欧州のクロスボーダー認証への取り組み

株式会社コスモス・コーポレイション
IT セキュリティー部責任者
濱口　総志　氏

■「電子署名指令」と eIDAS 規則

EU で 1999 年に採択された「電子署名指令」は、電子署名の法的効力、認証サービス事業者の責任、適格証明書（以下、QC）を発行する認証サービス事業者に対する適切な監査システムの確保などを定めていた。しかし、その実現に向けた取組は、各加盟国において国内法を制定して進めることとしていたため、監査の有無や監査時の使用技術規格、認証局間の規制の厳格さや監査コスト、法的解釈、適格証明書の相互運用性を保つために必要なトラストリストのフォーマットなどについて、ギャップと課題が生じていた。

「eIDAS 規則（以下、eIDAS）」は、eID と e トラストサービス（以下、eTS）（電子署名、電子シール、タイムスタンプ、電子配布、ウェブサイト認証など）について定めたもので、全ての加盟国に法律として直接適用される。2014 年 7 月 23 日に批准、同年 8 月 28 日に公開され、現在、実現に必要な技術規格として ETSI、CEN、EN の整備が進められている。eIDAS を補足する Delegated Act と個別仕様等を規定する Implementing Act については、認証局事業者とサービスプロバイダのニーズはあるが、策定の予定は確定していない。

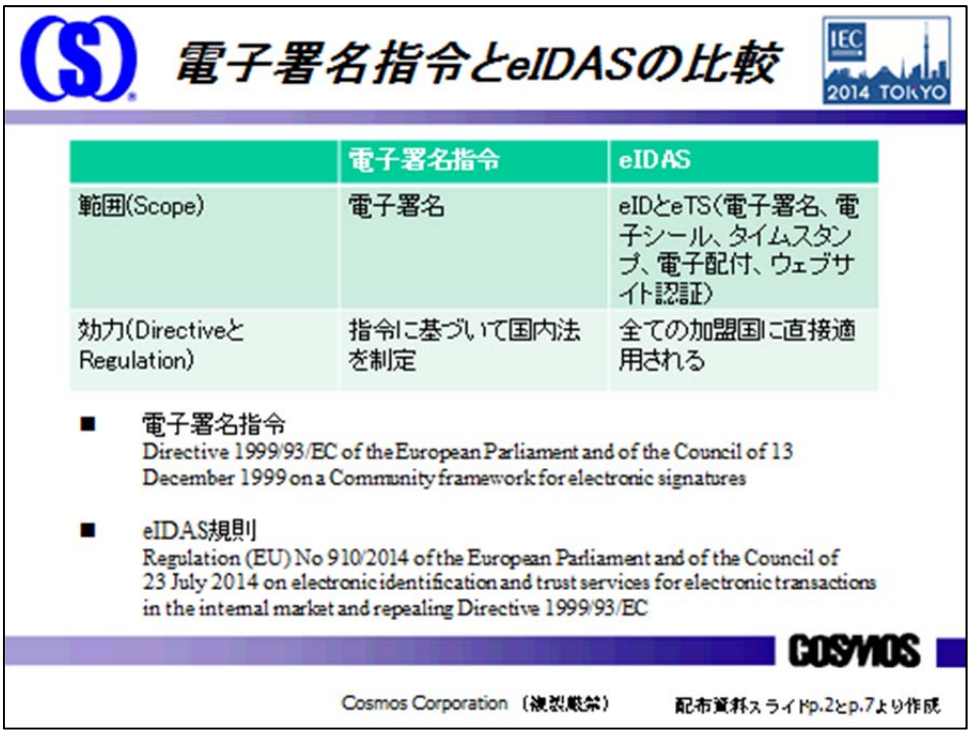

図 1

■eID と eTS についての規定

eIDAS は、公的機関のオンラインサービスにおいて eID を使った本人確認が必要な場合には他の加盟国の eID の受け入れを求めている。eID の保証レベルは 3 段階としているが、その測定基準は Implementing Act で規定するとしている。eID は通知後 2 か月でリストに掲載するとし、加盟各国には通知から 12 か月以内に相互承認を開始できるような体制整備を求めている。

