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

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user’s country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO’s member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail copyright@iso.org  
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>5</td>
</tr>
<tr>
<td>はじめに</td>
<td>6</td>
</tr>
<tr>
<td>1. 適用範囲</td>
<td>7</td>
</tr>
<tr>
<td>2. 引用規格</td>
<td>7</td>
</tr>
<tr>
<td>3. 用語定義</td>
<td>7</td>
</tr>
<tr>
<td>4. 略語</td>
<td>9</td>
</tr>
<tr>
<td>5. 医療分野における情報サービスの形態</td>
<td>11</td>
</tr>
<tr>
<td>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</td>
<td>11</td>
</tr>
<tr>
<td>5.2. 守るべき医療情報の種類（情報資産）</td>
<td>12</td>
</tr>
<tr>
<td>5.3. 医療分野におけるネットワークに求められる要件</td>
<td>13</td>
</tr>
<tr>
<td>6. 医療分野におけるネットワーク構築の考え方</td>
<td>13</td>
</tr>
<tr>
<td>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</td>
<td>14</td>
</tr>
<tr>
<td>6.1.1 責任分界点の明確化</td>
<td>14</td>
</tr>
<tr>
<td>6.1.2 医療機関等における留意事項</td>
<td>14</td>
</tr>
<tr>
<td>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</td>
<td>15</td>
</tr>
<tr>
<td>6.2.1 クローズドなネットワークで接続する場合</td>
<td>15</td>
</tr>
<tr>
<td>6.2.2 オープンなネットワークで接続されている場合</td>
<td>16</td>
</tr>
<tr>
<td>7. 脅威分析と対策</td>
<td>17</td>
</tr>
<tr>
<td>8. 医療分野におけるネットワーク構築</td>
<td>17</td>
</tr>
<tr>
<td>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</td>
<td>17</td>
</tr>
<tr>
<td>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</td>
<td>18</td>
</tr>
<tr>
<td>8.3. ダイナミック・オンデマンド VPN の活用</td>
<td>19</td>
</tr>
<tr>
<td>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</td>
<td>19</td>
</tr>
<tr>
<td>9.1. 健康ポータルによる地域医療連携モデル</td>
<td>20</td>
</tr>
<tr>
<td>9.2. オンラインメンテナンスモデル</td>
<td>20</td>
</tr>
<tr>
<td>9.3. 地域中核病院を中心とした地域医療連携モデル</td>
<td>21</td>
</tr>
<tr>
<td>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</td>
<td>22</td>
</tr>
<tr>
<td>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</td>
<td>23</td>
</tr>
</tbody>
</table>
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行う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ェアを変更せずにセキュアチャネルの形成ができることを望まれるので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には、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には、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るので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、そのよう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 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)
同じ建物の中にい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
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HEASNET</td>
<td>HEAlthcare information Secure NETwork consortium</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hash Message Authentication Code</td>
</tr>
<tr>
<td>IC</td>
<td>integrated circuit</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet key exchange</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IP-VPN</td>
<td>Internet-Protocol-based virtual private network</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>NAT</td>
<td>network address translation</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>OSP</td>
<td>online service provider</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>PKI</td>
<td>public key infrastructure</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SI</td>
<td>System Integrator</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of Service</td>
</tr>
<tr>
<td>TTL</td>
<td>time to live</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
</tbody>
</table>
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に、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、オーディング、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、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、時刻配信などの公開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わせをする。

— 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、送信元から送信元に確実に情報を送信届ける必要があり、「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元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、受信データに対する「盗聴」とおよび「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、不適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、情報の発信元である医療機関等から、情報が通信事業者に提供され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（正確性の確保）のことを指す。例えば、「暗号化」をおっける処置としても、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、仮に送信元から送信先への通信経路上での情報送信先の医療機関等に盗聴の可能性、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可能性が織り込まれた場合でも、医療機関等が適切な処置を取る必要がある。そのため、そのヒントの一つとして、医療機関等においては、情報がネットワークを通じて送信される場合、情報は暗号化されていることが望ましい。

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の適切な処置を取る必要がある。その一つの方法として、医療情報そのものを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には、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

ネットワークを通じて情報を伝送する場合、情報を暗号化したまま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、データが改変される可能性がある。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

ネットワークを通じ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、送信元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認証するために、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必要がある。

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閉鎖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ていないため、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、それぞれの接続形式について特徴を述べる。

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とりわけ技術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たことによる誤接続、誤送信のリスクや専用線と同様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送ることも可能である。

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の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間のネットワーク間が接続点を介して相互に接続されている形態も存在している。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前に送信する際に、一回、送信される情報の宛先を接続点で解読したり新たな情報を付加したりする場合がある。この際、偶然的に情報の中身が漏洩する可能性は無くはない。

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読解できないようにし、改ざんを検知可能に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要である。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を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、医療機関等の自らの責任においてセキュリティを確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が必要とするため、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、適切でない経路が構築されるリスクが存在する。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」が暗号化されるため、盗聴の危険度が低いが、暗号鍵の取り扱いが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、盗聴の危険度が低い。IPsec + IKE の組み合わせで、確実にその安全性を確保できる。

