Security White Paper 2019

Collection#1 事件と日本の被害

26 億 9,000 万件漏洩事件の中に「42 サイト」と「2,000 万パスワード」

平成最後の正月となる 2019 年 1 月 7 日頃、あるハッカーフォーラムに Collection#1（コレクション・ナンバー 1）という名称の巨大な漏洩データの塊の存在が投稿されました。 約 27 億件という巨大な情報漏洩事件であるため、2019 年 1 月 18 日以降、世界中の多くのメディアでこのことが報道されています。
ソリトンシステムズの分析の結果、日本の被害全体としては、パスワードを含むアカウント情報が 2,000 万、漏洩被害サイトが 42 ドメイン含まれていました。 その中には、これまで特定していない新規の日本の漏洩アカウントが 800 万あり、また、未発見の日本の漏洩被害サイトを 5 つ特定できました。

2019 / 02

はじめに

「平成」最後の正月となる 2019 年 1 月 7 日頃、あるハッカーフォーラムに『Collection#1』(コレクション・ナンバー 1)という名称の巨大な漏洩データの塊の存在が投稿されました。　この Collection#1 は、この少し前、2018 年末頃に闇サイト(Dark Web)上に出現した漏洩アカウント情報（電子メールアドレスとパスワードのセット）のデータベース名です[1]。　巨大漏洩データに関するハッカーフォーラム投稿のあったすぐ後に、ソリトンシステムズはこれを誰でも閲覧できる共有ファイルサービス上で発見し、日本の組織や日本人の被害分析を開始しました。　その数時間後、この巨大データは共有ファイルサービスから削除されています。

これまでの一連のホワイトペーパーでご紹介したマイクロソフト Regional Director（豪州）の Troy Hunt 氏も、この巨大データを発見し、「7 億 7,300 万件の Collection#1 データ漏洩」として、ハッカーフォーラム投稿の 10 日後である 2019 年 1 月 17 日に、自身のブログで分析結果を公表しています[2]。　Hunt 氏は、Collection#1 が、合計で約 27 億（2,692,818,238）行の電子メールアドレスとパスワードのセットであることや、合計で、約 11 億（1,160,253,228）のユニークな電子メールアドレスとパスワードのセットがあった[3]ことをブログに記載しています。　これらの数字やデータ容量など、他の分析情報を付き合わせた結果、Hunt 氏が解析したものとソリトンシステムズが発見したものは全く同じであると判断しています[4]。Hunt 氏のブログタイトルにある「7 億 7,300 万件」という数字は、約 26 億 9,000 万件のうちのユニークな電子メールアドレスの数であり、更に、一意のパスワードが 2,100 万以上であったと述べています。

26 億 9,000 万件の漏洩データ、ユニークな電子メールアドレスが 7 億 7,300 万といった、あまりにも巨大な数字が並ぶこともあり、Hunt 氏のブログを引用した海外の専門家やセキュリティ専門ジャーナリストの記事投稿が、2019 年 1 月 18 日以降相次いでいます。　そのセキュリティ専門ジャーナリストのひとりである Brian Krebs 氏は、Collection#1 を販売している人物と連絡を取り合い、Collection#1 同様に#2～#5 など、合計 7 つの巨大データの塊があることを記事にしています。Collection#1 の大きさは 87GB ですが、例えば Collection#2 の大きさは 500GB を超えており、結果として、7 つの巨大な漏洩データの塊の合計はテラバイトクラスとなるようです[5]。　Krebs 氏の記事から、7 つの巨大漏洩データのひとつが、『AntiPublic』コンボリストであることが分かりました。　これは、2017 年 8 月に無償配布開始したソリトンシステムズのホワイトペーパー 3 部作[6]で分析結果を記載した国籍不明のコンボリスト（漏洩情報名簿）です。　『AntiPublic』の登場は 2016 年 12 月ですから、7 つの巨大漏洩の中には 3 年以上前の古い情報が数多く混在しているものと推察できます。

ソリトンシステムズが発見し、本ホワイトペーパーで日本の被害分析を実施した Collection#1 の基本情報は以下の通りです。　絶対数として、無視できない量の日本の被害があることが分かります。

