2025 年 12 月 12 日
アスクル株式会社

ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告

（ランサムウェア攻撃によるシステム障害関連・第 13 報）

アスクル株式会社は、2025 年 10 月 19 日、ランサムウェア攻撃によるデータの暗号化とシステム障害により、大規模なサービス停止と保有情報の流出が確認される事態となり、多くのステークホルダーの皆様に多大なるご心配とご迷惑をおかけしております。

当社は外部専門機関の協力のもと、システム障害範囲の特定とランサムウェア攻撃の影響の詳細調査を進めてまいりました。

本日時点までに判明した調査結果等について、以下の通りご報告いたします。

■代表取締役社長 CEO 吉岡晃より

今般のランサムウェア攻撃により、お客様情報に加え一部のお取引先様の情報が外部へ流出しており、多大なご迷惑をおかけしております。また、当社物流システムに障害が発生してサービスが一時的に停止したことにより、お客様、お取引先様、物流受託サービスをご利用の企業様とそのお客様、株主の皆様をはじめ、多くのステークホルダーの皆様に多大なご迷惑とご心配をおかけしておりますこと、深くお詫び申し上げます。

当社は本件の重大性を厳粛に受け止め、影響の抑制とサービス復旧に全社を挙げて取り組んでまいりました。今後、ランサムウェア攻撃を踏まえた BCP の見直し・強化にも取り組んでまいります。

このたび、サービスの本格復旧フェーズへ移行するにあたり、サービスの安全性をご確認いただくとともに、現時点でお伝えできる調査結果、当社の対応、および安全性強化策について、二次被害防止のために開示が困難な内容を除き、可能な限り詳細にご報告いたします。

本報告が、当社の説明責任を果たすのみならず、本件に高いご関心をお寄せいただいている企業・組織におけるサイバー攻撃対策の一助となりましたら幸いでございます。

1. ランサムウェア攻撃の発生と対応の時系列

本件発覚以降の時系列は以下のとおりです。

日付	主な事象・対応状況
10 月 19 日	・午前、ランサムウェアによる攻撃を検知 ・ランサムウェア感染の疑いのあるシステムの切り離しとネットワーク遮断を実施 ・セキュリティ監視運用の強化 ・全パスワードの変更に着手 ・14 時、本社内に対策本部と同本部配下に事業継続部会・IT 復旧部会を設置 ・16 時半、「ASKUL」「ソロエルアリーナ」「LOHACO」受注／出荷業務停止
10 月 20 日	・外部専門機関へ支援要請。ログ解析、影響の詳細調査開始 ・意図しないデータ変更のチェック ・意図しないプログラムリリース有無の点検実施 ・プログラムのタイムスタンプ異常の点検実施
10 月 22 日	外部クラウドサービスへの不正アクセス発生
10 月 23 日	主要な外部クラウドサービスに関連するパスワードを変更完了 （以降、現時点で新たな侵入は確認されておりません）
10 月 24 日	・認証情報のリセット ・主要なアカウントパスワード変更の実施 ・管理アカウントの MFA（※1）適用 ・ランサムウェア検体抽出、EDR（※2）シグネチャ更新
10 月 29 日	出荷トライアル第１弾（FAX 注文・出荷 2 拠点／ケース品 37 アイテム出荷）開始

10 月 31 日	攻撃者により公開された情報（外部への流出）の確認を完了 ※10 月 30 日夜に公開された情報の調査の結果
11 月 4 日	情報流出専用お問い合わせ窓口を開設
11 月 7 日～10 日	出荷トライアル第１弾拡大（出荷5拠点→7 拠点、ケース品 37→230 アイテム）
11 月 11 日	攻撃者により公開された情報の確認を完了 ※11 月 10 日夜に公開された情報の調査の結果
11 月 12 日～ 12 月 3 日	出荷トライアル第 2 弾開始、拡大 ・ソロエルアリーナ Web サイト受注再開、ASKUL Web サイト受注再開 ・メディカル単品 500 アイテム、ケース品 596 アイテム、サプライヤー直送 1,450 万アイテム
12 月 2 日～ 12 月 9 日	・12 月 2 日夜に攻撃者により公開された情報を認識、調査開始 ・12 月 9 日 攻撃者により公開された情報の確認を完了

※1 Multi Factor Authentication：ID やパスワード（知識情報）に加え、認証の 3 要素である「（スマホなどの）所持情報」「（指紋、顔などの）生体情報」のうち、2 つ以上の異なる要素を組み合わせて認証を行う方法。多要素認証。

