の課題

ダークウェブは，犯罪組織が違法な売買を目的として利用しているケースもあり，サイバー攻撃に関するやり取りも数多く存在する。例えば，大量のマシンから一つのサービスに多量のリクエストやトラフィックを送り付けるDDoS（Distributed Denial of Service）攻撃を実行するサービスは，1時間あたり平均36～62ドルで売買されている。また，サーバへリモートアクセスするためのアクセス情報が60ドル以下で売買されている。[(1)] 自組織のサーバへのログイン情報が売買されているということは，サーバにログインされて情報を盗まれる被害者と，自組織のサーバから攻撃をしかけてしまう加害者の二つの側面が発生する。

また，社会に浸透したソーシャルメディアでは，フェイクアカウント（偽アカウント）やフェイクコンテンツがニュースで取り上げられるようになってきた。Facebookは，2018年1月から3月の四半期で5億8,300万件の偽アカウントを停止したと発表している。[(2)] クリアウェブであっても，ソーシャルメディア上で企業の公式アカウントを装う偽アカウントを作成された場合，自組織のブランド価値の棄損，あるいはお客様の金銭的被害といった影響が考えられる。しかし，ユーザーアカウント数が億を超える複数のソーシャルメディアサイトから，自組織の偽アカウントを見つけ出すことは容易ではない。

## 3. サービスの進め方

本サービスは，まず組織名やブランド名，役員などの重要人物の名前に加えて，e-mailアドレス，ドメイン名など特定の組織に特化したキーワードをダークウェブ自動巡回プログラムに登録する。そして，ダークウェブを含むインターネットを自動巡回するプログラムがリスクにつながる情報を収集し，これらのキーワードとの突き合わせを行う。

本章では，本サービスの実施内容と進め方について説明する（図-1）。

(1) 調査方針の決定

お客様の要望を確認し，何を重点的に調査するか

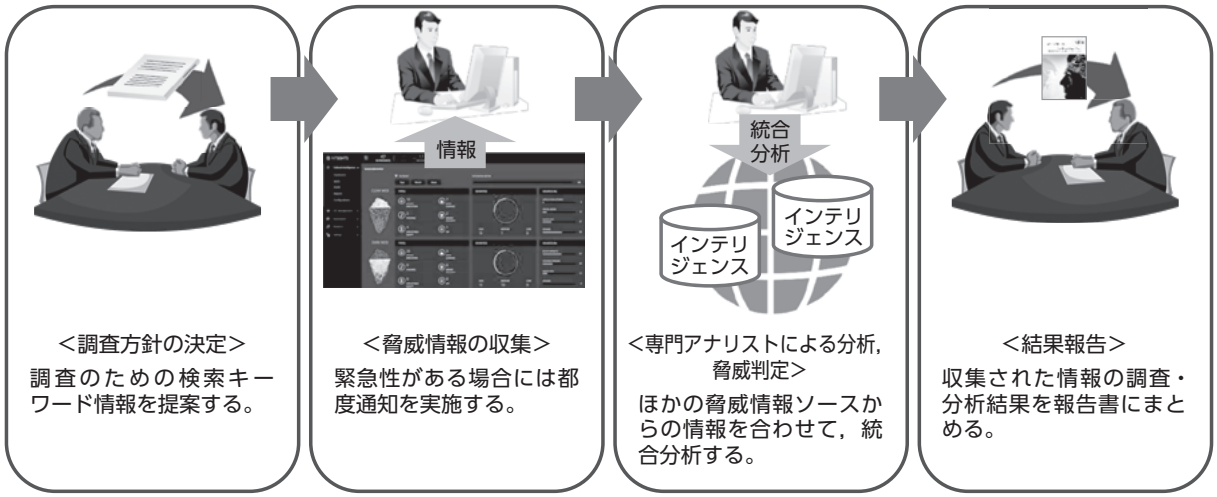


図-1　ダークウェブ調査サービスフロー

について意識合わせをする。その後，調査に必要なキーワードやブランド名・ドメイン名，所有IPアドレス，役員情報をお預かりする。お客様が知りたい情報を収集するためには，適切なキーワードの選定が重要となるが，抽象的なキーワードを登録するだけでは多くのノイズを含んでしまう。富士通は，ノイズを減らしながらお客様の希望する情報を収集するためのキーワード選定ノウハウを有しており，そのノウハウを基にキーワードを選定する。

### (2) 脅威情報の収集

誰でもアクセスできるクリアウェブにある情報だけでなく，ディープウェブやダークウェブにある情報の調査も実施する。イスラエルのサイバー脅威インテリジェンス企業であるIntSights Cyber Intelligence Ltd.と協業し,[3] 広範囲な情報の短時間収集，情報の精度・マッチング率の向上を実現している。

### (3) 専門アナリストによる分析，脅威判定

富士通は，セキュリティに関する情報を集約・分析するFUJITSU Advanced Artifact Analysis Laboratory（A3L）を設立した。A3Lではセキュリティインシデントの分析やマルウェアを解析し，複数の脅威情報（Cyber Threat Intelligence）を活用して新たな攻撃に対応している。A3Lに所属するOSINT（Open Source Intelligence）分析専門セキュリティアナリストが，それらの解析・分析ノウハウを基にインターネットを自動巡回するプログラムが検出した内容を精査し，誤情報を排除する。また，検出内容を精査する中で，お客様の対処の優先順位付けに役立つように，各検出事象について独自に脅威による被害の発生可能性をスコア付けする。そのため，お客様は精度の高い情報を基に現状の把握と対策の立案を行うことができる。

