フロント連携ワーキンググループ成果報告書（2013 年度上期）

2013 年 12 月 24 日

クラウド・ビジネス・アライアンス×ニッポンクラウドワーキンググループ

フロント連携ワーキンググループ

（目次）

1. はじめに

1-1. フロント連携ワーキンググループ

フロント連携ワーキンググループは、2009 年の CBA 設立当時から、SaaS を筆頭としたクラウドシステムをユーザ目線で使いこなすために、ユーザに見えない「縁の下の力持ち」として利便性を提供する技術を研究開発してきました。
2012 年度からは、ニッポンクラウドワーキンググループとも連携し、合同で活動を続けています。
これまで、以下のようなテーマを掘り下げて、毎月の議論を重ねてきており、その成果は実際のビジネスシーンでも活用されています。

- OpenSocial Gadget による SaaS 連携
- SAML と OpenSocial Gadget を組み合わせた認証連携
- 異なる組織間での相互認証連携

1-2. クラウドと認証

フロント連携ワーキンググループでは、これまでの活動をとおして「認証」の重要性を確認し、認証システムの機能的な深堀を実施してきました。本報告では、もう一度ユーザに近い部分での認証にかかわる問題を再検討することとし、CIJ 社を中心に認証（本人確認）方法の現状調査と、それぞれの方法の課題について検討・議論を実施しました。

2. 参加企業

株式会社ＣＩＪ

株式会社 CIJ は、「情報技術で人と社会にやさしい未来を創造します」をコンセプトに、確かな技術力とマネジメント力でお客様のご要望を実現する企業です。スマートフォンやタブレットを安心安全に利用するための無線侵入防止システムやタブレット端末を使用した会議システム等をご提供しています。

株式会社プロキューブ

株式会社プロキューブは、SOA、ESB、XSL、SAML などをキーワードとして、XML をベースとしたソリューションの提供を行っておりま す。XML をベースとすることにより、モジュールやシステム間の結合度を低くし、システムの拡張性・柔軟性・スケーラビリティを確保しています。
具体的なソリューションとして、以下のようなものがあります。
・認証基盤
・統合ディレクトリ
・ネットワーク認証管理

・ESB
・大学情報データベース
とくに大学向けの統合認証基盤は NetSoarer(ネットソアラとお読みください）シリーズとして、SAML 認証基盤、統合ディレクトリ、RADIUS サーバ、DHCP サーバを製品として提供しています。

有限会社ディアイピィ

ディアイピィは、設立以来培ってきたオープンソース Web アプリケーションに関するノウハウを活かして、コストパフォーマンスの高いシステム導入、運用を支援することを目指します。
・オンラインアンケート　LimeSurvey
・メールアーカイブ　MailArchiva
・メール問い合わせ管理　osTicket
・メール配信　PHPList
などをはじめとして、日本では普及していない海外で評判の高いソリューションも積極的に取り入れております。
昨今のクラウドコンピューティングとの高いシナジーを活かしたクラウドインテグレーションにも対応し、オープンソースの特性を活かしカスタマイズしたお客様だけのソリューションを最適な形でご提案して参ります。

株式会社ビーコンＩＴ

Unify IT をテーマに、様々なシステムの連携のソリューションを提供しています。今回 CBA のフロントエンド連携技術ワーキンググループでは幹事企業として、オープンソースの 企業情報ポータルである infoScoop を提供しております。infoScoop は OpenSocial Gadget に対応した連携の仕組みです。ソースコードは LGPL として公開されています。http://www.infoscoop.org/

ネットワンシステムズ株式会社

ネッ トワンシステムズ株式会社は、常に国内外の最先端技術動向を見極め、ネットワーク領域とプラットフォーム領域において、自ら検証した製品に高品質な技術 サービスを付加することによって、お客様のビジネス成功を目的として、生産性を高め、簡便に利活用できる IT 基盤ならびにコミュニケーションシステムを提 供しています。当該ワーキンググループへは、事務局として参加しております。

3. 認証について

日本語の「認証」には、英語の Authentication と Authorization という２つの機能が含まれており、しばしば混乱を招く要因となっています。この２つの機能を正確に表す日本語の定説は、未だに確立されていませんが、たとえば「本人確認」と「権限付与」といった意訳がわかり易いかもしれません。
ここでは、Authentication に焦点を絞って、その方法について解説します。ただし、１つの要素や経路で確認するだけの方法を比べても、あまり有意義ではありませんので、２つの要素や経路を使った、比較的「認証強度」が高いとされる方法について検討します。

3-1. 二要素認証

二要素認証とは、ユーザが知っている「知識」（ID・パスワード等）と、ユーザが持っている「所有物」（複製できない、もしくは複製しづらい機器や身体的特徴）を組み合わせることで認証強度を高める方法のことを示します。「知識」＋「知識」、「知識」＋「所有物」など組み合わせを行います。以下の表１にそれぞれの代表的な認証方式を示します。

