

LGWANリモートアクセスサービス ご紹介資料

J-LIS
承認済

株式会社シナジー



LGWAN-ASPコード
A831188

会社概要(事業概要)

商号	株式会社シナジー 
所在地	<p>【本社】 〒901-2223 沖縄県宜野湾市大山七丁目10番14号3階</p> <p>【東京支社】 〒105-0014 東京都港区芝一丁目10番11号 コスモ金杉橋ビル5階</p> <p>【名古屋支社】 〒460-0008 愛知県名古屋市中区栄二丁目9番26号 ポーラ名古屋ビル11F</p>
設立年月日	2010年4月13日
代表者	代表取締役 下地勝也
業務内容	<ul style="list-style-type: none"> ●システム開発 (行政/自治体・金融向けWeb・業務系アプリケーション 他) ●ソリューションサービス (自治体向け内部情報システム開発・販売・コンサルティング、校務支援システム販売 他) ●Webデザイン (サイト制作、Eコマースサイト運営 他) ●データセンタ事業 (ハウジング、LGWAN-ASPサービス等) ●沖縄インバウンド事業
資本金	8,000万円
社員数	100名(2020年4月現在)
主要取引銀行	沖縄銀行・琉球銀行・みずほ銀行・鹿児島銀行
認証・許認可	プライバシーマーク(認定番号:第18820311号) 労働者派遣事業(許可番号:派47-300261)

2010年

2015年

2016年

2017年

2018年

2019年

2020年

株式会社ディエムエイジェント設立

本社を宜野湾市真栄原に開設

資本金 1,000万に増額

3月、事業拡大のため、本社を沖縄県宜野湾市真志喜へ移転

資本金 1,300万に増額

合同会社アイエヌジーを吸収合併

株式会社シナジーへと商号変更

7月、事業拡大のため、
本社を沖縄県宜野湾市大山へ移転

8月、東京支社を東京都港区に設立

資本金 3,000万に増額

9月、沖縄情報通信センター内にデータセンター設立
データセンタ事業開始(ハウジング、ASPサービス)

資本金 5,000万に増額

1月、自社製品(内部情報系システムActiveCityシリーズ)の
LGWAN-ASPサービス開始

8月、名古屋支社を名古屋市中区に設立

4月、OIC事業部開設
沖縄インバウンド事業
(医療ツーリズム、インバウンドセミナー等)サービス開始

4月、デジタルトランスフォーメーション実現プロジェクト始動
(リモートサポート・保守、AIチャット、動画マニュアル配信 他)



沖縄本社



東京支社



名古屋支社

背景とコンセプト

新型コロナの第一波の余波を受けて…。

各市町村役場の担当者は一様に：

「職員の集団感染により住民サービスの継続が困難になってしまう

“最悪の状況”に陥ったとしても **最低限の業務が継続できる体制** を考えたい」



政令指定都市を除く1721市区町村のうち3月26日までの導入は **3%**の51自治体にとどまった。
 (総務省集計)



各都道府県様の課題(リモートが進まない理由)

在宅勤務については、

- ①個人情報が入ったノートパソコンは庁内から持ち出し禁止である。
- ②自宅などから庁内の情報システムにインターネット経由で接続できない。
- ③これまで許可されていた閉域SIM方式は、費用が高く導入が難しかった。

