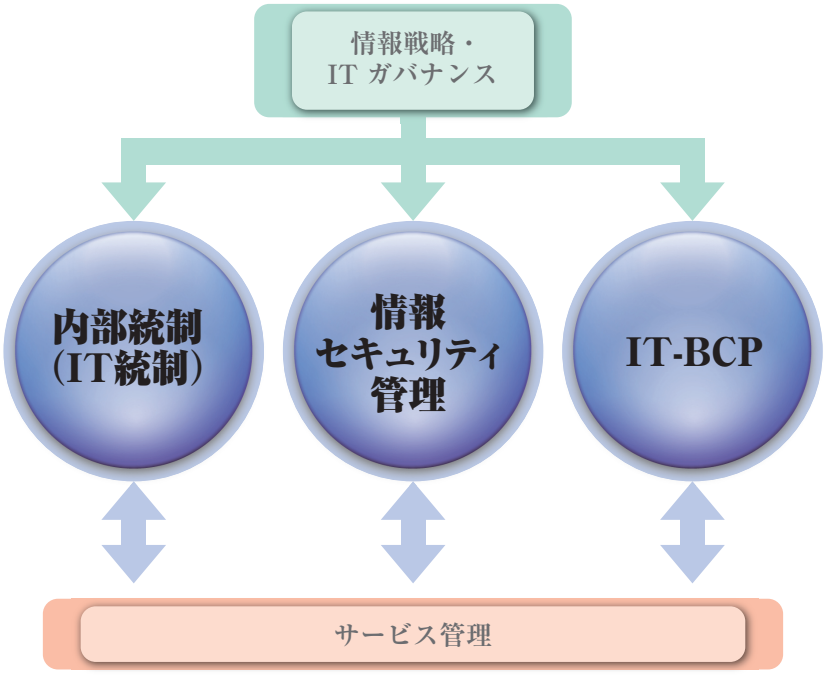
IT Risk Management

ITリスク管理

IT Risk Managementでは、情報化運営に関連するリスクを正確に把握し、
包括的 且つ 適切にコントロールするのに必要な手法やノウハウを提供します。

これら手法・ノウハウを活用することで、情報システムの機密性・完全性・可用性を維持し、
情報システムを安全に運用することが可能となります。

IT Risk Managementは、内部統制（IT統制）、情報セキュリティ管理、
IT-BCPの３つのメソドロジから構成されています。



野村総合研究所

内部統制(IT統制)

本メソドロジでは、会社法やJ-SOX等の内部統制のうち、IT統制の整備・運用に関わる手法を提供します。具体的には、内部統制整備で求められる必要なドキュメントのテンプレートや、内部統制の有効性を継続的に評価・改善する手法やノウハウを提供します。これらテンプレートを適用することで、短期間で抜け漏れのないIT統制を整備・運用することが可能となります。

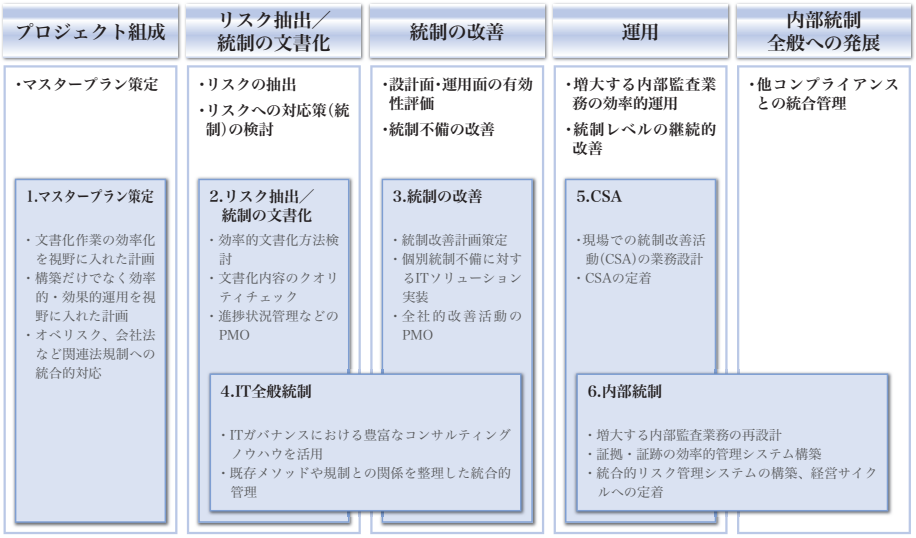
利点・期待効果

- 短期間で内部統制に必要な文書を整備することができます。
- ポイントを抑えた効率的な統制で、効果的な内部統制を実現することができます。
- 内部統制の有効性を継続的に向上させることができます。

