CYBER RISK JOURNAL

サイバーリスクジャーナル

TOKIO MARINE NICHIDO

サイバーインシデント対応の実情

1 サイバーインシデント対応からみた攻撃手法とその対策

2 サイバー攻撃発生時に直面する課題と求められる判断

3 インシデント発生時の情報公開

2025年10月発行

東京海上日動

次の一歩の力になる。

CONTENTS

サイバーインシデント対応の実情

はじめに 2

01 サイバーインシデント対応からみた攻撃手法とその対策 3

一般社団法人 ソフトウェア協会　フェロー　**板東 直樹** 氏

02 サイバー攻撃発生時に直面する課題と求められる判断 11

株式会社 関通　代表取締役社長　**達城 久裕** 氏

03 インシデント発生時の情報公開 17

株式会社 日本経済新聞社　**須藤 龍也** 氏

はじめに

セキュリティ啓発の現場で必ず耳にするのは、「弊社の規模では狙われない」、「地方には関係がない」といった意見である。株式会社帝国データバンクが公表した「サイバー攻撃に関する実態調査（2025年）」によれば、過去にサイバー攻撃を受けたことが「ある」と回答した企業の割合は、32.0%にのぼる。規模別では、「大企業」が41.9%で最も多く、「中小企業」が30.3%、うち「小規模企業」が28.1%であった。企業規模が大きいほどアタックサーフェス（攻撃対象となりうるポイント）が増加し、狙われやすいことは事実であるが、実際には大企業だけでなく中小企業も攻撃の対象となっていることが明らかである。また、上記調査はアンケート形式であるため、「サイバー攻撃を受けていることに気づいていない」企業が一定数存在している可能性も忘れてはならない。

通信規格のIPv4で利用されるIPアドレス（識別子）は、0と1を並べた2進数の32桁で表現される。そのため企業規模にかかわらず、外部向けに公開している機器やサービスがある以上は、都市部であっても離島であっても、攻撃者から見れば文字列のわずかな違いでしかない。一般に、インターネットへ公開されている機器は、検索エンジン等によるクロール（巡回）の対象となり、スキャンが常に行われている。外部からの偵察行為は日常的に行われており、いつでも攻撃されうる、という認識を持つことが必要である。

企業においてセキュリティへの意識が高まったきっかけを尋ねると、「実際にインシデントに直面したため」という声が多く挙げられる。しかし、攻撃を受けてから対策を講じるのでは遅い。自組織が攻撃された場合にどのような事態に陥るか、またどのような備え・対処が必要かを普段から想定いただくことが重要である。本誌では「インシデント対応の実情」をテーマに、平時から行うべき備え、サイバー攻撃発生時に直面する状況、そして被害に遭った際の情報公開について解説をいただいた。本誌が組織における対策を検討する一助となれば幸いである。

01 サイバーインシデント対応からみた攻撃手法とその対策

一般社団法人 ソフトウェア協会
フェロー
板東 直樹氏

板東 直樹 ばんどう・なおき
1983年ジャストシステム入社、1994年マイクロソフト入社、チャネルマーケティング部長、広報部長を経てシステム製品統括部長として、Windows及びサーバー製品全体のマーケティングを指揮。2000年にプライベートエクイティファンドからアップデートテクノロジー株式会社に参画。現代表取締役社長、BC Signpost株式会社取締役。経済産業省産業・内閣官房国家サイバー統括室合同ワーキンググループ委員。厚生労働省インシデント初動対応チームメンバー。一般社団法人ソフトウェア協会フェロー、Software ISAC共同代表。

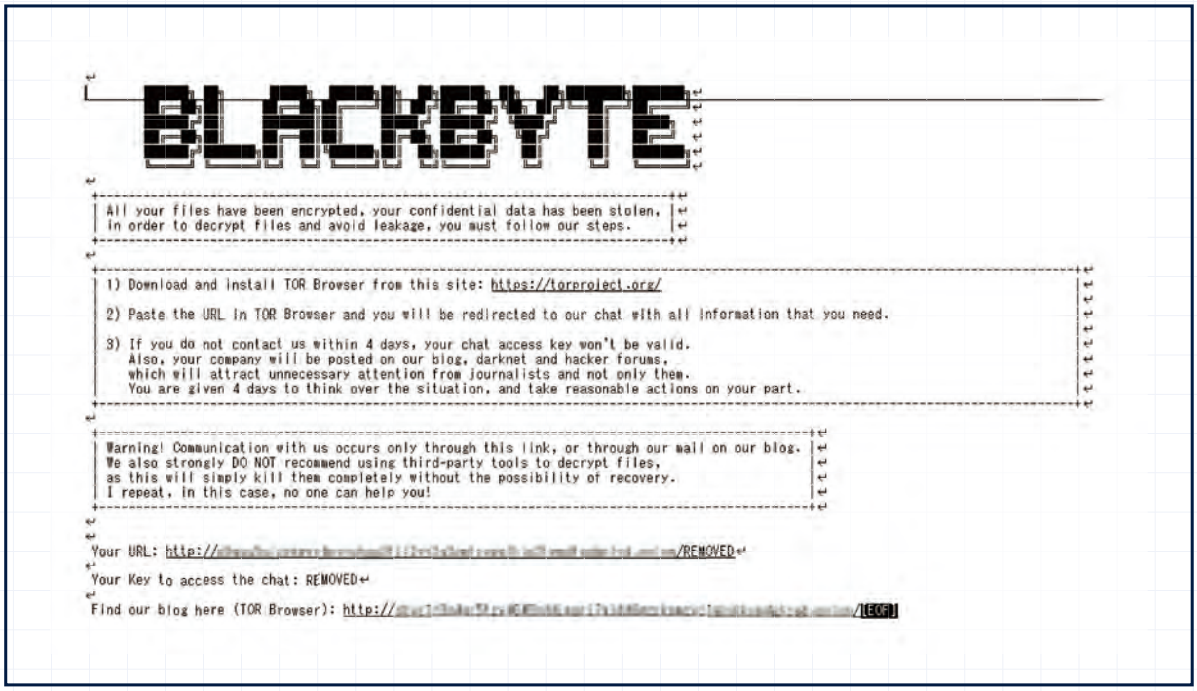
本稿では、私が関わった町工場やNPO法人、病院などでのランサムウェア事案をベースに、前半でランサムウェアのビジネスモデルを解説し、後半では、攻撃に悪用された脆弱性や設定を紹介するとともに、何故、そのような脆弱性が放置されたかを分析し、最後にコストをかけないランサムウェア対策を紹介していく。

1. ランサムウェアとは

既にご存じの方も多いと思うが、ランサムウェア（Ransomware）は文字通り、身代金＝RansomとSoftwareの合成である。システムを暗号化して脅迫状を表示する機能を有しており、「身代金ウイルス」とも呼ばれている。実際には、ランサムウェアが稼働する前段として、攻撃者が「手動」で組織のネットワークに侵入し、バックアップを破壊して復旧を困難にし、その後、ランサムウェアでシステムを暗号化して組織の機能を麻痺させる。この際、個人情報や契約書を窃取した上で、暗号化されたデータと個人情報を人質に身代金を要求するという悪質なサイバー攻撃である。

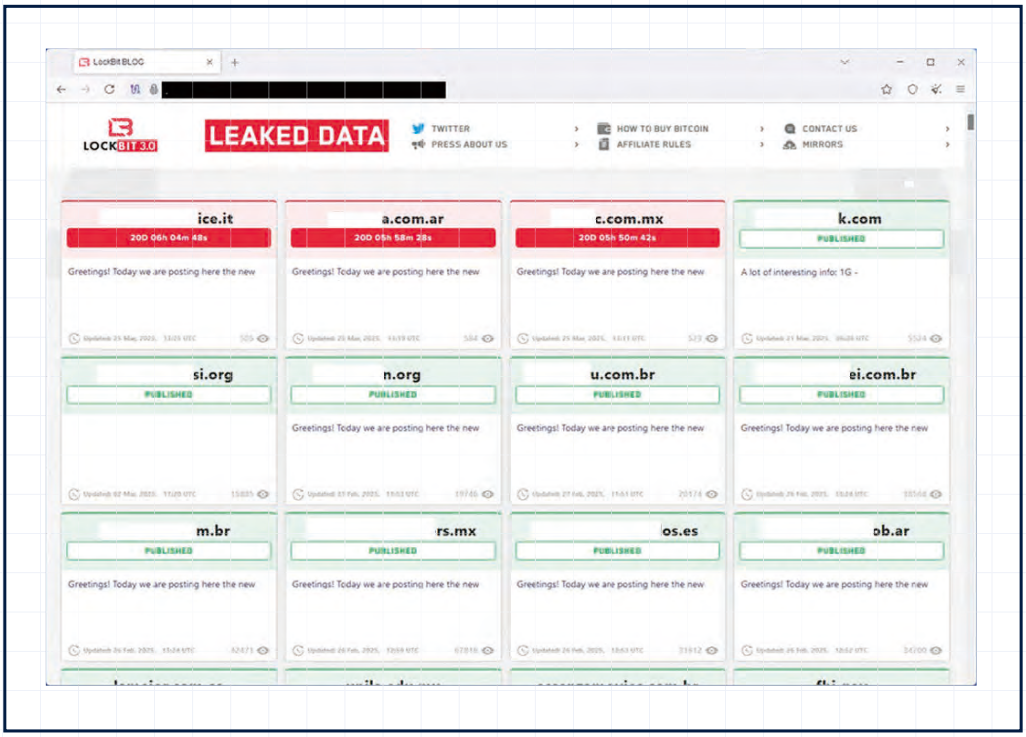
以下は、BLACKBYTEというランサムウェア集団の脅迫状で、「すべてのファイルが暗号化され、機密データが盗まれました。ファイルを復号化して漏洩を防ぐには、次の手順に従う必要があります。」とあり、TORブラウザー[*1]からダークウェブ上のチャットへアクセスし、連絡するように求めている。

