日本文紙データ交換機構　御中

SEDIO-VANにおける
文字コード変換（SJIS）対応について

2025年11月18日

株式会社JSOL
カスタマーエクスペリエンス事業本部

NTT DATA Group

アジェンダ

1．SEDIO-VANにおける文字コード変換（SJIS）対応について

【参考情報】

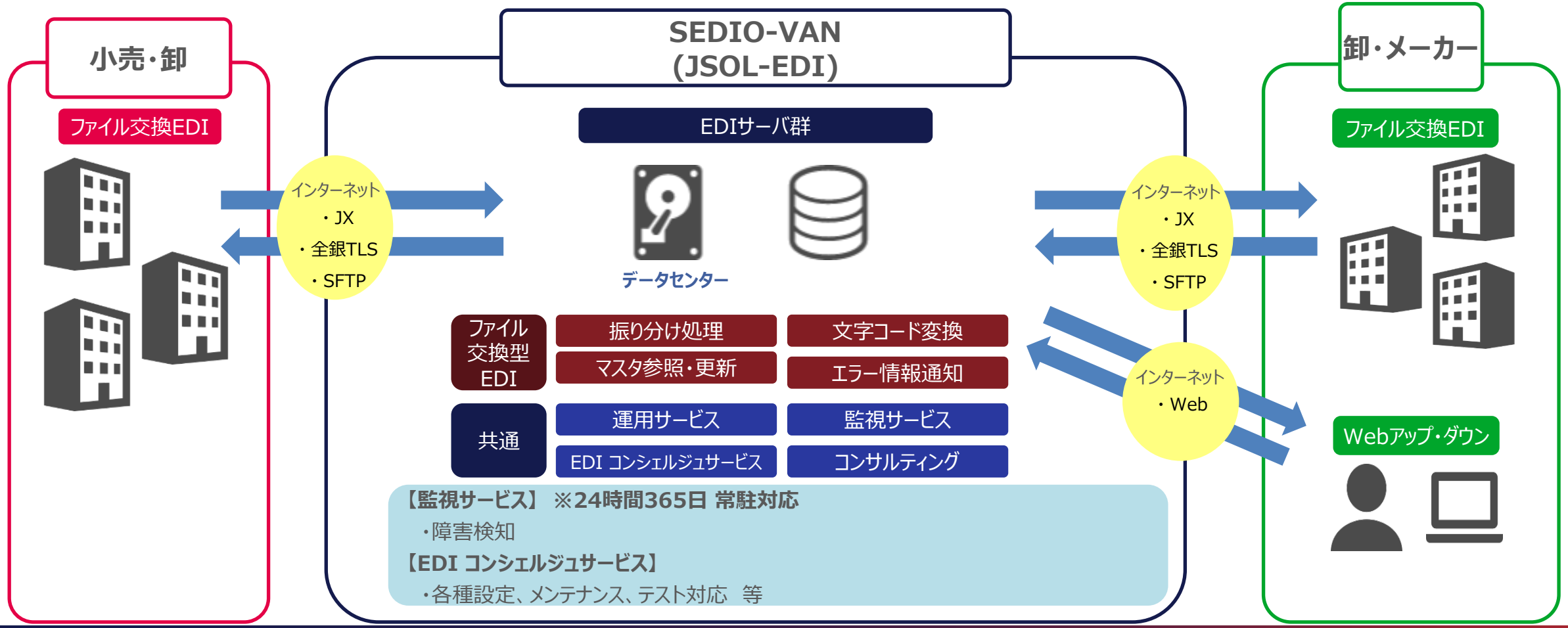
2．ランサムウェアについて

1. SEDIO-VANにおける 文字コード変換（SJIS）対応について

- SEDIO-VAN処理概要
- SEDIO-VANにおける振分けについて：標準仕様
- SEDIO-VANにおける振分けについて： IJS21の場合
- IJS21以外の通信手順への、文字コード変換の応用
- 今後のスケジュールおよび注意事項

