PostgreSQL インサイド

ランサムウェアに狙われる中小企業

万一への備えはバックアップ

ある日突然、脅迫メッセージが出力されると共に端末がロックされたりデータが暗号化されて使用できなくなったりする、といったランサムウェアによる被害が後を絶ちません。すでに何年も対策が叫ばれているものの、今も日本国内での被害件数は増加しており、かつ、被害企業の半数以上が中小企業との報告があります。
この記事ではランサムウェア被害の最近の状況をもとに、比較的すぐに始められるランサムウェア対策としても重要なバックアップについて、バックアップを実施していても復旧に失敗する原因や、復旧失敗のリスクを低減するためのポイントを説明します。

1. ランサムウェアとは

ランサムウェア（Ransomware）とは、感染した PC をロックしたり、重要なデータを暗号化したりして使用できなくし、その復旧と引き換えに身代金を要求する不正プログラムです。

近年の主流は英語で「human-operated ransomware attacks」、日本語では「侵入型ランサムウェア攻撃」「標的型ランサムウェア攻撃」と呼ばれるもので、攻撃者は、まず VPN 機器やリモートデスクトップなどの脆弱性を突いて企業内のネットワークに侵入します。または、フィッシングメールを送り、マルウェアに感染させることにより侵入することもあります。システムに侵入後は様々な権限を取得してランサムウェアを展開し、ファイルを暗号化した上で、解除キーを提供する代わりに身代金を払うよう脅迫メッセージを出力します。また近年では暗号化のみならずデータを外部サーバーに持ち出し、「身代金を払わなければデータを公開する」と脅迫する攻撃（「二重脅迫型」や「暴露型」と呼ばれます）も増えており、身代金を奪おうとする手口が多様化しています。

ランサムウェアに感染すると、ネットワークに接続している共有ファイルや他のサーバーのデータまで暗号化されることにより、企業のデータの大部分が使えなくなり、業務停止に追い込まれることになりかねません。さらに、１つの企業内にとどまらず、サプライチェーンを通じて子会社や取引先企業にまで感染が広がる事例も報告されています。

復旧には時間、費用、労力を要します。それだけでなく、被害を受けたためにビジネスチャンスを逃す可能性や、業務停止によって取引先企業にも損害を与えてしまう可能性が生じます。

2. 最近のランサムウェアの発生状況：中小企業の被害が増加

独立行政法人情報処理推進機構（以降、IPA）が発表した「情報セキュリティ 10 大脅威 2023」では、2022 年に組織を対象とした脅威の第 1 位がランサムウェアでした。ランサムウェアは「情報セキュリティ 10 大脅威 2022」においても 2021 年と 2020 年に第 1 位であることが示されており、2020 年から 3 年連続で第 1 位となっています。
この結果からランサムウェアの猛威は衰えることなく続いているように感じられます。

情報セキュリティ10大脅威 2023

順位	組織を対象とした脅威	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

圏外：昨年はランクインしなかった脅威

情報セキュリティ10大脅威 2022

順位	組織を対象とした脅威	前年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等の ニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	New
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

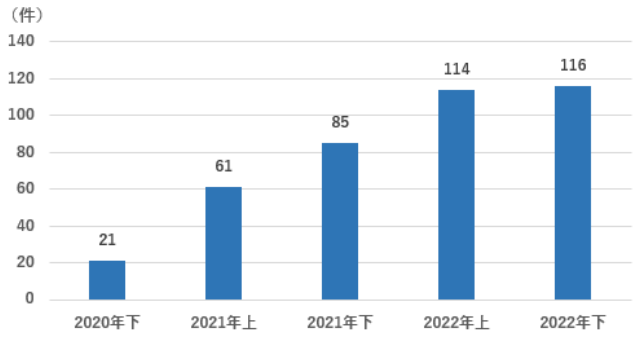
New：初めてランクインしたた脅威

出典：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2023」(URL:https://www.ipa.go.jp/security/10threats/10threats2023.html)、
および「情報セキュリティ10大脅威 2022」(URL:https://www.ipa.go.jp/security/10threats/10threats2022.html)を基に作成

