大阪市阿倍野区薬剤師会　様

支部合同研修会
保険薬局の情報セキュリティ対策について

令和7年2月1日

情報セキュリティシニアコンサルタント　中島 明彦

アジェンダ

1. 大阪急性期総合医療センターでのサイバー攻撃を受けた原因とその後の対応
2. 情報セキュリティの基礎知識
3. 調剤薬局における基本的な業務フローチャート
4. 調剤薬局で考えられる情報セキュリティリスク

Part 1

大阪急性期総合医療センターでの
サイバー攻撃を受けた原因とその後の対応

1-1. 大阪急性期･総合医療センターのシステム障害

同一手口のサイバー攻撃

CLICK!

約45秒の動画です

【大阪急性期･総合医療センター】
サイバー攻撃で診療ほとんど停止
“身代金”要求届く
（2022年10月31日）

17,000 回視聴

CLICK!

約90秒の動画です

「字が汚い医者多く紙カルテ苦労」
「輸血管理システム動かず」
病院サイバー攻撃１か月
（2022年12月1日）

5,867 回視聴

CLICK!

約５分間の動画です

サイバー攻撃から１か月
“機能停止”した病院のいま

（2022年12月1日）

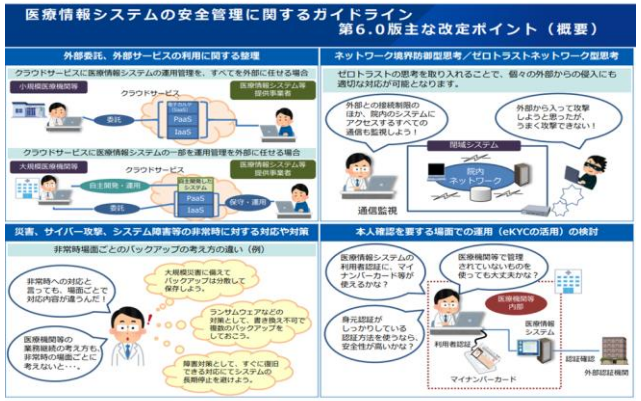
22,000 回視聴

1-2. タイムライン

時系列	出来事
2022年10月31日 6時頃	**ベルキッチンの一部端末でシステム障害が発生。**
同日　6時38分	大阪急性期・総合医療センターの**電子カルテシステムで障害発生。**
同日　7時20分頃	生長会が**ランサムウエア感染の可能性を確認**し、委託元病院のサテライト職員に対して**ネットワークを遮断を指示。**
同日　7時過ぎ	システム障害の発生を**同センター職員が把握。**
同日　8時頃	同センターの**ヘルプデスク事業者よりシステム事業者に連絡。**
同日　8時半頃	システム事業者が**同センターに到着し調査を開始。**
同日　9時頃	生長会、大阪急性期・医療センターが**ランサムウエア感染を確認し電子カルテシステムなどを停止。**
同日　9時	同センターが**外来診療等の通常の診療サービスを一時的に停止**すると案内。
同日　11時半過ぎ	同センターから**大阪府警へ被害相談のために通報。**
同日　18時頃	生長会がFortiGateのバージョンアップを実行。**これに起因するとみられるログの消失が発生。**
同日　20時頃	同センターがシステム障害発生を受けて**記者会見を開催。**
同日　21時頃	11月1日の同センターでの**診療を休診とすることを公表。**
2022年11月1日	同センターが**当面の間、診療を休診とすることを公表。**
2022年11月7日	**生長会がランサムウエアによるシステム障害の発生を公表。**
同日	同センターが生長会の**給食提供サービスのサーバーから侵入された可能性があると記者会見で公表。**

1-2. タイムライン

時系列	出来事
2022年11月10日	検査予約等を除いた**三次救急患者受け入れ、小児救急診療の一部（診察、処方箋発行、予約取得）を再開**。
2022年11月17日	**一般救急患者の受け入れを再開**。
2022年12月12日	**電子カルテを含む基幹システムが再稼働**。
2022年12月22日	呼吸器内科、血液・腫瘍内科を除く34の診療科で外来初診患者の受付を再開。**紙カルテでの暫定運用を終了**。
2023年　1月　4日	**全ての診療科での受付を再開**。
2023年　1月11日	画像診断、生理検査等の通常診療に係る**部門システムの復旧が完了。通常診療体制に復旧。**
2023年　1月25日	外部の有識者による**調査委員会第1回会合開催**。
2023年　3月28日	**情報セキュリティインシデント調査委員会の調査報告書を公開**。



医療情報システム
ガイドライン　6.0

CLICK!

1-3. 障害影響で通常診療が一時停止

◆ システム障害が発生したのは、大阪府立病院機構 大阪急性期・総合医療センター。
大阪市の総合病院で診療科36、病床数865床。**高度救命救急センター、地域がん診療連携拠点病院にも指定**されている。

◆ ランサムウエアによる実被害及び被害拡大防止措置による影響を受け、2022年10月31日20時時点で、電子カルテシステム及び関連するネットワークが完全に停止中。そのため、**同センター内で電子カルテが閲覧できない状況**となった。

◆ 障害の影響を受け、緊急的対応を要するものを除いた、**外来診療、予定手術、新規救急受入の一時的な停止を行っている。**
システム障害発生以後は、暫定的に紙カルテで対応。また手術延期に伴い一旦退院や転院となる患者もいる。診療受付に関する最新の情報は同センターのWebサイトに掲載。なお、**診療報酬の計算、薬の処方もできない状態**となっている。復旧時期は基幹システムが12月中旬、全体復旧は、2023年1月の見通しを示した。

◆ 近隣病院への支援依頼について、個別症例での対応を行った事実は確認していないが、災害、救急対応は調整が済んでいる。

◆ 今回のシステム障害により入院予定の患者や外来診療など、11月7日までに延べ約2670人に影響が出た。また予定手術の内77件が中止となった。
なお、**関連した情報流出の事実は確認していない。**また患者の健康状態への影響に関わる問題も発生していない（10月31日の記者会見時点）。

◆ **災害拠点病院ではBCPの準備が義務付けられているが・・・**
①紙カルテの長期運用は想定しておらず、
②訓練として毎年行っていた状況と全く異なっている、
③基本情報を記した紙カルテを準備しておくべきだったと災害対策室長もコメント。

1-4. ランサムウエアによる関連システムへの被害状況

障害後のシステム機器関連被害

場所	被害機器	復旧状況
大阪急性期・総合医療センター	感染が確認された**サーバーは31台** ※院内全体では約100台が稼働	・2022年12月11日時点で端末の復旧は200台余り（１割程度）に限られ紙カルテでの運用を継続。 ・2022年12月22日以降は端末の復旧が進み紙カルテの運用を終了。 ・システム復旧にあたっては、全てのサーバー、端末の初期化及び再インストールを実行。
	不審な通信の形跡が確認された**端末は約1,300台** ※院内端末の半数相当	
生長会	ベルキッチンサーバーは**3台**	
	NAS（NW-HDD）は**3台**	

障害後の診療サービスへの影響

日付		診療サービスへの影響
2022年10月31日～11月3日	2か月11日	緊急を除く通常診療は原則停止。
2022年11月4日以降		通常診療の内、予定手術は一部再開。
2022年12月22日以降		呼吸器内科、血液・腫瘍内科を除く34の診療科で外来初診患者の受付を再開。
2023年1月4日以降		全ての診療科での受付を再開。
2023年1月11日		通常診療に係るシステムが復旧。通常の受付手続を再開。

1-5. ランサムウエア「Phobos」とみられる攻撃

① 専門家チームによれば攻撃に用いられたランサムウエアはPhobosの亜種「Elbie」（拡張子が全てelbieだった）とみられ、**当時サーバー上の画面に英文の脅迫メッセージが表示されていた。**

② 脅迫メッセージの概ねの内容として、「**全てのファイルを暗号化しました。復号したければメールを送ってください。24時間以内に返信がない場合はこのメールアドレス宛に送ってください。復号にはビットコインを支払ってください。金額はあなたがメールを我々にいかに早く送るかによって変わります。支払い後にすべてのファイルを復元するツールを送ります。**」とするもの。なお、**被害に遭ったのはサーバーでPCではランサムウエアは確認されていない。**

③ 同センターは、**脅迫メッセージに記載された連絡は行っておらず、今後も含め交渉に応じない方針。対応については、厚生労働省などとも協議**する予定。

④ 事前に講じていた対策について、同センターは**徳島県の事例を受け、通信機器のファームウェアやウイルス対策ソフト本体の更新（直近では2022年8月頃に実施）などセキュリティ対策を講じていた。**

⑤ **バックアップは週に１回フルバックアップを取得しており、差分バックアップを日次で取得**。保存先はストレージ （HDD）及びテープ形式でも取得しているが、保全状況やバックアップ先との接続箇所について、安全性を含め状況を確認中。

LOCKBITが最も活発なグループとして君臨し、ダークホースのPhobosと8Baseが第2位に（2024年5月23日にデータと考察を追加・更新）

トレンドマイクロが確認した脅威件数のデータによるとランサムウェアグループは、2024年比較的ゆっくりとしたスタートを切り、第1四半期の時点でメール、URL、ファイルの各レイヤーで検出してブロックした**ランサムウェア脅威数は2,661,519件**でした。**2023年上半期の670万件**の半分以下となっています。

1-6. 給食提供サービスのサーバーから侵入された可能性

① 厚労省派遣専門家チームの調査結果より同センターの委託先（給食提供サービス：ベルキッチン）事業者である**生長会データセンター内サーバー経由で侵入された可能性が判明。又、同センターにはアジアを通信元とする不審なアクセスの大量発生が通信ログより確認された。**なお、生長会は同日公表した障害報告で関連については調査中だとする見解を示している。

② 同センターの電子カルテのオーダリングシステムで疾患や食事内容など食事情報に関係する発注が行われ、**院内の給食関係のシステムに情報が集約されベルキッチン宛に送信される仕組み**であった。サーバー間はベルキッチン側仕様で**RDP接続が常時**行われていた。

③ **攻撃はVPN機器に対して行われ機器はデータセンターのリモートメンテナンス用に使用**。同センターは**徳島県つるぎ町立半田病院と同一機器と公表（FortiGate）**。更に**この機器は当時5.4.8のバージョンが使用されていたことからソフトウエアの更新も行われていない状態**であり脆弱性が悪用され加えて**2021年に流出していたFortiGateの認証情報のリストに含まれていたことも判明。**

④ **侵入以後は、ウイルス対策機能などが無効化された形跡が確認**されている。

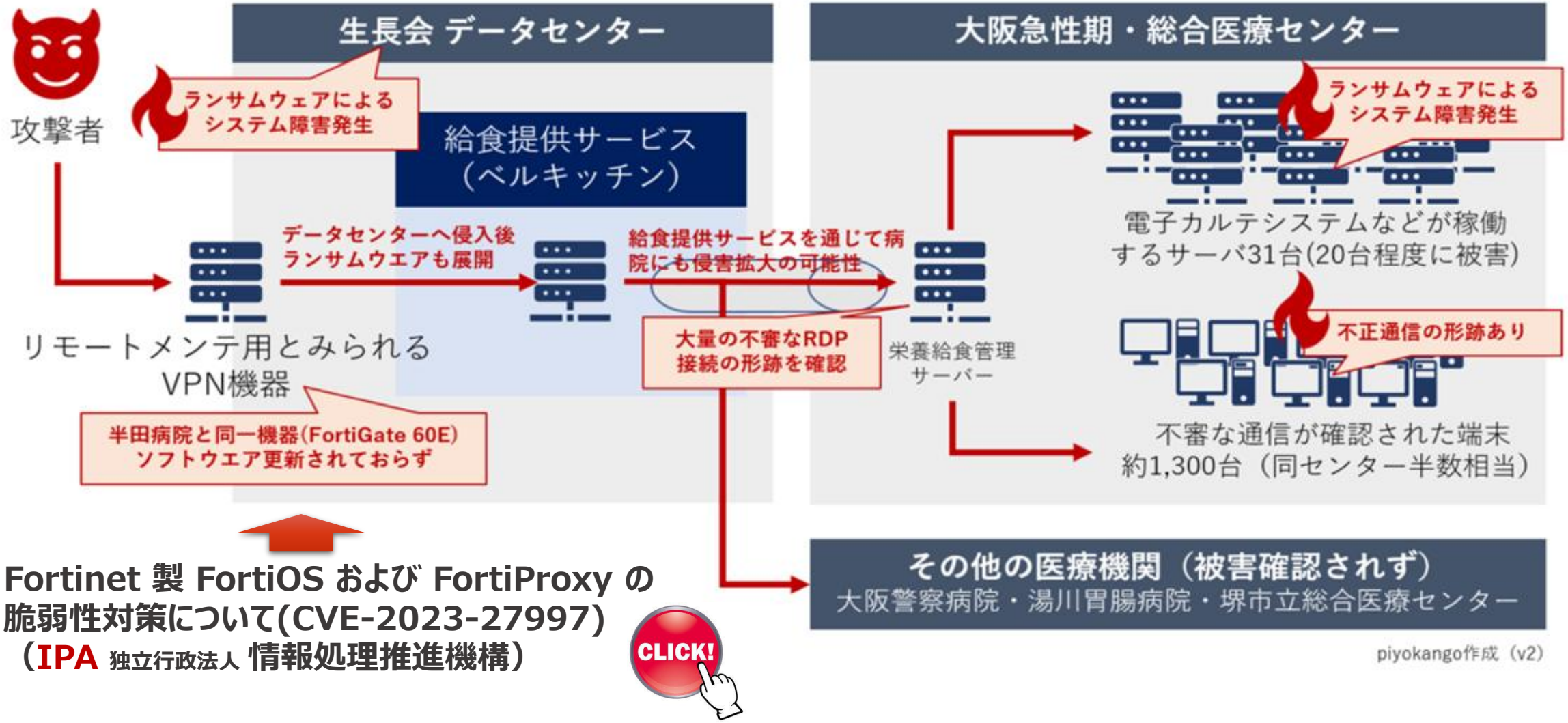
⑤ 当該サービスは生長会の４病院とそれ以外の４病院で利用していたが、**電子カルテシステムに影響が及んだのは大阪急性期・総合医療センターのみ。**外部の病院である大阪警察病院、湯川胃腸病院、堺市立総合医療センターは**いずれも診療サービスに影響は及んでいない。**湯川胃腸病院のみ、発生日当日給食が予定通りの時間よりも２時間ほど遅れて届いた。

