情報通信技術面における留意点

～テレワーク導入時のセキュリティ・マネジメントのポイント～

Flexible Work,
Flexible Business,
Flexible Life.

株式会社 テレワークマネジメント
鵜澤　純子

CONTENTS

1. テレワーク導入における課題

2.総務省　テレワークセキュリティガイドラインについて

3.技術・制度・人に関する情報セキュリティ対策例

4.情報へのアクセス方法とその特徴

5.マネジメント（労務管理等）の対策

弊社のご紹介

株式会社 テレワークマネジメントのご紹介

普及啓発

- テレワークに関する講演・研修
- テレワークセミナー定期実施
- メールマガジン定期配信
- 自治体テレワーク普及・推進事業

導入支援

190社以上の実績

- テレワーク導入コンサルティング
  - テレワークに関する調査/分析
  - テレワークツールの開発/販売
  - テレワーク勤務規則/制度策定サポート
- テレワーク研修・講演

ビジネス提案

- テレワークを活用した新しいビジネスの提案

政策提言

- 国の政策提言
- 自治体の施策提言

イクボスアワード2014 MEN

DIVERSITY 100 2014

IT経営実践認定企業

System, Hokkaido Family Education Support Companies

TWOO Telework Pioneer

ホワイト企業認定

総務省
地域情報化アドバイザー認定団体

1.テレワーク導入における課題

1.1.テレワーク導入における課題

平成29年版 情報通信白書より

2.総務省　テレワークセキュリティガイドラインについて

2.1.テレワークセキュリティガイドライン第4版について

- **総務省は「テレワークセキュリティガイドライン第4版」を平成30年4月13日に公表**（前回改定は平成25年3月29日）

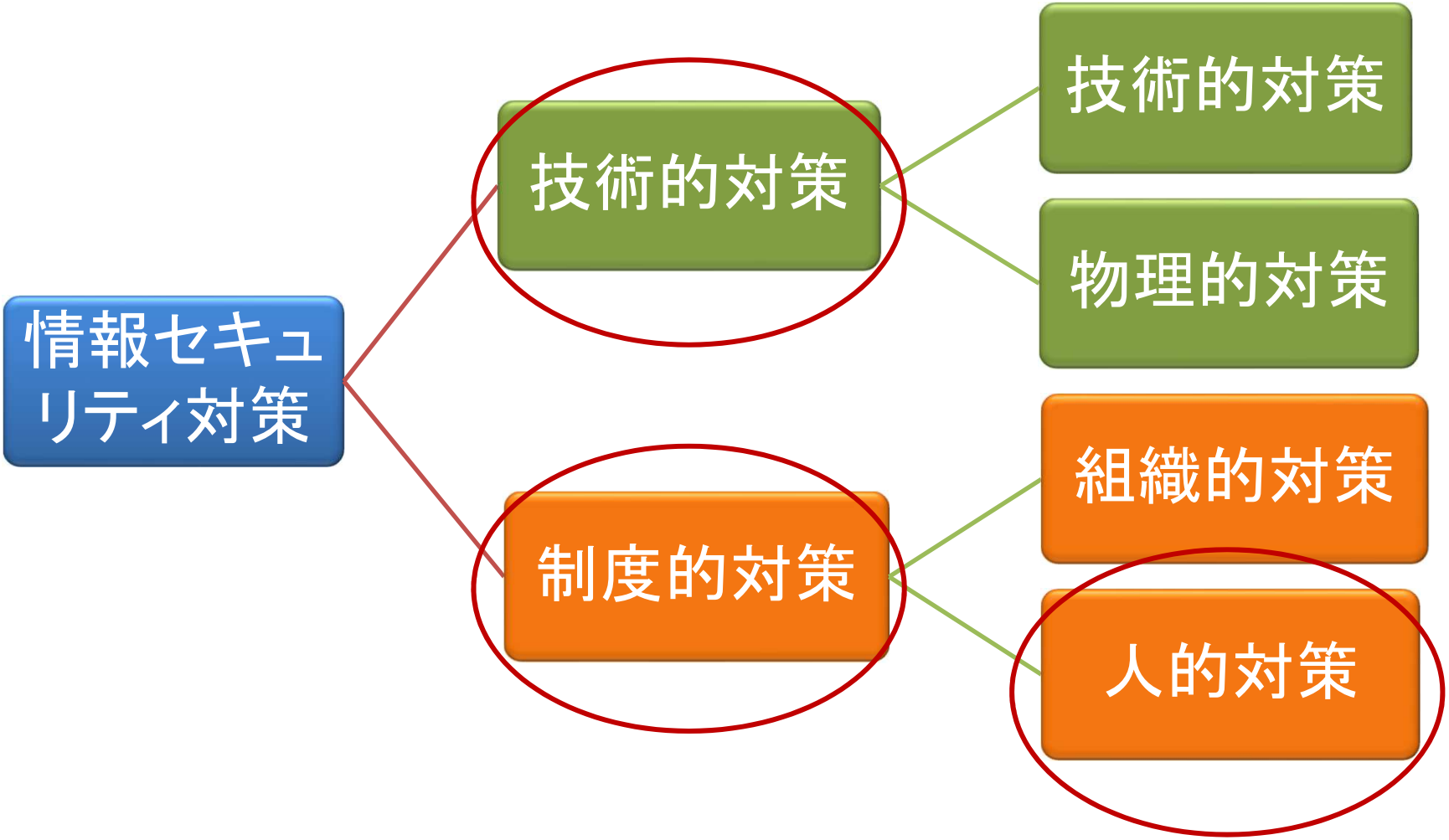
社会やサービスの変化に対応し、私用端末、SNSやクラウド、サテライトオフィス等を使う際の留意点を追加

