インターネットの信頼性（トラスト）の確保に向けて

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

■インターネットにおけるなりすましの脅威

標的型メール攻撃によって日本年金機構から大規模な情報漏えいがあったこと、日本を狙った遠隔操作マルウェア（Emdivi）による標的型攻撃キャンペーンの増加等に見られるように、インターネット上の情報の真贋を見分けることが困難になっている。インターネットにおける本物を認証することが重要になってきている。

■インターネット上の認証の重要性

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（あるいは装置）であることの信用を確立するプロセスのことを指す。

認証というのは本人、あるいは本物なのかということだけを確認することで、その本人あるいはデバイス等がそのサービスを受ける権利があるかまでを確認することは認可（オーソライゼーション）である。

2010年各府省情報化統括責任者（CIO）連絡会議で決定した「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」は、米国連邦政府のオンライン手続きでのリスク評価と電子認証を日本に取り込むために策定したもので、「登録」「発行・管理」「トークン」「認証プロセス」「署名等プロセス」で何をすべきかが明示されている。これは、電子申請が日本でなかなか普及しなかった時期に作られたものであり、現在も一般の民間企業では、ほとんど利用されていない。本ガイドラインが現在広く利用されているオンラインショッピングやネットバンキングに活用できるものかという議論が十分になされていないと感じる。

■電子署名がもたらす効果

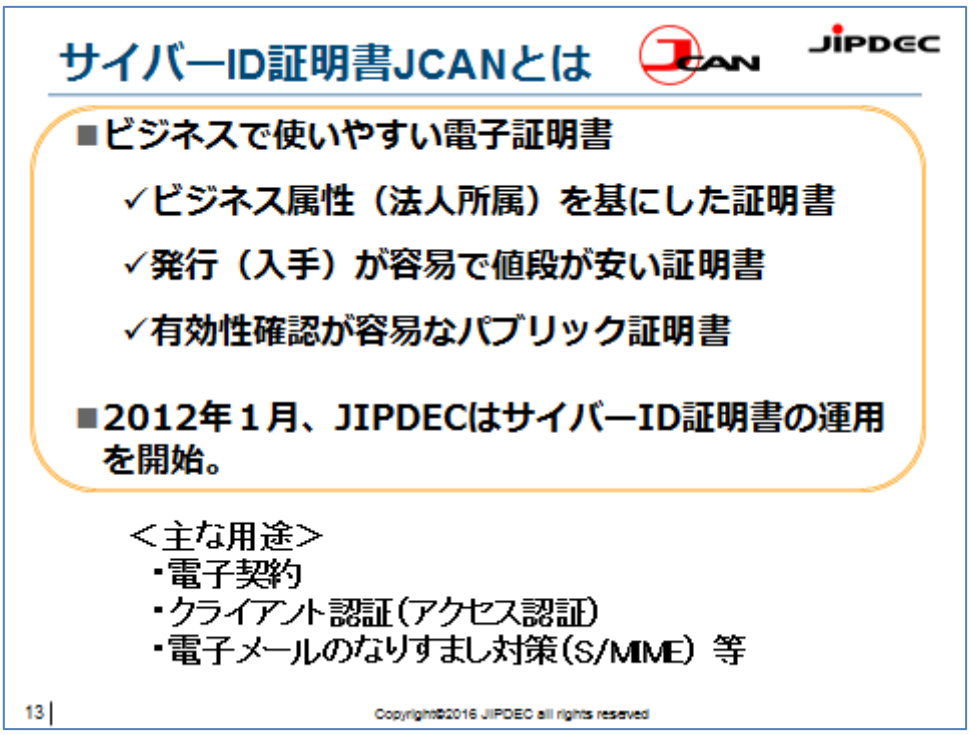
電子署名は主に、電子的に作られた文書（電子契約、電子申請書のようなもの）に証明書を付けることによってなりすまし／改ざん／否認行為対策をするものである。

電子署名法においては、基本的にPKI技術を使ったものが電子署名として認められて、私文書の真正性が推定されると規定されている。

JIPDECは、リアルな世界の署名、捺印に代わるものとしてサイバーID証明書JCANを電子契約ベンダーとともに提供している。JCANは、ビジネスで使い易く、パブリック証明書であり、汎用性が高い。主な用途としては、電子署名だけでなく電子認証、S/MIME