(活用する代表的な手法)

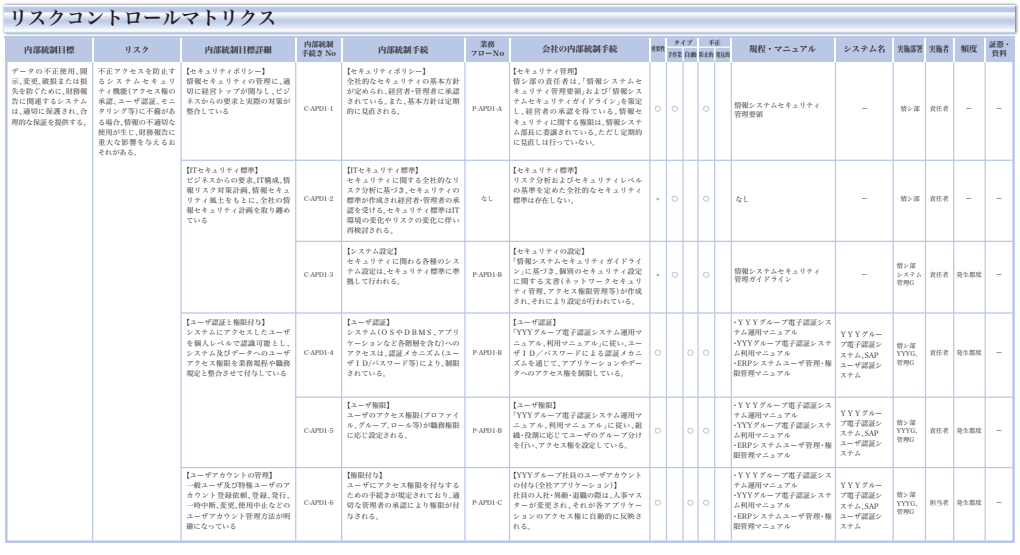
内部統制の発展段階と実施内容

内部統制の整備から運用・改善までの各フェーズにおける実施内容と施策のテンプレート

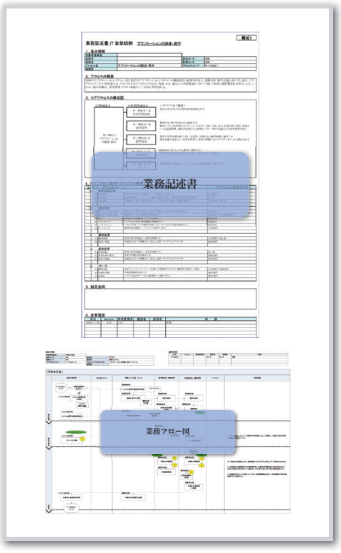


NRI内部統制 文書化3点セット

リスクコントロールマトリクス（RCM)、IT統制に関わる業務フロー図、業務記述書のテンプレート


リスクコントロールマトリクス

内部統制目標	リスク	内部統制目標詳細	内部統制手続き No	内部統制手続	業務フローNo	会社の内部統制手続	重要	タイプ 予防策	タイプ 自動	不正	不正 電脳	規程・マニュアル	システム名	実施部署	実施者	頻度	証憑・資料
データの不正使用、開示、変更、破損または損失を防ぐために、財務報告に関連するシステムは、適切に保護され、合理的な保証を提供する。	不正アクセスを防止するシステムセキュリティ機能(アクセス権の承認、ユーザ認証、モニタリング等)に不備がある場合、情報の不適切な使用が生じ、財務報告に重大な影響を与えるおそれがある。	【セキュリティポリシー】 情報セキュリティの管理に、適切に経営トップが関与し、ビジネスからの要求と実際の対策が整合している	C-APDI-1	【セキュリティポリシー】 全社的なセキュリティの基本方針が定められ、経営者・管理者に承認されている。また、基本方針は定期的に見直される。	P-APDI-A	【セキュリティ管理】 情シ部の責任者は、「情報システムセキュリティ管理要領」および「情報システムセキュリティガイドライン」を策定し、経営者の承認を得ている。情報セキュリティに関する権限は、情報システム部長に委譲されている。ただし定期的に見直しは行っていない。	○	○		○		情報システムセキュリティ管理要領	–	情シ部	責任者	–	–
		【ITセキュリティ標準】 ビジネスからの要求、IT構成、情報リスク対策計画、情報セキュリティ属上をもとに、全社の情報セキュリティ計画を取り纏めている	C-APDI-2	【ITセキュリティ標準】 セキュリティに関する全社的なリスク分析に基づき、セキュリティの標準が作成され経営者・管理者の承認を受ける。セキュリティ標準はIT環境の変化やリスクの変化に伴い再検討される。	なし	【セキュリティ標準】 リスク分析およびセキュリティレベルの基準を定めた全社的なセキュリティ標準は存在しない。	×	○		○		なし	–	情シ部	責任者	–	–