RDP（ Remote Desktop Protocol ）の脆弱性

RDPから不正侵入を許した場合、接続先のコンピューターの管理者アカウントが乗っ取られる可能性もある。**又、RDPで遠隔操作されてしまうと、勝手にマルウェアがインストールされたり、ほかのコンピューターに対する攻撃を仕掛ける踏み台にされたり、といった被害が考えられる。**

1-7. 給食提供サービスのサーバーから侵入経路予想

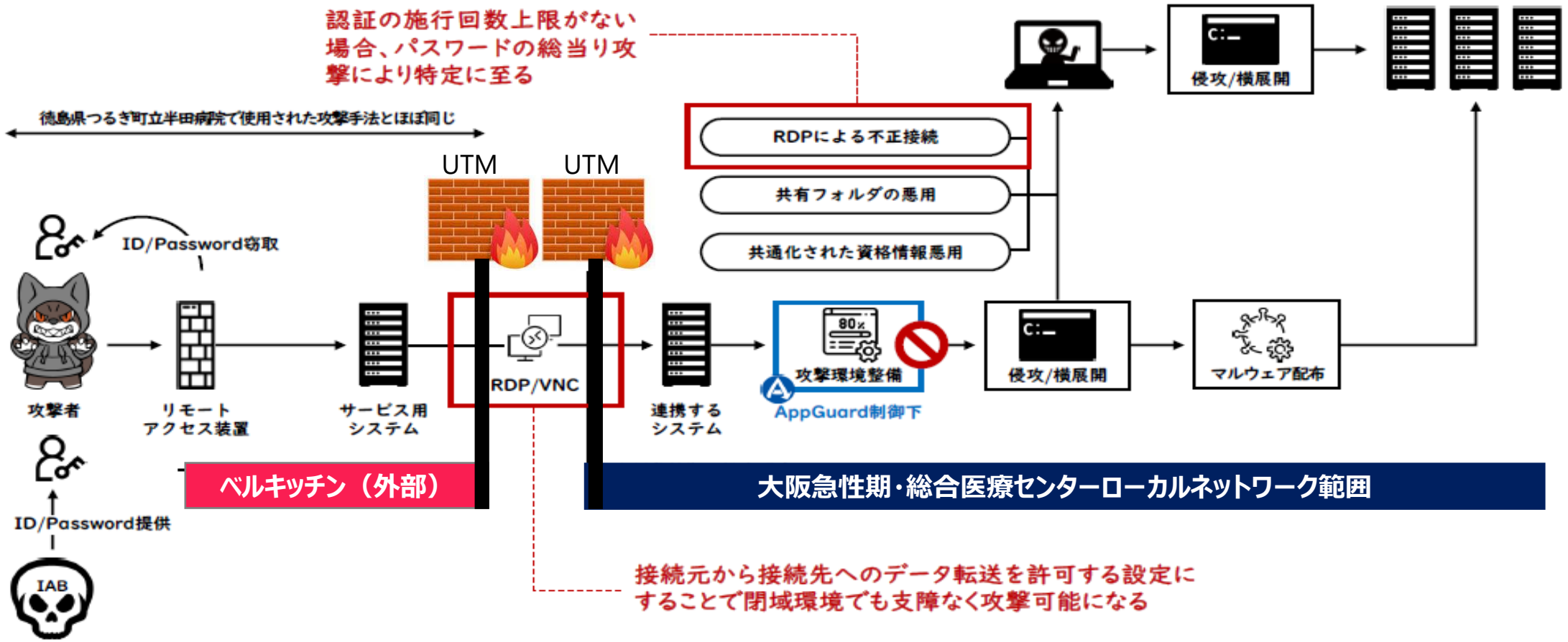
出典：piyokango作成(v2)



Fortinet 製 FortiOS および FortiProxy の脆弱性対策について(CVE-2023-27997)（IPA 独立行政法人 情報処理推進機構）

CLICK!

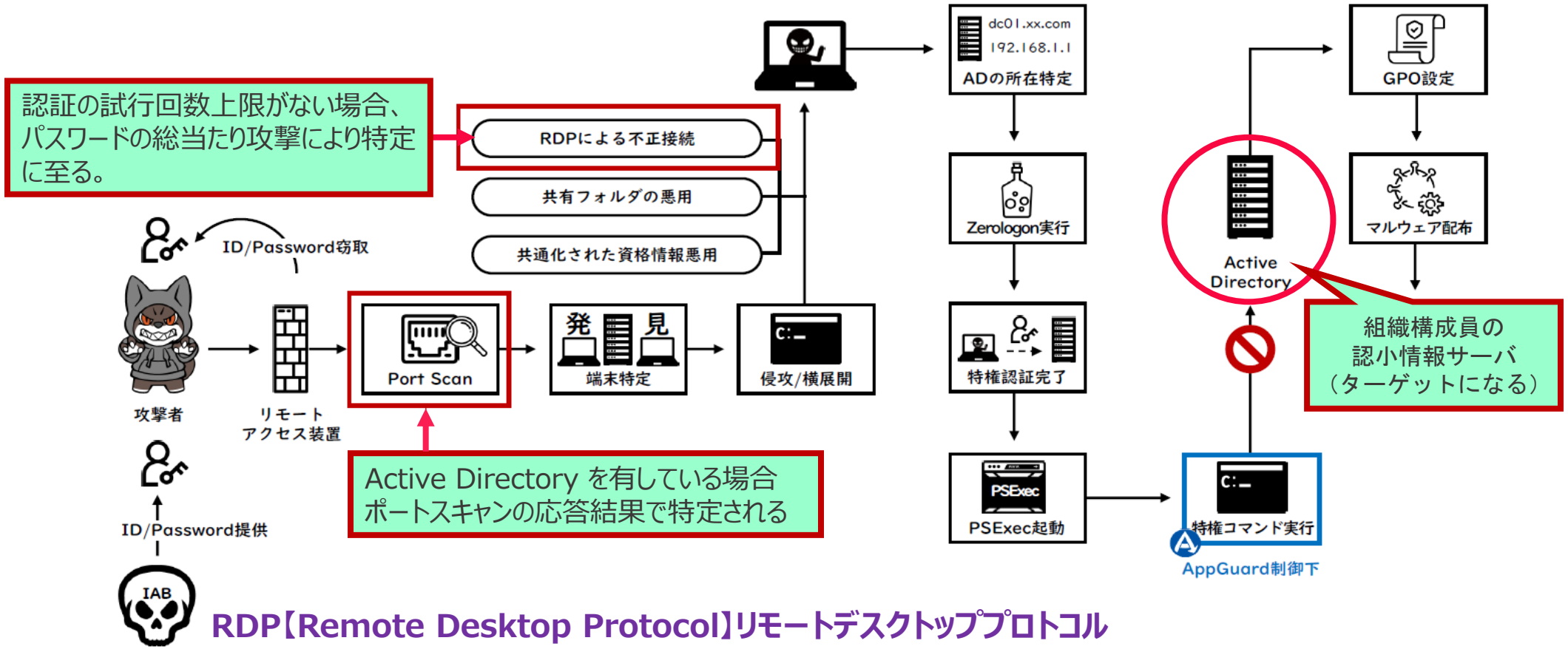
1-8. 大阪急性期･総合医療センターへの侵入手口分析　出典：Blue Planet-works



【原因】 **情報システムリモートメンテ用VPN機器のファームウェア等の更新が行われていなった。**通常購入後のバンドル期間が１年であるがバンドル期間経過後の継続手続きをしないケースが多い。**UTM保守サポート料金が高額で１年当りの金額が機器代金の20%相当であり二の足を踏む。**

1-9. 徳島県つるぎ町立半田病院への侵入手口分析

出典：Blue Planet-works



RDP【Remote Desktop Protocol】リモートデスクトッププロトコル

RDPとはサーバコンピュータの画面をネットワークを通じて別のコンピュータ（クライアント）に転送して表示・操作するリモートデスクトップ或いは仮想デスクトップでサーバとクライアントの通信に用いられる通信プロトコルの一つ。Microsoft社の開発。Windowsのリモートデスクトップなどで利用されている。

1-10. 情報セキュリティインシデント発生後の報道（BCP計画不具合）

「字が汚い医者多く紙カルテ苦労」「輸血管理システム動かず」病院サイバー攻撃１か月（2022年12月1日）

YouTube | MBS NEWS | 5732 回の視聴 | 2022年12月1日

紙カルテに苦労

↓

BCP計画に具体的手順がなし

#サイバー攻撃 #大阪急性期・総合医療センター で#電子カルテ のサーバーを管理する#ＩＤ と#パス 使い回し…

TikTok | ytvnews | 1万 回の視聴 | 2023年3月28日

ID＆PWの使いまわし

↓

情報セキュリティ手順書なし

1-11. 情報セキュリティインシデント発生後の災害防止対策？

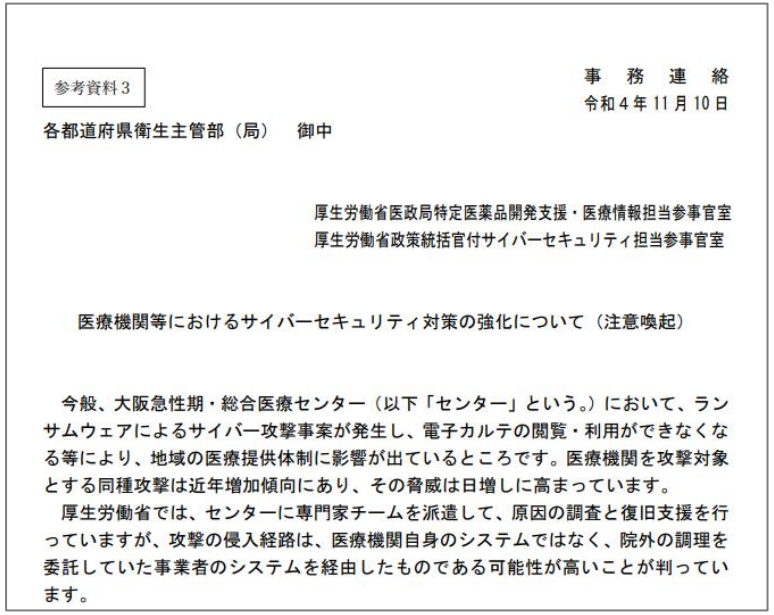
１．病院内における再発防止策等検討の調査委員会立ち上げ

外部の有識者を含めた調査委員会を2023年1月下旬に設置し、**3月末迄に原因や再発防止策を含む報告書の取り纏め予定**。

２．政府の動き

① 厚生労働省の**医療機関に対する初動対応支援**を行うため、ソフトウェア協会の専門家3名を現場に派遣し、感染原因の特定や対応の指示などを行っている。

②厚生労働省より、**全国の医療機関に対してサイバーセキュリティ対策の強化を求める注意喚起**を行った。



参考資料３

事　務　連　絡
令和４年 11 月 10 日

各都道府県衛生主管部（局）　御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）

今般、大阪急性期・総合医療センター（以下「センター」という。）において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出ているところです。医療機関を攻撃対象とする同種攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。

厚生労働省では、センターに専門家チームを派遣して、原因の調査と復旧支援を行っていますが、攻撃の侵入経路は、医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判っています。

① **サプライチェーンリスク全体の確認**
② **リスク低減のための措置**
③ **インシデントの早期検知**
④ **インシデント発生時の適切な対処・回復**
⑤ **金銭の支払いに対する対応**
⑥ **ランサムウェア特設ページの掲載**

https://www.nisc.go.jp/tokusetsu/stopransomware/index.html

Part 2

情報セキュリティの基礎知識

2-1. 情報セキュリティとは

事業の情報システムを取り巻くさまざまな脅威から情報資産を機密性・完全性・可用性（3要素）の確保を行いつつ、正常に維持することです。

1. **小規模事業者にも情報セキュリティが必要な理由**
   サイバー攻撃の増加、情報漏えいによる損害、顧客からの信頼失墜、法規制対応等

2. **小規模事業者が狙われる理由**
   相対的にセキュリティ対策が弱い、重要な情報への理解不足、攻撃の成功率が高い等

3. **小規模事業者が実施すべき簡単なセキュリティ対策**
   パスワード管理を徹底する、セキュリティソフトを導入する、従業員への教育を実施する、定期的なセキュリティ診断を行う等

2-2. 情報セキュリティの定義

1．情報セキュリティの定義

情報セキュリティとは、情報資産の機密性、完全性及び可用性を維持することをいう。

① 機密性	**情報にアクセスすることを認められた者だけ**が、情報にアクセスできる状態を確保することをいう。
② 完全性	**情報が破壊、改ざん、又は消去されていない状態**を、確保することをいう。
③ 可用性	**情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態**を確保することをいう。

2-3. 情報資産の定義

１．情報資産の定義

省庁の情報セキュリティガイドラインが対象とする**情報資産（Information Asset）はそれぞれの組織が収集した「ヒト・モノ・カネ」に関する情報の全てを指します。**

