Japan Information Security
Management Systems User Group

働き方改革における情報セキュリティ

日本ISMSユーザーズグループ
インプリメンテーション研究会

2018年12月7日

副主査　:尾崎 幸彦 (NECソリューションイノベータ株式会社)
:中村 昌登 (アイレット株式会社)

I.　はじめに

II. 働き方改革実現に伴う環境変化

III. リスクの例示に基づく、
ISO 27001管理策を活用した対応例

- ビジネスツール
- オフィス環境

IV. まとめ

I.はじめに

働き方改革とは？

テレワーク

≠

働き方改革

残業削減

≠

働き方改革

「働き方改革」とは

「一億総活躍社会」実現に向けた取り組み

引用元
首相官邸「働き方改革の実現」

政府の「働き方改革実行計画」における、11個の具体的施策

1.同一労働同一賃金など非正規雇用の処遇改善
- 同一労働同一賃金の実効性を確保する法制度とガイドラインの整備
- 法改正の施行に当たって

2.賃金引上げと労働生産性向上
- 企業への賃上げの働きかけや取引条件の改善
- 生産性向上支援など賃上げしやすい環境の整備

3.罰則付き時間外労働の上限規制の導入など長時間労働の是正

4.柔軟な働き方がしやすい環境整備
- 雇用型テレワークのガイドライン刷新と導入支援
- 非雇用型テレワークのガイドライン刷新と働き手への支援
- 副業・兼業の推進に向けたガイドラインや改定版モデル就業規則の策定

5.女性・若者の人材育成など活躍しやすい環境整備
- 女性のリカレント教育など個人の学び直しへの支援などの充実
- 多様な女性活躍の推進
- 就職氷河期世代や若者の活躍に向けた支援・環境整備

引用元
首相官邸「働き方改革の実現」

政府の「働き方改革実行計画」における、11個の具体的施策

6.病気の治療と仕事の両立
- 会社の意識改革と受入れ体制の整備
- トライアングル型支援などの推進
- 労働者の健康確保のための産業医・産業保健機能の強化

7.子育て・介護等と仕事の両立、障害者の就労
- 子育て・介護と仕事の両立支援策の充実・活用促進
- 障害者等の希望や能力を活かした就労支援の推進

8.雇用吸収力、付加価値の高い産業への転職・再就職支援
- 転職者の受入れ企業支援や転職者採用の拡大のための指針策定
- 転職・再就職の拡大に向けた職業能力・職場情報の見える化

9.誰にでもチャンスのある教育環境の整備

10.高齢者の就業促進

11.外国人材の受入れ

引用元
首相官邸「働き方改革の実現」

「一億総活躍社会」実現に向けた取り組み

「働き方改革」とは

「一億総活躍社会」実現に向けた取り組み

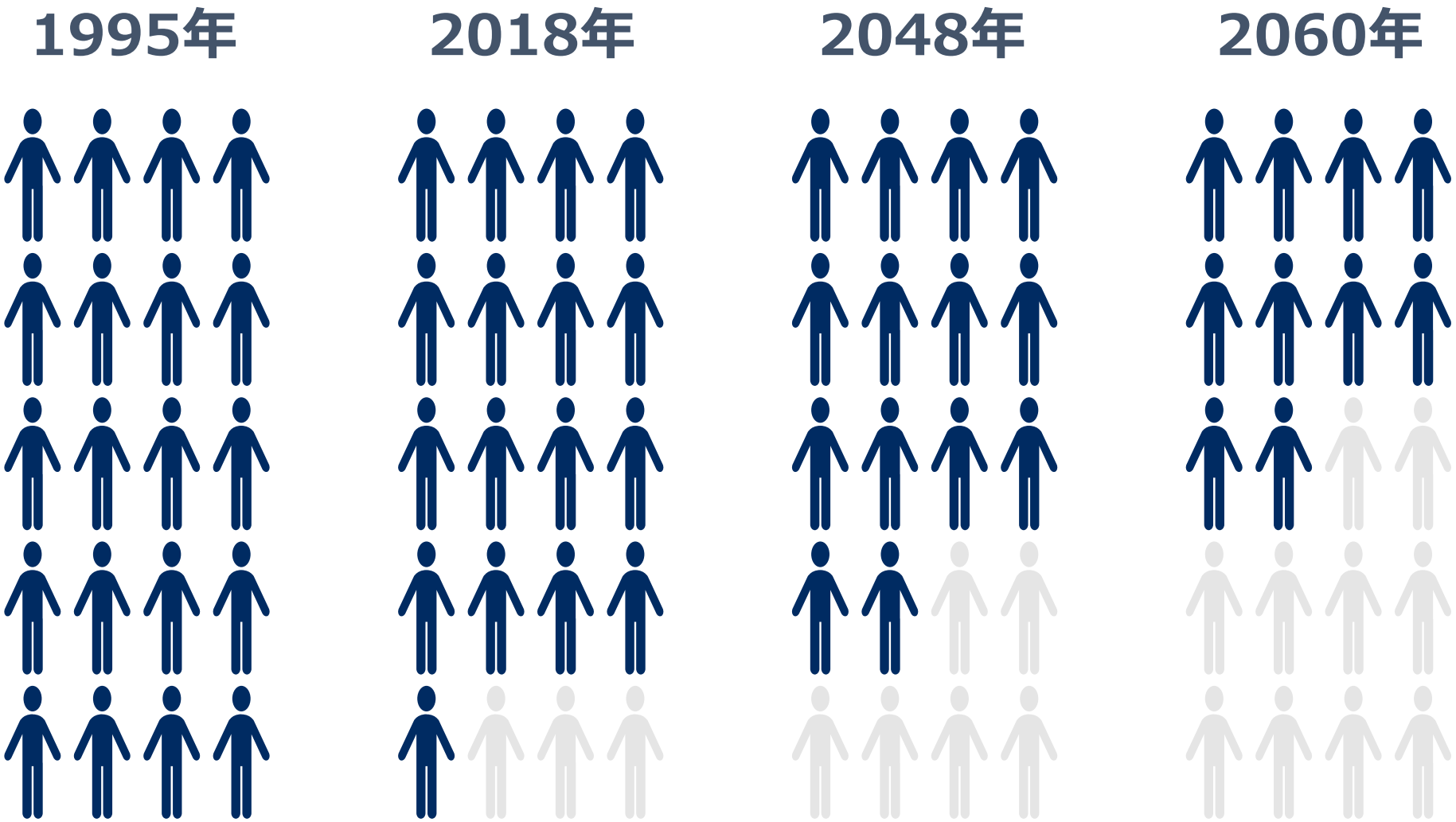
一億総活躍社会とは、少子高齢化が進む中でも、「50年後も人口1億人を維持し、職場・家庭・地域で誰しもが活躍できる社会」のこと