			C-APDI-3	【システム設定】 セキュリティに関わる各種のシステム設定は、セキュリティ標準に準拠して行われる。	P-APDI-B	【セキュリティの設定】 「情報システムセキュリティガイドライン」に基づき、脆弱のセキュリティ設定に関する文書(ネットワークセキュリティ管理、アクセス権限管理等)が作成され、それにより設定が行われている。	×	○		○		情報システムセキュリティ管理ガイドライン	–	情シ部システム管理G	責任者	発生都度	–
		【ユーザ認証と権限付与】 システムにアクセスしたユーザを個人レベルで認識可能とし、システム及びデータへのユーザアクセス権限を業務規程や職務規定と整合させて付与している	C-APDI-4	【ユーザ認証】 システム(OSやDBMS、アプリケーションなど各階層を含む)へのアクセスは、認証メカニズム(ユーザID/パスワード等)により、制限されている。	P-APDI-B	【ユーザ認証】 「YYYグループ電子認証システム運用マニュアル、利用マニュアル」に従い、ユーザID/パスワードによる認証メカニズムを通じて、アプリケーションやデータへのアクセス権を制限している。			○	○	○	・YYYグループ電子認証システム運用マニュアル ・YYYグループ電子認証システム利用マニュアル ・ERPシステムユーザ管理・権限管理マニュアル	YYYグループ電子認証システム、SAPユーザ認証システム	情シ部YYYG、管理G	責任者	発生都度	–
			C-APDI-5	【ユーザ権限】 ユーザのアクセス権限(プロファイル、グループ、ロール等)が職務権限に応じ設定される。	P-APDI-B	【ユーザ権限】 「YYYグループ電子認証システム運用マニュアル、利用マニュアル」に従い、組織・役割に応じてユーザのグループ分けを行い、アクセス権を設定している。		○		○	○	・YYYグループ電子認証システム運用マニュアル ・YYYグループ電子認証システム利用マニュアル ・ERPシステムユーザ管理・権限管理マニュアル	YYYグループ電子認証システム、SAPユーザ認証システム	情シ部YYYG、管理G	責任者	発生都度	–
		【ユーザアカウントの管理】 一般ユーザ及び特権ユーザのアカウント登録依頼、登録、発行、一時中断、変更、使用中止などのユーザアカウント管理方法が明確になっている	C-APDI-6	【権限付与】 ユーザにアクセス権限を付与するための手続きが規定されており、適切な管理者の承認により権限が付与される。	P-APDI-C	【YYYグループ社員のユーザアカウントの付与(全社アプリケーション)】 社員の入社・異動・退職の際は、人事マスターが変更され、それが各アプリケーションのアクセス権に自動的に反映される。		○		○	○	・YYYグループ電子認証システム運用マニュアル ・YYYグループ電子認証システム利用マニュアル ・ERPシステムユーザ管理・権限管理マニュアル	YYYグループ電子認証システム、SAPユーザ認証システム	情シ部YYYG、管理G	担当者	発生都度	–