「電子署名」については、eIDAS では eTS の一つとして取り扱っている。適格証明書を使った電子署名は、EU 域内の他国の署名も含めて、手書きの署名と同等とみなすとし、公的セクターにおいて電子署名を要求する場合は、適格電子署名を用いた署名を認めること、適格電子署名より高レベルのセキュリティを要求してはいけないことを定めている。また、電子署名指令の採択以降、その本来の趣旨と異なり、法人による電子署名を認めてしまっていた国もあったため、eIDAS には自然人のみが電子署名を行えることを明記している。

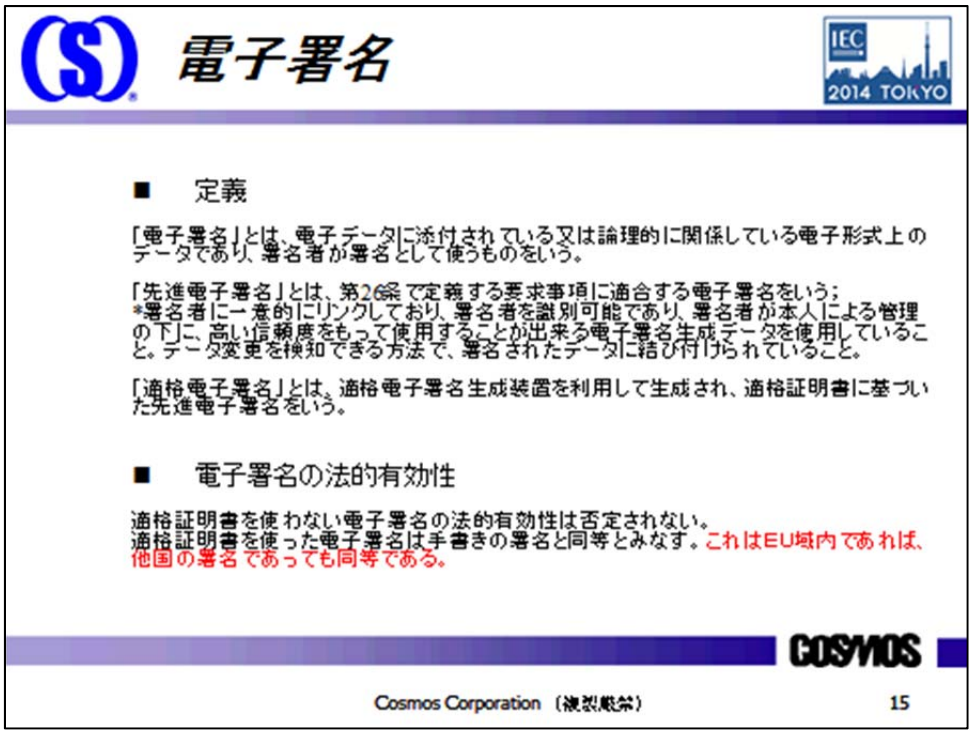

図 2

「電子シール」については、よく質問をいただくが、電子署名と同じような記載となっているものの、実際の法的効力は大きく異なる。電子署名は自然人の氏名または仮名を確認するために署名として使われ、電子シールは元の電子データの起源と完全性を保証し法人の名称を確認するために電子データへの添付などの形で使われる。

ドイツでは、電子シールは、企業ロゴのスタンプのようなもので、契約書などに付けられているが、請求書の有効性には影響せず、あまり法的効力を持っていないようである。電子シールは起源のみでなく完全性も保証するため、ドイツの法体系にインパクトを与える可能性はあ

るが、規則作成に携わった委員にも話を聞いたところ、日本における代表取締役の印鑑のようなレベルではなく、ゴム印レベルのようなものを想定しているとのことである。

また、これまでに法律で定められていなかった「電子タイムスタンプ」（時間情報と結びつけることにより、そのデータがその時間に存在していた証拠を確立するもの）についても法的有効性を認め、適格タイムスタンプは、その時刻の正確性とデータの完全性を保証し、他の全ての加盟国で通用するとしている。

