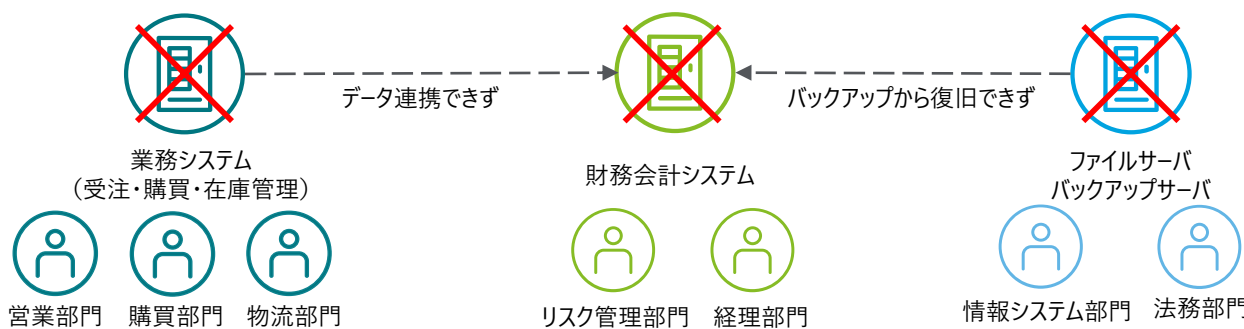


サイバーインシデント時の業務継続・復旧サービス

サイバー・危機管理・法務の専門家がワンチームとなり、深刻なサイバー攻撃からの復旧から、決算・J-SOXへの対応、ITガバナンスの強化までワンストップで支援します。

国内製造業におけるサイバー攻撃被害と対応事例

サイバー攻撃によって業務や決算が停止する深刻な状況に陥った場合には、業務の再開、決算・J-SOXへの対応、セキュリティ強化やシステムリカバリ・再構築といった対応を、決算開示期日を見据えたタイトなスケジュールで全社横断的に進めることになります。



業務の復旧

- 顧客からの受注や取引先からの納品、請求管理を手作業で対応
- 各顧客や取引先からのクレーム対応
- 各拠点における臨時棚卸対応
- 手作業負荷軽減のためにクラウドに暫定ERPを導入
- 暫定業務プロセスと内部統制を構築

決算・J-SOXへの対応

- システム復旧は断念し、クラウドに新会計システムを構築
- 紙帳票等をもとに経理伝票をエクセルで再作成
- 売上集計や入金消込を手作業管理
- 手作業等の暫定対応期間における複雑化した内部統制評価の対応
- 全社統制としてのITガバナンス強化の対応

インシデント対応・システム再構築

- バックアップサーバ暗号化によって、システムのリカバリを断念
- ファイルサーバ暗号化による作業データなどが消失
- 暗号化されたファイルの漏洩の可能性を個人情報保護委員会へ報告
- 従来システムの再構築とセキュリティ強化対応

J-SOXにおいても高まる「サイバーリスク」への対応

サイバー攻撃による業務・システム停止によって、有価証券報告書や四半期報告書の提出が遅延した場合に、内部統制報告書に「開示すべき重要な不備」を記載する例が出てきており、今やサイバー攻撃は会計不正やコンプライアンス違反と同等水準の財務報告上のリスクになりつつあります。

かかる状況を受け、金融庁が2022年12月に公表したいわゆる内部統制基準と実施基準改訂の公開草案では、「ITへの対応」の項目でサイバーリスクの高まりによるセキュリティの確保にまで言及されており、サイバー攻撃が決算に及ぼす影響が内部統制上の不備として検討される方針が明確化されようとしています。

財務報告に係る内部統制の評価及び監査の実施基準 「IT（情報技術）への対応」

ITへの対応とは、組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のITに対し**適時かつ適切**に対応することをいう。

<中略>

また、情報システムの開発・運用・保守などITに関する業務の全て又は一部を、外部組織に委託するケースもあり、かかるITの委託業務に係る統制の重要性が増している。さらに、クラウドやリモートアクセス等の様々な技術を活用するに当たっては、サイバーリスクの高まり等を踏まえ、**情報システムに係るセキュリティの確保が重要である。**

出所：金融庁「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（公開草案）」（2022年12月15日付）

※下線太字は特に重要な改訂予定の記載

支援事例の紹介

国内大手製造業：国内各拠点における大規模なランサム攻撃被害への対応として、サイバーフォレンジック、システム・業務復旧、決算・J-SOX対応、ITガバナンスの強化、これらの統合支援PMO業務をワンストップで支援しました。