「働き方改革」とは

労働力人口の減少

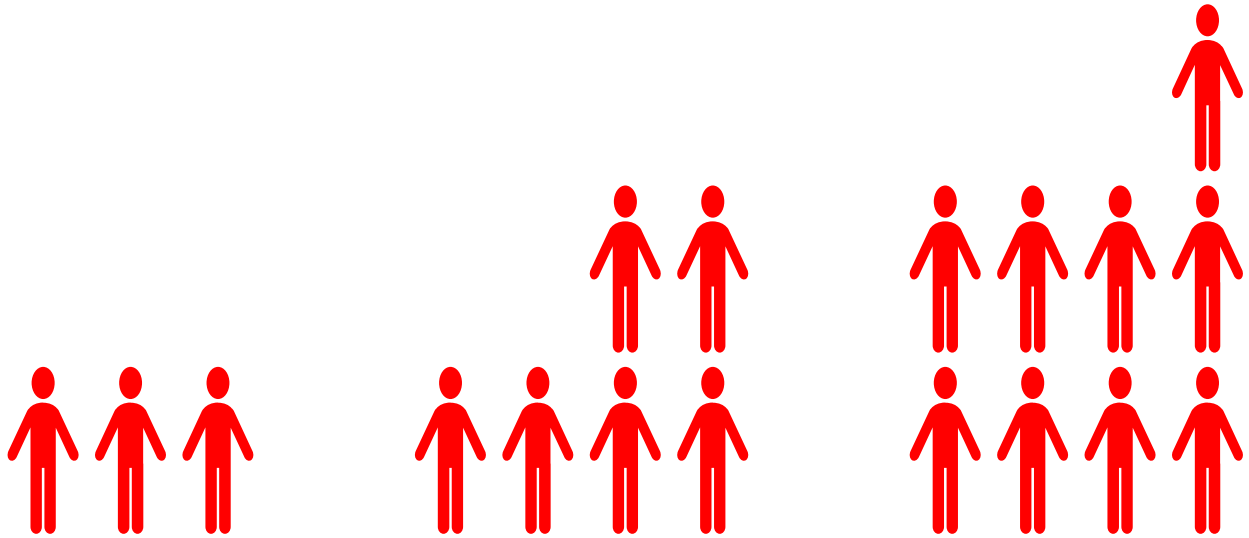
少子高齢化が進む中でも、
職場
で誰しもが活躍できる社会

労働力人口の減少



引用元
国立社会保障・人口問題研究所「日本の将来推計人口」

労働力人口の減少

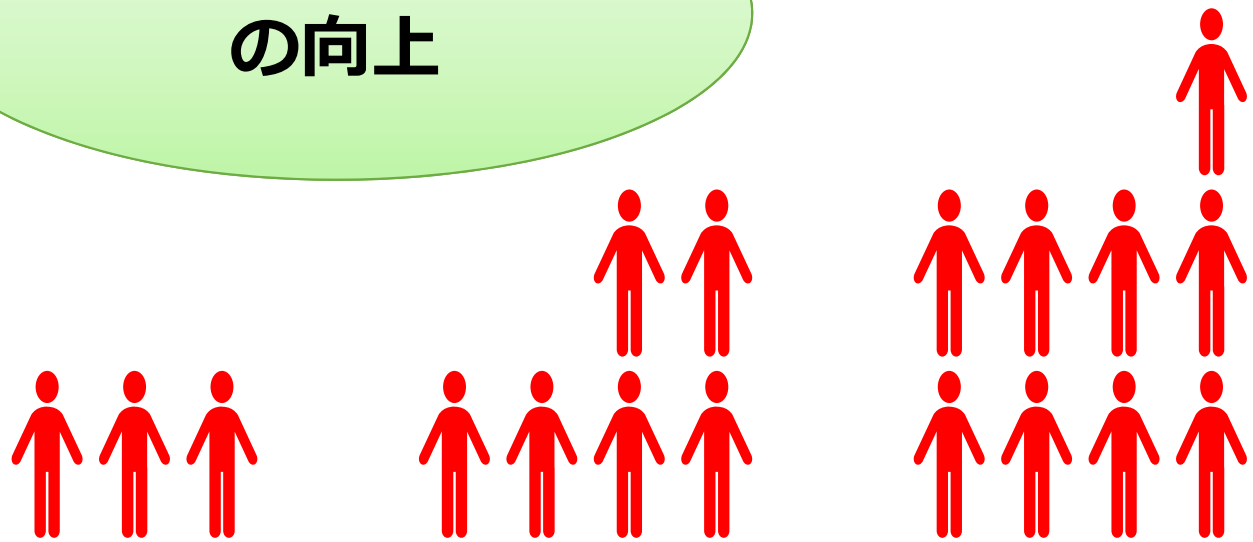


労働力人口減少への対策

働き手を増やす

出生率の向上

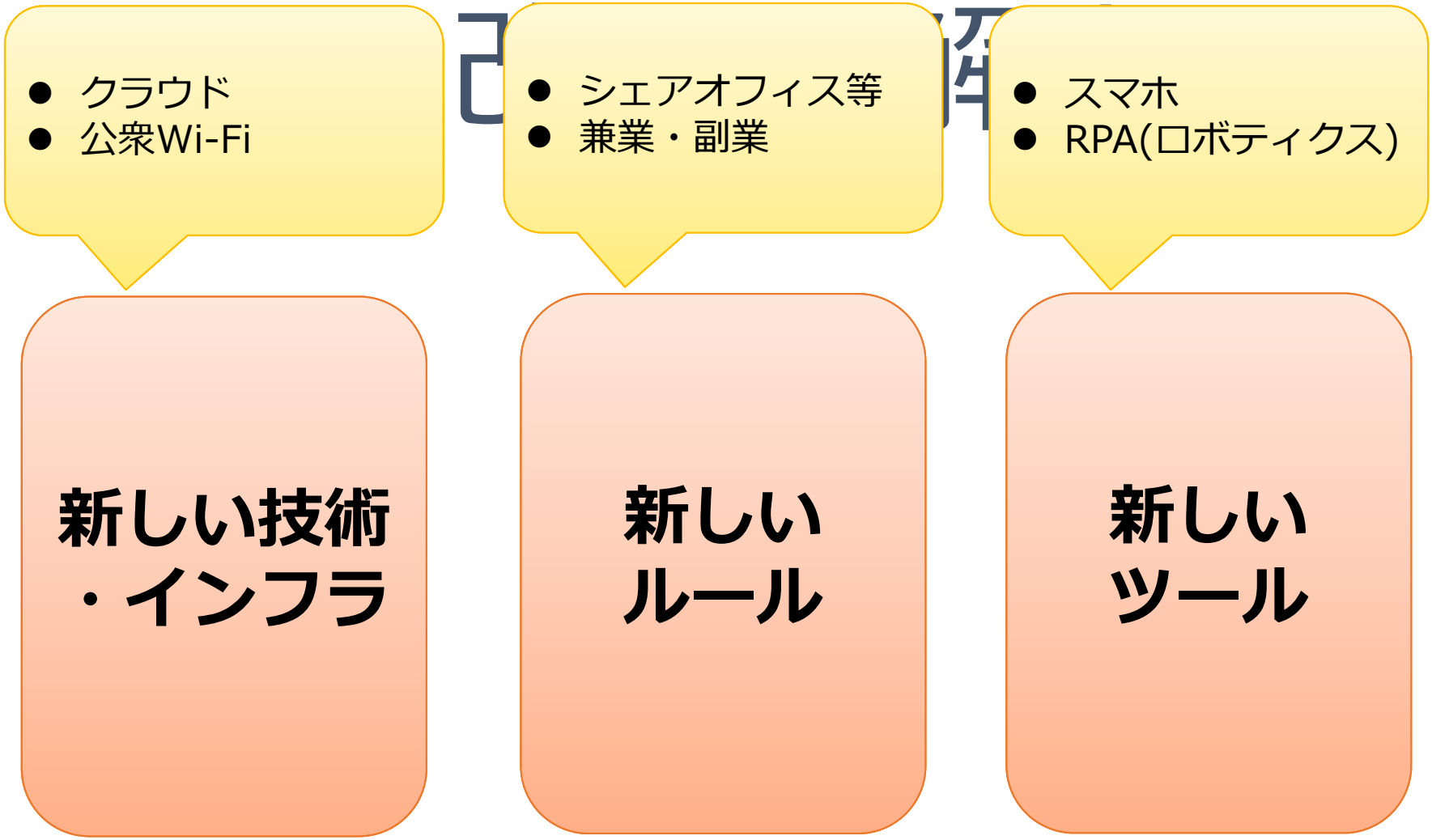
労働生産性の向上



ITで改善・解決

労働生産性
の向上

情報セキュリティへの影響



重大な変化が生じる

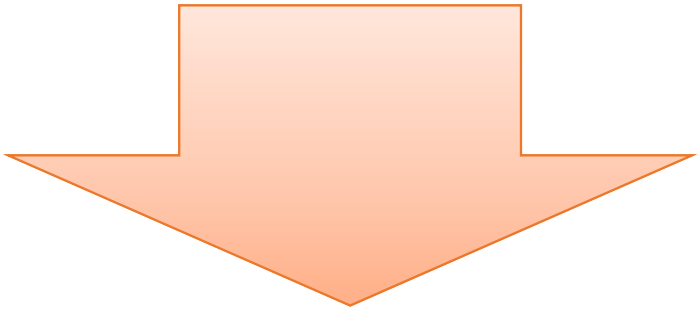
新しい技術・インフラ

新しいルール

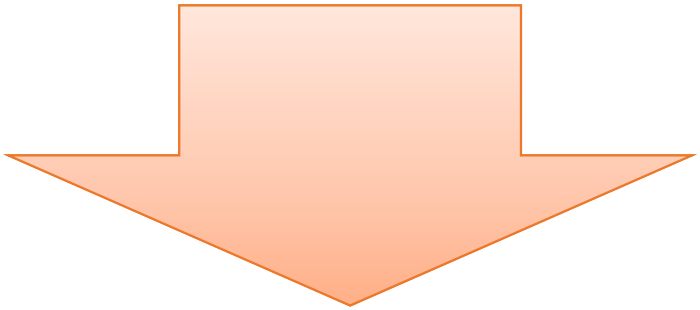
新しいツール

情報セキュリティへの影響

重大な変化が生じる



重大な変化が生じる



リスクアセスメントが必要

情報セキュリティへの影響

働き方改革から生じる

情報セキュリティ面への

重大な影響を踏まえた、

リスクアセスメントが必要

本テーマの目的

- 次章にて、「働き方改革から生じる情報セキュリティ上の変化」をまとめ、リスクと対応例を検討しました

- 皆さんの、リスクアセスメントの一助となれば幸いです

II.働き方改革実現に伴う環境変化

本章の内容

- 働き方改革に伴う変化により、情報セキュリティ面で起きていること
- 以下5つの視点での、チェックポイント

A.コミュニケーションツール

B.ビジネスツール

C.勤務場所の変化

D.デバイス類

E.オフィス環境

A.コミュニケーションツール

- スマートフォン（Android、iPhone）
