【技術レポート】

AIによる大量自動攻撃から守る、閉域セルラー構成

～見えない・届かない・止まらない～

株式会社ＩＤＹ 2026年11月10日

要旨

警察庁のランサムウェア被害調査では、感染経路の有効回答のうち、インターネットに露出したVPN機器からの侵入が2025年、2026年上半期ともに最多である［1］［2］。また2026年9月以降、国内では情報漏えいの公表が急増し、関係機関は攻撃者がAIを用いて標的の調査や侵害を行っている可能性を指摘している［4］［5］［8］。本レポートでは、インターネット上で接続を待ち受けるVPN装置が探索と侵害の起点となる構造を考察し、VPNを通信事業者の5G閉域網に置き換えて拠点間通信をインターネットから分離する「閉域セルラー構成」を提案する。本構成は「見えない・届かない・止まらない」の3要件を満たすことを目的とし、有線閉域網と比較して回線工事を要さず、複数通信事業者の閉域SIMによる冗長化を可能とする。

1. はじめに

拠点間通信や保守接続の手段として、インターネットVPNは広く用いられてきた。しかし、VPN装置はインターネット上で接続を待ち受けるため、その存在自体が探索の対象となる。攻撃の自動化が進む現在、この「インターネットから見えている入口」をいかに減らすかが重要な課題となっている。

本レポートでは、2章で統計と関係機関の公表に基づき現状を整理し、3章で攻撃の流れと成立要因、および対策に求められる要件を示す。4章で提案構成を、5章で冗長化方式を、6章で導入性を述べ、7章で適用範囲と制約を明らかにする。

2. 背景

2.1 ランサムウェアの感染経路

警察庁によれば、2026年上半期に警察へ報告されたランサムウェア被害は123件であり、半期として過去最多である［1］。感染経路について有効回答のあった36件のうち、VPN機器は18件（50.0%）、リモートデスクトップは9件（25.0%）であった。2025年においても、有効回答92件のうちVPN機器は61件（66.3%）であり［2］、VPN機器は2年連続で感染経路の最多となっている（図1）。

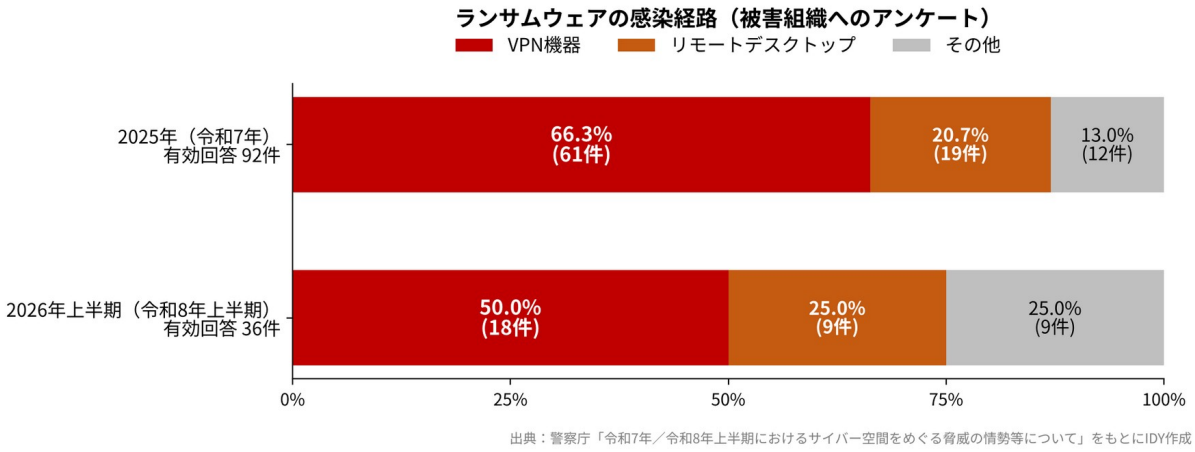


図1 ランサムウェアの感染経路の内訳（文献［1］［2］より作成）

2.2 AIを用いた大量自動攻撃と情報漏えいの増加

2026年9月以降、国内では情報漏えいの公表が急増した。調査会社MM総研によれば、2026年10月末までに公表されたサイバー攻撃による漏えい（可能性を含む）情報件数は約3億7,600万件であり、2025年1年間（4,953万件）の約7.6倍に達した。10月単月の情報件数は約1億8,500万件にのぼる。また、1~10月累計の事案数（661件）と100万件以上の大規模事案（45件）はいずれも過去5年で最多である［9］（図2）。

