忘れられる権利を有する生体認証と補助情報を付帯させた生体認証の提案

一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

バイオメトリクス研究会資料
Proceedings of Biometrics Workshop

忘れられる権利を有する生体認証と補助情報を付帯させた生体認証の提案

眞野 勇人† 米山 裕太† 高橋 健太‡ 西垣 正勝†

†静岡大学大学院情報学研究科 〒432-8011 浜松市中区城北 3-5-1
‡(株)日立製作所横浜研究所 〒244-0817 横浜市戸塚区吉田町 292

E-mail: nisigaki@inf.shizuoka.ac.jp

あらまし 本稿では，生体認証におけるプライバシ保護と利便性に関する要求に対して，それぞれの解決策を模索する．プライバシ保護の要求に対しては，生体情報に関する「忘れられる権利」を満たした生体認証の実現を目指し，ある程度の期間で自然に入れ替わる身体部位を利用する認証方式を提案する．利便性の要求に対しては，生体情報のマスキングや誤り訂正を行うための補助情報の管理が容易な生体認証の実現を目指し，補助情報を生体情報に付帯させる認証方式を提案する．

キーワード 生体認証，忘れられる権利，テンプレート保護，補助情報，利便性

Proposals of biometrics with the right to be forgotten and biometrics with self-recoverability

Yuto MANO† Yuta YONEYAMA† Kenta TAKAHASHI‡ Masakatsu NISHIGAKI†

†Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
‡Hitachi, Ltd. 292 Yoshida, Totsuka, Yokohama, 244-0817 Japan

E-mail: nisigaki@inf.shizuoka.ac.jp

Abstract The aim of this paper is address the privacy protection and usability requirements in the biometric authentication. For the privacy protection requirements, the biometrics which satisfies “the right to be forgotten” is essential, and therefore we propose to use a human body part that is replaced naturally in some period by new tissues. For the usability requirements, it is important to improve the handle ability of the helper data that are used for the masking/error-correction of the biometric information, and thus we propose to attach the helper data directly to our body parts.

Keyword biometrics, right to be forgotten, template protection, helper data, usability

1. はじめに

生体認証とは，人間の身体的特徴や行動的特徴から個人を認証する技術である．通常の生体認証では，事前に採取した生体情報をテンプレートとして登録し，認証時に取得した情報とテンプレートを比較することで認証を行う．近年では実用化が進み，PC，ATM，パスポートの認証手段としても利用されてきている．さらに，公開鍵基盤（PKI）における秘密鍵を生体情報で置き換える「テンプレート公開型生体認証基盤（PBI)」が提案されている[1]．PBI の実現によって，今後さらなる生体認証の普及が予想される．

生体情報は，パスワードやトークンを用いた認証方式と異なり，忘却・紛失・盗難の恐れがないという利点がある．しかし一方で，生体情報には大きく以下の二つの課題がある．一つ目の課題（課題 1）は，生体情報は基本的に生涯不変であり，任意に更新できないことである.生体情報は,個人の身体的な情報であり，生体情報から本人を特定することや，本人に関する副次的な情報を得ることが可能である．そのため，生体情報はプライバシ要求の高い情報であり，安全性の面でも生体情報の漏えいを防ぐ必要がある．二つ目の課題（課題 2）は，体調や環境，読み取り時の状況の変化などが原因で，生体情報に揺らぎが発生することである．生体情報のマッチングを正しく行うには，生体情報の誤差を吸収する必要がある．

課題 1 に関する近年の動向の一つとして,「忘れられる権利」がある．この権利は，インターネットにおけるプライバシ保護の在り方として提唱されていたものであるが，この程，EU が 2012 年に発表した一般データ保護規則案の 17 条において実際に明文化されるに至った[2]．インターネット上のユーザのプライバシ情報は，ユーザ自身の意思によって，その削除が行われなければならず，プライバシ情報を管理するサービスプロバイダは，ユーザからの削除要求に従い，当該

データを削除することが義務付けられる．

生体認証システムにおいては，ユーザからの依頼があった場合，システム管理者が登録テンプレートを削除することを保証しなくてはならない．しかし，ユーザがシステムに削除要求を行っても，本当にシステムからテンプレートを削除するかどうかはシステム管理者に委ねられることとなる．生体認証の場合は登録情報(生体情報)そのものがプライバシ情報であるため，パスワードを変更する等の「ユーザ側での対策」を講ずることができない．