技術の進歩や新たな脅威に対応し、無線LANの脆弱性や標的型攻撃への対策等を追加

「基本的対策事項」と、「推奨対策事項」に分けて解説

トラブル事例等の具体例の紹介

2.2.情報セキュリテイ対策の種類と手法



3.技術・制度・人に関する情報セキュリティ対策例

3.1.主な技術的対策のまとめ

利用端末の適切な管理（ウイルス対策・HDD暗号化・MDM等）

認証システムを強化（別の認証方式もプラス）

リモート化等によって利用端末に情報を保存しない

3.2.主な制度的・人的対策のまとめ

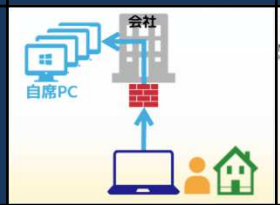
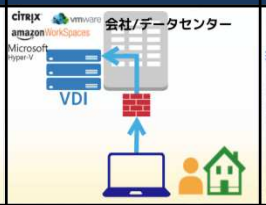
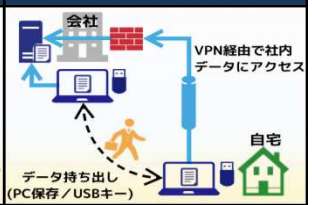
情報の機密度に応じた取扱い
（適切なアクセス権限の設定）

