セキュリティインシデント事例③
最近のトピック

Ver. 1.0.0

Edgecross コンソーシアム　テクニカル部会　セキュリティ WG

テクニカル部会　セキュリティWG
参加企業(敬称略、順不同)

株式会社立花エレテック

日本電気株式会社

三菱電機株式会社

Musarubra Japan 株式会社

日本マイクロソフト株式会社

TXOne Networks Japan 合同会社

フエニックス・コンタクト株式会社

株式会社 Empress Software Japan

アイレット株式会社

改定履歴

Ver.	改定内容	発行年月
1.0.0	初版発行	2024 年 10 月

目次

1. サプライチェーン対策

はじめに

概要

製造業におけるサプライチェーンを含めたセキュリティ対策は非常に重要な課題の 1 つとなっています。DX や IT 化の推進により製品製造は一社で完結することなく、関連会社、子会社取引先からの物品調達や納品など関係する会社は非常に多くなります。また、サプライチェーンには製造にかかわるサプライチェーンとして物品調達、納品だけに関わらず外部サービスを利用した連携やソフトウェア連携なども含まれます。そのため、製造業においてサプライチェーンへのセキュリティ対策を適用することは喫緊の課題と言えます。

用語

用語	説明
セキュリティインシデント	マルウェア感染や情報窃取など、セキュリティ上の問題である事象。
脆弱性	プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥。
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
ランサムウェア	身代金の要求を目的としたマルウェア。

参照情報

本ドキュメントは下記サイトの情報を基に作成しています。

- 2023 年、サプライチェーンにおけるセキュリティリスク動向～被害事例にみる企業が直面するリスクとは？
  https://www.trendmicro.com/ja_jp/jp-security/23/k/securitytrend-20231113-01.html

サプライチェーン攻撃

サプライチェーン攻撃の種類

サプライチェーン攻撃は、攻撃の手口から下記の 3 つに分類されます。いずれもサプライチェーンにおいて標的組織へ侵入するために組織やソフトウェアなどの脆弱なポイントを狙って攻撃を仕掛けるサイバー攻撃となります。

- ビジネスサプライチェーン攻撃:
  関連組織や子会社、取引先などを侵害し、標的組織への侵害を図る攻撃
- サービスサプライチェーン攻撃:
  サービス事業者を侵害し、サービスを通じてその顧客に被害を及ぼす攻撃
- ソフトウェアサプライチェーン攻撃:
  ソフトウェアそのものやアップデートプログラムなどに不正コードを混入し、標的組織に侵入する攻撃

サプライチェーン攻撃による影響

サプライチェーン攻撃を受けた場合、自社への侵入は発生しなかった場合でも物品調達に影響が出るなど、結果的に自社製品の製造への影響が発生する場合があります。また、製造への影響だけではなく、攻撃を受けた会社が保持している自社顧客情報の漏洩や自社サービスの停止など二次的な被害を受ける可能性があります。

サプライチェーン攻撃への対策が難しい理由の 1 つに自社のサイバーセキュリティ対策が万全であったとしてもサプライチェーンを構成する企業やサービス、ソフトウェアの一部に脆弱なポイントがあれば、その脆弱なポイントを突かれ攻撃を受けてしまう可能性があります。実際に 2022 年に発生した部品製造業者への侵害により、自動車製造にかかわる工場すべてが停止したという事例も発生しています。

サプライチェーン攻撃による影響は非常に大きくなる可能性を含んでおり、自社へのサイバーセキュリティ対策だけではなく、自社が利用するサプライチェーンすべてへの対策を行っていくことが必要と言えます。

サプライチェーン攻撃被害事例

ビジネスサプライチェーン攻撃事例

トレンドマイクロが行った集計（集計期間：2023 年 1 月～2023 年 10 月 31 日）において、日本国内で公表されたセキュリティインシデントは 316 件で、うち 4.4%となる 14 件がサプライチェーン攻撃によるものでした。14 件はいずれも、取引先や関係先を踏み台に、ネットワークや共有しているシステムを介して被害組織に侵入するビジネスサプライチェーン攻撃でした。これらのビジネスサプライチェーン攻撃を詳しくみると、様々な業種が被害対象となっていることが分かります（表 1）。注目すべきは、その被害です。8 割以上でシステム停止が発生しています。サプライチェーン攻撃が事業継続に影響を与えるセキュリティリスクとなる確率が高いことが分かります。また、表の 2～10 の被害は、海外拠点へのサイバー攻撃を発端に、本社、グループ会社および関連会社へとランサムウェア（Lockbit）の感染被害が拡散した事例です。サイバー攻撃がサプライチェーンを構成するネットワークを悪用して侵害範囲を拡大した場合に、被害が甚大なものになる可能性があることを象徴する事例と言えます。

