Soliton Systems
Security White Paper 2017

世界のハッキング事件による日本のアカウント情報漏洩分析－1 ～事件別の被害

Soliton

はじめに

2016 年 12 月、世界中のアカウント情報を集めた電子メールアドレスとパスワードのペアの巨大なリストが「アンチパブリック・コンボリスト」に掲載されました。2017 年 5 月 11 日の分析記事によると、このリストには 5 億 6,200 万の電子メールアドレスが含まれていて、多くはさまざまなオンラインシステムからハッキングされた複数の異なるパスワードで構成されていました [1]。

このコンボリスト分析記事を執筆した専門家によると、ここに掲載されているメールのドメインの 42%は Yahoo.com、7%は aol.com です。　そのほかのドメインを見ても、大半が個人向けのフリーメールアドレスとなっているとのことで、一見すると日本の企業や団体とはあまり関係ないように思われました。

同じタイミングで、ソリトンシステムズでは、世界中のサイバー犯罪に関して「オープン・ソース・インテリジェンス [2]」手法を使った被害分析の可能性を探っており、最初のテーマとして『日本企業または政府機関のアカウント情報がどの程度盗まれているのか？』の解析を選定しました。　ソリトンシステムズは、認証セキュリティの分野では、国内で圧倒的なシェアを誇っています。　その認証の最重要かつ基本的な情報は、ID とメールアドレスとパスワードを組合せた『アカウント情報』です。　認証セキュリティ分野の第一人者の責務として、まず最初は、サイバー犯罪によって漏洩した日本の『アカウント情報』被害を具体的に調査分析すべきと考えました。

1. オープン・ソース・インテリジェンス

オープン・ソース・インテリジェンス（以下、OSINT：オシント）は、一般的には諜報活動の分野のひとつとして知られています。　OSINT は、「合法的に入手できる情報やデータ」を「合法的に調べ、突き合わせる」ことで真実にたどり着く手法ですが、その適用分野によっては、細かいデータを少しずつ集めて調査分析するだけでも、相当な精度の情報が得られることがあると言われます。

サイバーセキュリティの世界では、民間企業や民間団体、有志の集まりなどが目的別にオープン・ソース・インテリジェンスのサイトを開設しており、有償・無償で提供しています。　各国の政府機関やサイバー防衛を生業とする民間企業は、分析目的に応じて、これを再利用しています。

インテリジェンスの種類	概要
シギント	SIGINT　(Signals Intelligence) 電話、無線、電磁波、GPS、IT ネットワークなどから情報を傍受する活動
イミント （イマジント）	IMINT　または　IMAGINT　(Imagery Intelligence) 偵察衛星や偵察機によって撮影された画像を継続的に分析する事で情報を得る手法
ヒューミント	HUMINT　(Human Intelligence) 人を介して行う諜報活動。合法活動や捕虜尋問等も含み、必ずしもスパイとは限らない
オシント	OSINT　(Open Source Intelligence) 一般に公開さている情報を収集して分析する諜報活動の手法

[1] https://threatpost.com/anti-public-combo-list-analysis-reveals-password-habits-improving/125627/