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。つまり、UDP 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するリスクを指摘されている。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を基に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因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て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、許可機器へのなりすまし防止

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が考えられ、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、製品の導入による、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の守るべき事項を網羅的にチェ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、医療機関等の機能によって下記のように分類し、チェックできるようにした。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
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、医療機関のネットワークセンタープリシートに分けた。このチェックシートで、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、医療機関の管理者、システムSI、SPがそれぞれ医療機関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。

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要件の対策のためネットワーク経路上のセキュリティを確保している形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・オンラインV рП インフォメーション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は Figure 1 に示すとおり、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じて病院の予約や自分の検診結果等をご確認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。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で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は Figure 2 に示すように、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の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、医療施設とクライアントの SI 番を個人情報保護に関するポリシーに依頼しておく必要がある。
9.3. 地域中核病院を中心とした地域医療連携モデル

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を、ネットワーク接続時に 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脆弱性を排除する。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ログインする場合は、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。
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、ネットワーク会議モデル

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を 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時に 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。
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、大学の附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 部外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 電子保存を受託する機関の限定

© ISO 2008 – All rights reserved
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とため、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は一つに絞ること。
— 拠点の入り口のアクセスポインで認証する。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 つのログをき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、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（端末一ネットワーク一端末間）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

<table>
<thead>
<tr>
<th>大区分</th>
<th>小区分</th>
<th>機能概要</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN管理機能</td>
<td>鍵交換機能 (IKE)</td>
<td>VPN接続に使用する暗号鍵を自動で交換する</td>
</tr>
<tr>
<td></td>
<td>暗号化機能 (IPsec)</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>認証機能 (IPsec)</td>
<td>通信データの送信元を認証する</td>
</tr>
<tr>
<td></td>
<td>VPN制御機能</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>VPN接続機能</td>
<td>VPN接続の接続/切断要求やデータの送受信を行う</td>
</tr>
<tr>
<td></td>
<td>初期登録機能</td>
<td>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）を記録する</td>
</tr>
<tr>
<td></td>
<td>機器情報参照機能</td>
<td>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</td>
</tr>
<tr>
<td>鍵管理機能</td>
<td>耐タンパ機能</td>
<td>論理的/物理的に記憶領域へのアクセスを制御する</td>
</tr>
<tr>
<td></td>
<td>暗号化処理機能</td>
<td>格納する鍵を暗号/複合処理する</td>
</tr>
<tr>
<td></td>
<td>AP管理機能</td>
<td>APの書き込み/削除やダウンロードしたAPの動作を制御する</td>
</tr>
<tr>
<td></td>
<td>記憶領域管理機能</td>
<td>鍵ベアや証明書を格納する領域のアクセス制御を行う</td>
</tr>
</tbody>
</table>

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、現在は人や機器の正体性を保証できないため、「なりすまし」によるクライアント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体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在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接続を防ぐことは不可能であり、ユーザの認証機関がユーザー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み合わ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 を参考に脅威の洗出を行った。

- 平文伝送
- 暗号化の保守
- 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・書き換え
- 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
- 情報の不正コピー
- 情報の不正・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に対応させて下記のように整理した。
表 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

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

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。

図 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、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場合としては、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ます、「送付すべき相手に」、「正しい内容を」、「内容を視みられない方法で」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数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を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無示の同意、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、同意および「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、その事業者が責任を負っているかが明白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利用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に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。

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が提供できない。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、情報を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（正確性の確保）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処の一つである。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伝送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る場合、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。その一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、前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の業務においては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乗載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、正当な内容を送信前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医療機関等は、送られた情報が確かに送信元の医療機関等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、電子署名を組み合わせることも考えられる。

B.4 選択すべきネットワークのセキュリティの考え方

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け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、確認をする責任がある。

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られているが、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。基本的には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、機密度の高くなる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、多くの場合、クル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じ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増えられる。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、上記の安全管理に加え、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しい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器、端末の利用者等を確実に確認する手段を確立した上で、情報をやり取りする機関間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観点から責任分野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するため、以下ではいくつかのケースを想定して留意点を述べる。

B.4.2 クローズドネットワークで接続する場合

ここで述べるクローズドネットワークとは、業務上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徴を述べる。

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、観点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、その導入にあたりはやや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がある。

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前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いことによる誤接続、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、閉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洩する可能性がないとは言えない。電気通信事業法があり、万が一偶発的に漏洩してもそれ以上の場合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、医療機関等から域外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接続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、どの階層でセキュリティを担保するかによって異なる。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

