

インターネットトラストの確立に向けた JIPDECの取組み

一般財団法人日本情報経済社会推進協会
常務理事 山内 徹



■インターネット上の情報の信頼性（トラスト）について

近年、インターネット上での「なりすまし」によるサイバー攻撃が頻発化している。いわゆる標的型攻撃にみられるようなメールによるものだけでなく、その他 Web サイトや SNS などにおけるなりすましもあり、インターネット上の情報の真正性を判断することがますます困難になってきている。しかし、こうした攻撃への対策が事後的なものに留まってしまうと、積極的な IT の利活用を阻害することにもつながりかねない。こうした状況に対して、インターネットを介して得られる情報の信頼性（トラスト）の確認手段を充実させ、事前に情報を選別できるようになれば、事後的ではない効果的なセキュリティ対応が可能になるのではないだろうか。

そこでわたしたちはインターネット上の情報の信頼性を「インターネットトラスト」と名付け、その確保に向けたさまざまな取組みを行っている。たとえばなりすまし対策としては、情報送信元の実在性や様々な属性を証明し、その内容を視認性に優れたかたちで示す仕組みとして、「サイバー法人台帳 ROBINS」というサービスを運用している。これは、第三者による確認情報を掲載しており、法人情報に関するホワイトリストとしての役割を果たすものである。

なお、こうした信頼性に関連する事例として、トラストリストという仕組みが欧州に存在する。これは、EU が eIDAS (Electronic identification and trust services) 規則を通じて加盟各国に対して義務付けているものである。このトラストリストには、トラストサービスのためのルールや、それに基づいてサービスを提供するプロバイダ、またそのプロバイダの提供サービスとステータス情報が記載されている。日本でもこうした取組みができないかということで、JIPDEC の電子署名・認証センターでも調査研究をすすめている。

■本人確認に関する調査研究

インターネットトラストに関するテーマのひとつに、オンライン認証がある。オンライン認証とは、ある行為の実行主体と、当該主体が行った登録情報との同一性をネットワークを介した状態で検証することによって、実行主体が登録された人物であることを確認するプロセスを指す。実際のサービス利用場面でいうと、サービス利用開始時にまず本人情報の登録を行い、その後サービスを利用する際にその登録情報と突き合わせて本人確認（認証）を行う、という一連の流れがオンライン認証である。

現在、オンライン認証の仕組みを用いるサービスは、通信販売やオークション、オンラインストアや宿泊場所のシェアリングなど、多岐に渡っており、今後も増加する見込みである。こうした各種サービスにおける本人確認の認証レベルはサービスによってまちまちだが、それらに横串をさす本人確認方法の評価の枠組みについて、JIPDECでも調査研究を行っているところである。この枠組みについては、本人確認方法の評価に加えて、そのサービス全体についても評価を行い、その両方の評価結果を公表するといった、欧州のトラストリストのようなホワイトリスト構想なども検討されているところである。

■IoT時代における認証基盤

昨今著しい進展を見せるIoT (Internet of Things) についても、トラストの考え方が重要である。IoTのシステムではさまざまな機器からのデータがインターネットを介してやりとりされるようになるが、それらのデータが本当に信頼できるものであることを証明するような仕組みが必要である。こうした仕組みとしては、IoTのハードウェア(センサー等)の真正性の証明(所有者等)や、IoTから得られるビッグデータの利用者の真正性の証明などを行うような認証基盤などが考えられる。本人確認の認証と同様に、IoT分野においても、今後、トラストの確保がより一層求められていくだろう。

■今後の取組み

こうした動向をふまえて、JIPDECは今後もインターネットトラストを推進していくため、インターネットトラストに関する普及啓発や、ROBINSやJCANの普及活動および新しい活用分野の開拓等に取り組んでいく。また、今年の4月以降には、産学官を横断するかたちで、インターネットトラストの確保に向けて取組む新たな組織の設置を考えている。

