セキュリティ対策 ❸

外部・内部からの不正アクセス防止

外部、および内部からの不正アクセスを防止するため、システム的な対策を実施しています。

外部からの不正アクセスの予防

- ✓ 多段にファイアウォールを設置し、必要な通信以外を遮断します。
- ✓ 不正アクセスの検知時は、必要に応じた被害拡大の防止、調査、対策を実施します。

システムへのアクセス制御と操作ログの取得

- ✓ 運用担当者がサーバへアクセスする際は、事前レビュー・承認を必要とする他、専用のGWサーバ（SecureCube / Access Check）上で認証・接続制限とログの取得を実施します。

※ SecureCube / Access Check はNRIセキュアが開発・販売している製品です。（参考 P.14）

外部からの不正アクセスの検知

- ✓ WAF（Web Application Firewall）を設置し、不正な攻撃パターンを検知します。検知後は、必要に応じた対策を実施します。

開発環境と運用環境の分離

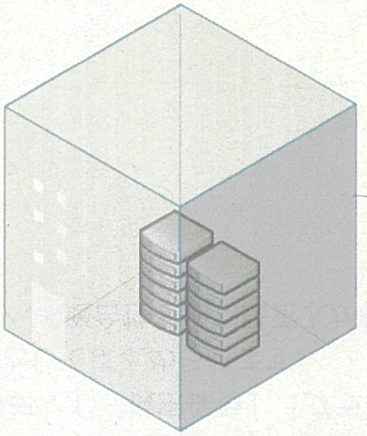
- ✓ 開発、運用チームの分離を行っており、メンバーの兼務はありません。

セキュリティ対策 ❹

サーバの物理的な保護

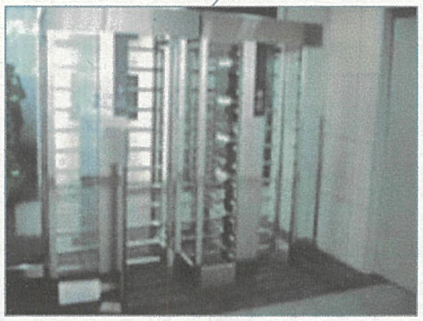
野村総合研究所の**Tier4相当の堅牢なデータセンター**内で運用・管理されています。

- ✓ 敷地内には**赤外線監視カメラ**を設置し、24時間有人監視を実施し、不正入館を防ぎます。
- ✓ 入館時には顔写真付き身分証明書による本人確認に加え、**マントラップゲート**を設置し、共連れを防ぎます。
- ✓ 各エリア毎に設けられた**生体認証装置**により、アクセス範囲を徹底的に制御しています。



- ✓ 本番データが入った媒体のデータセンターからの持出しは原則禁止しており、必要がある場合には事前許可・確認が必須となります。
- ✓ 出口では**X線検査装置**に加え、国内初となる**3Dホログラフィックボディスキャナー**を設けており、機器・媒体の持出しを徹底的に監視しています。

赤外線監視



マントラップゲート

生体認証装置

3Dホログラフィックボディスキャナー

【ご参考】第三者によるデータセンター評価

クラウド便が稼働している野村総合研究所のデータセンターでは、「セキュリティ」および「可用性」について**SOC2報告書**を取得しており、データセンター監査の代替として**SOC2報告書**の閲覧が可能です。

SOC２報告書とは

米国公認会計士協会（AICPA）が定めたトラストサービス規準(Trust Service Criteria)に従って実施されます。
「セキュリティ」「可用性」「処理のインテグリティ」「機密保持」「プライバシー」の五つから一つ以上を選択（複数選択可能）し評価が行われ、詳細な報告書（SOC2報告書）としてまとめられます。
グローバル基準（国際保証業務基準ISAE3000）への適合性を独立監査人が厳格な審査の上で、保証した評価基準で**国際的に信頼性が高い**とされています。

費用

無料で閲覧していただくことが可能です。
報告書は郵送いたします。

【注意事項】

① 複写は厳禁です。
　米国公認会計士協会の基準により、SOC2報告書の全部あるいは一部をコピーすることは禁じられています。
② 貴社及びその独立監査人のみの利用に限定され、それ以外の第三者に開示・漏えいすることは禁じられています。
③ 上記①②に同意する旨の受領書に、記名・押印いただき返送いただきます。

システム障害への対策

可用性を維持するための対策、及びセキュリティ対策の定期的な見直しを実施しています。

障害対策

✓ 機器の冗長化

サーバ、ネットワーク機器は冗長化構成をとっており、障害時は自動的にロードバランス、もしくは待機系に切り替えて、サービス停止を最小限にします。

✓ ネットワークの冗長化

複数の国内大手ISP社と、それぞれ1Gbpsのバックボーン帯域で結ばれているため、プロバイダ障害時にも継続してサービス利用が可能です。

✓ 電源の冗長化

電源は二重系統（それぞれ別変電所より配電）、蓄電池、自家発電装置を有しており、災害時などの停電に備えています。

障害検知・復旧

✓ 24時間365日監視

24時間365日、セキュリティ専門家がサービスの監視、サイバー攻撃のモニタリングを実施しています。障害を検知した場合には、弊社担当者へ通知されます。

✓ NCSIRTとの連携

自社内にNCSIRT（NRI-Secure Cyber Security Incident Response Team）を設けており、運用担当者と密に連携しています。新たな脅威に対しても、迅速に対処する体制・スキルを有しています。

