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対策のポイント～

Flexible Work,
Flexible Business,
Flexible Life.

TELEWORK MANAGEMENT 株式会社 テレワークマネジメント
鵜澤　純子

CONTENTS

1. 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.技術に関する対策

3.ルールと人に関する対策

<弊社のご紹介>

株式会社 テレワークマネジメント

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

240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

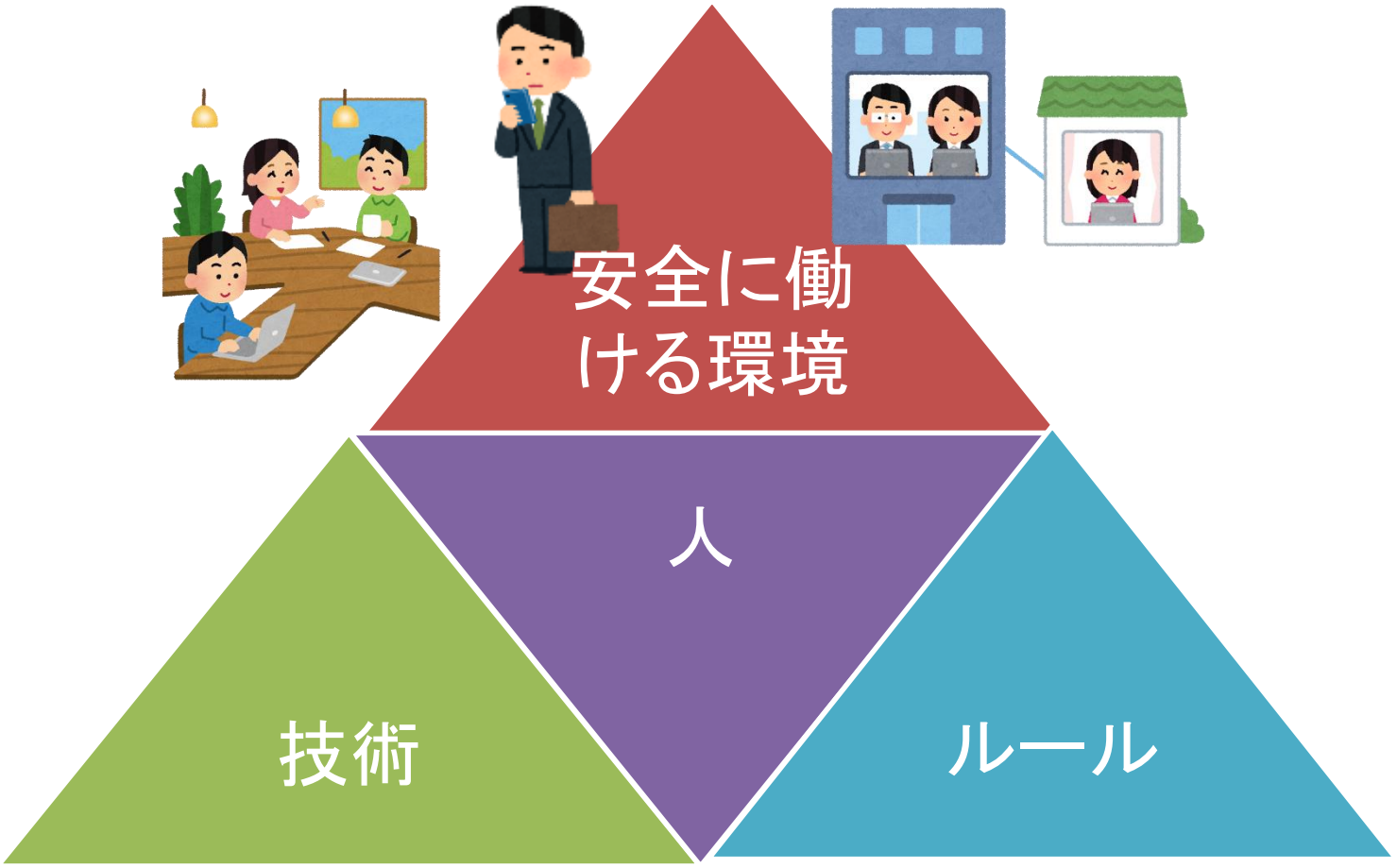
イクボスアワード2014 / DIVERSITY 100 2014 / IT経営実践認定企業 / Hokkaido Family Education Support Companies / TW100 Telework Pioneer / ホワイト企業認定

<総務省　テレワークセキュリティ ガイドラインについて>

株式会社 テレワークマネジメント

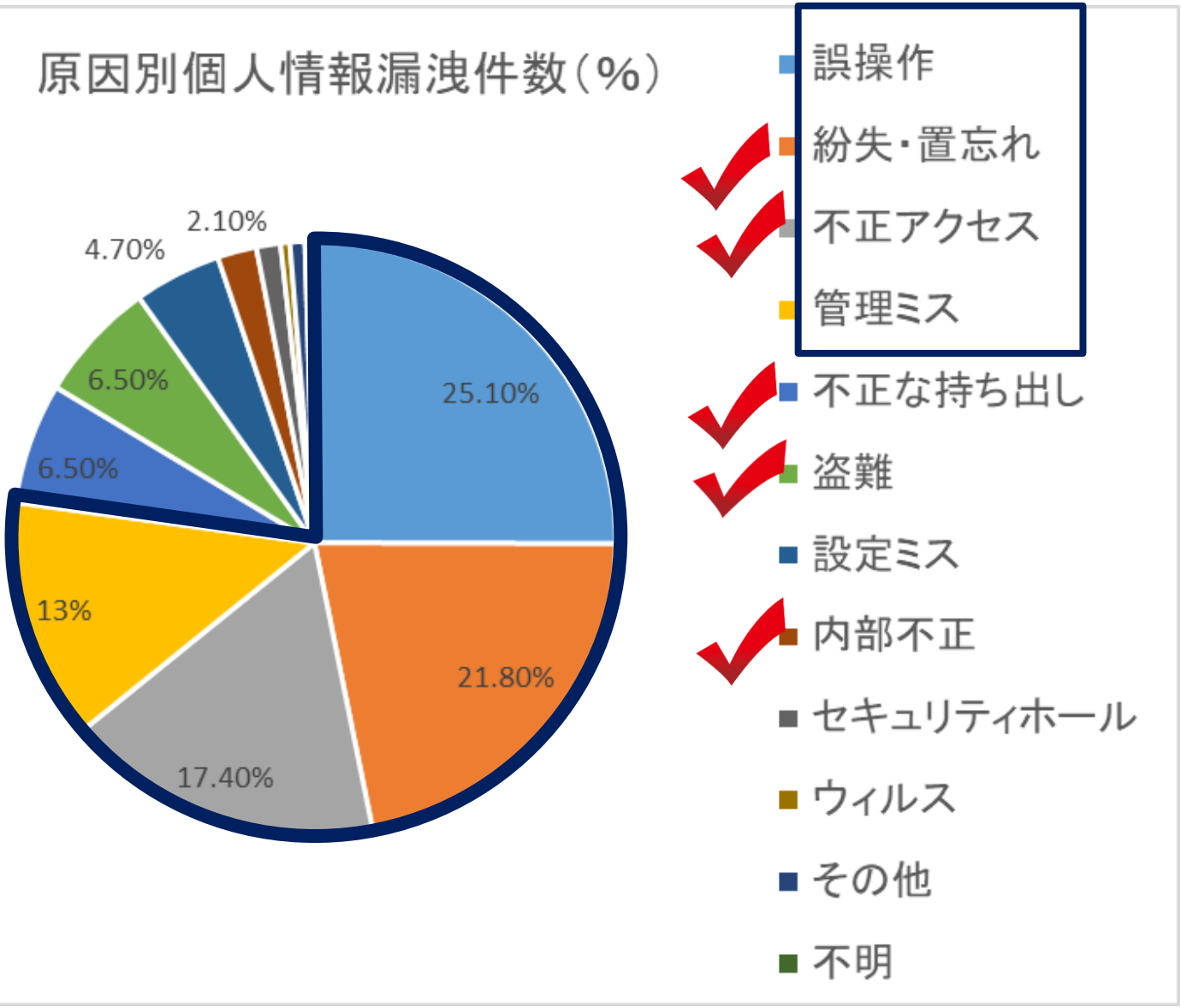
1.1.テレワークセキュリティガイドライン第4版

- **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）
- 働き方やICT技術などを、今の現状に合った内容にアップデート



