Vol.2010-CSEC-51 No.11
2010/12/10

多要素認証プラットフォームにおける認証技術組み合わせの評価方法について

山田 慈朗[†] 八木 哲志[†] 上野 磯生[†]
北川 毅[†] 高杉 英利[†]

十分なセキュリティを確保するために有用な多要素認証を実施する場合には認証技術の組み合わせを選ぶ必要がある．そこで，認証技術の組み合わせの優劣を評価する方法を提案する．

An Evaluation Method of Combined Authentication Techniques for a Multifactor Authentication Platform

Jiro YAMADA[†] Satoshi YAGI[†] Isoo UENO[†]
Takeshi KITAGAWA[†] and Hidetoshi TAKASUGI[†]

To select a suitable combination of authentication techniques, we propose an evaluation method of combined authentication techniques for a multifactor authentication platform.

1. はじめに

企業向けのクラウドコンピューティングやSaaS(Software as a Service)の普及に伴い，サービスを利用する際に認証が必要なWebサイトが増加している．現在，その認証には，ユーザIDとパスワードを組み合わせて実施するID／パスワード認証が多く用いられている．しかしながら，顧客情報や金融情報のようにセキュリティ的に重要な情報を取り扱うサービスにおいては ID／パスワード認証単体を実施するような単一の認証ではなく，複数の認証を組み合わせることが推奨されている[1]．そのため，金融情報を扱うインターネットバンキングのWebサイトにおいては，ID／パスワード認証に加えて乱数表による認証を実施する等，複数の認証手段を組み合わせることにより，認証の強度を確保している．また，クレジット業界でのガイドライン[2]，政府機関関係のガイドライン[3][4]においても多要素認証の記述があり，多要素認証導入の必要性が一段と高まってきている．

一方，多くのWebサイトが個別に認証を求めることになり，多数のIDやパスワードが必要となり，それらの管理が煩雑となるため，結果的に各ユーザがメモにID／パスワードの一覧を記載しておく等，ID／パスワードが漏洩・流出するリスクが高まっている．また，各 Web サイトにログインする度に，それぞれの ID／パスワードを入力することになり，ユーザにとっては不便でもある．上記を解決するための技術として，認証連携（シングルサインオン）技術があるが， ID／パスワードが漏洩したときに複数のサイトに侵入されてしまうことから，シングルサインオンを安全に利用するためには通常用いられる認証レベルよりも強固な認証を採用することが必要不可欠である．

しかしながら，実際に多要素認証を実施する際には，認証技術の組み合わせの優劣を評価し，組み合わせを選ぶ必要があるが，パスワード強度の評価手法[5]のように認証技術単体の評価手法はあっても，認証技術の組み合わせについて参考となる評価手法は見当たらず，組み合わせに関する整理や強度に関する考察がなされていない．そこで，認証技術の組み合わせを選ぶ場合の評価方法についての考え方を新たに提案する．本稿では，まず最初に組み合わせ対象となる認証技術について分類し，回線情報を利用する認証を分類の一つとして新たに追加し，回線認証の位置付けを明らかにした．次に，単一の認証技術に対する評価方法として，パスワード強度[5]の考え方を取り込みながら，ＩＤ／パスワード認証以外の認証技術にも適用できる汎用的な評価方法を示した．さらに複数の認証技術を組み合わせる場合の評価方法に拡張し，我々が開発した認証プラットフォーム[6]にて利用可能な 10 種類の認証技術の中から 3 種類

