Deloitte.
デロイト トーマツ

インシデント対応体制（CSIRT）の構築

リスクアセスメントに基づく段階的アプローチ

インシデント対応体制（CSIRT）の必要性

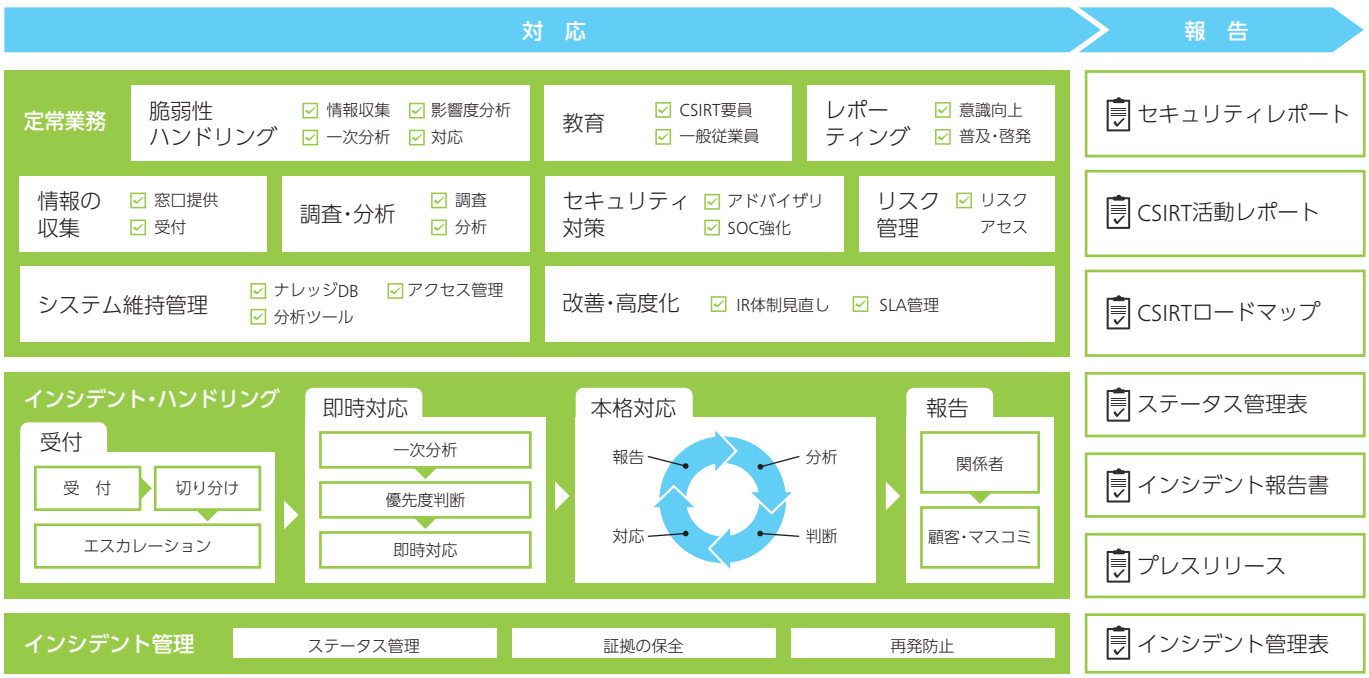
昨今の標的型サイバー攻撃に代表される高度な攻撃は、従来型の予防対策（FirewallやIPS等）だけでは限界を迎えています。実際にインシデントが発生した場合、被害の程度の把握、拡大防止、回復、社内外のステークホルダーへの報告等、担当者は様々な対応に迫られることになります。インシデント発生に備え、あらかじめ迅速・的確な対応を行い、影響を最小限にする仕組み作りが重要です。

このような状況を受け、インシデント対応を行う専用の体制「CSIRT：Computer Security Incident Response Team」を組織内に設置する企業が増えています。従来からのセキュリティ対応組織では、高度なサイバー攻撃に対してリソース面からもスピード感のある対応が難しいケースがあり、積極的なアクションが取られずに被害が拡大するケースが散見されます。従来からの対応組織である総務部門や情報システム部門、リーガル部門、ビジネス部門等、インシデントに関係する様々な組織の位置づけ・役割を含め、企業におけるサイバーセキュリティに対する対応体制について、CSIRTの枠組みを検討する中で、見直し・強化を図ることができます。

