

インターネットを介した遠隔二者間における 安全な契約関係を結ぶための提案

山田 遼† 堀 正弘† 小松 雄一† 山本 隆広† 庭野 栄一‡

NTT セキュアプラットフォーム研究所† 日本電信電話（株）研究企画部門‡

1. はじめに

インターネットの発達により、EC サイトを始め電子政府など様々な取引・手続きがインターネット上で実現されてきており、年々市場規模は増加しており BtoC の EC 市場では 2015 年現在 13 兆円、BtoB においては 280 兆円の取引が行われている [1].

このようなサービスは本来、オフライン上における契約関係をインターネット上で再現することで実現していると解釈することができる。特に B2C における売買契約では電子契約法を始め整備されつつある。今後、電子政府の推進等からオンラインで行われる契約として売買契約だけでなく様々な形態の契約が今後多く出てくることが予想される。例えば、行政処理を始めとする手続きにおける委任契約がある。これは書面に委任する権限を明記・捺印後に効力を発揮するが、この書面を交わすためには対面または郵送におけるお互いの書面記入が必要となる。ここで安全性を確保しながらインターネット上でこの契約を結ぶことができれば 2 者が遠隔地であっても迅速に契約が可能となる。以上のようにオンライン上における契約関係構築は今後さらに重要になってくると考えられる。

それをふまえて我々は遠隔地 2 者間においてネットワークを介し安全に契約成立する方式を検討した。

2. 現状の課題

本検討で登場する 2 者を説明のために片方を甲、もう片方を乙とする。現実世界における機微な契約では、対面することにより契約者双方が本人確認をした後に署名捺印を施し契約関係を結んでいる。この時その契約関係締結に関する情報（契約内容・契約者名など）この 2 者間以外に情報が知られることがない。一方、現状のシステムでは契約締結前に個人情報がネット

ワーク上に流通する課題がある。これは、ネットワーク上で契約関係を結ぶ際において多くの場合、2 者間の契約関係の構築のために、個人情報の検索（ニックネームや ID 等）で契約相手を特定しシステム上で関係づける手法をとっている。この手法では、契約者に関係しない人がシステムを利用し他人を検索することによるニックネームの実在性確認や、ID を適当に入れ検索結果から名前等の個人情報を収集することができる可能性があることを意味する。

今後より機微な契約関係を結ぶことを想定した場合は以上上げた課題に対しても対策が必要となる。

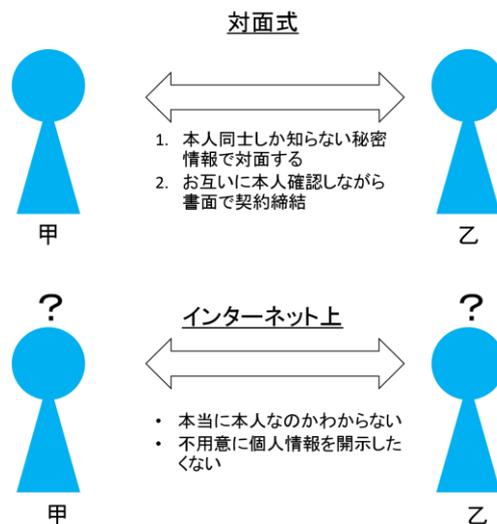


図 1 対面式とインターネット上の違い

3. 解決方針

以上の課題に対し、本検討では契約締結前にネットワーク上に個人情報が流れない契約締結方式を検討する。この解決方針として甲・乙しか知らない秘密情報をシステムに入力、システム上で照合・紐付けすることで個人情報を流通させることなく 2 者を関係付ける手法を考える。

1 対 1 の機微な契約を想定しているため、以下の前提をおいた

〔前提〕

・ 甲乙は該当する契約について予め結ぶことを

Proposing the Web Based Safe Method Having a Contract

†NTT Secure Platform Lab.

