平成 18 年度

# 「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

平成 19 年 3 月

HEASNET

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

< 目　次 >

1. 概　要 ..... 1
1.1 背　景 ..... 1
1.2 検討方針 ..... 1
1.3 検討の進め方 ..... 3
2. 医療分野におけるセキュアネットワーク基盤の要件 ..... 5
2.1 一般的な要件 ..... 5
2.2 セキュリティに関するガイドライン ..... 5
2.3 システムの現状整理 ..... 6
3. 検討範囲(TOE)の検討 ..... 8
3.1 検討のスコープ ..... 8
3.2 検討対象(TOE)の整理 ..... 10
3.2.1 TOE の全体像 ..... 10
3.2.2 検討範囲と OSI の関係 ..... 11
3.2.3 守るべき資産 ..... 13
4. ネットワークの脅威に対する対処方法 ..... 15
4.1 WAN の定義 ..... 15
4.1.1 一般的な分類 ..... 15
4.1.2 脅威の所在と課題 ..... 18
4.2 ネットワークにおける脅威とセキュリティ対策の整理 ..... 18
4.2.1 ch セキュリティ ..... 18
4.2.2 NW 機器の obj セキュリティ ..... 28
4.2.3 既存技術との比較･評価 ..... 30
5. ch セキュリティに関わる NW 機器のセキュリティ要件 ..... 32
5.1 法人間の接続における留意点(PP) ..... 32
5.2 セキュリティ対策の基本方針(ST) ..... 32
5.3 具体的なセキュリティ対策 ..... 34
5.3.1 通信モデルの定義 ..... 34
5.3.2 モデル間のサービスイメージ ..... 35
5.3.3 各通信モデルのセキュリティ要件 ..... 36
6. 構築時の確認事項 ..... 41
6.1 チェックシート ..... 41
6.2 付帯要件等 ..... 57

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

## 1.概　要

### 1.1 背　景

e-Japan 戦略 II の重点分野として取り上げられているように、医療分野での IT 社会基盤の整備が急務となっている。保健・医療・福祉情報セキュアネットワーク普及コンソーシアム（以下、「HEASNET」という。）では、セキュアネットワーク基盤を介して、ヘルスケア関連情報を医療関連機関間で共有することにより、国民に対して多様なヘルスケアサービスが提供され、安心・安全で暮らしやすい社会の実現を目指し、以下のような活動を行っている。

(1) セキュアなネットワーク基盤実現のための全体フレームワークの提起

(2) セキュリティポリシー等の運用条件や共通インタフェース等の相互接続条件の提起

(3) 提案した共通インタフェース仕様や共通ポリシー等の標準化等による普及活動

(4) 内外の関係機関、諸団体と連携したセキュアネットワークを利用したサービス普及促進活動

上記活動において、HEASNET の構成組織である技術委員会ではセキュアネットワーク基盤の現状調査、全体フレームワークモデルに係る検討、およびセキュアネットワーク基盤の相互接続に係る検討を行ってきた。検討の結果、セキュアネットワーク基盤を実現するための具体的な技術方式に関する検討、及び当該方式の安全性を客観的に担保するための仕組みについて検討を進めることになった。

これらの背景のもと、技術委員会の下位組織として第三者認証取得 WG を設置し、セキュアネットワーク基盤の安全性を担保するために、要求されるセキュリティ対策に係る対象範囲やセキュリティ対策の基礎情報を整理、検討した。

### 1.2 検討方針

患者の個人情報等の医療情報が流通するセキュアネットワーク基盤は、医療機関や通信機器等の複数要素から構成されており、セキュアネットワーク基盤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、セキュアネットワーク基盤そのものの運用面）それぞれの安全性を確保し、利用者にアピールする必要がある。

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ように、第三者認証制度や行政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できると考える。関連する第三者認証制度を以下にあげる。

(1) プライバシーマーク制度

認証取得の対象となる情報資産は、個人情報。

個人情報の入手経路、取扱いおよび苦情の受付相談窓口の設置など、個人情報のライフサイクル（入手、利用、保存、廃棄）に係るプロセスの管理に関する組織のマネジメントシステムに関する認証制度。

(2) ISMS 適合性評価制度

認証取得の対象となる情報資産は、組織にとって重要な情報資産。

技術面でのセキュリティ要件だけではなく、運用・管理面におけるセキュリティ要件についても要求している。

情報資産について、機密性、完全性、可用性の観点から適切に保護するマネジメントシステムを構築することが要求されている。

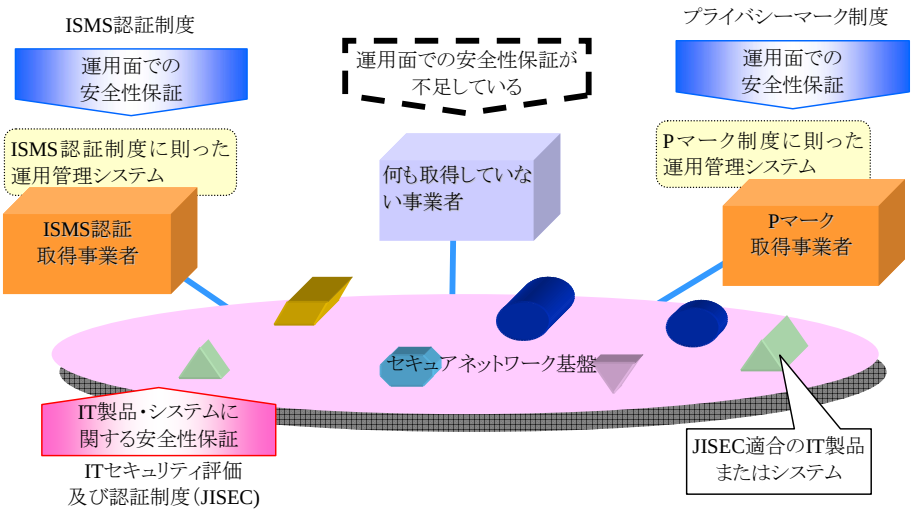
(3) IT セキュリティ評価及び認証制度（JISEC)

認証取得の対象は、情報資産を取り扱うシステムのセキュリティ要件。

セキュリティ機能について、不正利用に対抗できる有効なセキュリティ機能であることを機能設計レベルで検証する。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

IT 製品やシステムにおいて、セキュリティ要件が確実に保護されていることの保証を利用者に通知する。




第三者認証取得 WG では、ネットワークに係るセキュリティ要件を中心に検討する。ネットワークにおける安全性を確保する上で NW 機器（主にルータ）の担うセキュリティ要件を満たした製品が、複数の企業から製造・販売されると予想される。

ガイドライン等の基準を策定することにより、各製品による機能や運用方法はある程度共通化可能である。しかし、製品ごとに機能の実装方法が同一になるとは考えられず、セキュリティ要件を損なわないように各技術仕様に応じた運用仕様を遵守しなければならない。そのため、ガイドライン等の基準を策定する上では、製品の技術仕様と運用仕様の組合せを考慮して記述する必要がある。

本資料では、NW 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・運用すべての仕様について検討して明確化する。医療機関は、製品の導入に当たって、本資料にあるすべての仕様を満足させるように製品仕様で不足する部分については運用によってカバーできるよう、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導入すべきである。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

○通信に利用する技術や機器（利用機器等）

ISO/IEC15408
認証取得範囲

医療情報を伝送する場合、その通信データの安全性を確保することは必須条件といえる。ISO/IEC15408認証制度では、主にIT製品・システムのセキュリティ機能について、評価・検証している。

○セキュアネットワーク基盤の運用方法（運用面）

運用基準

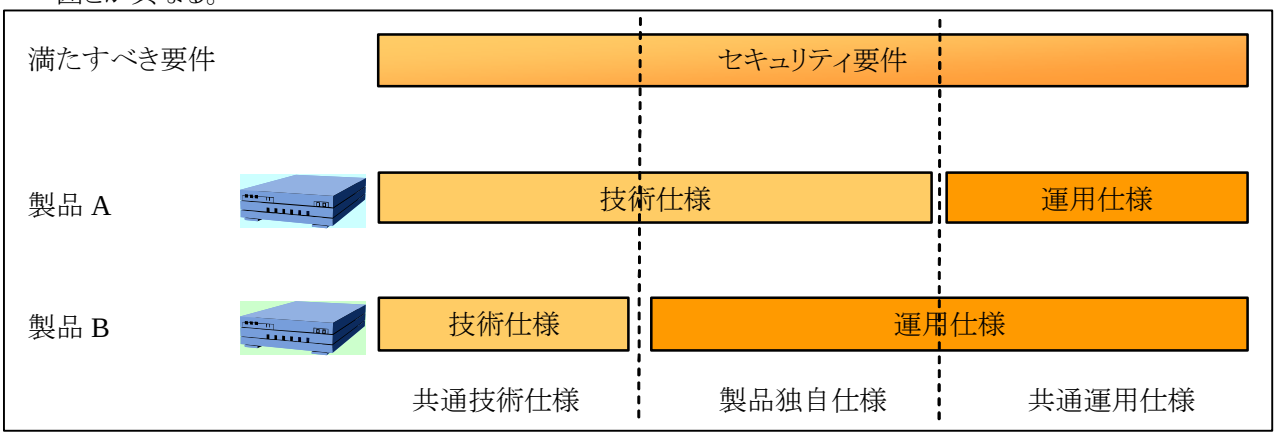
セキュアネットワーク基盤を運用する上で、機器の取扱い方法や機器 ID の払出方法などの運用方法について、現行の厚生労働省ガイドライン等を参考に、一定のセキュリティレベルを確保できたかを明文化された基準をもとに判断する必要がある。

○個人情報を取扱う医療機関や保守事業者（組織）

P マーク制度
ISMS 認証制度

医療分野で取扱う情報は、患者の個人情報など機微情報が多い。
従って、医療機関だけではなく、医療機器の保守事業者においても、組織としてセキュリティの高い運用体制を整備することが求められる。
現状は、プライバシーマーク制度や ISMS 認証適合制度といった第三者認証を取得することで、情報やシステムの運用体制について、一定の安全性が確保できていることを第三者により評価している。

製品により、技術（機能）で実現するセキュリティ要件の範囲と運用で実現するセキュリティ要件の範囲とが異なる。

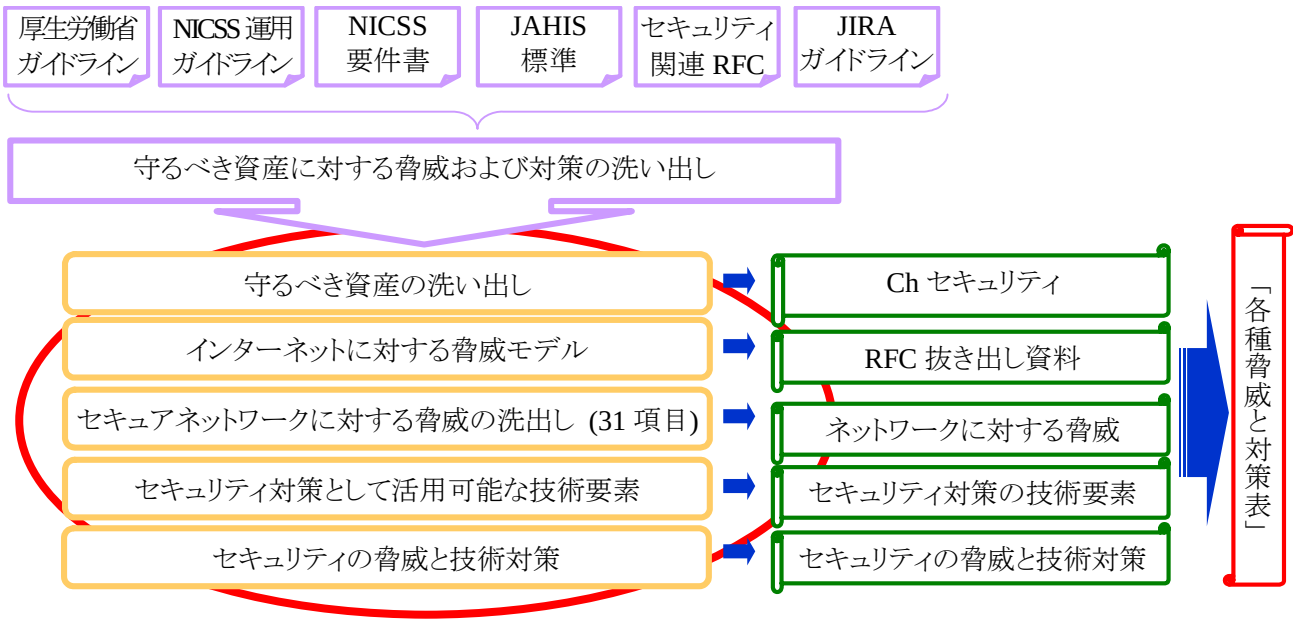



## 1.3 検討の進め方

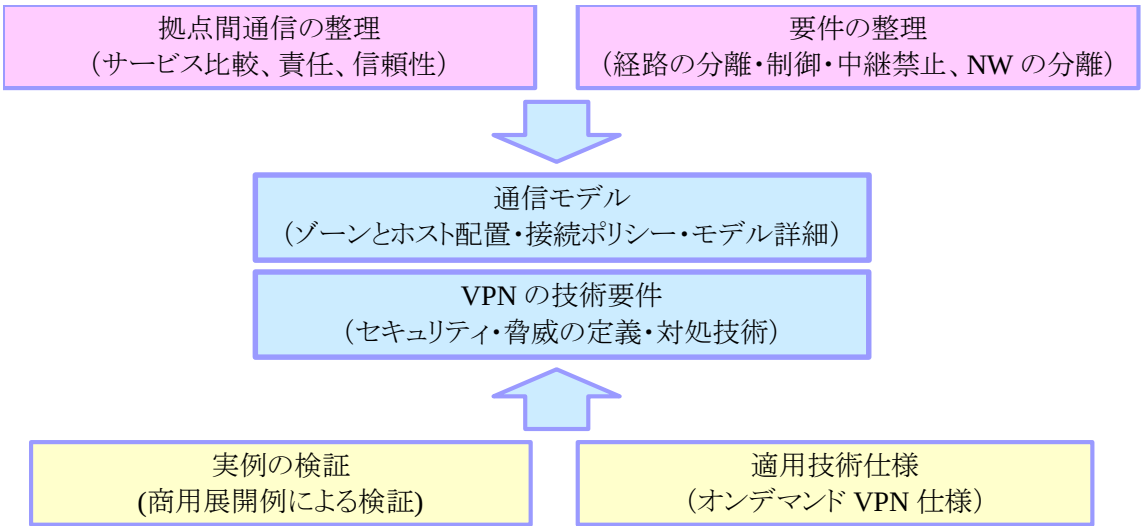
モデル確立に向けて諸要件を整理・分析し、それらを実際に構築したケースを元に検証する。

守るべき資産と脅威を明らかにし、モデルの評価を行う。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




本資料では、以下のように構成する。




本資料では、最終的に医療機関がネットワークシステムの導入に当たって考慮すべきセキュリティ的な技術・運用要件を下記のような構成のチェックシートとして提示する。

| 検討事項 | | 対策 |
|---|---|---|
| 3 拠点以上の接続か？ | ・2 つの異なる拠点と接続しますか？ | 5.1 法人間の接続における留意点<br>5.2 経路制御<br>5.2 不正中継禁止 |
| 2 拠点の接続か？ | ・オープンネットワークを使用するか？<br>・重要なデータが含まれているか？<br>・情報を公開するか？<br>・インターネットにアクセスするか？ | 2. セキュアネットワーク基盤<br>4. 暗号化の検討<br>5.3 ゾーン分けの検討<br>5.2 経路分離<br>5.3 通信モデル（大・小規模機関） |

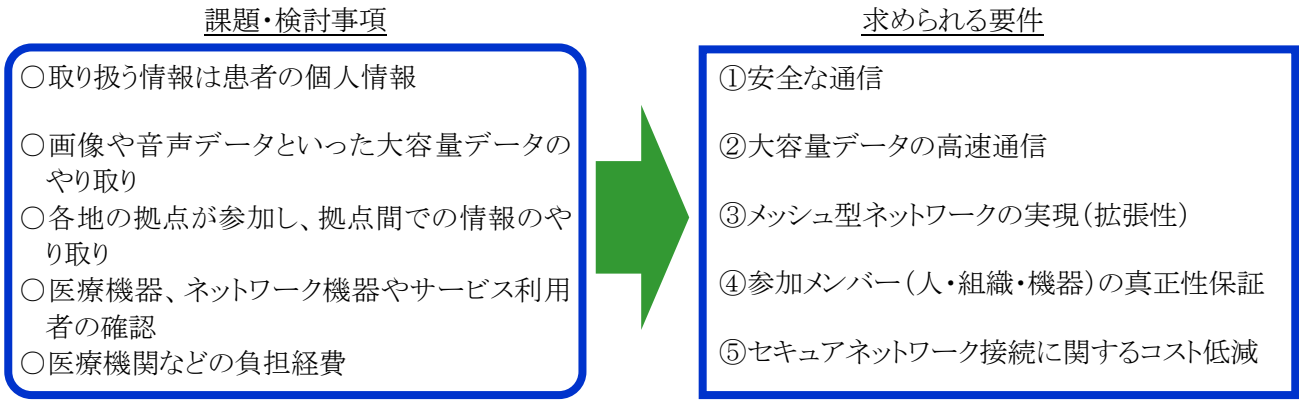
All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| | | | | |
|---|---|---|---|---|
| | | SP 契約するか？ | データの蓄積・公開サービスを利用するか？<br>タイムスタンプ、証明書の検証を行いますか？ | 5.3 通信モデル（サービスプロバイダ） |

2.医療分野におけるセキュアネットワーク基盤の要件

2.1 一般的な要件

医療分野におけるセキュアネットワーク基盤の構築において、検討すべき事項や課題及び求められる要件を以下にまとめる。




2.2 セキュリティに関するガイドライン

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を参照して要件を抽出した。参照したガイドラインについては、補足資料として別途添付する。特に関係のある厚生労働省のガイドラインについては、技術的検討に参照した部分を参考のため以下に示す。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は補足資料にないため要約を載せておく。

