付録 3

用語集

— 目次 —

用語集

[数字]

10BASE－T（テンベース・ティー）

ツイストペアケーブルを使った Ethernet の接続方式のこと。10BASE－T の「10」は Ethernet の伝送速度 10Mbps を、「T」はツイストペアケーブルをそれぞれ表わす。この形態では、ネットワークを構成する各ノードはハブによってスター状に接続され、ノード同士をハブなしで直接接続することはできない（特殊な結線をしたツイストペアケーブルを使えば 2 ノードに限り直結できるが、一般的ではない）。ハブからネットワークカードまでの最大長は 100m である。10BASE－T では各ノードを個別にネットワークに接続したり、切り離したりできるし、ある 1 つのノードで電気的なエラー（ショートなど）が発生しても、個別にパーティション（partition：電気的に切り離されること）が構成されるので、ネットワーク全体がダウンすることはない。

[A]

ARL（Authority Revocation List）

認証局レベルの証明書失効リスト。

ASP（Application Service Provider）

ビジネス用のアプリケーションソフトをインターネット経由で利用するサービスを提供する事業者のこと。ユーザは通常 Web ブラウザを使って、ASP の保有するサーバーにインストールされたアプリケーションソフトを利用する。

[C]

CA（Certificate Authority）

認証局の項参照。

CJK キャラクタ

Unicode に登録されている漢字。Unicode に登録した際に Chinese（中国語）、Japanese（日本語）、Korean（朝鮮語）の漢字をひとまとめにしたことから各国の頭文字をとって CJK と呼ばれる。

CP（Certificate Policy）

証明書ポリシーのこと。認証局（CA）を運用する際に証明書の利用目的を定める規約。

CPS（Certification Practice Statement）

認証局運用管理規範のこと。認証局（CA）を運用する際の運用方法を定める規約。

CRL（Certificate Revocation List）

失効したデジタル証明書のリストのこと。有効期間内に失効させられたデジタル証明書の一覧で、デジタル証明書の受取人は証明書と CRL を照合することにより、証明書が現在も有効であるかどうか確認できる。

CSP（Certification Service Provider）

証明書発行サービス提供者のこと。信頼される第三者が、電子証明書の発行、署名、失効、管理などのサービスを提供する。認証局も CSP の一種である。

[D]

DES（Data Encryption Standard）

1960 年代後半に IBM 社によって開発された秘密鍵暗号化アルゴリズムのこと。1977 年にアメリカ政府標準技術局（NIST）によって連邦情報処理基準に採用された。現在では DES を強化した 3DES（トリプル DES）が利用されることが多い。

[E]

EDI（Electric Data Interchange）

企業間の電子的なデータ交換のこと。企業グループ内や特定の企業間でネットワークを介して取引データ等が交換される。各国各業界で電子データのフォーマットやデータ交換プロトコルの標準化が進められている。

EDIFACT（Electric Data Interchange for Administration, Commerce and Transport）

国際連合が EDI の国際基準として策定した電子文書の標準交換フォーマットのこと。

EE（End Entity）

認証局以外の証明書被発行者のこと。

EPA（Economic Partnership Agreement）

経済連携協定のこと。貿易の自由化以外に投資、人の移動、知的財産権や競争政策でのルール作りなど幅広く経済的な関係を強化しようとする協定。FTA よりも広い概念を示す。

[F]

FIPS（Federal Information Processing Standard）

連邦政府情報処理標準のこと。

FTA（Free Trade Agreement）

自由貿易協定のこと。ある国や地域の間だけで輸出入品にかかる関税や外資規制を取り払い、貿易の拡大を目的にした協定。

[G]

GPKI（Government Public Key Infrastructure）

政府認証基盤の項参照。

[H]

HSM（Hardware Security Module）

秘密鍵を管理する専用装置のこと。

HS コード

世界的に使用されている国際貿易商品の分類コードのこと。通常は 6 桁の世界共通コードと 2～3 桁の各国が任意に設定するサブコードで構成される。HS は Harmonized Commodity Description and Coding System の略。

[I]

IDA（Infocomm Development Authority of Singapore）

シンガポールの情報通信開発庁のこと。

IEEE（Institute of Electrical and Electronics Engineers）

米国に本部がある世界的な電気電子学会のこと。エレクトロニクスに関する学会の開催、論文誌の発行、および専門委員会を開いて技術標準を定めている。

IP アドレス

インターネット等の IP ネットワークに接続するためにコンピュータ 1 台 1 台に割り振られる識別番号のこと。現在普及している IPv4 では、8 ビットずつ 4 つに区切られた 32 ビットの数値が使われており、「210.145.108.18」などのように、0 から 255 までの 10 進数の数字を 4 つ並べて表現する。

