資料3-2
事務局提出資料

テレワークの導入について

総 務 省

令和２年11月30日

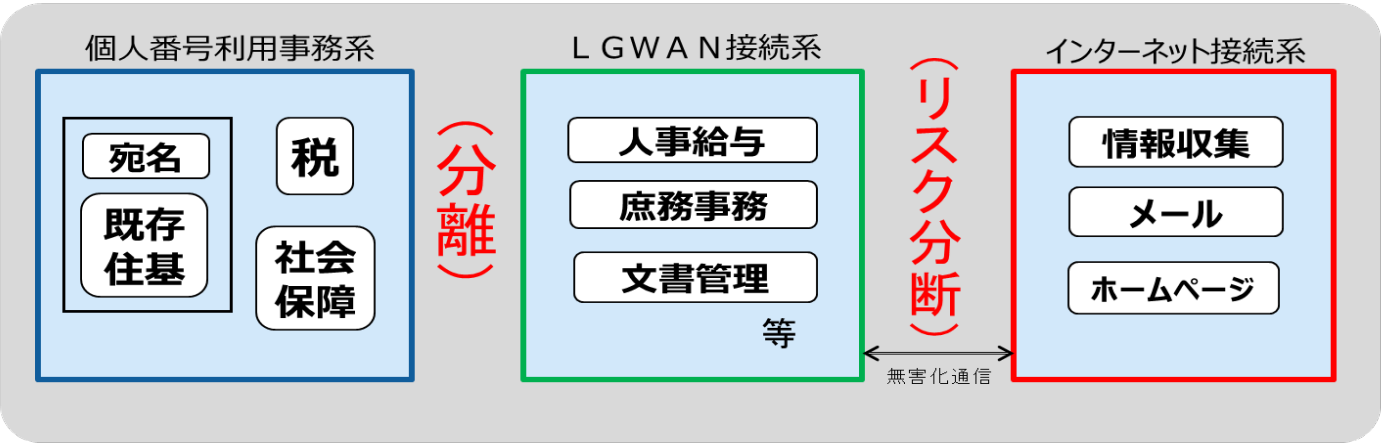
地域力創造グループ
地域情報政策室

「三層の対策」の概要

2015(H27)年～2017(H29)年

「三層の対策」によるセキュリティ強化

市区町村におけるネットワーク構成（イメージ）



① 個人番号利用事務系では、端末からの情報持ち出し不可設定等を図り、住民情報流出を徹底して防止

② LGWAN接続系とインターネット接続系を分割し、LGWAN環境のセキュリティ確保

③ 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度な情報セキュリティ対策を実施

2015.5　年金機構の情報漏えい事案発覚後、有識者による「自治体情報セキュリティ対策検討チーム」を設置
2015.11　検討チームより自治体の対策内容（「三層の対策」）について報告
2015.12　総務大臣通知により自治体に「三層の対策」を要請
2016.1　自治体が「三層の対策」に取り組むための補助金（H27補正）の説明会
2017.7　自治体による「三層の対策」への対応完了

「三層の対策」見直しについて

「三層の対策」

2015年の年金機構の情報漏えい事案を受け、**短期間**で自治体の情報セキュリティ対策を抜本的に強化　＝**「三層の対策」**

⇒　**インシデント数の大幅な減少を実現**

一方で、

①ユーザビリティへの影響

- ✓ **自治体内の情報ネットワークの分離・分割による事務効率の低下**
  例：マイナンバー利用事務系のシステムへのデータの取込み、インターネットメールの添付ファイルの取得など

②新たな時代の要請

- ✓ **行政アプリケーションを自前調達方式からサービス利用式へ**
  （政府における「クラウド・バイ・デフォルト」原則）
- ✓ **行政手続を紙から電子へ**（デジタル手続法を受けた行政手続のオンライン化）
- ✓ **働き方改革** (テレワーク等のリモートアクセス)
- ✓ **サイバー攻撃の増加、サイバー犯罪における手口の巧妙化　　等**

