脅威アクタープロフィール；LockBit

[TLP：White]

※本資料は Health ISAC が 2026 年 6 月に発行したレポートをもとに、Health ISAC Japan で内容を再構成し、一部加筆修正を行ったものとなります。

【エグゼクティブサマリー】

LockBit は、サイバー犯罪の歴史上、最も強固なランサムウェア・アズ・ア・サービス（RaaS）の一つです。2019 年後半に（当初は ABCD ランサムウェアとして）出現した LockBit は、世界的な脅威の状況を支配するまでに成長し、2022 年から 2023 年にかけて、世界のランサムウェア攻撃全体の約 40%を占めると推定されています。

（図：Lockbit ロゴ）

【脅威アクターのステータス】

現在も継続的に活動しています。

【脅威アクターの性質】

金銭的利益を追求するサイバー犯罪者で、ランサムウェア・アズ・ア・サービス（RaaS）です。

【医療分野への影響】

2026 年 6 月現在、医療分野は LockBit によって最も標的にされている業種の 1 つです。Health-ISAC の侵害データによると、ランサムウェアグループに起因する 3,483 件のインシデントのうち 232 件が医療分野で発生しており、病院およびヘルスケアが最多のサブセクター（ 109 件の被害者）で、次いで診療所、製薬、ウェルネス/フィットネスサービスとなっています。

脅威アクタープロフィール；LockBit

【概要】

LockBit の進化は、基本的なランサムウェアのスタートアップから、高度に組織化された自動化された犯罪組織への移行、そして国際的な法執行機関の取り締まり後の混乱した再建段階を反映しています。以下は、LockBit の系統の時系列的な歴史です。

（図:LockBit の歴史）

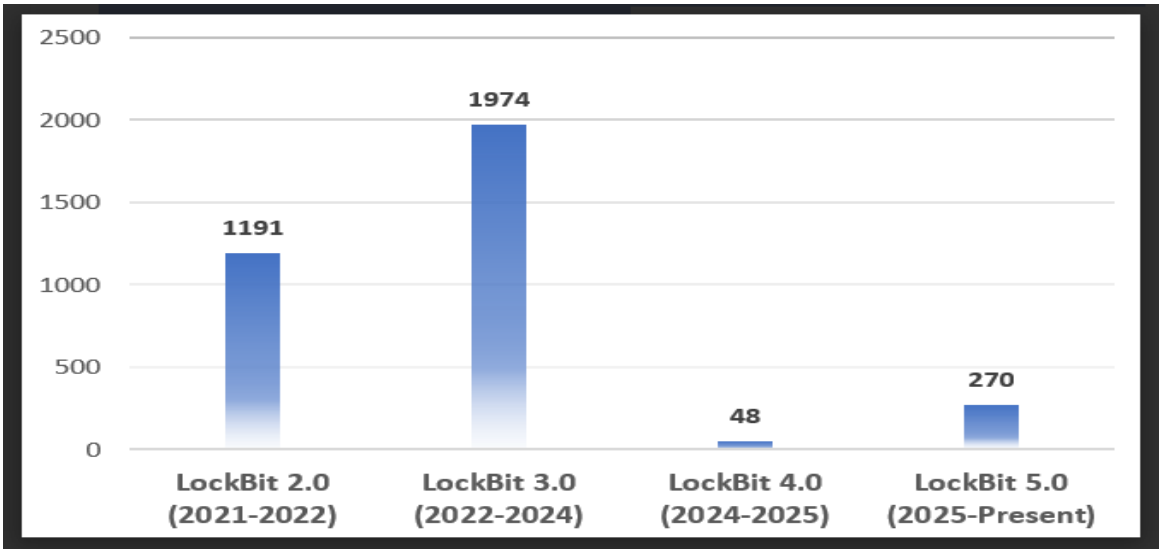
LockBit バージョン	活動時期	コア技術	特徴	主な影響
LockBit 1.0 (ABCD)	2019 年 9 月 ～ 2021 年 5 月	C/C++	**誕生期**：単純なファイル暗号化マルウェアとして登場し、その後「Ransomware-as-a-Service（RaaS）」モデルへ移行。	当初の拡大は比較的緩やかだったが、Linux・ESXi 向けロッカーの投入により拡大。
LockBit 2.0 (Red)	2021 年 6 月 ～ 2022 年 6 月	C/C++	**自動化の飛躍**：グループポリシーを利用して企業ネットワーク全体へ自動拡散。データ窃取ツール「StealBit」と脅迫用の「印刷型身代金要求書（Print Bombing）」を導入。	Conti ランサムウェアグループ崩壊後に急速拡大。感染速度が大幅に向上。
LockBit 3.0 (Black)	2022 年 6 月 ～ 2024 年初頭	モジュール型 C/C++	**全盛期**：BlackMatter のコードを流用。サイバー犯罪版「バグバウンティ制度」を開始。2022 年後半にはビルダーのソースコードが流出。	最も活動が活発だった亜種。2022～2023 年の世界のランサムウェア攻撃の最大 44%を占めた。
LockBit Green	2023 年 1 月～ 2023 年中頃（LockBit Black の派生版）	Conti コード	**Conti 統合版**：Conti 崩壊後、流出した Conti 系アフィリエイトを取り込むために特別に開発されたバージョン。	Conti 出身の攻撃者にとって非常に馴染みやすい環境を提供。
LockBit 4.0 (Next-Gen)	2024 年後半 ～	.NET	**法執行機関への対抗**：	Operation Cronos 後に再構築。防御・回避能力を重視した運用