項目	基本情報	Troy Hunt 氏の公開情報との比較
全件数	2,692,818,238　レコード	全く同じ（2,692,818,238 レコード）
全ファイル数	12,403　ファイル	約 12,000　ファイルと記載
日本「.jp」メール数	20,025,098　レコード	記載なし
日本「.jp」被害サイト数	42　ドメイン	38 ドメインのファイル名を公開

上表のうち、Collection#1 における我が国の被害状況に関する分析を以降に記載します。

[1] https://en.wikipedia.org/wiki/Collection_No._1
[2] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/
[3] パスワードは大文字と小文字を区別し、メールアドレスは大文字と小文字を区別しないものとして扱った場合の数字
[4] こういった事件の分析結果は、二次被害を防ぐために、意図的に正確な数字や一部のドメイン情報などを伏せることがあります
[5] https://krebsonsecurity.com/2019/01/773m-password-megabreach-is-years-old/
[6] https://www.soliton.co.jp/special/csa.html

1. アカウント情報に関する日本の被害全体像と属性分析

巨大漏洩データ『Collection#1』(コレクション・ナンバー１)の 12,000 を超えるファイル群の中に、日本の企業、公的機関、個人を含むアカウント情報（メールアドレスとパスワードのセット）がどの程度含まれているかを分析しました。　過去のホワイトペーパーと同様、ドメイン名の末尾が「.jp」となっているものを日本固有のものと仮定し、その合計や、属性を調べます。　前ページの表の通り、結果は以下となりました。

- 末尾が「.jp」： 約 2,000 万件（レコード）

全レコード数が 26 億 9,000 万ということを考えると、0.74%程度です。　過去に公開した一連のホワイトペーパーでも、何者かが編集した巨大漏洩データ中の「.jp」比率は 0.8% 程度でしたので、予想の範囲内と言えます。

日本の組織属性分析

日本固有の属性ドメインである「.jp」が付いている電子メールアドレスとパスワードのセット数、つまりアカウント数を、そのドメイン属性で分析します。　下表が調査分析結果の全体像です。　日本のアカウント情報のうち約半数が『co.jp』、即ち企業・会社（法人）の属性でした。　ここに、ネットワークサービスを示す『ne.jp』と、汎用ドメインや都道府県型ドメインである『.jp』を加えると、これら３つの組織属性の漏洩アカウントで全体の約 97%を占めることになります。

ドメイン	組織属性の種別	Soliton CSA で特定したアカウント数	比率%
CO.JP	企業・会社（国内で登記した法人） 信金・信組・投資組合を含む	9,644,507	48.16%
NE.JP	国内のネットワークサービス １サービスごとに１ドメイン名	5,320,035	26.57%
OR.JP	企業・会社以外の法人組織 財団、社団、医療、監査、宗教、特殊、農協、生協	521,546	2.60%
AC.JP	大学、大学校、高専、学術研究機関 学校法人、職業訓練校、職業訓練法人	84,003	0.42%
GR.JP	個人や法人により構成される任意団体	7,859	0.04%
ED.JP	保育所、幼稚園、小学校、中学校、高等学校 盲学校、聾学校、養護学校、専修学校	4,770	0.02%
AD.JP	JPNIC 会員となっている組織	9,621	0.05%
GO.JP	日本の政府機関 各省庁所管の研究所、特殊法人、独立行政法人	3,830	0.02%
LG.JP	地方公共団体 それらの組織が行う行政サービス	1,459	0.01%
.JP	上記の「属性型」ドメインではないドメイン 汎用ドメインや都道府県型ドメイン	4,427,468	22.11%

上記のように、見つかったアカウント情報のうち約半数が『co.jp』でした。　ただ、詳細に分析すると、実は企業が業務で利用する自社利用ドメインが多いわけではなく、圧倒的に多いのは、Yahoo! JAPAN のメールサービスである無料のヤフーメールです。　これが『co.jp』全体のうちの実に 75.9%を占めていました。 さらに、ネットワークサービスを提供する事業者の『ne.jp』アカウント情報については、1/3 程度がモバイル通信キャリアのユーザ向けドメインでした。　即ち「@docomo.ne.jp」、「@ezweb.ne.jp」、そして「@softbank.ne.jp」の３つのドメインです。

