



## 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

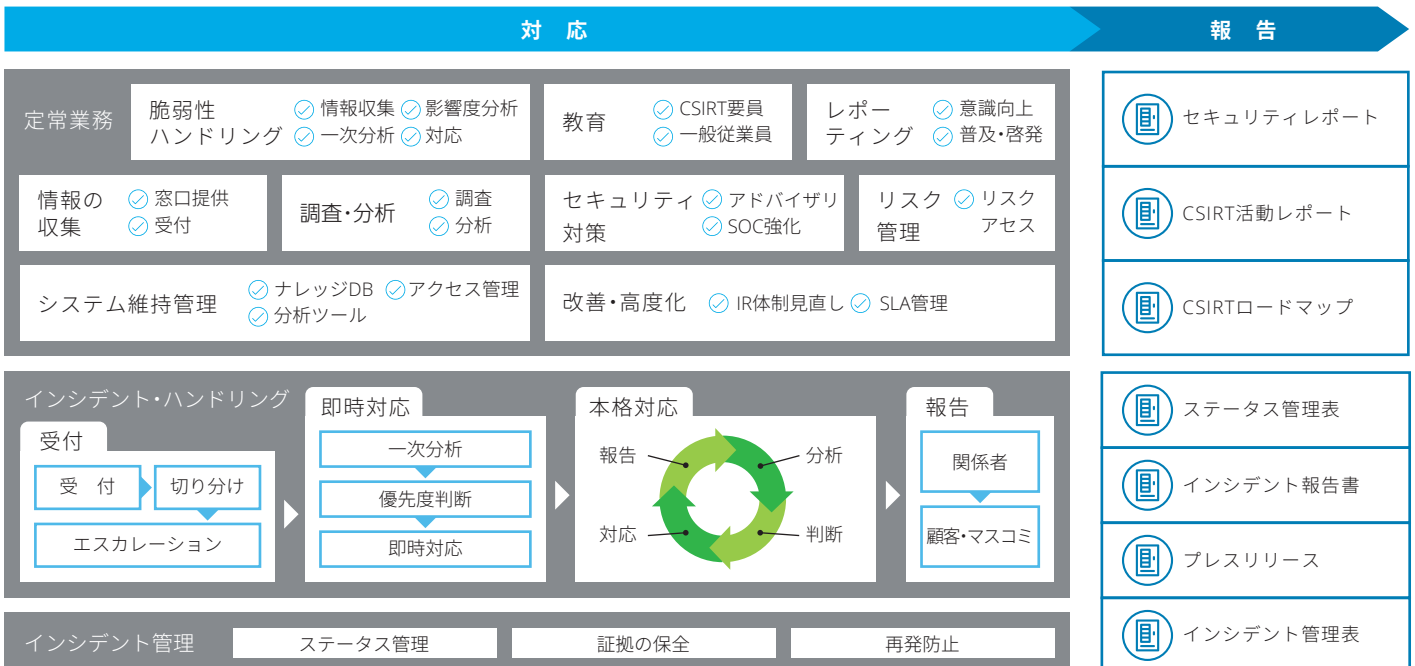
昨今の標的型サイバー攻撃に代表される高度な攻撃は、従来型の予防対策(FirewallやIPS等)だけでは限界を迎えています。実際にインシデントが発生した場合、被害の程度の把握、拡大防止、回復、社内外のステークホルダーへの報告等、担当者は様々な対応に迫られることになります。インシデント発生に備え、あらかじめ迅速・的確な対応を行い、影響を最小限にする仕組み作りが重要です。

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 トーマツ グループは、グローバルレベルでの長年の経験に基づく独自の метод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。

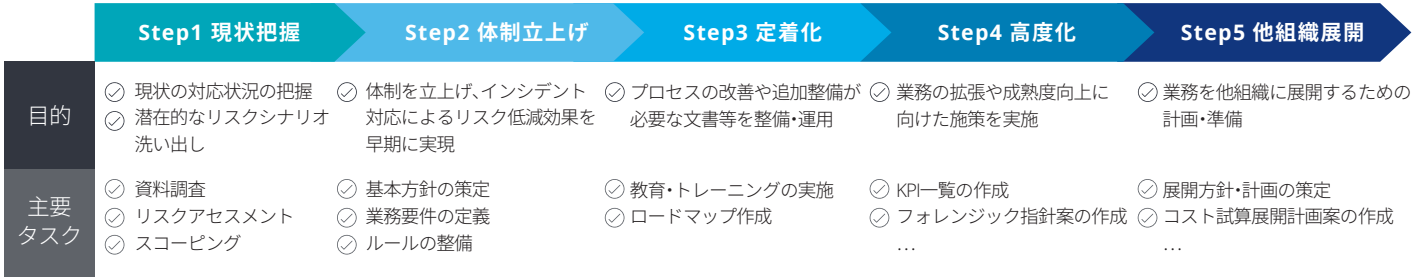
### CSIRTのグランド・デザイン







## 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。

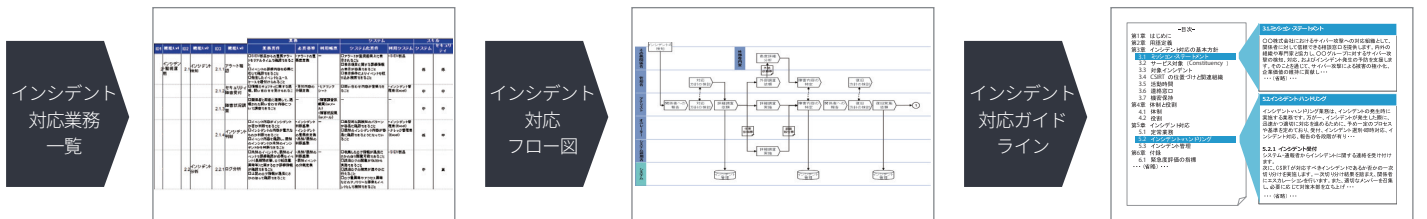
## CSIRT構築・展開の流れ



## 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)



## 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  
 名古屋 〒450-6337 愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋 Tel:052-565-5950

デロイト トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームおよびそのグループ法人(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザー合同会社、デロイト トーマツ 税理士法人およびDT弁護士法人を含む)の総称です。デロイト トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザー等を提供しています。また、国内約40都市に約8,700名の専門家(公認会計士、税理士、弁護士、コンサルタントなど)を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツグループWebサイト(www.deloitte.com/jp)をご覧ください。

Deloitte(デロイト)は、監査、コンサルティング、ファイナンシャルアドバイザーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを Fortune Global 500® の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約225,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド(“DTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数指します。DTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細はwww.deloitte.com/jp/aboutをご覧ください。

Member of  
**Deloitte Touche Tohmatsu Limited**