情報は、紙の資料や電子データ（USBメモリカード、CD-ROM、ボイスレコーダー、データベース、サーバーに保管されている電子データ）及び映像データ等多岐に渡ります。
又、事業等で蓄積された**経営や事業活動に関するノウハウも情報資産**と見なされます。

一方で、**重要でない情報**は、インターネット等を利用して見ることのできる、ホームページ、LINE、X（旧Twitter）等を通じて、**一般（世界中の人々）向けに公開**されている情報で、誰でも入手可能なものを指します。

情報とは、特定の事象や事実、知識、データなどについての知見や内容を指します。
これは、数値、文章、画像、音声などの形で表現されることがあります。情報は、私たちが世界を理解し意思決定を行うための重要な要素です。

2-4. 情報資産の分類

１．情報資産の分類

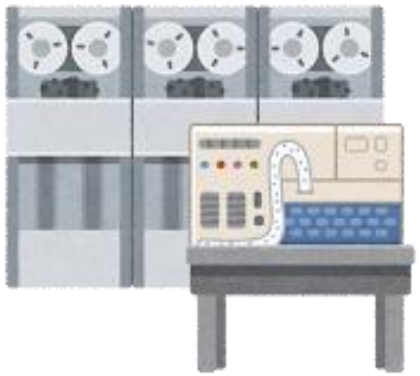
JISQ27002情報による資産の分類と対象となる情報資産の例は以下の通りです。

情報資産分類	対象の情報資産（例）
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資材、運用手順又はサポート手順、事業継続計画（BCP計画）、代替手段の取り決め、監査証跡、保存情報
ソフトウエア資産	業務用ソフトウェア、システムソフトウェア、開発用ツール、ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取り外し可能な媒体、その他の装置
サービス	計算処理、通信サービス、一般ユーティリティ（暖房、証明、電源等）
人、資格等	人、保有する資格・技能・経験
無形資産	組織の評判、イメージ

2-5. 情報資産の洗い出し

１．情報資産が「どこにあり」、「誰が管理し」、「どのような状況で扱われているか」

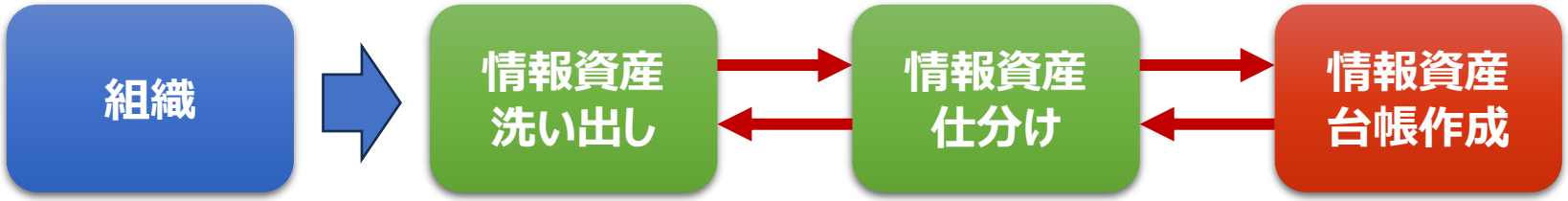
- 情報セキュリティを確保するには、保護すべき情報資産を明確にする必要がある。
- 保有する重要な業務情報は、財務／人事／顧客／戦略／技術情報などがる。
- 情報を処理するコンピュータ、ソフトウェア、記録媒体も情報資産である。
- 紙媒体、会話、物理的な施設・設備、さらには、人や組織イメージも含まれる。



2-5. 情報資産の洗い出し

2． 記録形態（紙、電子化、人の記憶、製品サンプルに実装）による情報資産の分類

- 情報資産は膨大→個々の情報ごとに洗い出すのでは無く、情報をグループ化
- 自組織の機密情報と他から預かった機密情報に分類
- 個人情報、営業機密のような重要な情報のタイプに分類
- 資産価値や属性（用途、保管場所、保存期間など）で分類
- 用途が同じパソコンやサーバをまとめてグループ化
- 情報のライフサイクルが同じものをグループ化



2-5. 情報資産の洗い出し

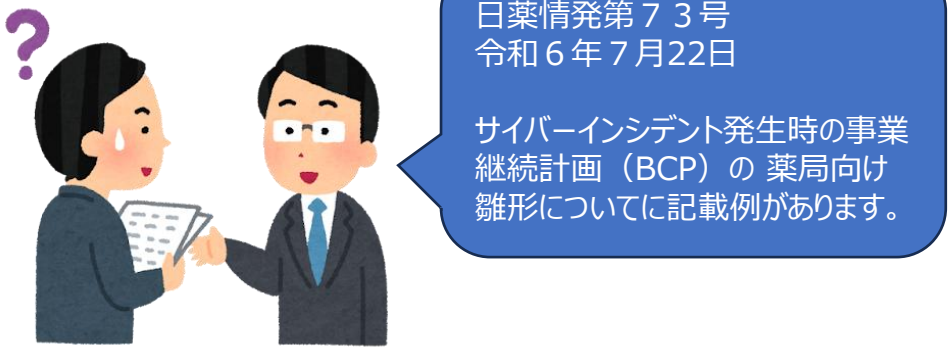
３．情報資産台帳で管理する項目

- 情報資産の種類、情報資産名
- 用途
- 影響（CAI）
- 業務上の価値（事業継続における重要度）
- 管理責任者・管理担当者
- 利用者の範囲
- 記録形態
- 保存場所
- 保存期間
- 廃棄方法
- その他（バックアップ、ライセンス情報等）

表〇:情報機器台帳(例)

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	主な利用者属性	登録日	状態	説明
001	A社	Win11	〇〇電子カルテ	2.0	192.168.0.0	Room1のPC1	Room1	薬剤師・事務職員・システム管理者	2020/12/1	稼働	
002	A社	Win11	〇〇電子カルテ	1.2	192.168.0.0	Room1のPC2	Room1	薬剤師・事務職員・システム管理者	2020/12/1	停止	メンテナンス
003	A社	Win8	〇〇電子カルテ	2.0	192.168.0.0	Room2のPC1	Room2	薬剤師・システム管理者	2014/10/1	稼働	
004	B社	Win11	〇〇管理システム	5.0.1	192.168.0.0	Room3のPC1	Room3	薬剤師・システム管理者	2021/8/1	稼働	

（出典:薬局におけるサイバーセキュリティ対策チェックリストマニュアル ～薬局・事業者向け～ ）



2-6. 情報資産に対する脅威

１．情報資産に対する脅威

情報資産に対する脅威として、以下の脅威を想定し情報セキュリティ対策を実施する。

① ネットワークを介して発生する脅威

- 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

2-6. 情報資産に対する脅威

１．情報資産に対する脅威

情報資産に対する脅威として、以下の脅威を想定し情報セキュリティ対策を実施する。

② ヒューマンエラーにより発生する脅威

- 情報資産の無断持出、無許可ソフトウェアの使用等の規定違反
- 設計・開発の不備、プログラム上の欠陥
- 機器の操作・設定ミス、機器等のメンテナンス不備
- 情報セキュリティ内部・外部監査機能の不備
- 委託管理の不備、マネジメントの欠陥
- 機器故障等の非意図的要因による情報資産の漏えい
- 機器故障等の非意図的要因による破壊・消去等

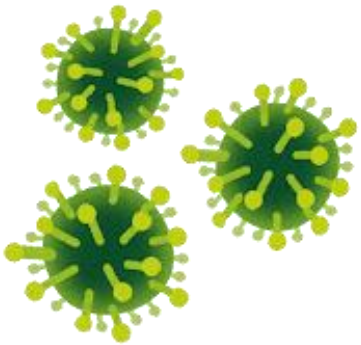
2-6. 情報資産に対する脅威

１．情報資産に対する脅威

情報資産に対する脅威として、以下の脅威を想定し情報セキュリティ対策を実施する。

③ 自然災害やパンデミック等により発生する脅威

- 地震、落雷、火災等災害によるサービス及び業務の停止等
- 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用機能不全等
- 電力供給／通信／水道供給の途絶等のインフラの障害からの波及等



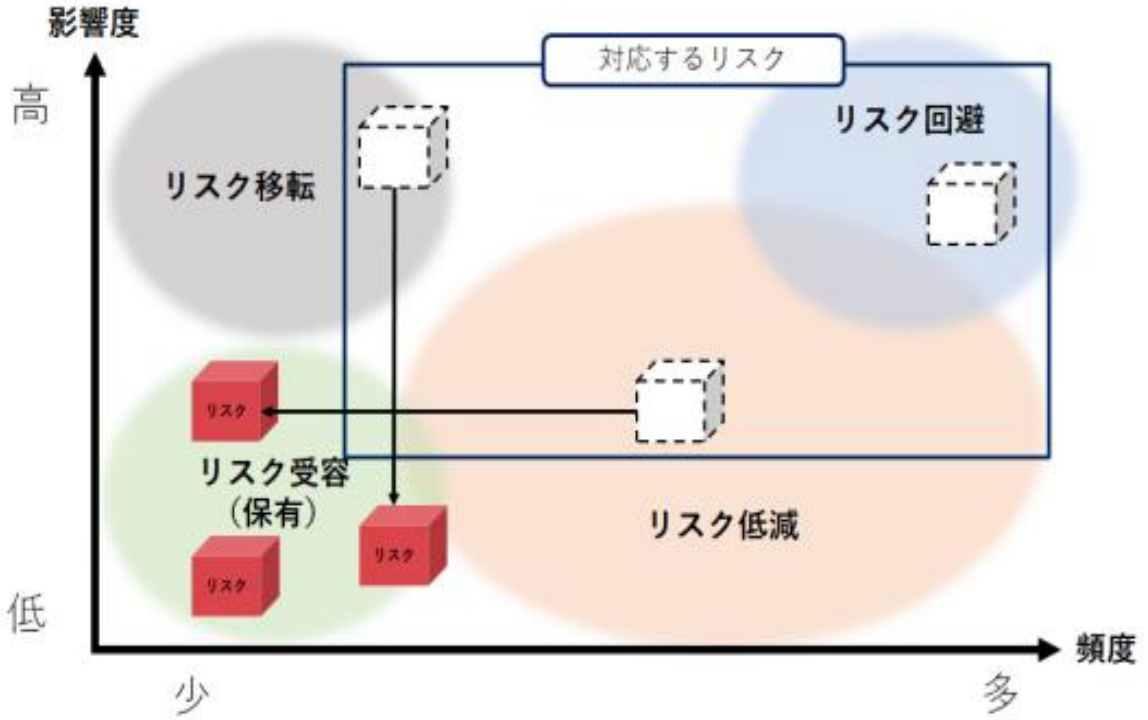
2-7. 情報セキュリティ対策の内容

1．情報セキュリティ対策

前頁の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じます。

- 組織体制
- **情報資産の分類と管理**
- 情報システム全体の強靭性の向上
- 物理的セキュリティ
- 人的セキュリティ
- 技術的セキュリティ
- 運用
- **業務委託と外部サービスの利用**
- 評価・見直し