テレワーク用セキュリティガイドラインの作成

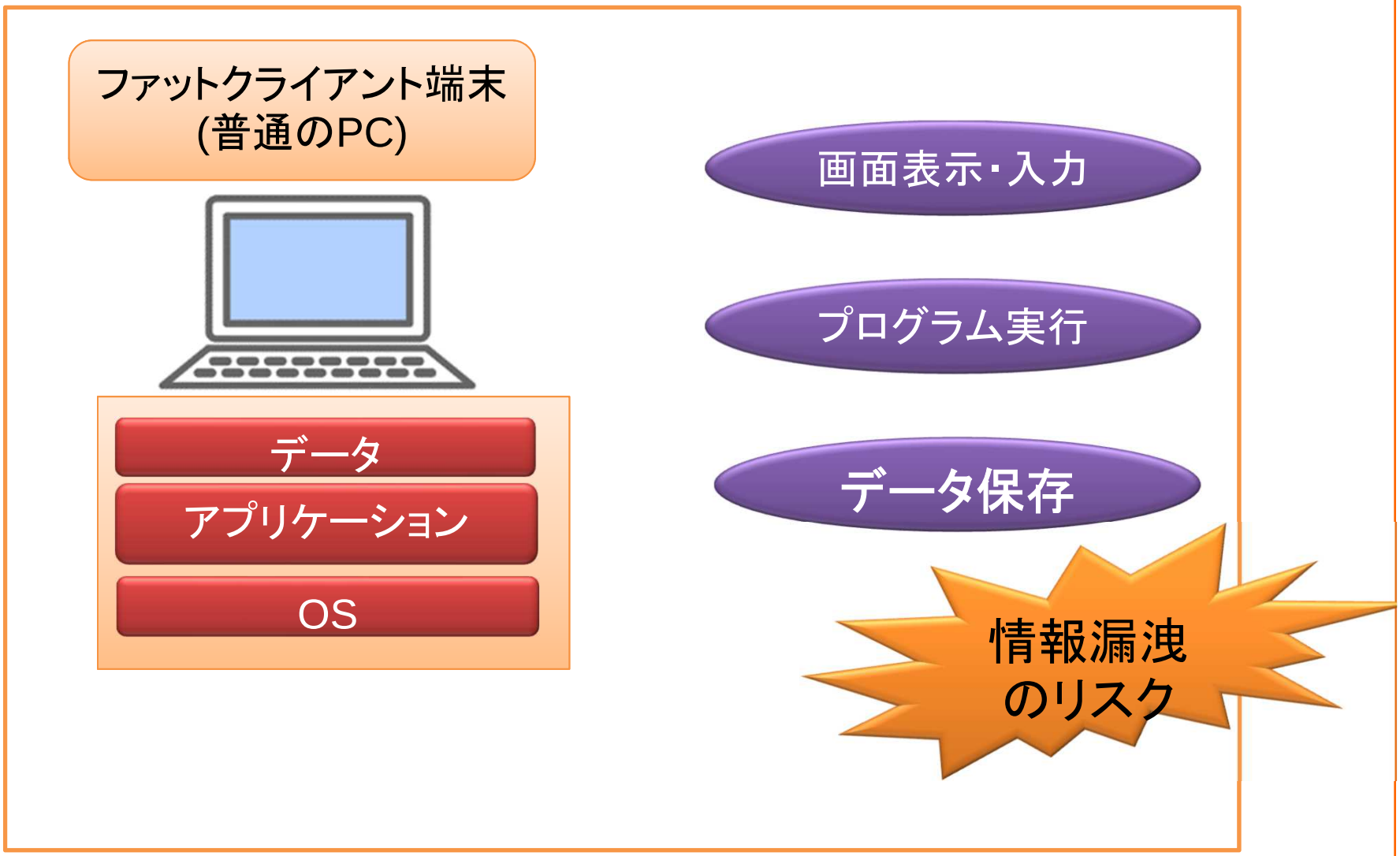
セキュリティ研修の継続的な実施

4.情報へのアクセス方法とその特徴

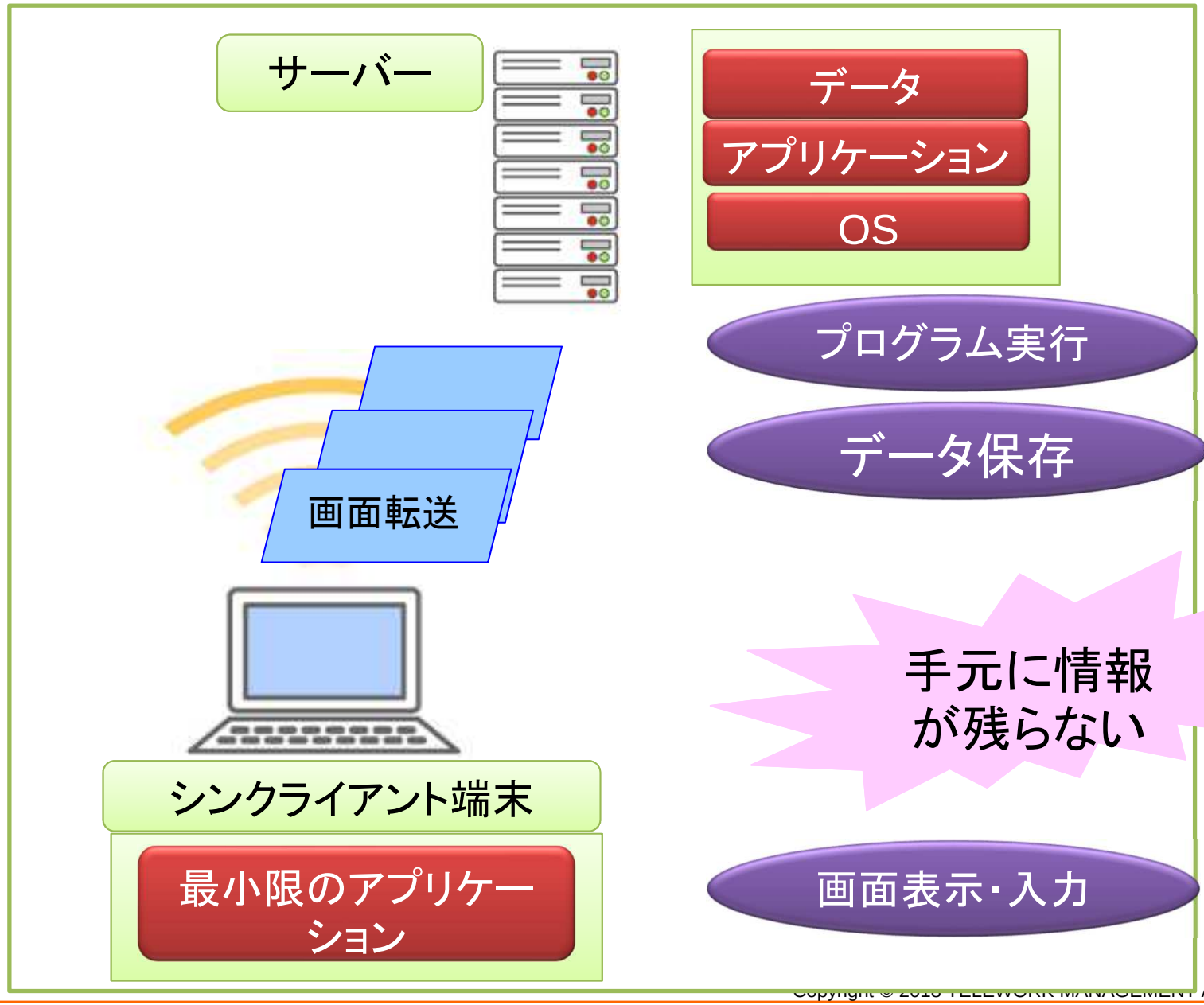
4.1.「情報を社外に持ち出し、保存するのかどうか」に注目

	リモートデスクトップ方式	仮想デスクトップ方式	クラウド型アプリ方式	セキュアブラウザ方式	アプリケーション分離方式	PC持ち帰り方式
						
概要	会社自席PCを遠隔操作	会社・データセンターのVDIを遠隔操作	クラウド型アプリを用いて業務	テレワーク端末にデータを残さないセキュアブラウザを使用	業務アプリとデータをコンテナ化して一般アプリと分離	会社とテレワークで同じ端末を使用
テレワーク端末への情報保存	保存しない	保存しない	どちらも可	保存しない	保存しない	保存する
データ漏洩等のリスク	危険性小さい	危険性小さい	危険性あり	危険性小さい	危険性小さい	危険性大きい
会社業務環境への脅威侵入	危険性小さい	危険性小さい	危険性あり	危険性小さい	危険性小さい	危険性大きい
会社と同じ業務環境	同じ	可能	可能	可能	可能	同じ
テレワーク端末の業務ソフト	リモートデスクトップツールのみ	仮想デスクトップツールのみ	必要	セキュアブラウザのみ	必要	ー
BYOD	可能	可能	危険性あり	可能	可能	危険性大きい
常時オンライン	必要	必要	一時的にオフラインでも可	一時的にオフラインでも可	一時的にオフラインでも可	不要