<技術に関する対策>

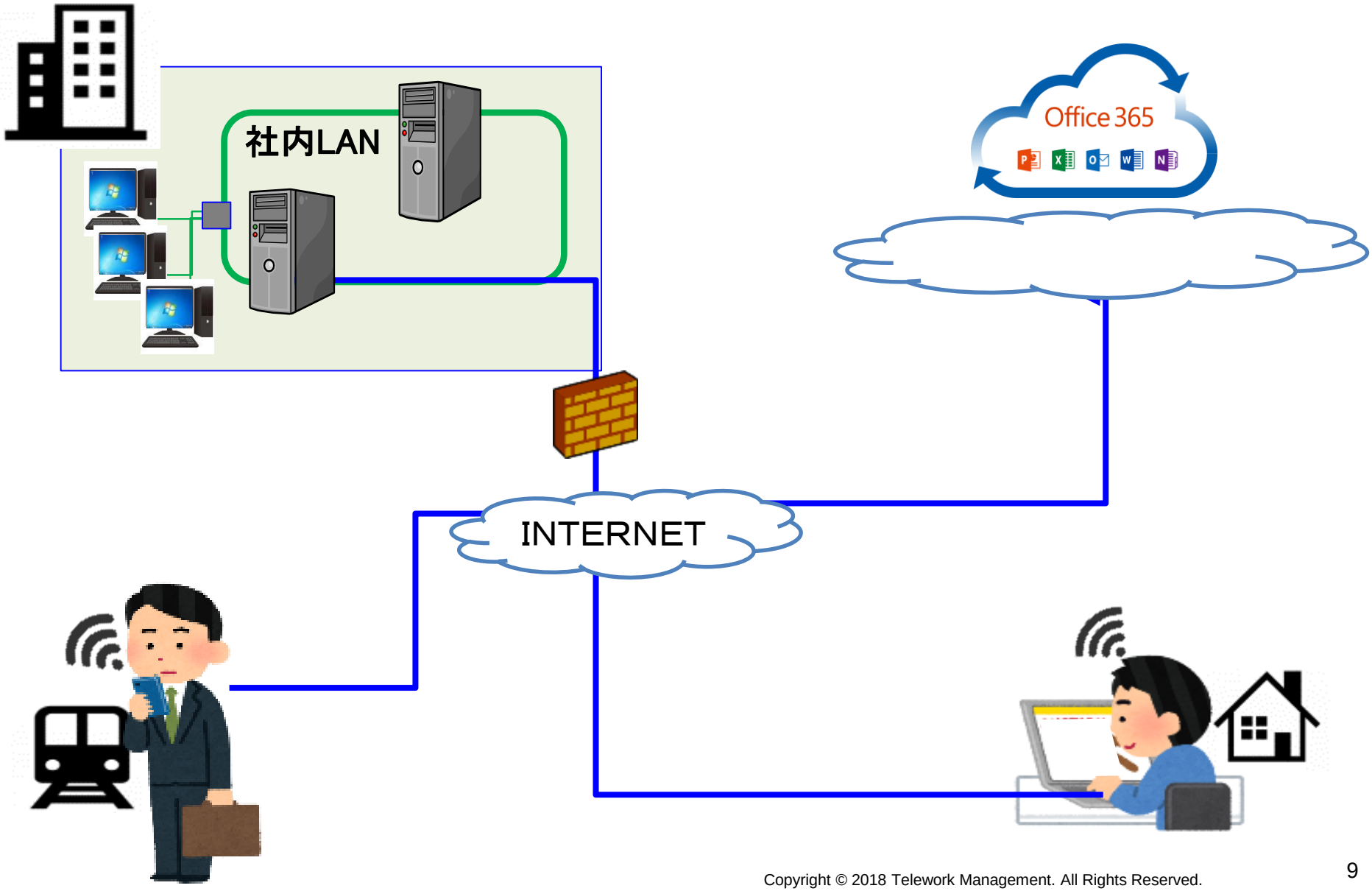
2.1.情報漏洩の原因



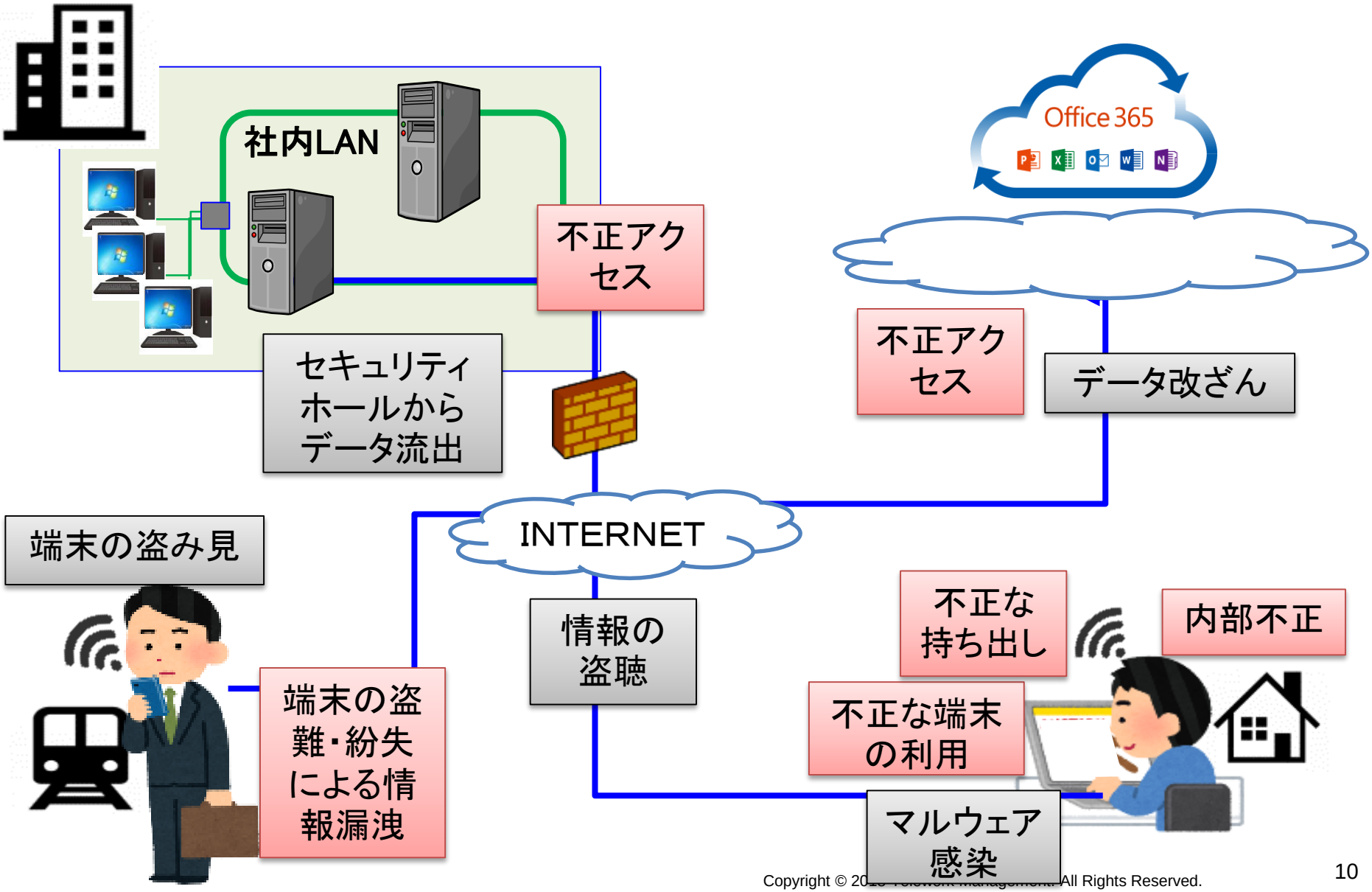
テレワークと関連が深いと考えられるもの

出展：NPO日本ネットワークセキュリティ協会「2017年情報セキュリティインシデントに関する調査報告」

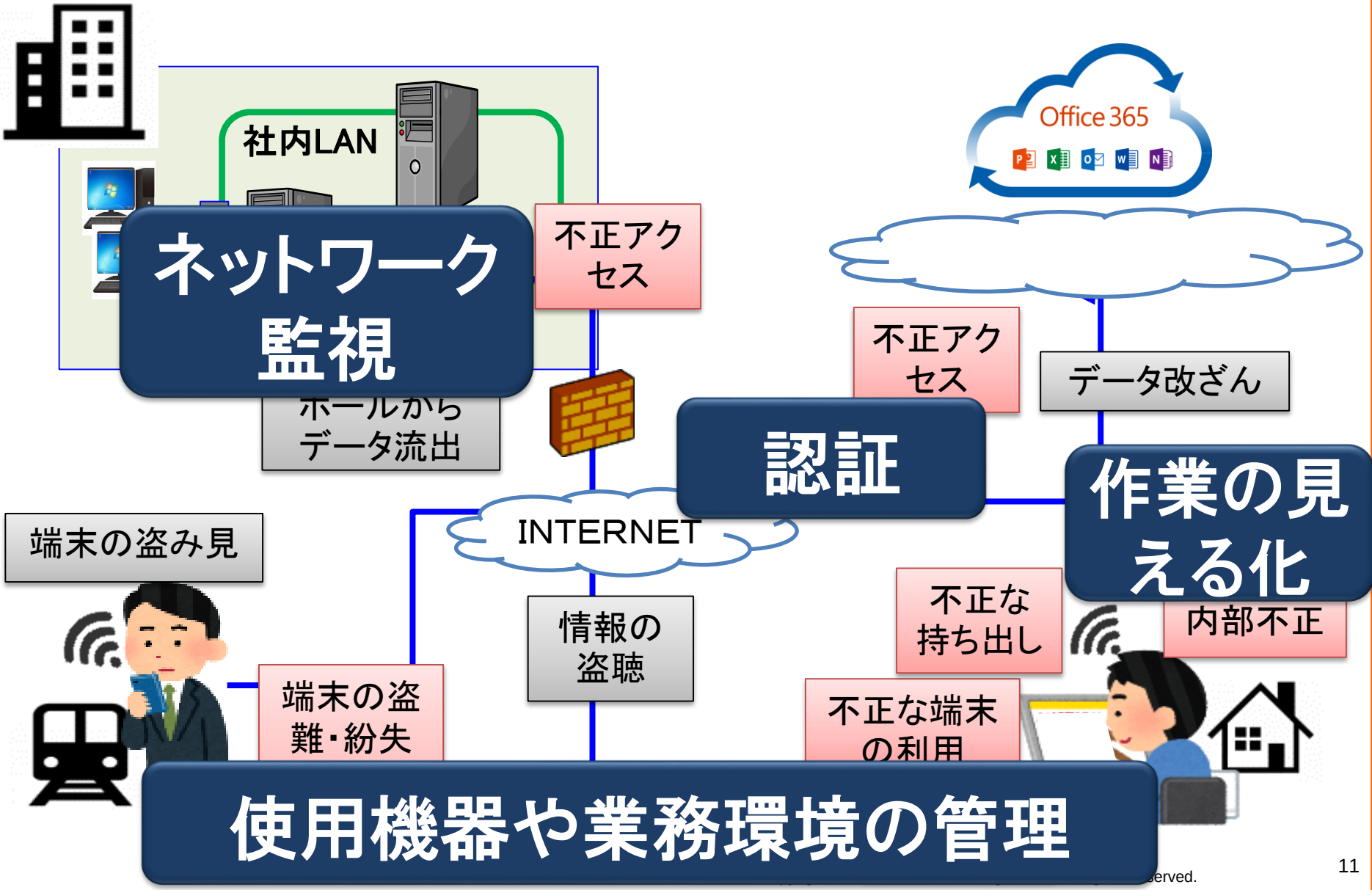
2.2.テレワーク時の情報セキュリティリスクのイメージ



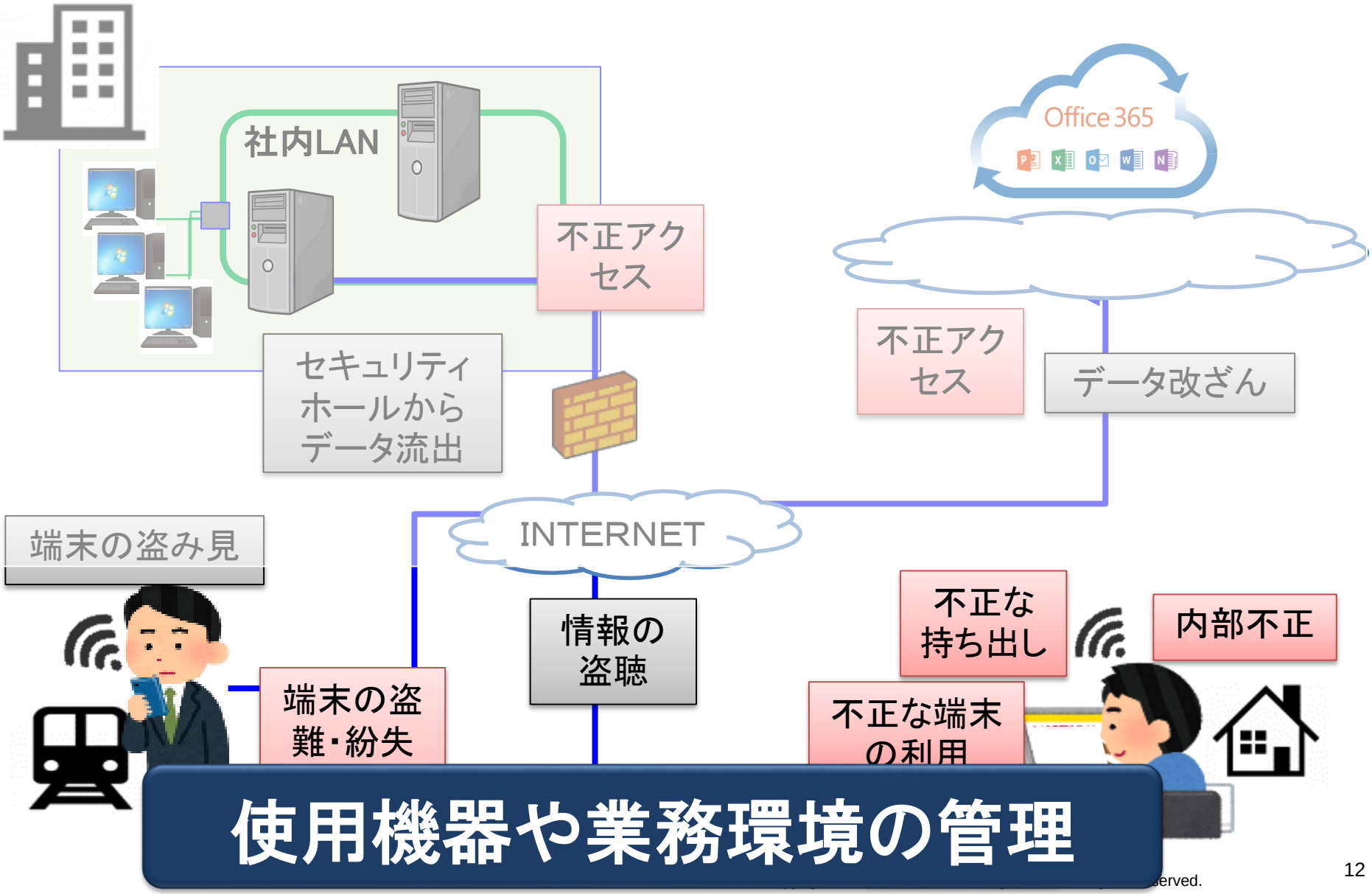
