資料4－1

地域における
セキュリティ・プライバシー人材

立命館大学情報理工学部
上原哲太郎
（芦屋市CIO補佐官）

RITSUMEIKAN

地域におけるICT人材不足

民間企業において…

- ICTサービスの
  クラウド移行が進むにつれ
  地域ICT企業における
  パッケージ中心のSI業は
  今後需要が縮む
- 新サービス創出にも結局は
  「若い」技術者が必要
  - 事業創出は地方でも可能
    だが事業の継続には
    地元に人材が必要
  - 地方で急速に進行する高齢化

地方公共団体において…

- 情報担当部署に
  人が足りない
  専門性が足りない
- この状況で
  地域情報化の施策を
  主体的に担当できる
  職員は希有

ICT利活用が不十分な中
セキュリティまで
目が届かない現状

地方自治体がリードする(べき)
地域の情報セキュリティ

警察

サイバー犯罪や
サイバーテロは
地域を選ばぬ脅威
官民とも対応力向上を
主体となって支援

自治体

住民情報の保護を軸に
情報セキュリティ向上を
企業にも対応を促し
産業振興も狙う

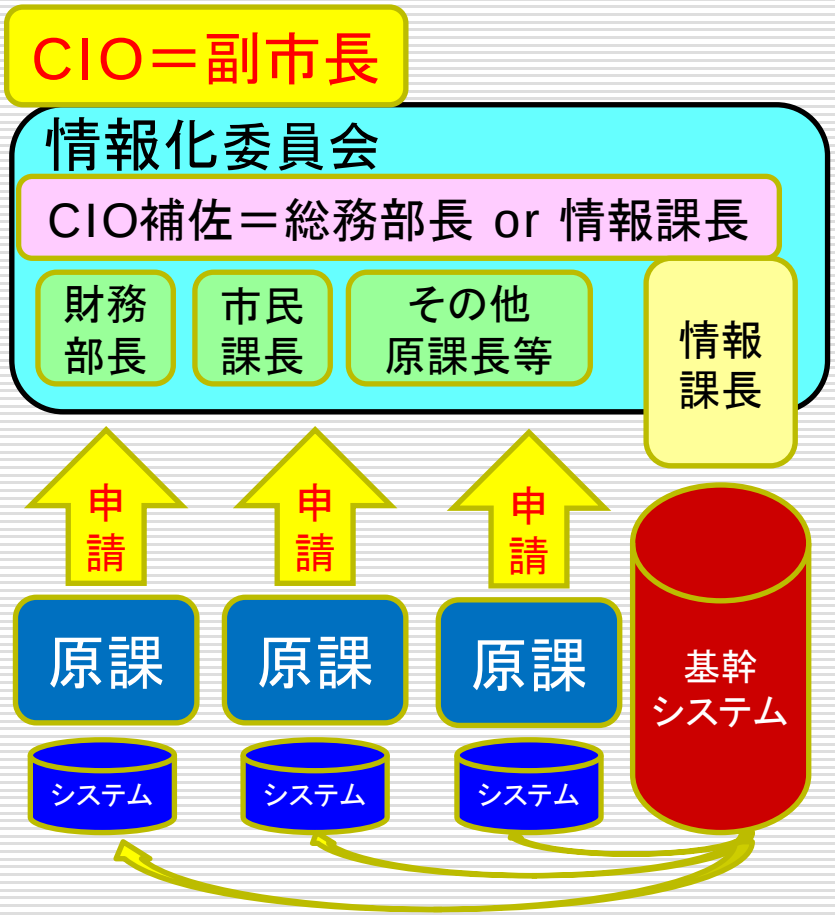
学校

情報モラル教育を軸に
生徒の意識向上を
間接的に保護者と
地域への教育啓蒙を

地域企業

ISMSやPマークは
公共からの要請
マイナンバー対応
セキュリティも
徐々に経営課題に

自治体職員のICT専門性向上を阻む「原課調達主義」



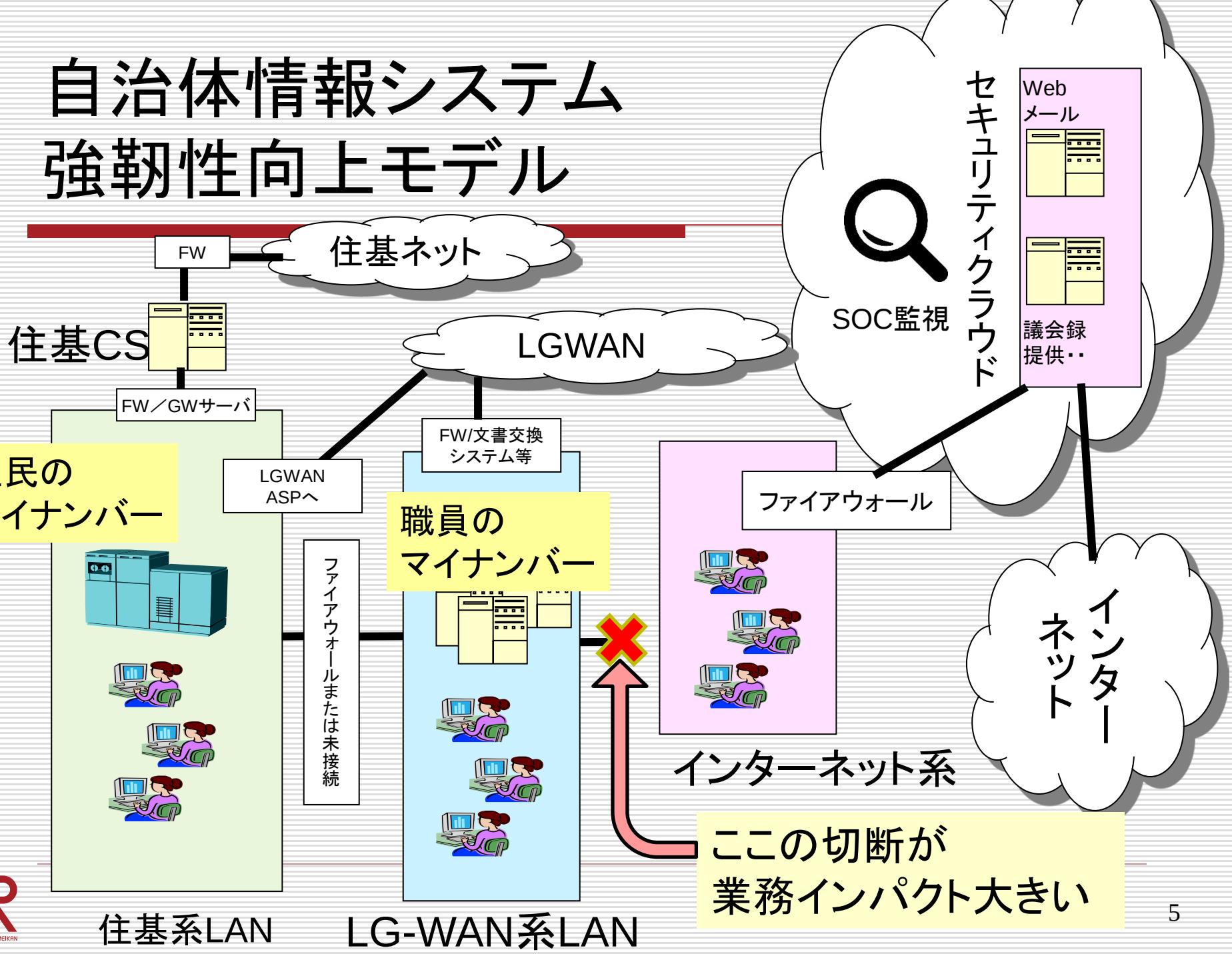
- 情報化委員会等に各原課がシステムを導入申請（予算も）
- 情報課はシステムを繋ぎ合わせるので精一杯
- 全体整合・最適化が進まない
  - 本来CIOの仕事だがCIOは充て職が多いCIO補佐の専門性も不十分
  - 全体を俯瞰できないとセキュリティ確保も困難
- 各原課がシステム導入業者に運用も「丸投げ」し依存する
  - 調達の適正性の判断力が低下
  - 調達後改修や追加調達の増加
  - 果ては業務そのものの専門性が失われる例も
    - システム業者のヘルプデスクに業務そのものの問い合わせが…

