「金融分野におけるサイバーセキュリティに関するガイドライン」との対比表

金融分野におけるサイバーセキュリティに関するガイドラインの対応事項と、安全対策基準（第13版）の基準小項目の関係は以下のとおり。

＜安全対策基準箇所の色分け＞　赤：新設 、青：改訂あり 、オレンジ：関連箇所（改訂なし）

金融分野におけるサイバーセキュリティに関するガイドライン		安全対策基準（第13版）
1.基本的考え方		－
1.1.	サイバーセキュリティに係る基本的考え方	ガイドラインの説明等であり、必要事項は記載済みと判断。安全対策基準への反映なし。
1.2.	金融機関等に求められる取組み	
1.2.1.	サイバーセキュリティ管理態勢	
1.2.2.	経営陣の関与・理解	
1.3.	業界団体や中央機関等の役割	
1.4.	本ガイドラインの適用対象等	
2.サイバーセキュリティ管理態勢		－
2.1.	サイバーセキュリティ管理態勢の構築	－
2.1.1.	基本方針、規程類の策定等	統1-1
2.1.2.	規程等及び業務プロセスの整備	統1-2
2.1.3.	経営資源の確保、人材の育成	統4-1
2.1.4.	リスク管理部門による牽制	統4、統4-2
2.1.5.	内部監査	監1-1

「金融分野におけるサイバーセキュリティに関するガイドライン」との対比表

金融分野におけるサイバーセキュリティに関するガイドライン		安全対策基準（第13版）
2.2.	サイバーセキュリティリスクの特定	―
2.2.1.	情報資産管理	統5-1
2.2.2.	リスク管理プロセス	統5-2
2.2.3.	ハードウェア・ソフトウェア等の脆弱性管理	統5-3
2.2.4.	脆弱性診断及びペネトレーションテスト	実14-2
2.2.5.	演習・訓練	統5-4
2.3.	サイバー攻撃の防御	実14
2.3.1.	認証・アクセス管理	統7、統12、実8、実9、実10、実25、実26、実27、実58、実138
2.3.2.	教育・研修	統5-5
2.3.3.	データ保護	統1、統12、実3、実14、実28、実30、実39、実41
2.3.4.	システムのセキュリティ対策	―
2.3.4.1.	ハードウェア・ソフトウェア管理	実15、実20、実48、実51、実75
2.3.4.2.	ログ管理	統12、実10、実14
2.3.4.3.	セキュリティ・バイ・デザイン	統20、実75、実89
2.3.4.4.	インフラストラクチャ（ネットワーク等）の技術的対策	実4、実14、実20、実34、実76、実146
2.3.4.5.	クラウド利用時の対策	統20、統24、実71

「金融分野におけるサイバーセキュリティに関するガイドライン」との対比表

金融分野におけるサイバーセキュリティに関するガイドライン		安全対策基準（第13版）
2.4.	サイバー攻撃の検知	ー
2.4.1.	監視	実14-1
2.5.	サイバーインシデント対応及び復旧	実73-1
2.5.1.	インシデント対応計画及びコンティンジェンシープランの策定	
2.5.2.	インシデントへの対応及び復旧	
2.6.	サードパーティリスク管理	統28
3.金融庁と関係機関の連携強化		ー
3.1.	情報共有・情報分析の強化	金融庁としての方針に関する記載であるため、安全対策基準への反映なし。
3.2.	捜査当局等との連携	
3.3.	国際連携の深化	
3.4.	官民連携	