＊1 ダークウェブにアクセスするための専用Webブラウザー。これを使用すると匿名性を確保しながらダークウェブが閲覧できる。但し、使用にあたっては、個人情報の漏洩や攻撃、ウイルス感染等のリスクを十分に検討の上、リスクを受容し使用する必要がある。



「4日以内にご連絡いただけない場合、チャットアクセスキーは無効になります。また、お客様の会社情報は当社のブログ、ダークネット、ハッカーフォーラムに掲載され、ジャーナリストだけでなく、第三者からも不必要な注目を集めることになります。状況をよく検討し、適切な措置を講じるために4日間の猶予が与えられます。」と脅迫を行っている。

下の図は、2025年3月時点でのランサムウェア集団Lockbit3.0のリークサイトである。交渉期間中の組織は赤色で公表までの残り時間が表示され、交渉決裂もしくはコンタクトしなかった組織は、緑色で「PUBLISHED」という表示になり、情報公開されてしまう。



実際にサイトをクリックすると、窃取された書類や運転免許証など、実際のデータが公開されている。リークサイトを調査しているRansomwatch[*2]によれば、このようなリークサイトは2025年6月現在で、492サイトあるとしている。

2. 組織体制

攻撃犯たちは大雑把に言えば3つの役割で構成されている。

- ✓ **オペレーター**：ランサムウェアの開発や身代金の交渉支援、リークサイトの運営を実施
- ✓ **アフィリエイト（実行犯）**：ネットワーク侵入やバックアップの破壊、システムの暗号化を実施
- ✓ **イニシャル・アクセス・ブローカー（IAB）**：さまざまな組織のVPN装置の管理者ID/パスワードや、システムの内部情報を販売

オペレーターとアフィリエイトの取り分は3:7とも4:6ともいわれているが、直接的なリスクを冒すアフィリエイトの取り分が多いようである。開発と実際の攻撃を分業することで、効率よく攻撃を展開することが可能となっている。IABはオペレーターやアフィリエイトに侵入先の情報を販売するが、VPN装置のID/パスワードなどは数十ドルから5,000ドルともいわれており、VPN装置の所有組織の売上や利益、従業員数といった脅迫先としての魅力も含めて販売されているという。また、ネットワーク内の管理者の情報や、セキュリティ装置の回避方法など、アフィリエイトにとって侵入後のリスクを低減する付加価値の高い情報などは数万ドルで販売されるともいう。このように、彼らは、リスクに応じた分業化を進めており、離合集散を重ねて日々攻撃を行っている。

実際に2021年に米国東海岸のパイプラインを運営していたコロニアル・パイプライン社が古いVPN装置から侵入され、パイプラインの制御系を含めた広範な攻撃を受け、燃料不足によるガソリンパニックや航空機の航行に多大な影響を出した。この際、同社は緊急避難として暗号化解除のための鍵を入手するために身代金を支払ったが、その額は440万ドル、邦貨にして6億円もの支払いを仮想通貨で行っている。また、全米1万5,000店の自動車販売店が使用するシステムを提供しているCDK Global社は、2024年に約2,500万ドルの身代金を支払ったという報道[*3]がある。攻撃犯にすれば一発当てれば、とてつもない金額の身代金が獲得できる訳で、オペレーター（元締め）、アフィリエイト（実行犯）、IAB（情報屋）という、まるでギャング映画の世界が実際にサイバー空間で繰り広げられているのである。

3. 実際の攻撃先と手口

一方で、前述のような大型案件ばかりを狙う組織だけではない。中小・中堅企業では、大企業に比べてセキュリティ対策が甘く、専任の担当者も設置されておらず侵入に気が付かない場合が多い。アフィリエイトにすれば、低リスクで、個人情報や対外的に機密とされる情報を数多く窃取した方が身代金獲得の

＊2　https://ransomwatch.telemetry.ltd/#/
＊3　CNN: How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom、https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars

チャンスが広がる訳であり、その意味で、中小・中堅企業は良いターゲットである。ただし、全部が身代金を支払うとは限らないので、多くは数を打てば当たるというモデルを実践していると考えられる。

つまり、多くのランサムギャングたちは、インターネットを通じて侵入の容易な組織にアクセスし、PCにログインした上で盗める情報を盗み、暗号化し、バックアップを破壊し、そして脅迫しているにすぎない。また、使用されているテクニックは、政府機関や研究所、高度な知財を有する半導体企業や航空宇宙企業などへの高度標的型攻撃とはまったく別な低次元のものである。暗号化のためのランサムウェアを除いて、侵入で使用しているツールやテクニックに特別なものはない。雑誌や広告で「巧妙化、高度化するサイバー攻撃」といったタイトルを目にするが、実際のランサムウェア被害現場の大半は脆弱なシステムが攻撃されているに過ぎない。

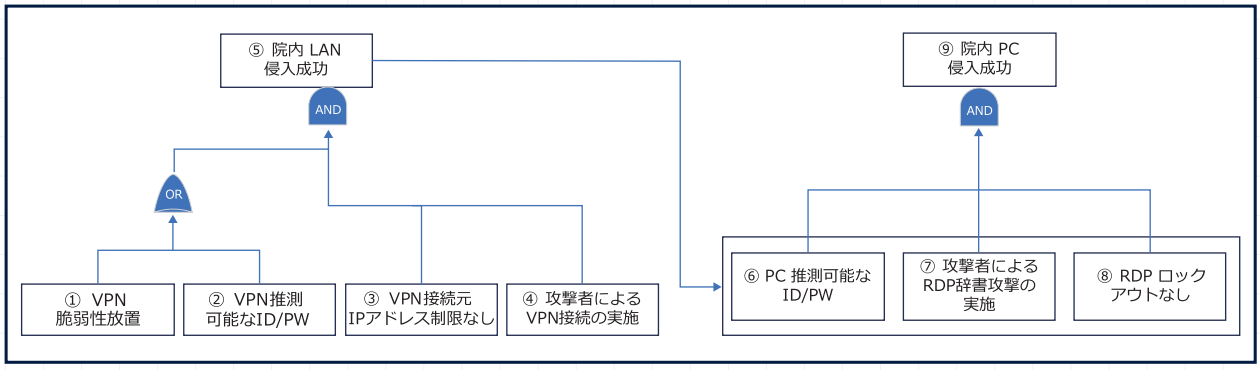
4. 岡山県精神科医療センターの事例

2024年5月19日、岡山県精神科医療センターはランサムウェア攻撃を受けた。被害は、電子カルテシステム等の仮想サーバー 23台と仮想用共有ストレージ 1台、仮想基盤用物理サーバー 3台、その他の物理サーバー 6台、医療情報系端末244台の暗号化によるシステム稼働障害と仮想用共有ストレージのデータ全喪失である。また、攻撃犯Xによる情報窃取が岡山県警により確認され、氏名、住所、生年月日、病名等を含む推定で最大40,000人分の個人情報の漏洩を招き、すべての患者への本人通知を余儀なくされた。復旧に要した時間は約3ヵ月、病院の試算では約65人月の工数がかかっている。

5. Fault Tree によるランサムウェアの分析

図1は岡山県精神科医療センターでランサムウェア攻撃犯がVPN経由で院内LANに侵入し、院内のPCに侵入するまでを簡易的に分析したFault Tree図である。図の左下から見ていきたい。

図 1　VPN 初期侵入〜院内 PC 侵入



① VPN 脆弱性放置

VPN装置や通信機器は、通信に特化しているコンピューターであり、WindowsやLinuxと変わらず脆弱性を有している。本件では、この脆弱性が放置されていた。この脆弱性は正規のIDとパスワードを使用しなくてもVPNに接続できた可能性があった。VPN装置は設定によるが、外部から機種やバージョンを確認でき、そこから脆弱性が判明してしまう場合がある。

② VPN 推測可能な ID/PW

VPNへの接続IDはAdministrator、パスワードはP@ssw0rdが設定されていた。Administratorとは Windows共通の管理者IDであり、パスワードもよく知られている推測可能なものだった。

攻撃犯は脆弱性を悪用したか、推測可能なパスワー

ドで接続を試みたと考えられており、以上2つはORゲートに接続されている。

③ VPN接続元IPアドレス制限なし

一般的に在宅勤務用のVPNでなく、保守目的のVPNであれば接続可能なIPアドレスを設定し、それ以外のIPアドレスの接続をブロックするが、この事案ではそのような設定がなされていなかった。

④ 攻撃者によるVPN接続の実施

こうした条件のもと、攻撃犯はVPN接続を実施した。

この中で着目したいのは、①もしくは②のいずれかと、③④はすべてAND条件であることだ。ANDであればどれか一つでも欠ければ⑤院内LAN侵入は成功しない。つまり、「③VPN接続元IPアドレス制限なし」を対策していれば、岡山県精神科医療センターのランサムウェア攻撃は起きていなかったのである。