2. 『Collection#1』漏洩データにおける日本の重要機関の被害

ドメインを用いた分析により、組織属性別のアカウント情報漏洩の全体像が判明しましたので、日本の重要組織について少し掘り下げた分析を試みました。　ここで、重要組織と認識し、個別の掘り下げを実施したのは以下の 2 つのキーワードで分類される組織です。

1. 政府機関（国の組織）：　『go.jp』ドメインを持つもの
2. 地方公共団体（県の組織）：　『lg.jp』ドメインを持つもの（今回、汎用ドメイン分析は割愛しました）

国の組織の被害状況

日本の政府機関に割り振られる『go.jp』ドメインは、中央省庁だけでなく、衆議院や参議院、各省庁所管の研究所、特殊法人、独立行政法人でも利用されています。　いわゆる職務用のアドレスとして用いられるため、各政府機関は厳格な運用ルールを定めています。　漏洩アカウント被害の多いドメインのトップ 10 を下記にまとめておきます。

属性	順位	被害分析結果		
		ドメイン名	組織名称	漏洩アカウント数
go.jp	1	aist.go.jp	国立研究開発法人 産業技術総合研究所	379
	2	affrc.go.jp	農林水産研究情報総合センター	162
	3	jica.go.jp	独立行政法人 国際協力機構	120
	4	jaea.go.jp	国立研究開発法人 日本原子力研究開発機構	98
	5	nims.go.jp	国立研究開発法人 物質・材料研究機構	96
	6	meti.go.jp	経済産業省	96
	7	mofa.go.jp	外務省	73
	8	mlit.go.jp	国土交通省	69
	9	nies.go.jp	国立研究開発法人 国立環境研究所	63
	10	nirs.go.jp	国立研究開発法人 放射線医学総合研究所	62

特徴を挙げるとするなら、海外とのコミュニケーションの多い組織と、研究開発関連の組織ということになります。

都道府県の組織の被害状況

本来は、地方自治体全体の分析をすべきですが、自治体の場合、都道府県型の汎用ドメインと「lg.jp」が混在しているだけでなく、全国統一の命名ルールがあるわけではないので、ここでは「lg.jp」だけを抽出した分析を試みました。漏洩アカウント被害の多い「lg.jp」ドメインのトップ 10 を下記にまとめておきます。

属性	順位	被害分析結果		
		ドメイン名	組織名称	漏洩アカウント数
lg.jp	1	pref.shiga.lg.jp	滋賀県	171
	2	pref.hyogo.lg.jp	兵庫県	63
	3	city.fujisawa.lg.jp	藤沢市（神奈川県）	32
	4	city.kumamoto.lg.jp	熊本市（熊本県）	31
	5	pref.okinawa.lg.jp	沖縄県	29
	6	pref.yamanashi.lg.jp	山梨県	23
		pref.nagasaki.lg.jp	長崎県	23
		pref.kumamoto.lg.jp	熊本県	23
	9	pref.kyoto.lg.jp	京都府	22
		mbox.pref.osaka.lg.jp	大阪府	22

トップ１０に共通する特徴は見出せていません。　さらに、滋賀県だけが群を抜いて多い理由も不明です。　前述の通り、自治体の場合、都道府県型の汎用ドメインを利用することも多いため、この「lg.jp」漏洩数ランキングは参考程度の情報であることをお断りしておきます。

3. 新規に発見した「.jp」漏えいアカウント被害は 800 万件

Collection#1 分析結果を加える以前、この分析を開始した 2019 年 1 月 15 日時点で、ソリトンシステムズが特定し、分析を完了した世界のデータ漏洩事件、国内の事件の数は下表の通りです。　すなわち、日本の企業や団体が侵害されたと思われる事件が約 200、日本以外のものが約 100、攻撃者が目的別に編集した巨大なデータ群が 8 種類です。

漏洩事件の分類	特定した事案の数	備考
世界の漏洩事件	102 事案	日本以外の事件
日本の漏洩事件	196 事案	「.jp」が被害者となっているもの
攻撃者が編集した巨大漏洩データ群	8 種類	攻撃者の国籍は不明

