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－2
～組織属性別の被害

Soliton

はじめに

ホワイトペーパー前作（2017 年 8 月 8 日発行の「事件別の被害」）の冒頭で、2016 年 12 月に登場した巨大なアカウント情報リスト「アンチパブリック・コンボリスト」と、それを分析した 2017 年 5 月 11 日の記事の存在をご紹介しました [1]。

このコンボリスト調査分析の詳細に関するブログ [2]では、漏洩アカウントに付随する電子メールアドレスのドメインに関する分析と、漏洩した平文パスワードの分析も公開されており、いずれもランキング情報が手に入ります。　パスワードについては、有名なパスワード管理システム『keeper』が発表する「世界でよく使われるパスワード・トップ 100」との比較もされていて、結論として、「123456」や「123456789」というパスワードがいかに危険であるかを具体的に示しています。

この調査分析の公開情報を、少し異なる視点で再計算すると、ドイツやフランス、英国については、「国としての」被害に関する具体的な知見が得られます。　調査分析のアナリスト達とは異なる切り口でのインテリジェンスです。　例えばドイツの場合、ドメイン名「web.de」を属性とする漏洩アカウント数が約 1,350 万であることや、それ以外のドメイン名である「gmx.de」「yahoo.de」「lycos.de」「epost.de」も含めた合計の漏洩アカウント数が約 4,508 万にも及んでいることが試算できます。　ドイツの人口が約 8,100 万人であることを鑑みると、たったひとつの「アンチパブリック・コンボリスト」に含まれる漏洩アカウントの影響度がいかに大きいかを推し量ることができます。

世界中で起きているハッキング事件については、上記のような調査分析記事が数多く出回っています。　世界中の Web メディア、ブログやニュースレター、新聞などあらゆるメディアに漏洩アカウントの調査分析記事が掲載されています。　ただ、残念なことに、それら分析記事の中で「日本の被害」が取り上げられることはまずありません。　当ホワイトペーパーは「日本」の漏洩アカウントだけを焦点とした調査分析を目的としています。

1. サイバー犯罪による国別被害状況と日本

日本の組織属性別分析の前に、サイバー犯罪の経済的被害に関して、世界の中で日本がどういう位置にあるのかについて触れておきます。　ここでは、米国の戦略国際問題研究所（CSIS）が米国マカフィーと共同調査し、2014 年 6 月に公表した「Estimating the Global Cost of Cybercrime[3]」から、他国との比較における日本の位置を確認します。

CSIS の調査レポートによれば、2014 年の調査時点で、世界で最も深刻なサイバー犯罪の経済的被害を被っているのはドイツとオランダです。　ドイツの GDP は日本に次ぐ世界第 4 位、オランダのそれは第 18 位。　GDP 世界 1 位の米国と 2 位の中国がそれに続く影響度となっています。　日本の位置は下表の通りで、極めて低いといえます。

国名	サイバー犯罪影響度（対 GDP）	GDP 影響度比較（日本＝ 1 の場合）
ドイツ	1.60％	80.0
オランダ	1.50％	75.0
米国	0.64％	32.0
中国	0.63％	31.5
シンガポール	0.41％	20.5
日本	0.02％	日本＝ 1 とする

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

[2] https://duo.com/blog/a-security-analysis-of-over-500-million-usernames-and-passwords

[3] https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf

2. 日本の組織属性別ドメイン

調査分析の対象は「日本の組織属性」ですが、日本の会社や団体などによっては「.com」「.net」といった属性のドメインをご利用のところもあるでしょう。　全ての日本の組織を網羅するのは事実上不可能ですので、ここでは、株式会社日本レジストリサービス（JPRS）が登録管理を行っている「.jp」ドメインを調査分析のキーとしました。　JPRS によると「.jp」ドメインを登録できるのは「日本国内に住所を持つ組織・個人・団体[4]」です。