(1) 医療情報システムの安全管理に関するガイドライン

「医療情報システムの安全管理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。

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

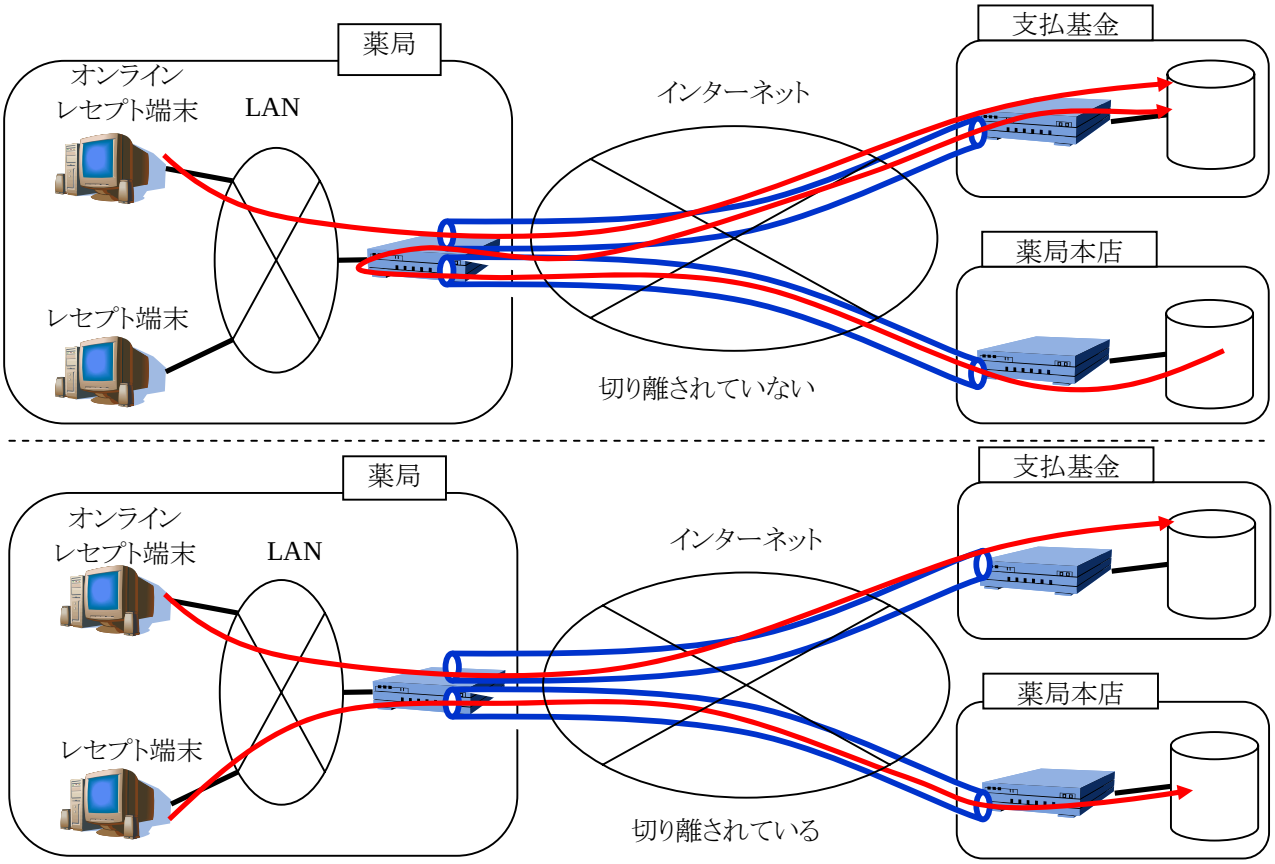
8.1.4 責任の明確化

(2) 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

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




(3) Requirements for Remote Sevices

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 Sesurity and Privacy Committee (SPC)で検討されたガイドライン Requirements for Remote Sevices の要約を以下に示す。

(a) 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。

(b) 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。

(c) 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。

(d) 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。

(e) 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。

(f) 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。

2.3 システムの現状整理

医療関連分野では、実際に IT を利用して下記のようなサービスが提供されている。セキュア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リモート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。サ

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

ービスの提供形態として、以下に列挙する。

(a) 情報提供サービス

他の医療機関から医療機関にある患者の診療・介護情報や情報提供情報にアクセスがある。

(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にある情報サイトにアクセスする。

(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蓄積した後で目的のサイトに情報が転送される。

(d) 情報処理サービス

医療機関から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。

(e) リモート保守サービス

医療機関が保守サービスを契約したサービス会社からリモートで医療機関に設置された機器の保守を受ける。

(f) 認証・監査基盤サービス

医療機関から公開鍵認証、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にアクセスする。

これらの分類に基づいて、現在行われている、あるいは想定されるサービスを列挙すると以下のようになる。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。

(i) 情報提供サービス

① (医療機関・福祉介護等医療関連サービス業務向け)地域連携サービス

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。

② (患者向け)診療・介護情報提供サービス

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。

③ (一般向け)医療・介護情報提供サービス

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。

(ii) (業務限定)インターネット接続サービス

学術情報サイト、厚労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。

(iii) 蓄積・中継サービス

① 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。

② 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。

③ 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。

(iv) 情報処理サービス

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

① ASP サービス

電子カルテ・レセプト等の医療機関向けのIT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。

② 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。

(v) 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。

(vi) 認証・監査基盤サービス

① タイムスタンプサービス

デジタル証明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。

② Validation Authority(VA)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。

## 3.検討範囲(TOE)の検討

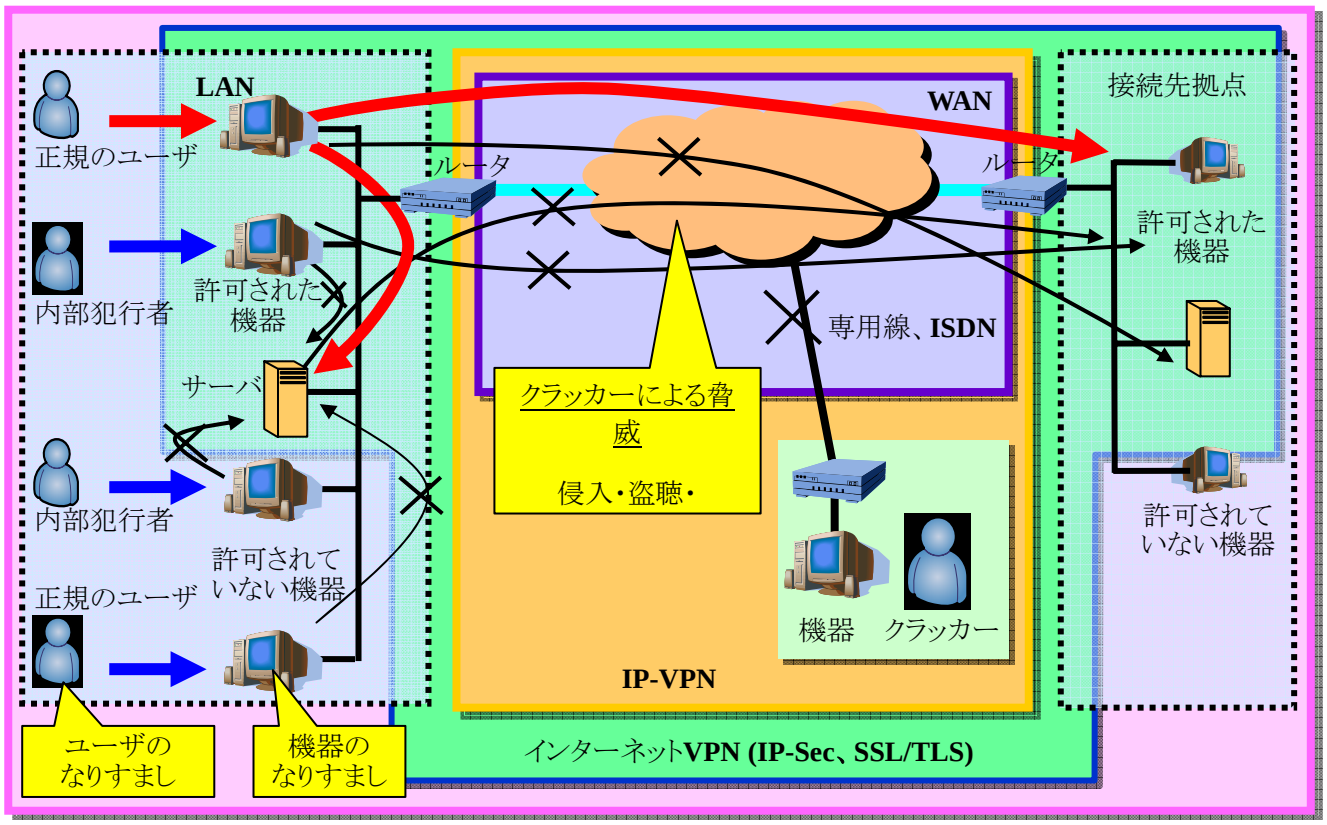
### 3.1 検討のスコープ

(1) アプリケーションとネットワークの関係

ネットワーク上の脅威を洗出す場合、下図に示すようにアプリケーション層（AP 層）に関する脅威とネットワーク層（NW 層）以下に対する脅威に分類できる。本 WG では、まず NW 層以下の脅威に絞り、以降の業務 AP の種別に依存しない脅威を含めた対策について検討を進める。

(2) ネットワークの全体像

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




専用線またはISDNが安全性を担保する範囲

IP-VPNが安全性を担保する範囲

インターネットVPN（IPSec)、インターネットVPN（SSL/TLS）が安全性を担保する範囲

セキュリティとして安全性を確保すべき範囲

(3) 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議論を展開している。二つの要件は、相反するものではなく、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実現する。以下の議論では、この考え方に沿ってネットワークにおけるデータの保護とデータそのものの保護について考え方を明確に分けて考察する。RFC3552 にある定義を以下に示す。

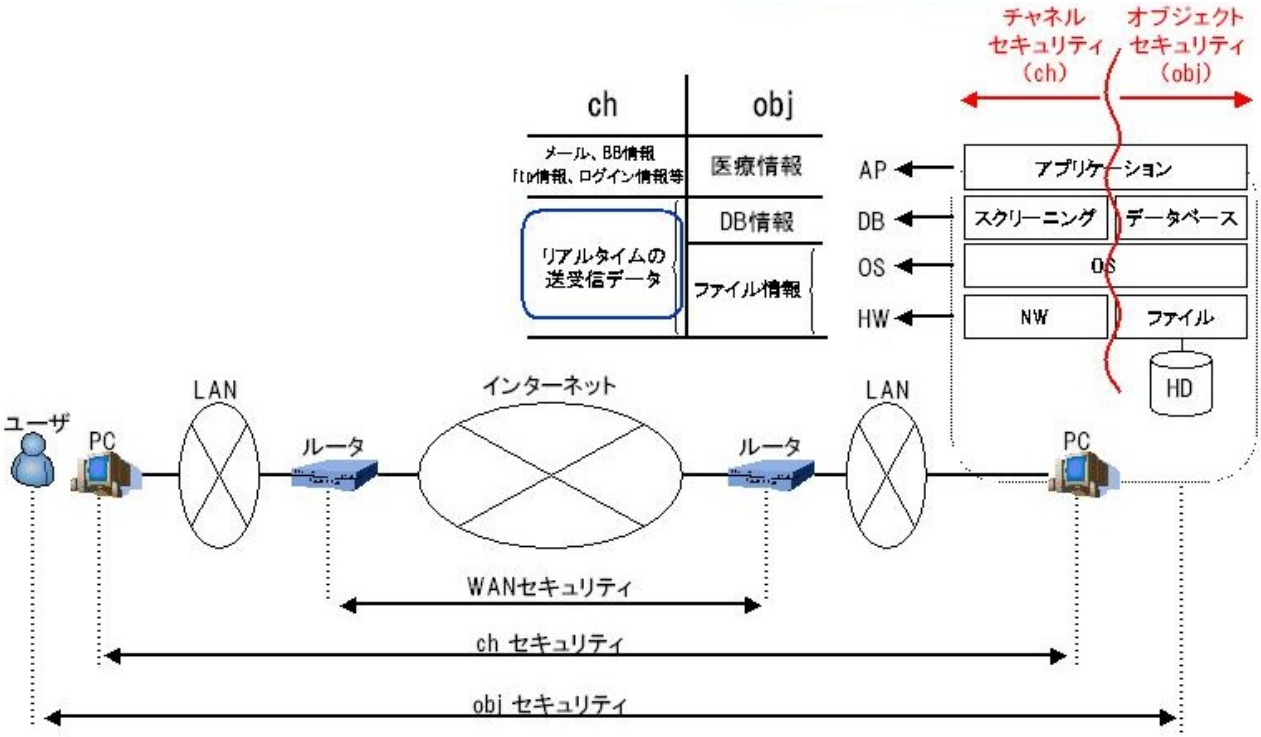
（RFC3552 より抜粋）

オブジェクトセキュリティとチャネルセキュリティを概念的に区別することが有用です。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をいいます。チャネルセキュリティ手段は、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しますが、そのチャネルは、オブジェクト境界について特別な知識をもちません。

電子メールメッセージの事例を考えます。メッセージが IPSec もしくは TLS によってセキュアにされたコネクション上を運ばれるとき、そのメッセージは、転送中は防護されています。しかし、これは、受信者のメールボックス中や、途中の中間スプールファイルでは防護されていません。さらに、メールサーバは、一般に、ユーザではなくデーモンとして動作するので、一般的に、メッセージの認証は、ユーザ認証ではなく、単にデーモン認証を意味するに過ぎません。さらに、メールのトランスポートは、ホップ by ホップなので、たとえユーザが中継の最初のホップを認証する場合でも、認証は、受信者によって安全に検証されることができません。逆に、電子メールメッセージが S/MIME または OpenPGP で防護されているとき、受信者によって検証・復号されるまで、メッセージ全体が

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

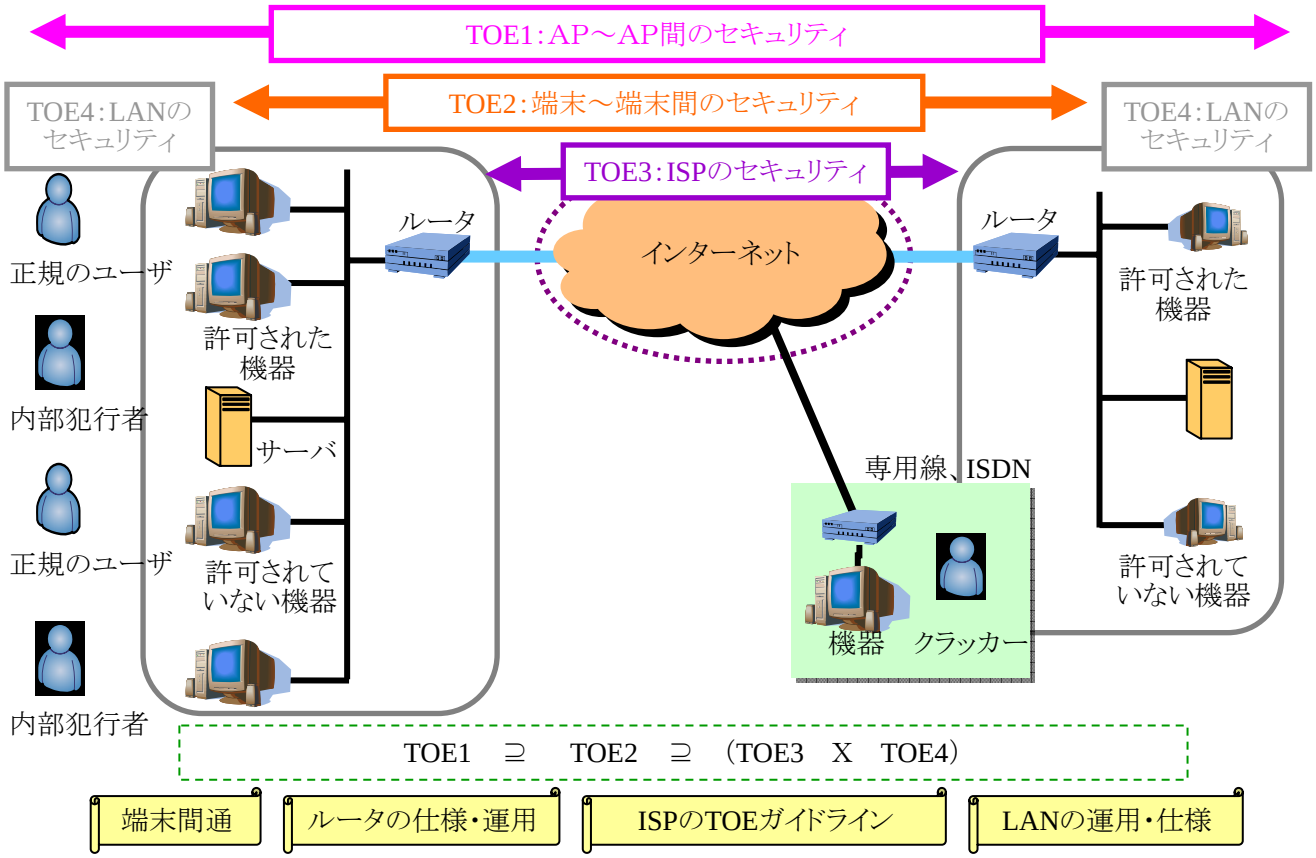
暗号化され、インテグリティが確保されます。これは、メッセージを送ったマシンではなく、実際の送信者についての強い認証も提供します。これはオブジェクトセキュリティです。さらに、受信者は、署名されたメッセージの真正性を第三者に提供できます。




