

認証方式の多様化に対するアカウント・アグリゲーション・サービス「Agurippa」の今後の取り組みについて

エヌ・ティ・ティ・ビズリンク株式会社(以下 NTTビズリンク、本社:東京都文京区、代表取締役社長:稲村美一郎)は、NTTコミュニケーションズ株式会社(本社:東京都千代田区、代表取締役社長:和才博美)が実施している次世代ネットワーク(NGN)のフィールドトライアル「ひかり認証サービストライアル」の協力企業としての参画を通じて蓄積した技術・ノウハウを活用して、NTT ビズリンクが提供する『アカウント・アグリゲーション・サービス「Agurippa」(*1)』のセキュリティ強化と利便性向上に取り組んでまいります。

1. サービス提供状況について

「Agurippa」は、利用者が持っている複数の銀行やクレジットカード等の取引を一括表示することにより資産状況などをリアルタイムに一括管理できる便利なサービスとして、2002 年 11 月よりサービスを開始しました。

現在では、国内最大級のアカウント・アグリゲーション・サービスとして、銀行、ポータルサイト、インターネットプロバイダーなど計8社にサービスを提供しており、オンラインサービス提供サイト数についても130を越えるサイトをカバーしています。

2. 今後の取り組みについて

銀行等におけるインターネットを利用した各種オンライン取引が社会的サービスとして定着しつつある一方で、これらのサービスの利用者を狙ったフィッシング詐欺やスパイウェア等による金融犯罪被害も増加しており、セキュリティ面での不安を持つ利用者も多く、より高度な認証技術の導入が求められています。

このような状況から、米国では2要素認証(*2)への対応が急ピッチで進められており、日本においてもオンラインバンキングサービスの安全性向上による利用促進を図るため、2要素認証の導入が進むことが予想されています。

このような動向を踏まえ、NTT ビズリンクでは、先端技術を用いた多要素認証(*2)技術の開発・運用ノウハウの習得を目的として、「ひかり認証サービストライアル(*3)」に協力企業として参画しております。

本トライアルでは、国内で初めて、「NGN の回線識別情報を利用した認証」と「リスクベース認証(*4)、または2WAY-SSL 認証(*5)」を組み合わせた多認証技術を採用した「ひかり認証サービス」の実証実験に取り組んでおります。

NTTビズリンクでは、本トライアルへの参画を通じて得られた最先端のセキュリティ技術を活用して、「Agurippa」のセキュリティ強化と利便性の向上を図ることにより、より安全に、安心してご利用いただけるサービスの提供に取り組んでまいります。

3. 本件に関するお問い合わせ先

エヌ・ティ・ティ・ビズリンク株式会社

データセンタ事業部 ビジネス開発部 サービスプラットフォーム担当

E-mail: agurippa@nttbiz.com

(*1)アカウント・アグリゲーション・サービス「Agurippa(アグリツパ)」

銀行預金残高、クレジットカード利用明細、証券取引情報、ポイント数など、複数の金融情報を Web 上で一括表示し、ユーザが資産及び負債の状況を一元管理することができるサービス。

詳細については、こちら(<http://www.nttbiz.com/service/asp/agurippa/index.html>)をご覧ください。

(*2)2要素認証／多要素認証

ID及びパスワードによる認証に加えそれ以外の認証方式(リスクベース認証、2WAY-SSL 認証、ワンタイムパスワード認証等)を2つ、または2つ以上組み合わせた認証方法。

(*3)ひかり認証サービストライアル

NTTコミュニケーションズ株式会社がNGNフィールドトライアルのひとつとして取り組んでいる実証実験。

従来のID・パスワードによる認証と、NGN回線における利用端末の状態や端末設定情報、行動特性など複数の情報を組み合わせることで、銀行決済や株式のオンライントレードなど、高い安全性が求められるサービスをより安全に認証する実験を行います。例えば、NGNから利用する場合は高額取引を可能とし、外出先などそれ以外の場合には特定の取引が行えないようにするなど利用環境に応じた設定が可能となります。

