栃木県
次期情報インフラ
更新方針

令和４（2022）年２月

1.次期情報インフラ更新に関する全体的な考えと背景

2.目指すべき方向性と現状インフラの課題

3.新しい働き方の要点

4.次期情報インフラへの変更ポイント

5.次期情報インフラ更新方針作成の経過

6.スケジュール

7.無線LANとSIM併用の必要性

8.セキュリティ対策

1. 次期情報インフラ更新に関する全体的な考えと背景

外部環境の変化

社会的な電子化ニーズの増大

●若年層を中心に生活のデジタル化が進んでおり、行政サービスの電子化が求められている

●タブレット等利便性の高い機器やオンラインサービスが広まっており、民間ではサービスの電子化環境が整いつつある

業務デジタル化の必要性の高まり

●デジタル社会形成基本法に基づく業務の標準化、行政機関相互のさらなる連携等が求められている

●感染症対策などから対面業務、事務室業務を見直す必要が生じている

現状の問題

1.県民視点

●証明書取得や行政手続は、特定の窓口や平日の昼間に行かなければならない

●行政サービスを申請する際、申請先ごとに同じ内容(名前、住所など)を記載する必要がある

2.職員視点

1. 働く場所に制約があり、多様な働き方の実現が困難である
2. 緊急的な執務室の変更に対応できていない
3. 業務が属人化しており、特定の人物がいないと業務が回らない

3.業務視点

1. 庁内における類似業務の処理手順に違いがあり、非効率が生じている
2. デジタル技術を活用できておらず、膨大な定型業務を人力処理している

- 職員数が限られ、行政課題が複雑多様化する中、効率的に働くための環境が整備されていない。ワークライフバランスの観点でも柔軟に働ける環境が不十分である。
- 情報セキュリティの観点から、業務環境がインターネットと分離されているため、便利なICTツールの利用が限られ、住民サービスの向上、業務効率化につなげにくい状況である。

2. 目指すべき方向性と現状インフラの課題

目指すべき方向性

1.県民視点

1. 行政サービスがオンラインで受けられる環境の整備
2. 申請書への住所、氏名等の記載を可能な限り不要とする仕組みづくり

県民サービスの充実

2.職員視点

1. 多様な働き方を実現
2. 執務体制の変更に柔軟に対応できるオフィスづくり
3. どこにいても必要な情報や状況を共有可能な環境を整備、業務の属人化を減少

職員の働き方改革・生産性向上

3.業務視点

1. 全庁横断的な業務改革を行い、統一した効率化手法を検討
2. ICTツールの活用により、県民サービスの向上させる

業務効率化

現状インフラの課題

- 業務システムは、セキュリティレベルの高いLGWAN系に集約しており**外部からアクセスしにくい**
- 庁内ネットワークは、インターネットに接続されておらずWeb会議等で専用端末が必要であり、**端末コスト、通信コストが増加**
- 業務端末からはLGWAN上のサービスしか利用できず、インターネット上の**利便性の高い様々なサービスが選べない**

職員の声　（DX推進員研修での調査から抽出）

県民サービスの質を高めるとともに、効率的かつ効果的に業務を行えるインフラの整備が必要

（参考）国の方針、他自治体や民間企業の例

- **骨太の方針(経済財政運営と改革の基本方針2021)**
  官民挙げたデジタル化の加速(デジタル・ガバメントの確立)、少子化の克服、子供を産み育てやすい社会の実現

- **DX推進手順書**
  BPRの取組みの徹底、自治体の行政手続のオンライン化、自治体のAI・RPAの利用推進、テレワークの推進、セキュリティ対策の徹底

- **他自治体の先進事例**
  埼玉県：業務端末をモバイル化、全台にSIMを導入（R3年度から順次導入）
  静岡県：業務端末をモバイル化、全台にSIMを導入（R2年度）
  神奈川県：業務端末をモバイル化、全台にSIMを導入（H30年度～R3年度）
  広島県：業務端末をモバイル化　https://biz.kddi.com/usecase/case_242/
  茨城県：業務端末をモバイル化、庁舎の全館Wi-Fi化（H30～R3年度）