※NCSIRTは、24時間体制でセキュリティモニタリングやインシデントハンドリングおよびセキュリティ情報の収集発信を行っている、弊社のセキュリティアナリストチームです。

NCSIRT

セキュリティ診断の実施

✓ プラットフォーム診断（月1回）、Webアプリケーション診断（年1回以上）、ペネトレーションテスト（年1回以上）を実施しています。

パッチの適用

✓ セキュリティ情報をモニタリングしており、新たなパッチが出た場合、①評価／テスト⇒②適用有無の判断⇒③リリースまでを迅速に行う体制があります。

セキュリティ対策 ⑥

組織および人材面での対策

組織および人材でのセキュリティ対策は、定期的な監査や見直しを実施しています。

分類	項目	クリプト便における対応
組織	✓ **組織体制の整備** 安全管理措置を講ずるための組織体制を整備する	管理規定において、組織体制は明記されている
	✓ **取扱規程等に基づく運用** 取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録	システムログは1年以上の長期保存をしている。顧客の利用実績は、顧客ごとの契約で取り決めている
	✓ **取扱状況を確認する手段の整備** 機密情報ファイルの取扱状況を確認するための手段を整備する。なお、取扱状況を確認するための記録等には、機密情報等は記載しない	NRIセキュアは機密情報を取り扱わないサービス仕様になっている。（ファイルは暗号化されてサーバに保管されるため、NRIセキュアでは閲覧できない）
	✓ **情報漏えい等事案に対応する体制の整備** 情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等を早急に公表すること	不測事態対策委員会が常設機関として存在し、事案が発生した際には、被害や損失を最小限にとどめ、かつ一刻も早い定常状態への復旧・回復を行うために、迅速かつ的確な対応行動がとれるようになっている
	✓ **取扱状況の把握及び安全管理措置の見直し** 機密情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む	監査委員が監査責任者の指揮のもと、機密情報の取扱い状況の評価を実施し、報告書を作成する。その結果でルールの見直しおよび改善が行われる
人材	✓ **事務取扱担当者の監督** 事業者は、取扱規程等に基づき適正に取り扱われるよう、担当者に対して監督を行う	ISMSおよびセキュリティ格付けによる外部監査、さらに内部監査に基づき、担当者が適正に処理を行っているかを監査している
	✓ **担当者の教育** 事業者は、機密情報の適正な取扱いを周知徹底するとともに適切な教育を行う	研修やOJTで、機密情報の取扱やセキュリティに関する教育を実施している
	✓ **機器及び電子媒体等の廃棄** 機密情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する	媒体破棄の場合には、破棄した記録は書面で管理される。ファイルの削除については、システムで自動的に削除を実施し、ログに削除された事が記録される

【ご参考】第三者機関によるセキュリティ評価

情報セキュリティ専門企業だから実現できる堅牢なセキュリティ。第三者機関からも高い評価を得ています。

ISO/IEC 27001

NRIセキュアは、ISMS（情報セキュリティマネジメントシステム）の国際規格であるISO/IEC 27001認証を全社で取得。
クリプト便においても、規格にのっとった、厳格なセキュリティマネジメントを実施しています。

IS 75215/ISO 27001:IJ 00347
ISO IEC 27001を全社で取得しています。
※ 国内事業所に限る

ISO/IEC 27017　ISO/IEC 27018

クリプト便は、クラウドサービスプロバイダとしてクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」、および、クラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」の認証※を取得しています。

CLOUD 712951　PII 712952

※ クラウドサービスに関する国際規格であるISO/IEC 27017に基づくISMSクラウドセキュリティ認証(JIP-ISMS517-1.0)、およびISO/IEC 27018に基づくプライベート認証を取得。

情報セキュリティ格付け最高位「AAAis」

クリプト便の運用業務に対して、日本セキュリティ格付機構より、情報セキュリティ格付け最高位※の「AAAis」を付与されました。

※ 2021年9月現在サービス最高レベルの格付け

AAAisで求められる2つの用件

- **要件1：**新たな脅威に迅速に対応し、常時、高水準の管理状態を維持、発展させている
- **要件2：**常時、リスクをモニタリングし、即時に柔軟な対応ができる