この問題に対し，テンプレート保護型生体認証方式が提案されている．その代表例が，生体情報と乱数情報を組み合わせることにより，テンプレートを更新可能とするキャンセラブル生体認証[3]である．しかし，登録テンプレートは生体情報をマスクしているに過ぎず，ある種の攻撃が成功すれば，生体情報を取り出せる可能性がある．事実，同一人物の登録テンプレートを複数収集し，乱数情報をホワイトノイズとしてキャンセルすることで元の生体情報を抽出するといった攻撃が提案されている[4]．

また，この乱数情報は，補助情報として認証の際にも必要となるため，IC カードなどのトークンや第三者機関のサーバに格納することになる．乱数情報をトークンに格納してユーザ自身が管理する場合，これを常に所持することが求められる．乱数情報をサーバに保管する場合，乱数情報をダウンロードするためのパスワードなどの情報をユーザが常に記憶していなければならない.トークン所持により紛失,盗難のリスクが，パスワードの記憶により忘却のリスクが発生する．すなわち，この方式では生体認証の利点を大きく損ねることになる．サーバに保管する場合は、さらにサーバの運用コストも発生する．秘密分散およびマルチパーティプロトコルを用いることで利便性を損なうことなく補助情報の管理を行うことも可能である[5]が，この場合もサーバの運用コストがかかる．

課題 2 に関しては,バイオメトリック暗号の分野で,誤り訂正符号等を用いて生体情報の誤差を訂正する方法が多数研究されている[6,7]．これらの方法では，生体情報の誤り訂正のための情報を補助情報として用意する[8]．ここで，補助情報は IC カードなどのトークンや第三者機関のサーバに格納する必要がある．このため，課題 1 と同様，ユーザの利便性の低下が問題となる．

利便性に関する最新動向としては，使い捨て RFID トークンを身体に直接装着して認証を行う方法が研究されている．具体的には，カプセル型の認証トークンを飲み込む方式や認証トークンを皮膚に張り付ける方式が提案されている[9]．これらの方式は，認証トークンを身体の一部として管理できるため，生体認証の利便性（忘却・紛失・盗難の恐れがない）を維持したまま，疑似的なワンタイム生体認証として機能する．ただし，トークンのみで認証を行うため，トークンの偽造に関する脆弱性が残る．

課題 1 および課題 2 に関する上述の議論の中から，生体認証が有するべき要求仕様を括り出すと以下の二つになる．

要求 1（プライバシ保護に関する要求）:

生体情報そのものを更新することができる生体認証の実現が理想的である．

要求 2（利便性に関する要求）:

補助情報の利用においてはユーザの利便性を損なうことのない生体認証の実現が理想的である．

本稿では，要求 1 および要求 2 に対して，それぞれの解決策を模索する．要求 1 に対しては，ある程度の期間で自然に入れ替わる身体部位を利用する認証方式を提案する．要求 2 に対しては，補助情報を生体情報に付帯させる認証方式を提案する．

2. 関連研究

本章では，要求 1 および要求 2 に対する関連研究としてキャンセラブル生体認証[3]，Fuzzy Commitment [10]，生体貼付型の使い捨て生体認証トークン[9]を紹介する．

2.1. キャンセラブル生体認証

キャンセラブル生体認証では，乱数情報を用いて生体情報をマスクし，その情報をテンプレートとしてサーバに登録する．乱数情報は，IC カードなどのトークンまたは第三者機関のサーバに保管され，認証の際に補助情報として使用される．

登録フェーズは以下の手順で行われる．

1. 登録者の生体情報Xを読み取る．
2. 登録者に対して乱数Rを生成し発行する．
3. 乱数Rを用いて生体情報Xを$\mathrm{X} \to \mathrm{T} = F_R(X)$と変換する．
4. $F_R(X)$をサーバに登録する．

認証フェーズは以下の手順で行われる．

1. 認証要求者の生体情報X'を読み取る．
2. 認証要求者の乱数Rを取得する．
3. 乱数Rを用いて生体情報X'を$\mathrm{X}' \to F_R(X')$と変換する．
4. $F_R(X)$と$F_R(X')$が十分類似していれば認証成功とする．