表 1 国内で公表されたビジネスサプライチェーン攻撃の被害事例

No	発覚/発表	業種/業界	被害	発覚原因	攻撃に使われた手口
1	2023 年 1 月	運輸・交通・インフラ	情報漏洩	未公表	ネットワーク共有していたサーバに侵害
2	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
3	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
4	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
5	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
6	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
7	2023 年 1 月	水産・農林・鉱業	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
8	2023 年 1 月	水産・農林・鉱業	障害発生（システム停止）、データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア（Lockbit）
9	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊	攻撃者による通知	ランサムウェア（Lockbit）

10	2023 年 1 月	製造	障害発生（システム停止）、データ改ざん/破壊	攻撃者による通知	ランサムウェア（Lockbit）
11	2023 年 1 月	建設・不動産	障害発生（システム停止）、データ改ざん/破壊	攻撃者による通知	ランサムウェア（Lockbit）
12	2023 年 4 月	製造	障害発生（システム停止）、情報漏洩	自己調査	ファイルサーバ侵害
13	2023 年 5 月	製造	情報投影	未公表	海外アカウント経由のクラウドプラットフォームへの侵害
14	2023 年 6 月	製造	障害発生（システム停止）、情報漏洩	自己調査	なりすまし

ビジネスサプライチェーン攻撃には至ってないものの、海外拠点などサプライチェーンを構成する関係先がサイバー攻撃を受けたことで、自社の情報が漏洩や、一時的なシステム停止を余儀なくされるなどサプライチェーンリスクが顕在化した事例も 16 件確認できました。そのうち半数以上は、海外拠点やグループ会社など自社傘下へのサイバー攻撃が発端でした（図 1）。サプライチェーンのセキュリティでは、業務委託先や調達先などの取引先など、自社以外への対策がまず話に上がることも多いですが、2023 年の被害動向をみると、自社が保有する拠点においてもセキュリティ対策の改善余地が残されているケースが多いことが分かります。

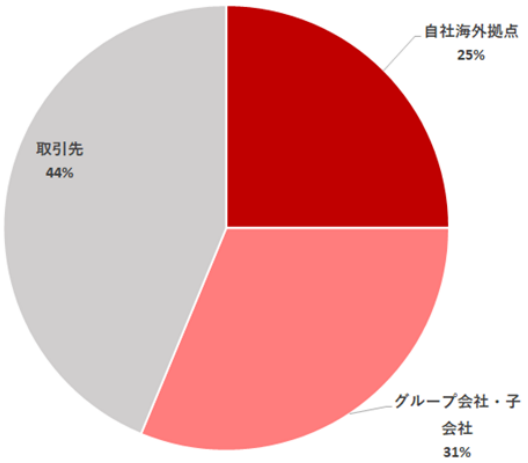

図 1 取引先や関連会社のサイバー攻撃によりセキュリティ被害が発生した事例

トレンドマイクロが行った調査期間中、IT サービスを介し、被害組織のネットワーク内部に侵入されるような「サービスサプライチェーン攻撃」について、この期間に公表内容から明確に判断される被害はありませんでした。しかし、利用している IT サービスがサイバー攻撃を受けることにより、二次的なセキュリティ被害を受けた事例は 40 件にも上りました。法人組織で広く利用される IT サービスがサイバー攻撃を受けることで、被害が広がる事例が多数確認されています。

表 2 IT サービスへのサイバー攻撃事例と利用社への影響

攻撃	被害事例
大手電気機器メーカーの提供するインターネットサービスへの不正アクセス	サービス利用社の通信情報の外部流出（2023 年 2 月）
エネルギー事業者向け管理システムへのマルウェア攻撃	システム利用社のユーザー向けサービスの停止（2023 年 6 月）

