オンライン資格確認等システムの導入・運用に係る
セキュリティアセスメントに基づいたセキュリティ対策例

令和３年１月
厚生労働省保険局

甲第87号証

改定履歴

版数	改定年月	該当箇所	内容
1.0	令和２年１月	初版	初版作成
1.1	令和２年２月	脅威の洗い出し	文言の見直し（「資格確認書類」という記載をケースごとに「マイナンバーカード」「健康保険証」に書き分け）
1.2	令和３年１月	別紙（セキュリティ対策例一覧）	T13「使用できるUSB機器の制限を実施すること。」について、「最低限実施することが望ましい対策例」となっていたが、本紙との表記ゆれ（正しくは本紙記載の「実施することを推奨する対策例」）があったため修正
		脆弱性及び脆弱性レベルの定義	意図的脅威に対する脆弱性レベルの設定方法について、誤記があったため修正

目次

1. セキュリティアセスメント実施の目的
2. 本資料に関する告知事項
3. セキュリティアセスメントの進め方
4. セキュリティアセスメント結果
    ①セキュリティアセスメントの実施範囲の検討
    ②資産の洗い出し
    ③脅威の洗い出し
    ④セキュリティ対策の検討
        ④-1. リスクシナリオの定義
        ④-2. リスクシナリオごとのセキュリティ対策の検討
        ④-3. 最低限実施することが望ましい対策の抽出
        ④-4. セキュリティ対策の実装例

1. セキュリティアセスメント実施の目的

目的	本セキュリティアセスメントは、オンライン資格確認等システムの導入にあたって、医療機関・薬局及びシステムベンダが安全管理ガイドラインに沿って医療機関・薬局のセキュリティ対策を考える際の参考となるように、事前にセキュリティリスクの評価を行い、医療機関・薬局が実施すべきセキュリティ対策の実装例を示すことを目的としています。
前提条件	本セキュリティアセスメントは、以下の前提に基づき実施したものです。 • 医療機関・薬局の施設やレセプトコンピュータ等の既存設備、オンライン請求ネットワーク、オンライン資格確認等システムについては、各種ガイドライン（政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）、医療情報システムの安全管理に関するガイドライン第5版、レセプトのオンライン請求に係るセキュリティに関するガイドライン等）に基づいた適切なセキュリティ対策が講じられているものとします。 • 医療機関・薬局内部ネットワークは、「オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書　1.0版」に記載されている基本的な構成例（図２．３．２-２）に基づいてアセスメントを実施しています。 • セキュリティアセスメントは、ISO/IEC 27005（Information security risk management）に定められたプロセスの考え方に沿って実施します。 • 本セキュリティアセスメントで対象とする資産や脅威の洗い出しにあたっては、JAHIS発行の「リモートサービスセキュリティガイドライン」を参考にします。

参照資料

セキュリティアセスメントを実施するにあたり、アセスメント実施プロセスの定義やアセスメント対象の特定等のために、以下の関連資料を参照しました。

#	参照資料	発行元
1	ISO/IEC 27005 （Information security risk management）	国際標準化機構（ISO）、国際電気標準会議（IEC）
2	ISO/IEC 27002 （Code of practice for information security management）	国際標準化機構（ISO）、国際電気標準会議（IEC）
3	医療情報システムの安全管理に関するガイドライン 第5版	厚生労働省
4	リモートサービスセキュリティガイドラインVer.3.0	保健医療福祉情報システム工業会（JAHIS）
5	情報の格付け及び取扱制限に関する規程 策定手引書	内閣サイバーセキュリティセンター（NISC）
6	情報セキュリティ10大脅威 2019	情報処理推進機構（IPA）
7	ENISA Threat Landscape Report 2018	欧州ネットワーク・情報セキュリティ機関（ENISA）
8	オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書　1.0版	厚生労働省
9	別紙1_医療機関・薬局に係る業務フロー_v1.0	厚生労働省

2. 本資料に関する告知事項

本セキュリティアセスメントの結果に基づいたシステムの導入・運用についてのあらゆる障害や損害について、厚生労働省保険局は何らの責任を負わないものとします。

本セキュリティアセスメントにおいては、「オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書　1.0版」に記載されている基本的な構成例（図２．３．２-２）に基づいてアセスメントを行っていますので、それ以外の構成についてはアセスメントを行っていません。本セキュリティアセスメントが想定している構成とは異なる構成の場合、本セキュリティアセスメントの結果を流用することは可能ですが、全てをカバーできない可能性があります。この場合、各医療機関・薬局により、本セキュリティアセスメントに記載のないリスクについてアセスメントを行う必要があります。

本セキュリティアセスメントは、令和元年９月時点でのセキュリティに関する技術状況及び関連省庁等から提示されているガイドライン等に沿って実施しています。セキュリティに関する要求事項については、社会情勢の変化や技術の進歩等によって変わり得るものであり、 技術的・制度的変化が大きい場合には、リスク分析の手法や適用する対策等、本セキュリティアセスメントの結果を見直す必要が生じる場合もあります。このため、医療機関・薬局のセキュリティ対策を実施する際は、本書に記載のセキュリティ対策例を参考にしつつも、その時点でのセキュリティに関する技術状況や関連省庁等から提示されるガイドライン等を確認し、各医療機関・薬局の状況に合わせた最適な対策を講じる必要があります。

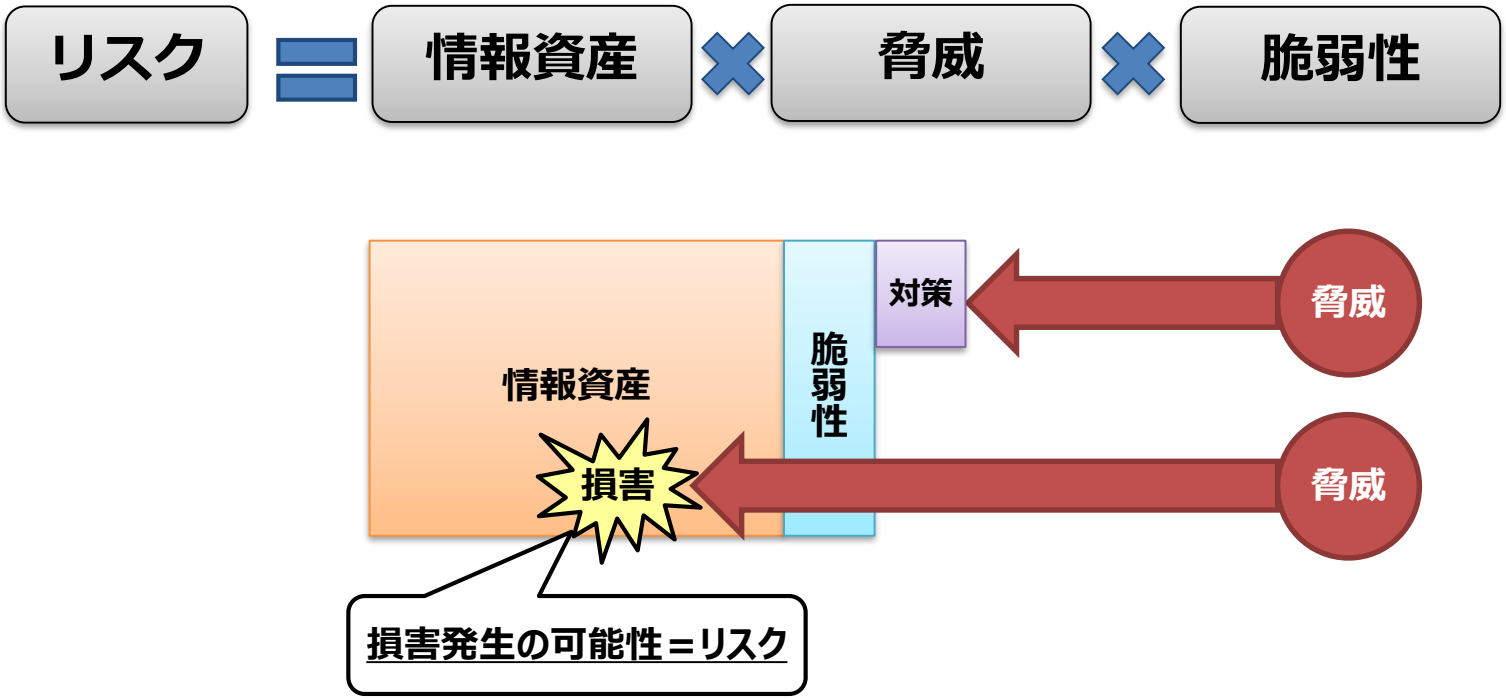
3. セキュリティアセスメントの進め方

本セキュリティアセスメントは、 ISO/IEC 27005（Information security risk management）に定められたプロセスの考え方に沿って、以下の4つのステップで進めます。
なお、オンライン資格確認等システムは、医療機関・薬局が遠隔地にあるサービスへ接続・利用するという、 参照資料「リモートサービスセキュリティガイドラインVer.3.0」のモデルと類似しているため、脅威や対策等の洗い出しの際には、リモートサービスセキュリティガイドラインを参考にします。