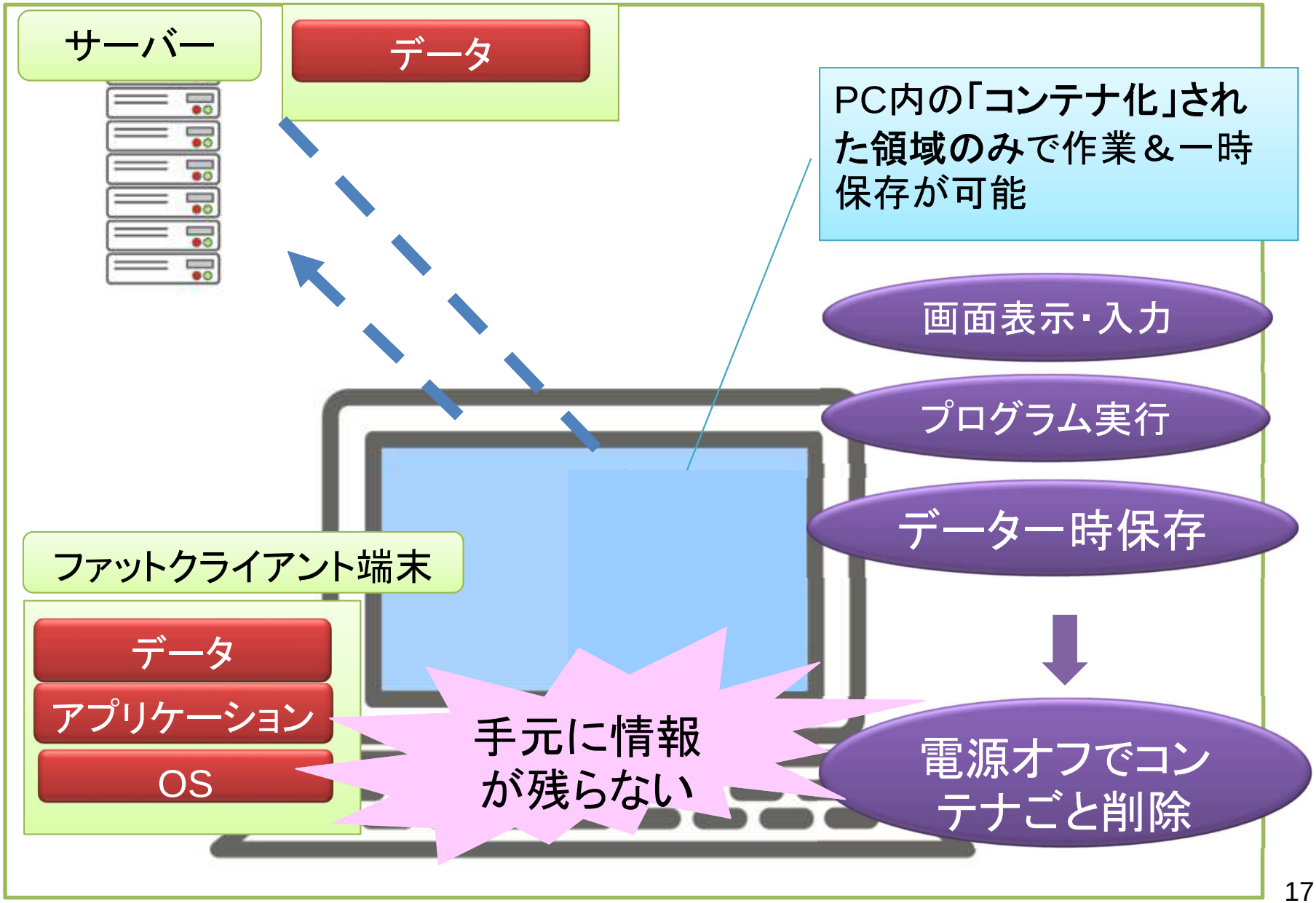
4.2.「情報を持ち出さない」技術：シンクライアント化とは？①



4.3.「情報を持ち出さない」技術：シンクライアント化とは？②

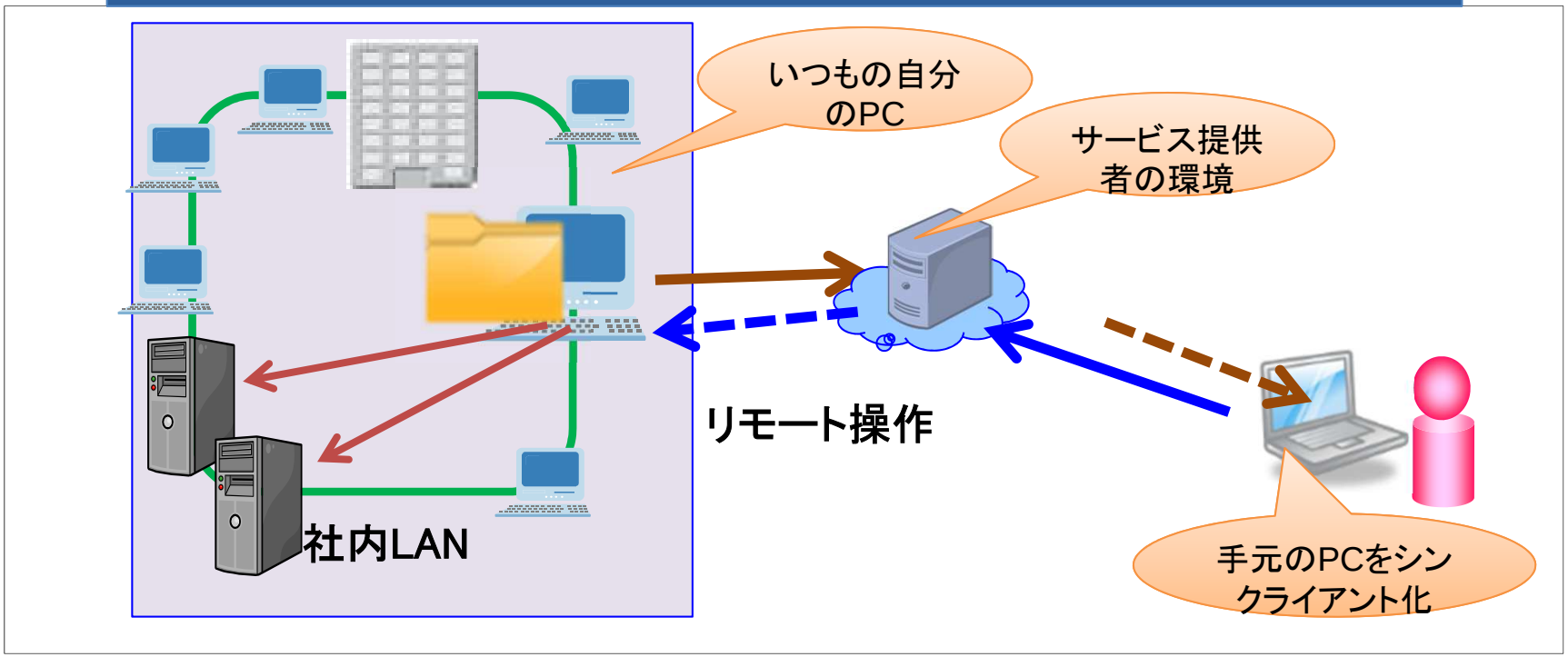


4.4.「情報を持ち出さない」技術：アプリケーション分離とは？