オンライン旅行会社が提供する宿泊予約情報管理システムへの不正アクセス	宿泊施設の顧客情報の漏洩、また顧客へのフィッシングサイトに誘導するメッセージ配信（2023 年 6 月～2023 年 8 月）
ウェブサイト向けのマーケティングツールへの不正アクセス	ツールのソースコードの書き換え、これによるツール利用社のウェブサイトに入力された顧客情報の漏洩（2023 年 1 月）
社会保険労務士（社労士）向けシステムへのランサムウェア攻撃	利用する社労士事務所および委託する給与計算など業務への影響（2023 年 6 月）

サプライチェーン攻撃への対策ポイント

3 種類のサプライチェーン攻撃には、それぞれの特性に応じた対策が必要となります。

ビジネスサプライチェーン攻撃対策

ビジネスサプライチェーン攻撃に対しては、表 3 のポイントで対策を検討することを推奨します。

表 3 ビジネスサプライチェーン攻撃対策

ポイント	内容
リスク評価	関係先のセキュリティレベルの確認や侵害された場合の影響を評価
セキュリティレベル標準化	サプライチェーンを構成する関係先とのセキュリティレベル標準化の要請
情報の確認	サプライチェーンを構成する関係先とのネットワーク接続点や共通システムにおけるセキュリティ対策状況や取り扱う情報の確認

サービスサプライチェーン攻撃対策

利用している外部サービスからのサプライチェーン攻撃を防ぐため、表 4 のポイントで対策を検討することを推奨します。

表 4 サービスサプライチェーン攻撃対策

ポイント	内容
サービス棚卸	利用しているサービスの内容やセキュリティ対策状況を把握
責任範囲の確認	ベンダーやサービス選定基準、評価方法の見直しと定期的な監査
インシデント対応プラン策定	サービス障害時を想定した対応プランの作成

ソフトウェアサプライチェーン攻撃対策

自社製品に組み込まれるソフトウェアを経由した攻撃を防ぐため、表 5 のポイントで対策を検討することを推奨します。

表 5 ソフトウェアサプライチェーン攻撃対策

ポイント	内容
セキュリティを意識した企画/設計	自社のサービス、システム開発において、企画段階にセキュリティを組み込むシフトレフトの採用
SBOM の活用	SBOM（Software Bill of Materials：ソフトウェア部品表）を作成し、自社サービスで利用しているソフトウェアの把握

Edgecross 基本ソフトウェア使用時に注意すべきこと

Edgecross 基本ソフトウェアの利用により情報を収集、可視化できますが、それは即ち、様々な機器が接続されることになります。そのため、マルウェア感染などが発生した場合、つながる機器への感染拡大のリスクが高まり、それは自社内だけでは済まない可能性もあります。そのため、Edgecross セキュリティガイドラインなどを参照し自社内外へ統一されたセキュリティポリシーの適用を行っていくことが重要となります。

また、セキュリティ対策は一度行えば終わりというわけではなく、最新の脅威に対応するために定期的な見直しと変更、強化も必要となります。

2. 製造業において可視化が重要な理由

～セキュリティ運用支援のための可視化～

はじめに

概要

工場内にてサイバー攻撃が発生した際、攻撃による工場設備や生産への影響を推測し、迅速かつ適切な対処をするため、攻撃による被害範囲の確定を早急に行う必要があります。工場における可視化（見える化）は、セキュリティの観点でも必要な取り組みとなります。

用語

用語	説明
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
NDR	《Network Detection and Response》 ネットワークの全体を監視し、脅威の検知・対処をする仕組み。
IDS	《Intrusion Detection System：侵入検知システム》 コンピュータやネットワーク上で発生するイベント(各種アクセス／処理実行、ログ出力、通信データなど)を監視・分析することで、偵察行為や不正侵入と考えられる兆候を検知・通知する仕組み。

参照情報

本ドキュメントは下記のドキュメントを参考に作成しています。

- 工場セキュリティガイドライン 概要編（東京大学 グリーンICTプロジェクト・Edgecrossコンソーシアム 合同 工場セキュリティWG）
  https://www.edgecross.org/ja/data-download/pdf/ECD-TE4-0009-02-JA.pdf

セキュリティ対策としての可視化

なぜ可視化が重要なのか

工場内にてサイバー攻撃が発生した際、攻撃による工場設備や生産への影響を推測し、迅速かつ適切な対処をするため、攻撃による被害範囲の確定を早急に行う必要があります。工場内にどういった機器が、どのように接続されているかを把握できていないと、被害範囲を確定することは困難です。また、すべての機器に対して対策が実施されたかを把握することができず、工場内が安全な状態になったことを確認することができません。そのため、事前に工場内の機器、ネットワークの接続状態を把握することが肝要です。

