e-NAVIGATOR/

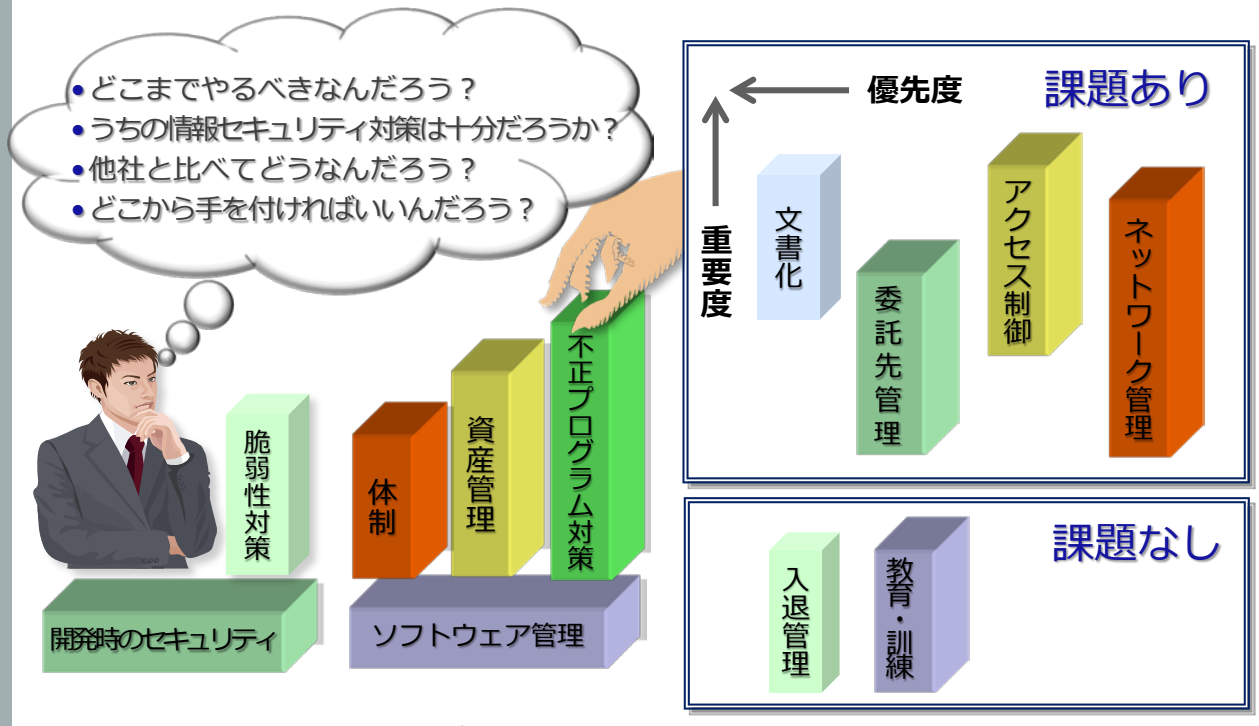
情報セキュリティリスクアセスメント

自社の情報セキュリティ対策を「どこから手を付けて、どこまでやればよいのかわからない。」と頭を抱えている企業は少なくないようです

本サービスは**松竹梅**の3コースを用意しており、課題認識のみならず、改善案の提示、ソリューションの提示、更にはこれらの導入ロードマップも提示します

情報セキュリティ対策整備の検討に有効な情報を提供します

- お客様の情報セキュリティ対策の現状を客観的に調査し**「あるべき姿」**と**「現状」**のギャップをお知らせします
- お客様の状況に合わせて最重要課題を探り、どこから始めるかご提案します
- お客様のご要望やスコープに合わせて事例、対策の進め方、製品や関連サービス、実装後の運用イメージなどをご紹介します



情報セキュリティの専門家が、課題を洗い出し、
重要度・優先度を整理します

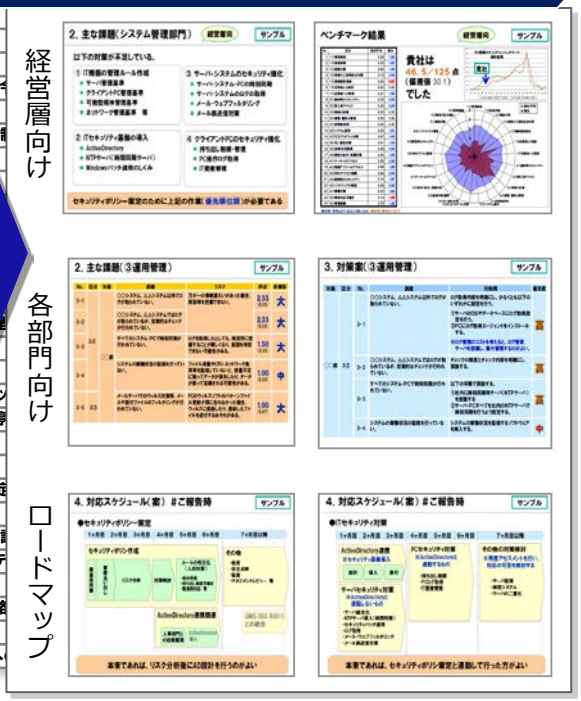
情報セキュリティクリスクアセスメント

■情報セキュリティ監査や情報セキュリティコンサルティングの豊富な経験を持つコンサルタントが担当します
■お客様の情報セキュリティの課題を明確化し、それを基にマネジメントシステムの構築や製品の導入が有効な領域の見定めをお手伝いします
■特にお客様の組織的取組、物理的施策、運用管理、アクセス制御、事業継続における課題を２７区分で整理し、的確な情報セキュリティ対策導入の方向性検討をお手伝いします
■アセスメントの結果から、お客様の取り組み方針とスケジュールを明確化できます

