ダークウェブから考えるサイバーセキュリティ

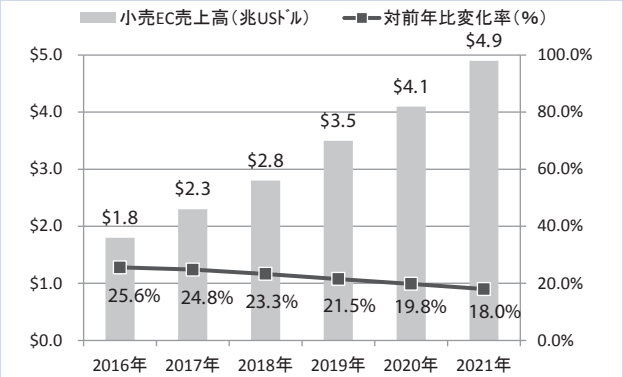
調査研究本部　主任研究員　**柏村 祐**(かしわむら たすく)

電子商取引市場の拡大

経済産業省の公表した調査によれば、世界の電子商取引市場が拡大している。

2017年世界のBtoC電子商取引市場規模は2兆3,000億ドルである。2021年まで対前年2桁成長が見込まれている(資料1)。

資料1　世界のB to C電子商取引市場規模の推移



(出所)経済産業省「平成29年度我が国におけるデータ駆動型社会に関わる基盤整備(電子商取引に関する市場調査)」

2017年の世界各国の電子商取引市場規模を見ると、日本を除いた各国が対前年比10%以上拡大しているのに対し、日本の市場規模は世界4位となっているものの、成長率は非常に低くなっている。

中国は対前年比35.1%、インドは対前年比42.1%と急激に成長している。特にインドの市場規模は現状では2.2兆円と小さく今後も成長が見込まれている(資料2)。

資料2　世界の各国別B to C電子商取引市場規模 (2017年)

ランキング	国名	市場規模(億米ドル)	日本円換算(110円換算)	対前年比
1	中国	11,153	122.6兆円	35.1%
2	米国	4,549	50兆円	16.3%
3	英国	1,126	12.3兆円	17.1%
4	日本	953	10.4兆円	6.0%
5	ドイツ	651	7.1兆円	11.3%
6	韓国	563	6.1兆円	20.9%
7	フランス	488	5.3兆円	16.9%
8	カナダ	340	3.7兆円	29.9%
9	オーストラリア	215	2.3兆円	12.3%
10	インド	209	2.2兆円	42.1%

(出所)資料1と同じ

ダークウェブの世界

我々が見ている電子商取引市場は氷山の一角に過ぎない。普段見えているサイトはサーフェス(表層)ウェブであり、企業などのデータベースや個人のSNS、メールはディープ(深層)ウェブと言われている。

そして、その先にあるのが検索サイト経由でアクセスできないダークウェブ*1である(資料3)。

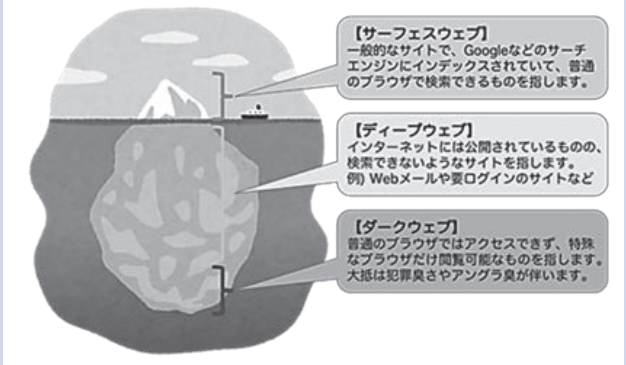
ダークウェブにアクセスするためには、ザ・オニオン・ルーター(以下Tor*2)と呼ばれる匿名化ソフトを通さなければならない。また、ダークウェブでは、すべての通信は暗号化され、場所を追跡できなくなっており、取引においては仮想通貨しか使用できないことが特徴である。