	縮退期	暫定復旧期	完全復旧期
インシデント発生	手作業代替対応	仮システムや一部復旧システム利用	復旧システムや新システム利用
サイバーフォレンジック	封じ込め・侵害調査 <ul style="list-style-type: none"> 攻撃手法や被害範囲の調査 漏洩情報のダークウェブモニタリング 個人情報保護委員会への報告対応助言 	応急的な対処 <ul style="list-style-type: none"> 発見された脆弱性への対処方針策定 適切なF/W配置やゼロトラストによる安全なネットワーク構成構築の助言 EDR等の監視体制の導入助言 	再発防止策実施 <ul style="list-style-type: none"> 技術面だけでなくITガバナンスの原因分析 ITガバナンス体制・ポリシーの改善助言 脆弱性管理・対処プロセスの構築 IT子会社や委託先の管理強化助言
システム・業務復旧	システムを利用しない縮退運用支援 <ul style="list-style-type: none"> 手作業運用できる最低限の業務を想定した縮退業務プロセスの構築支援 	リカバリ実施と仮システム構築 <ul style="list-style-type: none"> 既存システムリカバリ・仮システムの導入支援 仮システムに合わせた仮業務フローと内部統制の構築 	新業務プロセス構築 <ul style="list-style-type: none"> 仮業務中のデータフロー整理やDB再構築支援 新たな業務フローと内部統制の構築支援
決算・J-SOX対応	開示期限遅延と応急対応検討 <ul style="list-style-type: none"> 会計監査人・財務局への初動対応支援 決算・財務報告プロセス再構築支援 棚卸実施や入金・支払管理体制の構築支援 	手作業対応期のフォロー <ul style="list-style-type: none"> 請求誤り確認や入金消込体制構築支援 受注・出荷や棚卸資産管理体制の構築支援 暫定決算用帳票やダッシュボードの作成支援 	決算正常化への対応 <ul style="list-style-type: none"> 顧客との売掛金等のプレ残高確認支援 仮業務等を経て複雑化した業務プロセスと内部統制評価支援 リカバリ対応を含めたIT全般統制評価支援
全社統制・ITガバナンス	再発防止の基礎となる原因究明 <ul style="list-style-type: none"> サイバーフォレンジック調査と連携したセキュリティ施策の技術面・運用面の原因分析 	暫定セキュリティ強化措置の導入 <ul style="list-style-type: none"> 少なくとも同様の攻撃を防ぐための技術面・運用面における再発防止措置の整備・運用体制構築支援 	IT戦略とガバナンスの見直し <ul style="list-style-type: none"> 全社ITポリシーや運用マニュアルの再整備支援 セキュリティ強化や新たなIT戦略のロードマップ策定支援

デロイト トーマツ ファイナンシャルアドバイザリー合同会社
 フォレンジック & クライシスマネジメントサービス
 〒100-8363 東京都千代田区丸の内3-2-3 丸の内二重橋ビルディング
 TEL 03-6213-1180 FAX 03-6213-1085
 E-mail dt-cm@tohmatu.co.jp

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デロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスク アドバイザリー 合同会社、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 アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ グループ 合同会社を含む）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、監査・保証業務、リスク アドバイザリー、コンサルティング、ファイナンシャル アドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、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、デロイト トウシュート マツ リミテッド（“DTTL”）、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指します。DTTL（または“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すまたは拘束させることはありません。DTTL および DTTL 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。DTTL 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DTTLのメンバーファームであり、保証有限責任会社です。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（オークランド、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、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務・法務などに関連する最先端のサービスを、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し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で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175年余りの歴史を有し、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45万人超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、デロイト トウシュート マツ リミテッド（“DTTL”）、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DTTL、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得る損失および損害に対して責任を負いません。DTTL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

危機管理センター

インシデント発生時の緊急連絡先
 情報漏洩、法令違反、品質不正、会計不正、サイバー攻撃など、今すぐにご相談されたい方はこちら

メールでのお問い合わせは
 dt_emergency@tohmatu.co.jp
 24時間受付中

電話でのお問い合わせは
 **0120-123-281**
 平日9:00~17:00受付



BSI
 ANAB
 ACCREDITED
 MANAGEMENT SYSTEMS
 CERTIFICATION BODY

IS 669126 / ISO 27001



BSI
 UKAS
 MANAGEMENT SYSTEMS
 0003

BCMS 764479 / ISO 22301