2.2.テレワーク時の情報セキュリティリスクのイメージ



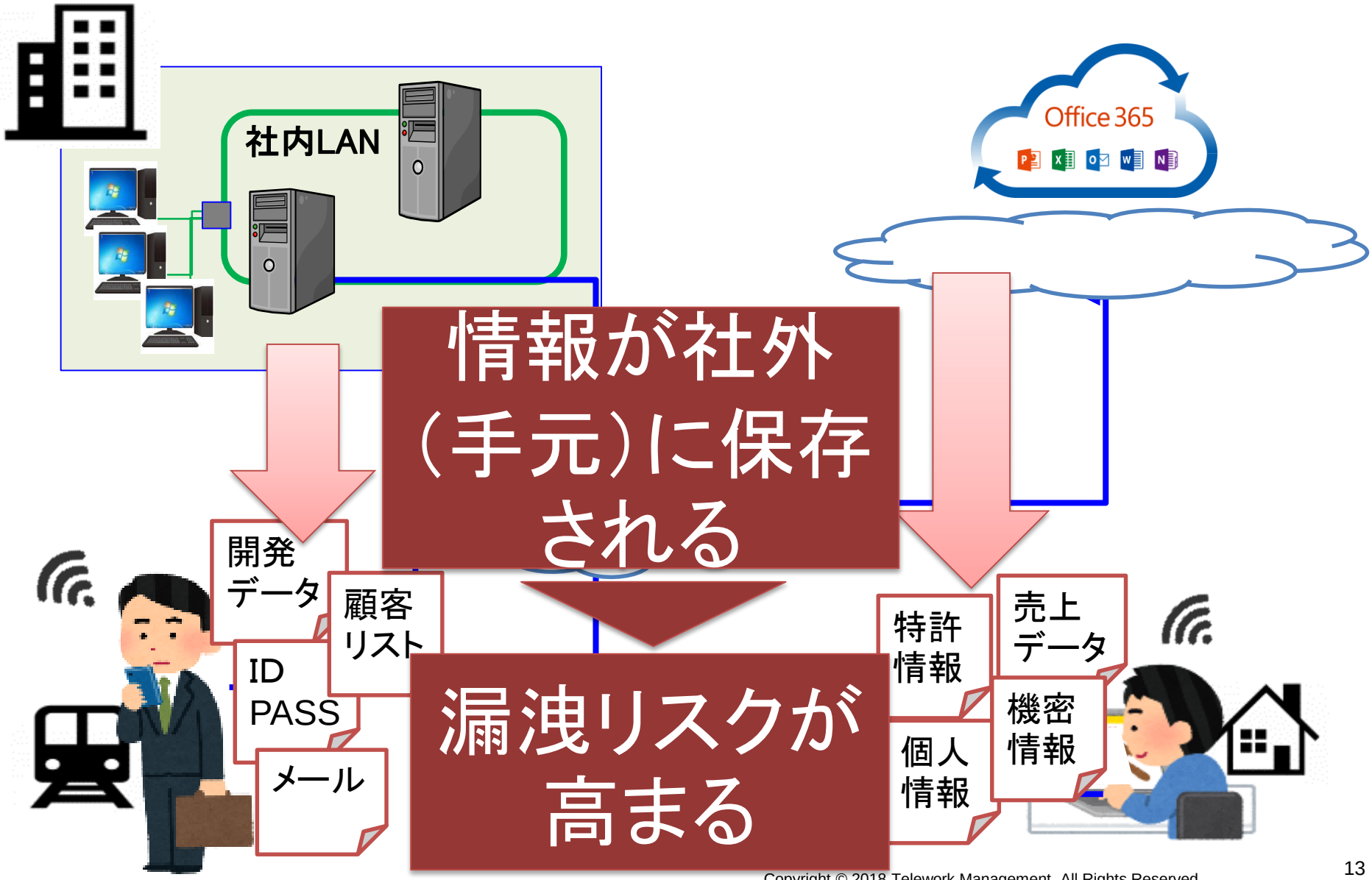
2.3.情報セキュリティリスクへの対策



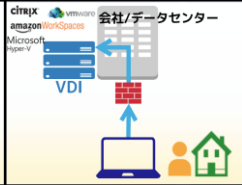
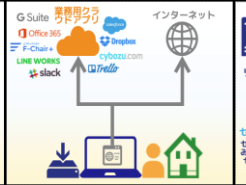
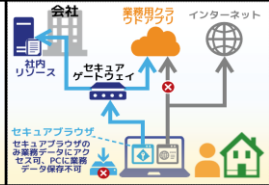
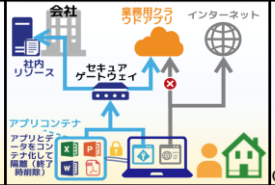
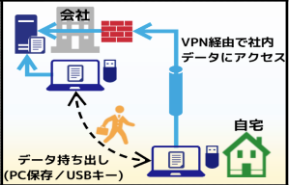
2.4. 対策その1：使用機器や業務環境の管理