PCI DSS

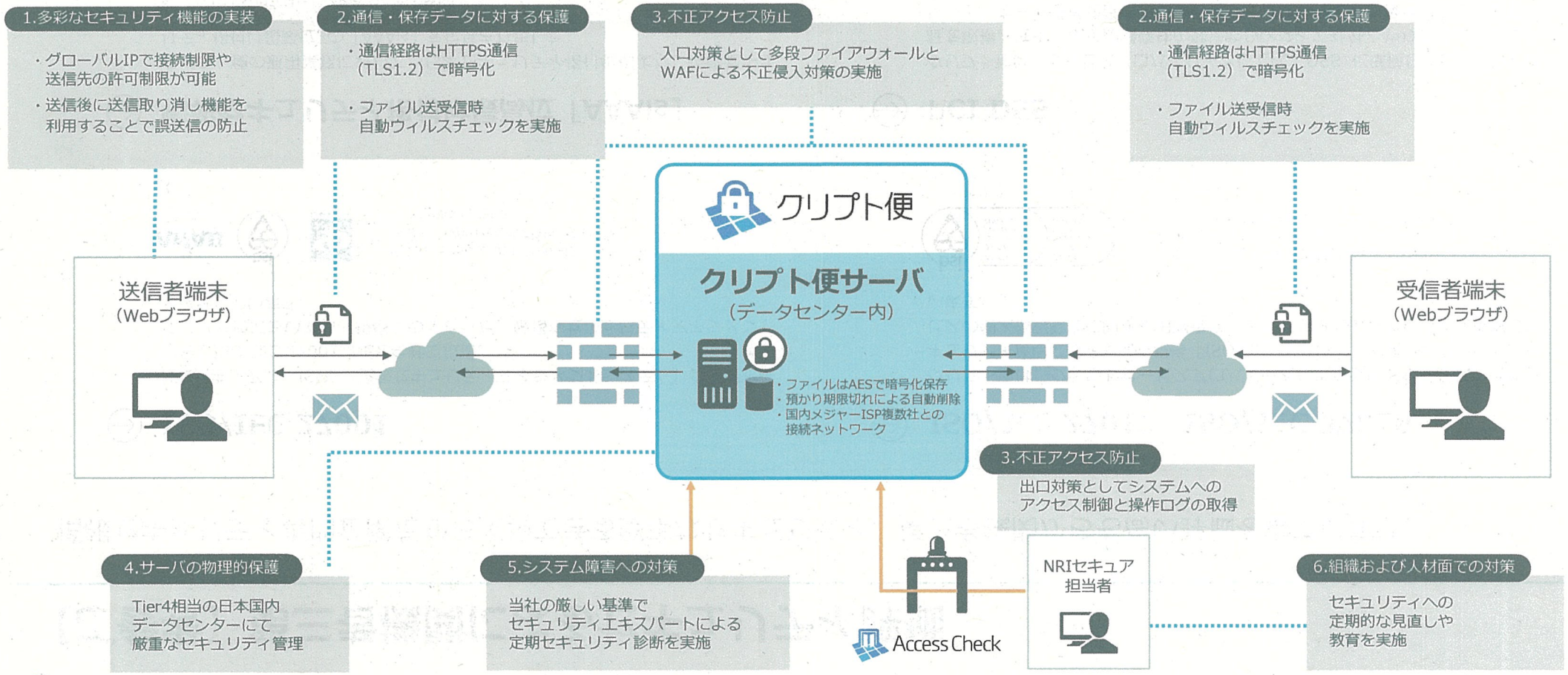
クリプト便は、サービスプロバイダーとしてPCI DSS※に準拠したことを示す認証を取得。従来、電子記録媒体の郵送やFAXなどで社外とやり取りしていたクレジットカード番号を含む重要情報も、クリプト便で取り扱うことが可能です。

GRCS - 2105

※ PCI DSS：Payment Card Industry Data Security Standardsの略称。クレジットカード情報の漏えいを防止するために、策定されたクレジットカード業界における国際的なセキュリティ基準。

