脆弱なパスワードの設定状況調査

宇田川　暢

新潟大学 情報基盤センター

udagawa@cais.niigata-u.ac.jp

Investigation of weak password usages

UDAGAWA Mitsuru

Center for Academic Information Service, Niigata Univ.

概要

新潟大学で教職員向けに提供しているメールシステムにおいて、脆弱なパスワードの利用によりインシデントが複数回発生している。この問題に対応するため、利用中のパスワードの強度チェックと、必要に応じてパスワード変更の強制を実施した。

1　はじめに

近年、様々な大学において教職員に対して大学が付与しているメールアカウントの乗っ取りによるスパムメールの送信が明らかとなっている。新潟大学においても 2018 年以降、短期間の間に何度も教職員のメールアカウント乗っ取りが発生し、複数回に渡ってお詫び文を公表する事態[1]となっている。

2　新潟大学におけるメール管理

2.1 学生用メールサービス

本学において、在学生を対象に提供しているメールサービスは Gmail となっている。本稿ではこの学生用メールサービスについては取り扱わない。

2.2 教職員用メールサービス

教職員に対しては、プロプライエタリなメールサーバ用ソフトウェアを利用して、オンプレミスでメールサービスを提供している。誰も管理していないアカウントが存在しないよう、本サービスの利用者は、年に一度のメール利用確認を行うことを義務づけられている。

3 不正アクセスへの対応

筆者は所属する部署において、新潟大学の教職員用メールサービスの運用に携わっており、その中で当該メールサービスのアカウントへの不正なアクセスの対応を行ってきた。しかしながら、以下のような攻撃者の多種多様な攻撃への対応が問題となっている。

3.1 ブルートフォース攻撃

ブルートフォース攻撃は、総当たり的にアカウントへのログイン試行を繰り返すタイプの不正アクセスの試みである。一般的にはアカウント名（この場合はメールアカウント）を固定し、パスワードをアカウント名などから推測してログイン試行を繰り返す。このタイプの攻撃は、特定のアカウントやアクセス元 IP アドレスからの連続したログイン試行の失敗に対して、一定時間ロックアウトをすることで緩和することが可能である。

3.2 ボットによる分散型ブルートフォース攻撃

ブルートフォース攻撃への対抗策として、アクセス元 IP アドレスのロックアウトを導入した後に顕在化した問題が、ボットネットによる分散型ブルートフォース攻撃である。ボットネットを構成する個々のボットは、複数の国の IP アドレスを使って分散的に不正アクセスを試みてくるため、前述のような IP アドレス単位でのロックアウトが有効な対応方法では無くなってしまう。

新潟大学では、この攻撃手法に対して、日本国外の IP アドレスからのメールサービスへのアクセスを遮断することで、不正アクセスのリスクを軽減する対応とした。

3.3 フィッシングメールによるアカウント窃取

メールシステム管理者などを装い、偽のログインフォームへ誘導してアカウントを窃取する攻撃メールは非常に多く、受信者によってはアカウント情報を騙し取られてしまうことがある。

この攻撃についてはメール本文をチェックして、フィッシング等の可能性が高い場合は当該メ

ールの題名に特定の文字列の付加を行うことのできるメールサーバ用セキュリティ製品を導入することで対応している。

3.4 漏洩したアカウント情報の利用

新潟大学のパスワードポリシーの一つに、パスワードの流用を禁止するという項目がある。しかしながら、主に利便性のため、学外のサービスと同じパスワードを設定し、そのパスワードがどこかのサービスから漏洩したため、他のサービスにおいても危殆化してしまうというケースが存在する。

また、漏洩したアカウントリストを元に、記号や文字の一部を変更してログイン試行を行うファジングという手法での攻撃を観測している。

4 メールパスワードのチェック方法

これらの攻撃手法に起因して発生したインシデントへの対応として、新潟大学の CSIRT からメールの利用確認に合わせて、メールパスワードの再設定をメールセキュリティ強化の一環として対応するよう依頼があった。しかしながら、単純にパスワードを再設定させるだけでは十分な対策にならないと考えたため、次のような対策を行った。