Collection#1 に含まれる約 2,000 万の日本の被害アカウントと特定済み被害との付き合せ

ソリトンシステムズでは、Collection#1 分析以前、この分析を開始した 2019 年 1 月 15 日時点で、日本固有の属性ドメインである「.jp」が付いている電子メールアドレスと暗号化／平文パスワードのセット数、つまりアカウント情報を、のべ数で約 8,700 万件特定していました。　これは名寄せなどの処理をする前の数字です。
Collection#1 では、「.jp」属性を持つアカウント情報が約 2,000 万件あったものの、これまでに特定した件数が非常に大きな数字であるため、「この大半は、既に特定済みの被害アカウント情報と同じものではないか」という仮説を立てました。　検証するために、Collection#1 に含まれる「.jp」アカウント情報を、それまでに特定済みの情報と付き合せることにしました。　付き合せた結果、特定済みの情報と一致しなかったものが、新たに見つかった「.jp」漏洩アカウントということになります。　結果は下表です。

カウントした対象	カウント条件	備考
Collection#1 に含まれていた「.jp」アカウント件数	そのままのレコード数	20,025,098
	重複削除を実施	11,454,286
新たに見つかった「.jp」漏洩アカウント件数	重複削除を実施	8,028,014

Collection#1 の分析により、新たに約 800 万件の「.jp」漏洩アカウントを発見しました。　これまでに特定した約 200 の日本の漏洩事件、約 100 の世界の漏洩事件にはなかったアカウント情報ですので、別の事件、別の手法などで盗まれた可能性が高いと考えます。

5. Collection#1 に含まれる我が国の被害に遭ったと思われるサイト一覧

巨大漏洩データ『Collection#1』（コレクション・ナンバー１）の 12,000 を超えるファイル群の中には、ハッキング対象となったサイトの URL をファイル名称として利用しているように見受けられるファイルが数多く存在します。　その中には『.jp』ドメインを使って命名されたものが 42 ファイルありました。　それらのファイルに記載されていたレコード数を「全数」として概数表記し、その数の多い順に並べて記載します。

Collection#1 内の国内被害サイト	漏洩アカウント			概要・備考など
	全数	.jp 属性	パスワード	
Vch	111,000	32,334	暗号	アイドル、グラビア、音楽等の仮想現実(VR)動画を提供するサイト（V チャンネル）から盗まれたと思われる大量のユーザーデータです。別の事案である通称「4000 サイト」事件で既に同じものを発見しており、この運営会社である株式会社エル・エー・ビーにはソリトンから通報済みです。
ラヴェーラ	101,000	76,550	平文	ドイツ生まれのオーガニックコスメであるラヴェーラを販売するサイトから盗まれたと思われる大量のユーザーデータです。別の事案である通称「3500 サイト」事件で既に発見しており、この運営元のアットスター株式会社にはソリトンから通報済みです。
株式会社エスビーシー	41,000	52	平文	労働者派遣事業や製造業務請負・物流業務請負をしている株式会社エスビーシーのサイトから盗まれたと思われるデータです。別の事案である通称「3500 サイト」事件で既に発見しています。
医学通信社	33,000	23,913	暗号	医療図書の出版をしている株式会社医学通信社のサイトから盗まれたと思われる大量のユーザーデータです。別の事案である通称「4000 サイト」事件で既に発見しており、株式会社医学通信社にはソリトンから通報済みです。
ポルシェ ジャパン	28,000	22,100	暗号	ドイツのポルシェ社の日本法人であるポルシェジャパンのサーバーが不正アクセスされた事件で、既に公表されています。公式ニュースリリースがあった 2018 年 2 月より 3 ヶ月前には、誰でも入手可能な状態になっていました。
卓球ファン net	17,000	13,857	暗号 平文	卓球ファンのための携帯電話向け情報サービスを提供している卓球ファン net のサイトから盗まれたと思われるユーザデータです。別の事案である通称「3500 サイト」事件で発見しています。株式会社卓球ファン net にはソリトンから通報済みです。