クリプト便のセキュリティ対策

クリプト便は情報セキュリティベンダーならではの高度なセキュリティ対策を実施。安心してご利用いただけます。



クリプト便の強みとは

クリプト便

クリプト便の強みは「**総合力の高いセキュリティ**」です。

抜け漏れのない万全な環境下で、お客様のファイルを

安全・確実に送受信することを実現させます。

NRI SECURE

www.nri-secure.co.jp

資料1-2

「自治体の情報システムについて」

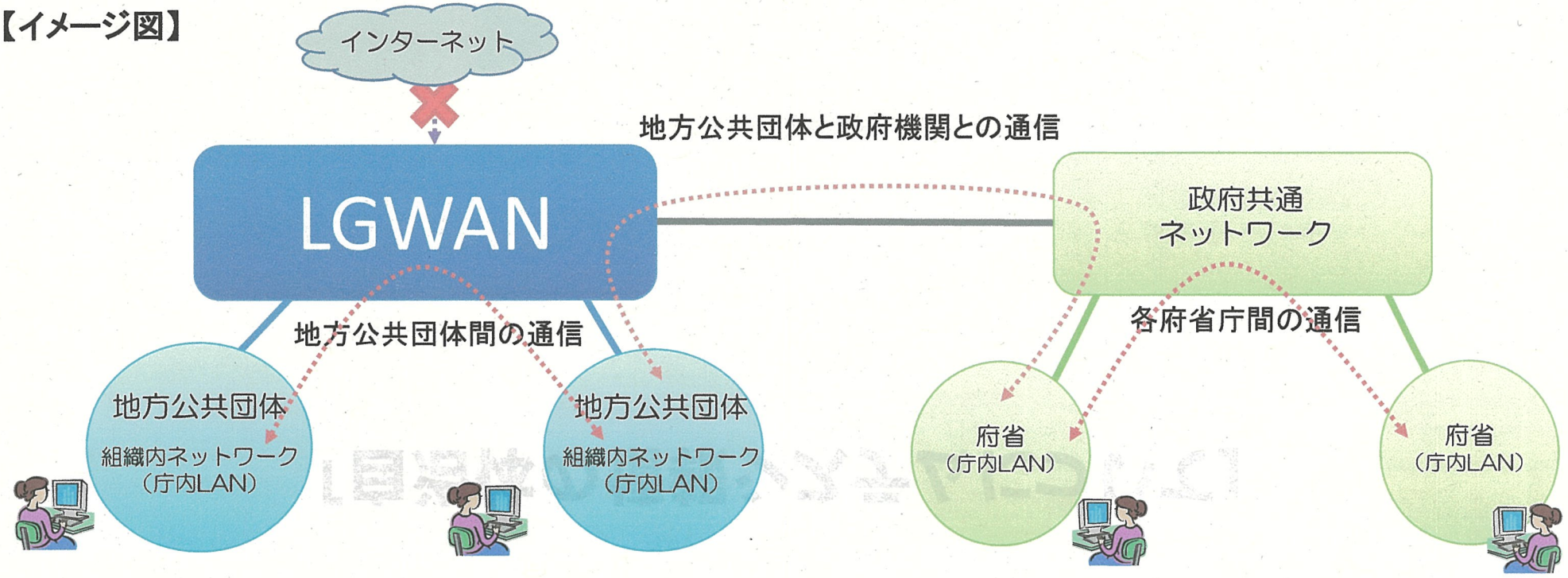
令和3年6月30日
総務省自治行政局

LGWAN（総合行政ネットワーク）の概要

○　LGWAN（総合行政ネットワーク）は、地方公共団体間や地方公共団体と政府機関間の通信を行うためのインターネットから分離された行政専用ネットワーク。

・平成13年度に全都道府県で構成される協議会により設置され、平成15年度に全市区町村が接続し本格運用開始。
　平成26年度に地方公共団体情報システム機構（J-LIS）に移管された。
・地方公共団体間の回線を集約することにより、高度なセキュリティを確保しつつ、コストを削減。

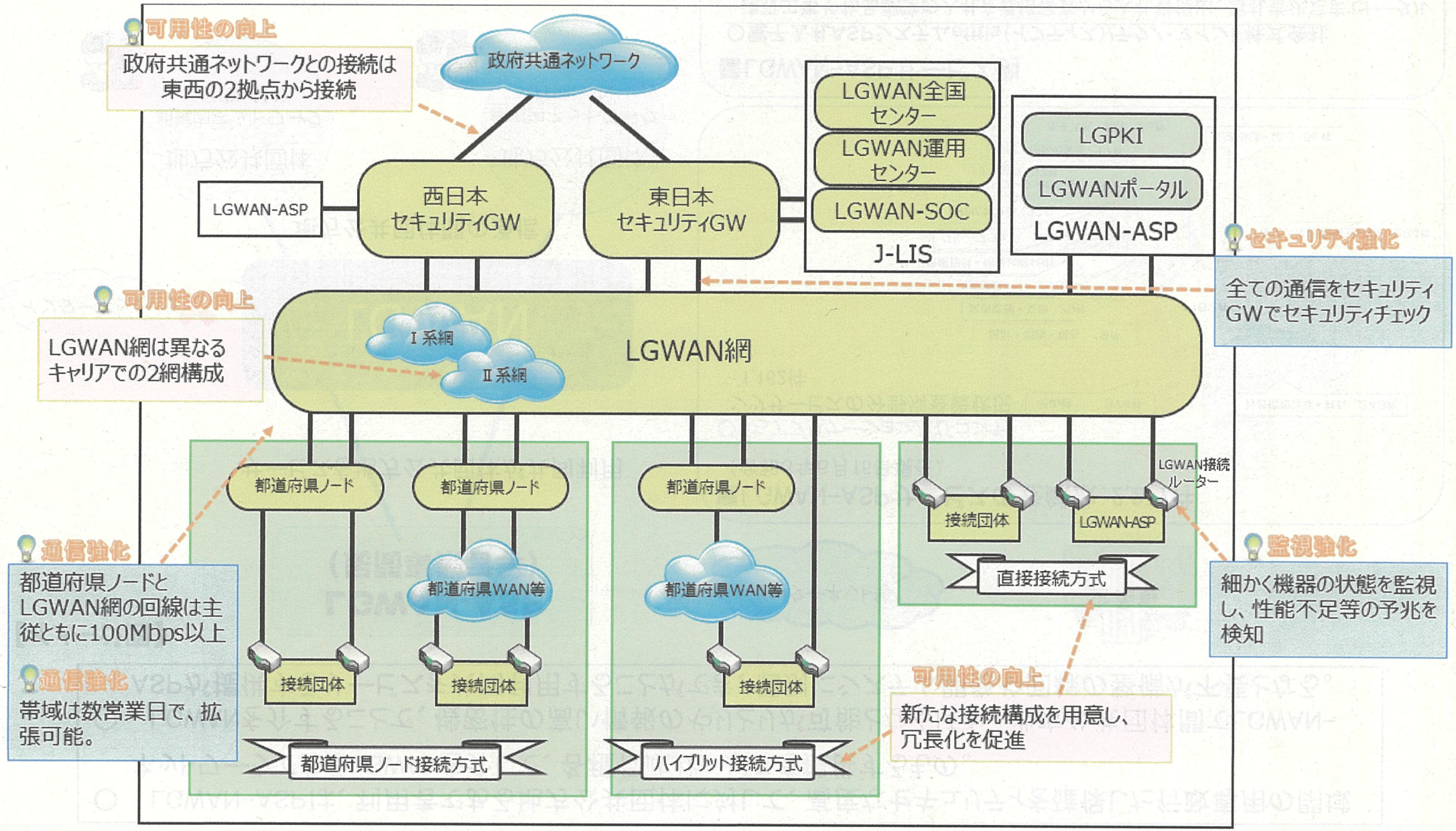
【イメージ図】



【通信されている主な情報（例）】

・地方公共団体間、地方公共団体と政府機関間のメールの送受信
・マイナンバーを用いた情報連携（税情報や社会保障の給付状況（年金情報、生活保護情報）等）
・地方税の電子申告の受付、国税庁から地方公共団体への申告情報の提供
・マイナンバーカードを活用した各種証明書のコンビニ交付
・防災・人命に係る緊急情報（J-アラート）　等