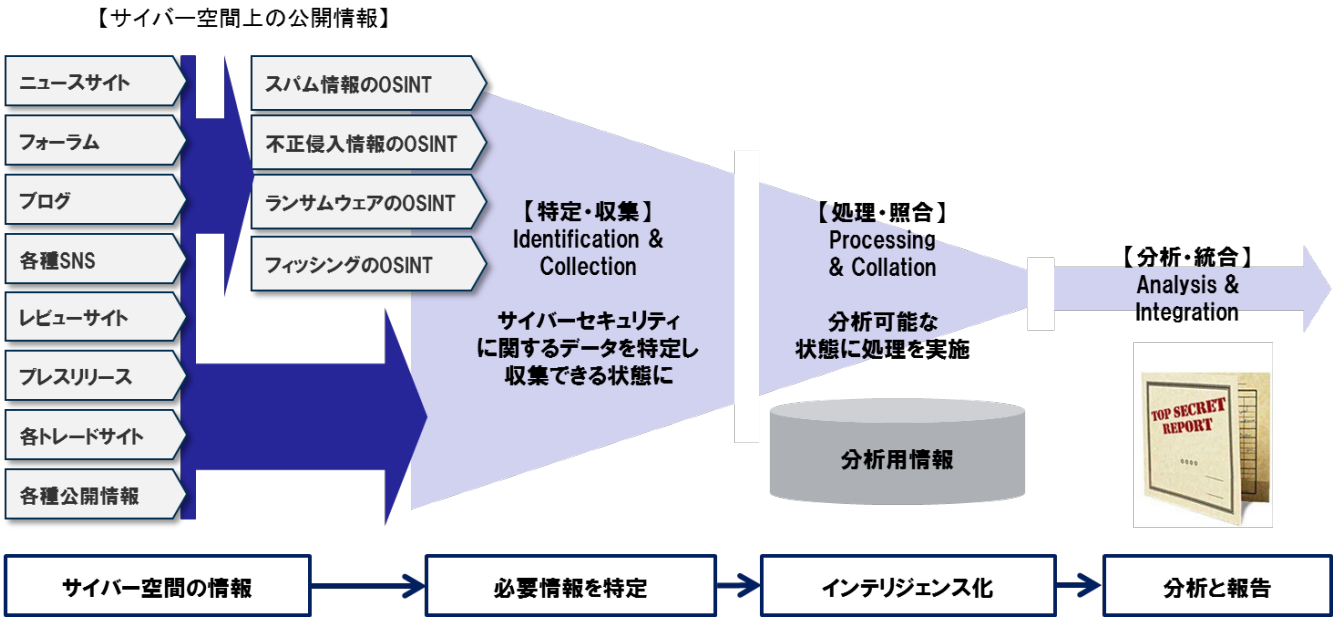
[2] Open-Source Intelligence (OSINT: オシント)は、オープンソース、つまり一般に公開されている膨大な情報の中から、合法的に必要な情報を収集・分析する活動のことです。国家安全保障の分野では、諜報活動のひとつと位置づけられます。

2. ソリトン・サイバー空間アナリティクス（Soliton CSA）

ソリトンシステムズ独自のサイバー空間アナリティクス（Soliton CSA = Soliton Cyber-Space Analytics）は、OSINTの手法を参考に、サイバー空間内部にある日本のサイバーセキュリティに関係する情報について、誰でも入手できる公開情報から特定し、整理・解析・分析しようと開発した基盤技術です。　目的とする調査分析対象を定めた後、その情報がサイバー空間のどこに存在するかを特定し、継続的にデータを収集します。

関連すると思われる公開情報は、様々なデータ形式で散在しているため、そのままでは何も調べることができません。Soliton CSA は、これらを検索可能な状態に処理し、ソート／マージ、分解などの追加処理とデータ照合などを実施することで、目的とする調査分析対象に関連した独自のインテリジェンスをつくります。最後に、報告に必要な追加解析と情報統合を実施し、目的に合致した調査分析結果を報告書としてまとめます。

この工程は、ソリトンシステムズがフォレンジック調査サービスの中で提供している『電子証拠開示』支援サービスの工程とほぼ同じです。　電子証拠開示では、調査分析の目的が社内不正や係争対応のための社内データの整理ですので、その情報が社内のどこに存在するかを特定するところから始まります。　これを「社内」ではなく、「サイバー空間」に置き換えたものが Soliton CSA の基盤技術上で展開される調査分析工程となります。



3. 有用な情報を与えてくれる世界の OSINT

ソリトンシステムズのサイバー空間アナリティクス（Soliton CSA = Soliton Cyber-Space Analytics）は、目的とする調査分析に必要な公開情報を特定するため、いくつかのサイバーセキュリティ関連 OSINT からそのヒントを得ています。　サイバーセキュリティ関連 OSINT は、『スパムやそれに関係する脅威』や『ランサムウェアに関係するもの』といった調査分析目的別に公開情報を特定・収集し、インテリジェンスとして提供しています。　世界中の専門家が集まり、協力しながら整理しているものもあれば、完全にプログラムで自動化しているもの、ユーザーの投稿によって品質を向上させているものなど、インプリメントの方法は様々です。