ここで，$F_R(\cdot)$は乱数Rによる変換処理を表す．乱数や変換関数を変更することで，テンプレート情報の更新が可能である．

2.2. Fuzzy Commitment

Fuzzy Commitment [10]は，バイオメトリック暗号の代表的な方式の一つである．Fuzzy Commitment では，生体情報を用いて秘密鍵をコミットする[1]．登録時と認証時の生体情報が十分近い場合に限り，コミットメントから秘密鍵を正しく復元することでき，この秘密鍵を用いて，認証や暗号，署名を行う．コミットメントは，IC カードなどのトークンまたは第三者機関のサーバに保管され，認証の際に補助情報として使用される．

登録フェーズは以下の手順で行われる．

1. 登録者の生体情報Xを読み取る．
2. 生体情報Xと同じビット長の誤り訂正符号$C = \{Ci\}$から符号語をランダムに選択し，これを秘密鍵Sとする．ここで，Cはtビット誤り訂正符号とする．
3. 秘密鍵Sと生体情報Xから補助情報$R = S \oplus X$を生成する．ここで，記号'⊕'は排他的論理和を表す．

認証フェーズは以下の手順で行われる．

1. 認証要求者の生体情報X'を読み取る．
2. 認証要求者の補助情報Rを取得する．
3. 補助情報Rと生体情報X'から$X' \oplus R$を生成する．$X' \oplus R = S \oplus (X \oplus X')$であるため，Xと$X'$のハミング距離がtよりも小さければ，$X' \oplus R$を誤り訂正することによって秘密鍵$S$を復元できる．
4. 登録時と認証時のSを比較して，一致していれば認証成功とする．

2.3. 生体貼付型使い捨て認証トークン

生体認証と同様に紛失や盗難の恐れのない認証を実現する方式として，RFID（Radio Frequency IDentification）を利用した使い捨て認証トークンを身体に直接装着する方法が研究されている．RFID タグを内包するカプセルを飲み込んで認証を行う方式や，RFID タグを皮膚に張り付けて認証を行う電子タトゥーが提案されている[9].

本稿執筆時現在において，これらの技術は商用化に至っていないが，疑似的にワンタイム生体認証を実現する方式として注目されている．しかし，認証の主体はトークン本体であるため，トークンの偽造に関する脆弱性が残る．特に電子タトゥー方式では，使い捨てられた RFID が悪用される恐れがある．また，カプセル方式では，異物を飲み込むことや，異物を体内に保管することに不快感を覚える利用者がいるかもしれない．

[1] Fuzzy Commitment は，秘密鍵（乱数）を用いて生体情報をコミットする方法であるという捉え方をすると，キャンセラブル生体認証の一方式と考えることも可能である．

3. 提案方式

本章では，1 章にて示した要求 1 および要求 2 に対して，それぞれの解決策を提案する．要求 1（プライバシ保護に関する要求）に対しては，生体情報に関する「忘れられる権利」を満たす生体認証の実現を目指し，ある程度の期間で自然に入れ替わる体の部位を利用する認証方式を検討する．要求 2（利便性に関する要求）に対しては，生体情報のマスキングや誤り訂正を行うための補助情報の管理が容易な生体認証の実現を目指し，補助情報を生体情報に付帯させる認証方式を提案する．

3.1. 忘れられる権利を有する生体認証

要求 1（プライバシ保護に関する要求）を満たす生体認証を実現するために，生体情報そのものを更新することができる生体認証について検討する．生体情報の更新を実現するためには，ある任意の期間で生体情報が入れ替わることが必要である．生体組織の入れ替わりとしては，代謝や老化が考えられる．ここでは，代謝を利用する例を二つ考えてみよう．

一つ目は，代謝が顕著な生体組織である爪や毛髪を用いた生体認証である．爪は毎日伸び続けることによって生え変わる．毛髪は毎日伸び続けた後，抜け落ちる．このため，ある日時の爪または毛髪の生体情報をテンプレートとして登録することによって，本人であっても爪が生え替わったり，毛髪が抜け落ちるまでの期間しか認証に成功しない生体認証が実現する．ただし，爪や毛髪に関する生体情報の内，何を特徴量として利用すれば適切であるかの検討が必要である．