よって、一般的なテレワークはできない。

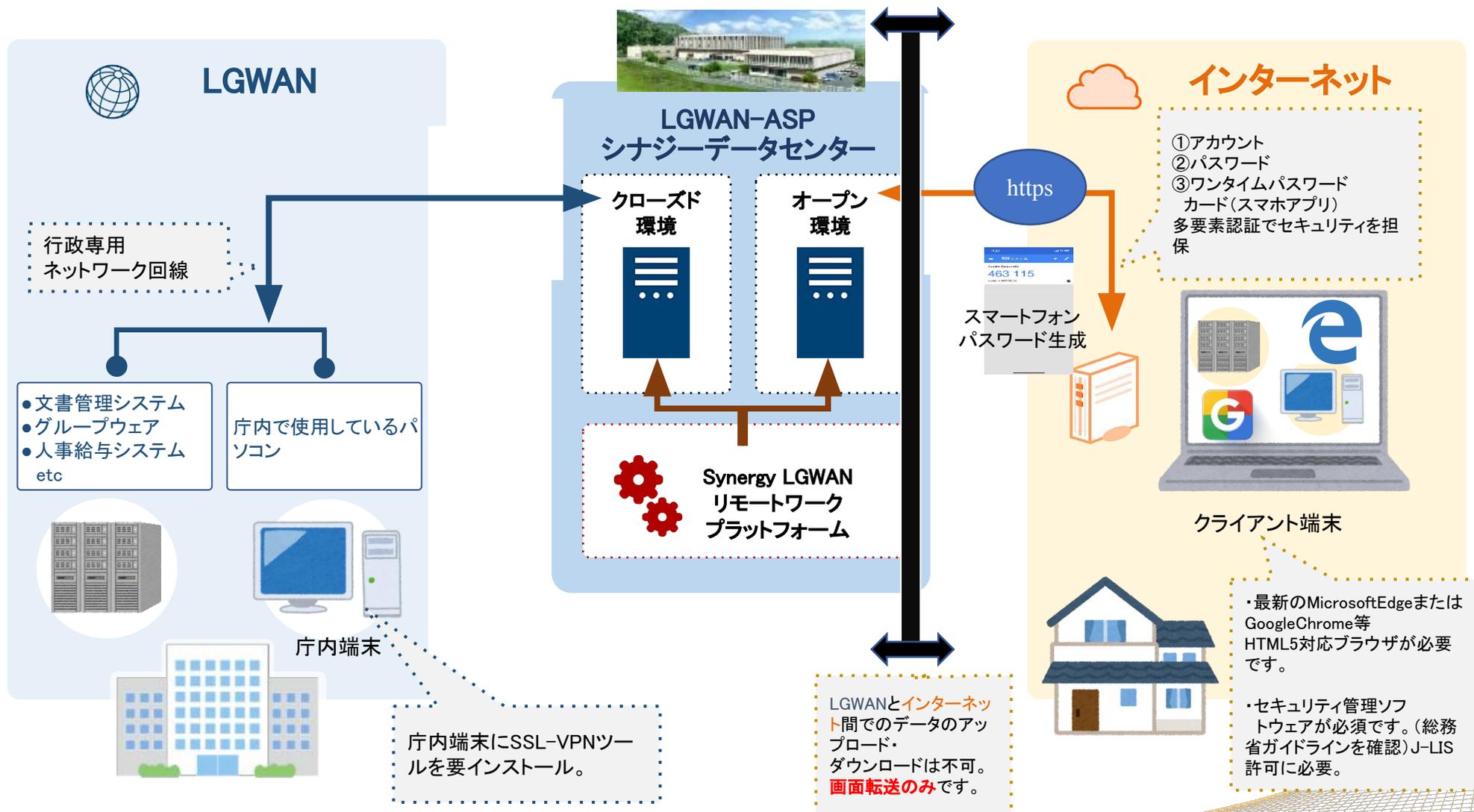
☆万が一にも、紛失や不正侵入による漏洩(ろうえい)があってはならないから



上記を解消し、自治体様でもリモートアクセスが可能なシステムを開発 (2020/9/30 J-LIS承認済)

