情報漏洩が大学に与えるセキュリティリスク

宇田川　暢

新潟大学 学術情報基盤機構 情報基盤センター

udagawa@cais.niigata-u.ac.jp

A Consideration on Information Leakage Causing a Threat against Japanese Universities

UDAGAWA Mitsuru

Center for Academic Information Service, Niigata Univ.

概要

2020 年に発生した 2 つセキュリティインシデントについて分析し、それらが日本国内の大学へ与える影響について考察する。片方は大学と直接関係のないサービスからのユーザ情報漏洩であり、不適切に保存されたパスワードが引き起こすリスクを、もう片方は適切に管理されていない VPN 装置の脆弱性を利用したアカウント漏洩からの内部ネットワーク侵入によるリスクを検討する。

1 はじめに

2020 年に 2 つのセキュリティインシデントが発生した。各インシデントについての説明と、漏洩した情報が大学の情報システムについてどのような影響を及ぼす可能性があるかの考察を行う。

2 インシデント 1：Peatix の情報漏洩

2.1 Peatix について

Peatix[1]はイベントやチケットの管理を行うことができるイベントプラットフォームで、アメリカに本社を持ち、日本国内にも日本法人が存在している。イベントを開催したいと思っている主催者は、イベントプラットフォームを利用することで、イベント概要説明サイト作成と参加者の管理、イベント参加費の徴収を一元的に行うことができる。

2.2 Peatix からの情報漏洩の発生

2020 年 11 月 17 日、Peatix の日本法人 Peatix Japan は、不正アクセスにより登録された利用者情報が漏洩したと発表した[1]。発表によると漏洩した情報は氏名、メールアドレス、暗号化されたパスワードなどのユーザアカウント情報について、最大 677 万件となっている。

本インシデントについての調査報告が 2020 年 12 月 16 日に公表された[2]。インシデントは 2020 年 10 月 16 日から 17 日にかけて発生し、不正アクセスの具体的な手段については特定不能であると報告されている。

2.3 漏洩したパスワードの不正利用疑い

2021 年に入り、メールアカウントへの不正アクセスによる迷惑メール送信のインシデントが、2020 年 11 月 27 日から 30 日にかけて発生していたことが愛媛大学から公表された[3]。

発表された内容の中に、「学外のイベント管理サービスに登録していた本学の学部用メールアドレス利用者のメールアカウントとパスワードが、同サービス運営会社が第三者による不正アクセスを受けた際に流出し、窃取されたものと推測されます。」という一文が記載されている。

時期的に Peatix のインシデントとの関連が疑われるが、Peatix の発表内容によると、漏洩情報に含まれるパスワードについて、暗号化されているとなっていたため、なぜ不正に利用することが可能であったかという疑問が生まれる。

3 Peatix の漏洩内容と暗号化パスワード

3.1 Peatix からの漏洩内容

暗号化されたパスワードの問題について確認するため、漏洩したとされる情報を入手して解析することとした。

Peatix から漏洩したアカウントと思われるファイルは、925,806,592 バイトの MySQL ダンプで、

[1] https://peatix.com/

最後が破損したバックアップであった。最後に記録されていた破損した無効な SQL 文を削り、データベースにリストアしたしたところ、以下のような概要であった。

・総レコード数： 4,347,461
・最終アカウント作成： 2019-01-20 23:09:58
・最終アカウント更新： 2020-10-16 23:46:13

この内容から、Peatix を利用していたユーザ情報のうち、2019 年 1 月 20 日迄に作成されたアカウントが漏洩していることがわかる。全ユーザ分のダンプをデータベースから作成または転送中に、なんらかの理由で処理が中断され、この部分までの情報漏洩となったと推測される。また、アカウント情報が更新された最新のレコードが 2020 年 10 月 16 日であったことから、調査報告において記載されたインシデント発生のタイミングと符合する。

ただし、この情報は Have I Been Pwned に掲載[4]されている、漏洩アカウント数 4,227,907 件という情報と件数が異なっている。

3.2 暗号化（ハッシュ化）されたパスワード

このデータベースには”password”というカラムがあり、そこに”{SSHA}”から始まる文字列が記録されている。SSHA は Salted SHA-1(Secure Hash Algorithm-1)を意味し、パスワード文字列にソルトを付与したものを SHA-1 でハッシュ化し、得られた 20 バイトの文字列にソルトを追加して Base64 形式でエンコードしたものが保存されている。