工場内の可視化ができていない場合に想定される被害例

工場内の可視化ができていない場合、以下のような被害が想定されます。

1. OA 端末でメールに添付されているファイル（マルウェア）を開いてしまい、OA 端末がマルウェアに感染する。
2. OA 端末から工場内の Historian にマルウェアの感染が拡大する。
3. 工場全体にマルウェアが蔓延し、機器の稼働停止が頻発する。
4. 工場全体で同時多発的に稼働停止が発生しているため、対策を打つべき箇所が把握できず、工場の稼働停止が続く。
5. 工場の稼働停止が 1 週間続き甚大な事業被害が発生する。

可視化の種類

工場内で行う可視化には、「ネットワークの可視化」と「機器状態の可視化」があります。「ネットワークの可視化」とは、工場内にある機器を把握し、それらが工場内のネットワーク内で行う通信を可視化することを指し、「機器状態の可視化」とは、工場内にある機器の構成状況を可視化することを指します。

セキュリティ対策として行う可視化

セキュリティ対策として行う可視化について、説明します。

ネットワークにおける可視化

工場では、制御装置・機器を中心に、システム全体を統合的に制御するために、ネットワークを介して周辺機能と連携する構成となっていることが多く、セキュリティ対策として可視化を行う場合においてもこの特質を考慮する必要があります。

ネットワークにおける可視化としては、表 3 を参考に実施する内容を検討することを推奨します。

表 6 ネットワークにおける可視化の例

項目	内容
接続機器の把握	ネットワークに接続されている機器を可視化する。例えば、機器を把握するために資産管理ツールなどを活用する。許可なく接続された機器を把握するために NDR などを活用することも有効である。
通信監視・制御	通信状況の可視化や監視、異常検知を行う。例えば、通信状況の可視化や監視のために NDR を設置する。ネットワーク内で発生した異常を検知するために IDS を設置することも有効である。

機器における可視化

工場では、生産設備や計算機などの機器(以降、機器)には、サーバ、端末(PC)、プリンタ、高性能な機器などがあります。

機器における可視化としては、表 5 を参考に実施する内容を検討することを推奨します。

表 7 機器における可視化の例

項目	内容
ログ取得	機器のシステムログを取得する。取得したログは、攻撃発生時に被害範囲を確定するために使う。
構成管理	機器内の構成情報を可視化し、管理する。機器の構成を統合的に管理する構成管理ツールなどを活用する。

3. 脆弱性対策

はじめに

概要

サイバー攻撃はセキュリティ上の欠陥である脆弱性を悪用しているため、脆弱性が存在しなければサイバー攻撃は成功しないと言っても過言ではありません。それにも関わらずサイバー攻撃の被害が絶えないのは、脆弱性が潜在していたり、公表されている脆弱性の対処ができていなかったりするからです。その意味では、脆弱性対策はセキュリティ対策の基本中の基本と言えます。

本稿では、脆弱性の事例や、Edgecross 使用時に脆弱性の観点で注意すべきことを記載していますので、日々怠りなく脆弱性対策に取り組まれることを推奨します。

用語

用語	説明
脆弱性	プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥。
セキュリティパッチ	アプリケーションの脆弱性を解消するための修正プログラム。
バッファオーバーフロー	データの一時記憶領域であるバッファに対して、想定以上の長さのデータが入力されること。
パストラバーサル	本来アクセスできないディレクトリに存在するファイルに対して、脆弱性を悪用してアクセスする手法。

参照情報

本ドキュメントに脆弱性の事例は下記サイトの情報を基に作成しています。

- JVN iPedia 脆弱性対策情報データベース
  https://jvndb.jvn.jp/index.html

脆弱性対策

脆弱性とは

脆弱性とは、プログラムの不具合や設計上のミスが原因となって発生するセキュリティ上の欠陥のことです。

近年は工場にもマルウェアが侵入し、拡散活動をすることで工場の操業が停止する事案が度々発生しています。マルウェアは USB デバイスや持込み機器から侵入し、ネットワーク上にある機器の脆弱性を利用して、その他機器への感染拡大を図ります。