におけるなりすまし対策にも使える。

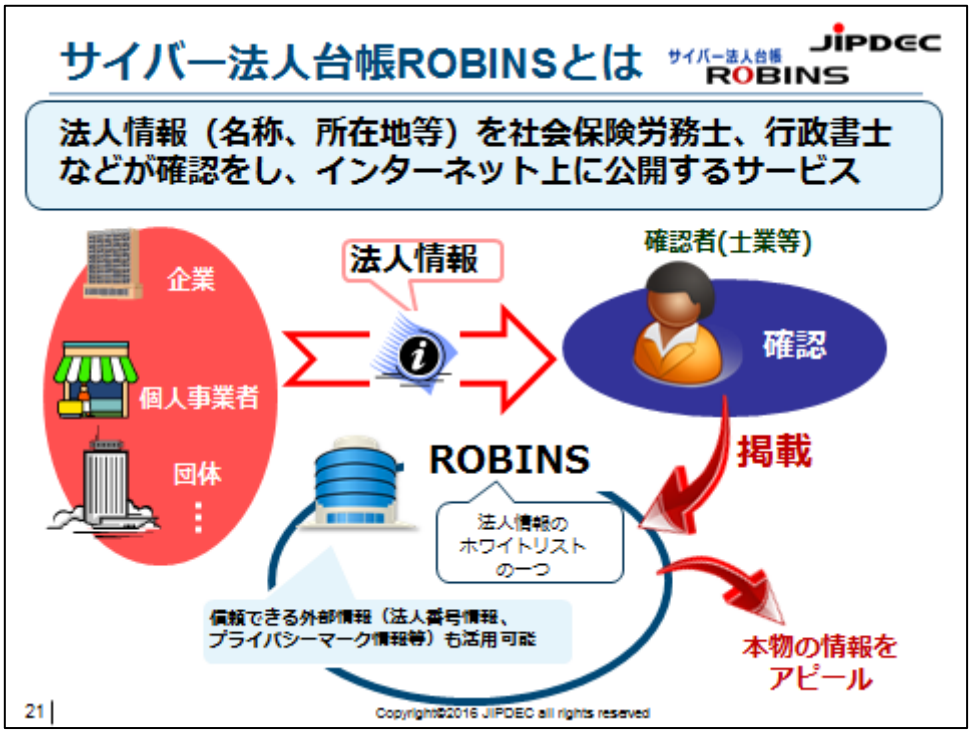
トラストアンカーとは、インターネット等における電子的な認証の手続きのために置かれる基点のことを指す。JCAN のトラストアンカーであるルート証明書は、主要な Web ブラウザや OS の証明書ストアと呼ばれる専用の格納場所に設定されている。



■なりすまし対策としてのサイバー法人台帳 ROBINS

なりすまし対策として、個人がドメイン１つ１つを本物であるか調べることは難しい。一方、企業はなりすまされないよう対策を講じることが必要である。何が本物であるかについて、明白な証拠があって、それをアプリケーションが自動的に確認し、利用者に対して視認性に優れた方法を通じて示すシステムが望まれているのではないか。このため、JIPDEC は、本物のホワイトリストの作成とその見える化を進めていきたい。

JIPDEC が進めている「サイバー法人台帳 ROBINS」は、法人情報（名称、所在地等）を社会保険労務士、行政書士などが確認をし、インターネット上に公開するサービスである。さらに、S/MIME や DKIM においては、メールの送信元が善意の組織かを確認できないという問題があったが、ROBINS を活用しては、DKIM という送信元のドメイン認証に加え、本当に正しい、なりすましでない企業から送られてきた、本物のメールであることが簡単に視認できる「安心マーク」によって本当に正しい、なりすましでない企業から送られてきたメールであることが確認できる。安心マークは現在、常陽銀行、スルガ銀行等で採用されている。



■インターネットの信頼性（トラスト）の確保に向けて

「トラスト」は「信頼」と和訳されるが、我が国において信頼という言葉の定義は十分明確になっていないようである。トラストの和訳と考えた際に、「信頼」というのは相手が自分に対して不利益なことを行えるような状況にあるものの、不利益を与えるとそれ以上の損害を被るためにそうはしないことが明らかである、という状況を指す。したがって企業間においてトラストで結び付いた関係を築いておけば安心できる。すなわち、安心できる状態にするためにトラストが必要なのである。

JIPDEC は、インターネットの信頼性（トラスト）基盤を強固にするための仕組みを構築するため、ベンダー、ユーザー、団体などの広範な分野、業種等が、一緒になりすましメール／Web 対策、アプリケーションの信頼性向上、メールドメインのレピュテーションサービスの立ち上げ、日本版トラストリスト（仮称）に関する提案などを検討する場（グループ）を設けていくことを考えているところである。