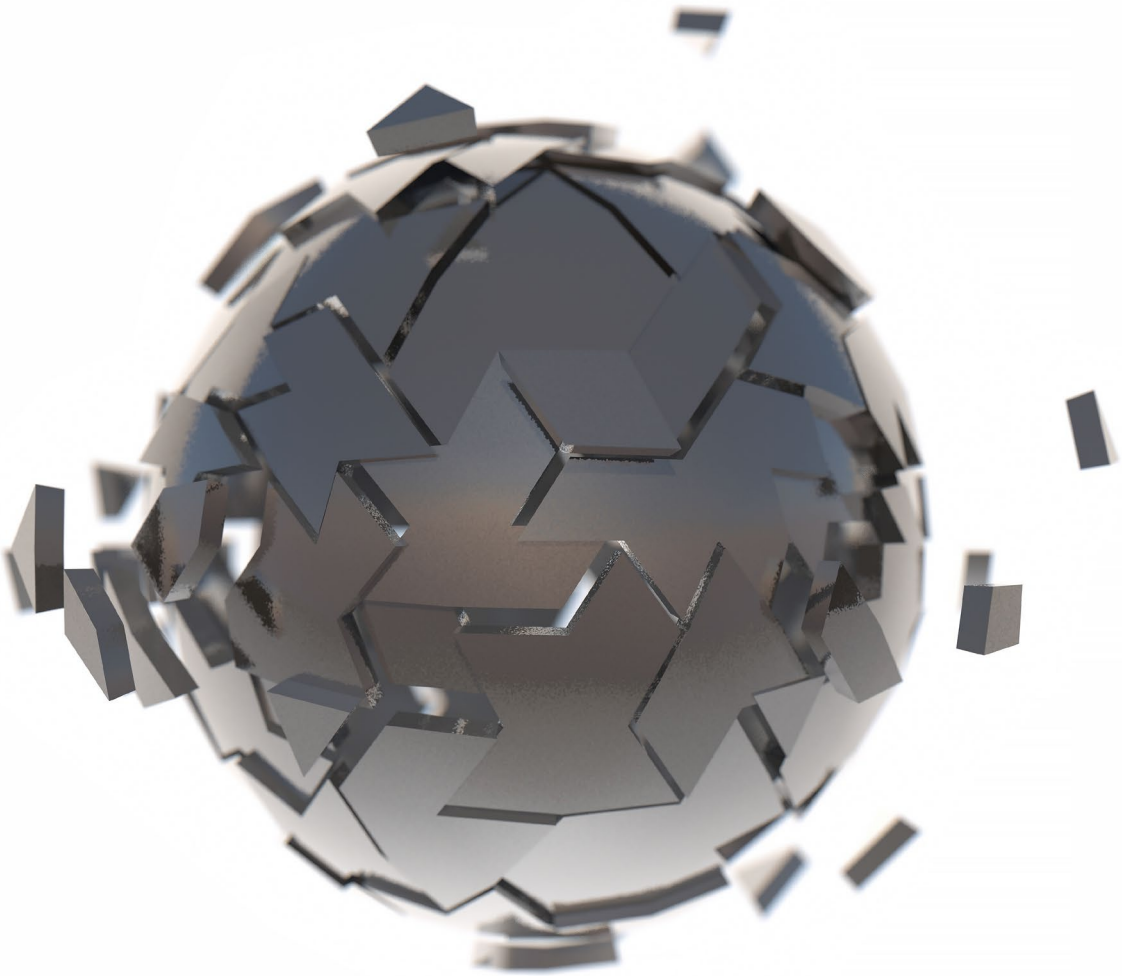
Deloitte.
デロイト トーマツ

トーマツ



サイバーセキュリティリスク管理態勢評価関連サービス

第三者評価、内部監査コソースなど

有限責任監査法人トーマツ

近年脅威の深刻化が著しいサイバーセキュリティリスクに対する対応及び高度化に向けて

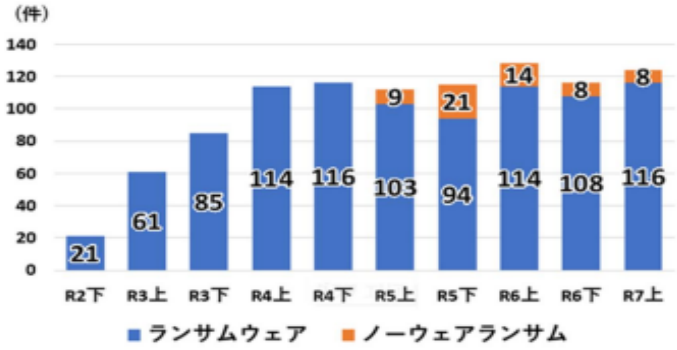
サイバーセキュリティの脅威と企業に求められる対策

現代において企業活動を行う際に情報システムを活用せずに経営を行うことは非常に難しく、顧客との接点、情報収集等でインターネットを活用することは日常となっている状況です。一方で、インターネット経由やサプライチェーン経由など、経路は様々ですが企業へのサイバー攻撃により企業活動が止められる被害は急増しています。このような背景から、各企業のサイバーセキュリティに対する対応の高度化が非常に重要になっています。