マルウェアの感染や拡散活動を抑えるためには、各機器の OS やアプリケーションなどの資産管理を適切に実施し、そのセキュリティパッチをタイムリーに適用することが求められます。

脆弱性の事例

様々な機器やソフトウェアにおいて脆弱性は日々見つかっており、脆弱性を放置しておくとサイバー攻撃を受ける危険性が高まります。そうした脆弱性の情報を収集するには、JPCERT/CC と IPA が共同で運営する JVN(Japan Vulnerability Notes)のポータルサイト JVN iPedia※が便利です。参考までに、JVN iPedia に登録されている脆弱性情報 のうち、FA の製品・OSS に関する 2024 年 1～4 月に公開された脆弱性の事例を表 8 に示します。

※JVN iPedia: https://jvndb.jvn.jp/index.html

表 8 FA 関連の脆弱性事例（2024 年 1～4 月）

No.	JVN iPedia 登録番号	対象	脆弱性
1	JVNDB-2024-003116	コントローラユーザ向けツール	・境界外読み取り ・バッファ開始位置にないポインタの開放
2	JVNDB-2024-003086	I/O ユニット	・不適切な入力検証
3	JVNDB-2024-003049	コントローラユーザ向けツール	・境界外書き込み ・境界外読み取り
4	JVNDB-2024-002942	コントローラ	・パストラバーサル
5	JVNDB-2024-002873	FA 製品	・不十分なリソースプールに起因するサービス運用妨害
6	JVNDB-2024-002852	制御システム向けソフト	・ファイル検索パスの制御不備
7	JVNDB-2024-002579	生産システム向けソフト	・NULL ポインタデリファレンスに関する脆弱性
8	JVNDB-2024-002399	CPU ユニット	・不適切な権限設定
9	JVNDB-2024-002215	制御システム向けソフト	・ハードコードされた認証情報の使用
10	JVNDB-2024-002282	コントローラ	・バッファエラー
11	JVNDB-2024-001162	コントローラ	・Capture-replay による認証回避
12	JVNDB-2024-001025	OPC UA ツール	・ログ出力内容の不適切な無害化
13	JVNDB-2024-001004	コントローラソフト	・スタックベースのバッファオーバーフロー
14	JVNDB-2024-001001	コントローラユーザ向けツール	・スタックベースのバッファオーバーフロー ・ メモリバッファエラー

Edgecross 使用時に注意すべきこと

(1) Edgecross 基本ソフトウェア

脆弱性を無くすため Edgecross 基本ソフトウェアは最新版を利用するようにしてください。セキュリティパッチの適用やバージョンアップは動作検証の上、実行することを推奨します。

Edgecross 基本ソフトの最新版は Edgecross のマーケットプレイス上で公開していますので参考にしてください。

(2) エッジアプリケーション、データコレクタ、IT ゲートウェイ

エッジアプリケーション、データコレクタ、IT ゲートウェイについては Edgecross の会員企業が開発していますので、その開発元やマーケットプレイスから情報を入手して脆弱性対策をしてください。

セキュリティパッチの適用やバージョンアップは動作検証の上、実施を推奨します。

Edgecross マーケットプレイス： https://www.marketplace.edgecross.org/

(3) OSS

OSS の脆弱性の対処はユーザに委ねられます。OSS の情報入手し、動作検証の上、アップデート作業を実施してください。

特に、PostgreSQL、PSQLODBC.DLL は Edgecross 基本ソフトウェアが使用する OSS です。

(4) Windows OS

Windows は、Windows Update により更新プログラムを適用して、常に最新の状態に保つための機能が備わっています。汎用的に利用する環境では常に最新の状態に更新することを推奨します。

ただし、更新プログラムには、再起動を伴うもの、更新に時間がかかるものがあります。動作環境と相性の問題や、不具合があるものも存在するため、実際には Edgecross の運用に問題ないことを確認してから更新することを推奨します。

特定の用途で利用する産業用 PC などでは、更新プログラムの適用を一時延期し、更新プログラムの動作検証用に試験用機器を用意するなどの対策が有効です。Microsoft 社は組織内の Windows 更新プログラムの適用を制御するためのソリューションとして、Windows Server Update Services (WSUS)を提供しています。