4.5.シンクライアントの活用例～リモートデスクトップ

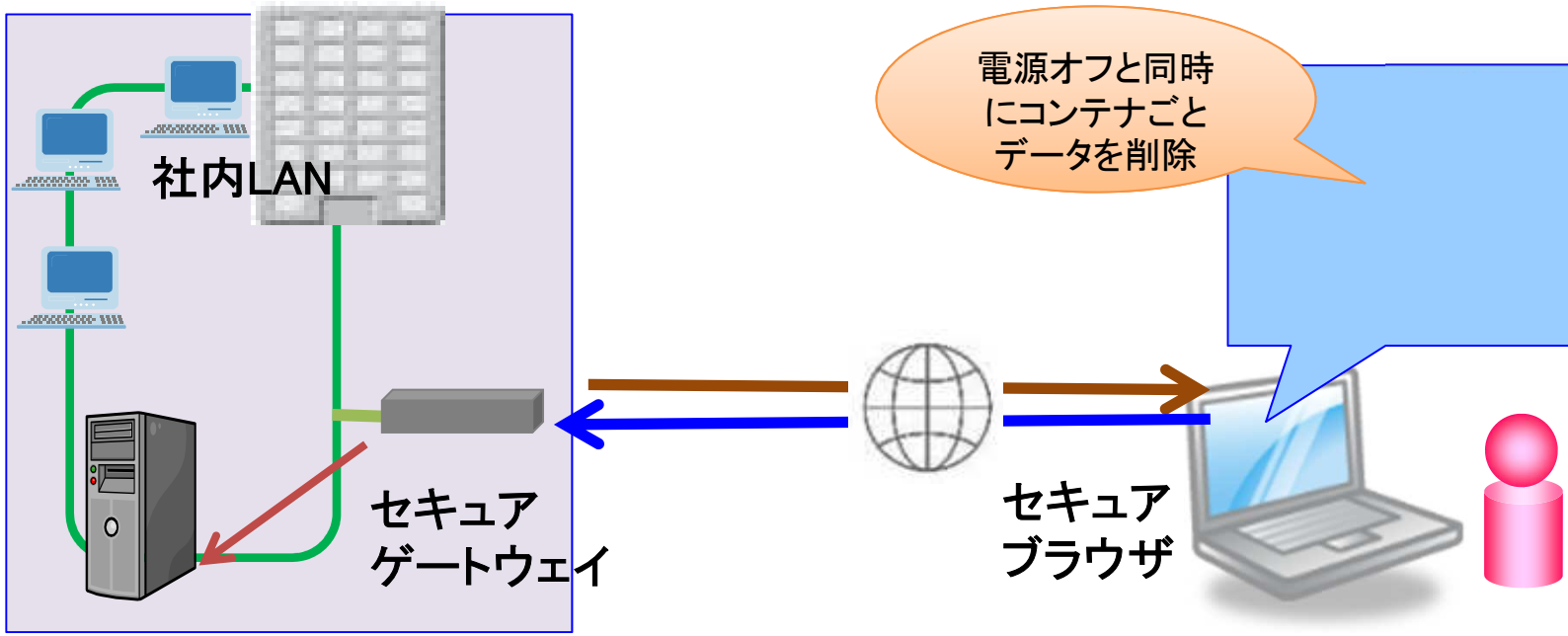
リモートデスクトップ方式



データを持ちださないので手元パソコンに業務データが残らない 【情報漏洩リスク最少】
手元パソコンが社内LANに直接接続しない 【手元パソコンから脅威が入り込まない】
会社での業務PC環境を手元で再現できる（印刷以外） 【すべての情報にアクセス可】