ドメイン	組織属性の種別
CO.JP	日本国内で登記を行っている会社。 ● 株式会社、有限会社、合同会社、合名会社、合資会社、相互会社など ● 信用金庫、信用組合、外国会社（日本で登記していること） ● 有限責任事業組合、企業組合、投資事業有限責任組合
NE.JP	日本国内のサービス提供者によるネットワークサービス用のドメイン。 1 サービスごとに 1 ドメイン名を登録可。
OR.JP	以下の法人組織が登録できるドメイン。 ● 財団法人、社団法人、医療法人、監査法人、宗教法人、特定非営利活動法人 ● 特殊法人、農業協同組合、消費生活協同組合など ● 国連等の公的な国際機関、国連 NGO やその日本支部、外国政府の在日公館など
AC.JP	高等教育機関、学術研究機関などのドメイン。 ● 大学、大学校、高等専門学校、大学共同利用機関などの学術研究機関 ● 学校法人、職業訓練校、職業訓練法人
GR.JP	個人や法人により構成される任意団体が登録できます。
ED.JP	初等中等教育機関および 18 歳未満を対象とした教育機関のドメイン。 ● 保育所、幼稚園、小学校、中学校、中等教育学校、高等学校 ● 盲学校、聾学校、養護学校、専修学校、 ● 各種学校のうち、主に 18 歳未満を対象とするもの
AD.JP	JPNIC 会員となっている組織が登録できます。
GO.JP	日本の政府機関や各省庁所管の研究所、特殊法人、独立行政法人が登録できます。 政府機関は、一つの組織で複数の GO.JP ドメイン名を登録できます。
LG.JP	地方公共団体と、それらの組織が行う行政サービスが登録できます。
.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。

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）で特定された漏洩アカウンドが、例えば「xxx.yyy@mail.zzz.ac.jp」のように末尾が『ac.jp』だった場合には、このアドレスが大学や高専、学術研究機関といった高等教育機関で利用されているものであることが分かります。

[4] https://jprs.jp/about/jp-dom/spec/

3. 組織属性別のアカウント情報漏洩分析

ホワイトペーパー前作（2017 年 8 月 8 日発行の「事件別の被害」）で記載した通り、2017 年 8 月現在で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）が特定できた漏洩アカウント数は約 20 億です。　世界には、私たちと同様にオープン・ソース・インテリジェンス手法を使って、様々なハッキング事件で漏洩したアカウント情報を公開情報から特定している人達がいます。　例えば、マイクロソフトのオーストラリア法人のディレクターである Tony Hunt 氏が、彼の運営サイト『';--have i been pwned?[5]』で、漏洩が判明したアカウント数を公開していますが、2017 年 8 月現在で約 40 億です。

特定した『.jp』の漏洩アカウント数は 988 万

Soliton CSA 基盤を使って、特定できたハッキング事件のデータから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を含むアカウント情報の漏洩数をカウントすると、約 1,120 万となりました。　ただ、同じ電子メールアドレスが別のハッキング事件でも漏洩しているものを名寄せし、出来る限りの重複排除を実施した結果、2017 年 8 月現在で特定した漏洩アカウント数は約 988 万となりました。

下表が調査分析結果の全体像です。　漏洩アカウントのうち半数以上が『co.jp』、即ち企業・会社（法人）の属性となっています。　約 3 割が国内ネットワークサービスである『ne.jp』ですので、この 2 つの組織属性の漏洩アカウントだけで全体の 82%を占めるという分析結果となりました。　ここに、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 93%を占めることになります。

ドメイン	組織属性の種別	Soliton CSA で特定した漏洩アカウント数	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	5,036,204	50.98%
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	3,035,103	30.72%
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	325,615	3.30%
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	200,962	2.03%
GR.JP	個人や法人により構成される任意団体	7,914	0.08%
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	5,989	0.06%
AD.JP	JPNIC 会員となっている組織	4,105	0.04%
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	14,720	0.15%
LG.JP	地方公共団体 それらの組織が行う行政サービス	4,499	0.05%
.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	1,244,419	12.60%

