TOKIO MARINE

リスクマネジメント最前線

2026 | No. 3

ランサムウェア攻撃による IT システム停止期間の長期化とその対応

三宅 諒介（サイバーセキュリティ事業部 主任研究員）
川口 貴久（ビジネスリスク本部 兼 経営企画部 主席研究員、マネージャー）
太田 瑛美（ビジネスリスク本部 副主任）

要約

近年、ランサムウェア攻撃による被害が長期化するケースが増えている。複数の要因が重なり、事業・業務に不可欠な IT システムの停止期間が事前の想定よりも長期化し、数カ月に及ぶこともある。他方、必ずしも優先事業・重要業務が IT システム停止期間を通じて停止している訳ではなく、IT システムが利用できない状況であっても、事業・業務の継続もしくは早期復旧が可能な場合がある。本レポートはランサムウェア攻撃による被害想定、特に IT システムの停止期間に焦点を当て、IT システムの停止期間の一般的傾向や停止期間の長期化要因を示し、企業に必要な対策を紹介する。

目次

1．サイバー攻撃の被害想定とITシステム停止期間

（1）ランサムウェア攻撃を想定した危機対応計画・BCP

企業の多くは、サイバー攻撃が発生した場合の危機対応計画・事業継続計画（BCP）を策定している。本来、サイバー攻撃といっても、ウェブサイトの改ざん、機密情報の漏洩、インターネット接続製品の障害等多岐にわたる。しかし、**多くの計画の被害想定はランサムウェア攻撃を前提とする**傾向にある。

なぜなら、第一に、ランサムウェア攻撃は実態として甚大な被害を与えることが少なくない。ITシステムの復旧（時点）の定義にもよるが、大手小売事業者（2025年10月）、大手総合飲料メーカー（2025年9月）、救急医療機関（2022年10月）は**ランサムウェア攻撃によって約2カ月間、事業に必要なITシステムが利用できなかった**。飲料メーカーと救急医療機関のケースでは、比較的最近のバックアップデータは健全だった（暗号化されなかった）が、主要なITシステムの復旧までに長い時間を要した。

第二に、ランサムウェア攻撃はサイバーセキュリティ・情報セキュリティを構成する多様な価値を脅かす。ランサムウェア攻撃は、情報セキュリティの「C」「I」「A」、すなわち①企業が保有する個人情報・営業秘密を窃取し、機密性（confidentiality）を脅かし、②探索活動を含めて、多くのデータやシステムにアクセスすることで、完全性（integrity）に疑念を与え、③データやプログラムの暗号化を通じて、可用性（availability）を制限する。

言い換えれば、企業はランサムウェア攻撃を念頭においた被害想定と対応態勢を整備することで、サイバー攻撃の甚大かつ多様な被害に備えることができる。

（2）ITシステムの停止期間の長期化

ランサムウェア攻撃の「被害想定」は、初期侵害経路、原因、影響の範囲と深さ等、様々な要素から構成される。しかし、IT部門やセキュリティ部門は別として、事業部門にとって重要な被害想定の核心は**どのようなシステムやアプリケーションがどれほどの期間、使えないのか**、である。ITシステムの利用可否と利用停止期間は、事業の継続に直結する問題である。BCPを策定済みの企業の多くはランサムウェア攻撃による被害として、IT系（メール、ファイル共有等）や業務系（経費処理、受発注等）のシステムやアプリケーションが「〇日」「〇週間」停止するといった想定をおいている。

しかし近年、ランサムウェア攻撃をはじめとしたサイバー攻撃による被害が甚大化するケースが増えている。特に、複数の要因が重なり、事業に不可欠なITシステムの**停止期間が事前の想定よりも長期化し、数カ月に及ぶ**こともある。いわば、**サイバー攻撃の「過酷事象」**[1]とも呼ぶべき被害様相が散見される。

他方、必ずしも優先事業・重要業務がITシステム停止期間を通じて停止している訳ではなく、ITシステムが利用できない状況であっても、事業・業務の継続もしくは早期復旧が可能な場合がある。このため、「目標復旧時間（Recovery Time Objective: RTO）」や「最大許容停止時間（Maximum Tolerable Period of Disruption: MTPD）」はほとんどの場合、事業面を指すものだが、事業・ビジネスとは異なる観点で、ITシステムのRTOやMTPD、停止期間のメインシナリオ・過酷事象シナリオを分析・想定しておくことが重要である。

