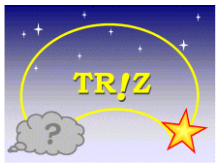
NPO法人 日本TRIZ協会 主催
第5回 日本TRIZシンポジウム 2009



TRIZ/USIT適用事例:
パスワードを思い出させる方法

2009年 9月10日～12日
国立女性教育会館 （埼玉県比企郡嵐山町）

上田祐太朗 (4回生)、鍋島裕貴(4回生)、
中川 徹
大阪学院大学 情報学部

発表の趣旨と 演習の進め方

- **中川ゼミ:「創造的な問題解決のための思考法」**
  その事例として演習した
- **「パスワードを思い出させる方法」**
- **少人数のゼミでの演習**
  -- 先生は毎回最初にリードして、学生が中身を発言、
  ホワイトボードに記録、デジカメで記録
- **TRIZ/USITを比較的自由に使って考察した**
- **USITで、問題定義、現在のシステムの分析 (機能と属性)、**
  理想のシステムの考察、アイデア出し
- **TRIZの物理的矛盾の確認、40の発明原理によるアイデア出し、**
- **解決策の整理・体系化、再考察 (USIT)**

問題設定:

- コンピュータ利用の場合に限らず、日常生活でも、
  パスワードを必要とする機会が多くなった。
- 多数の、多種類のパスワードを必要とする。
- 自分で設定できるパスワードの他に、
  システム側から与えられる (お仕着せの) パスワードがある。
- パスワードを覚えきれないので、適切な管理が必要
- 悪意のある他人に知られると、重大な被害を受ける
- 多数のパスワードを管理し、思い出させる方法を考察する

問題設定:「ID/パスワードを思い出させる方法」

(1) ID/パスワードが、自分で設定できる場合と
システム側から与えられる場合がある。両方を扱う。

(2) 自分で設定できる場合、どのように設定するのがよいか?
思い出させるにはどのようにするとよいか?

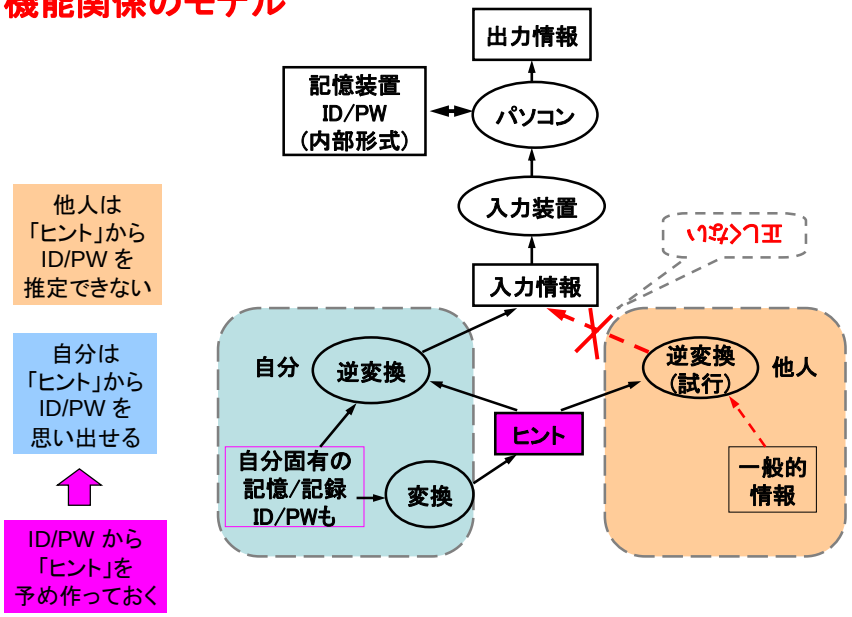
(3) システム側から与えられる(往々乱数的で複雑な) 場合に、
思い出させるにはどのようにするとよいか?

(4) 思い出させるヒントは、万一、他人に見られても大丈夫にする。
それには、どのようにヒントを作り、どのように保管すべきか?

(5) ヒントの媒体は、主として紙ベースとし、
コンピュータや携帯電話などの内蔵形式のものは別途考える。

(6) どうしても思い出せない場合は、再発行の方式を取る。
この方式はほぼ確立しており、今回の問題から除外した。

機能関係のモデル



属性の分析

問題の焦点は、パスワードとヒントの属性 にある。

どのような性質をもつパスワードとヒントであるのがよいか?