パスワードをハッシュ化する前にソルトを付与することで、同じパスワードでも異なる値を生成することが可能となる。また、ハッシュ化後にもソルトを追加しているのは、パスワード文字列が一致するかの比較時に必要なためである。

このカラムには”{SSHA}”の後に 32 文字の文字列が記録されていることから、4 バイトのソルト付き SHA-1 ハッシュであるとわかる。

SHA-1 のようなハッシュ関数は、パスワードなどから一方向にのみ計算可能なハッシュ値を得られるものである。

3.3 総当たりによるパスワードの解析

ソルト付きハッシュ形式で保存されたパスワードであれば、たとえ漏洩したとしても、不正に利用される危険性は無いように感じられる。しかしながら、総当たり攻撃によって元のパスワードを解析される可能性が存在する。

例えば、パスワードに使える文字をアルファベットの大文字と小文字、数字および記号 2 種類とすると、パスワード 1 文字当たり 64（≈2^6）通り、パスワード長が 8 文字の場合は 2^{48} 通りのパスワードとなる。ここで 1 秒あたり 10 億回 SHA-1 ハッシュを計算できるコンピュータで総当たりによる解析を行った場合、10 億≈2^{30} であることから、解析に必要な時間は最大で 2^{18} 秒≈3 日となる。

パスワードが 9 文字になると約 194 日、10 文字であれば約 34 年と指数関数的に総当たりに必要な計算時間が増加する。つまり、パスワード長が十分でない場合、パスワード解析が現実的なリスクとなりうる。

3.4 パスワード解析による実証

今回入手できたデータが Peatix からの漏洩データであるとの仮定のうえ、大学メールアドレスとのパスワードの使い回しにより、愛媛大学で発生したような不正アクセスの危険性があるとの立場に立ってパスワード解析を試みる。

4,347,461 アカウントのうち、”.ac.jp”で終わるメールアドレスのアカウントは 20,165 件であった。Peatix ではアカウントに Google などの SSO を利用してログインすることも可能で、その場合はパスワードを保存していないようである。”password”カラムが空のレコードを除いて絞り込むと、12,466 件となった。なお、第 3 レベルドメインで集計すると、1,090 ドメインとなった。ただし、この数にはメールアドレス登録時に誤入力したと見られるものも含まれている。

これらのアカウントについて、表 1 のコンピュータで hashcat[2]によるパスワード解析を試行した。このコンピュータでは SHA-1 ハッシュの計算を 1 秒あたりおよそ 84 億回行うことが可能である。

表 1　パスワード解析用コンピュータ

CPU	AMD Ryzen 5 5600X
メモリ	64GB
GPU	GeForce RTX 3060Ti
OS	Fedora 33
GPU Driver Version	460.32.03
CUDA Version	11.2
hashcat Version	6.1.1
SHA-1 解析の性能	約 84 億ハッシュ/秒

hashcat は特定の機能を持つ CPU や、GPGPU を用いてパスワード解析を行うためのソフトウェアであり、総当たりやパスワードマスクを用いた解

析にも対応している。今回利用した解析用コンピュータの CPU では hashcat で利用することができないため、GPU のみの利用となっている。

本論文では、計算時間の削減のため、8 文字以下の総当たり攻撃とし、パスワードマスクに hashcat デフォルトのパターン(表 2)を利用した。表 3 に示すように、パスワードマスクを利用することで大幅に計算量と計算時間を削減することが可能となるが、代わりにパターン外のパスワードについては取りこぼすことになる。

表 2　デフォルトのパスワードマスク（8 文字時）

1 文字目	アルファベット大文字 アルファベット小文字 数字
2 文字目～7 文字目	アルファベット小文字 数字
8 文字目	アルファベット小文字 数字 記号 [*!$@_,]

表 3　総当たりの試行回数・時間比較（SSHA）

パスワード長	全パターン	マスクあり
7 文字	$2^{45.99}$ 回 約 2.3 時間	$2^{36.97}$ 回 約 16 秒
8 文字	$2^{52.56}$ 回 約 9.1 日	$2^{42.33}$ 回 約 11 分
9 文字	$2^{59.13}$ 回 約 2.4 年	$2^{47.69}$ 回 約 7.5 時間