3.2 検討対象(TOE)の整理

3.2.1 TOE の全体像

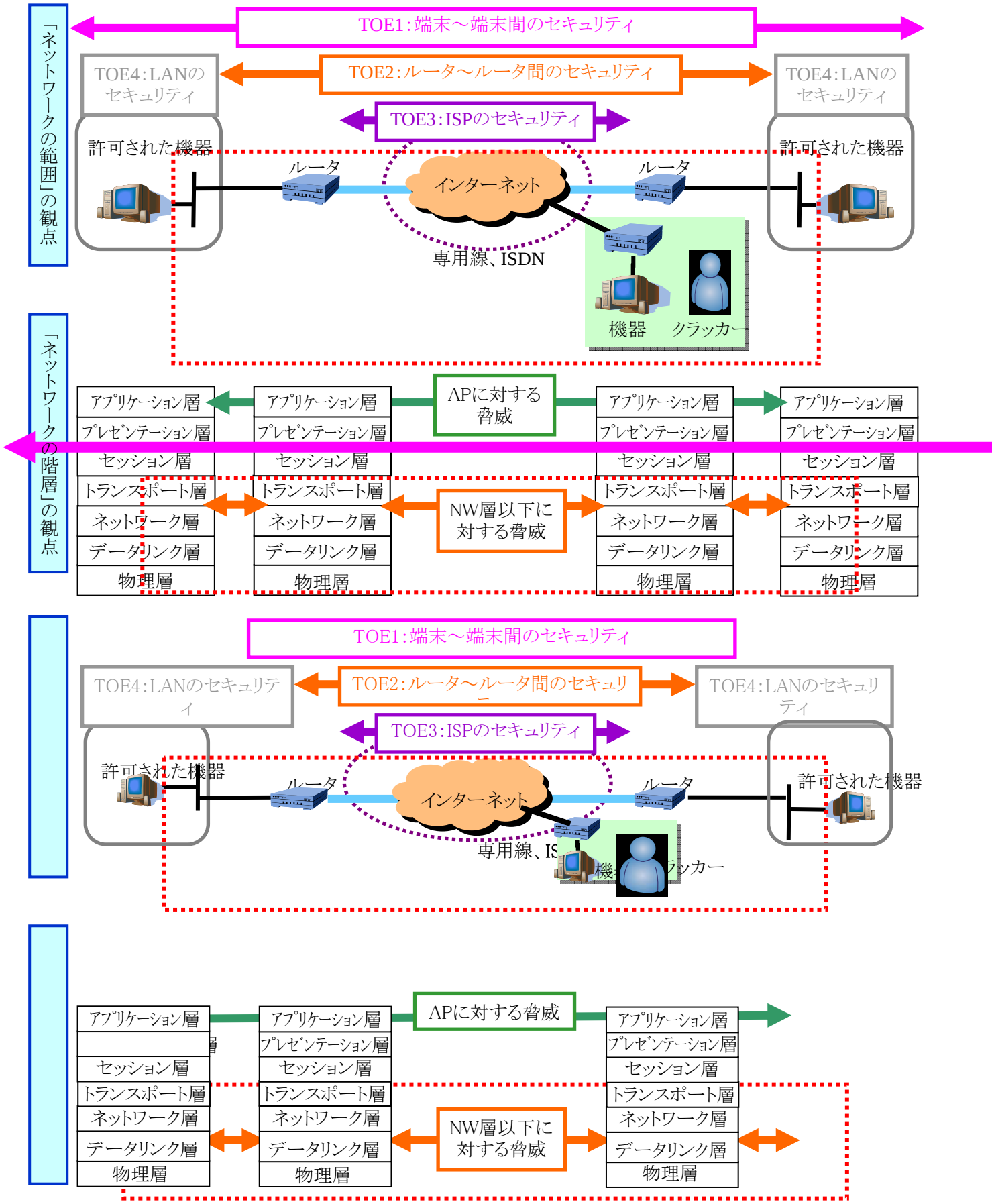
All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




3.2.2 検討範囲と OSI の関係

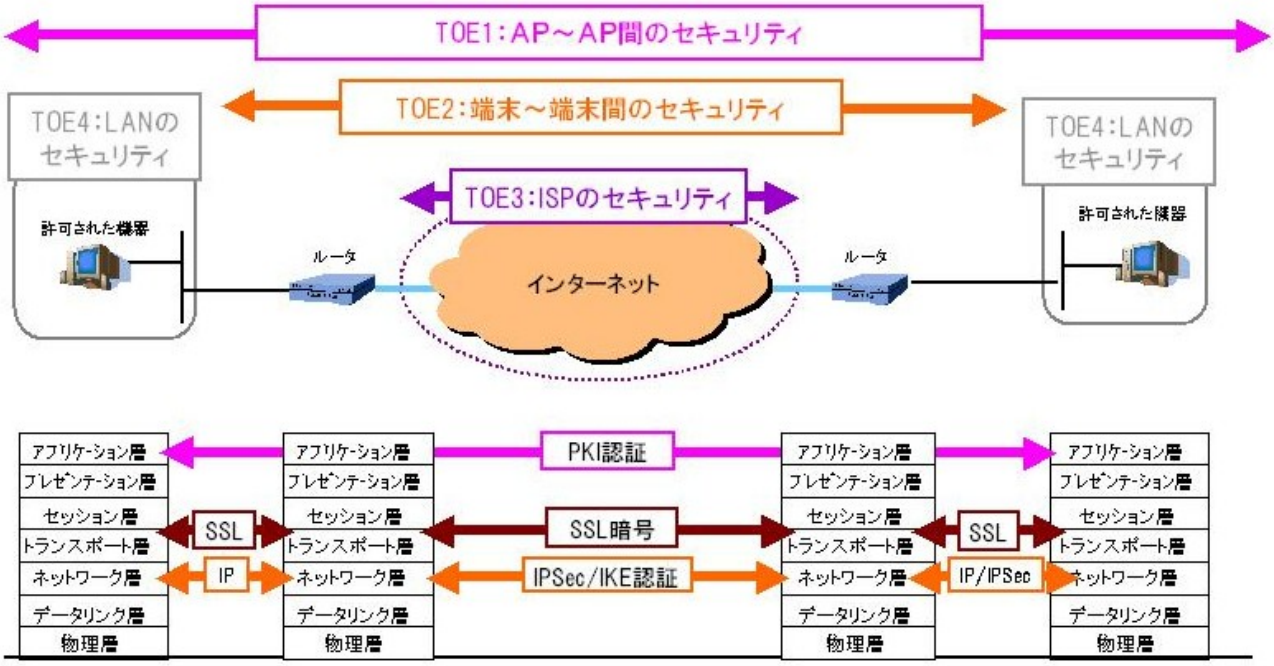
前頁までの検討結果をまとめると、本 WG で検討対象とする範囲は下記の赤点線で囲った範囲となる。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007



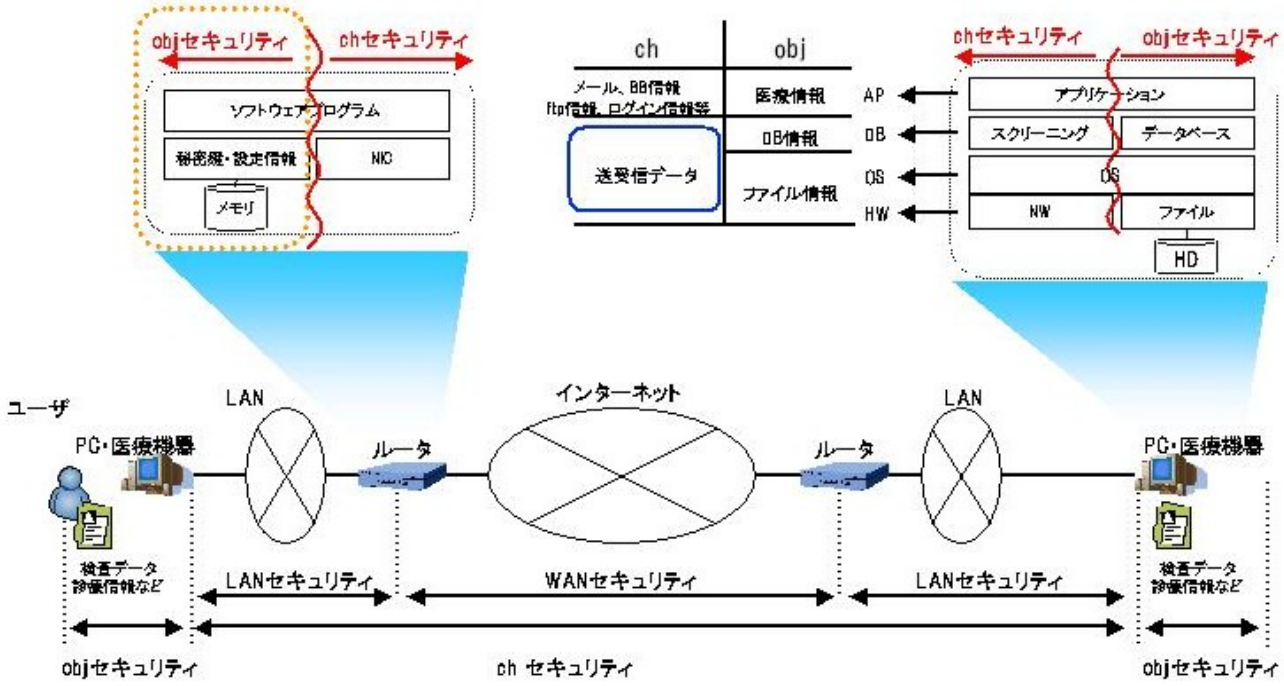

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

暗号通信技術との対応で整理すると、下記のような関係になる。基本的には、AP に対する脅威を守る SSL や S/MINE のような技術の通信上のトラヒックセキュリティを守る下位の IP 層レベルでのトラヒックセキュリティを担保が主眼であり、すべてのトランスポート層以上の暗号化技術と組合せて利用することが前提である。




3.2.3 守るべき資産

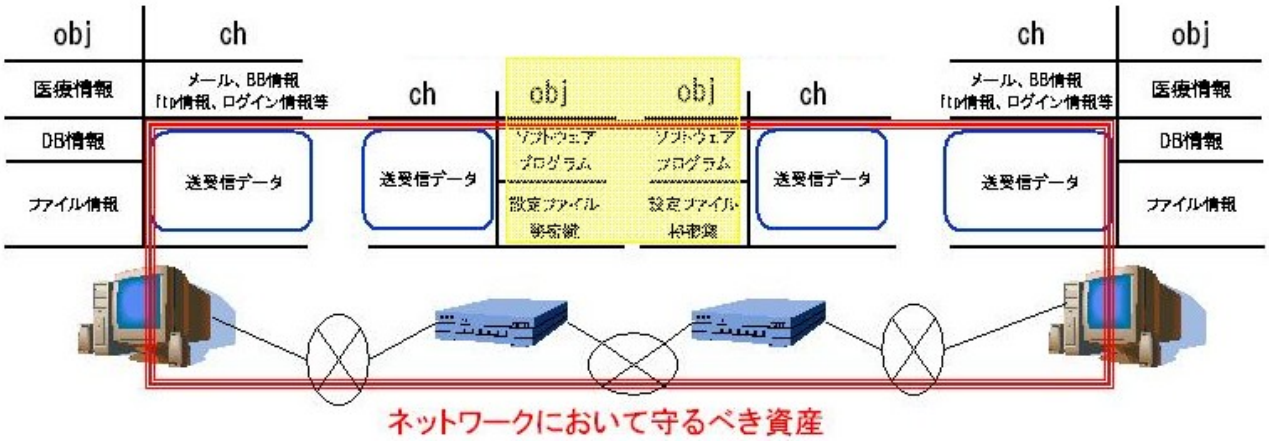
セキュアネットワーク基盤全体（端末ーネットワークー端末間）において、検討対象とする範囲を明確に定義しなおすと、「ch セキュリティ」と「NW 機器の obj セキュリティ」とに分類できる。




All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

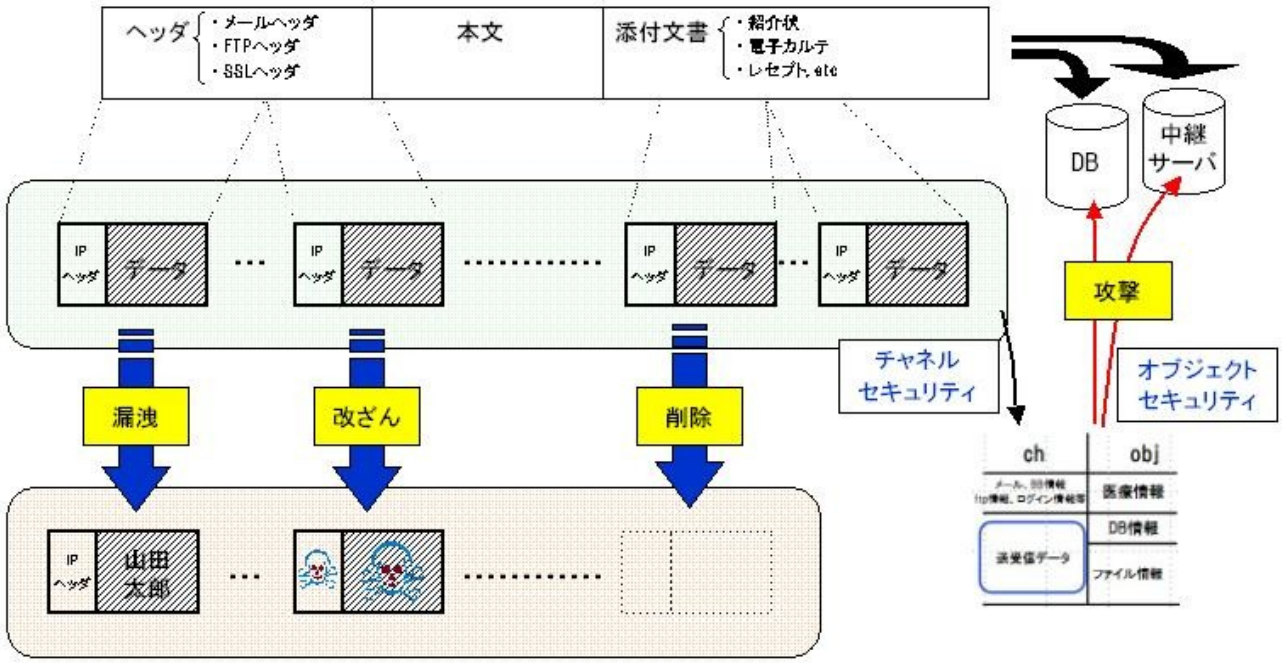
前章で整理した通り、検討対象とする範囲において守るべき資産としては、下記に示される事項について検討しなければならない。端末間のchセキュリティ　　⇒　送受信データ

(2) NW 機器の obj セキュリティ ⇒　NW 機器の設定ファイルや秘密鍵等




(a) 送受信データの定義

送受信データは、下図に示すように複数のパケットに分割されて送信される。端末間の ch セキュリティを守るということは各パケットの IP ヘッダやデータ部分を守ることに他ならない。




(b) NW 機器の obj セキュリティに関わる構成機能

| 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 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 大区分 | 小区分 | 機能概要 |
|---|---|---|
| | 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 |

4.ネットワークの脅威に対する対処方法

4.1 WAN の定義

4.1.1 一般的な分類

一般的に拠点間のアクセスに用いられる WAN の形態には主に以下のものがあげられる。

(1) 専用線

(2) ISDN

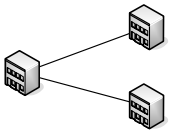
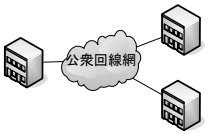
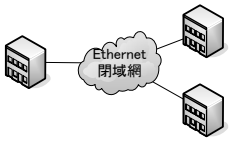
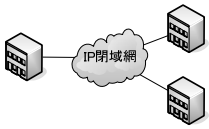
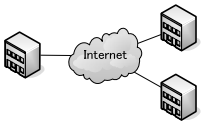
(3) 閉域網

(a) 広域イーサネット

(b) IP-VPN

(4) オープンネットワーク

(a) インターネット(インターネット VPN によって安全性を確保)

| 項目 | 専用線 | ISDN | 広域イーサネット | IP-VPN | インターネット |
|---|---|---|---|---|---|
| バックボーン | 専用回線 | 公衆回線 | 通信事業者保有網 | 通信業者保有網 | インターネット |
| 網プライベート性 | 常時占有 | 利用時占有 | 常時共有 | 常時共有 | 常時共有 |
| 接続先<br>識別方法 | 拠点間直結 | 電話番号 | MAC アドレス | サービス用<br>IP アドレス | グローバル<br>IP アドレス |
| 接続先管理者 | サービス<br>プロバイダ | ユーザ | サービス<br>プロバイダ | サービス<br>プロバイダ | ユーザ |
| 接続範囲 | サービス加入者 | 電話加入者 | サービス加入者 | サービス加入者 | インターネット接続者 |
| 同時接続 | 1:1 | 1:1 | N:N | N:N | N:N |
| イメージ |  |  |  |  |  |

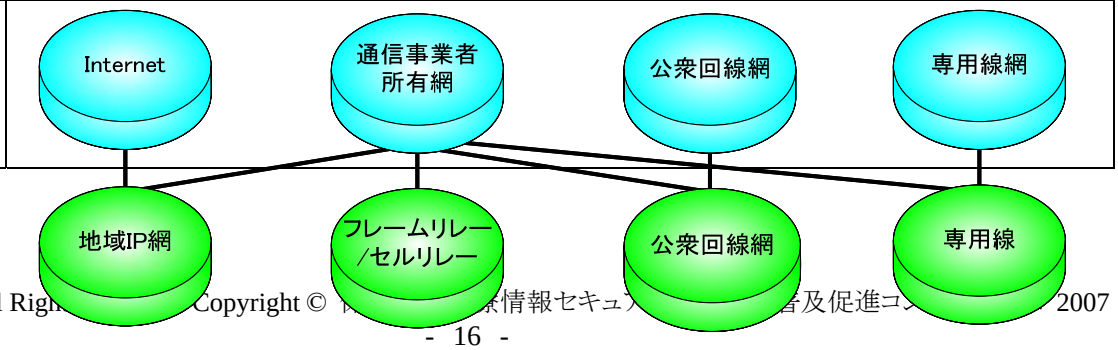
アクセス形態の違いから通信回線による比較を下記にまとめる。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 評価項目 | 専用線 | ISDN | VPN(閉域 IP 網) |
|---|---|---|---|
| 安全な通信 | 物理的に専用のネットワークを介して通信を行う為、通信経路におけるデータの機密性は保証される。 | 電話回線を介しての通信となる為、電話回線の安全性に依存することになるが、実質的には機密性は保証されていると言える。 | 通信データの暗号化機能を利用することにより、データの機密性を確保できる。(機密性は使用する暗号の強度に依存する) |
| 大容量データの高速通信 | 大容量高速通信については、契約内容に基づき対応可能である。また、通信中の品質保証については、契約帯域は完全保証される。 | 大容量高速通信については、技術仕様により対応が困難である(64kbps～1.5Mbps)。また、通信中の品質保証については、保証される。 | 大容量高速通信については、契約する回線速度に基づき対応可能である。また、通信中の品質保証については、インターネットを介するとベストエフォートとなる。 |
| ネットワークの拡張性 | 新たに通信する拠点を拡張する場合、既存の拠点と追加拠点の間に物理的に回線を敷設する必要がある。 | ISDN 回線を利用できる環境であれば、容易に拡張可能である。 | 方式による違いはあるものの、基本的にメッシュ型ネットワークに適した方式である為、拡張性は高い。 |
| 構成メンバーの真正性 | 事業者指定の機器を利用する為、ルータ等の機器の真正性は保証される。 | 事業者指定の機器を利用する為、ルータ等の機器の真正性は保証される。 | IP-VPN の場合、事業者指定の機器を利用する為、ルータ等の機器の真正性は保証される。<br>インターネット VPN の場合、機器認証/利用者認証を利用することにより、真正性は保証される。 |
| セキュアネット接続に関するコスト | イニシャルコスト、ランニングコスト共に高価である。通信距離に比例して通信費も高額になる。 | イニシャルコスト、ランニングコスト共に低価である。 | イニシャルコスト、ランニングコスト共に専用線と比較した場合、低価である。 |