表１　二要素認証の代表的な認証方式

ユーザが知っていること	ユーザが持っているもの
ユーザ ID、 パスワード、パスフレーズ、暗証番号 氏名や生年月日や住所等の情報 絵や記号のパターン	IC カード ワンタイムパスワード（ソフト型、ハード型） USB トークン、乱数表など 電子証明書、共通鍵、認可情報 指紋、静脈、虹彩、網膜、声紋、筆跡

ここで、物理的なトークンを導入することのメリットはそれが盗まれたことを、被害者が確実に把握できる点です。一般的に物理的なトークンが盗まれた場合は、それが内蔵する鍵を失効させる運用を行うことで、被害を最小化しています。
表２には、それぞれの機器（デバイス）の特徴を示します。

表２　二要素認証に使用する機器（デバイス）の特徴

機器(デバイス)	秘密が外に出ない（演算能力がある）	耐タンパ性がある	コピー耐性
接触型 IC カード	○	○	○
FeliCa	×	○	○
OTP HW	○	○	○
OTP SW	○	×	△
USB キー	○	○	○
USB キー (廉価版)	×	×	△

生体	×	×	○？
ファイル	×	×	×
乱数表	×	×	×

このように二要素認証は、運用を間違わなければ認証強度の向上に役立ちますが、悪意のある専門家によって攻撃を受ける場合があります。以下にいくつかの攻撃手法と、その方法に対する考察を列挙します。

- セキュリティトークンがコピーできる場合の攻撃
  ～ゴルフ場キャッシュカードスキャン事件～

  ゴルフ場の貴重品ロッカーに Web カメラをしかけ、盗撮するという事件がありました。セキュリティトークンの強度を考察する上で参考になる事案ですので、ここで紹介します。
  犯人は、朝、ゴルフ客が貴重品を預けるところを盗撮し、貴重品ロッカーの暗証番号を盗み読みしました。その後、ゴルフ客がゴルフしている間に貴重品ロッカーから財布を抜き出し、キャッシュカード（※）をスキャニングし、何も盗まずに元に戻しました。後日、スキャニングデータからキャッシュカードを偽造し、銀行の ATM でお金を引き出しました。暗証番号は貴重品ロッカーと同じもので試してみることにより、かなり高い率で引き出しに成功したと言われています。
  この事件のキーとなるポイントは、犯人がキャッシュカードのスキャニングだけを行い、何も盗まずに財布をロッカーに戻している点です。このことにより、被害者は自分のキャッシュカードが盗まれていることに気がつかず、犯罪が発覚しにくいという特性がありました。
  企業等の認証システムに対比して考えた場合、利用者の秘密情報が盗み取られていないことを担保できない状況では、不正アクセスを検知することすらできず、二要素認証を導入した効果が半減すると言えます。これを確実に防止するためには、耐タンパ性があり、かつ、秘密情報が外に出てこないハードウェアセキュリティトークン（接触型 IC カード、OTP トークン）を利用する必要があります。
  （※）ここでの「キャッシュカード」は磁気ストライプのものを指しております。IC キャッシュカードはスキャニングではコピーできず、セキュリティトークンとしては、耐タンパ性とコピー耐性のあるセキュリティトークンになりますので、磁気ストライプ型のものより安全と言えます。

- キーロガーなど、パソコンの情報をキャプチャする攻撃に対する耐性
  キーロガーやリモートデスクトップ等パソコンの操作情報をキャプチャするようなソフトウェアを仕込まれて、パスワードが盗まれる場合があります。これらのソフトウェアでは、キーボードの入力履歴やウィンドウに入力された内容のキャプチャによりパスワードを盗み取ります。このような脅威に対しては、秘密情報そのものが画面を経由しない OTP、IC カード、ファイルによる SSL 相互認証等の２要素認証が有効です。
  しかしながら、２要素目の認証方式として、画像記憶型の認証方式を利用する場合は、キーロガーのような攻撃に対する耐性はなく、注意する必要があります。たと

えば、マトリックス上で記憶している形になぞったり、記憶している画像が表示されている場所の番号を入力したりする認証方式があります。これらの認証方式は、画面と同時に入力値がキャプチャされると、画像情報が攻撃者に漏れるので、耐性はありません。また、秘密情報を人間が記憶する方式であるため、パスワードと同じく秘密情報が盗まれていないことを確認する手段がなく、セキュリティの強度としては、パスワードと同等ということになります。さらに、ウィルスやワーム等の攻撃ではなく、Web カメラで入力画面を盗撮されるだけで秘密情報が盗まれる可能性もあります。最近では、モバイル環境の発達により屋外でパソコンやタブレットを操作する人も多く、このような盗撮攻撃に対する耐性も考慮する必要があります。
マトリックスから画像に対応する番号を入力する認証方式で番号を乱数で発生させる場合にそのパスワードを「ワンタイムパスワード」と称している製品が見受けられますが、上記のように、本来のワンタイムパスワードのようなセキュリティ強度を持っているとは言えないため、注意して区別する必要があります。

