ISO TC 215/SC

Date: 2008-11-06

ISO 11636:2008(E)

ISO TC 215/SC /WG 4

Secretariat: ANSI

Health informatics — Dynamic on-demand virtual private network for health information infrastructure

本日本語ドキュメントは、ISO TC215/WG4 へ TR として提案したダイナミック・オンデマンド VPN の医療分野における有効性の理解を促進する目的とする。

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 11636 was prepared by Technical Committee ISO/TC 215, *Health informatics*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

はじめに

現在、医療情報の受渡しは、紙ベースでの運用、あるいは、企業等で本社と支社などを結ぶ企業ネットワークとして使われている専用線、ISDN 等の公衆網、もしくは「公衆サービス網」として「通信事業者が管理する専用のサービス網」の上に、特定ユーザ用のネットワークを仮想的に実現している IP-VPN 等、あらかじめ固定された組織間を結ぶ専用ネットワークにより行われるが用いられることが多い。そのため、セキュリティを維持しながら安心して医療情報を受け渡す方法が限られており、コストも高い。

医療分野においては、診療報酬のオンライン請求、医療機器のオンラインメンテナンス、健診情報サービス、医療画像による診断を含む遠隔医療、地域医療連携サービス等、様々なサービスでのネットワーク利用がある。しかし、このようなサービスを提供するためには、複数の医療機関間で医療情報を受け渡す必要があり、一つの医療機関から見たとき、複数の医療機関を選択してダイナミックに切換え接続可能とするネットワークが必要となる。

多くの医療機関へ安価にネットワークを普及させるためには、インターネット接続などのオープンなネットワークを使用して複数の医療機関、医療機器事業者、患者等個人を接続することが可能である。

我々は、オープンネットワークにおけるセキュアチャネルシステムとして、ネットワークレイヤーにおいて認証と暗号鍵の交換を伴う IPsec + IKE 方式の VPN、また他の方式として、セッションレイヤーにおいてクライアント端末と SSL サーバ間の Web ブラウザにおける暗号通信を行う SSL プロトコルを使うことができる。SSL プロトコルは、Web アプリケーションへの親和性は高いが、その他のアプリケーション、例えば e メール、FTP、独自のクライアント/サーバシステムでは使えないことがある。一方、医療機関においては、アプリケーションソフトウエアを変更せずにセキュアチャネルの形成ができることが望まれるので IPsec + IKE 方式の方が利用面で医療分野への親和性が高い。さらに、SSL にはよく知られている下層からの攻撃、セッション乗っ取り、ARP ステートメント等不可避な本質的リスクがある。

しかし、IPsec + IKE 方式の一般的な VPN は、ネットワーク機器の設定が複雑であり、専門的な知識が無く設定した場合は、医療情報の担保を保障できない。また、固定接続の VPN は、固定の組織間の接続しかできない。

最近、オープンなネットワークで接続する VPN であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のため、ネットワーク機器の設定を含め、ネットワーク経路上のセキュリティを担保した形態でサービス提供する方式が実用化しつつある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。これにより、医療機関のセキュリティに対する責任が軽減され、医療機関のように IT 技術者の少ない分野には最適である。

本 TR で紹介するダイナミック・オンデマンド VPN はこうした VPN の一つで、一般的に使われている通常の VPN サービスである 1 対 1 の固定接続ではなく、N 対 N に接続を容易に切換えられ、ネットワーク機器の接続パラメータを回線事業者が自動的に設定される。これは、医療機関の責任やネットワーク機器の設定の専門的知識が要求されないので、医療機関ネットワーク基盤として適している。また、インターネットを利用できるので安価なネットワークを要求する医療機関にとっても好都合である。

本 TR は、医療ネットワークにおいて予想される脅威を掲げ、またダイナミック・オンデマンド VPN が如何に医療分野に適用されたかを示す。

Health informatics — Dynamic on-demand virtual private network for health information infrastructure

1. 適用範囲

このドキュメントは、医療分野におけるネットワーク要件、医療分野のためのオープンネットワークのためのネットワークセキュリティ、そして個人情報を含む医療情報の外部機関との交換のためのセキュリティ管理を示すものである。
これらの要件は、セキュリティ運用と医療分野におけるセキュリティ課題の評価、そしてダイナミック・オンデマンド VPN の様なマネージド VPN の有効性を理解する助けとなるであろう。
この TR は、医療情報の交換のためにダイナミック・オンデマンド VPN によるセキュリティ対策の例を示すものであり、ダイナミック・オンデマンド VPN それ自身を規定するものではない。
これらの例は、その様な利用環境におけるポテンシャルリスクのためのネットワークソリューションを提供する。

2. 引用規格

以下の参照ドキュメントは、この TR の基本要素である。

ISO/IEC 18028-5: Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks

ISO/IEC 27799: Health informatics - Security management in health using ISO/IEC 17799

“Security and Privacy Requirements for Remote Servicing”, by NEMA/COCIR/JIRA Security and Privacy Committee (SPC)

3. 用語定義

この TR では、以下の用語を定義する。

3.1

DMZ (demilitarized zone)

外部とデータ交換をするエリア

3.2

HSZ (high security zone)

一部のリモート保守を除いて外部と直接データ交換をしないエリア

3.3

IPsec

IPsec は、インターネットで暗号通信を行なうための規格で、暗号技術を用いて、IP パケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである。

3.4

Internet VPN

インターネットを経由して構築される VPN のこと。インターネット VPN を経由することによって、機密を保持したまま遠隔地のネットワーク同士を LAN で接続しているのと同じように運用することができる。

3.5

IP-VPN

通信事業者の保有する広域 IP 通信網を経由して構築される VPN のこと。 IP-VPN を経由することによって、遠隔地のネットワーク同士を LAN で接続しているのと同じように運用することができる。

3.6

LAN (local area network)

同じ建物の中にあるコンピュータやプリンタなどを接続し、データをやり取りするネットワーク

3.7

医療費のオンライン請求 (ISO への提案した TR では、オンライン請求は日本特有と指摘を受け、用語解説を削除)

平成 20 年 2 月 20 日付け厚生労働省保険局長通知において、診療報酬のオンライン請求で使用する通信回線に、従前の「ISDN 回線を利用したダイヤルアップ」及び「閉域 IP 網を利用した IP－VPN 接続」に加え、「IPsec と IKE を組み合わせたダイナミック・オンデマンド VPN を例とする接続インターネット接続」についても選択可能であることが示された。

3.8

OSI リファレンスモデル

ISO により制定された、異機種間のデータ通信を実現するためのネットワーク構造の設計方針「OSI」に基づき、コンピュータなどの通信機器の持つべき機能を階層構造に分割したモデル。通信機能を 7 階層に分け、各層ごとに標準的な機能モジュールを定義している。

3.9

SI（サービスプロバイダー）

OSP 通信事業者とオンラインサービスプロバイダー間で、情報交換を行うサービス.

3.10

中継サービス

医療機関と外部機関間をネットワーク機器により情報交換を行う目的としたサービス

3.11

リモートアクセス

電話回線などを通じて、ネットワークやコンピュータに外から接続すること。遠隔地のコンピュータにリモートアクセスすることによって、そのコンピュータを、目の前にある時と同じように直接操作することができる。

3.12

審査支払基金

医療機関から請求された医療費（診療報酬）の審査を行い、適正な支払いを行う機関のこと。審査は診療担当者の代表・保険者（健康保険組合など）の代表・学識経験者の三者で構成される委員会で行われる。医療機関は診療報酬明細書（レセプト）を提出して、医療保険の支払い機関に医療費を請求する。社会保険診療報酬支払基金などの機関は、レセプトを審査したうえで、請求のあった医療機関に診療報酬を支払うという流れになる。

3.13

SSL

インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われている WWW や FTP などのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号などを安全に送受信することができる。

3.14

SZ (security zone)

機関内で情報の入出力を行う、外部とのやり取りが制限されるエリア

3.15

VPN (virtual private network)

公衆回線をあたかも専用回線であるかのように利用できるサービス。企業内ネットワークの拠点間接続などに使われ、専用回線を導入するよりコストを抑えられる。

3.16

WAN (wide area network)

電話回線や専用線を使って、本社－支社間など地理的に離れた地点にあるコンピュータ同士を接続し、データをやり取りすることを言う。

4. 略語

この TR では、以下の略語を定義する。

AES	Advanced Encryption Standard
AH	authentication header
ASP	application service provider

ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HEASNET	HEAlthcare information Secure NETwork consortium
HMAC	Hash Message Authentication Code
IC	integrated circuit
IKE	Internet key exchange
IPsec	Internet Protocol Security
IP-VPN	Internet-Protocol-based virtual private network
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IT	information technology
LAN	local area network
L2TP	Layer 2 Tunneling Protocol
NAT	network address translation
OSI	Open Systems Interconnection
OSP	online service provider
OSPF	Open Shortest Path First
PKI	public key infrastructure
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SHA	Secure Hash Algorithm
SI	System Integrator
TLS	Transport Layer Security
TOS	Type of Service
TTL	time to live
WAN	wide area network

5. 医療分野における情報サービスの形態

5.1. 医療分野における現在、もしくは期待される情報サービスの傾向

医療分野では、実際に下記のような情報サービスが提供されている。ネットワーク上では、これらのサービスが相互に影響を与えないよう、データ機密性の確保やアクセス制御によるセキュリティの確保を考慮しなければならない。現在行われている、あるいは想定される情報サービスのネットワークの利用形態を明確にするため、これらのサービスのサービス提供形態をデータアクセスの特徴に基づいて整理する。

a) **情報提供サービス**

他の医療機関から当該医療機関にある患者の医療情報にアクセスがある。例えば、以下がある。

— **地域連携サービス(医療機関・福祉介護等医療関連サービス業務向け)**
診療記録、検査データ、診療サマリ、健診データ等の患者個人の診療や介護記録を紹介状、地域連携 DB 等の様々な形態で情報提供する。

— **診療・介護情報提供サービス(患者向け)**
患者個人の診療・介護記録を一定の範囲で患者個人に開示する。

— **医療・介護情報提供サービス(一般向け)**
病院情報、疾患情報、他各種の医療・介護に関連する情報を一般向けに提供する。

b) **インターネット接続サービス**

医療機関からインターネット上にある情報サイトにアクセスする。例えば、以下がある。

— **インターネット接続サービス(業務限定)**
学術情報サイト、厚生労働省等の業務関連の情報提供サイトで医療機関が各自のセキュリティポリシーに沿って安全と判断したサイトに業務用のクライアントからインターネット経由でアクセスする。

c) 蓄積・中継サービス

他の医療機関や医療機関外の機関と情報を交換するために医療機関内あるいは医療機関外のいずれかの場所にいったん情報を蓄積した後で相手に情報が転送される。例えば以下がある。

— **メールサービス**
電子メールを送受信サーバで蓄積・中継する。

— **オンラインレセプトサービス**
レセプトを電子的に受信して他の機関に中継する。例えば、**支払い基金**がレセプトを受信して審査して保険者に**レセプト**を中継・伝送する。

— **検査データ配信サービス**
臨床検査、画像検査等の検査結果を検査会社から配信する。検査結果は、**電子カルテ**やオーダリング、部門システム等での利用があるため、データ配信後にこれらのシステムからデータが参照できるような構成が望ましい。

d) **情報処理サービス**

医療機関から情報処理を委託された外部機関が医療機関の情報を受け取って代行して処理する。例えば以下がある。

— **ASP サービス**
電子カルテ・レセプト等の医療機関向けのサービスを共同利用型サービスとして提供する。医療情報は、外部に保存される。

— **外部保存(バックアップ) サービス**
院内の**電子カルテ**、オーダリング、部門システムの障害や災害によるデータ破損時のシステム復旧のためにバックアップデータを外部機関に伝送して保存する。

e) **リモート保守サービス**
医療機器の異常診断や障害回復等の各種保守サービスを契約したサービス会社からリモートで受ける。契約した会社は、契約した機器との間でのみ接続できるようにする必要がある。

f) **認証・監査基盤サービス**
医療機関が情報をアクセスするため公開鍵認証、デジタル署名、時刻配信などの公共性のある基盤サービスを利用する。例えば、以下がある。

— **タイムスタンプサービス**
デジタル署名にうつタイムスタンプの発行や監査用ログ収集のためのシステムの時刻合せをする。

— **VA(Validation Authority)サービス**
認証(CA)局の発行した公開鍵証明書が有効かどうかを検証する。
これらのシステムの提供形態を分析してネットワークの安全な接続形態を規定する。

5.2. 守るべき医療情報の種類（情報資産）

ネットワークに対する外部からの攻撃は、ますます頻繁に行われるようになっており、これらのネットワーク脅威から守るべき医療情報は、機密性、完全性、可用性を保護しなければならない。ISO/IEC27799 5.4 によれば医療分野における守るべき情報としては、以下の様なものが挙げられる。

— 個人医療情報

— 匿名識別のための何らかの方式を経由して個人医療情報から得た匿名データ

— 個人医療情報から個人識別データを取り除いた匿名データを含む統計および研究用データ

— 臨床判断支援データ(医薬品副作用データ等)を含む特定の患者または複数の患者に関連しない臨床/医療情報

— 健康管理者およびスタッフに関するデータ

— 公共健康調査に関連する情報

— 医療情報システムで作成されたオーディットトレールデータ。（これには個人医療情報や個人医療情報から抽出した匿名データ、個人医療情報に関してユーザが行った行為に関するデータを含む。）

— 医療情報システムに関するアクセス制御データおよびその他のセキュリティ関連のシステム構成データを含むシステムセキュリティデータ。

これらの守るべき医療情報は、今後ネットワークを介して、診療報酬のオンライン請求、医療機器のオンラインメンテナンス、健診情報サービス、医療画像による診断を含む遠隔医療、地域医療連携サービス等の医療・健康・保健サービスに利用されていくが、プライバシーの観点からの患者の個人情報に対する医療情報セキュリティを確保すべく、よりセキュアなネットワークが望まれる。

5.3. 医療分野におけるネットワークに求められる要件

医療分野におけるネットワークとして注目すべき特徴は以下である。
— 取り扱う情報は、患者のセンシティブな個人情報である
— 画像や音声データ等、大容量データを扱う
— 地域の拠点が参加し、複数拠点間での情報のやり取りが必要になる
— 通信をする相手が増えることにより、医療機器、ネットワーク機器やサービス利用者の確認が必要になる
— 医療機器などによるネットワークの構築経費負担が発生する

これらの特徴をふまえると、医療分野におけるネットワークに対して、求められる要件は、以下となる。
— 安全な通信
— 大容量データの高速通信
— メッシュ型ネットワークの実現と拡張性
— 参加メンバ（利用者、組織、機器）の真正性保証
— セキュアネットワーク接続に関するコスト削減

6. 医療分野におけるネットワーク構築の考え方

外部と医療情報等を交換するケースとしては、地域医療連携で中核病院、診療所、薬局、検査センター等と相互に連携してネットワークで医療情報等のやり取りや、診療報酬の請求のために審査支払機関等とネットワークで接続する ASP 型のサービスを利用する場合等が考えられる。
外部と医療情報を外部ネットワークを利用して交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送受信データに対する「盗聴」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。
本章では、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。

6.1. 外部と個人情報を含む医療情報を交換する場合の安全管理に関する考え方

6.1.1 責任分界点の明確化

提供元医療機関等と提供先機関は通信経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意する必要がある。その上で、自らの責任範囲において、オンラインサービス提供事業者や回線提供事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにする必要がある。

6.1.2 医療機関等における留意事項

情報を伝送するまでの医療情報の管理責任は医療機関等にある。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の医療機関等に受け渡しされるまでの一連の流れ全般において適用される。
ただし、ここでいう管理責任とは電子的に記載されている情報の内容であり、その記載内容や記載者の正当性の保持（真正性の確保）のことを指す。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても第三者がその情報を判読できないようにしておく処置のことを指す。また、改ざん検知を行うために電子署名を付与することも対策のひとつである。
このような視点から見れば、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

a) 「盗聴」の危険性に対する対応

ネットワークを通して情報を交換する場合には、伝送途中に仮想的な迂回路を形成して情報を盗み取る可能性、またネットワーク機器に物理的な機材を取り付けて盗み取る等の行為が行われる可能性がある。医療機関等においては、万が一、伝送途中で情報が盗み取られた場合、また意図しない情報漏洩や誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要がある。そのひとつの方法として医療情報そのものの暗号化が考えられる。どのタイミングで、どの程度の暗号強度の暗号化を施すかについては伝送しようとする情報の機密性の高さや医療機関等で構築している情報システムの運用方法によって異なる。医療機関等の設備から情報がネットワークを通して伝送される場合は、情報は暗号化されていることが望ましい。

b) 「改ざん」の危険性への対応

ネットワークを通して情報を伝送する場合に、情報を暗号化して伝送する場合には改ざんへの危険性は軽減されるが、ネットワーク経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性がある。また、情報を暗号化せずに伝送する可能性も有り、その為、改ざんに対する対処は確実に実施しておく必要がある。改ざんを検知する方法としては、電子署名を用いる等が想定される。

c) 「なりすまし」の危険性への対応

ネットワークを通して情報を伝送する場合、ネットワークが非対面による情報伝達手段であるため、情報を送ろうとする医療機関等は、送信先の医療機関等が確かに意図した相手であるかを確認しなくてはならない。また、情報の受け手となる送信先の医療機関等は、その情報の送信元の医療機関等が確かに

通信しようとしている相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であるかを確認しなくてはならない。そのため、通信の起点と終点で相手を適切に識別するために、公開鍵暗号方式や共有鍵暗号方式等の認証の仕組みを用いて情報を伝送するまえに相互に認証するべきである。また、改ざん防止と併せて、送信元の医療機関等であることを確認するために、医療情報等に対して電子署名を組み合わせることも対策となる。

6.2. 医療機関等が選択すべきネットワークのセキュリティの考え方

情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の 2 つに類型化される。

— 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合

— 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合

このように、医療機関等において医療情報を、ネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークの提供サービスの形態は様々存在するため、以降では幾つかのケースを想定して留意点を述べる。

6.2.1 クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網でありインターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」の危険性は比較的低いが、物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。

以下、それぞれの接続方式について特長を述べる。

a) **専用線で接続されている場合**

品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入にあたってはやり取りされる情報の重要性と情報の量等の兼ね合いを見極める必要もある。

b) **公衆網で接続されている場合**

電話番号を確認する仕組みを用いなかったことによる誤接続、誤送信のリスクや専用線と同様で拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため、大量の情報もしくは画像等の容量の大きな情報を送信する際に適用範囲を適切に見定める必要がある。

c) **閉域 IP 通信網で接続されている場合**

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

以上の３つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。しかし、接続サービスだけでは一般に送られる情報そのものに対する暗号化は施されていない。また異なる通信事業者のネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとは言えない。

そのため、クローズドなネットワークを選択した場合であっても、「6.1.2. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入するなどの措置を取る必要がある。

6.2.2 オープンなネットワークで接続されている場合

現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療連携の仕組みを構築したりする等、その利用範囲が拡大して行くことが考えられる。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を取らなければならない。

a) 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保した形態で情報交換を行う場合

オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

b) 医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の自己責任において導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI 階層モデル」で定義される 7 階層のうち、どこの階層でセキュリティを担保するかによって異なってくる。

例えば、SSL を用いた通信方式を用いる場合、5 階層目の「セッション層」と言われる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ないが、通信を開始する前のネゴシエーションが暗号化されていないので、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。一方、IPSec を用いる場合は、2 階層目もしくは 3 階層目の「ネットワーク層」と言われる部分より下位の層で経路の暗号化手続きがなされるため、SSL よりは危険度が低いが、経路を暗号化するための暗号鍵の取り交しに IKE を用いてネゴシエーションの内容(IPsecSA)自体が暗号化されるため、盗聴の危険がなく、IPsec + IKE の組み合わせで、確実にその安全性を確保している。

また、SSL/TLS（SSLv3 の修正版）の通信方式は、RFC3552 によれば「TLS は、TCP または SCTP のような信頼できるプロトコルに依存すること」との記述があり、SSL 自体がトランスポート層として TCP を使うため、UDP（ユーザーデータグラムプロトコル）を使うアプリケーションに対応していない。また、TLS は、IPsec が無い IP 層の攻撃の影響を受ける。これによって、LAN のアクセスポイントにセッション乗っ取りや ARP 詐称等のセキュリティホールが発生しるリスクが指摘されている。また、金融等で実際にデータの抜き取りや改ざんによる金銭的な被害が報告された事例もある。