二つ目は，生体組織にわざと傷をつけるという方法である．人間の体には代謝にともなう自然治癒機能が備わっているため，時間経過と共に傷は癒えて消えていく．傷をつけた生体組織は再び全く同じ傷をつけることができない限り，二度と再現できない．このため，傷をつけた生体組織の生体情報をテンプレートとして登録することによって，本人であっても傷が治るまでの期間しか認証に成功しない生体認証が実現する．ただし，実際に身体に傷をつける方式は現実的ではない．

一つ目の方法と二つ目の方法を組み合わせて，爪にわざと傷をつけるような方法も考えられるだろう．爪には痛覚がないので，ある程度であれば表面を薄く削っても苦痛はない．また，爪に瞬間接着剤を薄く塗ったり，小さな装飾品を（日常生活の中では剥がれないように）貼り付けても良いだろう．女性の間でネイルアートが流行していることから，爪を綺麗に加工するという認証方式であれば，ユーザにも受け入れられるのではないかと推測される．

以下では，爪に傷をつける例を用いて忘れられる権

利を有する生体認証の手順を説明する（図 1）.

3.1.1. 登録フェーズ

1. 爪に任意の傷をつける.
2. 傷をつけた爪の生体情報を読み取り，その特徴量をXとする.
3. Xをテンプレートとして登録する.

3.1.2. 認証フェーズ

1. 爪の生体情報を読み取り，その特徴量をX′とする.
2. XとX′が十分類似していれば認証成功とする.

爪はある日数で生え替わってしまうため，本人であろうとも認証に成功する期間が限られることになる.

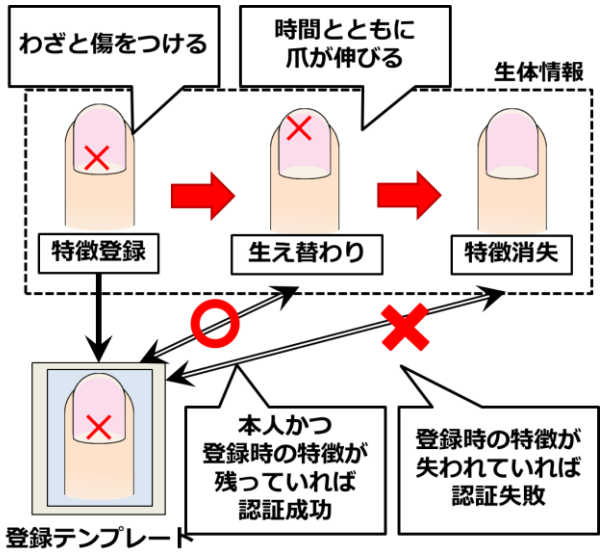

図 1：忘れられる権利を有する生体認証の概念図

3.2 補助情報を付帯させた生体認証

要求 2（利便性に関する要求）を満たす生体認証を実現するために，補助情報（キャンセラブル生体認証における乱数情報，バイオメトリック暗号における誤り訂正情報）を生体情報に付帯させる生体認証について検討する.

電子タトゥー[9]においても RFID 回路を皮膚に直接貼り付ける方法が検討されているが，装着していることがほとんど感じられない貼付物であれば，ユーザも負担なく貼付物を常時装着できるのではないだろうか. 例えば，医療用のサージカルテープ[11]などは，装着感や違和感もほとんどなく，日常生活上の耐久性も備えている. そこで，補助情報を QR コードのような形で貼付物に印刷し，これを生体に直接貼付する方法を考えてみよう.

生体情報そのものに補助情報を付帯させることによって，ユーザは補助情報の管理から解放される. また，生体情報の提示とともに補助情報を読み取ることが可能であり，生体情報の提示のみで生体情報のマスキング（キャンセラブル生体認証）や生体情報の復元（バイオメトリック暗号）が可能となる.

以下では，Fuzzy Commitment の例を用いて補助情報付帯型の生体認証の手順を説明する（図 2(a)）. 同様の手順でキャンセラブル生体認証も実現可能である（図 2(b)）.