<table>
<thead>
<tr>
<th>階層</th>
<th>層</th>
<th>効果</th>
</tr>
</thead>
<tbody>
<tr>
<td>第7層</td>
<td>アプリケーション層</td>
<td>FTPやMail等のサービスをユーザに提供</td>
</tr>
<tr>
<td>第6層</td>
<td>プレゼンテーション層</td>
<td>データを人に分かり、通信に適した形式に変換</td>
</tr>
<tr>
<td>第5層</td>
<td>セッション層</td>
<td>データ経路の確立と開放に関係する層</td>
</tr>
<tr>
<td>第4層</td>
<td>ネットワーク層</td>
<td>データを確実に送る為に規定されている層</td>
</tr>
<tr>
<td>第3層</td>
<td>アドレスタイリング層</td>
<td>アドレス管理と経路の選択層</td>
</tr>
<tr>
<td>第2層</td>
<td>データリンク層</td>
<td>物理通信用層の確立するために規定されている層</td>
</tr>
<tr>
<td>第1層</td>
<td>物理層</td>
<td>ビットデータを電気的、物理的に変換、機器の形態・特性を規定している層</td>
</tr>
</tbody>
</table>

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」と言える部分で経路の暗号化手続きが取られるため、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す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取られるため、SSLプロトコルを使った暗号通信よりは危険度が低いか、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ります。

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
く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提供をする場合であり、第 8 章で定める診療録及び診療等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を提供する場合、第一に意識しておく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、情報提供を行う場合は、医療機関等が自ら実施して患者等に情報提供する場合であり、第 8 章で定める診療録及び診療等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、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る。

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がある。認証手段としては PKI による認証、Kerberos や One Time Password のように鍵配布、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。

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。

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

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。

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がある。認証手段としては PKI による認証、Kerberos や One Time Password のように鍵配布、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
・ 送信元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
・ 传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
・ 阻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明確にすること。
一 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には、責任分界点も含めた整理と契約の締結。
一 患者等に対する説明責任の明確化。
一 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。
一 交換した医療情報等に対する結果責任の明確化。
個人情報の取得に関わらず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得に関する秘密事項。
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、プロトコルの設定、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) 繰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利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の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。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、外局と下記のような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する。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

<table>
<thead>
<tr>
<th></th>
<th>医療機関等</th>
<th>ＳＰ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>大規模機関</td>
<td>小規模機関</td>
</tr>
<tr>
<td>機能・設備</td>
<td>外部に情報提供できる設備を有する</td>
<td>外部に情報提供できる設備を有しない</td>
</tr>
<tr>
<td>参照図</td>
<td>Figure C.1</td>
<td>Figure C.2</td>
</tr>
<tr>
<td>必要となるチェックシート</td>
<td>大規模機関チェックシート</td>
<td>小規模機関チェックシート</td>
</tr>
</tbody>
</table>

**Figure C.1 — 大規模機関のネットワーク構成例**

- **VPN connection**
- **Non-VPN connection**

*Figures C.1, C.2, C.3*
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

<table>
<thead>
<tr>
<th>実施者の種別</th>
<th>定義</th>
<th>大規模機関</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理者</td>
<td>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。</td>
<td>○（※） - -</td>
<td>（※）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。</td>
</tr>
<tr>
<td>SI</td>
<td>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。</td>
<td>- ○ -</td>
<td></td>
</tr>
<tr>
<td>SP</td>
<td>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。</td>
<td>- - ○（※）</td>
<td></td>
</tr>
</tbody>
</table>
(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
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>大規模機関</td>
</tr>
<tr>
<td>1. 通信形態</td>
<td>〇</td>
</tr>
<tr>
<td>2. 通信ポリシー</td>
<td>〇 〇</td>
</tr>
<tr>
<td>3. 拠点内の技術的セキュリティ</td>
<td>〇 〇 〇</td>
</tr>
<tr>
<td>4. サービス種別</td>
<td></td>
</tr>
<tr>
<td>4-1 医療機関向けの情報提供ASPサービスの展開</td>
<td>▲</td>
</tr>
<tr>
<td>4-2 医療機関向けの情報提供ASPサービスの利用</td>
<td>▲</td>
</tr>
<tr>
<td>4-3 医療機関以外の情報提供ASPサービス（外部保存型）の利用</td>
<td>▲</td>
</tr>
<tr>
<td>4-4 医療機関以外の情報提供ASPサービス（内部保存型）の利用</td>
<td>▲</td>
</tr>
<tr>
<td>4-5 医療機関以外の情報提供ASPサービス（外部保存型）の利用</td>
<td>▲</td>
</tr>
<tr>
<td>4-6 医療機関以外の情報提供ASPサービス（外部保存型）の利用</td>
<td>▲</td>
</tr>
<tr>
<td>5. 拠点内の物理的セキュリティ</td>
<td>〇 〇</td>
</tr>
</tbody>
</table>