次に、院内LANに接続した攻撃犯はPCへの侵入を試みる。

⑥ PC推測可能なID/PW、

⑦ 攻撃者によるRDP辞書攻撃の実施

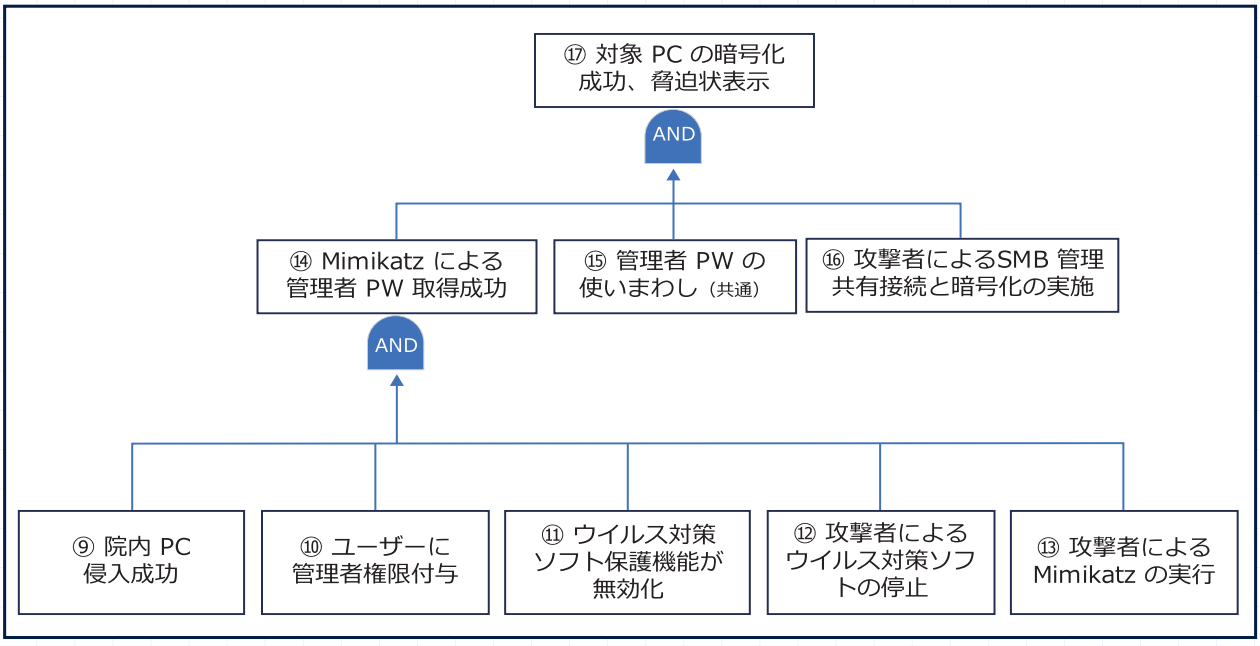
一般的に攻撃犯はVPN接続に成功すると、院内のPCにRDP接続を試みる。RDPは接続先のPCの画面を手元のPCに転送し、手元PCのキーボードやマウス操作を接続先PCに転送してくれるため、遠隔地のPC操作に大変便利な機能である。RDP接続時にはID/パスワードの入力が必要となるため、攻撃犯は様々なパスワードを推測した上で辞書を作成し、プログラムからRDP接続を次々と試みる。推測したパスワード辞書と、実際に使用されているパスワードが合致すれば、侵入が成功する。残念ながら、PCの管理者に設定されていたID/パスワードは、VPNと同じAdministrator、P@ssw0rdであったため、容易に突破されたと考えられる。

⑧ RDPロックアウトなし

Windowsにはこのような辞書攻撃を回避するため、ロックアウトという機能が用意されている。10回連続してパスワードを間違えたら15分間ログオンを禁止するというものであるが、このロックアウト設定はなされていなかった。このため、無限にログオンを試行できてしまった。

ここでも、⑥から⑧はANDゲートである。従って、推測困難なパスワードが設定されていれば侵入は確実に防げたし、RDPロックアウトを行っていれば攻撃の遅延ができ、もしかすると攻撃犯は諦めて撤退したかもしれない。次に、「⑨院内PC侵入成功」したアフィリエイトは何をしたのか。以下の図2をご覧いただきたい。

図2　院内PC侵入～攻撃完了



⑩ ユーザーに管理者権限を付与

病院は電子カルテベンダーの要請に基づき、すべてのユーザーに管理者権限を与えていた。管理者権限があれば、Windowsのすべての設定変更が自由になる。

⑪ ウイルス対策ソフト保護機能が無効化

最近のウイルス対策ソフトは、ランサムウェア攻撃に備えて、管理者権限を有していても無効化設定ができないようになっている。しかし、病院のウイルス対策ソフトには、そのような設定がなされていなかった。

⑫ 攻撃者によるウイルス対策ソフトの停止

アフィリエイトは、管理者権限が与えられていることを確認の上、ウイルス対策ソフトを停止した。これにより、パスワード解析ツールや様々な攻撃ツールを自由自在に扱えるようになった。

⑬ 攻撃者によるMimikatzの実行

MimikatzとはWindowsの内部に保存されているIDとパスワード情報を解析する攻撃ツールである。大半のアフィリエイトは好んでMimikatzを使い、Windowsに保存されているすべてのID/パスワードを入手する。ID/パスワードが多数手に入れば、攻撃の範囲が広がり身代金の獲得がしやすくなる。

⑭ Mimikatzによる管理者PW取得成功

すでにPCに侵入した際にID：Administrator、PW:P@ssw0rdは取得していたが、改めてWindowsに保存されている管理者パスワードを確認したと考えられている。また、他の管理者ID/パスワードを入手できれば、水平展開で有利になる。

⑮ 管理者PWの使いまわし（共通）

院内のPCの管理者パスワードはすべて共通だった。管理上、このような設定が横行している場合が多いが、これが原因ですべてに水平展開が可能となってしまった。

⑯ 攻撃者によるSMB管理共有接続と暗号化の実施

SMB管理共有とは、Windowsの基本機能であり、様々なセキュリティ設定を配布したりする際に使用する機能である。接続先のコンピューターの管理者のID/パスワードがあれば、このSMB共有を使い、コンピュータ内のファイルを自由に操作可能である。アフィリエイトはこの管理共有接続を実施した上で、暗号化を実施した。

この2段のステップも、すべてがANDゲートである。「⑩ ユーザーに管理者権限を付与」でなく、標準ユーザーでの運用であれば、「⑬ 攻撃者によるMimikatzの実行」は防げたし、「⑮ 管理者PWの使いまわし（共通）」がなければ、水平展開は困難であり、数台程度の被害で済んだかもしれない。

6. 他施設での事例

国内でランサムウェアの被害にあった病院で私が直接対処、もしくはヒヤリングした事案でも、ほぼ、同様の原因でランサムウェア攻撃の被害にあっている。

施設名	侵入経路	侵入を許した原因
徳島県つるぎ町立半田病院	保守用VPN装置	脆弱性の放置、接続元IPアドレス制限の欠如、ユーザーへの管理者権限付与
大阪急性期・総合医療センター	保守用VPN装置	
C病院	保守用VPN装置	
D病院	保守用VPN装置	
鹿児島県国分生協病院	保守用ルーター	認証及び接続元IPアドレス制限の欠如、ユーザーへの管理者権限付与

民間企業は報告書の公表やニュースリリースを行わないため、具体的な掲出を控えるが、数多くの事案での原因は全く共通であり、これは病院特有のものではないことに留意頂きたい。すべては、「脆弱性の放置」、「接続元IPアドレス制限の欠如」、「ユーザーへの管理者権限付与」という脆弱性の連鎖が原因である。

7. 正常性バイアスの存在

被害に遭ったあらゆる組織のユーザーは「何故、うちがランサムウェアにやられたのか、こんな小さな組織を狙っても仕方ないのに」と口を揃えて言う。もし、読者諸賢が攻撃に遭遇したとしても、同じ思いをするのではないだろうか。しかし、ここに大きな落とし穴があると私は考えている。恐縮だが被害者の多くは、すべてのサイバー攻撃は政府や防衛、研究所などを狙うもので自分たちは関係ない、関係ないから安全だという都合の良い思い込みをしている。ここに正常性バイアスが存在している。しかし、この数年でサイバー攻撃の対象に中小企業も含まれるようになったことは、紛れもない事実である。自分らも攻撃の対象となる時代なのだという認識を持ち、正常性バイアスを捨て去らないと、攻撃に直面するリスクは高いままとなる。インターネット越しに攻撃を仕掛けるアフィリエイトにしてみれば、脆弱性が放置されたVPN装置は格好の餌食であり、放っておく理由がない。弱いシステムは攻撃の対象なのである。

また、病院のシステムを構築した医療情報システムベンダーも口を揃えて「病院は閉域網だから大丈夫だと思っていた。」と言う。確かにインターネットに接続していない「完全な閉域網」なら脆弱性管理はしなくても大丈夫だろう。しかし、その考え方をインターネットに接しているVPN装置に適用してはならない。

そこは閉域網ではなく、悪意溢れる世界なのである。国内病院のランサムウェア事案は、すべて医療情報システムベンダーの正常性バイアスがもたらした「人災」と、私は考えている。

オペレーター、アフィリエイト、IABのエコシステムは今後さらに発展し活発化するだろう。自社も攻撃されるかもしれない、という思いが、備えの第一歩となる事をご理解いただきたい。

8. コストをかけないランサムウェア対策

最後に運用の変更とWindowsの標準機能を活用し効果的なランサムウェア対策を紹介する。

- **パスフレーズの使用**

  キーボードに打刻されている文字、記号等は94種ある。従って1桁のパスワードは94の組み合わせ、2桁では94×94＝8,836の組み合わせが考えられる。つまり、組み合わせ数は94のべき乗となる。1桁増やせば94倍、組み合わせ数が増える。ところが、長く複雑なパスワードは記憶が不可能だ。そこで、3つくらいの単語を組み合わせるパスフレーズが推奨されている。