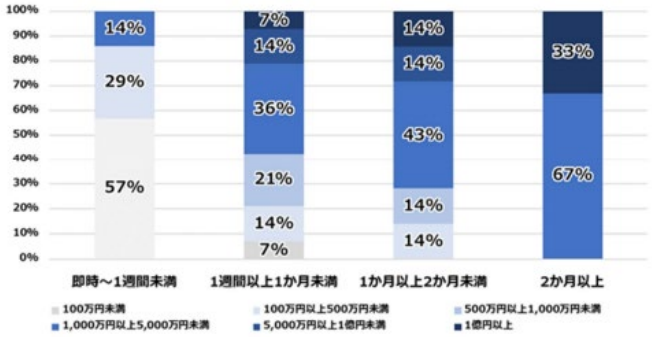
サイバー攻撃で被害を被ると、対処にかかる時間、人的・金額的なリソースを被害対応に割くこととなり、事業活動へ実態的な影響を与えることとなります。サイバー攻撃の中でも特にランサムウェアによる被害件数は依然として高水準で推移しており、年々被害が深刻化しています。さらに、攻撃スピードがより速く、検知が難しいノーウェアランサムという新しい手法も出現しています。復旧にかかる時間も費用も増加傾向であり、攻撃件数の傾向、攻撃手法の進化という観点でも、サイバー攻撃への防御は非常に重視されています。

サイバー攻撃への対応の中で難しい点として、サイバー攻撃に対応するシステムの導入だけでは済まず、サイバー攻撃・システム脆弱性に関する情報の収集、具体的に攻撃を受けた際の対応手順の事前整備、自社への攻撃に関する情報収集と分析といった、組織全体の対応の見直しも求められている点が挙げられます。この継続的な対応にかかる観点から、様々な情報セキュリティに関する機関や、政府当局もサイバーセキュリティの重要性を認識しており、その対処に関するガイドライン等が様々提示されています。

【図表３：ランサムウェア被害報告件数】



【図表４：ランサムウェア被害からの復旧期間と費用の関係性】



※　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも 100 にならない。

(出典)警察庁「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf)

サイバーセキュリティリスクに対する管理態勢評価業務

デロイト トーマツではサイバーセキュリティへの対応及び高度化の取り組みとして、「サイバーセキュリティに関するガイドライン」に基づき以下の対応アプローチを実施します。

第三者評価業務
- ガイドラインに基づき、サイバーセキュリティ管理態勢にかかる第三者評価を実施
- 客観的な視点での評価と偏重のない改善案を提示

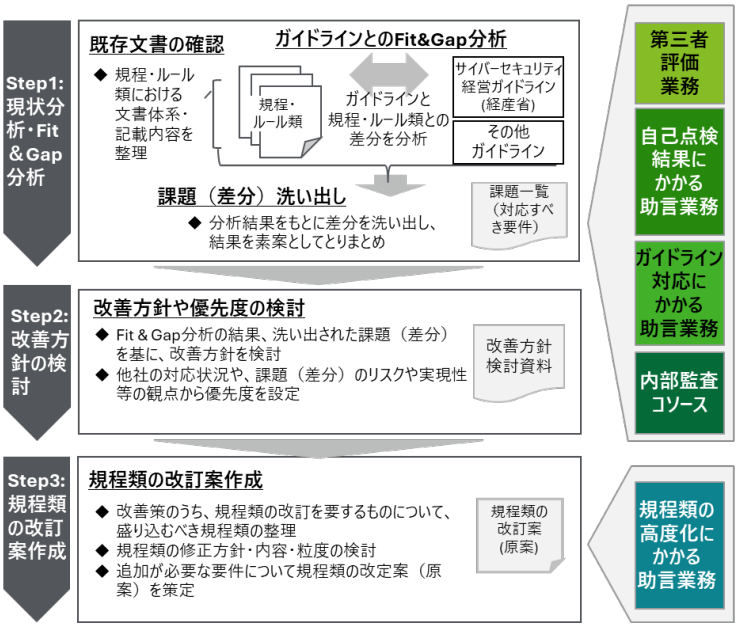
自己点検結果にかかる助言業務
- クライアントが実施する自己点検の結果に対する助言及び自己点検の高度化に貢献

ガイドライン対応にかかる助言業務
- ガイドラインとのFit&Gap分析を実施し課題（差分）を抽出
- 他社の対応状況やリスクを踏まえ、課題（差分）への対応方針の検討にかかる助言を実施

内部監査コソース
- ガイドラインの対応状況やサイバーセキュリティ管理態勢にかかる内部監査への助言を実施
- 内部監査の高度化に貢献

規程類の高度化にかかる助言業務
- 規程類の策定や高度化にかかる助言を実施
- サイバーセキュリティ領域における各業界の固有ポイントを踏まえ、業務プロセスの設計や規程の高度化に貢献