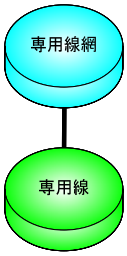
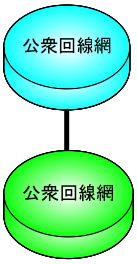
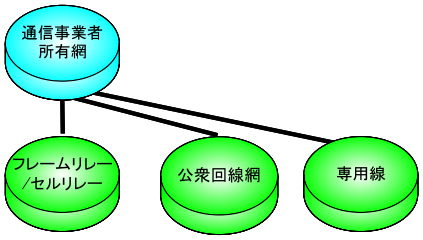
一方、WAN の形態は、加入者ネットワークから中継系ネットワークを経て再び加入者ネットワークに接続されることで、拠点間の通信が実現されている。複数の事業者所有ネットワークを経由する場合、接続点において情報の盗聴・漏洩に対し信頼性が考慮する必要がある。また、加入者系と中継系の組合せによっては、中継系の特性を活かしたスループットの保障やセキュリティの担保ができない場合がある。このため、ガイドラインの策定に当たってセキュリティの観点からは中継系と加入者系の共有の度合いを考慮して WAN の特徴を整理する必要がある。

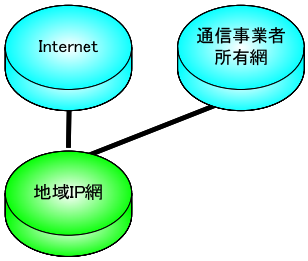
| 中継系ネットワーク | | | | |
|---|---|---|---|---|
| 種別 | インターネット | 通信事業者所有網 | 公衆回線 | 専用線網 |
| 占有状態 | 常時共有 | 常時共有 | 利用時占有 | 常時占有 |
| 機密性 | 低 | 低 | 高 | 高 |
| 接続イメージ | | | | |




All Rig Copyright © 情報セキュ 及促進コ 2007

| | | | | |
|---|---|---|---|---|
| 種別 | 地域 IP 網 | フレームリレー/セルリレー | 公衆回線 | 専用線 |
| 占有状態 | 常時共有 | 常時占有 | 利用時占有 | 常時占有 |
| 機密性 | 低 | 高 | 高 | 高 |
| 加入者系ネットワーク | | | | |

| コストに応じて回線品質やスループットが保証される接続形態 | | |
|---|---|---|
| 専用線 | 公衆網 | 閉域 IP 網 |
|  |  |  |
| 常時1:1で独占的に線を使用する。 | 利用時は独占的に1:1で回線を使用する。 | 複数の利用者で網を共有するが、品質やセキュリティは通信事業者が担保する。 |
| 通信業者によりスループット、回線品質などが保証されている。 | | |

| 回線品質やスループットを割り切ってコストを抑えた接続形態 |
|---|
| オープンネットワーク |
|  |
| 複数の利用者と網を共有する。 |
| 通信業者によってスループット、回線品質などが保証されない。<br>共用網を経由するため、ユーザは通信路を暗号化する必要がある |

専用線、IP-VPN、広域イーサ方式は、単一事業者、あるいは契約によって同一レベルのセキュリティが確保できる。しかし、広域イーサ方式は、複数の事業者を束ねた契約主体が必要になり、医療分野の実情にあった契約締結が難しい。ISDN は、大容量高速通信への対応が難しい。

地域 IP 網は共有型 NW のため、事業者が検知できないデータの盗聴、改ざん、挿入やセッション乗っ取りなどのハッキング手法が知られており、セキュリティに関する脆弱性に問題がある。このため、このような共有型の IP ネットワークを組合せたネットワークはオープンネットワークとして扱った方が安全である。このようなオープンネットワークは、一般的にユーザ側で通信に関するセキュリティを担保する手段を講じる必要がある。オープンネットワークは、共用型のため、通信事業者がスループットの保障やセキュリティの担保が難しい。このため、ユー

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

ザの側でセキュリティを高める技術を採用して他方式と同等の安全性を確保する必要がある。

4.1.2 脅威の所在と課題

(1) NW 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障された専用線、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。

(2) オープンネットワークは、インターネット VPN(SSL/TLS)やインターネット VPN（IPSec）のような 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、インターネット VPN（SSL/TLS）には、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。

(3) 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。

(4) 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 カードを用いた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。

4.2 ネットワークにおける脅威とセキュリティ対策の整理

4.2.1 ch セキュリティ

(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 を参考に洗出しを行った。下記に洗出した脅威と解説をまとめる。

| 類型 | 脅 威 | 解 説 |
|---|---|---|
| T1 | 平文伝送 | 送受信データが通信路上を平文で伝送されているために、送受信データを盗聴することにより情報漏洩が起こる可能性がある。 |
| T2 | 共有パスワード | エンティティ認証に使用されるパスワードが平文で伝送されているため、送受信データを盗聴することによりパスワードを取得される可能性がある。その結果として、取得したパスワードを利用してサーバにログインされる危険性がある。 |
| T3 | 辞書攻撃 | 「平文」と「暗号文」および「暗号文」と「ハッシュ関数」を取得している場合に、攻撃者は正しい応答をもたらす秘密鍵（パスワード）を発見するまで、（辞書ファイルのような）よくある単語リストから選択した文字列を秘密鍵の候補として試行する。その結果として、エンティティ間の認証に使用される秘密鍵が漏洩する可能性がある。 |
| T4 | 推定攻撃 | 「平文」と「暗号文」および「暗号文」と「ハッシュ関数」を取得している場合に、攻撃者は正しい応答をもたらす秘密鍵（パスワード）を発見するまで、すべての共有された秘密鍵（パスワード）の候補を試行する。その結果として、エンティティ間の認証に使用される秘密鍵が漏洩する可能性がある。 |
| T5 | NIS,解読ツールの存在 | 「平文」と「暗号文」および「暗号文」と「ハッシュ関数」を取得している場合に、攻撃者は正しい応答をもたらす秘密鍵（パスワード）を発見するまで、すべての共有された秘密鍵（パスワード）の候補を試行を解読ツールを用いて実施する。解読ツールを用いることにより、秘密鍵を判別するために要する時間を短縮することができる。その結果として、エンティティ間の認証に使用される秘密鍵が漏洩する可能性がある。 |
| T6 | トポロジーの破壊 | 攻撃者は、データを送受信するためにトポロジーを破壊して、攻撃者自身をパス上に配置します。その結果として、盗聴や IP ヘッダの改ざん等のより多くの攻撃をしかける |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 類型 | 脅 威 | 解 説 |
|---|---|---|
| | | ことが可能になるため、パス上を送受信されるデータが攻撃される危険性が増大する。 |
| T7 | 同一リンク上の判別 | パス上の特殊ケースとして、攻撃者が同一リンク上ローカルネットワーク上に存在する場合がある。ローカルネットワーク上に位置するホストと、そうでないホストを区別できない場合に外部ネットワークからの攻撃を許してしまう可能性が増大する。 |
| T8 | 常用プロトコルでの攻撃 | HTTP や SMTP, SOAP などの一般的にファイアウォールを通過するプロトコルにおける攻撃に対して暗号化ペイロードやメッセージ認証の対策で影響を軽減しない場合に、LAN セキュリティの侵害を引き起こす危険性がある。 |
| T9 | 内部の脅威 | 攻撃者が内部ネットワークに存在している場合には、通常、ネットワークを送受信されるいかなるデータを読むこと、変更すること、および削除することが可能となる。このような攻撃者からの盗聴、改ざん、削除などの攻撃に耐えうるよう対策すべきである。 |
| T10 | 情報の不正コピー | ウィルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウィルスには、単にシステムの設定を変更したり、隠れてしまうものもある。 |
| T11 | セッション乗っ取り | エンティティ間の認証を行わないと、確立したセッションにおいて攻撃者が中間者が入り込むことが可能となる。攻撃者は、一方のエンティティから送信されたパケットを盗聴し、対象サーバに到達する前にパケットを挿入することで、中間者攻撃を成功させることが可能となる。 |
| T12 | ARP 詐称<br>(IP アドレス詐称) | 攻撃者は LAN 上のホストの ARP テーブルの書き換えを行うことにより、送信者が意図した宛先ではなく攻撃者にパケットを送信させることができる。 |
| T13 | アクセスの証明 | 否認防止とは、一般的に、送信者が送信事実を否定したり、受信者が受信事実を否定したりすることである。攻撃者がこれらの事実を否定することを防止することはできないが、通信が行われた記録を適切に収集・管理することにより、証拠を提出して、これらの事象が発生していることで対応することが可能となる。 |
| T14 | TCP SYN パケット挿入 | メッセージ挿入攻撃において、攻撃者は、いくつかの選択された属性についてメッセージを偽装し、ネットワーク中に挿入する。攻撃者は、これらの挿入されたメッセージの応答を受け取る必要がないため、これらの攻撃は送信元アドレスを偽造されることがしばしばある。 |
| T15 | TLS RST 偽装 | トランスポート層のトラフィックセキュリティの対策を実施していない状況では、メッセージ挿入攻撃を実施することで TCP コネクションをリセットすることが可能となる。その結果として、TLS/SSL コネクションの切断が行われる可能性がある。 |
| T16 | シーケンス番号推測攻撃 | 攻撃者は標的に信頼されたホストの口を塞ぎ、標的に話しかける際に、信頼されたホストの IP アドレスを偽装して、次に最初に使われるシーケンス番号を推測することに基づく 3 ウェイハンドシェイクを完結させる。標的への通常のコネクションは シーケンス番号の状態の情報を集めるのに使用され、このシーケンス全体が、アドレスに基づく認証と組み合わされて、攻撃者が標的となるホスト上でコマンドを実行できるようになる可能性がある。 |
| T17 | MAC チェック未使用 | メッセージ変更攻撃において、攻撃者は、回線からメッセージを削除し、それを変更し、ネットワーク中に再投入する。攻撃者がメッセージ中にデータを送ることを望むが、同時に、その一部を変更することを望む場合、この種の攻撃は特に有効となる。 |
| T18 | ホスト to ホスト SA | ホスト間での認証において暗号化されたメッセージのやり取りを実施していると、攻撃者が利用できるホストに到達した際に複号されたメッセージを、同一ホスト内の別のポートに転送することにより、暗号文を参照される可能性がある。 |
| T19 | ウィルス混入後の転送 | ウィルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウィルスには、単にシステムの設定を変更したり、隠れてしまうものもある。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 類型 | 脅　威 | 解　　説 |
|---|---|---|
| T20 | 情報の破壊・書換え | ウィルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウィルスには、単にシステムの設定を変更したり、隠れてしまうものもある。 |
| T21 | メッセージ盗聴後再送 | 例えば、クレジットカードによる購入や株取引のように、何らかのサービスを要求するために S/MIME メッセージが使われる事例がある。攻撃者が被害者の邪魔をするだけの場合にはサービスを 2 回実行することを望むため、攻撃者はメッセージを補足し、たとえそれを理解できなくても、再送することにより結果的にトランザクションを 2 回実行させることが可能となる。 |
| T22 | 自動発呼による再送 | ISDN 回線では，同一電話番号に連続して規定回数(3 回)発呼しても接続できなかった場合，その電話番号への発呼を規定時間(3 分間)抑止する必要があります。このため，何らかの要因によって発呼規制状態の通信相手への送信データが発生しても，ISDN への発呼が行えない場合があります。なお，通信相手指定の show peer コマンドによって，発呼規制状態にあるかどうかを確認できます。 |
| T23 | TCP SYN フラッド攻撃 | 攻撃者がパケットを挿入することによって、被害者に膨大な資源（この場合はメモリ）を浪費させることができる。あわせて攻撃者は、この行為を被害者から全くデータを受け取らずに行うことができるため、攻撃を匿名で行うことができる。 |
| T24 | DDoS | DDoS において、攻撃者は、標的マシンを同時に攻撃するように、数多くのマシンを準備し、数多くのマシンに攻撃のリモートによる開始ができるプログラムをしかけることによって達成される。 |
| T25 | 災害・物理的破壊 | ネットワーク機器等に倒壊防止対策等の保護措置を施していない場合、災害や破壊行為などを受けることにより、機器が正常に動作せず提供中のサービスが停止してしまう可能性がある。 |
| T26 | 不正な用法 | しばしば Web サーバはあらゆるユーザにデータを提供しますが、ページを変更する権限を特定のユーザに限定している。一般公衆によるこのような変更が「不正な用法」である。 |
| T27 | 不適切な用法 | 一般的に、ユーザは電子メールを送ることが許可されているが、一定の大きさ以上のファイルやウィルスに感染したファイルを送信することは禁止されている。このような行為は「不適切な用法」である。 |
| T28 | なりすまし | 正規のユーザが使用する、ID や秘密鍵を使用して、エンティティ認証や権限の認可を行うため、攻撃を検知しにくい。証拠収集やアーカイビングしている証跡を確認することで検知することが可能である。 |
| T29 | サービス中断による不正処理 | 通信中にネットワーク機器の故障やネットワーク回線が何らかの理由で切断された場合、処理途中でサービスが異常終了する可能性がある。異常終了した場合、それまでの入力データがどのように処理されるか想定できない危険性がある。 |
| T30 | 改ざん | オブジェクトセキュリティにおけるデータインテグリティを侵害する行為。そのために、なりすましが行われることもある。 |
| T31 | 過失・盗難・紛失 | セキュリティインシデントは、故意または過失によって引き起こされる場合がある。後者は、誰かがドアをロックすることを忘れた場合、もしくは、ルータ中のアクセスリストを有効にし忘れた場合に引き起こされる。 |

(2) 脅威への対処方法の検討

セキュリティ関連の RFC をもとに、ch セキュリティに対する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。