  母誕生日三月→hahatannjoubisangatsu　21桁
  鎌倉梅雨紫陽花→kamakuratsuyuajisai　19桁

  16桁を超えるようなパスフレーズに辞書攻撃は成立しない。1秒間に1億回試行しても天文学的な時間がかかる。なお、パスワード全般に複雑さや定期変更を求めるのは非推奨となっていることに留意頂きたい。

- **漏洩したパスワードのチェック**

  クラウドサービスが攻撃を受けると、アカウントのIDとパスワードが漏洩する。そしてダークウェブに公開されたり、売買されて悪用される。こうした漏洩パスワードを収集し、チェックできるサイトhttps://haveibeenpwned.com/がある。このサイトは、FBIなどと協力しており、信頼できるサイトである。どんなに長く複雑なパスワードも漏洩すればひとたまりもない。ぜひ、チェックしてほしい。なお、当該サイトは暗号化して通信しているので入力したパスワードが漏洩することはない。

- **脆弱性管理の実施**

  いうまでもなく、Windows Updateを実施するとともに、VPN、Firewall、ルーター等の通信機器についても脆弱性情報を入手し、アップデートを実施頂きたい。各装置の管理者パスワードは当然、16桁以上のパスフレーズに変更すれば辞書攻撃は成立しづらくなるが、できれば2要素認証が望ましい。

- **標準ユーザーでの運用**

  Fault Tree分析でも明らかなように、管理者権限は危険極まりない。今日から標準ユーザーを作成し、通常の業務はすべて標準ユーザーで実施すべきである。どうしても管理者権限が必要なアプリ

ケーションがあるならば、2要素認証の導入を検討してほしい。

- **ウイルス対策ソフトの改ざん防止（標準ユーザーとの組み合わせ）**

  Windows 11の検索で「改ざん防止」と入力すると「ウイルスと脅威の防止の設定」というDefenderウイルス対策の設定画面を選択できる。そこで、「改ざん防止」をオンにするだけで、標準ユーザーはDefenderウイルス対策のサービスを停止することができなくなる。この状態を保つことでMimikatzなどのパスワード解析ツールは駆除可能となる。他のウイルス対策ソフトにも同様の機能があるので、今、すぐにでも設定を実施いただきたい。

- **電子メールの添付ファイル**

  もう一つの攻撃ベクトルとして電子メールの添付ファイルがある。特に、悪意あるOfficeマクロを開こうとすると、「セキュリティの警告、マクロが無効にされました。このファイルにはウイルスやその他のセキュリティ上の脅威が含まれている可能性があります。」と既定で表示されるはずだ。このような警告メッセージが出た場合等は、それ以上絶対に開かないよう社内教育を徹底したい。

高額なEDRやセキュリティ製品の導入を行っても、これらの設定が杜撰であれば効果が半減する可能性がある。実際にEDRをバイパスする手法が多数報告[*4]されている。紙面の都合上、紹介できないが、これ以外にも、LSA保護、Local Administrator Password Solution、Windows Hello for Business、Credential Guardなど、Windows搭載のセキュリティ機能を有効にすることで、ランサムウェアの攻撃を局所化することができる。以上の機能について詳しいベンダーがいれば、それはセキュリティに詳しい信頼できるベンダーといえるだろう。ぜひ、そのようなベンダーと実効性のあるセキュリティ対策を実施していただきたい。

＊4　TA Phone Home：EDR Evasion Testing Reveals Extortion Actor's Toolkit：https://unit42.paloaltonetworks.com/edr-bypass-extortion-attempt-thwarted/
Ransomhubランサムウェアが EDRKillShifterを使ってEDRとウイルス対策を無効化する方法：
https://www.trendmicro.com/en_us/research/24/i/how-ransomhub-ransomware-uses-edrkillshifter-to-disable-edr-and-.html
ランサムウェア集団がEDRバイパスツールをますます巧みに利用している：
https://www.cybersecuritydive.com/news/ransomware-gangs-vulnerable-drivers-edr-killers-increasing/743709/

02 サイバー攻撃発生時に直面する課題と求められる判断

株式会社 関通
代表取締役社長
達城 久裕氏

達城 久裕 たつしろ・ひさひろ
22歳で軽トラック一台から創業し、関通をEC物流のパイオニア企業へと育てた達城久裕。どんな局面でも現場と人を大切にし、変化に柔軟に対応してきた。2024年、前代未聞のランサムウェア被害を受けるも、陣頭に立ち復旧を指揮。その経験をもとに「サイバーガバナンスラボ」を設立。自身の実体験を共有し、備えを支えるための実践型コミュニティを立ち上げた。

人生には「上り坂」「下り坂」があると言われるが、予期せぬ事態に見舞われた時、「魔坂」という坂と「真っ逆さま」という坂があることを思い知らされることがある。まさに「まさかこんなこと起きないだろう」と思える事象が簡単に起こってしまう恐怖を体験したのが、サイバー攻撃の瞬間であった。

多くの企業が「サイバー攻撃？まさか、自分には関係ない」と考えているのではないだろうか。かつての私もそうであったし、あなたも同じように考えているかもしれない。しかし、「うちの会社は大丈夫」「狙われるのは大企業だけ」「ウイルス対策ソフトも入れているから問題ない」といった油断が、企業を破滅に追い込む可能性がある。ランサムウェアの攻撃者は、決してターゲットを選ばない。

この記事は、単なる体験談ではなく、経営者・リーダーとして、会社を守るために「何を準備し、どう対応すべきか」を具体的に示すものである。もし明日、あなたの会社がサイバー攻撃に遭ったら、社員を守り、業務を再開するためにどのような手順を踏めば良いのか。そもそも、事前にどのような対策をしておくべきなのか。記事を読み終える頃には、サイバー攻撃に対する経営者としての判断力を身につけ、具体的な対策を真剣に検討したくなるはずだ。企業の未来は、リーダーであるあなたの決断にかかっている。

1. 突如襲いかかるサイバー攻撃とその瞬間

株式会社関通は、1983年に創業した総合物流企業である。2025年4月、代表取締役社長である私は、生涯忘れることのない、リアルな一日を経験した。それは「通信が不通です。ネットワークが落ちています！」という一報から始まった。そして9月12日、サーバーの中身のすべてを暗号化されてしまったのである。その後に何が起きるのか知る由もなく、「不安」と「暗闇」が関係者全員の心模様であった。分かっていたのは、会社が40年間で経験したことのない大きなダメージを受けることは間違いないだろうということだけだった。

翌朝7時、役員が集まり緊急ミーティングが開かれた。状況の共有と、対策の決定が急務であった。まず、**緊急対策室の立ち上げ**が決定された。次に、全社的な指示が即座に出された。通信が途絶え、社内システムは完全に停止し、インターネットにも接

続できない状況に陥った。

この状況下で、何よりも大切だったのは「一人一人が冷静に動く」ことであった。私は社員たちに「混乱しても何も解決しない。やるべきことを一つずつ進めるしかない」と伝え、明確な指示を出した。同時に、セキュリティ専門家、サイバー攻撃対策専門企業、リスクマネジメント企業、損害保険会社といった外部の専門家が集まり、対応にあたった。

2. 初動対応に求められる判断

サイバー攻撃が発覚した瞬間、社内の誰もが頭を抱えた。情報が不足している状態で、最も適切な判断を下さなければならない。しかし、明確な正解はない。それでも、動かなければならなかった。会社の存続、取引先の信頼、社員の安全。そのすべてが、この初動対応の正しさに懸かっていた。

最初の大きな判断の分かれ目となったのは、**関係各所への報告**であった。何を、誰に、どのタイミングで伝えるのか。まず、法律上の義務として報告が必要な機関がいくつか存在する。警察（サイバー犯罪対策課へ届け出）、国土交通省（物流機能停止の場合など）などが該当する。まずは事実関係を整理し、相談という形で一次報告を行い、その後に総合的な判断を基に被害届の提出の是非を決定すべきである。私見ではあるが、早急な被害届の提出は必要ないと考えている。その影響を鑑みた上で、届け出を決定するのが良いだろう。

これらに加えて、社内外への報告が必要であった。お客様（サービス停止の影響を受ける取引先）や、第三者機関（個人情報保護委員会など）への報告も求められる場合がある。

最も悩ましかったのは、**お客様への報告**のタイミングであった。誤った情報を流せば信用を失う。しかし連絡が遅れれば、「何かを隠しているのでは?」という疑念を持たれてしまいかねない。私たちは、報告に関して次の原則を決定した。

- **現時点の事実のみを説明する。**
- **一社一社に丁寧に報告する。**

状況を端的にまとめた文書を作成し、スピードと正確性のバランスを取りながら報告を進めていくことが求められる。

社内への報告対応も重要である。情報が錯綜する中で不確定な情報を流せば、社内はパニックに陥り、取引先の信頼を失いかねない。**「まず事実だけを、分かりやすく伝える」**という方針を鉄則として、情報の整理と伝達を始めるべきだ。社員には「とにかく落ち着いて行動してほしい」と伝えた。

また、この段階で**正確な情報収集**が不可欠であった。

- サイバー攻撃の侵入口はどこか?
- 被害範囲はどこまで広がっているか?
- 外部に情報が漏洩しているのか?
- システム復旧の見込みはどれくらいか?