LGWANの構成（第四次LGWAN）

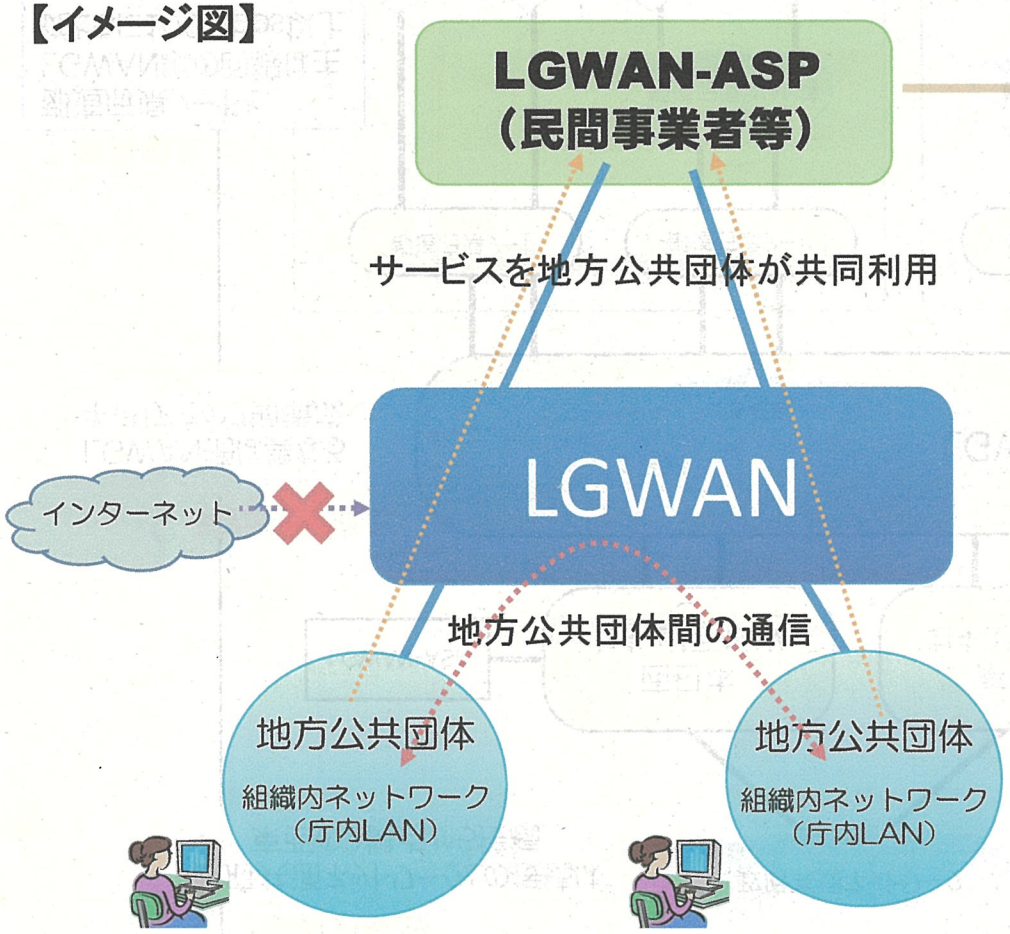


LGWAN-ASP（LGWAN-Application Service Provider ）の概要

○　LGWAN-ASPは、利用者である地方公共団体に対して、高度なセキュリティを確保した行政専用の閉域ネットワークであるLGWANを介して、各種行政サービスを提供するもの。

○　LGWANを介することで、機密性の高い情報のやりとりが可能となるほか、地方公共団体間でLGWAN-ASPが提供するサービスを共同利用することができ、個別にシステム開発や回線の整備が不要となる。

