TRIZ/USIT 適用事例：パスワードを思い出させる方法

上田祐太朗 、鍋島裕貴、 中川　徹 （大阪学院大学）

概要

本件は情報学部 3 年生のゼミでの、TRIZ/USIT による問題解決演習（半年余）をまとめたものである。コンピュータ利用でも日常生活でも、しばしばパスワードを使うようになった。自分が選択・設定した簡単なものから、システム（先方）から指定された乱数的な複雑なものまでが多数あり、頭で記憶できる範囲を越えている。このパスワードを必要に応じて思い出させるための補助的情報（「ヒント」）が、具体的な形で必要である。その「ヒント」をどのように作ればよいのかが本件の課題である。機能分析、属性分析、などを通じて問題を掘り下げた。「ヒント」は他人に見られ／使われると、パスワードを破られる危険が増大する。そこで、「ヒント」は自分には分かりやすく、一方、他人には分かりにくい必要がある。これは TRIZ でいう物理的矛盾であり、解読する「主体」によって分離すべきであると認識した。さらに TRIZ の 40 の発明原理をベースにして種々の解決策アイデアを出した。望ましい解決策は、いくつかの基本的な考え方に従い、簡単な変換法（暗号化法）を組み合わせて利用することであろう。

内容説明

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ことが多くなった。自分で設定できる 4 桁数字や 8 桁までの英数字などの場合から、システムが乱数で生成して割り当ててきた12桁の英数字などまで、一人で多数の ID/パスワードを持っている。それらは記憶できる範囲をはるかに越えている。

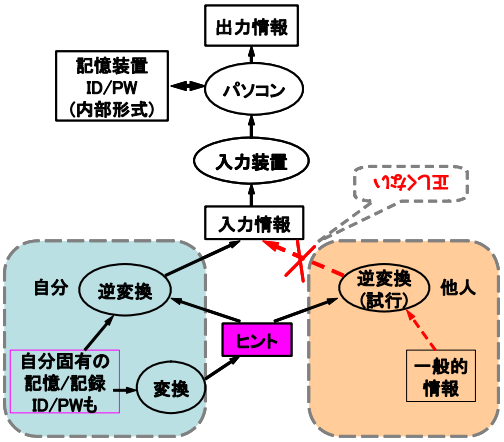
システムから ID とパスワードの入力を求められ、それらを覚えていない場合に、思い出すためにはどのようにすればよいのか？何らかのメモによる補助が有効だが、それが悪意のある他人に見られる／使われると重大な被害が生じる。他人に見られたとしても大丈夫な、パスワードを思い出させるヒントをどのように作ればよいのかが、本研究の課題である。

本研究は、2008 年 10 月から半年余り、情報学部の 3 年生のゼミで、TRIZ およびUSIT を用いて、議論・検討した結果をまとめたものである。

問題設定としては、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(往々乱数的で複雑な)場合の両方を扱う。ヒントを用意する媒体は、主として紙ベースで持ち運ぶものとし、コンピュータや携帯電話などの内蔵形式のものは後日別途考えることにした。

本件の機能関係のモデルを図のように描いた。ここで「ヒント」は、何らかの具体的な形をもった情報であり、他人の目に触れる危険も想定している。この「ヒント」は、自分には(自分が設定した、またはお仕着せの複雑な)パスワードを復元することを助けるが、一方、他人にはパスワードの推定を非常に困難にしなければならない。

ついで、「ヒント」（およびその作成法と復元法）が持つ属性を分析した。桁数、文字種、規則性、パスワード



の個数、相互関連性、意味など、多様な属性がある。これらの、情報としての抽象的な属性の他に、媒体(紙など)への記述形式や保持方法などの具体的な属性もある。

これら種々の属性を使って、「ヒント」を（パスワードへの復元に関して）「分かりやすくする」ことも、「分かりにくくする」ことも容易にできるが、それだけでは解決策にならない。「自分」には分かりやすく、「他人」には分かりにくいことが、本課題の要求である。われわれはこれを、TRIZ でいう「物理的矛盾」として捉え、(解読する)「主体」によって分離すべきことを理解した。

この理解を踏まえて、40 の発明原理を用いて、種々の解決策を考察した。「自分が設定したパスワードとお仕着せのパスワードとは区別した扱いにする」、「ダミー情報を積極的に紛れ込ませる」、「汎用的、一律的でない独自の（すなわち他人が推定しにくい）変換法を作る」、「比較的やさしい（独自の）暗号化（変換）を 2 段階に行なう」、「変換/逆変換の方法は別に暗号化して所持する」などの解決策があり、これらを組み合わせて使うことが適切であろうと考えている。