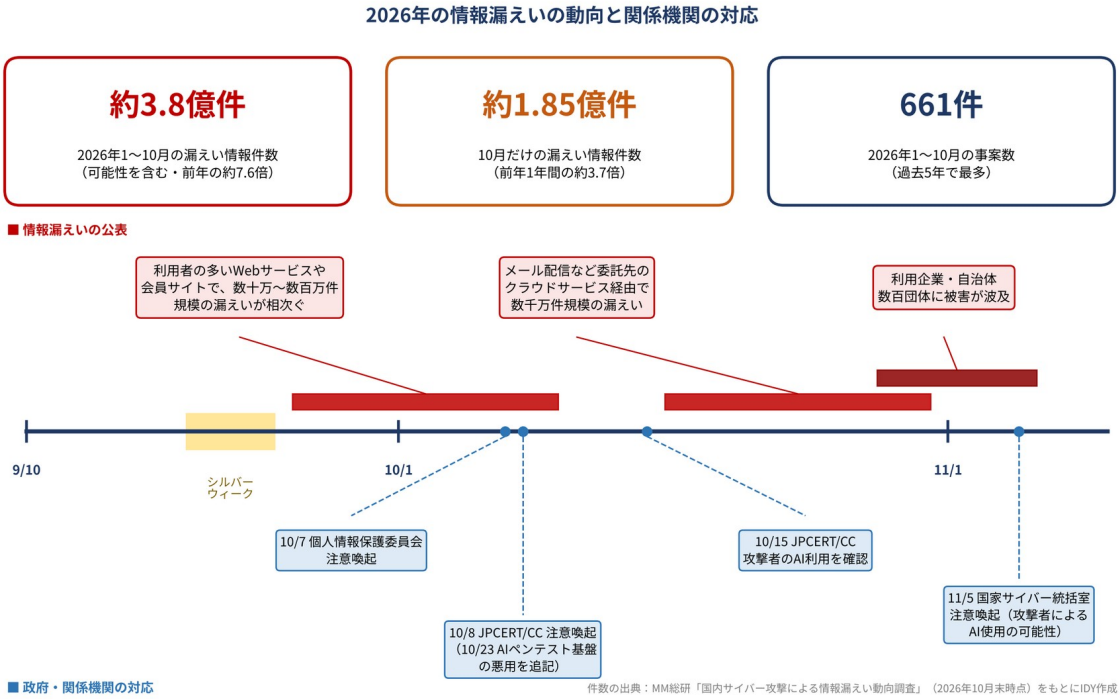


図2 2026年の情報漏えいの動向と関係機関の対応
（件数は文献［9］より作成）

これを受けて、個人情報保護委員会［3］、JPCERT/CC［4］、内閣官房国家サイバー統括室［6］、総務省［7］などが相次いで注意喚起を行った。JPCERT/CCは、攻撃に使用された可能性のあるインフラの調査において、攻撃者がAIを利用して既知の脆弱性のスキャン等を行っていたことを確認している［5］。また国家サイバー統括室は、攻撃者が標的の調査や侵害にAIを使用している可能性が高いと指摘している［8］。AIの利用により、攻撃者はインターネットから到達可能な機器を、人手では困難な規模と速度で探索し得る。

3. 課題と要因

3.1 攻撃の典型的な流れ

VPN装置を起点とする攻撃は、一般に図3の流れをとる。攻撃者はまずスキャンにより公開されたVPN装置とその機種を特定し、脆弱性の悪用または窃取した認証情報により正規利用者としてログインする。侵入後は内部の偵察と横展開を行い、最終的にデータの窃取とランサムウェアによる暗号化に至る。

