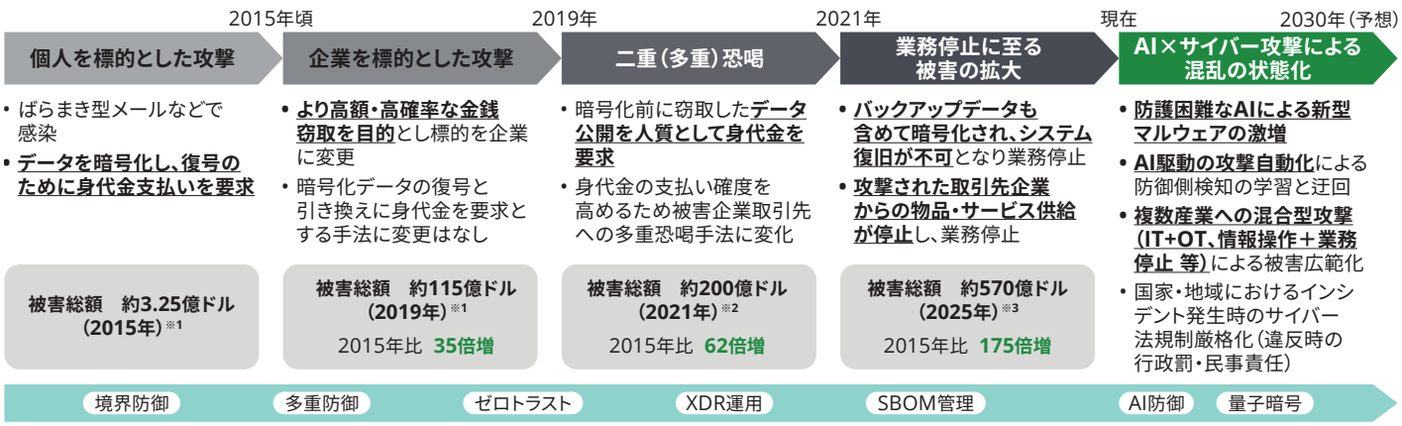
Deloitte.
デロイト トーマツ
Together makes progress

Cyber BCP
–高度化するサイバー攻撃から事業継続を守る–

高度化するサイバー攻撃の被害を最小限にして迅速な回復を実現

ランサムウェア攻撃による被害の深刻化

RaaS・AI等のテクノロジーの登場により、マルウェアによるサイバー攻撃の敷居は下がり攻撃が急増、今まさに攻撃者優位が深刻さを増す時代の幕開け前夜の様相を呈しています。特にランサムウェア攻撃による脅威は深刻化の一途を辿っており、近年では特に業務停止による影響が深刻化し重大リスクとなっています。



※1. Steve Morgan. “Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019” . CYBERCRIME MAGAZINE. 2017-11, https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/, (参照 2025-9-26) .

※2. David Braue. “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031” . CYBERCRIME MAGAZINE. 2021-6, https://cybersecurityventures.com/ransomware-report-2021/, (参照 2025-9-26) .

※3. CYBER SECURITY Ventures. “GLOBAL RANSOMWARE DAMAGE COST PREDICTIONS IN USD, 2025 TO 2031” . CYBERCRIME MAGAZINE. 2023-11, https://cybersecurityventures.com/wp-content/uploads/2023/11/RansomwareCost.pdf, (参照 2025-9-26) .

レジリエンス確立に求められるサイバーセキュリティのあり方

サイバー攻撃・ランサムウェアによる被害発生が不可避となるなかで、サイバーレジリエンスの実現により、事業影響を最小限に食い止める施策が求められています。サイバーレジリエンス実現の根幹となるのがサイバーBCPであり、企業が高まるサイバー攻撃の脅威に対抗し、仮に攻撃を受けたとしても、柔軟性をもって有事体制を編成し、事業を継続していくために最も重要となります。