詳細については、NTTコミュニケーションズ株式会社のひかり認証サービス紹介用ホームページ

(<http://www.ntt.com/ict/future/hikari/>)をご覧ください。

(*4) リスクベース認証

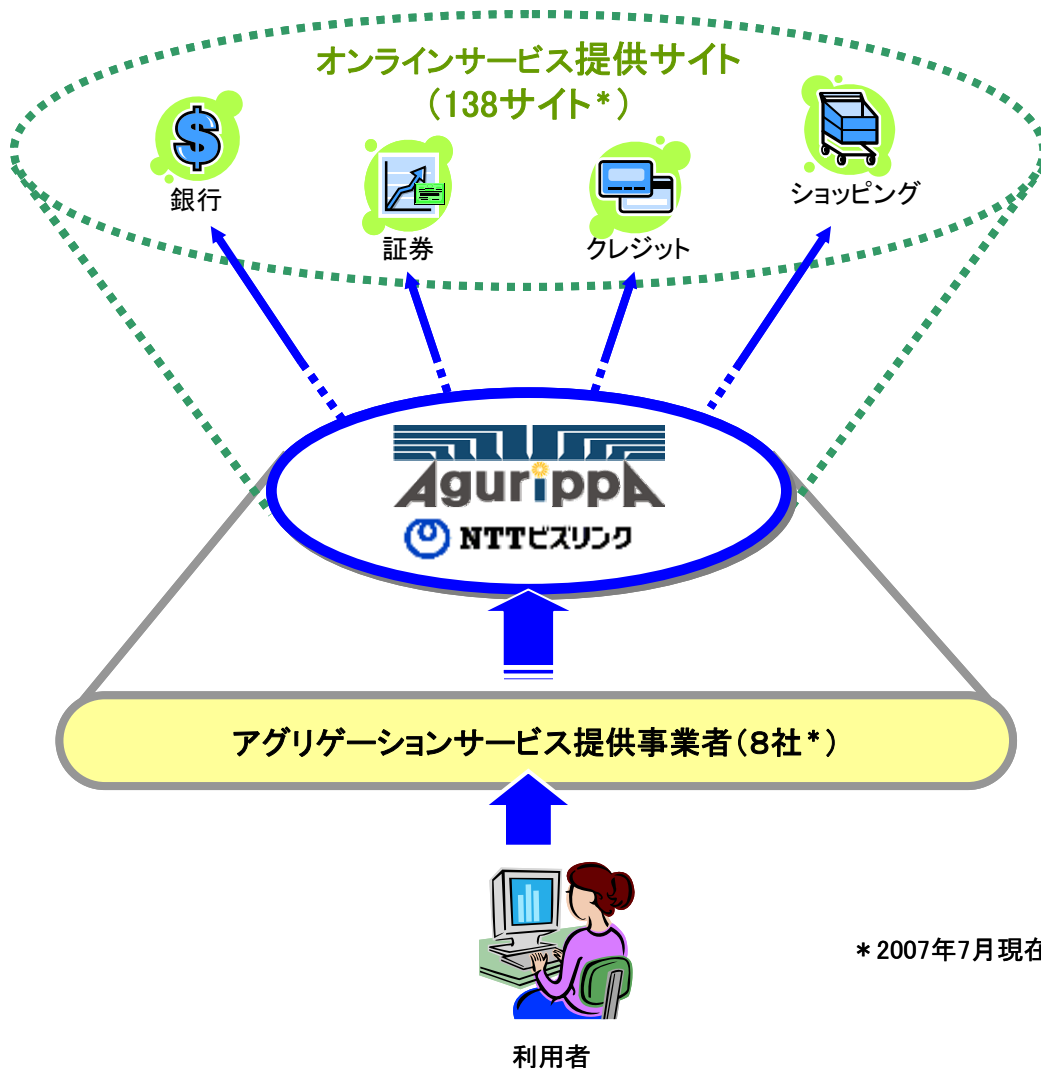
ユーザ情報(デバイス情報、IPアドレス、行動特性)などからリスク係数を算出し認証判定する機能