| 脅威の定義 | 直接的な対策を示すセキュリティ関連 RFC とその記述 |
|---|---|

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

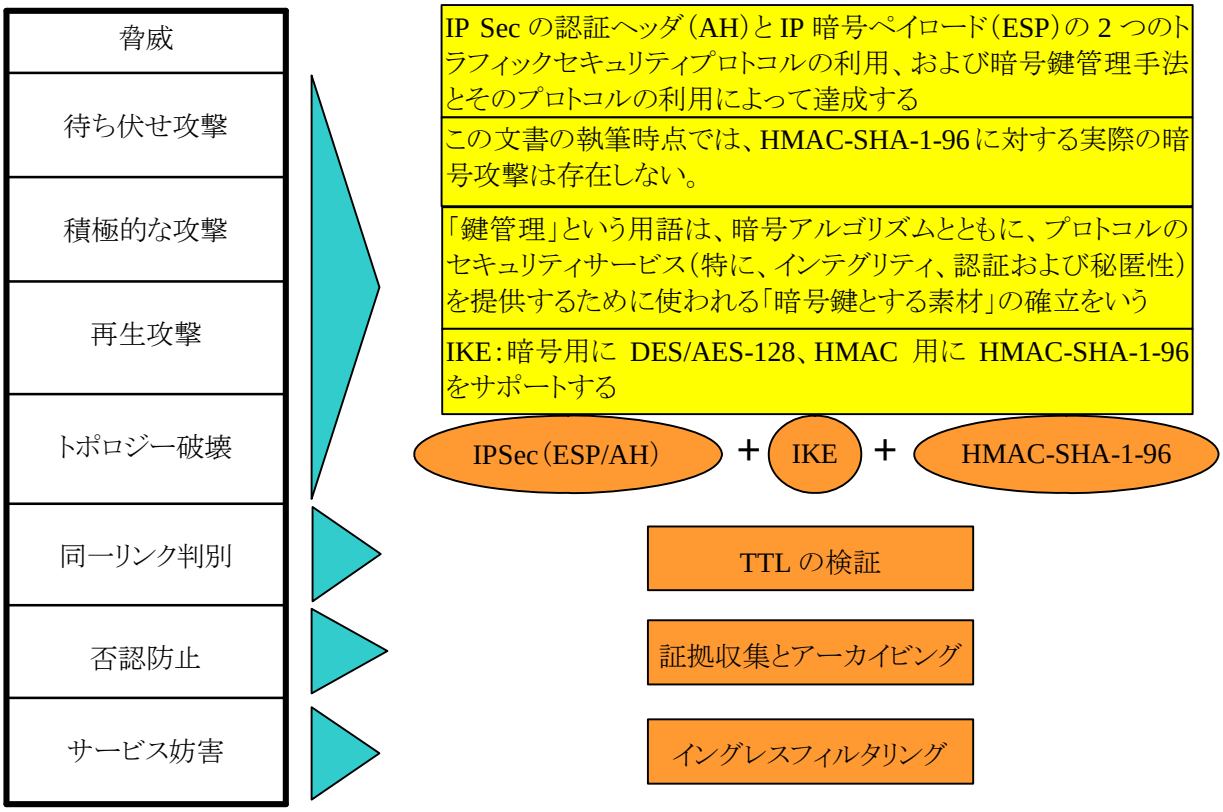
| 脅威の定義 | 直接的な対策を示すセキュリティ関連 RFC とその記述 | |
|---|---|---|
| 待ち伏せ攻撃（Passive Attack）<br>認証システムに対する攻撃のひとつ。これは、ストリーム中に何らデータを注入しないが、代わりに、待ち伏せつつ他の主体間を送られる情報を監視できることに依拠する。この情報は、後で正規のセッションに見えるものの際に使われる可能性がある。＜RFC1704＞ | RFC2406 | ESP は守秘性、データ生成元認証、コネクションレスインテグリティ、リプレイ防止サービス（部分的なシーケンスインテグリティの形式）、そして限定されたトラヒックフロー 守秘性を提供するために使用される。 |
| | RFC3552 | 「インターネットにおいて使われている多くのプロトコルは、それらが少なくとも待ち伏せ攻撃から防護されるようにするために、より強い認証メカニズムをもつ必要がある」と確信しています。また盗聴のような待ち伏せ攻撃に対する最低限の防護は、非開示パスワードシステムを使うことです。HMAC [RFC2104] は、選好される shared-secret 認証テクニックです。両者が同一の秘密鍵を知っている場合、HMAC は、あらゆる任意のメッセージを認証するために使えます。これは、乱雑なチャレンジを含み、これは、「HMAC は、古いセッションのリプレイを予防するために採用できること」を意味します。 |
| 積極的な攻撃（Active Attack）<br>データストリーム中に偽のパケットを注入することによって、あるいは、データ ストリームを運ぶパケットを変更することによって、不正に、データを変更したり、認証を得たり、あるいは、認可を得たりする試み。<br>＜RFC1704＞ | RFC2406 | IP 認証ヘッダは、IP データグラムに対してコネクションレスインテグリティとデータ生成元認証を提供し、さらにリプレイに対する保護を提供するために使用される。 |
| | RFC2828 | $ keyed hash （鍵付ハッシュ）<br>(I) 暗号技術的ハッシュ（例：[R1828]）。ここで、ハッシュ 結果への対応は、暗号技術的鍵である 2 番目の入力パラメータによって多様となる。（checksum 参照。）<br>(C) 入力データオブジェクトが変更された場合、新しいハッシュ結果は、その秘密鍵の知識無しには正しく計算できない。それゆえ、秘密鍵は、たとえ、そのデータについて積極的な攻撃の脅威があるときにもチェックサムとして使えるように、そのハッシュ結果を防護する。少なくとも 2 つの形態の鍵付ハッシュがある。:<br>* 鍵付暗号化アルゴリズムに基づく関数。（例： Data Authentication Code 参照。）<br>* ハッシュ結果を対応づける前に、入力データオブジェクトパラメータと鍵パラメータを結合すること（例： 連鎖させること）によって拡張された鍵無しハッシュに基づく関数 。（例： HMAC 参照。） |
| 再生攻撃（Replay Attack）<br>以前に送信された正規のメッセージ（あるいは、メッセージの一部）を記録し、再生することによる認証システムに対する攻撃。（パスワード、あるいは、電子的に転送されるバイオメトリックデータのような）あらゆる一定の認証情報は、本物であるかのように見えるメッセージを偽造するために記録されて、後で使われる可能性がある。<br>＜RFC1704＞ | RFC3631 | HMAC は、選好される shared-secret 認証テクニックです。両者が同一の秘密鍵を知っている場合、HMAC は、あらゆる任意のメッセージを認証するために使えます。これは、乱雑なチャレンジを含み、これは、「HMAC は、古いセッションのリプレイを予防するために採用できること」を意味します。 |
| | RFC4107 | 自動化された鍵管理とマニュアル鍵管理は、まったく異なる機能を提供します。特に、自動化された鍵管理テクニックと関連づけられたプロトコルは、ピアが生きていることを確認し、再生（replay）攻撃から護り、短期セッション鍵の源泉を認証し、プロトコル状態情報を短期セッション鍵と関連づけ、「フレッシュな短期セッション鍵が生成されていること」を確認します。さらに、自動化された鍵管理プロトコルは、暗号アルゴリズムについての交渉メカニズムを含めることによって、相互運用可能性を向上することができます。これらの可変な機能は、マニュアル鍵管理で達成することが不可能、もしくは、極めて面倒です。 |
| トポロジーの破壊<br>それゆえ、攻撃がデータを受け取ることができることに依拠する | RFC2196 | チェックサムは、たとえその侵入者が物理的なネットワークへの直接のアクセスができても、にせのパケットを受け取ることを防ぎます。シーケンス番号や、他のユニークな（一意の）識別子と併用す |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 脅威の定義 | 直接的な対策を示すセキュリティ関連 RFC とその記述 | |
|---|---|---|
| 場合、パス外のホストは、まず、自身をパス上におくために、トポロジーを壊さなければなりません。＜RFC3552＞ | | ることで、チェックサムは、「リプレイ（真似）」攻撃という、古い（当時は適切だった）ルーティング情報が侵入者、もしくは誤動作させられるルータによって返送される攻撃も防ぐことができます。概ね完全なセキュリティは、シーケンス（通番）ないし固有な識別子とルーティング情報の完全な暗号化によって可能です。これは侵入者がネットワークのトポロジー（構成）を推定するのを防ぎます。暗号化の欠点は、情報を処理するのにかかるオーバーヘッド（負荷）です。 |
| 同一リンクの判別<br>パス上の特殊ケースは、同一リンク上にいることです。状況によっては、ローカルネットワーク上のホストと、そうでないホストを区別することが望まれます。＜RFC3552＞ | RFC3552 | このための標準的テクニックは、IP TTL の値 [IP] を検証することです。TTL は、各転送者によって、減算されなければならないので、プロトコルは、「TTL が 255 にセットすること」と、「すべての受信者が TTL を検証すること」を命令できます。次に、受信者は、「確認しているパケットは、同一のリンク上からのものである」と信じる根拠をもちます。トンネリングシステムがある状態でこのテクニックを使用するときは注意が必要です。そのようなシステムでは、TTL を減算せずにパケットを通過させる可能性があるからです。 |
| 否認防止<br>システムがデータインテグリティを提供するとき、受信者は、送信者の身元と「彼は、送信者が送ろうとしたデータを受け取っていること」の両方に確信をもつことができます。しかし、彼は、必ずしもこの事実を第三者に実証することができるとは限りません。これを実現する機能は、「否認防止」と呼ばれています。＜RFC3552＞ | RFC3227 | 4.1 カストディの連鎖<br>あなたは、「どのように証拠が発見されたか」、「どのように扱われたか」および「それについて起きたすべての事項」を明確に記述することができるはずです。<br>下記事項が、文書化される必要があります。<br>＊ どこで／いつ／誰によって、証拠が発見、収集されたか。<br>＊ どこで／いつ／誰によって、証拠が対処、検査されたか。<br>＊ 誰が証拠のカストディとなり、その期間は。どのように、それは保存されたか。<br>＊ いつ、証拠のカストディを変えたか、いつ、どのように転送が行われたか。（送付番号等を含む。） |
| サービス妨害攻撃<br>問題のひとつは、「攻撃者は、しばしば被害者を迷惑させるために多くのサービス妨害攻撃から選択できること」であり、これらの攻撃の大部分が阻止できないので、普通の有識者は、しばしば、「可能性はあっても予防できない多くの他のサービス妨害攻撃があるとき、サービス妨害攻撃のうちの一種を防護する点はない」と想定します。＜RFC3552＞ | RFC2827 | 攻撃者が、正規に通知されているプリフィックス（ IP アドレス）の範囲内にない、偽った発信元アドレスを使用することをはばむために、すべてのインターネット接続プロバイダーには、この文書に記述されたフィルタリングを実装することが強く薦められます。 |

これら RFC の議論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、補足資料に付記した各脅威について具体的な攻撃方法を想定した脅威モデルを作成した。これらの作成した脅威モデルをもとに、厚労省ガ他の各種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 ch セキュリティのセキュリティ対策として、下表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。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 大分類 | 中分類 | 対策 | 考慮すべき事項 | 参照文書 | |
|---|---|---|---|---|---|
| 通信セキュリティ | エンティティ間の認証 | 単純なユーザ名/パスワード | 通信路の暗号化（秘匿化） | RFC3552 (BCP:72) | RFC の「セキュリティについての考慮事項」についての文章を書くためのガイドライン |
| | | ユーザ名/ワンタイムパスワードスキーム | | | |
| | | ユーザ名/チャレンジレスポンススキーム | | | |
| | | 共有鍵 | 自動鍵管理(IKE) | RFC4307 | IKEv2 における利用のための暗号アルゴリズム |
| | | | | RFC4109 | IKEv1 用アルゴリズム |
| | | | Moduler Exponential (MODP)グループ | RFC3526 | インターネット鍵交換プロトコル(IKE)のための追加 Moduler Exponential (MODP)Diffie-Hellman グループ |
| | | 鍵配布センター | 自動鍵配布(kerberos) | RFC1510 | Kerberos ネットワーク認証サービス(v5) |
| | | 証明書 | PKI | RFC4630 | インターネット X.509PKI および CRL プロファイルにおける Directory String 処理についての更新 |
| | 守秘性 | 暗号化ペイロード(ESP) | 暗号ハッシュ関数 (HMAC-SHA1-96) | RFC4305 | ESP および AH についての暗号化アルゴリズム実装要件 |
| | | | | RFC4302 | IP 認証ヘッダ |
| | | | 暗号アルゴリズム (3DES) | RFC1851 | ESP トリプル DES 変換 |
| | | | 暗号アルゴリズム (CBC モード) | RFC2451 | ESP CBC モード暗号アルゴリズム |
| | | | 暗号アルゴリズム (CBC モード AES) | RFC3502 | AES-CBC 暗号アルゴリズムと IPSec でのその使用法 |
| | データインテグリティ | メッセージ認証 | 暗号ハッシュ関数 (HMAC-SHA1-96) | RFC4305 | ESP および AH についての暗号化アルゴリズム実装要件 |
| | | | | RFC4302 | IP 認証ヘッダ |
| 否認防止 | | 証拠収集とアーカイビング | 収集手順<br>アーカイブ手順 | RFC3227 (BCP:55) | 証拠収集とアーカイビングのためのガイドライン |
| システムセキュリティ | 不正な用法/不適切な用法 | 認証と認可 | エンティティ間の認証<br>守秘性<br>データインテグリティ | RFC3552 (BCP:72) | RFC の「セキュリティについての考慮事項」についての文章を書くためのガイドライン |
| | サービス妨害 | イングレスフィルタリング | 境界フィルタリング<br>ソースアドレスフィルタリング | RFC3704 (BCP:84) | マルチホームされたネットワークのためのイングレスフィルタリング |
| | | | | RFC2827 (BCP:38) | ネットワークのイングレスフィルタリング:発信元 IP アドレスを偽ったサービス妨害攻撃をくじく |
| トラヒックセキュリティ | | IPsec | IP 暗号化ペイロード<br>IP 認証ヘッダ<br>自動鍵管理(IKE,Kerberos) | RFC3552 (BCP:72) | RFC の「セキュリティについての考慮事項」についての文章を書くためのガイドライン |
| | | | | RFC4301 | インターネットプロトコルのためのセキュリティアーキテクチャ |
| | | | | RFC3531 | インターネットについてのセキュリティメカニズム |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

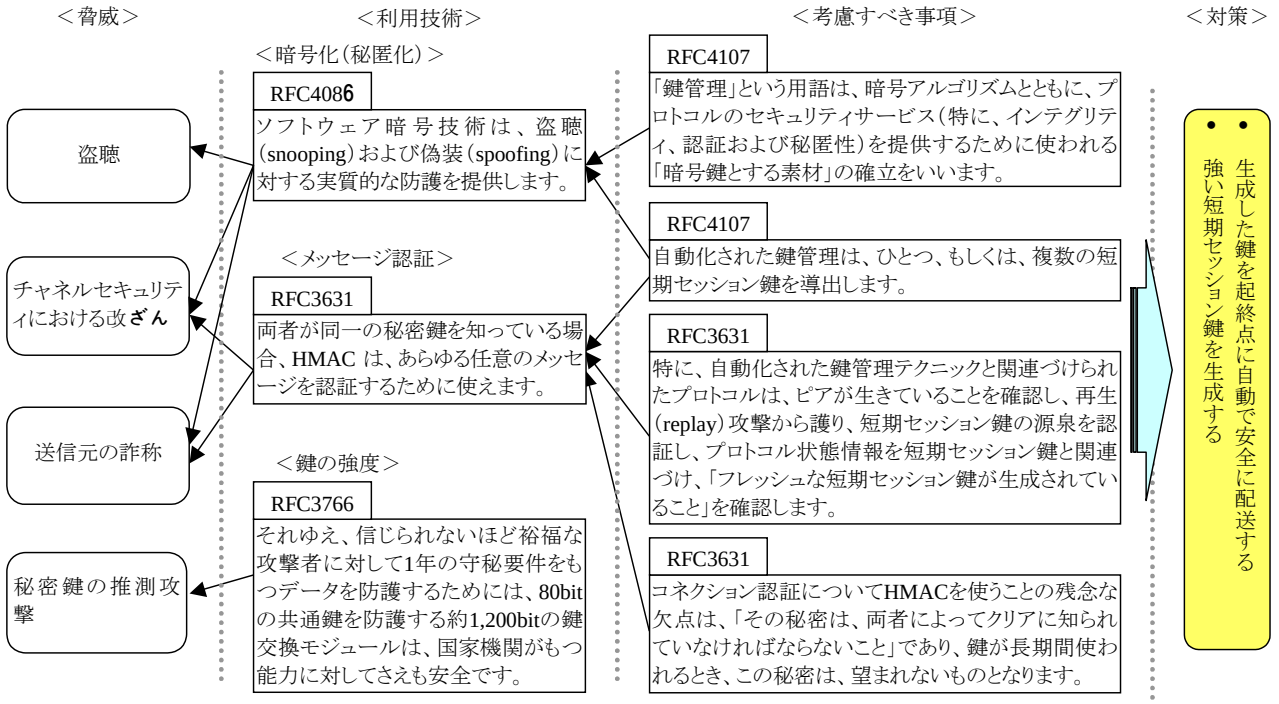
| 脅威 ＼ 対策 | | | | 通信セキュリティ | | | | | | | 否認防止 | システムセキュリティ | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | エンティティ間の認証 | | | 守秘性 | | | データインテグリティ | 証拠収集とアーカイビング | 不正な用法/不適切な用法 | サービス妨害 |
| | | | | | | | IPSec + IKE+自動鍵管理 | | | | | | |
| | | | | ユーザ名/パスワード | ユーザ名/ワンタイム | ユーザ名/チャレンジ | 共有鍵 | 証明書（公開鍵） | ペイロード（ESP） | メッセージ認証 | | 認証と認可 | イングレスフィルタリング |
| 盗聴 | 待ち伏せ攻撃 | 盗聴 | T1. 平文伝送 | × | - | - | - | - | ◎ | - | - | - | - |
| | | パスワード盗聴 | T2. 共有パスワード | × | ◎ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ | △ |
| | | オフラインでの暗号技術的攻撃 | T3. 辞書攻撃 | × | × | × | ◎ | ◎ | ◎ | △ | △ | △ | △ |
| | | | T4. 推定攻撃 | × | × | × | ◎ | ◎ | ◎ | △ | △ | △ | △ |
| | | | T5. NIS、解読ツールの存在 | × | × | × | ◎ | ◎ | ◎ | △ | △ | △ | △ |
| | トポロジー | パス外からの攻撃 | T6. トポロジーの破壊 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| | | | T7. 同一リンク上の判別 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| | | ファイアウォール | T8. 常用プロトコルでの攻撃 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| | | | T9. 内部の脅威 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| 侵入 | 積極的な攻撃 | 中間者 | T11. セッション乗取り | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| | | | T12. ARP 詐称(IP アドレス詐称) | △ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| | 否認防止 | | T13. アクセスの証明 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | ◎ | △ | △ |
| 改ざん | 積極的な攻撃 | メッセージ挿入 | T14. TCP SYN パケット挿入 | △ | △ | △ | △ | △ | ◎ | ◎ | △ | △ | △ |
| | | | T15. TLS RST 偽装 | △ | △ | △ | △ | △ | ◎ | ◎ | △ | △ | △ |
| | | メッセージ削除 | T16. シーケンス番号推測攻撃 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | △ |
| | | メッセージ変更 | T17. MAC チェック未使用 | △ | △ | △ | △ | △ | ◎ | ◎ | △ | △ | △ |
| | | | T18. ホスト to ホスト SA | △ | △ | △ | △ | △ | ◎ | ◎ | △ | △ | △ |
| 妨害 | | リプレイ攻撃 | T21. メッセージ盗聴後再送 | △ | △ | △ | ◎ | ◎ | ◎ | ◎ | △ | △ | ◎ |
| | | | T22. 自動発呼による再送 | △ | △ | △ | ◎ | ◎ | △ | ◎ | △ | △ | ◎ |
| | 妨害攻撃 | ブラインド妨害 | T23. TCPSYN フラッド攻撃 | △ | △ | △ | ◎ | ◎ | △ | ◎ | △ | △ | ◎ |
| | | 分散型妨害 | T24. DDoS | △ | △ | △ | ◎ | ◎ | △ | ◎ | △ | △ | ◎ |
| | | | T25.災害・物理的な破壊 | | | | | | | | | | |
| | | | T26. 不正な用法 | △ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | △ | ◎ | △ |
| | | | T27. 不適切な用法 | △ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | △ | ◎ | △ |
| | | | T28. なりすまし | △ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | △ |
| | | | T29.サービス中断による不正処理 | | | | | | | | | | |
| | | | T30.改ざん | △ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | △ |
| | | | T31.過失・盗難・紛失 | | | | | | | | | | |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

(3) 脅威への対処技術(ST)

(a) IKE

下記のような事由がある為、拠点間の認証において自動鍵配送(IKE)の利用が必要となる。また、接続時の機器認証において、盗難、紛失等の過失や故意を問わず、なりすましを防止するため、秘密鍵や認証情報は認証の時点で最新の状況を確認できるようにしておく必要がある。このようなセッション単位に厳密な認証を行い、強い短期セッション鍵を生成して IPSec の ESP トンネルモードで通信を行うインターネット VPN 方式を本資料ではオンデマンド(インターネット)VPN と呼ぶ。




適用パラメータは以下のようにする。

- 認証プロトコル:IKE
- 認証方式:公開鍵方式または自動鍵配送機能を適用した共通鍵方式による相互認証
- 暗号化共通鍵長:Diffie-Hellman MODP グループ 2（離散対数 1024 ビット）

(b) IPSec

トラフィックセキュリティを確保するためには、IPSec が有効な技術である。IPSec の特徴として、下記に示す2つのモードがあり、用途や保護対象の違いによりモードを選択することになる。また、IP（平文パケット）では実装していない「認証」「暗号化」の機能を有する。（「暗号化」はトンネルモードのみ）

一般的な入れ子をサポートするための要求条件は存在しないが、トランスポートモードでは、AH および ESP の両方をパケットに適用することができることに注意すること。この場合、SA 確立の手順では、最初に ESP をパケットに適用し、次に AH を適用することを保証しなければならない(MUST)。＜RFC2401 より抜粋＞

適用パラメータは以下のようにする。

- 伝送プロトコル:IPsec
- IP 暗号化ペイロード: ESP トンネルモード

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

●暗号化方式:3DES/AES + HMAC-SHA-1-96 + IKE

●メッセージ認証:HMAC-SHA-1-96 + IKE

IPSec のモード

| | IP パケット | IPSec パケット | |
|---|---|---|---|
| | | トランスポート・モード | トンネル・モード |
| パケットの構成 | IP ヘッダ / データ | 元の IP データグラムのデータ部だけが保護対象<br>IP ヘッダ / データ<br>IP ヘッダ / SEC ヘッダ / データ | 元の IP データグラム全体が保護対象<br>IP ヘッダ / データ<br>新 IP ヘッダ / SEC ヘッダ / IP ヘッダ / データ |
| IP アドレス | ACL | | |
| チェックサム | 誤り検知 | | |