KISA （Korea Information Security Agency）

韓国情報保護振興院のこと。情報保護に関する評価、政策、標準などを扱っ

ている。

[L]

LDAP（Lightweight Directory Access Protocol）

インターネットやイントラネットなどの TCP/IP ネットワークでディレクトリデータベースにアクセスするためのプロトコルのこと。

[M]

MIME（MuItipurpose Internet Mail Extensions）

インターネットの電子メールでワープロ文書や表計算データなど様々な種類の情報を添付ファイルとして授受する仕組みのこと。電子メールはもともとテキストだけの送受信を目的としていたが、多目的な情報を利用できるように機能拡張したものが MIME である。

[N]

NIST（National Institute of Standards and Technology）

米国商務省が管轄する情報機関で研究所を持ち技術指針や政府内における標準や運用基準の策定に務めている機関のこと。

[O]

OID（Object Identifier）

オブジェクト識別子のこと。ネットワークを介して通信する際、当事者同士があらかじめ認識しておくべき対象をオブジェクトと呼び、その国際的な一意識別を行うために付与した数字列を言う。

[P]

PID（Policy Identifier）

ポリシー識別子のこと。OID の一つでポリシーの識別を行うための数字列を言う。

PKI（Public Key Infrastructure）

公開鍵基盤のこと。公開鍵暗号方式という技術を利用した、セキュリティの基盤をいう。

POP3（Post Office Protocol version3）

インターネットやイントラネット上でメール・ソフトなどを使ってメールサーバーにアクセスし、電子メールの内容を取り出すためのプロトコルの一つ。「ポップ・スリー」と読む。

[R]

RA（ Registration Authority）

電子証明書発行の申請者の本人を確認し、主として登録業務を行う機関のこと。証明書の発行申請者の本人確認と業務を行う。

RFC3280（Request For Comments3280）

RFC はインターネットに関する技術の標準を定める団体である IETF（Internet Engineering Task Force）が正式に発行する文書のこと。RFC3280 にはインターネット向けに定義した X.509 証明書と CRL のプロファイルが含まれる。

RSA

現在、広く普及している公開鍵暗号方式の一つ。RSA 暗号方式では、十分に大きな 2 つの素数を掛け合わせた数の素因数分解が難しいことを暗号技術の基礎として利用している。RSA の文字は発明者であるリベスト（Rivest)、シャミア（Shamir)、 アドルマン（Adleman）の頭文字を取ったもの。

[S]

S/MIME（Secure/ MuItipurpose Internet Mail Extensions）

インターネット電子メールの代表的な暗号化方式のこと。電子メールの暗号化と電子署名に関する国際規格であり、MIME の機能拡張版である。メッセージの暗号化と電子署名を行う機能を持つ。S/MIME は公開鍵暗号方式と共通鍵暗号方式を併用する。

SMTP（Simple Mail Transfer Protocol）

インターネット上で電子メールの転送に利用されているプロトコルの一つで、利用者がメールをメールサーバーに送信するのに用いられる。

SSL（Secure Socket Layer）

ウェブサーバーとブラウザ等の間のセキュリティを強化するためのプロトコルのこと。デファクトスタンダードとして一般に多く利用されている。

[T]

TSA（ Time-Stamping Authority）

タイムスタンプ局のこと。電子文書が作成された時刻を証明する機関のこと。

[U]

UCR（Unique Consignment Reference）

世界税関機関（World Customs Organization）が推奨する貨物を特定するための「年下 1 桁」＋「国番号」＋「会社 ID コード」＋「会社内管理番号」からなる番号のこと。

UTF8（Unicode Text Format）

UTF は Unicode のテキストをデータとして入出力する時に用いるフォーマットのこと。 Unicode コンソーシアムでは UTF-7, UTF-8, UTF-16 の 3 種類が定義されているが、UTF-8 の最大の特徴は、ASCII 文字については ASCII コードとまったく同じエンコーディングが行われることである。ファイル名やドメイン名など ASCII コードの範囲で定義される文字列の入出力に向いている。

[W]

WCO（World Customs Organization）

世界税関機構のこと。各国の関税制度の調和・簡易化と関税行政の国際協力を推進する国際機関で、本部はベルギーのブリュッセルに置かれており、2005 年１月現在、164 カ国・地域が加盟している。