Windows 更新プログラムの入手元として WSUS を選択する場合、グループ ポリシーを使って Windows PC を WSUS サーバに向けるように設定します。Windows Update から更新プログラムが定期的に WSUS サーバにダウンロードされ、WSUS 管理コンソールまたはグループ ポリシーを通じて管理、承認、展開され、企業の更新プログラムの管理が合理化されます。

4. ランサムウェア対策

はじめに

概要

OT 分野は、IT 分野と比較して、本来自動化に重点を置いているため、わずかな時間のダウンタイムであっても、業務上および財務上重大な損失を起こし、より脆弱になります。この脆弱性は、操業停止による被害コストが高くなり身代金支払いの可能性が高まることから、OT 分野を狙うサイバー犯罪者にとっては、特に魅力的に映っています。

2023 年には、BlackCat、LockBit、Medusa、CL0P などの有名なランサムウェアグループの活動が特に活発になり、それぞれが特定の分野を標的にしています。

参照情報

本ドキュメントは下記サイトの情報を基に作成しています。

- IT/OT の統合化がもたらす危機 2023 年の OT/ICS サイバーセキュリティレポート
  https://www.txone.com/ja/security-reports-ja/OT-ics-cybersecurity-2023/

ランサムウェア攻撃

ランサムウェアとは

近年、サイバー攻撃者が用いる手法は大きく変化し、かつてないほど高度で破壊的な攻撃が行われるようになりました。

ランサムウェアはデータを不正に暗号化することにより、データを利用不可能な状態にした上で、復元と引き換えに身代金を要求する悪質なマルウェアを指します。ランサムウェアによって暗号化されたファイルを復元することは、極めて難しく、仮に身代金を支払ってもファイルが元に戻る保証はありません。

さらに、ランサムウェアや侵入のためのツール一式をサービスとして提供する RaaS（Ransomware-as-a-Service）が登場し、高度な技術を持たない人でも対価を支払うことで簡単に攻撃を行える環境が整っており、ランサムウェアを使った攻撃が増える要因の1つとなっています。同一の RaaS 利用した攻撃者のグループをランサムウェアグループと呼びます。

データの暗号化だけではなく、データを窃取し公開することにより身代金の支払いを要求する二重脅迫、事業やサービスの遂行を妨害する三重脅迫、窃取したデータを使って顧客に連絡することにより評判を貶める四重脅迫といった多重脅迫が増加しており、攻撃はますます悪質化しつつあります。

ランサムウェア攻撃被害事例

ランサムウェア攻撃事例

2023 年以降 OT の分野は、LockBit、CL0P、BlackCat、Medusa など、主に RaaS グループによる高度なランサムウェア攻撃に増々さらされることとなりました。これらのグループは戦略を綿密化し、二重、三重の恐喝の手口に移行して、さまざまな業界で広範なデータ侵害を引き起こしています。

次表に 2023 年以降に発生したランサムウェア攻撃被害事例を示します。

表 9 ランサムウェア攻撃被害事例

発生時期	ランサムウェア	業種	被害状況	発生個所
2023 年 1 月	LockBit 3.0	製造業	海外現地法人で不正アクセス。	日本
2023 年 1 月	Sandworm	IT	複数のデータストレージシステム上のファイル破壊。	海外
2023 年 2 月	LockBit 3.0	インフラ	データ漏えいの脅迫。カスタマーサービスに影響したが、給水には影響なし。	海外
2023 年 3 月	Cl0p	インフラ	データ侵害。顧客データ等への影響はなし。	日本
2023 年 3 月	Stormous	製造業	ランサムウェアグループにより同社の 14%の企業データが流出。	日本
2023 年 4 月	LockBit 3.0	製造業	一部サーバーと PC 端末に感染が確認された。サーバーの停止、ネットワークの遮断、全システムの停止などを実施。	日本
2023 年 4 月	BlackByte	販売業	ランサムウェア被害について財務情報を含むデータのサンプルをランサムウェアグループによる Web サイト公開。	日本
2023 年 4 月	Money Message	製造業	ソースコードなどを盗み出し、約 6 億円の身代金要求。	海外
2023 年 5 月	Black Basta	製造業	数百台のデバイスが侵害。	海外
2023 年 5 月	LockBit 3.0	サービス業	ハッカーによる$ 300,000 の身代金要求。	日本

