

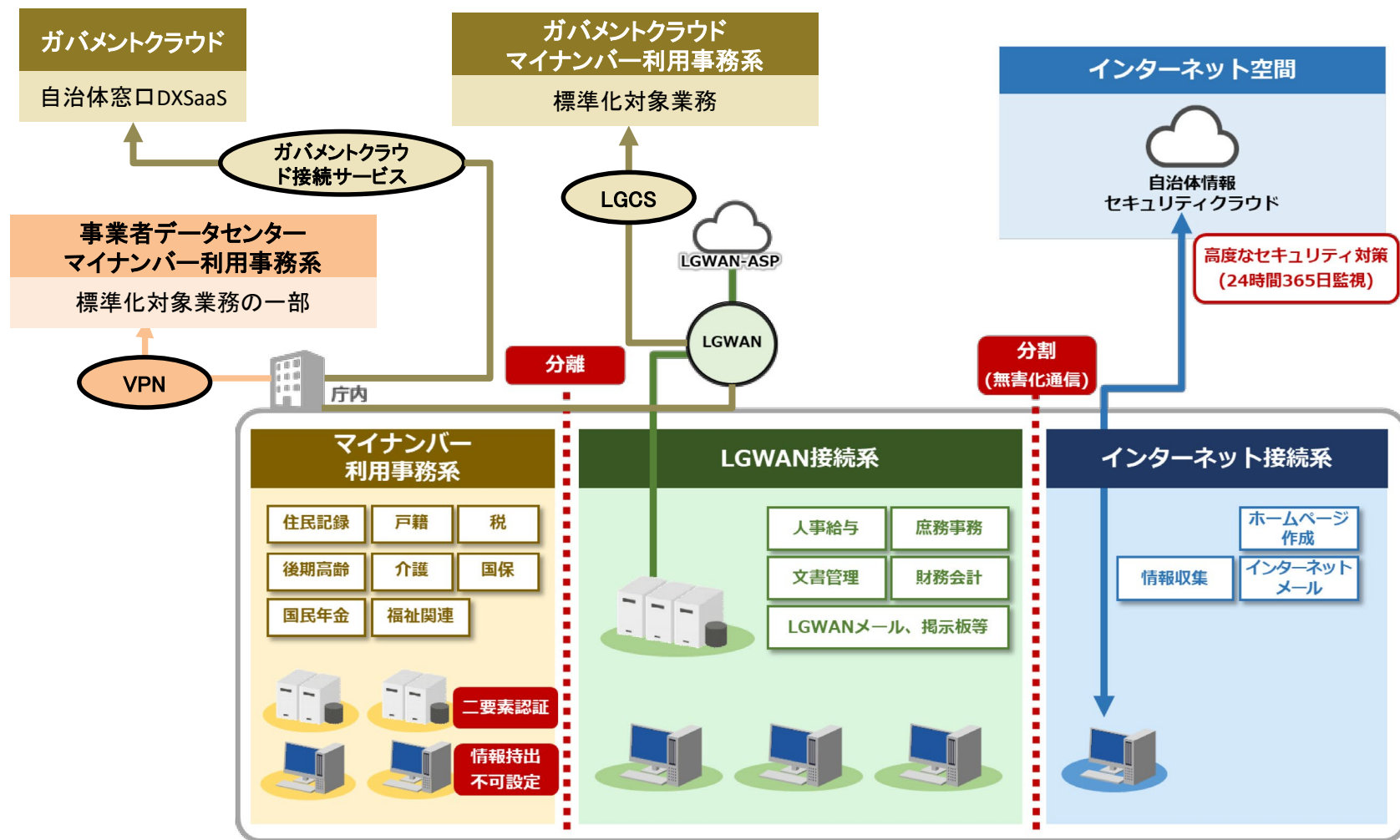
都城市におけるサイバーセキュリティ の現状と課題について

【説明事項】

- 1 情報システム構成
- 2 クラウド利用状況
- 3 ネットワーク規模
- 4 課内体制
- 5 研修・訓練
- 6 直面する課題
- 7 協議会への期待

【説明事項】

1 情報システム構成



【説明事項】

2 クラウド利用状況

区分	現状	今後の計画
基幹業務システム	<ul style="list-style-type: none"> ➤ 一部を事業者DCで運用(閉域網接続) ➤ アクセス制御・暗号化・監査ログを実施 ➤ 遠隔バックアップ・冗長構成で災害対策 	R7年度より順次ガバメントクラウドへ移行
窓口DXSaaS	<ul style="list-style-type: none"> ➤ R5年度よりガバメントクラウド上で利用開始 	接続方式を「ガバメントクラウド接続サービス」から「LGCS」へ移行予定