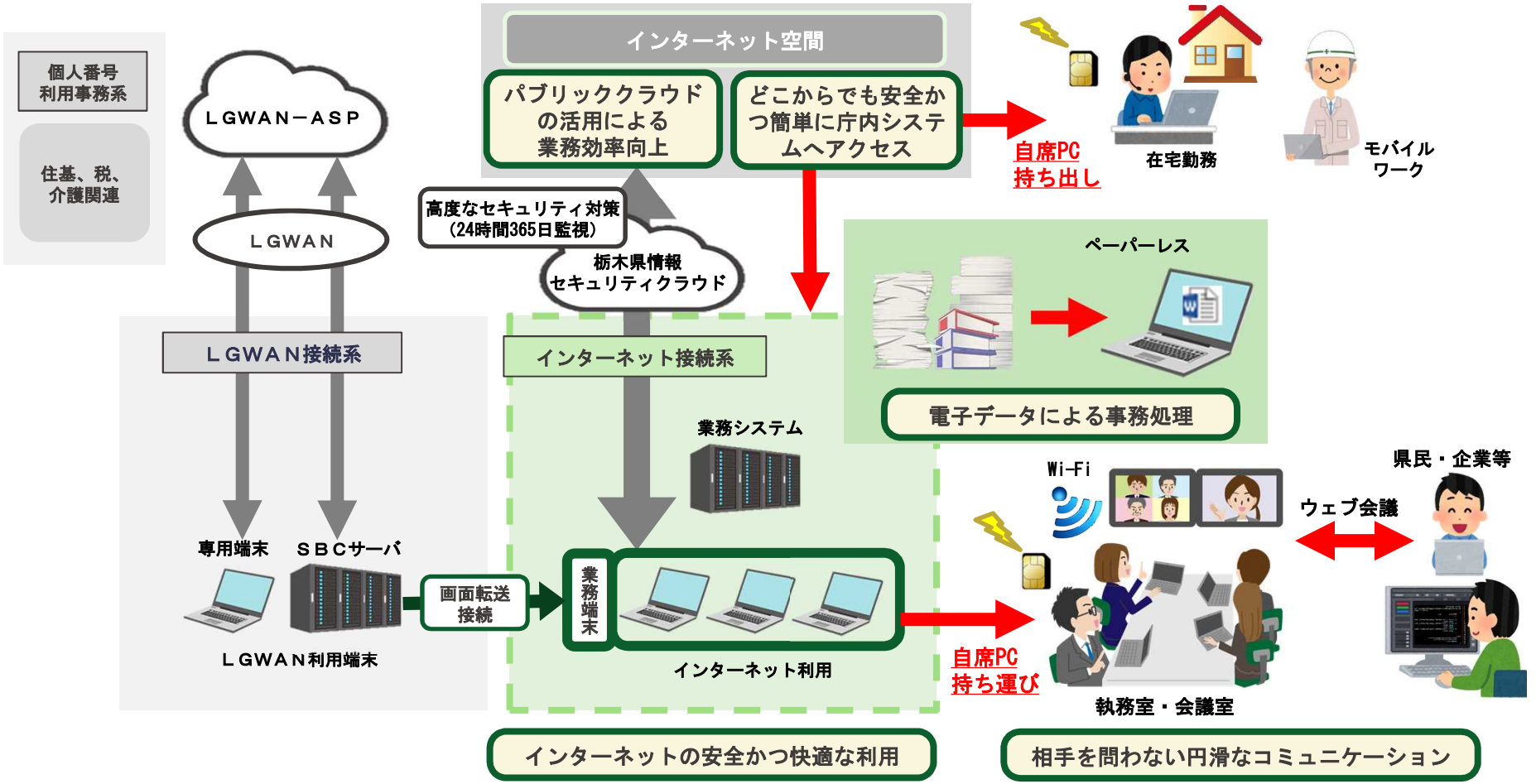
- **民間企業の成功例**
  NTT：転勤・単身赴任を廃止へ　コロナ後もテレワーク　https://www.nikkei.com/article/DGXZQOUC2886R0Y1A920C2000000/
  キャスター：700人全社員フルリモート企業　https://newswitch.jp/p/21467
  大和証券グループ：全社員へのテレワーク制度の導入　http://www.daiwa-grp.jp/data/attach/3069_021_20200302c.pdf