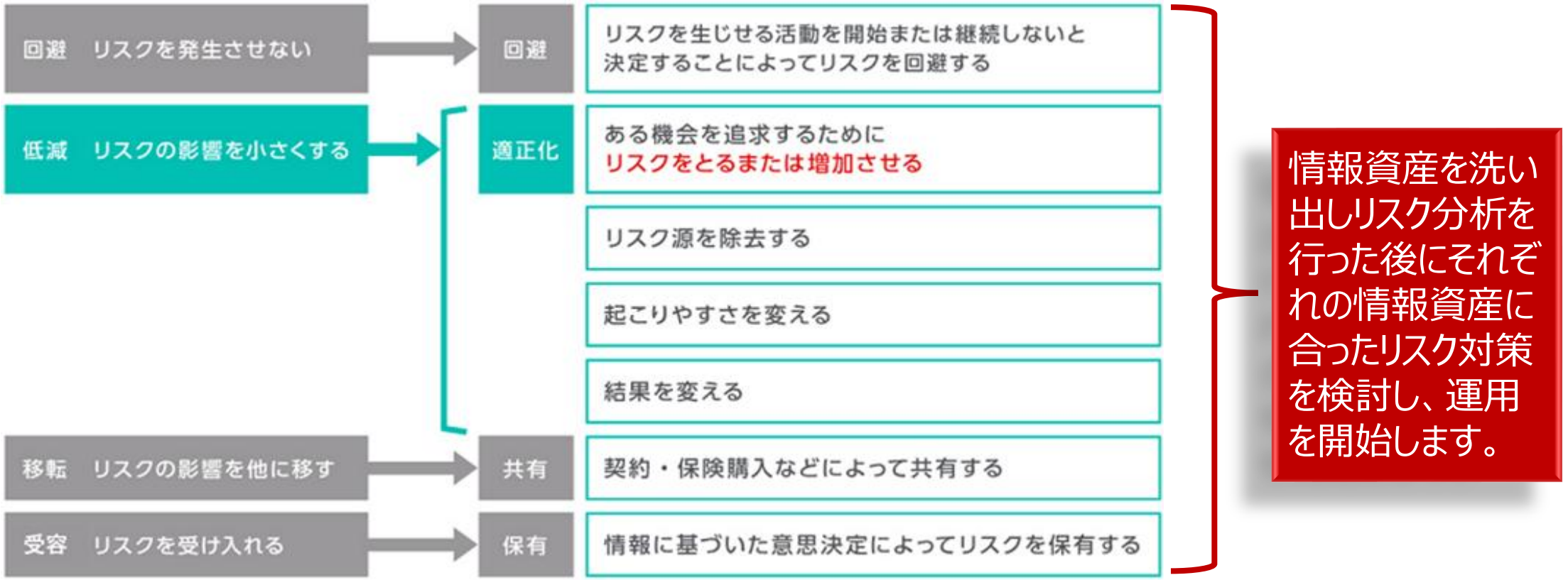
リスクの検討と対応イメージ



2-8. 情報セキュリティリスクへの対応の変化（ゼロトラスト）

1．情報セキュリティリスクへの対応の変化

情報セキュリティリスクは、ISO31000:2009により拡充され対応されています。



2-9. ゼロトラスの定義

1．ゼロトラストの定義

ゼロトラストとは、その言葉の通り**「信頼（Trust）を何に対しても与えない（Zero）」**という前提に立ったセキュリティ対策の考え方です。

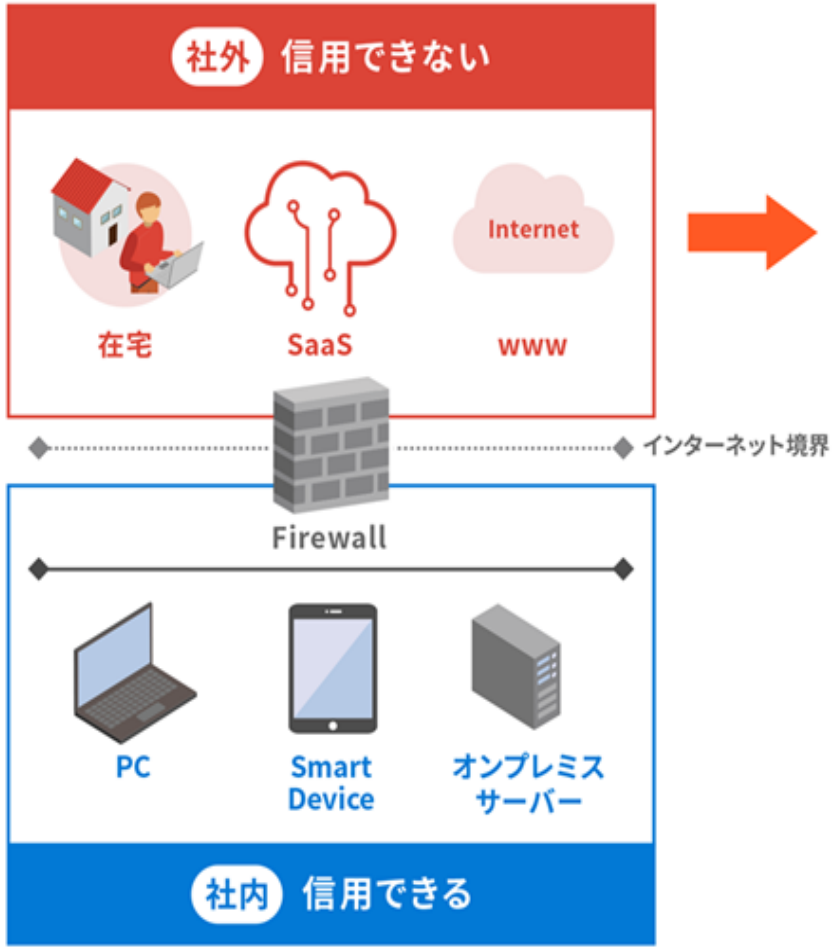
①信頼しない	内部のネットワークも含め、すべてのトラフィック（ネットワークを流れる情報）は信頼できないとみなし、**常にすべてのリクエスト（何かを求めること）を検証する必要がある**という考え方。
②常に検証	すべてのユーザー、デバイス、アプリケーションに対して、**常にアクセスを確認し、検証**しますが、これには、多要素認証や暗号化などの技術が使用されます。
③最小権限	**必要最低限の権限のみを付与**することで、万一の障害発生時にも影響を最小限に抑える。
④セグメント化	ネットワークを細かく分割し、**異なるセグメント間でのアクセスを厳密に制御**すれば、障害が発生しても被害が限定される。

※どんな時でもすべてのアクセスは疑わしいと考えることがゼロトラストの基本です。

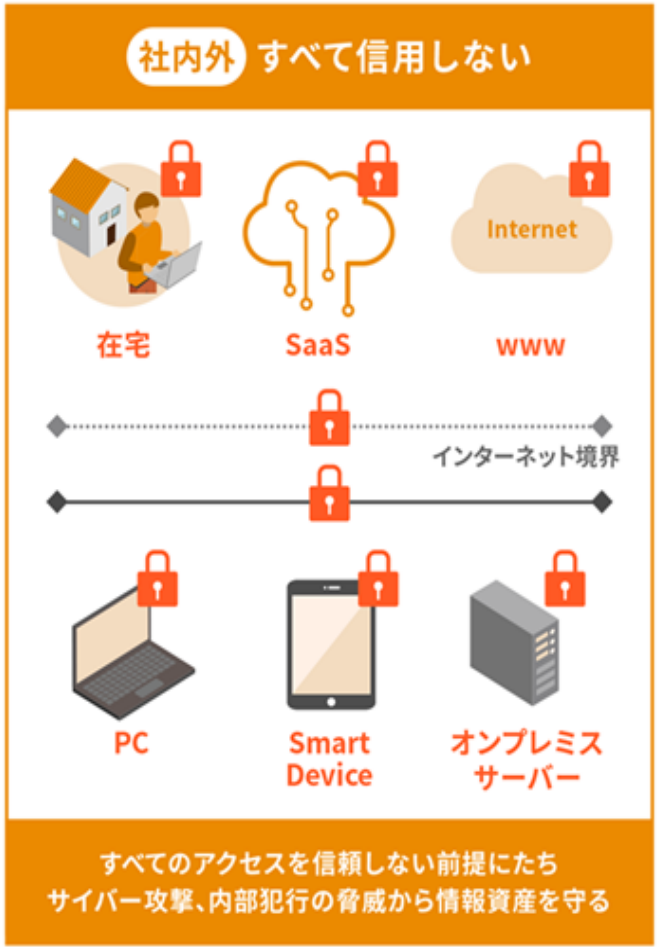
（参考）ゼロトラスの運用イメージ

出典：京セラみらいエンビジョン株式会社

従来の境界型セキュリティ



ゼロトラストセキュリティ



対策

運用管理
- セキュリティ監視センター（SOC）
- セキュリティ運用管理の外部委託（MSS）

Cloud制御
- 危険なサイトへのアクセス制御（SWG）
- セキュリティポリシーとアクセス制御（CASB）

認証
- クラウド上での認証とID管理（IDaas）
- 動的VPNで通信を確保（SDP）

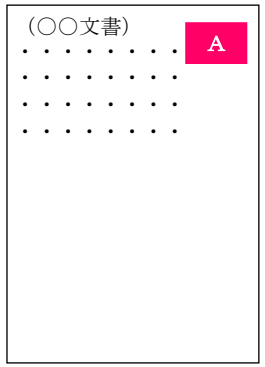
ネットワーク
- 柔軟なネットワーク（SD-WAN）
- 新しい境界防御（NGWF）
- 拠点からインターネット接続（LBO）

端末防御
- ウイルス感染防止（EPP）
- ウイルスのふるまい検知（EDR）
- 端末管理（IT資産管理）

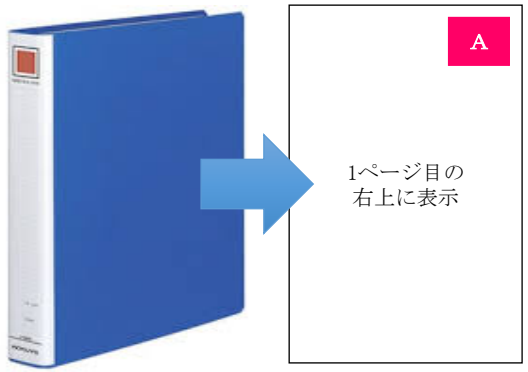
2-10. 情報資産の分類と管理

1．情報資産の分類と管理

情報資産を適切に管理するためには、情報の重要度によって分類し管理方法を決定します。**一般的に情報資産は、「情報」「ソフトウェア」「物理的資産」「サービス」等に分類されます。**分類された情報資産は、情報の種類によって、**「極秘」「対外秘」「コピー厳禁」**など、重要度で分けたラベル付けを行うことで、情報の取り扱いの重要度が一目でわかります。



＜ 紙文書 ＞



＜ チューブファイル ＞

＜ CD／DVD-R ＞

＜ USBメモリ＞

注１）
USBメモリは、本組合で許可されたもののみ利用可能。

注２）
CD/DVD/USBの利用時には必ず「電磁的記録媒体利用記録簿」に記録し管理者の許可を得て利用すること。

2-11. 情報資産の保管

1．情報資産の保管

情報資産の分類ごとに保管場所を決めておくことも大事です。

① 重要書類や極秘資料は**所定の管理場所に保管し鍵をかける。**

② 保管場所には**特定の人物しか出入りできないようにする。**

③ USBメモリスティックなどの**保存媒体は責任者が管理する。**

最終的に誰が何処に鍵を保管するかが大事！

Part 3

調剤薬局における基本的な業務フローチャート
～セキュリティの観点から取り扱いに疑問を感じるポイント～

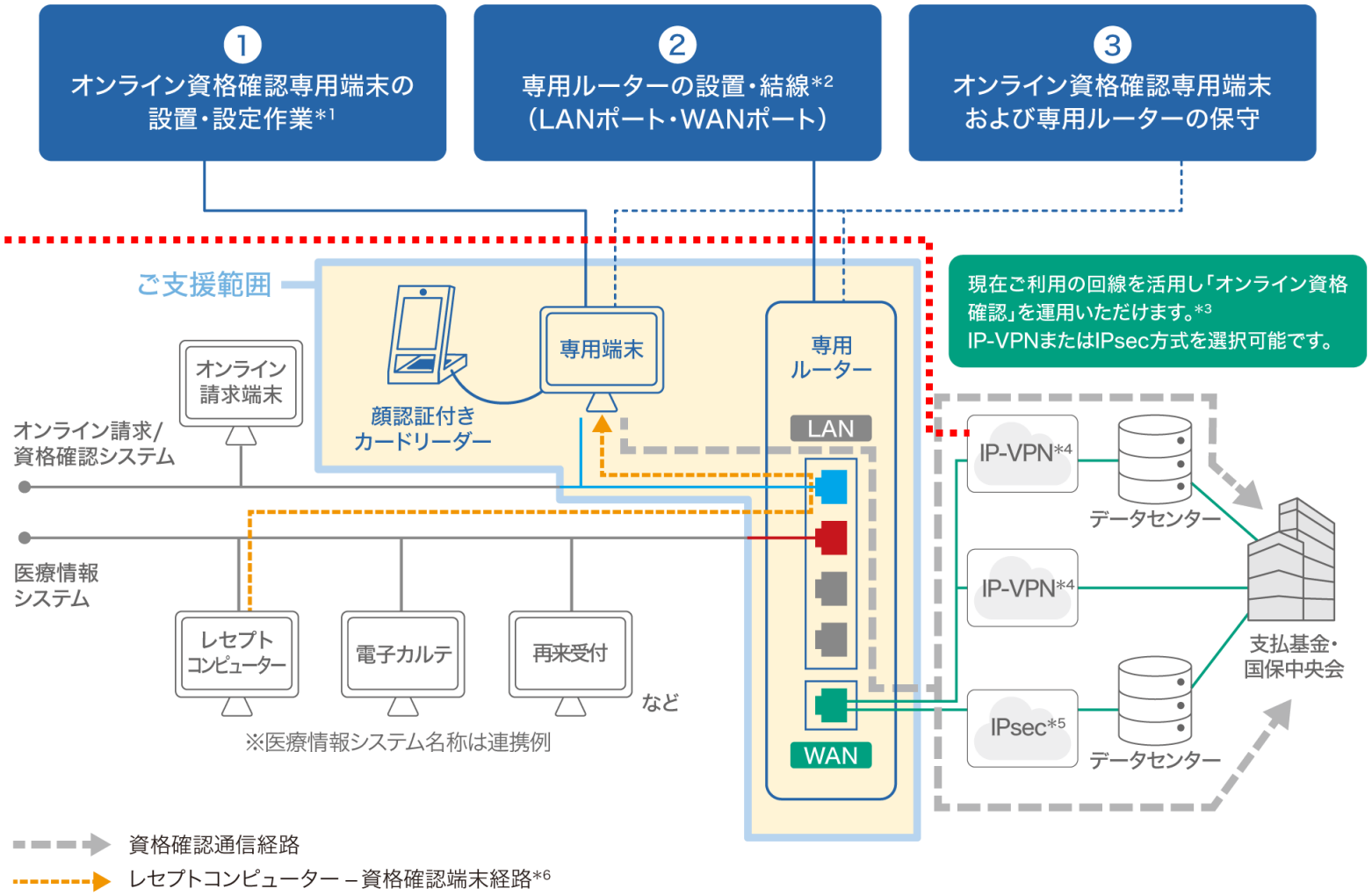
3-1. オンライン資格確認における情報セキュリティ対策

オンライン資格確認端末の整備

【ご質問】

オンライン資格確認端末を購入設置された時、ネットワーク接続において**既設のインターネット回線や既設のルーター装置を利用**しておられますか？

あるいは、左図のようにオンライン資格確認用の専用回線、専用ルーター、専用端末を購入し設置されましたか？



3-2. 調剤薬局の主な業務フローから見る情報セキュリティリスクの洗い出し

1 **処方箋受付**
処方箋を受取、保険証・マイナンバーカードの利用の確認、お薬手帳の有無の確認

2 **患者情報収集**
患者の体質、アレルギー歴、副作用歴などの情報の確認、併用薬の有無や、現在の服薬状況や残薬の確認

3 **処方内容の確認**
処方箋をコンピュータに入力し、保険点数の計算入力された処方のチェック。
処方内容に問題があれば疑義照会。

4 **薬の調剤・監査**
処方に基づいて、調剤患者の服薬コンプラアンスがあがるための、工夫の必要性の吟味（粉砕・一包化・味など）最終監査。

5 **薬のお渡しと服薬指導**
薬剤情報提供書・薬袋・調剤明細書・領収書の作成・印刷。患者に薬の適正な使用方法について情報提供・指導。

6 **投薬後**
薬歴の記載。必要な患者には投薬後、必要なタイミングにて服薬フォローなど。
必要性がある場合は、処方医に報告処方箋・調剤録など保管（３年もしくは５年）。