[1] 「過酷事象」の考え方はサイバー攻撃に限定されない。例えば、首都直下地震対策検討ワーキンググループの被害想定でも「過酷事象」という考え方が示されている。

（3）ITシステム停止期間と事業停止期間

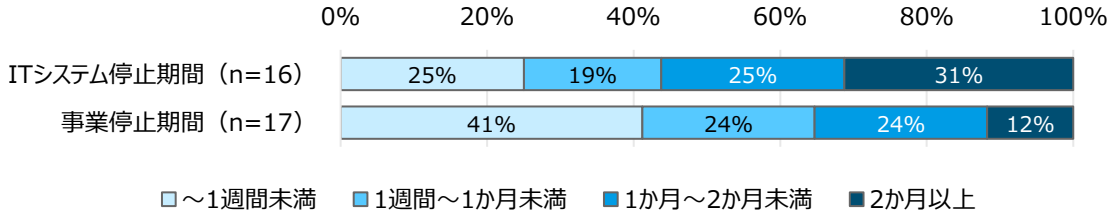
ランサムウェア攻撃の被害を評価する際、「ITシステム停止期間」と「事業停止期間」を明確に区別する必要がある。本稿における「ITシステム停止期間」とは、攻撃によって、優先事業や重要業務に不可欠な**主要ITシステムが停止してから復旧・再稼働するまでの期間**を指し、「復旧」には、優先事業や重要業務に関連する主要ITシステムの新規インスタンスや仮想化基盤等の再構築・クリーン作業、バックアップデータの再投入、システムの健全性確認、システム間連携の調整等、技術的な復旧作業の工程が含まれる。一方、「事業停止期間」とは、ランサムウェア攻撃によって**企業の優先事業や重要業務が停止してから再開するまでの期間**を指し、ITシステム停止期間とは異なる場合がある。

筆者らが国内外の重大ランサムウェア攻撃22事例を対象に行った被害調査では、**ITシステム停止期間が数カ月に及んだ企業でも、事業停止期間は数日から数週間に抑えられている**ケースが見られた。これは、企業が手作業やFAX等の代替手段等により、主要ITシステムが利用できない環境でも重要業務を再開・継続できるためである。特に、システム導入以前のアナログ作業の記録や経験者が現場に残っている企業では、そのノウハウを活用することで、早期から事業を再開できる可能性が高い。この調査において、**ITシステムの平均停止期間は45日間、1カ月以上の停止が56.3%**を占めている。

警察庁が公表している「サイバー空間をめぐる脅威の情勢等」の統計データ（2021-2025年上期）によると、ランサムウェア攻撃から復旧までに1カ月以上を要した被害企業（「復旧中」を含む）の割合は、44-49%で推移している。約半数の企業が長期間の復旧作業を強いられており、2カ月以上を要する深刻な事案も毎年一定数発生している。警察庁データは「復旧」を明確に定義していないが、ITシステムの復旧とみられ、前述の国内外22事案を対象としたランサムウェア攻撃調査の結果とほぼ整合する。

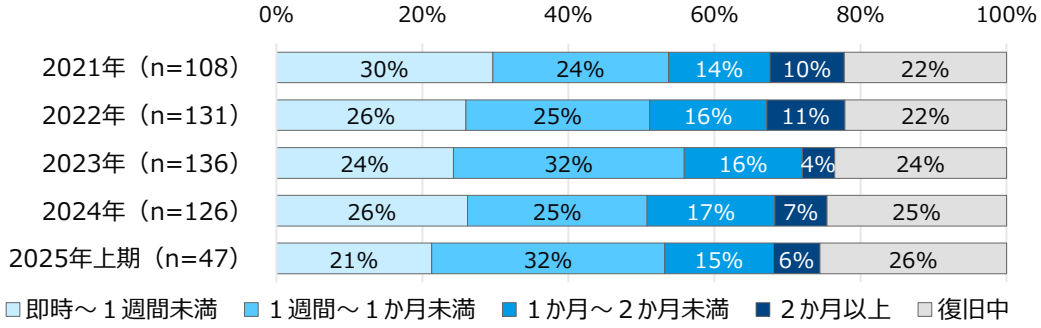
現状では、ランサムウェア攻撃を受けた企業の約半数がITシステム復旧に1カ月以上を要している。この長期化要因を理解することが、適切な対策を講じる上で重要となる。