Soliton CSA が情報特定のヒントを得ている主な OSINT を以下にご紹介しておきます。

調査目的	OSINT 名称	概要
スパムを中心にリアルタイムの脅威全般	SPAMHAUS	スパムハウス・プロジェクトは、迷惑メールやフィッシング、マルウェア、ボットネットなどのリアルタイム脅威情報を提供している NPO。 1998 年に設立され、スイスのジュネーブ及びイギリスのロンドンを中心に活動しています。現在、10 か国、フォレンジックスペシャリストを含む合計 38 名で運営しています。
スパムを中心に攻撃者情報	stop-forum-spam	ストップ・フォーラム・スパムは、スパマー（迷惑メール送信者や組織）やオンラインフォーラム、ブログに不正書き込みを行うサイバー攻撃者のリストを提供しています。リストには、メールアドレスや IP アドレス、ユーザー名、迷惑行為の頻度、ログが含まれます。
不正侵入	SNORT	スノートは、IDS（Intrusion Detection System, 不正侵入検知システム）機能をもつフリーのソフトウェアとして有名です。 匿名通信（TOR)を含む様々な不正侵入の攻撃手法の情報を集めたルールを提供しています。
不正侵入	EMERGING THREATS	エマージング スレッツは、匿名通信を含む様々な不正侵入の攻撃手法の情報を集めたルールを提供しています。ここが提供する IP レピュテーション（IP アドレスブラックリスト）には、脅威分析によって危険性があると判断された IP アドレスの情報がカテゴリーごとに登録されています。
ランサムウェア	ransomeware tracker	ランサムウェアトラッカーは、ランサムウェアに関連するボットネット、C＆C サーバー、配布サイト、支払いサイトのドメイン名や IP アドレス、URL の情報を提供しています。 次のランサムウェアの情報を提供しています。 TeslaCrypt、CryptoWall、TorrentLocker、PadCrypt、Locky、CTB-Locker、FAKBEN、PayCrypt
ゼロデイフィッシング	OpenPhish	オープンフィッシュは、完全に自動化されたゼロデイフィッシングサイトの特定・収集システムです。 独自の AI 技術によって完全に自動化されたこの特定システムは、人間が介入することなく、また他のブラックリストも利用しません。
フィッシング	PhishTank	フィッシュタンクは、OpenDNS 社（2005 年設立）によって運営されるフィッシング情報サイトです。 フィッシングサイト情報を誰でも投稿することができ、そのデータを API で提供してくれています。巧妙な犯罪に対して、皆で立ち向かおうという姿勢のオープン・ソース・インテリジェンスです。

4. 事件別のアカウント情報漏洩分析

2017 年 8 月現在、この 1 年くらいの世界のハッキング事件について、分かる範囲で調べてみると月平均で 20 件程度が報道されているようです。　更に 2010 年以降で、ハッキングによってアカウント情報が盗まれた事件をカウントすると 200 を超えることが分かりました。現時点で、Soliton CSA が特定できた事件は、その 2 割に過ぎません。

わずか 2 割ではありますが、これらの特定された事件のうち、Soliton CSA で解析可能な漏洩アカウント情報の数は、現時点で約 20 億となっています。　これだけの数があるのは、検索エンジン提供会社のフリーメールや、携帯電話のキャリアメールなど、ひとりが複数のメールアドレスを持つ時代であることが原因だと考えています。

日本の被害状況を推察する指標の設定

今回、Soliton CSA 基盤を使って、日本のアカウント漏洩被害状況を分析するに際し、日本固有の属性ドメインである『.jp』が付いているメールアドレスを含むアカウント情報の数を重要な指標と定義しました。　もちろん、日本人や日本の組織であっても『.com』や『.net』を始めとする『.jp』以外の属性ドメインを利用している場合もあるでしょう。

正確な被害状況というより、全体像の把握を目的として、日本の被害状況は『.jp』が付いているメールアドレスを含むアカウント情報の数と強い相関があるという仮説を立てて調査分析を実施しています。

大規模コンボリスト

冒頭の「はじめに」でご紹介した 2016 年末に登場した大規模コンボリストについては、既に何人かの専門家が内容を分析しています。　実は、冒頭でご紹介した「アンチパブリック・コンボリスト」と同じくらいのタイミングで、やはり大規模なアカウントリストである「エクスプロイト・イン・コンボリスト」も登場しているのですが、日本ではその報道をまったく見かけません。