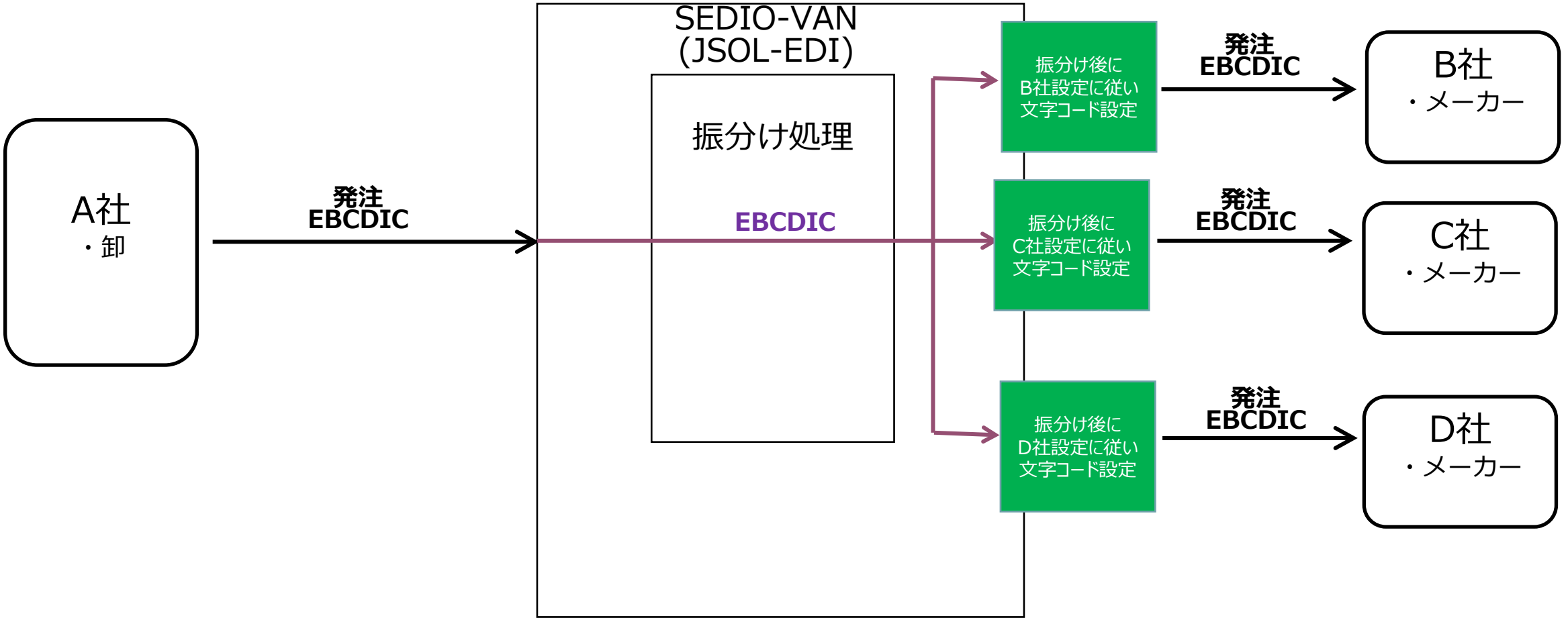
SEDIO-VAN処理概要

文具・紙製品業界のデータ交換システムで、小売店・卸店・メーカー間のデータ交換を行うことができるVANです。
SEDIO-VANでは、下記のとおり複数の通信手順によるデータ送受信を行い、振分け処理を行っています。
SEDIO-VANで送受信されるデータにおける文字コードの標準仕様は、“EBCDIC”となっておりますが、
IJS21を使用されているユーザー様はIJS21の仕様に則り、“SJIS”で送受信されています。