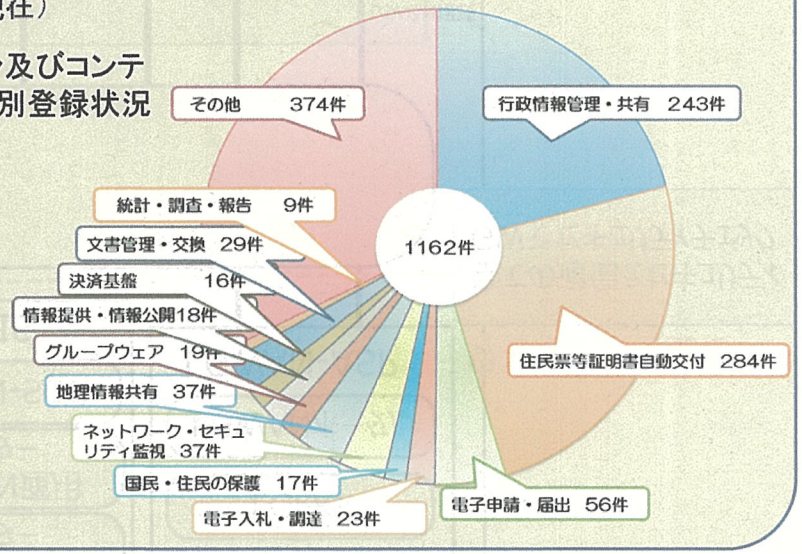
【イメージ図】



■LGWAN-ASPサービスの登録数：2,277件

（令和3年6月16日現在）

○うちアプリケーション及びコンテンツサービスの分野別登録状況：1,162件



■LGWAN-ASPサービス例

○電子入札ASPシステムefftis（イフティス）/テクノ・マインド株式会社

建設工事や物品調達の入札を資格審査から入札書提出、落札者決定までトータルでサポートし、入札業務の効率化を図るサービス。

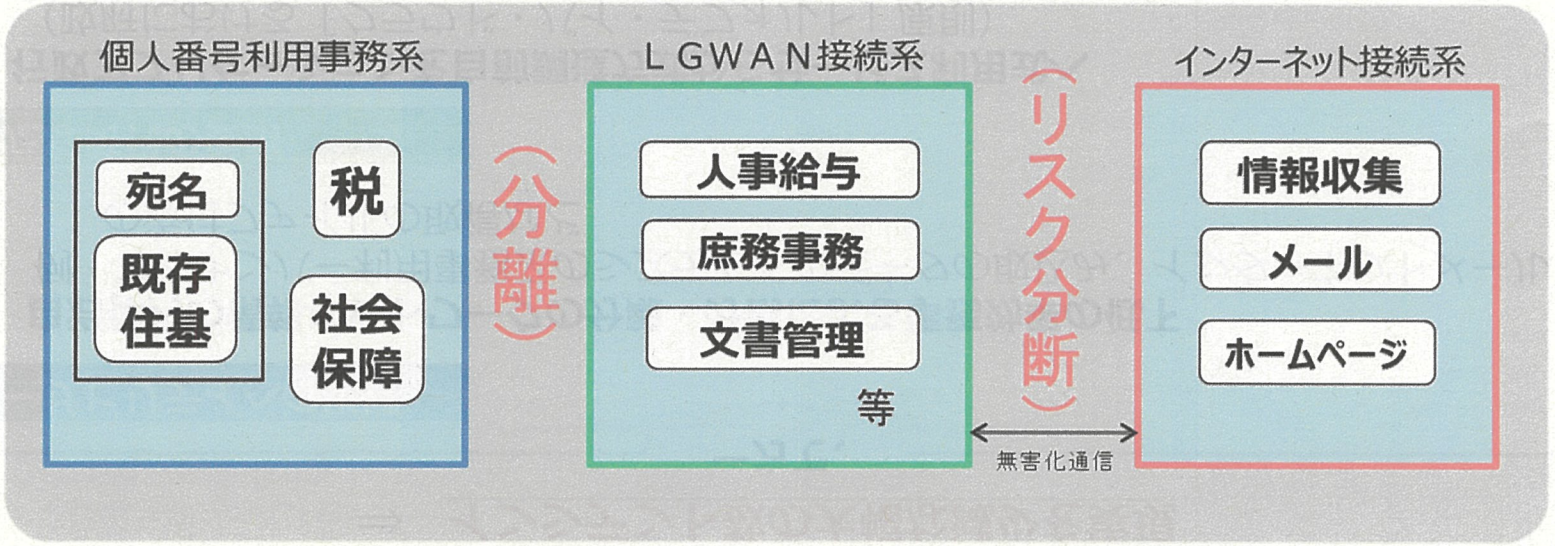
○人事給与システム/株式会社エイチ・アイ・ディ

情報の一元管理を行い、人事情報管理・給与計算・年末調整計算・実態調査・予算推計・決算統計等の機能を提供。

「三層の対策」によるセキュリティ強化

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
〔2015.10　マイナンバー法（行政手続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）の施行〕
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

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

「三層の対策」の見直し

「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、**令和２年５月に「三層の対策」の見直しを公表**

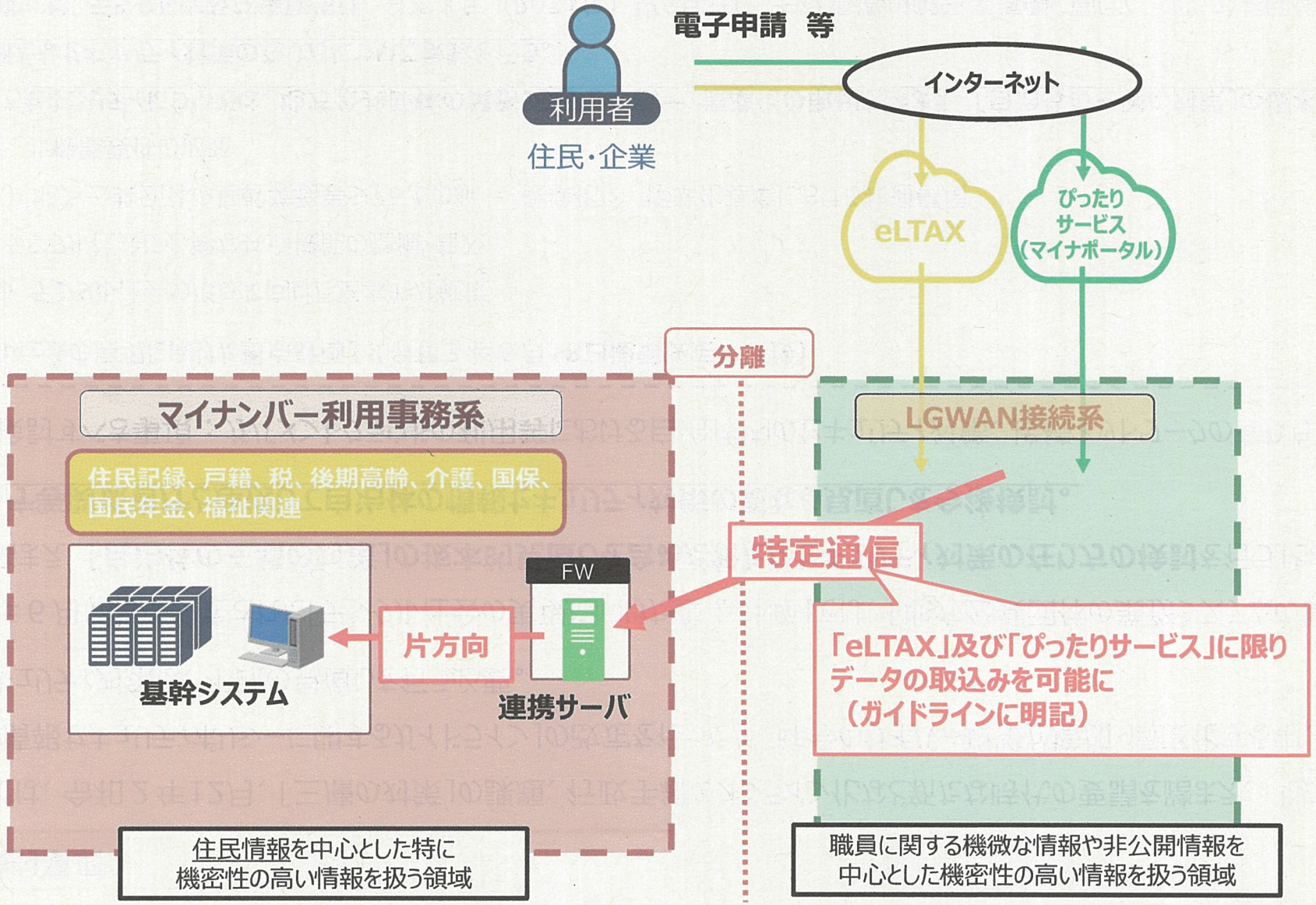
上記とりまとめを踏まえ、「地方公共団体における情報セキュリティポリシーに関するガイドライン」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」を改定（令和２年12月28日）