7. 脅威分析と対策

医療分野におけるネットワークに対して、求められる要件をその構築の考え方に従って実現する為には脅威分析を行い、その対策を技術的あるいは運用により実施しなくてはならない。

患者の個人情報を含む医療情報を交換するネットワークは、医療機関や通信機器等の複数要素から構成されており、ネットワーク全体の安全性を担保するためには、各要素（プレイヤー、利用技術、ネットワークそのものの運用面）それぞれの安全性を確保すべきである。ネットワーク全体を網羅して、医療機関がネットワーク導入に当たって考慮すべきセキュリティに関する技術・運用の仕様について検討し、要件を明確化すべきである。

各要素の安全性は、一定水準のセキュリティレベルを維持できる様に、各種標準やガイドラインといった明確な基準やルールに則ることで、確保する。

脅威分析はネットワーク全体を網羅して医療機関がネットワーク導入にあたって考慮すべきセキュリティに関する技術・運用の仕様について検討する必要がある。詳細は、Annex A に示す。Annex A では RFC を基盤にして守るべき資産やネットワーク上の脅威を踏まえ、脅威モデルを想定し、各ガイドラインやセキュリティ関連の RFC 等の参考文書を参照し、各種セキュリティ対策の検討、及びその有効性を評価している。現状において、利用可能な技術要素を組合せたチャネルセキュリティのセキュリティ対策としては、VPN の方式として IPsec + IKE が有効であると結論つけられている。

8. 医療分野におけるネットワーク構築

8.1. 外部と個人情報を含む医療情報を交換する場合の安全管理に対する最低限のガイドライン

チャネルセキュリティ確保の観点から「盗聴」、「改ざん」、「なりすまし」等のネットワークの脅威に対しては、以下のような対策が、必要である。

a) セキュアなネットワーク経路を確保
   — ネットワーク経路でのメッセージ挿入、ウイルス混入などの防止
   — 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴の防止
   — セッション乗っ取り、IP アドレス詐称などのなりすまし防止
   上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することがあげられる。
b) データ送受信の拠点の出入口、使用機器で利用者の必要な単位で相手確認
   対策例:
   — PKI による認証
   — 事前配布された共通鍵の利用
c) 正規利用者、許可機器への成りすまし防止
d) ルータ機器は安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定
e) 送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施。
   — SSL/TLS の利用
   — S/MIME の利用
   — ファイルに対する暗号化
   — 暗号化の鍵については電子政府推奨暗号を使用
f) 医療機関間の情報通信において、医療機関等、通信事業者、システムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社などの組織間で責任分界点、責任の所在を契約書等で明確化
g) リモートメンテナンスを実施する場合は不必要なログインの防止
h) 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認

8.2. ネットワークのセキュリティ評価の為のチェックシートの活用

医療においてネットワークの利用が想定されるサービスとしては、レセプトオンライン請求、オンラインメンテナンス、検診情報サービス、医療画像による診断を含む遠隔医療や医療地域連携サービス等があり、医療機関から見ると接続相手は固定ではなく、場合に応じて複数の接続先を切り替える事が想定される。その際に、扱う医療情報を信頼できるものとするため、Annex B に示す「ガイドライン第２版」に準拠した安全なプロバイダを選択することが望ましい。医療機関は、製品の導入にあたり、ガイドラインに記された全ての仕様を満足させるために、製品仕様で不足する部分については運用によりカバーできるよう、製品仕様だけでなく運用条件やコストについても考慮して製品を選定することが望ましい。医療機関におけるネットワークセキュリティを評価するために、ガイドラインに規定された医療機関等が医療情報を扱う際に守るべき事項を網羅的にチックシートとしてまとめた。詳細は Annex C に示す。本チェックシートには、医療機関等が運用上守るべき事項から、技術的・システム的に守るべき事項まで全て網羅されている。医療機関等が自機関のチェックがし易いように、医療機関等をその機能によって下記のように分類し、チェックができるようにした。また、医療機関等が「ガイドライン第 2 版」を守るためには、医療機関等だけではなく、システム SI、またネットワークサービスや ASP サービス等を提供するサービス・プロバイダ（SP）は医療機関等の外にあって医療機関等の一部としてサービス機能を提供することになるため、医療機関等に準じて「ガイドライン第 2 版」の遵守をする必要がある。SP の提供するサービス内容や機能がこれを満足している必要がある。このため、チェックシー

トをサービス機能の提供者とそのチェックすべき事項に沿って、医療機関の管理者、システム SI、SP のチェックシートに分けた。本チェックシートで、医療機関の管理者、システム SI、SP がそれぞれ医療機関のネットワークセキュリティを評価し、製品仕様だけでなく運用条件やコストについても考慮して製品を選定するべきである。

8.3. ダイナミック・オンデマンド VPN の活用

高度な医療機器が地方の中規模・小規模医療機関まで普及し、装置の性能向上に伴い、より高度な診断能力が求められるが、それに対応した専門医の絶対数が不足している。そこで期待されるのが、遠隔診断支援等 IT の活用である。遠隔診断ならば、専門医が時間をかけて依頼病院まで移動する必要もなく、迅速・簡便に支援すること可能である。只、IT を活用したとしても、必要な検査の絶対数が減るわけでもなく、診断に対するニーズは、一層高度化している。迅速に画像を送ることができれば、更に依頼件数や医療機関も増えるかもしれない。　依頼病院と遠隔診断を行う病院等のシステムが密結合になるほか、利用施設の広がりとともに、その都度の通信の組み合わせも複雑になる。したがって、施設間ネットワークは高い安全性を担保しつつ、データ流通を適切に N 対 N の接続をコントロールできるものが望ましい。さらに、ネットワーク技術者が常駐しない医療機関でも容易に安価に利用できることも必要で、責任分解点として医療機関の責任が少ないものが望ましい。こうした、施設間のネットワークインフラとして、8.1 のガイドラインを満たす一例としてインターネット回線にダイナミック・オンデマンド VPN を利用することで、この両立が可能となる。ダイナミック・オンデマンド VPN は、拠点と拠点を結ぶ機器の正当性も保証することができ、医療機関とサービス提供者との責任分界点が明確であるほか、設定や利用を行う人の認証も確実に行い得るため、運用上も高い安全性を担保できる。それに加えて、接続の組み合わせも複数設定しておき、必要なときに必要な相手とだけ、安全に通信を行うことが、可能である。ダイナミック・オンデマンド VPN の仕様概要は Annex D に示している。

ダイナミック・オンデマンド VPN はマネージド VPN で回線接続等の責任がサービスプロバイダーに属するが、医療施設側の遵守義務もあるので、特に機微な情報を扱う医療情報ネットワークではその遵守をプロバイダの義務遵守と同様に透明性を確保して監視する必要がある。

9. 外部と医療情報を交換する場合にダイナミック・オンライン VPN によりセキュリティ対策を行った事例

ケーススタディでは、外部と医療情報を交換する場合にダイナミック・オンラインＶＰＮによりセキュリティ対策を行った事例を示す。

第 5.3 章の要求事項や第 8.1 章のガイドライン事項を満足し、6.2.章の「医療機関等が選択すべきネットワークのセキュリティの考え方」の「オープンなネットワークで接続されている場合」で述べられた「オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供する」ネットワークの一例としてダイナミック･オンデマンド VPN が応用できる。医療地域連携サービス、遠隔医療、オンラインメンテナンス等の分野で導入されはじめているので。以下にその適用モデルを紹介する。

9.1. 健康ポータルによる地域医療連携モデル

地域医療連携モデルを Figure 1 に示すが、地域において医療機関（地域中核病院、診療所等）、総合検診センター、調剤薬局等の間でネットワークを経由して、必要に応じて医療情報の交換を行い、患者も、自宅からポータルを通して病院の予約や自分の検診結果等を参照できるようにするモデルである。中核病院は、診療所から紹介状及び患者の診断データを貰い、患者を診断し、検査結果は、総合検診センターから受け取り、また処方情報は調剤薬局へネットワークを介して渡す等、地域中核病院から見たネットワークの接続先は、固定ではなくＮ対Ｎの通信相手の切り替えが必要である。またネットワークを介して医療情報が交換されるために、ネットワークには、十分なセキュリティが求められる。その為にはダイナミック・オンデマンド VPN を用いて各施設にダイナミック・オンデマンド用の VPN 機器を設置し、インターネット経由で、サービス提供者の管理のもとに通信を行うことによりセキュアな通信を実現する。

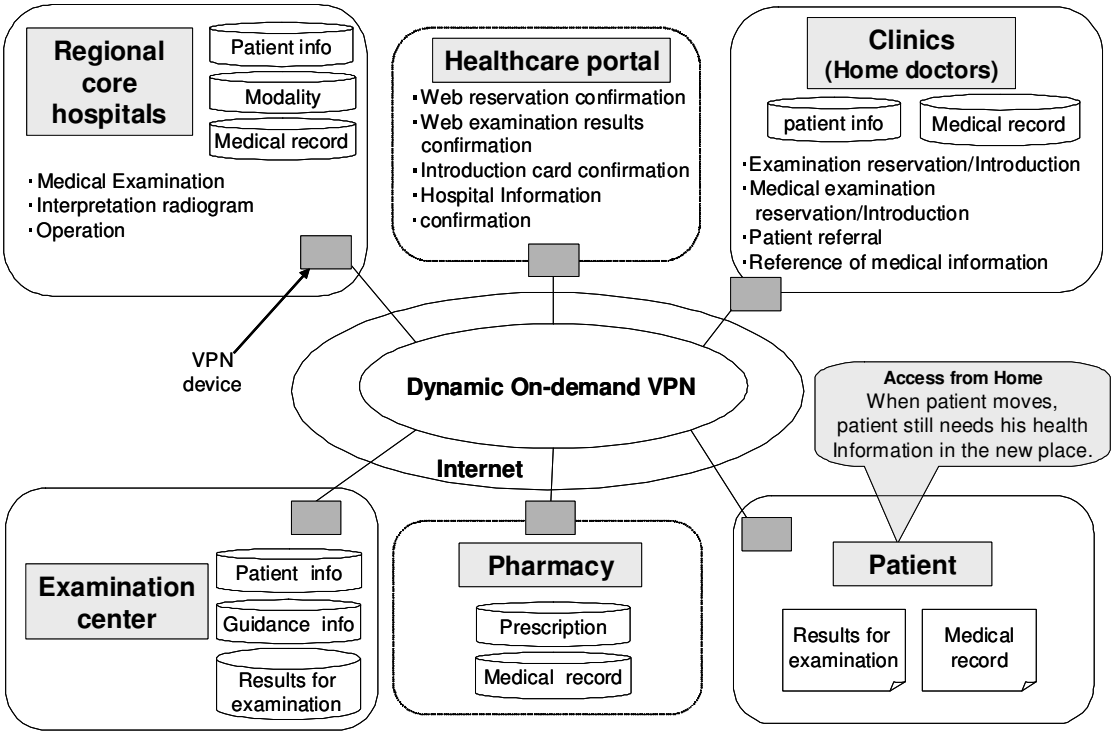


Figure 1 — ダイナミック・オンデマンド VPN を利用した健康ポータルによる地域医療連携モデル

9.2. オンラインメンテナンスモデル

オンラインメンテナンスモデルを Figure 2 に示す。医療機器 SI、SI が、ネットワークを介して、医療関連機関に設置されている医療機器、システムのメンテナンスを行うモデルである。メンテナンスは、機器の状態把握や再現の為、医療機器内の実際のデータを使用する可能性があり、ネットワークを介して実際のデータの転送を行う場合がある。その為には、ネットワークは、SI が色々な医療機関と接続、医療機関から見れば、色々な SI と接続し、契約した相手以外とは接続できないことや、アプリケーションを変更しないためにはＮ対Ｎで通信相手を切り替えられ、IP レベルのセキュアなネットワークが必要である。これを満足するものとしてダイナミック・オンデマンド VPN 機器を医療施設およびリモートサービスに設置し、インターネット経由でセキュアな通信を行い、リモートメンテナンスを実現する。この場合、医療施設とれモーとメンテナンス SI 間で個人情報保護に関するポリシーを交換しておく必要がある。

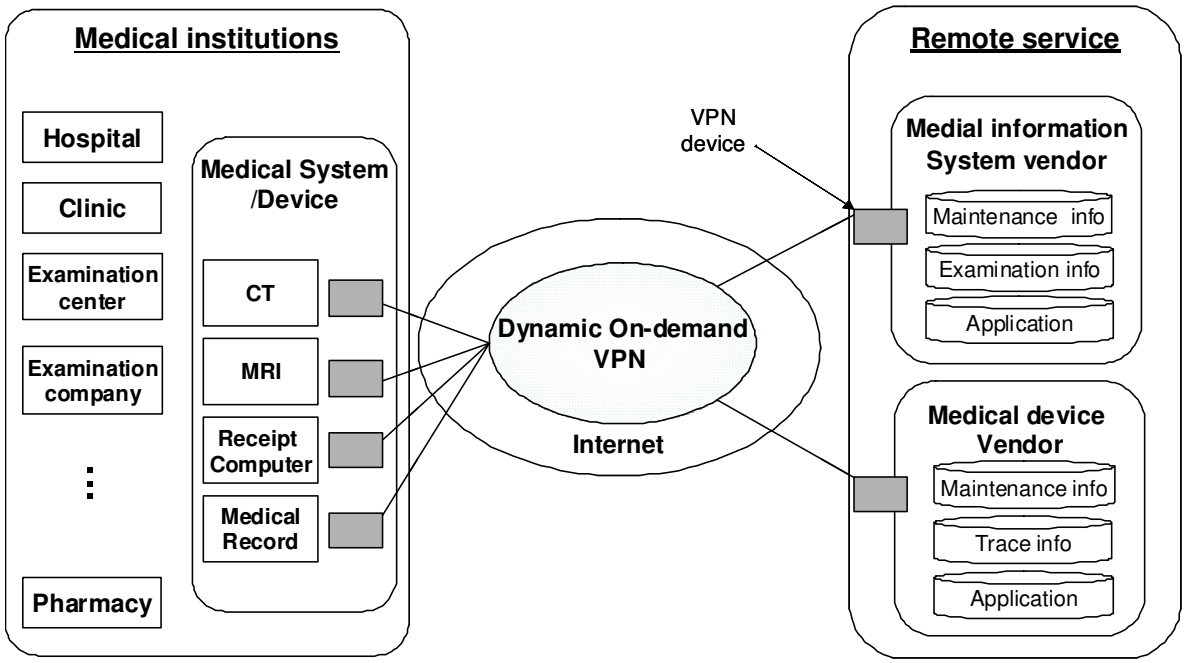


Figure 2 — ダイナミック・オンデマンド VPN を利用したオンラインメンテナンスモデル

9.3. 地域中核病院を中心とした地域医療連携モデル

A 地域中核病院と地域の診療所とが、診察の分担や、病状に応じて互いに患者を紹介し、必要な情報の提供や共有化を行うことで連携する地域完結型医療の実現を図るため、Figure 3 に示すようにダイナミック・オンデマンド VPN を用いて地域中核病院と、診療所などを接続することで安全な地域医療連携ネットワークを構築できる。この地域医療連携ネットワークでは、紹介状、診断予約、診療情報等の機密メール、情報共有などのサービスを提供することを目的としている。 地域医療連携ネットワークは、地域中核病院と診療所などを、ネットワーク接続毎に IKE 認証した上で、IPSec/AES で VPN 接続することにより、ネットワーク経路の脅威を排除する。地域中核病院では、セキュアゾーンである院外接続用のネットワークと、ハイセキュアゾーンである院内ネットワークとはファイアウォールにて分離しアクセス制御を行う。また，診療所の PC から院外接続用のセキュアゾーンにあるサーバへのアクセスは、ダイナミック・オンデマンド VPN を利用して通信を行う。導入後の医療機関の評価としては、

- 予約をとるのが楽になる
- 中核病院営業時間に関係なく予約業務等が行える
- 暗号化をしておりセキュリティ面で優れたシステムが、ルータ１つという設備投資で利用できることが魅力

等が期待される。

術後の急性期病院、長期療養型の連携、慢性期の診療所との連携の為に医療情報を交換する為にそれぞれの施設に、ダイナミック・オンデマンド VPN の VPN 機器を設置してセキュアな通信を行う。

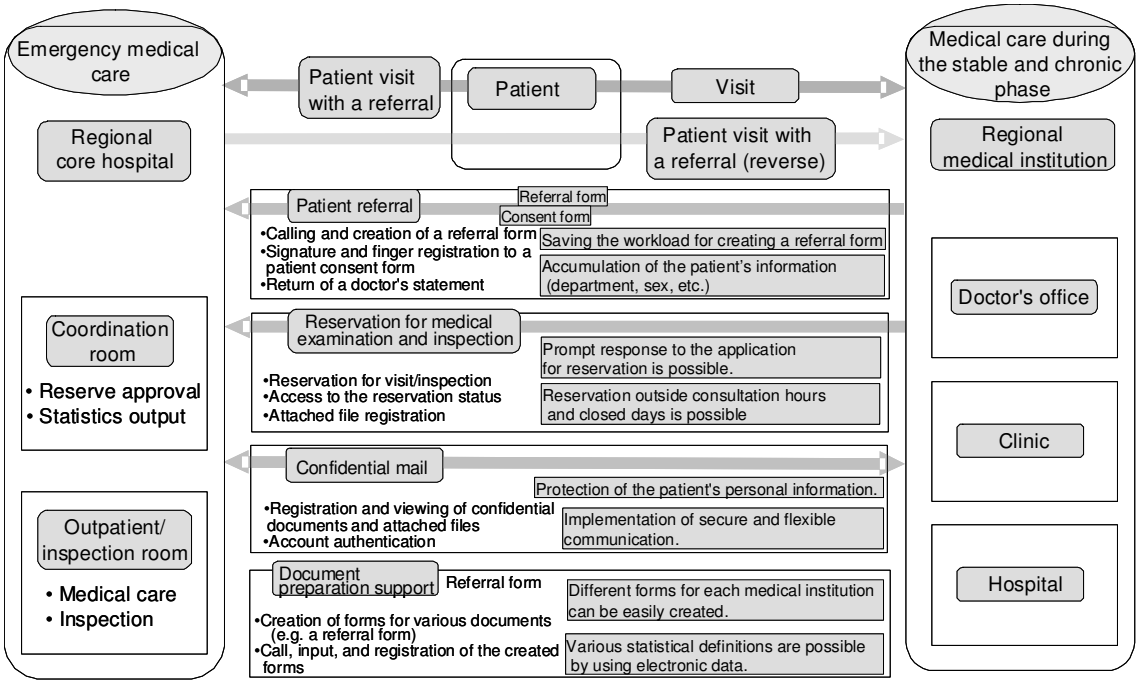


Figure 3 — ダイナミック・オンデマンド VPN を利用した地域中核病院を中心とした地域医療連携

9.4. 大学病院と研究機関、地域病院間で連携した画像診断、リモートメンテナンス、ネット会議モデル

画像診断のための医療機関間の大容量データの伝送、また医療機器のリモートメンテナンスのためにネットワークを介して実際のデータを用いて機器の診断を行う等、ネットワークには個人情報が流れることがあり、ネットワークにおける盗聴の脅威がある。そのため機器の認証によるセキュリティ向上、また複数接続を目的として、ダイナミック・オンデマンド VPN を適用した。

Figure 4 に示すように大学病院・研究機関・医療機器 SI が連携するリモートメンテナンスネットワークを構築し、画像診断、機器のリモートメンテナンス、ネット会議などのサービスを展開している。本ネットワークでは、付属病院、学内に併設された研究機関、医療センター並びに地域病院に設置された画像サーバ間をダイナミック・オンデマンド VPN で接続する心臓エコーの画像診断支援ネットワークを構築した。画像診断支援ネットワークでは、診断画像の転送、ネットコンファレンス、病理関連資料の共有などのサービスを提供している。また、本ネットワークを利用して医療機器 SI に設置したリモート保守端末と CT や MRI 等の医療検査機器を VPN で接続してリモートメンテナンスを提供している。本ネットワークは、学内 LAN 内の接続に L2TP トンネリングが使用されているため、トンネルの基点と終点でセッション確立毎に IKE/PKI 認証した上で IP-SEC/AES で VPN 接続する。また、B 大学では、院内 LAN と外部接続安全性を検証するため、院内ネットワークと院外接続用のセキュアゾーンを物理的な切替スイッチを用いてネットワーク適時切り替えて利用する構成とする。