[X]

X.509

電子鍵証明書および証明書失効リスト（CRL）の標準仕様のこと。ITU（国際電気通信連合）が 1988 年に勧告した。

XML（eXtensive Markup Language）

文書やデータの意味や構造を記述するための言語の一つ。XML はユーザが独自のタグを指定できることから、マークアップ言語を作成するためのメタ言語とも言われる。SGML のサブセットとして考案され、任意のデータを HTML と同様の感覚で送受信できることを目標に作成されたものである。

[あ]行

インボイス（いんぼいす）

輸出者が輸入者に対して出荷時に発行する商品明細や数量、価格が記載されている書類のこと。輸出国と輸入国の通関当局に輸出入を申請する際に添付されることもある。

[か]行

共通方式（きょうつうあんごうほうしき）

情報の暗号化と復号に同じ鍵を用いる暗号技術のこと。

検証局（けんしょうきょく）

証明者検証者に代わって証明書の検証を行うシステム。略称 VA（Validation Authority）。

公開鍵暗号方式（こうかいかぎあんごうほうしき）

暗号化する鍵と復号する鍵が異なる暗号方式。非対称暗号とも呼ばれる。公開鍵暗号を秘匿に使う場合、送信者は受信者の公開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、もとの平文（ひらぶん）を得る。電子署名に利用する場合には、送信者は自分の秘密鍵で電子署名を作成し、受信者は電子署名に公開鍵を用いて電子署名を検証する。

公開鍵証明書（こうかいかぎしょうめいしょ）

利用者の公開鍵がその利用者に属するものであることを示す証明書のこと。

国連貿易開発会議（こくれんぼうえきかいはつかいぎ）

開発と貿易、資金、技術、投資及び持続可能な開発の分野における相互に関連する問題を統合して取り扱うための国連での中心的な場。

略称 UNCTAD（United Nations Conference on Trade and Development）。

[さ]行

商業送り状（しょうぎょうおくりじょう）

インボイスの項参照。

正規化（せいきか）

データを一定のルールに従って変形し、利用しやすくすること。XML においてはテキスト形式を採用しているため、ホワイトスペースの扱いや要素の出現順序などに寛容だがアプリケーションに XML 文書のデータを渡す場合や、

データが改竄されていないことを証明するための署名などを行う場合には XML 文書を一定のルールに従って整形しなおす必要がある。ここでの正規化はこの作業を指す。

政府認証基盤（せいふにんしょうきばん）

日本政府が運用している認証基盤のこと。政府が発行する許可証などに電子署名を付加するための基盤を提供する。

[た]行

電子署名（でんししょめい）

電子データに署名情報を付加し、その電子データの真正性を証明する技術のこと。署名には公開鍵暗号が用いられる。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って、送信者の署名を確認する。

特恵 ECO （とくけい ECO）

電子化された特恵原産地証明書のことを指す。ECO は Electronic Certificate of Origin の略。

特恵原産地証明書（とくけいげんさんちしょうめいしょ）

原産品の輸入関税を減免申請する際に、当該品が各々の国で生産されたものであることを証明する書類である。なお、証明書の最終的な利用者は輸入国側税関である。

トラストアンカ（とらすとあんか）

電子署名および公開鍵証明書の検証を行う場合に、検証者が信頼して利用する根元の情報。

[な]行

認証局（にんしょうきょく）

公開鍵証明書を発行する機関のこと。認証局は企業がサービスとして行うこともある。略称 CA（Certificate Authority）。

[は]行

ハッシュ関数（はっしゅかんすう）

ドキュメントや数字などの文字列の羅列から１対１の対応をもつ一定長のデータ（ハッシュ値）に要約するための関数・手順のこと。ハッシュ値は元のデータが１文字でも違うとまったく別の値になる性質を持つ。ハッシュ値からは

元のデータは復元できない。

船荷証券（ふなにしょうけん）

船会社が貨物を船積地点で受け取ったことを証明するとともに、指定された場所まで運送し、その船荷証券の正当な所有者に引き渡すことを約束した有価証券のこと。裏書きにより譲渡が可能であり、貨物の引取りには、原則としてその提示が必要となる。B／L（Bill of Lading）とも呼ばれる。

[ら]行

リポジトリサービスプロバイダ

電子文書を交換するシステムにおいて、送受信されたメッセージのトレーシング照会をはじめ、すべてのメッセージの送受信履歴について、管理・証明を行うサービス提供者のこと。