3-2. 二経路認証

二経路認証とは、インターネット経由で ID・パスワード認証を行い、その後に電話にて本人確認するなど異なる通信経路で認証を行うことです。以下の表３に代表的な認証経路を示します。

表 ３　二経路認証の代表的な認証経路

認証経路	バリエーション
インターネット網　×　インターネット網	有線と無線、異なるキャリア、異なる通信方式、SNS 等異なるサイト、・・・
インターネット網　×　電話網	電話コール、メール、IP メッセージ、位置情報、携帯のトークン、・・・
インターネット網　×　郵便・小包	アクセスキー送付、・・・
インターネット網　×　人	訪問、・・・

このように、２つの異なる通信経路を使用することで、その２つの経路を同時に利用可能である本人を特定するための認証強度が向上することが期待できます。

3-3. 二要素認証と二経路認証の組み合わせ方

なりすましを確実に防ぐためには高い認証強度の組み合わせの選択が必要ですが、一般的に認証強度が高くなると利便性が低くなるため、サービスの種類や扱うデータの種類、および利用範囲等により適切な認証方式を選択することが重要になります。
また、「なりすまし」されたときに発見できるような仕組みを持った認証基盤や、被害を補填する保険をあわせて選択することで、利便性を損なわずに最適な認証方式を採用することができます。

たとえば、ネット銀行へのアクセスでは従来通りにID・パスワードに加えて、質問やパターンを組み合わせた「知識」＋「知識（もちもの）」の認証を用いていることが多いようです。
これは、幅広いユーザ層を対象にしたサービスのために、複雑な認証方式は利用できないユーザを考慮して、より簡易で「なりすまし」されにくい方法を採用した結果と言えます。
また、ネット銀行では、接続した端末や時間などのアクセス履歴から、「なりすまし」されたことを発見する仕組みを持っており、これらの複合でシステムの認証強度を高く保っています。

3-4. やってはいけない二要素認証と二経路認証の組み合わせ

絵や記号のパターンを使った認証や、秘密の質問、生年月日など総当りアタックや辞書攻撃で時間さえあれば解けてしまうものは、認証強度が低いとされます。

IPAが公開した「コンピュータウイルス・不正アクセスの届出状況[9月分および第3四半期]について（第08-23-133号）（http://www.ipa.go.jp/security/txt/2008/10outline.html）」のなかで紹介されている「表1-1： 使用できる文字数と入力桁数によるパスワードの最大解読時間」によると、英字２６文字（大文字、小文字区別無)の8桁の最大解読時間は17日です。生年月日は8桁ですが、1～12ヶ月など有限なためもっと早く解読できます。

絵や記号のパターンについても、ある程度規則性があるために総当りアタックにより解読できてしまう可能性が高くなります。
２要素認証を利用していたとしても、認証強度が弱いものであればID・パスワードのみを利用していることと同じと考えたほうが良いです。
なお、総当りアタックを防止するために、表示イメージ中の文字等を入力するようなサービスもありますが、サービス提供者が総当りアタックを行うのを防ぐことはできません。認証強度を意識して、利用者が防御することが最も重要です。

4. クラウドと認証

クラウド環境の充実は、ユーザが選択できるサービスの幅が広がり、ユーザ毎の組み合わせの自由度が広がる反面、それぞれのサービスで個別に認証を実施しなければならないと言った「煩雑さ」を伴うことにもなりかねません。
しかしながら、クラウド環境のこのような状況になって初めて優位性が確認された認証のための技術も存在しています。
この章では、クラウド環境になって必要性が認識された技術のトピックを紹介します。

4-1. クラウド環境の認証方式

(1)　認証連携

複数のサービスで個々に認証する煩雑さを解消するための方法として、SNS サイトの認証を他のサービスで利用するものがあります。この「認証代行」はサービス間の信頼関係があれば、１つサービスで認証されると、別のサービスも利用できる仕組みです。
サービス（サーバ）が他のサービスの WebAPI を利用するケースにおいても、複数のサービスをまとめて１つのサービスとしている場合は、入り口の認証強度の高いサービスで認証することとなります。

なお、CBA フロント連携ワーキンググループの 2012 年度成果として、「認証連携」についてまとめていますので、必要により参照ください。

(2)　人間以外のアクセス

サービスが手軽に利用できるクラウド環境では、人間がサービスを利用する他に、サービス（サーバ）が他のサービスを利用するケースや、機器・設備がサービスを利用するケースもあります。人間がアクセスする場合は「知識」を利用することで認証強度が維持できましたが、サービス（サーバ）や機器・設備のアクセスでは、それらが持っている「所有物」による認証のみとなり認証強度の維持が困難となります。高価な演算機能や耐タンパ性をもつ専用ハードウェア（高価）の利用、デバイスそのものの真贋性対策、紛失・改ざん検出のための運用体制など、特別な対応を検討する必要があります。