	2025 年中頃		2024 年の大規模摘発「Operation Cronos」後にゼロから再構築。派手な自動化機能を削減し、高度なステルス性に重点を置いた。	へ移行。
LockBit 5.0	2025 年 9 月 ～ 現在	クロスプラットフォーム・バイナリ	**再建**：アフィリエイト参加費を 500 ドルまで引き下げ。Windows、Linux、VMware 環境にネイティブ対応し、「Invisible（不可視）暗号化モード」を搭載。	LockBit が摘発後に再設計した戦略を採用。マルチ OS 対応とステルス性を重視。

この組織は、綿密に管理されたアフィリエイトネットワークに依存しています。2024 年初頭に大規模な多国籍法執行機関による摘発（オペレーション・クロノス）が行われ、情報漏洩サイトとインフラが押収されたにもかかわらず、LockBit は活動を継続しており、コア開発者たちはサーバーの再構築、LockBit 3.0 や LockBit Black などの新バージョンのリリース、そして新たなアフィリエイトの募集を試みています。このグループは、二重の恐喝戦術に重点を置き、ファイルを暗号化すると同時に機密データを盗み出し、被害者に金銭を支払わせます。

LockBit の被害規模はバージョンによって大きく異なり、中でも LockBit 3.0 は史上最も著名で破壊的なランサムウェアとして台頭しています。

（図：Lockbit2.0 以降の被害者報告数）



脅威アクタープロフィール；LockBit

【活動地域】

北米は依然として全地域の中で最優先ターゲットであり、特に米国とカナダがそれに続き、次いでヨーロッパとアジア太平洋地域が続いています。アジア太平洋地域ではオーストラリアが最もターゲットとなっています。

【攻撃の特徴】

LockBit は、現在も世界で最も影響力の大きいランサムウェアグループの一つであり、高度な自動化機能と大規模な横展開能力を特徴としています。

まず、VPN 機器やリモートアクセス機器の脆弱性、Citrix Bleed や Fortinet 製品などの公開脆弱性、盗まれた VPN や RDP 認証情報を悪用して組織内部へ侵入します。また、初期アクセスブローカー（IAB）から購入した認証情報を利用するほか、内部関係者へ金銭を提示して協力者を募る事例も確認されています。

侵入後は直ちに暗号化を行うのではなく、Advanced IP Scanner や NetScan などを利用してネットワーク構成を調査し、Active Directory、ファイルサーバー、バックアップサーバー、仮想基盤などの重要資産を特定します。さらに BloodHound や SharpHound を利用して Active Directory の構造を分析し、ドメイン管理者権限への最短経路を探索します。