※パスワードマスクはデフォルト、試行速度は毎秒 84 億回

3.5 解析結果

65 日に渡るパスワード解析の結果、12,466 件中、4,808 件（38.6%）のパスワードが解析された。つまり 38.6%のパスワードが典型的なパターンと思われるパスワードマスクに適合するものであったことになる。8 文字未満のパスワードが確認されなかったことから、現在確認することはできないが、漏洩インシデント以前のパスワードポリシーは 8 文字以上であれば文字種などに制限はなかったと推測される。

解析されたパスワードは表 4 のような特徴を持っている。なお、pwscore[3]での評価時にはユーザ名として 16 文字のダッシュを使用し、パスワード中にユーザ名が含まれると評価されないようにした。

表 4　パスワード解析結果（重複あり）

パターン	該当数
数字のみ	593
アルファベット小文字のみ	504
アルファベットのみ	512
アルファベットと数字のみ	4,785
使用している文字が 1 種類	19
使用している文字が 2 種類	21
使用している文字が 3 種類	92
使用している文字が 4 種類	260
使用している文字が 5 種類	540
使用している文字が 6 種類	1,142
使用している文字が 7 種類	1,645
使用している文字が 8 種類	1,089
アルファベット 1 文字＋数字 7 文字	65
アルファベット 2 文字＋数字 6 文字	216
アルファベット 3 文字＋数字 5 文字	113
アルファベット 4 文字＋数字 4 文字	1,280
アルファベット 5 文字＋数字 3 文字	278
アルファベット 6 文字＋数字 2 文字	437
アルファベット 7 文字＋数字 1 文字	233
数字 1 文字＋アルファベット 7 文字	17
数字 2 文字＋アルファベット 6 文字	32
数字 3 文字＋アルファベット 5 文字	25
数字 4 文字＋アルファベット 4 文字	181
数字 5 文字＋アルファベット 3 文字	13
数字 6 文字＋アルファベット 2 文字	42
数字 7 文字＋アルファベット 1 文字	33
pwscore のチェックで問題あり	1,363
cracklib の辞書の単語を含む	683

4 インシデント 2：VPN 装置の情報漏洩

4.1 FortiGate について

2020 年には、Fortinet 社製 UTM（統合脅威管理）製品である FortiGate の一部ファームウェアの脆弱性についてもインシデントが発生している。同製品は、いわゆる次世代ファイアウォールの他、VPN 接続のための装置としても利用できる。

[2] https://hashcat.net/hashcat/

[3] https://github.com/cgwalters/libpwquality-git

4.2 FortiGate の脆弱性

2019 年 8 月の Black Hat USA 2019 において、DEVCORE 社のセキュリティ研究者により、複数の SSL VPN 装置の脆弱性が紹介された[5]。

ここで紹介された FortiGate の脆弱性は

(1) ディレクトリトラバーサルにより、認証なしで任意のファイルの内容を表示可能（CVE-2018-13379）
(2) 認証なしでヒープオーバーフローによる任意コード実行が可能（CVE-2018-13381）
(3) 非公開のパラメータを指定することで、認証なしで任意にパスワードリセットが可能（CVE-2018-13382）

というものであった。

また、既にこの脆弱性を修正するアップデートプログラムが配布されていることについても言及されている。

日本国内では本脆弱性情報について、2019 年 9 月に JPCERT/CC により他社製 SSL VPN 装置の脆弱性情報とともに、注意喚起がなされている[6]。注意喚起の中で、脆弱性を利用しての情報窃取目的とみられるスキャン行為が観測されている旨が記載されており、この時点で既に脆弱性による情報漏洩リスクが顕在化していた。

4.3 脆弱性を持つ VPN 装置リストの公開

脆弱性情報の公開からおよそ一年後の 2020 年 11 月に、ディレクトリトラバーサルの脆弱性が未修正の VPN 装置の URL リスト（以下、URL リスト）が海外のフォーラムに掲載された[7]。URL リストには、ログイン情報が平文で記載された VPN 装置上のファイル（クレデンシャル情報）にアクセス可能な IP アドレスベースの URL が 49,577 件記載されているものであった。

また、その数日後には同じフォーラムにリストの URL から取得したファイルを集めたアーカイブ（以下、クレデンシャルリスト）も公開された。すなわち、脆弱性への対応がなされていなかった VPN 装置の IP アドレスと対になる、アカウント情報がリストとして公開されたことになる。

5 公開された VPN 装置のリスト

5.1 公開された IP アドレスリストの分析

URL リストに対し、GeoIP データベースを用いて、当該 IP アドレスがどの国のどの組織に割り当てられたものか調査することにした。

GeoIP データベースは Maxmind 社[4]が提供する IP ジオロケーションサービスで、当該 IP アドレスが割り当てられた組織名や ASN(Autonomous Network Number)、都市程度の場所まで把握することが可能となる。ただし、詳細な情報が含まれたデータベースは有償での提供となっている。