[5] https://haveibeenpwned.com/

『.jp』の漏洩アカウントの電子メールアドレスのサブドメイン数は約 38 万

約 988 万の漏洩アカウントに附帯する電子メールアドレスの最もシンプルな構成表記は「名前@サブドメイン.jp」です。　この表記では、@（アットマーク）以降を「サブドメイン」と記述します。　このサブドメインは、「soliton」のように、その組織名を単純表記しているものもあれば、「metro.tokyo」のように、2 語の組合せで組織名を表記するもの、3 語以上の組合せで何らかの分類を実施しているものなど、様々です。

Soliton CSA で特定できた約 988 万の漏洩アカウントの電子メールの「属性」となるサブドメイン数は約 38 万でした。　単純な割り算で、漏洩アカウントはサブドメイン当りの平均で 26 程度あるということになります。

なお、『.jp』ドメインを管理する株式会社日本レジストリサービス（JPRS）は、毎月、登録ドメインの数を公表しており、それによると、2017 年 8 月 1 日現在のドメイン総合計は 1,478,575 となっています。[6]　この数には約 100 万の汎用 JP ドメインが含まれており、属性型・地域型 JP ドメイン名は約 47 万です。　当ホワイトペーパーでは「サブドメイン」を単位にしていますので、この統計との単純比較はできませんが、属性型・地域型 JP ドメインの数が約 47 万の国で、約 38 万のサブドメインが関連する漏洩アカウントが特定できたことは、分析者の予想をはるかに上回っています。

4. 重要組織のアカウント情報漏洩分析

ドメインを用いた調査分析で、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、特定できた約 988 万のアカウントと、その属性である約 38 万のサブドメインを使って、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、個別調査を実施したのは以下の 3 つのキーワードで分類される組織です。

1. 政府機関：　『go.jp』ドメインを持つもの
2. 地方公共団体：　『lg.jp』ドメイン、または、都道府県型 JP ドメインを持つもの
3. 重要インフラ：　政府が「重要インフラの情報セキュリティ対策に係る第 3 次行動計画[7]」で定めた業種

上記の一部に関する詳細な調査分析結果については、関係機関に通報するとともに、既に個別の調査報告書を提出しました。

政府機関のアカウント情報漏洩分析

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、衆議院や参議院でも利用されてれています。さらに、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おり、2017 年 8 月 1 日現在の JPRS での『go.jp』ドメイン登録数は 582 となっています。　前述の通り、漏洩が特定できた『go.jp』アカウント数は 14,720 で、特定した全体の漏洩数の 0.15%でした。　人事院の公開資料[8]に平成 29 年度の国家公務員数がありますので、これらを全て比較できる様に下表にまとめます。

属性	比較対象	調査結果		
		ドメイン数	サブドメイン数	アカウント数
GO.JP	全数	582	（不明）	（不明） ※国家公務員は約 584,000
	Soliton CSA で 特定できた漏洩アカウント	178	929	14,720

6 https://jprs.jp/about/stats/registered/

7 https://www.nisc.go.jp/active/infra/pdf/infra_rt3_r1.pdf

8 http://www.jinji.go.jp/booklet/booklet_Part5.pdf

主要ハッキング事件別の政府機関アカウント情報漏洩数ランキング

ホワイトペーパー前作（2017 年 8 月 8 日発行の「事件別の被害」）では、世界中で発生したハッキング事件ごとに特定できた漏洩アカウント数をまとめました。　政府機関の漏洩アカウントについて詳細分析を実施すると、その政府機関ならではの特徴が見てとれます。