リスク
① 処方箋・保険証・薬手帳のコピーをとる
② 処方箋・保険証のスキャンをして取り込む
③ マイナンバーカード読取機の設置場所
④ 電子お薬手帳

リスク
⑤ 問診の処理（紙・デジタル）

リスク

リスク

リスク
⑥ 患者の名前を呼んで良いか？　受付番号の方が良いか？
⑦ 服薬指導の声が周りに聞こえる？

リスク
⑧ 処方箋の保管方法
⑨ 薬歴の保管方法
→紙薬歴は、カギのかかる書庫？
→デジタルデータは、パスワードの管理？

❶ 処方箋受付リスク

- ◆ 処方箋を受け取り
- ◆ 保険証・マイナンバーカードの利用の確認
- ◆ お薬手帳の有無の確認。

リスクマネジメント（リスク分析）

① 情報資産に該当するか
② 情報資産分類は、「極秘」「対外秘」「コピー禁止」のどれに概要するのか？
③ 情報資産の管理方法はどうするのか？
④ 該当するリスクは、「回避」「低減」「移転」「需要」するのか？

ケース：01	処方箋や保険証、保険証のコピーしたデータの取り扱いについて、気をつけたいこと！
ケース：02	処方箋や保険証、保険証のスキャンしたデータの取り扱いについて、気をつけたいこと！
ケース：03	マイナンバーカードの読取り機械の設置場所について、気をつけることはあるか？
ケース：04	電子お薬手帳は、多くの場合、外部委託をしていますが、委託先で情報が漏洩した場合に、薬局は確認できるのか？
ケース：05	委託先を検討する場合、何を確認すれば安全と考えられるか？

❶ 処方箋受付リスク 【回答例】

ケース：01	被保険者証や処方箋のコピーしたデータの取り扱いについて、気をつけたいこと！
（回答）	◆ 例えば、被保険者証や処方箋のコピーを複合機などで取得した場合、複合機に内蔵しているハードディスクに保存されているか否かがセキュリティポイントとなります。 ◆ 購入業者に複合機の設定内容を確認して下さい。 ※メーカーへハードディスクの利用しないように設定変更を依頼してください。 ※マイナンバー法施行時に各複合機メーカーが対応しています。

ケース：02	被保険者証や処方箋のスキャンしたデータの取り扱いについて、気をつけたいこと！
（回答）	◆ 例えば、被保険者証や処方箋のスキャンをデータ複合機などで取得した場合、複合機のディスクに保存されているか否かがセキュリティポイントとなります。 ◆ 複合機の設定を確認して下さい。 ※メーカーへハードディスクの利用しないように設定変更を依頼してください。 ※マイナンバー法施行時に各複合機メーカーが対応しています。

❶ 処方箋受付リスク 【回答例】

ケース：03	マイナンバーカードの読取り機械の設置場所について、気をつけることはあるか？
（回答）	◆ オンライン資格確認機器の設置は、利用者の使い易い場所としてカウンター等に設置するのが一般的です。 ◆ 機器の底面に転倒防止リスク用の「耐震シート（耐震７）」を添付してください。 ※シートは粘着レベルを維持するために厚みのあるシートを利用すること。 ※100均ではなくメーカー製品を利用してください。

ケース：04	電子お薬手帳は、多くの場合、外部委託をしていますが、委託先で情報が漏洩した場合に、薬局は確認できるのか？
（回答）	◆ 電子お薬手帳サービスを提供している業者との業務委託契約に情報漏えい時の監査実施が記載されていれば、直接確認をすることが出来ます。 ◆ 契約に監査事項の記載がなければ、個人情報保護委員会に提出される情報漏えい報告書を確認することが出来ますが、当事者でない限り個別対応は難しいと思います。 ※https://www.ppc.go.jp/personalinfo/legal/leakAction/#about

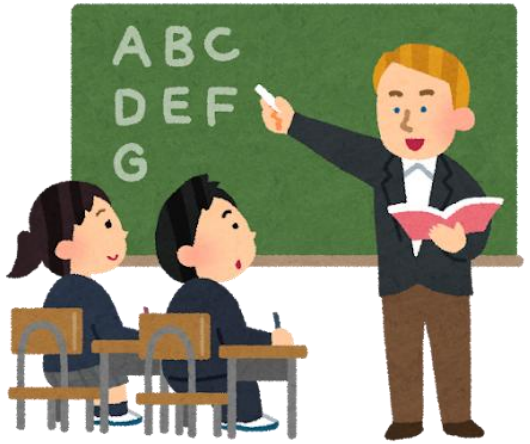
【参考】主なクラウドサービスの提供形態（外資系の独占）

オンプレミス	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
アプリケーション	アプリケーション	アプリケーション	アプリケーション
ミドルウェア	ミドルウェア	ミドルウェア	ミドルウェア
OS	OS	OS	OS
ハードウェア	ハードウェア	ハードウェア	ハードウェア

○IaaSサービス
Amazon、マイクロソフト、Google等外資系メガクラウドベンダーがサービスを展開。

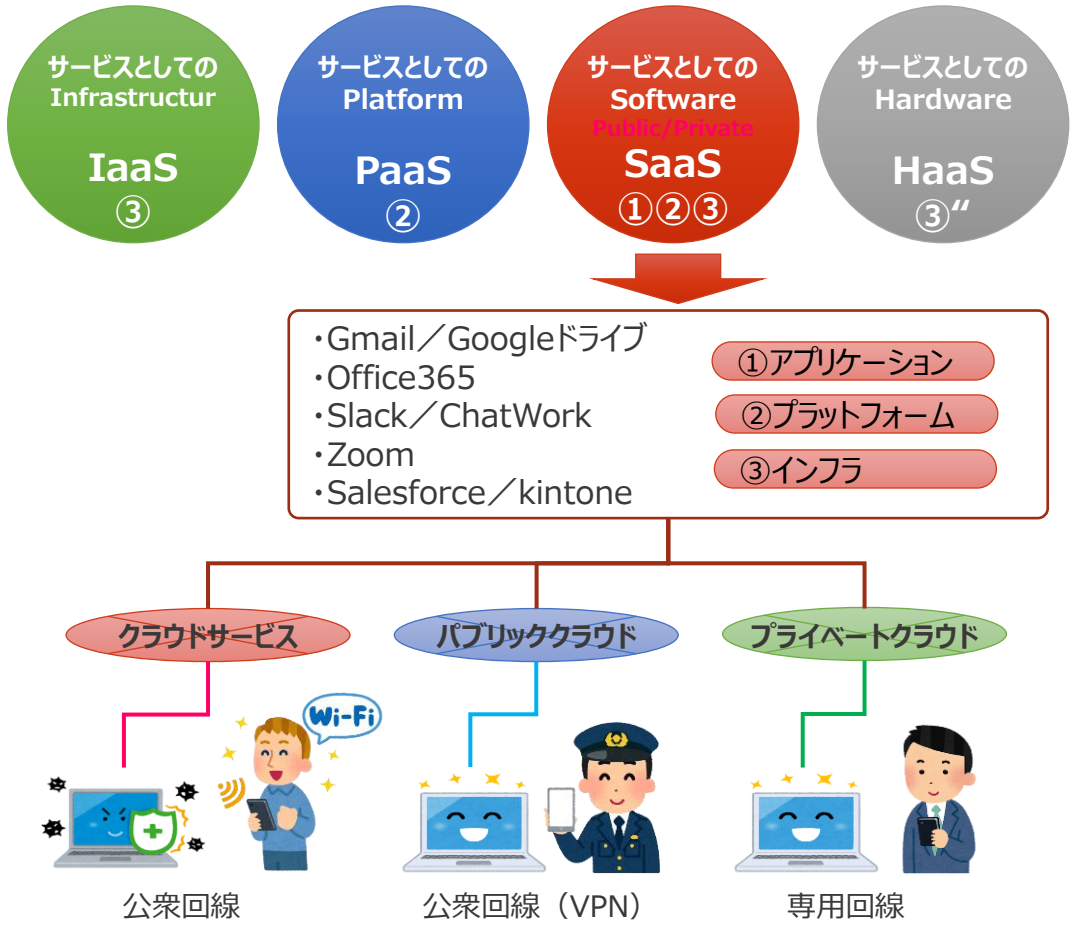
○PaaSサービス
Google App Engine、Heroku等外資系メガクラウドベンダーがサービスを展開。

○SaaSサービス
Office365、Gmail、Dropbox、サイボウズなどのグループウェア　etc.

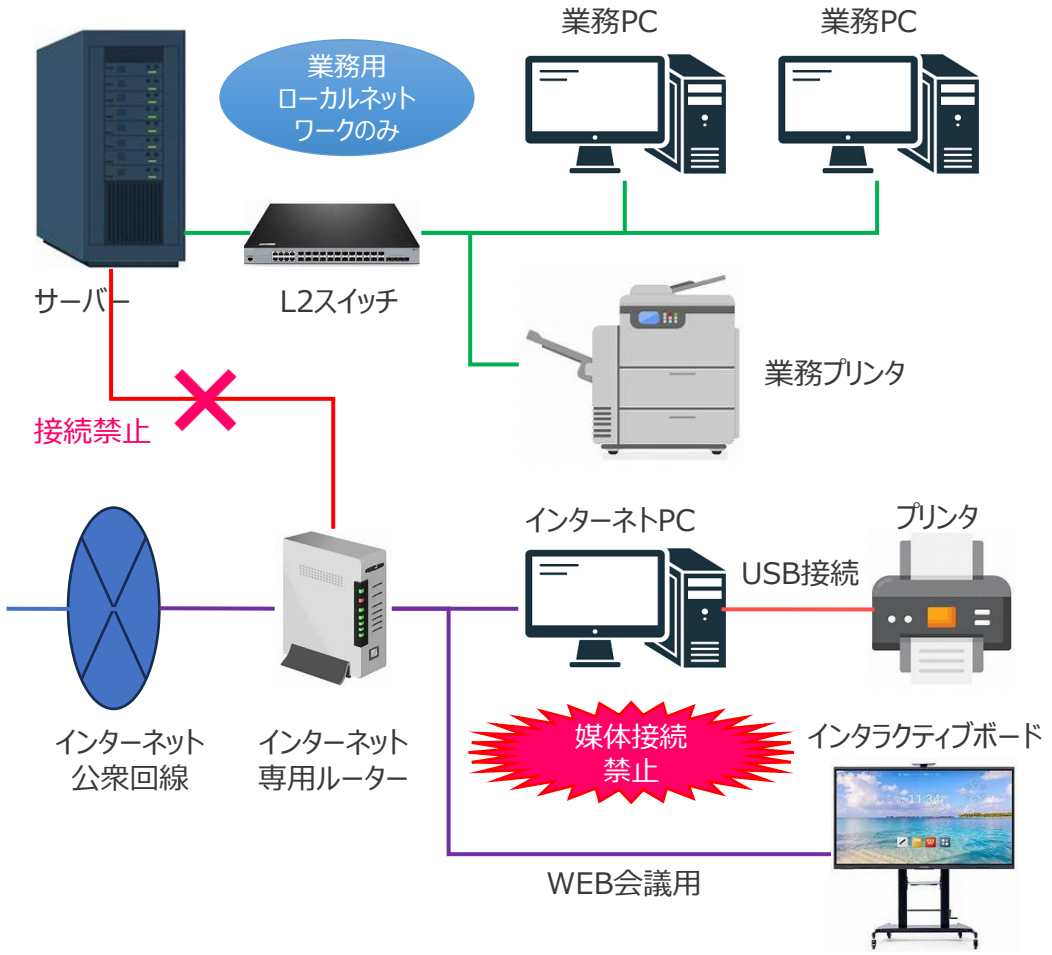


【参考】クラウドサービスリスクと情報システムの責任分界

○クラウドサービス（ISMAP）



○オンプレミス（ローカル利用）



❶ 処方箋受付リスク 【回答例】

ケース：05	委託先を検討する場合、何を確認すれば安全と考えられるか？
（回答）	◆ 個人情報保護に関する会社としての資格を取得し、何回更新しているか。 ※一般財団法人日本情報経済社会推進協会　https://privacymark.jp/ ◆ 情報セキュリティ）に関する会社としての資格を取得し、何回更新しているか。 ※情報マネジメントシステム認定センター　https://isms.jp/ ◆ 利用している企業に一部上場企業が含まれているか否かを確認すること。

JQA-IM0016
公共ＢＰＯサービス部
データセンター運用部
データセンター企画部 企画グループ

JQA-IT0054
公共ＢＰＯサービス部
データセンター運用部
データセンター企画部 企画グループ

JQA-BC0020
公共ＢＰＯサービス部
データセンター運用部
データセンター企画部 企画グループ

11820011(13)

【参考】「クラウド・バイ・デフォルト原則」を踏まえた政府情報システムの整備

ISMAP（イスマップ）とは、政府が導入しているクラウドサービスのセキュリティ評価・登録制度です。

ISMAPに登録されていれば、政府が求めるセキュリティ要件を満たしているクラウドサービスであることの証明となるため、セキュリティ水準の確保や円滑なサービスの導入を進める上での指標として利用することが可能です。

