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

1　はじめに

オンラインサービスでよく利用されているパスワードは，利用者が適切に設定・管理する必要がある．そのため，総務省は推奨方針「**パスワードを複数のサービスで使い回さない**」,「**流出時に使い回ししていないパスワードに速やかに変更する**」[1] などを公開している．しかし，推奨を破り被害にあう事例は，多く報告されている [2]．被害の軽減には，推奨方針の有効性の啓蒙が必要であり，効果的な啓蒙には根拠を要する．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モデルおよび手法を提案し，推奨方針の有効性を検証することで，情報セキュリティ教育に貢献する．

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を使い回すこと**」である．類似パスワードは，使い回しているパスワードの基となる文字列 (以下，**使い回し根**) を有するものとする．

使い回しのリスク [3] 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**の積である．被害確率は，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．攻撃は**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，あるサイトの ID・パスワードを，他のサイトに対しても試す攻撃のことである．

2　パスワードモデル

パスワードの表現とパスワード空間

あるパスワード i をネットワーク科学 [4] の知見を用いて，**パスワードノード** n_i で表す．図 1 に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 の被害コスト，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} を有する．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**とし，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．

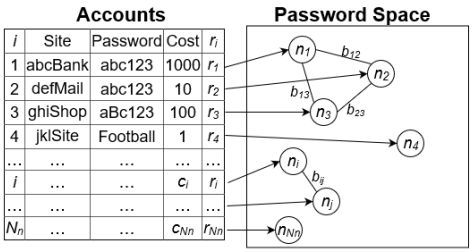

図 1　アカウント情報とパスワードノード

パスワードノードの生成手順は次の 4 ステップである．**Step1:** 使い回し根をランダム選択する．**Step2:** 選択した使い回し根をもつパスワードノードを生成する．**Step3:** 被害コストを設定する． **Step4:** 類似パスワードノードとパスワードブランチを繋ぐ．

パスワードノードの更新

利用者は，更新をどのようにおこなうのかを表す**更新方策** M_U に従ってパスワード更新をおこなう．本研究では 3 つの更新方策「更新なし (以下，M_{U1})」,「流出パスワードを使い回しありで更新 (以下，M_{U2})」,「流出パスワードを使い回しなしで更新 (以下，M_{U3})」を考える．

パスワードリスト攻撃モデル

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**)．流出入手は，パスワードノードを対象とし，必ず成功すると仮定する．推測入手は，攻撃者が入手したパスワードの類似パスワードノードを対象とし，パスワードブランチ b_{ij} でつながったノードを対象とした成功確率を，**推測入手確率** P_{Gij} とする．

3　シミュレーションの結果と考察

想定環境のシナリオは，次の 4 ステップである．**Step1:**利用者はパスワード空間を生成する．**Step2:**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．**Step3:**攻撃者は流出したパスワードを入手し攻撃する．**Step4:**攻撃者はパスワードを推測し攻撃する．

想定シナリオより，5 つの仮定「生成パスワード数は 25 個 ($N_n = 25$)」,「ルート数は 1〜6 で変動 ($N_r = 1, 2, \cdots, 6$)」,「全てのパスワードの被害コストは 4 つの整数 1，10，100，1000 からランダム選択 ($c_i = 1, 10, 100, 1000$)」,「更新方策は 3 つ M_{U1}，M_{U2}，M_{U3}」,「全ての推測入手確率は 0〜0.5 の実数からランダム選択 ($0 \leq P_{Gij} < 0.5$)」をおく．

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，利用者が全体の何 % の被害コストを失ったかを表す**期待総被害コスト率**

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

を用いる．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．

以上の想定環境で，ルート数 N_r を 1〜6 まで変動させた場合の，3 つの更新方策 M_{U1}，M_{U2}，M_{U3} について，シミュレーションを 1000 回実施し，期待総被害コスト率の平均値ならびに 95% 信頼区間を算出した．シミュレーションには artisoc[5] を用いた．シミュレーション結果を図 2 に示す．グラフは，M_{U1}，M_{U2}，M_{U3} がそれぞれ更新方策，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．

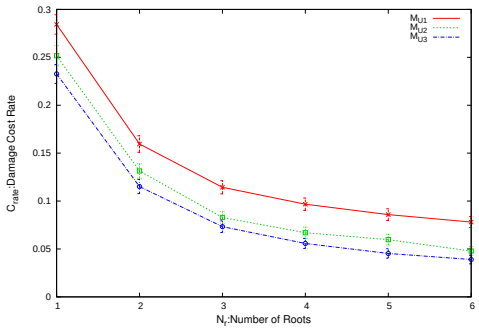

図 2　ルート数 N_r と期待総被害コスト率 C_{rate} の関係

以上の結果より，ルート数を増加させる，流出時に使い回しありで更新する，使い回しなしで更新する，ことでパスワードリスト攻撃の被害が減少することがわかる．したがって，総務省の推奨方針「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．流出時に使い回ししていないパスワードに速やかに変更する」[1] は，有効であることがわかる．

4　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モデルおよび手法を提案した．さらに，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．今後の課題は，モデルのさらなる検証と拡張，および検証結果を情報セキュリティ教育へ還元することである．

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] デビッド・ヴォーズ，『入門リスク分析』，勁草書房，2008．[4] 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．[5] 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．