IPSec トンネルモード

| | AH トンネルモード | ESP トンネルモード |
|---|---|---|
| パケットの構成 | IP ヘッダ / データ<br>新 IP ヘッダ / AH ヘッダ / IP ヘッダ / データ<br>認証する範囲 | IP ヘッダ / データ<br>新 IP ヘッダ / AH ヘッダ / IP ヘッダ / データ / ESP トレーラ / ESP 認証ヘッダ<br>暗号化される範囲<br>認証する範囲 |
| IP アドレス | ACL | ACL |
| ペイロードのハッシュ | 認証、改ざん検知 | 認証、改ざん検知 |
| 暗号化 | 非秘匿化 | 暗号化ペイロード |

(c) 否認防止

RFC3227 に準拠した証拠収集とアーカイビングを実施する。

(d) サービス妨害

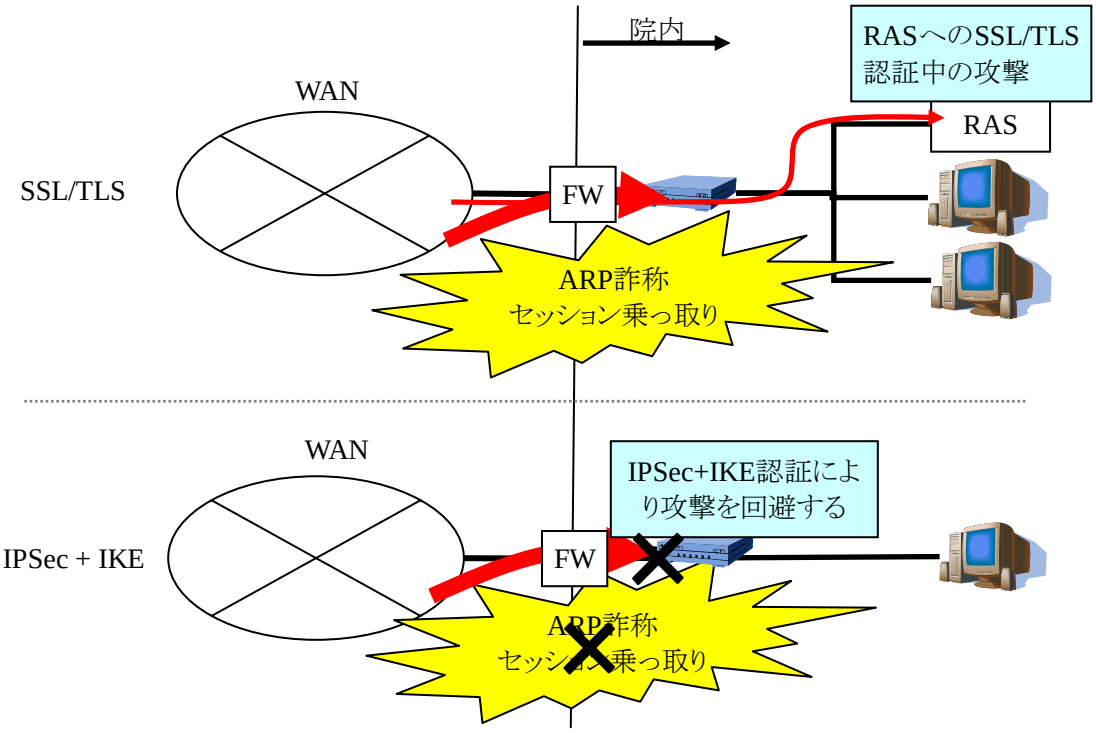
イングレスフィルタリングを提供する ISP と契約してサービス妨害の発生を抑えるようにする。

(e) 上位 AP の脅威との関係

アプリケーション層において TCP コネクションのためにチャネルセキュリティを提供する最も普及したアプローチは、SSL もしくは、その後継である TLS を使うことです。TLS は、IPSec がない IP 層の攻撃の影響を受けます。典型的には、これらの攻撃は、何らかのサービス妨害またはコネクション切断の形態をとります。例えば、攻撃者は、SSL コネクションを切断するために、TCP RST を偽装する可能性があります。TLS は、「切断攻撃」を検知す

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

るメカニズムをもっていますが、これらは、被害者に攻撃されていることを単に知らせるだけで、このような攻撃に直面したとき、コネクション存続性を提供しません。逆に、IPSec が使われている場合、このような偽装された RST を、TCP コネクションに影響を与えずに棄却できます。偽装された RST もしくは、TCP コネクション上の他のこのような攻撃が懸念される場合、AH/ESP もしくは TCP MD5 オプション[TCPMD5]が選ぶべき選択肢です。<RFC3552>




4.2.2 NW 機器の obj セキュリティ

(a) NW 機器における脅威(PP)の定義

NW 機器のリモート保守は、ネットワークを介してアクセスが行われるため、セキュリティ要件としては ch セキュリティがそのまま適用される。NW 機器の守るべきソフトウェアや設定情報等の機能要素を以下に挙げる。NW 機器の下記の機能や情報の盗難、改ざん、破壊等のハッキング行為が脅威として規定できる。

| 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 |

(b) 脅威への対処方法の検討

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

このような情報の盗難、改ざん、破壊等のセキュリティ要件を規定した IC カードのセキュリティに関する脅威に対する対策を参考に技術要素を下記のように整理した。

(i) NW 機器に係るセキュリティ要件

| | 項目 | 分類 | セキュリティ要件 |
|---|---|---|---|
| 1 | セキュアメモリ製造時における仮鍵および仮証明書の入手 | 運 | セキュアメモリ供給者は、規定された安全な手順に従い、登録認定機関から仮鍵および仮証明書を入手しなければならない。 |
| 2 | 登録された組織、団体との取引 | 利 | 機器製造者は、登録されたセキュアメモリ供給者および機器登録管理センターのみと取引しなければならない。 |
| 3 | 機器 ID の安全な格納 | 技・運 | 機器製造者は、機器登録管理センターから付与された機器 ID を安全にセキュアメモリ内に格納しなければならない。 |
| 4 | 正当なセキュアメモリの入手 | 運 | 機器製造者は、登録認定されたセキュアメモリ供給者から正当なセキュアメモリを入手しなければならない。 |
| 5 | セキュアメモリの輸送時の保護 | 技・運 | セキュアメモリの輸送に伴う盗難、改ざんを防ぐための措置を講じなければならない。 |
| 6 | 機器製造者における仮鍵の安全な入手 | 運 | 機器製造者は、セキュアメモリを輸送する際の輸送途中におけるセキュアメモリ改ざん防止、盗難後の偽造防止のために、セキュアメモリ供給者がセキュアメモリに埋め込んだ仮鍵を、セキュアメモリ供給者から安全に入手しなければならない。 |
| 7 | 機器出荷時におけるセキュアメモリのアクセス制御機能 | 技・運 | 機器出荷時に機器製造者は、セキュアメモリへのアクセス制御機能を有効にしなければならない。 |
| 8 | 機器の輸送時の保護 | 運 | 機器製造者は、利用者に安全に機器を渡さなければならない。 |
| 9 | 正当な AP の搭載に係る保証 | 利 | 機器登録管理センターは、搭載を許可した AP がセキュアメモリにダウンロードされることを、AP 搭載許可証により保証しなければならない。 |
| 10 | 機器によるサービス提供者の認証 | 技 | 機器によるサービス提供者の認証は、サービス提供者が登録認定機関から発行を受けた証明書を用いて行う。 |
| 11 | 正当な機器製造者による製造者情報の書込み | 技・運 | セキュアメモリに製造者情報を書き込む際、登録認定機関の公開鍵により機器製造者の公開鍵証明書を検証し、正しい場合のみ機器製造者の製造者情報を書き込まなければならない。 |
| 12 | AP 搭載許可証および AP 削除許可証の検証機能の具備 | 技 | セキュアメモリは、規定された公開鍵を用いて AP 搭載許可証および AP 削除許可証の正当性を検証する機能を有していなければならない。 |

(ii) NW 機器のセキュリティ機能要件

| | 項目 | 分類 | セキュリティ要件 |
|---|---|---|---|
| 1 | 機器 ID の安全な格納 | 技 | セキュアメモリ内に格納する情報に対して、論理的/物理的にアクセスを制御すること |
| 2 | セキュアメモリの輸送時の保護 | 技 | セキュアメモリ内に格納する鍵を暗号処理して格納できること |
| 3 | 機器出荷時におけるセキュアメモリのアクセス制御機能 | 技 | セキュアメモリ内に格納する情報に対して、論理的/物理的にアクセスを制御すること |
| 4 | 機器によるサービス提供者の認証 | 技 | セキュアメモリ内に事前に格納してある登録認定機関の証明書とサービス提供者から提示される証明書を検証できること |
| 5 | 正当な機器製造者による製造者情報の書込み | 技 | セキュアメモリに製造者情報を書き込む際、登録認定機関の公開鍵により機器製造者の公開鍵証明書を検証すること<br>また、正しい場合のみ機器製造者の製造者情報を書き込めるように制御すること |

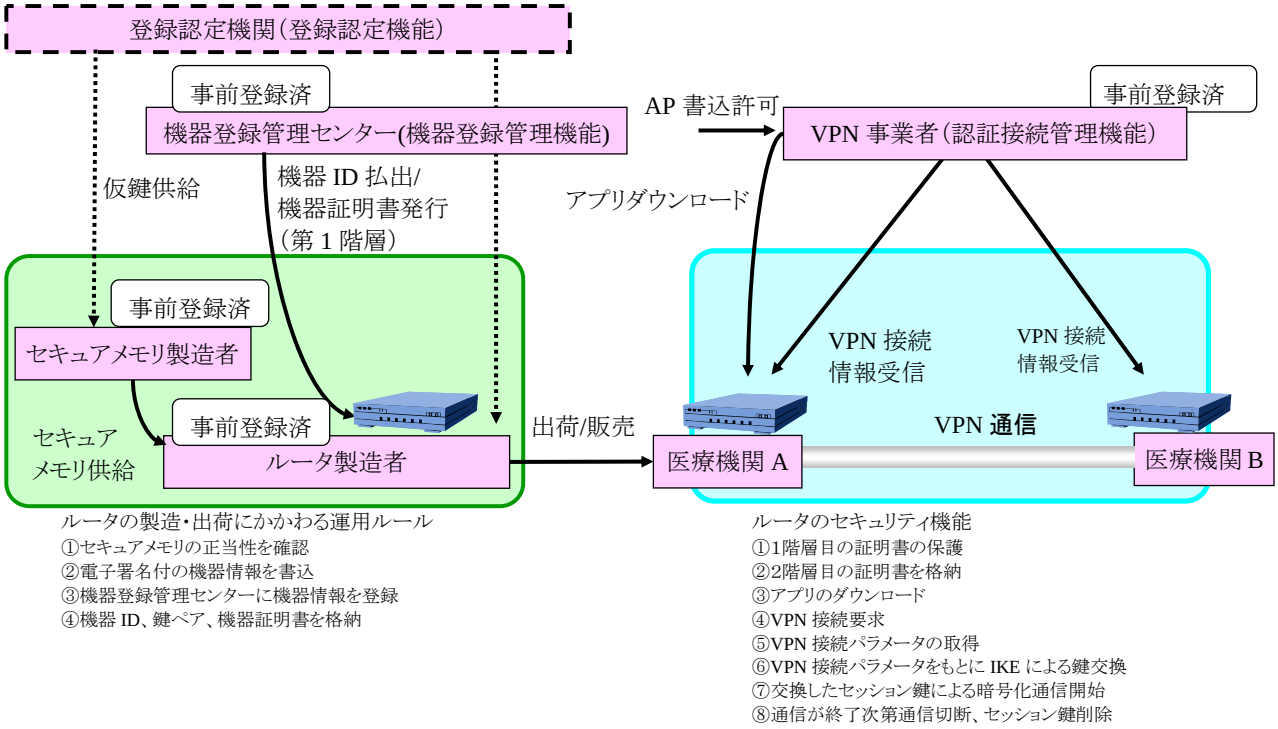
All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| | | | |
|---|---|---|---|
| 6 | AP 搭載許可証および AP 削除許可証の検証機能の具備 | 技 | セキュアメモリ内に事前に格納してある登録認定機関の証明書と AP 搭載許可証及び AP 削除許可証を検証できること<br>また、正しい場合のみ AP を書き込み/削除できるように制御すること |

(iii) NW 機器の製造・出荷に係る運用セキュリティ要件

| | 項目 | 分類 | セキュリティ要件 |
|---|---|---|---|
| 1 | セキュアメモリ製造時における仮鍵および仮証明書の入手 | 運 | セキュアメモリ供給者は、規定された安全な手順に従い、登録認定機関から仮鍵および仮証明書を入手すること |
| 2 | 機器 ID の安全な格納 | 運 | 機器製造者は、機器登録管理センターから付与された機器 ID を安全にセキュアメモリ内に格納すること |
| 3 | 正当なセキュアメモリの入手 | 運 | 機器製造者は、登録認定されたセキュアメモリ供給者から正当なセキュアメモリを入手すること |
| 4 | セキュアメモリの輸送時の保護 | 運 | セキュアメモリの輸送に伴う盗難、改ざんを防ぐための措置を講じること |
| 5 | 機器製造者における仮鍵の安全な入手 | 運 | 機器製造者は、セキュアメモリ供給者によりセキュアメモリに埋め込まれた仮鍵を、セキュアメモリ供給者から安全に入手すること |
| 6 | 機器出荷時におけるセキュアメモリのアクセス制御機能 | 運 | 機器出荷時に機器製造者は、セキュアメモリへのアクセス制御機能を有効にすること |
| 7 | 機器の輸送時の保護 | 運 | 機器製造者は、利用者に安全に機器を渡すこと |
| 8 | 正当な機器製造者による製造者情報の書込み | 運 | セキュアメモリに製造者情報を書き込む際、登録認定機関から発行された証明書（公開鍵）を提示し、製造者情報を書き込むこと |

(c) 脅威への対処技術(ST)




4.2.3 既存技術との比較・評価

ネットワーク上の脅威等に対する各種方式の対応状況を下記にまとめる。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

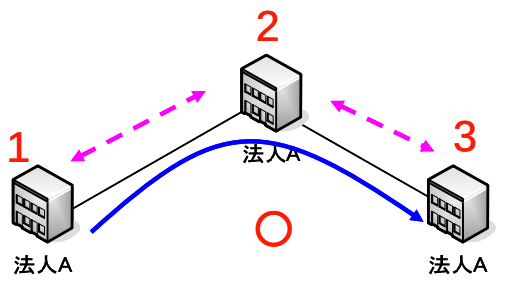
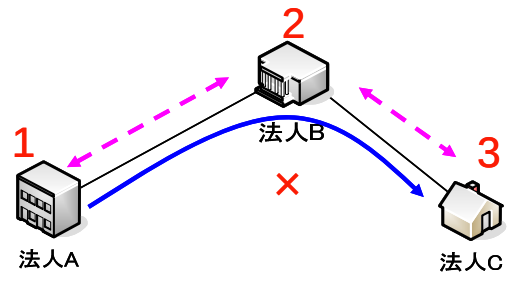
| 比較対象 | | | | | VPN | | | | 専用線 | 公衆回線 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | オンデマンド VPN | IP-VPN | インターネット VPN | | | |
| 評価項目 | | | | 階層 | | | | SSL/TLS | | |
| | | | | | | IKE+IPSec | | IP | | |
| | | | | | ISDN/ADSL/光 | | | | 専用線 | ISDN |
| 安全性 | 盗聴 | 待ち伏せ攻撃 | 盗聴 | T1. 平文伝送 | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ |
| | | | パスワード盗聴 | T2. 共有パスワード | ◎ | ◎ | △(対応策あり) | △ | ◎ | ◎ |
| | | | オフラインでの暗号技術的攻撃 | T3. 辞書攻撃 | ◎ | ◎ | △ | △ | ◎ | ◎ |
| | | | | T4. 推定攻撃 | ◎ | ◎ | △ | △ | ◎ | ◎ |
| | | | | T5. NIS、解読ツールの存在 | ◎ | ◎ | △ | △ | ◎ | ◎ |
| | | トポロジー | パス外からの攻撃 | T6. トポロジーの破壊 | ◎ | ◎ | △ | ×(脆弱) | ◎ | ◎ |
| | | | | T7. 同一リンク上の判別 | ◎ | △ | △ | × | | |
| | | | ファイアウォール | T8. 常用プロトコルでの攻撃 | ◎ | △ | △ | △ | | |
| | | | | T9. 内部の脅威 | △ | △ | | | | |
| | | 不適切な用法 | ウィルス | T10. 情報の不正コピー | | | | | | |
| | 侵入 | 積極的な攻撃 | 中間者 | T11. セッション乗取り | ◎ | ◎ | △ | △ | ◎ | ◎ |
| | | | | T12. ARP 詐称(IP アドレス詐称) | ◎ | ◎ | △ | △ | ◎ | ◎ |
| | | 否認防止 | T13. アクセスの証明 | | △ | | | | | |
| | 改ざん | 積極的な攻撃 | メッセージ挿入 | T14. TCP SYN パケット挿入 | ◎ | ◎ | ◎ | × | ◎ | ◎ |
| | | | | T15. TLS RST 偽装 | ◎ | ◎ | ◎ | × | ◎ | ◎ |
| | | | メッセージ削除 | T16. シーケンス番号推測攻撃 | ◎ | ◎ | ◎ | × | ◎ | ◎ |
| | | | メッセージ変更 | T17. MAC チェック未使用 | ◎ | ◎ | △ | × | ◎ | ◎ |
| | | | | T18. ホスト to ホスト SA | ◎ | ◎ | △ | × | ◎ | ◎ |
| | | 不適切な用法 | ウィルス | T19. ウィルス混入後の転送 | | | | | | |
| | | | | T20. 情報の破壊・書換え | | | | | | |
| | 妨害 | 積極的な攻撃 | リプレイ攻撃 | T21. メッセージ盗聴後再送 | △ | ◎ | △ | × | ◎ | ◎ |
| | | | | T22. 自動発呼による再送 | ◎ | ◎ | ◎ | ◎ | ◎ | △ |
| | | 妨害攻撃 | Blind 妨害 | T23. TCPSYN フラッド攻撃 | △ | △ | △ | △ | ◎ | ◎ |
| | | | 分散型妨害 | T24. DDoS | △ | △ | △ | △ | ◎ | ◎ |
| 伝送量 | | | | | ◎(大) | × | ◎ | ◎ | ×(小) | × |
| 拡張性 | 複数サービスの相乗り(保守回線の統合) | | | | ◎(最良) | △ | △ | ○ | ×(不可) | × |
| | 電話・FAX の相乗り | | | | ◎ | △ | △ | ○ | × | × |
| | インターネット接続 | | | | ◎ | △ | △ | ○ | × | × |
| コスト | センタ・システム | | | | ◎(最安価) | × | ○ | ○ | ×(高価) | × |
| | クライアント | | | | ○ | △ | ○ | ○ | × | ◎ |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