  - 電話アプリ （LINE、Skype）
  - チャットサービス（Hangout 、Slack）

業務用電話が携帯電話からスマートフォンにかわることにより、管理すべき項目も変わっています。携帯電話では端末や契約の管理で済みましたが、スマートフォンの場合は、**パソコンと同じく各種アプリがインストール**されます。そのため、**アカウント**や**アプリケーションの管理**も必要になります。
正しく管理していますか？

スマートフォンにかわることにより、業務用端末で電話アプリやチャットサービスの利用が可能になりました。アプリ等の利用ルールは定められていますか？

業務に不要なアプリや不正なアプリのインストールや、
アプリのルール外利用をされないよう対策をしていますか？

コミュニケーションツールでのリスク例

スマートフォンに関連したリスク

情報システム部

パソコン

アカウント管理
ウイルス対策
物品管理
セキュリティ対策 etc.

総務部

携帯電話

スマートフォン

物品管理
契約管理

新しい管理項目

物品管理
契約管理
アカウント管理
セキュリティ対策 etc.

携帯電話は、日頃セキュリティと深い関わりのある情報システム部ではなく、総務部の管轄の場合があります。

携帯電話の際は**物品管理**と**契約管理**がメインであったため、**スマートフォンも同様の管理**をしている場合があります。

アカウントの使い回し、**全社同じパスワードの強制**、**個人アカウントの業務利用**、**セキュリティ対策の未実施**など、対策がとられていない場合があります。

B.ビジネスツール

- Office Suiteのクラウド化（G Suite、O365）
- ファイルサーバーのクラウド化（Google Drive、OneDrive）
- 自動化・RPA（WinActor、UI Path）
- 電子ホワイトボード