個々のハッキング事件別の分析の前に、まずはこの 2 つの大規模コンボリストを解析し、『.jp』が付いているメールアドレスを含むアカウント情報の数を調べました。

リスト名	登場年月	Soliton CSA で特定できた漏洩アカウント			概要
		全数	『.jp』属性	漏洩内容	
Exploit.In 国籍不明	2016 年 12 月	5 億 9,343 万	61 万	メールアドレス 平文パスワード	2016 年末に「Exploit.In」という名前で「8 億件のコンボリスト」と宣伝した電子メールアドレスとパスワードのペアの巨大なリストが登場しました。容量が 75GB を超えるデータベースとなっていて、過去に盗まれた様々な漏洩データで構成されているようです。
AntiPublic 国籍不明	2016 年 12 月	4 億 5,796 万	452 万	メールアドレス 平文パスワード	「はじめに」でご紹介したもの。 専用検索ツールはロシア語表記になっています。上記の「Exploit.In」と同様、アカウント情報の多くは、様々なオンラインシステムからハッキングされた複数の異なるパスワードで構成されていました。

世界のハッキングによるアカウント情報漏洩事件

これ以降は、Soliton CSA でアカウント情報漏洩が特定できた個別のハッキング事件別に分析結果を記載します。ハッキング被害にあったサイトとその運営会社が所属する国についても記載しました。
順序は、Soliton CSA で特定できた漏洩アカウントの総数の多いものから表記してあります。　これは、必ずしもその事件で漏洩したアカウント数を正しく反映しているものではありません。　あくまで、現時点で特定できた総数の順であることと、特定できた全ての事件ではなく、一部の事件であることをお断りしておきます。

ハッキング被害者	事件発覚年月	Soliton CSA で特定できた漏洩アカウント			備考など
		全漏洩数	『.jp』属性	漏洩内容	
Myspace 米国	2013 年 6 月	3 億 5,942 万	93 万	アカウント名 メールアドレス 暗号パスワード	米 Time 傘下のソーシャルメディア「Myspace」が不正侵入を受けた事件です。この暗号パスワードというのは、最初の 10 文字の SHA-1 ハッシュでした。
Linked In 米国	2012 年 6 月	1 億 6,461 万	15 万	メールアドレス 暗号パスワード	ビジネス SNS「LinkedIn」です。発覚当初は 650 万アカウント漏洩だと報道されていましたが 1 億を超えていました。ロシア人の容疑者がチェコ共和国で逮捕されています。
Adobe 米国	2013 年 10 月	1 億 5,244 万	294 万	アカウント ID メールアドレス 暗号パスワード パスワードヒント	ソフトウェア会社の「Adobe」です。アカウント情報のみならず、主力製品である「Photoshop」のソースコードが流出していたことも判明しています。
Badoo 英国	2016 年 6 月	1 億 1,200 万	28 万	アカウント ID メールアドレス 暗号パスワード 生年月日	成人向け出会い系のコミュニティーサイトです。グローバルでサービスを提供し、日本語ページもあります。世界で 3 億ユーザ以上の登録があり、月間 6000 万のアクティブユーザを持つといわれます。
VK ロシア	2016 年 6 月	9,334 万	3 千	メールアドレス 平文パスワード	VK はロシアの Facebook とも言われるヨーロッパ最大の SNS サイトです。漏洩当時、1 ビットコイン（約 6 万円）でアカウント情報が販売されていました。
DropBox 米国	2012 年 6 月	6,865 万	110 万	メールアドレス 暗号パスワード	写真や文章、動画のファイルをどこでも簡単に共有できるオンラインストレージサービス。パスワードの半分、約 3200 万件は強度の強い BCrypt を使ってハッシュ化されています。残りは SHA-1 でした。