(*5) 2WAY-SSL 認証

クライアント-サーバ双方向でSSL認証を行う機能

<参考資料>

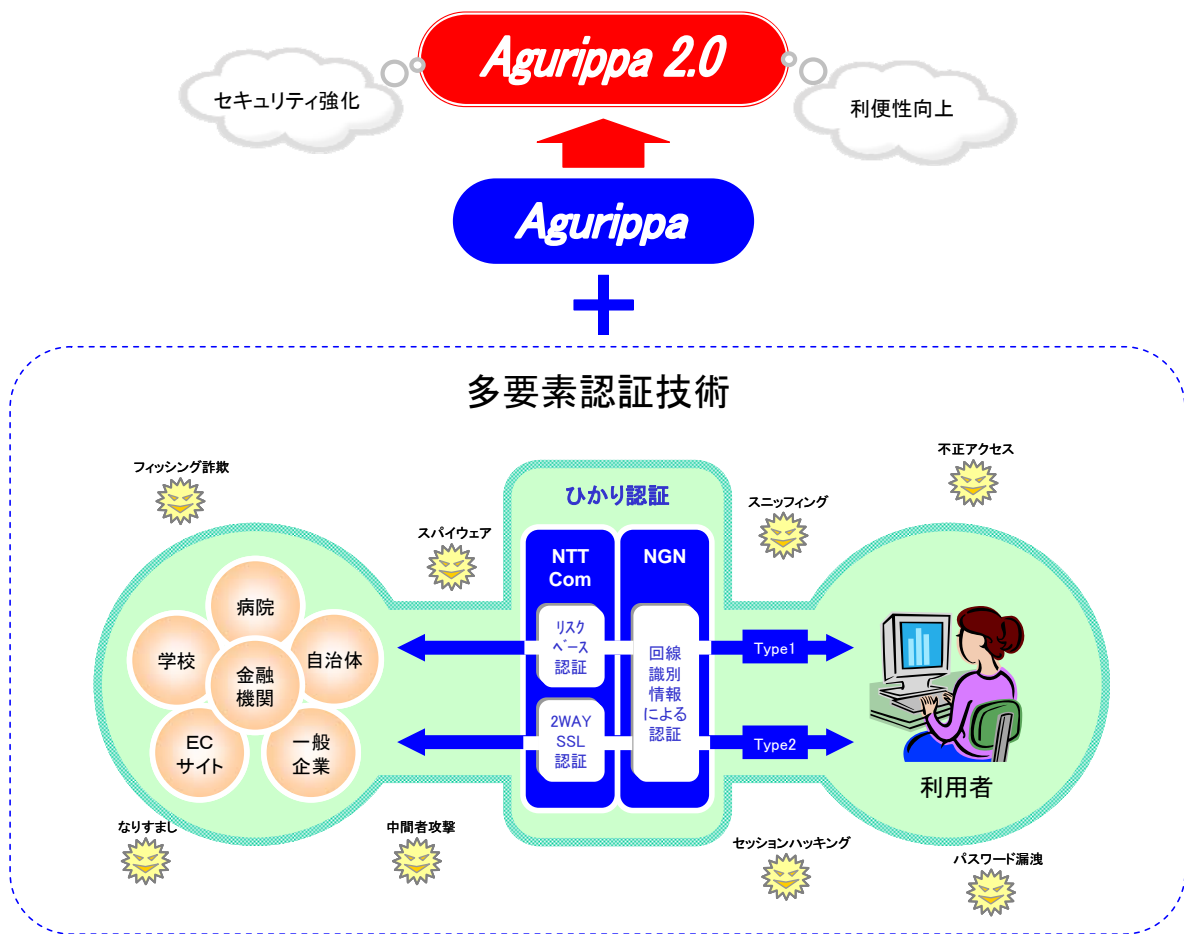
■アカウント・アグリゲーション・サービス「Agurippa(アグリツパ)」概念図



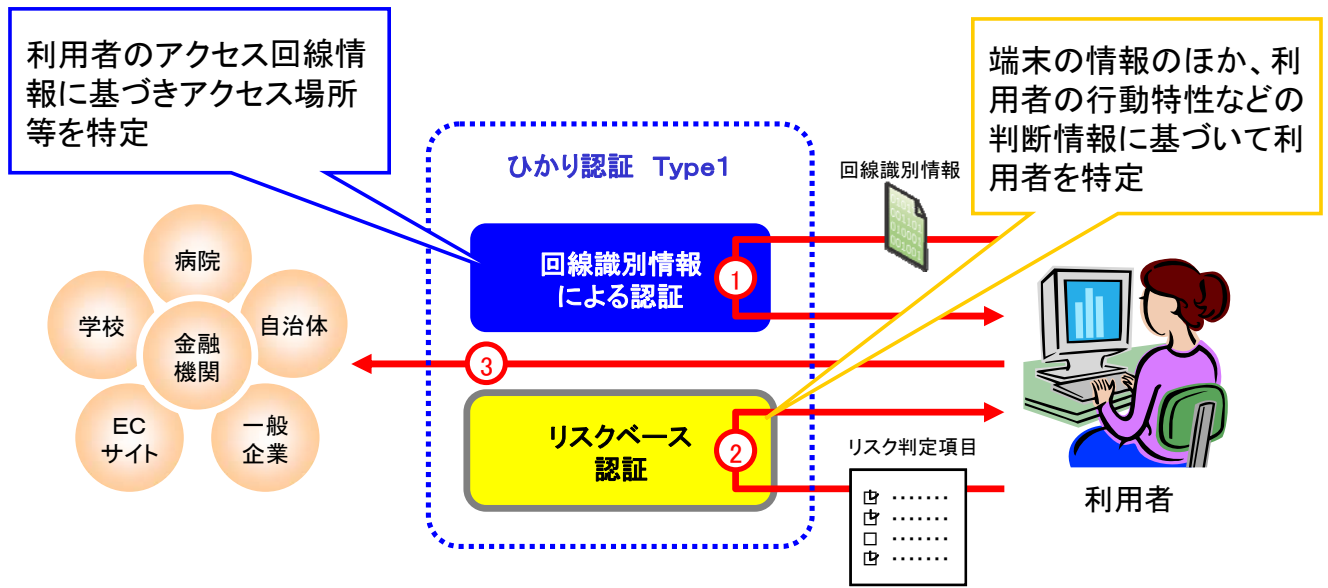
* 2007年7月現在

■ Agurippa のセキュリティ強化／利便性向上 (Agurippa 2.0)