*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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理者 (医療機関等)</td>
<td>管理者チェックシートで接続環境を明確にする。</td>
<td>接続する機関とSI、SP すべてのチェックシートを集める。</td>
<td>未記入項目の技術的・運用的解決方法を決定する。</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>目的</th>
<th>対象</th>
<th>項目</th>
<th>機能要素</th>
<th>判定基準</th>
<th>判定条件</th>
<th>チェック結果</th>
<th>ガイドライン適用項目</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>接続先機の確認</td>
<td>1-1</td>
<td>1</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機関間接続先機を接続する場合、接続する大規模機関間接続先機は「大規模機関間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-1</td>
<td>2</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機関間接続先機を接続する場合、接続する大規模機関間接続先機は「大規模機関間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-1</td>
<td>3</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機関間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-1</td>
<td>4</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機関間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-1</td>
<td>5</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 5</td>
</tr>
<tr>
<td>2</td>
<td>接続先機の確認</td>
<td>2-1</td>
<td>1</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-1</td>
<td>2</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-1</td>
<td>3</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-1</td>
<td>4</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-1</td>
<td>5</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 5</td>
</tr>
<tr>
<td>3</td>
<td>接続先機の確認</td>
<td>3-1</td>
<td>1</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-1</td>
<td>2</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-1</td>
<td>3</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-1</td>
<td>4</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-1</td>
<td>5</td>
<td>同一法人に接続する場合</td>
<td>機関間セキュリティ基準の確認</td>
<td>異なる法人の大規模機間接続先機を接続する場合、接続する大規模機間接続先機は「大規模機間チェックシート」の項目をチェックし、条件を満たしている。</td>
<td>□</td>
<td>A 11 B 5</td>
</tr>
<tr>
<td>ID</td>
<td>内容</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-5</td>
<td>各ホストに対するウィルスチェック</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5</td>
<td>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、インターネット経由で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対策を行う。</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>ID</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-6-1</td>
<td>拠点内におけるセキュリティ対策などの関連機能の実装</td>
</tr>
<tr>
<td>3-6</td>
<td>内部セキュリティサービスの実施</td>
</tr>
<tr>
<td>3-7</td>
<td>サービス提供ユーザの認証</td>
</tr>
<tr>
<td>3-8</td>
<td>外部ASPからのサービス機能の利用を受ける場合にオープンネットワークを用いる場合のセキュリティ対策</td>
</tr>
<tr>
<td>3-9</td>
<td>データまたは機器のHigh Secure Zoneへの配置・検証</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>ID</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>高セキュリティ対策</td>
</tr>
<tr>
<td>5.2</td>
<td>各ホストに対するウィルスチェック</td>
</tr>
<tr>
<td>5.3</td>
<td>パッチファイルは常に最新の状態である。</td>
</tr>
<tr>
<td>5.4</td>
<td>ウイルス・DoS攻撃等に対する防御対策を実施する。</td>
</tr>
<tr>
<td>5.5</td>
<td>ハイセキュリティゾーンの設定</td>
</tr>
<tr>
<td>5.6</td>
<td>データまたは機器のHigh Secure Zoneへの配置・検証</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>ID</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.10</td>
<td>ID/パスワードによるアカウント管理を実施する。</td>
</tr>
<tr>
<td>6.11</td>
<td>サービス提供ユーザを認証する。</td>
</tr>
<tr>
<td>6.12</td>
<td>ナビゲーション機能の実装</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>ID</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3</td>
<td>サーバ機能の実施</td>
</tr>
<tr>
<td>7.4</td>
<td>サービスの提供におけるユーザを識別するための認証を実施する。</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>ID</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>モニタリング機能の実装</td>
</tr>
<tr>
<td>9.2</td>
<td>通信用のセキュリティ機能の実装</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>ID</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>サービスの提供におけるユーザを識別するための認証を実施する。</td>
</tr>
<tr>
<td>10.2</td>
<td>サービスの提供におけるユーザを識別するための認証を実施する。</td>
</tr>
</tbody>
</table>

---

© ISO 2008 – All rights reserved
<table>
<thead>
<tr>
<th>6.10 C (9)</th>
<th>6.11 B-16.11 B 36.11 C 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-4-1 情報の提供または公開</td>
<td>ASPサービスを利用する際のユーザの認証</td>
</tr>
<tr>
<td>ASPサービスを利用する際のユーザの認証を行うためについてチェックする。</td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>□</td>
</tr>
<tr>
<td></td>
<td>□</td>
</tr>
<tr>
<td>4-4-2 サービス提供ユーザの認証</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>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。</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>ASPサービスを利用して取得した医療情報等がHigh Secure Zoneに格納されているかチェックする。</td>
<td>□</td>
</tr>
<tr>
<td>4-3 医療機関向けの情報提供</td>
<td>サービス提供ユーザの認証</td>
</tr>
<tr>
<td>ASPサービスを用いる際のユーザの認証しているかチェックする。</td>
<td>□</td>
</tr>
<tr>
<td>4-2-1 ASPサービスを利用する利用者の認証</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>4-2-2 情報提供ASPサービス利用におけるセキュリティ対策</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>サービスを提供するホスト・機器がHigh Secure Zoneに配置されているかチェックする。</td>
<td>□</td>
</tr>
<tr>
<td>4-2-3 ASPサービス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</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>ASPサービスにおいては、High Secure Zoneに保存される重要データや機密を守るとともに、不正アクセスを防止するため、上記のセキュリティ対策が行われているかチェックする。</td>
<td>□</td>
</tr>
<tr>
<td>4-2 医療機関向けの情報提供</td>
<td>サービス提供ユーザの認証</td>
</tr>
<tr>
<td>4-2-4 ホストのHigh Secure Zoneへの配置・格納</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>4-1 ホストのHigh Secure Zoneへの配置・格納</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>高度な物理的なセキュリティ対策が行われているかチェックする。</td>
<td>□</td>
</tr>
<tr>
<td>4-1 医療機関向けの情報提供</td>
<td>サービス提供ユーザの認証</td>
</tr>
<tr>
<td>ファイアウォール機能</td>
<td>サーチ機能</td>
</tr>
<tr>
<td>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。</td>
<td>□</td>
</tr>
<tr>
<td>4-0 医療機関向けの情報提供</td>
<td>サービス提供ユーザの認証</td>
</tr>
</tbody>
</table>
ウィルス、DoS攻撃等に対する防御対策を行っている。
改ざんや侵入に対する不正パケットの検知・遮断対策を行っている。
アクセス監視を行っている。
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