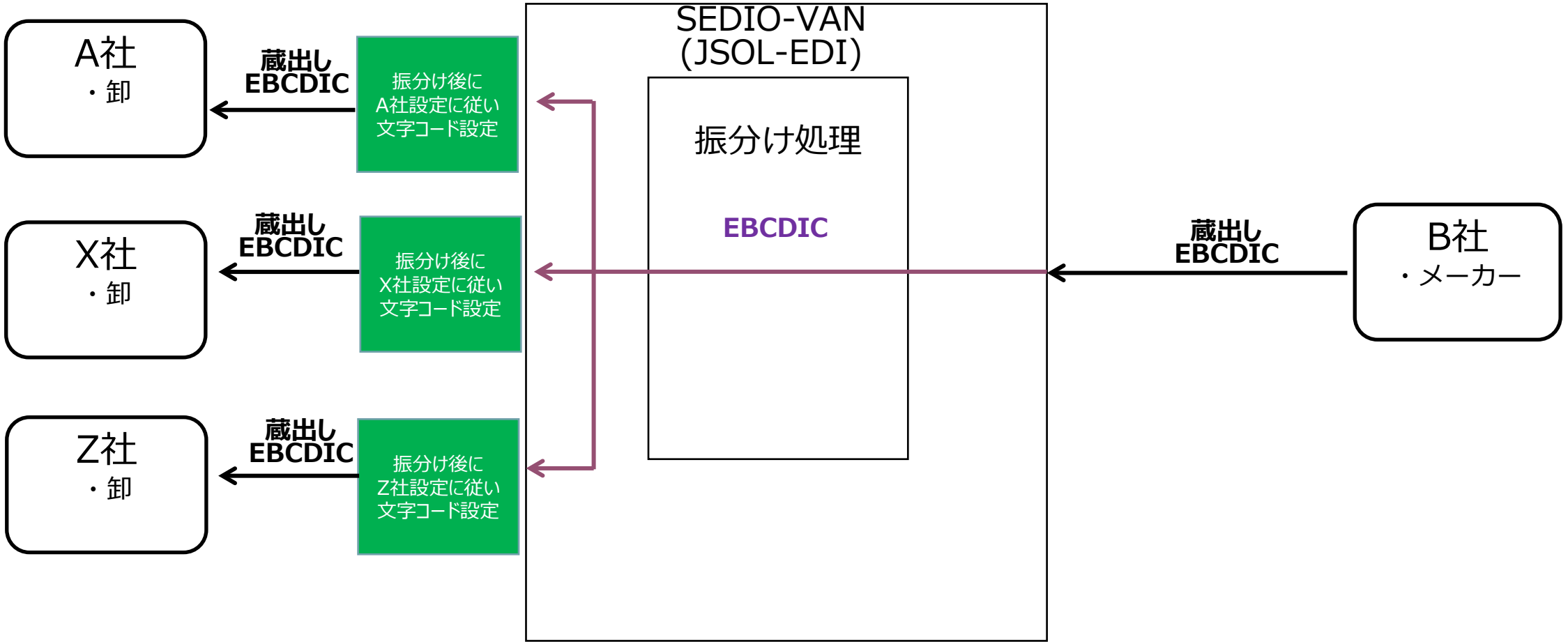
SEDIO-VANにおける振分けについて：標準仕様（卸様 ⇒ メーカー様）

SEDIO-VANに取り込まれたデータは、**EBCDICにて振分け処理**を行った後に、
受信側ユーザーの設定にしたがって文字コードを設定します。
受信側設定が“EBCDIC”であれば、SEDIO-VANの標準仕様＝EBCDICなので、何も変換せずにセットします。



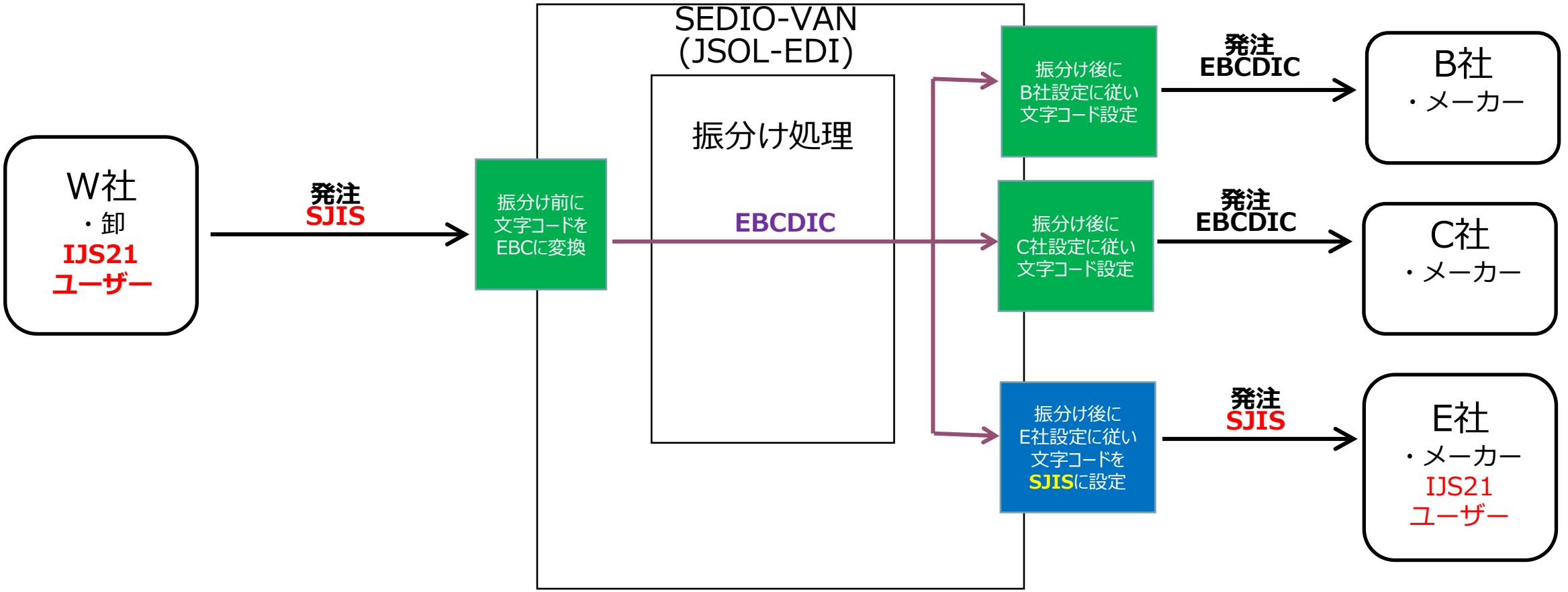
SEDIO-VANにおける振分けについて：標準仕様（　卸様　⇐　メーカー様）

SEDIO-VANに取り込まれたデータは、**EBCDICにて振分け処理**を行った後に、
受信側ユーザーの設定にしたがって文字コードを設定します。
受信側設定が“EBCDIC”であれば、SEDIO-VANの標準仕様＝EBCDICなので、何も変換せずにセットします。