■ 図1：重大ランサムウェア攻撃22事例のITシステム停止期間と事業停止期間



出典：東京海上ディーアール作成。

■ 図2：（警察庁）ランサムウェア攻撃から復旧までに要する時間



出典：警察庁「サイバー空間をめぐる脅威の情勢等」の統計データを基に筆者作成。サンプル数の27-36%が大企業

2．IT システム停止期間の長期化要因

（1）長期化要因の全体像

本パートでは、ランサムウェア攻撃の大規模被害 22 事案から、何が IT システムの停止期間を長期化させるのか、その要因を整理・考察する。実際の被害例からみても、**ランサムウェア被害が発生した際に、IT システムの停止期間を長期化させる単一の要因を特定することは困難**であり、様々な要因が複合的に絡み合うことで、復旧に要する時間が長期化しているケースが多いように見受けられる。しかし、22 事案からは共通の傾向も抽出可能であり、IT システム停止期間の長期化要因は表 1 の通り、大きく**「システム運用に関する要因」と「組織・体制に関する要因」に整理**できる。

■ 表 1：ランサムウェア被害における IT システム停止期間を長期化させる要因（抜粋）

分類	要因	復旧への影響
システム運用に関する要因	データやシステムのバックアップ**【重要】**	▪ バックアップデータもランサムウェアによって暗号化された場合、復旧の起点を失い、データ及びシステム復旧が長期化する可能性がある。 ▪ バックアップデータが被害を免れていたとしても、システム間の整合性検証で復旧は長期化する可能性がある。（後述）
	システム、ドメイン等の特権管理	▪ 特権アカウントを窃取されると、被害がシステム基盤やネットワーク全体に波及し、一からシステムの再構築が必要となり、復旧が長期化する可能性がある。（クラウド環境や仮想化基盤、ドメイン全体等）
	ログの収集と調査**【重要】**	▪ ログが不足している場合は、適切な調査ができず、信頼回復や追加調査対応が求められ、復旧が長期化する可能性がある。（後述） ▪ 報告・対外公表においても、適切な調査に基づく対応が困難な場合は、ステークホルダーからの信頼回復が遅れ、インシデントの収束やシステム復旧が長期化する可能性がある。（後述）
組織・体制に関する要因	IT 資産管理[2]	▪ IT 資産管理に不備があると、脆弱性対応が適切に行えず侵害の要因を生んだり、調査範囲・対象の特定が難航し、余計なリソースを消費したりする可能性がある。
	インシデント対応態勢の整備状況	▪ インシデントを想定した態勢整備が不足していると、対応に抜け漏れや手戻りが発生し、インシデントの収束が長期化する可能性がある。
	報告・対外公表**【重要】**	▪ ランサムウェア被害は事業に与える影響が大きいため、ステークホルダーからの信頼回復や、組織としての説明責任を果たすためには、調査に基づく適切な情報開示が重要となる。 ▪ 取引先等が過度な頻度での報告や情報開示を要求する場合は、そのような対応に現場リソースが費やされ、調査作業や復旧作業が後ろ倒しになる可能性がある。（後述）

出典：筆者作成。

[2] IT 資産管理とは、自組織が保有する PC やサーバ、ネットワーク機器等の情報資産を誰が何処にどれ程所有していて、それらがどのように相互に接続されているのかを適切に把握することを指す。

システム運用面では、バックアップの適切な管理、特権アカウントの保護、ログの収集と調査が重要となる。組織・体制面では、情報資産の適切な管理、インシデント対応の事前準備、ステークホルダーに対する適切な対外公表が復旧期間を左右する。これらが適切に対処されていない場合、被害の拡大や調査の難航、対応の遅延を招き、結果としてシステム復旧やステークホルダーからの信頼回復に長期間を要することになる。続いて、以下では上記で整理した要因のうち、特に重要と思われる三つの要因をピックアップし、詳細を解説する。