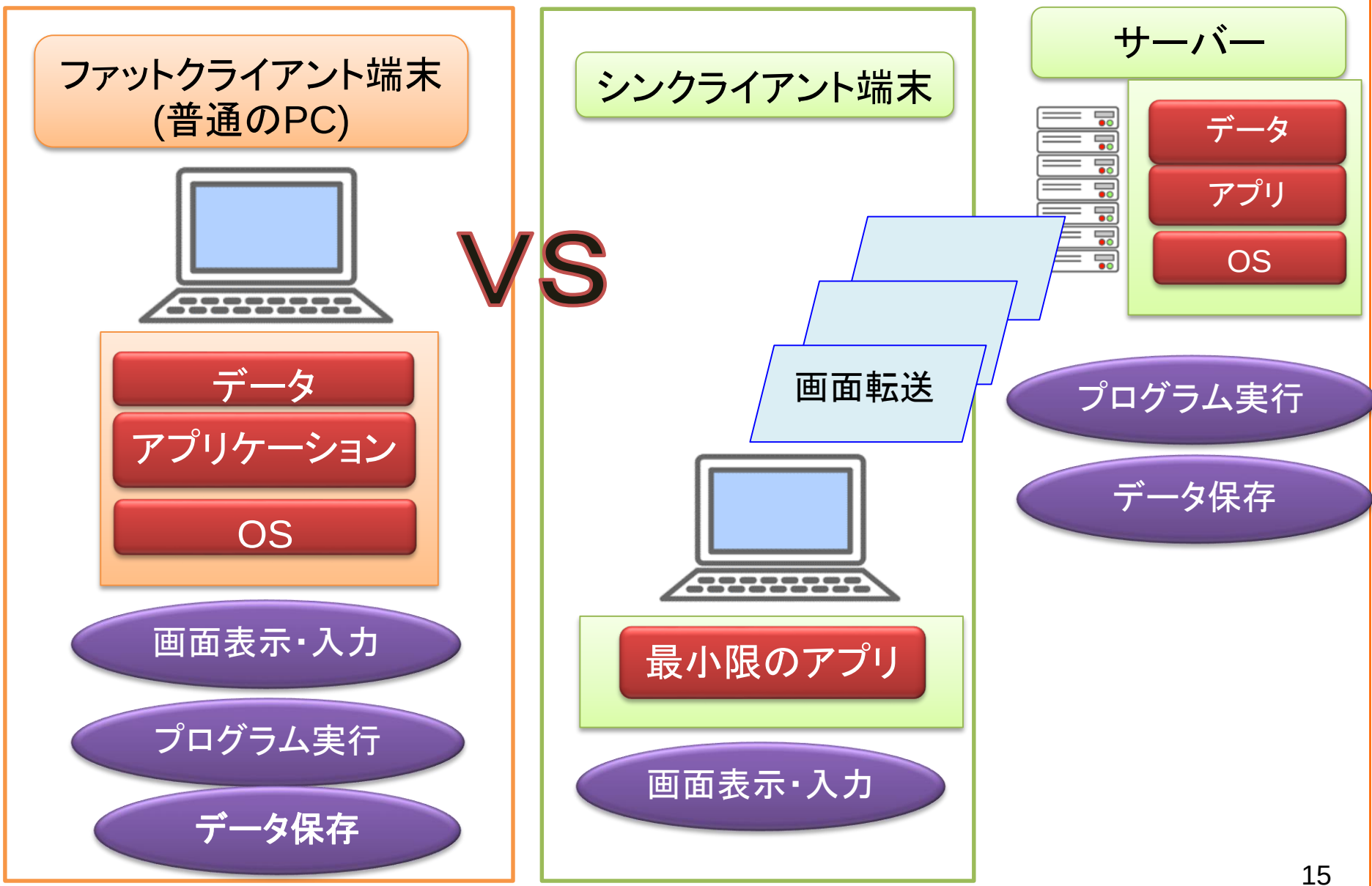
2.5.テレワークで仕事をすると何が起きる？



2.6.テレワークの方法に応じた対策が必要

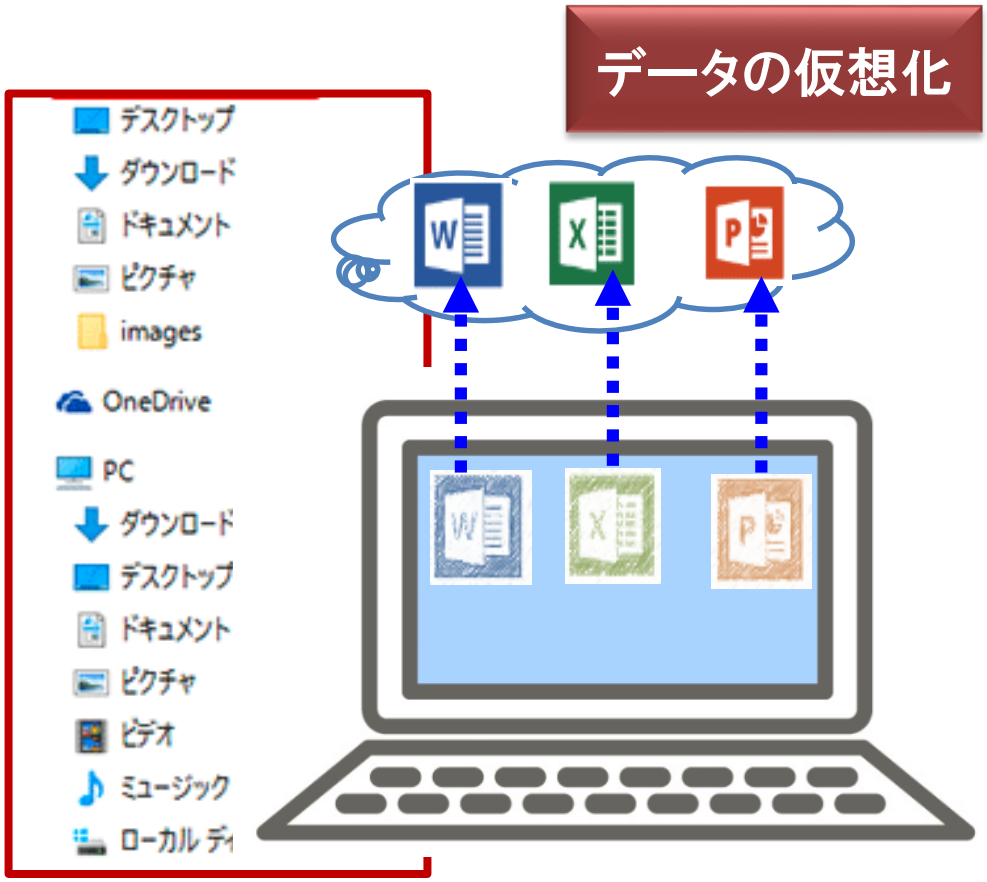
	リモートデスクトップ方式	仮想デスクトップ方式	クラウド型アプリ方式	セキュアブラウザ方式	アプリケーション分離方式	PC持ち帰り方式
						
概要	会社自席PCを遠隔操作	会社・データセンターのVDIを遠隔操作	クラウド型アプリを用いて業務	テレワーク端末にデータを残さないセキュアブラウザを使用	業務アプリとデータをコンテナ化して一般アプリと分離	会社とテレワークで同じ端末を使用
テレワーク端末への情報保存	保存しない	保存しない	どちらも可	保存しない	保存しない	保存する
データ漏洩等のリスク	危険性小さい	危険性小さい	危険性あり	危険性小さい	危険性小さい	危険性大きい
会社業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