3.2.1. 登録フェーズ

1. 登録者の生体情報Xを読み取る.
2. 生体情報Xと同じビット長の誤り訂正符号 $C = \{Ci\}$から符号語をランダムに選択し，これを秘密鍵Sとする. ここで，Cはtビット誤りを訂正符号とする.
3. 秘密鍵Sと生体情報Xから補助情報$R = S \oplus X$を生成する. ここで，記号'⊕'は排他的論理和を表す.
4. 補助情報Rを QR コード化し，貼付物に印刷する.
5. ユーザは貼付物を身体に貼る.

貼付物を貼る位置は，手順 1 で生体情報を読み取った部位が隠れない位置である必要がある. また，手順 1 で生体情報を読み取った部位の近傍に貼付するようにすれば，生体情報と補助情報を一度にスキャンできるため，認証装置の小型化と認証手順の簡素化が達成できる.

3.2.2. 認証フェーズ

1. 認証要求者の生体情報X′を読み取る.
2. 認証要求者の貼付物から補助情報Rを読み取る.
3. 補助情報Rと生体情報X′から$X' \oplus R$を生成する. $X' \oplus R = S \oplus (X \oplus X')$であるため，XとX′のハミング距離がtよりも小さければ，$X' \oplus R$を誤り訂正することによって秘密鍵Sを復元できる.
4. 登録時と認証時のSを比較して，一致していれば認証成功とする.

ユーザが貼付物を剥がしてしまえば，本人でさえ認証に成功しなくなるため，ユーザ自身が認証可能期間をコントロールできる. 貼付物に印刷されているのは補助情報のみであるので，不正者が貼付物を取得したとしても，正規ユーザの生体情報を入手できない限り悪用は難しい.

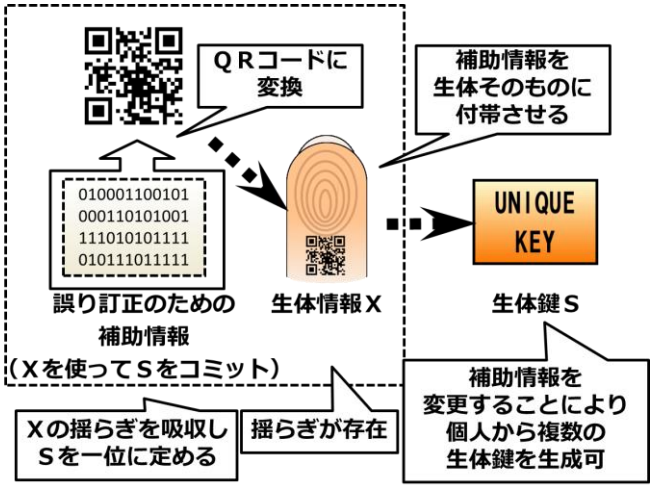

図 2(a)：補助情報付帯型生体認証（バイオメトリック暗号）の概念図

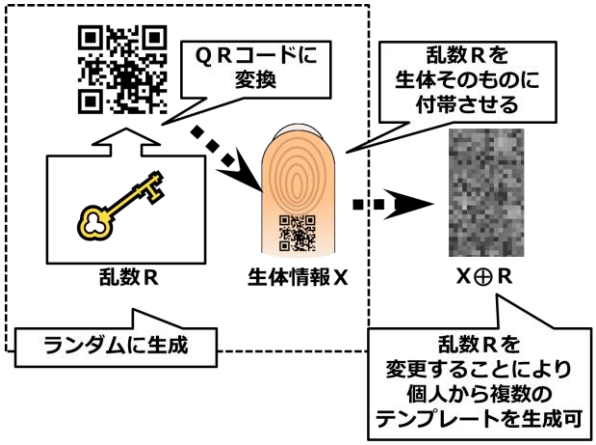

図 2(b)：補助情報付帯型生体認証（キャンセラブル生体認証）の概念図

4. 考察

4.1 忘れられる権利を有する生体認証

生体情報そのものを更新することができる生体認証となっているため，プライバシ保護の観点からは理想的な認証方式といえる．キャンセラブル生体認証のように，ユーザが補助情報（乱数情報）を管理する必要もないため，生体情報の有する利便性の高さも損なうことのない認証方式となっている．