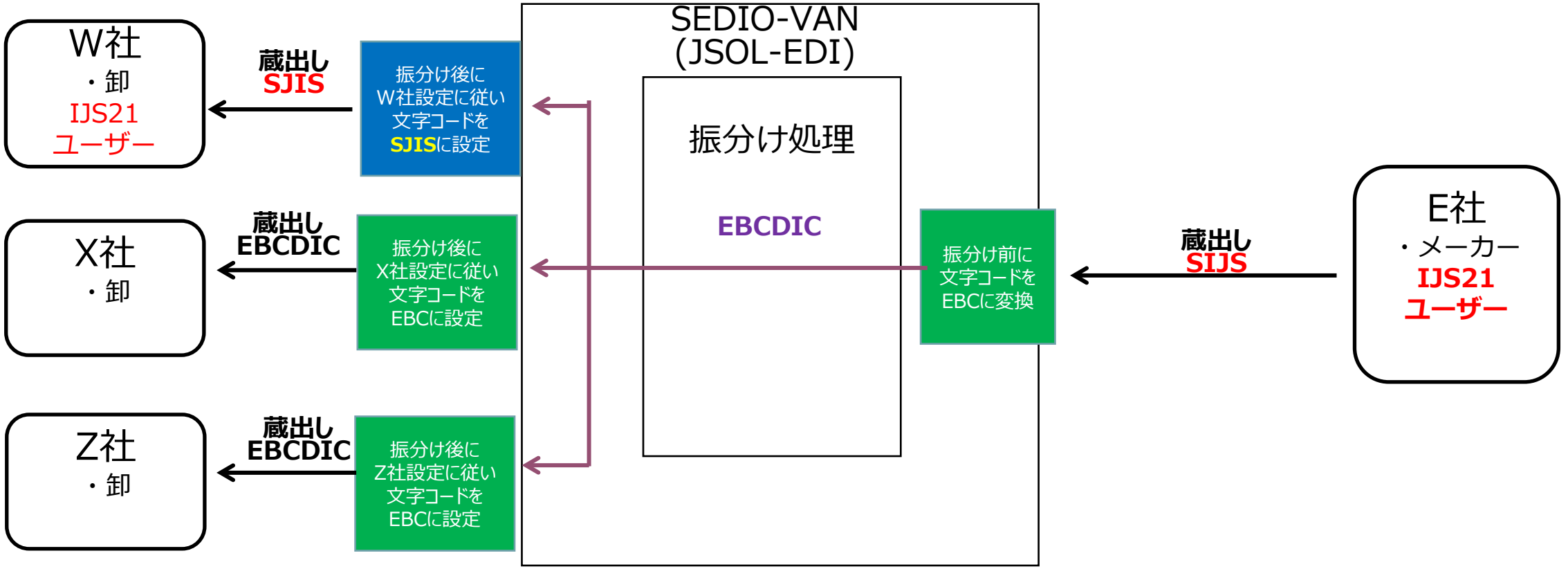
SEDIO-VANにおける振分けについて： IJS21の場合（卸様 ⇒ メーカー様）

W社（卸様）がIJS21ユーザーである場合、W社から送られてくるデータの文字コードは“SJIS”となっています。
この場合も、標準仕様と同様に、SEDIO-VANに取り込まれたデータは“EBCDIC”へと変換し、EBCDICにて振分け処理を行います。
受信側設定が“EBCDIC”であれば、SEDIO-VANの標準仕様＝EBCDICなので、何も変換せずにセットしますので、
送信側ユーザーの設定が、受信側ユーザーに影響する事はありません。
また、下図の様に受信側E社がIJS21を使用されている場合、受信側設定は“SJIS” になりますので、SJISに変換してセットされます。
送信側／受信側ともに、卸様／メーカー様の違いに伴う、文字コード変換の仕様の違いはありません。



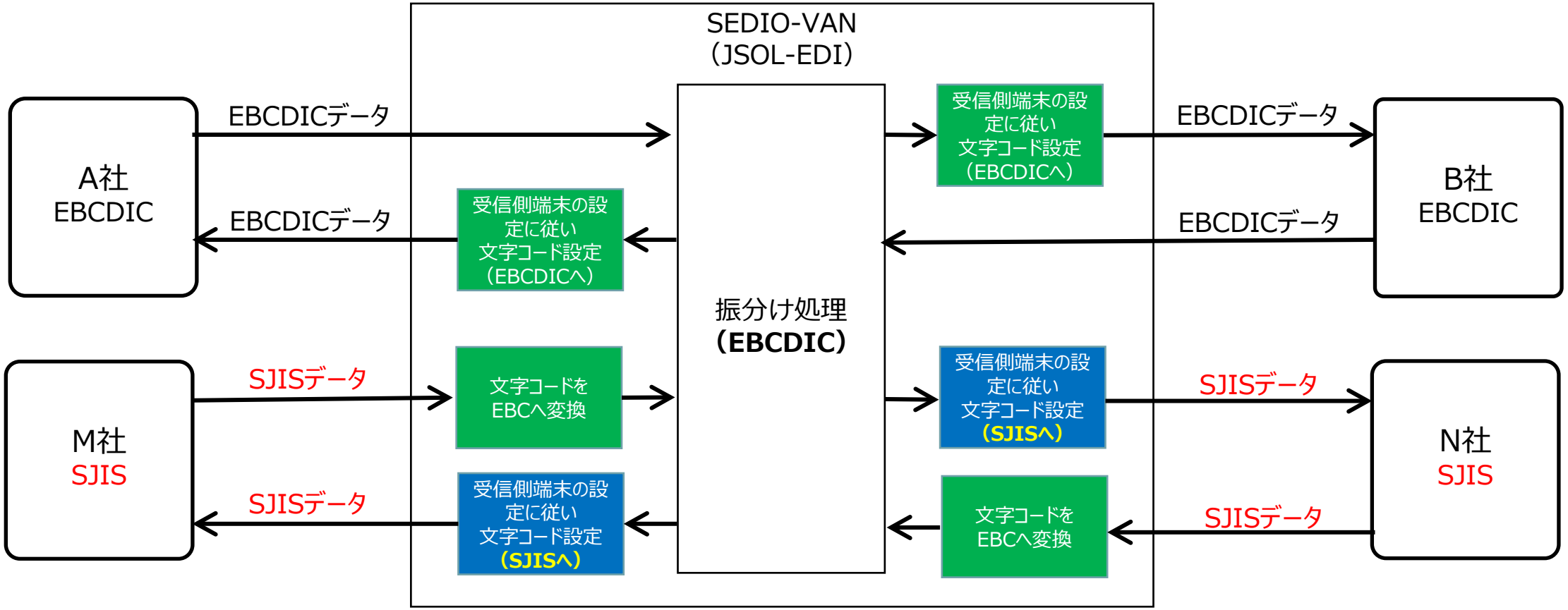
SEDIO-VANにおける振分けについて： IJS21の場合（卸様 ⇐ メーカー様）