例えば、米国の民間インテリジェンス機関であるストラトフォー（Stratfor Global Intelligence）がハッカー集団 Anonymous に顧客情報を奪われ、インターネット上で暴露された事件では、「民間インテリジェンスを必要とするであろう政府組織」の漏洩アカウントが数多く見つかっています。　また、特定分野の専門装置のオンラインショップである 1394 Store.com のハッキング事件での漏洩アカウントには、国立研究開発法人のものが多く見つかりました。

以下では、国内でもユーザーが多い 3 つのサービスがハッキング被害を被った事件について、漏洩アカウント数の多い政府機関のランキングを調査分析しました。　そもそも政府機関によって職員の数、即ち保有するアカウント数がまったく異なりますから、漏洩アカウントの絶対数のランキングが持つ意味はそれほど深刻なものではないと考えます。ここでも政府機関ならではの特徴が現れています。

ハッキング被害者	被害者のサービス	Soliton CSA で特定できた漏洩アカウント		政府機関のアカウント情報漏洩数ランキング（多い順）
		全ての『.jp』属性	漏洩内容	
Adobe 米国	デザイン／イメージング／出版用ソフトウェア	294 万	アカウント ID メールアドレス 暗号化パスワード パスワードのヒント	①　産業技術総合研究所 ②　農林水産研究情報総合センター ③　日本原子力研究開発機構
Linked In 米国	ビジネスに特化したソーシャルネットワーク	15 万	メールアドレス 暗号化パスワード	①　国際協力機構 ②　産業技術総合研究所 ③　外務省
DropBox 米国	共同作業用のオンラインストレージサービス	110 万	メールアドレス 暗号化パスワード	①　産業技術総合研究所 ②　農林水産研究情報総合センター ③　国立病院機構

全てのランキングに登場する国立研究開発法人 産業技術総合研究所は、日本最大規模の公的研究機関ですので、アカウント絶対数の多いことが影響しているものと思われます。　Linked In の漏洩アカウントランキングに登場する独立行政法人 国際協力機構（JICA）や外務省については、海外の人たちとのコミュニケーションツールとして、世界で 3 億人以上が登録するという Linked In を利用していたことが推察できます。

地方公共団体のアカウント情報漏洩分析

地方公共団体やそのサービスに割り振られる『lg.jp』ドメインは、2017 年 8 月 1 日現在の JPRS 登録数が 1,883 となっています。　前述の通り、漏洩が特定できた『lg.jp』アカウント数は 4,499 で、特定した全体の漏洩数の 0.05%でした。　この『lg.jp』ドメインで、漏洩が確認できたサブドメイン数は 815 ありますので、単純な割り算では、サブドメインあたり平均で 5.5 アカウントの情報が漏洩している計算になります。

属性	比較対象	調査結果		
		ドメイン数	サブドメイン数	アカウント数
LG.JP	全数	1,883	（不明）	（不明）
	Soliton CSA で 特定できた漏洩アカウント	N/A	815	4,499

地方公共団体については、「都道府県型 JP ドメイン [9]」についての個別具体的な調査分析が必要だと思われます。　この都道府県型ドメインは、株式会社日本レジストリサービス（JPRS）が 1993 年 12 月に登録を開始し、2012 年 3 月末に新規受付を終了した「地域型 JP ドメイン」を改善したもの。　例えば、東京都であれば「AAA.tokyo.jp」、北海道なら「BBB.hokkaido.jp」といった具合に、47 都道府県を第 2 レベルとし、第 3 レベルに任意の文字列を登録可能なドメイン名です。

都道府県型 JP ドメインだけでは地方公共団体被害の全体分析は難しい

例えば、東京都のホームページのドメインは都道府県型 JP ドメインである「metro.tokyo.jp」です。　それに対し、大阪府ホームページのドメインは、地方公共団体の LG.JP 属性ドメインである「pref.osaka.lg.jp」となっています。　また、都道府県型 JP ドメインは、地方公共団体に限らず、その地域発・地域向けの情報提供を目的とした組織・個人であれば登録できますので、「個別に指定された調査対象ドメイン」でないと詳細な分析は困難です。