3. 新しい働き方の要点

＜コンセプト＞　**デジタル技術を活用して「どこでも」効率的かつ効果的に仕事ができる環境づくり**

理想	現状	新しい働き方	必要な施策
どこからでもアクセス	・自席でないと業務ができない ・既存端末は持ち出し不可 ・Web会議は専用端末のみ	・場所、時間を問わず必要な時に安全に業務が行える ・端末を変えずにWeb会議が行える	業務プロセス改善 （業務を見直し無駄を省く）
ペーパーレス	・紙を介した情報伝達が中心 ・法令や慣習による押印文化 ・紙から情報を探す非効率性	・紙を介さない情報伝達や決裁 ・押印を極力廃止し電子承認へ ・情報をデータ化し検索性を向上	情報インフラ整備 （必要な機器を揃える） ●テレワーク可能なモバイル型PC ●チャットツール ●Web会議ツール ●遠隔監視ツール ●ウイルス検知ソフト ●クラウドストレージ ●他オンラインツール
スムーズなコミュニケーション	・原則、対面会議が基本 ・連絡は電話、内線が中心 ・内線電話数にも制限がある	・チャットで迅速に情報伝達 ・離れていても職員の状態(在席、会議中、休暇など)がわかる	
安全で快適なネットワーク	・120システムがLGWAN系に所属 ・外部から接続できる仕組み構築には労力がかかる	・LGWANに残るシステムでも外部から安全に接続できる ・庁内/庁外問わず、端末1台で業務が行える	
クラウドの活用	・庁内にサーバーを置く前提であり災害リスクがある ・システム構築を検討できる職員が少ない	・クラウドを活用し、庁内にサーバーを置かない ・システム導入プロセスを標準化する	職員の意識変革 （職員の意識を変える）