その後、Mimikatz や LSASS メモリダンプツールを利用して認証情報を窃取し、Kerberos や LLMNR など Windows 認証機能の悪用を通じて権限昇格を実施します。最終的にはドメイン管理者権限を取得し、組織全体を制御可能な状態を構築します。

LockBit の特徴は、攻撃の多くを自動化している点にあります。AnyDesk、Atera、Splashtop などの正規リモート管理ツールや、Cobalt Strike、Brute Ratel などの商用 C2 フレームワークを利用して継続的なアクセスを維持します。また、PsExec や Impacket、Windows 標準機能を利用した横展開に加え、Active Directory のグループポリシー（GPO）を悪用してランサムウェアをドメイン全体へ一斉配布することが可能です。

十分な権限と支配範囲を確保した後は、機密情報の窃取が行われます。LockBit は独自ツールである StealBit を利用し、財務情報、契約文書、個人情報、内部資料などを自動的に収集・圧縮し、攻撃者が管理するクラウドストレージへ送信します。また、Rclone などのツールも利用されます。これらは暗号化後に実施される二重恐喝のための準備でもあります。

暗号化の直前には、防御機能と復旧手段の無効化が行われます。BYOVD（Bring Your Own Vulnerable Driver）を利用して EDR やアンチウイルス製品を強制終了するほか、Microsoft Defender の無効化、Windows イベントトレーシング（ETW）の改変、メモリ上での実行による検知回避などを実施します。さらに、ボリュームシャドウコピーやイベントログを削除し、Veeam や Acronis などのバックアップサービスを停止することで復旧を困難にします。

その後、Windows、Linux、VMware ESXi 環境向けに最適化された暗号化プログラムを実行します。LockBit はマルチスレッド処理による高速暗号化を特徴としており、短時間で大量のローカルファイルやネットワーク共有ファイルを暗号化することが可能です。また、一部の亜種ではネットワークプリンタへ身代金要求文書を大量印刷する「Print Bombing」を実施し、組織内部に混乱と心理的圧力を与えることも確認されています。

最後に、リークサイトや交渉サイトを通じて被害組織と接触し、盗み出した情報の公開を示唆しながら身代金の支払いを要求します。暗号化による業務停止だけでなく、情報公開を利用した二重恐喝を組み合わせることで、被害組織に対する圧力を強めています。

【暴露サイト、感染ファイル等】

- **データ暴露サイト（一例）**
  - hxxp://lockbitapiahy43zttdhslabjvx4q6k24xx7r33qtcvwqehmnnqxy3yd[.]onion
  - hxxp://lockbitapo3wkqddx2ka7t45hejurybzzjpos4cpeliudgv35kkizrid[.]onion
  - hxxp://lockbitapp24bvbi43n3qmtfcasf2veaeagjxatgbwtxnsh5w32mljad[.]onion
  - hxxp://lockbitapyum2wks2lbcnrovcgxj7ne3ua7hhcmshh3s3ajtpookohqd[.]onion

LockBit の Tor URL は、特にオペレーション・クロノス以降、国際的な法執行機関による積極的な妨害行為や定期的なインフラストラクチャのローテーションにより、頻繁に変更されています。

- **暗号化されたファイル拡張子:**
  - .abcd
  - .lockbit
  - .[9 ランダムな英数字文字列]（例: .hlp6izvki）
  - .[16 個のランダムな英数字文字列]（例：.a1b2c3d4e5f6g7h8）

- **身代金要求テキスト**
  - ReadMeForDecrypt.txt

【戦術、技術、手順（TTP）】

攻撃は以下の流れで一般的に行われます。

戦術	ID	技術	手順 / 観測可能値
実行	T1059	コマンド／スクリプトインタープリタ（Command and Scripting Interpreter）	自動化された PowerShell スクリプトまたはネイティブ CMD スクリプトを使用して、ローダーを実行し、デプロイメントパラメータを渡します。
実行	T1106	ネイティブ API（Native API）	低レベルの Windows API を直接実行し、マネージドランタイム環境をバイパスすることで