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。

6.10 C (9) 6.11 B 6.11 C 1 6.10 C (9)

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。

ID/パスワードによるアカウント管理を行っている。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っている。
ウィルス、DoS攻撃等に対する防御対策を行っている。
改ざんや侵入に対する不正パケットの検知・遮断対策を行っている。
アクセス監視を行っている。
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-3 6.11 C

High Secure Zoneに配置されている。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。

【提供サービス項目例】
・情報提供サービス
・ソールサービス
・医療機関向けの重要情報提供ASPサービス
・タイムスタンプサービス
・IDサービス
ASPサービスを利用する際の認証方法についてチェックする。

認証方法
パスワードによる認証を使用している。
指紋スキャナーによる認証を使用している。
バイオメトリック認証を使用している。

4-5-1 ASPサービス利用時のユーザ認証を行う方法についてチェックする。

セキュリティ対策
ASPサービスにおいては、High Secure Zoneにあたる重要なデータや機器を改ざんや侵入から守るために、左記のセキュリティ対策を整え、接続を行う。

6.10 C (9) 6.11 B 6.11 C 1 6.10 C (9)

・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

4-5-2 装置提供ASPサービスの利用におけるセキュリティ対策
ホスト機能
ディールの、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・遮断対策を行う。

4-5-3 ASPサービスを利用する際の小規模サービス、プロバイダサービスとの同時利用の禁止
ホスト機能
ホストによる接続受け入れを禁止する。
ホストは接続を受け入れない不正アクセスを防ぐ。
接続を試みた場合、ホストは拒否する。

4-5-4 情報提供ASPサービスの利用におけるセキュリティ対策
ホスト機能
情報提供ASPサービスにおいては、High Secure Zoneにあたる重要なデータや機器を改ざんや侵入から守るために、左記のセキュリティ対策を整え、接続を行う。

6.10 C (9) 6.11 B 6.11 C 1 6.10 C (9)

4-5 医療機関向けの重要情報提供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

4-4-3 外部ASPからのサービス機能の利用
ホスト機能
ホストは使用中の外部ASPからのサービス機能を確認し、不正アクセスによる改ざん情報漏えいを防ぐ。

4-4-4 重要データまたは機器のHigh Secure Zoneへの配置・格納
ホスト機能
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) 6.11 B 6.11 C 1 6.10 C (9)

50
<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.11 B-1</td>
<td>High Secure Zoneにあ る 重要 データ や機器 を 改ざ ぬ 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 。</td>
</tr>
<tr>
<td>6.11 B-3</td>
<td>中継 サービス 、ASPサ ービス との 同時利用 を禁 止 している 。す りょうで 、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 。</td>
</tr>
<tr>
<td>4-7-5</td>
<td>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</td>
</tr>
<tr>
<td>4-7-4</td>
<td>ユーザ による 他ISPメールサーバ ( Web メール )の利用</td>
</tr>
<tr>
<td>4-7-3</td>
<td>メールサー ビス を提供 する ユーザ の 認証</td>
</tr>
<tr>
<td>4-7-2</td>
<td>不正 なメール 転送 の禁止</td>
</tr>
<tr>
<td>4-7-1</td>
<td>メール のス クリーニング の実施</td>
</tr>
<tr>
<td>4-2</td>
<td>インターネ ット接続サービス を利用する ユーザ の認証</td>
</tr>
<tr>
<td>4-1</td>
<td>サイト閲覧の制限</td>
</tr>
<tr>
<td>3-1</td>
<td>サイト閲覧の制限</td>
</tr>
</tbody>
</table>

**メール機能**

メールの送受信 を行う 相手 が制限 されてい る。

6.5 B (4) 6.5 B (5)

スパムメール を防止 し ている 。
送受信時 にウィルスチ ゲック が行われ 、不審 なメール は削除 もしく は 隔離 されている 。

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)

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 を行っている 。 □

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)

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。
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 。 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 。 □