デロイト トーマツがご提案するガイドライン対応アプローチ



評価フレームワークの比較

検討軸	経産省サイバーセキュリティ経営ガイドライン	金融庁サイバーガイドライン	CRI Profile	NIST CSF	CIS Controls
特徴	➢ 業界問わず ➢ 大企業及び中小企業(小規模事業者を除く)の経営者向けのガイドライン	➢ 金融機関向け ➢ 網羅的な評価項目	➢ 金融機関向け ➢ 網羅的な評価項目	➢ 業界問わず ➢ 網羅的な評価項目	➢ 業界問わず ➢ 技術的側面にフォーカス
評価区分	経営者が認識すべき「3原則」及び責任者となる担当幹部（CISOなど）へ指示すべき「重要10項目」を要求	基本的な対応と規模等による2段階の要求	規模やリスク等による4段階の要求レベル	4段階評価結果（Tier≒成熟度）	規模やリスク等による3段階の要求レベル
目的適合性	➢ ガバナンスを含めた全般的な評価が可能	➢ ガバナンスを含めた全般的な評価が可能	➢ ガバナンスを含めた全般的な評価が可能	➢ ガバナンスを含めた全般的な評価が可能	➢ 技術面の評価軸となっており、全般評価には不足
新規性	➢ 2015年12月に経済産業省とIPAにより初版を策定 ➢ 2017年以降改定がなかったが、2023年3月にv3.0が公開	➢ 監督指針に紐づくガイドラインとして新規にリリース ➢ 2024年10月公表	➢ 更新頻度が高く、新たな脅威の有無の把握と対応状況の明確化が期待できる	➢ 2018年以降改定がなかったが、2024年2月にv2.0が公開 ➢ v2.0より、「ガバナンス」「サプライチェーン」にかかる評価項目が追加	➢ 更新頻度が高く、実際の攻撃事例や最新の対策動向をタイムリーに反映、具体的なベストプラクティスが提示
信頼性	➢ 業界問わず広く利用されている	➢ 国内の幅広い金融機関が対象	➢ 国内外での導入は途上	➢ 業界問わず広く利用されている	➢ 業界問わず利用されている
提供機関	➢ 経済産業省	➢ 金融庁	➢ Cyber Risk Institute(CRI)	➢ 米国国立標準技術研究所（NIST）	➢ The Center for Internet Security（CIS）

自社の目的に沿ったガイドラインを選択

サイバーセキュリティに関するガイドラインは複数存在するため、自社の背景、業務環境、特徴や目的を基にサイバーセキュリティ管理態勢に合ったガイドラインを選定することが、サイバーセキュリティリスクに対する対応及び高度化を実現できると考えられます。

また、サイバーセキュリティは一律の対応を求めるものではなく、自社を取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえたうえで、サイバーセキュリティリスクを特定、評価し、リスクに見合った提言措置を講ずる「リスクベース・アプローチ」が求められています。加えて、サイバー空間に国境はないと言われるように、グローバル共通のリスクでもあることから、海外で発表されているガイドラインも併せて参考にすることで、より高度なリスク管理を目指すことが可能です。

デロイト トーマツの強み・実績

グローバルな競争環境の変化の中でサイバーセキュリティをより積極的な経営への「投資」と位置づけ、トップダウンでのサイバーセキュリティ対策推進が求められている中で、デロイト トーマツはサイバーセキュリティにかかる継続的な高度化の取り組みに貢献します。

1 サイバーセキュリティアセスメントにかかる多数の支援実績

- サイバーセキュリティに係る現状を適切に把握し、継続的に評価を実施するためには、国内外で広く利用されている基準（CRI Profile、NIST CSF等）を用いて網羅的にアセスメントすることが肝要です。評価結果に恣意性が入らないことで、対外的なアカウンタビリティも確保することが可能です。
- 当社は、国内外で広く利用されているサイバーセキュリティ基準を用いたアセスメントを多数実施しており、延べ100社以上の実績を有しています。

2 サイバーセキュリティに関する一気通貫のサービス提供と高度な専門性

- 人・モノ・組織・社会インフラなどがあらゆる境界を越えてつながりあうデジタル時代に突入し、サイバー空間におけるビジネスの加速、それを支えるセキュリティの強化は経営課題になっております
- 当社は監査法人を母体としていることから第三者評価が強みであると同時に、戦略からオペレーションに至るまで、デジタル社会で勝ち抜くための一気通貫のサービスを提供しており、貴社環境にフィットする現実的な改善策の提示が可能です。

3 環境に対する理解を活用

- 延べ100社以上の実績を有している当社ならではの環境理解を活かし、効率的に現状を把握・分析します。
- 貴社全体のレベルアップを最優先に考えた深度ある評価を実施します。

※貴社および貴社との関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容が提供できない可能性があります。詳細はお問合わせください。

Deloitte. トーマツ.
デロイト トーマツ

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory