アスクルのサイバーセキュリティ

ASKUL

お客様の安心・安全を守り、「うれしい」を届け続けるために。

発生内容のご報告

アスクルは2025年10月19日、外部からの不正アクセスによりランサムウェアに感染し、サービスが一時的に停止するとともに、お客様情報・一部のお取引先情報が外部へ流出いたしました。

対象のお客様には、個別にお詫びのご連絡を差し上げておりますが、改めて、お客様情報を流出させてしまいましたことを深くお詫び申し上げます。

【アスクル 情報流出専用お問い合わせ窓口】(平日のみ・受付時間 9時～17時)

TEL：0120-023-219

050 で始まる IP 電話から：03-6731-7879(通話料はお客様ご負担)

発生から現在までの流れ

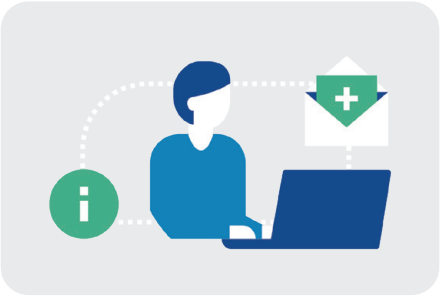
発生日	対応状況
10月19日	攻撃検知、ネットワーク遮断、 全パスワード変更に着手、サービスの停止
10月22日	外部クラウドサービスへの不正アクセス発生
10月23日	主要な外部クラウドサービスのパスワード変更完了
10月31日	外部に公開された情報を確認
11月11日	外部に公開された情報を確認
12月　9日	外部に公開された情報を確認

※アスクルは、LOHACO 決済においてお客様のクレジットカード情報を受け取らない仕組みとしており、個人のお客様のクレジットカード情報は保有しておりません。

3つの重要な取り組み

アスクルはお客様に安心・安全にサービスを使い続けていただくために、以下の3つの重要な取り組みを実施いたします。

01 情報開示



必要な情報を、わかりやすくお伝えします。

対策の状況や復旧の進捗を、お客様にとって分かりやすい形で丁寧にお知らせします。

02 安全対策

安心してご利用いただけるサービスへ。

セキュリティ・仕組み・体制を根本から強化し、お客様の情報を守り、安心してご利用いただけるサービスを実現します。

03 今後のセキュリティ強化

より強い基盤づくりを進め、改善を続けます。

今回発生した内容を教訓として、システムや運用を継続的に改善し、セキュリティ基盤の成熟度向上を進めていきます。

安全対策

今回の攻撃を受け、アスクルでは以下の対策を速やかに実施しております。

- ✓ 感染の疑いのあるシステム・ネットワークの分離
- ✓ 感染端末と感染サーバの隔離
- ✓ セキュリティ監視運用の強化
- ✓ 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
- ✓ プログラムのタイムスタンプ異常の点検
- ✓ 認証情報のリセット
- ✓ アカウントのパスワード変更
- ✓ 管理アカウントのMFA(※1)
- ✓ ランサムウェア検体抽出、およびEDR(※2)シグネチャ更新

安全な"新しい環境"でサービスをご提供

今回攻撃の影響を受けて問題が発生したサーバや機器がつながらないようにネットワークを分離し、安全なネットワークのみで新しい構成として整理しました。

安全なサービスを速やかに再開することを目指し、最適な形で各システムの再構築を行いました。お客様に安心してご利用いただけるよう、引き続き安全対策を最優先に復旧を進めてまいります。

これらの対応により、攻撃の広がりは封じ込められ、現在のシステムは安全に稼働している状態であることを確認しています。

※1 Multi Factor Authenticationのこと。多要素認証。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。
※2 Endpoint Detection and Responseのこと。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。

今後のセキュリティ強化

アスクルは今回の発生内容を受け、今後、より強いセキュリティ体制を築くための取り組みを積極的に進めていきます。

中期的な対策 再発を防ぐための仕組みづくり

日々の運用レベルから仕組みを強化し、
“気づける・防げる・対応できる”体制へと進化させます。

- 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(※3)24/365管理高度化
- IT/OT(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)

長期的な対策 セキュリティ基盤の成熟度向上

根本から強いサービス基盤を構築し、
”より強いサービス”をつくるための継続的アップデートを行います。

- 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

※3 Security Operation Centerのこと。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。

アスクルお客様サービスデスク 0120-345-861 携帯電話からもご利用いただけます。
●受付時間：月曜～土曜日(午前９時～午後６時)※日曜祝日は休業
●IP 電話からのお問い合わせ TEL03-6731-7864(通話料はお客様のご負担となります。)
※お電話のおかけ間違いにはご注意ください。

ソロエルアリーナお客様サービスデスク 0120-115-844 携帯電話からもご利用いただけます。
●受付時間：月曜～土曜日(午前９時～午後６時)※日曜祝日は休業
●IP 電話からのお問い合わせ TEL03-6731-7871(通話料はお客様のご負担となります。)
※お電話のおかけ間違いにはご注意ください。

掲載内容は2025年12月12日時点のものです。

アスクル株式会社 東京都江東区豊洲3-2-3