E社（メーカー様）がIJS21ユーザーである場合、E社から送られてくるデータの文字コードは“SJIS”となっています。
この場合も、標準仕様と同様に、SEDIO-VANに取り込まれたデータは“EBCDIC”へと変換し、EBCDICにて振分け処理を行います。
受信側設定が“EBCDIC”であれば、SEDIO-VANの標準仕様＝EBCDICなので、何も変換せずにセットしますので、
送信側ユーザーの設定が、受信側ユーザーに影響する事はありません。
また、下図の様に受信側W者がIJS21を使用されている場合、受信側設定は“SJIS” になりますので、SJISに変換してセットされます。
送信側／受信側ともに、卸様／メーカー様の違いに伴う、文字コード変換の仕様の違いはありません。



IJS21以外の通信手順への、文字コード変換の応用

文字コード“SJIS”の利用を希望されるM社が、SEDIO-VANに新たに入会された場合、
または既存ユーザーで“EBCDIC”を利用されていたN社が、“SJIS”への変更を希望された場合、
前述までの文字コード変換設定をご利用されることで、取引先様の設定に影響することなく、SJISデータでの送受信が可能になります。
※使用される“SJIS”データについて、以下の点をご注意ください。
１）データフォーマットについて：SEDIO標準フォーマットを遵守しているデータであること。
２）レコード長について：“EBCDIC”使用時は128バイトですが、“SJIS”使用時は改行コード（CRLF）を含めた130バイトとなります。



今後のスケジュールについて

文字コード変更機能拡張の拡張について、今後の対応事項・スケジュールは、以下のように想定しています。

No	対応項目	想定時期
1	申請書の改訂	2025年12月
2	サービス開始時期	2026年01月頃
3	SEDIO様ホームページへの掲載	要調整
4	SEDIO-VANユーザー様アナウンス	要調整