脅威アクタープロフィール；LockBit

戦術	ID	技術	手順 / 観測可能値
			暗号化を高速化します。
永続化	T1078	有効なアカウント（Valid Accounts）	不正に入手した、高い権限を持つ企業または管理者の認証情報を利用して、環境へのアクセスを維持する。
防御回避	T1055.012	プロセスインジェクション：プロセスホローイング（Process Injection: Process Hollowing）	svchost.exe や defrag.exe などの正規のシステムバイナリにランサムウェアのコアコードを注入します。
防御回避	T1562.001	防御機能の妨害：ツールの無効化または変更（Impair Defenses: Disable or Modify Tools）	ETW ブラインディング: EtwEventWrite のメモリを 0xC3 (ret) 命令でパッチし、EDR ログテレメトリを無効にします。
防御回避	T1027	難読化されたファイルまたは情報（Obfuscated Files or Information）	カスタムシード（0xA879 および 0xB97A など）で初期化された動的ハッシュアルゴリズムを使用して、内部文字列を暗号化します。
防御回避	T1070.001	痕跡の削除：Windows イベントログの消去（Indicator Removal: Clear Windows Event Logs）	自動化されたユーティリティを使用して、セキュリティ、システム、およびアプリケーションのログトラックをプログラムによってクリアします。
探索	T1518.001	ソフトウェアの探索：セキュリティソフトウェアの探索（Software Discovery: Security Software Discovery）	ローカルプロセスとシステムサービスをスキャンして、実行中のウイルス対策エージェントまたは EDR エージェントを特定し、警告を発します。
認証情報アクセス	T1003.001	OS 認証情報ダンピング：LSASS メモリ（OS Credential Dumping: LSASS Memory）	特殊なダンプスクリプトを使用して LSASS プロセス空間を標的とし、アクティブなドメイントークンを抽出します。
探索	T1082	システム情報の探索（System Information Discovery）	ホスト OS のアーキテクチャを照会し、Windows、Linux、または VMware ESXi 仮想化ノードに合わせて実行を調整します。
探索	T1135	ネットワーク共有の探索（Network Share Discovery）	暗号化パスをマッピングするために使用可能なローカルおよび隠し管理共有（C$、ADMIN$）を列挙します。
横展開	T1021.002	リモートサービス：SMB／Windows 管理共有（Remote Services: SMB/Windows Admin Shares）	内部ネットワークサブネットを横方向に移動して、ローダーを隣接するインフラストラクチャにプッシュします。
情報窃取	T1567.002	Web サービスを介したデータ窃取：クラウドストレージへの窃取（Exfiltration Over Web Service: Exfiltration to Cloud Storage）	特殊な自動データスクレイピングコンポーネントを介して、機密性の高いディレクトリ構造をクラウドストレージに抜き出す。

戦術	ID	技術	手順 / 観測可能値
インパクト	T1486	データ暗号化による影響（Data Encrypted for Impact）	ChaCha20 対称ストリームと X25519（ECC）鍵交換を利用した、高速な並列ハイブリッド暗号化を実行します。
インパクト	T1490	システム復旧の妨害（Inhibit System Recovery）	シャドウコピー（vssadmin）を削除し、アクティブなサーバーバックアップを終了し、デフォルトのリカバリサイクルを中断します。

【国内医療機関が優先的に実施すべき対策】

国内医療機関における医療情報システム・ネットワーク環境管理の特性を踏まえ、攻撃特徴や TTP を考慮した観点より、国内医療機関が特に優先すべき三つの対策例とその理由を示します。

1. **診療系ネットワークへ到達可能な外部アクセス経路と特権認証情報の防御（初期侵入対策）**
   - 診療系ネットワークに接続する保守 VPN、Citrix、RDP、リモートメンテナンス装置等を棚卸しし、不要な外部公開を廃止
   - VPN、RDP、Citrix、ID プロバイダー等に FIDO2／WebAuthn 等のフィッシング耐性を有する MFA を適用
   - Fortinet、Citrix、Palo Alto 等の外部公開機器について、重大脆弱性を優先して迅速にパッチ適用
   - 保守 VPN は接続元 IP、接続時間、接続対象システムを限定し、常時接続を避ける
   - ドメイン管理者や外部保守アカウントには PAM／JIT を適用し、高権限を常時付与しない

