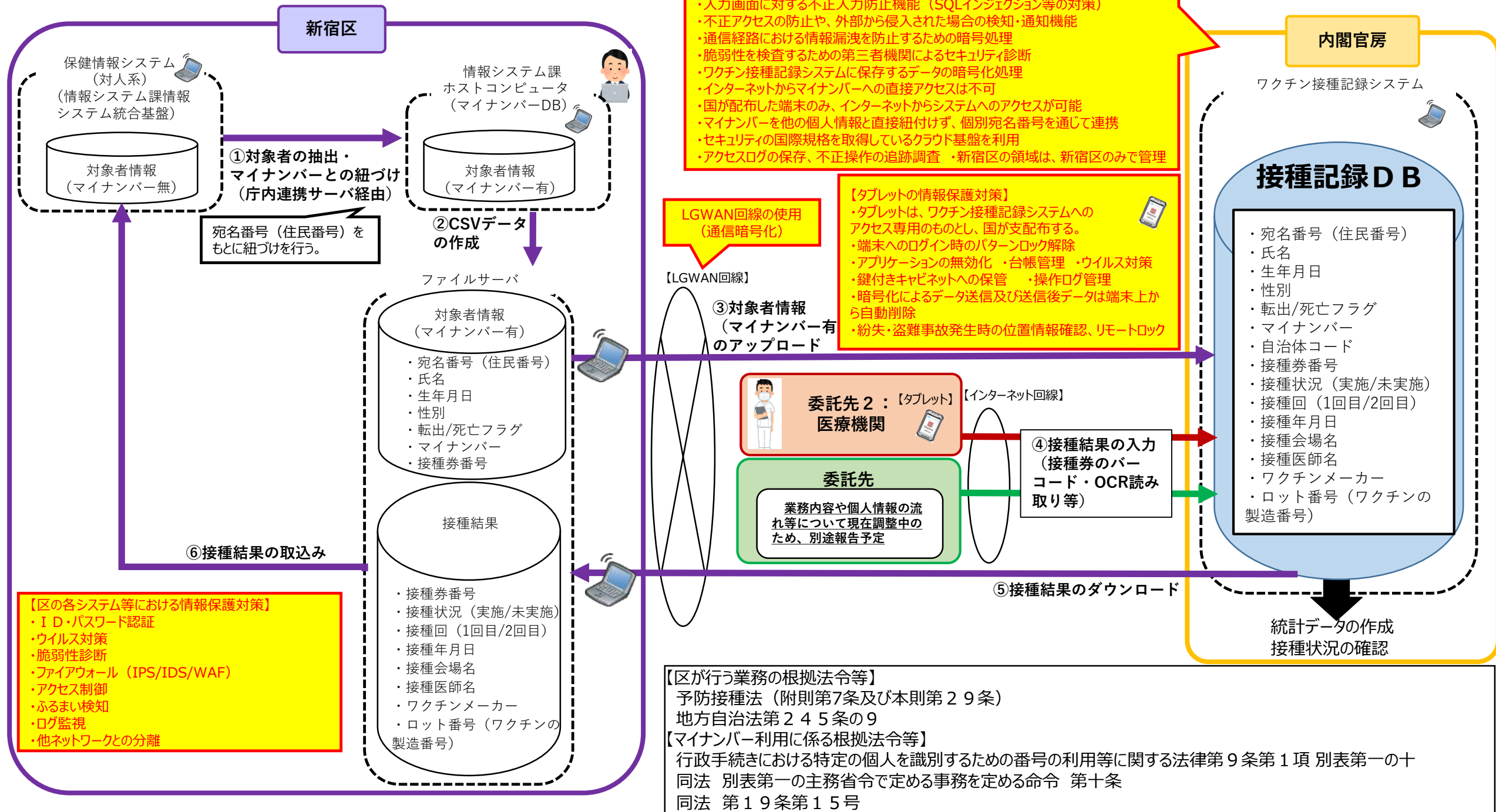


ワクチン接種記録システムとの外部結合に係る個人情報の流れ

(資料47-2)



政府機関の情報セキュリティ対策のための統一基準に準拠して開発・運用を行う。

- ・入力画面に対する不正入力防止機能 (SQLインジェクション等の対策)
- ・不正アクセスの防止や、外部から侵入された場合の検知・通知機能
- ・通信経路における情報漏洩を防止するための暗号処理
- ・脆弱性を検査するための第三者機関によるセキュリティ診断
- ・ワクチン接種記録システムに保存するデータの暗号化処理
- ・インターネットからマイナンバーへの直接アクセスは不可
- ・国が配布した端末のみ、インターネットからシステムへのアクセスが可能
- ・マイナンバーを他の個人情報と直接紐付けず、個別宛名番号を通じて連携
- ・セキュリティの国際規格を取得しているクラウド基盤を利用
- ・アクセスログの保存、不正操作の追跡調査
- ・新宿区の領域は、新宿区のみで管理

【タブレットの情報保護対策】

- ・タブレットは、ワクチン接種記録システムへのアクセス専用のもとし、国が支配布する。
- ・端末へのログイン時のパターンロック解除
- ・アプリケーションの無効化
- ・台帳管理
- ・ウイルス対策
- ・鍵付きキャビネットへの保管
- ・操作ログ管理
- ・暗号化によるデータ送信及び送信後データは端末上から自動削除
- ・紛失・盗難事故発生時の位置情報確認、リモートロック

【区の各システム等における情報保護対策】

- ・ID・パスワード認証
- ・ウイルス対策
- ・脆弱性診断
- ・ファイアウォール (IPS/IDS/WAF)
- ・アクセス制御
- ・ふるまい検知
- ・ログ監視
- ・他ネットワークとの分離

【区が行う業務の根拠法令等】

予防接種法 (附則第7条及び本則第29条)

地方自治法第245条の9

【マイナンバー利用に係る根拠法令等】

行政手続きにおける特定の個人を識別するための番号の利用等に関する法律第9条第1項 別表第一の十 同法 別表第一の主務省令で定める事務を定める命令 第十条 同法 第19条第15号