システム概要① 全体イメージ図

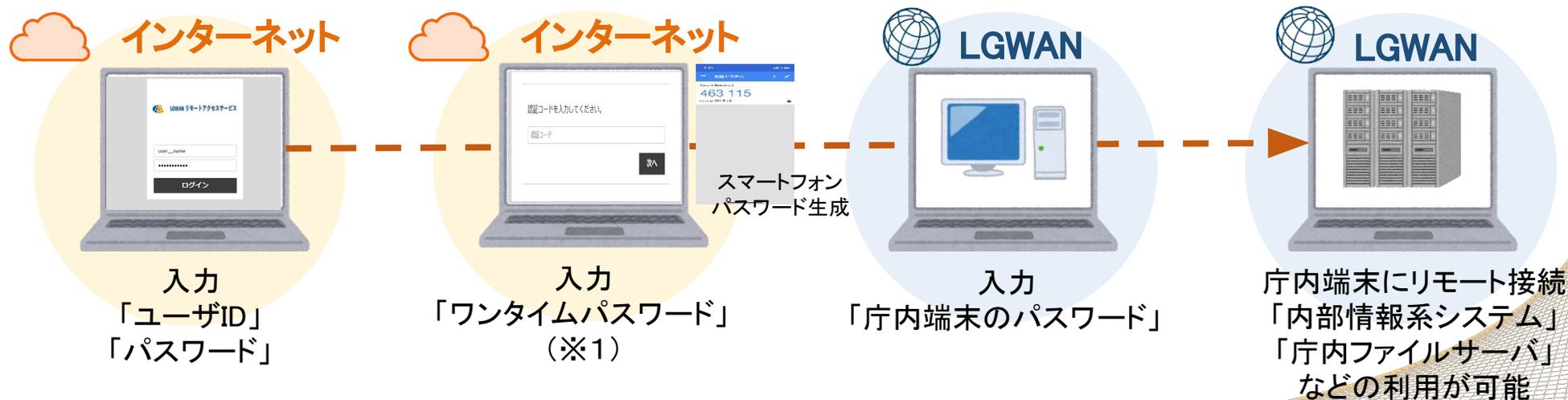
弊社データセンターを介し、インターネット経由でLGWANへアクセス



リモートアクセスサービスの操作イメージ



実際の操作イメージ



ワンタイムパスワード

「ワンタイムパスワード」とは、文字通り一回限りの使い捨てパスワードを意味します。

認証の度に異なるパスワードを毎回生成し使用するため、漏洩のリスクを回避し高い安全性が保たれます。

また、生成されたワンタイムパスワードは規定の時間を経過、または一度認証に成功すると破棄され、同じものは使えない仕組みになっており、パスワード管理の負担も軽減できます。

「ワンタイムパスワード」の生成方法

お手持ちのスマートフォン (ios、android) で「Google Authenticator」アプリをインストールし起動させます。

リモートアクセス時、端末の画面にQRコードが初回のみ発行されます。発行されたQRコードを「Google Authenticator」をインストールしたスマートフォンで読み取ります。

読み取り後は、アプリを起動するごとにワンタイムパスワード(複数桁)が表示されます。ワンタイムパスワードは30秒ごとに生成され、一定時間が経つと無効になりますので、生成されている間にワンタイムパスワードを入力します。

入力が間に合わなかった場合は自動でワンタイムパスワードが発行されますので再度入力します。一度QRコードの読み取りを完了させれば、以降リモートアクセス時は「Google Authenticator」を起動するだけでパスワードが生成されます。



端末に表示されたQRコード画面
リモート接続初回時に表示
スマートフォンで読み取る

QRコード読み取り



スマートフォン画面
「ワンタイムパスワード生成」

生成された
パスワード入力



入力
「ワンタイムパスワード」

特徴・メリット

- **クライアント端末**にリモートアクセスに関する**専用のアプリケーションをインストールする必要はありません**。
「Google Chrome」や「Microsoft Edge」などのブラウザを用いて、**庁内端末へリモート接続を行います**。(OSはWindows10.Pro以上)
- 庁内の**LGWAN環境にある普段お使いの端末を遠隔で操作** できます。
- 庁内端末からデータセンターへは**SSL-VPNをインストールし暗号化**。セキュアな接続を保ちます。SSL-VPNツールの設定は1台あたり5分～10分程度で可能。
- リモートアクセス実現により、家族の介護や育児中で **働くことが難しい職員様の就労機会創出**に繋がられます。また **在宅の機会が多い職員様でも、ご自宅から庁内端末へアクセスし業務をおこなうことが可能です**。