①セキュリティアセスメントの実施範囲の検討	• セキュリティアセスメントの実施範囲を明確にします。
②資産の洗い出し	• 決定した実施範囲に存在するセキュリティ上保護すべき資産（データ）の洗い出しを実施します。 • 洗い出した資産の特性に応じた、重要度の設定を行います。
③脅威の洗い出し	• 保護すべき資産に対して、具体的な攻撃手法等を想定して脅威の洗い出しを行います。
④セキュリティ対策の検討	• 脅威を防ぐために必要なセキュリティ対策を検討します。

（参考）本セキュリティアセスメントにおけるリスクの定義

情報セキュリティにおけるリスクとは、情報資産の弱点（脆弱性）をついて脅威が侵入し、情報資産へ損害や影響を発生させる可能性を指します。情報資産にどのような脅威や脆弱性があるかを明確にし、対策を講じることで情報資産における損害発生の可能性（＝リスク）を減らすことが可能となります。
本セキュリティアセスメントでは、情報資産及び資産に影響を与える可能性のある脅威を洗い出した上で、資産に対する脆弱性が存在している（＝対策が実施されていない）ものとし、医療機関・薬局がオンライン資格確認等システムの利用を開始するにあたって対策を講ずべきリスクを明確にします。

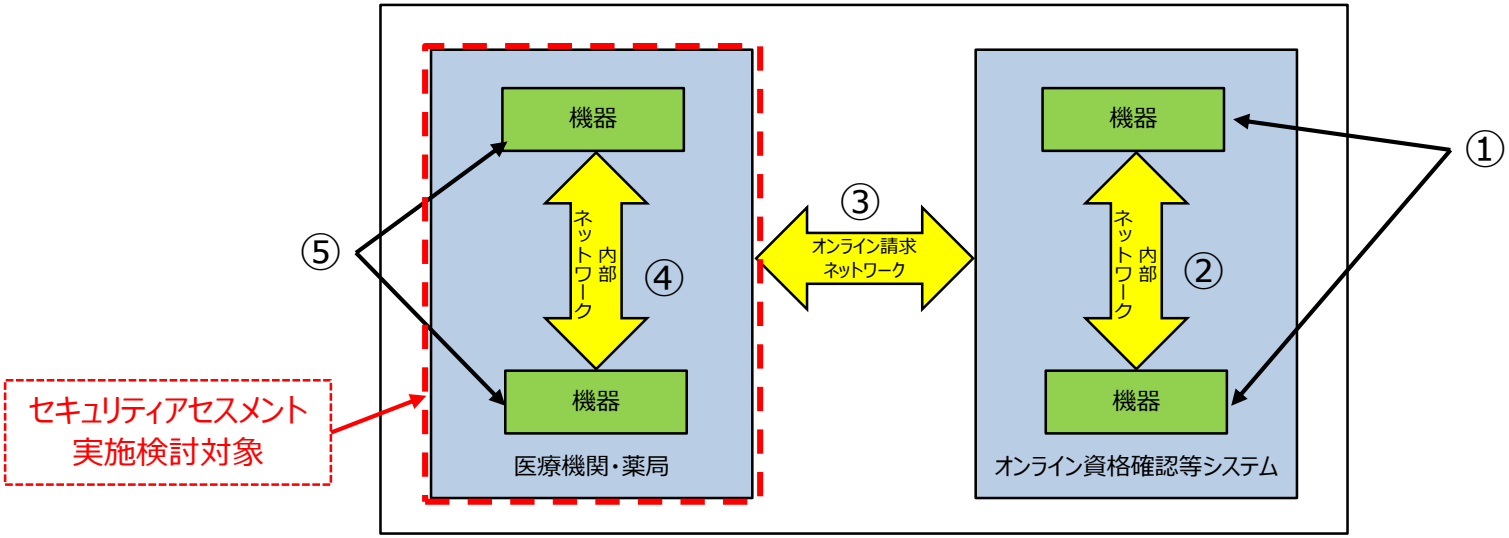


４．セキュリティアセスメント結果

①セキュリティアセスメントの実施範囲の検討

4. セキュリティアセスメント結果
①セキュリティアセスメントの実施範囲の検討（1/2）

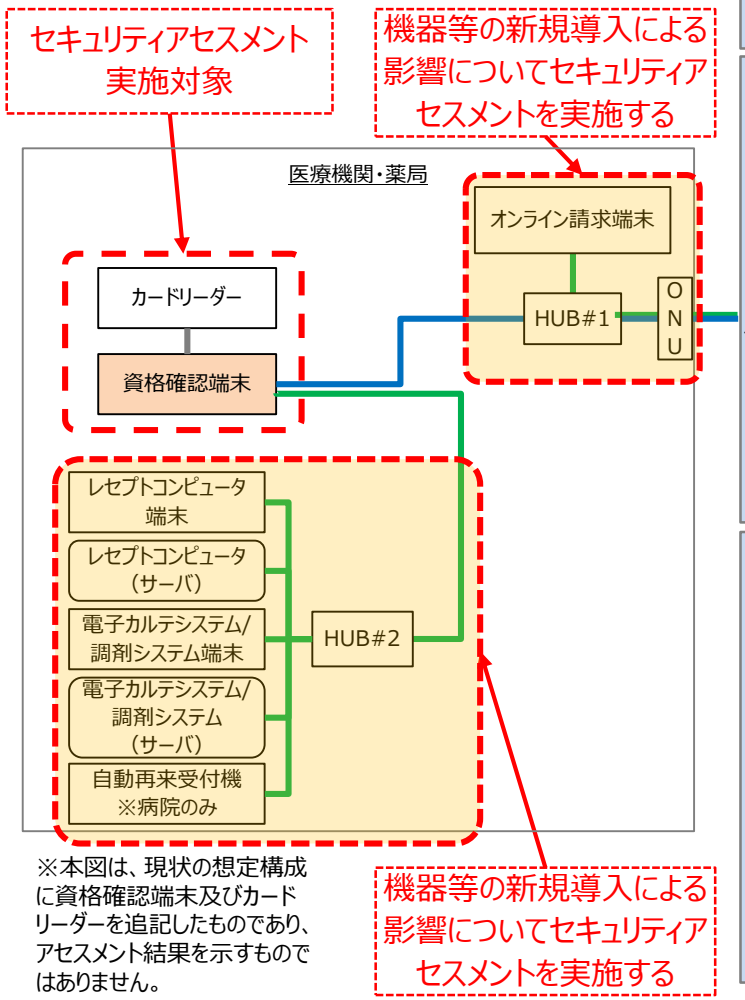
方針として、オンライン資格確認等システムの全体の構成を、リモートサービスセキュリティガイドラインに記載されている「リモートサービスのシステムの想定」を参考に5つに分類し、医療機関・薬局内部ネットワーク(④)及び機器(⑤)をセキュリティアセスメントの実施範囲とします。



#	オンライン資格確認等システムにおける構成要素	セキュリティアセスメント実施対象
①	オンライン資格確認等システム構成機器	対象外（オンライン資格確認等システム側で対応）
②	オンライン資格確認等システム内部ネットワーク	対象外（オンライン資格確認等システム側で対応）
③	オンライン請求ネットワーク	対象外（オンライン請求ネットワーク側で対応）
④	医療機関・薬局内部ネットワーク	対象（次ページで詳細を検討）
⑤	医療機関・薬局内保守対象機器	対象（次ページで詳細を検討）

4. セキュリティアセスメント結果
①セキュリティアセスメントの実施範囲の検討（2/2）

医療機関・薬局のおけるセキュリティアセスメントは、「オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書　1.0版」に記載されている基本的な構成例について、オンライン資格確認等システムの利用開始にあたって新規に導入する機器、それによって構成に変更が生じる機器及びネットワークを対象とします。



※本図は、現状の想定構成に資格確認端末及びカードリーダーを追記したものであり、アセスメント結果を示すものではありません。

構成要素	構成要素の詳細	アセスメント対象	補足
医療機関・薬局内保守対象機器	ONU	-	機器等の新規導入に伴う影響についてのみアセスメント対象とする
	オンライン請求端末	-	
	HUB#1	-	
	資格確認端末	対象	-
	カードリーダー	対象	-
	その他システム及び構成端末（レセプトコンピュータ端末等）	-	機器等の新規導入に伴う影響についてのみアセスメント対象とする
	HUB#2	-	
医療機関・薬局内ネットワーク	ONU～HUB#1	対象	ONUのインターフェースまでが対象となる（インターフェースは含まない）
	HUB#1～オンライン請求端末	-	機器等の新規導入に伴う影響についてのみアセスメント対象とする
	資格確認端末～HUB#1	対象	-
	資格確認端末～HUB#2	対象	-
	HUB#2～その他システム及び構成端末（レセプトコンピュータ端末等）	-	既存で十分なセキュリティ対策がなされている前提で、アセスメント対象外とする

4. セキュリティアセスメント結果

②資産の洗い出し

4. セキュリティアセスメント結果
②資産の洗い出し（1/3）

本セキュリティアセスメントの対象となる資産を、リモートサービスセキュリティガイドラインに記載の「資産の分類」を参考にして整理します。オンライン資格確認等システムの利用開始以前から存在している資産やプリントアウトした紙等については、既存でセキュリティ対策が実施されているものと想定して、アセスメントの対象外とします。