（参考）新しい働き方のイメージ①



（参考）新しい働き方のイメージ②

「どこにいてもつながる・働ける」環境を整備（イメージ図）

実現に必要な情報インフラ

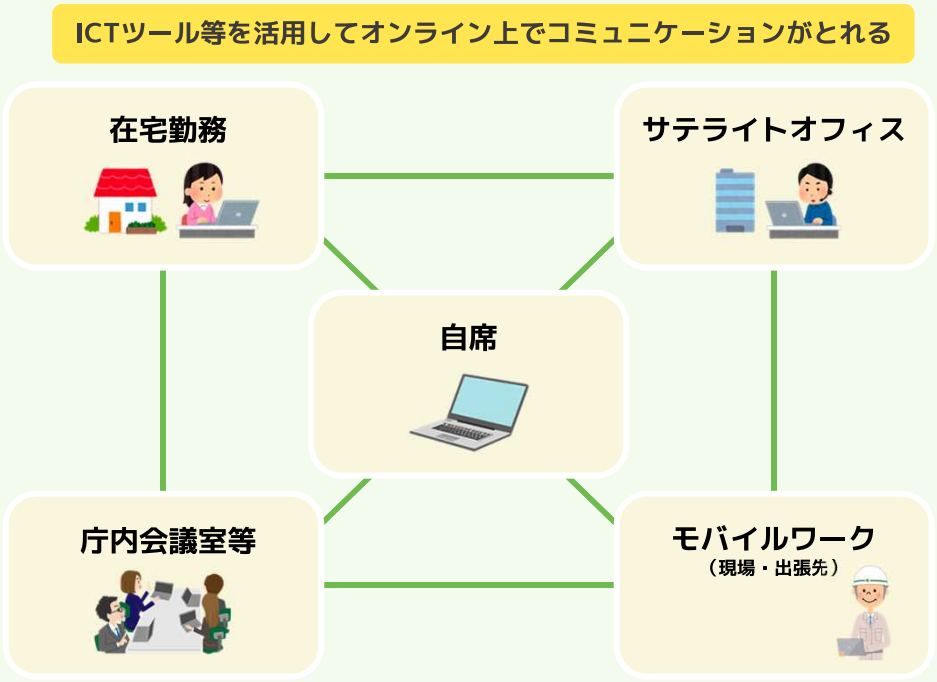
1.モバイル型PC
小型軽量で持ち運びやすい。無線で通信可能

2.Web会議ツール
どこでもレク、会議、打ち合わせ等ができる

3.チャットツール
どこでも会話形式でのメッセージのやり取りができる

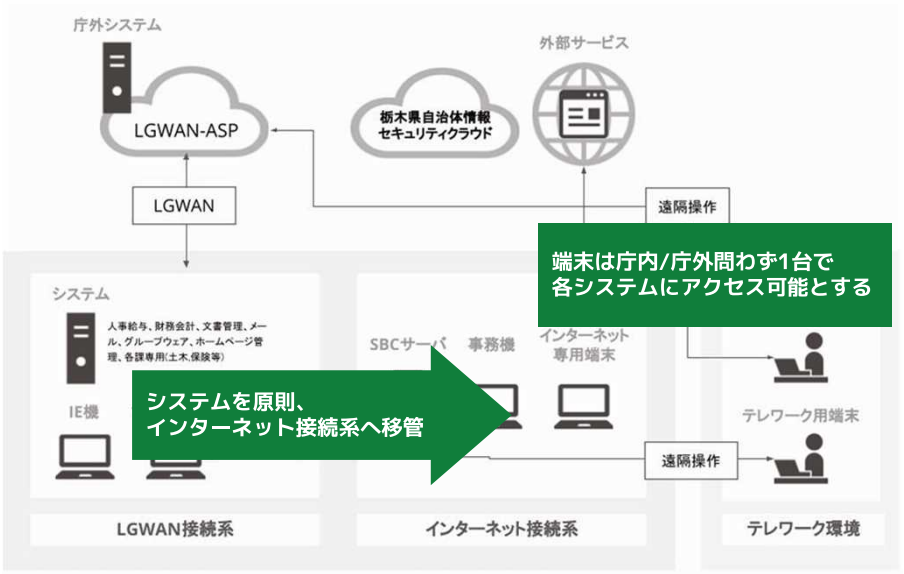
4.クラウドストレージ
クラウド上でデータの共有ができる

5.遠隔監視ツールやウイルス検知ソフト
リモートでパソコンの制御等が可能

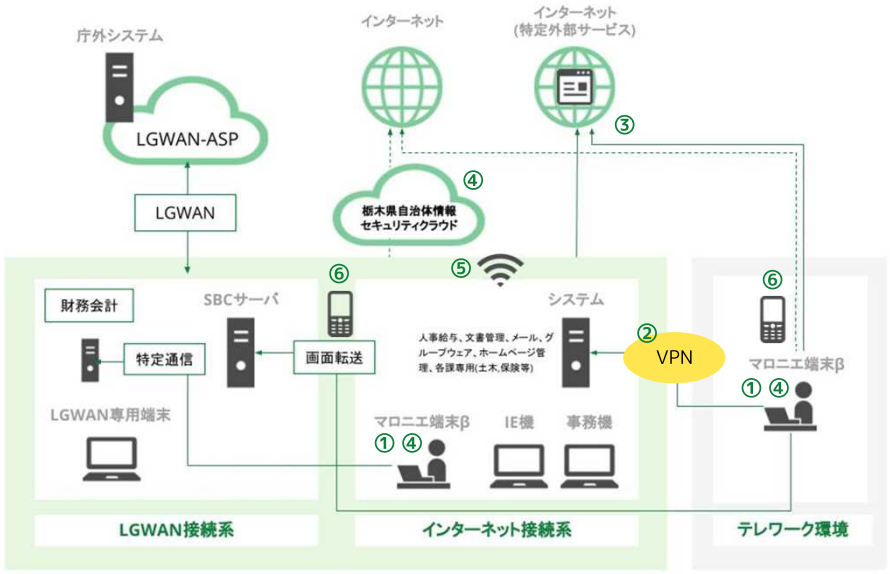


4. 次期情報インフラへの変更ポイント

Before



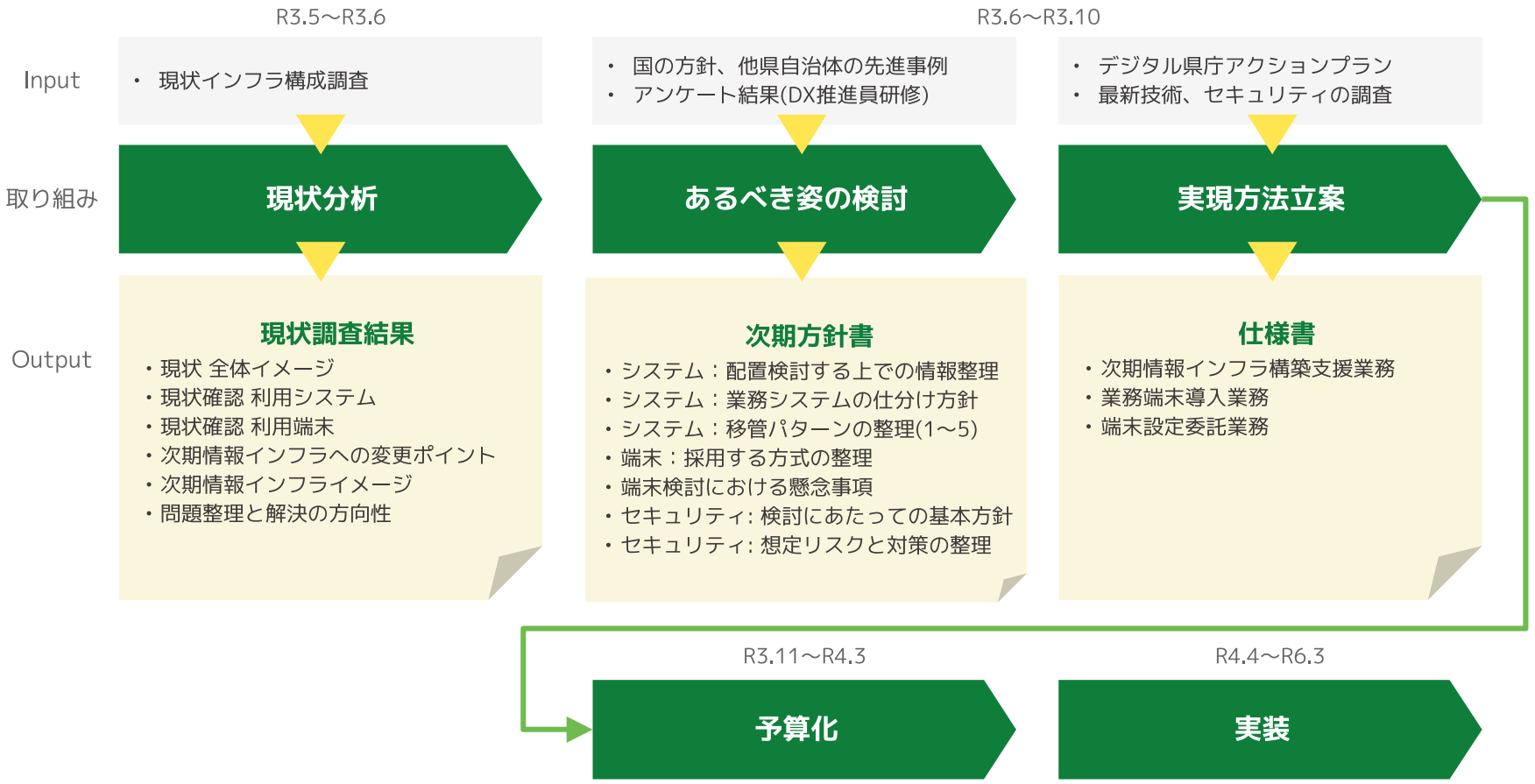
After



情報インフラ整備に必要な機器設備