2. ランサムウェアについて

- はじめに
- 現状の脅威
- 被害リスク
- 被害事例
- 攻撃手法の理解
- 防御策と予防

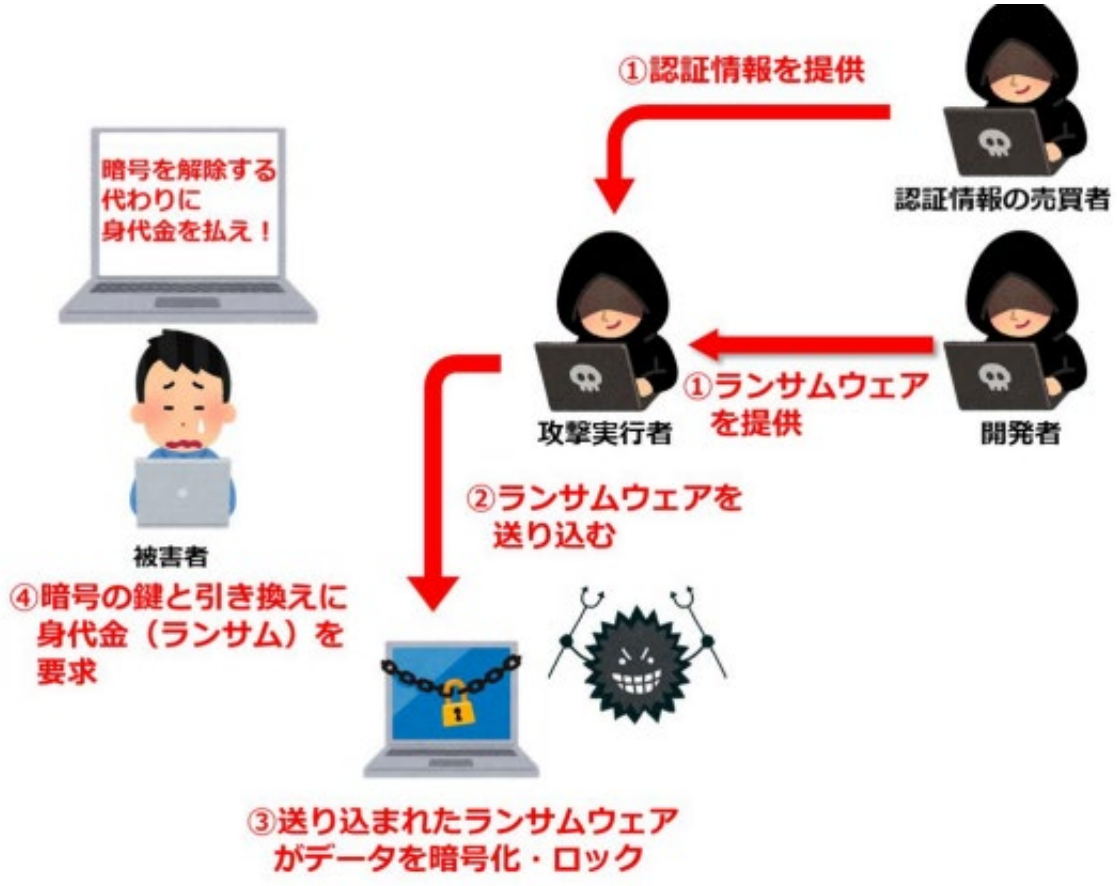
はじめに

ランサムウェアとはサイバー攻撃の一種で以下のようなものを指します。

・Ransom：身代金
・Software：ソフトウェア

ランサムウェアとは上記の言葉を組み合わせた言葉で、
パソコン等に保存されているデータを暗号化して
使用できない状態にした上で、
そのデータを復号および窃取したデータの非公開を条件に
対価（金銭や暗号資産）を要求する不正プログラムです。

感染するとデータが暗号化されたことで、
システムが動作しなくなり**業務が停止**してしまう場合があります。
また攻撃者により窃取されたデータ、個人情報などが
流出するケースもあります。

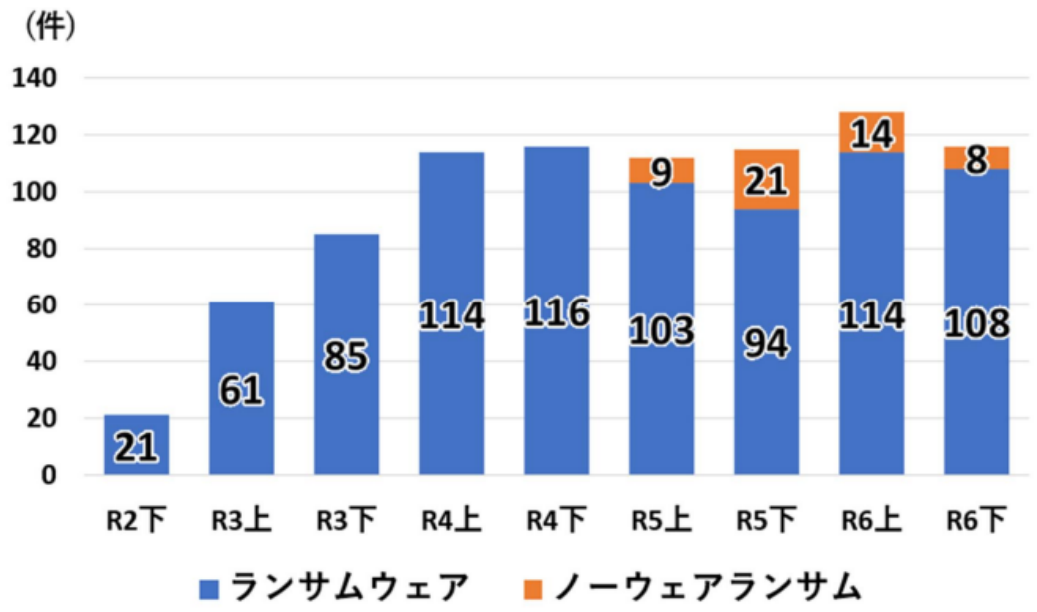


警視庁.令和６年におけるサイバー空間をめぐる脅威の情勢等について ．
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf.(参照2025-11-11)

現状の脅威

ランサムウェアによる被害件数は令和2年の下期から令和6年の下期の間に約5～6倍にまで増えています。
IPA(独立行政法人情報処理推進機構)はランサムウェアによる被害を社会的に影響の大きかったセキュリティ上の脅威として情報セキュリティ10大脅威の1位に挙げています。

1　企業・団体等における被害の報告件数の推移



※ノーウェアランサムの被害については、令和５年上半期から集計。

警視庁.令和６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 .
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf.(参照2025-11-11)