[†] ＮＴＴコミュニケーションズ（株）
NTT Communications Corporation

を組み合わせた場合の評価結果例を示した．

2. 認証技術の分類

認証技術を分類する場合，一般的には，認証に利用する情報に基づき，記憶による認証，生体情報による認証，所有物による認証の３種類に分類することが多いが，回線による認証も分類に加えて検討することとした．これは，Web サービスの認証は通常，ネットワーク経由での認証であり，回線情報を比較的容易に入手でき，利便性の高い認証が実現できるため，回線による認証も分類に加えている．生体認証については専用装置が必要になる等，手軽に利用することが難しいため，今回は検討の対象外とした．また，認証技術の組み合わせを考える場合には，人を識別する／端末を識別する／回線を識別するといったように，識別対象による分類も重要なため，この分類も加えている．例えば，ユーザを認証するためには，認証技術の組み合わせの中に人を識別する認証が必須であることや，人・端末・回線を識別する認証を組み合わせることで，あまり利便性を落とさずに高いセキュリティを実現できるといったように，認証技術の組み合わせを考える際に識別対象による分類は有用である．各分類に対する認証技術の例も含め，図１としてまとめた．なお，認証技術の例として記載した携帯電話認証については，回線としての分類も有り得るが，本検討では所有物としての側面（例えば，所有物として盗難・紛失する場合があること）を重視し，所有物としての分類として考えることとする．

一般的な分類

利用情報による分類
記憶
生体
所有物

本検討での分類

識別対象による分類	利用情報による分類	認証技術の例
人	記憶	ＩＤ／パスワード認証 マトリクス認証
	生体	指紋・静脈認証、虹彩認証 顔認証、音声認証
	所有物	ＩＣカード認証 ワンタイムパスワード認証
端末		携帯電話認証 機器認証
回線	回線	ＮＧＮ回線認証 発ＩＰアドレス認証

図 1　認証技術の分類

3. 認証技術の評価方法

多要素認証を実施する場合には，認証技術の組み合わせの優劣を判断するために，認証技術の組み合わせに対する評価方法が必要となる．ただし，組み合わせの優劣を判断できればよいため，厳密な定量評価は不要で，目安となる相対的な評価尺度があればよい．以下に評価の基本的な考え方を示す．

まず，重要となるのが，認証を組み合わせることにより，認証強度のレベルを把握することであり，認証強度の評価を行う．ここで，組み合わせの候補を絞り込んだ後，ユーザや端末環境の対象範囲に問題が無いかといった適用範囲の確認と，利用者が簡単に認証を利用できるかといった利便性の面での確認を実施することにより，認証の組み合わせを選択する．

以下，認証強度の評価方法を示す．攻撃の難しさを数値化したものを認証強度とし，攻撃が難しい（攻撃耐性が高い）ほど認証強度が高く，攻撃が易しい（攻撃耐性が低い）ほど認証強度が低いと考える．攻撃の種類については，認証技術の種類（記憶系，所有物系，回線系）に依らず，ほぼ共通的に考えることができる基本的な攻撃と，認証技術の種類毎に異なる攻撃に分類し，それぞれの攻撃耐性を評価する．

（１）単一の認証技術の評価

単一の認証技術の認証強度については，以下の通り，認証技術に依らず共通的な基本攻撃耐性と，認証技術の種類（記憶系，所有物系，回線系）毎に異なる攻撃耐性を各々５段階評価し，最も低い評価の値を認証強度とする．

$$S_i = \min_j S_{i,j}$$

ここで，

S_i：認証技術 i の認証強度

①基本攻撃耐性

$S_{i,1}$：認証技術 i における総当たり攻撃耐性
（総当たりの組み合わせ数の大小により５段階評価を行う）

$S_{i,2}$：認証技術 i における辞書攻撃耐性
（辞書攻撃の可否と総当り攻撃耐性の大小により５段階評価を行う）

②記憶系攻撃耐性

$S_{i,3}$：認証技術 i におけるショルダーハック攻撃耐性
（盗み見る情報がキー入力情報のみか，その他の情報も必要かにより５段階評価を行う）

$S_{i,4}$：認証技術 i におけるフィッシング攻撃耐性

（静的な情報／動的な情報を盗むかどうかにより５段階評価を行う）

③所有物系攻撃耐性

$S_{i,5}$：認証技術 i における所有物の盗難時の攻撃耐性
（盗難の難しさや盗難されてもガードがかかっているかにより５段階評価を行う）

$S_{i,6}$：認証技術 i における所有物の成りすまし攻撃耐性
（認証情報の入手の難しさや複製の難しさにより５段階評価を行う）

④回線系攻撃耐性

$S_{i,7}$：認証技術 i における回線の成りすまし攻撃耐性
（任意の回線に成りすましが可能かやある条件を満足する回線のみ成りすましが可能かにより５段階評価を行う）