（２）個別要因： バックアップからの復旧における課題

データやシステムがランサムウェアによって暗号化されたとしても、バックアップが適切に取得・保管されていれば、バックアップデータからシステム復旧を開始することが可能となる。一方で、バックアップデータが同一ネットワーク上等に保管されていた場合、表 1 記載の通り、バックアップデータ含め暗号化の被害に遭い、システム復旧に要する時間が長期化し得る。このため、バックアップはランサムウェア対策の筆頭として挙げられることが多い。しかしながら、**バックアップを取得していたからといって、必ずしも IT システムの復旧が短期化するわけではない**。実際に、冒頭で述べたように過去に発生したランサムウェアインシデントの事例においても、比較的直近のバックアップデータが被害を免れていたにも関わらず、復旧に数カ月を要したケースは複数確認することができる。なぜ、このような事態が生じるのだろうか。

ランサムウェアの特徴として、ネットワークに接続されている複数のシステムが同時多発的に破壊される点が挙げられる。データ連携を行っている各システムが個別にバックアップを取得していた場合、バックアップを取得したタイミングや、暗号化の被害を免れていたバックアップデータの世代が各システムで異なる場合、**システム間で復旧データの整合性を調整する必要が生じる**。仮に各システムがバラバラの時点で復旧してしまった場合、各システム間で保存されているデータ（在庫データ、売上データ、受注残データ等）が不整合を起こし、システムのエラーや二重計上等の問題が生じるためである。このような事態を避けるためには、データ連携を行っている各システムの利用可能なバックアップデータを確認し、全システムで利用可能な最も古い時点のバックアップデータを基準に各システムを復旧させる必要がある。復旧した時点のバックアップデータと現時点の状況との間にギャップが生じることになり、失われた期間のデータについては手作業でデータを復元する必要がある。また、暗号化を免れていたからといって、そのバックアップデータを直ちに利用できるとは限らない。バックアップデータが直近の場合、既にその時点のデータが攻撃者によって汚染されている可能性があるためである。したがって、**適切な調査によって侵害時期を特定し、どの時点のバックアップデータから真正性[3]や安全性が担保されるか等の検証も必要**となる。

このように、比較的直近のバックアップデータが暗号化の被害を免れていたとしても、システム間のデータ整合性の調整作業や、バックアップデータの安全性の検証作業が必要となる。このような調整・検証作業への対応によって、IT システムの復旧が長期化する可能性がある。

（３）個別要因： ログデータの収集と調査

バックアップデータの真正性・安全性を検証するためには、各システム、サーバ、PC、ネットワーク機器等に記録されているログデータを調査する必要がある。ログデータを調査することによって初めて、侵入された時期の特定や、侵入後に攻撃者がどのような行動を取ったのか、攻撃のタイムラインを明らかにし、侵入やその後の被害の拡大に至った原因や被害範囲の特定が可能となる。このような調査を行うためには、調査の材料となるログデータを平時から適切に取得・保管する必要がある。ログデータを適切に取得・保管していない場合や、攻撃者によってログデータが破壊・改ざんされ

[3] 真正性：情報、人、デバイス等が正当なものであることを保証する特性のこと。

てしまった場合は、適切な調査を行うことができない。その結果、**侵入時期や原因、被害範囲の特定が困難となり、「このような攻撃が行われたのではないか」というような仮定に基づく対応に終始する**こととなる。結果として、安全性の確証が得られずにバックアップデータの利用が制限されたり、侵入原因が特定できないために様々な可能性を考慮した対策が求められたり、被害範囲が特定できないためにシステムや端末の再構築を行う範囲が拡大するなど、**本来は不要な様々な対応が追加で発生する**可能性がある。

また、後述する報告・対外公表への対応においても、適切な調査を行うことが極めて重要となる。報告・対外公表の対応においては、単に情報を開示するだけでなく、取引先やステークホルダーからの IT システムの復旧に対する理解と合意を取得することが、システムの利用再開やサービス提供の再開において不可欠となる。取引先は、被害を受けた組織のシステムを再び利用することに対してセキュリティ面での懸念を抱くため、単純にシステムを元の状態に復旧させただけでは利用再開の承認を得ることは困難である。このような場合、**適切な調査に基づいた根本原因の特定と、納得感のある再発防止策の提示が求められる。**しかし、調査が不十分である場合、取引先等からの問い合わせや指摘事項に対して曖昧な回答に終始してしまい、追加の指摘事項や更なる対策の実施、追加調査を求められて対応に手戻りが生じる可能性がある。結果として、ステークホルダーからの信頼回復が遅れるだけでなく、IT システムの復旧・利用再開に対する承認が得られず、システムの本格的な復旧や事業の正常化が大幅に遅延することになる。このように、取引先等のステークホルダーへの適切な説明と合意取得は、IT システムの停止期間を決定する重要な要素であり、その前提として適切な調査とログデータの収集・保管が極めて重要となる。