4.1 正規表現によるパスワードチェック

本メールサービスの利用に当たって、パスワードを設定する際には入力値チェックが行われる。これは正規表現により、文字数や文字種などが定められたパスワードポリシーに従っているかをチェックする。この正規表現に基づくパスワードチェックは、以前から導入されているものである。

4.2 pwscore を利用したパスワードチェック

CrackLib [2]というパッケージに含まれているパスワードリストの辞書を利用し、与えられたユーザ名とパスワードの組み合わせから強度を評価する pwscore [3]コマンドがある。これを利用する事で、パスワード中にユーザ名が含まれている、辞書に掲載されているパスワードである、同じような文字が何度も使われているといった脆弱なパスワードの場合にはパスワード変更を拒否することが可能になる。

4.3 漏洩リストによるパスワードチェック

学内システムのセキュリティ向上のためとはいえ、Collection #1 [4]や Breach Compilation [5]のような漏洩したアカウント情報のリストを一国立大学の情報基盤センターが恒常的に収集、分析することは困難である。幸い、”Have I Been Pwned” [6]（以下、HIBP）というサービスが Troy Hunt により提供されており、パスワードチェック API を利用する事で、安全に指定したパスワードが漏洩リストに掲載されたもので無いか確認することが可能となっている。

具体的には、パスワードの SHA1 ハッシュ値を取得し、最初の 5 文字を送信することで、該当するハッシュ値のリストを HIBP から取得、手元で照合することで漏洩リストに含まれているかの確認を行う。SHA1 ハッシュ値は 16 進数で 40 文字のため、一致した場合はほぼ確実に漏洩したパスワードであると考えられる。

5 メールパスワード確認の実施

前掲の pwscore および HIBP によるパスワードチェック機構を導入し、以下のようなフローでのパスワードチェックをメール利用確認時に追加することを提案し、CSIRT 担当者から了承を得て実施することとなった。

(1) メール利用確認システム（以下、本システム）へのログインする（本システムは利用確認依頼メール記載のハッシュ付き URL＋OTP によるログインと、メールアドレスとパスワードを利用したログインの 2 通りのログイン方法がある）。
(2) 現在のパスワードを入力するよう要求する。パスワードが不明のため、チェックをスキップする場合は(5)へ。
(3) メール用認証サーバにて認証し、入力されたパスワードが現在のパスワードと一致しない場合は(2)へ戻る。
(4) 入力したパスワードのチェックを行い、問題がなければ(6)の登録情報の確認へ、正規表現、pwscore および HIBP でのチェックのいずれかに引っかかった場合は(5)へ移る。
(5) 新しいパスワードを入力させ、正規表現、pwscore、HIBP の全てのチェックに通った場合にはパスワードを更新し、(6)へ移る。
(6) 利用者の登録情報を確認し、継続利用を申請する。

6 実施結果

今年度の利用確認対象となった 2,937 アカウントに対して依頼メールを送付したところ、およそ

2ヶ月の実施期間に2,702アカウントでのパスワード確認が実施された。そのうち、パスワードを変更したアカウントは564アカウントだった。

前述のように、本システムへのログイン時には、現在利用中のパスワードを知らなくてもログインできるような仕組みが備わっている。そのため、パスワードを変更した利用者は、基本的にパスワードが不明か、パスワードチェックで問題が起こったかのどちらかとなる。前者が395アカウント、後者が169アカウントだった。

このパスワード確認の処理において、パスワードチェックを通らなかった際に、問題となったパスワードそのものや、その理由を記録していなかったため、どのようなパスワードが使われていたのか直接知ることはできない。ただし、エラーページのHTML出力の際にウェブサーバから送信されたデータサイズから問題となった項目を推測することができる。本システムが動作しているウェブサーバのアクセスログと、メール用認証サーバの認証ログを突き合わせることで調査と集計を行った。

なお、このパスワードチェックは、「正規表現によるチェック」、「pwscoreによるチェック」、「HIBPによるチェック」の順に行われ、それぞれのチェックで問題が見つかった場合は、全てのチェックを行った後にまとめて結果を表示する仕様となっている。