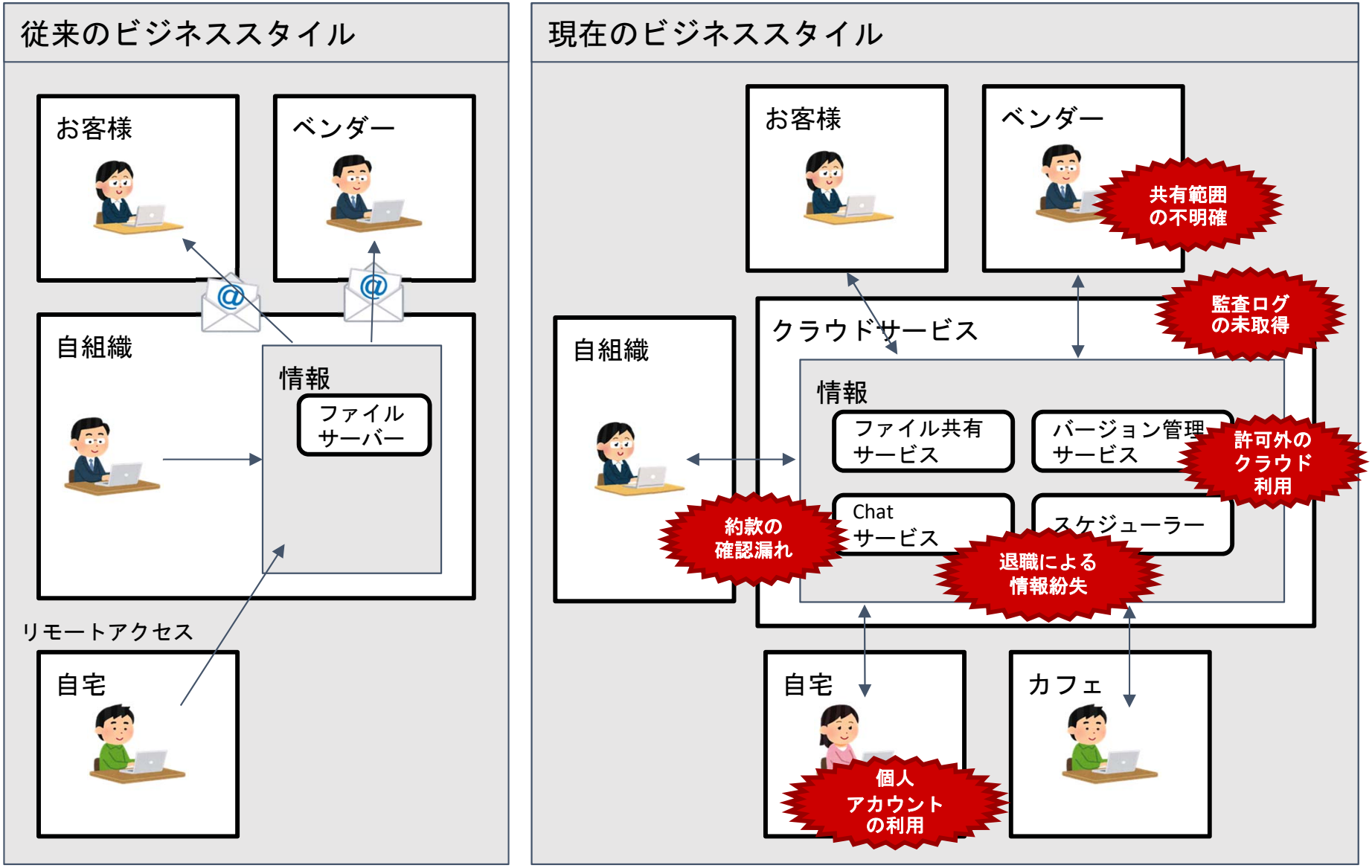
クラウドサービスの利用により、社内のサーバーにデータが保管されている状況から、クラウド上にデータが保存されるように変化しています。

社内サーバーでは明確な**バックアップ・世代管理など**がクラウドサービスでは不明確になる場合があります。
有事の際に必要な**監査ログ**が、クラウドサービスでは**追加機能**の場合があります。
責任の明確化や契約の確認など、クラウドサービスは適切に管理されていますか？

クラウドサービスは、社外の方にアクセス権を付与する事も可能です。
アクセス権付与ルールは明確ですか？

ビジネスツールでのリスク例

ビジネススタイルの変化



後ほどリスクアセスメントを実施

C.勤務場所の変化

- リモートデスクトップ（Xen desktop、Horizon）
- サテライトオフィス・シェアオフィス・レンタルオフィス

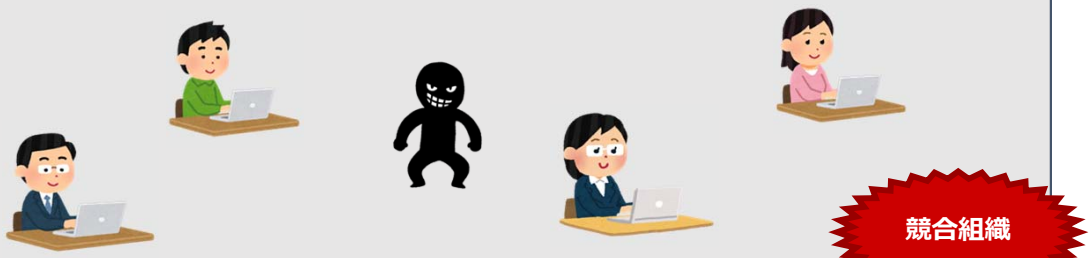
リモートワークで組織のサーバー等に接続する場合、リモートデスクトップは通常のクライアントコンピューターと利用出来るソフトウェアが異なる場合が有ります。（端末管理ソフト等）
通常のクライアントコンピューターと同等のセキュリティ対策が出来ない場合、リモートデスクトップに特化した対策やルールは定めていますか？
（端末ログ管理やウイルス感染時のルール等）

シェアオフィスでは異なる企業の方が近い場所で働いています。
覗き見や盗難による情報漏洩が発生しないよう、シェアオフィスを選ぶ際の基準として**個室や防音など**を**チェックしていますか？**
また、**シェアオフィスで取り扱える情報**は考慮されていますか？
パソコンなどの**のぞき込み**に留意するよう、**教育を実施**していますか？

勤務場所の変化でのリスク例

シェアオフィスに関連したリスク

シェアオフィス



自組織だけでは無い、複数の組織に所属する利用者がフリーアドレスで利用する。

シェアオフィスは、異なる組織の方が近い場所で働いています。
「組織が契約している」ため、「カフェなどのパブリックエリアより安全」という感覚で利用していませんか？

隣で働いている方は異なる**組織の方**です。
打ち合わせや電話の音声から**機密情報の流出**は発生していませんか？
ショルダーハッキングには十分注意を払っていますか？
利用者に対し、**安全に利用するための教育**を実施していますか？

D.デバイス類

- BYOD（私有端末の業務利用）
- MDM（端末管理アプリケーション）

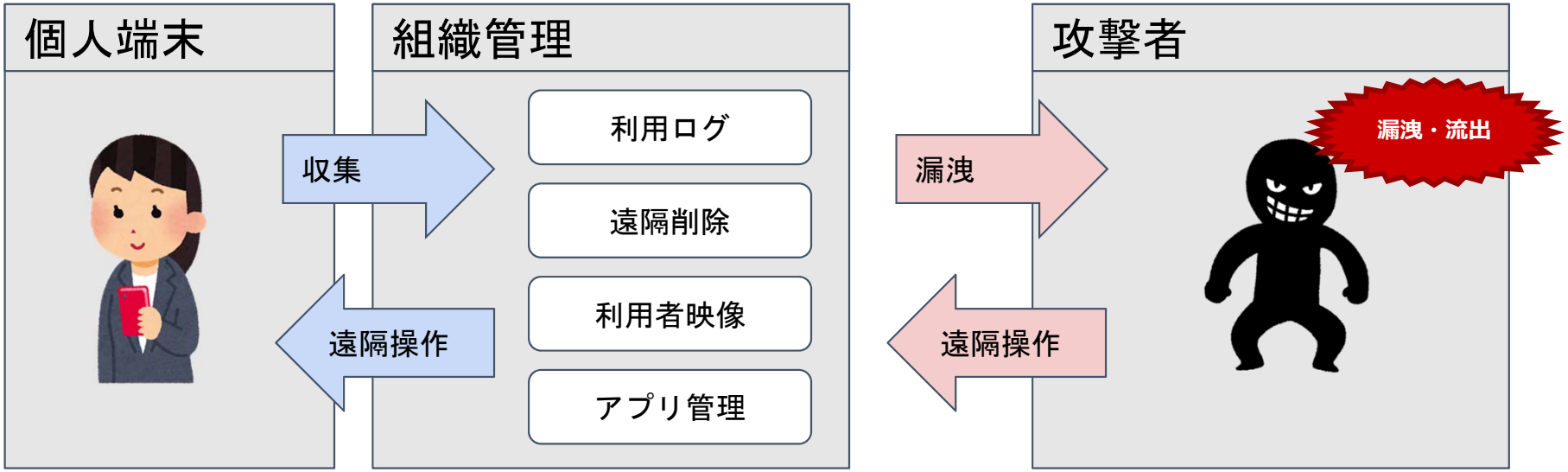
個人の私有端末を業務上で利用する場合が増えてきています。

利便性だけで利用すると、端末の管理や利用してよい業務範囲が不明確となります。
個人端末を利用する場合のルールを規定していますか？

MDM等管理ツールを利用する場合は、**収集情報**などを**利用者に明示し合意を得ていますか？**
収集情報は管理上必要最小限とし、**過剰に情報を収集することがないよう**設定していますか？
漏洩時に情報流出の被害が大きくなるリスクがあります。