Collection#1 内の国内被害サイト	漏洩アカウント			概要・備考など
	全数	.jp 属性	パスワード	
イージーライダース	15,000	12,070	平文	アメリカンスタイルのカスタムバイク・パーツの EC サイトから盗まれたと思われる大量のデータです。別事件でも同じものが発見されています。ハッカー向けフォーラム Nulled に投稿され、そのリンクがラトビア共和国のファイル共有サイトに公開されてました。株式会社イージーライダースにはソリトンから通報済みです。
ペットストリート	8,000	7,372	平文	株式会社マイスターズが運営するペットのコミュニティサイトであるペットストリート（PETST）から盗まれたと思われるユーザ情報です。今回「Collection #1」事件で初めて発覚しました。
しずとく	5,600	5,216	暗号	株式会社しずとくが運営する静岡県のスーパーマーケット特売情報を提供するポータルサイト（しずとく）から盗まれたと思われるユーザーデータです。別の事案である通称「3500 サイト」事件で既に発見しています。
メジカルビュー社	5,400	4,501	平文	医学・看護学・医療全般に関する医学領域の専門書を出版するメジカルビュー社のサイトから盗まれたユーザーデータです。既に公表済みの事案でもあり、通称「3500 サイト」事件で既に発見しています。株式会社メジカルビュー社にはソリトンから通報済みです。
岡山国際サーキット	5,400	4,397	暗号	モーターレースの行われる岡山国際サーキット場のサイトから盗まれたと思われるユーザー情報です。別事案である通称「3500 サイト」事件で既に発見しています。運営元の株式会社岡山国際サーキットにはソリトンから通報済みです。
住まいのプロショップ ヒラオカ	5,200	4,135	平文 暗号	広島県福山市で住宅建築やリフォーム業を営んでいる株式会社平岡設備工業のサイトから盗まれたと思われるユーザ情報漏洩です。「Collection #1」事件で初めて発見しました。ソリトンから株式会社平岡設備工業には通報済みです。
チュ・ジフン 日本公式サイト	5,500	4,424	平文	チュ・ジフン日本公式サイトから盗まれたと思われるユーザ情報漏洩です。別事案である通称「2800 サイト」事件で既に発見しています。運営会社である株式会社デジタルアドベンチャーにはソリトンから通報済みです。
テックトランス	5,000	2,161	平文	CD/DVD プレス販売や新宿ライブハウス MARZ を運営しているテックトランス株式会社から盗まれたと思われるユーザ情報漏洩です。「Collection #1」事件で初めて発見しました。ソリトンからテックトランス株式会社には通報済みです。

Collection#1 内の国内被害サイト	特定した漏洩アカウント			概要・備考など
	全数	.jp 属性	パスワード	
ダートコーヒー	5,000	4,210	平文	ダートコーヒーの通販サイトから盗まれたと思われるユーザ情報漏洩です。別事案である通称「2800 サイト」事件で既に発見しています。ダートコーヒー株式会社にはソリトンから通報済みです。
アクロビジョン	5,000	4,090	暗号	株式会社アクロビジョンが運営する IT 求人サイトから盗まれたと思われるユーザ情報漏洩です。別事案である通称「4000 サイト」事件で既に発見しています。ソリトンから株式会社アクロビジョンには通報済みです。
ウーマンズワーカー	4,300	3,723	平文	風俗関係の女性向け求人情報サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
メンズワーカー	5,600	3,702	平文	風俗関係の男性向け求人情報サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
ナイトワーカー	5,600	3,680	平文	キャバクラなど全国のウォーターズ系求人情報サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
おおた工業フェア	4,300	3,785	暗号	公益財団法人の大田区産業振興協会が主催する高度技術・技能展の展示会案内サイトから盗まれたと思われるユーザー情報です。別の事案である通称「4000 サイト」事件で既に発見しています。
鍛冶屋せんべい	3,400	1,652	平文	東京葛飾の老舗である鍛冶屋せんべいの EC サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。有限会社鍛冶屋煎餅にはソリトンから通報済みです。
マカオ観光局	3,200	2,611	平文	マカオ政府観光局の WEB サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で発見済みです。マカオ観光局にはソリトンから通報済みです。
確認の取れない「.jp」サイト	3,200	非公開	非公開	URL には「.jp」と記載があるものの、被害サイトの特定ができなかったものです。
Luxology	3,000	2,205	平文	3D コンテンツ制作ソフトの MODO を取り扱った EC サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見されています。