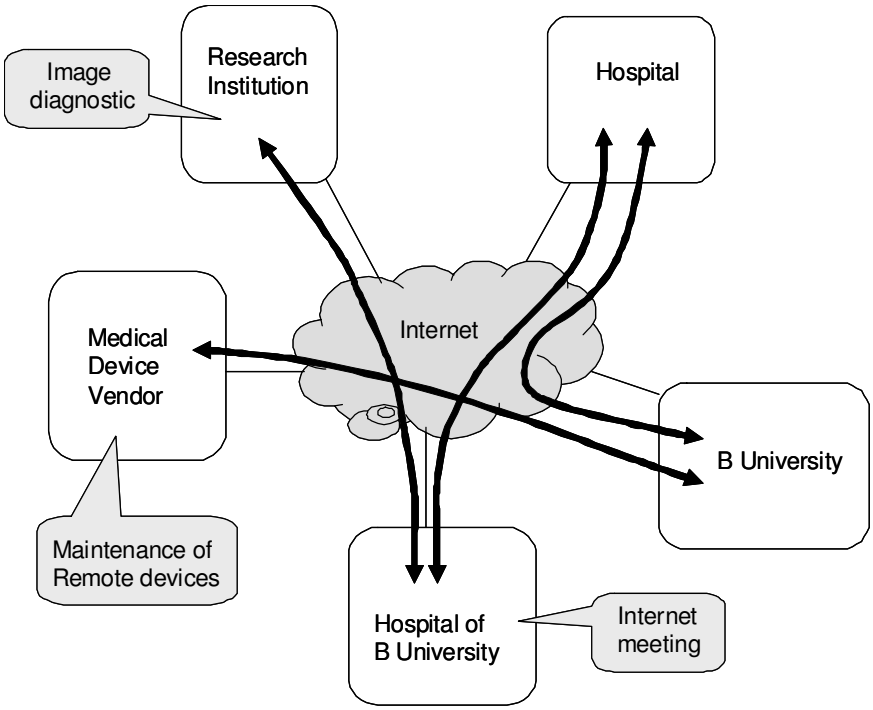


Figure 4 — ダイナミック･オンデマンド VPN を利用した遠隔画像診断、リモートメンテナンス、ネット会議

9.5. 大学病院を中心にした病院間の遠隔画像診断、遠隔病理診断、ネット会議モデル

Figure 5 は大学病院が県内病院を連携するネットワークを構築し、診断画像の転送、病理関連資料の共有、ネット会議などのサービスを行っている。大学は、病理診断医の不足を補うため、大学の付属病院に設置した画像サーバと病理診断医を派遣している県内の病院にある病理標本の取り込みサーバをダイナミック・オンデマンド VPN で接続する病理診断ネットワークを構築している。病理診断ネットワークでは、病理標本の遠隔取込み、診断画像の転送、ネットコンファレンス、病理関連資料の共有などのサービスを提供している。大学では、病理診断ネットワーク用の画像サーバをセキュアゾーンに配置して県内の病院のセキュアゾーンにある病理標本の取り込みサーバと連携する。大学や各病院では、院内LANに接続されたPCからインターネットやセキュアゾーン内のホストとの通信する場合はルータやファイアウォールを経由してアクセス制御やウィルスチェックを行う。病理診断ネットワークでは、画像サーバと拠点間接続ルータ間の院内 LAN と拠点間のインターネットの 3 つのパスについてそれぞれセッション確立毎に IKE/PKI 認証した上で IP-SEC/AES で VPN 接続し、通信経路の脅威を、院内外を問わずに排除できるようにしている。また、サーバ付属の通信機器と拠点間ルータは、NTC で時刻同期を取った上でダイナミック・オンデマンド VPN の管理サーバに通信ログを保管できるため、アクセスに関する否認防止やシステム監査におけるトレーサビリティが保証できる構成になっている。

合わせて、放射線画像の遠隔診断やネット会議もダイナミック・オンデマンド VPN のセキュアチャネルを用いてインターネット経由で行っている。

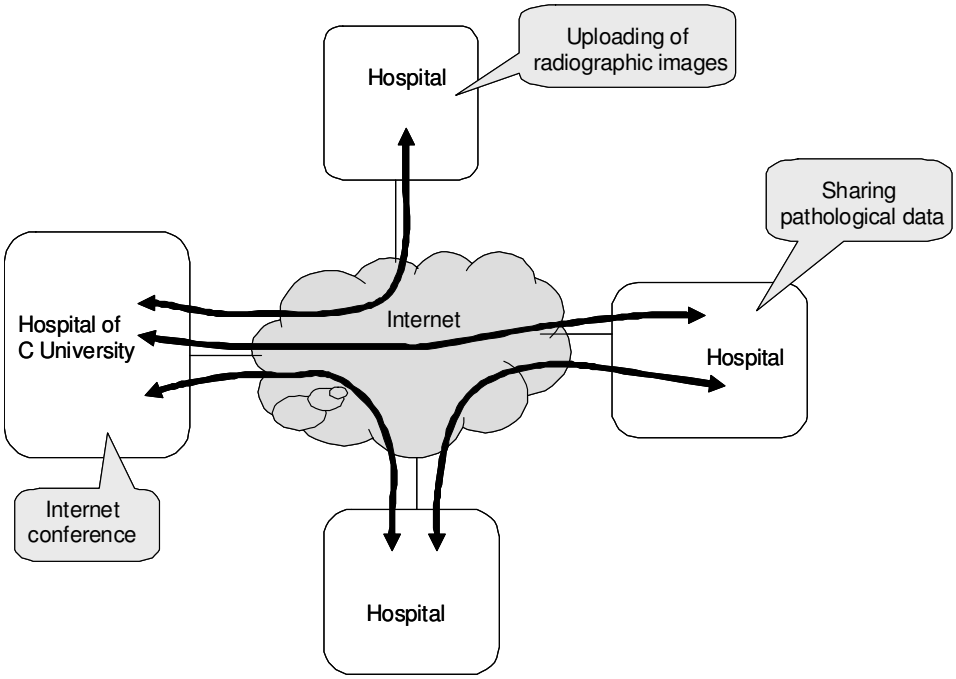


Figure 5 — ダイナミック・オンデマンド VPN を利用した遠隔画像診断、遠隔病理診断、ネット会議

Annex A
(informative)

脅威分析と対策

A.1 ネットワークに関するセキュリティ要件の抽出

セキュリティ要件を検討するため、これまでに出されたガイドラインや要件、セキュリティに関するRFC を参照して要件を抽出した。

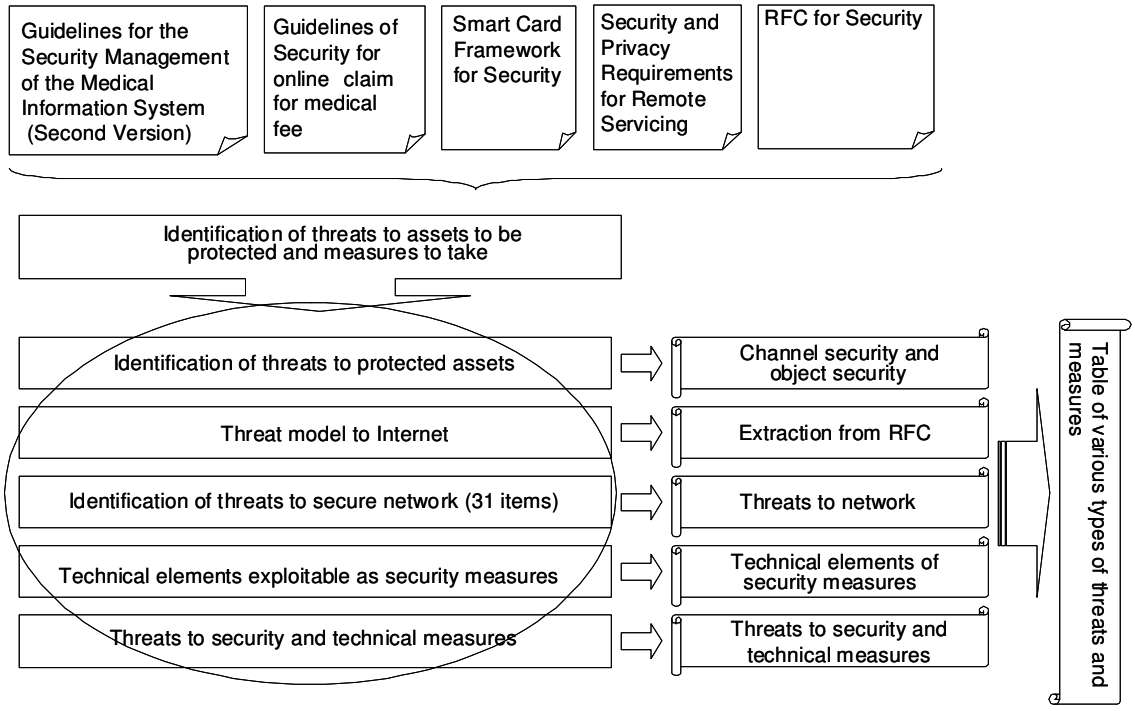


Figure A.1 — ネットワークセキュチティの脅威分析

関係のあるガイドラインとして厚生労働省の「医療情報システムの安全管理に関するガイドライン第２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」については、技術的検討に参照した部分を以下に示す。また、日米欧の画像機器工業会が欧米のプライバシー保護関連の法令に対応するために検討したガイドラインについても示す。

a) 医療情報システムの安全管理に関するガイドライン第２版（Annex B 参照）

「医療情報システムの安全管理に関するガイドライン第２版」の中でも特に下記の章節の技術情報を参照した。

6.9 外部と個人情報を含む医療情報を交換する場合の安全管理
8 診療録及び診療諸記録を外部に保存する際の基準
8.1 電子媒体による外部保存をネットワークを通じて行う場合
8.1.1 電子保存の３ 基準の遵守
8.1.2 外部保存を受託する機関の限定

8.1.3 個人情報の保護
8.1.4 責任の明確化

b) 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

「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」の中でも特に下記の章節の技術情報を参照した。
5.技術的セキュリティ：ネットワーク間のフィルタリングの必要性

Figure A.2 は、別々のネットワーク間で、フィルタリングがされていることを示す。

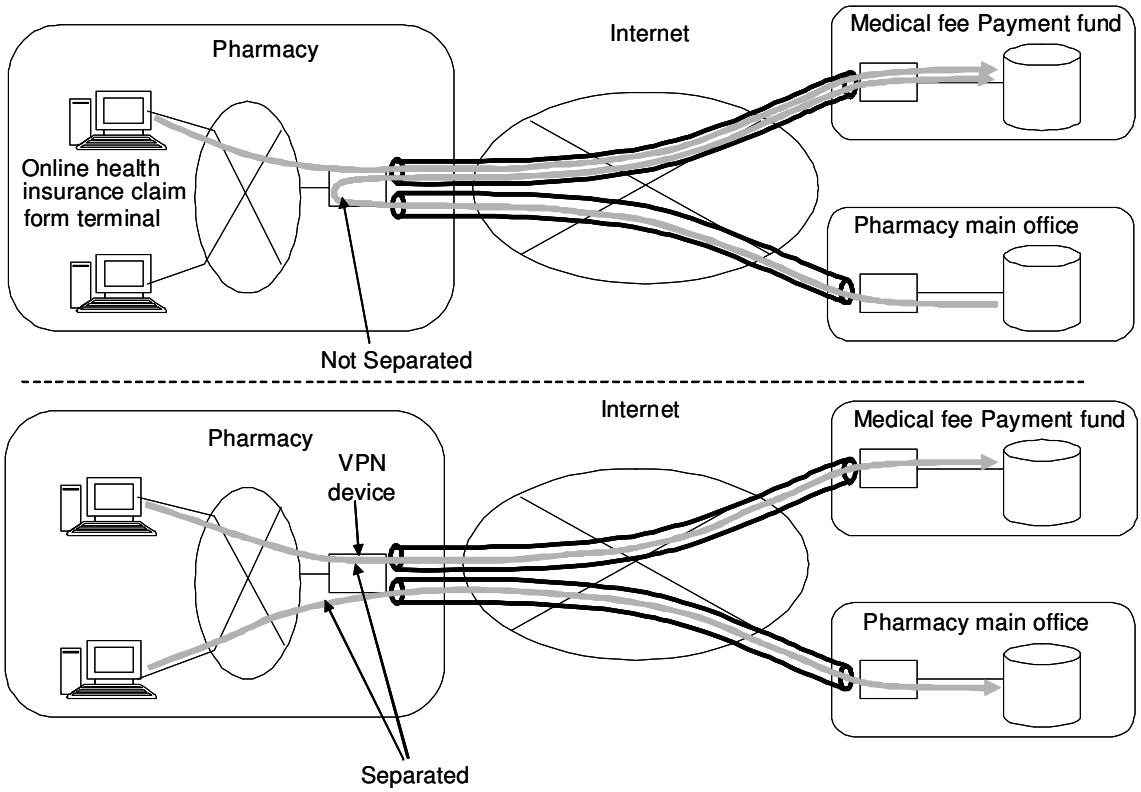


Figure A.2 — ネットワーク間のフィルタリングの必要性

c) Security and Privacy Requirements for Remote Servicing

医療の国際化や保険情報等の通信で先行する諸外国での対応を参考とするため、日米欧の画像機器工業会が欧米のプライバシー保護関連の法令に対応するために設置した Security and Privacy Committee (SPC)で検討されたガイドライン Requirements for Remote Services を以下に示す。

— リモートサービスの医療機関並びに医療関連機関の拠点のアクセスポイントは一つに絞るようにすること。
— 拠点の入り口のアクセスポイントで認証する。誰がアクセスしたか認証することが望ましいが、発信元で対応が付けられれば、どこの機関からの通信か認証できればよい。
— 医療機関は、アクセス状況を常に監視できるようにしておき、不正な通信を発見した場合は当該通信を遮断できるようにすること。

— 通信の秘密が守られるように暗号化しなければならない。できれば、PKI を応用した暗号化が望ましい。通信に関する誰がいつ何処にアクセスしたかというログは、発信元、医療機関のアクセスポイント、アクセスされた場所の 3 箇所で取ること。必要があれば、その 3 つのログをつき合わせてシステム監査ができること。
— 医療機関は、セキュリティポリシーを策定し、ネットワークを通じてアクセスする医療機関、医療関連機関に対してそれを遵守させること。

A.2 守るべき資産としてのチャネルセキュリティとオブジェクトセキュリティ

RFC3552 では、セキュリティ要件をチャネルセキュリティとオブジェクトセキュリティの二つに分けて対象を明確にしている。二つの要件は、相互に補完しつつ、ひとつのデータオブジェクトに関するセキュリティの確保を定義している。オブジェクトセキュリティは、データオブジェクト全体に適用されるセキュリティ手段であり、チャネルセキュリティは、オブジェクトを透過的に運ぶことができるセキュアチャネルを提供する。
ネットワーク全体（端末ーネットワークー端末間）において、検討対象とする範囲を明確に定義しなおすと、「チャネルセキュリティ」と「ネットワーク機器のオブジェクトセキュリティ」とに分類できる。
検討対象とする範囲において守るべき資産としては、下記に示される事項について検討しなければならない。
端末間のチャネルセキュリティ ⇨ 送受信データ
ネットワーク機器のオブジェクトセキュリティ ⇨ ネットワーク機器の設定ファイルや秘密鍵等

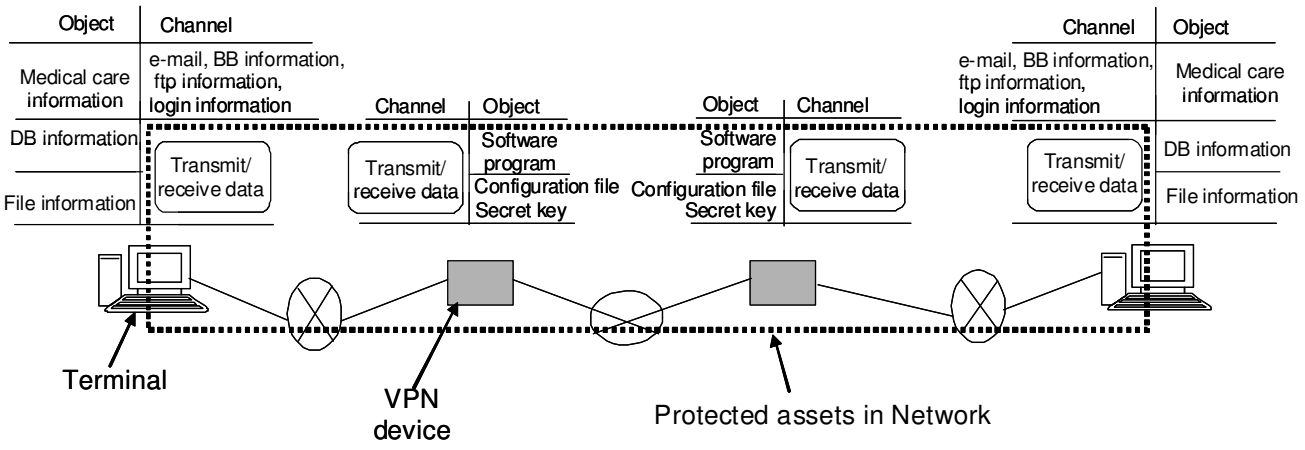


Figure A.3 — チャネルセキュリティとオブジェクトセキュリティ

A.3 ネットワーク機器のオブジェクトセキュリティに関わる構成機能

Table A.1 — ネットワーク機器の設定情報の機能要素

大区分	小区分	機能概要
VPN 管理機能		
	鍵交換機能（IKE)	VPN 接続に使用する暗号鍵を自動で交換する
	暗号化機能（IPsec）	通信データの機密性を確保するためにデータを暗号化する
	認証機能（IPsec)	通信データの送信元を認証する
	VPN 制御機能	VPN 接続に必要なパラメータを接続管理センターから取得する
	VPN 接続機能	VPN 接続の接続/切断要求やデータの送受信を行う
	初期登録機能	製造時にセキュアな記憶領域に初期情報（製造者署名付き機器情報）を登録する
	機器情報参照機能	セキュアな記憶領域に格納されている機器情報を読み出す
鍵管理機能		
	耐タンパ機能	論理的/物理的に記憶領域へのアクセスを制御する
	暗号化処理機能	格納する鍵を暗号/複合処理する
	AP 管理機能	AP の書込/削除やダウンロードした AP の動作を制御する
	記憶領域管理機能	鍵ペアや証明書を格納する領域のアクセス制御を行う

A.4 脅威の所在と課題

— ネットワーク接続されている企業の情報漏えいに関する脅威の約 80%は組織の内部（LAN 上）に存在しており、通信事業者によって保証された専用線、ISDN、IP-VPN 等の WAN 上の脅威のみを対象とした対策だけでは端末間を結ぶ通信路のセキュリティ対策は不十分である。

— オープンネットワークは、SSL/TLS をプロトコルとした暗号通信においては WAN および LAN 上の脅威を対象として暗号化を行っている。しかし、現在は人や機器の真正性までは保証できないため、「なりすまし」によるクラッカーによる攻撃が存在するという脅威がある。さらに、下位の IP 層からの攻撃という自身では解決できない脆弱性が存在する。

— インターネット VPN は、PKI 技術等を活用して「なりすまし」の困難な認証環境を実現することによって現時点で最も安全なネットワーク環境を提供できる。また、「なりすまし」を排除することによって、プロトコル本来の機能を活かして第三者によるデータの盗聴、改ざん等のハッキング操作を検知して通信路切断ができるなどの機器間での安全な通信を保証できる。

— いずれの方式においても、許可された端末からの不正操作を防ぐことは不可能であり、ユーザの真正性を保証するユーザ認証機能については、IC カード等を用いた本人確認の為のログイン認証などの方法を組合せて対策を講じる必要がある。