情報セキュリティ10大脅威 2024

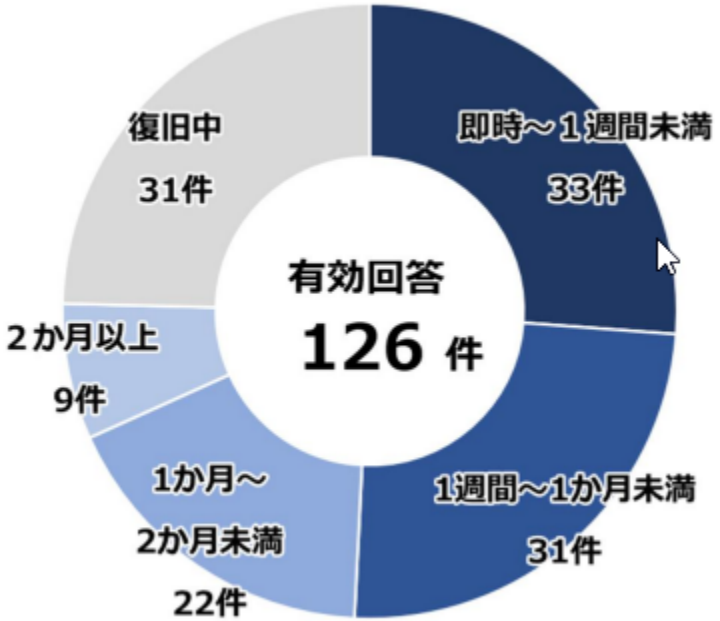
IPA

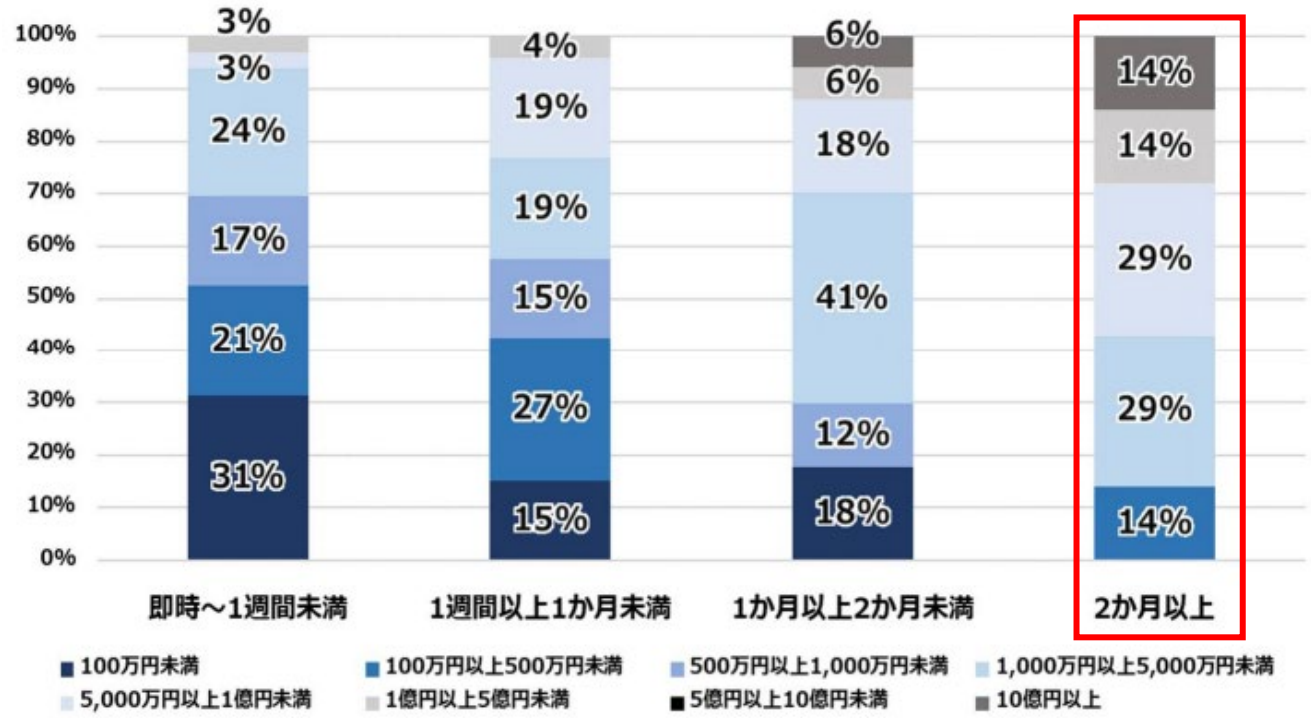
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した脅威	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化(アンダーグラウンドサービス)	2017年	2年連続2回目

IPA情報処理推進機構.情報セキュリティ10大脅威 2025組織編.
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf.(参照2025-11-11)

被害リスク

**左の表はランサムウェアによる被害の発生から復旧までの期間を表しています。
1か月の間で復旧できたケースは50%しかありません。
右の表はランサムウェア被害による調査・復旧にかかる期間と費用の関係を表しています。
復旧に2か月以上かかったケースでは3割以上が復旧のためにかかった費用が1億円を超えています。**





警視庁.令和６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 ．
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf.(参照2025-11-11)

被害事例

**ランサムウェアによる被害を受けると、業務が停止するほどの大きな損害を受け、
攻撃者により個人情報などの情報が流出する危険性もあります。
以下に挙げるのは国内でのランサムウェアによる被害事例です。**

No	業種	被害状況
1	医療	電子カルテおよび会計システムが使用不可となり患者データにアクセスできなくなった。 復旧に2か月を要した。 すでに判明していた脆弱性を放置したままで利用していたVPN装置がきっかけとなって、ランサムウェアに感染したという報告がされている。
2	製造業	社内ネットワークシステムに大規模な障害が発生し工場で生産が停止した。 完成した商品を検査するシステムに障害が起き一時出荷を見合わせた。 社内サーバーに外部から侵入され、本社や間接部門でシステムにアクセスできず、電子メールのやりとりもできないといった事態にまで発展した。
3	教育機関	学生や職員のアカウントを管理するサーバーが感染し約4万件の個人情報が流出しサーバーの復旧が完了するまでに1か月半近くを要した。 ランサムウェア侵入の原因は、ファイアウォールの設定ミスにあった。