基本攻撃耐性としては，認証技術のほとんどで実施可能な総当たり攻撃と，総当たり攻撃を効率化した攻撃と解釈できる辞書攻撃の２つについて攻撃耐性を評価する．記憶系攻撃耐性としては，入力した情報を盗む手法として代表的なショルダーハック攻撃とフィッシング攻撃について攻撃耐性を評価する．所有物系攻撃耐性としては，所有物自身の盗難時の攻撃と所有物の情報が盗まれ，複製された場合の攻撃について攻撃耐性を評価する．回線系攻撃耐性としては，回線情報が盗まれた場合の攻撃について攻撃耐性を評価する．

各攻撃耐性の値の最小値を認証強度とする理由は，攻撃者にとってはいずれかの攻撃が成功すればよく，最も攻撃しやすい（最も攻撃に弱い）ほうの攻撃耐性の値を代表値とすべきと考えるためである．

（２）複数の認証技術の組み合わせの評価

複数の認証技術を組み合わせた場合の認証強度については，異なる種類（記憶系，所有物系，回線系）の認証技術を組み合わせたかどうかによる重み係数を乗じた上で各認証技術の認証強度の和を算出したものを認証強度とする．

$$T_I = C_k \sum_{i \in I} S_i$$

ここで，

I：組み合わせる認証技術の集合

T_I：組み合わせる認証技術の認証強度

C_k：k 種類（記憶系，所有物系，回線系）の認証技術を組み合わせる場合の重み係数

S_i：認証技術 i の認証強度

組み合わせる認証技術すべてに対して攻撃が成功しなければ認証は破られないため，各認証技術の認証強度の和を組み合わせ時の認証強度としているが，同一種類の認証技術を組み合わせる（例．記憶系の認証技術のみ組み合わせる）よりも，異なる種類の認証技術を組み合わせるほうが攻撃が難しいと考え，組み合わせる認証技術の種類の数に応じて重み係数を乗じている．なお，組み合わせる認証技術の種類の数が大きくなるほど，より攻撃が難しくなると考え，重み係数 C_k は k に関して単調増加関数を想定している．

4. 認証技術の評価結果例

我々は，高セキュリティとユーザ利便性の両立を目指し，認証の組み合わせを柔軟に設定できる多要素認証および認証連携を実現する認証プラットフォーム[6]を開発しており，本プラットフォームで利用可能な認証技術に関して評価手法を適用し，単一の認証技術および複数の認証技術の組み合わせについて評価した．