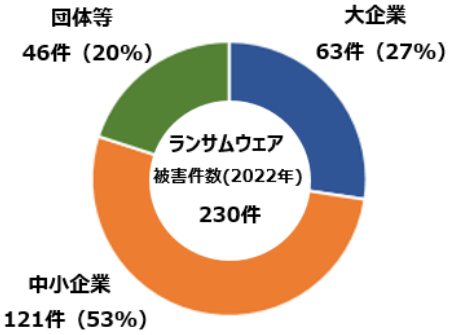
- 「情報セキュリティ 10 大脅威 2023」（IPA のオフィシャルページへ）
  https://www.ipa.go.jp/security/10threats/10threats2023.html
- 「情報セキュリティ 10 大脅威 2022」（IPA のオフィシャルページへ）
  https://www.ipa.go.jp/security/10threats/10threats2022.html

警察庁が発表した「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」によると、令和 4 年（2022 年）中に警察庁に報告された被害件数は前年比 57.5%増と右肩上がりに増えています。また、被害を受けるのはニュースで取り上げられるような大企業ばかりではありません。同レポートによると、被害企業・団体の規模では大企業の 27%に対し中小企業が 53%を占めています。

【企業・団体等におけるランサムウェア被害の報告件数の推移】



【ランサムウェア被害の企業・団体等の規模別報告件数】



出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」
(URL:https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf)を基に作成

前年のレポート（「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」）と比較すると、大企業の占める割合は 34%と報告されており 7%減少しています。また、被害件数の増加率では、大企業が 49 件から 69 件で 28%増、中小企業は 79 件から 121 件で 53%増と、中小企業の増加率が上回っています。これらのことから、被害が大企業から中小企業にシフトする傾向であることがうかがえます。

中堅病院が被害を受けた例としてよく取り上げられるのは、ある町立の病院の事例です。VPN の脆弱性からランサムウェアの侵入を許し、その後セキュリティ対策の不備を突かれ多数の PC やサーバーにログインされて感染が拡大しました。結果、カルテが参照できなくなるなど医療の提供に大きな制限が生じ、復旧まで 2 か月を要するという甚大な被害を受けました。

- 「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁のオフィシャルページへ）
  https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
- 「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁のオフィシャルページへ）
  https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

なぜ中小企業が狙われるのでしょうか。2021 年に実施された IPA の中小企業を対象としたアンケート調査には、以下のような結果が示されています。

- 過去 3 期における IT 投資額において、「投資していない」が 30%。
- 過去 3 期における情報セキュリティ対策投資額において、「投資していない」が 31.1%。その理由として「必要性を感じていない」が最も多く 40.5%。「費用対効果が見えない」が 24.9%、「コストがかかりすぎる」が 22.0%と続いている。
- 情報セキュリティ対策の組織体制において、「組織的には行っていない（各自の対応）」が 49.2%と最も多い。
- 従業員に対する情報セキュリティ教育の実施状況において、「特に実施していない」が 55.1%と最も多い。
- 「2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -調査報告書-」（IPA のオフィシャルページへ）
  https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

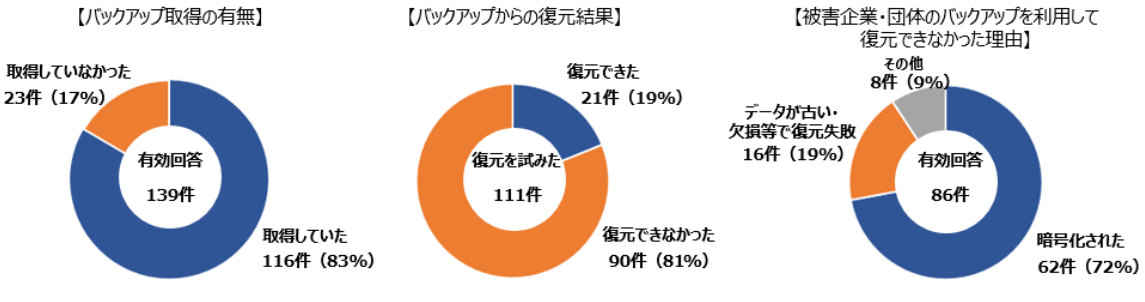
セキュリティ対策への投資の優先度を低くせざるをえなかったり、セキュリティ部門が無く組織的な対策の実施や社内教育・訓練が行われていなかったりする企業では、攻撃者の侵入が容易になるような脆弱性をシステムに抱えてしまう可能性が高くなると考えられます。
また、先に述べたサプライチェーン攻撃の起点として、システムに侵入しやすい企業が狙われることも考えられます。攻撃者は感染した企業を踏み台として業務上の関連を悪用し、子会社や取引先への攻撃を行います。攻撃対象の企業では業務上のやりとりを利用して侵入されるため、その検知が困難になります。