Collection#1 内の国内被害サイト	特定した漏洩アカウント			概要・備考など
	全数	.jp 属性	パスワード	
サッカーカードフォーラム	3,000	318	平文	サッカーカード専門のトレード掲示板や全国のトレーディングカードショップの情報提供等を行っているフォーラムサイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見されています。
ゲーム FinalFantasy 関連個人情報サイト	2,800	1,649	平文	人気ゲーム Final Fantasy に関する個人運営の情報サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見されています。
風俗情報 MANZOKU	2,100	2,064	平文	神奈川の風俗情報サイト「Manzoku」へリダイレクトされる元のサイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「3500 サイト」事件で既に発見されています。
尼崎市の健診予約サイトあまけん	2,000	1,464	平文	尼崎市の検診スケジュールサイトから盗まれたと思われるユーザ情報漏洩です。別の事案「2800 サイト」事件で既に発見。尼崎市には兵庫県警から通報があり、2018 年 3 月以降、その被害について公式な発表がされています。また、日経コンピュータ 2018 年 6 月 21 日号「動かないコンピュータ」で詳細が報じられました。
アーティフィシャルインテリアブーケ協会	1,900	1,474	暗号	生花をリアルに再現する造花であるアーティフィシャルフラワーを扱う協会のサイトから盗まれたと思われるユーザーデータです。別の事案である通称「4000 サイト」事件で既に発見しています。ソリトンから協会に通報済みです。
van ガイド	1,900	980	平文	カナダのバンクーバー街歩きガイドのサイト「van ガイド」から盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
フリーブックジャパン	1,900	1,388	平文	様々なジャンルの無料レポートを配信するサイト（フリーブックジャパン）から盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
日本工業大学	1,900	1,647	平文	日本工業大学から盗まれたと思われる情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。日本工業大学にはソリトンから通報済みです。
そーしゃるぱーく	1,800	1,104	平文	無料の SNS 作成・運営の個人サイト（そーしゃるぱーく）から盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。

Collection#1 内の国内被害サイト	特定した漏洩アカウント			概要・備考など
	全数	.jp 属性	パスワード	
麗嬢	1,700	1,481	平文	吉原の高級ソープランド「麗嬢」のサイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
フーバイト	1,700	938	平文	風俗求人情報サイト（フーバイト）から盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。
静岡神社庁	1,600	1,286	平文	全国 8 万の神社を包括する神社本庁の地方事務所の 1 つである静岡神社庁のサイトから盗まれたと思われるユーザ情報漏洩です。今回の「Collection #1」事件で初めて発見しました。
世一旅行社 Itms	1,600	659	平文	日本向けの韓国旅行会社である世一旅行社のサイト「Itms」から盗まれたと思われるユーザ情報漏洩です。「Collection #1」事件で初めて発見しています。
大阪弁護士協同組合	1,100	1,040	平文	大阪弁護士協同組合の WEB サイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。ホームページがメンテナンス中のため通報できていません。
おきなわ不動産市場	1,100	677	平文	沖縄の賃貸アパート等の情報サイト（おきなわ不動産市場）から盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。運営会社の有限会社沖縄不動産市場にはソリトンから通報済みです。
ＮＰＯ法人 くまっこステーション	900	767	平文	熊本でひとり親家庭をサポートする NPO 法人くまっこステーションのサイトから盗まれたと思われるユーザ情報漏洩です。別の事案である通称「2800 サイト」事件で既に発見しています。この NPO は 2018 年 3 月末日に解散しています。
株式会社ナベヤ	600	488	暗号	精密治具、精密マシンデバイス、鋳造部品等を生産している岐阜県の株式会社ナベヤのサイトから盗まれたと思われるユーザーデータです。別の事案である「3500 サイト」事件で既に発見しています。株式会社ナベヤにはソリトンから通報済みです。

6. 新規に発見した「.jp」被害サイトは５つ＋１

巨大漏洩データ『Collection#1』(コレクション・ナンバー１)の 12,000 を超えるファイル群の中には、『.jp』ドメインを使って命名されたものが 42 ファイルありました。　その 42 ファイルの概要は前項の一覧表の通りです。

一覧表の概要欄に記載のある通り、『Collection#1』とは別の事案で、既に発見されているファイルが非常に多いことが分かります。　特に、ホワイトペーパー前作[7]で、攻撃者同士のデータ交換・売買用の巨大ファイルとして、その存在を指摘した「2,800 サイト」と「4,000 サイト」で発見されたものと同じ内容のファイルが数多く見つかりました。　既に発見されているファイルと新規ファイルに関するサマリーは下表になります。