	予防に力を入れたサイバーセキュリティ		迅速な回復を目標としたサイバーセキュリティ
目的	攻撃による被害を出さないことに注力 ・セキュリティリスクの発生可能性を最小化 特定 → 防御 → 検知 → 対応 → 復旧	×	**攻撃の被害を受けることを前提に被害を最小化し迅速な回復を実現（“レジリエンス”の確立）** 特定 → 防御 → 検知 → 対応 → 復旧
視点	**防御主導のIT視点** • 情報システム部門が中心となり、防御やシステムの安全性に注力 • 業務継続や顧客対応は各部門の判断に依存 • “システムを守ること”が軸		**事業継続主導の経営視点** • 経営・事業・ITが運携し、事業中断リスクを管理・対応 • 顧客・取引先・社会への影響を最小化する視点で意思決定 • “事業を止めないごと”が軸
進め方	• EDR、SOC、脆弱性管理など、特定・防御・検知への技術投資 • インシデント発生後は各システム・部署に任せた個別対応		• **サイバーBCP*の策定と実装** *Cyber-Business Continuity Plan

サイバーBCP 整備における課題と取組

サイバー攻撃による壊滅的な状態から通常業務への迅速・効率的な復帰までには、多くの関係者の関与と施策が必要であり、あるべき姿実現までの戦略を立て推進することが肝要です。

危機対応態勢
単一システム障害への備えはあるが、大規模なサイバー攻撃への全社的な対応に適した体制・プロセスが十分に整備されていないケースが多く見受けられます

多数のサードパーティ
現代の複雑なエコシステムやサプライチェーンでは統合的な復旧アプローチが求められますが、復旧計画ではこの点が十分に考慮されていないことが多くあります

財務面優先の意思決定
壊滅的なサイバー攻撃の際、組織は復旧のスピードやコストを優先した意思決定を迫られ、セキュリティ対策が後回しになる傾向があります

復旧の優先順位付け
被害の生じたITインフラ復旧が場当たり的に行われ、ビジネス継続に必要とするものとの間にギャップが生じることで、復旧がさらに遅れる原因となる場合があります

データバックアップと保管
従来型の復旧手法は、壊滅的なデータ破壊が生じた際には万全とは言えません。すべてのバックアップが感染し利用不可となるリスクがあります

コミュニケーションの手段確保
ネットワーク依存型のコミュニケーション手段は、インシデント発生時に利用できなくなり、社内外の情報伝達が制限されることがあります

人・モノのリソース確保
限られた重要リソースへの過度な依存や、物理インフラの損傷・過負荷によって、さらなる復旧の遅延が発生する可能性があります

復旧作業への備え
組織は、広範囲に影響が及ぶ深刻なサイバー攻撃からの復旧を支援するための文書や計画、ツールが不足しています

※Deloitte UK “Digital Resilience and Enterprise Recovery”より

事業継続を守るサイバーBCPの確立に向けた戦略

デロイト トーマツ グループのサイバーBCP 整備におけるアプローチ

サイバーBCP 整備の取組は段階的な目標を定め推進することで、ステークホルダーとの合意形成を図りつつ、確実にあるべき姿に到達します。デロイト トーマツ グループは組織のサイバーレジリエンスを高めるサイバーBCP 策定アプローチの全てのPhaseにおいてサービスの提供が可能です。

	Phase1 方針・戦略策定	Phase2 計画立案・復旧手順整備フェーズ	Phase3 運用フェーズ	Phase4 展開・定着化フェーズ	Phase5 技術的対策によるBCP強靭化
取組	• 中長期の取組となるサイバーBCP策定に向け、ビジネスの優先度、ストラクチャーやステークホルダー、想定リスク等の全体骨子を戦略・方針として纏める • 戦略・方針を経営全体で合意形成する	• 対策本部体制とステークホルダーの役割・責任定義 • サイバーBCP取組の拠り所となる規程文書類、対応フローを作成 • 事業システムの復旧手順整備	• 最重要システムなど、一部システムでの運用開始しつつ、手順の改善を図る • 全従業員（経営層を含む）教育・訓練により定着を図る	• Phase2の成果を活用し、事業部門、グループ会社等へ展開しサイバーBCPの取り組みを全社に拡大する	• テクノロジー導入により被害範囲の極小化、検知の強化、回復プロセスの高速化など有事に備えたITシステムのレジリエンス強靭化を図る

合同会社デロイト トーマツ
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtllc
【国内ネットワーク】東京・大阪・名古屋・福岡

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