ISMAPに登録されたクラウドサービスは、「ISMAPクラウドサービスリスト」として公式サイトに公開されており、政府のシステム調達に限らず、民間企業でも制度を活用することで、安全性の高いクラウドサービスを選択できるようになります。

本制度を利用することにより、**政府機関等は、情報セキュリティ対策の実施状況の直接 確認が省略できる**とともにサービスの範囲やセキュリティ対策の範囲について情報提供がなされることで、**一定の情報セキュリティ対策の実施が確認されたクラウドサービスを効率的に調達することが可能**となります。

※今後の調達の参考となるリスト参照先（https://www.ismap.go.jp/csm?id=cloud_service_list）

【参考】ISMAPに登録されたサービス例（ソフトバンク）

- **ホワイトクラウド ASPIRE**
  VMwareの仮想化基盤をベースに、ソフトバンクの信頼性の高いネットワークサービスをはじめデータセンターやマネージドサービス等、多様なサービスとの連携が可能なSLA99.999%を誇る国産クラウドサービスです。
  ☛ https://www.softbank.jp/biz/cloud/iaas/aspire/

- **PrimeDrive**
  ファイルの送付・共有を安全かつシンプルな操作で実現できる法人向けオンラインストレージサービスです。
  オンラインストレージでのデータ受け渡しにおける情報漏えいの防止に必要不可欠なセキュリティ機能を備えており、大容量ファイルの送付や重要なファイルのセキュアな受け渡しに適しています。
  ☛ https://www.softbank.jp/biz/services/collaboration/primedrive/

- **ビジネス・コンシェル デバイスマネジメント**
  複数台のスマートフォンやタブレット端末をリモートで一元管理・運用できるMDM（Mobile Device Management）サービスです。利用者とデバイスの情報管理だけでなく、リモートでの端末制御やセキュリティの一括設定ができます。
  ☛ https://www.softbank.jp/biz/services/security/bcdm/

❷ 患者情報収集リスク

- ◆ 患者の体質、アレルギー歴、副作用歴などの情報の確認。
- ◆ 併用薬の有無や、現在の服薬状況や残薬の確認。

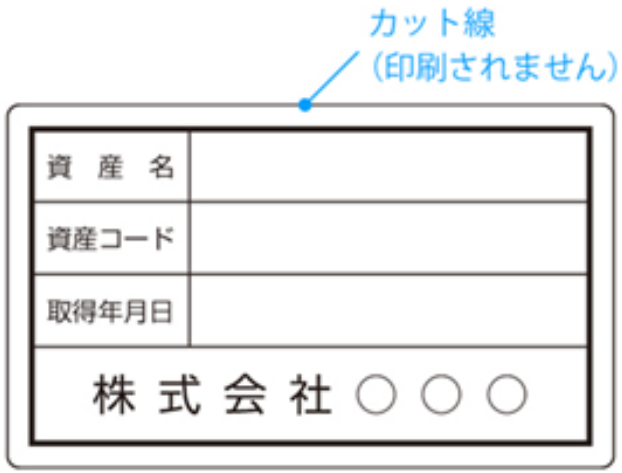
リスクマネジメント（リスク分析）

① 情報資産に該当するか
② 情報資産分類は、「極秘」「対外秘」「コピー禁止」のどれに概要するのか？
③ 情報資産の管理方法はどうするのか？
④ 該当するリスクは、「回避」「低減」「移転」「需要」するのか？

ケース：06	患者の問診を紙媒体、もしくはデジタル媒体で行う場合、その保管について気をつけたほうがいいことはなにか？

❷ 患者情報収集リスク 【回答】

ケース：06	患者の問診を紙媒体、もしくはデジタル媒体で行う場合、その保管について気をつけたほうがいいことはなにか?
（回答）	◆ 紙媒体は、紙媒体をケースか箱に保管し、鍵のかかるキャビネット等に保管してください。 ※紙媒体の種類に応じて保存期限と廃棄期限を決め、箱かケースに記載してください。 ◆ 電磁的記録媒体の保管は、鍵のかかる机引き出し、キャビネット、ロッカーで保管しますが、まず媒体に管理番号シールを貼ってから管理責任者が保管してください。 ※紙媒体の種類に応じて保存期限と廃棄期限を決めシールに記載してください。



セキュリティレベル 7 以上
重要書類の細断サイズを含むセキュリティの
国際標準「 ISO／IEC 21964-1,2,3 」

❸ 処方内容の確認

- ◆ 処方箋をコンピュータに入力
- ◆ 保険点数の計算入力された処方チェック
- ◆ 処方内容に問題があれば疑義照会。

リスクマネジメント（リスク分析）

① 情報資産に該当するか
② 情報資産分類は、「極秘」「対外秘」「コピー禁止」のどれに概要するのか？
③ 情報資産の管理方法はどうするのか？
④ 該当するリスクは、「回避」「低減」「移転」「需要」するのか？

ケース：07	レセコン会社によって、セキュリティレベルに差があるか？
ケース：08	レセコンのシステムの１つである、オンプレ型とクラウド型とで、セキュリティに対する対策に違いがあるか?
ケース：09	オンプレ型とクラウド型のどちらのタイプが、セキュリティレベルが高いと考えられるか？
ケース：10	情報漏洩が、結果的にレセコン会社にあったかどうかを調べる手立てはあるか？
ケース：11	国は医療機関に対して求めているレベルというものがあるか？
ケース：12	昨日と今日とでセキュリティの世界は変わるのか、逆にセキュリティの世界で不変のものはあるか
ケース：13	セキュリティが突破され、情報が漏洩された場合、どこに連絡、対応をもとめれば 良いか?
ケース：14	薬局としては、a.レセプトデータ盗難　b.患者薬歴データ盗難　c.盗難データを元に脅迫（金銭要求）d.盗難データ売買を防ぐことができれば、セキュリティ対策として問題ないのではないか？　この考え方は誤りか？

❸ 処方内容の確認 【回答例】

ケース：07	レセコン会社によって、セキュリティレベルに差があるか？
（回答）	◆ レセコンの機器は、ハード、OS、ソフトで構成されますが、メーカーがどのレベルまで生産に関与しているかがポイントですが、基本的にサプライチェーンをほぼ利用しています。 ※海外や国内生産、組立や検査のみ国内、販売のみ等の確認が必要です。 ◆ レセコンのOSレベル（自社・メーカー・オープン）、ログイン認証（多要素）、アクセス権限（管理者権限）、導入後のセキュリティサービスレベルにも大きな差があります。

ケース：08	レセコンのシステムの１つである、オンプレ型とクラウド型とで、セキュリティに対する対策に違いがあるか?
（回答）	◆ オンプレ型は、基本的に購入者の責任でセキュリティ対策を構築・運用する必要があります。 ※遠隔保守というサービス利用は、セキュリティリスクが高くなります。 ◆ クラウド型は、クラウドサービス会社にネットワーク及びレセコンのセキュリティ対策を依存（エンドポイント以外）することができます。 ※セキュリティレベルを高くするとサービスコストは当然高額となります。

❸ 処方内容の確認 【回答例】

ケース：09	オンプレ型とクラウド型のどちらのタイプが、セキュリティレベルが高いと考えられるか？
（回答）	◆ ローカルネットワーク（外部とのネットワーク接続なし）のみで業務システムのすべてをを運用している場合は、オンプレ型の方がネットワークセキュリティレベルは高いといえます。 ※保守やメンテナンスも業者を呼んで作業をさせることが前提です。 ◆ クラウドサービス利用を併用する場合は、クラウド型の方がセキュリティレベルは高くなります。 ※外部との接続回線は、専用回線又は暗号化されていることが前提です。

ケース：10	情報漏洩が、結果的にレセコン会社にあったかどうかを調べる手立てはあるか？
（回答）	◆ 情報漏えいの内容が機密情報や要配慮個人情報であれば、１件でも漏洩すれば個人情報保護委員会への報告が義務づけられています。 ◆ レセコン会社が漏えいした情報に個人情報が含まれている場合、あるいは含まれていることが懸念される場合は、個人情報保護法相談ダイヤルに電話してください。 ※https://www.ppc.go.jp/personalinfo/pipldial/

❸ 処方内容の確認 【回答例】

ケース：11	国は医療機関に対して求めているレベルというものがあるか？
（回答）	◆ 国は医療機関及び薬局に、医療情報システムの安全管理に関するガイドライン 第6.0版（令和5年5月）の遵守を求めています。 ※https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html ※薬局におけるサイバーセキュリティ対策チェックリスト(令和６年５月) ※医療情報システム部門等におけるBCPのひな形

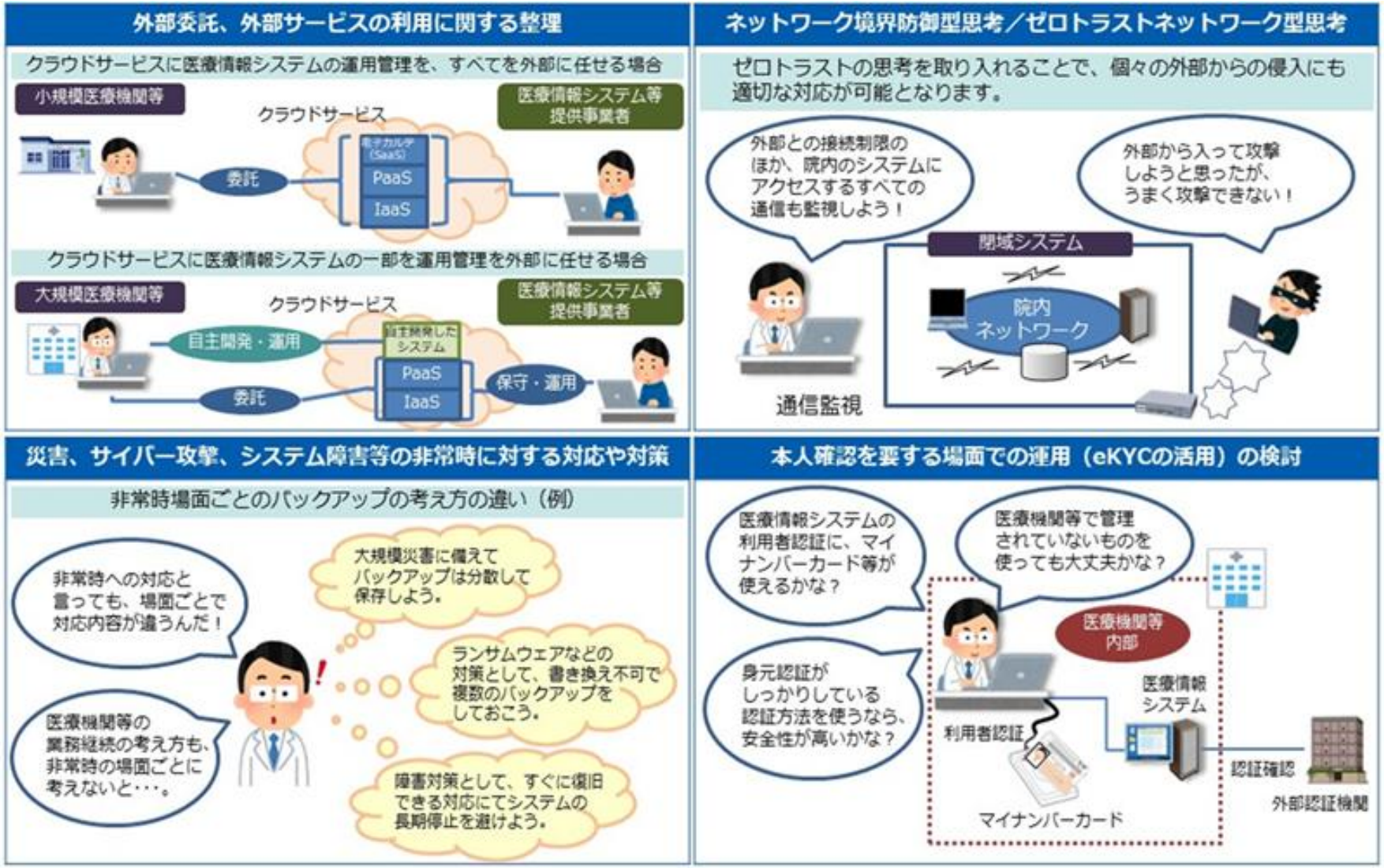
第２ 改定の概要　※１．は省略

２．外部委託、外部サービスの利用に関する整理
クラウドサービスの特徴を踏まえたリスクや対策の考え方を整理するとともに、医療機関等のシステム類型別に責任分界の考え方等を整理する。

３．情報セキュリティに関する考え方の整理
ネットワークの安全性の考え方や認証のあり方を踏まえて、ゼロトラスト思考に則した対策の考え方を示すほか、サイバー攻撃を含む非常時に対する具体的な対応について整理する。

４．新技術、制度・規格の変更への対応
オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置等について整理する。

【参考】医療情報システムの安全管理に関するガイドラインの概要



クラウドサービス

ゼロトラスト

BCP計画・訓練

eKYC

Electronic Know Your Customer
オンライン本人確認
・企業／法人
・個人事業主

【参考】個人認証サービスのマイナンバー利用による変化

証明書類Web取得サービスとは

オンラインで、公的個人認証（JPKI）や各種書類の取得ができるサービスです。
マイナンバーカードのICチップ読み取りか本人確認書類をアップロードで取得する
本人確認方法が選択可能。合わせて、申し込みに必要な各種書類も取得できます。
さらに、本人確認書類や各種提出書類の画像について、目視による確認作業も可能です。

民間サービス先行

公的機関に1本化!