（４）個別要因： 報告・対外公表への対応

ランサムウェア被害において、IT システムの停止期間を長期化する要因の三つ目として、取引先や公的機関等ステークホルダーに対する報告・対外公表の対応が挙げられる。ランサムウェアは、他のサイバーインシデントと比較して事業へ与える影響が大きい。システム停止が引き起こされることによって、事業の一時的な中断や、事業を継続できたとしても縮退運用を余儀なくされるため、インシデント発生の事実を対外的に公表することが必要となる。

先述の通り、適切な調査に基づく説明がステークホルダーからの信頼回復において重要となるが、一方で、そのような調査を行うにあたっての実務的な課題として、**取引先等への報告・対外公表への対応が現場リソースを逼迫させ、調査や復旧対応が後ろ倒しになる問題**が挙げられる。ランサムウェア被害のような重大インシデントが発生した場合、複数の取引先や公的機関等から、被害状況や復旧の見込み、対応の進捗状況等について報告を求められるケースが多い。これらの報告対応には、社内の状況整理、資料作成、説明準備、報告内容の社内承認等、相応の時間と人的リソースを要する。**報告先の組織によっては、日次や同日に複数回といった過剰ともいえる高頻度での報告を求められるケースも存在する。**このような場合、報告対応に現場リソースが費やされ、調査作業や復旧作業に十分な人員や時間を割くことができなくなる。結果として、現場のリソースが不足することで、調査作業や復旧作業の遅れにつながり得るため、報告・対外公表への対応におけるリソース消費の問題は、IT システムの停止期間を長期化させる重要な要因の一つとなり得る。

本パートでは、ランサムウェア被害において何が IT システムの停止期間を長期化させるのか、その要因について「システム運用に関する要因」と、「組織・体制に関する要因」に大別して概要を紹介し、続いて特に長期化に影響を及ぼすと考えられる三つの要因を提示した。冒頭で述べたように、実際の事例等を参照しても、これらの要因が複合的に発生することによって、IT システムの停止期間が長期化していることが多く、ランサムウェア被害から IT システムを短期間で復旧することの難易度の高さが窺える。したがって、各組織においては、ランサムウェアに対する未然対策だけでなく、IT システムが長期間停止することを想定した、事業継続計画の策定が求められる。

3．企業に求められる対応・対策

昨今、日本でランサムウェア攻撃による被害甚大化事案が確認される中、企業はこれを機会にサイバー攻撃対応態勢を確認・見直すことが期待される。少なくとも、①IT システム停止期間等のランサムウェア攻撃による被害想定の検証・見直し、②早期復旧に向けた初動対応プロセスの確立、③これらを含む全社レベルでの危機対応・事業継続態勢の高度化が必要である。

（1）被害想定の検証・見直し

ランサムウェア攻撃への対応計画・BCP の前提となる被害想定は表 2 の要素を含むことが望ましい。被害想定の構成要素は、①IT 部門や CSIRT 等によるインシデント対応やシステム復旧に直結するもの、②ユーザ部門（その他コーポレート部門や事業部門）による全社的危機対応・事業継続に直結するものに大別される。もちろん、実際の被害は想定と異なるものかもしれないが、これらは実際の攻撃発生時に把握すべき要素・推定すべき要素でもある。企業は、既存の被害想定の構成要素に不足がないのか、IT システムの停止期間が妥当かを検証することが望ましい。IT システムの停止期間については、企業規模や IT システムへの依存度・複雑性にもよるが、**もし、既存の危機対応計画・BCP の IT システムの停止期間が「日」単位、「週」単位であれば、それは見直した方が良い**可能性が高い。