認証プラットフォームの機能概要は図３の通りであり，利用可能な認証技術は以下の１０種類である．

①ID/パスワード認証：
ID とパスワードによる認証

②マトリクス認証：
乱数表内の指定位置の乱数を入力することによる認証

③メールチャネル認証：
メールで別途送付されるワンタイムパスワードを入力することによる認証

④IC カード認証：
IC カード内の証明書情報に基づいた認証

⑤機器認証（証明書）：
端末内の証明書情報に基づいた認証

⑥機器認証（クッキー）：
端末内のクッキー情報に基づいた認証

⑦機器認証（MAC アドレス）：
端末の MAC アドレスに基づいた認証

⑧携帯電話 ID 認証：
携帯電話の ID 情報に基づいた認証

⑨発 IP アドレス認証：
端末の発 IP アドレスに基づいた認証

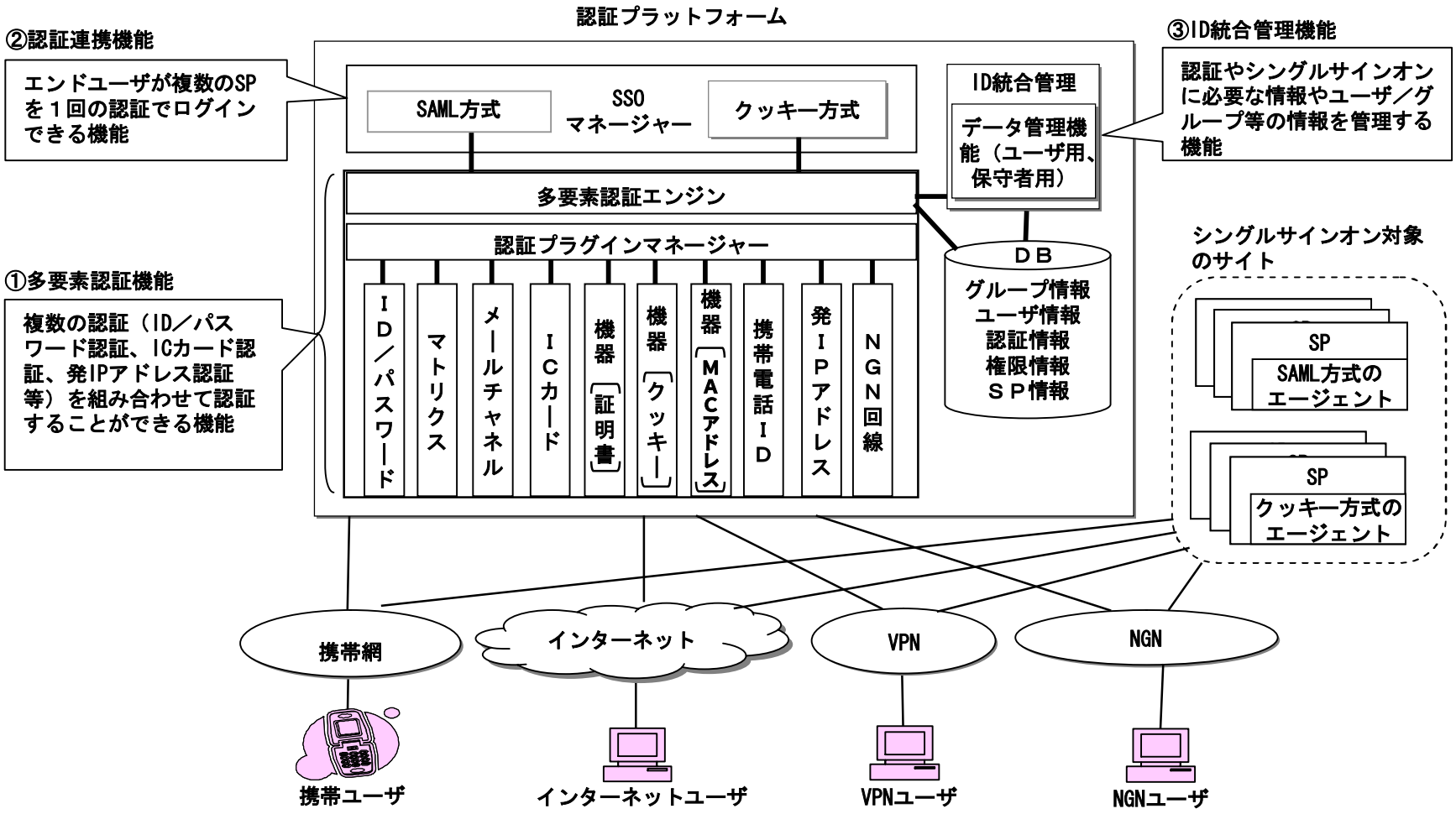

図 2　認証プラットフォームの機能構成

⑩NGN 回線認証：
NGN の回線 ID に基づいた認証

（1）単一の認証技術の評価結果例
認証プラットフォームで利用可能な認証技術それぞれについて，３節の（1）にて提示した評価方法を用いて認証強度を評価した例を表１に示す.

