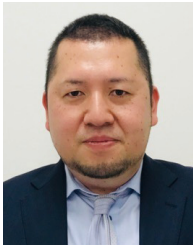
特集
Special Feature

［最新のデジタル・フォレンジック事情］

6 盗まれた個人情報の市場価値
～デジタル・フォレンジックに携わる現場より

応用



松本　隆　（株）ディー・エヌ・エー

盗まれた個人情報の「その後」

東京商工リサーチが独自に集計し，今年の 1 月に公開した「上場企業の個人情報漏えい・紛失事故」調査（2020 年版）によると，2020 年に上場企業とその子会社で，個人情報の漏えい・紛失事故を公表したのは 88 社，事故件数は 103 社，個人情報の漏えいは 2,515 万 47 人分だった．この数字はプレスリリースやお知らせなど，流出元となった企業の自主的な開示情報を発表日ベースで集計したものである．そもそも企業が事故を起こしたことに気付いていなかったり，閉じられた関係者の中で処理されたケースも考えると，実際の数字はこれ以上である可能性が高い．情報漏えい・紛失事故の原因は「ウイルス感染・不正アクセス」等の，いわゆるサイバー攻撃が全体の約 5 割を占めている．また，1 事故当たりの情報漏えい・紛失件数の平均は，紙媒体が中心の「紛失・誤廃棄」の 7 万 4,768 件に比べ，サイバー攻撃による被害は 57 万 8,714 件と突出して大きい．大量の顧客データベースの中身をダンプ（データをファイルに書き出して保存すること）し，丸ごと抜きとるようなサイバー攻撃の被害が，従来のアナログな事故に比べきわめて深刻であることが，改めてデータで示される形となった．

サイバー攻撃などによって，組織から違法な手段で盗まれた個人情報は，さまざまな場所で取引される．ダークウェブに存在するマーケットプレイス（以下ダークマーケット）や個人情報オークション，犯罪系コミュニティ，SNS，コミュニケーションアプリ……たとえば 2020 年 11 月に発覚した Peatix のインシデントでは，個人情報を売買するサイトに Peatix のデータが商品として追加されたことがきっかけで，情報漏えいの事実が明らかになった．最初にサイトに商品が売りに出されてから，わずか 2 日間で，盗まれたデータは Instagram のストーリー機能や Telegram のチャネルで個別に取引され，会員制のロシア語のハッキングフォーラムや有名な英語のフォーラム等にまで拡散していった．

盗まれた個人情報は，データブローカーやコミュニティの共有者を通じて，多様な犯罪者コミュニティに拡散されていく．筆者はデジタル・フォレンジック調査の中で，サイバー犯罪者が攻撃にかけるコストに注目し，数ある情報共有プラットフォームの中から，個人情報を売買するダークマーケットの調査を行った．盗まれた個人情報が，成熟しつつある犯罪者の市場でどのような価値を付けているのかについて共有したい．

盗まれた個人情報の価値

ダークマーケットで販売されている個人情報は多岐にわたる．個人情報と聞くと，情報漏えいのニュースで取り上げられることの多い住民基本台帳の 4 情報（氏名／住所／性別／生年月日）や，特定の

個人を識別するマイナンバーのような個人識別符号を想像する読者が多いだろう．しかし，昨今のダークマーケットでは，4 情報のような「特定の個人を識別する情報」はほとんど流通していない．よほどの有名人の情報でもない限り需要がないからだ．