これらの正確な情報がなければ、社外向けの報告どころか、社内への指示すら出すことはできない。事実と憶測を分けることは、最も重要である。

3. 復旧過程で直面する多様な課題

サイバー攻撃後の復旧過程では、想像を超える多様な課題に直面した。

技術的な復旧の課題は最も喫緊であった。被害拡大を防ぐためには、旧ネットワークは完全に遮断し、新しいネットワークのみを利用することが必須であった。私たちが下した判断は、「新しい環境を構築する以上、完全に切り替えなければならない。時間がかかっても、根本から入れ替える」というものであった。これは従業員にとって大きな負担を伴う決断であったが、再感染のリスクを考慮した結果であった。

新しいネットワークの設計においては、「完全な安全性の確保」が最重要テーマとされた。攻撃の侵入経路が特定できていない以上、ゼロからネットワークを設計するのが最も安全な方法であり、その方針が決定された。

また、**システム開発部門では自社開発のクラウド型倉庫管理システム：クラウドトーマスの早期復旧**を目指す体制を組んだ。しかし、長年築き上げた自動化システムを捨てるという**「苦渋の選択」**を迫られる局面もあった。サイバー攻撃から2週間以上が経過しても正常な業務に戻れず、このままではさらなる難題に直面するという状況で、自動化システムを捨てる決断を下した。それは大きな痛みを伴う決断だったが、未来の関通を救う唯一の道なのだと全員が理解していた。これからは紙と手作業での受注処理を標準とし、最も安全な形で新たな自動化の仕組みを再構築することになった。システムに頼らない新しい業務フローを構築しよう、という方針が打ち出された。

事業継続に関する課題も山積した。システムが完全に停止したため、出荷作業はアナログに頼らざるを得なかった。アナログによる出荷と棚卸作業のみで対応を続けた。採算を度外視した人員配置も行うことを決定した。しかし、紙の伝票、手書きのリスト、電話での確認といった人手による業務は想像以上に過酷であった。

請求業務も大きな課題の一つであった。システムが攻撃を受け、請求データがすべて失われたため、経理部はゼロから請求業務を組み立て直さなければならなかった。経理部員は「請求データがない…」という絶望的な状況で業務を進めた。過去の請求データを総動員し、倉庫現場と連携して出荷記録を1件ずつ手作業で確認しながら、お客様が納得してくれる請求書を作るという決意で取り組んだ。最終的に、影響を受けた取引先の請求については、状況を精査し、個別対応とする方針を決定した。請求業務を止めないことで関通の財務基盤を守ると同時に、取引先の信頼も維持することが重要だった。

顧客・取引先対応は、信頼維持のために最も重要な課題であった。お客様からは「いつから出荷できるのか？」という問い合わせが殺到した。復旧に際して、「どのお客様から、どのように復旧させていくのか？」という優先順位と手順を明確にするためのミーティングが行われた。すべてのお客様を一度に復旧させるのは不可能であり、お客様ごとに異なる業務フローやデータ管理方法、対応可能な代替手段を整理し、一つずつ復旧へと導くことが求められた。お客様ごとに最優先事項を整理し、各部門がスムーズに動けるように調整を行った。データが完全に復旧できるお客様もいれば、一部の機能を使えないまま運用せざるを得ないお客様もいた。一社一社と対話することで、要望を聞き、できる限りの対応をする方針を貫いた。営業担当者は、それぞれのお客様と話し合い、「何ができるのか」「どこまでなら対応できるのか」を丁寧に詰めていった。例えば、注文リストをCSVデータで送信してもらい、手作業で処理するといった方法を提案した。

ステークホルダー対応も複雑であった。国土交通省への報告内容を最終確認し、被害状況、物流機能の復旧状況、今後の見通し、対応方針を重視して取りまとめた。報告文書を作成し、正式に提出した。関通の信頼を守るためにも、事実を隠すことなく、しかし不要な混乱を生む形でない形で報告することが重要だった。

損害保険会社との交渉は難航した。契約上、今回のランサムウェア攻撃に対する補償は可能である一方、取引先からの逸失利益に関する損害賠償請求は補償対象外となる可能性があると示唆された。これは「それでは意味がありません」と即座に反論する事態となり、弁護士もサポートに入った。関通のビジネスはBtoBであり、取引先の損害がそのまま関通の損害であると主張した。条件の適切な証明がされない限り認定は難しいと言われ、証明のために弁護士、サーバー事業者、セキュリティ専門家など関係者にお願いするしかなかった。関通の未来は、この損害保険の適用にかかっていた。

個人情報漏洩の可能性についても慎重に調査を進めた。取引先の個人情報が格納されていたサーバーが攻撃を受けた可能性があり、実際のデータ流出は確認されていないが、一定のリスクがあるとの結論に達した。個人情報保護委員会への追加報告を行い、取引先への説明会実施、継続的なモニタリングと情報提供の体制強化を今後の対応計画とした。この問題については、個人情報保護委員会や法律事務所と事前協議を重ねた。何もかも公開すれば良いというものではないが、お客様や取引先に不安を抱かせたままでは関通の信頼は崩れてしまう。細心の注意を払いながら、「今の時点で伝えられる事実」と「調査中の事項」を明確に区別し、慎重に対応を進めるしかなかった 。個人情報漏洩に関する問い合わせも増加した。

労働環境と社員ケアも深刻な問題であった。シス

テムが正常に動かない中で、社員たちはアナログ対応を強いられ、物流現場の最前線には想像を絶する負担がのしかかっていた。疲労の蓄積、不満の声、精神的なプレッシャー。「このままでは、本当に人が倒れてしまう」という危機感があった。会社が生き残るためには、まず社員を守らなければならない。緊急時の単なる福利厚生ではなく、「この会社は、社員を本気で守ろうとしている」というメッセージを伝えたかった。

具体的には、7連勤が続く社員がいる状況に対し、労働時間の管理について議論し、これ以上の長時間労働を禁止する判断を下した。7連勤を超えた場合は必ず1日休暇を取ること、1日の労働時間は最大10時間までとすること、必要に応じて派遣スタッフを増員すること、タクシー代とホテル代は会社が負担し社員の負担を軽減すること、といった決定事項をまとめた。また、現場社員の疲労だけでなく栄養状態も心配し、昼食補助制度を導入した。すぐに食べられる弁当の支給、社員食堂の無料化、コンビニの買い出し費用補助などを実施した。さらに、休憩時間の柔軟な運用も認めた。役員に対しては、「サイバー攻撃対応金」を特別支給する決定を下し、経営トップが持つべき責任を果たしながら負担にも報いる姿勢を示した。「誰かの負担が、極端に増えないようにしなければならない」と考え、管理職の業務負担が過剰な場合には人員サポートを手配した。サイバー攻撃対策金として、社員の急な出費（通信費、通勤費、立て替え費用など）に対応するための即時支給も行った。これらの施策が、社員の士気低下を防ぎ、復旧スピードを維持する大きな要因になった。

経済的な損失と資金準備も避けて通れない課題であった。物流業務が停止したことによる直接的な売上損失に加え、取引先の離脱、追加のシステム復旧費用、損害賠償の可能性など、考えられるすべてのマイナス要素に耐えうる資金の準備が必要となった。今回のサイバー攻撃を乗り越えるために、関通では20億円の対策資金を準備した。会社存続のために一番必要なのは、現金であった。

4. 危機に求められるリーダーの判断

危機に直面した時、リーダーに最も求められるのは**決断力**である。決断力は、平時には測れない。非常時にこそ問われる。関通が未曽有の危機を乗り越えられたのは、経営陣だけではなく、現場で必死に働き対応に追われていた社員たちがいたからこそだが、その社員たちの進むべき方向性を示し、動きを統制するのはリーダーの役割である。リーダーが迷い、判断がブレると、組織はたちまち混乱して士気は低下する。

経営者には「指揮官」としての役割が求められる。会社全体の状況を見渡し、どの部署がどのような役割を果たすべきかを瞬時に決めることが求められる。通常業務の延長ではなく戦時の非常事態として物事を捉え、社員の意識を変えながら統率し、緊急対応の体制を整えるべきだ。

また、「盾」としての役割も重要である。サイバー攻撃の被害に対する批判やクレームの矢面に立つのは、経営者の責務である。取引先やお客様、メディアからの問い合わせに対して全責任を背負う姿勢を見せることで、社員が萎縮せずに業務に専念できる環境を作ることができる。私は報道機関からの取材依頼に対し、「申し訳ないが、取材はお断りする」と即座に返答し、インシデント対応中は取材を断るという方針を社内メンバーに再通達した。

意思決定のスピードも企業の生命線である。一分一秒を争う状況で、どこまでスピードを上げられるかが命題であった。まず状況把握と初動対応を最優先とし、システム完全封鎖、緊急対策本部の設置、警察・セキュリティ会社との連携、取引先への迅速な報告といった初動の決定を即座に行った。

しかし、情報がすべて揃うのを待っていては何も進まない。不完全な情報の中でも、最善の決断を下す覚悟を持たなければならない。リスクを恐れて決断を遅らせれば、被害は拡大し、会社は取り返しのつかない状態に陥る。リーダーにはその覚悟が求められる。

5. 信頼回復への長く険しい道

サイバー攻撃によって、関通は一時的に多くの取引先からの信頼を失った。物流が滞り、請求業務も混乱し、「関通はもうダメかもしれない」とささやかれることもあった。システム停止により、お客様の事業にも大きな影響を与えてしまい、「もう任せられない」と判断する企業が出るのも当然であった。