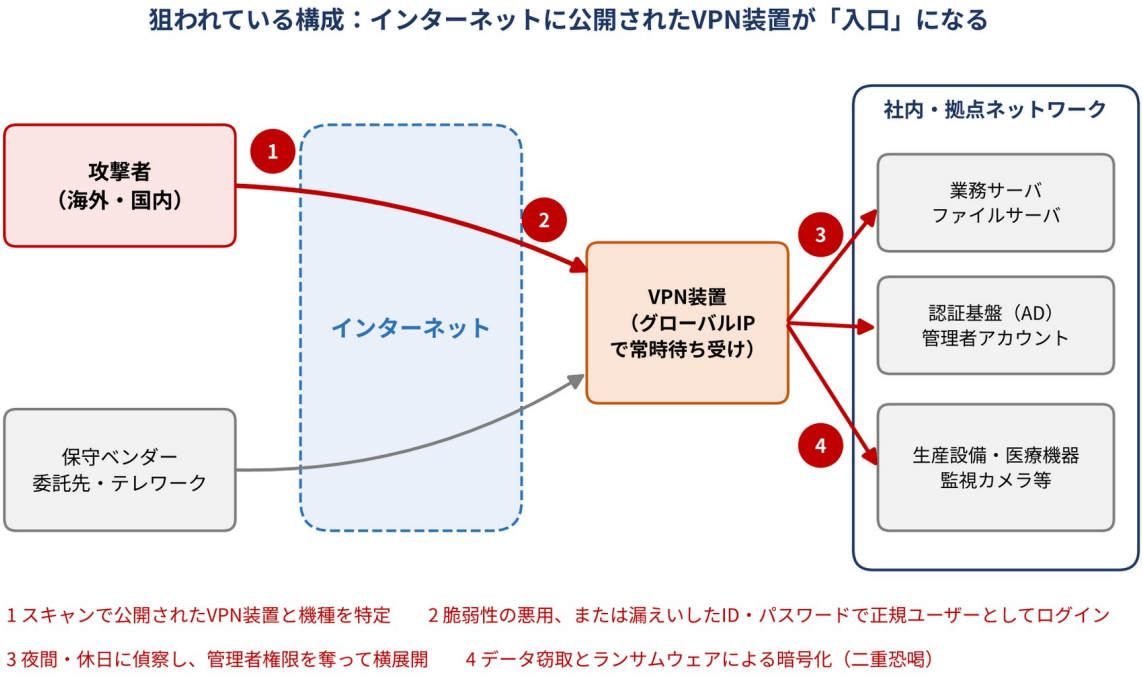


図3 VPN装置を起点とする典型的な攻撃の流れ

こうした被害を背景に、インターネットに露出したVPN装置を廃止し、他の接続方式へ置き換える動きが広がっている。

3.2 攻撃が成立する主な要因

前節の攻撃が成立する主な要因は、次の3点である。

（1）入口の露出

VPN装置はインターネット上で接続を待ち受けるため、探索により発見される。脆弱性が公表されると、修正の適用が遅れた機器が短期間のうちに標的となる。

（2）認証情報への依存

接続の可否がIDとパスワード等の認証情報に依存するため、認証情報が漏えいすると正規利用者として侵入される。

（3）入口の増加

拠点や委託先の増加に伴いVPNの入口と管理対象が増え、機器の更新や監視が行き届きにくくなる。

3.3 対策に求められる要件

以上を踏まえ、本レポートでは対策の要件を次の3点と定義する。

（a）見えない：インターネット上に接続の待ち受け口を置かず、探索の対象とならないこと。

（b）届かない：通信事業者に登録されたSIMを持つ機器以外は網に接続できず、認証情報のみでは接続が成立しないこと。

（c）止まらない：通信事業者の障害や輻輳に対して冗長性を持ち、閉域化によって業務の継続性が損なわれないこと。

4. 提案構成

4.1 有線閉域網とセルラー閉域網の比較

インターネットから分離する手段としては、有線の閉域網（IP-VPNや専用線）も存在する。しかし、拠点が多数に分散する場合、全拠点に有線の閉域回線を敷設するには回線工事、費用、開通までの期間を要する。これに対し、通信事業者の閉域網サービスに対応したSIMを用いるセルラー閉域網は、回線工事を要さずに開通できる（表1）。