パスワード／ヒントの持つ属性:

(a) 具体物 (「媒体」) としてのパスワード／ヒントが持つ属性

記述物、記述形式、保持方法、など

⇨ (主として) 他人に渡る／見られる危険度 に関係する

(b) 情報 (「記号」) としてのパスワード／ヒントが持つ属性

桁数、文字種、規則性、意味、相互関連性、など

⇨ (主として) 他人に渡り／見られたときに、
パスワードを推定される危険度に関係する

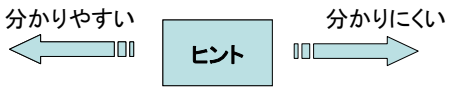
ヒントから元のパスワードの思い出し／推定 (暗号破り) が
容易か、困難か? ＝これがこの問題の焦点

情報としてのパスワード／ヒントの諸属性

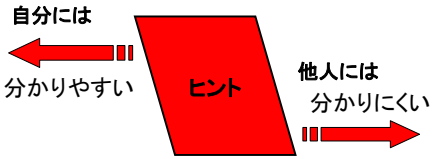
パスワードの分かりやすさ	「分かりやすい」	「分かりにくい」
	パスワードを覚えやすい、 ヒントから思い出しやすい、 ヒントから推定しやすい	パスワードを覚えにくい、 ヒントから思い出しにくい、 ヒントから推定しにくい
単純さ	**単純である**	複雑である
桁数／文字数	4 桁 7±2 桁 まで	8 文字 16 文字 (クレジット番号) 24 文字 (ソフトのキー番号)
文字種	数字 (10種) 英字 (26種) 英数字 (36種)	英数＋特殊文字＝(46種) 英数＋英大文字＝(62種)
規則性	規則的な要素を入れる: 1111…、123…、….321、 121212…、abcdef…. abcd 1234 efgh 5678	規則性を無くす 並ぶ順番を不規則にする ごちゃまぜにする 究極的には乱数でランダムに

単語	・1つの単語で構成する ・単純な文にする ・アイウエオ作文 … ・しりとり	・いくつかの単語を組み合わせる ・単語の中で文字の順番を変える ・意味の通らない文 ・単語を重ねて組み合わせる ・単語の途中の文字からしりとり
意味	・自分の情報 ・常用単語(名詞、固有名詞) ・好きな単語、好きなもの ・ある仲間(範疇)の言葉	・よく知られていない単語 (ロシア語、イタリア語つづり) ・普通の人が知らない単語 (専門用語、特別な地名、方言) ・連想から外れた単語
他のパスワードとの関係	・パターンが同じ ・一部分だけを変える ・意味につながりがある	・まったく独立な違うパターンにする ・複数部分を変える ・不規則に並べる
パスワードの階層	1段階のパスワード	2段階 (多段階) のパスワード (パスワードで入ってから、もう1つのパスワードを要求する)