   LockBit は、VPN やリモートアクセス機器の脆弱性、盗まれた VPN・RDP 認証情報、初期アクセスブローカーから購入した認証情報等を主要な侵入口として利用します。 国内医療機関では、診療系ネットワークは原則インターネットから分離されている一方、電子カルテや医療機器を保守する VPN 等が外部から診療系へ到達できる例外経路となります。したがって、**認証情報を盗まれても使わせないことと、診療系へ直接到達できる外部接続口そのものを最小化すること**が最優先となります。

2. **AD・GPO・EDR を含む管理基盤の防御と高速横展開の封じ込め（全体感染対策）**
   - BloodHound、SharpHound、Mimikatz、LSASS メモリダンプ等の利用を監視
   - PsExec、Impacket、PowerShell、WMI、SMB／Windows 管理共有等の利用を必要な管理端末間だけに制限
   - GPO の作成・変更・配布を監査し、通常と異なる一斉展開や権限変更をリアルタイムで検知
   - EDR の改ざん防止・管理ロック機能を有効化し、BYOVD や Defender 停止等による

防御無効化を監視

- 情報系 NW、診療系 NW、サーバー管理 NW、仮想基盤管理 NW を分離し、不要な管理通信を遮断

LockBit は、侵入後に AD 構造を調査してドメイン管理者への最短経路を探索し、Mimikatz 等で認証情報を窃取した後、PsExec や GPO を利用してランサムウェアをドメイン全体へ一斉配布します。 さらに、BYOVD による EDR 停止、Defender 無効化、イベントログ削除などを行い、監視能力そのものを弱体化します。電子カルテ、検査、画像、部門システム等が同じ AD 環境に属している場合、**一つの特権アカウント侵害が診療系全体の一斉感染につながるため、AD・GPO・EDR を独立した防御境界として扱うこと**が重要です。

3. **ESXi・バックアップ基盤の独立化と高速暗号化・二重恐喝への備え（診療継続対策）**
   - ESXi、Hyper-V 等の仮想化基盤管理ネットワークを一般の診療系 NW から分離
   - 仮想基盤管理者と AD 管理者の認証情報を分離し、MFA と専用管理端末を適用
   - ESXi 上での大量 VM 停止や異常な管理コマンド実行を監視
   - オフラインまたはイミュータブルバックアップを保持し、Veeam 等のバックアップ基盤を通常の AD 管理権限から分離
   - vssadmin によるシャドウコピー削除、バックアップサービス停止、イベントログ消去を重点監視
   - StealBit、Rclone 等による患者情報・機密情報の大量収集、圧縮、クラウド送信を検知
   - 電子カルテ、PACS、部門システム、仮想基盤について、クリーン環境からの復旧試験と IT-BCP 訓練を実施

   LockBit は暗号化前に StealBit や Rclone 等で機密情報を窃取し、その後、EDR や Defender を無効化し、シャドウコピーやバックアップサービスを停止して復旧手段を破壊します。さらに、Windows だけでなく Linux や VMware ESXi 環境にも対応し、高速な並列暗号化によって多数のシステムを短時間で停止させます。 特に LockBit 5.0 では Windows、Linux、VMware へのクロスプラットフォーム対応が明示されており、仮想基盤そのものが主要標的となっています。電子カルテ、検査、画像、部門システム等を仮想基盤へ集約している場合、ESXi 等を侵害されれば複数の診療機能が同時に停止します。そのため、**仮想基盤まで到達させないこと、バックアップを攻撃者から独立させること、暗号化されても診療を復旧できること**が最後の防衛線となります。

上記の通り、国内医療機関における LockBit 対策では、**①外部アクセスと特権認証情報を守る、②AD・GPO・EDR を悪用した高速横展開を止める、③ESXi とバックアップを独立させて診療継続性を確保する**ことを優先すべきです。

以上