日常化するサイバー攻撃、問われる官民の責務

用語集

クライアント証明書	個人や組織を認証し発行される電子証明書。クライアントがシステムやサービス、メールなどを利用する際、サーバーに対してクライアントが正規の利用者であることを証明する。
センシングデータ	感知機器（センサー）などを使用して集められたデータ。センサーを搭載したIoT機器により、温度、湿度、光、動き、音、臭い、味などのさまざまな情報が収集される。
多要素認証	利用者本人であることを認証する際に、記憶、所有物、生体情報の3要素のうち、2つ以上の認証情報を組み合わせる方法。セキュリティがより強化される。
タリン・マニュアル	サイバー空間における国際法の適用に関する手引。国際法上、サイバー戦における「武力攻撃」は定説がないため、その解釈例を示そうしたもの。2013年、NATOのサイバー防衛協力センターが公表。
NAS（ナス）, Network Attached Storage	ネットワーク経由で利用できる外部記憶装置のこと。
秘密鍵	公開鍵暗号方式による暗号化や電子署名を利用する場合に、他人に見せることなく所有する鍵のこと。暗号化された通信を受け取った者は、秘密鍵を用いてデータを解読する。
ファームウェア	ハードウェアの基本的な制御のために、コンピュータなど機器に組み込まれたソフトウェアのこと。
プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順などの国際標準規則のこと。
ボットネット	「ボット」は、コンピュータを外部から遠隔操作するためのコンピュータウイルス。「ボットネット」は、ボットに感染したコンピュータのネットワーク。インターネット上から攻撃者が指示を出すと、ボットネットに接続されたコンピュータは、迷惑メールの配信や他のコンピュータへの攻撃、情報の窃取などを行う。
ランサムウェア	感染すると、端末等に保存されているデータを暗号化して使用できない状態にする不正プログラム。犯罪者は、そのデータを復号する対価として金銭（身代金）を要求する。

出所）警察庁、総務省、外務省、首相官邸、イミダス、NTTITトレンド用語、GMOグローバルサイン、デジサートの資料等を元に作成。