7 集計結果

パスワードチェックで問題が見つかった169アカウントについて、集計した結果は表1のようになった。

表1　問題が見つかったパスワード

発見された問題	件数	比率
ユーザ名の一部が含まれる	99	58.6%
辞書に掲載されている	22	13.0%
大文字と小文字の入れ替えのみ	14	8.3%
単純・系統的（パターン繰り返し）	10	5.9%
HIBPに掲載されている	8	4.7%
HIBP掲載 ＋ 辞書に掲載	7	4.1%
利用されている文字種が少ない	4	2.4%
HIBP掲載 ＋ ユーザ名の一部	1	0.6%
HIBP掲載 ＋ 文字種が少ない	1	0.6%
HIBP掲載 ＋ 単純・系統的	1	0.6%
（特定不能）	2	1.2%

ユーザ名の一部が含まれているパスワードが最も多く、次いで辞書に掲載されたパスワード、（辞書に掲載されたパスワードと比較して）大文字と小文字の入れ替えのみされたパスワード、簡単すぎるパスワードとなっている。これらはpwscoreにて問題が見つかったものとなる。

HIBPに掲載されたパスワードとして検出されたものは合計で18アカウントだったが、10件を除いてpwscoreでのチェックにおいても検出することが可能であり、前述のように全件をHIBPでチェックしているにもかかわらず、検出比率は低いものとなっている。しかしながら、HIBPでのみ問題として検出できたパスワードがあったことから、HIBPの導入に意味が無いとは言えないと考える。

本システムではpwscoreの出力メッセージを利用者に対して問題点が分かりやすいメッセージに変更して表示するようにしている。この出力メッセージは、正規表現によるチェックを通過したパスワードを利用していることを前提としている。この想定を外れたパスワードが与えられた際に、特定不能のメッセージ出力が行われたと考えられる。

8 今後の課題

今回のパスワード確認の実施の結果、最低でも6%の利用者が脆弱なパスワードを利用しており、うち13%はユーザ名がパスワードに含まれた、推測しやすいパスワードを利用していたものと予想される。パスワードポリシーとしてパスワード中にユーザ名を含めないことを定め、パスワード変更画面にその旨を記載していても、全てのユーザが従ってくれることを期待することは危険で、システム中にチェックする機構を備えることが重要であるという教訓を得ることができた。このような仕組みを他の認証サービスのパスワード変更ページにおいても取り入れることを検討したい。

今回のメール確認は教職員用メールアカウントの全利用者を対象にしたものではなく、特定の部局や新規アカウント取得者、何らかの事情で自ら利用確認を行うことができなかった利用者からの依頼を受けて代行したアカウントについては、今回のパスワードチェックを実施していない。これらのアカウントの利用者の中に脆弱なパスワードを利用している可能性があり、今回パスワード

確認の対象外となったアカウントについても同様の措置を行うことを CSIRT に対して推奨した。

参考文献

[1] 新潟大学「サイト内検索結果」、（https://www.niigata-u.ac.jp/result/?q=メール被害%E3%80%80 迷惑|漏洩%E3%80%80 inurl:news 閲覧日：2020 年 10 月 14 日）

[2] GitHub「cracklib/cracklib」、（https://github.com/cracklib/cracklib 閲覧日：2020 年 10 月 14 日）

[3] GitHub「cgwalters /libpwquality-git」、（https://github.com/cgwalters/libpwquality-git 閲覧日：2020 年 10 月 14 日）

[4] Troy Hunt「The 773 Million Record "Collection #1" Data Breach」、（https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/ 閲覧日：2020 年 10 月 14 日）

[5] GitHub Gist「scottlinux/breachcompilation.txt」、（https://gist.github.com/scottlinux/9a3b11257ac575e4f71de811322ce6b3 閲覧日：2020 年 10 月 14 日）

[6] Have I Been Pwned「';--have i been pwned? Check if you have an account that has been compromised in a data breach」、（https://haveibeenpwned.com/ 閲覧日：2020 年 10 月 14 日）