A.5 ネットワークにおける脅威とセキュリティ対策の整理（チャネルセキュリティ）

A.5.1 ネットワークにおける脅威(PP)の定義

インターネットに関する脅威について､セキュリティ関連の RFC を参考に 31 の脅威の洗出しを行った。

— 平文伝送
— 共有パスワード
— 辞書攻撃
— 推定攻撃
— NIS
— 解読ツールの存在
— トポロジーの破壊
— 同一リンク上の判別
— 常用プロトコルでの攻撃
— 内部の脅威
— 情報の不正コピー
— セッション乗っ取り
— ARP 詐称（IP アドレス詐称）
— アクセスの証明
— TCP SYN パケット挿入
— TLS RST 偽装
— シーケンス番号推測攻撃
— MAC チェック未使用
— ホスト to ホスト SA
— ウィルス混入後の転送
— 情報の破壊・書換え
— メッセージ盗聴後再送
— 自動発呼による再送
— TCP　SYN フラッド攻撃
— DdoS
— 災害・物理的破壊
— 不正な用法
— 不適切な用法
— なりすまし
— サービス中断による不正処理
— 改ざん
— 過失・盗難・紛失

A.5.2 脅威への対策方法の検討

セキュリティ関連の RFC をもとに、チャネルセキュリティの脅威に対する対策に活用可能な技術要素について RFC の記述に沿って脅威と対応させて下記のように整理した。

Table A.2 — ネットワーク脅威に対しての直接的な対策を示すセキュリティ関連 RFC

脅威の定義	直接的な対策を示すセキュリティ関連 RFC
待ち伏せ攻撃（Passive Attack）＜RFC1704＞	RFC2406
	RFC3552
積極的な攻撃（Active Attack）＜RFC1704＞	RFC2406
	RFC2828
再生攻撃（Replay Attack）＜RFC1704＞	RFC3631
	RFC4107
トポロジーの破壊＜RFC3552＞	RFC2196
同一リンクの判別＜RFC3552＞	RFC3552
否認防止＜RFC3552＞	RFC3227
サービス妨害攻撃＜RFC3552＞	RFC2827

これら RFC を基盤にして守るべき資産やネットワーク上の脅威を踏まえ、脅威モデルを想定し、各ガイドラインやセキュリティ関連の RFC 等の参考文書を参照し、各種セキュリティ対策の検討、及びその有効性を評価した。現状において、利用可能な技術要素を組合せたチャネルセキュリティのセキュリティ対策として、下記に示される対策モデルが有効なセキュリティ対策と考える。

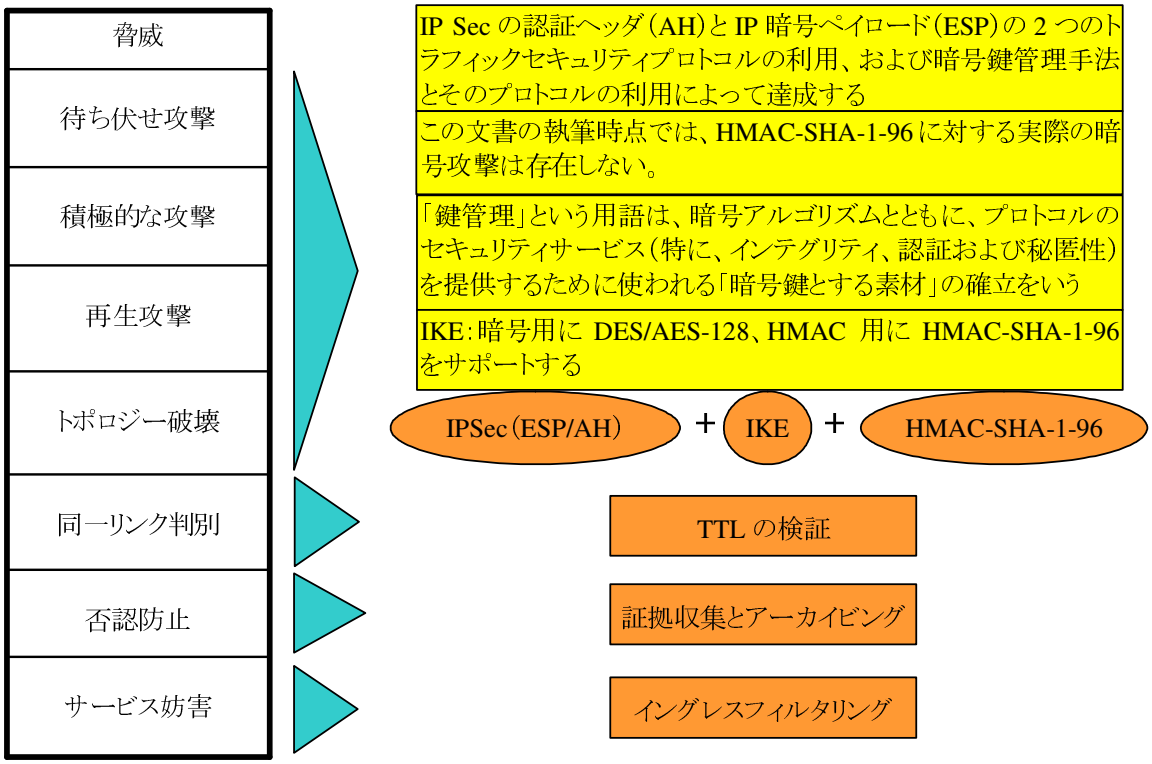


Figure A.4 — 具体的な攻撃方法を想定した脅威モデル

参考文献

Annex B （厚生労働省（2007 年 3 月）「医療情報システムの安全管理に関するガイドライン」（第 2 版）の 6.10 章）

Annex B
(informative)

外部と個人情報を含む医療情報を交換する場合の安全管理

（「医療情報システムの安全管理に関するガイドライン」（第 2 版）の 6.10 章）

B.1 基本的な考え方

ここでは、組織の外部と情報交換を行う場合に、個人情報保護およびネットワークのセキュリティに関して特に留意すべき項目について述べる。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP 型のサービスを利用する場合等が考えられる。

外部と医療情報を、外部ネットワークを利用して交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送受信データに対する「盗聴」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。

ただし、本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について記述する。

なお、医療機関等が法令による義務の有無に関わらず、個人情報を含む医療情報の保存を外部に委託する場合は、情報の不適切な二次利用を防止する等、特段の個人情報保護に関する配慮が必要なため、８章に別途まとめて記述を行う。

B.2 責任分界点の明確化

医療情報を外部に提供することは個人情報保護法上、委託と第三者提供の２種類があり、遵守すべき事項が異なる。

委託の場合、管理責任は提供元医療機関等にあり、契約と監督で管理責任を果たす責務があり、説明責任・結果責任を負わなければならない。提供先機関は契約遵守と報告義務を負う。

第三者提供の場合、提供元は同法第 23 条で規定された例外を除き、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」のⅢ－5－（3）－①のア～エに相当する場合は同ガイドラインで明記された方法で黙示の同意、それ以外の場合は明示の同意を得なければならない。また提供先は同法第 15 条、第 16 条にしたがって利用目的を特定し、同法および「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」にしたがって個人情報保護を達成する責務を負う。これらの要件を満たして提供された情報に対して提供元は責任を負わない。

オンラインで情報を提供する場合、情報の主体である患者と情報が乖離する。患者と乖離している間は情報を取り扱う事業者のどれかが責任を負う必要があり、どの事業者が責任を負っているかが明確で誤解のないものでなければならない。また患者にとっての苦情の申し入れ先や開示等の要求先が明白でなければならない。

提供元医療機関等、オンラインサービス提供事業者、回線提供事業者、提供先機関または提供先になる可能性がある事業者等が関係事業者になりえる。以下の原則で責任分界点を考える必要がある。

まず、提供元医療機関等と提供先機関は通信経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意する必要がある。その上で、自らの責任範囲において、オンラインサービス提供事業者や回線提供事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにする必要がある。ただし、前述のように結果責任、説明責任は委託の場合は提供元事業者、第三者提供の場合は提供元医療機関等または提供先機関にあり、オンラインサービス提供事業者や回線提供事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

回線事業者の提供する回線の発信元との責任分界点以前に適切に暗号化され、送信先との責任分界点以降に復号される場合は、回線事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲や回線の可用性等の品質に関しては契約で明らかにすること。

オンラインサービス提供事業者の管理範囲の開始される責任分界点に情報が到達する以前に適切に暗号化され、管理範囲の終了する責任分界点以降に復号される場合は、オンラインサービス提供事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲やサービスの可用性等の品質に関しては契約で明らかにすること。

法令で定められている場合などの特別な事情により、オンラインサービス提供事業者および回線提供事業者のいずれかに暗号化されていない医療情報が送信される場合は、オンラインサービスもしくは回線において盗聴の脅威に対する対策を施す必要があるため、当該医療情報の通信経路上の管理責任を負っている医療機関等はオンラインサービス提供事業者もしくは回線提供事業者と医療情報の管理責任についての明確化をおこない、オンラインサービス提供事業者もしくは回線提供事業者に対して管理責任の一部もしくは全部を委託する場合はそれぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければならない。

提供元医療機関等と提供先機関が１対１通信である場合、または１対Ｎであってもあらかじめ提供先または提供先となる可能性がある機関を特定できる場合は委託または第三者提供の要件にしたがって両機関等が責務を果たさなければならない。

提供元医療機関等と提供先機関が１対Ｎ通信で、提供先機関が一つでも特定できない場合は原則として医療情報を提供できない。ただし法令で定められている場合等の例外を除く。

リモートログイン機能を用いたデータアクセスには、代表的用途としてシステムメンテナンスを目的とした遠隔保守のためのアクセスが考えられる。しかし、制限がゆるいと一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。

他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。適切に管理されたリモートログイン機能のみに制限しなければならない。

B.3 医療機関等における留意事項

ここでは「B-2. 責任分界点の明確化」で述べた責任の内、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の医療機関等に受け渡しされるまでの一連の流れ全般において適用される。

ただし、誤解のないように整理しておくべきことは、ここでいう管理責任とは電子的に記載されている情報の内容であり、その記載内容や記載者の正当性の保持（真正性の確保）のことを指す。つまり、後述する「B-4. 選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても第三者がその情報を判読できないようにしておく処置のことを指す。また、改ざん検知を行うために電子署名を付与することも対策のひとつである。一方、「B-4. 選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。

このような視点から見れば、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

a)「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。例えば、ネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取られら場合、またネットワーク機器に物理的な機材を取り付けて盗み取る等、明らかな犯罪行為であり、必ずしも医療機関等の責任といえない事例も想定される。一方で、不適切なネットワーク機材の設定により、意図しない情報漏洩や誤送信等も想定され、このような場合には医療機関等における責任が発生する事例も考えられる。

このように様々な事例が考えられる中で、医療機関等においては、万が一、伝送途中で情報が盗み取られた場合、また意図しない情報漏洩や誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要がある。そのひとつの方法として医療情報の暗号化が考えられる。ここでいう暗号化とは、先に例示した通りであり、情報そのものの暗号化のことを指している。

どの程度の暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密性の高さや医療機関等で構築している情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ではあるが、少なくとも情報を伝送し、医療機関等の設備から情報が乖離する段階においては暗号化されていることが望ましい。

さらに、この盗聴防止については、例えば ID とパスワードを用いたリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は上記のような留意点を保守委託業者等に確認し、監督する責任を負う。

b)「改ざん」の危険性への対応

ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えることも重要な要素である。情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要がある。

また、後述する「B-4. 選択すべきネットワークセキュリティの考え方」のネットワークの構成によっては、情報を暗号化せずに伝送する可能性も否定できず、その場合には改ざんに対する対処は確実に実施しておく必要がある。なお、改ざんを検知するための方法としては、電子署名を用いる等が想定される。

c)「なりすまし」の危険性への対応

ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の医療機関等が確かに意図した相手であるかを確認しなくてはならない。逆に、情報の受け手となる送信先の医療機関等は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であるかを確認しなくてはならない。これは、ネットワークが非対面による情報伝達手段であることに起因するものである。

そのため、例えば通信の起点と終点で医療機関等を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられる。また、改ざん防止と併せて、送信元の医療機関等であることを確認するために、医療情報等に対して電子署名を組み合わせることも考えられる。

また、上記の危険性がサイバー攻撃による場合の対応は「6.9　災害等の非常時の対応」を参照されたい。

B.4 選択すべきネットワークのセキュリティの考え方

B.4.1 概要

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、同じく医療機関等の情報を受信する機関の外部ネットワーク接続点までのことを指し、医療機関等の内部で構成される LAN は対象とならない。ただし、「B-1．責任分界点の明確化」でも触れた通り、接続先の医療機関等のネットワーク構成や経路設計によって意図しない情報漏洩が起こる可能性については留意をし、確認をする責務がある。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等としては交換しようとする情報の機密度の整理をする必要がある。「B-2．医療機関等における留意事項」では情報そのものに対する暗号化について触れているが、同様の観点から、情報の機密度に応じてネットワーク種別も選択しなくてはならない。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、機密度の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の 2 つに類型化される。

a)　回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合

回線事業者とオンラインサービス提供事業者が提供するネットワークサービスの内、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、インターネット VPN サービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は最終的な結果責任を負うにせよ、管理責任の大部分をこれらの事業者に委託できる。もちろん自らの医療機関等

においては、善良なる管理者として注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り自医療機関等のシステムの安全管理を確認しなくてはならない。

b) 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合

例えば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入されたネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識のない者が安易にネットワークを構築し、医療情報等を脅威にさらさないように万全の対策を実施する必要がある。
そのため、例えば情報の送信元と送信先に設置される機器や医療機関内に設置されている情報発信端末、端末に導入されている機能、端末の利用者等を確実に確認する手段を確立したり、情報をやり取りする機関同士での情報の取り扱いに関する契約の締結、脅威が発生した際に備えて、通信事業者がネットワーク経路上のセキュリティを担保する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等を考慮しなくてはならない。

このように、医療機関等において医療情報をネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークの提供サービスの形態は様々存在するため、以降では幾つかのケースを想定して留意点を述べる。

B.4.2 クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、いわゆるインターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」の危険性は比較的低い。ただし、「B-2. 医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。また、ウイルス対策ソフトのウイルス定義ファイルや OS のセキュリティパッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

以下、それぞれの接続方式について特長を述べる。

a) 専用線で接続されている場合

専用線接続とは、2 地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続である。通信事業者によってネットワークの品質と通信速度（「帯域」という）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入にあたってはやり取りされる情報の重要性と情報の量等の兼ね合いを見極める必要もある。

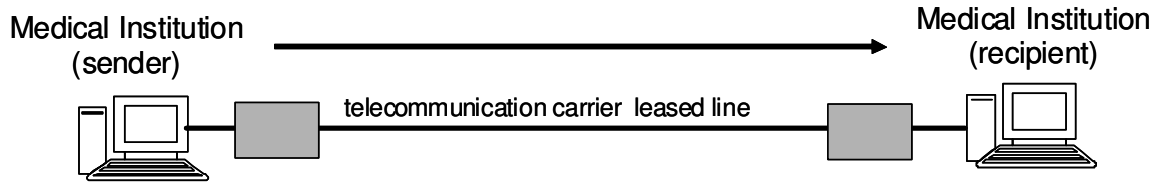


Figure B.1 — 専用線で接続されている場合

b) **公衆網で接続されている場合**

公衆網とは ISDN やダイアルアップ接続など、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続先はインターネットサービスプロバイダ（以下、ISP）に接続する接続方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISP を介して接続する場合は、ISP から先がいわゆるインターネット接続となるため、満たすべき要件としては後述する「Ⅱ．オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイアルしてネットワーク接続を確立するため、ネットワークを確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続、誤送信のリスクや専用線と同様で拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため、大量の情報もしくは画像等の容量の大きな情報を送信する際に適用範囲を適切に見定める必要がある。

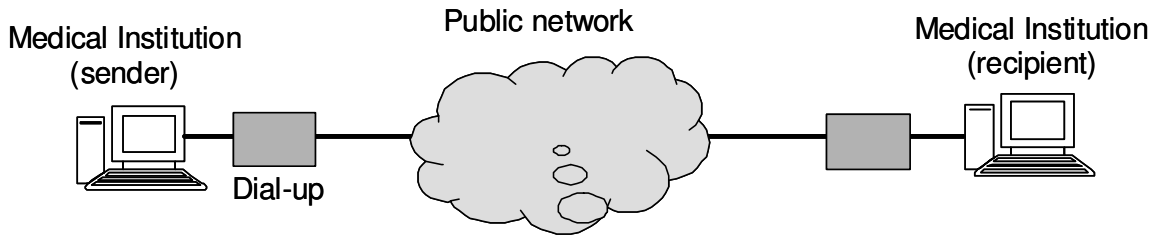


Figure B.2 — 公衆網で接続されている場合

c) **閉域 IP 通信網で接続されている場合**

ここで定義する閉域 IP 通信網とは、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を言う。このような接続サービスを本ガイドラインでは IP-VPN と呼び、クローズドなネットワークとして取り扱う。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

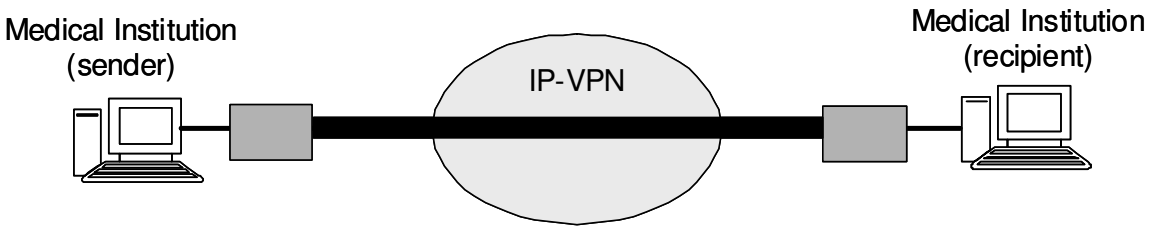


Figure B.3 — 単一の通信事業者が提供する閉域ネットワークで接続されている場合

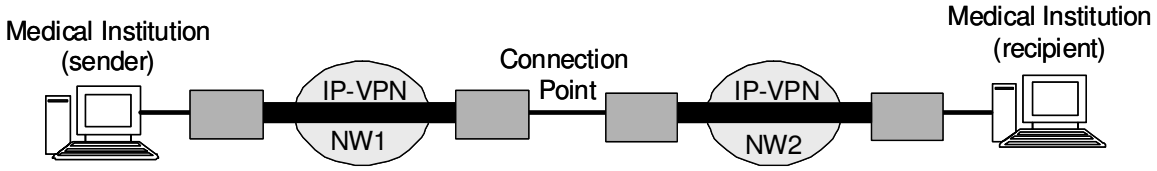


Figure B.4 —中間で複数の閉域ネットワークが相互接続して接続されている場合

以上の３つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。しかし、接続サービスだけでは一般に送られる情報そのものに対する暗号化は施されていない。また異なる通信事業者のネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとは言えない。電気通信事業法があり、万が一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。そのほか、医療機関等から閉域 IP 通信網に接続する点など、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

そのため、クローズドなネットワークを選択した場合であっても、「B-3. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入するなどの措置を取る必要がある。

B.4.3 オープンなネットワークで接続されている場合

いわゆるインターネットによる接続形態である。現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療連携の仕組みを構築したりする等、その利用範囲が拡大して行くことが考えられる。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を取らなければならない。

ただし、B-4.1 の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の自己責任において導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI 階層モデル」で定義される 7 階層のうち、どこの階層でセキュリティを担保するかによって異なってくる。OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム；HEASNET）；平成 19 年 2 月」が参考になる。

Table B.1 — OSI 階層モデル

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関係する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択ための層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電気的、物理的に変換。機器の形状・特性を規定している層

例えば、SSL プロトコルを用いる場合、5 階層目の「セッション層」と言われる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ないが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。一方、IPsec を用いる場合は、2 階層目もしくは 3 階層目の「ネットワーク層」と言われる部分より下位の層で経路の暗号化手続きがなされるため、SSL プロトコルを使った暗号通信よりは危険度が低いが、経路を暗号化するための暗号鍵の取り交しに IKE といわれる標準的手順を組み合わせる等して、確実にその安全性を確保する必要がある。

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要がある。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。

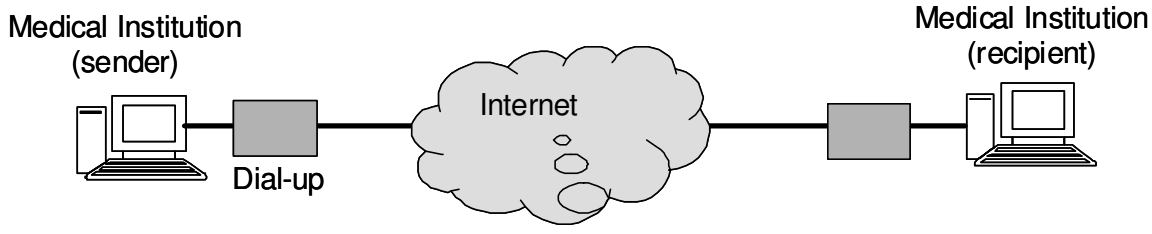


Figure B.5 —オープンネットワークで接続されている場合

B.4.4 患者等に診療情報等を提供する場合

診療情報等の開示が進む中、ネットワークを介して患者（または家族等）に診療情報等を提供する、もしくは医療機関内の診療情報等を閲覧する可能性も出てきた。本ガイドラインは、医療機関等間にお