よくある質問

- ① Q. このサービスで何ができますか？
 A. 庁内で普段お使いの端末を遠隔で操作することができます。
- ② Q. ActiveCityのサービスを使っていない場合は、リモートアクセスサービスはできないのですか。
 A. ActiveCityのサービスを利用していなくても、オンプレミスシステムへの利用が可能です。
- ③ Q. ウィルスに感染されたパソコンから、アクセスされた場合、データセンターのオープン環境ではどのように守っているのでしょうか。プラットフォームを乗り越えてクローズド環境へ行くことはありませんか。
 A. LGWANリモートサービスでは、インターネット側はブラウザですが、キーボードとマウス情報以外のデータは、サーバ側に送信しないので、ウィルスに感染したファイルがアップロードされることはありませんが、総務省ガイドラインより庁外端末へのセキュリティー対策は必須のため、事前にウィルスに感染していない前提でご利用頂きます。
- ④ Q. 在宅勤務の場合、いつ使用しているのか管理することはできますか？
 A. セキュリティ管理ソフトウェアのPC操作ログ管理でログを取得し、操作時間等を確認することができます。（別途セキュリティ管理ソフトウェアのご案内となります。）
- ⑤ Q. 通信速度など確認したいため、無料でトライアルは可能ですか？
 A. 可能です。無料トライアルを期間限定でお申込みをホームページで受付しております。
- ⑥ Q. 契約期間はどれくらいから可能ですか？
 A. 1年からのご契約となります。

よくある質問

⑦ Q. 自宅にある個人のパソコンを使用してもよいですか？

A. 市町村様のセキュリティポリシーによるものと認識しております。

リモートアクセスのため、自宅のクライアント端末と庁内端末間で、データのアップロード・ダウンロード等の保存はできません。また、J-LIS申請に伴い、別途セキュリティ管理ソフトウェアをインストールする必要があります。別途セキュリティー対策ソフトの御見積も可能です。

⑧ Q. 構築期間はどれくらいかかりますか？

A. 概ね1,2カ月と考えております。お客様の規模により構築期間が変動する場合があります。

⑨ Q. 庁内端末やクライアント端末に何かソフトウェアのインストールが必要ですか？

A. 庁内端末へはVPN用ソフト(オープンソース)のインストールが必要です。クライアント端末にはGoogle ChromeやMicrosoft Edge等のHTML5対応のブラウザが必要です。

⑩ Q. 総務省の強靱化ポリシーは担保されていますか？

A. 総務省のセキュリティガイドラインに沿った開発を行っています。

⑪ Q. SynergyLGWANリモートワークプラットフォームとは何をしていますか？

A. 通信のセキュリティを担保したプラットフォームです。

⑫ Q. 遠隔操作であればクライアント端末へセキュリティソフトは不要ですか？

A. セキュリティレベルを上げるためにも、導入・設定することを推奨します。

よくある質問

⑬ Q. 何ライセンスからの販売ですか？

A. ライセンスの考え方は、テレワークが対象となる職員数分が必要となります。
例えば、総職員数が100人の場合、テレワーク対象の職員が50人であれば 50ライセンスを契約します。
職員様が利用しているパソコン自体との契約になります。最低ライセンス数は50ライセンスです。