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 。
<table>
<thead>
<tr>
<th>リモート保守サービスの利用</th>
<th>データベースの構成</th>
<th>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</th>
</tr>
</thead>
<tbody>
<tr>
<td>データベースの構成</td>
<td>データベースの利用</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>セキュリティ対策</td>
<td>ローカルネットワーク</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>防止対策</td>
<td>データ保護対策</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>特殊対策</td>
<td>認証技術</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>防止対策</td>
<td>データ保護対策</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>特殊対策</td>
<td>認証技術</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>防止対策</td>
<td>データ保護対策</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>特殊対策</td>
<td>認証技術</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>防止対策</td>
<td>データ保護対策</td>
<td>システムの機器または情報を守するために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>特殊対策</td>
<td>認証技術</td>
<td>システムの機器または情報を守するために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>外部サービス提供機関への接続（中継サービス）</th>
<th>外部サービス提供機関との接続</th>
<th>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</th>
</tr>
</thead>
<tbody>
<tr>
<td>外部サービス提供機関への接続（中継サービス）</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守するために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守るために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
<tr>
<td>外部サービス提供機関との接続</td>
<td>外部サービス提供機関との接続</td>
<td>システムの機器または情報を守ために、高齢セキュアゾーンを設置しているかチェックする。</td>
</tr>
</tbody>
</table>

© ISO 2008 – All rights reserved
### 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

<table>
<thead>
<tr>
<th>対策項目</th>
<th>対策内容</th>
<th>検査項目</th>
</tr>
</thead>
<tbody>
<tr>
<td>ステルスモード</td>
<td>ステルスモードが設定されている。</td>
<td>□</td>
</tr>
<tr>
<td>ANY接続拒否</td>
<td>ANY接続拒否が設定されている。</td>
<td>□</td>
</tr>
<tr>
<td>SSIDによるアクセス制限</td>
<td>SSIDによってアクセス制限をしている。</td>
<td>□</td>
</tr>
<tr>
<td>MACアドレスによるアクセス制限</td>
<td>MACアドレスによってアクセス制限をしている。</td>
<td>□</td>
</tr>
<tr>
<td>電子証明書</td>
<td>電子証明書によってアクセスチェックしている。</td>
<td>□</td>
</tr>
<tr>
<td>WPA/TKIPによる暗号化</td>
<td>WPA/TKIPによって暗号化している。</td>
<td>□</td>
</tr>
<tr>
<td>WPA2/AESによる暗号化</td>
<td>WPA2/AESによって暗号化している。</td>
<td>□</td>
</tr>
<tr>
<td>PCのアドホックモードの禁止</td>
<td>PCのアドホックモードを禁止している。</td>
<td>□</td>
</tr>
<tr>
<td>電波を発する機器の利用（ゲーム機など）の制限</td>
<td>電波を発する機器の利用（ゲーム機など）を制限している。</td>
<td>□</td>
</tr>
</tbody>
</table>

### 6-1-2 情報および情報機器の持ち出し管理

<table>
<thead>
<tr>
<th>対策項目</th>
<th>対策内容</th>
<th>検査項目</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理方法</td>
<td>情報および情報機器の管理方法を定めている。</td>
<td>□</td>
</tr>
<tr>
<td>盗難・紛失時対応</td>
<td>盗難・紛失時対応を運用規定内に含めている。</td>
<td>□</td>
</tr>
<tr>
<td>教育</td>
<td>周知徹底している。</td>
<td>□</td>
</tr>
<tr>
<td>個人所有の端末</td>
<td>個人所有の端末においても同等の対策を行っている。</td>
<td>□</td>
</tr>
<tr>
<td>所在把握</td>
<td>情報の種類、機器などを管理管理している。</td>
<td>□</td>
</tr>
<tr>
<td>パスワード</td>
<td>パスワードを設定している。</td>
<td>□</td>
</tr>
<tr>
<td>コンピュータウィルス対策</td>
<td>コンピュータウィルス対策ソフトを導入している。</td>
<td>□</td>
</tr>
<tr>
<td>ファイアウォール</td>
<td>パーソナルファイアウォールを導入している。</td>
<td>□</td>
</tr>
<tr>
<td>利用環境の制限</td>
<td>利用環境の制限。</td>
<td>□</td>
</tr>
</tbody>
</table>