※セキュリティアセスメントの対象とする資産の詳細については、「別紙1．資産」参照。

資産分類1	資産分類2	資産詳細（例、「別紙1．資産」参照）	アセスメント対象
医療機関・薬局内保守対象機器	メモリ・ディスク・画面上のPHI※1	資格確認端末に記録された患者の資格情報等	対象
	暗号アルゴリズムと鍵と鍵配送方式	資格確認端末に記録されたオンライン資格確認等システム用暗号鍵等	対象
	メモリ・ディスク・画面上のPHI※1のメモやプリントアウトの紙	資格確認端末に記録された、患者の資格情報等のメモやプリントアウトの紙等	既存ガイドラインに従いセキュリティ対策をしている想定のため対象外とする
	メモリ・ディスク・画面上のPHI ※1のバックアップ媒体	資格確認端末に記録された、患者の資格情報等のバックアップディスク等	対象
	PHI※1を扱うソフトウェア	資格確認端末上で使用されるソフトウェア等	対象
	PHI※1を扱う機器	資格確認端末等	対象
	PHI※1を扱う機器の環境設備	資格確認端末が接続する電気系統等	既存ガイドラインに従いセキュリティ対策をしている想定のため対象外とする
	PHI※1を扱う操作者	資格確認業務を行う担当者等	既存ガイドラインに従いセキュリティ対策をしている想定のため対象外とする

※1 PHI：保護対象の医療情報（Protected Healthcare Information）

4. セキュリティアセスメント結果
②資産の洗い出し（2/3）

（つづき）

資産分類1	資産分類2	資産詳細（例、「別紙1. 資産」参照）	アセスメント対象
医療機関・薬局内ネットワーク	内部ネットワーク上のPHI※1	医療機関・薬局内部ネットワークを通信する、患者の資格情報等	対象
	上記通信トレースのメモやプリントアウトの紙	上記通信トレースのメモやプリントアウトの紙	メモ・紙へのプリントアウトは実施しない想定のため対象外とする
	上記通信トレースのバックアップ媒体	上記通信トレースのバックアップ媒体	バックアップ媒体は使用しない想定のため対象外とする
	ネットワーク機器のソフトウェア	医療機関・薬局内部ネットワークを構成するネットワーク機器のOS	対象
	ネットワーク機器	医療機関・薬局内部ネットワークを構成するネットワーク機器（ルータ、ハブ）	対象
	ネットワーク機器の環境設備	医療機関・薬局内部ネットワークを構成するネットワーク機器を格納するラック	既存ガイドラインに従いセキュリティ対策をしている想定のため対象外とする
	ネットワーク機器の操作者	医療機関・薬局内部ネットワークを構成するネットワーク機器の運用担当者	既存ガイドラインに従いセキュリティ対策をしている想定のため対象外とする
資格確認等業務固有の資産	資格確認書類	マイナンバーカード、健康保険証	対象
	メモリ・ディスク・画面上のオンライン資格確認等業務固有資産	資格確認端末内のメモリ等で一時的に保有するマイナンバーカード内の顔写真情報等	対象
	内部ネットワーク上のオンライン資格確認等業務固有資産	医療機関・薬局内部ネットワークを通信する利用者証明用電子証明書等	対象

※1 PHI：保護対象の医療情報（Protected Healthcare Information）

4. セキュリティアセスメント結果
②資産の洗い出し（3/3） - 重要度の設定

洗い出した資産について、参照資料「情報の格付け及び取扱制限に関する規程　策定手引書」を参考にして、資産ごとに機密性・完全性・可用性の3つの区分で評価を行い、3つの区分の評価の最大値をその資産の重要度として設定します。

※セキュリティアセスメントの対象とする資産の詳細及び設定した重要度については、「別紙1．資産」参照。

区分	重要度	基準
機密性	3	情報漏洩時の影響が大きく特別な管理が必要な、患者の個人情報、及び個人情報の流出につながる重要な資産 ハードウェア資産の場合、機密情報が確実に保存されている資産
	2	特定個人情報と同等程度に考えられるべき資産、情報漏洩によりサービスの提供に支障を及ぼすような資産（単体でデータの内容の意味が分かる情報、もしくはそれらの情報を保持する資産） ハードウェア資産の場合、機密情報が保存される可能性ある資産
	1	情報の漏洩によりサービスの提供に大きな影響を及ぼさないような資産（単体でデータの意味が分からない情報、もしくはそれらの情報を保持する資産） ハードウェア資産の場合、機密情報が保存されない資産
完全性	2	セキュリティ運用上重要な資産（ログなど）は、「2」とする。また、改ざん・破壊によりサービス提供に即時的に影響を及ぼす資産（容易に戻すことができない情報）
	1	改ざん・破壊によりサービス提供に即時的に影響を及ぼさない資産（容易に戻すことが可能な情報）
可用性	2	滅失、紛失によりサービス提供に即時的に影響を及ぼす資産（容易に戻すことができない情報）
	1	滅失、紛失によりサービス提供に即時的に影響を及ぼさない資産（容易に戻すことが可能な情報）

4. セキュリティアセスメント結果

③脅威の洗い出し

4. セキュリティアセスメント結果

③脅威の洗い出し - 脅威の定義と分類

脅威とは情報資産に対して危害を与える事象を指します。
ISO27002では、脅威を発生原因から「人為的脅威(意図的)」「人為的脅威(偶発的)」「環境的脅威」の３つに分類しており、本リスクアセスメントでは、この分類に基づいて脅威の洗い出しを行います。

脅威の分類		脅威の概要
人為的脅威	意図的脅威	人が意図して行う脅威。 何らかの意思を持った侵入者・攻撃者が組織の情報システムに侵入して情報を盗んだり、情報システムをコンピュータウイルスなどで攻撃して操作不能に陥れたりします。 例）不正アクセス、盗聴、改ざん、サービス妨害など
	偶発的脅威	人による意図せず起こる脅威。 操作ミスや設定ミスで情報システムに障害を引き起こします。 例）データの誤削除、データの大量アップロードなど
環境的脅威		脅威源が自然や環境による脅威。 地震や火災、停電などにより、情報システムが操作不能に陥る脅威です。 例）地震、落雷、故障など

4. セキュリティアセスメント結果

③脅威の洗い出し - 脅威の分類ごとの洗い出し方

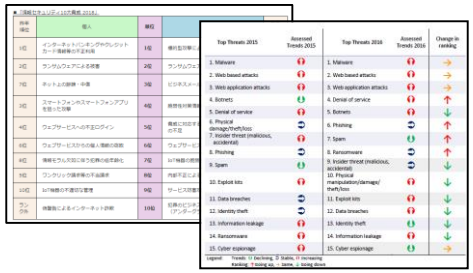
意図的脅威と偶発的脅威の洗い出し方法について以下に示します。

- 意図的脅威は、ガイドライン等の参照資料及び近年の脅威トレンドから洗い出す
- 偶発的脅威は、本システムにおける業務フローを参照し、業務の中で想定される偶発的脅威を洗い出す
- 環境的脅威は、「故障」及び「被災」の二通りとする

脅威の分類　　洗い出しの進め方

意図的脅威

参照資料・脅威トレンド



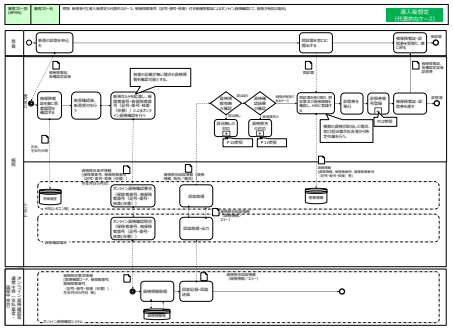
参照資料及び脅威トレンドから脅威を洗い出す

脅威

XX攻撃　●●攻撃　□□攻撃　○○攻撃　△△攻撃　▲▲攻撃

偶発的脅威

業務フロー



想定される誤操作や設定ミスを脅威として洗い出す

脅威

XXX　●●●　□□□　○○○　△△△　▲▲▲

環境的脅威

「故障」及び「被災」の二通りとする

4. セキュリティアセスメント結果
③脅威の洗い出し - 脅威レベルの設定

洗い出した脅威について、意図的脅威・偶発的脅威・環境的脅威のそれぞれで発生頻度・発生可能性に応じた脅威レベルを設定します。

脅威の分類		脅威レベル	基準
人為的脅威	意図的脅威	3	➢ 近い将来に発生することが予想される脅威 ➢ 対象システムのライフサイクル（使用期間）において、複数回の発生が想定される脅威
		2	➢ システムのライフサイクルにおいて、発生することが想定される脅威
		1	➢ 分析対象システムのライフサイクルにおいては、発生することが想定しがたい脅威
	偶発的脅威	3	1ヵ月に一度以上発生する可能性のある脅威
		2	1年に一度以上発生する可能性のある脅威
		1	3年以内に一度も発生しないと考えられる脅威
環境的脅威		3	1ヵ月に一度以上発生する可能性のある脅威
		2	1年に一度以上発生する可能性のある脅威
		1	3年以内に一度も発生しないと考えられる脅威