GeoIP データベースについて、今回は無償で提供されている GeoLite2 Country データベースを利用し、また、URL リストが作成されたであろう時期を跨ぐ 2020 年 8 月 11 日と、2021 年 6 月 8 日の GeoLite2 Country データベースで結果を比較することとした。

URL リストに国と組織名、ASN およびクレデンシャルリストのファイルサイズを加えたリスト（以下、分析用リスト）を作成し、両 GeoLite2 Country データベースの結果を比較したところ、2 つの IP アドレスについて、2021 年 6 月 8 日のデータベースでは新たに日本国内において利用されている IP アドレスとなっていた。しかしながら、他の IP ジオロケーションサービスである ipinfo.io[5]や DBIP[6]では日本国外であると表示されたため、2020 年 8 月 11 日の GeoLite2 Country データベースの結果のみを採用することとした。本来であれば全ての IP アドレスについて、複数の IP ジオロケーションサービスを利用して評価すべきであるが、本論文では解析時間の削減のため、GeoLite2 Country データベースのみの利用とした。集計した結果は表 5 となった。

表 5　URL リスト分析結果

パターン	該当数
全 IP アドレス	49,562
有効なクレデンシャル	33,894
日本国内の IP アドレス	5,476
日本国内 IP＋有効なクレデンシャル	2,767

表 5 では全 IP アドレスで 49,562 件となっており、URL リストの 49,577 件と比較すると 15 件ほど少なくなっている。これは URL リストに IP アドレスの重複があったためであり、ユニークな IP アドレスは 49,562 件となる。

また、クレデンシャルリストのうち、ファイルサイズが 100kB を超えているものを有効なクレデ

[4] https://www.maxmind.com/
[5] https://ipinfo.io/
[6] https://db-ip.com/

ンシャル情報が保存されているファイルと判断し、表中で表示している。つまり、有効なクレデンシャル情報の場合は、ログイン情報が漏洩しているとみなすことができる。ファイルサイズがそれより小さなものは、URL のクロール時に既に脆弱性が修正されており、正常にクレデンシャル情報を窃取できなかったものと思われる。

URL リストに記載があるものの、クレデンシャルリストには有効なクレデンシャル情報が保存されていなかったケースについて、URL リストは 2020 年 11 月の公開より前に作成されたもので、脅威アクターの間でのみ流通していたものであると推測される。

URL リストの分析結果について、具体的な列挙は避けるが、IP アドレスに紐づけられた組織名などから、日本国内の大学で利用していることが確認できたものや、SINET の運用に関係していると推測されるものも存在した。

6 攻撃のエントリポイントとしての VPN

VPN は文字通り端末と VPN 装置間で仮想的なネットワークを構築することが可能となる。VPN の通信は強固に暗号化されており、第三者がその経路上で通信を盗聴することは非常に困難である。しかしながら、VPN 装置へのアクセス権を攻撃者が手に入れた場合は、VPN はセキュリティ上の意味を持たないどころか、攻撃者に対して組織内部のネットワークへアクセスできる環境を提供することになる。

2020 年は COVID-19 により、リモートワークが全世界的に必要とされることとなった。それに伴い、VPN 接続の需要が高まった結果、既に利用しなくなった古い VPN 装置が再度利用されることとなり、未修正の脆弱性を利用して社内ネットワークがランサムウェアにより攻撃されたケースも存在する[9]。また、VPN 装置自体に脆弱性が無いとしても、不適切な運用のため、大規模な影響を受けたケースも存在している[10]。

7 大学に対する脅威としての考察

これらの情報漏洩が実際の脅威として大学に与えうる影響、およびその対応方法について考察してみる。

7.1 オンラインアカウント情報が漏洩するケース

Peatix から漏洩した情報は、利用者のアカウント情報であった。一般的に利用者は管理すべきアカウント情報が増えることを嫌い、パスワードの使いまわしをしたがるものである。もし漏洩したユーザ名とパスワードが利用者の所属する大学のメールアドレスと同じであった場合、大学の提供するサービスに不正にログインされてしまう恐れがあり、実際に今回のケースでもそのように推測されるインシデントが報告されている。

