ネットワーク科学を用いた
パスワード使い回しリスクの定量評価

愛知県立大学　*坂下航平　SAKASHITA Kohei
愛知県立大学　　奥田隆史　OKUDA Takashi
*愛知県立大学　情報科学部　情報科学科　メディア・ロボティクスコース
*〒 480-1198 愛知県長久手市茨ケ廻間 1522-3
*E-mail: is151040@cis.aichi-pu.ac.jp

1　はじめに

インターネット上のオンラインサービスにおける大多数の個人認証は，パスワードが利用されている．パスワードはサービス利用者が適切に設定･管理をおこなう必要がある．これを促すため，総務省はパスワード設定・管理の推奨方針を公開している [1]．推奨方針には「**パスワードを複数のサービスで使い回さない**」がある．しかしながら，**パスワードの使い回し**をしてしまい，不正ログインなどの攻撃被害にあう事例が多く報告されている [2]．このような被害が多くなってきたこともあり，これまで推奨されてきた「パスワードは定期的に変更する」が改められ「**パスワードの定期的変更は不要である．パスワード流出時に使い回していないパスワードに速やかに更新する**」[1] が新しく推奨されるようになった [3]．

被害を減少させるには，利用者に対し，攻撃の対策である推奨方針を啓発することが重要である [4]．さらに，効果的な啓発には，推奨方針の有効性の根拠を要する．そこで，本研究では，パスワードの使い回しリスクを定量的に評価する手法を提案するとともに，推奨方針の有効性を検証する．

以下，第 2 節ではパスワードの使い回しとそのリスクを説明する．第 3 節ではネットワークの科学の知見を利用したパスワードモデルを説明する．第 4 節ではパスワードリスト攻撃モデルを説明する．第 5 節では，モデルに数値例を適用し，使い回し，更新方策と攻撃被害の関係をシミュレーションにより検証し，推奨方針の有効性を考察する．最後に，第 6 節で本稿をまとめ，今後の課題を述べる．

2　使い回しとそのリスク

本節では，パスワードの使い回しと，使い回しリスクの評価方法を説明する．

一般にパスワードの使い回しとは,「複数のサービスで同一のパスワードを使い回すこと」[1] である．本研究における使い回しは，「**複数のサービスで類似したパスワード (以下，類似パスワード) を使い回すこと**」も含む．ここで，類似パスワードは，同一の**使い回し根**を有するものとする．使い回し根は，使い回しているパスワードの基となる文字列とする．例えば，2 つの類似パスワード “abc1” と “abc2” の使い回し根は “abc” である．

使い回しのリスク [5] は，**期待総被害コスト**で評価する．期待総被害コストは，**被害確率**と**被害コスト**の積とする．被害確率は，クラッカーや攻撃者の攻撃が成功する確率とする．被害コストは，パスワードが破られたときに受ける被害の大きさとする．被害コストとして，本研究では，利用者の金銭的損失を想定する．

攻撃として，本研究では**パスワードリスト攻撃**を想定する．パスワードリスト攻撃とは，あるサービスの ID・パスワードを何らかの方法で入手し，他の様々なサービスに対しても試す攻撃のことである．同一のパスワードを使い回している場合，攻撃を許し，被害を受ける．同一のパスワードを使い回していない場合でも，類似パスワードを使い回していれば，攻撃者の推測でパスワードリスト攻撃を許す可能性がある．

3　パスワードモデル

本節では，利用者のアカウント情報，および利用者の行動をモデル化したパスワードモデルを説明する．パスワードモデルには，2 つの構成要素「パスワード空間」,「パスワード更新モデル」がある．

以下．第 3.1 節では，パスワードのモデル表現およびパスワード空間を説明する．第 3.2 節では，パスワードノードの生成手順を説明する．第 3.3 節では，パスワード更新モデルと更新方策を説明する．

3.1　パスワードの表現とパスワード空間

パスワードをネットワーク科学 [6][7] の知見を用いて表現する．本研究では，あるパスワード i をパスワードノード n_i で表す．図 1 にある利用者のアカウント情報とパスワードノードおよびその関係を示す．c_i はパスワード i が破られた場合の被害コストを表す．r_i はパスワード i の使い回し根を表す．2 つの類似パスワード i と j は，パスワードブランチ b_{ij} をもつとする．つまり，パスワードノード n_i と n_j はパスワードブランチ b_{ij} により繋がる．