情報セキュリティ管理

本メソドロジでは、情報セキュリティに関わる各種標準を提供します。具体的には、ISMSをベースとした、情報セキュリティ管理の標準ポリシー /ガイドラインや、技術対策の実装に向けた情報セキュリティ対策基準等を提供します。
また、情報セキュリティのPDCAサイクル確立に向けた、アセスメントシートやセキュリティ対策レベルのスコアリング基準等を提供します。これらテンプレートを適用することで、継続的且つ網羅的な情報セキュリティ対策の強化を図ることが可能となります。

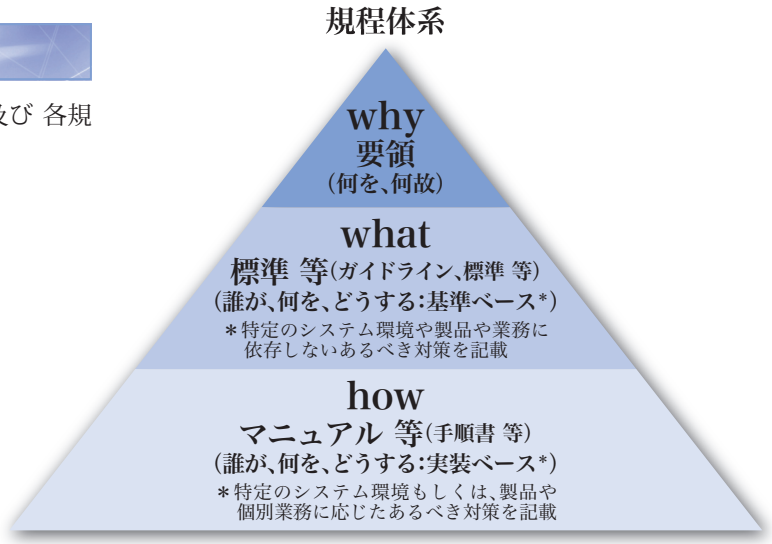
利点・期待効果

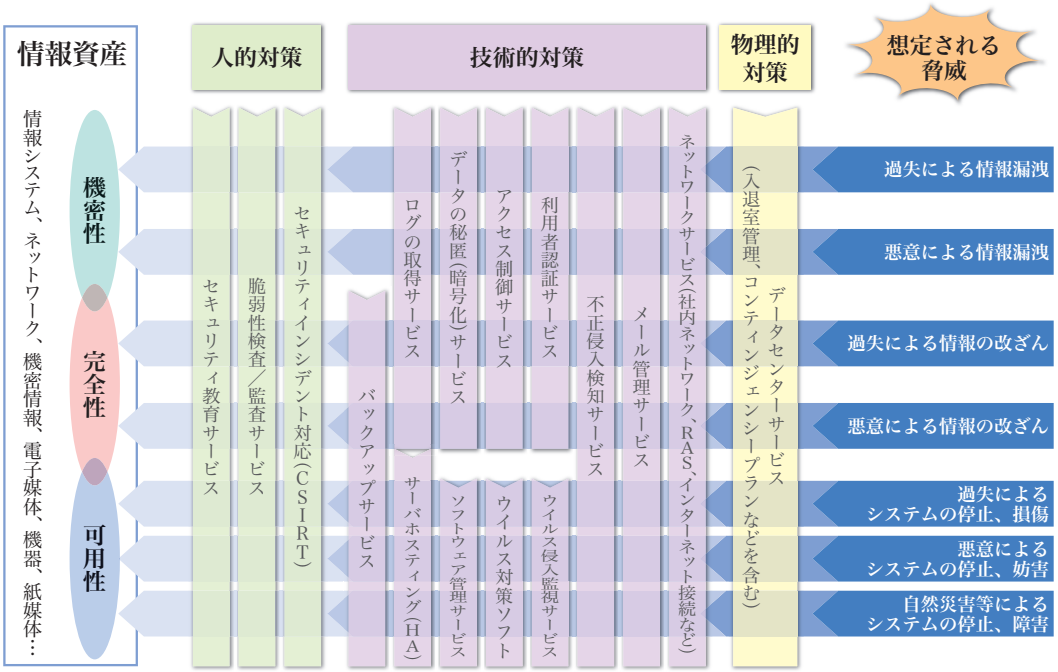
- 現状の情報セキュリティ対策レベルを可視化し、潜在リスクを把握することができます。
- 短期間で情報セキュリティに関わる規定・基準を整備・統合することができます。
- 情報セキュリティ対策レベルを継続的に向上することができます。