本稿では爪や毛髪などの「自然に生え変わる生体情報」を利用するというアイデアを提案したが，そのような生体情報に対する具体的な特徴量の抽出方法，および認証精度に関しては今後の検討課題である．また，不正者が抜け落ちた毛髪を盗むことによって,なりすましができてしまう可能性や，成長速度のゆらぎによって認証可能期間を定められないという問題についても対処していかなければならない．

生体情報の加工については，登録時に爪の表面に傷をつけたり，装飾を施すなどの方法の実現可能性を調査していく必要がある．爪を加工することによって，爪側から照射した赤外線光に回折を生じさせ，スキャンされる指静脈パターンを変化させるようなことも可能かもしれない．また，指表面に瞬間接着剤を塗布することによって，指紋パターンを変化させるような方法も考えられる．

4.2 補助情報を付帯させた生体認証

補助情報を生体情報に付帯させることによって，利便性を低下させることなく，キャンセラブル生体認証やバイオメトリック暗号を実現できる．

本稿では補助情報を QR コード化するというアイデアを提案したが，既存のキャンセラブル生体認証やバイオメトリック暗号における補助情報の情報量は一般的に大きいため，情報を書き込むためにある程度以上の面積が必要であると考えられる．印刷面積を小さくするための符号方式が必要である．

補助情報を身体に付帯させる方法についての検討も重要である．現時点においては，我々は以下の二つの方法について調査をしていく予定である．一つは補助情報をシール形式で体表面に張り付ける方法，もう一つは補助情報を塗料で体表面に吹き付ける（印刷する）方法である．後者の方法では，可視光線では発色せずに紫外線に反応する塗料を用いるなどの工夫によって，ユーザの心的負担を抑えることも可能であると考える．

5. まとめ

本稿では，生体認証におけるプライバシ保護と利便性に関する要求に対して，忘れられる権利を有する生体認証と補助情報を身体に付帯させる生体認証に関するアイデアを提案した．実用化に向けて，具体的な方法の検討を行っていくとともに，様々な実験を通じてその可用性を評価していくことを今後の課題としたい．

参考文献

[1] 高橋健太等：“秘密鍵に曖昧さを許す証明可能安全な電子署名と，テンプレート公開生体型認証基盤への応用,” 2013年暗号とセキュリティシンポジウム (SCIS2013), 2013.

[2] EUROPEAN COMMISION: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, available from < http://www.aclweb.org/anthology/P/P12/P12-2061.pdf> (accessed 2013/08/20).

[3] N. K. Ratha, J. H. Connell and R. M. Bolle: Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, Vol. 40, No. 3, pp.614-634 2001.

[4] 披田野清良等：Fuzzy Commitment Scheme における生体情報の推定困難性に関する一考察，情報科学技術フォーラム (FIT2011), pp.229-230, 2011

[5] K. Takahashi and S. Hirata: Parameter management schemes for cancelable biometrics, Computational Intelligence in Biometrics and Identity Management (CIBIM2011), pp.145-151, 2011.

[6] X. Boyen: Reusable cryptographic fuzzy extractors, Proceedings of the 11th ACM conference on Computer and communications security (CCS2004), pp.82-91, 2004.

[7] Y. Dodis, et Al: Robust fuzzy extractors and authenticated key agreement from close secrets, In Advances in Cryptology (CRYPTO2006), pp.232-250, 2006.

[8] Y. Dodis, et Al: Fuzzy extractors: how to generate strong keys, Advances in Cryptology (EUROCRYPT2004), pp.523-540, 2004.

[9] V. Woollaston: The hi-tech tattoo that could replace ALL your passwords: Motorola reveals plans for ink and even pills to identify us, Mail Online, available from < http://www.dailymail.co.uk/sciencetech/article-2333203/Moto-X-Motorola-reveals-plans-ink-pills-replace-ALL-passwords.html > (accessed 2013/08/20).

[10] A. Juels, and M. Wattenberg: A fuzzy commitment scheme, Proceedings of the 6th ACM conference on Computer and communications security (CCS1999), pp.28-36, 1999.

[11] 3M 住友スリーエム：3M|サージカルテープ・伸縮包帯|医療従事者向け｜医療用製品｜スリーエムヘルスケア，入手先 <http://www.mmm.co.jp/hc/medical/pro/tape/> (参照 2013/08/20).