4.6.アプリケーション分離（ラッピング）方式

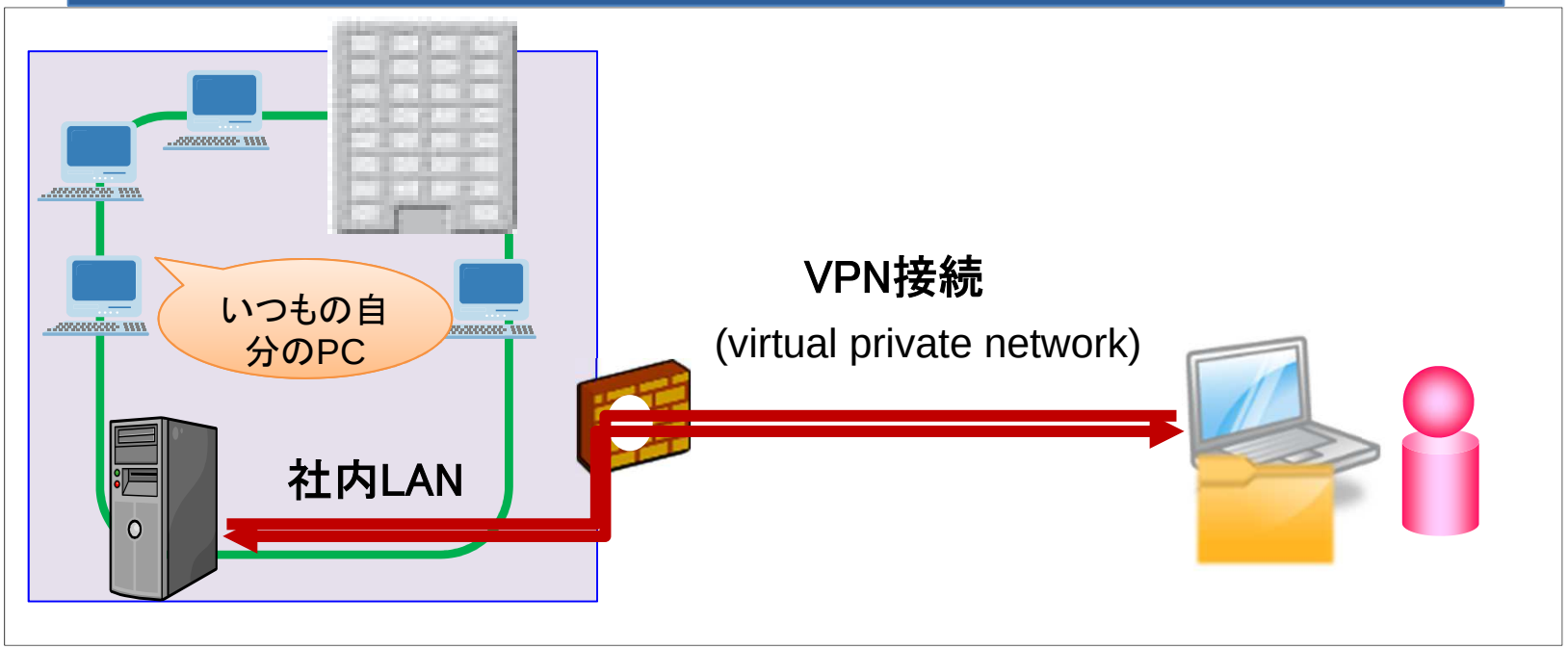
アプリケーション分離方式



データは仮想のコンテナ領域のみに保存。コンテナごと自動削除されるため、手元パソコン内に業務データが残らない。【情報漏洩リスク最少】
手元パソコンをセキュアブラウザ・セキュアゲートウェイ経由で接続 【手元パソコンから脅威が入り込まない】
コンテナ内で使えるアプリのみ使用可能 【限定的な情報を利用可】