■ 表 2：ランサムウェア攻撃の被害想定に必要な要素

分類	被害想定の構成要素
主に IT 部門や CSIRT 等によるインシデント対応やシステム復旧に直結	■ ランサムウェア攻撃の初期侵害経路と初期侵害時点（ランサムウェアの稼働時点を起点に何日・何週間・何カ月前に侵害されたのか） ■ ランサムウェア攻撃の検知・発見の手段 ■ ランサムウェア攻撃による影響の範囲と深さ ■ バックアップの有無、健全性、復旧可能時点 ■ ログの有無、完全性
	■ 情報漏洩の有無、脅迫の有無 ■ 攻撃者プロファイル
主にユーザ部門による全社的危機対応・事業継続に直結	■ 主要なアプリケーションやシステムごとの利用可否 ■ 主要なアプリケーションやシステムごとの利用停止期間

出典：筆者作成。

（2）早期復旧に向けた初動対応プロセスの確立

上記（1）の被害想定の見直しと並行して、難易度は高いものの、組織には可能な限り短期間での復旧に向けた対策が求められる。対応が多岐にわたるため、紙幅の都合上、早期復旧に求められる全容を詳細に解説することは困難だが、**復旧を早期化するために特に重要となるのは、①適切なログの収集・保全、②専門家の早期支援による調査対象の適切な選定**の 2 点と考える。なぜならば、IT システムをバックアップから復旧させるにしても、取引先やステークホルダーに報告・対外公表を行うにしても、再発防止策を検討するにしても、**前提として、適切な調査によって原因や被害範囲が特定されている必要があるから**である。したがって、上記の①と②を可能にするような事前の態勢を整備することが重要となる。①については、調査を行うための前提として、調査の材料となるログの収集の重要性について第 2 章で述べた通りであり、「どの機器のどのような種類のログをどれくらいの期間保持するのか」について、運用の負荷や保持にかかるコストと検証しながら、組織として意思決定する必要がある。また、調査を行うためには、ログの上書きを防止するために被害発生時の状況を適切に保全することも重要である。そのためには、被害を検知し

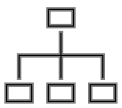
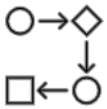
た際の初動対応プロセス（保全や関係部署への通報）を確立し、教育等を通じて社内へ周知することが不可欠である。②についてだが、調査対応にも相応の期間を要するため、初動の段階で調査対象を適切に選定することは、侵害時期や原因、被害範囲の早期特定に寄与し、また追加調査等の手戻りの防止にもつながる。**調査対象を適切に選定するためには、経験及び知見が豊富なインシデントハンドラー等の専門家にインシデントの初動から支援を要請することが重要**となる。インシデント対応態勢といえば、組織内の役割分担や連絡体制の整備に焦点が当たることが多いが、早期復旧を可能にするためには、インシデント対応プロセスに外部機関を含む専門家の早期支援を組み込むことが不可欠である。

（３）全社レベルでの危機対応・事業継続態勢の確立

企業は上記（２）の初動対応プロセスの確立に加え、全社レベルでの危機対応・事業継続態勢を構築・高度化する必要がある。現在ではほとんど確認されないが、かつては、サイバーセキュリティの専門性・特殊性が強調され、全社レベルでのサイバー攻撃対応＝インシデント対応、対応責任者＝CISO と考える企業や経営者も少なくなかった。しかし、大規模地震や不祥事・法令違反への対応と同様に、サイバー攻撃対応を最高経営責任者が指揮しないことはあり得ないし、特定のコーポレート部門だけで完結することもない。

今日では、多くの企業が全社レベルでのサイバー攻撃対応態勢を確立している、もしくは直近の大規模ランサムウェア攻撃事案を踏まえて点検中であろう。表 3 は、現在の危機対応・事業継続態勢を簡易的に検証するためのチェックリストである。