表1 有線閉域網とセルラー閉域網の比較

観点	有線の閉域網	セルラーの閉域網
導入コスト	拠点ごとに回線工事と 月額費用が必要	回線工事が不要 機器費・SIM／閉域網サービスの 利用料が必要
導入までの時間	開通まで 数週間から数か月	契約とSIMの準備が整っていれば 早ければ数時間※1
設置場所	回線を引ける 固定拠点に限られる	仮設拠点、屋外設備、 車両などにも設置可能

表1 有線閉域網とセルラー閉域網の比較

観点	有線の閉域網	セルラーの閉域網
冗長化	2回線目の工事と 契約が必要	複数のSIMで、 通信事業者をまたいで冗長化
移設・増設	再工事が必要	機器とSIMを移すだけ

※1 閉域網サービスの契約とSIMの準備が整っている場合の、機器の設置・設定に要する時間の目安。

ただし、大容量の通信が常時発生する大規模な固定拠点においては、有線閉域網も引き続き有力な選択肢である。拠点の規模と用途に応じて、両者を併用する構成も考えられる。

4.2 IDY推奨の閉域セルラー構成

提案構成では、拠点とセンター（本社またはデータセンター）の間を、iR800BやiR730B等のIDY製5Gエッジゲートウェイと通信事業者の5G閉域網で接続する。インターネットへの出口は設けず、拠点間の通信を閉域網内で完結させる（図4）。