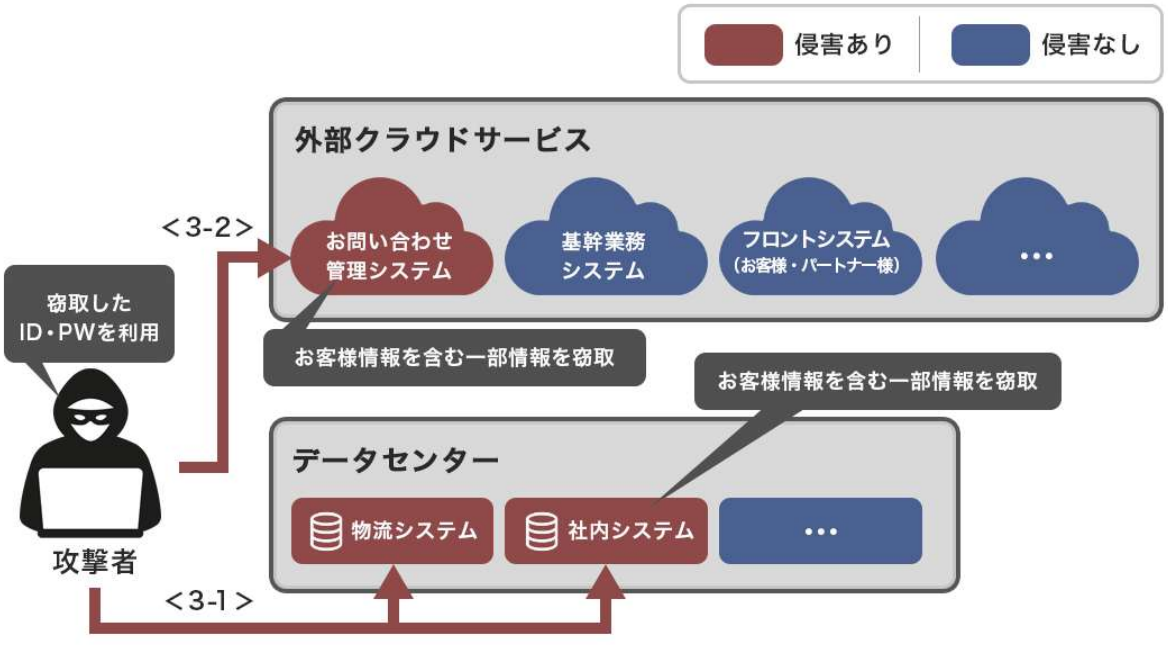
※2 Endpoint Detection and Response：PC、スマートフォン、サーバといったエンドポイントに侵入したサイバー攻撃の痕跡を検知し、迅速に対応するためのセキュリティ対策。

2. 流出が確認された情報

・流出が確認された個人情報の概要（2025 年 12 月 12 日時点）は以下のとおりです。
・本日、同内容について個人情報保護委員会へ確報を提出いたしました。
・該当するお客様・お取引先様等には、個別に通知を行っております。また、公開された情報が悪用される可能性を踏まえ、当社は長期的に監視体制を継続し、必要に応じて追加対応を実施していきます。
・今後、攻撃者による新たな情報公開が確認された場合は、対象となる方に個別通知を行うとともに、影響範囲や内容に応じて公表の要否を適切に判断いたします。
・なお、LOHACO 決済ではお客様のクレジットカード情報を当社が受け取らない仕組みとしており、当社は個人のお客様のクレジットカード情報を保有しておりません。
・二次被害防止の観点から、以下の情報の詳細については公表を差し控えさせていただきます。

事業所向けサービスに関するお客様情報の一部	約 59 万件
個人向けサービスに関するお客様情報の一部	約 13 万 2,000 件
取引先（業務委託先、エージェント、商品仕入先等）に関する情報の一部	約 1 万 5,000 件
役員・社員等に関する情報の一部（グループ会社含む）	約 2,700 件

3. 被害範囲と影響の詳細



＜侵害範囲・イメージ＞

・外部専門機関によるフォレンジック調査の結果、以下の事実を確認しております。
・なお、一部の通信ログおよびアクセスログが失われていたことから、攻撃者が閲覧した可能性のある情報の範囲を完全に特定することは困難であると判断しております。