4. セキュリティアセスメント結果

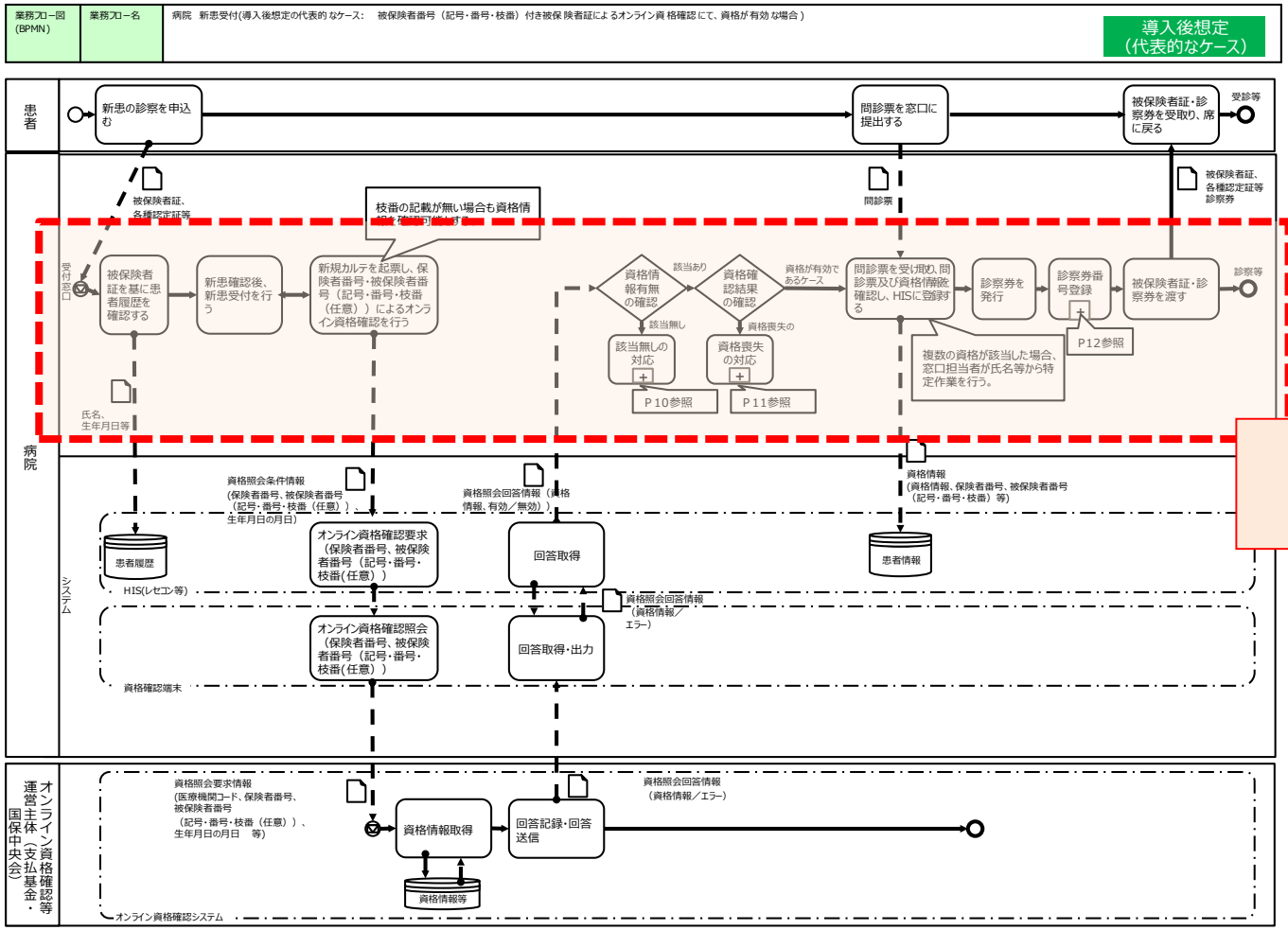
③脅威の洗い出し - 意図的脅威

意図的脅威は、参照資料「リモートサービスセキュリティガイドライン Ver.3.0（#4）」、「情報セキュリティ10大脅威 2019（#6）」、「ENISA Threat Landscape Report 2018（#7）」から本システムの構成をもとに11の脅威を洗い出し、前ページで定義した脅威レベルを設定しました。

No	意図的脅威	脅威の概要	参照資料 #4	参照資料 #6	参照資料 #7	脅威レベル
1	タッピングによる情報漏洩	ネットワークにタッピング装置等を不正に接続され、情報が漏洩する			●	2
2	タンパリングによる情報漏洩	機器が不正に改造（改ざん）され、情報が漏洩する	●		●	2
3	漏洩電磁波による情報漏洩	機器等から発生する電磁波を不正に解析され、情報が漏洩する			●	2
4	破壊によるサービス不能	機器等を物理的に破壊することで、サービスの提供を不能にする		●	●	2
5	不正ログイン/成りすましによる情報漏洩、改ざん	なりすまし等による不正ログインにより、情報が漏洩する又は情報が改ざんされる	●	●	●	2
6	バックドアや情報を盗み出すプログラムの挿入による情報漏洩	コンピュータウイルス等の不正プログラムにより、情報が漏洩する	●	●	●	2
7	情報を不正に暗号化するプログラムの挿入によるサービス不能	ランサムウェア等の不正プログラムにより、情報を不正に暗号化しサービスの提供を不能にする	●	●		2
8	暗号化データの解読による情報漏洩	暗号化されたデータを、権限のない悪意者が不正に解読し、情報が漏洩する			●	2
9	覗き見による情報漏洩	正当な権限を持った担当者等の行為を覗き見することで、情報が漏洩する			●	3
10	差換えによる改ざん	情報の不正な改ざん		●	●	2
11	持出/盗用による情報漏洩	機器等を不正に持ち出す又は機器等の盗難により、情報が漏洩する		●	●	3

4. セキュリティアセスメント結果
③脅威の洗い出し - 偶発的脅威の洗い出し（1/3）

「医療機関・薬局にかかる業務フロー」から、医療機関・薬局の担当者や患者が実施するアクションをユースケースとして抜き出し、各ユースケースで想定される偶発的な脅威を洗い出しました。



業務フローから一連のアクションをユースケースとして抜き出し、そのユースケースで想定される作業ミスや設定ミス等を偶発的脅威として定義する

Copyright © 2019 Accenture All rights reserved.

4. セキュリティアセスメント結果
③脅威の洗い出し - 偶発的脅威の洗い出し（2/3）

業務フローから洗い出した偶発的脅威を、以下に示します。
※業務フローは数が多く、重複する部分も多いため、似ている業務フローをカテゴライズした上で、ユースケースの洗い出しを実施。

#	カテゴリ（※）	ユースケース	偶発的脅威	脅威レベル
1	利用開始手続き	医療機関・薬局の窓口担当者が、患者の資格確認をマイナンバーカードを利用して行うための初回登録を行う	患者から誤ってマイナンバーカードを受け取り、カード裏面に記載されている個人番号（マイナンバー）を取得する	2
2			誤って患者の同意を得ずに資格確認を行い、資格情報の紐付けを行う	2
3			誤って患者自身のものとは異なるマイナンバーカードで資格確認を行い、異なる人物の資格情報の紐付けを行う（顔の似ている双子等）	2
4	受付（マイナンバーカード）	医療機関・薬局の窓口担当者が、患者の資格確認を行う	患者から誤ってマイナンバーカードを受け取り、カード裏面に記載されている個人番号（マイナンバー）を取得する	2
5			誤って券面写真の確認を行わずに資格確認を行い、資格情報を取得する（目視確認のケース）	2
6			誤って患者自身のものとは異なるマイナンバーカードで資格確認を行い、異なる人物の資格情報を取得する（顔の似ている双子等）	2
7	受付（健康保険証）	医療機関・薬局の窓口担当者が、患者の資格確認を行う	照会に必要な資格情報の入力内容に誤りがあり、異なる患者の資格情報を取得・閲覧する	2
8			誤って患者自身のものとは異なる健康保険証で資格確認を行い、異なる人物の資格情報を取得する	2
9	受付（処方せん）	薬局の窓口担当者が、患者の資格確認を行う	照会に必要な資格情報の入力内容に誤りがあり、異なる患者の資格情報を取得・閲覧する	2
10	照会番号（患者番号）登録	医療機関・薬局の窓口担当者が、照会番号（患者番号）の登録を行う	照会番号の入力内容に誤りがあり、異なる照会番号を登録する	2

4. セキュリティアセスメント結果
③脅威の洗い出し - 偶発的脅威の洗い出し（3/3）

（つづき）

※業務フローは数が多く、重複する部分も多いため、似ている業務フローをカテゴライズした上で、ユースケースの洗い出しを実施。

#	カテゴリ（※）	ユースケース	偶発的脅威	脅威レベル
11	医療機関コード変更	医療機関・薬局の職員が、医療機関コードの変更申請を行う	変更する医療機関コードの記入に誤りがあり、異なる医療機関コードに変更する	1
12		オンライン資格確認等システム運営主体職員が、医療機関コードの変更を行う	変更する医療機関コードの入力に誤りがあり、異なる医療機関コードに変更する	1
13	薬剤情報/特定健診情報閲覧	医療機関・薬局の窓口担当者が、患者の薬剤情報を閲覧する	同意の意思がなかったにもかかわらず、誤って患者が「同意」を押下してしまい、薬剤情報を取得する	2
14			患者の同意を得ずに薬剤情報を取得する	2
15		医師・薬剤師が、患者の薬剤情報を閲覧する	薬剤情報の照会要求情報に誤りがあり、異なる患者の薬剤情報を取得・閲覧する	2
16		医療機関の窓口担当者が、患者の特定健診情報を閲覧する	同意の意思がなかったにもかかわらず、誤って患者が「同意」を押下してしまい、特定健診情報を取得する	2
17			患者の同意を得ずに特定健診情報を取得する	2
18		医師が、患者の特定健診情報を閲覧する	特定健診情報の照会要求情報に誤りがあり、異なる患者の特定健診情報を取得・閲覧する	2
19	メンテナンス	システム保守担当者が各システム・各サーバに対して更新を行う	誤って異なるシステム・サーバを更新する	2
20			誤った設定内容で更新する	2
21			誤った更新操作を行い、システム・サーバを停止する	2