‡NTT R&D Planning Department

Ryo YAMADA† Masahiro HORI† Yuichi KOMATU†

Takahiro YAMAMOTO† Eikazu NIWANO‡

お互いに了解している

- ・甲乙は電話やSMS, 対面等の別の経路でコミュニケーションがとれる

このとき秘密情報として甲乙それぞれに紐付けられた一時IDをシステムから払い出し、システム外で交換する。そして、お互い相手の一時IDをシステムに入力することで個人情報がオンライン上に流通することなく2者を関係づけることができる。

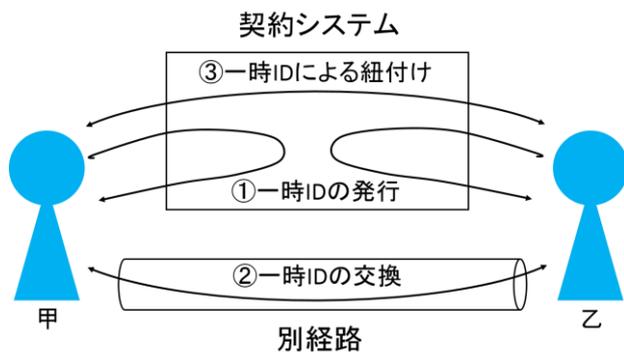


図2 解決方針概念図

4. システム概要

システムの機能として甲・乙双方に時限的に有効な個人IDとなる一時IDをそれぞれ払い出す機能と、制限時間以内であれば一時IDと契約関係を結びたい2者である甲乙を紐付けることができる機能により構成される。このとき先に上げた課題を解決するためには、一時IDに関して以下の要件を満たすことが必要となる。

〔要件〕

- ・一時IDは必要十分な有効期限を持つ
- ・一時IDに紐付けられた個人情報はその所有者以外には知ることはできない
- ・一時IDによる甲・乙のマッチングが図れた後に初めて甲・乙はネットワーク上で相手の個人情報について知ることができる

そのために、既存のシステムで相手先の確認を促すフェーズがあるが本システムにおいて要件を満たすためにはこのフェーズはあってはならない。

5. システム構成

システム構成例を図3に示す。この中で特徴的な機能について説明する。システム構成例の中で実線は電磁的に繋がっており、破線部は人の手によって(モニタから情報を得て、手で入力する)情報は受け渡されるものとする。甲・

乙はそれぞれPC等からそれぞれ自分の一時IDを取得し、その後携帯等を使い異なる経路にてこの一時IDをお互いに交換する。そして、お互いに自分のPCにこの一時IDを入力する。このとき、仲介サーバの「関係付け機能」では甲・乙からそれぞれお互いの一時IDを受け取ることでこの甲・乙が関係を結ぶ試行をしている情報を保持しその情報はこの機能の外に出ることがない。

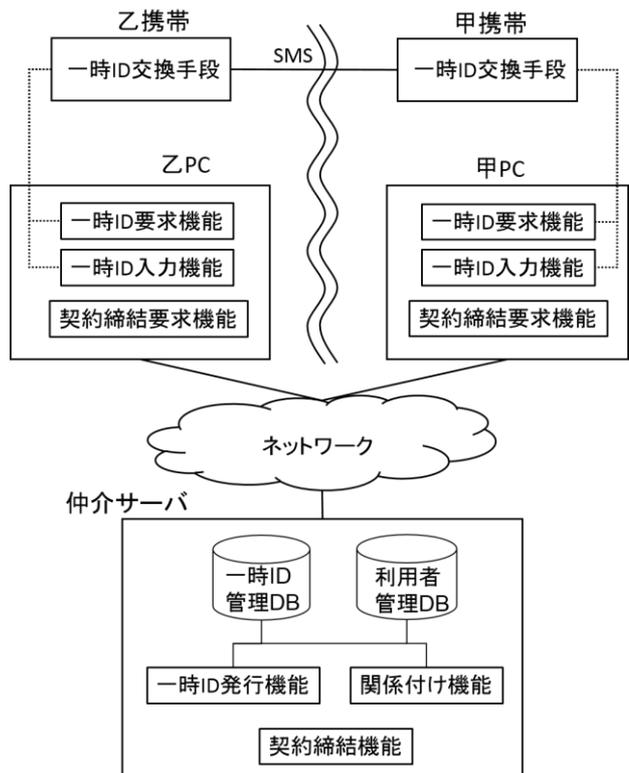


図3 システム構成

以上のシステム構成によって、契約締結前に契約に関する情報をネットワークに流通させずに先に契約関係を構築することができる。

6. まとめ

本検討では、今後インターネットを介した契約が多様化してくることを見越して遠隔地2者間において安全に契約関係を結べる方式を提案した。この手法を用いることにより今後、ネットワークを介して売買契約だけではない個人2者間における厳密な契約関係を結べるようになることが期待できる。

参考文献

[1] 『平成26年度我が国経済社会の情報化・サービス化に係る基盤整備(電子商取引に関する市場調査)報告書』経済産業省商務情報政策局情報経済課, 経済産業省, 2015, p. 24-45.