ランサムウェアを含めサイバー攻撃は、国際的な紛争などの社会経済情勢や、技術の進歩などに応じて今後も手口を変化させていくでしょう。新たな脅威の情報や注意喚起は、警察庁、内閣官房 内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity（NISC））をはじめ各省庁や、IPA、一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center（JPCERT/CC））といった団体からも行われており、情報セキュリティ対策への意識は高まっていると思われます。しかし、今もなお被害件数が増え続けていることから、感染への防御対策を行うと共に、防御を突破されることも想定して備えるほうがよいでしょう。

3. 万一への備え、バックアップとその課題

先に述べたような「人材・予算・知識」の課題を踏まえ、情報セキュリティ対策の基本をしっかり行うことが重要になります。中でもバックアップは、それを実施していたために復旧できた例もあるため、万一感染してしまったときの備えとして重要です。
ランサムウェアによってデータが暗号化されても、バックアップデータまで感染していなければ復旧できる可能性があります。例えば最低限、顧客マスターのデータベースだけでもバックアップをクラウドに保管や、外部記憶媒体にバックアップしてオフラインにしておくと、他のデータが復旧するまでの間でもビジネスの継続や復旧までの時間を短縮できる可能性があります。

しかし、先の警察庁のレポートによると、バックアップを実施していたにもかかわらず復旧できなかったものが 81%に及び、その理由は「暗号化された」が 72%、「データが古い・欠損等で復元失敗」が 19%を占めています。



出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」
(URL:https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf)を基に作成

これらの理由に対し、どのようにすれば復旧失敗のリスクを下げられるかを計画しておく必要があります。

4. 復旧失敗のリスクを下げるには

バックアップ運用の設計時に、どの時点のデータの状態に戻したいか（RPO：目標復旧ポイント）に対し、バックアップの取得日時や間隔を適切に設定する必要があります。それらが適切でないと、データの欠損による復旧失敗の原因となります。また、バックアップが最新の１世代だけだと、もし感染に気付かないままバックアップを取得してしまった場合、そのバックアップは復旧に使用できません。バックアップが複数世代あれば、感染前の世代が存在する可能性が高まります。

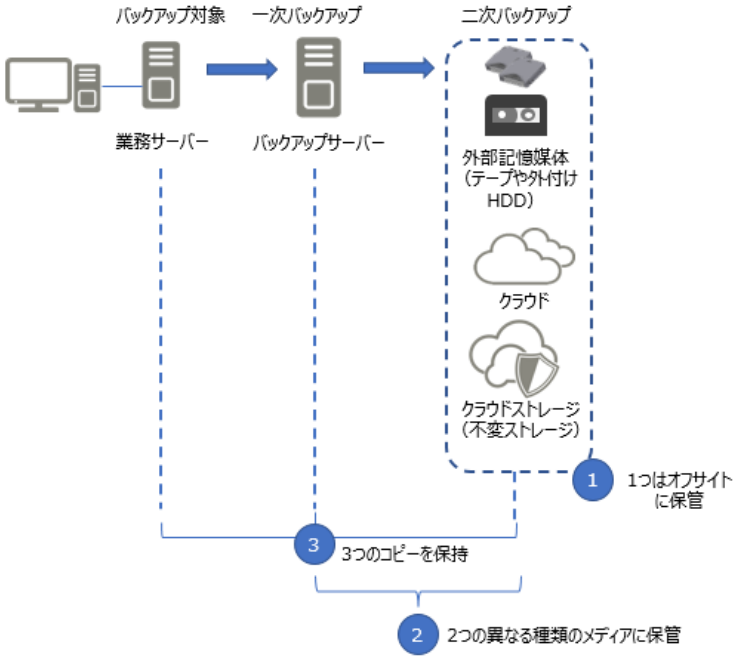
バックアップ先のデータが暗号化されて復旧に失敗するケースに対しては、そのリスクを下げ、より安全な保管先を選定する必要があります。

