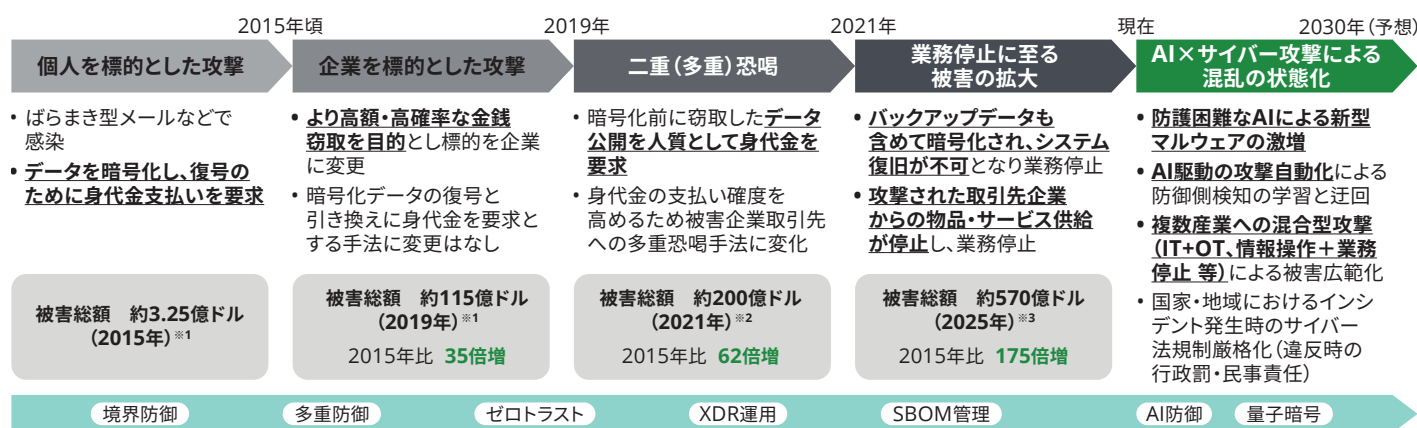


## Cyber BCP - 高度化するサイバー攻撃から事業継続を守る -

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が連携し、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。

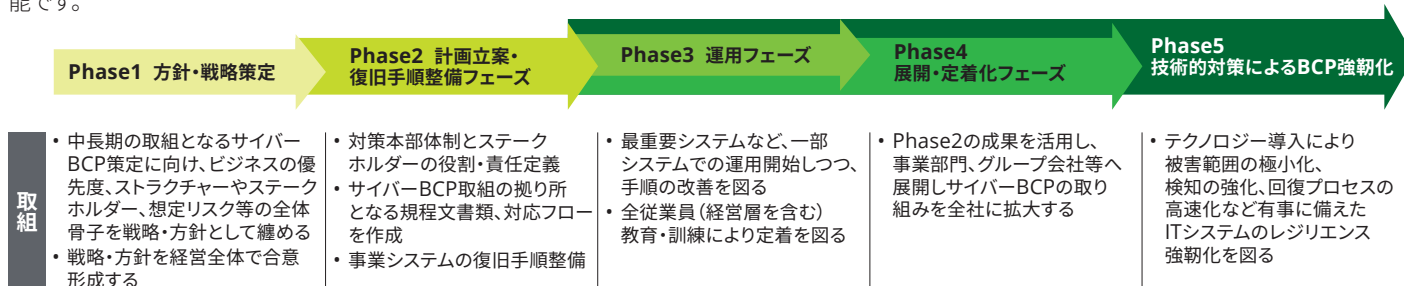
<b>危機対応態勢</b> 単一システム障害への備えはあるが、大規模なサイバー攻撃への全社的な対応に適した体制・プロセスが十分に整備されていないケースが多く見受けられます	<b>多数のサードパーティ</b> 現代の複雑なエコシステムやサプライチェーンでは統合的な復旧アプローチが求められますが、復旧計画ではこの点が十分に考慮されていないことが多くあります	<b>財務面優先の意思決定</b> 壊滅的なサイバー攻撃の際、組織は復旧のスピードやコストを優先した意思決定を迫られ、セキュリティ対策が後回しになる傾向があります
<b>復旧の優先順位付け</b> 被害の生じたITインフラ復旧が場当たり的に行われ、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	<b>データバックアップと保管</b> 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	<b>コミュニケーションの手段確保</b> 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
<b>人・モノのリソース確保</b> 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	<b>復旧作業への備え</b> 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。



## 合同会社デロイト トーマツ

Mail ra\_info@tohmatu.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

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイト トーマツ、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プロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、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）とは、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバル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れらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を含みます。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Globalはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。

デロイト アジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オーストラリア、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能な継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.comをご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバル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れらの関係法人（総称して“デロイトネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDeloitte Global、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生したいかなる損失および損害に対しても責任を負いません。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体です。

Member of  
Deloitte Touche Tohmatsu Limited

© 2026. For information, contact Deloitte Tohmatsu Group.



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