「三層の対策」の効果や課題、新たな時代の要請を踏まえ、**効率性・利便性を向上させた新たな自治体情報セキュリティ対策を検討会において検討**し、**本年５月に「三層の対策」の見直しを公表**

※ 主な見直し内容
三層の対策の見直し（マイナンバー利用事務系の分離・LGWAN接続系とインターネット接続系の分割の見直し）、次期「自治体情報セキュリティクラウド」の在り方の提示、昨今の地方公共団体における重大インシデント（例：神奈川県ＨＤＤ流出事案）を踏まえた対策の強化、各地方公共団体の情報セキュリティ体制・インシデント即応体制の強化　　等

※ 現在、「地方公共団体における情報セキュリティポリシーに関するガイドライン」について改定作業中

地方公共団体のテレワークのセキュリティに関する通知について

新型コロナウィルスへの対応等を踏まえたテレワークセキュリティ要件について（令和２年８月18日通知）

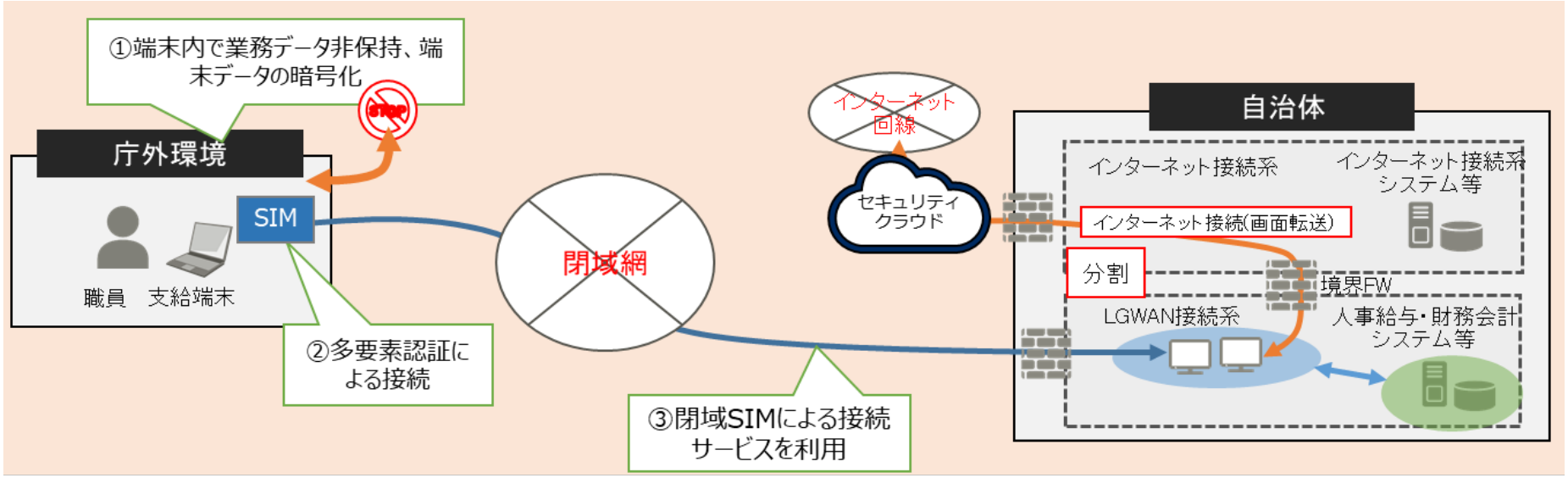
【通知の概要】

○　自治体におけるコロナウィルスへの対応等による業務継続や働き方改革の要請の急速な高まりを踏まえ、従来から通知していた閉域ＳＩＭによる接続サービスを利用したテレワーク方式に加え、比較的速やかに導入が可能なインターネット回線を使用した安全性の高いテレワーク方式やテレワークの導入に当たっての基本的な考え方等を通知