4-2. 二要素認証と二経路認証の最新動向

(1)　Twitter の２要素認証

ユーザ名とパスワードを入力した後に登録した電話番号の SMS 宛に 6 桁のコードが送信され、そのコードを入力する仕組みです。

(2)　Symantec O3

認証ゲートウェイの機能をクラウドサービスとして提供したもの。ID とパスワードとワンタイムパスワードで複数のクラウドサービスと SAML 連携します。

(3)　RSA Authentication Manager 8

ID とパスワードとワンタイムパスワードに加えて、リスクベース認証を導入。リスクベース認証はアクセスしてきたデバイスのプロファイルやユーザの振る舞い、ロケー

ションなどの情報を分析して、「なりすましの疑い」を判断した場合に、「秘密の質問」や登録したメールアドレスにコードを送信して、そのコードを入力する「オンデマンドトークン」といった追加の認証の仕組みです。

(4) Microsoft LiveSide

ID とパスワードとセキュリティコードを入力する仕組みです。セキュリティコードはアプリケーションで生成します。

(5) セキュアスカイ・テクノロジー 「Scutum（スキュータム）」

ユーザ名とパスワードを入力した後に登録した電話番号の SMS 宛にワンタイムトークンが送信され、そのトークンを入力する仕組みです。

(6) Google Apps

ユーザ名とパスワードを入力した後に携帯電話でテキスト、音声通話、モバイル アプリを介して受け取ったコードの入力をする仕組みです。

(7) Facebook

新しい端末あるいはブラウザからログインする時に、承認済みの端末に表示されるメッセージに承認するか、あるいは、あらかじめ登録された電話番号の SMS 宛に送られるパスコードを入力する仕組みです。

5. 考察

認証はシステムの中で重要な要素の一つですから、丁寧に検討する価値のある要素です。正しい理解と正しい選択が必要ですし、ただ右にならうだけでなく、自分・自社で吟味することも大切です。そうすれば、万一、間違った選択をしたとしても、それに気づいたり修正したりすることができます。包丁や洗剤とは違うので、一見わかりやすい説明にだまされて、強度の足りない認証技術に手を出さないようにしましょう。

日々技術は進み、クラウド時代、便利になる一方、複雑さが増しセキュリティの確保も一見難しくなっています。ただ、進んだ技術と複雑さは、ただセキュリティを落とすだけでなく、認証に関連する要素を正しく吟味すれば、セキュリティの向上につなげることもできます。

いつでもどこでもアクセスできることがクラウドの利点ですが、企業の利用や機器・設備の利用の場合は、「いつでもどこでも」を多少制限した仮想的なプライベートクラウドを提供することも有効と考えます。

タブレットやスマートフォンが普及し、また機器や設備が無線 LAN を利用してインターネット上のクラウドサービスを利用するケースにおいては、アクセスできる場所が管理されることで「なりすまし」を防止することができます。

アクセスポイントごとに無線 LAN へのアクセスについて機器認証を行い、その機器のみクラウドサービスを利用できる方式を提案します。「所有物」＋「知識」の２要素認証となり、所有物の認証範囲はアクセスポイントを持つ企業が管理することになります。

また、個人向けのインターネット経由のサービスの場合も、インターネットからのアクセスを一部に制限するという考え方ができます。例えば、一部のネットバンキングでは、ソース IP アドレスによるアクセス制限ができます。インターネット全体からのアクセスが必要のないサービスもありますので、個人毎に、日本からのみ・自分の利用しているキャリア・プロバイダのみ、などの制限を加えることで、脅威を軽減させることができます。

クラウド時代、丁寧な検討と工夫により、便利でセキュアなシステムの実現が可能です。

6. 参考文献

[1] クラウド・ビジネス・アライアンス
<http://www.cloud-business.jp/>

[2] ニッポンクラウドワーキンググループ
<http://ncwg.jp/>

[3] フロント連携ワーキンググループ成果報告書
・フロント連携ワーキンググループ成果報告書（2010 年上期）2010.11.22
<http://www.cloud-business.jp/report/technical/output/docs/CBATechFront2010H1.pdf>
・フロント連携ワーキンググループ成果報告書（2010 年下期）2011.9.30
<http://www.cloud-business.jp/report/technical/output/docs/CBATechFront2010H2.pdf>
・フロント連携ワーキンググループ成果報告書（2012 年度）2012.3.28
<http://www.cloud-business.jp/report/technical/output/docs/CBATechFront2012.pdf>

--
以上