4. セキュリティアセスメント結果
③脅威の洗い出し - 脆弱性及び脆弱性レベルの定義

洗い出した脅威の一つ一つについて、脅威によって利用されるおそれのある脆弱性（情報システムの弱点）を定義します。また、脆弱性に対して、攻撃の難易度（攻撃者/行為者のスキル、攻撃実施可能な場所）に応じた脆弱性レベルを設定します。

※　一般的には、対策の実施状況に応じて脆弱性レベルを設定しますが、本セキュリティアセスメントは設計中のシステムに対する評価であることから、攻撃の難易度に置き換えて評価します。

※　意図的脅威に対する脆弱性は、「対象システムに物理的にアクセスすることによって攻撃可能」な場合は脆弱性レベル1とし、対象システムに（内部・外部に関わらず）ネットワーク経由での攻撃可能な場合は、攻撃者/行為者のスキルによって脆弱性レベルを設定するものとします。

脆弱性の分類		脆弱性レベル	基準	
			攻撃者/行為者のスキル	攻撃実施可能な場所
人為的脅威に対する脆弱性	意図的脅威に対する脆弱性	3	特別なスキルを持たない者が、公開されている情報を調査すれば攻撃可能	対象システムを外部ネットワークからリモートで攻撃可能
		2	専門能力を持つ者によって、攻撃可能	対象システムが属する内部ネットワークから攻撃可能
		1	高度な専門知識や設備を持つ者（国家レベルのサイバー攻撃者及びそれに準ずる団体）によってのみ攻撃可能	対象システムに物理的にアクセスすることによって攻撃可能
	偶発的脅威に対する脆弱性	3	専門能力がある者が注意していてもリスクが顕在化する恐れがある状況	-
		2	専門能力がある者が注意していればリスクが顕在化する恐れがない状況	-
		1	一般者が注意していればリスクが顕在化する恐れがない状況	-
環境的脅威に対する脆弱性		3	専門能力がある者が注意していてもリスクが顕在化する恐れがある状況	-
		2	専門能力がある者が注意していればリスクが顕在化する恐れがない状況	-
		1	一般者が注意していればリスクが顕在化する恐れがない状況	-

4. セキュリティアセスメント結果
③脅威の洗い出し - 脆弱性の定義（1/4）

脅威に対して想定しうる脆弱性を、以下に示します。

脅威の種類	脅威	脅威レベル	脆弱性	脆弱性レベル
意図的脅威	タッピングによる情報漏洩	2	対象機器の設置エリアへのアクセスを制限していない	1
			対象機器へのアクセスを制限していない（施錠できるラック内に設置する等）	1
			対象機器自体や機器内部へのアクセスを制限していない（機器接続など）	1
	タンパリングによる情報漏洩	2	対象機器の設置エリアへのアクセスを制限していない	1
			対象機器へのアクセスを制限していない（施錠できるラック内に設置する等）	1
			対象機器自体や機器内部へのアクセスを制限していない（機器接続など）	1
	漏洩電磁波による情報漏洩	2	対象機器へのアクセスを制限していない（道路からの距離など）	1
	破壊によるサービス不能	2	対象機器の設置エリアへのアクセスを制限していない	1
			対象機器へのアクセスを制限していない（施錠できるラック内に設置する等）	1
			対象機器自体や機器内部へのアクセスを制限していない（機器接続など）	1
	不正ログイン/成りすましによる情報漏洩、改ざん	2	想定しない手段によるアクセスを制限していない	1
			ユーザの認証を行っていない	3
			認証用ID、パスワードが漏洩している	3
			辞書攻撃等の認証対策ができていない	2
			対象ファイルが暗号化されておらず、誰でも読み取り可能な状態にある	2
			対象ファイルへ誰でもアクセス可能な状態である	2
			本番環境内に個人情報を含むテストデータが残存している	2

4. セキュリティアセスメント結果
③脅威の洗い出し - 脆弱性の定義（2/4）

（続き、意図的脅威）

脅威の種類	脅威	脅威レベル	脆弱性	脆弱性レベル
意図的脅威	バックドアや情報を盗み出すプログラムの挿入による情報漏洩	2	外部からの不審なプログラムファイルの持ち込みを制限していない	3
			セキュリティパッチが適用されず、不審なプログラムファイルが悪用する脆弱性が放置されている	3
			不審なプログラムファイルによるアクセスを制限していない	2
			不審なプログラムファイルが拡散するために悪用する仕組み（ファイル共有等）が不必要に有効になっている	2
	情報を不正に暗号化するプログラムの挿入によるサービス不能	2	外部からの不審なプログラムファイルの持ち込みを制限していない	3
			セキュリティパッチが適用されず、不審なプログラムファイルが悪用する脆弱性が放置されている	3
			不審なプログラムファイルによるアクセスを制限していない	2
			不審なプログラムファイルが拡散するために悪用する仕組み（ファイル共有等）が不必要に有効になっている	2
	暗号化データの解読による情報漏洩	2	データ保護に使用する暗号強度が低い	2
			通信に使用する暗号強度が低い	2
			無線LANの暗号化設定等に不備がある	3
	覗き見による情報漏洩	3	対象機器の設置エリアへのアクセスを制限していない	1
			対象機器の画面が誰でも覗き見られる状態にある	1
	差換えによる改ざん	2	対象ファイルが暗号化されておらず、誰でも読み取り可能な状態にある	2
			対象ファイルへ誰でもアクセス可能な状態である	2
			対象ファイルの変更を制限していない	2
	持出/盗用による情報漏洩	3	対象機器の設置エリアへのアクセスを制限していない	1
			対象機器へのアクセスを制限していない（施錠できるラック内に設置する等）	1
			対象機器自体や機器内部へのアクセスを制限していない（機器接続など）	1

4. セキュリティアセスメント結果
③脅威の洗い出し - 脆弱性の定義（3/4）

（続き、偶発的脅威）

脅威の種類	カテゴリ	脅威	脅威レベル	脆弱性	脆弱性レベル
偶発的脅威	利用開始手続き	患者から誤ってマイナンバーカードを受け取り、券面（裏）に記載されている個人番号（マイナンバー）を取得する	3	提出書類の物理的な受け渡しを制限していない	1
		誤って患者の同意を得ずに資格確認を行い、資格情報を取得する	2	同意取得の有無を検知していない	1
		誤って患者自身のものとは異なるマイナンバーカードで資格確認を行い、異なる人物の資格情報を取得する（顔の似ている双子等）	2	提出書類の誤りを検知していない	1
	受付（マイナンバーカード）	患者から誤ってマイナンバーカードを受け取り、券面（裏）に記載されている個人番号（マイナンバー）を取得する	3	提出書類の物理的な受け渡しを制限していない	1
		誤って券面写真の確認を行わずに資格確認を行い、資格情報を取得する（目視確認のケース）	2	目視確認の際に、券面写真を適切に確認することを担当者に徹底していない	1
		誤って患者自身のものとは異なるマイナンバーカードで資格確認を行い、異なる人物の資格情報を取得する（顔の似ている双子等）	2	提出書類の誤りを検知していない	1
	受付（健康保険証）	照会に必要な資格情報の入力内容に誤りがあり、異なる患者の資格情報を取得・閲覧する	2	入力内容の誤りを検知していない	1
		誤って患者自身のものとは異なる健康保険証で資格確認を行い、異なる人物の資格情報を取得する	2	提示された健康保険証が、本人のものか確認を行っていない	2
	受付（処方せん）	照会に必要な資格情報の入力内容に誤りがあり、異なる患者の資格情報を取得・閲覧する	2	入力内容の誤りを検知していない	1
	照会番号（患者番号）登録	照会番号の入力内容に誤りがあり、異なる照会番号を登録する	2	入力内容の誤りを検知していない	1

4. セキュリティアセスメント結果
③脅威の洗い出し - 脆弱性の定義（4/4）

（続き、偶発的脅威及び環境的脅威）

脅威の種類	カテゴリ	脅威	脅威レベル	脆弱性	脆弱性レベル
偶発的脅威	医療機関コード変更	変更する医療機関コードの記入に誤りがあり、異なる医療機関コードに変更する	1	入力内容の誤りを検知していない	1
		変更する医療機関コードの入力に誤りがあり、異なる医療機関コードに変更する	1	入力内容の誤りを検知していない	1
	薬剤情報照会	患者の同意を得ずに薬剤情報を取得する	2	同意取得の有無を検知していない	0
		薬剤情報の照会要求内容に誤りがあり、異なる患者の薬剤情報を取得・閲覧する	2	入力内容の誤りを検知していない	1
		同意の意思がなかったにもかかわらず、誤って患者が「同意」を押下してしまい、薬剤情報を取得する	3	「同意」ボタンを押すことによる影響について、患者への周知が十分でない	1
	特定健診情報照会	患者の同意を得ずに特定健診情報を取得する	2	同意取得の有無を検知していない	0
		同意の意思がなかったにもかかわらず、誤って患者が「同意」を押下してしまい、特定健診情報を取得する	3	「同意」ボタンを押すことによる影響について、患者への周知が十分でない	1
		特定健診情報の照会要求内容に誤りがあり、異なる患者の特定健診情報を取得・閲覧する	2	入力内容の誤りを検知していない	1
	メンテナンス	誤って異なるシステム・サーバを更新する	1	更新対象サーバの誤りを検知していない	2
		誤った設定内容で更新する	1	更新内容の誤りを検知していない	2
		誤った更新操作を行い、システム・サーバを停止する	1	更新内容の誤りを検知していない	2
環境的脅威		故障によるサービス不能	1※	落下して破損する可能性のある場所やホコリ、振動等によって故障しやすい場所に設置されている	3
		故障によるサービス不能	1※	故障時の対応が用意されていない	2
		被災によるサービス不能	1	被災時の対応が用意されていない	2