4.7.その他のアクセス例～PC持ち帰り方式

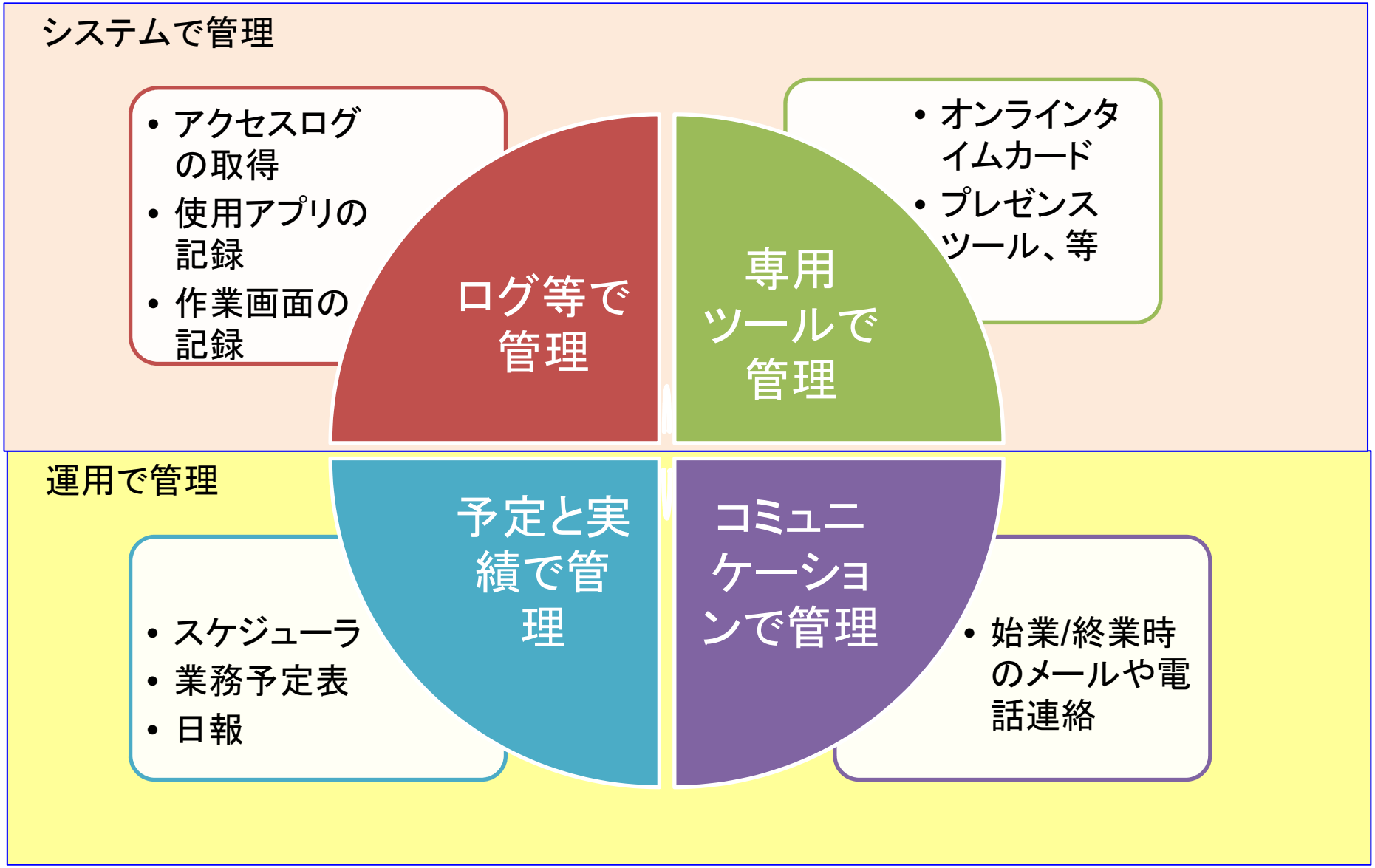
PC持ち帰り方式



データを持ちだせるため、手元パソコン内に業務データが残る 【パソコンの盗難・紛失時には情報漏洩のリスク】
手元パソコンを直接接続 【手元パソコンから脅威が入り込むリスク】
社内LANにつながるPCの環境を再現 【すべての情報にアクセス可】

5.マネジメント（労務管理等）の対策

5.1.システムと運用の両方で多角的に「見える化」



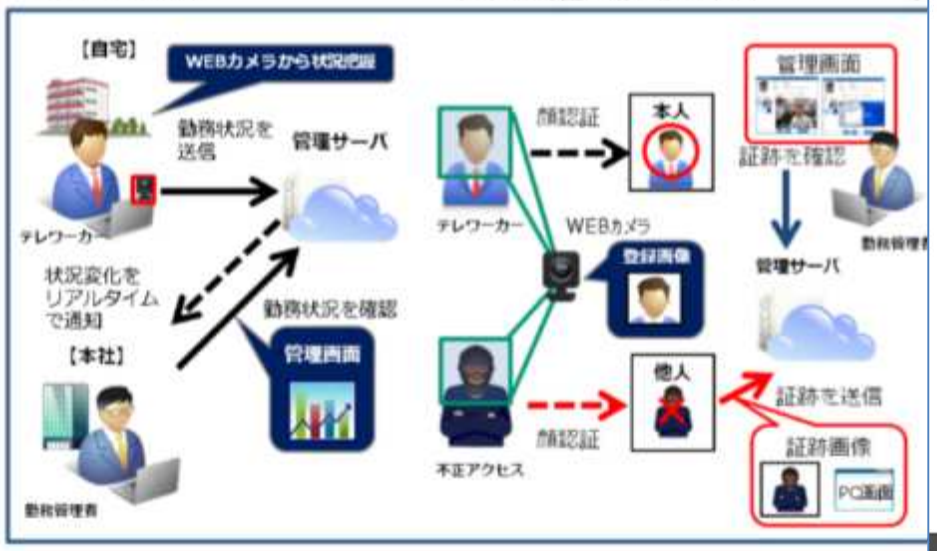
5.2.離れている社員をICTで「見える化」

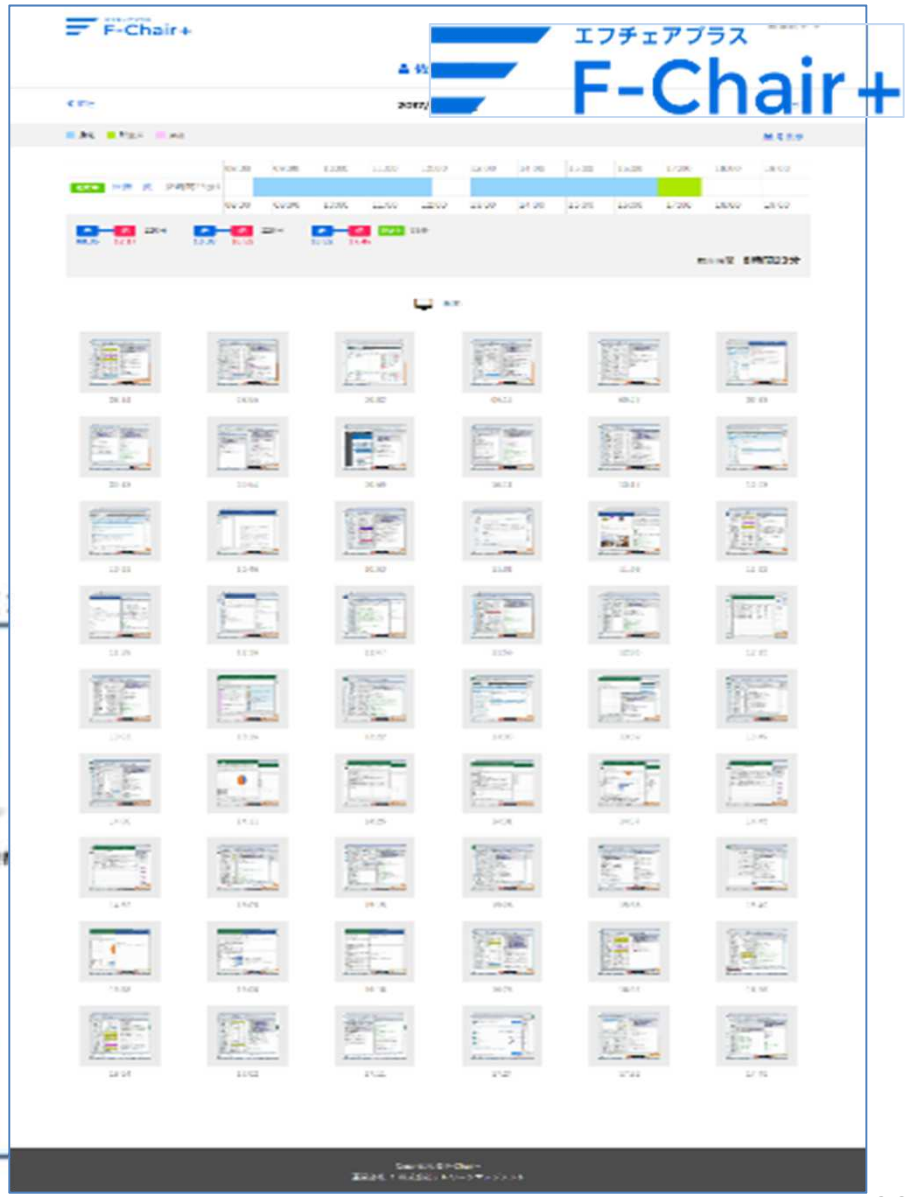
単なる時間管理・記録だけでなく作業画面の記録や顔認証による在席確認など多様な機能を持つ商品も