5.ch セキュリティに関わる NW 機器のセキュリティ要件

5.1 法人間の接続における留意点(PP)

同一法人間と異なる法人間とでは、責任の主体が異なる。複数の拠点を VPN 接続する際の留意点について整理する。

| 項目 | 接続する3拠点が同一の法人である場合 | 接続する3拠点が異なる法人である場合 |
|---|---|---|
| VPN 接続状況 | 拠点1と拠点2は VPN 接続可<br>拠点2と拠点3は VPN 接続可<br>拠点3と拠点1は VPN 接続不可 | 拠点1と拠点2が VPN 接続<br>拠点2と拠点3が VPN 接続<br>拠点3と拠点1は VPN 接続不可 |
| 留意点 | 拠点2が拠点1と拠点3を中継する場合、社内のポリシーによっては許可できる。その際の責任の主体は法人 A の管理者にある。 | 拠点2は拠点1と拠点3を中継してはならない。拠点1と拠点3は VPN 接続の合意をしていないので、不正なアクセスとなる。その際の責任の主体は法人 B にある。<br>また、拠点1と拠点3が VPN 接続の合意がなされている場合でも、拠点2は中継を行ってはならない。 |
| イメージ |  |  |

オンラインレセプト・メール・AP ダウンロード、タイムスタンプ等の標準的なアプリケーションの脆弱性、危険度などを考慮すると、一般的な VPN 接続を適用する場合、以下の 4 つの要件が必要になる。これらを整理し、適正なモデル確立への条件を検証する。

(1) VPN 接続、non-VPN 接続の経路分離
(2) 異なる VPN 間の経路制御
(3) VPN 間の不正中継禁止
(4) ゾーンの分離

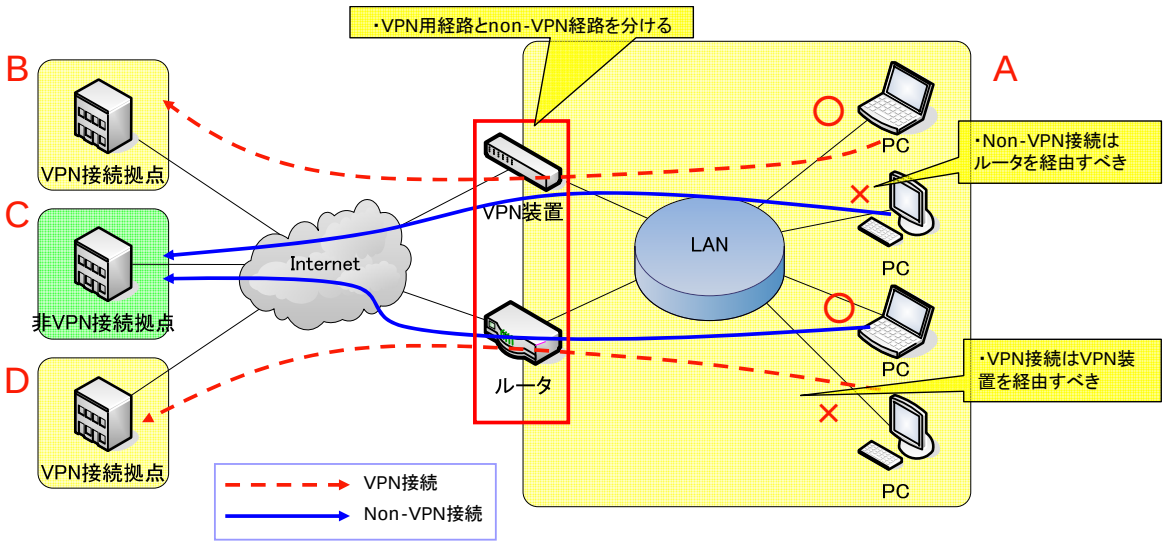
5.2 セキュリティ対策の基本方針(ST)

異なる法人間で VPN 接続を行う際に考慮すべき事項としてガイドラインを示す。

(1) VPN 接続、non-VPN 接続の経路分離

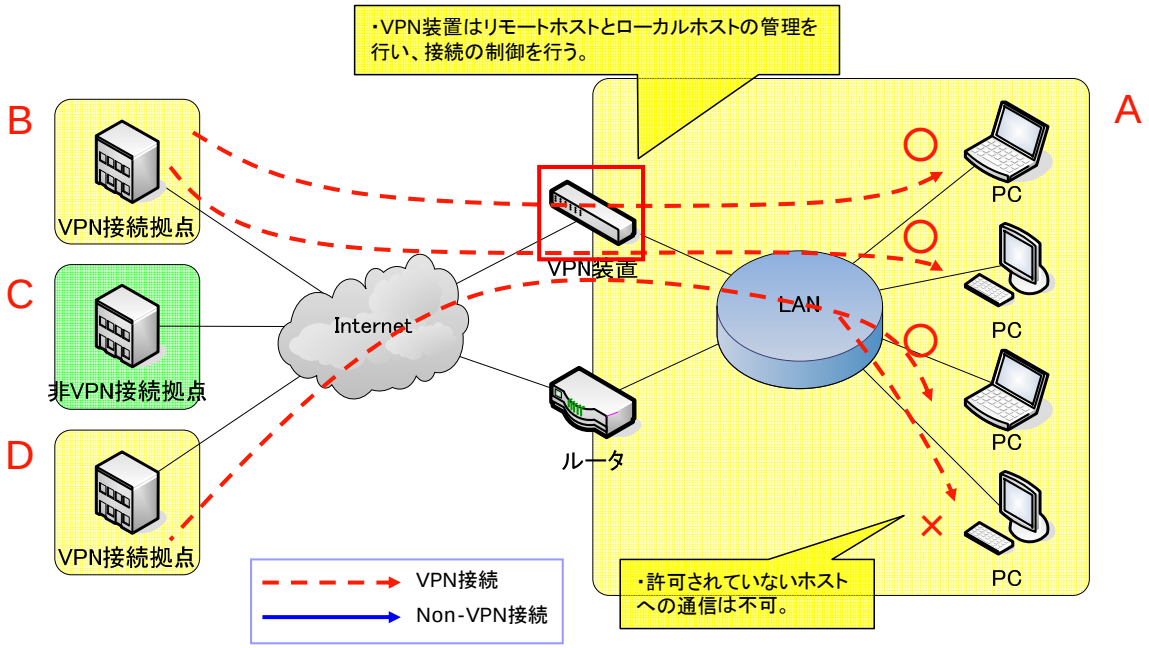
インターネット接続点において、VPN 接続と non-VPN 接続とで経路を物理的に分離する。通信ルートを分けることで外部からの不正なアクセスを防止し、VPN 接続のセキュアな経路を確保する。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




(2) 異なる VPN 間の経路制御

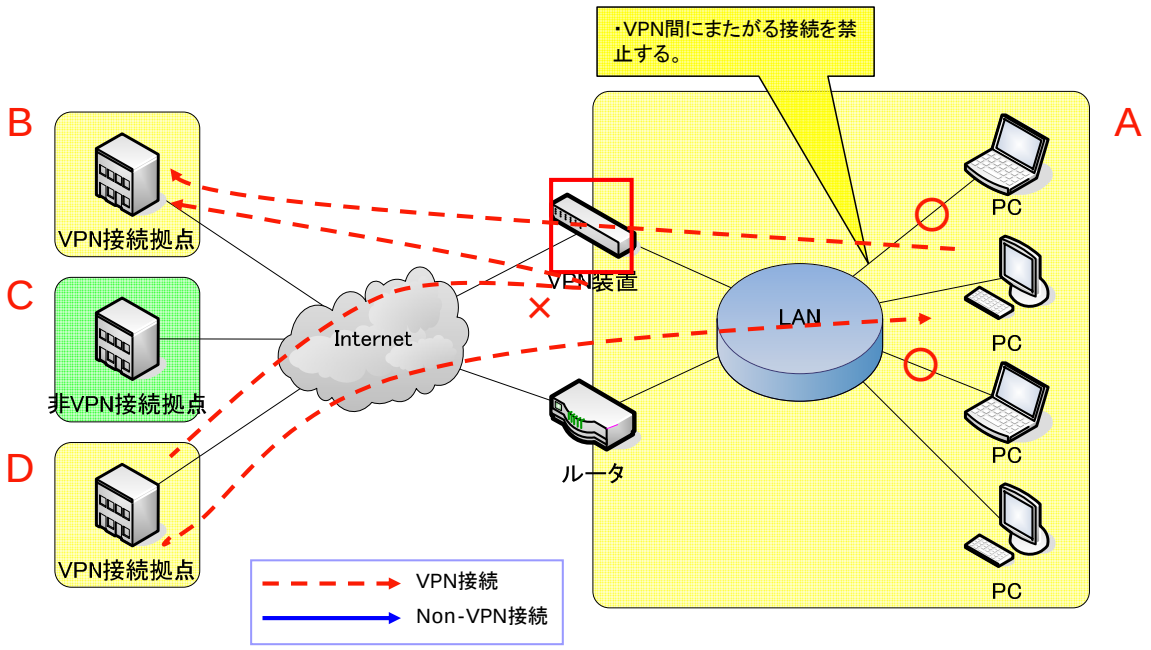
VPN 装置においてリモート拠点ホストからの接続を、ローカル拠点のホストまたは IP アドレスレベルで制御し、VPN 接続に対して制限を設ける。ピア・ツー・ピアで VPN 接続制御を実現する。




(3) VPN 間の不正中継禁止

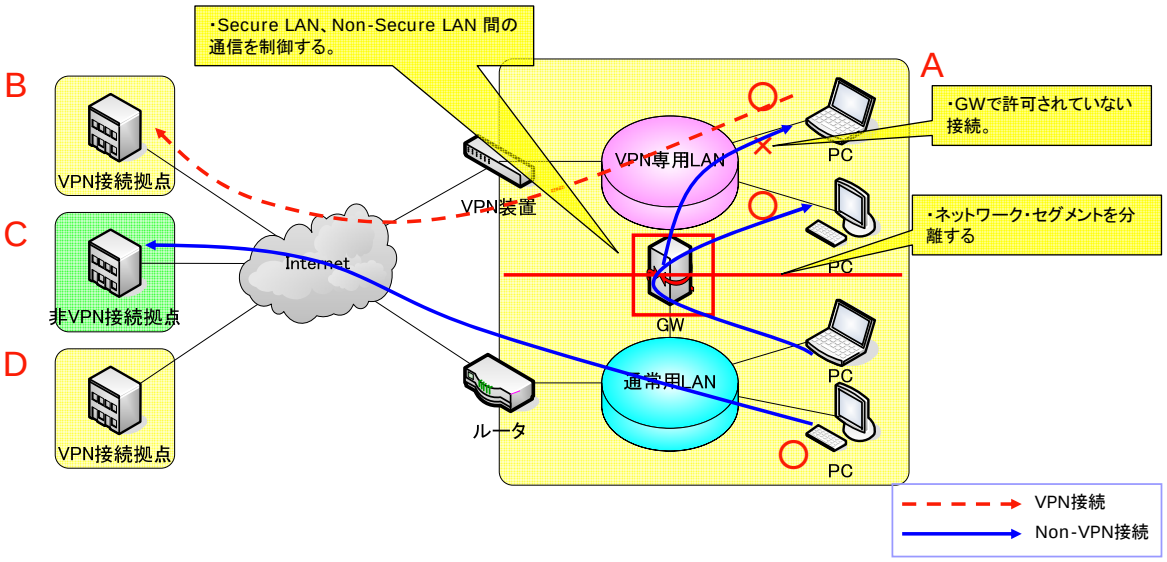
許可されていない VPN 接続(B,D 間)をある拠点(A)を経由しての接続は不可。不正な中継アクセスを禁止する。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




(4) ゾーンの分離

他拠点へアクセスする際は VPN 接続専用ゾーンと通常接続用ゾーンを設け、不適切なホストからの VPN 接続を防止する。また VPN 接続専用ゾーンと通常接続用ゾーンの間の通信を制御・制限することで、VPN 接続を行う PC のセキュリティを高める。




5.3 具体的なセキュリティ対策

5.3.1 通信モデルの定義

(1) 機器の配置とゾーンの定義

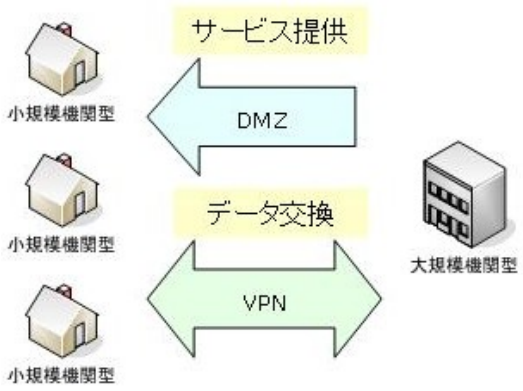
ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してカテゴライズされる必要がある。カテゴライズされたホストは同等のポリシーを実装するゾーンに配置し、ゾーンの一貫したポリシーで運営されるべきである。

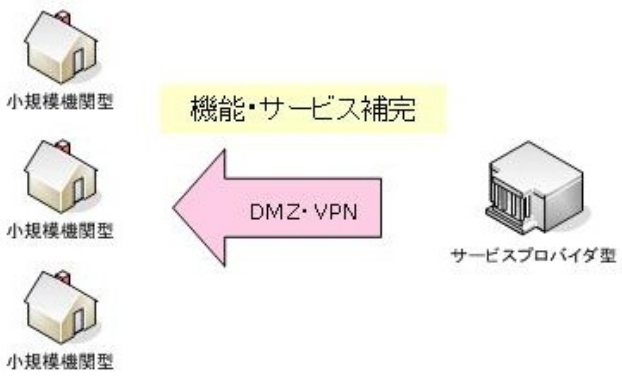
All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 項目 | High Secure Zone | DMZ | Secure Zone |
|---|---|---|---|
| 配置するホスト | 電子カルテ・レセプトなどの守るべき資産を格納・蓄積するホストを配置する。他のゾーンからの接続を制限し、情報連携などで外部へ接続する際は VPN でデータを安全に送受信する。 | 外部へサービスを提供・情報を公開するホストを配置する。ウィルスチェックゲートウェイ・プロキシサーバ・パケットチェックなどを実施し、外部からの脅威に備える。DMZ からの接続は不許可。 | 業務用クライアントを配置する。インターネット上の情報の閲覧を行う。他のゾーンからの接続を制限し、情報連携などで外部へ接続する際は VPN でデータを安全に送受信する。 |
| 格納データ・<br>展開するサービスの例 | 電子カルテサーバ<br>レセプトサーバ<br>バックアップサーバ<br>リモート保守端末 | メールサーバ<br>外部プロキシサーバ<br>地域連携サーバ<br>プロキシサーバ<br>ASP サービス 等 | 業務用クライアント 等<br>内部プロキシサーバ<br>医療機器 |

(2) プレイヤー別の通信モデル

拠点規模、性能、連携を考慮して、次の3つのモデルパターンを提案する。



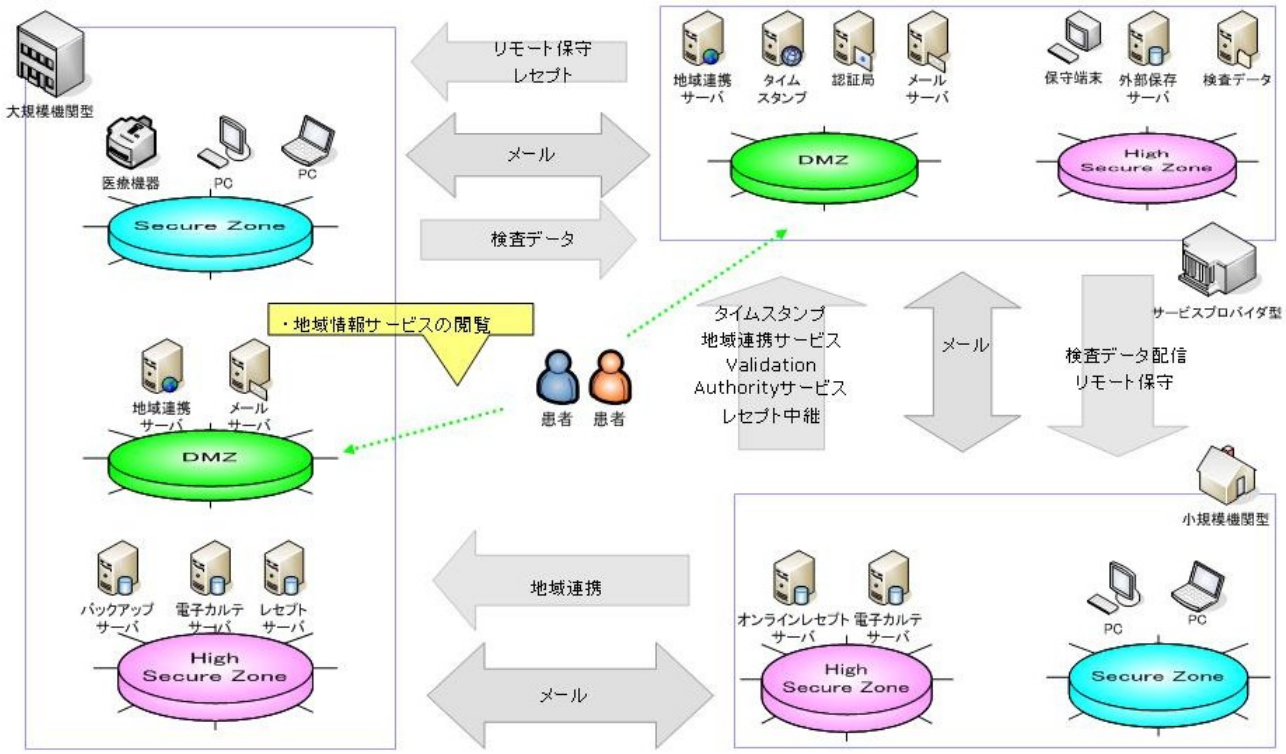

| モデル | ターゲット | ゾーン構成 | 主な役割・運用 |
|---|---|---|---|
| 大規模機関型 | サービスを展開する拠点。病院・自治体・医療機器・情報関連ベンダなど。 | High Secure Zone, Secure Zone, DMZ を配置する。 | 地域連携情報やメールサービスを提供。VPN で他の拠点と接続し、電子カルテ情報の交換・レセプト計算サービスを行う。 |
| 小規模機関型 | サービスを利用する拠点。医院・薬局など。 | High Secure Zone, Secure Zone を配置する。 | 地域連携情報などを利用。<br>VPN で他の拠点と接続し、電子カルテ情報の交換・レセプト計算サービスを利用する。 |
| サービスプロバイダ型 | 小規模機関では展開が困難な機能・サービスを提供し補完する拠点。 | High Secure Zone, DMZ を配置する。 | 小規模機関が実装困難な DMZ 機能を提供することで、大規模機関相当のサービスを展開可能にする。 |

