1ZA-07

確率モデルおよびネットワーク科学によるパスワード使い回しリスクの定量的解析

坂下航平 †　　奥田隆史 †

愛知県立大学情報科学部情報科学科 †

1 はじめに

インターネット上の大多数のオンラインサービスにおける個人認証はパスワードが利用されている．パスワードは特別な機器を必要としない知識認証である．一方で，パスワードは利用者が適切に設定・管理を行う必要がある．適切に設定・管理するための推奨方針を総務省は公知している [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，**パスワード使い回し**をしてしまい不正アクセスの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，これまでの推奨「パスワードは定期的に変更する」が，新しい推奨「**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**」に改められた [1]．そこで，本研究では，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するとともに，新しい推奨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について述べる．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提案し，第 4 節ではパスワードリスト攻撃モデルを提案する．第 5 節では，使い回しと攻撃被害，更新方策と攻撃被害をシミュレーションにより検証し，新しい推奨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 パスワードの使い回しとそのリスク

一般にパスワードの使い回し (以下，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”である [1]．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**」も含む．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．使い回し根とは，使い回しているパスワードの基となる文字列のことである．例えば，2 つの類似パスワード “abc123” と “abcdef” の使い回し根は “abc” である．

使い回しのリスクは，**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 [3]．被害確率は，クラッカーや攻撃者の攻撃が成功する確率である．被害コストとは，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．

攻撃として，本稿では**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．最近では攻撃者による推測により，類似パスワードの使い回しであったとしてもパスワードリスト攻撃を許す可能性が高まっている．

3 パスワードモデル

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 [4][5] 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．S_i はパスワード i の使い回し根を表す．

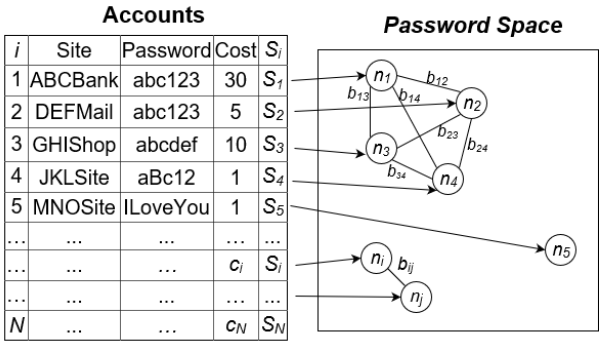

図 1: アカウント情報とパスワードノード

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} を持つ．つまり，i と j は同一の使い回し根を持つ．あるパスワードノードのパスワードブランチの総数を**次数**と呼ぶ．

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**と呼ぶ．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，使い回し根の種類数をルート数 R とする．

使い回しパスワードの生成

使い回しパスワードノードは次の手順で生成する．

1. 使い回し根をランダム選択する．
2. 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．
3. パスワードノードに被害コストを設定する．
4. 類似パスワードノードとブランチを結ぶ．
5. 1〜4 を N 回繰り返す．

ランダム選択とは，一様分布の確率で使い回し根を選択することである．

パスワードノード更新

利用者は，ある更新方策に従ってパスワード更新を行う．更新方策とは，更新をどのように行うのかを表し，「更新タイミング」,「更新パスワード数 U_n」,「更新パスワードの選択方法 M_B」,「更新パスワードの使い回し根の選択方法 M_A」がある．本稿でどのような更新方策を設定するかは第 5 節 (数値例) で示す．

4 パスワードリスト攻撃モデル

パスワードリスト攻撃を行うために，攻撃者は，流出したパスワードをあらかじめ入手する (**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 (**推測入手**)．

流出入手の場合の攻撃は，パスワードノードを対象にして行う．攻撃者がパスワードノード n_i を対象とした流出入手の成功確率を**流出入手確率** P_{Li} とする．モデル上での流出入手のルールは「攻撃者はパスワードノード 1 つをランダム選択し，確率 P_{Li} でパスワードノードを入手する」である．このときに入手したパスワードノードを，**初期流出パスワード**とする．

推測入手の場合の攻撃は，パスワードブランチを対象にして行う．攻撃者がパスワードブランチ b_{ij} を対象とした推測による入手の成功確率を，**推測入手確率** P_{Gij}

A quantitative analysis of re-use password risk by using probability models and complex network models

†Kouhei SAKASHITA, Takashi OKUDA

†Department of Information Science and Technology, Faculty of Information Science and Technology, Aichi Prefectural University

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.