※一部の資産（患者が直接触れる可能性のあるカードリーダー）については故障の発生頻度が高いと想定し、脅威レベル2とする。詳細は別紙3参照。

4. セキュリティアセスメント結果
③脅威の洗い出し - 資産と意図的脅威のマッピング

ここまでに洗い出した対象資産及び脅威（意図的脅威、偶発的脅威、環境的脅威）について、資産に影響を与える可能性のある脅威をマッピングします。

資産				脅威																															
高位区分1	高位区分2	高位詳細	PHI	意図的脅威											偶発的脅威																	環境的脅威	
				意図的脅威											不正利用			受付（マイナンバーカード）			受付（被保険者証）		受付（処方箋）											
				ウィピングによる盗聴に	ランサムウェアによる改ざん、暗号化	偽造電磁波によるなりすまし、暗号化	偽造メールによるサービス不能化	不正なログインにより改ざん、なりすまし	バックドアや情報を盗みのためのプログラムを埋め込むことによる暗号化	情報を不正に取得化するプログラムを埋め込むサービス不能化	暗号化データ・ランサムによる暗号化	他者用にによる暗号化、なりすまし	悪意入れによるなりすまし、暗号化	改ざんにより暗号化、なりすまし	患者から誤ってマイナンバーカードを受け取り、無断に記載されている個人情報を取得する	誤って患者の同意を得ずに資格確認を行い、資格情報を取得する	誤って患者自身のために資格確認書類で資格情報を行い、資格情報を取得する	患者から誤ってマイナンバーカードを受け取り、無断に記載されている個人情報を取得する	誤って患者の同意を得ずに資格情報を行い、資格情報を取得する	誤って患者自身のために資格確認書類で資格情報を行い、資格情報を取得する	保険者情報の入力内容に誤りがあり、異なる患者の資格情報を取得・閲覧する	保険者情報の入力内容に誤りがあり、異なる患者の資格情報を取得・閲覧する	照会番号（患者番号）の入力内容に誤りがあり、異なる患者の資格情報を取得する	医療機関コード変更を誤って医療機関コードを変更する	変更する医療機関コードを入力に誤りがあり、異なる医療機関コードを変更する	特定健診情報照会に誤って患者の同意を得ずに特定健診情報を取得する	特定健診情報の取得内容に誤りがあり、異なる患者の特定健診情報を取得・閲覧する	薬剤情報照会に患者の同意を得ずに薬剤情報を取得する	薬剤情報の取得内容に誤りがあり、異なる患者の薬剤情報を取得・閲覧する	メンテナンス誤って異なるシステムサーバを更新する	誤った内容で更新する	誤って更新操作を行い、システムサーバを停止する	故障によりサービス不能化	地震によりサービス不能化
医療機関・薬局内 論理分離機器	JPKI-ディバス-高速上のPHEIII1	保険情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	○	○	–	–	–	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–
		被保険者情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	○	○	–	–	–	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–
		個人単位被保険者情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		高齢者受給者証情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		限度額適用認定証関連情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		限度額適用・標準負担額減額認定証情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		特定疾病療養受療証情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		医療機関コード	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–
		処方箋	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–
		照会番号	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–
		特定健診情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–
		薬剤情報	対象	–	–	–	–	–	–	○	○	○	○	○	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–
	ネットワーク機器のソフトウェア	既存院内システム用ネットワーク機器（CNU、HUB#1、HUB#2、無線LAN機器）用ソフトウェア		–	–	–	–	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	○	○	○	–	–
	ネットワーク機器	CNU	-	○	○	○	○	○	○	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	○	○	○	○	○
		HUB#1	-	○	○	○	○	○	○	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	○	○	○	○	○
		HUB#2	-	○	○	○	○	○	○	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	○	○	○	○	○
		無線LAN機器	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	○	○	○	–	–
患者	高機能認証端	マイナンバーカード	-	–	–	–	–	–	–	–	–	○	○	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	JPKI-ディバス-高速上の オンライン資格確認業務窓口の資産	被保険者証	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		マイナンバーのシリアル番号	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		マイナンバーの認証鍵情報	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		マイナンバーの利用者証明用電子証明書	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		マイナンバーの失効	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		CRLの上位写真情報	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		検証機関証明用電子証明書	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	HCPエリア内部ネットワーク上の オンライン資格確認業務窓口の資産	マイナンバーのシリアル番号	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		マイナンバーの利用者証明用電子証明書	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		検証機関証明用電子証明書	-	–	–	–	–	–	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

詳細は、「別紙2. 資産と脅威のマッピング」を参照

4. セキュリティアセスメント結果

④セキュリティ対策の検討

4. セキュリティアセスメント結果
④情報セキュリティ対策の検討

洗い出した資産、脅威、脆弱性に基づいて定義したリスクシナリオごとに、参照資料「医療情報システムの安全管理に関するガイドライン　第5版」や「リモートサービスセキュリティガイドラインVer.3.0」等を参考にして、有効と考えられるセキュリティ対策例を検討します。

「情報セキュリティ対策の検討」の進め方	各ステップの説明
④-1. リスクシナリオ・リスク評価値の定義	• 洗い出した資産、脅威及び脆弱性から、リスクシナリオを定義し、資産、脅威及び脆弱性の評価からリスク評価値を算出します
④-2. 対策を実施すべきリスクシナリオの抽出	• 定義したリスクシナリオに対して、医療機関・薬局の状況や費用の制約等を踏まえ、 算出したリスク評価値に基づいて対策を実施すべきリスクシナリオを抽出します
④-3. リスクシナリオごとのセキュリティ対策例の検討	• 対策を実施すべきリスクシナリオに対して、「医療情報システムの安全管理に関するガイドライン」や「リモートサービスセキュリティガイドライン」等を参考にし、有効と考えられるセキュリティ対策の例を検討します
④-4. セキュリティ対策実施によるリスク評価値の低下	• 対策を実施することによって、リスク評価値がどの程度低下するかを算出します
④-5. セキュリティ対策の実装例	• 策定したセキュリティ対策例について、基本的な構成における実装例を策定します

4. セキュリティアセスメント結果
④-1. リスクシナリオ・リスク評価値の定義

ここまでに洗い出した情報資産、脅威、脆弱性からリスクシナリオを定義します。
また、情報資産の重要度、脅威レベル、脆弱性レベルを掛け合わせ、リスク評価値を算出します。
※リスクシナリオ及びリスク評価値の詳細は、「別紙3. リスクシナリオ及び対策」を参照。

情報資産

メモリ・ディスク・画面上のPHI	重要度：3

×

脅威

情報を不正に暗号化するプログラムの挿入によるサービス不能	脅威レベル：2

×

脆弱性

外部からの不審なプログラムファイルの持ち込みを制限していない	脆弱性レベル：3

＝

リスクシナリオ

PHIを保有している機器で、情報を不正に暗号化するプログラムが実行され、PHIが利用できなくなる	リスク評価値：18

4. セキュリティアセスメント結果
④-2. 対策を実施すべきリスクシナリオの抽出

リスクシナリオの内、資産の重大度、脅威レベル、脆弱性レベルから算出されるリスク評価値が高いリスクシナリオに対してセキュリティ対策を検討します。
実施すべき対策は、各医療機関・薬局の対策実施状況に応じて異なるため、本セキュリティアセスメントでは、リスク評価値の最大値に対して上から1/3のラインで線を引いていますが、どこに線を引くかは各医療機関・薬局でご判断が必要です。

資産の重大度	1			2			3		
脅威レベル / 脆弱性レベル	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27

対策を実施すべきリスクシナリオとして抽出

4. セキュリティアセスメント結果
④-3. リスクシナリオごとのセキュリティ対策例の検討（1/4）

参照資料「医療情報システムの安全管理に関するガイドライン　第5版」や「リモートサービスセキュリティガイドラインVer.3.0」を参考にし、本システムの特性等を考慮して、リスクシナリオに対して有効と考えられる対策の例を、「技術的対策(T)」「物理的対策(P)」「人的/組織的対策(H)」「その他のシステムにて実施する対策(A)」の４分類で策定します。
また、策定したセキュリティ対策を、以下の2つに分類します。

対策の分類	説明
最低限実施することが望ましい対策例	リスク評価値を許容できる値まで下げるために必要な対策。複数の対策がある場合は、すべての実施が必要。
実施することを推奨する対策例	必須の対策ではないが、セキュリティ強化のために実施することを推奨する対策

