情報セキュリティガバナンス：取締役会と役員に対するガイダンス

情報セキュリティガバナンスは、情報を保護するリーダーと、組織構造、さらにプロセスから構成されている。

責任		成果
取締役会は、情報セキュリティに関して、次のような点から戦略的なオーバーサイトを行う。 ●情報および情報セキュリティの、組織にとっての重要性を理解する ●情報セキュリティへの投資について、組織の戦略とリスクプロフィールとの整合をレビューする ●包括的な情報セキュリティプログラムの開発ならびに導入を承認する ●プログラムの妥当性ならびに有効性に関して、役員に定期的な報告を求める	**管理に当たる取締役会と役員は、次の点をレビューしなければならない。** ●情報資源が最適化されることを保証する目的で、現在ならびに将来行われる情報資源に対して行われる投資の規模と収益 ●技術が組織とビジネスのプラクティスを変化させ、これによってコストを削減しながら新しい機会と価値を作り出す可能性	**情報セキュリティガバナンスの基本的な成果には、次の 5 つが含まれている必要がある。** ●戦略的整合：情報セキュリティとビジネスの戦略が戦略的に整合し、組織の目標をサポートしている ●リスクの管理：リスクを管理および軽減し、さらに情報資源に生じる可能性のある影響を許容可能なレベルにまで減少するよう、適切に対策している ●資源の管理：情報セキュリティに対する知識とインフラストラクチャを効率的かつ有効に利用している ●成果の測定：情報セキュリティガバナンスの指標を測定し、モニタリングし、またこれについて報告し、組織の目標が達成されていることを保証している ●価値の実現：組織の目標をサポートする情報セキュリティ投資を最適化することで、価値が実現されている

情報セキュリティガバナンスの利点

●顧客関係において信頼性を増大する
●企業の評判を保護する
●プライバシーの侵害の可能性、ならびに法的責任が発生する可能性を減少する
●取引相手とのやり取りの際にさらなる信頼性を提供する
●電子取引を処理する新しく改善された方法を実現する
●予見されている結果をもたらすこと、すなわちプロセスを妨害する可能性のあるリスク要因を軽減させることで運用コストを減少させる

包括的なセキュリティプログラムには、次のものが含まれる

●セキュリティポリシーの作成/維持
●役割、責任、権威、説明責任の割り振り
●標準、指標、プラクティス、手続きから構成されるセキュリティおよびコントロールフレームワークの作成/維持
●定期的なビジネス評価およびビジネスインパクト分析
●情報資産の所有者の分類と割り振り
●人、プロセス、技術に対する十分で、有効かつテスト済みのコントロール
●セキュリティの要素をモニタリングするプロセス
●情報セキュリティのインシデントの管理
●情報のユーザならびにサプライヤに対する、有効な本人確認ならびにアクセスの管理プロセス
●セキュリティ成果の有効なモニタリングと指標
●全てのユーザ、役員マネージャ、取締役会の構成員の、情報セキュリティ要件に関する教育
●年次的に情報セキュリティ評価を行い、成果レポートを取締役会に対して提出
●情報セキュリティの欠陥に対処するための是正措置の計画
●セキュリティプロセスの運用の訓練
●中断および災害が発生した場合の、業務継続のための計画の作成とテスト

この資料は、『*情報セキュリティガバナンス：取締役会と役員に対するガイダンス　第2版*』に基づいている。