ハッキング被害者	事件発覚年月	Soliton CSA で特定できた漏洩アカウント			備考など
		全漏洩数	『.jp』属性	漏洩内容	
tumblr 米国	2013 年 3 月	6,545 万	21 万	メールアドレス 暗号パスワード	タンブラーは米国 Yahoo!が買収したブログとミニブログ、そしてソーシャルブックマークを統合したマイクロブログサービスを提供する会社です。『.jp』アカウントが 20 万以上ありました。
Zoosk 米国	2016 年 5 月	5,258 万	5 万 2 千	メールアドレス 暗号パスワード	米国のオンライン・デートのサイト。つまり、出会い系サイトです。意外にも『.jp』属性のアカウント情報が 5 万以上特定できました。漏洩パスワードは、MD5 アルゴリズムにより暗号化されていました。
Invest Bank UAE	2016 年 5 月	5,000 万	22	メールアドレス クレジットカード番号 有効期限 口座番号 口座開設日 口座限度額 電話番号	インベスト・バンクは、アラブ首長国連邦の銀行です。トルコのハッカー集団であるブースハッカーズ（Bozkurt Hackers）により攻撃を受け、クレジットカードやアカウント情報が漏えいしました。
iMesh 米国	2013 年 9 月	4,947 万	1 万 3 千	ユーザー名 メールアドレス IP アドレス 暗号パスワード	アイメッシュは音楽や動画を共有する P2P ソフトのサイトです。漏洩したパスワードは、MD5 アルゴリズムにより暗号化されていました。
Fling 米国	2013 年 4 月	4,077 万	2 万 6 千	ユーザー名 メールアドレス 平文パスワード 性別 生年月日 性的嗜好	自称 "世界最高のアダルト SNS"のウェブサイトです。漏洩データには、性的嗜好や性的関心のような機密性の高い個人的属性も含まれています。『.jp』属性アカウント情報が 2 万以上あります。
Last.fm 英国	2012 年 9 月	3,722 万	11 万	ユーザー名 メールアドレス 暗号パスワード 平文パスワード	ラストエフエムは、世界最大のオンライン・ミュージックカタログを提供し、無料で音楽・動画の視聴が行えるサービスを提供しています。発生から 4 年後の 2016 年 9 月に初めて被害規模が分かりました。
Twitter 米国	2016 年 6 月	3,289 万	2 万	メールアドレス 平文パスワード	オンラインニュース及び SNS サービスを提供。情報漏洩 DB を構築している「LeakedSource」が、Twitter アカウント情報漏洩を公表するも Twitter 側はこれを否定。

ハッキング被害者	事件発覚年月	Soliton CSA で特定できた漏洩アカウント			備考など
		全漏洩数	『.jp』属性	漏洩内容	
ASHLEY MADISON カナダ	2015 年 7 月	3,081 万	15	ユーザー名 メールアドレス 暗号パスワード 生年月日 民族 性別 住所・電話番号 性的嗜好	カナダの既婚者向け出会い系サイト。要するに不倫サイトです。この情報漏洩により、数名が自殺するという事態に発展しました。サイト運営会社は、アメリカの連邦取引委員会との和解で、160 万ドルの罰金支払いとサイバーセキュリティ対策の強化を合意しています。
17 Media 台湾	2015 年 9 月	2,800 万	1,300	ユーザー名 メールアドレス 暗号化パスワード	17 メディアは台湾のモバイルアプリ提供会社で、ライブビデオ及びリアルタイムコンテンツ共有サービスを提供しています。
淘宝网 中国	2016 年 5 月	2,115 万	1,000	メールアドレス 平文パスワード	アリババグループのネット決済システム「支付宝（アリペイ）」の個人情報が、ショッピングサイト「淘宝（タオバオ）」で運営する店舗を通じて漏洩し、上海市松江区に住む男性が 100 万元近くを騙し取られていたことがわかりました。
178.COM 中国	2011 年 12 月	900 万	0	ユーザー名 メールアドレス 平文パスワード	178 ドットコムは中国の玄人向けゲームネットワークです。特定できた範囲内において『.jp』属性の登録はありませんでした。
开心网 中国	2012 年 1 月	600 万	160	ユーザー名 メールアドレス 暗号パスワード	かいしん（Kaixin001）は中国で急成長した SNS サービスを提供しています。
xat 英国	2015 年 11 月	596 万	620	ユーザー名 メールアドレス 平文パスワード アクセス履歴	XAT はオンラインチャットルームのサービスを提供しています。 漏洩したパスワードは平文で、Soliton CSA の分析では 11 桁の数字でした。
Stratfor Global Intelligence 米国	2012 年 2 月	554 万	1,800	ユーザー名 メールアドレス 暗号化パスワード クレジットカード番号 有効期限 セキュリティコード	ハッカー集団 Anonymous が、民間インテリジェンス機関であるストラトフォーの顧客情報を入手し、インターネットで暴露したと公言した事件です。 公開された顧客リストには世界各国の政府機関や企業名が並んでおり、日本大使館や日本貿易振興機構（JETRO）など日本関連の団体、大手電機メーカーや金融機関の社名も含まれていました。