【説明事項】

3 ネットワーク規模

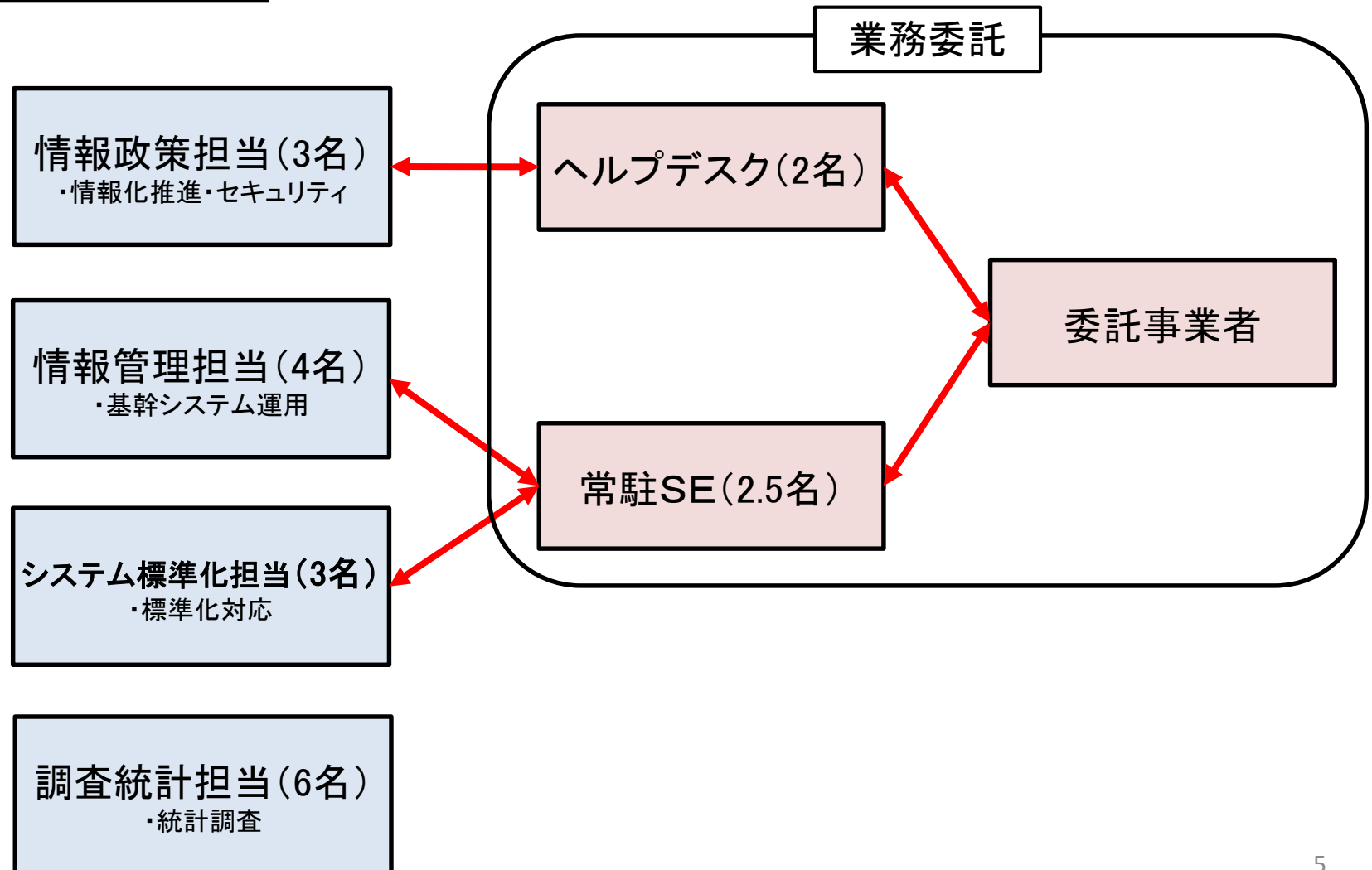
- サーバー及びシステム
 - ・サーバー：約70台
 - ・システム：約230

- 職員用PC台数
 - ・マイナンバー利用事務系：約500台
 - ・LGWAN接続系：約2,000台
 - ・インターネット接続系：約300台

- 接続拠点数
 - ・ネットワーク本庁以外の拠点数
38箇所＋学校54校＋保育所6箇所

【説明事項】

4 課内体制



【説明事項】

5 研修・訓練

対象者	研修内容
一般職員	<ul style="list-style-type: none">➤ 情報セキュリティポリシー➤ セキュリティ及びネットワーク
管理職	<ul style="list-style-type: none">➤ サイバーセキュリティ(県警)
情報政策課	<ul style="list-style-type: none">➤ 実践的サイバー防御演習「CYDER(サイダー)」➤ リモートラーニング研修(J-LIS)
職員+事業者	<ul style="list-style-type: none">➤ 基幹系情報システム障害対応訓練

【説明事項】

6 直面する課題

- 業者依存による知識の空洞化
 - ・ セキュリティ対策の多くを外部業者に委託
 - ・ 職員は「理解はできるが設定はしない」立場に留まる
 - ・ 技術的判断力・初動対応力が育たず、インシデント時に支障
- ネットワークの複雑化と職員スキルの乖離
 - ・ ネットワークやシステム環境が高度化し、次々と新技術が登場
 - ・ 異動で配属された職員にとって敷居が高い
 - ・ 実務経験不足で構成理解が困難
- 影響
 - ・ インシデント初動対応の遅れ
 - ・ 人材不足の深刻化
 - ・ 運用は安定しているが「属人化リスク」増大

【説明事項】

7 協議会への期待

期待事項	期待する効果
迅速で安全な情報共有	➤ 国や他自治体からの脅威情報をリアルタイムで受け取り、初動対応を迅速化
情報の信頼性と分析支援	➤ 協議会で整理・分析された情報を活用し、判断の精度を向上

協議会には、情報共有と連携を通じて、自治体が初動対応に必要な知見を得られる場となることを期待します。