デバイス類でのリスク例

MDMに関連したリスク



情報を収集する際は、**改正個人情報保護法**や**GDPR**への配慮が必要となります。

不要なログ収集は、**管理稼働の増加**や、**漏洩時の影響**を大きくします。
そのため、必要最小限のログ収集を選択することが望ましいです。

E.オフィス環境

- 公衆WiFi
- リモート会議

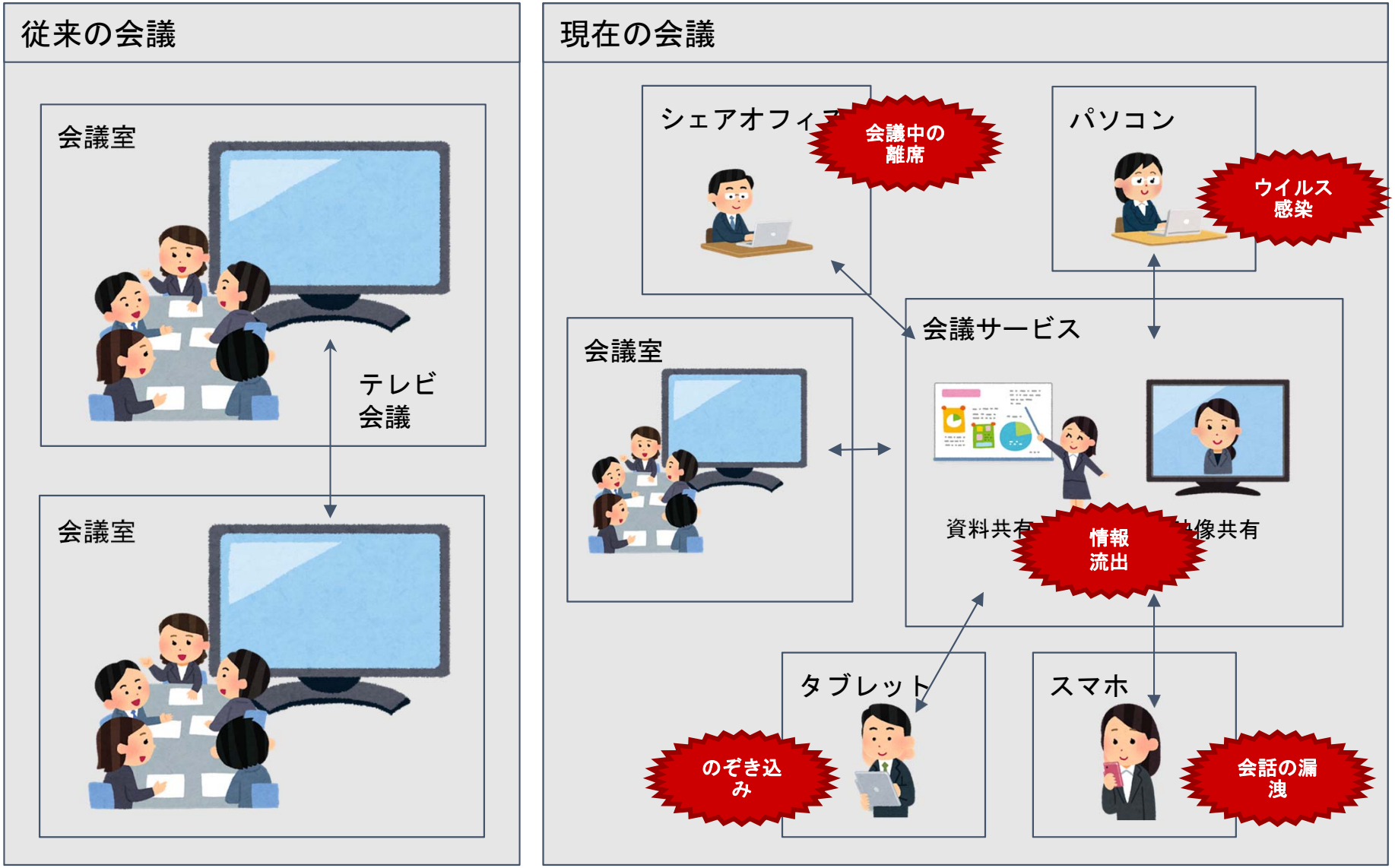
公衆WiFiが広く提供され、便利に利用できるようになっていますが、
現在の公衆WiFiは設置の規制がなく、管理者が不明のアクセスポイントも存在しています。
公衆WiFiを利用する際は、**提供者や管理者**を確認していますか？

通信の秘密等通信事業者に課せられている法的責任は、公衆Wi-fi設置者には適用されません
盗聴による情報の漏洩が発生しないように、**暗号化等の対策**を実施していますか？

公衆WiFi利用時には、**近くの端末と直接通信**できる場合があります。
通常の接続より、端末のセキュリティレベルが低下する場合がありますが、
接続する端末を適切に保護し、**ウイルス感染**のリスクを管理していますか？