ハッキング被害者	事件発覚年月	Soliton CSA で特定できた漏洩アカウント			備考など
		全漏洩数	『.jp』属性	漏洩内容	
LEET 英国	2016 年 8 月	508 万	7,200	ユーザー名 メールアドレス 暗号化パスワード IP アドレス アクセス履歴	リートはマインクラフト（ブロックを配置して冒険するゲーム）のサーバーを提供するサイトです。 暗号パスワードは SHA512 ハッシュでした。
Yahoo! 米国	2014 年 9 月	500 万	400	メールアドレス 平文パスワード	米国 Yahoo!から、2014 年に 5 億人のユーザー情報が漏洩し、国家関与のハッカー攻撃が疑われると言われた有名な事件です。Soliton CSA では、このうち約 500 万アカウントを特定しています。
ABUSE-WITH.US 米国	2016 年 7 月	410 万	100	ユーザー名 メールアドレス 暗号パスワード	アビューズウィズ・ドットアスは 2013 年に始まったハッキングのオンラインフォーラムです。管理者はハッカーでニックネーム「Xerx3s」を名乗っています。
Adult-Friend-Finder 米国	2015 年 5 月	387 万	830	ユーザー名 メールアドレス 暗号パスワード 生年月日 性別・人種 IP アドレス	米国アダルト・フレンド・ファインダーは、その名の通り、成人向けの出会い系サイトです。この手のサイトの中では米国で最も古くからあると言われています。
NETELLER マン島 (英国)	2015 年？月	362 万	3 万 4 千	口座番号、残高 名前 生年月日 住所 電話番号 メールアドレス	ネッテラーはオンライン金融サービスを提供しています。親会社である Paysafe 社の発表により、この漏洩件数は利用者の 2%未満であることと、パスワードが漏洩していないことが判明しています。
dlh.Net ドイツ	2016 年 7 月	326 万	2,300	メールアドレス 暗号パスワード 平文パスワード 誕生日	DLH ドットネットはゲームニュースやレビュー、オンラインフォーラムを提供しています。一部ユーザーのパスワードは平文で、他は MD5 暗号化パスワードで漏洩しています。
XSplit 香港	2013 年 11 月	298 万	12 万	ユーザー名 メールアドレス 暗号パスワード	X スプリットはユーチューブライブなどのストリーミングプラットフォームに直接生放送するサービスやレコーディングした動画などを簡単にインターネット上にアップロードするサービスを提供しています。

ハッキング被害者	事件発覚年月	Soliton CSA で特定できた漏洩アカウント			備考など
		全漏洩数	『.jp』属性	漏洩内容	
NAUGHTY AMERICA 米国	2016 年 3 月	140 万	2,600	ユーザー名 メールアドレス 暗号パスワード 生年月日	ノーティアメリカはポルノサイトです。漏洩した 380 万アカウントのうち 140 万を特定しました。 米国セキュリティ会社ブログによれば、事件当時、漏洩アドレスとパスワードの MD5 ハッシュが、ダークWeb で 0.7048 ビットコイン（約 3 万円）で販売されていたようです。
Forbes 米国	2014 年 2 月	106 万	450	ユーザー名 メールアドレス 暗号化パスワード ユーザーページ	フォーブスは日本でもよく知られた経済雑誌です。書かれた記事が原因でシリア電子軍（SEA：Syrian Electronic Army）により攻撃を受け、メールアドレスやユーザー登録情報などが漏洩しました。
LIBERO イタリア	2016 年 7 月	90 万	40	ユーザー名 メールアドレス 平文パスワード	リベロはイタリアで無料メールサービスやニュース、オンラインフォーラムをサービス提供しています。 運営会社によると、「他社と同様の攻撃を受けた」とのことです。
BRAZZERS カナダ	2013 年 3 月	79 万	2 千	ユーザー名 メールアドレス 平文パスワード	ブラザースはカナダの大手ポルノ動画サイトです。この事件に前後して、別のポルノ動画共有サイト「YouPorn」から、100 万人分のログイン情報が漏洩した事件もありましたが、まだ特定できていません。
Black Hat World 英国	2014 年 6 月	78 万	110	ユーザー名 生年月日 メールアドレス 暗号化パスワード ユーザーページ Yahoo アドレス MSN アドレス Skype ID	ブラックハット・ワールドは検索エンジン最適化などのインターネットマーケティングサービスやオンラインフォーラムサービスを提供しています。 Yahoo や Skype などの情報も漏洩していました。
Nulled.io 米国	2016 年 5 月	53 万	1,100	ユーザー名 メールアドレス 暗号化パスワード 生年月日 Twitter ID	Nulled.io は、窃取されたユーザーの個人情報や海賊版ソフトウェア、漏洩したコンテンツデータなどを共有するためのアンダーグラウンドのハッカーフォーラムです。
カタール国立銀行 カタール	2015 年 7 月	46 万	60	メールアドレス 氏名 住所 電話番号 口座情報 パスポート番号	カタール国立銀行の Web への SQL インジェクションによる大規模漏洩事件です。カタールの王族、英国 MI6 を含む諜報機関からアルジャジーラまで、様々な顧客のファイルがあったようです。

