演習 5-2：箇条 6.1.2ISMS リスクアセスメント

目的：「JIS Q 27001:2014」が要求するリスクアセスメントプロセスを理解する

時間：

グループ作業　　60 分

グループ　プレゼンテーション　40 分

指示説明：考察する組織の保有する情報を 3 つ挙げ以下の検討を行ってください。

各グループは検討結果をクラス全体に説明します。

1.以下のリスク基準を定めてください

・リスク受容基準

・情報セキュリティリスクアセスメントを実施するための基準

2.評価基準を定めてください

3.適用範囲の中の情報を 3 つ挙げ、機密性、完全性、可用性の喪失に伴うリスクを特定してください。

4.リスク所有者を特定してください。

5.発生可能性、起こりうる結果についてのアセスメントを行いリスクレベルを決定してください。

6.リスク基準と比較し、リスクの優先順位づけを行ってください。

情報	情報の価値(※)	リスクの特定(喪失に伴うリスク)			リスク所有者	発生可能性(※)	起こり得る結果(※)	リスクレベル	リスクの優先順位
		機密性(※)	完全性(※)	可用性(※)					