サイバーセキュリティの定義

サイバーセキュリティ基本法の サイバーセキュリティの定義

「サイバーセキュリティ」とは、
電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることをいう。

（出典：平成二十六年法律第百四号　サイバーセキュリティ基本法 より抜粋）

情報の CIA

機密性（Confidentiality）
完全性（Integrity）
可用性（Availability）

平成 26 年法律第 104 号サイバーセキュリティ基本法の第 2 条に、サイバーセキュリティが定義されています。
サイバーセキュリティ基本法では、サイバーセキュリティに関する基本的施策等について規定しています。内閣に、サイバーセキュリティ戦略本部を設置し、事務局を務める内閣官房内閣サイバーセキュリティセンター（NISC）においても、様々な取り組みがなされていて、その中にサイバーセキュリティ戦略案の作成や、施策の実施の推進などがあります。
この基本法に定義されているサイバーセキュリティには、必要な措置として、

- 情報の漏えい、滅失又は毀損の防止、安全管理
- 情報システムと情報通信ネットワークの安全性、信頼性の確保

をあげており、「その措置が講じられている状態が、適切に維持管理されていることをいう」と表現されています。
措置の対象となる情報は、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報」なので、人が話す内容などは含まれないことになりますが、これは明らかにコンピュータで取り扱うことができるデータを指していて、そのデータについて、情報セキュリティ対策の必要があるといえます。
情報セキュリティとは、一般的には「情報の機密性、完全性、可用性の 3 要素を維持すること」であるため、この情報の CIA（Confidentiality,Integrity,Availability の頭文字）が、サイバーセキュリティにとっても要となります。
機密性（Confidentiality）は、情報に関して正当な権限を持った者だけが、情報にアクセスできること、完全性（Integrity）は、情報に関して破壊、改ざん又は消去されていないこと、可用性（Availability）は、情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできることです。
措置の対象となる、「情報」、「情報システム」、「情報通信ネットワーク」については、DDos 攻撃や、ゼロディ攻撃など外部からのサイバー攻撃に対する対策だけでなく、内部不正や、人間の心理的な隙や行動のミスにつけ込んで秘密情報を入手するソーシャル・エンジニアリングを狙ったフィッシングなどまでを含めて、安全管理や信頼性の確保のために必要な措置が講じられ継続的に維持管理されていなければいけません。
サイバーセキュリティの定義をあらためて再確認すれば、私たちがどの様な措置を講ずるべきか理解し易くなります。