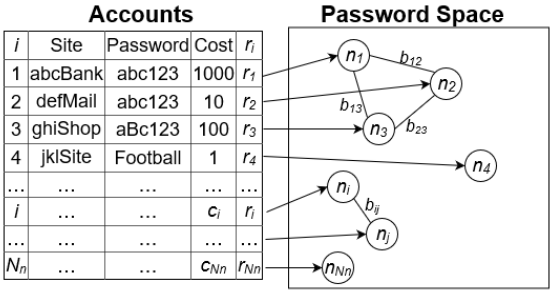

図 1: アカウント情報とパスワードノード

ある利用者の全てのパスワードノードの集合をパスワード空間とする．パスワード空間に存在するパスワードノードの総数をパスワード数 N_n，使い回し根の種類の総数をルート数 N_r とする．

3.2　パスワードノードの生成手順

パスワードノードの生成手順は次の **Step:1**〜**Step:4** とする．

Step:1 使い回しをおこなう場合は，使い回し根を一様の確率で選択 (以下，ランダム選択) する．

Step:2 選択した使い回し根をもつパスワードノード n_{N_n+1} を生成する．

Step:3 n_{N_n+1} に被害コスト c_{N_n+1} を設定する．

Step:4 類似パスワードノードとパスワードブランチを繋ぐ．

ただし，使い回しをおこなわない場合は，使い回し根を選択せず，新しい使い回し根を生成する．

3.3　パスワード更新モデルと更新方策

パスワードの更新は，パスワードノードの生成と無効化で表現する．ここで，パスワードノード n_i の無効化とは，n_i の被害コスト c_i を 0 にすることとする．更新の手順は次の **Step:1**，**Step:2** とする．ただし，更新するパスワードを i とする．

Step:1 新しいパスワードノード n_{N_n+1} を生成する．ただし，n_{N_n+1} の被害コスト c_{N_n+1} を c_i とする．

Step:2 更新パスワードノード n_i を無効化する．

パスワード更新は，ある更新方策 M_U に従っておこなう．ここで，更新方策とは，更新をどのようにおこなうのかを表し，4 つのパラメータ「更新パスワード自体の選択方法 M_a」,「更新パスワードの使い回し根の選択方法 M_b」,「更新タイミング M_t」,「更新パスワード数 N_u」により定める．以下，更新方策 M_U のパラメータは，$\boldsymbol{M_U = \{M_a, M_b, M_t, N_u\}}$ と表記する．各更新方策のパラメータ M_a, M_b, M_t, N_u がとる値を次に示す．

更新パスワード自体の選択方法 $\boldsymbol{M_a}$ 流出したパスワードの類似パスワードからランダム選択する．ただし，流出したパスワードは必ず選択する (以下，LP)．

更新パスワードの使い回し根の選択方法 $\boldsymbol{M_b}$ 更新するパスワードと同一の使い回し根を選択する (以下，SR)，または，新しい使い回し根を生成する (以下，NR)．

更新タイミング $\boldsymbol{M_t}$ パスワード流出後ただちにパスワード更新する (以下，AL)．

更新パスワード数 $\boldsymbol{N_u}$ 0 以上の整数値をとる．

ただし，$N_u = 0$ のときは M_a, M_b, M_t の値に関わらず，更新しないことを意味する．

4　パスワードリスト攻撃モデル

本節では，パスワードリスト攻撃モデルを説明する．ただし，簡単のため，本研究では利用者の ID は全て同一であるとする．

パスワードリスト攻撃をおこなうために，攻撃者は，流出したパスワードをあらかじめ入手する (以下，**流出入手**)．さらに，攻撃者は，流出パスワードから推測してパスワードを入手することもできる (以下，**推測入手**)．パスワード空間における流出入手，推測入手の対象と成功確率をそれぞれ次に示す．

流出入手 パスワードノードを対象におこなう．パスワードノード n_i を対象にした流出入手の成功確率を**流出入手確率** P_{Li} とする．

推測入手 推測入手の場合は，攻撃者が既に入手したパスワードとブランチで繋がっているパスワードノードを対象におこなう．パスワードブランチ b_{ij} でつながったノードを対象にした推測入手の成功確率を，**推測入手確率** P_{Gij} とする．

攻撃者は,「利用者のパスワード空間が完成した直後」に攻撃を始め，流出入手をおこなった後，推測入手をおこなう．

5　数値例

本節では前述したパスワードモデル，パスワードリスト攻撃モデルに数値例を適用する．利用者のルート数と更新方策によって，パスワードリスト攻撃の被害がどのように変化するのかをシミュレーションにより検証する．検証結果からパスワード設定・管理の推奨方針の有効性を考察する．