© ISO 2008 – All rights reserved
| 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 |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>対策項目</td>
</tr>
<tr>
<td>パスワード</td>
</tr>
<tr>
<td>① ② ③ ④ ⑤</td>
</tr>
<tr>
<td>⑥ ⑦ ⑧ ⑨ ⑩</td>
</tr>
<tr>
<td>⑪ ⑫ ⑬ ⑭ ⑮</td>
</tr>
<tr>
<td>⑯ ⑰ ⑱ ⑲ ⑳</td>
</tr>
<tr>
<td>㉑ ㉒ ㉓ ㉔ ㉕</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6-1-4 モバイルを使用する際の考え方</th>
</tr>
</thead>
<tbody>
<tr>
<td>対策項目</td>
</tr>
<tr>
<td>パスワード</td>
</tr>
<tr>
<td>① ② ③ ④ ⑤</td>
</tr>
<tr>
<td>⑥ ⑦ ⑧ ⑨ ⑩</td>
</tr>
<tr>
<td>⑪ ⑫ ⑬ ⑭ ⑮</td>
</tr>
<tr>
<td>⑯ ⑰ ⑱ ⑲ ⑳</td>
</tr>
<tr>
<td>㉑ ㉒ ㉓ ㉔ ㉕</td>
</tr>
</tbody>
</table>

| 対策項目 |
| パスワード  |
| ① ② ③ ④ ⑤ |
| ⑥ ⑦ ⑧ ⑨ ⑩ |
| ⑪ ⑫ ⑬ ⑭ ⑮ |
| ⑯ ⑰ ⑱ ⑲ ⑳ |
| ㉑ ㉒ ㉓ ㉔ ㉕ |

| 対策項目 |
| パスワード  |
| ① ② ③ ④ ⑤ |
| ⑥ ⑦ ⑧ ⑨ ⑩ |
| ⑪ ⑫ ⑬ ⑭ ⑮ |
| ⑯ ⑰ ⑱ ⑲ ⑳ |
| ㉑ ㉒ ㉓ ㉔ ㉕ |

<p>| 対策項目 |
| パスワード  |
| ① ② ③ ④ ⑤ |
| ⑥ ⑦ ⑧ ⑨ ⑩ |
| ⑪ ⑫ ⑬ ⑭ ⑮ |
| ⑯ ⑰ ⑱ ⑲ ⑳ |
| ㉑ ㉒ ㉓ ㉔ ㉕ |</p>
<table>
<thead>
<tr>
<th>対策項目</th>
<th>対策項目</th>
<th>対策項目</th>
<th>対策項目</th>
</tr>
</thead>
<tbody>
<tr>
<td>ファイアウォール導入している。</td>
<td>ファイアウォールを導入している。</td>
<td>ファイアウォールを導入している。</td>
<td>ファイアウォールを導入している。</td>
</tr>
<tr>
<td>SSL通信による暗号化が行なわれている。</td>
<td>SSL通信による暗号化が行なわれている。</td>
<td>SSL通信による暗号化が行なわれている。</td>
<td>SSL通信による暗号化が行なわれている。</td>
</tr>
<tr>
<td>PKI個人認証等の対策を行っている。</td>
<td>PKI個人認証等の対策を行っている。</td>
<td>PKI個人認証等の対策を行っている。</td>
<td>PKI個人認証等の対策を行っている。</td>
</tr>
<tr>
<td>患者への説明がなされているか。</td>
<td>患者への説明がなされているか。</td>
<td>患者への説明がなされているか。</td>
<td>患者への説明がなされているか。</td>
</tr>
<tr>
<td>患者説明</td>
<td>患者説明</td>
<td>患者説明</td>
<td>患者説明</td>
</tr>
<tr>
<td>患者への説明や提供目的の説明を実施している。</td>
<td>患者への説明や提供目的の説明を実施している。</td>
<td>患者への説明や提供目的の説明を実施している。</td>
<td>患者への説明や提供目的の説明を実施している。</td>
</tr>
<tr>
<td>責任分界点</td>
<td>責任分界点</td>
<td>責任分界点</td>
<td>責任分界点</td>
</tr>
<tr>
<td>ITに係る以外の法律规范等を含めて明確な対策を立て、それぞれの責任を明確にしている。</td>
<td>ITに係る以外の法律规范等を含めて明確な対策を立て、それぞれの責任を明確にしている。</td>
<td>ITに係る以外の法律规范等を含めて明確な対策を立て、それぞれの責任を明確にしている。</td>
<td>ITに係る以外の法律规范等を含めて明確な対策を立て、それぞれの責任を明確にしている。</td>
</tr>
</tbody>
</table>

未認証のネットワークに対する考え方を含め、術後に挙げた日程以外への業務を除く。
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