表 1　単一の認証技術の評価例（認証強度）

利用情報による分類	認証技術	基本攻撃耐性		記憶系攻撃耐性		所有物系攻撃耐性		回線系攻撃耐性	認証強度 S_i
		$S_{i,1}$	$S_{i,2}$	$S_{i,3}$	$S_{i,4}$	$S_{i,5}$	$S_{i,6}$	$S_{i,7}$	
記憶	ID/パスワード認証	3	2	1	2				1
記憶	マトリクス認証	3	2	3	2				2
所有物	メールチャネル認証	3	5			4	5		3
所有物	ICカード認証	5	5			4	5		4
所有物	携帯電話認証	2	5			3	5		2
所有物	機器認証（証明書）	5	5			4	5		4
所有物	機器認証(MACアドレス)	2	5			4	1		1
所有物	機器認証(クッキー)	4	5			4	3		3
回線	NGN回線認証	5	5					5	5
回線	発IPアドレス認証	2	5					2	2

（2）複数の認証技術の組み合わせの評価結果例
認証プラットフォームで利用可能な認証技術の中から，人・端末・回線を識別する認証技術を各々１種類ずつ選び，３つの認証技術を組み合わせた場合に，３節の（2）にて提示した評価方法を用いて認証強度を評価した例を表２に示す.

表 2　認証技術の組み合わせの評価例（認証強度）

識別対象による分類	利用情報による分類	認証技術	各々の認証強度 S_i	組み合わせの認証強度 T_I
人	記憶	ID/パスワード認証	1	12
端末	所有物	機器認証(クッキー)	3	
回線	回線	発IPアドレス認証	2	

この評価例では C_1=1, C_2=1.5, C_3=2 とした.

認証強度が高い認証技術を組み合わせれば，とても高い認証強度を得ることができるが，単体では認証強度が低い認証技術でも組み合わせ方によっては，簡単に利用できる認証でありながら，高い認証強度を得ることができる.

5. まとめ

十分なセキュリティを確保するためには多要素認証を導入することが重要であり，実際に多要素認証を使用する際に認証技術の組み合わせを選ぶための評価方法についての考え方を提案した．本稿では，まず最初に組み合わせ対象となる認証技術を分類し，回線情報を利用する認証を分類の一つとして新たに追加した．次に単一の認証技術に対する評価方法として，ＩＤ／パスワード認証以外の認証技術にも適用できる汎用的な評価方法を示した．さらに複数の認証技術を組み合わせる場合の評価方法に拡張した．提案評価方法は，認証強度の観点から評価するものであり，認証技術の組み合わせの優劣を相対的に評価する尺度として適用するものである．今回の検討では生体認証を検討の対象外としたが，生体認証にも適用できる評価方法への拡張が今後の課題である.

参考文献

1) FFIEC: Authentication in an Internet Banking Environment, (2005).
2) PCI Security Standards Council: Payment Card Industry （PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン 1.2.1,(2009).
3) 情報セキュリティ政策会議: 政府機関の情報セキュリティ対策のための統一基準(第 4 版), (2009).
4) 電子政府ガイドライン作成検討会: オンライン手続におけるリスク評価及び電子署名・認証ガイドライン, (2010).
5) NIST: Electronic Authentication Guideline, NIST Special Publication 800-63(2006).
6) 山田慈朗，八木哲志，上野磯生，北川 毅，高杉 英利: 認証連携機能を兼ね備えた多要素認証プラットフォームの開発，信学技報, ICSS2010-52, pp.47-52(2010).