結果的に管理することに…

地方自治体におけるセキュリティ

- 基本的に情報は公開するべき
  厳重な管理が求められるのは住民の情報
- よってセキュリティは「個人情報保護」を軸に進む
  - 住基ネットとマイナンバーを中心に
- 手段は揃っているが実効しているか？
  - 「個人情報条例」都道府県市町村は100％制定だが…
    - 特別地方公共団体（広域連合・一部事務組合）に制定漏れ
    - 改正個人情報保護法対応への遅れ
      （特に「匿名加工」問題：自治体IoTからの情報利活用の障害？）
    - 個人情報保護審議会等の有無や運営の温度差
  - セキュリティポリシー制定も100％だが…
    - 基本方針と対策基準はあるが実施手順が不十分な例多し
  - セキュリティ監査もガイドラインがあるが…
    - 基礎自治体では内部監査実施が25％程度　外部監査5％程度

自治体情報システム
強靭性向上モデル



地方自治体におけるICT利活用を本質的に進めるために

- 情報システムの運用管理を自治体における「基幹業務」と捉え直すべき
  - 情報システムの設計から調達運用までを自治体側で主体的に行える体制にならないと…
  - そのためにキャリアモデルから考え直すべき
    - 自治体に専門職がないわけではない
    - そもそも情報職は本当に「専門職」か？
- 「強靭化」は業務フロー見直しのよい機会
  - フロー整理と適切なシステム化でセキュリティと業務効率の両立を目指す
  - うまく業務を実装できれば民間企業への範にもなるはず
- 全体を俯瞰した上で戦略的に情報セキュリティ対策を実施できる人材が必要
- その専門性は地域情報化施策やセキュリティ施策にも生かせるはず