- ・「Agurippa 2.0」は、“簡単・便利”な Agurippa をさらに“安心・安全”にご利用いただけるサービスとすることを旨としたNTTビズリンクの取り組みです。
- ・実証実験に取り組んでいる「ひかり認証サービス」では、回線識別情報による認証と他の認証機能を組み合わせた認証技術を採用しており、フィッシング詐欺などのセキュリティリスクを防止することのできる強固なセキュリティを実現しています。
- ・ひかり認証サービスには、利用者のニーズ・利用環境に応じた柔軟な認証サービス（ひかり認証Type 1／ひかり認証Type 2）を用意しています。

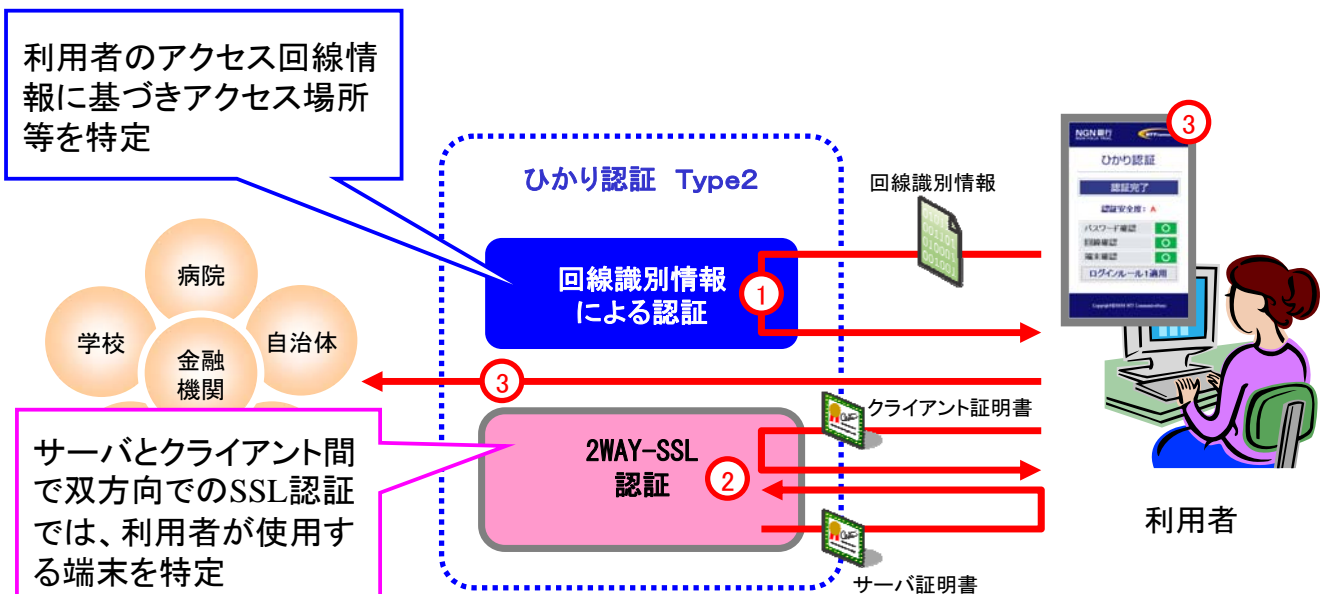


■ ひかり認証サービス (Type 1) 概要図



- ① 利用者が使っているアクセス回線の回線識別情報により認証する。
- ② 利用者が使っているパソコン端末情報、行動特性情報などのリスクベース情報により認証する。
- ③ 回線識別情報による認証結果と、リスク情報による認証結果があらかじめ設定した値を上回るとログイン可能となる。

■ ひかり認証サービス (Type 2) 概要図



- ① 利用者が使っているアクセス回線の回線識別情報により認証する。
- ② SSL証明書を用いてサーバとクライアント間を双方向で認証する。
- ③ 回線識別情報による認証結果とSSL証明書による双方向認証結果に基づいてログイン可能とする。