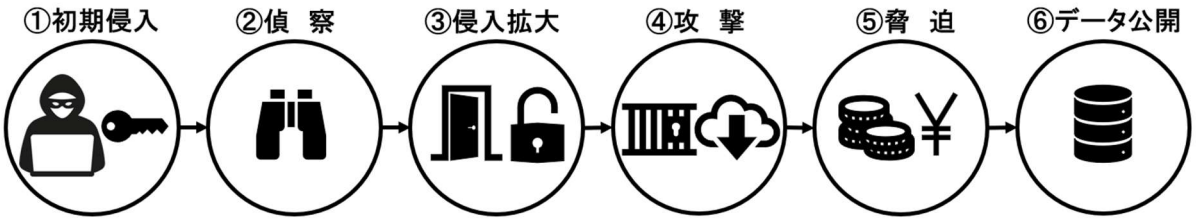
3-1 物流・社内システムへの侵害

・物流システム・社内システムでランサムウェアの感染が確認され、一部データ（バックアップデータを含む）が暗号化されて使用不能になるとともに、当該データの一部が攻撃者により窃取され、公開（流出）されました。
・物流センターを管理運営する複数の物流システムが暗号化され、同データセンター内のバックアップファイルも暗号化されたため、復旧に時間を要しました。
・当社物流センターは、自動倉庫設備やピッキングシステム等、高度に自動化された構造となっており、その稼働をつかさどる物流システムが停止したことで、物流センターの出荷業務を全面停止する重大な影響を及ぼしました。

3-2 外部クラウドサービスへの侵害

・上記 3-1 の侵害の結果、何らかの形で外部クラウドサービス上のお問い合わせ管理システムのアカウントが窃取され、当該アカウントの侵害が確認されました。
・当該お問い合わせ管理システムの情報の一部が窃取され、攻撃者によって公開（流出）されました。
・基幹業務システム、フロントシステム（お客様向け EC サイトやパートナー様向けサービス）は、侵害の痕跡がなかったことを確認しています。

4. 攻撃手法の詳細分析



時期	2025/6/5	2025/6 ～ 2025/10/9	2025/7/9 ～ 2025/10/19	2025/10/19～	2025/10/19 2025/10/21 2025/10/27	2025/10/30 2025/11/10 2025/12/2
概要	業務委託先用のアカウントを使用して社外より初期侵入	管理者権限等の取得を目標としたログイン試行(全て失敗)	脆弱性対策ソフトを無効化したうえで物流システムおよび社内システム、端末に侵入拡大し、ランサムウェア配置	事前設定された時刻にランサムウェアが起動し、サーバ暗号化ファイル削除クラウド情報窃取	メールによる脅迫文送付	リークサイト上でサンプルデータ公開

4-1 攻撃者による侵入の概要

・調査の結果、攻撃者は当社ネットワーク内に侵入するために、認証情報を窃取し不正に使用したと推定しています。初期侵入に成功した後、攻撃者はネットワークに偵察を開始し、複数のサーバにアクセスするための認証情報の収集を試みました。
・その後、攻撃者は、EDR 等の脆弱性対策ソフトを無効化したうえで複数のサーバ間を移動し、必要な権限を取得してネットワーク全体へのアクセス能力を取得していきました。
・なお、本件では複数種のランサムウェアが使用されました。この中には、当時の EDR シグネチャでは、検知が難しいランサムウェアも含まれていました。

4-2 ランサムウェア展開とバックアップファイルの削除

・攻撃者は必要な権限を奪取した後、ランサムウェアを複数サーバに展開し、ファイル暗号化を一斉に行いました。その際、バックアップファイルの削除も同時に行われたことが確認されています。これにより、一部システムの復旧に時間を要することとなりました。

5. 初動対応

5-1 ネットワーク遮断等による拡大防止

・当社は異常を検知した後、感染が疑われるネットワークを物理的に切断し、攻撃者の不正アクセス経路を遮

断する措置を実施しました。データセンターや物流センター間の通信も遮断し、感染の拡大防止に努めました。感染端末の隔離・ランサムウェア検体の抽出と EDR シグネチャの更新を実施しました。

5-2 アカウント管理の再構築

・全管理者アカウントを含む主要なアカウントのパスワードをリセットし、併せて主要なシステムに MFA（多要素認証）を適用することにより、不正アクセスの継続を防ぎました。