※ 主な改定内容

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

「自治体情報セキュリティ対策の見直し」のポイント（令和2年5月22日公表）

マイナンバー利用事務系の分離の見直し



自治体情報セキュリティ対策に関する今後の検討

今後の検討事項

○ 総務省では、令和２年12月、「三層の対策」の課題、行政手続のオンライン化など新たな時代の要請を踏まえ、「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」の改定を行ったが、昨今のサイバー攻撃が増加・高度化する中、自治体の情報セキュリティ対策は、不断の見直しを行う必要。

○ 令和３年６月に閣議決定された「デジタル社会の実現に向けた重点計画」では、「地方公共団体の業務システムの標準化・共通化を踏まえ、**「自治体の三層の対策」の抜本的見直しを含めた新たなセキュリティ対策の在り方の検討**を行う」とされており、**デジタル庁等関係省庁と連携して自治体の情報セキュリティ対策の更なる見直しを今後検討。**

※検討すべき事項：ガバメントクラウドの利用等における自治体内のセキュリティ対策、接続ネットワークの在り方　等

○「デジタル社会の実現に向けた重点計画」（令和３年６月18日閣議決定）（抄）

第２部　デジタル社会の形成に向けた基本的な施策

１．デジタル社会に必要な共通機能の整備・普及

（３）地方公共団体の基幹業務等システムの統一・標準化②　標準化基準における共通事項

イ　非機能要件の拡充

このうち**セキュリティについては、地方公共団体の業務システムの統一・標準化の取組を踏まえ、「自治体の三層の対策」の抜本的見直しを含めた新たなセキュリティ対策の在り方について検討を行う。**

具体的には、デジタル庁及び総務省は、令和３年（2021年）夏を目途に、先行事業の検証・実稼働に向けて、地方公共団体のガバメントクラウド活用に関するセキュリティ対策に関する要件を整理した上で、先行事業を通じた検討も踏まえつつ、**令和４年度（2022年度）の夏を目途に、基幹業務等のシステムの標準化基準の作成とあわせて、地方公共団体のガバメントクラウド活用に関するセキュリティ対策の方針を決定する。**

自治体におけるクラウドの活用とセキュリティポリシーガイドラインの関係

○ **各地方公共団体は組織の実態に応じて情報セキュリティポリシーを策定し、自らの責任で情報セキュリティ対策を実施**。

○ 総務省では、**地方公共団体の情報セキュリティポリシーを策定する際の参考として、「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」を作成し、地方公共団体に対して助言**。

○ 当ガイドラインでは、自治体におけるクラウドの活用にあたり、主に以下の事項について規定。

第２編　地方公共団体における情報セキュリティポリシー（例文）
　第２章　情報セキュリティ対策基準（例文）
　8.外部サービスの活用
　8.4クラウドサービスの利用
　①情報セキュリティ管理者は、クラウドサービス（民間事業者が提供するものに限らず、本市が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。
　②**情報セキュリティ管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない**。（※）
　③情報セキュリティ管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。
　④情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。
　⑤情報セキュリティ管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

第３編　地方公共団体における情報セキュリティポリシーガイドライン（解説）　抜粋
（※）インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、**住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある**。

個人情報保護法改正後の個人情報の管理のあり方

■個人情報保護制度の見直しに関するタスクフォース「個人情報保護制度の見直しに関する最終報告」（令和2年12月）抜粋

現在、地方公共団体の条例には、オンライン結合（通信回線を通じた電子計算機の結合をいう。）による個人情報の提供について、行個法にはない制限規定を置く例が多く見られる。