調査結果を区分毎にスコアリング ＞ 報告書作成（ご要望に応じて報告会を開催）

#	区分		ヒアリング内容
1	組織的取組	1①管理規程	セキュリティポリシー・規程、承認、点検・監査の明記
2		1②リスクアセスメント	現状調査、リスク把握、リスク対応計画
3		1③推進体制	情報セキュリティ管理者、部門の推進者、各員の役割、法令
4		1④資産分類	資産目録・管理台帳、管理レベル分け、マル秘表示
5		1⑤情報の工程毎安全対策	情報のライフサイクル毎のセキュリティ対策（手順、取扱者
6		1⑥業務委託契約	選定、SLA、定期的な状況報告
7		1⑦従業者との契約	就業規則での懲戒、入社時誓約書、退職時誓約書
8		1⑧従業者への教育	定期的、全従業者、階層別（役割毎）
9	物理的施策	2①建物等のセキュリティ	セキュリティエリアの区分・明確化、部外者管理、入退
10		2②第三者アクセス	出入り業者（運送業者、清掃業者、メンテナンス 等）
11		2③機器の設置	サーバルームへの入室管理、入り口の配置、盗み見防
12		2④書類・媒体の管理	施錠保管、モバイルPC、媒体の管理、廃棄処分、机上
13	運用管理	3①実稼動環境	開発環境の分離、重要データのテストでの使用、変更管
14		3②システム運用	手順書作成・運用、監視、ログ管理、時刻同期
15		3③バックアップ	バックアップ手順・バックアップ計画の明確化
16		3④不正プログラム対策	ウィルス対策、パタンファイル更新、定期的なウィルスチェッ
17		3⑤ぜい弱性対策	脆弱性情報収集、パッチ適用・テスト、不要なサービスの停
18		3⑥通信NW保護策	VPN・SSL、メールの暗号化、無線LANの暗号化
19		3⑦媒体の紛失・盗難対策	持ち出し制限ルール、暗号化、モバイルPCのユーザ認証
20	アクセス制御	4①データへのアクセス	ID管理（変更・退職時含む）、ID共有しない、パスワード設定
21		4②業務アプリへのアクセス	システム毎のアクセス権の見直し
22		4③NWのアクセス制御	リモートアクセスの認証、セグメント分離、無線LANの設置
23		4④開発時のセキュリティ	入力・出力データのチェック、業務処理プロセス、セキュリテ
24		4⑤ソフトウェアの管理	導入・変更管理手順、ソースコードのアクセス制限、
25	事業継続	5①障害対策	バックアップ、ログ、運用記録、対応手順、訓練、緊急連絡
26		5②事故対応手続き	手順書、エスカレーションルール
27		5③事業継続	事業への影響度把握、復旧手順、バックアップシステムへ

出典：IPA「情報セキュリティベンチマーク（http://www.ipa.go.jp/security/benchmark/）」より



■３つのコースは以下の通りです

梅コース	ベスラインアプローチ	セキュリティ基準(例:ISO/IEC 27001)とのギャップ分析
竹コース	詳細リスク分析アプローチ	情報資産を洗い出し、情報資産毎のリスク分析
松コース	組み合わせアプローチ	ベースラインと詳細リスクを組み合わせてリスク分析

■お客様の状況やご要望に応じて、提供範囲や提供内容のカスタマイズも可能です
■ロードマップに記す対策の導入にあたっては、以下のようなソリューションを用意しております

社内ルール整備	情報セキュリティポリシー、システム運用ルール、業務可視化(業務フロー 等)
ＰＣ対策強化	暗号化、シンクライアント、ウィルス・ワーム対策、資産管理
ネットワーク対策強化	検疫システム、ＩＤＳ／ＩＰＳ、ＷＡＦ、パケットモニタリング
サーバ対策強化	統合ＩＤ管理、統合ログ管理、サーバ監視
災害対策強化	システム仮想化、遠隔地バックアップ
内部統制強化	電子申請（ワークフロー）、メールアーカイブ
セキュリティコスト低減	クラウド、ＡＳＰサービス利用、電子保存
標的型攻撃対策	標的型攻撃対策アプライアンス

お問い合わせは、下記へ

NECソリューションイノベータ　九州支社

〒814-8567　福岡市早良区百道浜二丁目4-1（NEC九州システムセンター）
URL: https://www.nec-solutioninnovators.co.jp/sl/securityconsul/management/asses/index.html
E-mail: qislcm@nes.jp.nec.com