2.7.「情報を手元に残さない」技術：シンクライアント化



2.8.「情報を手元に残さない」技術：その他の方法

PC内の**「コンテナ化」された領域のみ**で作業＆ファイルの一時保存が可能。アプリ終了でコンテナごと削除

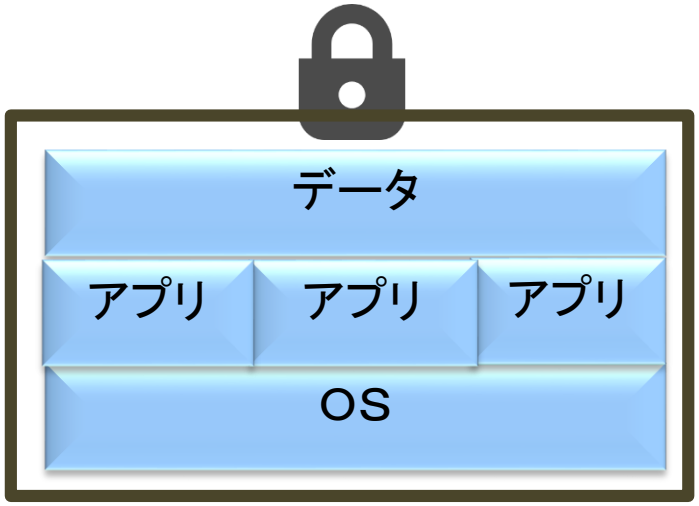


デスクトップ、ドキュメントフォルダ内の**ファイルを仮想化**し、実体をクラウドに保存。手元ではキャッシュを使って作業を行い、電源オフでキャッシュも削除

2.9.「手元に残ってしまった情報」への対応策

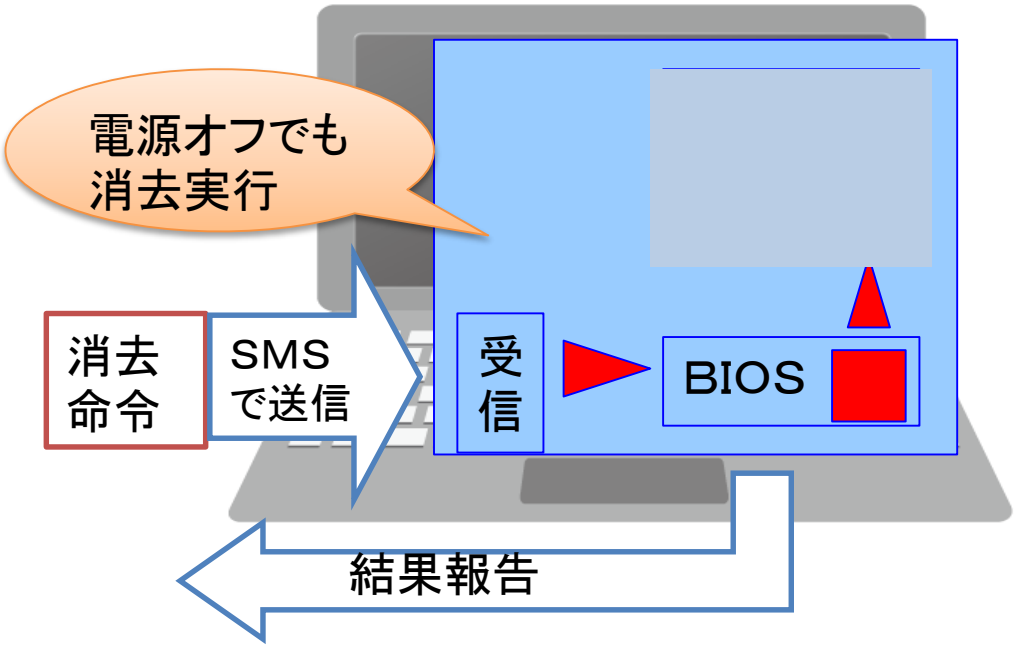
PCのハードディスクの暗号化

データをフォルダ・ファイル単位で暗号化するのではなく、OS領域やシステムファイル領域を含めたハードディスクを丸ごと暗号化

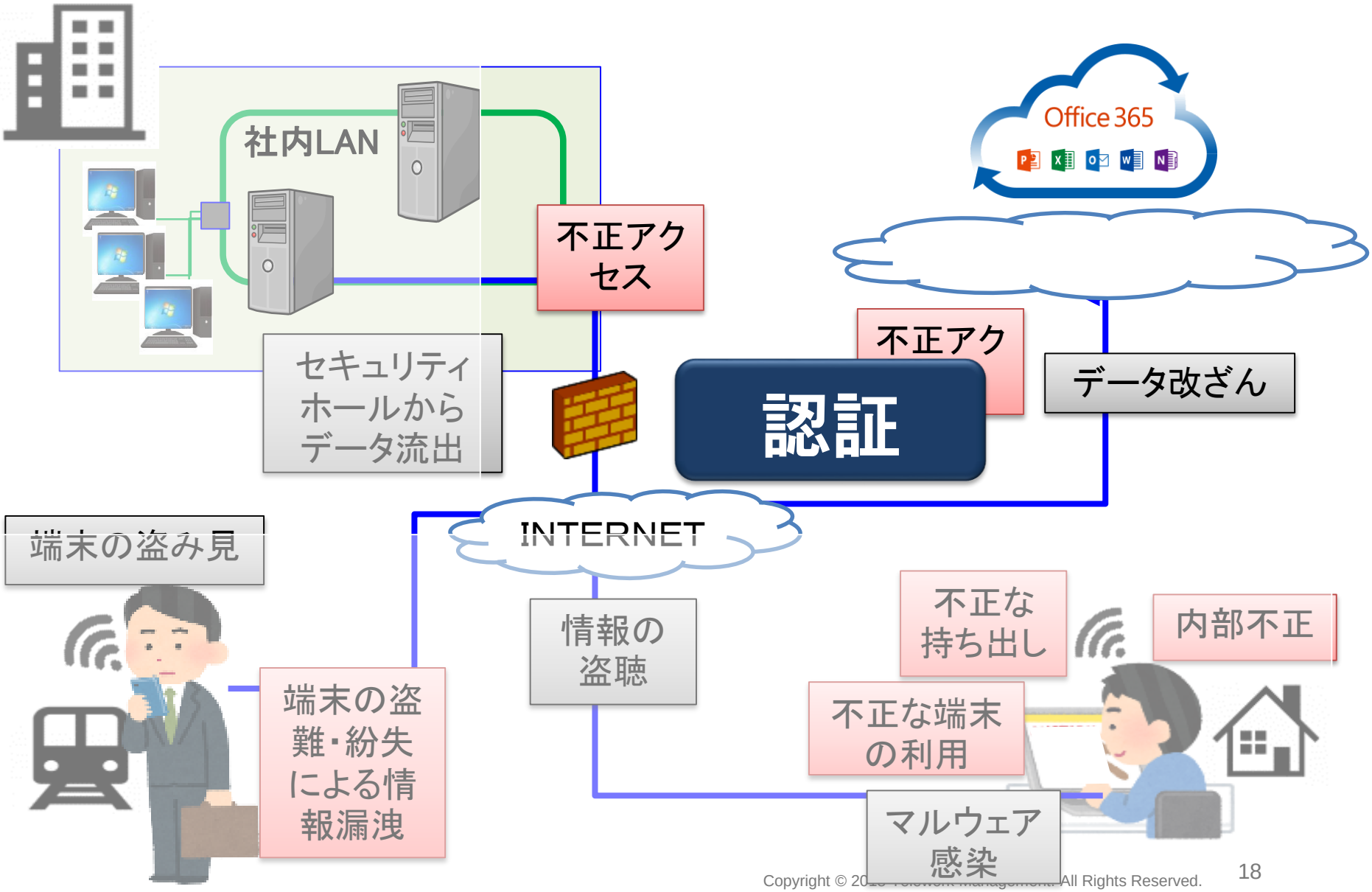


PCのハードディスクのリモートワイプ

端末に保存されたデータを、ネットワークを経由した遠隔操作で消去。電源オフでも実行可能な製品も。



2.10.対策その2：認証



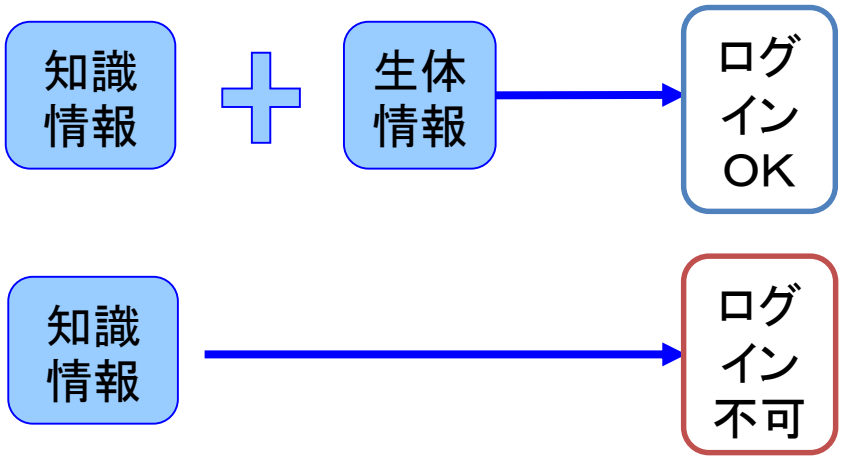
2.11.「認証」を強化することで不正アクセス等を防止

多要素認証による本人確認

【知識情報】
ID，パスワード、PIN番号など

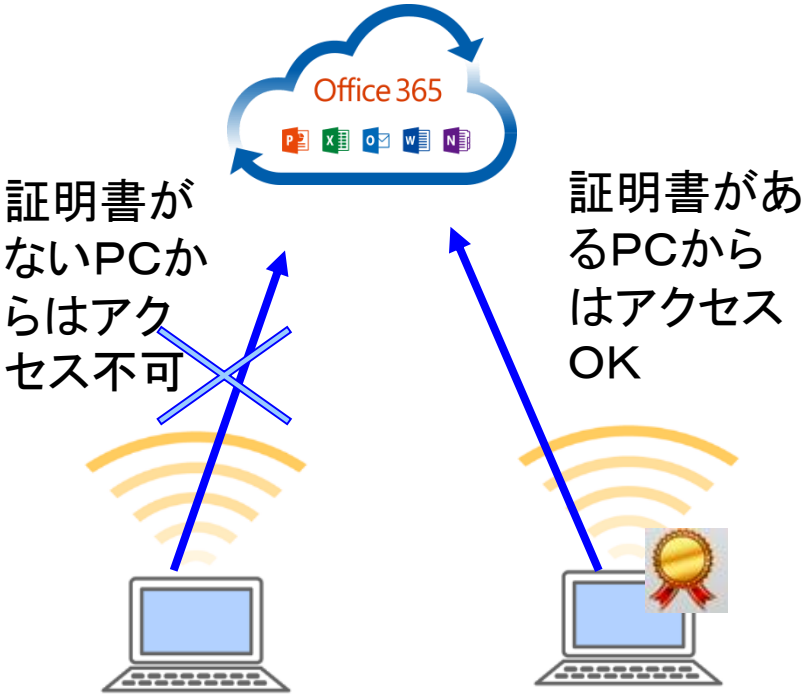
【所持情報】
ワンタイムパスワード、SMS認証、USBトークン、マトリックス認証など