オフィス環境でのリスク例

会議の変化

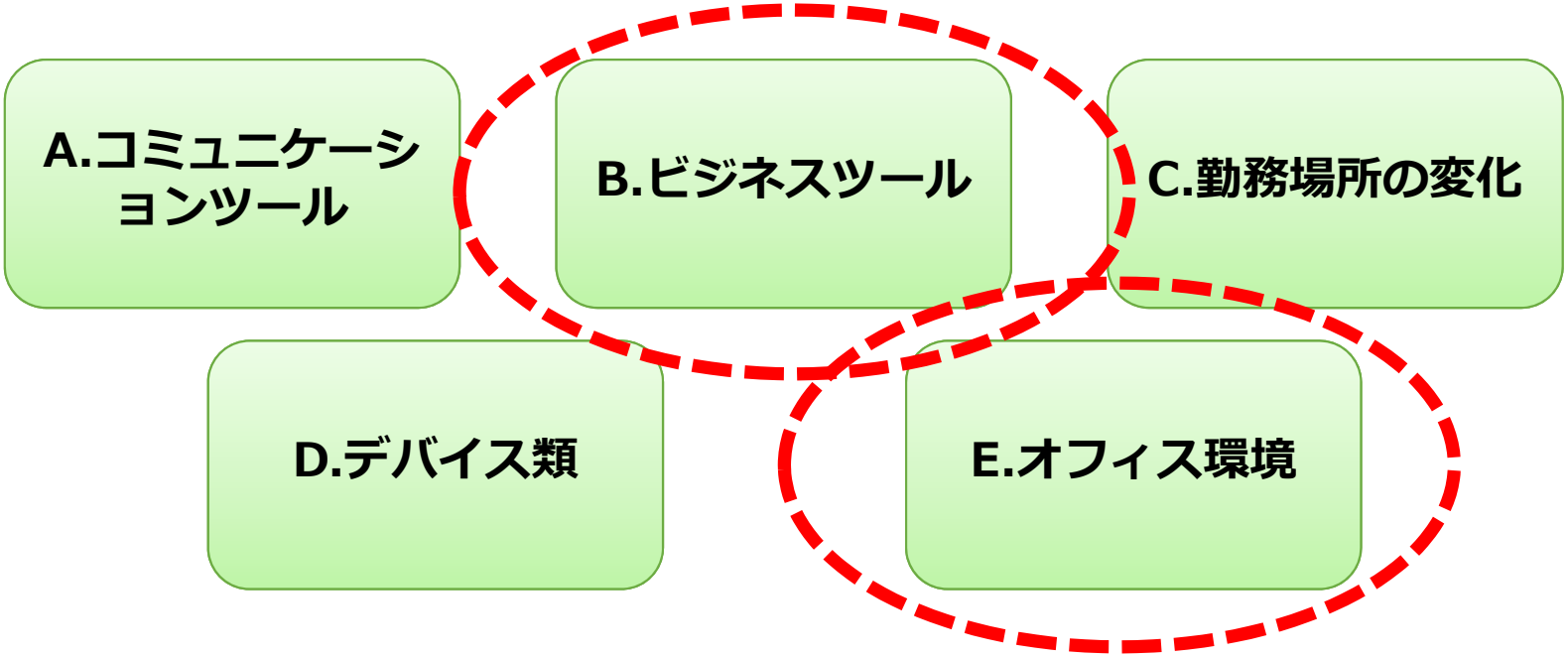


後ほどリスクアセスメントを実施

III. リスクの例示に基づく、ISO 27001管理策を活用した対応例

本章の内容

- 以下二点にて、ISO 27001管理策を活用した対応を例示します

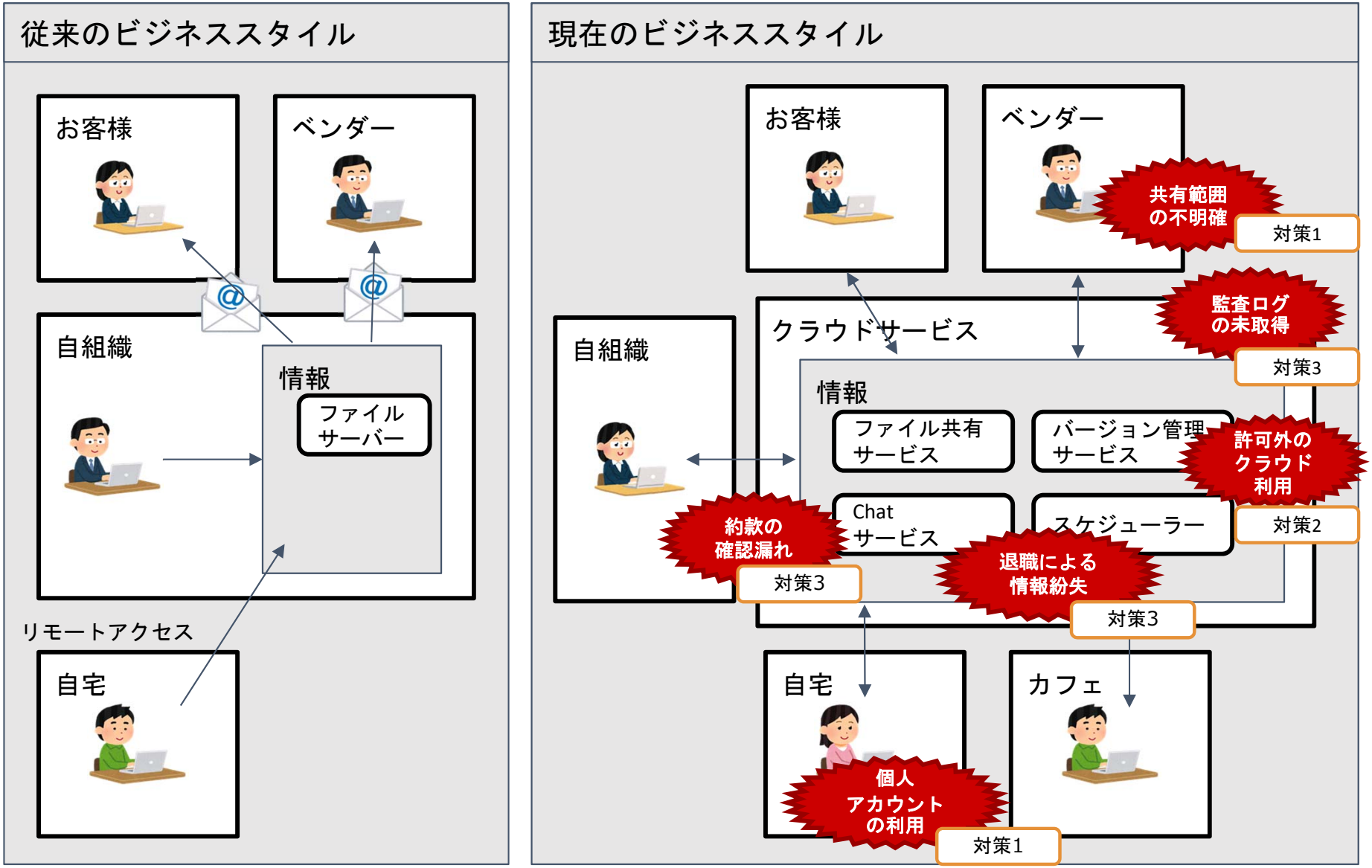


リスクの例示に基づく、
ISO 27001管理策を活用した対応例

B.ビジネスツール

ビジネスツールでのリスク例

ビジネススタイルの変化



ビジネスツールでの対策1：情報流通の明確化

同一のサービスを利用することにより、関係組織に意図せず情報が流通するリスク。

クラウドサービスの共有範囲は明確で、アクセス権は適切に管理されていますか？

- **他社と共有する場合、共有する情報、共有範囲、削除のプロセスは定まっていますか？**
- **アクセスする個人は特定されて、追加・削除のプロセスは適切に運用されていますか？**

管理策実践の例

- クラウドサービス向けの情報管理ルールを制定する。（A.8.1.3）
- 法人に属する個人としてアカウントを取得し、退職時にアカウントを削除する。（A.9.2.1）
- 自組織の対策だけで無く、関係組織のアクセス権管理も意識する。（A.15.1.3）