<table>
<thead>
<tr>
<th>実施者の種別</th>
<th>定義</th>
<th>小規模機関</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>管理者チェックシート</td>
<td>SIチェックシート</td>
</tr>
<tr>
<td>管理者</td>
<td>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。</td>
<td>○（※）</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>（※） 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。</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI</td>
<td>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。</td>
<td>-</td>
<td>○</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>提供サービス項目</th>
<th>「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</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>小規模機関</td>
</tr>
<tr>
<td></td>
<td>管理者チェックシート</td>
</tr>
<tr>
<td></td>
<td>ベンダチェックシート</td>
</tr>
<tr>
<td>1. 通信形態</td>
<td>○</td>
</tr>
<tr>
<td>2. 通信ポリシー</td>
<td>○</td>
</tr>
<tr>
<td>3. 拠点内の技術的セキュリティ</td>
<td>○</td>
</tr>
<tr>
<td>4. サービス種別</td>
<td></td>
</tr>
<tr>
<td>4-1 医療機関向けの情報提供ASPサービスの展開</td>
<td>▲</td>
</tr>
<tr>
<td>4-2 医療機関向けの情報提供ASPサービスの利用</td>
<td>▲</td>
</tr>
<tr>
<td>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</td>
<td>▲</td>
</tr>
<tr>
<td>4-4 医療機関以外への情報提供ASPサービスの展開</td>
<td>▲</td>
</tr>
<tr>
<td>4-5 医療機関以外への情報提供ASPサービスの利用</td>
<td>▲</td>
</tr>
<tr>
<td>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</td>
<td>▲</td>
</tr>
<tr>
<td>4-7 メールサービス（プロバイダサービス）</td>
<td>▲</td>
</tr>
<tr>
<td>4-8 インターネット接続サービス（プロバイダサービス）</td>
<td>▲</td>
</tr>
<tr>
<td>4-9 リモート保守サービスの利用</td>
<td>▲</td>
</tr>
<tr>
<td>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）</td>
<td>▲</td>
</tr>
<tr>
<td>5. 拠点内の物理的セキュリティ</td>
<td>○</td>
</tr>
</tbody>
</table>

*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。

<table>
<thead>
<tr>
<th>Step1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理者 (医療機関等)</td>
<td>管理者チェックシートで接続環境を明確にする。</td>
<td>接続する機関とSI、すべてのチェックシートを集める。</td>
<td>未記入項目の技術的・運用的解決方法を決定する。</td>
</tr>
<tr>
<td>SI</td>
<td>提示</td>
<td>システムの構築状況を2つのチェックシートでチェック</td>
<td>提示</td>
</tr>
</tbody>
</table>
| | | | 2つのチェックシートにシステムの状況を記入する。

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、書面にて取扱う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

<table>
<thead>
<tr>
<th>実施者の種別</th>
<th>定義</th>
<th>SP</th>
<th>備考</th>
</tr>
</thead>
<tbody>
<tr>
<td>管理者</td>
<td>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。</td>
<td>○（※）</td>
<td></td>
</tr>
<tr>
<td>SI</td>
<td>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。</td>
<td>-</td>
<td>○</td>
</tr>
<tr>
<td>SP</td>
<td>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。</td>
<td>-</td>
<td>- ○（※）</td>
</tr>
</tbody>
</table>

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。

Table C.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

<table>
<thead>
<tr>
<th>チェックシートリスク項目</th>
<th>VPNサービス</th>
<th>ASPサービス</th>
<th>ASPプロバイダ要件</th>
<th>ASPプロバイダ（個別サービス）要件</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 通信形態</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>2. 通信ポリシー</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>3. 拠点内の技術的セキュリティ</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4. サービス種別 *1</td>
<td></td>
<td></td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-1 医療機関向け情報提供ASPサービスの展開</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-2 医療機関向け情報提供ASPサービスの利用</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-3 医療機関向け情報提供ASPサービス（外部保存型）の利用</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-4 医療機関以外向け情報提供ASPサービスの展開</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-5 医療機関以外向け情報提供ASPサービスの利用</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-6 医療機関以外向け情報提供ASPサービス（外部保存型）の利用</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-7 メールサービス（プロバイダサービス）</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-8 インターネット接続サービス（プロバイダサービス）</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-9 リモート保守サービスの利用</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>4-10 外部サービス提供者医療機関への接続（中継サービス）</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>5. 拠点内の技術的セキュリティ</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

*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おり、利用者からは、VPN は私設ネットワークのように見え、また、私設ネットワークと同様機能としてサービスが提供される。VPN は以下の様々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。
- 異なる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頼性。
- 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、この一般的で特徴の上に更に VPN ユーザと管理者の信頼性、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せている。
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。

© ISO 2008 – All rights reserved
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 利用者と管理者的信頼性が担保できる。
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
<table>
<thead>
<tr>
<th>比較項目</th>
<th>ダイナミック・オンデマンドVPN</th>
<th>インターネットVPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>機器認証</td>
<td>・VPN装置にPKIチップを搭載し、電子証明書を格納&lt;br&gt;・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</td>
<td>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</td>
</tr>
<tr>
<td>環境設定（使い勝手）</td>
<td>・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、通信が始開できる&lt;br&gt;・別の相手に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</td>
<td>VPN装置設置時に設定した地点間ににおけるVPN接続しかできず、新たなる相手と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</td>
</tr>
<tr>
<td>対象者</td>
<td>・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</td>
<td>特定のVPNサービス事業者に限定の可能性がある</td>
</tr>
</tbody>
</table>

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可能であり、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信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、成り立ち、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ブリケーションソフトウェアの変更が不要

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ェ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
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配り、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続きを示す。

68
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がある。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 を構築するまでのが時間である。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。

© ISO 2008 – All rights reserved
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、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で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と、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れてしまうため、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、以下のようないくつかが考えられる。

- 使用するドメインでアドレスの整合性をとる
- 既存の競合に製品で解決する
- グローバルアドレスを使用する
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。