さらに，パスワード数が非常に多い場合における推奨方針の有効性を検証する．2 つの検証におけるパスワード数は，通常の場合は利用者の平均パスワード数 [8] の 25 個，パスワード数が非常に多い場合は 300 個とする．

以下，第 5.1 節で想定環境を述べる．第 5.2 節でシミュレーション結果と考察を述べる．

5.1　想定環境

ここでは，想定環境として，想定シナリオ，仮定，評価指標を述べる

本数値例の想定シナリオは，次の **Step:1**〜**Step:4** とする．

Step:1 利用者はパスワード空間を生成する．

Step:2 パスワードノード 1 つをランダム選択し，流出したパスワードとする．

Step:3 利用者はパスワード流出を知り有限個のパスワード更新をする．

Step:4 攻撃者は流出したパスワードを入手しパスワードリスト攻撃をする．

この想定シナリオに基づく本数値例の仮定を次に示す．

仮定 1 生成するパスワード数は 25，300 個とする ($N_n = 25, 300$)．

仮定 2 ルート数は 1〜6 個とする ($N_r = 1, 2, \cdots, 6$)．

仮定 3 全てのパスワードノードの被害コストは 1，10，100，1000 万円からランダム選択とする ($c_i = 1, 10, 100, 1000$)．

仮定 4 更新方策は 3 つ「更新しない (以下，M_{U1})」，「流出時に使い回しありで更新する (以下，M_{U2})」,「流出時に使い回しなしで更新する (以下，M_{U3})」とする ($M_{U1} = \{-, -, -, 0\}$, $M_{U2} = \{LP, SR, AL, 1\}$, $M_{U3} = \{LP, NR, AL, 1\}$)．

仮定 5 全ての流出入手確率は 1 とする ($P_{Li} = 1$)．

仮定 6 全ての推測入手確率は 0 以上 0.5 未満の実数からランダム選択とする ($0 \leq P_{Gij} < 0.5$)．

本数値例の評価指標は，利用者により被害コストの総計が異なることから，**期待総被害コスト率** C_{rate} とする．C_{rate} は利用者が全体の何%の被害コストを失ったかを表し，式 (1) で求める．

$$C_{rate} = \sum_{n_i \in A_p} c_i / \sum_{i=0}^{N_n} c_i \tag{1}$$

ここで，A_p は，攻撃者が入手したパスワードノードの集合を表す．また，攻撃者がパスワードノード n_i を入手したとき，$n_i \in A_p$ と表記する．

5.2　シミュレーション結果と考察

以上の想定環境で，各パスワード数 ($N_n = 25, 300$)，ルート数 ($N_r = 1, 2, \cdots, 6$)，更新方策 (M_{U1}, M_{U2}, M_{U3}) の組，合計 36 組に対してシミュレーションを 1000 回ずつ実施し，期待総被害コスト

率 C_{rate} の平均値ならびに 95%信頼区間を算出する．シミュレーションには artisoc[9] を利用する．

$N_n = 25$ の場合のシミュレーション結果を図 2 に示す．グラフは，縦軸が期待総被害コスト率 C_{rate}，横軸がルート数 N_r，エラーバーが 95%信頼区間を示す．また，M_{U1}，M_{U2}，M_{U3} がそれぞれの更新方策を示す．さらに，$N_n = 300$ の場合のシミュレーション結果を図 3 に示す．グラフの見方は，図 2 と同様である．

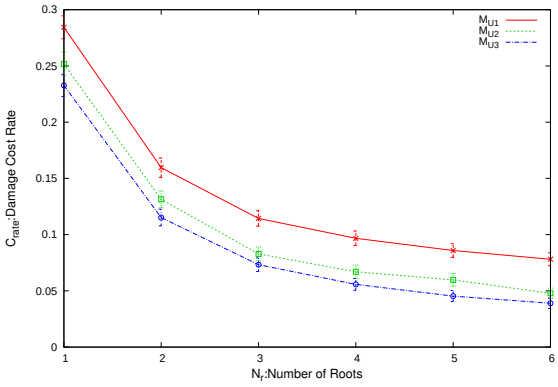

図 2: ルート数 N_r と期待総被害コスト率 C_{rate} の関係 ($N_n = 25$ の場合)

