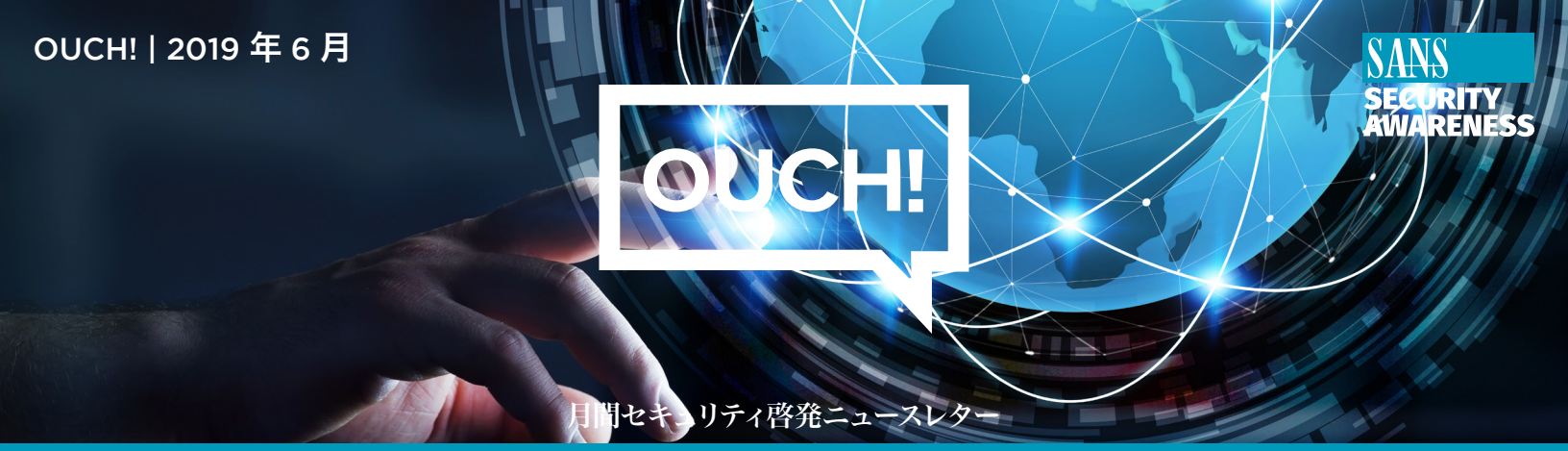

ダークウェブ

はじめに

他人やメディアが「ダークウェブ」という言葉を使っているのを聞いて、「ダークウェブとは何か」あるいは「ダークウェブについて何かやるべきことがあるのか」と考えたことがあるかもしれません。今回は、ダークウェブとは何か、あなたにとってダークウェブはどのような意味があるのかについて説明します。

ダークウェブとは何か？

ダークウェブは、セキュアな状態かつ匿名で通信を行ったり、情報を共有したりするために設計されたインターネット上の複数のシステムから構成されています。そのため、一つのダークウェブというものはなく、特定の1組織によって運営されるFacebookのようなものとは異なります。むしろダークウェブは、別々の人が管理する個々のシステムやネットワークの集合体であり、その用途も様々です。これらのシステムはインターネットに接続されており、インターネットの一部を構成していますが、多くの場合一般的な検索エンジンからは探すことができません。これらのサイトを探したりアクセスしたりするには、あなたのコンピュータに特別なソフトウェアをインストールする必要があります。一つの例として、Tor Projectというものがあり、Tor Browserをダウンロードしてインストールしなければなりません。Tor Browserを介してウェブサーバにアクセスすると、あなたの暗号化されたトラフィックが、Torを使用している他のコンピュータ内を流れます。これらのコンピュータ間を移動する際に、発信元IPアドレスが変更されます。つまり、ウェブサイトに到達する時に、あなたのオンラインでの活動が匿名化されるということです。ダークウェブには他にも、Zeronet、Freenet、I2Pといったものがあります。