ヒントを 分かりやすくしたり、
分かりにくくしたりするだけでは、
解決策にならない。

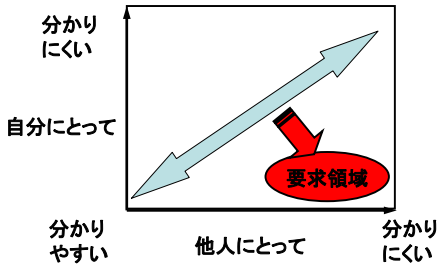


本課題の要求は、



**TRIZでいう「物理的矛盾」
として理解した。**

**その矛盾を、
解読する「主体」によって
分離すればよい。**

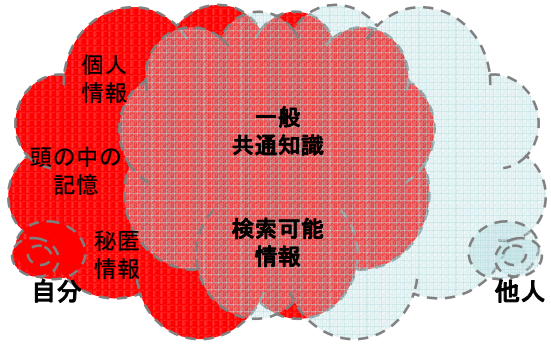


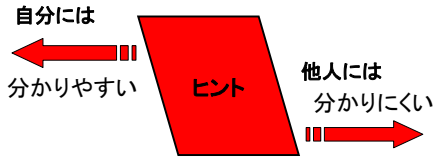
自分と他人のモデル

問題になる相手は
「悪意のある他人」だから、

自分だけが知っている情報
の範囲は意外と狭くて、

どんどん侵食されている
と考える必要がある。





この理解を踏まえて、TRIZの40の発明原理を使ってアイデア出しをした。
また、その結果を整理し、再考察した。

解決策の基本方針

(1) 自分が設定するパスワードとお仕着せのパスワードとは区別して扱う。
ヒントの作成法や所持方法に関しても。

(2) ダミー情報をヒントの中に積極的に紛れ込ませる

(3) 汎用的、一律的でない独自の変換法を作り、それを使ってヒントを作る。

(4) 比較的やさしい（独自の）暗号化（変換）を2段階に行ない、ヒントを作る。

(5) ヒントを逆変換する方法（ヒントの解読法）は別に暗号化して所持する

(6) これらの解決策を組み合わせて使う。

(1) 自分が設定するパスワードとお仕着せのパスワードとは区別して扱う。

自分が設定するパスワード

パスワードの作り方自身が
問題の中心

パスワードを
自分には分かりやすく、
他人には分かりにくく 選ぶ

パスワードを覚えておけること
が多い。

--> できるだけ省略した形の
ヒントにする
意味による関連が中心。

お仕着せのパスワード

パスワードは一方的に与えられる。

乱数的で、複雑なことが多い。
各文字には関連性がない。

パスワードを覚えておけない。

個別の文字を完全に復元できる
ことが必要。

--> ヒントに入れるべき情報を
省略できない。
意味による変換は使わない。

(2) ダミー情報をヒントの中に積極的に紛れ込ませる

自分が設定するパスワード

自分用には、

ヒントそのものは、ごく簡単な
削減した情報でよい。
それをダミー情報の中に
まぎれこませる。
(ダミーの海の中に、
小さなヒント)

他人には、

ダミー情報とヒントとを
区別できない。

お仕着せのパスワード

パスワードの情報 に比べて、

・削減したヒント:
→ 自分でも思い出せない。ダメ。

・対応したヒント:
→ 自分だけでなく、他人にも、
解読が比較的容易。ダメ。

・余分な情報 (ダミー) を含むヒント:
→ 自分はダミー削除容易。
他人は、ダミーの除去困難で、
解読困難。 → 良い方針。

(3) 汎用的、一律的でない独自の変換法を作り、それを使ってヒントを作る。

自分が設定するパスワード

パスワードの設定に際して、
一般名詞 (汎用的) を使わず、
規則的なものを使わない。

自分の造語 (＝独自の語)。
ランダムに生成し、語呂合わせが
できる適当なものを選ぶ。

ヒントは、意味の連想 (変換)で作る。

ありきたり (汎用的)な連想でなく、
パスワードごとに臨機応変の
(一律的でない) 連想を用いる。

お仕着せのパスワード

パスワード → ヒントの変換が問題。

変換がありきたり (汎用的)だと、
ヒント→パスワードの解読
(逆変換)も容易になる。
(解読される危険が大きい)

部分的に変換を作用させる
＝ 一律でない (局所的)
(ダミーも、一律でない効果がある)

汎用的でない＆一律的でない
→独自の変換法。
他人が推定しにくい。

(4) 比較的やさしい (独自の) 暗号化 (変換) を2段階に行ない、ヒントを作る。

自分が設定するパスワード

パスワードから、連想による変換を
2段階で行ない、ヒントを作る。

パスワード
-- (連想1) -> --(連想2)->
ヒント

1回の連想で特別なヒントを
作るのは難しい。
2回の連想で変換すると、
随分違ったヒントが得られる。

自分には覚えやすく、
他人には分かりにくい。

お仕着せのパスワード

パスワードから、比較的簡単な変換
を2段階で行なう。

パスワード
-- (変換1) -> --(変換2)->
ヒント

各変換法はやさしいものにする。

ダミーの挿入/削除は容易な変換。
局所化も容易な変換の例。

(5) ヒントを逆変換する方法 (ヒントの解読法) は別に暗号化して所持する

自分が設定するパスワード

自分が設定した場合には、
パスワードも ヒントも
覚えておきやすい。

ヒントさえあれば、十分であろう。

お仕着せのパスワード

ヒントだけがあっても、
ヒントを逆変換する方法
(ヒントの解読法) を覚えておく
のは難しい。

==> 逆変換法のメモが必要。

このメモも何らかの形で暗号化
(符号化) しておく必要がある。

この暗号化したメモは、
ヒントとは別に所持するのがよい。

(6) これらの解決策を組み合わせて使う。