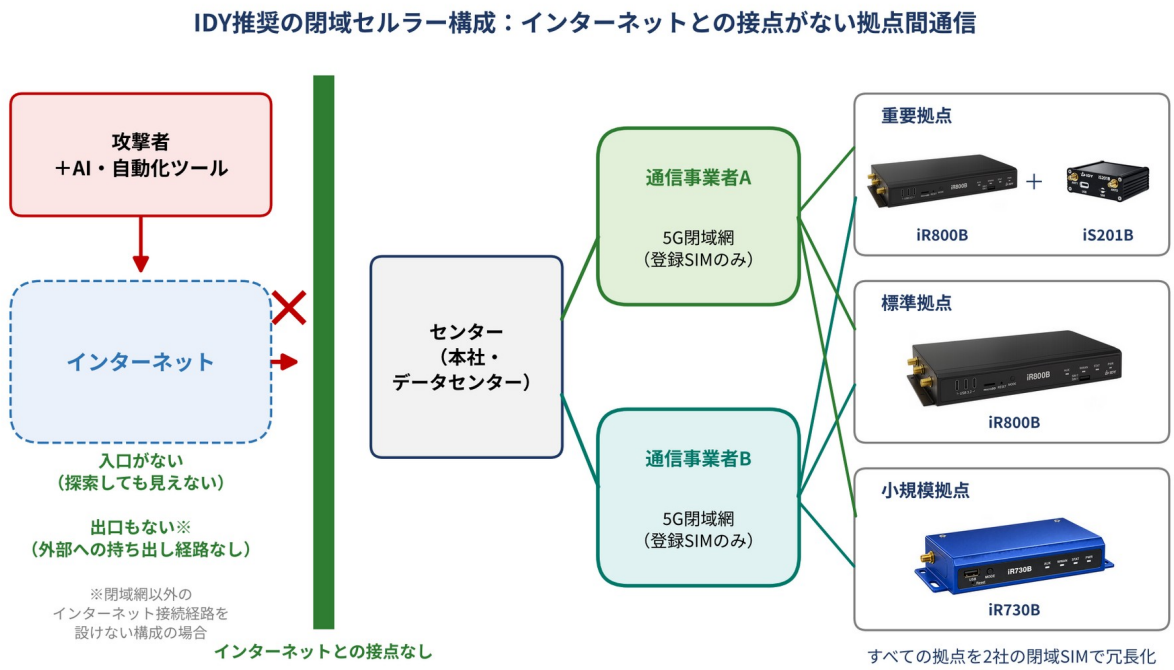


図4 IDY推奨の閉域セルラー構成

本構成と3.3節の要件との対応は次のとおりである。

（a）見えない：グローバルIPアドレスで接続を待ち受けるVPN装置が存在しないため、探索により入口が発見されない。

（b）届かない：閉域網に接続できるのは、通信事業者に登録されたSIMを装着した機器に限られる。委託先の接続も、SIM単位で限定・停止できる。

（c）止まらない：すべての拠点において、2社の閉域SIMにより通信事業者をまたいだ冗長化を行う（5章）。

加えて、閉域網以外のインターネット接続経路を設けない構成では、拠点内の機器が侵害された場合においても、外部の指令サーバーとの通信やインターネットへのデータ持ち出しの経路が存在しない。インターネットVPNとの比較を表2に示す。

表2 インターネットVPNと閉域セルラー構成の比較

観点	インターネットVPN	閉域セルラー構成
AIによる探索	グローバルIPで 待ち受けるため、 探索で発見される	インターネットに待ち受け口がなく、 探索の対象にならない
接続できる条件	ID・パスワード （＋証明書等） 盗まれると突破される	登録済みSIM＋閉域網内の認証 SIMのない機器は接続不可
脆弱性の影響	公開されたVPN装置の 脆弱性が直接狙われる	外部から到達できないため、 悪用の前提が成立しにくい
インターネット への経路	あり （持ち出しや外部との 通信に使われ得る）	閉域網からはなし （他のインターネット接続経路を 設けない構成の場合）

4.3 提案構成に求められる要件とiR800Bの適合性

VPNを閉域セルラー構成に置き換えた後も業務を維持するためには、拠点側の機器に、5Gの通信性能、拠点の基幹として設置可能な有線性能、および冗長性が求められる。表3に、これらの要件に対するiR800Bの適合性を示す。

表3 提案構成に求められる要件とiR800Bの適合性

項目	iR800Bの仕様	要件への適合
通信性能	5G（SA／NSA、Sub-6） iR800B-101／iR800B-102： 3GPP Release 16準拠 iR800B-107： 3GPP Release 17準拠 実測DL 1.94Gbps※2	VPNからの置き換え後も 拠点間通信の速度を 維持しやすい
冗長化	物理SIM×2（nanoSIM） iS201Bとの組み合わせで 3 SIM・2 Active	通信事業者をまたいだ冗長化 最上位構成では 2回線を同時に運用
自動復旧	再接続→ソフトリセット→ ハードリセット→ 本体再起動	無人拠点においても 通信途絶から自律的に復旧

表3 提案構成に求められる要件とiR800Bの適合性

項目	iR800Bの仕様	要件への適合
有線インターフェース	10GbE SFP+×1 10GbE RJ-45×1 1GbE RJ-45×2	拠点ネットワークの 基幹機器として設置可能
環境性能	鉄道車両用品の振動・衝撃試験 （JIS E 4031:2013 分類1A） 自動車部品の振動試験 （JIS D 1601:1995）	工場、屋外、車両など 多様な設置環境に適合
開発・製造	国内メーカーによる 開発・製造	運用仕様に応じた カスタマイズと長期保守が可能

※2 iR800B-102による当社測定値［10］。Anritsu MT8000A（5G SA n79、2CC CA、総帯域幅200MHz、4×4 MIMO）、10GbE経由のLAN側PCでiperf3を実行（標準のUSB接続構成）。PCIe接続構成では2.34Gbps、製品内部でのiperf3では2.45Gbpsを確認している。

5. 冗長化方式

セルラー閉域網の採用にあたり最も懸念されるのは、通信事業者の障害や輻輳による通信の途絶である。IDYは、拠点の重要度に応じて3段階の冗長構成を用意している（図5）［11］。