地方公共団体情報システム機構
公的個人認証サービス

❸ 処方内容の確認 【回答例】

ケース：12	昨日と今日とでセキュリティの世界は変わるのか、逆にセキュリティの世界で不変のものはあるか？
（回答）	◆ セキュリティの世界は、変化のスピードが恐ろしく速いですが、セキュリティの世界が変わるか否かは、皆さんが利用する情報処理運用環境に委ねられます。 **※オンプレ型での運用、クラウドサービス併用型、フルクラウドサービス型** ◆ マルウェアは１日100万個作られ、最近ではAI利用によるマルウェア作成ができるため発生するウイルスの数は爆発的に増えています。又、ウイルスは誰でも買える時代になりました。

❸ 処方内容の確認 【回答例】

ケース：13	セキュリティが突破され、情報が漏洩された場合、どこに連絡、対応をもとめれば 良いか?
（回答）	◆ セキュリティが突破された事実の把握は難しく、多くは外部からの情報入手がトリガー情報となります。まず、取引メーカー、サイバー警察を優先して連絡してください。 ※大阪府警 ☛ https://www.police.pref.osaka.lg.jp/sodan/4525.html ◆ 情報漏えいの件数や関与にもよりますが、事業に関係するステークホルダー（利害関係者）に対する連絡と対応が必要となります。

ケース：14	薬局としては、「レセプトデータ盗難　b.患者薬歴データ盗難　c.盗難データを元に脅迫（金銭要求）d.盗難データ売買」を防ぐことができれば、セキュリティ対策として問題ないのではないか？　この考え方は誤りか？
（回答）	◆ 各薬局にある情報資産は異なります。基本的には重要な情報が含まれているデータや紙に対する情報セキュリティ対策ができており、かつ継続的な運用ができていれば、事業者としての改善要求は少なくなります。 ◆ 犯罪者による盗難や脅迫等による情報漏えいであっても、結果として事業者に損害賠償責任が発生しますので、サイバー保険等に入るのも一案です。

❹ 薬の調剤･監査

- ◆ 処方箋をコンピュータに入力
- ◆ 保険点数の計算入力された処方チェック
- ◆ 処方内容に問題があれば疑義照会。

リスクマネジメント（リスク分析）

① 情報資産に該当するか
② 情報資産分類は、「極秘」「対外秘」「コピー禁止」のどれに概要するのか？
③ 情報資産の管理方法はどうするのか？
④ 該当するリスクは、「回避」「低減」「移転」「需要」するのか？

ケース：15	**情報漏洩において、上記a～d 以外で何を守れば良いか？**
ケース：16	**「身代金要求ウイルス」に感染し、業務がSTOP してしまった場合、どのように対応すればいいか？**
ケース：17	**情報漏洩がおきていたことがわかった場合、薬局として患者にどのような補償をしなければならないか？**
ケース：18	**薬局の事故として、過去にそのような事例はあるか？**

❹ 薬の調剤･監査 【回答例】

ケース：15	情報漏洩において、上記a～d 以外で何を守れば良いか？
（回答）	◆ 情報セキュリティ対策は、情報システムを利用している環境と範囲により異なりますが、主なものとしては、入退出管理、クラウドサービス利用状況、障害･事故管理、IT継続性、認証と権限、ネットワークのアクセス制限、パッチの適用、ウイルス及び悪意のあるプログラムに対する対策、記憶媒体の管理、スマートデバイス、電子メールの利用、Webの管理、ログの取得、バックアップ、容量･能力の管理、変更管理、構成管理、SNSの利用などがあります。

ケース：16	「身代金要求ウイルス」に感染し、業務がSTOP してしまった場合、どのように対応すればいいか？
（回答）	① 端末のネットワーク切断をしてください（端末の電源は切断しないでください）。 ② 大阪府警本部に電話してください。サイバー対策本部にてランサムウェアの種類や対応を検討してくれます。最新でなければ駆除も可能な技術を持っています。 ※電話番号：06-6943-1234 （代表） ③ 利用している情報システムの提供業者に電話をして、対応してもらってください。

❹ 薬の調剤･監査 【回答例】

ケース：17	情報漏洩がおきていたことがわかった場合、薬局として患者にどのような補償をしなければならないか？
（回答）	◆ 情報漏えいの事実が認められ、対象件数が判明した後で保証の有無を検討します。 ◆ 公的な団体や医療機関では、情報漏えいの疑いがる段階で公表義務があります。 ◆ 保有する情報件数にもよりますが、保険加入し、弁護士に手続きを任せることが得策です。 ◆ 判例に基づく個人情報漏えいの損害賠償額は、１件で10,000円～15,000円です。 ◆ 情報漏えいされた方が裁判してこない限り、日本ではお詫び文章の公表で済んでいます。

ケース：18	薬局の事故として、過去にそのような事例はあるか？
（回答）	◆ 個人情報漏えいに関する薬局の事例はあります。 ※個人情報の事案は、次ページにてご紹介しますが、昨年10月に個人情報保護委員会から、薬局に対して安全管理措置の具体的な取り組み事例などを記載した注意喚起文を公表されています。

【参考】個人情報漏洩で注意喚起～薬局で誤交付など868件（2024/10/16）

政府の個人情報保護委員会は、病院・診療所、薬局における要配慮個人情報を含む個人データの漏洩等事案を踏まえ、安全管理措置の具体的な取り組み事例などを記載した注意喚起文を公表し、8日付で関連団体に周知した。

2024年4～6月に報告された薬局の漏洩事案は868件。

そのうち誤交付が792件（91.2%）と大半を占め、郵便・宅配便の誤配や宛名誤り、誤封入、FAX誤送信などの誤送付が61件（7.0%）、紛失等が15件（1.7%）となっている。

薬局における誤交付による漏洩等は、患者の家族を含む患者に他の患者のお薬手帳・お薬手帳シール、診療明細書・領収書、処方薬・薬袋、薬剤情報提供書などを間違って手渡し、お薬手帳シール貼り間違え、会計処理ミスなどにより引き起こされる事例が典型的となっている。

同委員会は、**個人データの漏洩等を防止するため、業務フローの策定や本人確認を確実に行うための措置を既に講じている場合でも、個人情報の保護に関する法律についてのガイドラインに示す安全管理措置に基づき、改めてこれまでの取り組みの有効性の検証を行うよう求めている。**

個人データの取り扱いに関する規律の整備では、以下の内容を周知した。

- 窓口業務を遺漏なく進めていくため、患者に渡す書類等のセットに関するチェックシートを整備する
- 現場で使用するチェックシート等は簡潔で視覚的に分かりやすいものとする
- 患者と受け渡しを行う書類等の書式を統一する

患者に渡す処方薬・薬袋、薬剤情報提供文等については「ダブルチェックを適切に行う」、人員面でダブルチェックが難しい場合は「指差し確認や自身による再確認の励行など、より堅確なチェックを徹底することとする」などを促している。

⑥ 投薬後

- ◆ 薬剤情報提供書・薬袋・調剤明細書・領収書の作成・印刷。
- ◆ 患者に薬の適正な使用方法について情報提供・指導。

リスクマネジメント（リスク分析）

① 情報資産に該当するか
② 情報資産分類は、「極秘」「対外秘」「コピー禁止」のどれに概要するのか？
③ 情報資産の管理方法はどうするのか？
④ 該当するリスクは、「回避」「低減」「移転」「需要」するのか？

ケース：19	患者を呼ぶのに、名前を呼ぶことに患者の個人情報を漏らしているということになるか？
ケース：20	服薬指導の内容が他の患者に聞こえてしまったことで個人情報の漏洩として過去に補償を行ったような事例はあるか？
ケース：21	薬歴を電子化している薬局が多いが、その薬歴へのログインID とパスワードの管理について、良い方法があるか？
ケース：22	レセコンだけでなく、ネットにつながっている機器をサイバー攻撃から守る手技・知識や心構えを知りたい？
ケース：23	患者に送る郵送物などの印刷がレセコンからできないため、レセコンとは別のパソコンで患者住所などを取り扱っているが、そのような患者情報はUSB などで管理し、パソコンに直接保存しない方が良いか？

❺薬のお渡しと服薬指導 【回答例】

ケース：19	患者を呼ぶのに、名前を呼ぶことに患者の個人情報を漏らしているということになるか？
（回答）	◆ 情報漏えいの事実が認められ、対象件数が判明した後で保証の有無を検討します。 ◆ 公的な団体や医療機関では、情報漏えいの疑いがる段階で公表義務があります。 ◆ 保有する情報件数にもよりますが、保険加入し、弁護士に手続きを任せることが得策です。 ◆ 判例に基づく個人情報漏えいの損害賠償額は、１件で10,000円～15,000円です。 ◆ 情報漏えいされた方が裁判してこない限り、日本ではお詫び文章の公表で済んでいます。

ケース：20	服薬指導の内容が、他の患者に聞こえてしまったことで、個人情報の漏えいとして、過去に補償を行ったような事例はあるか？
（回答）	◆ 個人情報漏えいに関する薬局の事例はありますが、店舗内の服薬指導の内容を起因とする個人情報漏えい事案は見つかりませんでした。 ◆ 薬局で患者のプライバシーが守られず、他の顧客に個人情報が漏れてしまった場合、その患者はプライバシー侵害を理由に訴訟を起こすことが出来ます。 ◆ 個人情報の漏えいが原因で精神的苦痛が発生したとして損害賠償を請求できます。

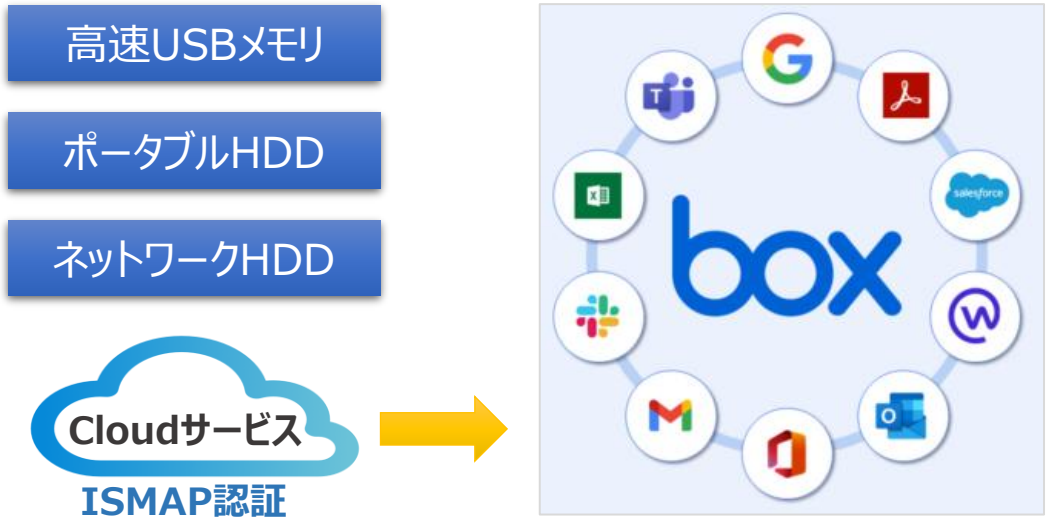
❻ 投薬後 【回答例】

ケース：21	薬歴を電子化している薬局が多いが、その薬歴へのログインID とパスワードの管理について、良い方法があるか？
（回答）	◆ PC立ち上げ時のバイオスパスワードの利用 ◆ 数字、大文字、小文字、特殊文字を含む12桁以上のパスワードを設定する ◆ 多要素認証、多段階認証等の別の認証方法を追加する ◆ ログインIDやパスワードは個人の手帳に記入保管することをお勧めします ◆ 指定されたIPアドレスやデバイス以外からのアクセス制御も不正アクセスに有効です

ケース：22	レセコンだけでなく、ネットにつながっている機器をサイバー攻撃から守る手技･知識や心構えを知りたい？
（回答）	◆ 一般的には、情報システムを利用する端末やプリンタ等を外部ネットワークに接続することなく、利用するデバイスを制限すれば、情報セキュリティリスクは大幅に軽減されます。 ◆ 運用コストは増加しますが、外部ネットワークをすべて専用線に変更し、インターネットを利用する機器と業務システム系機器のネットワークを物理的に分離することもお勧めします。 ※具体的な方法は、「調剤薬局で考えられる情報セキュリティリスク」で説明します。

❻ 投薬後 【回答例】

ケース：23	患者に送る郵送物などの印刷がレセコンからできないため、レセコンとは別のパソコンで患者住所などを取り扱っているが、そのような患者情報はUSBメモリなどで管理し、パソコンに直接保存しない方が良いか？
（回答）	◆ 患者の住所･氏名のみでも顧客情報となるため、その重要度により判断が必要です。 ◆ パソコンが外部ネットワークに接続されず、セキュリティ対策が出来ているのであれば、むしろパソコンにデータを保存し、バックアップにUSBメモリを利用されたいかがでしょうか。 ◆ 本来、USBメモリは一時的なデータ授受用のデバイスです。又、突然データが消えたり、アクセス出来なくなるリスクもあるためデータ保存場所として利用するのはお勧めできません。



Part 4

調剤薬局で考えられる情報セキュリティリスク

4-1. 調剤薬局におけるリスク

■ 調剤薬局における情報セキュリティリスクには、以下のようなものがあります。

① 外部からのサイバー攻撃
ランサムウェアやその他のマルウェアによる攻撃は、システムやデータを破壊したり、患者情報を盗んだりする可能性があります。

② 内部からの情報漏洩
薬局の内部関係者が故意に或いは間違って、患者情報を持ち出すことによる情報漏洩もリスクの一つです。

③ システムの脆弱性
セキュリティパッチの適用の遅れや不要なソフトウェアの稼働によるシステムの脆弱性がサイバー攻撃の原因となることがあります。

④ データのバックアップと復旧
インシデント発生時、事業継続に必要なバックアップの実施、復旧手順の確認ができていないとBCPリスクが高まります。

⑤ 物理的なセキュリティ
外部からの不正アクセスや機器等の盗難等に対する物理的なセキュリティ対策が不足している場合もリスクが高まります。

これらの情報セキュリティリスクに対処するためには、厚生労働省が提供する「医療情報システムの安全管理に関するガイドライン 6.0」を参照し、適切なセキュリティ対策を講じることが重要です。また、**薬局におけるサイバーセキュリティ対策チェックリストの確認や情報資産台帳の更新などを行い**、情報セキュリティ対策の継続実施をおこなわなければなりません。