ユーザ情報のデータベースが漏洩したとしても、適切な処理がしてあればパスワードを復元や推測することはできないが、残念ながら利用者はそのサービスでパスワードがどのように管理されているか知ることはできない。仮に複数のサービスから平文のパスワードを含むアカウント情報が漏洩したとしても、その他のサービスで利用しているパスワードが推測されないよう、規則性の無いパスワードを利用することが望ましいと考える。

ただし、大学関係者が学外で利用しているサービスのアカウント情報に何を利用しているか、当該大学のシステム管理者が知ることは知ることは不可能であるため、ログイン情報を使いまわされたとしてもリスクを緩和できる多要素認証の導入が求められているのが現実である。

7.2 VPN 装置のアカウント情報が漏洩するケース

VPN 装置は大学の情報部門が学生および教職員に学内のシステム等を学外からセキュアに利用させるために設置している場合もあるが、システム導入時に導入を担当したベンダがリモートメンテナンスのために設置している場合も少なくない。

後者についてはベンダのみが利用するため、VPN 装置のファームウェアのアップデートが全く行われていないという場合も少なくないと考えられ、実際に今回の漏洩したクレデンシャル情報のリストがその事実を示している。導入される際に情報部門がシステム構成をチェックし、定期的なアップデートの実施と作業報告を当該システムの学内担当者に行うよう意見することが望ましいと考える。

組織内だけで利用しているサーバについて、通常の手段では外部からアクセスできないことから、脆弱性を悪用されるリスクが少ないとして管理がおざなりになっている場合が少なくないが、内部ネットワークに侵入されるとそのリスクが深刻なものになる。また、VPN 装置と他のシステムとでログイン情報が共通である可能性が考えられ、しかもベンダがシステム導入時にリモート管理用に

用意した VPN 装置の場合、その性質上、当該システムで使い回している特権アカウントである可能性がある。その場合、VPN 装置からアカウントの情報が漏洩した際に、内部ネットワークへの侵入に加えて、別の脆弱性を利用することなく機密情報を扱うシステムへのログインを許してしまう恐れがあるため、ベンダには VPN 装置のような裏口となるシステムには専用のアカウントを利用するよう指示する必要がある。

参考文献

[1] Peatix 「Peatix への不正アクセス事象に関するお詫びとお知らせ」、(https://peatix.com/event/1721625 閲覧日：2021 年 6 月 6 日)

[2] Peatix 「弊社が運営する「Peatix（https://peatix.com/）」への不正アクセス事象に関する 第三者調査機関による調査結果のご報告と今後の対応について」(https://announcement.peatix.com/20201216_ja.pdf 閲覧：2021 年 6 月 6 日)

[3] 愛媛大学「不正アクセスによる迷惑メールの送信について」(https://www.ehime-u.ac.jp/post-143243/ 閲覧日：2021 年 6 月 6 日)

[4] Have I Been Pwned 「Pwned websites」(https://haveibeenpwned.com/PwnedWebsites#Peatix 閲覧日：2021 年 6 月 6 日)

[5] Black Hat USA 2019 「Infiltrating Corporate Intranet Like NSA - Pre-auth RCE on Leading SSL VPNs」(https://www.blackhat.com/us-19/briefings/schedule/index.html#infiltrating-corporate-intranet-like-nsa---pre-auth-rce-on-leading-ssl-vpns-15545 閲覧日：2021 年 6 月 7 日)

[6] JPCERT/CC 「複数の SSL VPN 製品の脆弱性に関する注意喚起」(https://www.jpcert.or.jp/at/2019/at190033.html 閲覧日：2021 年 6 月 7 日)

[7] BLEEPING COMPUTER 「Hacker posts exploits for over 49,000 vulnerable Fortinet VPNs」(https://www.bleepingcomputer.com/news/security/hacker-posts-exploits-for-over-49-000-vulnerable-fortinet-vpns/ 閲覧日：2021 年 6 月 7 日)

[8] BLEEPING COMPUTER 「Passwords exposed for almost 50,000 vulnerable Fortinet VPNs」(https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/ 閲覧日：2021 年 6 月 7 日)

[9] CAPCOM 「不正アクセスに関する調査結果のご報告【第 4 報】」(https://www.capcom.co.jp/ir/news/html/210413.html 閲覧日：2021 年 9 月 12 日)

[10] REUTERS「One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators」(https://jp.reuters.com/article/us-usa-congress-colonial-co-idCAKCN2DK1PQ 閲覧日：2021 年 9 月 12 日)