図5 拠点の重要度に応じた冗長構成

最上位の構成は、iR800Bに5G USBモデム iS201BをUSB 3.2で接続するものである。3枚のSIMを用い、2本の通信経路を同時に運用する（2 Active）。iR800B-107との組み合わせでは、3回線すべてを基地局に登録した状態で維持し、2本をActive、1本をStandbyとして運用する。待機回線を登録済みに保つことにより、再登録を伴う構成と比較して切り替え開始までの処理を

短縮できる。iR800B-102との組み合わせにおいても2本の経路を同時に運用できるが、内蔵の待機SIMへの切り替え時には基地局への登録処理を要するため、切り替えに時間を要する。

冗長性を評価するうえで重要なのはSIMの枚数ではなく、基地局に登録される回線数、同時に通信可能な回線数、および障害時の切り替え先である。IDYは、回線状態の監視、障害の判定、経路の選択、切り替え後の疎通確認、復旧の判定までを一つの通信制御として設計している。また全機種において、通信の途絶を検知すると、回線の再接続、無線通信部のソフトリセット、ハードリセット、本体の再起動の順に段階的な復旧を試みる。

※3 切り替え時間は、回線の登録状態、通信事業者、検出条件、ルーティング等の構成により異なる。帯域合成や無瞬断での切り替えは、用途に応じたシステム構成・制御として個別に検討を要する。

6. 導入性

脆弱性の修正やシステムの再構築には、一般に数か月以上を要し、その間も探索は継続される。これに対し、閉域セルラー構成は既存のシステムを改修せずに導入でき、閉域網サービスの契約とSIMの準備が整っていれば、機器の設置と設定は早ければ数時間で完了する（※1、図6）。したがって本構成は、根本的な改修が完了するまでの間に入口を削減する手段としても有効である。

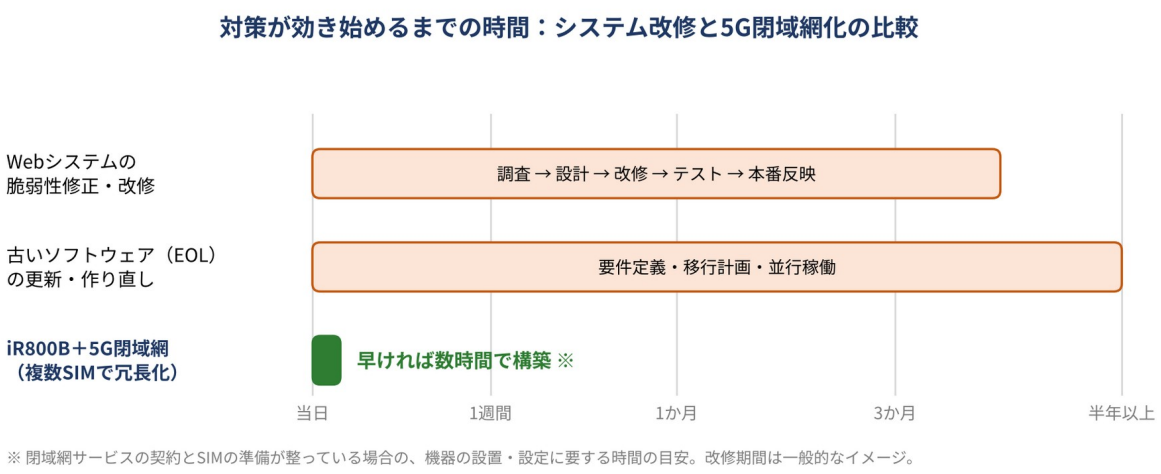


図6 対策が効果を発揮するまでの期間の比較（一般的なイメージ）

7. 適用範囲と制約

本構成の適用対象は、拠点間通信および保守接続など、従来インターネットVPNで実現していた非公開の通信である。利用者に公開するWebサイトやWebサービスは、インターネットからの到達性を前提とするため本構成の適用範囲外であり、WAF、脆弱性診断、修正プログラムの迅速な適用等の対策と併用する必要がある。

また、閉域網においても、接続を許可された機器が侵害された場合には内部への侵入が生じ得るため、拠点内機器の管理および更新は引き続き必要である。拠点またはセンターに閉域網以外のインターネット回線が存在する場合は、当該経路の管理と監視も必要となる。