もともとアメリカの研究所で政府通信の保護を目的として開発されたTorは、当初、人権団体やジャーナリストがプライバシー保護のツールとして利用していた。

一方で、匿名性が確保されたダークウェブに目を付けた犯罪組織が、薬物や武器、クレジットカード番号やパスポートなどの売買に使用している。

2018年5月17日には、米サイバーセキュリティー企業が、「日本人の個人情報を集めたとみられる2億件以上のデータが、匿名性の高いダークウェブ上で販売されているのが見つかった」と発表している。データには氏名、住所、生年月日、携帯電話番号が含まれていたというから驚

資料3　ダークウェブの位置づけ



(出所)Qiitaより

きである。

合法の電子商取引市場が拡大するのと同時に、ダークウェブにおける違法な電子商取引市場も拡大しているのである。

ダークウェブへの対策

ダークウェブの脅威は違法取引に留まらない。匿名性という優位性を武器に、ダークウェブからのサイバー攻撃が拡大し続けている。

国立研究開発法人情報通信研究機構で実施した調査結果では、観測されたサイバー攻撃関連通信は、2005年当初は1IPアドレス当たり年間19,066パケットであったが、2018年には1IPアドレス当たり年間789,876パケットと増加し、約30倍もの規模に拡大している(資料4)。

観測された主なサイバー攻撃の対象は、WEBカメラやルータ等のIoT機器だったことが判明している。サイバー攻撃が成功した場合、WEBカメラは乗っ取られ、ネットに接続された電子機器は乗っ取られる危険性がある。

最近ではダークウェブ対策として、脅威インテリジェンスサービスが注目されている。脅威インテリジェンスサービスとは、ダークウェブなどの情報を収集または分析し、顧客企業と関連性がある脅威情報を配信するものである。

従来の一般的なセキュリティ対策は、システムに侵入されないために、ファイアウォールやウイルス対策ソフトを導入することに留まっていた。

脅威インテリジェンスサービスは、あえてダークウェブの世界に入り込み、諜報活動をして事前に脅威となる情報を先回りして感知する。

イスラエルに拠点がある脅威インテリジェンスサービスを展開する企業のCEOによれば、「オリンピックが開催される日本では、今後ダークウェブからのサイバー攻撃は増加すると見ている。」とのことであった。

オリンピック・パラリンピックの開催までの期間は既に400日を切っており、関連する企業や地方自治体は、リスクを正確に認識し、セキュリティを強化することが求められている。

資料4　ダークネット観測統計

年	年間 総観測ﾊﾟｹｯﾄ数	観測 IPｱﾄﾞﾚｽ数	1IPｱﾄﾞﾚｽ当りの年間 総観測ﾊﾟｹｯﾄ数
2005	約3.1億	約1.6万	19.066
2006	約8.1億	約10万	17.231
2007	約19.9億	約10万	19.118
2008	約22.9億	約12万	22.710
2009	約35.7億	約12万	36.190
2010	約56.5億	約12万	50.128
2011	約45.4億	約12万	40.654
2012	約77.8億	約19万	53.085
2013	約128.8億	約21万	63.655
2014	約256.6億	約24万	115.323
2015	約545.1億	約28万	213.523
2016	約1,281億	約30万	469.104
2017	約1,504億	約30万	559.125
2018	約2,121億	約30万	789,876

(出所)NICTER 観測レポート2018 より

おわりに

米国防総省は2011年7月に初の「サイバー戦略」を公表し、サイバー空間を陸、海、空、宇宙空間に次ぐ第5の新たな戦場と宣言している。米政府は関連施設のネットワークが攻撃を受けた場合、軍事報復を行う可能性を排除していない。

「サイバー戦略」が発表されてから約8年経った今、残念ながらサイバー攻撃の状況は右肩上がりに増えているのが実態である。つまり、サイバー攻撃の一翼を担っているダークウェブは、案外身近な所にあるカオスなのである。

ネット社会を生きる我々は、ダークウェブの脅威を把握し、必要な対策を講じていくことが必要ではないだろうか。

【注釈】
*1　ダークウェブはダークネットに存在するWorld Wide Webコンテンツ
*2　Torとは、TCP/IPにおける接続経路の匿名化を実現するための規格、及びそのリファレンス実装であるソフトウェアの名称