➢関連リスク

✓情報流出

✓不正アクセス

ビジネスツールでの対策2：クラウドサービス管理

安全性を確認できないクラウドの利用による情報流出のリスク

組織として利用可能なクラウドを選定し、安全性が確認できないクラウド利用を抑止していますか？

- **約款を確認し、合意出来ない事項がないか確認をしていますか？**
- **許可外のクラウドはアクセスが制限されていますか？**
- **Office Suite製品の場合、機能ごとのアクセス制限が適用されていますか？**

管理策実践の例

- CASB (Cloud Access Security Broker) 製品を導入し、クラウドアクセスコントロールを実施。（A.9.2.2）
- 利用者からの要請を受けて、機能やリスクを評価し社内導入する仕組みを構築する。（A.12.6.2）

➢関連リスク

✓野良クラウド（Rogue cloud）の利用

✓情報流出

ビジネスツールでの対策3：サービスの堅牢化

有事の際の証拠紛失や、社員等の退職によるデータの紛失が発生するリスク。

利用するサービスは堅牢ですか？

- **有事に備えて、必要な監査ログや情報の保全を図っていますか？**
- **社員の退職とともに、情報資産にアクセス不可能とならない対策がとられていますか？**

管理策実践の例

- 監査に必要なログを取得出来るよう、オプションサービスを申し込む。（A.14.4.2）
- サービスの特性（個人・組織）を理解し、組織として必要な情報を混在利用しない。（A.8.2.3）

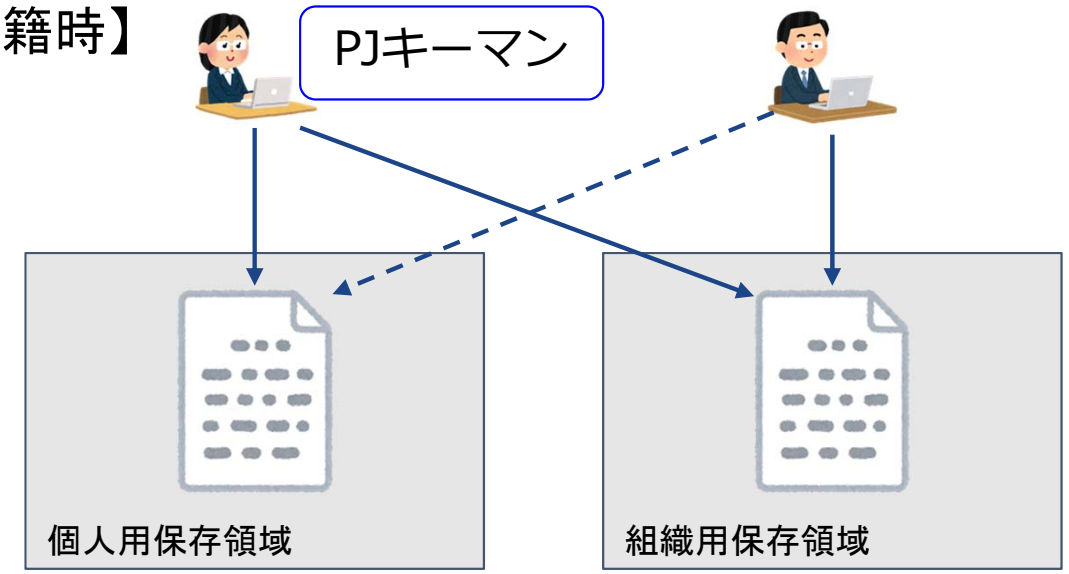
➢関連リスク

✓証拠の紛失

✓情報の紛失

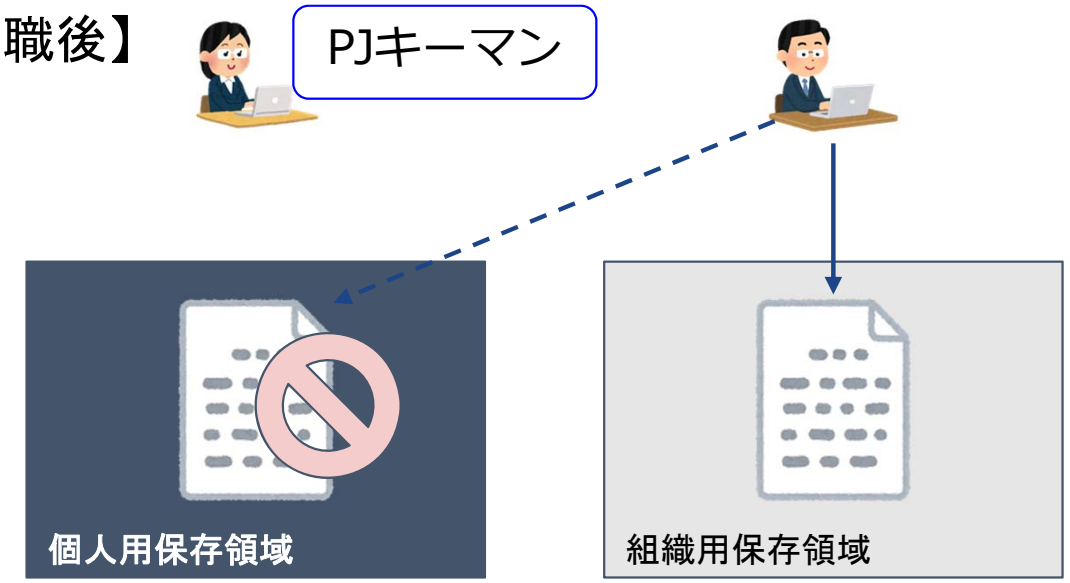
補足：クラウド上のデータ保存に関する注意

【在籍時】



個人用保存領域に置かれたファイルであっても、**アクセス権**を付与すれば**問題なく利用**できる。
そのため、保存場所を意識せずに利用している場合がある。
問題に気がつかない。