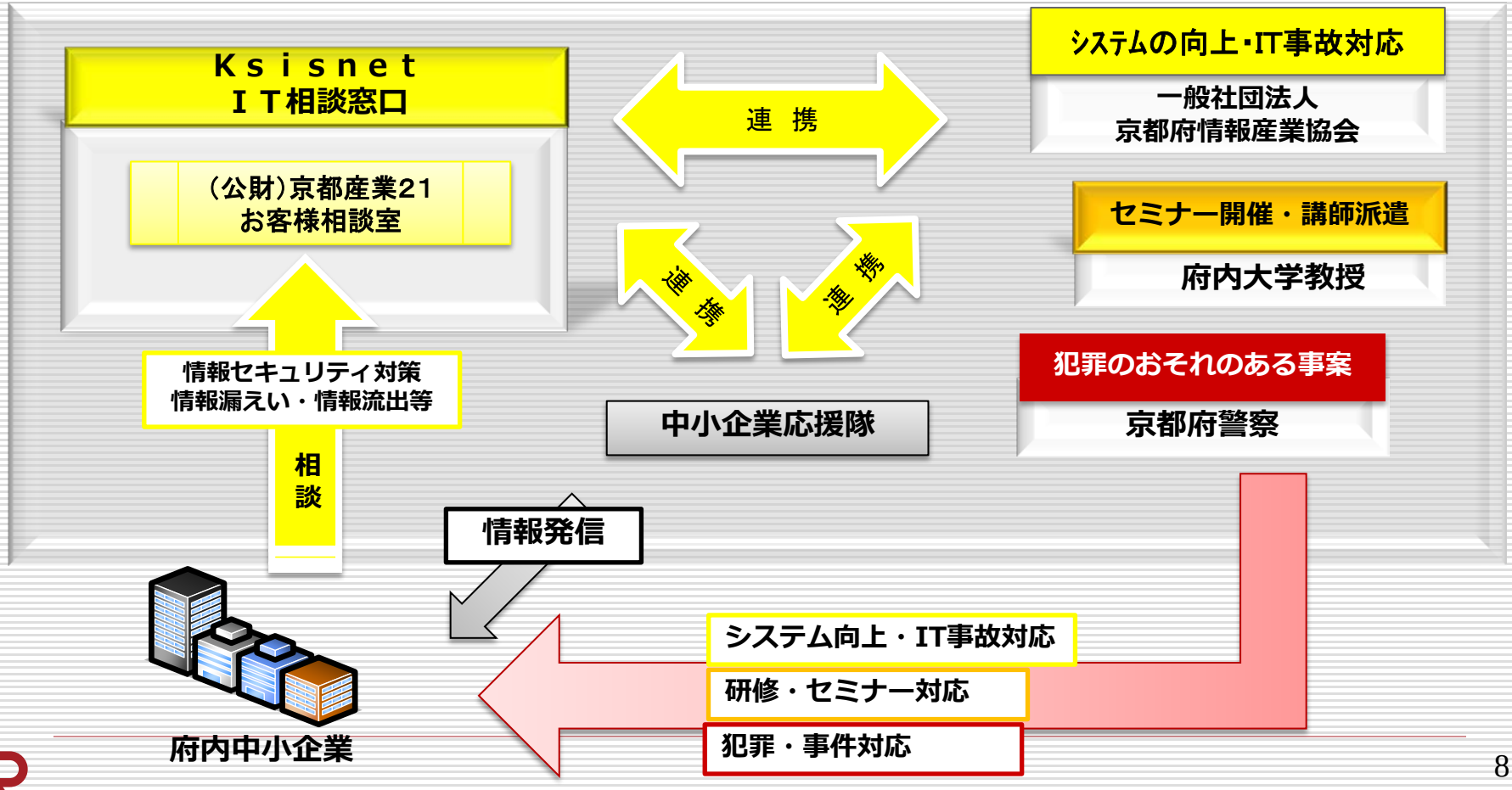
RITSUMEIKAN

地方におけるセキュリティ産業振興と人材育成

- セキュリティこそ地域に根ざした産業にできる
  - セキュリティ監視業と障害・事故対応（インシデントレスポンス＝IR）は「現場作業」を伴う
  - サイバー犯罪や事故が地方企業で発生した場合対応できる人材や組織は地方にこそ必要
- 地方でも持続するICTビジネスモデルを
  - 平時は地域産業のICT利活用支援とセキュリティ監視（ミニSOC業務）
  - 事故が発生した場合はIR支援
    - 高い専門性が必要な分野
    - ただし、かかる費用をどうするかが課題

「地場を地場で守る」産学公連携組織の例

Ksisnet
Kyoto Small and Medium Enterprises Information Security Support Network
京都中小企業情報セキュリティ支援ネットワーク



http://ksisnet.kyoto

IoT時代はプライバシー≧セキュリティ

- セキュリティは本来は「情報資産の保護」だがIoTでは…
  - 個々の「モノ」の情報資産の価値は疑問
    - センサネットワークのような大規模情報収集系では
      システムの乗っ取りと悪用（DoS等）対策が課題
    - プラントや自動車等の制御を伴うシステムになると
      乗っ取り悪用が物的人的被害をもたらす
- IoTを通じた情報収集時と活用時に
  プライバシーにかかる情報を適切に扱えるかが課題
  - 単なる漏洩はセキュリティの知識で対応可能
  - プライバシー論に関する知識を有する人材や
    匿名加工（非識別加工）等の技術的理解ができる人材が
    今後求められてくる
  - 地方自治体にプライバシー人材を十分配置できないと
    自治体発のオープンデータの利活用の障害に
    - 「適切な（自治体版）非識別加工」の判断の問題
      基準が自治体によって異なりうるので混乱の元に