脅威のスコア付けは0～3の4段階あり，スコア3は既に直接的な被害が発生している，もしくは今後発生する可能性が高い事象である。スコア2は，直接的な被害の発生は確認されていないものの，今後発生する可能性がある事象である。スコア1は，直接的な被害発生が低い事象，スコア0は脅威のない事象としている。例えば，従業員のパスワードを含むログイン情報が発見された場合には，スコア3である。

### (4) 結果報告

調査分析結果は，報告用の脅威情報レポートとしてまとめる。脅威スコアが高い項目については，どのように対処すべきかのアドバイスも実施する。

以上が本サービスの進め方であるが，サービスの利用期間は，半年以上と設定させていただいている。本サービスは，2か月目以降は脅威スコアの高い事象を検出した場合には，速報としてすぐにお客様にお伝えすることでアクセス情報の漏えいなどへの対応に役立っている。また継続調査を行うことにより，機密情報の漏えい，ソーシャルメディアの偽アカウント，攻撃の兆候といった事象を迅速に検

出・通知できるため，早期の対処に効果がある。なお，本サービスを1か月程度で実施する短期調査サービスも提供している。

## 4. 脅威の検知事例

本サービスでは，ダークウェブを含むインターネット上の様々な脅威を検知できる。本章では，その事例を紹介する。

### (1) 今後攻撃される可能性がある脅威やリスク

攻撃予告のターゲットリストに掲載されている従業員情報や，所有サーバにリモートアクセスするためのアクセス情報が販売されているといったことを検知する。それらの動向を基にして，自組織のどこがターゲットとされているか，またどのような攻撃が来る可能性があるかを推測することができ，防衛策の検討・適用に役立つ。

### (2) フィッシング詐欺や偽サイトに利用される危険性のあるドメイン名

例えば第三者が正規ドメインである「fujitsu.com」の類似ドメイン「fujitus.com」（sとuの順番を入れ替えている）を取得しているとする。この場合，ドメインの登録者やそのサイトのWebコンテンツが正規ドメインのもののコピーになっていないかといった情報からフィッシングサイトかどうか判断する。一般ユーザがフィッシングサイトにアクセスすると，マルウェアの感染やアクセス情報の搾取といった被害が想定される。暫定的な対処として，自社の社員が誤ってフィッシングサイトへアクセスしないよう社内のプロキシサーバでフィッシングサイトへのアクセスをブロックすることが考えられる。また，根本的な対処としては法的機関への相談や一般社団法人JPCERTコーディネーションセンターへ相談することが考えられる。

### (3) 自社Webサーバ，端末，ソフトウェアの設定ミス

自社Webサーバの設定ミスによって，ディレクトリ内のファイル一覧情報の表示が可能となっている事象や，Cookieの設定に関する問題点を検出する。また，DNSサーバでAXFR転送（全てのゾーン情報を同期）がアクセス制限なしに可能な設定になっている場合も検出する。

このほかにも，自社のサーバにおいて使用しているソフトウェアが古く，脆弱性が残存している場合にも検出する。

### (4) 機密文書，メールアドレス，アクセス情報などの漏えい

誰でもアクセスできるサイトに「関係社外秘」や「Confidential」といった文字の入った自組織のドキュメントが存在する場合に検出する。また，システムへログインするためのIDとパスワードが漏えいしている場合に検出する。更に，ダークウェブで売買されているクレジットカード番号の情報についても検出を行う。

### (5) ソーシャルメディアの偽アカウント，偽モバイルアプリ，商標やロゴの無断利用，不買運動

自組織の名前を利用した不審なソーシャルメディアアカウントを検出することができる。また，自組織の名前が入った不審なモバイルアプリがアプリケーションストアで配布されているケースも検出できる。このようなアプリにマルウェアが仕込まれていると，モバイル端末の盗聴，情報流出，ブランドイメージの棄損につながる。

### (6) 役員に対する脅威やリスク

ソーシャルメディア上で自組織の役員への誹謗中傷や犯行予告を検出する。また，役員へのなりすましも検出する。近年，役員の偽アカウントが第三者によってソーシャルメディアに作成され，偽りの投稿をするケースなどが広く発生している。一般の人からは，そのアカウントが本物か偽物か区別がつきにくく，投稿内容によっては役員本人や企業の信用を失うこととなる。

## 5. むすび

本稿では，FUJITSU Security Solution 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の背景，調査の効果的な進め方，および本サービスで検出できる脅威の事例について述べた。富士通は，これまで蓄積したサービス提供実績，SEノウハウ，A3Lの分析力を活かし，お客様のICT運用への対応を取っていくとともに，脅威への対処方法を継続的に提案していきたい。

## 参考文献

(1) Deloitte：Black-market ecosystem.
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf
(2) Facebookニュースルーム：規定違反に対する措置件数を初公表.
https://ja.newsroom.fb.com/news/2018/05/enforcement-numbers/
(3) 富士通：多様化するサイバー攻撃への包括的な対策を目的に、「グローバルマネージドセキュリティサービス」を大幅強化.
http://pr.fujitsu.com/jp/news/2018/05/9.html

## 著者紹介

**河本　聡**（かわもと　さとし）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティ関連のオファリング業務に従事。

**川原　勝広**（かわはら　かつひろ）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティ関連のサービス企画開発に従事。