ける情報のやり取りを想定しているが、今後、このような事例も十分想定される。そのため、ここでその際の考え方について触れる。ただし、ここで触れる考え方は、医療機関等が自ら実施して患者等に情報を提供する場合であり、第 8 章で定める診療録及び診療諸記録を外部に保存している場合は、第三者に委託しており、委託先が情報提供を行うことになるため想定しない。

ネットワークを介して患者等に診療情報等を提供する場合、第一に意識しておかなければならないことは、情報を閲覧する患者等のセキュリティ知識と環境に大きな差があるということである。また、一旦情報を提供すれば、その責任の所在は医療機関等ではなく、患者等にも発生する。しかし、セキュリティ知識に大きな差がある以上、情報を提供する医療機関等が患者等の納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任があり、説明が不足している中で万が一情報漏洩等の事故が起きた場合は、その責任を逃れることはできないことを認識しなくてはならない。

また、今まで述べてきたような専用線等のネットワーク接続形態で患者等に情報を提供することは、患者等が自宅に専用線を敷設する必要が生じるため現実的ではなく、提供に用いるネットワークとしてはオープンネットワークを介することになる。この場合、盗聴等の危険性は極めて高く、かつ、その危険を回避する術を患者等に付託することも難しい。

医療機関等における基本的な留意事項は、既に B-2 や B-3 で述べられているが、オープンネットワーク接続であるため利活用と安全面両者を考慮したセキュリティ対策が必須である。特に、患者等に情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けしておく必要がある。そのため、ファイアウォール、アクセス監視、通信の SSL 暗号化、PKI 個人認証等の技術を用いる必要がある。

このように、患者等に情報を提供する場合には、ネットワークのセキュリティ対策のみならず、医療機関等内部の情報システムのセキュリティ対策、情報の主体者となる患者等へ危険性や提供目的の納得できる説明、また非 IT に係わる各種の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にした上で実施しなくてはならない。

B.5 最低限のガイドライン

a) ネットワーク経路でのメッセージ挿入、ウイルス混入などの改ざんを防止する対策をとること。施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。セッション乗っ取り、IP アドレス詐称などのなりすましを防止する対策をとること。
上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することがあげられる。

b) データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワードなどの容易に解読されない方法を用いるのが望ましい。

c) 施設内において、正規利用者への成りすまし、許可機器への成りすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。

d) ルータなどのネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる

機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。

e) 送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化などの対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。

f) 医療機関間の情報通信には、当該医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社など多くの組織が関連する。

そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。

- 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定
- 送信元の医療機関等がネットワークに接続できない場合の対処
- 送信先の医療機関等がネットワークに接続できなかった場合の対処
- ネットワークの経路途中が不通または著しい遅延の場合の対処
- 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処
- 伝送情報の暗号化に不具合があった場合の対処
- 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
- 障害が起こった場合に障害部位を切り分ける責任
- 送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処

また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。

— 通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。
— 患者等に対する説明責任の明確化。
— 事故発生時における復旧作業・他施設や SI との連絡に当たる専任の管理者の設置。
— 交換した医療情報等に対する結果責任の明確化。
個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

g) リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。

また、メンテナンス自体は「6.8 章　情報システムの改造と保守」を参照すること。

h) 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また上記 1 および 4 を満たしていることを確認すること。

Annex C
(informative)

技術・運用基準チェックシート（「医療システムの安全管理に関するガイドライン第 2 版」向け）

C.1 はじめに

本チェックシートは、「ガイドライン第 2 版」に規定された医療機関等が医療情報を扱う際に守るべき事項を網羅的にまとめたものである。本チェックシートには、医療機関等が運用上守るべき事項から、技術的・システム的に守るべき事項まで全て網羅されている。医療機関等が自分の機関のチェックがし易いように、医療機関等をその機能によって下記のように分類し、チェックができるようにした。また、医療機関等が「ガイドライン第 2 版」を守るためには、医療機関等だけではなく、システム SI、またネットワークサービスや ASP サービス等を提供するサービス・プロバイダ（SP）は医療機関等の外にあって医療機関等の一部としてサービス機能を提供することになるため、医療機関等に準じて「ガイドライン第 2 版」の遵守をする必要がある。SP の提供するサービス内容や機能がこれを満足している必要がある。このため、チェックシートをサービス機能の提供者とそのチェックすべき事項に沿って、医療機関の管理者、システム SI、SP のチェックシートに分けた。

a) 大規模機関
大規模機関は、機関内の LAN 経由で複数の職員が医療情報や経理情報等の個人情報や機密情報を入出力や共有する。さらに、情報交換または情報提供するための設備を所有し、それらの一部の情報については、外部と下記のような NW 構成で情報交換する。大規模機関の構成を Figure C.1 に示す。

b) 小規模機関
小規模機関は、機関内の LAN 経由で複数の職員が医療情報や経理情報等の個人情報や機密情報を入出力や共有します。インターネット接続、メール等の情報交換、情報提供や外部保存等のサービスは SP の提供サービスを利用する。外部とは Figure C.2 のような NW 構成で情報交換する。

c) SPs
SP は、医療機関等で発生した個人情報や機密情報を外部保存、またはその一部の情報を他の機関と情報交換または情報提供するための設備を所有し、それらの情報を下記のような NW 構成で情報交換する。また、タイムスタンプ、インターネット接続、コンテンツ・スクリーニング等の共通的なサービスも提供する。

大規模機関、小規模機関、SP の特徴と、使用するチェックシート Table C.1 にまとめました。

Table C.1 — 各機関の概要

	医療機関等		ＳＰ
	大規模機関	小規模機関	
機能・設備	外部に情報提供できる設備を有する	外部に情報提供できる設備を有しない	回線事業者・オンラインサービス提供事業者
参照図	Figure C.1	Figure C.2	Figure C.3
必要となるチェックシート	大規模機関チェックシート	小規模機関チェックシート	ＳＰチェックシート

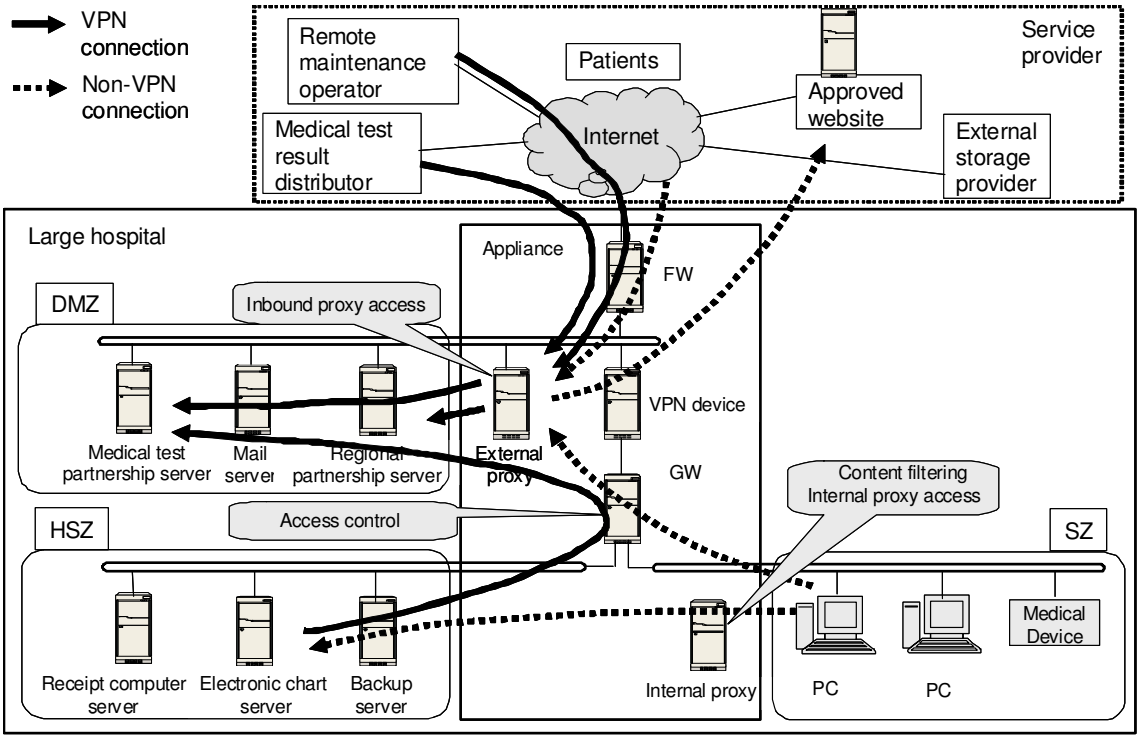


Figure C.1 — 大規模機関のネットワーク構成例

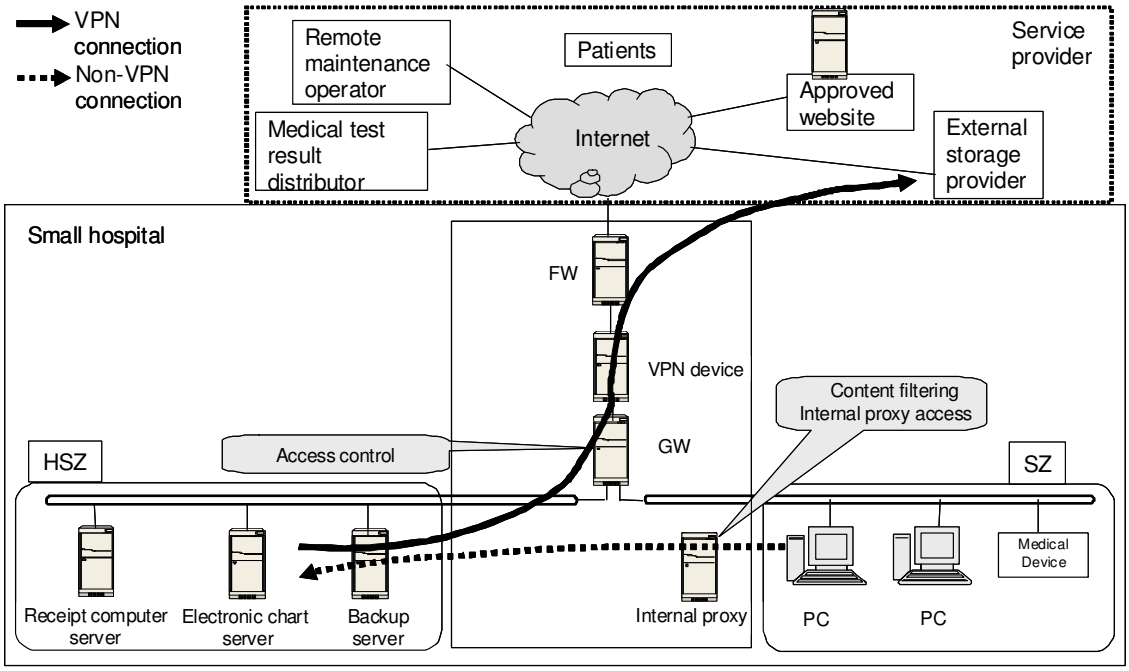


Figure C.2 — 小規模機関のネットワーク構成例

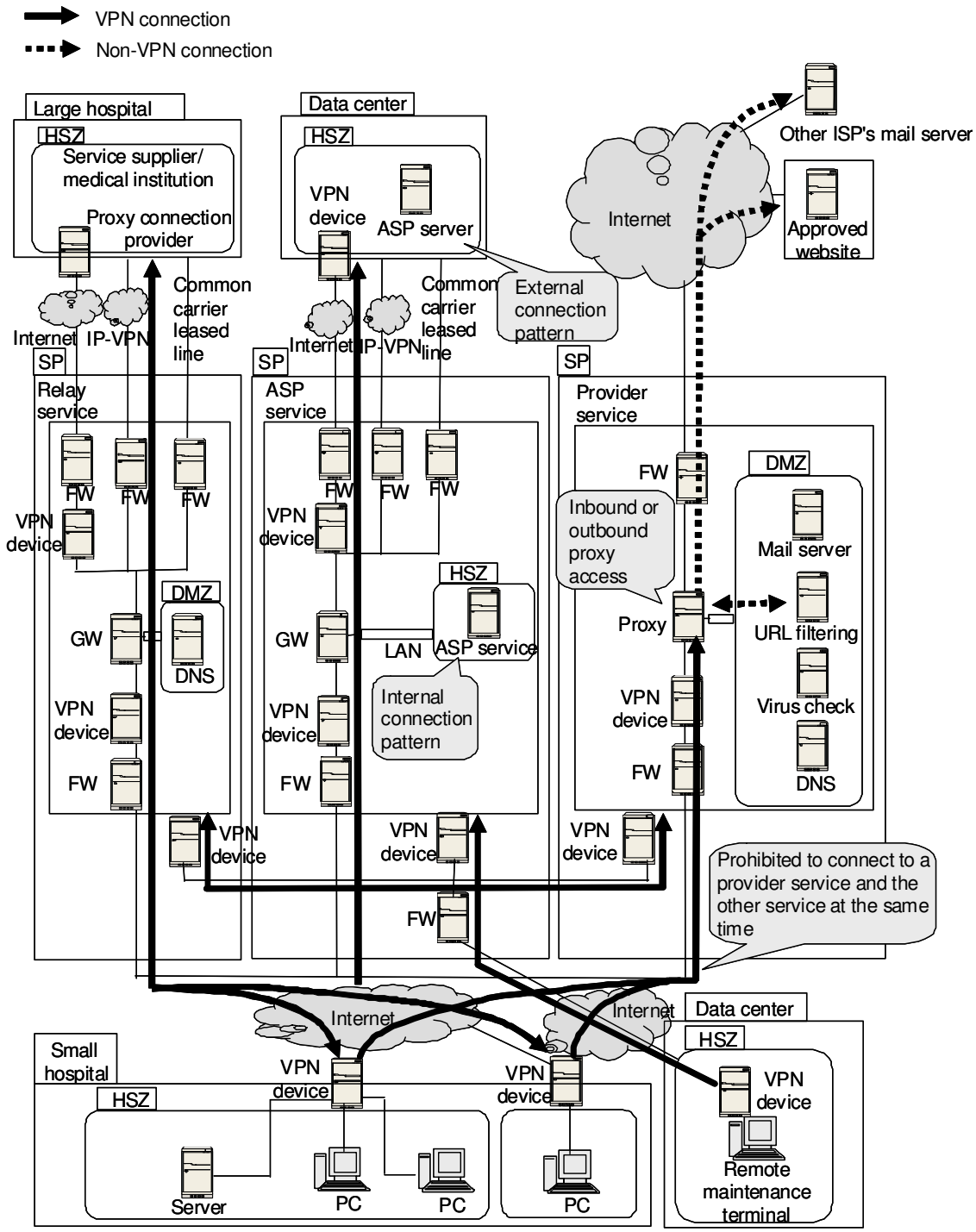


Figure C.3 — SP のネットワーク構成例

C.2　大規模機関用チェックシートの使用方法について

このチェックシートは外部に情報提供できる設備を有する（SP サービスを外部へ提供できる）医療機関等について、チェックを実施するためのものである。外部に情報提供できる設備を有さない（SP サービスを外部へ提供できない）医療機関等については、小規模機関用チェックシートを利用する。

(1) チェックシートの構成について

大規模機関用チェックシートはチェック実施者の種別に応じて、管理者用チェックシート、SI 用チェックシート、SP 用チェックシートの３枚より構成される。

Table C.2 — 大規模機関のチェックシート構成

実施者の種別	定義	大規模機関			備考
		管理者チェックシート	SI チェックシート	SP チェックシート	
管理者	各機関を運営する組織、またはその管理責任者を対象としている。	○（※）	－	－	（※）各機関の管理者が、チェックが出来ない項目については、SI の設計責任者に確認すること。
SI	各機関のネットワークおよびシステムを設計・構築するシステムインテグレータ等を対象としている。	－	○	－	
SP	提供するサービス機能を外部委託（アウトソーシング）する場合に、その委託先の SP の運営する組織、またはその管理責任者を対象としている。	－	－	○（※）	

(2) チェックシートのチェック項目について

Table　C.3 に、チェック実施対象者とチェックシートの各入力項目との関係を示す。○部分は全てチェックを実施し、また▲部分については、該当するサービス（提供サービスや利用サービス）に応じてチェックを実施する。

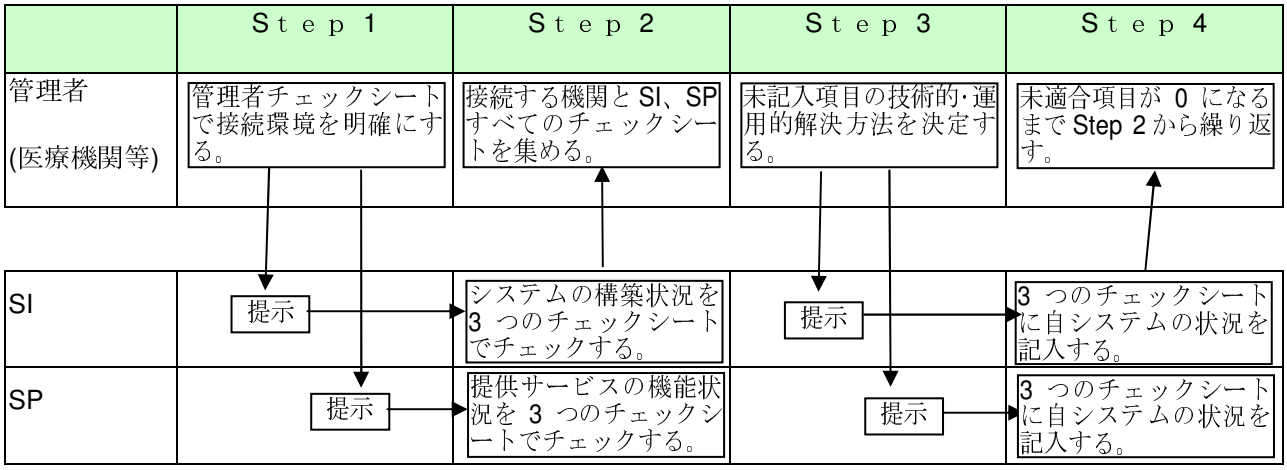
Table C.3 — 大規模機関における提供サービスとチェックシートの対応

提供サービス項目	「医療情報システムの安全管理に関するガイドライン」 技術・運用基準チェックシート		
	大規模機関		
	管理者チェックシート	ベンダチェックシート	SPチェックシート
1. 通信形態	○		
2. 通信ポリシー	○	○	○
3. 拠点内の技術的セキュリティ	○	○	○
4. サービス種別			
4-1 医療機関向けの情報提供ASPサービスの展開	▲	▲	
4-2 医療機関向けの情報提供ASPサービスの利用			
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用	▲	▲	▲
4-4 医療機関以外への情報提供ASPサービスの展開	▲	▲	
4-5 医療機関以外への情報提供ASPサービスの利用			
4-6 医療機関以外への情報提供ASPサービス（外部保存型）の利用	▲	▲	▲
4-7 メールサービス（プロバイダサービス）	▲	▲	
4-8 インターネット接続サービス（プロバイダサービス）	▲	▲	
4-9 リモート保守サービスの利用	▲	▲	
4-10 外部サービス提供機関/大規模医療サービス機関への接続（中継サービス）	▲	▲	▲
5. 拠点内の物理的セキュリティ	○	○	

*1 サービス種別の▲ヶ所は、提供サービス（または利用サービス）に応じてチェックすること。
個別サービスを提供・利用する際は、該当する全ての個別項目をチェックすること。

チェックシートのチェック手順を Figure C.4 に示す。下記手順でガイドラインへの適合性チェックを実施する必要がある。

Figure C.4 — 大規模機関のチェック手順



医療機関等の管理者は、本チェックシートで SI 並びに SP の提供するサービス内容や機能について確認した上で、未対応項目に対する対策や責任の分担を明確にしてから導入すべきである。責任の分担については、書面にて取交すことを徹底するべきである。