8. まとめ

本レポートでは、インターネット上で接続を待ち受けるVPN装置が探索と侵害の起点となる構造を考察し、拠点間通信を5G閉域網へ移行する閉域セルラー構成を提案した。本構成は、待ち受け口の排除（見えない）、SIMによる接続制御（届かない）、複数通信事業者による冗長化（止まらない）の3要件を満たし、有線閉域網と比較して回線工事を要さず短期間で導入できる。拠点の重要度に応じて、iR800BとiS201Bの組み合わせ、iR800B単体、iR730Bの3段階の構成を選択することで、セキュリティと事業継続性の両立を図ることができる。

参考文献

［1］警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2026年9月10日）

［2］警察庁「令和7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」（2026年3月）

［3］個人情報保護委員会「大規模な漏えい等事案を踏まえた対応について（注意喚起）」（2026年10月7日）

［4］JPCERT/CC「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」（JPCERT-AT-2026-0030、2026年10月8日公開、10月23日更新）

［5］JPCERT/CC「連続不正アクセス事案の攻撃手法に関する調査」（JPCERT/CC Eyes、2026年10月15日）

［6］内閣官房国家サイバー統括室「不正アクセスによる漏えい等の事案を踏まえた対応について」（2026年10月9日）

［7］総務省「不正アクセスによる情報漏えい等の事案を踏まえた対応について（注意喚起）」（2026年10月9日）

［8］内閣官房国家サイバー統括室「個人情報の漏えい等につながる不正アクセスへの対策について」（2026年11月5日）

［9］MM総研「国内サイバー攻撃による情報漏えい動向調査」（2026年10月末時点、2026年11月4日発表）

［9・報道］NHKニュース「サイバー攻撃で情報漏えいの可能性 10月は1億8500万件あまりに」（2026年11月4日）

［10］株式会社ＩＤＹ「エッジ・製品エンジニアリング」（https://idy-design.com/ja/technology/edge-product-engineering）

［11］株式会社ＩＤＹ「レジリエントMulti-RAT」（https://idy-design.com/ja/technology/resilient-multi-rat）

［12］株式会社ＩＤＹ「iR800B」製品情報（https://idy-design.com/ja/products/ir800b）

［13］株式会社ＩＤＹ「iS201B」製品情報（https://idy-design.com/ja/products/is201b）

［14］株式会社ＩＤＹ「iR730B」製品情報（https://idy-design.com/ja/products/ir730b）

※ 記載の会社名・製品名は各社の商標または登録商標である。

付録 製品仕様

A.1 5Gエッジゲートウェイ iR800B



10GbEに対応した産業向け5Gエッジゲートウェイであり、提案構成において拠点側の中核を担う。

表A.1 iR800Bの主な仕様［12］

項目	仕様
3GPP	iR800B-101 / -102 (Rel.16) iR800B-107 (Rel.17)
5G NR CA	iR800B-101 : 2CC CA / 120MHz iR800B-102 : 3CC CA / 200MHz
LTE Bands	B1 / B3 / B8 / B18 / B19 / B26 / B28 / B39 / B40 / B41 / B42
5G NR Bands	n1 / n3 / n28 / n40 / n41 / n77 / n78 / n79
MIMO	DL 4 × 4 MIMO / UL 2 × 2 MIMO
5G Mode	SA / NSA / Sub-6
SIM	nanoSIM × 2
10GbE	SFP+ × 1 / RJ-45 × 1
1GbE	RJ-45 × 2
Wireless LAN	Wi-Fi 6 （WISE CONNECT® Wi-Fiモジュール装着時）
Bluetooth	Bluetooth 5.2
Expansion Interface	WISE CONNECT®
CPU	Arm Cortex-A73 Quad-core / 1.8GHz
USB	USB 3.2 Host × 3
Storage	8 GB eMMC / microSD
Industrial I/O	RS232 / RS485 / DIO × 2
Positioning	GNSS
Power Input	DC 9~24V / USB PD 65W以上・20V出力対応
Dimensions / Weight	105 × 200 × 25mm / 650g （WISE CONNECT®モジュール等を除く）