とする．推測入手確率は，ブランチの両端のパスワード文字列の差違で決まる．モデル上での推測入手のルールは,「入手したパスワードの類似パスワードノードを，それぞれ確率 P_{Gij} で入手する」である．

攻撃の開始条件・終了条件について説明する．攻撃は,「利用者のパスワード空間が完成した直後」のみとする．攻撃者は，**最大推測回数** A_s まで攻撃を繰り返す．

5 数値例

ここ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を活用した数値例を示す．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．

想定環境

シミュレーションの想定シナリオは，

1. 利用者はパスワード空間を生成する，
2. 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，
3. 攻撃者は流出したパスワードを入手し攻撃する，
4. 攻撃者はパスワードを推測し攻撃する，推測は最大推測回数まで繰り返す，

とする．

利用者に関しては下記の仮定 1〜6 を仮定する．表 1 にパラメーターをまとめる．

仮定 1 生成パスワード数は 30 個 ($N = 30$).

仮定 2 全てのパスワードの被害コストは全て 1($c_i = 1$).

仮定 3 パスワード流出後，ただちにパスワード更新．

仮定 4 1 回の最大更新パスワード数は 5 個 ($U_n = 5$). $U_n = 0$ のときは更新しないことを意味する．

仮定 5 更新パスワードの選択方法は $SRRC$. $SRRC$ とは初期流出パスワードと類似のパスワードからランダム選択すること．

仮定 6 パスワード空間のルート数は $R = 1, 2, \cdots, 6$ とする．更新パスワードの使い回し根の選択方法 M_A は SR または NR とする．SR は初期流出パスワードと同一の使い回し根を使うこと．NR は新しい使い回し根を生成すること．

表 1: 利用者のパラメーター ($N = 30$, $c_i = 1$)

R	U_n	M_B	M_A
1 ⋮ 6	0	-	-
1 ⋮ 6	5	SRRC	SR NR

攻撃者については仮定 7〜9 を仮定する．

仮定 7 流出入手確率は 1($P_{Li} = 1$).

仮定 8 パスワードノード生成時にブランチを 2 つまでランダム選択し，推測入手確率を 0.1($P_{Gij} = 0.1$) とする．他のブランチは $P_{Gij} = 0$ とする．

仮定 9 攻撃はパスワード空間生成終了後とし最大推測回数は 15($A_s = 15$).

本数値例の評価指標は，利用するサイトにより被害コストが異なることから，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**

$$C_r = \sum_{n_i \in A_p} c_i / \sum_{i=0}^{N} c_i \qquad (1)$$

を利用する．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．また，攻撃者がパスワードノード n_i を入手したときは，$n_i \in A_p$ と表記する．

評価例

以上の想定環境，パラメータで 2000 回の計算機シミュレーションを実施し，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．その結果を図 2 に示す．シミュレーションには artisoc を用いた [6].

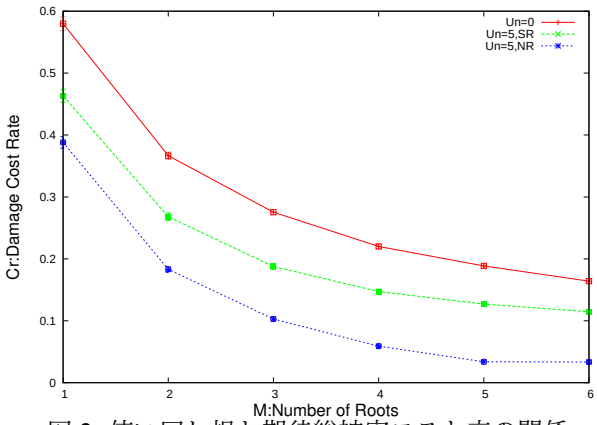

図 2: 使い回し根と期待総被害コスト率の関係

以上の結果より，ルート数を増加させる，流出時に更新を行う，という行動でパスワードリスト攻撃の被害が減ることがわかる．さらに，更新方策 M_A を NR で行うことで被害が減ることがわかる．また，ルート数を増加させたときの効果は，NR での更新を取り入れた場合よりも大きい．したがって，総務省の新しい推奨「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．

6 おわりに

本研究では，ネットワーク科学の知見を活用し，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新しい推奨の有効性を示した．今後の課題は，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，2018 年 10 月閲覧.

[2] 警視庁，『警視庁サイバー犯罪対策プロジェクト：統計』，http://www.npa.go.jp/cyber/statics/index.html，2018 年 12 月閲覧.

[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] 増田直紀，今野紀雄,『複雑ネットワークの科学』，産業図書，2005.

[6] 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.

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.