ハッキング被害者	事件発覚年月	Soliton CSA で特定できた漏洩アカウント			備考など
		全漏洩数	『.jp』属性	漏洩内容	
PS3HAX NETWORK 米国	2015 年 6 月	45 万	1,700	ユーザー名 生年月日 メールアドレス 暗号化パスワード IP アドレス Yahoo アドレス MSN アドレス Skype ID	PS3 ハックスネットワークは、その名の通り、ソニーのプレイステーション 3 のハッキング情報共有サイトです。vBulletin プラットフォームを利用したフォーラムはよく狙われることが分かっています。
acne.org 米国	2014 年 11 月	43 万	280	ユーザー名 生年月日 メールアドレス 暗号化パスワード IP アドレス Twitter ID	アクネはその名の通り、ニキビに関するトリートメント情報を提供する会員サイトサービスです。ユーザーから公開ブログを通じて、漏洩の指摘や個人情報管理に対し、サイト掲載の利用規約の違反だと指摘があった事件です。
TURRENT INVITES 米国	2016 年 8 月	40 万	230	ユーザー名 メールアドレス 暗号化パスワード	トレントインバイトは P2P ソフトであるトレントのオンラインフォーラムのサイトです。vBulletin を利用したフォーラムサイトはよく狙われることが分かっています。
MINE FIELD フランス	2015 年 6 月	19 万	10	ユーザー名 生年月日 メールアドレス 暗号化パスワード IP アドレス Twitter ID	マインフィールドはマルチプレイ地雷探しゲームを提供するサイトです。オンラインマルチプレイ型のマインスイーパー。
musulim match.com 英国	2016 年 6 月	15 万	2	メールアドレス	ムスリムマッチはその名の通り、イスラム教信者向け無料出会い系サイト。『.jp』属性があるとは予想していませんでした。
RuneHQ 中国	2008 年 3 月	8 万	5	ユーザー名 メールアドレス 暗号化パスワード	ルーン HQ は、MMORPG（Massively Multiplayer Online Role-Playing Game）すなわち、同時に大勢が参加するオンラインロールプレイングゲームです。
1394 Store.com 米国	2016 年 6 月	2 万	210	メールアドレス 平文パスワード	1394 ストアドットコムは Firewire や USB 製品を主に映像・医療産業用の専門家にオンライン販売しているサイトです。日本の政府機関である研究開発法人も利用しています。

5. 本年の事件：巨大アカウント情報バックアップの「うっかりミス」

今年に入ってから今まで（2017 年 1 月～8 月）で、最大のアカウント情報漏洩は、恐らく「River City Media」（RCM）の事件でしょう。　漏洩アカウント情報の件数は当初 14 億と報道され、しかも、これらは迷惑メールを送信するために業者が集めていたものでした。　この業者が、迷惑メールのバックアップファイル操作を「うっかりミス」したことで露呈しました [3]。

この事件の始まりは、MacOS を中心とするセキュリティソフト MacKeeper の研究者であるクリス・ビッカリー氏のチームが、2017 年 1 月に不審なファイルを発見したこと。　しかも、このファイルは一般にアクセスできる状態で、パスワードをかけずに保存されていたということです [4]。　実はこのファイルは、RCM が迷惑メール送信用に整理していたアカウント情報のバックアップそのものでした。