「電子登録配布サービス」（電子手段により送信されたデータの取扱に関する証拠を提供するサービス）については、法的有効性や要件について定めているが、例えば「メールの受信時」とは、開封時／メールボックスへの到達時／受信サーバーでの受信時のどの時点を指すか、といった点について、専門家の間で合意が取れておらず、詳細には規定していない。この他の TS である「検証サービス」、「適格保存サービス」、「ウェブサイト認証」についてはあまり具体的に規定せず、「詳細は Implementing Act で定める」としている。

■トラストサービスと認証局適格トラストサービスプロバイダについて

eIDAS では、発行対象の自然人や法人の身元・属性を証明し適格証明書を発行する「認証局適格トラストサービスプロバイダ（以下 QTSP）」については、登録プロセス、失効、セキュリティ対策と専門性について規定した。また、加盟各国には QTSP のリスト（トラストリスト）を、EU 議会にはトラストリストのリストを、自動処理可能な形で公開・維持するよう求めたほか、トラストリストに掲載された QTSP がその証として使用できる「EU トラストマーク」というマークが作られた。加盟国には国内または他の加盟国の監督機関を指定すること、QTSP には少なくとも 2 年ごとに適合性調査機関から自費で監査を受けることを求め、監督機関はいつでも QTSP に対する監査が可能、監督機関の指摘に従わないサービスプロバイダは地位を取消されることを規定している。

EU 域外の国のトラストサービスに対する要求事項は、以前よりも少し厳しい内容となり、その国または国際機関との合意の下でのみ EU 域内のトラストサービスと同等とみなすとしている。

■eIDAS で実現されることと今後について

eIDAS により、eID の国境を越えたセキュアな認証による外国の大学への出願や電子健康情報へのアクセスなどの利便性向上、外国に移住する手続きや外国の案件に対する入札のオンライン化・効率化、ユーザ名とパスワードによるログインから eID 認証となることによるセキュリティの向上などが実現でき、様々な面でメリットがある。認証局にとっては、他の加盟国への参入が容易となり、市場の拡大および競争力の向上につながり、市民にとってのサービスの選択肢の拡大、新規ビジネスの可能性や雇用の創出にもつながる。

現在、電子調達の相互運用性、eID の相互運用性、電子処方箋の相互運用性などに関する実証実験が行われている。PEPS 方式の認証には、市民とサービスプロバイダとの間で直接の相互認証がない、適用方法が複雑、常にデータが PEPS を経由するため攻撃対象となりやすい

などの課題があり、フランスの ANSSI とドイツの BSI が共同で、STORK MW[*1] に基づいた eIDAS token の技術仕様を作成し、β版を Web サイトで公開している。

■会場からの質問

会場質問　：EU 域内で個人認証や ID の認定に関する法制度が国により異なるなかでのクロスボーダーの認証の前提として、本人確認（自然人と ID との間の認証）のレベルはどの程度確保されるのだろうか。

濱口氏より　：各国で eID を発行する仕組みが異なるので保証レベルが各国で異なり、eID を利用していない国については、健康保険カードなどで代用可能ではないかという議論がなされている。基本的には、「受入国よりも eID カード発行国の方が高い信頼性を有する」という条件を満たす場合のみ、相互認証が実現するので、自国の仕組みより信頼性の低い eID が流入することはないようになっている。

会場コメント：日本でも導入が予定されているマイナンバーに係る大きな課題として「番号の盗難」という課題がある。

濱口氏より　：アイデンティティの盗難は非常に大きな問題である。eID の盗難・紛失の場合、その eID を失効させ、新しい eID を受領し新たなパスワードを設定することとなっているが、最初に eID の発行を受ける前に、既に生体情報などが盗まれていた場合、本人確認はどのように行うか、参照する資料は何をもとに作られたものなのか、といった点が問題になってくるため、長期的な検討が必要だろう。

以上

[*1] **S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed **M**iddle **W**ear：EU 全体で eID の相互運用性プラットフォームを確立するプロジェクト