6. 原因分析と再発防止策

（1）不正アクセス

原因分析	✓当時のログが削除されており、原因の完全な究明は困難な状況です。 ✓例外的に多要素認証を適用していなかった業務委託先に対して付与していた管理者アカウントの ID とパスワードが何らかの方法で（※）漏洩し不正利用されたことが確認されており、当該アカウントでの不正アクセスがあったことが確認されております。 ＜※調査により判明した事項＞ ・当該業務委託先管理のノート PC について、OS 更新の過程で侵入時点のログが消去されており、当該ログを確認することはできませんでした。 ・VPN 機器ベンダが、2025 年 9 月末頃に脆弱性を公表しておりましたが、脆弱性を悪用した侵入の痕跡は確認されませんでした。 ・当社社員 PC には不正侵入や情報窃取の痕跡は（当社社員 PC からの漏洩）確認されませんでした。
再発防止策	当社および業務委託先における ①全てのリモートアクセスに MFA の徹底 ②管理者権限の厳格な運用 ③従事者の再教育

（2）侵入検知の遅れ

原因分析	✓侵害が発生したデータセンターではサーバに EDR が未導入であり、また 24 時間監視も行われていなかったため、不正アクセスや侵害を即時検知できませんでした。
再発防止策	①24 時間 365 日の監視と即時対応の体制整備 ②EDR 導入を含む、網羅的で多層的な検知体制の構築

（3）復旧の長期化

原因分析	✓侵害が発生したサーバでは、オンラインバックアップは実施していましたが、ランサムウェア攻撃を想定したバックアップ環境を構築していなかったため、一部バックアップも暗号化され、迅速な復旧が困難となりました。 ✓セキュリティ対策を適用すべき PC・サーバの台数が多かったことに加え、一部 OS バージョンアップ作業に時間を要しました。
再発防止策	①ランサムウェア攻撃を想定したバックアップ環境の構築 ②機器管理の詳細化

7. システムの復旧と安全性確保

7-1 クリーン化の実施

・当社は、攻撃者が侵害した可能性のある端末やサーバについて、EDR やフォレンジックツールを用いた徹底的なスキャンを行い、汚染が疑われる機器は廃棄または OS 再インストール等のクリーン化を実施しました。この作業により、脅威が残存している兆候は確認されておりません。

7-2 新規システム環境への移行

・復旧までに一定の時間を要しましたが、汚染の可能性を残した既存環境を部分的に修復するのではなく、安全が確認された新しい環境をゼロから構築する方式を採用しました。

7-3 安全確認の実施

・外部専門機関と協働し、基幹業務システム・フロントシステム等についても徹底調査し、侵害有無を精査した結果、その他の主要システムが侵害された事実は確認されず、安全性が確保されていることを確認しました。

8. セキュリティ強化のロードマップ

フェーズ	短期（発生～数週間）	中期（数週間～数か月）	長期（半年～）
目指す姿	封じ込めと安全確保	仕組みの高度化	成熟度向上と運用定着
対応事項	✓ 不正アクセス経路の遮断 ✓ 感染端末の隔離 ✓ 全アカウントのパスワード変更 ✓ 全端末のEDR強化 ✓ 残存脅威調査・対策 ✓ MFAの徹底	✓ SaaSログ監視の強化 ✓ EDR／メールセキュリティ／ネットワーク防御等の継続的強化 ✓ SOC※1 24/365管理高度化 ✓ IT/OT ※2（物流設備）の統合的横断的リスク管理の高度化 ✓ セキュリティ研修プログラムの高度化（ロール別）	✓ 不正アクセスを防ぐ仕組み・運用ルールを含むセキュリティ対策の継続的アップデート ✓ ランサムウェア事案を踏まえたBCP（事業継続計画）の見直し・強化 ✓ 外部専門機関による定期的なアセスメント実施

8-1 短期フェーズ（封じ込めと安全確保）

・短期フェーズでは、不正アクセス経路の遮断、EDR 強化や残存脅威調査・対策、MFA の徹底など、早期の封じ込めと安全性確保を最優先としました。

8-2 中期フェーズ（仕組みの高度化）

・中期フェーズでは、監視体制の 24/365 管理高度化、権限管理フレームワークの見直し、従事者に対する教育体系の強化など、運用基盤の強化を重点的に進めています。

※1 Security Operation Center：ネットワークの監視を行い、リアルタイムで脅威を検知・対処する役割を担うサイバーセキュリティの専門組織チーム

※2 Operational Technology(運用技術)