ファイルの分類	最初の発見場所	ファイル数	備考
既に別事案で 発見されているもの	2800 サイト事件	22	
	4000 サイト事件	5	
	3500 サイト事件	7	
	個別の漏洩事件	2	
新規に発見	Collection#1	6	１ファイルは被害者の特定できず

42 の被害サイトと思われるものの中で、今回、新たに発見したのは５つの被害サイトです。　ファイルとしては、もうひとつあるのですが、被害者の特定ができていません。　もちろん、全てのサイト運用者には、連絡が取れる範囲内において、事実を通報し、注意喚起を実施しています。

最初の発見場所について補足しておきます。　攻撃者同士のデータ交換・売買用「2,800 サイト」と「4,000 サイト」事件については、既に分析結果を公表しておりますが、今回は新たに「3500 サイト」事件というものが登場しています。　実は、これ以外に「6000 サイト」事件と呼んでいるものもあります[8]。　ホワイトペーパー前作のあとに発見した巨大ファイル群が２つあり、それを「3500 サイト」「6000 サイト」事件と呼んでいます。　そのあとに今回の『Collection#1』を発見しました。

なお、「3500 サイト」や「6000 サイト」については、ホワイトペーパーによる分析結果の公表は行いませんが、お客様のご依頼で個別調査する場合は、これらの未公表事件による被害についても分析対象として報告書に記載しています。

[7] https://www.soliton.co.jp/special/csa1807.html
[8] 事件の名称である「2800 サイト」「4000 サイト」「3500 サイト」「6000 サイト」は全てソリトンが命名したものです

7. まとめ

『Collection#1』(コレクション・ナンバー１)事件で、日本の被害全体としては、パスワードを含むアカウント情報が 2,000 万、被害サイトは 42 でした。　分析の結果、ソリトンシステムズがこれまで特定していない日本の漏洩アカウントを 800 万発見でき、また、新たに日本の被害サイトを５つ特定できた、というのがまとめとなります。　今回の事件の分析完了に伴い、ソリトンシステムズが調査可能な漏洩アカウント情報数は、のべ 80 億件となりました。

ソリトンシステムズが、「漏洩アカウント被害調査」と称して、ドメイン単位でのパスワード漏洩状況を調査分析するサービスを発表したのは、2017 年 10 月 5 日のことです。　本ホワイトペーパー執筆時点で、サービス発表から 1 年 4 ヶ月が経ち、累計調査数は 1,000 ドメインとなりました。　たいへん数多くの調査依頼を頂いています。　また、調査サービス発表以来、情報セキュリティ専門メディアよりも、一般向けの大手メディアで取上げられることが多く、「パスワードは漏洩している」という事実に対する関心の高さを感じています。

同様の調査サービスは、米国やイスラエルなどのセキュリティ・インテリジェンス先進国の調査会社が提供していますし、一連のホワイトペーパーでもご紹介している Troy Hunt 氏のサイトで個別に確認することも可能です。　だいたいどこも、現時点では 70～80 億件程度の漏洩データを収集しており、外部から見ると同じことをやっているように見えるはずです。

ソリトンシステムズのパスワード漏洩調査の特徴は、徹底して「日本の被害」の分析にこだわっていることです。　この調査サービスを通じて、日本の企業、日本の重要組織、そして日本人の被害状況を明らかにし、具体的かつ効果的な対策・対処が実施できるようにしたいと考えています。　調査によって特定された漏洩事件の数も、世界の事案数より常に日本の事案数が多いという状況が続いています。　「日本の被害」分析へのこだわりは今後も同様です。

今回の分析対象は 2019 年 1 月 17 日以降に報道された『Collection#1』のみでした。　Collection#1 同様に#2～#5 が存在することは冒頭に記載した通りです。　こちらについても「日本の被害」が分析完了し、新しい事実が発見されたなら、個別通報などの注意喚起活動後に公開する計画があります。

【著者】株式会社ソリトンシステムズ　執行役員　長谷部泰幸

【分析協力】サイバーリサーチ株式会社　代表取締役　藤田有悟

Soliton Systems Security White Paper 2019

Collecton#1 事件と日本の被害～
26 億 9,000 万件漏洩事件の中に「42 サイト」と「2,000 万パスワード」

発行　　初版 2019 年 2 月 1 日
発行所　　株式会社ソリトンシステムズ
お問合せ先　　netsales@soliton.co.jp