しかし、**ＩＴの活用は行政サービスの向上や行政運営の効率化に大きく寄与しており、個人情報の流通に限り物理的な結合を禁止することは合理性を欠く**ものであり、場合によっては、個人情報の円滑な利用を阻害して国民に不利益を被らせるおそれもある。また、**行個法においては、オンライン結合制限規定がなくとも、第６条、第８条等により、個人情報の安全性の確保等が図られている**。このため、オンライン結合制限規定を置くことは不要になると考えられ、共通ルールには当該規定は設けないこととすることが適当である。

その場合、**地方公共団体等は、情報セキュリティを含めた安全確保措置の在り方や目的外利用・提供の「相当な理由」や「特別な理由」の具体的な判断に資するために国が示すガイドライン等に基づいた運用を行うことによって、個人情報を適切に管理し、みだりに利用・提供しないことを担保していくことが望ましい**。

■改正後の個人情報保護法の内容

・地方公共団体についても、現在の「行政機関の保有する情報の保護に関する法律」（以下、行個法）と同様に、**安全確保措置（第66条　※行個法第6条に相当）や目的外利用・提供の制限（第69条 ※行個法第8条に相当）等の適切な運用により、個人情報を管理する**こととされた。

○改正後の個人情報の保護に関する法律（抄）

（安全管理措置）

第六十六条　行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

2　前項の規定は、次の各号に掲げる者が当該各号に定める業務を行う場合における個人情報の取扱いについて準用する。

一　行政機関等から個人情報の取扱いの委託を受けた者　当該委託を受けた業務

二～四　略

五　前各号に掲げる者から当該各号に定める業務の委託（二以上の段階にわたる委託を含む。）を受けた者　当該委託を受けた業務

（利用及び提供の制限）

第六十九条　行政機関の長等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

2　前項の規定にかかわらず、行政機関の長等は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

一　本人の同意があるとき、又は本人に提供するとき。

二　行政機関等が法令の定める所掌事務又は業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当の理由があるとき。

三　他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当の理由があるとき。

四　前三号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由があるとき。

3～4　略

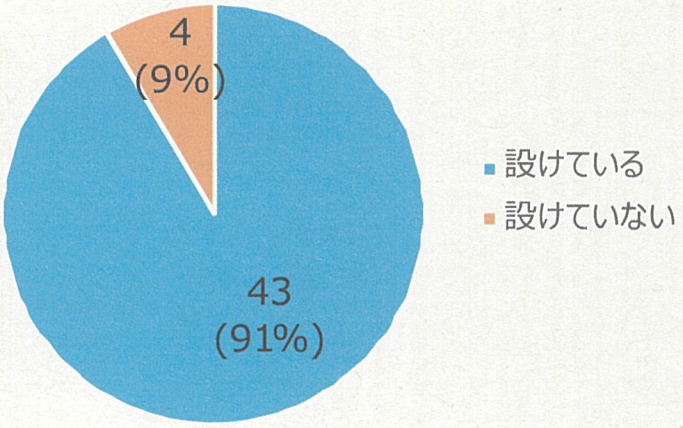
（参考）オンライン結合制限に係る個人情報保護条例の規定

令和２年11月27日第10回「個人情報保護制度の見直しに関する検討会」（内閣官房）資料３より抜粋

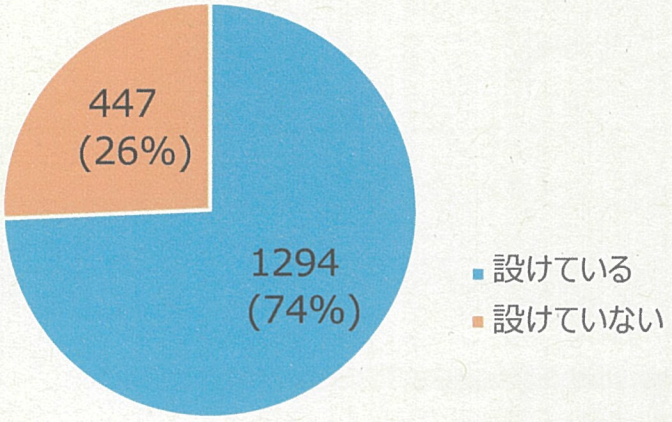
- オンライン結合による個人情報の外部提供を制限する規定を、都道府県では９割程度、市区町村では７割程度の団体が設けている。
- 規定を設けている団体における外部提供を可能とする要件は以下のとおり。

【オンライン結合制限規定を設けているか】

都道府県



市区町村



【外部提供を可能とする要件について】

（都道府県）

外部提供について、法令の定めがある場合、犯罪捜査を目的とする場合その他公益上の必要性があると認められること。	35団体	81. 4%
個人の権利利益を侵害するおそれがないと認められること。	20団体	46. 5%
個人情報の漏洩のおそれがないと認められること。	18団体	41. 9%
その他	31団体	72. 1%

（市区町村）

外部提供について、法令の定めがある場合、犯罪捜査を目的とする場合その他公益上の必要性があると認められること。	1,044団体	80. 7%
個人の権利利益を侵害するおそれがないと認められること。	738団体	57. 0%
個人情報の漏洩のおそれがないと認められること。	425団体	32. 8%
その他	513団体	39. 7%

＜「その他」の例＞
- 本人の同意があるとき。
- 個人の生命、身体又は財産の安全を守るため緊急かつやむを得ないと認められるとき。
- 国、独立行政法人等以外の地方公共団体又は地方独立行政法人に提供するとき。
- 事務の目的、内容等に鑑み、行政サービスの向上、事務処理の効率化に資するなど社会一般の利益を図るために必要であること。
- 個人情報保護審査会の意見を聴くこと。
- 必要な保護措置（セキュリティ対策）を講じていること。