大規模機関用チェックシートを Table C.4 に示す。

Table C.4 — 大規模機関のチェックリスト

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
1. 通信形態							
1-1 接続相手の確認	1-1-1 他の接続先拠点におけるセキュリティ基準の確認	-	異なる法人の大規模機関型拠点と接続する場合、接続する大規模機関型拠点は「大規模機関チェックシート」の項目をチェックし、条件を満たしている。	異なる法人と接続を行う際は、接続相手のセキュリティポリシーを明確にし、責任を明確にする必要がある。すべての接続拠点のチェックシートが条件を満たすように運営されている。	□	6.11 B-1 6.11 B-3	
		-	異なる法人の小規模機関型拠点と接続する場合、接続する小規模機関型拠点は「小規模機関型 チェックシート」の項目をチェックし、条件を満たしている。		□		
		-	サービスプロバイダと接続する場合、接続するサービスプロバイダは「サービスプロバイダチェックシート」の項目をチェックし、条件を満たしている。		□		
2. 通信ポリシー							
2-2 オープンネットワークの利用した拠点間の接続	2-2-1 同一法人以外の複数拠点と接続する場合の不正中継。異なる法人間で複数接続を行う際は、責任主体は各拠点にあり、不正な中継を禁止する必要がある。	VPN機能	ネットワークを利用して拠点間の接続をする場合、自拠点と接続された二つ以上の拠点を結んで不正な中継が禁止されてい				
			ネットワークを利用して拠点間の接続をする場合、拠点と接続された２つ以上の拠点を結んで不正な中継が禁止されているかチェックする。	左記の不正な中継を禁止する対策が行われている。	□	6.11 C 4	
2-3 他拠点との接続処理	2-3-1 接続先拠点との通信に関する合意	VPN機能	下記の項目について拠点間で確認を行う。				
			文書によるサービス内容・運用形態の確認と合意がされている	左記の不正な中継を禁止する対策が行われている。	□	6.5 B (5)	
			VPN通信における合意がされている				
3. 拠点内の技術的セキュリティ							
3-3 High Secure Zone のセキュリティ	3-3-4 大規模機関のHigh Secure Zoneを起点とした他拠点への接続	プロキシ機能 ／VPN機能 ／ファイアウォール機能	大規模機関への接続において、SPのHigh Secure Zoneにある重要データや機器を改ざんや侵入から守るため、次のセキュリティ機能を整備する必要がある。				
			サービス妨害（DoS攻撃など）対策している。	左記の対策を実施しない場合は、High Secure Zoneからの大規模機関への接続を行わない。	□	6.5 B (1) 6.5 B (2) 6.5 B (3) 6.5 B (4) 6.5 B (5)	
			データの改ざん、不正侵入などに対する検知・防御・遮断対策している。				
			安全なインターネット接続の担保をしている。				
			ウィルス感染対策を行っている。				
			接続における認証を行っている。				
			通信経路の安全対策をしている。				
			アクセス監視をしている。				

3-5 DMZ のセキュリティ	3-5-1 各ホストに対するウィルスチェック	各ホスト	ウィルスチェックが正常に機能しているかチェックする。				
			ウィルス定義ファイルは常に最新のものを使用している。	格納したデータにウィルスが混在されていた場合の、発病・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。	□	6.5 B (4)	
3-6 内部セキュリティサービス	3-6-1 拠点内におけるセキュリティパッチなどの更新機能の実装	ゲートウェイ機能 ／プロキシ機能	セキュリティパッチの状態をチェックする。				
			パッチファイルは常に最新の状態である。	セキュリティパッチなどをインターネット経由で行う際、インターネット通信を許可されていないホスト・ゾーンに対して、パッチのダウンロードを行い必要なホストに配布することでセキュリティホールに対する攻撃の対策を行う。	□	6.5 B (4) 6.5 B (5) 6.11 B-3 I	
4. サービス種別							
4-1 医療機関向けの情報提供ASPサービスの展開 【提供サービス項目例】 ・情報提供サービス ・メールサービス ・地域連携サービス ・検査データ配信サービス ・外部保存サービス ・タイムスタンプサービス ・VAサービス	4-1-1 医療機関向けの情報提供または公開	ファイアウォール機能	不正利用防止のため次のセキュリティ対策が行われているかチェックする。				
			アクセス制限により不正利用を防止する。	ファイアウォールなどによるセキュリティ対策を行い、接続先拠点と通信に関して合意がなされている接続先・接続元IP アドレスのみ接続を許可し、合意のなされていない自拠点から他拠点への不正なアクセスと、その逆を防ぐ。	□	6.10 C (9) 6.11 B2	
	4-1-2 サービス提供ユーザの認証	サーバ機能	ASPサービスの提供においてユーザを識別するための認証しているかチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.5 B (1) 6.5 C (7) 6.10 C (9)	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリック認証を行う。		□		
	4-1-3 外部ASPからのサービス機能の提供を受ける場合にオープンネットワークを利用する場合のセキュリティ対策	プロキシ機能 ／VPN機能 ／ファイアウォール機能	実施されているセキュリティ対策をチェックする。				
			セキュリティ対策				
			ウィルス、DoS攻撃等に対する防御対策を行う。	医療機関向けに情報を公開・提供する場合、High Secure Zoneにある重要データや機器を改ざんや侵入から守るため、左記のセキュリティ機能を実装する。	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)	
			改ざんや侵入に対する不正パケットの検知・遮断対策をしている。				
			アクセス監視をしている。				
			なりすまし防止のための通信経路の暗号化対策を行う。			6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-1-4 データまたは機器のHigh Secure Zoneへの配置・格納	ゾーン	医療機関向けに情報提供を行う場合、重要データや機器を改ざんや侵入から守るために次のセキュリティ対策を整備する。				
			ゾーン種別				
			High Secure Zoneに配置している。	ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してHigh Secure Zoneに配置をする。	□	6.10 C (9) 7.3 B 7.4 C	

4-2 医療機関向けの情報提供ASPサービスの利用 【提供サービス項目例】 ・情報提供サービス ・メールサービス ・地域連携サービス ・検査データ配信サービス ・外部保存サービス ・タイムスタンプサービス ・VAサービス	4-2-1 ASPサービスを利用する利用者の認証	サーバ機能	ASPサービス利用時のユーザ認証を行うの方法についてチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.5 B (1) 6.5 C (7) 6.10 C (9)	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリック認証を行う。		□		
	4-2-2 情報提供ASPサービスの利用におけるセキュリティ対策	プロキシ機能 ／VPN機能 ／ファイアウォール機能	小規模機関にて実施されているセキュリティ対策をチェックする。				
			セキュリティ対策				
			ウィルス、DoS攻撃等に対する防御対策を行う。	ASPサービスにおいては、High Secure Zoneにある医療情報等の重要データや機器を改ざんや侵入から守るため、左記のセキュリティ要件を整え、接続を行う。	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)	
			改ざんや侵入に対する不正パケットの検知・遮断対策をしている。				
			アクセス監視をしている。				
			なりすまし防止のための通信経路の暗号化対策を行う。			6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-2-3 ASPサービスを利用する際の中継サービス、プロバイダサービスとの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			プロバイダサービスとの同時利用の禁止を行う。	中継サービス、プロバイダサービス、リモート保守サービスとの同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 C (9) 6.11 B-3	
			中継サービスとの同時利用の禁止を行う。				
	4-2-4 ホストのHigh Secure Zoneへの配置・格納	ゾーン	ASPサービスにより取得した医療情報がHigh Secure Zoneに格納されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してHigh Secure Zoneに配置をする。	□	6.10 C (9) 7.3 B 7.4 C	
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用 【提供サービス項目例】 ・アウトソーシング	4-3-1 外部保存型ASPサービスを利用するホスト・機器の配置。	ゾーン	利用するホスト・機器がHigh Secure Zoneに配置されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	不正なアクセスによる改ざん・情報漏えいを防ぐため、外部保存サービスを提供する機器へのアクセスはHigh Secure Zoneに配置されたホスト端末のみ許可する。	□	6.4 B③ 6.10 C (9)	
4-4 医療機関以外への重要情報提供ASPサービスの展開 【提供サービス項目例】 ・情報提供サービス ・メールサービス ・地域連携サービス ・外部保存サービス ・タイムスタンプサービス ・VAサービス	4-4-1 情報の提供または公開	ファイアウォール機能	不正利用防止のため次のセキュリティ対策が行われているかチェックする。				
			アクセス制限により不正利用を防止する。	ファイアウォールなどによるセキュリティ対策を行い、接続先拠点と通信に関して合意がなされている接続先・接続元IP アドレスのみ接続を許可し、合意のなされていない自拠点から他拠点への不正なアクセスと、その逆を防ぐ。	□	6.10 C (9) 6.11 B2	
	4-4-2 サービス提供ユーザの認証	サーバ機能	ASPサービスの提供においてユーザを識別するための認証しているかチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.5 B (1) 6.5 C (7) 6.10 C (9)	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリック認証を行う。		□		

	4-4-3 外部ASPからのサービス機能の提供を受ける場合にオープンネットワークを利用する場合のセキュリティ対策	プロキシ機能 ／VPN機能 ／ファイアウォール機能	実施されているセキュリティ対策をチェックする。				
			セキュリティ対策				
			ウィルス、DoS攻撃等に対する防御対策を行う。 改ざんや侵入に対する不正パケットの検知・遮断対策をしている。 アクセス監視をしている。 なりすまし防止のための通信経路の暗号化対策を行う。	重要な情報を公開・提供する場合、High Secure Zoneにある重要データや機器を改ざんや侵入から守るため、左記のセキュリティ機能を実装する。	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-4-4 重要なデータまたは機器のHigh Secure Zoneへの配置・格納	ゾーン	医療機関向けに情報提供を行う場合、重要データや機器を改ざんや侵入から守るために次のセキュリティ対策を整備する。				
			ゾーン種別				
			High Secure Zoneに配置している。	ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してHigh Secure Zoneに配置をする。	□	6.10 C (9) 7.3 B 7.4 C	
4-5 医療機関以外での重要情報提供ASPサービスの利用 【提供サービス項目例】 ・情報提供サービス ・メールサービス ・地域連携サービス ・外部保存サービス ・タイムスタンプサービス ・VAサービス	4-5-1 ASPサービスを利用する利用者の認証	サーバ機能	ASPサービス利用時のユーザ認証を行うの方法についてチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。 ICカード/スマートカードでの認証を行っている。 バイオメトリック認証を行う。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□ □ □	6.5 B (1) 6.5 C (7) 6.10 C (9)	
	4-5-2 情報提供ASPサービスの利用におけるセキュリティ対策	プロキシ機能 ／VPN機能 ／ファイアウォール機能	小規模機関にて実施されているセキュリティ対策をチェックする。				
			セキュリティ対策				
			ウィルス、DoS攻撃等に対する防御対策を行う。 改ざんや侵入に対する不正パケットの検知・遮断対策をしている。 アクセス監視をしている。 なりすまし防止のための通信経路の暗号化対策を行う。	ASPサービスにおいては、High Secure Zoneにある重要データや機器を改ざんや侵入から守るため、左記のセキュリティ要件を整え、接続を行う。	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9) 6.10 C (9) 6.11 B-1 6.11 B 3 6.11 C 1	
	4-5-3 ASPサービスを利用する際の中継サービス、プロバイダサービスとの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			プロバイダサービスとの同時利用の禁止を行う。 中継サービスとの同時利用の禁止を行う。	中継サービス、プロバイダサービス、リモート保守サービスとの同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 C (9) 6.11 B-3	
	4-5-4 ホストのHigh Secure Zoneへの配置・格納	ゾーン	ASPサービスにより取得した重要な情報がHigh Secure Zoneに格納されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してHigh Secure Zoneに配置をする。	□	6.10 C (9) 7.3 B 7.4 C	
4-6 医療機関以外での重要情報提供ASPサービス（外部保存型）の利用 【提供サービス項目例】 ・アウトソーシング	4-6-1 外部保存型ASPサービスを利用するホスト・機器の配置。	ゾーン	利用するホスト・機器がHigh Secure Zoneに配置されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	不正なアクセスによる改ざん・情報漏えいを防ぐため、外部保存サービスを提供する機器へのアクセスはHigh Secure Zoneに配置されたホスト端末のみ許可する。	□	6.4 B③ 6.10 C (9)	

4-7 メールサービス（プロバイダサービス） 【提供サービス項目例】 ・メールサービス	4-7-1 メールのスクリーニングの実施	ゲートウェイ機能	スパムメール・ウィルス添付メール等から内部が守られているかチェックする。				
			メールの送受信を行う相手が制限されている。 スパムメールを防止している。 送受信時にウィルスチェックが行われ、不審なメールは削除もしくは隔離されている。	High Secure Zoneにある重要データや機器を改ざんや侵入から守るため、左記のセキュリティ対策を行わなければならない。対策を実施しない場合は、サービスの利用を禁止する。	□	6.5 B (4) 6.5 B (5)	
	4-7-2 不正なメール転送の禁止	メール機能	メール転送が適切に行われているかチェックする。				
			適切なメール転送処理を行っている。	不正メール転送の踏み台になることを防止しなければならない。	□	6.5 B (4) 6.5 B (5)	
	4-7-3 メールサービスを提供するユーザの認証	ゲートウェイ機能／サーバ機能	メールサービスの提供において認証にどのような方法を用いているかチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。 ICカード/スマートカードでの認証を行っている。 バイオメトリック認証を行う。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□ □ □	6.5 B (1) 6.5 C (7)	
	4-7-4 ユーザによる他ISPメールサーバ（Webメール）の利用	ゲートウェイ機能／プロキシ機能	ユーザの希望によりWebメールを利用する場合、利用上のリスクについて説明と合意が行われたかチェックする。				
			SPが提供するインターネット接続サービスを利用したWebメールを利用している。	インターネット接続サービスにおけるWebメールの利用にあたっては、利用上のリスク等についてユーザへ説明し、合意を行った上で利用を許可する。	□	8.1.3 C (1)②	
	4-7-5 メールサービス（プロバイダサービス）を利用する際の中継サービス、ASPサービスとの同時利用を禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			ASPサービスとの同時利用を禁止しているしている。 中継サービスとの同時利用の禁止を行う。	中継サービス、ASPサービス、リモート保守サービスとの同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.11 B-3	
4-8 インターネット接続サービス（プロバイダサービス） 【提供サービス項目例】 ・インターネット接続サービス	4-8-1 サイト閲覧の制限	ゲートウェイ機能	業務・サービスで必要なサイトのみ閲覧を許可しているかチェックする。				
			URLホワイトリスト機能によるスクリーニングが行われている。 スクリーニングにより不適切なサイトが閲覧できないようになっている。 コンテンツフィルタにより、必要のない実行プログラムが動作しないようになっている。	左記の機能により、業務上で必要なサイトのみを許可し、不正サイトによるウィルスの混入・情報漏えいなどを防止しなければならない。	□	6.5 B (4) 6.5 B (5)	
	4-8-2 インターネット接続サービスを利用するユーザの認証	ゲートウェイ機能／サーバ機能	インターネット接続サービスの提供においてユーザを認証する機能にどの技術を用いているかチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。 ICカード/スマートカードでの認証を行っている。 バイオメトリックによる認証を行っている。	サービスを提供しているユーザを認証することで、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□ □ □	6.11 B-1 6.11 C-7 8.1.1 C③	
	4-8-3 インターネットのサイト閲覧に際して、外部サービス提供機関への中継サービス、ASPサービスとの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			ASPサービスとの同時利用を禁止しているしている。 中継サービスとの同時利用の禁止を行う。	中継サービス、ASPサービスとの同時利用を禁止しているしている。することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる	□	6.11 B-3	

4-9 リモート保守サービスの利用 【提供サービス項目例】 ・リモート保守サービス	4-9-1 リモート保守端末の配置	ゾーン	利用するホスト・機器がHigh Secure Zoneに配置されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	リモート保守作業およびリモート監視において、システムの機器または情報を守るため、High Secure Zoneへ配置しなければならない。	□	8.1	
	4-9-2 リモート保守作業者の認証	ゲートウェイ機能／サーバ機能	リモート保守作業者の利用者認証にどのような方法を用いているかチェックする。				
			導入される認証技術				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.11 B-1 6.11 C-7 8.1.1 C③	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリックによる認証を行っている。		□		
	4-9-3 リモート保守作業者による不正作業・操作を防ぐための対策	–	リモート保守において導入されている規定をチェックする。				
			規定すべき要件				
			リモート保守作業者の管理規定を設けている。	個人情報の保護やシステムの安全な運用を行うために、左記の運用規定等を設けている。	□	8.1.1 C③	
			リモート端末、ネットワークに関する管理規定を設けている。				
			リモート端末を許可された要員以外による不正操作を防ぐ対策規定を設けている。				
			リモート保守作業を行う際の記録、授受データの処理に関する規定を設けている。				
			リモート端末が増設・移動される場合の規定を設けている。				
4-10 外部サービス提供機関/大規模医療サービス機関への接続（中継サービス） 【提供サービス項目例】 ・VPNサービス ・IXサービス ・ASPサービス	4-10-1 外部のサービス提供機関に接続する機器またはデータの配置	ゾーン	外部のサービス提供機関に接続する機器がHigh Secure Zoneに配置されているかチェックする。				
			外部のサービス提供機関に接続する機器が設置されたゾーン				
			High Secure Zoneに配置している。	システムの機器または情報を守るため、High Secure Zoneへ配置する。	□	6.5 B (5) 6.10 C (9)	
	4-10-2 外部サービス提供機関のサービス提供を受けるユーザの認証	ゲートウェイ機能／サーバ機能	外部サービス提供機関のサービスの利用者認証にどのような方法を用いているかチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.10 C (9) 6.11 B-1 6.11 C-7 8.1.1 C③	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリックによる認証を行っている。		□		
	4-10-3 外部サービス提供機関との接続におけるセキュリティ対策	–	実施されているセキュリティ対策をチェックする。				
			ウィルス、DoS攻撃等に対する防御対策を行う。	High Secure Zoneにある重要データや機器を改ざんや侵入から守るため、守るべきセキュリティ要件を整え、接続を行う。	□	6.5 B (1) 6.5 B (4) 6.5 B (5) 6.10 C (9)	
			改ざんや侵入に対する不正パケットの検知・遮断対策をしている。				
			利用者認証を行う。				
			アクセス監視をしている。				
	4-10-4 外部サービス提供機関との中継サービスにおいて、プロバイダサービス、ASPサービスの同時利用の禁止	–	他サービスとの同時利用を禁止しているかチェックする。				
			ASPサービスとの同時利用を禁止している。	プロバイダサービス、ASPサービスの同時利用を禁止し、何らかのインシデントが発生した場合の他サービスへの脅威の拡散を防ぐ。	□	6.10 C (9) 6.11 B-3	
			プロバイダサービスとの同時利用の禁止を行う。				
	4-10-5 外部サービス提供機関との接続に関する文書等による合意と接続認可	–	外部サービス提供機関との接続に際してチェックする。				
			文書によるサービス内容・運用形態の確認を行う。	外部サービス提供機関との接続を行うにあたっては、文書等による合意と接続認可を受ける。	□	6.10 C (9) 6.5 B (5)	
			サービス提供機関との合意と接続認可を行う。				