JPRS の 2013 年 3 月 4 日の発表によると、「都道府県型 JP ドメイン名」の 2013 年 3 月 1 日現在の累計登録数が 1 万件を突破し、11,078 件となったとのことです [10]。　この発表において、登録数の多い 5 つの都道府県型 JP ドメイン名の登録数が公開されていますので、その数字との比較において、Soliton CSA が特定できた漏洩アカウントが所属する都道府県型 JP ドメイン数をまとめます。

属性	地域	サブドメイン		
		ドメインの表記	JPRS 登録数 （2013 年 3 月発表）	漏洩が特定できたドメイン数 （2017 年 8 月）
都道府県型 JP	東京	○○○.tokyo.jp	2,426	117
	大阪	○○○.osaka.jp	724	84
	京都	○○○.kyoto.jp	484	33
	福岡	○○○.fukuoka.jp	395	56
	北海道	○○○.hokkaido.jp	333	115

9 https://jprs.co.jp/press/2011/110926.html

10 https://jprs.co.jp/press/2013/130304.html

重要インフラとは何か

ここでの「重要インフラ」の定義は、以下の内閣サイバーセキュリティセンター（NISC）の表現[11]をそのまま以下に記載します。

“「重要インフラ」とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものをいいます。”

具体的な業種として、2017 年 8 月時点では以下の 13 分野が指定されています。

重要インフラ 13 分野	所管省庁
情報通信	総務省
金融	金融庁
航空	国土交通省
鉄道	国土交通省
電力	経済産業省
ガス	経済産業省
政府・行政サービス（地方公共団体を含む）	総務省
医療	厚生労働省
水道	厚生労働省
物流	国土交通省
化学	経済産業省
クレジット	経済産業省
石油	経済産業省

[11] https://www.nisc.go.jp/active/infra/outline.html

重要インフラのアカウント情報漏洩分析

「重要インフラ」の 13 業種に関するアカウント情報漏洩の全体像を調査分析することを考えると、これら業種に所属する事業者が多すぎます。　「重要インフラ」の被害の全体像を見るには、個別事業者の詳細分析を積み重ねる必要があります。　そこまでの個別調査分析をしなくても、私たちが直面している現実のスナップショットを見る分には、いくつかサンプル調査を実施すれば良いと考えました。　ここでは、重要インフラ 13 分野のサンプル調査分析結果を記載します。

重要インフラ 13 分野に所属する事業者について、全部で数 10 社をサンプルとして取り上げ、これまでに特定した 988 万の漏洩アカウントの中に、そのサンプル事業者のドメイン名があるか否かを調査した結果が下表です。

重要インフラ	サンプル調査対象	サンプル事業者のドメイン調査結果
情報通信	グループ企業を含む通信事業者 8 社	8 社全てに漏洩アカウントあり
金融	銀行 3 行＋証券 5 社	全てに漏洩アカウントあり
航空	航空会社 2 社	2 社とも漏洩アカウントあり
鉄道	グループ企業を含む鉄道 22 社	22 社全てに漏洩アカウントあり
電力	電力会社 10 社	10 社全てに漏洩アカウントあり
ガス	都市ガス 4 社	4 社全てに漏洩アカウントあり
政府・ 行政サービス	GO.JP ドメインの組織・サービスと LG.JP ドメインの組織・サービス	当ホワイトペーパーに記述 (178 の GO.JP ドメインなど)
医療	国内製薬メーカー5 社	5 社全てに漏洩アカウントあり
水道	某都市の水道局、下水道局	水道局はあり、下水道局は見当たらない
物流	物流 4 社	4 社全てに漏洩アカウントあり
化学	化学業 3 社	3 社全てに漏洩アカウントあり
クレジット	国内信販企業 2 社	2 社とも漏洩アカウントあり