サービス概要

デロイトは、グローバルレベルでの長年の経験に基づく独自の方法論を活用し、企業のインシデント対応体制（CSIRT）構築を支援します。デロイトの方法論は、ビジネス視点とリスクアプローチに重点を置き、優先度の高いリスクを考慮した、実効性のある対応プロセスを整備し、企業にとって最適なインシデント対応体制（CSIRT）を早期に実現します。

CSIRTのグランド・デザイン



サービスの流れ

まずは、CSIRTがハンドリング対象とすべき、緊急度の高いリスク発生シナリオを明確化した上で必要となるプロセスを定義し、インシデント対応体制を早期に立ち上げます。次に、中長期的に目指す姿と達成時期に基づき、対応能力の高度化、他組織へ展開を図ります。これらのタスクは、デロイトの方法論に基づいて開発された各種アセスメントシートやテンプレートを活用し、効果的に実現します。

CSIRT構築・展開の流れ

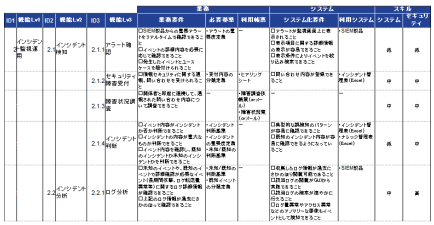
	Step1 現状把握	Step2 体制立上げ	Step3 定着化	Step4 高度化	Step5 他組織展開
目的	☑ 現状の対応状況の把握 ☑ 潜在的なリスクシナリオ洗い出し	☑ 体制を立上げ、インシデント対応によるリスク低減効果を早期に実現	☑ プロセスの改善や追加整備が必要な文書等を整備・運用	☑ 業務の拡張や成熟度向上に向けた施策を実施	☑ 業務を他組織に展開するための計画・準備
主要タスク	☑ 資料調査 ☑ リスクアセスメント ☑ スコーピング	☑ 基本方針の策定 ☑ 業務要件の定義 ☑ ルールの整備	☑ 教育・トレーニングの実施 ☑ ロードマップ作成	☑ KPI一覧の作成 ☑ フォレンジック指針案の作成 …	☑ 展開方針・計画の策定 ☑ コスト試算展開計画案の作成 …

CSIRT立上げ時のポイント（例）

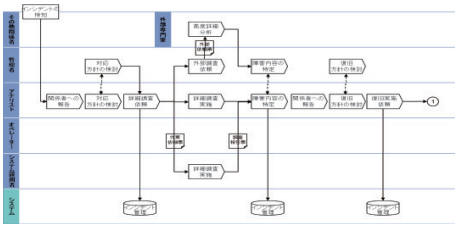
達成目標レベル	短期的、中期的に目指すインシデント対応レベルおよび達成時期
組織での位置付け	役割や、社内の関係部署（総務部門、法務部門、広報部門等）・外部組織との連携方法
ミッション・スコープ	管理対象とするインシデント種別、インシデント対応業務のスコープ等
業務プロセス	CSIRTがハンドリングする業務要件と具体的なプロセスの定義、判断基準の策定

主要な成果物（例）

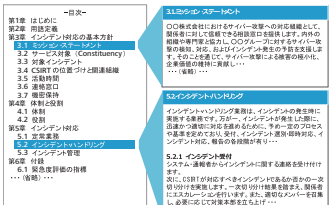
インシデント対応業務一覧



インシデント対応フロー図



インシデント対応ガイドライン



国内ネットワーク

有限責任監査法人トーマツ

東　京　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1112
大　阪　〒541-0042　大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング　Tel:06-4560-6021
名古屋　〒450-8530　愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館　Tel:052-565-5517
福　岡　〒810-0001　福岡県福岡市中央区天神1-4-2 エルガーラ　Tel:092-751-1517

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300