【表 6：NIST フレームワークには存在し、ISO27001 には存在しないもの】

機能	カテゴリー	サブカテゴリー
特定	ビジネス環境	重要インフラとその産業分野における企業の位置づけを特定し、伝達している。
		企業のミッション、目標、活動に関して優先順位を定め、伝達している。
	ガバナンス	ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。
	リスクアセスメント	内外からの脅威を特定し、文書化している。
	リスク管理戦略	リスク管理プロセスが自組織の利害関係者によって確立、管理され、承認されている。
		自組織のリスク許容度を決定し、明確にしている。
		企業によるリスク許容度の決定が、重要インフラにおける自組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。
防御	情報を保護するためのプロセス及び手順	保護プロセスを継続的に改善している。
検知	異常とイベント	ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定し、管理している。
		イベントデータを複数の情報源やセンサーから収集し、相互に関連づけている。
		イベントがもたらす影響を特定している。
		インシデント警告の閾値を定めている。
	セキュリティの継続的なモニタリング	発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている。
		発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている。
		権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。
対応	伝達	対応計画に従って、利害関係者との間で調整を行っている。
		サイバーセキュリティに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている。
	改善	対応戦略を更新している。
復旧	改善	学んだ教訓を復旧計画に取り入れている。

		復旧戦略を更新している。
	伝達	広報活動を管理している。
		イベント発生後に評判を回復している。
		復旧活動について内部利害関係者と役員、そして経営陣に伝達している。