たとえばあるダークマーケットでは，ミシガン州の市民の個人情報が販売されている．基本の氏名／住所／性別／生年月日のほかに，SSN（社会保障番号）／携帯電話番号／メールアドレスといった情報が付加され，1 件あたり＄5 で取引される．このミシガン州のデータのように，特定の個人にかかわる情報をとりまとめたデータを，Fullz（Fullzinfo：フルズ）と呼ぶ．この Fullz が昨今のダークマーケットで売買される個人情報の基準となる．あるベンダは，運転免許証の両面スキャン単体を＄41 で販売しているが，別のベンダは，Fullz に運転免許証の表面／裏面のスキャン画像を付加して，＄100 で販売している．ダークマーケットでは，個人情報がとりまとめられた Fullz よりも，運転免許証のスキャンデータの価値のほうが高く，さらに Fullz に紐づけられた運転免許証は，Fullz と免許証データの単純な合計金額の 2 倍以上の価値を付けている計算になる．

これら商品の値付けから，ダークマーケットの利用者にとって対価を支払う価値のある個人情報は，より深く「特定の個人になりすますための情報」だということが見えてくる．市場が Fullz 単体よりも運転免許証データ方が高い価値を付けたのは，具体的な悪用のしやすさにあると考えられえる．ダークマーケットで商品を購入する犯罪者は，入手したデータを活用し，自分の非合法なビジネスや活動の目的を達するために購入するのであって，個人的な趣味で集めているわけではない．3 つの事例の中で最も高い価値を付けた Fullz と運転免許証のスキャンの組合せでは，多くの非対面サービスで，他人になりすましたアカウントの新規開設が可能になるだろう．そこで自分のビジネスを展開して回収する目論見があるからこそ，犯罪者は先行して投資をする．

個人情報を購入する犯罪者の目的が，銀行や暗号資産交換業者の他人名義の口座開設であった場合，金融機関による KYC（Know Your Customer：サービス利用のための身元確認）プロセスによって，なりすましを検出されるリスクが残る．犯罪者側の観点では，可能であれば手持ちのデータで金融機関の KYC を通し，なりすましアカウントを自ら開設，管理したい．悪用する際の，不正送金やマネーロンダリングの運用の幅が広がるからだ．しかし，他人になりすますため入念に準備したところで，口座開設時の不正発覚リスクをゼロにすることはできない．

金融機関の KYC に伴う不正発覚リスクを嫌う犯罪者のために，別のベンダは「マルタに本拠地を置く暗号資産交換業者」の身元確認済みアカウントを＄185 で販売している．アカウントは，ID ／パスワード／認証用メールアドレス／ 2 要素認証用の SMS アクセスがセットとなっている．ダークマーケットでの金融資産情報の売買は，一般的に他人の口座の残高をアカウントごと販売するケースが主流だ．しかし，ベンダの説明によるとこのアカウントの残高は 0 だという．これは，他人名義の身元確認済み口座を提供することに意味があるということを示している．ダークマーケットにおいて，ベンダは購入者に対し，単に仕入れた商品をそのまま販売するのではなく，暗号資産の不正送金やマネーロンダリング等の，具体的な悪用方法まで提案していると考えられる．

盗まれたクレジットカード情報

盗まれたクレジットカード情報は，ダークマーケットの定番商品でもある．マーケットは世情を強く反映しており，Gemini Advisory による Gemini Annual Report 2020 では，COVID-19 がクレジットカードの不正利用にも大きな影響を与えていると解説している．興味深いので紹介すると，3 月の世

界的な COVID-19 ロックダウン制限以降，CNP（Card Not Present：オンラインでのクレカ不正利用）が右肩上がりに増加している一方で，CP（Card Present：POS（Point of sale system）や ATM など偽造／スキミングによる不正利用）が激減する結果となった．巣ごもり需要によってオンラインでのクレカ不正決済が増加したが，不正利用者も COVID-19 感染リスクを嫌い，偽造カードを手に外出する機会が激減しているのだという．

昨今のダークマーケットでは，氏名／住所／性別／生年月日の 4 情報に値が付きにくくなったのと同様に，クレジットカードの基本情報（カード会員番号／名義／有効期限／セキュリティコード）のみの価値が減少する傾向にある．カード会社や代理店側での不正決済対応が進み，カードの情報だけでは悪用時の不正発覚リスクが高くなっているためだ．