遠隔の社員の「見える化」

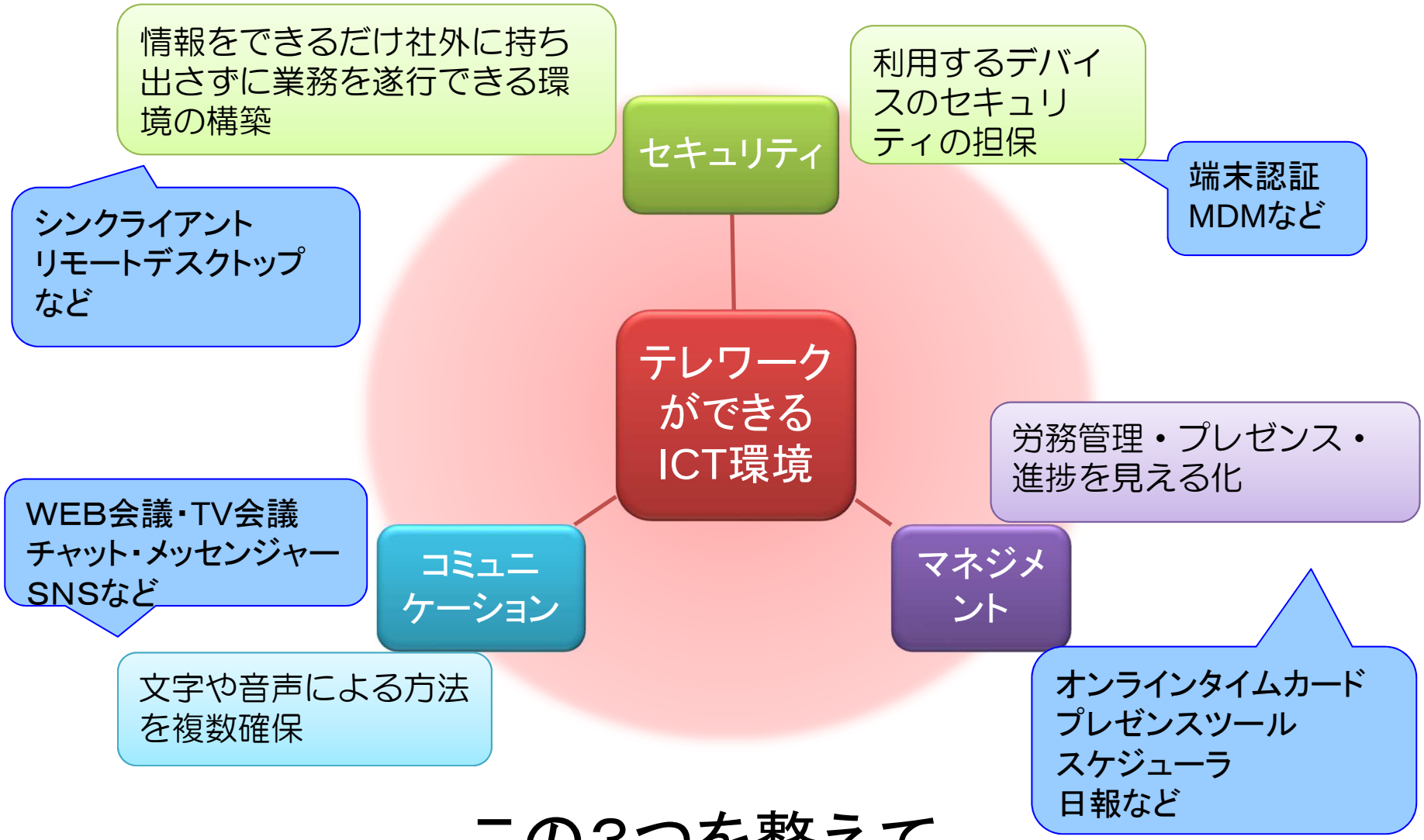
テレワークサポーター

（1）システム構成　（2）顔認証技術を用いた検出





【まとめ】テレワーク実施に必要なICT環境構築のポイント



この3つを整えて

「いつもの仕事がどこでもできる」環境に。

ご清聴いただきありがとうございました。