

3 用語及び定義

ISO 27001:2005 の用語及び定義の表記順序は、BS 7799-2:2002 との整合性に配慮し、英語表記のアルファベット順に記載されているため、翻訳すると一見すると脈絡無く用語が並んでいるように見えます。以下の3つに大別して整理すると理解しやすいでしょう。

情報セキュリティに関する用語の定義	3.1 資産 (asset)		
	3.4 情報セキュリティ (Information security)	3.3 機密性 (confidentiality)	
		3.8 完全性 (integrity)	
		3.2 可用性 (availability)	
	3.5 情報セキュリティ事象 (Information security event)		
3.6 情報セキュリティインシデント (Information security incident)			
リスクマネジメントに関する用語の定義	3.14 リスクマネジメント (risk management)		
	3.12 リスクアセスメント (risk assessment)	3.11 リスク分析 (risk analysis)	リスク因子 リスク算定
		3.13 リスク評価 (risk evaluation)	
	3.15 リスク対応 (risk treatment)		リスクの低減
			リスクの保有
			リスクの回避
		リスクの移転	
3.9 残留リスク (residual risk)			
3.10 リスク受容 (risk acceptance)			
マネジメントシステムに関する用語の定義	3.7 情報セキュリティマネジメントシステム (Information security management system)		
	3.16 適用宣言書 (statement of applicability)		

■ 情報セキュリティ

情報の不適切な保護は、漏えいや内容が不正確、必要時に使えない等の業務に支障をきたすといったリスクがあります。「情報セキュリティ」とは、重要な情報をこうしたリスクから守ることで

■ 機密性 (confidentiality)

認可された者だけが情報にアクセスできることを確実にすること。情報の機密性は、「情報が漏えいしないようにすること」により確保されます。

■ 完全性 (integrity)

完全性には、情報が改ざんされないこと、つまり情報そのものの完全性の確保。情報が不正な手段に変更されないようにすること、つまり管理方法による確保の二つの意味があります。

■ 可用性 (availability)

認可された利用者が、必要な時に、適切な関連する資産にアクセスできることを確実にすること。「自然災害やシステムダウンにより、情報にアクセスできないこと」に関連します。

■ リスクマネジメント

リスクに関して組織を指揮し、管理する調整された活動。リスクとは、「組織の活動の遂行を阻害する事象の発生の可能性」。

■ リスクアセスメント

「リスク分析」から「リスク評価」までのプロセス。

■ リスク分析

「リスク因子を特定するための、及び「リスクを算定」するための情報の体系的な使用。

■ リスク因子

脅威と脆弱性を組み合わせたもの。「暗号化されていない通信の機密性」により、引き起こされる情報漏えい(脅威)がリスク因子となります。

■ リスク算定

算定されたリスク因子の発生可能性と、それにより引き起こされる事象の結果を検討すること。「暗号化されていない通信にて引き起こされる情報漏えいにより被る損害」を計算すること。

■ リスク評価

リスクの重大さを決定するため、算定されたリスクを与えられたリスク評価基準と比較するプロセス。

■ リスク対応

リスクを変更させるための方策を選択および実施するプロセス。詳細は、「4.2.1 f)」をご参照ください。

■ 残留リスク

リスク対応後にまだ残っているリスク。

■ リスク受容

リスク対応後の残留リスクを受容する意思決定のこと。これはリスク評価基準に依存します。