表A.1 iR800Bの主な仕様［12］

項目	仕様
Storage / Humidity	-20~+70℃ / 10~95%（結露なきこと）
Operating Temperature	-10℃ 〜 +60℃
Railway Vibration	JIS E4031:2013 — 鉄道車両用品―振動及び衝撃試験方法 / 分類1A
Automotive Vibration	JIS D1601:1995 — 自動車部品振動試験方法

A.2 5G USBモデム iS201B



USBバスパワーで動作する5G USBモデムであり、iR800BとUSB 3.2で接続することで3枚目のSIMによる独立した通信経路を追加する。

表A.2 iS201Bの主な仕様［13］

項目	仕様
Models	iS201B-101 / iS201B-102
3GPP	Rel.16 / 5G SA・NSA
5G NR	Sub-6GHz / n1・n3・n28・n40・n41・n77・n78・n79
5G NR CA	iS201B-101 : 2CC CA / 120MHz iS201B-102 : 2CC / 3CC CA / 200MHz
MIMO	DL 4x4 MIMO / UL 2x2 MIMO
LTE	101：Cat.18・最大5CA / 102：Cat.20・最大7CA
USB	USB 3.2 Type-C／USBバスパワー給電
SIM	nanoSIM x1
Antenna	LTE/Sub-6 SMA x4 / GNSS x1
Power	USBバスパワー 7.5W（15W以上推奨）
Dimensions / Weight	60（SMA含む86）x 81 x 32mm / 190g
Operating Temperature	-10〜60°C
Storage / Humidity	-20〜70°C / 10〜95%（結露なきこと）

iS201Bの実測スループットは、Windowsで下り3,060Mbps、Ubuntuで下り3,030Mbpsである。当社評価環境でiS201BをPCに接続し、端末側のiperf3で測定した（2CC CA 200MHz、4×4 MIMO）。実際の通信速度はネットワーク、無線条件、OS、測定条件等により異なる。

A.3 5Gエッジゲートウェイ iR730B



iR700Bシリーズの小型・堅牢設計と産業I/Oを継承した5G・LTE対応の産業用5Gエッジゲートウェイであり、ファンレスのコンパクトな筐体により分散する小規模拠点への設置に適する。

表A.3 iR730Bの主な仕様［14］

項目	仕様
Models	iR730B-001 / -002 / -101 / -102
3GPP	iR730B-001 / -002 : Rel.15 iR730B-101 / -102 : Rel.16
Mobile Network	UMTS / LTE / 5G Sub-6GHz
5G mmWave	標準仕様には含まず
GNSS / GPS	オプション（アンテナ / FW / 別途相談）
Ethernet	1GbE LAN × 1 / 1GbE LAN-WAN × 1
Expansion Interface	WISE CONNECT® （型式・モジュール仕様による）
Antenna	SMA connector × 6
USB	USB 2.0 × 1
Serial / DIO	RS232 / RS485 / DIO1 / DIO2 × 1
Display	電源LED / Status LED / WWAN LED / AUX LED
Buttons	MODEスイッチ / RESETスイッチ
Power Input	DC 5V–16V / AC adapter: DC12V output
Size	77.9 × 125 × 24.8 mm
Weight	約320g（WISE CONNECT®モジュール、アンテナ、ACアダプター含む）
Power Consumption	最大 約20W（5G/LTE・LAN使用時）
Operating Temperature	-10°C ～ +60°C
Storage Temperature	-20°C ～ +70°C
Humidity	10% ～ 95% RH （結露なきこと）
Environment	JIS D1601:1995 — 自動車部品振動試験方法 JIS E4031:2013 — 鉄道車両用品―振動及び衝撃試験方法

お問い合わせ

本構成の導入検討、既存のVPNおよび拠点間接続からの移行に関するご相談は、当社ウェブサイトのお問い合わせフォームにて受け付けています。

株式会社ＩＤＹ

お問い合わせフォーム
https://idy-design.com/ja/contact