しかし、これをただ受け入れるわけにはいかなかった。**「このままでは終われない」「関通は決して逃げない」**と心に決め、信頼回復のための行動を続けた。

信頼回復において最も重要だったのは、**情報開示の徹底**であった。事態の進捗、復旧状況、セキュリティ強化策などを定期的に公開し、透明性を確保することを最優先とした。取引先やお客様にとって最も不安なのは、「状況が分からないこと」だからだ。定期的なレポート発信（公式サイトやプレスリリースで週単位の復旧進捗報告）、オンライン説明会の開催などを実施し、お客様が抱える疑問や懸念を直接解消し、迅速に対応することで誠意を示した。不十分な情報開示や曖昧な説明は、疑念を生む要因になりかねない。正直に、すべてを開示するという決断が、結果的に信頼を守る上で極めて重要であった。

また、**経営陣による直接の顧客対応**も極めて重要なポイントであった。経営トップが責任を持って説明することで、会社としての誠意を示すことができる。現場任せにせず、社長や役員自らが主要顧客と直接向き合うことの重要性を痛感した。

信頼は、一朝一夕には築けない。失った信頼は、一瞬では戻らない。何か特別な策を講じればすぐに取り戻せるものではなく、**日々の積み重ねが、信頼を回復する唯一の方法**である。厳しい言葉を浴びせられることもあったが、逃げずに、誠実に向き合い続けた。その結果、すぐに信頼を取り戻せなくても、「関通は少なからず、誠実に対応しようとしている」「関通は、私たちのお客様を軽視していない」と感じてもらうことができた。**「関通はどんな困難があっても、誠実に向き合い続ける企業だ」**と思ってもらえるようになったことが、何よりの成果であった。

6. 危機から得た教訓と未来への示唆

今回のサイバー攻撃は、従来の自然災害や取引先倒産、物流トラブルといった「目に見える危機」とは全く異なる性質を持っていた。それは**「見えない敵」**であり、いつどこから攻撃を受けるか予測が難しく、被害の全容把握にも時間がかかる。情報の混乱が起きやすく、不確実性の高い状況での判断が求められる。

この経験から得られた教訓は、サイバー攻撃は「経営課題」であるということだ。セキュリティはIT部門だけの問題ではなく、経営レベルで取り組むべき課題である。サイバー攻撃の影響はシステム障害にとどまらず、経済的損失、ブランド毀損、取引先との関係悪化など、企業経営全体に及ぶ。セキュリティ対策を経営計画の一環とし、役員レベルで定期的なセキュリティレビューを実施し、危機管理マニュアルを整備し実際の対応フローをシミュレーションするといった取り組みは、今後の企業経営に必須となる。

また、どれだけ対策を講じても「完全防御」は不可能だが、「被害軽減」は可能である。多層防御の徹底（ゼロトラストモデルの採用）、インシデント対応訓練の実施、迅速な被害状況の可視化、適切なサイバー保険の導入といった手段は確実に存在する。どれほどセキュリティ対策を強化しても100%の防御は不可能である以上、被害が発生した場合に備えてサイバー保険に加入することは必須である。保険の適用範囲をしっかり確認し、損害賠償や復旧費用がどこまでカバーされるのかを理解しておくことが重要だ。経済的損失を保険で補えるという事実こそが、企業が事業継続に取り組む上での大きな支えとなる。

サイバー攻撃への対応は、テクノロジーだけでは解決できない。むしろ、IT人材のスキルと判断力が復旧スピードを左右する。社員向けのセキュリティ教育を徹底し、有事の際の指揮系統を明確にすること。インシデント対応マニュアルを作成し訓練を繰り返すことが重要だ。

サイバー攻撃は、いつ、どの企業にも起こりうる。大切なのは「自社は大丈夫」という過信を捨て、「攻

撃を受けた際にどのように対応するか」を真剣に考え続けることだ。そして、その準備こそが、企業の存続を左右する最大の要素となる。**「防げるか?」ではなく、「どう乗り越えるか?」**。それこそが今、サイバー攻撃のリスクに直面する企業に求められている視点なのかもしれない。

危機に直面した時、組織の本当の強さが試される。関通は、システムがすべて使えなくなった状況でも、社員一人一人が「今、自分にできることは何か?」を考え、行動に移した。指示を待つのではなく、主体的に動く。この姿勢こそ、関通の最大の強みであった。普段の業務が順調に回っている時には見えづらいが、危機に直面した時、会社を支えているのは「人」なのだと痛感した。

関通は、この危機を単なる「危機に直面した経験」ではなく、「企業を進化させる転機」と捉え、得られた学びを継承していく。**「責任逃れ」をせず、徹底的に対応する。「学ぶ姿勢」を持ち、企業をアップデートし続ける。**そして、「被災企業」として自社の経験を広く共有し、物流業界や他の企業のサイバー攻撃対策に貢献していくことが、我々の使命であると考えている。サイバー攻撃対策コミュニティ「サイバーガバナンスラボ」の立ち上げもその一環である。

サイバー攻撃という試練は、関通に大きな傷を残したが、同時に、関通をより強く、より誠実な企業へと成長させる機会にもなった。一つ一つの誠実な行動が積み重なった時、再び信頼を築くことができる。サイバー攻撃の被害を通して、信頼の重みについて身をもって学んだ。

この記事の内容が少しでも読者の参考になれば、それは関通にとって今回の経験を未来へ活かすための一つの「形」となると思う。企業に対するサイバー攻撃の事例は今後も増加していくことが予想される。**著書「サイバー攻撃 その瞬間 社長の決定」**には私の経験した危機の具体的なエピソードや思考の軌跡、そして数々の対策実例が記されている。このリアルな経験から得られた知見が、企業のサイバーセキュリティ・ガバナンス強化の一助となることを願っている。事件はまだ終わっていない。これは、物流ビジネスのさらなる変革への始まりなのだ。

03 インシデント発生時の情報公開

株式会社 日本経済新聞社
須藤 龍也氏

須藤 龍也 すどう・たつや
主にサイバーセキュリティー分野を担当する編集委員として、2024年10月に日本経済新聞社に入社。前職は朝日新聞社で、国内外のサイバー攻撃事案やハッカーの動向を10年以上にわたり追い続けた。LINEの情報が中国や韓国からアクセスできる状態にあった問題をスクープし、2021年度の日本新聞協会賞を受賞。このほか三菱電機へのサイバー攻撃（2020年）、神奈川県庁のHDD流出・転売事件（2019年）などを特報した。エンジニア採用が振り出しという変わり種。著書に「チャイナスタンダード」（共著）など

1. はじめに

サイバーインシデントが発生した時、当事者が真っ先に思い浮かぶのは、「情報公開をどうするか」ではないだろうか。取引先への説明や対外的な公表について何を説明すべきか、どのタイミングで公表すべきか、悩みはつきない。

筆者はサイバーセキュリティ分野の専門記者を10年以上担当し、数多くのインシデントを取材してきた。ここで得られた知見を記事に書くだけではなく、企業経営者やセキュリティ実務担当者らを対象にした講演などでも情報発信をしている。

これまでの取材で得られた知見を先に申し上げれば、「事実と真正面から向き合い、誠実な内容を公表する組織ほど、結果として評価が高くなる」ということである。それは「情報公開とは何か」という本質の一端を示していると考えている。

本稿では、過去の取材で得られた事実をいくつか例示しながら、サイバーインシデント発生時の情報公開について考えていきたい。

2.「即断」を求められる経営層

情報公開について述べる前に、前提となるサイバーインシデント発生時の状況について簡単に触れておきたい。現在、多くの企業や組織が警戒しているのが、ランサムウエア（身代金要求型ウイルス）の脅威ではないかと考える。

ランサムウエアが発動すると、パソコンやサーバーのデータが破壊（正確には暗号化）され、多くの事業が停止に追い込まれる。パソコンの画面を見ると「盗まれたデータを公開する」といった脅迫文とともに、サイバー犯罪集団と交渉するよう要求が記されているのが一般的である。

経営者はその時、複数の難しい判断を同時並行で行わなければならない状況になる。

・犯罪集団と交渉するかどうか
・事業継続の目処と被害調査の実施
・取引先への説明
・対外的な公表の有無

いずれも即断に近い、迅速な判断が求められる。

ちなみにトップが最後までブレない判断と姿勢を貫く組織ほど、たとえ途中で不利な状況に置かれても持ち直し、復旧が早いという共通点を取材で感じている。

サイバー攻撃を受けた組織が置かれる状況は、「災害」に似ている。前触れもなく被災し、事業継続が危ぶまれる状況に一気に突き落とされる。災害と異なるのは、犯罪集団が仕掛ける「サイバーテロ」であり、組織から一歩外に出れば、普段と変わらない平穏な日常が流れていることである。

3.「被害者」が「加害者」になる

昨今はサイバー攻撃の脅威が知れ渡るようになり、取引先や顧客も状況を理解し冷静に対応するケースが増えている。一方で情報公開をめぐる対応のまずさによって、トラブルに発展するケースも少なくない。