【退職後】



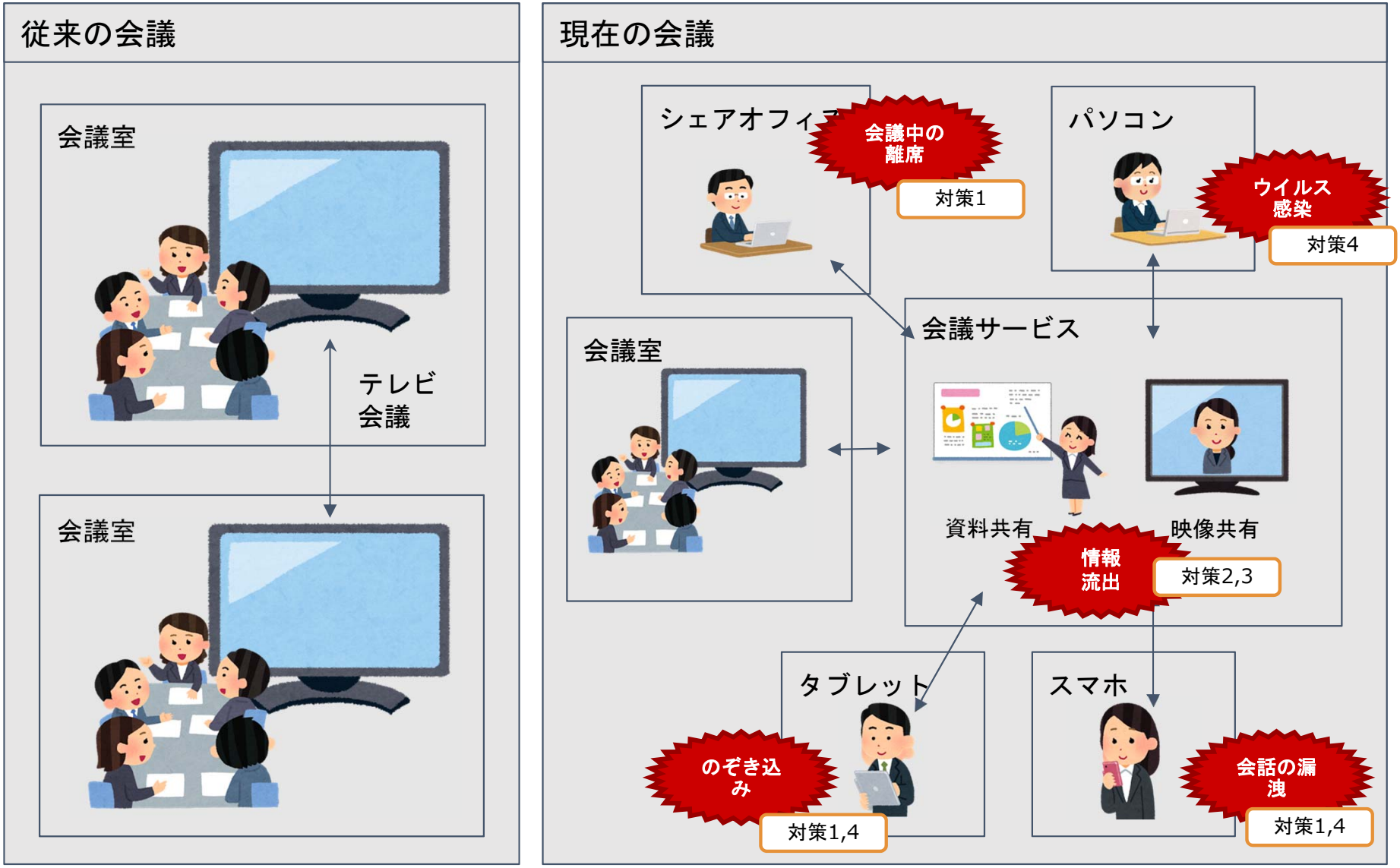
個人用の領域のため、退職の**アカウント削除**により、個人用保存領域の**ファイルがアクセスできなくなる。**
重要な資料を個人領域で作成した場合には、**情報紛失のリスク**となる。

リスクの例示に基づく、
ISO 27001管理策を活用した対応例

E.オフィス環境

オフィス環境でのリスク例

会議の変化



オフィス環境での対策1:会議中の情報漏洩対策

どこからでも参加できることから、
安全でない環境で会議に参加してしまうリスク。

リモート会議に参加してよい環境を規定していますか？

- 公衆環境（カフェ、公園、駅、etc）から参加していませんか？
- のぞき見はされませんか？　話声は他の人の耳に入っていませんか？

管理策実践の例

- リモート会議に参加して良い環境を規定する。（A.11.1.1）
- 利用者教育を行い、のぞき見や盗聴など無いように周囲に注意を払うことが出来るようにする。（A.7.2.2）
- 会議中の端末は常に管理下に置く。（A.11.2.1）

➢関連リスク

✓のぞき込み・盗聴

✓盗難

オフィス環境での対策2:クラウドサービスの管理

クラウドサービスの約款内容やサービス設定の不備により、
意図せず情報漏洩が発生するリスク。

利用するクラウドサービスは適切ですか？

- **会議資料の安全は約款で担保されていますか？**
- **利用者・サービス間の責任分解は明確ですか？**
- **外部認証を取得し、継続的なセキュリティ対策がなされていることを確認していますか？**

管理策実践の例

- サービスの検討は、セキュリティも考慮する。（A.15.2.1）
- アップロードした資料の所有権を確認する。（A.15.1.2）
- 外部認証の取得を確認する。（A.15.1.3、ISO 27017）

➢関連リスク

✓サービス提供者への情報漏洩

補足：データ流通の注意

リモート会議のサービスであっても、**様々な機能**が提供されています。

メリット、デメリットを**検討**し、機能を検討した上で利用する機能を選択することが重要となります。

例
ファイル共有は、隠れたシートや文字列による情報流出のリスクがあるため、画面共有のみ許可する。

遠隔操作機能は、ほか端末を操作する事が無いため利用しない。

オフィス環境での対策3:サービス内容の適正化

サービスの設定をデフォルトのまま利用することにより、必要な管理策がとられないまま利用するリスク。

サービスの設定は、自組織のポリシーに合わせて最適化されていますか？

- **サービスは、目的を達成するために正しく設定されていますか？**
- **オプションサービスの必要性について検討を実施していますか？**

管理策実践の例

- 設定を適切に行い、企業の許可しない利用を抑制する。（A.14.2.3）
- 参加ログの保存を確実にして、証拠の保全をはかる。（A.12.4.1）
- 会議の参加者を管理し、不正アクセスを防止する。（A.9.1.2）

➢関連リスク

✓第三者からの不正アクセス

オフィス環境での対策4:接続元端末の管理

端末の管理不十分により、
端末を介した情報漏洩が発生するリスク。

リモート会議に接続を許可する端末は管理がされていますか？

- ウイルス感染による漏洩リスク。
- 共有端末からのアクセスにより認証情報が漏洩するリスク。

管理策実践の例

- ウイルス対策を実施し、感染を防止する。（A.12.2.1）
- リモート会議に利用する端末を規定し、許可外の端末からの利用を禁止する。（A.9.4.1）
- 高度なセキュリティ（多要素認証etc）により、不正アクセスを防止する。（A.9.1.2）

➢関連リスク

✓ウイルス感染

✓共有端末の正しくない利用

IV.まとめ

働き方改革と情報セキュリティリスク

「労働人口減少への対策」→働き方改革

ITを活用して対応(改革)

重大な変化が生じる

重大な変化

以下をサンプルとし、変化とリスクを例示しました

- A.コミュニケーションツール
- B.ビジネスツール
- C.勤務場所の変化
- D.デバイス類
- E.オフィス環境

重大な変化

と、言えば！

変化とISMS

重大な変化

リスクアセスメント

8.運用
8.2 情報セキュリティリスクアセスメント

組織は，あらかじめ定めた間隔で，又は重大な変更が提案されたか若しくは重大な変化が生じた場合に，6.1.2 a)で確立した基準を考慮して，情報セキュリティリスクアセスメントを実施しなければならない。

マネジメントレビュー

9.3 マネジメントレビュー

マネジメントレビューは，次の事項を考慮しなければならない。
b) ISMS に関連する外部及び内部の課題の変化

変化とISMS

B.ビジネスツール

リスクアセスメント

27001管理策にて対応可能

E.オフィス環境

働き方改革から生じる情報セキュリティ上の変化への、ISMSの活用による対応例を紹介いたしました。
皆さんの活動の一助となれば、幸いです。

ご清聴ありがとうございました