【生体情報】
指紋認証、顔認証など

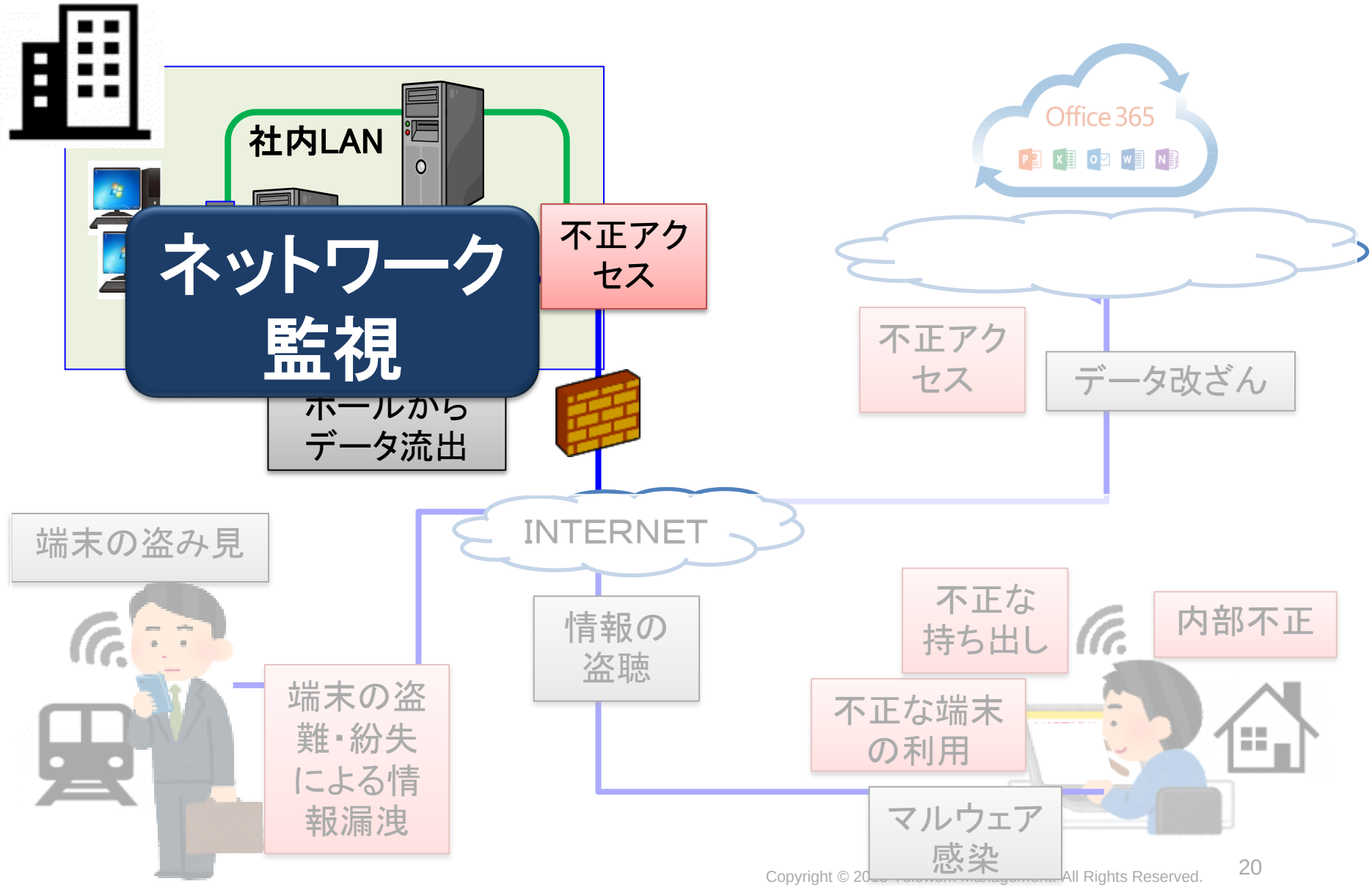


クライアント証明書による利用端末の限定

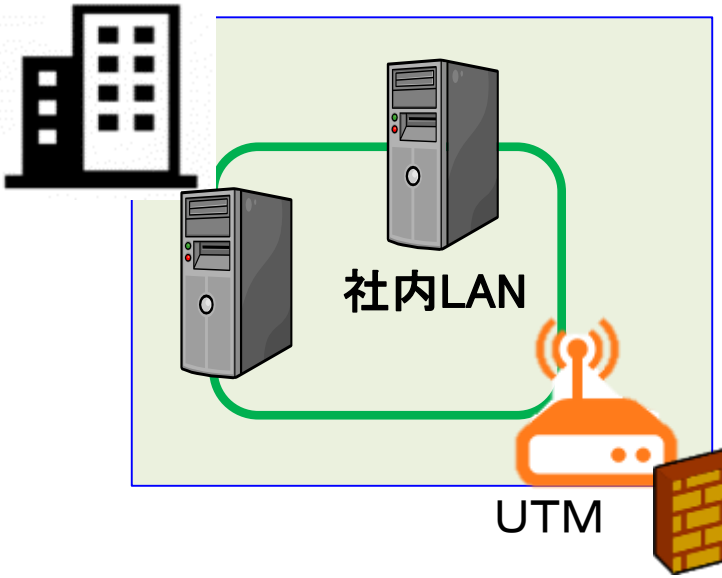
クライアント証明書をユーザのデバイスにインストールすることで、ユーザが正規の利用者であることを認証。



2.12.対策その3：ネットワーク監視



2.13.社内ネットワークの「水際対策」



UTM (Unified Threat Management＝統合脅威管理) とは、複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行う機器