⑭ Q. コロナウィルスに罹患した職員のみを対象と考えているのですが？

A. コロナ対策としての限定的・暫定的なサービスではなく、リモートワークの定着を推進しているため、ご提供するラ イセンスは
職員数と同数となります。

⑮ Q. ライセンスの使い回しは可能ですか。

A. 原則、庁舎内端末の数とライセンス数は同じとなるため、使い回しはできません。クライアント側の端末に数の制限 はございま
せん。

⑯ Q. リモート動作中の庁内端末の画面はどのように表示されるのでしょうか。庁内では画面が見えているのでしょうか。

A. リモート中はロック画面になり、操作中の画面は見えないようになっています。

⑰ Q. 接続ができないなど、何かあった場合の問い合わせ窓口はありますか。

A. サポート窓口を設けています。メールや電話、WEB会議ツールなどで対応させて頂いております。
(平日9:00~17:00)

⑱ Q. インターネット回線使用時のセキュリティの担保を教えてください。

A. 画面転送や多要素認証、SSL暗号化でセキュリティを担保しております。

セキュリティ管理ソフトウェア

ハンモック社製IT統合管理ソフト AssetViewのご提案

AssetViewは、在宅ワーク・リモートワーク用として庁内から持ち出す、あるいは貸し出す業務端末のセキュリティ対策、また運用管理対策のツールとしてご活用頂けます。

- 例)・リモート作業時の操作ログを取得する。→ 業務状況を「見える化」する。
- ・特定のURL接続の設定 → 業務以外の接続を禁止しセキュリティ意識を高める。
 - ・USBメモリ等、デバイスを制御 → 情報漏えいのリスクを低減する。

また、リモートワーク時の管理だけでなく、企業や自治体のIT資産管理からセキュリティ管理まで1つの製品で統合管理が出来るソフトウェアですので、以下の課題を解決する事が出来ます。

<h3>PC運用管理</h3> <p>社内端末の運用管理 課題解決 社内業務端末の運用を効率的に行いたい</p> <p>AssetView A IT資産管理 AssetView D アプリケーション配布 AssetView RC リモートコンソール AssetView MDM スマートデバイス管理</p>		<h3>PC更新管理</h3> <p>Windows 10 更新管理の課題解決 Windows 10 移行後のアップデート管理を安全に行いたい</p> <p>AssetView P PC更新管理</p>
<h3>データ流出対策</h3> <p>データ流出の課題解決 社内データが流出した際に有効な対応が必要</p> <p>AssetView I 個人情報検索 AssetView K ファイル制御・暗号化</p>	<h3>内部不正対策</h3> <p>内部不正を防ぐための課題解決 業務中の従業員の行動を監視したい・制御したい</p> <p>AssetView M PC操作ログ管理 AssetView G デバイス制御 AssetView S 不正PC遮断 AssetView Mail 電子メール監視 (オンプレミス版のみ提供)</p>	<h3>Webフィルタリング管理</h3> <p>不正サイトへのアクセス制御 禁止サイトやSNSにアクセスの制限をかけたい</p> <p>AssetView F Webフィルタリング</p>
<h3>ウイルス対策</h3> <p>ウイルス感染の課題解決 ウイルスからの感染を防止したい</p> <p>AssetView V ウイルス対策</p>		

セキュリティ管理ソフトウェア(推奨)

I. AssetView ご提供機能構成

以下の標準機能をベースにオプション機能を1機能から追加してご利用することができます。

標準機能(必須機能)
IT資産管理の基本的な機能をご提供

AssetView A IT資産管理	AssetView D アプリケーション配布	AssetView M PC操作ログ管理	AssetView G デバイス制御
AssetView I 個人情報検索	AssetView S 不正PC遮断	AssetView RC リモートコンソール	

オプション機能(1機能から選択可能)

AssetView V ウイルス対策	AssetView F Webフィルタリング	AssetView K ファイル制御・暗号化	AssetView MDM スマートデバイス管理
------------------------------	----------------------------------	----------------------------------	------------------------------------

II. リモートワーク時の業務対応機能イメージ

① リモートワーク時の業務対応機能は、標準機能である「PC操作ログ管理」と「デバイス制御」が対応します。

AssetView M
PC操作ログ管理

内部不正による
情報漏洩対策

AssetView G
デバイス制御

外部媒体による
持ち出し制御

② セキュリティ強化策として「ウイルス対策」機能を追加、より安全なリモートワーク環境を整えます。

AssetView V
ウイルス対策

ウイルス侵入検知・駆除

※ソフトウェアの価格は、クライアント数やオプション機能によって変動がありますので、弊社担当までお問合せ下さい。