そこで，ベンダは Fullz とクレジットカード情報のセットを販売することで，決済時にカード名義人になりすまし，カード会社やオンラインショップのセキュリティを突破する手段を提供している．なお，Fullz という呼称は広義には個人情報に紐づくクレジットカード情報等をとりまとめたものを指す場合があるが，今回リサーチ対象としたダークマーケットおよびベンダは，それぞれを別の商品として取り扱っていたため，解説でも別の要素として取り上げている．

クレジットカードとセットで販売される Fullz は，カード会社やオンラインショップのセキュリティの向上によって，多様化している．請求書送付先住所／メールアドレス／電話番号，さらに母親の旧姓／好きな映画などのいわゆる秘密の質問が含まれることがある．Fullz とセットになったカード情報の価格は，それほど高価ではない．あるベンダは US のカード情報を＄25 で販売している．ちなみにこのベンダは日本のカード情報のセットも手掛けていて，価格は $49 となっている．US と JP の価格差についての説明はないが，市場で倍近い値が付くということは，それだけ JP のカードに需要があるといえる．

Fullz に加える情報を，利用者のニーズに合わせてカスタマイズ可能なベンダも存在する．まず利用者は＄60 を支払い，クレジットカード情報と Fullz の基本セットを購入する．このセットには，カードの名義人になりすますための Fullz のほかに，IP アドレス／タイムゾーン／言語／位置情報／ユーザエージェントといった，名義人が利用する環境ごとなりすますための情報が含まれている．この基本セットに加え，オプションとして SSN：Social Security Number（US）や Sort Code（UK ／ IE），SIN：Social Insurance Number（CA）などの公的な ID を，用途や場面に応じて組み合わせることができる．ここまで利用者目線のサービスは，ダークマーケットでもなかなかお目にかかることはない．

少し変わったところでは，本人認証サービス 3D セキュアを回避するクレジットカード情報も販売されている．3D セキュアとは，ユーザがあらかじめカード会社に登録してあるパスワード等の情報を，決済時に入力し，照合することで不正決済を防ぐ仕組みだ．カード情報を販売するベンダの説明によると，購入者にカード情報を納品する直前に，ベンダが自ら Fullz を利用してカード名義人になりすまし，カード会社のサイトで 3D セキュアの登録を行い，登録したアクセス／ユーザエージェント情報ごと購入者に納品するのだという．突破するという仕組みは至ってシンプルだが，悪意のあるベンダによって本人確認のための追加情報を登録されてしまっては，決済時にカードの不正利用を検出することは非常に難しいだろう．

コンボリストと Credential Stuffing

Fullz 以外にも，ダークマーケットでは過去に漏えいしたメールアカウントや，SNS アカウントが販売されている．これらの商品は驚くほど安価である．たとえば 57 万件の日本のユーザのメール

アドレスが＄9.99で提供されている．また，のべ1億6,400万件分のLinkedinのアカウント情報がわずか＄14で売りに出されている．これらの情報は，ハッキングフォーラムやコミュニティで無料で共有されていたりする．過去に流出したアカウントを販売するベンダの多くは転売者で，フォーラムやコミュニティ等に点在している漏えいアカウントのリストをとりまとめ，タグをつけてダークマーケットで販売している．大量のメールやSNSのアカウントは，ダークマーケットで一定の需要がある．

漏えいから一定期間を経たアカウントは，すでにパスワードの変更などの対策がされ，利用できない可能性が高い．それなのになぜマーケットで根強い需要があるのだろうか？

理由の1つが，ここ数年猛威を振るっているCredential Stuffing（リスト型アカウントハッキング）におけるコンボリストとしての活用だ．Credential Stuffingを仕掛ける攻撃者は，過去に流出したアカウントリスト等を入手し，別のサービスでのログインを試みる．過去に流出したアカウントとパスワードのセットを，複数のサービスで使いまわしをしているユーザがいれば，攻撃者はサービスのアカウントを乗っ取り，正規のユーザになりすますことができる．