6. 無線LAN・モバイル・リモートアクセス							
6-1 無線・モバイルのセキュリティ	6-1-1 無線LANのセキュリティ	無線機能	無線LANの使用を特定されないような対策が採られているかチェックする。				
			対策項目				
			ステルスモード	ステルスモードが設定されている。	□	6.5 C-8	
			ANY接続拒否	ANY接続拒否が設定されている。	□		
			不正アクセス対策がされているかチェックする。				
			対策項目				
			SSIDによるアクセス制限	SSIDによってアクセス制限をしている。	□	6.5 C-8	
			MACアドレスによるアクセス制限	MACアドレスによってアクセス制限をしている。	□		
			電子証明書	電子証明書によってアクセスチェックしている。	□		
			不正な情報取得に対する対策がされてる。				
			対策項目				
			WPA/TKIPによる暗号化	WPA/TKIPによって暗号化している。	□	6.5 C-8	
			WPA2/AESによる暗号化	WPA2/AESによって暗号化している。	□		
			無線LANの業務利用エリアにおける、電波干渉による利用トラブルへの対策をおこなっている。				
			対策項目				
			PCのアドホックモードの禁止	PCのアドホックモードを禁止している。	□	6.5 C-8	
			電波を発する機器の利用（ゲーム機など）の制限	電波を発する機器の利用（ゲーム機など）を制限している。	□		
	6-1-2 情報および情報機器の持ち出し管理	無線機能	情報および情報機器の運用規定の内容をチェックする。				
			対策項目				
			持ち出し管理の運用規定	持ち出し管理に関する運用規定を定めている	□	6.9 C-1～4 6.9 C-10	
			管理方法	情報および情報機器の管理方法を定めている	□		
			盗難、紛失時の対応	盗難、紛失時の対応を運用規定内に含めている	□		
			教育	運用規定の教育および周知徹底している	□		
			個人所有の端末	個人所有の端末においても同等の対策を行っている	□		
			情報が格納された情報機器、可搬媒体の所在を把握しているかチェックする。				
			対策項目				
			所在把握	情報の種類、機器などを台帳管理している	□	6.9 C-5	
			情報機器に対するパスワードの設定指導項目をチェックする。				
			対策項目				
			パスワード	起動パスワードを設定	□	6.9 C-6	
			なりすまし対策	推定されやすいパスワードの設定回避	□		
				定期的にパスワードを変更	□		
			盗難、紛失時の対策のための指導項目をチェックする。				
			対策項目				
			暗号化	ディスク、ファイルなどの暗号化をしている。	□	6.9 C-7	
			パスワード	アクセスパスワードを設定している。	□		
			情報機器をネットワークに接続する際の漏洩、改ざんなどへの対策の指導項目をチェックする。				
			対策項目				
			コンピュータウィルス対策	コンピュータウィルス対策ソフトを導入している。	□	6.9 C-8	
			ファイアウォール	パーソナルファイアウォールを導入している。	□		
			不正な利用環境のチェックをする。				
			対策項目				
			利用環境の制限	ファイル交換ソフト（Winnyなど）などがインストールされた端末での利用を禁止している。	□	6.9 C-9	

6-1-3 医療情報もしくは医療機関へのアクセスの個人端末の利用する際の環境の管理	無線機能	情報機器に対するパスワードの設定指導項目をチェックする。					
		対策項目					
		パスワード	起動パスワードを設定	□	6.9 C-6		
		なりすまし対策	推定されやすいパスワードの設定回避	□			
			定期的にパスワードを変更	□			
		盗難、紛失時の対策のための指導項目をチェックする。					
		対策項目					
		暗号化	ディスク、ファイルなどの暗号化をしている。	□	6.9 C-7		
		パスワード	アクセスパスワードを設定している。	□			
		情報機器をネットワークに接続する際の漏洩、改ざんなどへの対策の指導項目をチェックする。					
		対策項目					
		コンピュータウィルス対策	コンピュータウィルス対策ソフトを導入している。	□	6.9 C-8		
		ファイアウォール	パーソナルファイアウォールを導入している。	□			
		不正な利用環境のチェックをする。					
		対策項目					
		利用環境の制限	ファイル交換ソフト(Winnyなど)などがインストールされた端末での利用を禁止している。	□	6.9 C-8		
6-1-4 モバイルを使用する際の考え方	無線機能	選択するサービスの仕様を確認する。					
		対策項目					
		契約確認	事業者に対して契約の確認をしている。	□	6.10 C-6 6.10 C-8		
		盗聴･改ざんを防ぐことが可能な仕組みを導入しているかチェックする。					
		対策項目					
		コンテンツの暗号化	SSL通信の使用	□	6.10 C-5		
			コンテンツの暗号化がされている	□			
			メールの場合はS/MIMEを使用している	□			
		(公衆網（電話網）を経由して直接ダイアルアップする場合)					
		接続先が間違いないかどうかを確認する。					
		対策項目					
		接続先確認	接続設定を確認する。	□	6.10 C-2		
		アクセス認証されているかを確認する。					
		対策項目					
		アクセス認証	ID,PWやワンタイムPWによるアクセス認証がされている	□	6.10 C-3 6.5		
				□			
				□			
		(インターネットを経由して接続する場合)					
		使用する端末の仕様の確認を行う。					
		対策項目					
		通信仕様	端末でSSL通信が利用できる	□	6.10 C-5		
		サービスの仕様を確認する。					
		対策項目					
		通信仕様	接続経路にIPSecとIKEが適用されている	□	6.10 C-1		
		(閉域ネットワーク（IP-VPN網）を経由して接続する場合)					
		使用する端末の仕様の確認を行う。					
		対策項目					
		通信仕様	端末でSSL通信が利用できる	□	6.10 C-5		

	6-1-5 患者等に診療情報等を提供する場合のネットワークに関する考え方(4-4 医療機関以外への重要情報提供ASPサービスの展開とチェックと比べて矛盾しないこと)	無線機能	不正な利用環境のチェックをする。					
			対策項目					
			院内システムの確認を行う	システムやアプリケーションを切り分けを実施している	□	6.10 C-9		
			情報を公開しているコンピュータシステムを通じ，医療機関等の内部のシステムに不正な侵入等が起こらないようにする。					
			対策項目					
			ファイアウォール	ファイアウォールを導入している。	□	6.10 C-9		
			アクセス監視	アクセス監視の実施している	□			
			SSL通信による暗号化	SSL通信による暗号化が行われている	□			
			PKI個人認証等の対策	PKI個人認証等の対策を行う	□			
			患者への説明がなされているか。					
			対策項目					
			患者説明	患者へ危険性や提供目的の納得できる説明を実施している	□	6.10 C-9		
			責任分界点が明確化にする。					
			対策項目					
			責任分界点	ITに係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にしている	□	6.10 C-9		

C.3 小規模機関用チェックシートの使用方法について

このチェックシートは外部に情報提供できる設備を有しない医療機関等について、チェックを実施するためのものである。外部に情報提供できる設備を有する（SP サービスを外部へ提供できる）医療機関等については、大規模機関用チェックシートをご利用すること。

a) チェックシートの構成について

小規模機関用チェックシートはチェック実施者の種別に応じて、管理者用チェックシート、SI 用チェックシートの 2 枚より構成される。

Table C.5 — 小規模機関のチェックシート構成

実施者の種別	定義	小規模機関		備考
		管理者チェックシート	SI チェックシート	
管理者	各機関を運営する組織、またはその管理責任者を対象としている。	○（※）	-	（※）各機関の管理者が、チェックが出来ない項目については、SI の設計責任者に確認すること。
SI	各機関のネットワークおよびシステムを設計・構築するシステムインテグレータ等を対象としている。	-	○	

b)　チェックシートのチェック項目について

チェックシートは実施対象者ごとに管理者用・SI 用チェックシートから構成されている。Table C.6 は、提供サービスとチェックシートの対応を示す。○部分は全てチェックを実施し、また▲部分については、該当するサービス（利用サービス）に応じてチェックを実施する。

Table C.6 —小規模機関における提供サービスとチェックシートの項目

提供サービス項目	「医療情報システムの安全管理に関するガイドライン」 技術・運用基準チェックシート	
	小規模機関	
	管理者チェックシート	ベンダチェックシート
1. 通信形態	○	
2. 通信ポリシー	○	○
3. 拠点内の技術的セキュリティ	○	○
4. サービス種別		
4-1 医療機関向けの情報提供ASPサービスの展開		
4-2 医療機関向けの情報提供ASPサービスの利用	▲	
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用		
4-4 医療機関以外への情報提供ASPサービスの展開		
4-5 医療機関以外への情報提供ASPサービスの利用	▲	
4-6 医療機関以外への情報提供ASPサービス（外部保存型）の利用		
4-7 メールサービス（プロバイダサービス）	▲	
4-8 インターネット接続サービス（プロバイダサービス）	▲	▲
4-9 リモート保守サービスの利用		
4-10 外部サービス提供機関/大規模医療サービス機関への接続（中継サービス）	▲	
5. 拠点内の物理的セキュリティ		○

*1 サービス種別の▲ヶ所は、利用サービスに応じてチェックすること。
個別サービスを利用する際は、該当する全ての個別項目をチェックすること。

チェックシートは管理者用・SI 用チェックシートからなる。Figure C.5 に示す手順でガイドラインへの適合性チェックを実施する必要がある。

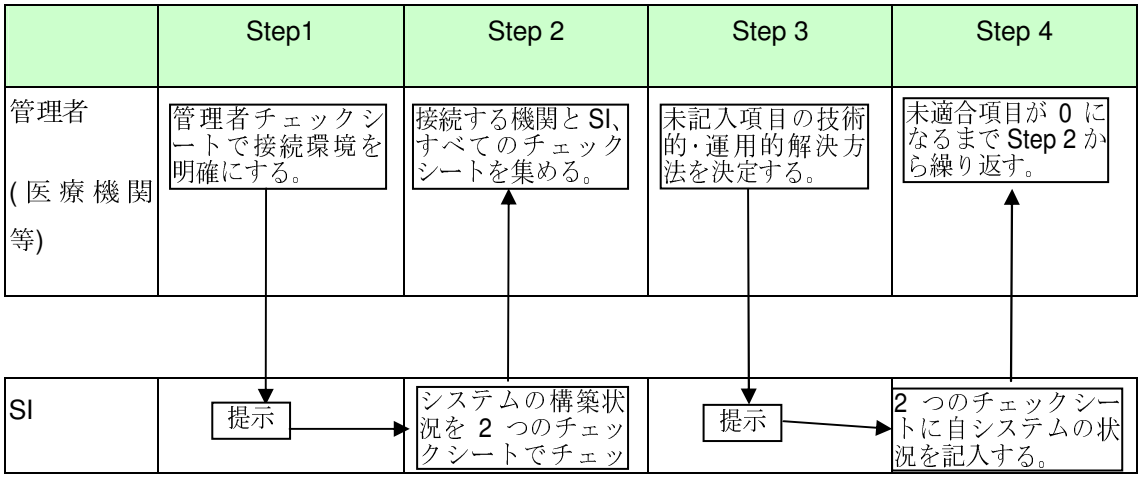


Figure C.5 — 小規模機関のチェック手順

医療機関等の管理者は、本チェックシートで確認した上で、未対応項目に対する対策や責任の分担を明確にしてから導入すべきである。責任の分担については、書面にて取交すことを徹底すべきである。

C.4 SP のチェックシートの使用方法について

a) チェックシートの構成について

SP 用チェックシートはチェック実施者の種別に応じて、管理者用チェックシート、SI 用チェックシート、SP 用チェックシートの３枚から構成される。

Table C.7 — SP のチェックシート構成

実施者の種別	定義	SP			備考
		管理者チェックシート	SI チェックシート	SP チェックシート	
管理者	各機関を運営する組織、またはその管理責任者を対象としている。	○（※）	－	－	（※）管理者が、チェックが出来ない項目については、SI の設計責任者に確認すること。
SI	各機関のネットワークおよびシステムを設計･構築するシステムインテグレータ等を対象としている。	－	○	－	
SP	提供するサービス機能を外部委託（アウトソーシング）する場合に、その委託先の SP の運営する組織、またはその管理責任者を対象としている。	－	－	○（※）	

SP は、上記管理者用チェックシート、SI 用チェックシート、SP 用チェックシートの、全てのシートのチェックを実施する必要がある。

b)　チェックシートのチェック項目について

チェックシートは管理者、SI、SP の３つのチェックシートから構成されるが、各シートのチェック項目については、SP が医療機関等に提供するサービスの種類により異なる。

— VPN プロバイダサービスを提供
医療機関等に対し、VPN サービスを提供する VPN プロバイダは、チェックシート記載の VPN プロバイダ要件へのチェックを実施する。
— ASP プロバイダサービスを提供
医療機関等に対し、VPN サービスだけではなく、ASP サービスをも提供するプロバイダは、チェックシート記載の ASP プロバイダ要件へのチェックも実施する。
— ASP プロバイダ・サービス（個別サービス）を提供
医療機関等に対し、メールや、インターネット接続、情報提供サービス等の個別 ASP サービスを提供するプロバイダは、チェックシート記載の個別 ASP プロバイダ要件へのチェックも実施する

TableC.8 には､SP 用チェックシートの各入力項目と SP の提供サービスによるチェック該当部分との関係を示します。SP は提供サービスに応じて、チェックシートの該当入力項目のチェック（下表○部分のチェック）を実施する。

Table C.8 — SP の提供サービスとチェックシートの対応

チェックシート入力項目	VPN プロバイダ要件		ASP プロバイダ要件	ASPプロバイダ（個別サービス）要件									
	VPNサービス	IXサービス	ASPサービス	地域連携サービス	情報提供サービス	リモート保守サービス	メールサービス	インターネット接続サービス	外部保存サービス	検査データ配信サービス	タイムスタンプサービス	VAサービス	アウトソーシング
1. 通信形態	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 通信ポリシー	○	○	○	○	○	○	○	○	○	○	○	○	○
3. 拠点内の技術的セキュリティ			○	○	○	○	○	○	○	○	○	○	○
4. サービス種別 *1													
4-1 医療機関向けの情報提供ASPサービスの展開				○	○		○		○	○	○	○	
4-2 医療機関向けの情報提供ASPサービスの利用													
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用				○	○		○		○	○	○	○	○
4-4 医療機関以外への情報提供ASPサービスの展開				○	○		○		○		○	○	
4-5 医療機関以外への情報提供ASPサービスの利用													
4-6 医療機関以外への情報提供ASPサービス（外部保存型）の利用													○
4-7 メールサービス（プロバイダサービス）							○						
4-8 インターネット接続サービス（プロバイダサービス）								○					
4-9 リモート保守サービスの利用						○							
4-10 外部サービス提供機関/大規模医療サービス機関への接続（中継サービス）	○	○	○										
5. 拠点内の物理的セキュリティ	○	○	○	○	○	○	○	○	○	○	○	○	○

*1　提供するサービス項目が複数存在する場合は、該当する全ての個別項目をチェックすること。また、上記表の個別の ASP サービス要件にないサービスを提供する場合は、「４．サービス種別」の中で、提供サービスが該当する項目を全て選択し、チェックすること。

また、サービス提供をする医療機関等に対し、医療機関等の機能に応じて大規模機関チェックシート、または小規模機関チェックシートの管理者用・SI 用・SP 用チェックシートのチェックを実施し、ガイドラインに基づいた安全性を担保する必要がある。そのため、SP は、医療機関等用のチェックシートの判定基準が確保されるように、大規模機関チェックシートまたは小規模機関チェックシートのチェック内容について、その責任範囲を記載した契約書または覚書を医療機関等と取交し、保管する必要がある。

Annex D
(informative)

ダイナミック・オンデマンド VPN の概要

D.1 VPN のセキュリティ

ISO/IEC18028-1 において、VPN は既存のネットワークのインフラを使用して構築する私設ネットワークと定義してあり、利用者からは、VPN は私設ネットワークのように見える。また、私設ネットワークと同じ機能としてサービスが提供される。VPN は以下のような様々な用途に使用できる。
－移動中または離れた場所にいる社員から会社への遠隔通信。
－異なった場所にある組織間のリンク。予備のインフラとしての冗長リンクも含む。
－他の組織/取引先との通信用に、ある組織のネットワークへの接続を設定する。

そして、13.2.9.2 の不正アクセスのセキュリティリスクより安全ではないネットワークを使用した通信における最も大きな安全上のリスクは、機密性のある重要な情報が承認されていない組織にアクセスされ、不正に開示されたり改竄されたりすることである。
また、ISO/IEC18028-5、6 における VPN セキュリティの目的として、VPN セキュリティの主な目的は不正アクセスからの保護であり、VPN は以下に示すような、より幅の広いネットワークセキュリティの目的を達成するために使用できる。
－ネットワーク内の情報の保護、ネットワークに接続されている機器内の情報の保護、ネットワークを使用したサービスの保護
－サポートしているネットワークインフラの保護
－ネットワーク管理システムの保護
（18028-5　7　VPN セキュリティの要件）
上記 6 項で示した目的を達成するために、以下を保証できるように VPN を実装しなければならない。
－VPN のエンドポイント間を移送中のデータとコードの機密。
－VPN のエンドポイント間を移送中のデータとコードの完全性。
－VPN ユーザと管理者の信ぴょう性。
－VPN ユーザと管理者の承認（権限付与）。
－VPN エンドポイントとネットワークインフラの可用性。

ダイナミック・オンデマンド VPN は、この一般的な特徴の上に更に VPN ユーザと管理者の信ぴょう性、VPN ユーザと管理者の承認（権限付与）について改善し、尚且つ固定の接続相手だけでなくインターネットの様に、接続先の汎用性を持たしている。
ダイナミック・オンデマンド VPN は、ネットワークの脅威の対策として、以下の機能を実現する。

a) IPSec と IKE を利用することによるセキュアな通信路を確保でき、機密性が担保できる。
b) 安全性が確認できる機器を利用でき、拠点の出入り口、使用機器の認証ができ、接続者同士の正当性を担保できる。
c) 認証手段として PKI による認証、もしくは Kerberos のような鍵配布、もしくは事前配布された共通鍵の利用による認証が可能であり、VPN 利用者と管理者の信ぴょう性が担保できる。
d) 接続先の設定がダイナミック・オンデマンド VPN のプロバイダにより管理され、N 対 N の回線が実現でき、利用者の責任が削減される。

D.2 ダイナミック・オンデマンド VPN の目的

Figure D.1 に示すようにダイナミック・オンデマンド VPN は、IP-VPN のように管理されたセキュリティ品質と、インターネット上にセキュリティを確保して通信できる安価なインターネット VPN の双方の優れた点をネットワークプロバイダーの管理責任により実現する特徴を持っており、今後の医療向けネットワークとして最適である。Tabel D.1 にダイナミック・オンデマンド VPN とインターネット VPN との比較を示す。ダイナミック・オンデマンド VPN は、「認証レベルが高い」、「オンデマンドに任意の拠点間 VPN 接続が容易」、「ユーザの VPN 環境の設定負荷が軽い」等の点でインターネット VPN に対して優位である。その上、従来のプロバイダ主導で構築されるネットワークと異なり、ユーザの接続ポリシーをダイナミックに切り替えられるユーザ主導の社会インフラ的位置づけを持つネットワーク基盤である。

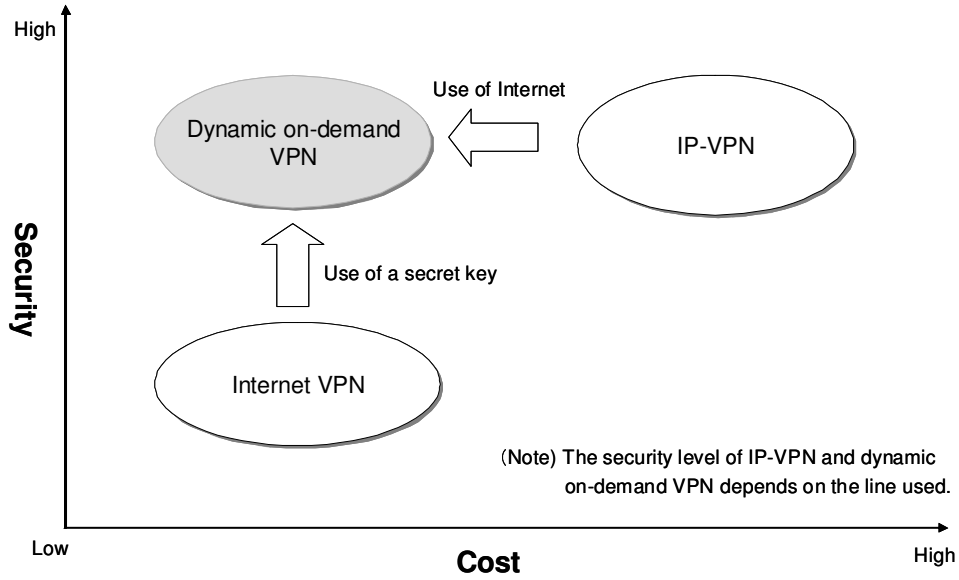


Figure D.1 — ダイナミック・オンデマンド VPN の位置付け

比較項目	ダイナミック・オンデマンドVPN	インターネットVPN
機器認証	・VPN装置にPKIチップを搭載し、電子証明書を格納 ・電子証明書によりセンターとVPN装置が認証を行い、機器のなりすましを防止	既存のVPN装置には、認証機能が無いので**機器の特定が出来ない**
環境設定（使い勝手）	・VPN装置設置時に機器認証とオンデマンドVPNサービスの認証をインターネット経由で行い、通信が開始できる ・別の相手と新たに通信を行う場合は、機器認証を元にサービスのための証明書をネットワークからダウンロードすることにより、通信が開始できる	VPN装置設置時に設定した拠点間におけるVPN接続しかできず、新たな相手とVPN接続を行う場合は、管理者が手動で鍵の設定をする必要がある
対象者	・ VPNの構成情報を接続時に配布することと，証明書で保障されたIDで識別しているため，どのインターネットプロバイダでも適用可能	特定のVPNサービス事業者に限定の可能性がある