参考

冒頭で触れた「二重脅迫型」「暴露型」攻撃に対しては、データを暗号化しておき、もし盗み出されても情報流出しないように備えておくことが重要です。ただし、暗号を解除するための暗号鍵をデータと同じサーバーに保存しておくと攻撃者に窃盗される恐れがあるため、別の場所に保管することでリスクを低減できます。

バックアップ保管先の安全性を高めるには

侵入型ランサムウェア攻撃では、攻撃者はバックアップからの復旧を阻害してより確実に身代金を取るためにバックアップ先まで標的にします。バックアップの保管先を、攻撃者に侵入されたサーバーから直接アクセスできるディスク領域や共有フォルダーなどにしていると、そこもランサムウェアに感染して暗号化され、データの復旧ができなくなります。
このような被害を防ぐために、「3-2-1」ルールの考え方が参考になります。これは重要なデータを損失や破損から保護するためのバックアップの考え方で、2012 年に米国国土安全保障省配下の情報セキュリティ対策組織である、US-CERT（United States Computer Emergency Readiness Team）が提唱したものです。「ファイルのコピーを３つ保持する」「２つの異なる種類のメディアに保管する」「１つをオフサイト（例えば自社施設と物理的に離れた場所）に保管する」という３つのルールに則ってバックアップを保管することを推奨しています。



オフサイトの保管先としては、外付け HDD やテープにバックアップしオフライン（物理的に隔離）にしておく方法がサイバーセキュリティの観点では強力と言えるでしょう。

参考

バックアップ時はオンラインで実施し、その後ネットワークから切り離してオフラインで保管することを「エアギャップ」と呼びます。エアギャップにはソフトウェアによって論理的にデータへのアクセスを制限するなどの手法もあります。

また、クラウドの不変ストレージに保管することも安全性を高めます。不変ストレージはイミュータブルストレージとも呼ばれ、一度書き込んだら書き換えができません。このため、ランサムウェアの攻撃を受けてもデータ改変を防ぐことができます。この機能は Microsoft Azure Storage の Azure Blob Storage や Amazon S3（Simple Storage Service）のオブジェクトロックなどで提供されています。
それぞれ取扱いのしやすさや費用など違いがありますので、保管したいデータの種類やバックアップの頻度、データ量などを考慮して選定してください。

訓練を実施する

攻撃は予期せぬ時に突然行われます。いざというときに迅速に対応できるように、復旧計画を立て、マニュアルを作成して定期的に復旧作業の訓練を行うことが大切です。マニュアルは一度作成してもシステム構成や運用が変更されると陳腐化するため、定期的に見直して最新化しておきましょう。訓練の際には計画に従って正しく作業できるか、RPO（目標復旧ポイント）や RTO（目標復旧時間）を達成できているかなどをチェックしましょう。

5. まとめ

安全な方法でバックアップを保管することはビジネスの継続性を向上させます。これはシステム品質の向上を意味します。専用のストレージや通信プロトコルを備え、自動化などにより運用の手間を抑えることができるバックアップソリューションを利用すれば、より安全性が高まるでしょう。ただ、費用もかかります。しかし、費用をかけず対策を怠ればリスクが高まります。兼ね合いを考えることが重要です。

なお、富士通のデータベース Fujitsu Enterprise Postgres のオペレーターを利用することで、データベースの自動バックアップをオブジェクトストレージに取得することができます。オブジェクトストレージは Amazon S3、Azure Blob Storage、Google Cloud Storage をサポートしています。Fujitsu Enterprise Postgres のオペレーターの機能や特長については、以下を参照してください。

- コンテナ型データベースで運用コストを削減～ Enterprise Postgres の高可用オペレーター機能 ～

また、Fujitsu Enterprise Postgres はデータベースの格納データを暗号化する透過的データ暗号化機能を備えており、使用するキーストアとしてクラウドの鍵管理システムを利用可能です。これにより、データベースの暗号化データと暗号キーを別々に保管することができます。

- クラウド鍵管理サービス連携：「Fujitsu Enterprise Postgres 15 SP1 リリース」

2023 年 10 月 11 日