①テレワーク可能なモバイルPC 6200台（予備機含む）、SIM6000台
②VPN敷設
③チャットツール、Web会議ツール
④セキュリティ対策ソフトウェア
⑤庁内無線LAN環境
⑥電話/内線

5. 次期情報インフラ更新方針作成の経過



6. スケジュール


タスク
R3年度
R4年度
R5年度
R6年度
業者選定
R4.2 公示
R4.3 入札
②
次期情報インフラ整備
(β'モデル移行)
R4.4-8 移行
R4.9 完了
新環境運用開始
①
③
④
端末導入
6,200台
出先
3,600台
現行端末
R4.12 リース満了
R4.4- 調達・キッティング
R4.9-12 導入
利用開始
本庁
2,600台
現行端末
R6.12 リース満了
R4.4- 調達・キッティング
R5.1-3 導入
利用開始
①
SIM導入
6,000回線
出先・本庁
6,000回線
R4.4- 電波対策工事
R4.9 導入
テレワークのみ利用開始
検証期間を設けて庁内でも利用
⑤
無線LAN
導入
本庁一部
導入
R3年度中利用開始
本庁全体
導入
R4年度中利用開始
那須(新庁舎)
導入
R4年度中利用開始
出先機関
導入
R5年度以降順次利用開始
⑥
電話/内線
全職員
最適なあり方の検討

7. 無線LANとSIM併用の必要性

通信手段	特徴	問題点
無線LAN 	・安定した通信速度を得られる ・コストを一定に抑えられる	・働く場所が限られる (庁内の無線LANが届く場所のみに限定) ・利用箇所数の増減時に大規模な工事が必要
SIM 	・場所を問わず利用できる ・工事不要で利用数の増減ができる	・通信障害時(災害時等)に業務ができないリスクがある ・多くの職員が利用過多となれば通信コストが増加する

無線ＬＡＮの問題点は**ＳＩＭ利用で解消**できる

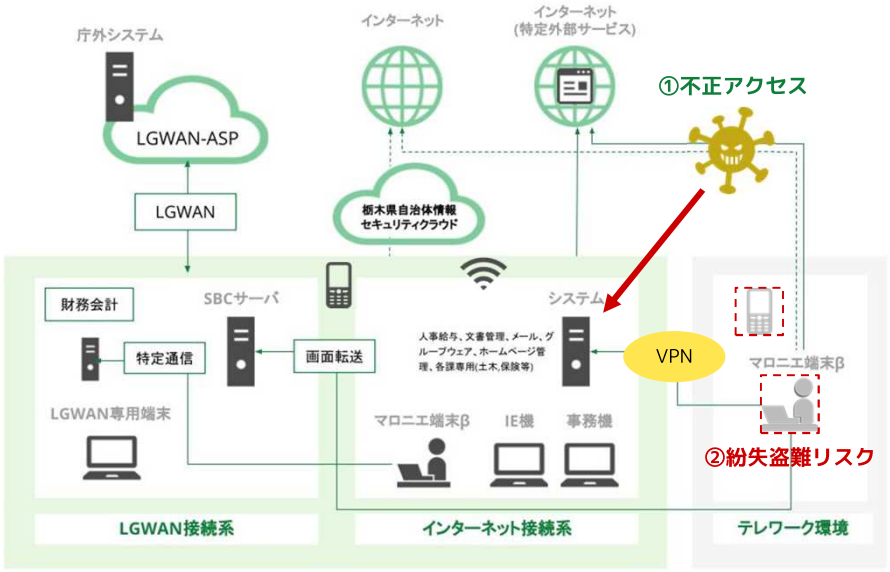
SIMの問題点は**無線LAN利用で解消**できる

- 無線LANとSIMを併用することにより、それぞれが持つ問題点をカバーできる
- コストを抑えながらどこからでもアクセスできる柔軟な環境が構築できる
  （庁内に居る時は無線LANを利用し、庁外はSIMを利用する旨を記載したガイドラインの制定は必要）