社内LAN

・情報漏洩防止
・不適切なアプリの利用
・不正サイトへのアクセス防止
・ウィルス感染メールの送信
・C＆Cサーバとの通信

出口対策

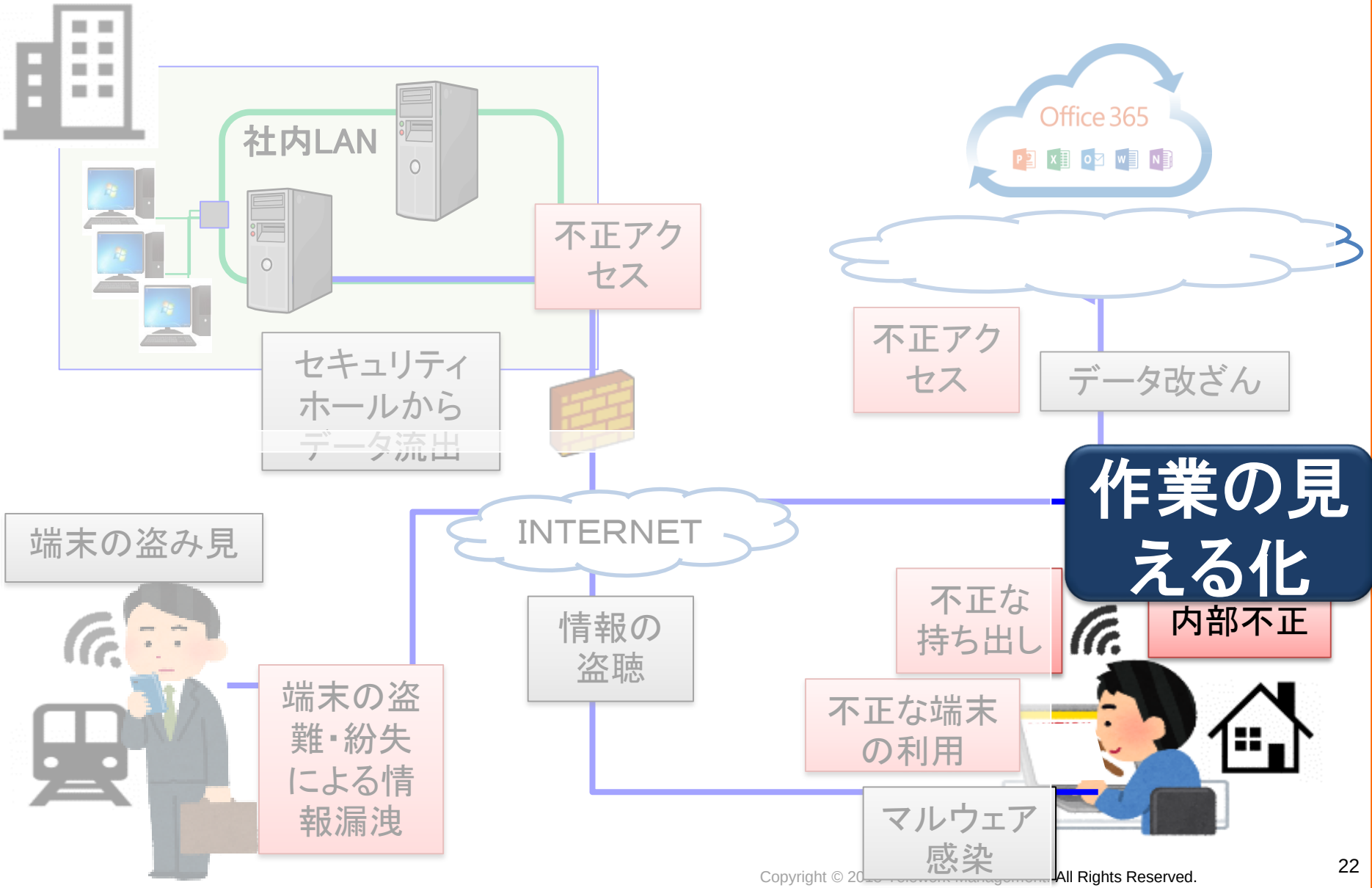
入口対策

UTM

インターネット（社外）

・ウィルス
・迷惑メール
・ネットワーク攻撃
・マルウエア、スパイウェア
・標的型攻撃

2.14.対策その4：作業の見える化

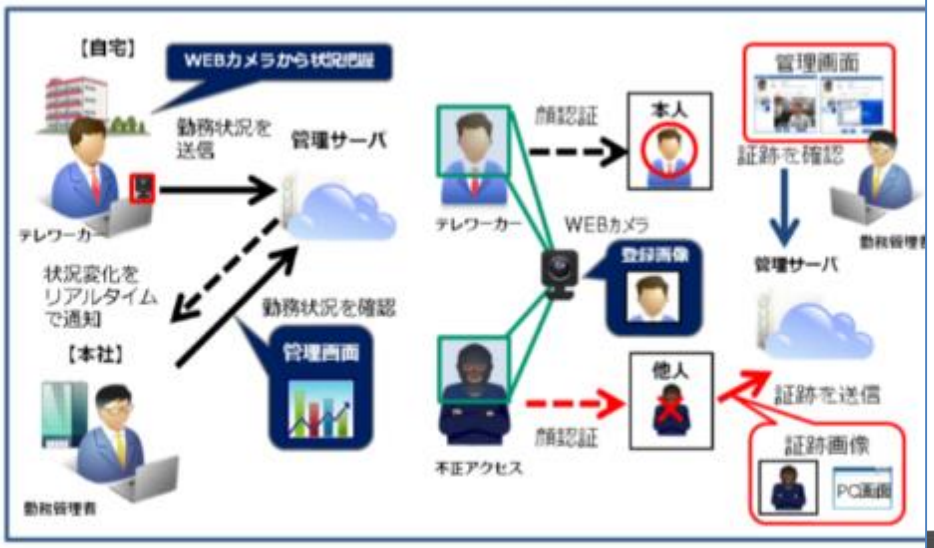


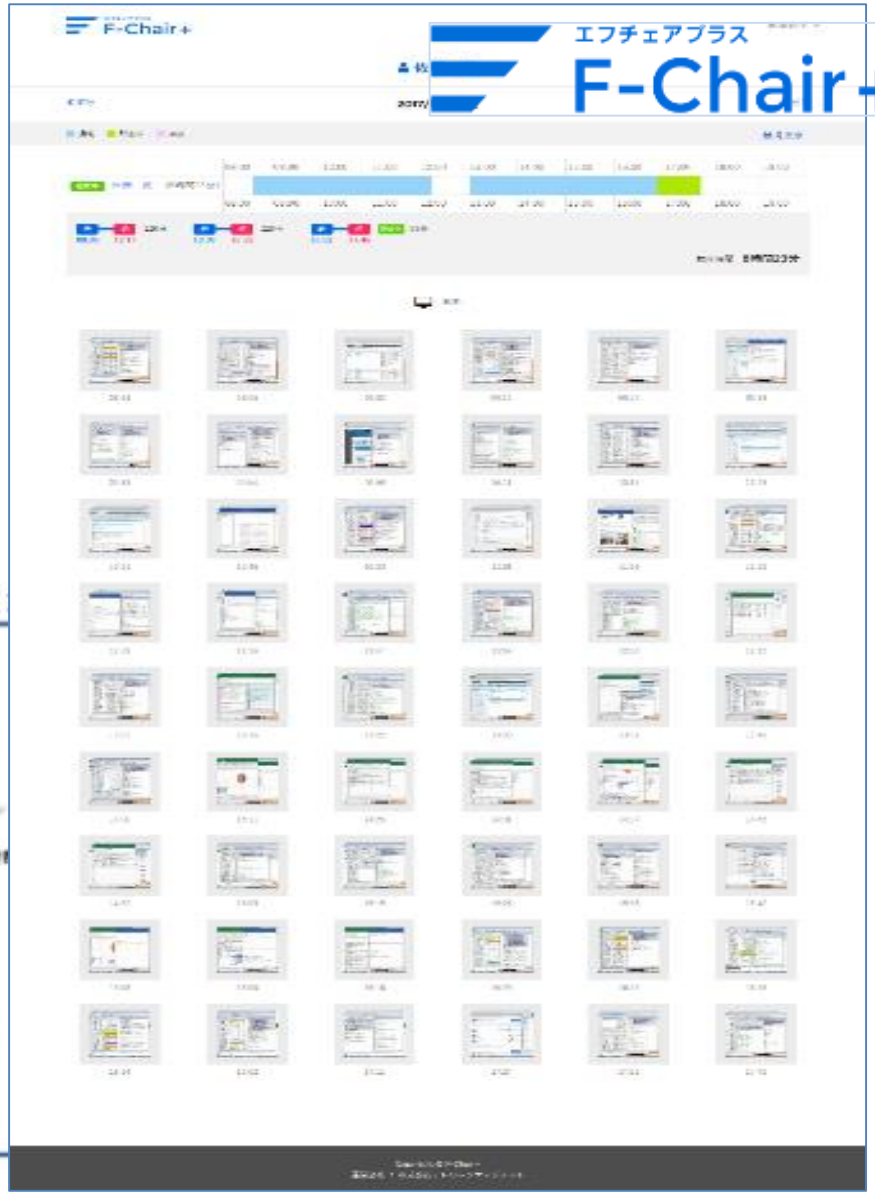
2.15.内部不正対策=ログ取得、手元の見える化

時間管理・記録と併せ、
作業画面の記録や
顔認証により、
遠隔の社員を見える化

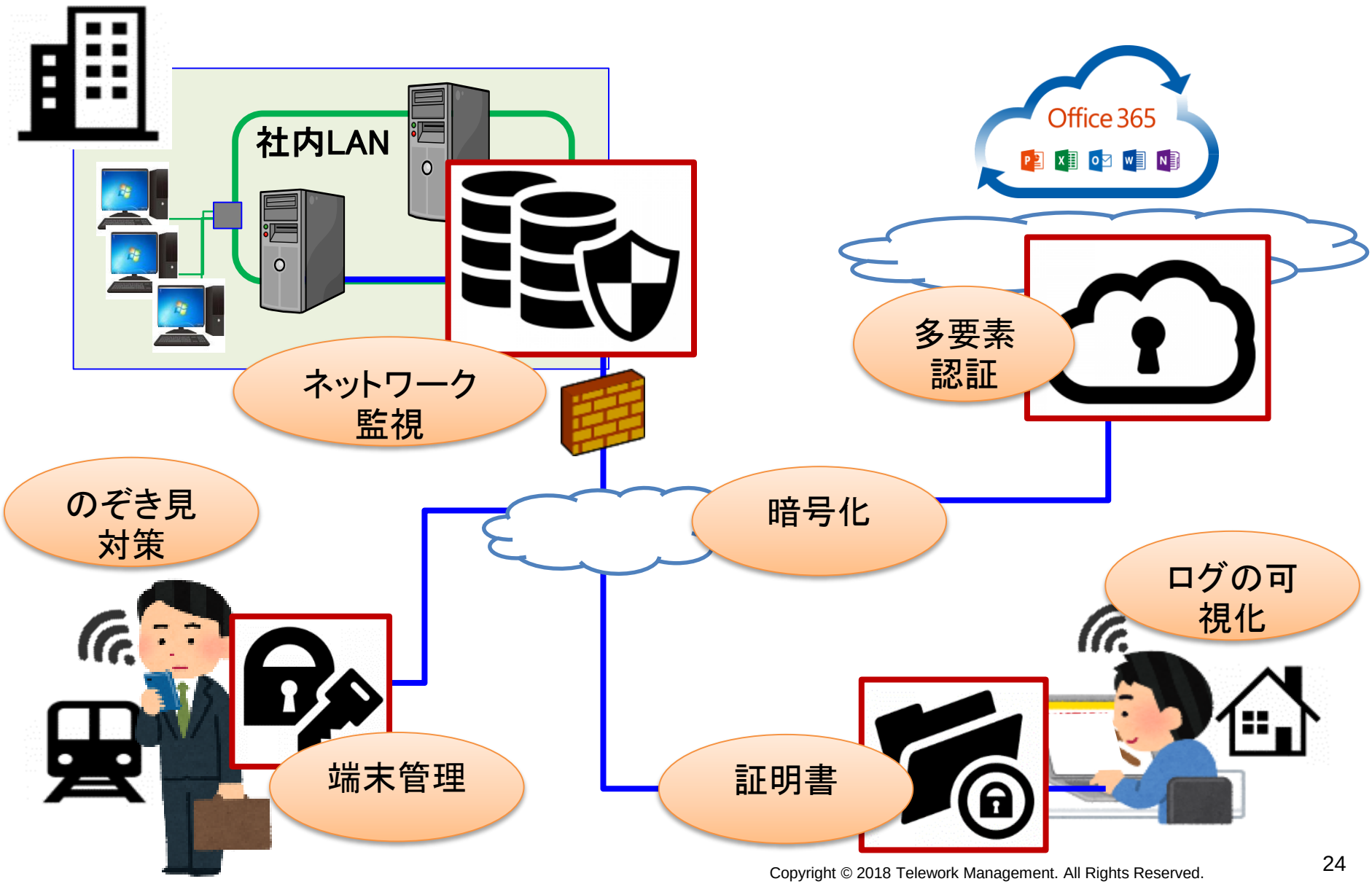
テレワーク
サポーター

（1）システム構成　　（2）顔認証技術を用いた検出





2.16.情報セキュリティリスクに様々な技術を組み合わせた対策を



<ルールと人に関する対策>

3.1.ルールに関する対策

情報セキュリティ保全対策の大枠を作る

1
- 対策の必要性を理解し、必要な人材、予算を割り当てる

2
- 情報セキュリティポリシーを定め、PDCAで定期的に管理するルールを作る

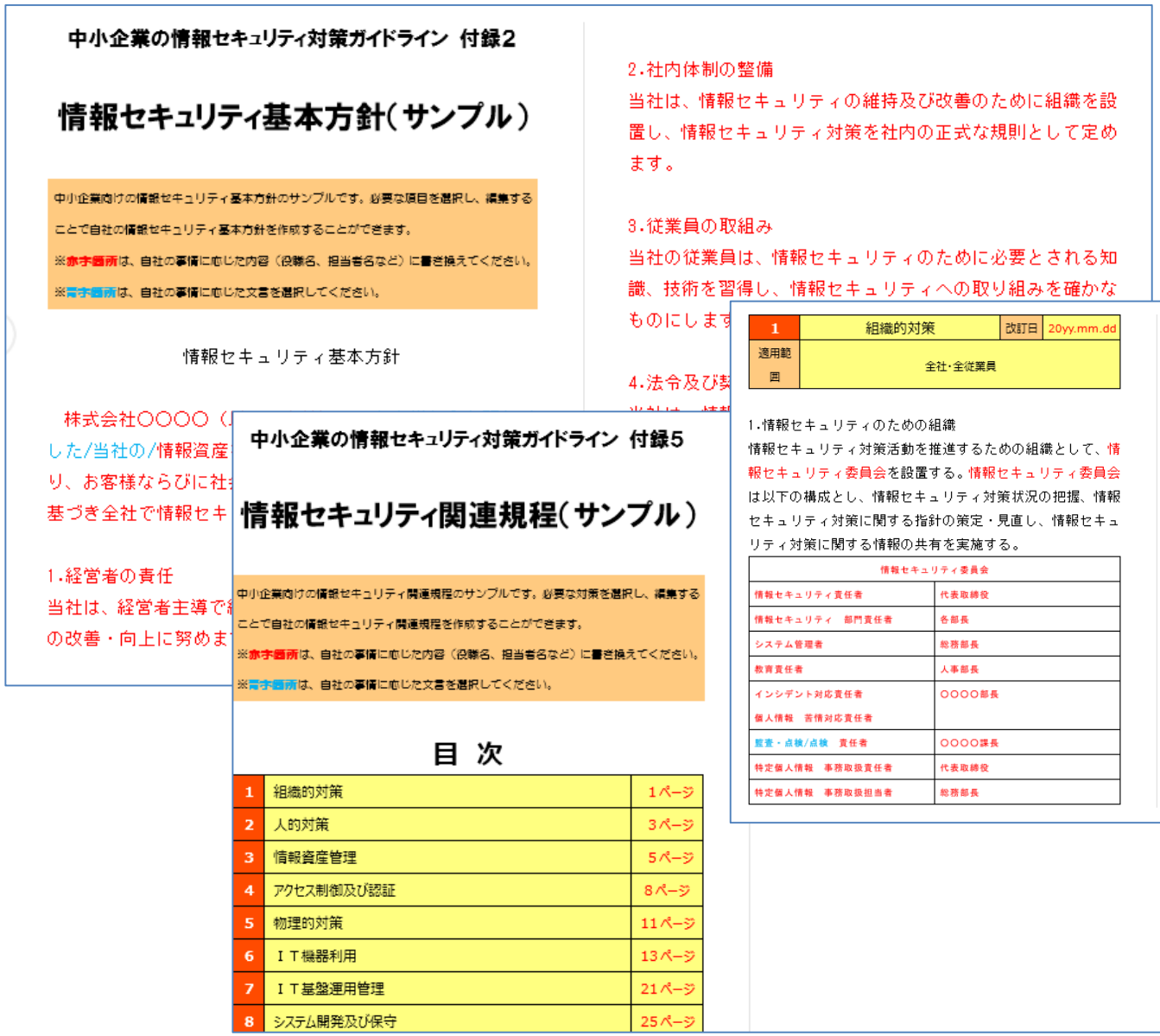
3
- 社内の情報資産を重要度に応じたレベル分けを行い、テレワークでの利用可否と、利用可の場合の取扱い方法を定める

3.2.（参考）IPA「中小企業の情報セキュリティ対策ガイドライン」

「サイバーセキュリティ経営ガイドライン」の改訂や、中小企業等を対象としたクラウドサービスの充実化などの環境変化を受けて、2019年３月に第3版改訂

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

3.3.（参考）冊子に含まれる各種ひな形



中小企業の情報セキュリティ対策ガイドライン 付録2

情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。

※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。