ある受託企業が2024年、ランサムウエアの被害にあった。この企業は自治体や企業など顧客から個人情報を預かり、処理をする企業である。

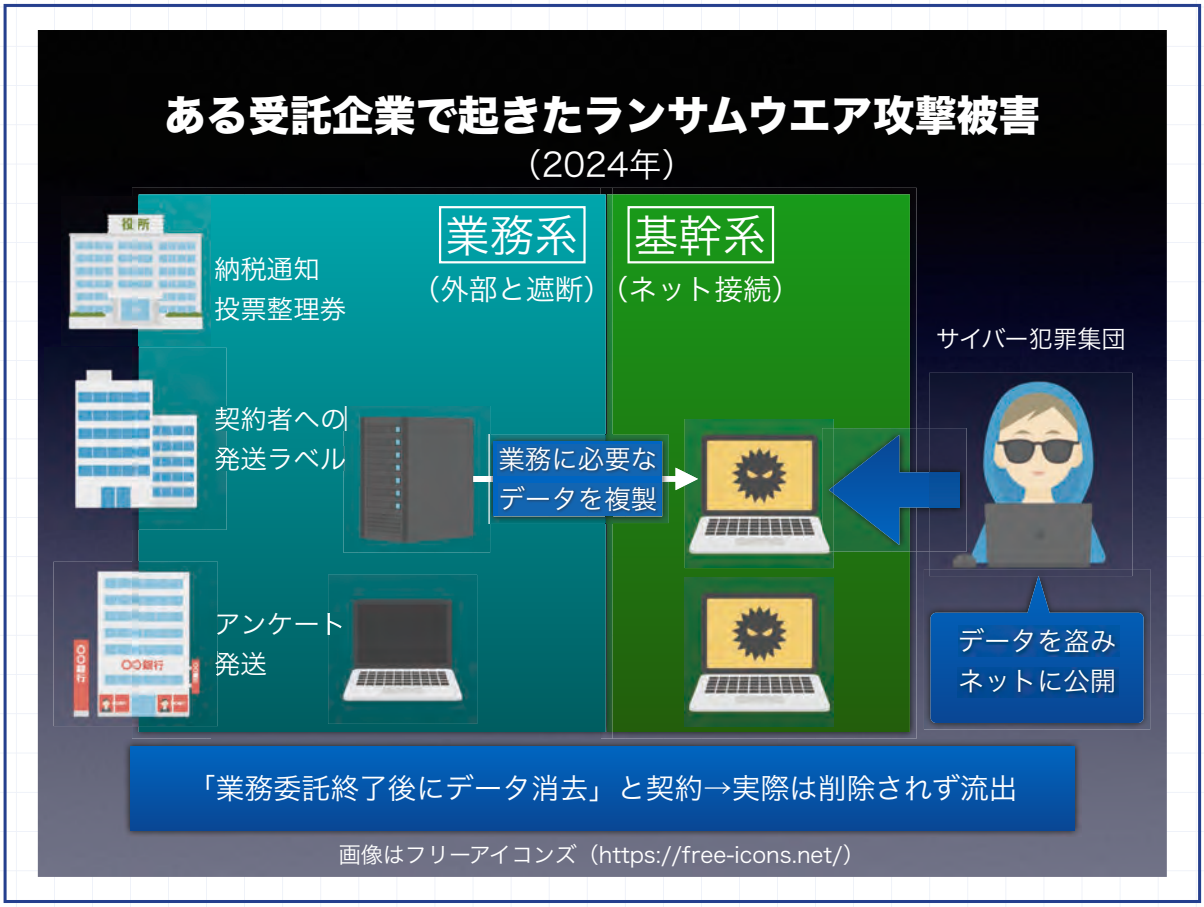
複数の顧客が発表した内容を総合すると、この企業は預かった個人情報などを「業務系」と呼ばれるネットワーク上で管理していた。外部のインターネットと切り離された環境下に置かれていたという。

ところがサイバー犯罪集団が、公式サイト上に企業から盗み取った情報を暴露したことで、情報流出が発覚してしまった。

ネットと切り離された環境下に置かれていた顧客の個人情報がなぜ犯罪集団の手に渡ったのか。それは、ネットに接続されていた「基幹系」ネットワークにも情報の一部が保管されていたからである。

基幹系ネットワークは、この企業の一般業務で使うパソコンなどが接続されていた。本来ならば顧客から預かった情報を取り扱うべきではない場所だが、業務系ネットワークから情報がコピーされていた。何らかの事情があり、個別に対応したデータの中に含まれていたとみられる。

図表　「被害者」が「加害者」になる



実は上記の詳しい状況について、この企業は対外的に公表をしていない。顧客である自治体や企業の発表によって明らかになったことばかりである。

経緯を詳細に公表した自治体に取材したところ、この企業との業務委託が終了後、提供した個人情報を速やかに削除する旨の契約となっており、削除したとの報告も受けていたという。ところが実際は契約に反し、削除されず残った情報が流出してしまった。

「(この企業の)説明が納得いくものではないため、住民への説明責任もあり詳細を明らかにした」と当時、自治体の担当者は筆者に説明した。言葉の端々から相当の憤りが感じられた。

このほか取材に応じた顧客企業によると、「ネットから遮断した業務系ネットワークに(預かった個人情報を)保管しており、情報流出はない」と当初、この企業から説明を受けたという。ところが後日、流出していたとの報告を受けた。この一件で企業との取引関係を解除したという。

サイバー攻撃を受けた組織は外部から預かった情報の流出リスクを常にはらみ、加害性を持ち得る。以前はサイバー攻撃に対する社会的な理解が乏しく、単に情報流出を引き起こした組織として批判にさらされていた時代があった。今は意図せぬ攻撃に見舞われた被害者としての側面がまずは知られるようになり、批判が抑えられている。

ところが、顧客に対して不誠実な対応を取ったり約束を反故にしたりすれば、一気に加害者としての立場が強くなる。そうなれば補償など問題が複雑化し、事案解決が遠のいてしまう。

4.「加害性」がみなされる組織に共通すること

これまでの取材から、このような組織には、ある共通点があると考えている。それは、ランサムウエア攻撃を受けた状況を経営層がそもそも理解できていないということである。

筆者は企業経営者を対象にした講演などで、「状況」「現実」「対応」という3つのフェーズに分けてランサムウエア被害について説明している。パソコンに犯行声明のようなメッセージが表示されている「状況」に見舞われた時、すでに起きている「現実」を直視してもらうためである。

・内部情報は盗まれたものと認識する
・被害を矮小化せず最悪の想定で臨む
・隠してもムダ、犯罪集団は公表済み

実はこの状況をわかっていない経営者がいまだに多い。

繰り返しになるが、ランサムウエアが発動したということは、すでに組織の内部が侵害されていることを意味する。侵入したサイバー犯罪集団はあらかじめ、ときには数カ月かけて組織の内部情報を根こそぎ盗み取る。

その上で、盗んだ情報と犯行声明を公表し、組織が抱える顧客やステークホルダーなど、世間に広く知らしめる行動に出る。外部からの圧力を高め、組織を窮地に追い込んでいく。

サイバー犯罪集団は、つぶさに社会の実像を研究している。週末や連休期間中、深夜にあえてランサムウエアを発動させるのも、手遅れを誘発するためである。被害組織にプレッシャーをかける有力な手段として、情報公開を選んでいる。

ランサムウエア攻撃を受けてコンピューターが停止したことは、単なるシステム障害ではない。企業の存続が危ぶまれる危機管理案件である。多額の損害と信用の失墜を覚悟しなければならない。

それだけに、速やかな事業継続と信用回復がカギとなる。そこで最後のフェーズとなる「対応」で、筆者は特に二つの重要性を訴えている。

・透明性の高い対応が後に評価される
・教訓を込めた公表で世論が味方する

いずれも、過去のインシデント取材で得られた知見をもとにしている。そのきっかけとなった一例を取り上げたい。

5. 情報公開が人をつなぎ、病院を救った

ランサムウエアが世界的に猛威を振い始めたのは、2020年のことだ。リモートワークの増加で、これま

で組織内で閉じられた「閉域網」のネットワークに外部から接続する必要に迫られた。その結節点となるVPN（仮想私設通信網）機器の脆弱性（欠陥）を突くサイバー攻撃手法が見つかってしまい、悪用した犯罪集団が次々と組織の内部に侵入、大きな被害が相次いだ。

日本でも同じ時期、特に病院の被害が大きくクローズアップされた。徳島県つるぎ町立半田病院の事例がきっかけとされる。四国山地の中山間地にある、ベッド数120床の小さな病院だが、地域で唯一お産を受け入れる、数少ない救急病院である。そんな病院がランサムウエア攻撃により約2カ月にわたり停止したことで、地域の医療に甚大な影響が出た。

実は2021年10月31日の発生当初、被害が広く知られることはなかった。この日は衆議院選挙の投開票日で、メディアは選挙報道一色であった。半田病院は徳島市中心部から車で1時間30分ほどかかる場所にあり、この日夕方、病院で開いた緊急記者会見に出席できたのは地元の徳島新聞の記者だけという悪条件も重なった。

地方が抱える問題も状況の悪化に拍車をかけた。人材難と情報不足である。病院は頼れるセキュリティ会社のつてがなく、200台あるパソコンのウイルスチェックなどを自前で行うなど、手探りの復旧作業をしばらくの間、強いられていた。

筆者が最初に現地を取材したのは、発生から半月後のことである。地元テレビ局が報じたローカルニュースのネット記事をたまたま見つけたことがきっかけであった。病院内の対策本部に招き入れられ、そこで見たのは、3人の職員がパソコンにウイルス対策ソフトを1台ずつインストールしている姿であった。

ベンダー経由で紹介されたデータ復旧会社のフォレンジック調査が不完全で、無害化されたはずのパソコンからウイルスが再び見つかり、パソコンのチェックを全てやり直すなど現場が混乱していた。