8. セキュリティ対策

次期情報インフラ構築に伴い、高まるリスクは以下のとおり。

1. 業務環境をインターネット接続系に移管することによる
   外部からの不正アクセス脅威
2. 端末を持ち出す機会増加による、紛失・盗難リスク



次期情報インフラ環境は、「セキュリティ製品」と「職員への啓蒙(情報セキュリティ教育)」の2軸で安全性を確保する。

想定リスク	原因	防止策（させない）	発生後の対策（広げない）
端末の盗難・紛失	不注意 (置き忘れ)	外出時は常時携帯	リモートワイプ (遠隔消去)
不正アクセス	端末の脆弱性	修正プログラム 適用	端末監視
	システムの脆弱性	調査・改修	アクセスログ 採取
	不注意 (ﾌﾘｰｱｸｾｽﾎﾟｲﾝﾄへの接続)	許可ﾈｯﾄﾜｰｸ制限	端末監視
	リスト攻撃	多要素認証(ｽﾏｰﾄﾌｫﾝへのﾜﾝﾀｲﾑﾊﾟｽｺｰﾄﾞ、生体情報) GPSで場所特定	端末監視
IDパスワード流出	不注意 (付箋、他職員とID共有等)	紙媒体で保存しない パスワードの複雑化	ID変更、停止
	フィッシング詐欺	URLフィルタリング	端末監視
データ流出	メール誤送信	オンラインストレージ利用	ファイル削除
マルウェア 感染	不注意 (怪しい添付メール)	送信者・タイトルの確認	アクセスログ採取

*上記防止策は対策の一例である点に留意
*次期インフラ環境の整備時には改めてセキュリティポリシーなどを作成予定

（参考）セキュリティ10大脅威

■「情報セキュリティ10大脅威 2021」　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位

3位　テレワーク等のニューノーマルな働き方を狙った攻撃

攻撃手口/発生要因

テレワーク環境や管理体制の不備

- テレワーク用ソフトの脆弱性を悪用した不正アクセス
- 急なテレワーク移行による管理体制の不備
- 私物PCや自宅ネットワークの利用 ※私物PCからの情報漏えいのおそれ

2020年の事例/傾向1

脆弱性の悪用によりVPNのパスワード流出

- 2020年8月、VPN製品の脆弱性が悪用されて窃取された
- 認証情報、約900件がインターネット上で公開されていた
- 悪用された脆弱性やその対策に関する情報は2019年4月に公開済みだった
- 更新プログラムを適用していないVPN製品が狙われた

2020年の事例/傾向2

テレワーク中にウイルス感染、社内に拡大 (※1)

- 社有PCにて在宅勤務
- 社内ネットワークを経由せずに外部ネットワークに接続
- SNSを利用した際にウイルスに感染
- 当該従業員が出社した際に当該PCを社内ネットワークに接続
- 社内ネットワークにウイルス感染が拡大

組織(セキュリティ担当者、システム担当者)の対策

被害の予防(被害に備えた対策含む)

- セキュリティに強いテレワーク環境の採用(シンクライアント、VPN、ZTNA等)
- テレワークの規程や運用ルールの整備　組織支給PCと私物PCの違いも考慮
- セキュリティ教育の実施
- テレワークで利用するソフトウェアの脆弱性情報収集と周知、対策状況の管理
- セキュリティパッチの適用(VPN装置、ネットワーク機器、PC)

出典（IPA（独立行政法人情報処理推進機構）、情報セキュリティ10大脅威 2021［組織編］、https://www.ipa.go.jp/files/000089239.pdf）