この事件の中心である RCM は、表向きは「マーケティング企業」ですが、その実態は、大量の迷惑メールを送り付けている世界最大級の迷惑メール集団だとビッカリー氏は主張しています。そのアカウント情報の出所については、インターネットで会員登録した情報が、本人の知らないうちにアフィリエイトに共有されていたことも考えられると指摘しています。

この巨大な漏洩アカウント情報を発見した MacKeeper のチームは、当ホワイトペーパーの「3.有用な情報を与えてくれる世界の OSINT」でご紹介した SPAMHAUS のチーム、ならびに、CSO オンラインのチーム [5]と協力して、様々な調査分析をすすめました。　その結果、迷惑メール集団 RCM の業務の実態も明らかになったといいます。

分析チームは、RCM の内部でやり取りされていたメッセージの内容から判断して、RCM が大量の迷惑メールを送信するため違法な IP 乗っ取りの手口を使ったり、脆弱性のあるメールサーバを見付けて悪用したりしていたと結論付けています。　この調査分析結果については捜査当局にも通報し、さらに OSINT である SPAMHAUS は、RCM の全インフラをブラックリスト化して阻止する方針を打ち出しました。

[3] http://www.itmedia.co.jp/enterprise/articles/1703/07/news064.html

[4] https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire

[5] http://www.csoonline.com/article/3176433/security/spammers-expose-their-entire-operation-through-bad-backups.html

6. まとめ

当ホワイトペーパー「4.事件別のアカウント情報漏洩分析」の冒頭で、2017 年 8 月現在、この 1 年くらいの世界のハッキング事件について、分かる範囲で調べてみると月平均で 20 件程度が報道されているようだと記述しました。　更に 2010 年以降で、ハッキングによってアカウント情報が盗まれた事件をカウントすると 200 を超えることが分かったとも記載しました。

月平均 20 件の報道ということは、ほぼ全ての営業日に何らかの「アカウント情報漏洩」報道がある計算になりますが、そこまでの実感をお持ちの方はいないものと思います。　欧州や米国で発生したハッキングによって、実は日本に割当てられた『.jp』属性のアカウント情報が、普通にサイバー空間の中に存在していることをご存じない方のほうが多いのではないと考えます。

ソリトンシステムズでは、IT を使って様々な不正調査を実施するチームが活躍しています。　その内容が、社内不正や係争に関わるものが大半であるため広告宣伝してはおりませんが、サイバーセキュリティ事件や、民事・刑事事件も含め、年間数 10 件の多種多様な事案の調査をしています。

東証一部上場企業のお客様で 2 年連続発生した『不正送金事件』を調査したことがありました。　社員が気付かないうちに、日本の銀行口座から海外の口座に大金が送金されていたという事案です。　実はこの事案について、不正侵入や不正プログラム等々、多面的な調査分析を実施したのですが、調査の範囲内において、「普通ではないことや、怪しいと思われる痕跡」が何ひとつありませんでした。

このときの調査報告書の結論は、「正規のアカウント情報が不正に使われている可能性が高い」というものでした。
では、その正規アカウント情報はどうやって漏洩したのか。　それが、社内からではなく、まったく知らない他国で起きたハッキング事件で漏洩していたという可能性も十分に考えられます。　特にパスワードを使いまわしている場合は要注意です。

企業や組織にとっての、アカウント情報漏洩の主なリスクをまとめると以下になるでしょう。

- 誰にも悟られず「不正アクセス」されてしまうリスク
- 「なりすまし」によって業務システムを操作されてしまうリスク
- 「フィッシング詐欺の加害者」として企業名や組織名を利用されてしまうリスク

このホワイトペーパーの続編では、「組織属性別の被害」の調査分析結果を公開します。

【著者】株式会社ソリトンシステムズ　執行役員　長谷部泰幸

Soliton Systems Security White Paper 2017
世界のハッキング事件による日本のアカウント情報漏洩分析― 1
～事件別の被害

発行　初版 2017 年 8 月 8 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
記載されている会社名、製品名またはサービス名は各社の商標または登録商標です。
無断転載、無断複製、無許可による電子媒体等への入力を禁じます。