■ 表 3：全社レベルでの危機対応・事業継続態勢の検証のための簡易チェックリスト

分類	チェック項目
体制 	□ サイバー攻撃に関する**全社的危機対応組織と構成部門**は明確か？（危機対応には IT 部門・SOC・CSIRT だけではなく、全社的な危機対応・事業継続を担う経営企画、広報、法務、人事、総務、事業部門等の関与が必要） □ サイバー攻撃の**影響度や重大性を初期的・暫定的に評価する指標・基準**はあるか？ あるいは、全社危機管理態勢で定義される「重大性」「切迫度」「緊急度」等はサイバー攻撃にも適用可能か？ 等
プロセス 	□ サイバー攻撃を検知・発見した**直後の初動対応プロセス**が決まっているか？ 想定される検知・発見の経路、検知・発見後の連絡先・手段、被害拡大の防止策、初動対応組織は決まっているか？ □ サイバー攻撃による**被害拡大を防止するための措置**（メールを含む外部接続遮断、セグメントの隔離・分離、特定システムやアプリケーションの停止等）が定められているか？ 措置の一覧、各措置の判断権限者、判断基準、判断・実行手順等が決められているか？ □ IT システムが利用できない場合、**オフラインで優先事業・重要業務を継続**するための手段が確立されているか？ 等
ツール 	□ メールやチャット等の社内ネットワーク経由・認証コミュニケーション手段が利用できなかった場合の**コミュニケーション・連絡ツール**が準備されているか？ □ サイバー攻撃発生に**連携・報告すべき外部連携先**は洗い出されているか？ 規制当局、国家サイバー統括室（NCO）、最寄り警察署、個人情報保護委員会、業界団体・業界 ISAC、JPCERT/CC、IPA、SIer、セキュリティベンダ、損害保険会社、弁護士、証券取引所等のコンタクトリストは整備されているか？ 等

出典：筆者作成。

著者略歴

三宅 諒介　　サイバーセキュリティ事業部 主任研究員

2021 年、東京海上日動リスクコンサルティング（現：東京海上ディーアール）入社。以降、サイバーリスクアセスメント、CSIRT 構築支援、セキュリティ管理規程策定支援、インシデント対応フロー策定支援、経営層・一般従業員向けセキュリティ教育、各種セミナー登壇等に多数従事。2024 年より米国 NPO 法人 ISC2 の認定インストラクターとして、CC 資格認定トレーニングを提供。
CISSP, CC, CISA, 情報処理安全確保支援士（第 024921 号）
本稿の２．および３．（２）を執筆。

川口 貴久　　ビジネスリスク本部 兼 経営企画部 主席研究員、マネージャー

2010 年、東京海上日動リスクコンサルティング（現：東京海上ディーアール）入社。以降、リスクマネジメント態勢の構築・高度化支援、地政学リスクやサイバーリスク対応支援に多数従事。この他、一橋大学法学研究科非常勤講師（2022 年 4 月～現在、ただし上期に限る）、サイバーセキュリティ法制学会理事（2025 年 5 月～現在）、国家サイバー統括室「サイバーセキュリティ推進専門家会議」構成員（2025 年 9 月～現在）等。
本稿の１．（１）～（２）、３．（１）、（３）を執筆。

太田 瑛美　　ビジネスリスク本部 副主任

2021 年、東京海上日動リスクコンサルティング（現：東京海上ディーアール）入社。以降、地政学リスクの動向調査、大規模サイバー攻撃事態に関する調査、サイバーセキュリティに関する経営層向けハンドブックの企画・作成、「サイバー安全保障と能動的サイバー防御」に関する調査研究プロジェクトの運営等に従事。
本稿の１．（３）を執筆。

コンサルティングおよびソリューションの紹介

東京海上ディーアールは、企業のサイバー攻撃対応態勢の構築・確立のため、以下の多様なソリューション（抜粋）を提供しています。ご関心があれば、https://www.tokio-dr.jp/contact/service/ までお問合せ下さい（お問い合わせ時は「リスクマネジメント最前線をご覧になった」旨をご記載ください）。

- セキュリティ管理規程策定支援
- CSIRT 構築支援
- サイバー攻撃を想定した全社危機対応計画・事業継続計画の策定支援
- 既存の危機対応計画・事業継続計画（被害想定を含む）の第三者評価・改善提案
- 経営層・一般従業員向けセキュリティ研修
- サイバー攻撃対応演習の企画・運営支援
  - 経営層向け意思決定演習
  - 全社対策本部向け演習
  - CSIRT 向け演習

[2026 年 3 月 5 日発行]

東京海上ディーアール株式会社

〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594　Fax. 03-5288-6626 https://www.tokio-dr.jp/