誰がダークウェブを使うのか？

ダークウェブにおいてはサイバー犯罪者が主な住人です。彼らはダークウェブ上で、ドラッグの購入や、ハッキングによって搾取した数ギガバイトに及ぶデータの販売を目的として、ウェブサイトやフォーラムを運営しています。こうした活動は全て匿名かつセキュアな状態で行われます。例えば、サイバー犯罪者が銀行やオンラインショッピングサイトをハッキングする際、彼らは可能な限り多くの情報を窃取し、盗んだ情報をダークウェブ上にサイトを持つ他のサイバー犯罪者に売ります。

一方、ダークウェブの利用者には、正当な理由を持つ者もいます。例えば、検閲が厳しい国の人々は、自身のプライバシーを守り、匿名性を保ったまま、ダークウェブのネットワークを使って情報を共有したり、世界で何が起きているのかを確認したりすることができます。ジャーナリストや不正を告発しようとする者、プライバシーを真剣に考

えている人たちは、匿名性を高め、検閲を回避するためにダークウェブを利用できるのです。またこのような人たちは、Tor Browserのようなテクノロジーを、ダークウェブにアクセスするためだけでなく、匿名で通常のインターネットを閲覧するために使っています。

何をするべきか？

ダークウェブにアクセスする特段の理由が無い限り、ダークウェブの利用はお勧めしません。いくつかのダークウェブ上のサイトは犯罪目的で利用されており、その多くは目的達成のため、ピアネットワーク内にあるあなたのコンピュータを利用します。また場合によっては、あなたのコンピュータが綿密に調査されたり、攻撃を受けたりする可能性があります。複数の企業は、あなたの名前や他の個人情報がサイバー犯罪者に窃取され、ダークウェブ上で公開されていることを通知してくれる監視サービスを提供しています。しかしこうしたサービスの真の価値には疑問が残ります。あなた自身を守る最善の方法は、あなたの個人情報が既にダークウェブ上にあり、サイバー犯罪者に利用されていると仮定して行動することです。そのため、次に挙げる対策を取ることをお勧めします。

- **公的機関を騙り、罰金の支払いなどの行動を直ちに取るよう迫る電話やメールを警戒しましょう。犯罪者はさらに、どこかで入手したあなたに関する情報を使って、個人を標的とした攻撃を展開してくる可能性があります。**
- **自分のクレジットカードと銀行口座における取引を監視しましょう。取引の発生を毎日通知するよう設定しても良いかもしれません。そうすることで、金融詐欺の発生を検知することができます。もし実際に検知したら、すぐにその事実をクレジットカード会社や銀行に連絡しましょう。**
- **クレジットフリーズ*を実施し、クレジットスコアへのアクセスを制限しましょう。クレジットフリーズはクレジットカードの利用に影響を及ぼすものではなく、個人情報の窃取からあなた自身を守るために取れる最も効果的な手段の一つです。（米国の場合）**
- ***訳注：米国において、カードの利用や支払い状況などを点数化したクレジットスコアは、ローンや住宅借り上げ時に参考にされるが、スコアに対する照会を一時的に停止し、意図しないカードの新規作成やローン契約を防ぐ仕組み。Equifaxによる個人情報流出事件を契機に、近年利用者が増えてきている。**

ゲストエディタ

ミカ・ホフマン氏（@WebBreacher）は、Spotlight Infosec LLCの主任研究員であり、SANS OSINTコースの講師および著者です。彼のサイバーセキュリティやオープン・ソース・インテリジェンスに対する情熱は、彼のプロジェクトや教材、教育スタイルに表れています。

リソース

個人を標的とした詐欺:	https://www.sans.org/u/RfW
ソーシャルエンジニアリングについて:	https://www.sans.org/u/Rg1
Identity Theft:	https://www.identitytheft.gov
クレジットフリーズ:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser:	https://www.torproject.org/
SANS OSINT Course:	https://sans.org/sec487

 Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田　剛