コンボリストの基本構成は「USER & PASS」と「EMAIL & PASS」の組合せとなる．「EMAIL & PASS」形式のリストはたとえばSpotify，Netflix，Huluなどのサイトで使用できる．「USER & PASS」形式のリストはSpotify，Steam，Minecraftなどのサイトで使用できる．Spotifyのように両方にリストされているサービスの場合は「USER & PASS」形式と「EMAIL & PASS」形式の両方を受け入れることができる．

ただし，コンボリストとして利用する目的で，アカウントリストを購入しても，そのままログインできる歩留まりは非常に低いことが予想される．すでに述べたように，情報漏えいを認識したアカウントでは，流出したパスワードの他サービスでの使いまわしを避けている可能性が高いし，そもそもベンダによってリストにでたらめなデータが水増しされている可能性もある．

そこで攻撃者は，OpenBulletのような自動アカウントチェッカーを利用する．目的のサービスのユーザインタフェースに最適化されたConfigを事前に設定し，そのサービスで検証したいリストを指定するだけで，実際にログイン試行を行い，リスト内の大量のアカウントの有効性を自動的に検証してくれる．また，プロキシサーバのリストを読み込ませることで，IPアドレスを切り替えながらログイン試行し，アクセスログをかく乱するアンチ・フォレンジック機能も搭載している．アカウントチェッカーは，ハッキングコミュニティで有志により開発／共有されるオープンソースのものもあれば，ベンダによって開発／サポートされた有償のものもある．アカウントチェッカーは，一度価値を失ったコンボリストに再び命を吹き込むツールといえる．

盗まれた個人情報と今後の対策

ダークマーケットという，一般人が足を踏み入れがたい閉ざされた市場で，盗まれた個人情報は確かに売買されている．ただし，多くの人が想像するような，住所／氏名など4情報が羅列された名簿のようなデータではなく，Fullzと呼ばれるような，より深く「他人になりすます」ための情報により高い値が付く傾向にある．販売される情報の希少性や，金融資産のアクセス情報など，直接的金銭的価値も考慮はされているが，一方で具体的な悪用のしやすさや，悪用者の安全性に考慮された商品がより評価され，価格に反映されている．

10年前，Silk Roadが唯一無二の市場だった時代とは異なり，いまやダークマーケットは成熟しており，盗まれた個人情報は，市場全体で悪用者の需要と供給量による価格の調整メカニズムを通じて，複

数のマーケットを見比べても，およそ同様の水準で取引されている．当局によるマーケットの摘発も，ほんのわずかな間マーケット利用者を混乱させるが，目立つサービスを見せしめに 1 つや 2 つ閉鎖させたところで，市場はもはや揺らぐことはない．今回のダークマーケットにおける盗まれた個人情報の価格調査によって，市場への「商品」の供給を断ち，再販による「再利用」を防ぐといった，犯罪のコストを上げ，盗まれた個人情報の市場価格を揺さぶるといった観点が重要であると分かってきた．企業や組織は，管理している個人情報を正確に把握し，「個人情報の市場価値」「情報が盗まれた場合のインパクト」に見合った評価をし，それに応じた管理体制を構築したい．また，盗まれた場合のなりすましやすさ，悪用のしやすさを減じるための対策についても，投資を続けていく必要があるだろう．攻撃者がターゲットとする組織を入念に下調べするように，我々もまた，攻撃者の動向を継続的に調査し効果的な対策を探り続けていくしかない．

（2021 年 5 月 31 日受付）

■松本　隆　takashi.matsumoto@dena.com

（株）ディー・エヌ・エー DeNA CERT メンバ．副業として某官庁サイバー・アナリスト．デジタル・フォレンジック研究会理事．東京電機大学総合研究所客員研究員．