【通知のポイント】

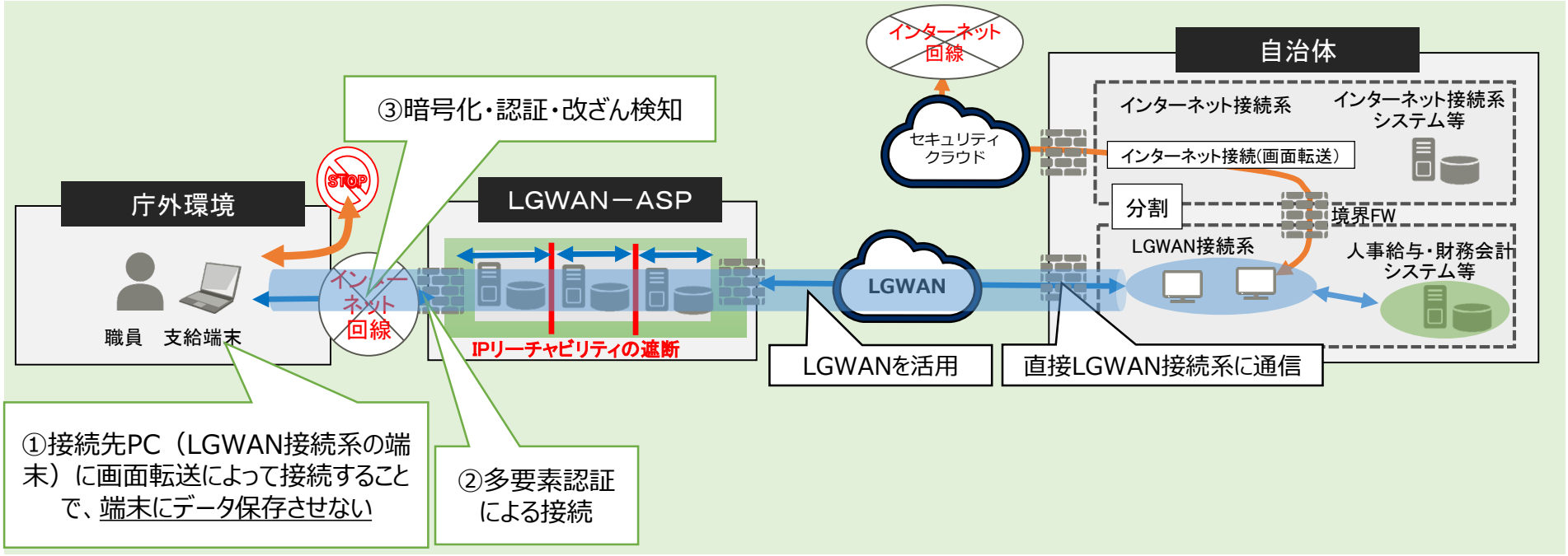
・庁外からのテレワークの検討にあたっては、「取り扱う情報の重要性」を踏まえ、対象資産を明確にすること
・取り扱う情報の重要性によっては、テレワークを認めないように規則を定めたり、アクセス制御などの技術的対策を行うこと
・大量又は機微な住民情報を扱う業務については、庁舎と同等の物理的な対策がなされたサテライトオフィスを除き、テレワークの対象外とすること
・安全性の高いテレワーク方式として以下の方式が想定されること
①閉域SIMによる接続サービスを利用してLGWAN接続系の端末に接続するモデル
②LGWAN-ASPサービスを利用して庁内にあるLGWAN接続系の端末に接続するモデル
③インターネット接続系を経由してLGWAN接続系の端末に接続するモデル

想定される方式①：閉域SIMによる接続サービスを利用してLGWAN接続系の端末に接続するモデル



	区分	留意点	対策のポイント
①	庁外環境の端末	端末の盗難・紛失による情報漏えいへの対策	端末内で**業務データの保存禁止**、**端末データの暗号化**を行う
②	閉域SIMへの接続	なりすましへの対策	閉域SIMに接続する際は**多要素認証**を用いる
③	通信経路	情報の漏えい・改ざんへの対策	**閉域SIMによる接続サービス**を利用する