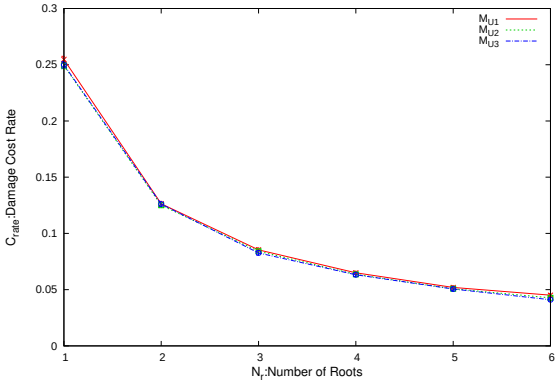

図 3: ルート数 N_r と期待総被害コスト率 C_{rate} の関係 ($N_n = 300$ の場合)

パスワード数 $N_n = 25$ の場合のルート数 N_r と期待総被害コスト率 C_{rate} の関係を考察する．M_{U1}, M_{U2}, M_{U3} の全ての場合で，N_r の増加に伴い C_{rate} が減少する．ここから，使い回し根の種類の増加により，パスワードリスト攻撃の被害が減少するといえる．

パスワード数 $N_n = 25$ の場合の更新方策 M_U と期待総被害コスト率 C_{rate} の関係を考察する．N_r が同じ場合は，M_{U1}, M_{U2}, M_{U3} の順に C_{rate} が小さい．ここから，流出時の更新により，パスワードリスト攻撃の被害が減少するといえる．また，流出時の更新を使い回しなしでおこなうことで，さらに被害が少し減少するといえる．

パスワード数 $N_n = 300$ の場合のルート数 N_r と期待総被害コスト率 C_{rate} の関係を考察する．M_{U1}, M_{U2}, M_{U3} の全ての場合で，N_r の増加に伴い C_{rate} が減少する．ここから，$N_n = 25$ の場合と同様に，$N_n = 300$ の場合も使い回し根の種類の増加により，被害が減少するといえる．

パスワード数 $N_n = 300$ の場合の更新方策 M_U と期待総被害コスト率 C_{rate} の関係を考察する．N_r が同じ場合は，M_{U1}, M_{U2}, M_{U3} にかかわらず，C_{rate} はほぼ変わらない．ここから，$N_n = 25$ の場合には見られた流出時の更新による被害の減少は，$N_n = 300$ の場合にはないといえる．

以上の結果・考察より，総務省の推奨「パスワードを複数のサービスで使い回さない」,「パスワードの定期的変更は不要である．パスワード流出時に使い回していないパスワードに速やかに更新する」[1] は，有効であるといえる．ただし，パスワード数が非常に多い場合は,「パスワードを使い回さない」は有効であるが,「パスワード流出時に更新する」は有効であるとはいえない．

6 おわりに

本研究では，ネットワーク科学の知見を利用し，パスワード使い回しリスクを定量的に評価する手法を提案した．さらに，パスワードリスト攻撃を想定したシミュレーションにより，使い回しリスクを定量的に評価した．評価結果から，パスワードに関する総務省の推奨方針の有効性を示した．しかし，利用するパスワード数が非常に多い場合，推奨の 1 つである「パスワード流出時の更新」の有効性は示せなかった．

今後の課題は，利用パスワード数に関わらず有効性のある更新方策の検討，モデルのさらなる検証と拡張，および本研究で得られた検証結果を情報セキュリティ教育へ還元していくことである．

参考文献

[1] 総務省，『国民のための情報セキュリティサイト』，http://www.soumu.go.jp/main_

sosiki/joho_tsusin/security/basic/privacy/01-2.html，2019 年 2 月閲覧.

[2] 国家公安委員会：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 (2018)

[3] “国が方針一転「簡単な文字列になりがち」”，朝日新聞朝刊，2018 年 4 月 22 日.

[4] 独立行政法人情報処理推進機構：オンライン本人認証方式の実態調査報告書 (2014)

[5] デビッド・ヴォーズ,『入門リスク分析』，勁草書房，2008.

[6] 林幸雄，大久保潤他,『ネットワークの科学〜つながりに隠れた現象をひもとく〜』，近代科学社，2007.

[7] 増田直紀，今野紀雄,『複雑ネットワークの科学』，産業図書，2005.

[8] Dinei Florencio，Cormac Herley，*“A Large-Scale Study of Web Password Habits ”*，WWW ’07 Proceedings of the 16th international conference on World Wide Web，pp.657-666，2007-8-12.

[9] 山影進,『人口社会構築指南〜artisoc によるマルチエージェント・シュミレーション入門〜』，書籍工房早山，2011.