Table D.1 — ダイナミック・オンデマンド VPN とインターネット VPN の比較

D.3 ダイナミック・オンデマンド VPN の接続方法

ダイナミック・オンデマンド VPN はオンラインで N 対 N の相手を自由に切換えられることを特徴としている。具体的には PKI 機能を持った IC チップ(PKI チップ) を VPN 機器（ルータ）に搭載し、PKI チップの二階層 PKI 機能を利用して、ダイナミック・オンデマンド VPN サービス提供者がネットワーク経由で VPN 接続用のサービス証明書と接続情報をオンライン配送することにより接続相手先をオンラインで容易に切り替える事ができる。PKI チップの二階層 PKI 機能は、IC カードの認証技術の応用である。

Figure D.2 にダイナミック・オンデマンド VPN の接続形態の概要を示す。サービス証明書および接続情報を、ダイナミック・オンデマンド VPN サービス提供者からネットワーク経由で各 VPN 機器にダウンロードすることにより、地域中核病院、総合検査センター、医療機器会社を含むグループ A を形成し、その中のメンバ同士で VPN 通信が可能となる。また地域中核病院、診療所、調剤薬局、患者を含むグループ B を形成し、その中のメンバ同士で VPN 通信が、可能となる。接続情報は各機器から、接続申請が出され、接続相手との接続条件が満たされれば各機器は接続情報をダウンロードすることができ、この情報を元に通信の用が発生の都度、通信の接続を開始する。ダイナミック・オンデマンド VPN サービス提供者は、グループ A 内のメンバ、グループ B 内のメンバの接続情報を管理しており、この接続情報で許可された接続以外の相手とは接続が出来ない。また、サービス証明書あるいは接続情報を持たないグループ C に属する機器はグループ A やグループ B とは接続が出来ない。

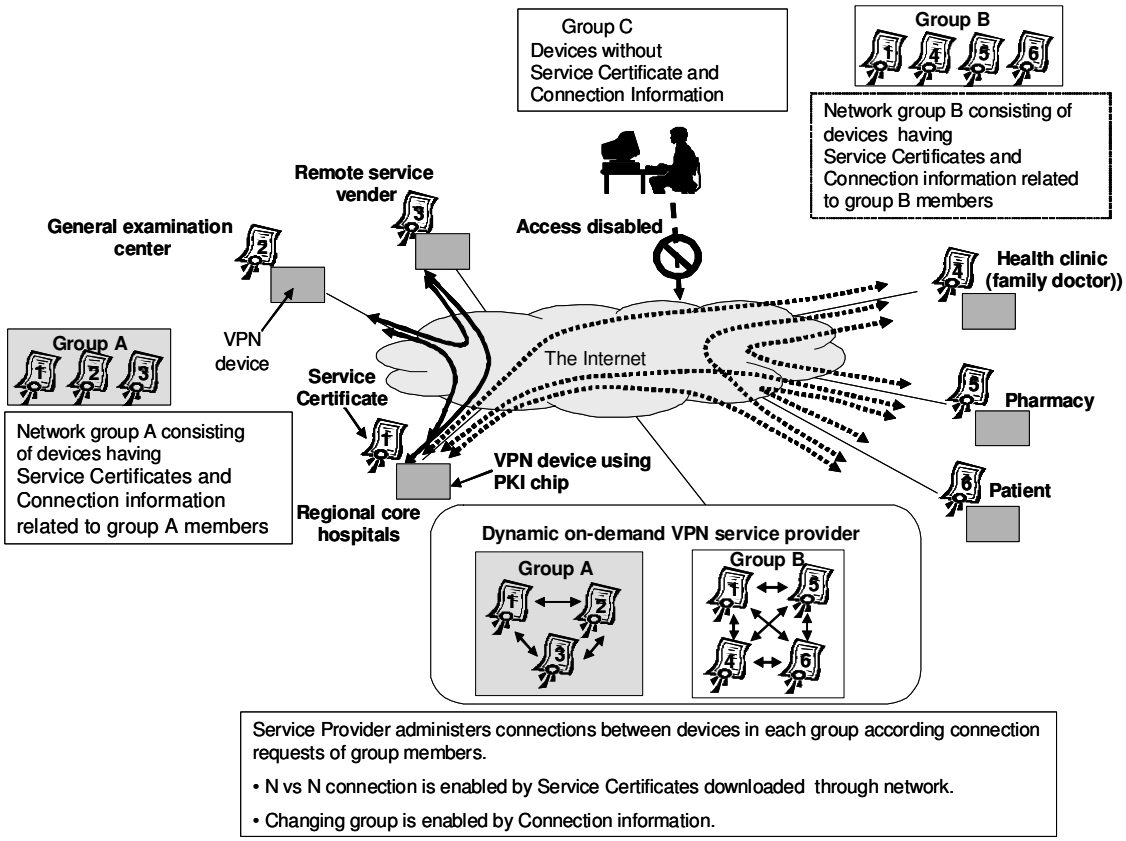


Figure D.2 — ダイナミック・オンデマンド VPN の概要

D.4 ダイナミック・オンデマンド VPN の特徴

ダイナミック・オンデマンド VPN は、以下のような特徴を持つことにより、セキュアで尚且つオンデマンドに N 対 N のメッシュ型通信が可能となる。

a) PKI チップの二階層 PKI 機能により、VPN 機器、VPN サービス利用者の正当性を認証
b) VPN の IPsec 接続に必要なパラメータや鍵配送をオンラインで行うことにより VPN 設定が可能
c) IPsec による通信チャネルにより、成りすまし、改ざん、盗聴を防止
d) IP 層でセキュリティを保証するのでアプリケーションソフトウエアの変更が不要
e) 必要に応じてどの医療関係機関とも接続できるメッシュ型通信（1 対 1 ではなく N 対 N 通信）
f) 患者の来院等、診療に応じて接続できるオンデマンド通信（繋ぎっぱなしではなく、要求に応じた接続）
g) 複数地点で連携した遠隔診療を実現するマルチセッション通信（1 本の回線で複数相手接続）

h) 接続ポリシーが VPN プロバイダの定めた一律のポリシーだけではなく、個々の加入者のポリシーも加味可能

D.5 二階層 PKI チップを用いた VPN 機器

ダイナミック・オンデマンド VPN サービスを可能にするために、Figure D.3 に示すように PKI チップを VPN 機器に組み込む。VPN 機器購入時に機器を登録し、一階層目の PKI チップに機器証明書を搭載する。機器の所有者は、ダイナミック・オンデマンド VPN サービス提供者に対して一階層目の PKI で機器証明書により機器の正当性を認証し、VPN サービスを受けるためのサービス証明書を PKI チップにネットワーク経由でダウンロードする。接続を行う場合は二階層目の PKI でサービス証明書によりダイナミック・オンデマンド VPN センターと認証をして、接続情報をダウンロードし、安全に VPN サービスを開始することができる。

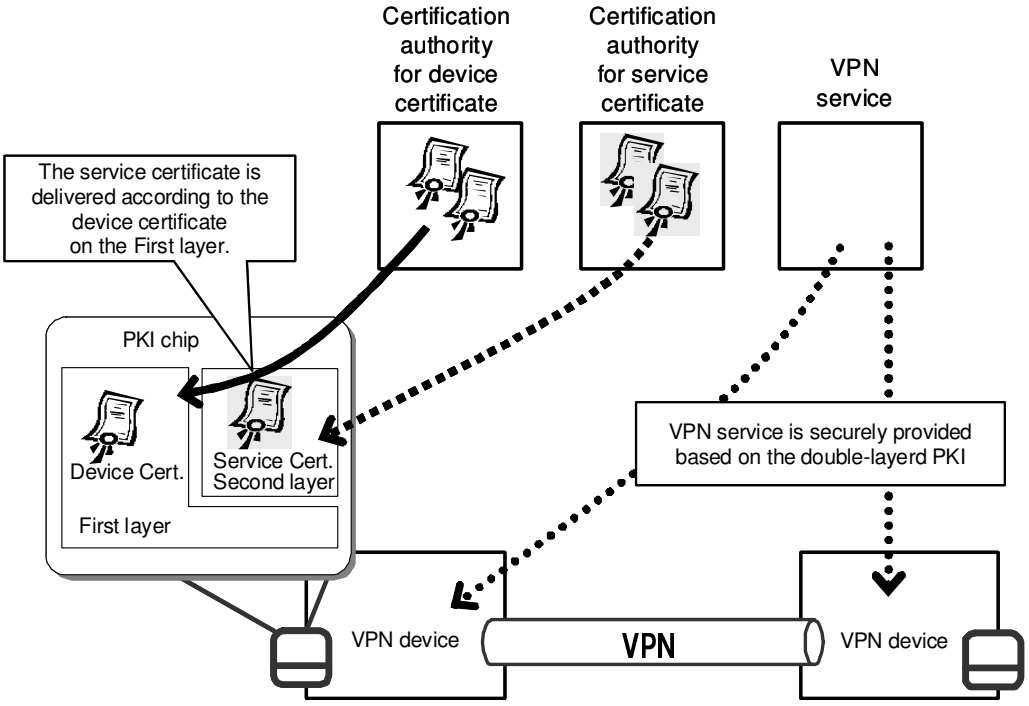


Figure D.3 — PKI チップへの機器証明書、サービス証明書のダウンロード

D.6 VPN 機器の登録と接続申請

ISO 18028-5 より、小規模 VPN （例: シングル利用者と中央システム間）では VPN 機能の実装はソフトウエアの使用で充分だが、多くの場合、VPN 機能を提供する機器を使用することにより大きな利点が得られる。例えば、管理の容易さとより安全なプラットフォームでの運用が可能であり、要求される認証プラットフォームとしては、例えば、ディレクトリ、PKI、または RADIUS）がある。例えばこれにより、権限付与された利用者しか中

央には接続できないようにすることが可能である。そして、VPN 機器は正しく管理すべきである。VPN 機器の管理とは、VPN 機器の設定や監視に必要なプロセスのことを示す。VPN の設定とは、ネットワーク構成や、必要なポート/アプリケーションアクセスに合わせて機器を設定したり、証明書の実装（上位レイヤーの VPN 用）を行ったり、他のネットワーク機器に対すると同様に VPN 機器のネットワーク監視を継続することである。

ダイナミック・オンデマンド VPN では、機器の安全性を保証するために、VPN 機器を機器証明書発行機関に登録し、機器証明書を VPN 機器に搭載する。そして、この機器証明書を元に VPN のサービス証明書をネットワークからダウンロードするので、機器の安全性が担保され、機器の成りすましを防ぐことができ、拠点の出入り口、使用機器の認証ができ、接続者同士の正当性を担保できる。

ダイナミック・オンデマンド VPN における機器のセキュリティを確保するために、VPN 機器を機器登録機関に登録して VPN 機器の機器証明書を発行して貰い、機器に搭載する。VPN サービスは、機器証明書をセンターが認証して、VPN サービス証明書をダウンロードし、サービス証明書を認証して行われる。これにより、機器セキュリティが確保され、VPN 機器の成りすましを防げ、ISO/IEC18028-5 を満足する。

Figure D.4 は、利用者が、ダイナミック・オンデマンド VPN サービスを受ける前の申請手続きの例である。

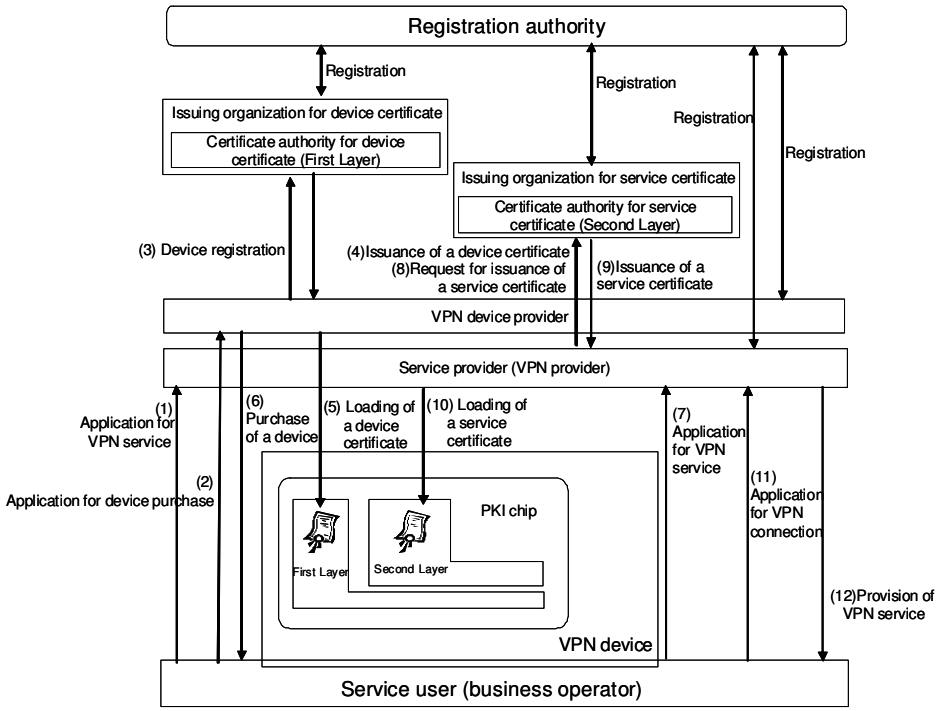


Figure D.4 — ダイナミック・オンデマンド VPN のサービス開始手順

Figure D.4 にサービス利用者がダイナミック・オンデマンド VPN を利用するまでの申請手順例を示す。

サービス提供者、VPN 機器提供者、機器証明書発行機関、サービス証明書発行機関は、登録認定機関に、事業者、機関登録申請を行い、認定を受ける。

a) サービス利用者は、サービス提供者に VPN サービスの加入申請を行う。
b) サービス利用者は、VPN 機器提供者に VPN 機器購入申請を行う。
（VPN サービス加入申請と VPN 機器購入申請は、同時に行われる可能性はある。またサービス提供者が VPN 機器を代行提供（販売）する事はある。）
c) VPN 機器提供者は、サービス利用者が購入予定の VPN 機器を、機器証明書発行機関に登録する。
d) 機器証明書発行機関は、登録のあった VPN 機器に対して、機器証明書を発行する。
e) VPN 機器提供者は、機器証明書を、登録のあった VPN 機器の IC チップの 1 階層目に搭載する。
f) サービス利用者は、機器証明書が搭載された VPN 機器を購入（入手）する。
g) サービス利用者は、サービス提供者に、VPN サービス利用申請をする。
h) サービス提供者は、サービス利用者用のサービス証明書の発行をサービス証明書発行機関に依頼する。
i) サービス証明書発行機関は、サービス提供者に、サービス利用者用のサービス証明書を発行する。
j) サービス提供者は、サービス証明書を、サービス利用者の VPN 機器の IC チップの２階層目に搭載する。
k) サービス利用者は、VPN 接続申請を、サービス提供者にする。
l) サービス提供者は、サービス利用者に対して、VPN サービスを提供する。

D.7 ダイナミック・オンデマンド VPN の適用の留意事項

a) ダイナミック・オンデマンド VPN を使用設定する際の時間

・セットアップの時間

通常の通信に比べ，ダイナミック・オンデマンド VPN ではセットアップの時間として IPsec を構築するまでの時間がかかる。これは，VPN サービスを受けるために必要な時間と，IPsec を開始するための時間に分けられるが、セットアップとして必要な時間である．IPsec を開始するための時間は，接続先を選択し IPsec を構築するまでの時間である．利用者が設定を行うハンドリングも含まれるが，30 秒以下で接続は完了する．

・オーバーヘッド

通常の暗号化しない通信よりも，IPsec(EPS 適用)によって通信した際は時間がかかりこの部分がオーバーヘッドとなる．オーバーヘッドは基本的には暗号化・復号化によるものである．この留意点は通常の IPsec 方式を適用したものと共通である．

・リアルタイムトラフィック
　トラフィックの速度はダイナミック・オンデマンド VPN で使用する回線の影響を受ける．現在多くの利用者が使用しているインターネットは，ベストエフォート型のサービスとなっているため，ダイナミック・オンデマンド VPN はその影響を受け，ベストエフォート型のサービスとなる．

b) ダイナミック・オンデマンド VPN を使用する際の通信品質

・QoS，パケットタギング(Diffserv)
　ダイナミック・オンデマンド VPN では，IPsec の技術で ESP を適用しているため，QoS を確保するための技術としては，レイヤ 2 以下の技術と Diffserv の技術が適用可能である．この問題は通常の IPsec を適用したときと同様の留意事項である。

　※Diffserv は，IP パケットの TOS フィールドにある Differentiated Service Code Point を使用しており，このフィールドは，IPsec を適用しても Differentiated Service Code Point はオリジナルパケットの物をコピーするため影響を受けない

c) ダイナミック・オンデマンド VPN の IP アドレス

・NAT
　NAT を行った際にそのままだと通信できないプロトコルがある(FTP，SIP 等)。この問題は通常の IPsec を適用したときと共通である．

・Firewall
　ISAKMP(500/UDP)と ESP(プロトコル ID:50)を通過させる必要がある。この問題は通常の IPsec を適用したときと共通である。

・ダイナミックルーティングプロトコル
　IPsec 接続時は，ルーティングプロトコルが ESP によって暗号化されて転送される．ダイナミック・オンデマンド VPN の場合，IPsec の接続／切断を利用者が任意で行うことが出来るため，ネットワーク構造が利用者によって変更されることになる．リンクステート型(OSPF 等)を使用している場合は再計算が行われることになり，ルータに負荷がかかってしまうため，ルーティングプロトコルの種類によっては注意が必要になる．

・既存の IP アドレスに対する影響
　他の SP の異なるネットワークが接続される場合, IP アドレスが競合する可能性がある．
　解決方法としては，以下のような方式が考えられる．
　　－使用するドメインでアドレスの整合性をとる
　　－アドレスの競合について製品で解決する
　　－グローバルアドレスを適用する

D.8 二階層 PKI の特徴

二階層 PKI とは、Fig.5 に示すようにチップ管理の認証とサービスの利用権に関する認証を、独立でレベルの異なる鍵で実現する考え方であり、二階層 PKI により、多様なサービスを便利かつ安全に利用することが可能である。

－１階層目：機器認証→サービス・アプリの搭載を含むチップの認証・管理に利用される PKI
－２階層目：利用権認証→サービス提供時に利用される PKI

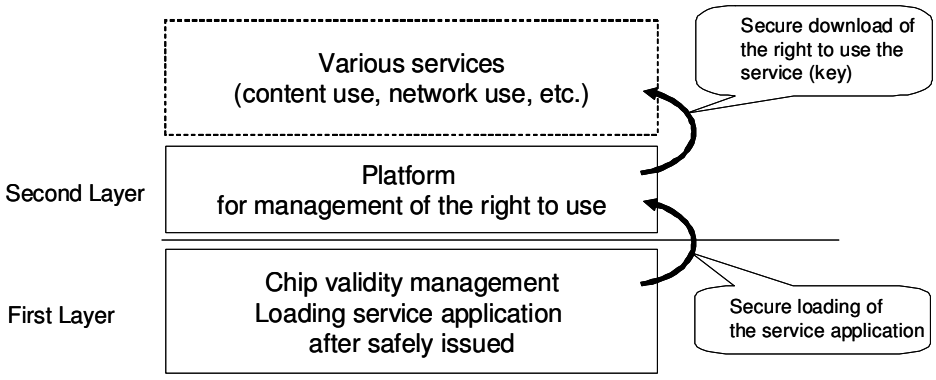


Figure D.5 — 二階層 PKI の概念

D.9 まとめ

ダイナミック・オンデマンド VPN は VPN 機器に搭載した PKI チップの二階層 PKI 機能により、機器認証、VPN のサービス認証をしてセキュアに通信を行うものであり、また接続相手を変える場合は新たなサービス証明書をダウンロードすれば N：N の VPN 接続が可能となり、セキュリティと利用の柔軟性から、医療分野でのセキュアなネットワークの用件を満たす通信方式の一つとして適用できる。