防御策と予防

**昨今サイバーセキュリティ対策はどの企業にとっても必要不可欠となっています。
ランサムウェア感染を防ぐ対策としてまずは次の基本ルールを定着させ、サイバーセキュリティ意識を高めていきましょう。
あわせて、企業としてどのようにサイバーセキュリティ対策を推進するか、基本方針を定めることも重要です。**

サイバーセキュリティの基本ルール

・OSやソフトウェアは常に最新の状態にしよう
・ウイルス対策ソフトを導入しよう
・パスワードを強化しよう
・共有設定を見直そう
・脅威や攻撃の手口を知ろう

警視庁.マルウェア「ランサムウェア」の脅威と対策（対策編）.
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html.(参照2025-11-11)

攻撃手法の理解

下の表は従来のランサムウェア攻撃と最新のランサムウェア攻撃の特徴について表しています。
近年では侵入手口がメールやWebサイトから、VPN機器やリモートデスクトップへ遷移しています。

	従来のランサムウェア攻撃	最新のランサムウェア攻撃
主な侵入手口	メールやWebサイト	VPN機器やリモートデスクトップ
ターゲット	不特定多数	特定の組織や企業
犯行の特長	ばらまき型で、手口の形式は単調なものが多い	巧妙な計画に基づき、手動で行われる

Wiz LANSCOPE サイバーセキュリティに関する情報サイト.ランサムウェアの6つの感染経路と対策、感染した場合の対処法を解説.
https://www.lanscope.jp/blogs/cyber_attack_cpdi_blog/20230403_29782/.(参照2025-11-11)

攻撃手法の理解

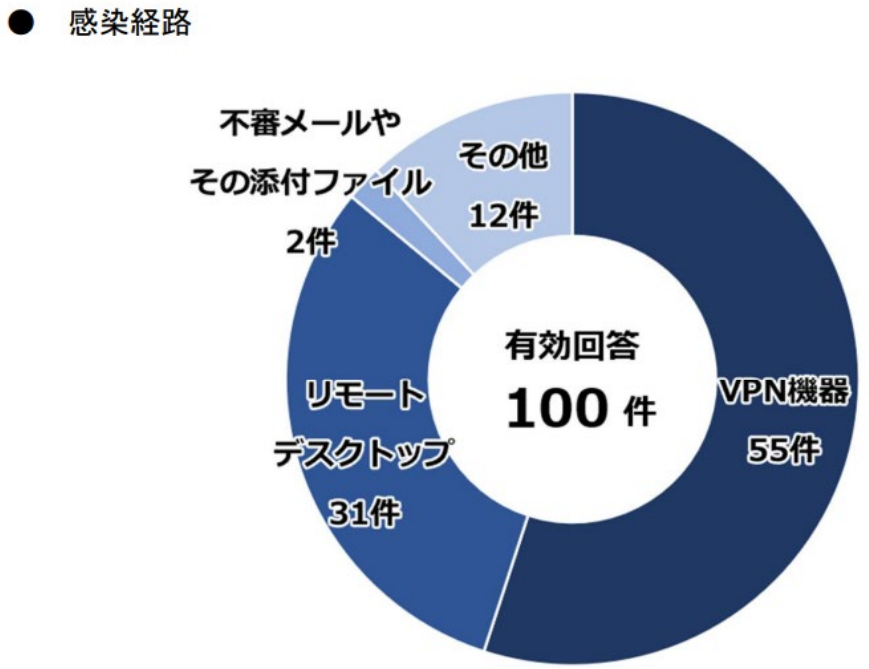
右の図はランサムウェアの侵入手口を表しています。
VPN機器とリモートデスクトップが件数の約80%を占めている背景および侵入手口は以下の通りです。

・VPN機器

背景：テレワークや複数拠点での情報共有のために導入が進みましたが、
その反面ランサムウェアの侵入経路として狙われる事例が増えています。
侵入手口：脆弱性を利用し、認証をパスする。
何らかの方法で入手した認証情報を悪用する。

・リモートデスクトップ

背景：テレワークの普及によりセキュリティ対策をしていない
リモートデスクトップが増え、感染経路として狙われることが増えました。
侵入手口：漏洩した認証情報(ログインID/パスワード)悪用する。
リモートデスクトップの通信規約の脆弱性を利用する。



警視庁.令和６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 .
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf.(参照2025-11-11)

SBUN_TM102_TM102R1102_C251110103020095000
SBUN_TM705_TM705R1705_C251107122623333000
SBUN_TM720_TM720R1720_C251107223004164000
SBUN_TM702_TM702R1702_C251107090236572001

今はない、答えを創る。

JSOL

NTT DATA Group