取材に訪れた時も、1台のパソコンからランサムウエアウイルスが検出された。それを駆除する男性職員は、病院でたった一人のシステム担当者であった。責任を痛感し、退職届を忍ばせながら復旧作業に従事していたと知ったのは、だいぶ後のことである。

「全て公開しますのでなんでも取材してください。社会にこの現実を伝えてください。こんな悲劇が繰り返されないよう、窮状を知ってほしい」。開口一番、取材に対応してくれた病院事務長が放った言葉が今も忘れられない。

サイバー攻撃に直面した医師や看護師らへの取材をもとに、当時在籍していた朝日新聞で1面、社会面を使った大型のルポルタージュ記事を掲載した。発生から1カ月後のことである。

掲載から数日後、この記事を読んだある人物から筆者に連絡があった。「病院を支援したい。担当者とつないでほしい」。IT企業の業界団体、一般社団法人ソフトウェア協会の理事（当時）が、セキュリティ企業の仲間数人とともに手弁当で病院に駆けつけた。そこで初めて病院はセキュリティ専門家とつながることができた。

6.「公開する」ということ

発生から約8カ月後の2022年6月、専門家たちの手によってまとめられた半田病院の調査報告書が公開された。3分冊からなる報告書は、被害に関する詳細な調査結果と、情報システム機器をランサムウエアから守るための基礎知識や設定例の「技術編」、組織におけるセキュリティ対策事例や管理手法をまとめた「ガイドライン」に分かれる。

インシデント報告書としては考えられない充実した内容である。半田病院の公式サイトに掲載されている報告書ページの前書きには、「全国の病院や事業所のセキュリティ強化に貢献できればと考え公開した」という病院事業管理者の思いが記されている。

筆者の取材にも管理者の医師はこう答えている。「サイバー攻撃がどういうものかなんて、正直知りませんでした。私たちの認識不足も含め、他の病院が攻撃を受けないためにも、詳細な状況を公表することが責任だと思いました」

サイバー攻撃を受けた組織が対外的に公表する動機の一つに、個人情報保護法に基づく報告義務がある。必要最小限の記述にとどめる公表をする企業とやり取りをすると、法令上の義務が出発点となっているとしか思えない対応が返ってくる。私見だが、「セキュリティの観点から…」という理由で説明をしたがらない組織と共通した意識を感じる。

対して半田病院の報告書や取材対応からは、公表内容を教訓にしてほしいとの思いが込められている。それは受け手にも伝わり、被害を最小限に抑えられた事例が実際にある。

半田病院が報告書を公表した2週間後にランサムウエア攻撃を受けた徳島県鳴門市の病院は、数日で復旧することができた。徳島県医師会での講演で半田病院の医師からバックアップの重要性を聞かされ、電子カルテのバックアップを刷新していたことが幸いした。

被害発生から4年近くが経過した今も、半田病院には全国から講演依頼が舞い込む。海外からも注目され、シンガポールの放送局CNAが2022年11月、半田病院の特集番組を放映している（When A Japanese Hospital's IT System Was Held For Ransom、https://www.youtube.com/watch?v=XaVkzX7NjmA）。

報告書を見れば一目瞭然だが、攻撃を受けた時の半田病院のネットワークは脆弱そのものであった。そうした実態も含めて全てを公開し、二度と繰り返してほしくないという関係者の思いが重なった結果、社会から広く共感が得られ、世論が味方する結果となったと筆者は考える。

公表とは単に、説明責任を果たす手段だけにとどまらない。被害組織の信頼を回復し、社会貢献につながるチャンスの場でもある。

7. 組織の性格がわかる「記者会見」

社会に大きな影響を与えるインシデントに発展した場合、被害組織が記者会見を開くことがある。組織が自発的に開催する場合もあれば、メディア側の要請を受けて開く場合もある。いずれにせよ、主催は被害組織である。

会見を開く基準のようなものはない。例えば経営トップが説明しなければ社会が納得しないといった状況判断も考え方の一つになる。多くのメディアを集め、同じ情報を一度に伝えることができる会見の性質を捉えれば、緊急性のある内容を社会に広く伝えたい場合に用いる手段であるとも言える。

一方でトップの発言や一挙手一投足に注目が集まるため、会見は組織にとって諸刃の剣とも言える。

筆者がここ最近で最も印象に残った記者会見を取り上げたい。2020年10月1日、東京証券取引所でシステム障害が発生し、株式売買が終日停止した。これを受けて同日夕方、東証が緊急会見を開いた。役員や幹部らの的確な情報公開と整然とした説明が評判を呼び、SNSなどで大きな話題になった。

東証は株券などの売買代金が1日あたり平均3.5兆円（当時）にのぼり、日本経済を動かす大動脈である。システム障害により引き起こされた売買停止のインパクトは絶大である。会見を開く必要性は容易に想像できる。

過去の取材から、大規模システム障害など重大インシデントに関する記者会見では、経営陣が記者の質問にしどろもどろになるパターンが多く見受けられる。矢継ぎ早の質問と会場の異様な雰囲気に気圧され、尋常ではないプレッシャーに直面するためである。

ところが、会見に出席した日本取引所グループ（JPX）の最高情報責任者（CIO）は、記者の質問によどみなく答え、技術的な解説も噛み砕いてわかりやすく説明していた。「システムの隅々まで知り尽くしている。主体的に携わっている」と当時、思った記憶がある。

答えの一つひとつに、説得力があると感じた記者会見は、実はあまり多くない。大抵のケースは部下が作成した想定問答を読み上げたり、「……と聞いている」といった伝聞調だったりする。

逆に東証の会見は、自分の言葉で説明していることが強く印象づけられ、これが納得感を増す結果となった。その時点で判明していない事実関係については「わからない」と言い、ごまかすような雰囲気は感じられなかった。システム障害というマイナスの局面から、東証のレピュテーション（評判）を上げるに至ったのである。

記者会見のポイントは「適材適所の人材を出席させる」ことにある。経営トップが全てを答える必要はない。記者と真正面から向き合い、それぞれが誠実に言葉をつないで説明する。正直な話、そのような会見になると逆に記者が雰囲気に呑まれ、質問が尻すぼみになることが多い。

この原稿を執筆するにあたり、なぜ日本取引所グ

ループCIOが自分の言葉で説明し、整然とした対応をすることができたのか調べることにした。すると、2021年6月1日の文春オンラインでCIOのインタビュー記事が見つかった（東証システム障害で話題に　横山隆介CIOが語る「ベンダー任せにしない」理由、https://bunshun.jp/articles/-/45718）。

記事には、かつての苦い経験が書かれていた。2005年から06年にかけて相次いだシステム障害への対応が教訓になっているとのことであった。開発ベンダーにおんぶに抱っこではなく、ユーザー企業として主体的に関わり、「自分ごと」として考えるようになったことが大きいという。

8. サイバー被害を「不祥事」とは考えない

最後に、サイバーインシデントに対する情報公開を考える時の「心構え」のようなものを示して本稿を終わりにしたい。

サイバー攻撃の被害を公表する際、情報流出のリスクや顧客や取引先に迷惑をかけた状況などから、おわびで始まる文面が多い。当事者としては仕方がない部分である。

ただ被害組織の不祥事かといえば、そうではない。不祥事と内部で捉えてしまうと、その後の対応が後ろ向きになり、受け身になりがちである。そこは認識を切り離す必要がある。

筆者は経営者を対象にした講演の最後に、このような言葉をスライドで映して締めくくるようにしている。

・「言わない理由」を考えると後ろ向きになり「言えない理由」を考えると前向きになる
・「メディアに説明」すると考えれば対策になり「お客さんに説明」すると考えれば誠意になる
・「発表」することは公益性のある社会貢献であり「公表」することで救われる人たちや組織がある

大事なことは、情報公開を前提とした対応を考えることである。「ここまでは説明できる」「言えない理由を正直に説明しよう」と考えるようになり、自ずと筋道を立てた説明が出来上がる。

逆に公表したくない姿勢で臨むと、辻褄を合わせるのに一苦労である。その結果、「セキュリティの観点から…」というお決まりの言葉が頻出するようになる。

メディア対応の時、記者に説明するための方策を考えると、自ずと危機管理対応になる。メディアに揚げ足を取られないための文面に気を取られ、中身が伴わない対応になりがちである。

そんな時は、記者の向こう側で情報を待っているお客さんやステークホルダーの姿を想像する。誠意のある説明をしようと考える。何を話せば良いか自然と頭の中に浮かんでくるようになる。

「発表」とは多くの人たちに対し、誰も知らないことを伝えることであり、特定の情報を公にすることが「公表」である。

つまり、社会に対して説明し、かつ必要とされる人たちに情報を届けることこそが、情報公開の本質であり求められていることであると筆者は考えている。

サイバー犯罪集団やハッカーは日頃から、攻撃の手口や盗み取った情報を水面下で共有し、次の攻撃を考えている。一方で私たちの社会はインシデント発生時など情報共有に大きな壁が立ちはだかり、対応が後手に回っているのが実情である。

サイバー攻撃の「脅威」を社会全体が共有することで、セキュリティ対策の強化につながると筆者は信じている。そのために被害組織の経験やノウハウが重要な情報源になる。そんな社会の実現のため、筆者も微力ながら尽力する次第である。

本誌についてのお問い合わせは下記にお願い致します。

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
会社URL：https://www.tokio-dr.jp/
サイバーセキュリティ事業部：https://www.tokio-dr.jp/service/cyber/
（担当：サイバーセキュリティ事業部 高木宏典）

東京海上日動火災保険株式会社

www.tokiomarine-nichido.co.jp

お問い合わせ先

K08-22600 新 202510