策定したセキュリティ対策の例を、以下に示します。
※リスクシナリオに対するセキュリティ対策の詳細は、「別紙3. リスクシナリオ及び対策」を参照。

リスクシナリオ

PHIを保有している機器で、情報を不正に暗号化するプログラムが実行され、PHIが利用できなくなる

セキュリティ対策例

【最低限実施することが望ましい対策例】
T11: IPsec+IKEの利用や閉域網の利用等、ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。
T17: ファイアウォールやルータのステートフルパケットインスペクション機能を用いて、外部ネットワークからのアクセスを制限すること。
T18: セキュリティ要件の異なるシステム間や安全管理上の重要部分との境界にはファイアウォール等を設置し、ネットワークを物理的もしくは論理的に分割すること。
H12: システム構築時や外部からの情報受領時には、ウイルス等の不正なソフトウェアが混入していないか確認すること。
A01: IPsec事業者等において、医療機関等間における通信を制限すること。

【実施することを推奨する対策例】
H16: ルータ等のネットワーク機器は、信頼できるベンダ（ISO/IEC15408の認証取得等）が用意するもの等、安全性が確認できる機器を利用すること。

4. セキュリティアセスメント結果
④-3. リスクシナリオごとのセキュリティ対策例の検討（2/4）

凡例
○：最低限実施することが望ましい対策
△：最低限実施することが望ましい対策の内、既に実施済と考えられる対策

検討したセキュリティ対策例を、対策の種別ごとに示します。
※なお、リスク評価値の低いリスクシナリオに対するセキュリティ対策についても、参考情報として、「別紙3. リスクシナリオ及び対策」に記載。

通番	対策番号	対策例	対策種別			最低限実施することが望ましい対策例
			技術的対策	物理的対策	人的/組織的対策	
1	T02	情報システムへのアクセスにおける利用者の識別と認証を行うこと。	●	-	-	○
2	T07	認証に用いられる手段としては2要素認証や生体認証、複雑で長いパスワード等、より認証強度が高い方式を採用すること。	●	-	-	-
3	T11	IPsec+IKEの利用や閉域網の利用等、ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。	●	-	-	△
4	T12	一般に公開された脆弱性に対処するため、診療に影響が出ない範囲でOSのセキュリティパッチを適切に適用すること。	●	-	-	○
5	T13	使用できるUSB機器の制限を実施すること。	●	-	-	○
6	T15	ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	●	-	-	○
7	T17	ファイアウォールやルータのステートフルパケットインスペクション機能を用いて、外部ネットワークからのアクセスを制限すること。	●	-	-	○
8	T18	セキュリティ要件の異なるシステム間や安全管理上の重要部分との境界にはファイアウォール等を設置し、ネットワークを物理的もしくは論理的に分割すること。	●	-	-	○
9	T19	実行可能なアプリケーションをホワイトリスト方式で制限すること。	●	-	-	-
10	T20	無線LANを導入する場合は、以下の対策を実施すること。 ・ステルスモード、ANY 接続拒否等の対策を行い、利用者以外に無線LANの利用を特定されないようにすること ・MACアドレスやクライアント証明書によるアクセス制限を行うこと。 ・WPA2/AES等により、通信を暗号化し情報を保護すること。	●	-	-	○

4. セキュリティアセスメント結果
④-3. リスクシナリオごとのセキュリティ対策例の検討（3/4）

凡例
○：最低限実施することが望ましい対策
△：最低限実施することが望ましい対策の内、既に実施済と考えられる対策

（続き、人的/組織的対策）

通番	対策番号	対策例	対策種別			最低限実施することが望ましい対策例
			技術的対策	物理的対策	人的/組織的対策	
11	H03	メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を特定できる情報を含む作業記録を残すこと（ただし、個人情報そのものを作業記録に記載しないこと）。	-	-	●	-
12	H08	個人情報、及び重要情報の思わぬ漏洩を防ぐため、運用方法について従業員に十分な周知を行うこと。	-	-	●	○
13	H09	個人情報の思わぬ漏洩を防ぐため、運用方法について患者に十分な周知を行うこと。	-	-	●	○
14	H10	本人の識別・認証にユーザID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つようにすること。	-	-	●	△
15	H12	システム構築時や外部からの情報受領時には、ウイルス等の不正なソフトウェアが混入していないか確認すること。	-	-	●	△
16	H13	2要素認証を採用している場合を除き、パスワードは定期的に変更すること。（最長でも2 ヶ月以内に変更する）	-	-	●	△
17	H14	類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。極端に短い文字列を使用しないこと。	-	-	●	△
18	H16	ルータ等のネットワーク機器は、信頼できるベンダ（ISO/IEC15408の認証取得等）が用意するもの等、安全性が確認できる機器を利用すること。	-	-	●	-
19	H21	本システムで取り扱う情報、本システム構成する機器・ソフトウェアをリストアップした上で重要度に応じた分類を行い、常にリストを最新の状態に維持すること。	-	-	●	△

4. セキュリティアセスメント結果
④-3. リスクシナリオごとのセキュリティ対策例の検討（4/4）

凡例
○：最低限実施することが望ましい対策
△：最低限実施することが望ましい対策の内、既に実施済と考えられる対策

（続き、オンライン資格確認等システムやオンライン請求ネットワークにて実施する対策）

通番	対策番号	対策例	対策種別			最低限実施することが望ましい対策例
			技術的対策	物理的対策	人的/組織的対策	
20	A01	IPsec事業者等において、医療機関・薬局間における通信を制限すること。	-	-	-	△

4. セキュリティアセスメント結果
④-4.セキュリティ対策実施によるリスク評価値の低下

前項までで検討したセキュリティ対策を実施することによって、対策を実施すべきとして抽出したリスクシナリオのリスク評価値がどの程度低下するかを算出します。
算出した結果は、「別紙3. リスクシナリオ及び対策」の「リスク評価（対策実施後）」列を参照。

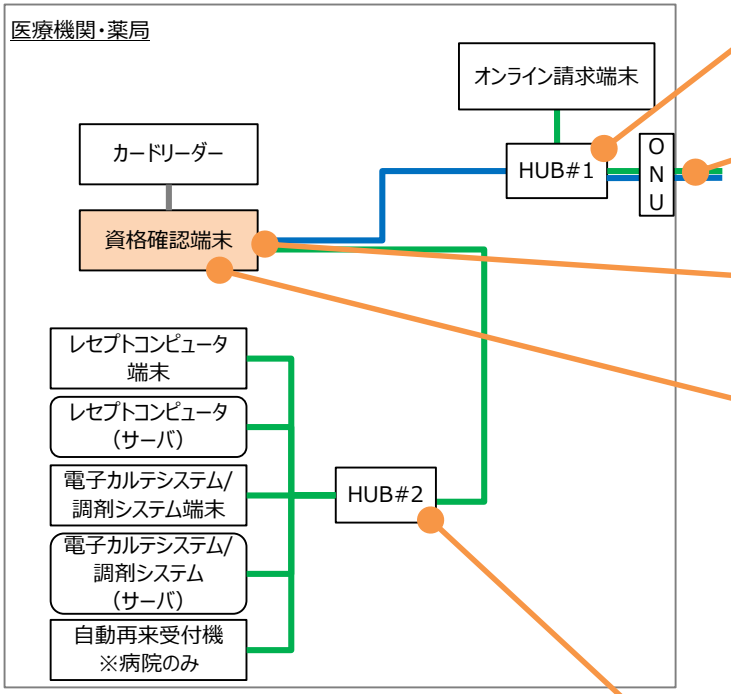
4. セキュリティアセスメント結果

④-5. セキュリティ対策の実装例

4. セキュリティアセスメント結果
④-5. セキュリティ対策の実装例 - 基本的な構成において想定される脅威

凡例
- IPv4での通信
- IPv6での通信

セキュリティ対策の実装例を示すにあたり、基本的な構成において想定される脅威を下図に示します。



ネットワーク
- ✓ **他の医療機関・薬局等からのアクセスが制限されておらず、バックドアや情報を盗み出すプログラムファイルが実行され、保有する情報が流出する**

ネットワーク
- ✓ **暗号化されていない回線等を利用しているため、ネットワーク経路でのメッセージ挿入、ウイルス混入等が行われる**

ネットワーク
- ✓ **IPv4とIPv6の通信が混在することで、ネットワークが不安定化し、可用性が低下する**

端末
- ✓ **ユーザ認証を行っていないために資格確認端末に不正ログインされ、保有する情報が改ざんまたは漏洩する**
- ✓ **セキュリティパッチが適用されず、不審なプログラムファイルが悪用する脆弱性が放置されているため、バックドアや情報を盗み出すプログラムファイルが実行され、保有する情報が流出する**
- ✓ **ウイルス対策ソフトウェアが導入されておらず、バックドアや情報を盗み出すプログラムファイルが実行され、保有する情報が流出する**

ネットワーク
- ✓ **資格確認端末から院内システムへのアクセスが制限されていないため、バックドアや情報を盗み出すプログラムファイルが院内システムに感染する**