（活用する代表的な手法）

情報セキュリティ管理規定体系

要領・標準・マニュアルに層別化された規定体系、及び 各規定にて整備すべき事項、及び 文書のテンプレート





情報セキュリティ対策集

想定される脅威に対する具体的な対策の一覧集（人的対策・技術的対策・物理的対策に分けて整理）

IT-BCP

本メソドロジでは、地震やパンデミック等のディザスター環境下において、必要なITサービスの提供を継続させる、又は 早期復旧するのに必要な手法やテンプレートを提供します。具体的には、重要なITサービスの特定方法や、ITサービス継続計画書や復旧手順書等、災害発生時に利用する各種ドキュメントのテンプレートを提供します。これら手法・ノウハウを活用することで、効果的なITサービス継続計画を短期間で策定・導入することが可能となります。

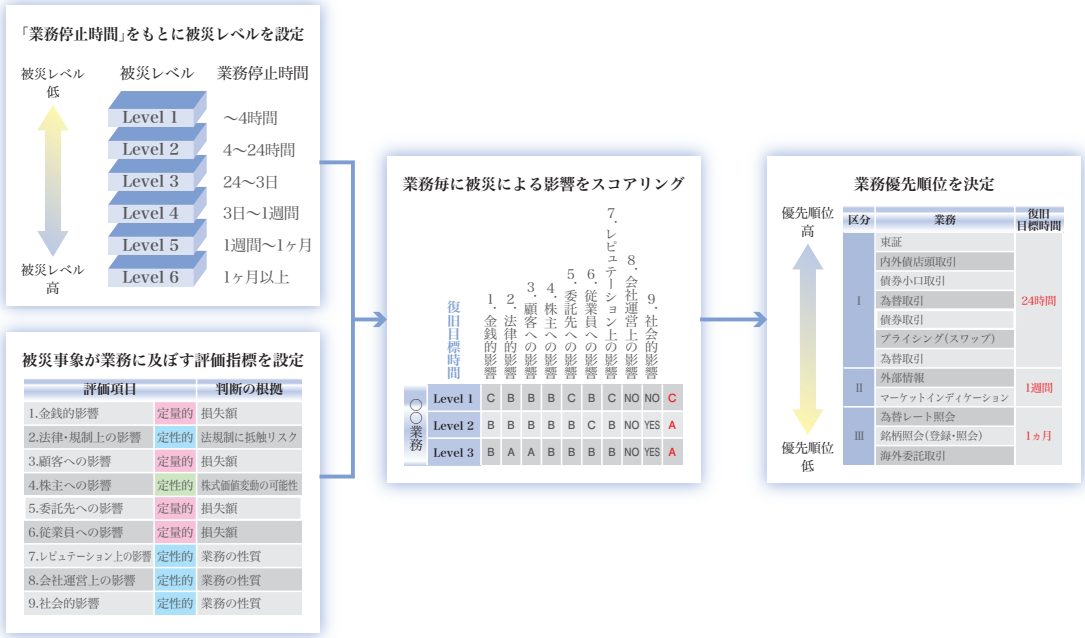
利点・期待効果

- 災害発生時に優先復旧させるITサービスを明確にすることできます。
- 災害発生時の各組織の役割や復旧に向けた対策・手順を明確にすることができます。
- 定期訓練・テストを通じて、災害発生時のIT要員の動きを慣熟させることができます。

（活用する代表的な手法）

ITサービスの重要性判定

業務停止に伴い、各業務がどの程度影響を受けるのかを９つの視点より分析し、業務毎の重要性を定義した上で、被災時の目標復旧時間（RTO）や目標復旧ポイント（RPO）を決定する手法



ITサービス継続計画のテンプレート

災害発生から復旧までを４つのフェーズに分け、各フェーズにおける復旧業務フローやチェックリスト、実際の災害対策本部にて使用する各種テンプレート