これまで特定できたハッキング事件での漏洩アカウントには、某都市下水道局のドメインを除き、重要インフラ 13 業種のサンプル事業者全てのドメインが含まれていたということが判りました。

上記サンプルのうち、「鉄道」から 1 社を選び、少し具体的に掘り下げてみます。　鉄道事業者数は、国土交通省の統計情報によると、平成 28 年 4 月 1 日現在で、ＪＲグループ 6 社の他、大手私鉄 16 社、準大手私鉄 5 社など 200 以上あります[12]。　このうちのひとつの会社をサンプルとして取り上げ、どのハッキング事件からアカウント情報が漏洩したかについて調査分析してみました。　その結果は下表となります。

事件	Soliton CSA で特定できた漏洩アカウント概要		対象鉄道会社ドメインで 特定した漏洩アカウント数
	全ての『.jp』属性の数	パスワードの状態	
Exploit.In	61 万	平文	6
AntiPublic	452 万	平文	11
Adobe	294 万	暗号化	25
Linked In	15 万	暗号化	14
NETELLER	3 万	なし	1

[12] http://www.mlit.go.jp/common/001137390.pdf

5. まとめ

私たちが知らないところで、私たちのアカウント情報が盗まれ、しかもサイバー空間上に漂っている。

このことに対し、ある程度のリアリティを持って認識していただくために、日本独自の『.jp』を持つ組織属性別の分析結果を公表いたしました。　個別の組織の、個別の漏洩アカウントや、附帯する電子メールアドレス、個別のパスワード状況に対する分析結果を公表するわけにはいきませんので、できるだけ具体的な数字の分析や、組織名、ドメイン名といったレベルまでの分析で留めています。

もちろん、弊社（ソリトンシステムズ）の漏洩アカウント情報は詳細調査を実施済みです。　その調査結果は、社内の情報セキュリティ委員会に報告され、既に必要な対応アクションが実施されています。

サイバーセキュリティ分析の専門家の中には、Soliton CSA のような、OSINT（オープン・ソース・インテリジェンス）手法で入手した調査分析には、あまり価値がないという立場の方もいるようです。　Dark Web と呼ばれる、いわゆる「闇サイト」に入り込まないと、本当に重要な情報は得られないという考えです。　確かに、例えばクレジットカードや法人銀行口座に関連するアカウント情報や、人気のある Facebook や Instagram の盗まれたアカウント情報などは、違法性の高い「闇サイト」を活用しなければ調査できそうにありません。　ただ、「闇サイト」は、アカウント情報云々よりも、薬物や武器の販売、さらには人身売買の取引空間でもありますので、その調査は私たち民間企業ではなく、法執行機関の守備範囲であると考えています。

ここで言う価値の有無は、その情報の「販売価値」のことを示しているという側面もあるようです。　調査分析の結果に価値があるか否かは、分析の専門家が決めることではなく、その組織のマネジメントが決めることです。　組織のマネジメントが『現状を把握すること』に価値を見出すか否か。　これが重要です。

サイバーセキュリティは、あまりにも技術的要素が前面に出ているため忘れがちですが、組織のマネジメントにとっては、「リスク管理または危機管理」の対象のひとつにすぎません。　組織のリスク管理・危機管理を効果的に実現するための活動項目分類のひとつの考え方として、下記の 4 分類があります。

1. 現状を把握する　：内部要因調査・外部環境変化の把握・診断による把握
2. 防ぐ手段を講じる　：リーダーシップ・基準/ルール策定・教育・評価システム・懲罰
3. リスクを発見する　：内部/外部監査・内部通報/アラート・モニタリング
4. 対処する　：対処体制構築・対処マニュアル・外部専門家の活用

現状を把握できているからこそ、防ぐ手段やリスク発見策の優先順位を決めることができますし、適正な投資判断も可能となるものと考えています。

【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－２
～組織属性別の被害

発行　初版 2017 年 8 月 15 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