8-3 長期フェーズ（成熟度向上と運用定着）

・長期フェーズでは、不正アクセスを防ぐ仕組み・運用ルールを含むセキュリティ対策の継続的アップデートやランサムウェア事案を踏まえた BCP（事業継続計画）の見直し・強化、外部専門機関による定期的なアセスメント実施等、長期的なセキュリティ基盤の成熟度向上を進めてまいります。

9. NIST フレームワークに基づくセキュリティ強化

・高度化するサイバー攻撃を早期に検知し対応するため、米国標準技術研究所（NIST）が定めたサイバーセキュリティ基準（※）に基づき、現在のセキュリティレベルを多角的に評価し、必要な強化ポイントを体系的に洗い出しました。これにより、管理策の妥当性や必要な改善点を明確化しました。

【主な強化施策例】

（1）アクセス制御強化（AC-17）

・全リモートアクセスの MFA 必須化

・セッション記録・アクセスログの分析強化

（2）検知能力強化（AU-2）

・SOC の監視強化

・資産の整合性監視の強化

※NIST CSF：NIST が策定した、組織がサイバーセキュリティリスクを管理・軽減するためのフレームワーク（Cybersecurity Framework）

NIST SP800 シリーズ：NIST が発行するサイバーセキュリティおよび情報システムに関するガイドラインや標準コレクション

10. セキュリティガバナンス体制の再構築

本件を通じて再認識した高度化するサイバー攻撃の脅威を踏まえ、リスク管理体制、全社的な統制・役割分担の明確化など、改善・強化すべき点を中心に、今期（2026 年 5 月期）中にセキュリティガバナンス体制の再構築を進めてまいります。

11. 情報公開方針と外部連携

11-1 攻撃者との接触と身代金支払に関する方針

・当社は、犯罪行為を助長させないという社会的責任の観点から、攻撃者とは接触しておらず、身代金の支払いはもとより、いかなる交渉も行っておりません。

11-2 透明性を重視した情報発信

・事実に基づく透明性の高い情報発信を基本とし、ステークホルダーの皆様に対して適切な時期に必要な情報を開示してまいります。ただし、攻撃手口の模倣や追加攻撃を含む二次被害防止の観点から詳細の開示を

控えさせていただく場合がございます。

11-3 外部ステークホルダーとの連携

・警察や個人情報保護委員会など関係監督官庁に対し、早期報告を行っております。また、本件を通じて得られた知見を社会全体のセキュリティ強化に還元することが重要であると考え、外部ステークホルダーとの積極的な連携を進めています。

・インシデント共有コミュニティ（例：JPCERT/CC※）への情報提供
：他社・他組織の防御力向上に寄与し、国内のサイバーセキュリティ水準の向上に貢献してまいります。

・サプライチェーン全体への情報共有
：サプライチェーン全体の安全性向上を目的として、必要な情報を適切に共有してまいります。

・今後も、官民連携の枠組みや外部専門機関との協働を強化し、当社のみならず社会全体のサイバー攻撃による被害抑止に資する活動を継続してまいります。

※Japan Computer Emergency Response Team Coordination Center

12.業績への影響

すでにお知らせのとおり、本件により財務数値の精査に十分な時間を確保する必要が生じましたため、第 2 四半期決算発表を延期する判断をいたしました。関係者の皆様にはご迷惑をおかけし、深くお詫び申し上げます。発表時期は改めてお知らせいたします。

以上

【参考：これまでの発表】

2025 年 10 月 19 日：ランサムウェア攻撃によるシステム障害を確認、プレスリリース（第 1 報）を発表
2025 年 10 月 22 日：調査状況とサービス現況（第 2 報）を発表
2025 年 10 月 29 日：一部商品の出荷トライアル運用開始（第 3 報）を発表
2025 年 10 月 31 日：一部報道について（第 4 報）を発表
2025 年 10 月 31 日：情報流出に関するお詫びとお知らせ（第 5 報）を発表
2025 年 11 月 6 日：サービスの復旧状況について（第 6 報）を発表
2025 年 11 月 11 日：情報流出に関するお知らせとお詫び（第 7 報）を発表
2025 年 11 月 12 日：サービスの復旧状況について（第 8 報）を発表
2025 年 11 月 14 日：3PL 事業に関する情報流出可能性について（第 9 報）を発表
2025 年 11 月 19 日：サービスの復旧状況について（第 10 報）を発表
2025 年 11 月 28 日：サービスの復旧状況について（第 11 報）を発表
2025 年 12 月 3 日：サービスの復旧状況について（第 12 報）を発表
2025 年 12 月 12 日：ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告
（第 13 報・本リリース）を発表