発生時期	ランサムウェア	業種	被害状況	発生個所
2023 年 6 月	LockBit	製造業	データの漏えい。発表では、個人情報・財務情報・知的財産は侵害されておらず、業務に重大な影響はなし。	日本
2023 年 6 月	Cl0p	製造業	データ漏えい。重要データは盗まれていないと発表あり。	海外
2023 年 6 月	Qilin	建設業	ハッカーによる 600GB 超のデータ盗難。	日本
2023 年 6 月	Cl0p	サービス業	従業員の個人データ約 6800 人分が漏えい。	日本
2023 年 6 月	Mallox	IT	ハッカーによる 60GB 超のデータ盗難。	日本
2023 年 7 月	LockBit 3.0	インフラ	サーバー暗号化によりによる大規模システム障害、3 日間の操業停止。	日本
2023 年 8 月	NoName	インフラ	鉄道の緊急停止など運行に支障。	海外
2023 年 8 月	Mallox	製造業	ハッカーによる 144GB のデータ盗難	日本
2023 年 9 月	BlackByte	製造業	一部サーバーでランサムウェアによる第三者の不正アクセス。攻撃検知直後にサーバーを停止し、隔離したが生産や配送などの業務に影響。	日本
2023 年 9 月	Ransomed.vc	通信業	100 万ドル以上の身代金要求。	日本
2023 年 9 月	BlackCat	製造業	顧客のエンジニアリング情報を含むビジネスとパートナーに関する機密データの流出。	日本
2023 年 9 月	Dark Angel	製造業	大量データの盗難、暗号。約 77 億円の身代金要求。	海外
2023 年 9 月	BlackCat	運輸業	ハッカーによるデータ盗難。サイバーセキュリティインシデントが	日本

発生時期	ランサムウェア	業種	被害状況	発生個所
			配送遅延につながったことも確認。	
2023 年 10 月	LockBit 3.0	製造業	大量のデータが漏えい。一部データは公開。	海外
2023 年 11 月	LockBit	製造業	検査データ、ラボテスト、財務文書などの重要データを盗まれ、身代金を要求。その後、データ流出。	日本
2023 年 11 月	Medusa	金融業	ヨーロッパとアフリカの一部のシステムで不正アクセスを検出。ハッカーがすべてのデータのファイルツリー構造を含む.TXT ファイルを含むサンプルデータを公開。	日本
2023 年 11 月	BlackCat	製造業	同社のグローバルウェブサイトはアクセス不能となり、一部のシステムは停止し、電子メールの送受信に遅延が発生した。	日本
2023 年 12 月	Akira	製造業	オーストラリアとニュージーランドにある同社のネットワークシステムの一部に、権限のない第三者が不正にアクセスしたことを確認した。	日本
2024 年 1 月	LockBit 3.0	製造業	ハッカーによるデータ盗難、一部データは漏えい。	日本
2024 年 2 月	LockBit 3.0	製造業	357GB の文書流出とデータのサンプルが公開された。	日本
2024 年 3 月	LockBit 3.0	製造業	複数業務用コンピュータのマルウェア感染、影響を受けたシステムをネットワークから切断。個人情報や顧客情報を含むファイルを盗難された可能性があることを発見された。	日本

発生時期	ランサムウェア	業種	被害状況	発生個所
2024 年 3 月	BlackCat	建設業	ハッカーによる5TB 超のデータ盗難、アップロードされた。	日本
2024 年 3 月	LockBit 3.0	製造業	ランサムウェア攻撃により、業務システムが暗号化された。	日本

Edgecross 基本ソフトウェア使用時に注意すべきこと

Edgecross 基本ソフトウェアの利用により情報を収集、可視化できますが、それは即ち、さまざまな機器が接続されることになります。そのため、マルウェア感染などが発生した場合、つながる機器への感染拡大のリスクが高まり、それは自社内だけでは済まない可能性もあります。そのため、Edgecross セキュリティガイドラインなどを参照し自社内外へ統一されたセキュリティポリシーの適用を行っていくことが重要となります。

また、セキュリティ対策は一度行えば終わりというわけではなく、最新の脅威に対応するために定期的な見直しと変更、強化も必要となります。

なお、下記ドキュメントの 5 章にも Edgecross で推奨されるランサムウェア対策が記載されていますので、参考にしてください。

- セキュリティインシデント事例① 半導体製造企業の事例
  https://www.edgecross.org/client_info/EDGECROSS/view/userweb/ext/ja/data-download/pdf/Security_incident_1.pdf