※青字箇所は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社〇〇〇〇（
した/当社の/情報資産
り、お客様ならびに社
基づき全社で情報セキ

1.経営者の責任
当社は、経営者主導で
の改善・向上に努めま

2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み
当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします

4.法令及び契

中小企業の情報セキュリティ対策ガイドライン 付録5

情報セキュリティ関連規程（サンプル）

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。

※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。

※青字箇所は、自社の事情に応じた文言を選択してください。

目 次

1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1.情報セキュリティのための組織
情報セキュリティ対策活動を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員会	
情報セキュリティ責任者	代表取締役
情報セキュリティ　部門責任者	各部長
システム管理者	総務部長
教育責任者	人事部長
インシデント対応責任者 個人情報　苦情対応責任者	○○○○部長
監査・点検/点検　責任者	○○○○課長
特定個人情報　事務取扱責任者	代表取締役
特定個人情報　事務取扱担当者	総務部長

体制図を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を行う。

2.情報セキュリティ取組みの監査・点検/点検

3.4.人に関する対策

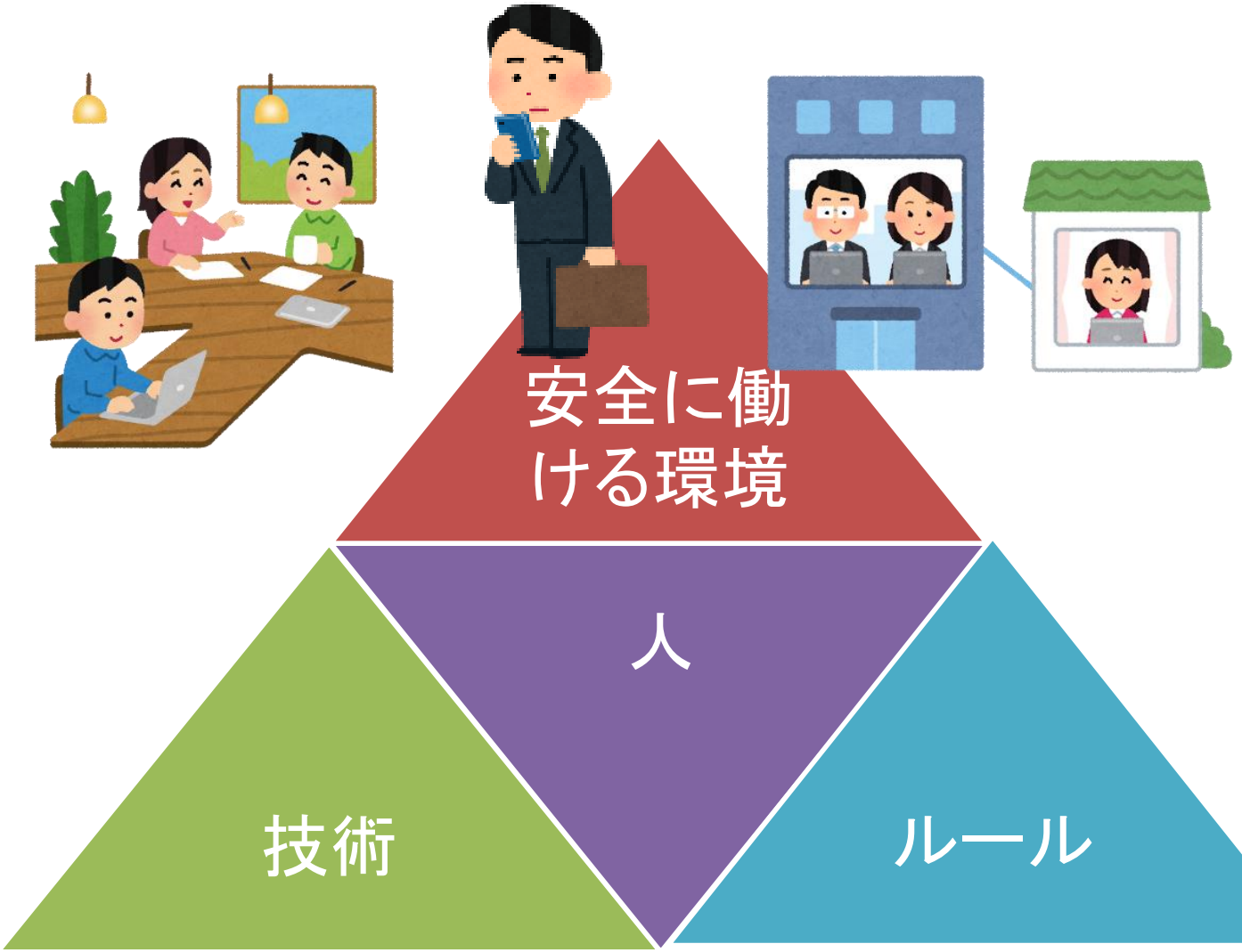
■ 作ったルールを守るのは人～教育研修が重要

1
- 研修などを通じて、作成したルールの社内周知、広報を行う。

2
- 事故を想定した実践的な訓練を実施する

3
- 訓練の結果を踏まえ、周知・理解が足りない部分をさらに広報する

3.5.安全な環境でテレワークを！



ご清聴いただきありがとうございました。