ネットワーク
- ✓ **無線LANの設定に不備があり、暗号化された通信が傍受・解読され、PHIが流出する**

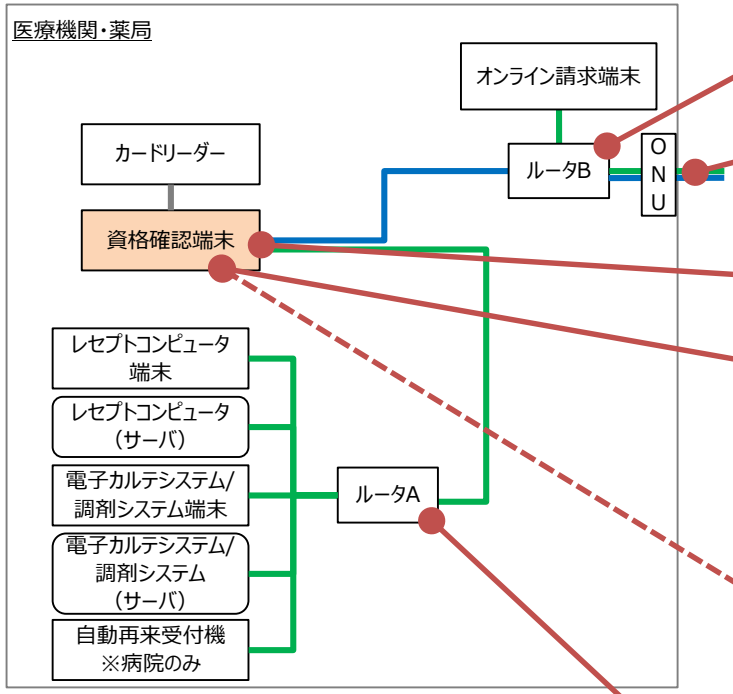
4. セキュリティアセスメント結果
④-5. セキュリティ対策の実装例（1/3）

凡例
- IPv4での通信
- IPv6での通信
- 最低限実施することが望ましい対策
- 実施することを推奨する対策

基本的な構成において想定される脅威を踏まえ、前項までで洗い出したセキュリティ対策の内、技術的対策の実装例を示します。

IP-VPNの場合

➢ 前提：IP-VPNを使用してオンライン請求を実施していること。または、独立したオンライン請求端末を用いてオンライン請求を実施する予定であること。



ネットワーク
- ✓ **T17: ルータBの導入（PPPoEパススルー設定が必要）、ステートフルインスペクション機能の有効化**

ネットワーク
- ✓ **T11: IP-VPN（閉域網）の利用**

ネットワーク
- ✓ **T18: 資格確認端末へのNIC2枚差し等による通信経路の物理的な分離**

端末
- ✓ **T02: 利用者の認証、複雑なパスワードの設定**
- ✓ **T12: Windowsのセキュリティパッチの定期的な適用**
- ✓ **T15: ウイルス対策ソフトウェアの導入**

端末
- ✓ **T07: 2要素認証や生体認証、複雑で長いパスワードの導入**
- ✓ **T13: 使用できるUSB機器の制限**
- ✓ **T19: 実行可能なアプリケーションをホワイトリスト方式で制限する**

ネットワーク
- ✓ **T18: ルータAの導入、不必要な通信（資格確認端末からレセコン等への通信）の拒否**

ネットワーク
- ✓ **T20: 無線LANのセキュリティ対策（無線LANを使用する場合）**

（SSIDのステルス化、Any接続拒否、MACアドレスやクライアント証明書等によるアクセス制限、WPA2/3による暗号化）

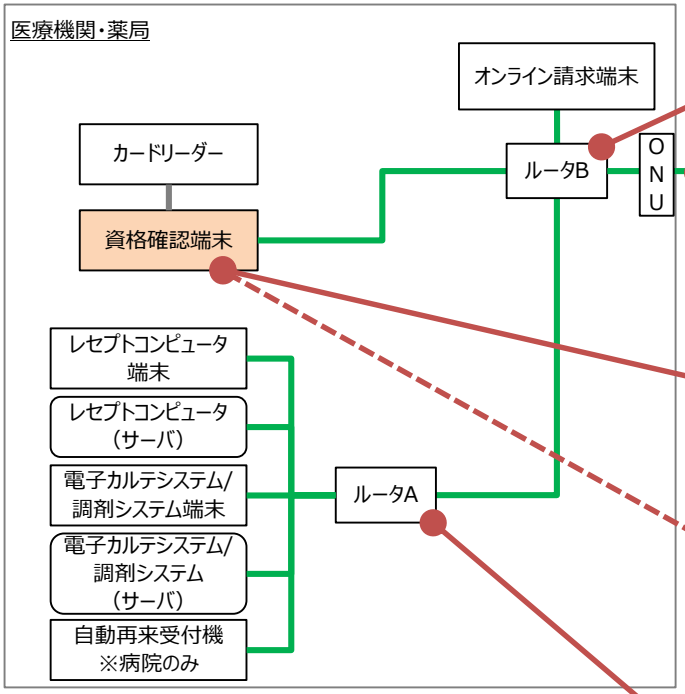
4. セキュリティアセスメント結果
④-5. セキュリティ対策の実装例（2/3）

凡例
- IPv4での通信
- IPv6での通信
- 最低限実施することが望ましい対策
- 実施することを推奨する対策

（続き）

IPsec（ルータ型）の場合

- IPsecを使用してオンライン請求を実施していること。または、独立したオンライン請求端末を用いてオンライン請求を実施する予定であること。
- 既にルータBに相当するものが導入されており、ステートフルインスペクション機能等により外部ネットワークからのアクセスが制限されていること。



ネットワーク
- ✓ **T17: ルータBでのステートフルインスペクション機能の有効化**

ネットワーク
- ✓ **T11: IPsec+IKEの利用**

端末
- ✓ **T02: 利用者の認証**
- ✓ **T12: Windowsのセキュリティパッチの定期的な適用**
- ✓ **T15: ウイルス対策ソフトウェアの導入**

端末
- ✓ **T07: 2要素認証や生体認証、複雑で長いパスワードの導入**
- ✓ **T13: 使用できるUSB機器の制限**
- ✓ **T19: 実行可能なアプリケーションをホワイトリスト方式で制限する**

ネットワーク
- ✓ **T18: ルータAの導入、不必要な通信（資格確認端末からレセコン等への通信）の拒否**

ネットワーク
- ✓ **T20: 無線LANのセキュリティ対策（無線LANを使用する場合）**
  （SSIDのステルス化、Any接続拒否、MACアドレスやクライアント証明書等によるアクセス制限、WPA2/3による暗号化）

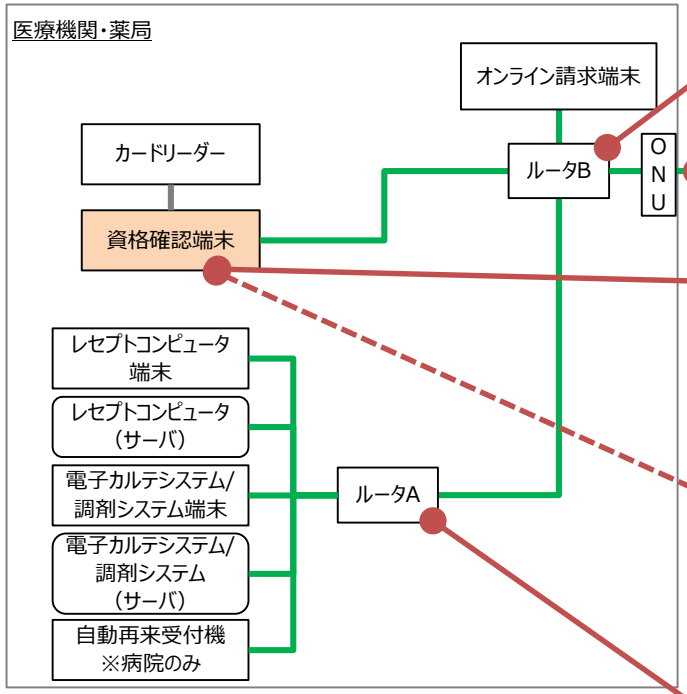
4. セキュリティアセスメント結果
④-5. セキュリティ対策の実装例（3/3）

凡例
- IPv4での通信
- IPv6での通信
- 最低限実施することが望ましい対策
- 実施することを推奨する対策

（続き）

IPsec（クライアント型/PCキー型/USBキー型）の場合

➢ IPsecを使用してオンライン請求を実施していること。または、独立したオンライン請求端末を用いてオンライン請求を実施する予定であること。



ネットワーク
- ✓ **T17: ルータBの導入（導入されていない場合に導入。VPNパススルー設定が必要）、ステートフルインスペクション機能の有効化**

ネットワーク
- ✓ **T11: IPsec+IKEの利用**

端末
- ✓ **T02: 利用者の認証**
- ✓ **T12: Windowsのセキュリティパッチの定期的な適用**
- ✓ **T15: ウイルス対策ソフトウェアの導入**

端末
- ✓ **T07: 2要素認証や生体認証、複雑で長いパスワードの導入**
- ✓ **T13: 使用できるUSB機器の制限**
- ✓ **T19: 実行可能なアプリケーションをホワイトリスト方式で制限する**

ネットワーク
- ✓ **T18: ルータAの導入、不必要な通信（資格確認端末からレセコン等への通信）の拒否**

ネットワーク
- ✓ **T20: 無線LANのセキュリティ対策（無線LANを使用する場合）**
  （SSIDのステルス化、Any接続拒否、MACアドレスやクライアント証明書等によるアクセス制限、WPA2/3による暗号化）