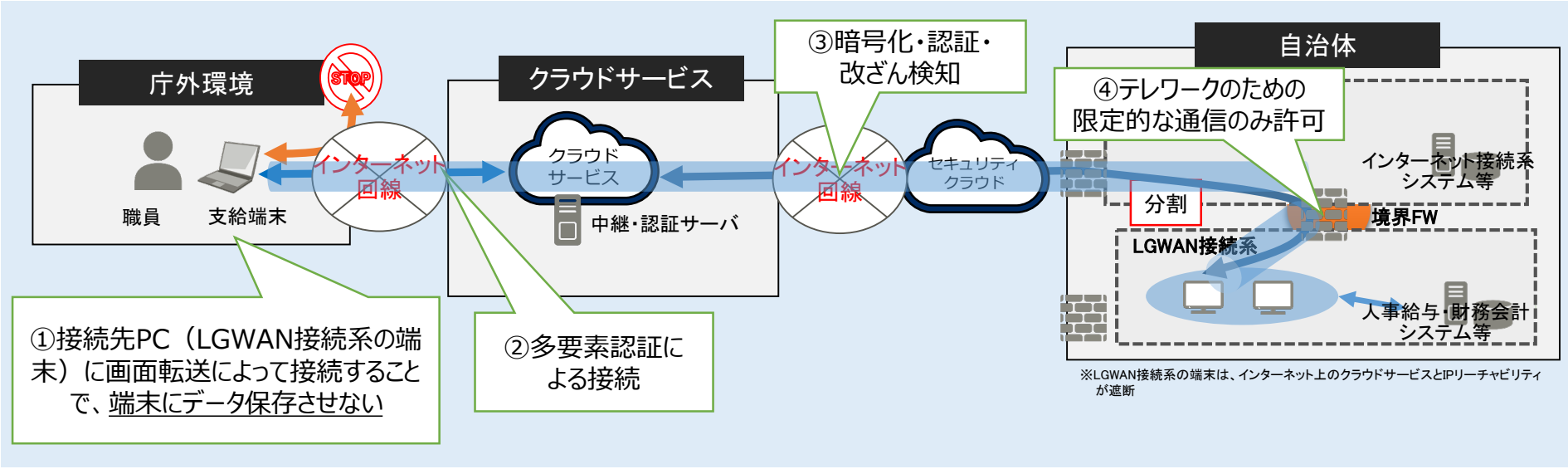
想定される方式②：LGWAN-ASPサービスを利用して庁内にあるLGWAN接続系の端末に接続するモデル



	区分	留意点	対策のポイント
①	庁外環境の端末	端末の盗難・紛失による情報漏えいへの対策	庁内へのリモートアクセスは**画面転送による接続**とし**端末に情報を保存させない**
②	LGWAN-ASP	なりすましへの対策	LGWAN-ASPサービスにログインする際は**多要素認証**を用いる
③	通信経路	情報の漏えい・改ざんへの対策	**通信を暗号化し、認証・改ざん検知**等の仕組み（TLSやIPsecの利用）を設ける

※J-LISが実証実験を予定しており、参加団体を公募を実施（11月11日まで）

想定される方式③：インターネット接続系を経由してLGWAN接続系の端末に接続するモデル



	区分	留意点	対策のポイント
①	庁外環境の端末	端末の盗難・紛失による情報漏えいへの対策	庁内へのリモートアクセスは**画面転送による接続**とし**端末に情報を保存させない**
②	クラウドサービスへの接続	なりすましへの対策	クラウドサービス（中継サーバ等）にログインする際は**多要素認証**を用いる
③	通信経路	情報の漏えい・改ざんへの対策	**通信を暗号化し、認証・改ざん検知**等の仕組み（TLSやIPsecの利用）を設ける
④	LGWAN接続系へのアクセス	原則として、LGWAN接続系とインターネットとの通信は不可	**テレワークのための限定的な通信のみ**LGWAN接続系への通信を許可（LGWAN接続系とインターネット接続間）