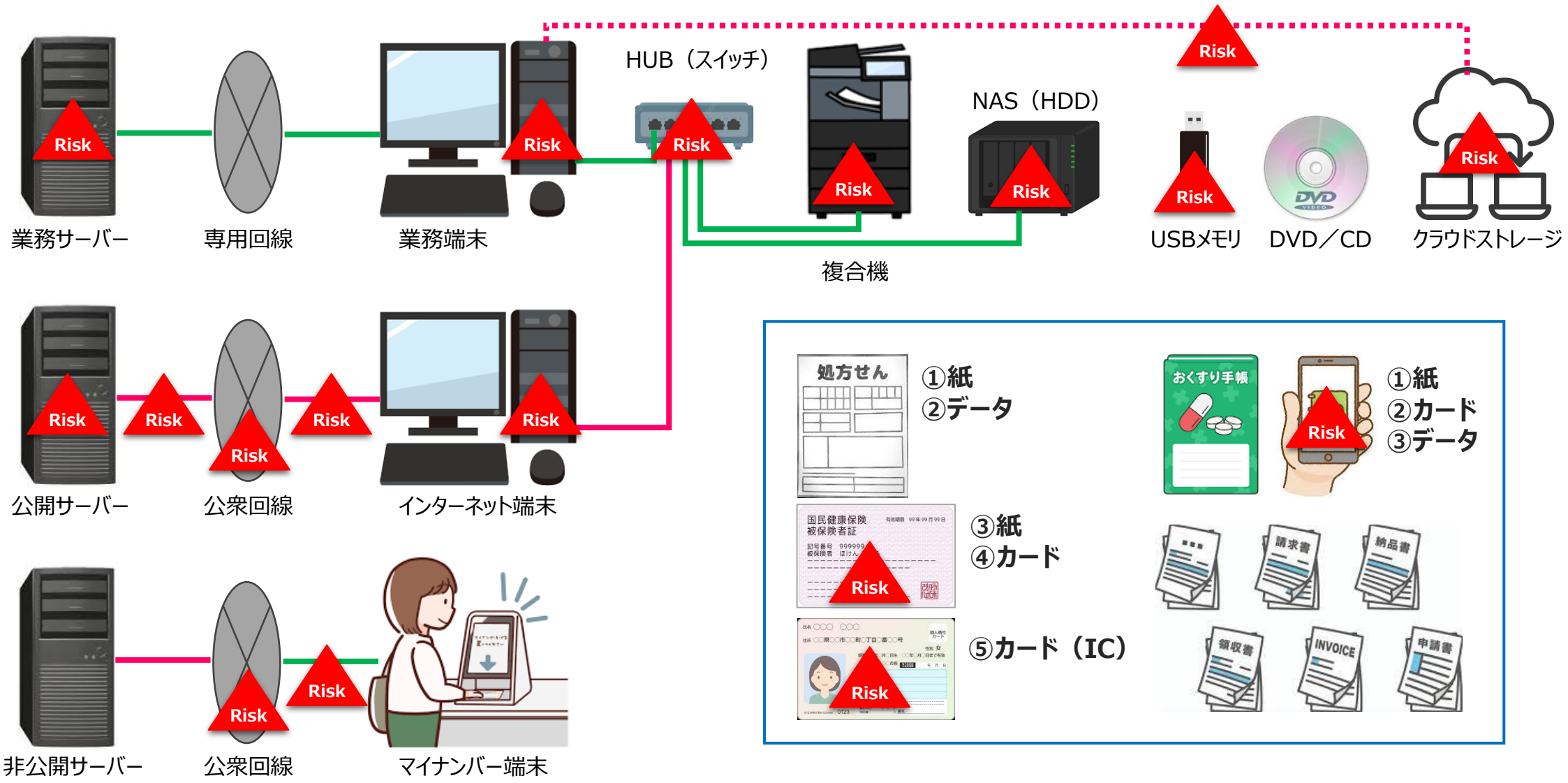
4-2. 調剤薬局における情報セキュリティ対策（実現可能性を重視）

■ 調剤薬局における情報セキュリティリ対策には、以下のようなものがあります。

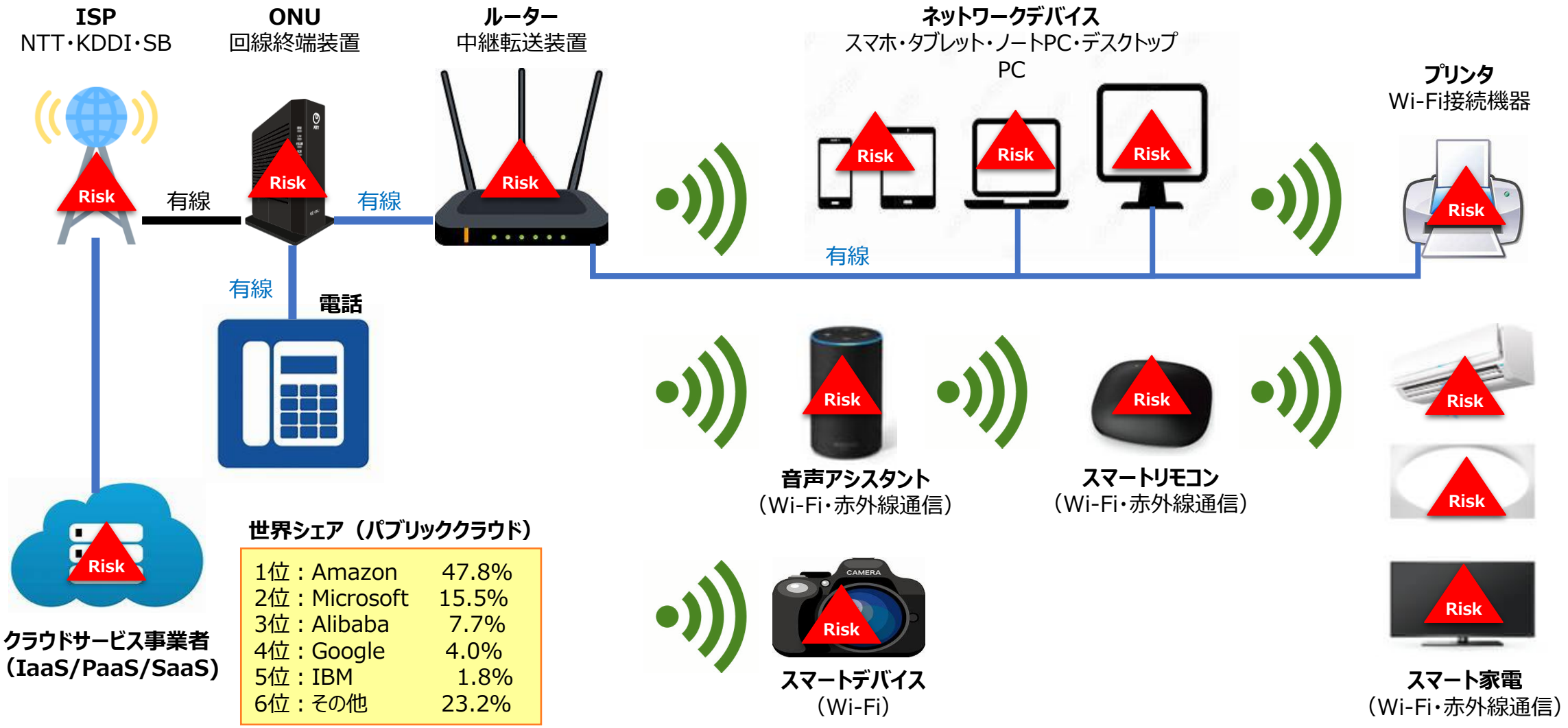
① セキュリティポリシーの策定
② **アクセス管理**
③ 定期的なセキュリティ研修
④ **物理的セキュリティの強化**
⑤ セキュリティソフトウェアの導入
⑥ **データのバックアップ**
⑦ **システムの更新とパッチ適用**
⑨ インシデント対応計画の策定
⑩ **従業員の意識向上**
⑪ 患者のプライバシー保護
⑫ **モバイルデバイスの管理**
⑬ 定期的なリスク評価
⑭ 法規制の遵守
⑮ 監査実施・BCP計画・**患者教育**

これらの対策を総合的に実施することで、薬局における情報セキュリティリスクを大幅に軽減することができます。又、専門家によるセキュリティ監査を定期的に行い、セキュリティ体制の見直しと改善を継続することも重要です。**情報セキュリティは日々進化するため、常に最新の情報を得て対策を更新する必要があります。**

4-3. 調剤薬局における業務運用リスクポイントの考え方



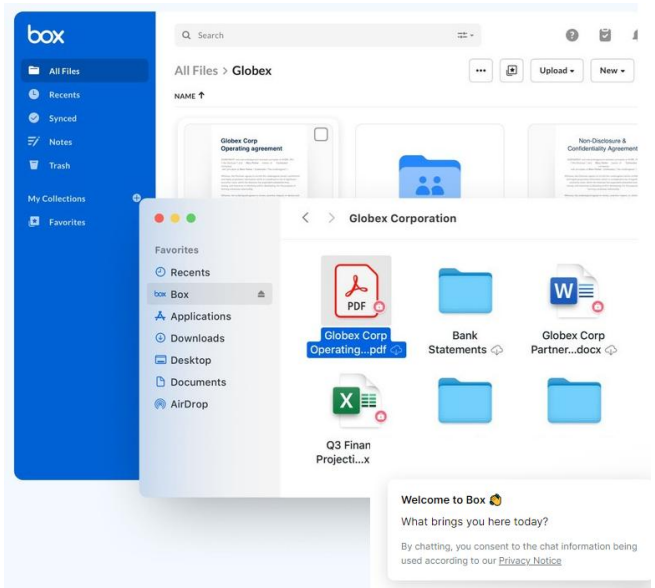
4-4. 家庭におけるインターネットリスクポイントの考え方



【参考】セキュアなクラウドバックアップ（クラウドサービスの選択基準）

ローカルドライブを解放し、デスクトップで業務を遂行

Box Driveは、クラウドに保存したあらゆるファイルをデスクトップから容易に操作する機能を提供します。貴重なローカルドライブの容量を消費することもありません。使い慣れたローカルドライブのユーザーインターフェースでファイルを選択し、ローカルのファイルと同様に編集。クラウドへの自動保存も可能です。ドキュメントを新規に作成する場合も、編集する場合も、変更は全てクラウドバックアップを通じてBoxに自動的に保存されます。オフライン時に加えた編集も後で自動的に反映されます。



セキュリティ
サーバーサイド暗号化、MFA、IAM、SSO、および独自のマルチユーザー認証機能を含む多層的なセキュリティでデータを保護します。

コンプライアンス
Wasabiは、SOC 2、ISO 27001、PCI-DSSの認定を受けたトップクラスのデータセンターでグローバルに展開しています。

イミュータビリティ（不変性）
Wasabi Object Lockを利用すると、設定した期間中はオブジェクトやストレージバケットの変更や削除ができなくなります。

予測可能なコスト
下り転送料金やAPIリクエストに追加のコストがかからず、請求額が予測できます。ハイパースケーラーとのコスト削減を比較してください。

【参考】日本の電波周波数割当表（皆さんが利用している電波の利用範囲）

周波数帯域（GHz）	名称	電波天文以外の主な用途
0.2 – 0.25 GHz	G バンド	公共業務（移動）・航空管制通信
0.25 – 0.5 GHz	P バンド	公共業務（移動）・航空管制通信・計画着陸システム（ILS）・アマチュア無線・特定小電力無線・公共/一般業務（固定・移動）
0.5 – 2.0 GHz	L バンド	テレビ放送（13 – 53 ch）・エリア放送・携帯電話・ITS・アマチュア無線・特定ラジオマイク・航空無線航行
2 – 4 GHz	S バンド	公共業務（固定・移動）・放送事業・移動衛星・各種レーダー・アマチュア無線・無線LAN等
4 – 8 GHz	C バンド	携帯電話・航空無線航行・ローカル5G・無線LAN・各種レーダー・放送事業（固定・移動）
8 – 12 GHz	X バンド	宇宙研究・地球探査衛星・航空無線航行・アマチュア無線・放送事業（固定・移動）・各種レーダー
12 – 18 GHz	Ku バンド	CS放送・電通業務（固定衛星）・各種レーダー・BS CSフィーダーリンク・公共業務（移動）
18 – 26 GHz	K バンド	電通業務（固定衛星）・無線アクセスシステム・公共/一般業務（固定）・各種レーダー・アマチュア無線・衛星間通信
26 – 40 GHz	Ka バンド	各種レーダー・携帯電話・ローカル５G・超広帯域無線システム
33 – 50 GHz	Q バンド	各種レーダー・公共/一般業務（固定・移動）・アマチュア無線・放送業務（移動）
40 – 75 GHz	V バンド	小電力データ通信システム等・放送事業（移動）・簡易無線・公共業務（移動）
75 – 111 GHz	W バンド	自動車レーダー（特定小電力）・アマチュア無線・放送事業（移動）

本日は長時間にわたる研修お疲れ様でした。