5.3.2 モデル間のサービスイメージ

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

これらの通信モデルをリモートサービスの提供・利用の視点で役割を明確にする。さらに、リモートサービスの利用側と提供側の視点で前節の通信モデルが受けもつ役割を規定にする。この役割に沿って、各機関の具備すべきセキュリティ要件や機能要素を明らかにする。モデル別のゾーン配置と、拠点間の主なサービスイメージを示す。

| サービス項目 | 利用者 | | 提供者 | |
|---|---|---|---|---|
| | 小規模医療機関 | 大規模医療機関 | 大規模医療機関 | サービスプロバイダ |
| (医療機関・福祉介護等医療関連サービス業務向け)地域連携サービス | | | | |
| (患者向け)診療情報・介護情報提供サービス | | | | |
| (一般向け)医療・介護情報提供サービス | | | | |
| (業務限定)インターネット接続サービス | | | | |
| メールサービス | | | | |
| オンラインレセプトサービス | | | | |
| ASP サービス | | | | |
| 検査データ配信サービス | | | | |
| 外部保存(バックアップ) サービス | | | | |
| リモート保守サービス | | | | |
| タイムスタンプサービス | | | | |
| Validation Authority(VA)サービス | | | | |




5.3.3 各通信モデルのセキュリティ要件

(1) 大規模機関型モデルのセキュリティ要件

(a) 詳細モデル

各ネットワーク機器・ホストに実装すべき機能とゾーン間・サービスの経路を示す。主にアクセスコントロール・

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

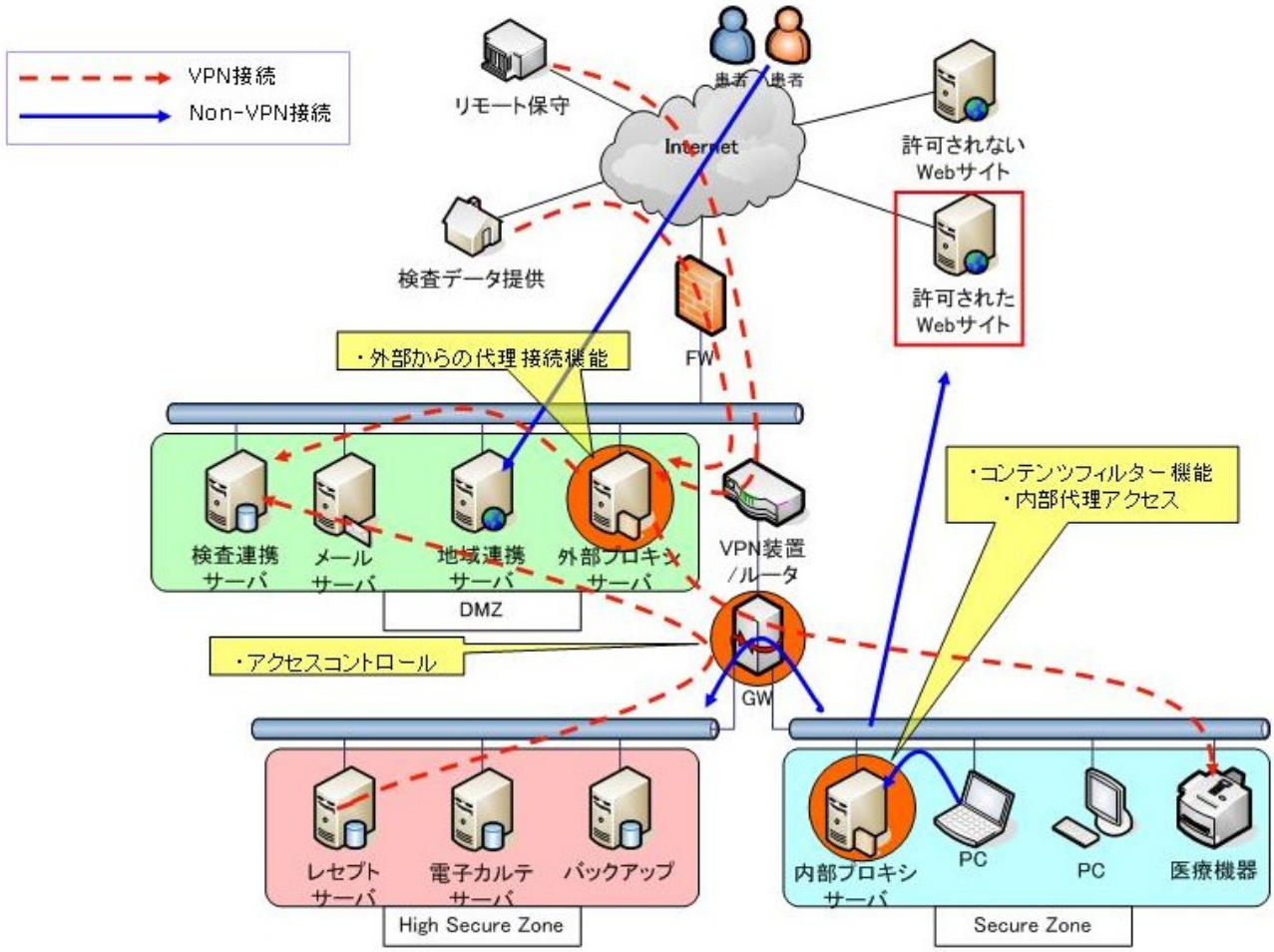
ウィルスチェック・プロキシ等を実装する。VPN 装置は合意されている他拠点と暗号化通信を行い、WAN におけるセキュリティを保つ。

| 区分 | 場所 | 概要 | 説明 |
|---|---|---|---|
| ファイアウォール機能 | アクセスポイント | 外部からのアクセスをブロックする。DMZ へのアクセスを許可する。 | 外部から High Secure Zone, Secure Zone への接続は禁止。IDS 検知機能を装備する。 |
| VPN 機能 | ファイアウォール配下 | VPN の接続先・接続元を制御する。暗号化。 | リモートアクセスの、通信路を暗号化する。合意のある拠点のみ通信を許可する。外部プロキシ機能を中継させる。 |
| 外部プロキシ機能 | DMZ | 外部からのアクセスに対する代理接続処理を行う。他のゾーンへの代理通信を行う。 | High Secure Zone, High Secure Zone へのアクセス制御、フィルターをおこなう。メールのウィルスチェックを行う。 |
| ゲートウェイ機能 | ゾーン接続点 | High Secure Zone, Secure Zone, DMZ の通信を制御する。レイヤ 4 以上で処理可能であることが望ましい。 | アクセスコントロール、ウィルスチェック、スクリーニング等を行う。 |
| 内部プロキシ機能 | Secure Zone,<br>High Secure Zone | 全ての内部ホストから外部への通信の代理をする。外部 WWW サービスへの代理をする。 | アクセスログを記録して、通信の履歴を残す。コンテンツフィルタなどで Web アクセスを制限する。ウィルスチェック等のスクリーニング機能を具備する。セキュリティパッチなどの更新・管理機能を有するとよい。 |

| 経路 | 説明 | サービス・事例 |
|---|---|---|
| 拠点内の<br>ゾーン間通信 | ゲートウェイ機能で IP レベル・アプリケーションレベルでの通信制御を行う。High Secure Zone へは内部プロキシ機能による代理通信を行い、直接的な接続を避ける。 | 拠点内のデータ移行・更新 |
| 他拠点からの<br>DMZ への接続 | ファイアウォール機能で IP アドレス・ポートレベルでの制御を行う。<br>公開するサイトの閲覧拠点を限定する。 | 地域連携などの情報提供。 |
| 他拠点への<br>VPN 接続 | ゲートウェイで接続元のホストを限定する。VPN 装置を経由して他拠点へアクセスする。 | 検査データの交換。ASP サービスの利用。 |
| 他拠点から<br>VPN 接続 | ファイアウォール機能で VPN 接続元チェックを行う。外部プロキシ機能による代理通信で直接接続をさせない。ゲートウェイでウィルスチェック・経路の制御を行う。 | リモート保守、検査データの提供。 |
| インターネット接続 | ゲートウェイで Secure Zone からの接続のみを許可する。内部プロキシのコンテンツフィルタ機能で接続サイトを限定する。 | 地域連携などの情報提供サービスの閲覧。 |

(b) NW 設計例

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




(2) 小規模機関型モデルのセキュリティ要件

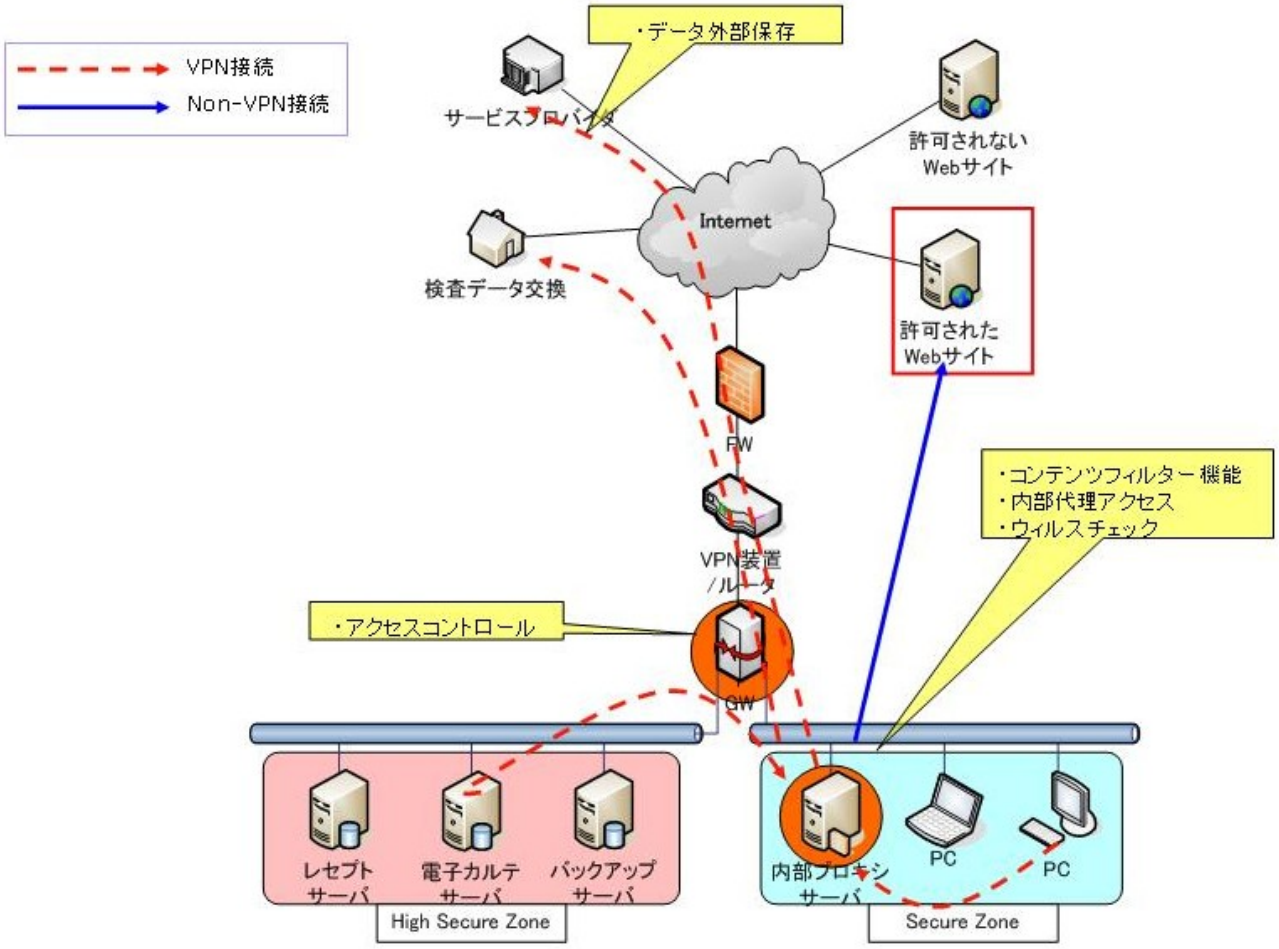
(a) 詳細モデル

| 区分 | 場所 | 概要 | 説明 |
|---|---|---|---|
| ファイアウォール機能 | アクセスポイント | 外部からのアクセスをブロックする。DMZ へのアクセスを許可する。 | 外部から High Secure Zone, Secure Zone への接続は禁止。IDS 検知機能を装備する。 |
| VPN 機能 | ファイアウォール配下 | VPN の接続先・接続元を制御する。 | リモートアクセスの、通信路を暗号化する。合意のある拠点のみ通信を許可する。外部プロキシ機能を中継させる。 |
| ゲートウェイ機能 | ゾーン接続点 | High Secure Zone, Secure Zone, DMZ の通信を制御する。レイヤ 4 以上で処理可能であることが望ましい。 | アクセスコントロール、ウィルスチェック、等を行う。 |
| 内部プロキシ機能 | Secure Zone,<br>High Secure Zone | 全ての内部ホストから外部への通信の代理をする。外部 WWW サービスへの代理をする。 | アクセスログを記録して、通信の履歴を残す。コンテンツフィルタなどで Web アクセスを制限するスクリーニング機能を具備する。ウィルスチェック等を行う。セキュリティパッチなどの更新・管理機能を有するとよい。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 経路 | 説明 | サービス・事例 |
|---|---|---|
| 拠点内の<br>ゾーン間通信 | ゲートウェイ機能で IP レベル・アプリケーションレベルでの通信制御を行う。High Secure Zone へは内部プロキシ機能による代理通信を行い、直接的な接続を避ける。 | 拠点内のデータ移行・更新 |
| 他拠点への<br>VPN 接続 | ゲートウェイで接続元のホストを限定する。VPN 装置を経由して他拠点へアクセスする。 | 検査データの交換。ASP サービスの利用。データの外部保存。 |
| 他拠点から<br>VPN 接続 | ファイアウォール機能で VPN 接続元チェックを行う。外部プロキシ機能による代理通信で直接接続をさせない。ゲートウェイでウィルスチェック・経路の制御を行う。 | 検査データ配信の利用。 |
| インターネット接続 | ゲートウェイで Secure Zone からの接続のみを許可する。内部プロキシのコンテンツフィルタ機能で接続サイトを限定する。 | 地域連携などの情報提供サービスの閲覧。タイムスタンプ・VA サービスの利用。 |

(b) NW 設計例




(3) サービスプロバイダ型モデルのセキュリティ要件

(a) 詳細モデル

| 区分 | 場所 | 概要 | 説明 |
|---|---|---|---|

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

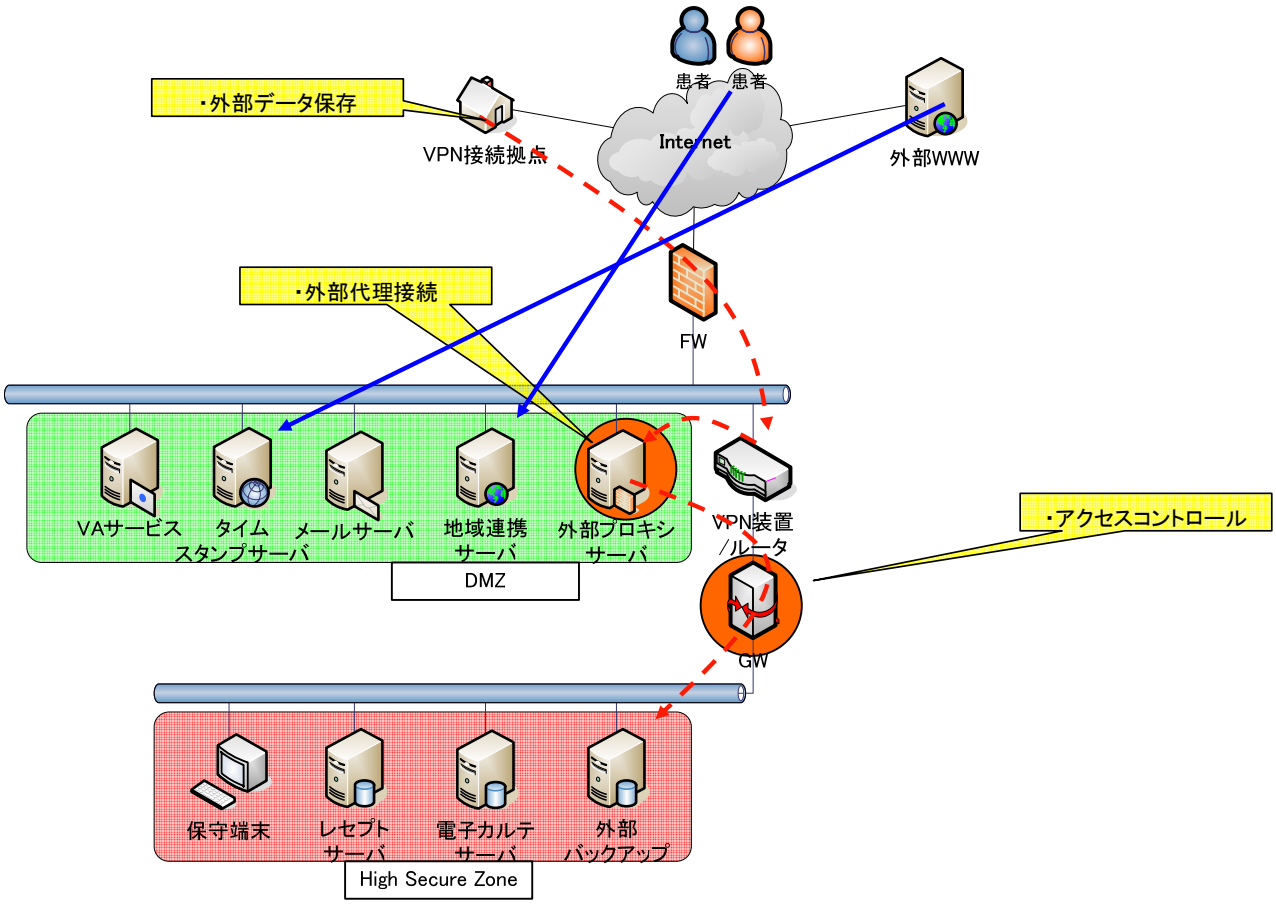
| | | | |
|---|---|---|---|
| ファイアウォール機能 | アクセスポイント | 外部からのアクセスをブロックする。DMZ へのアクセスを許可する。 | 外部から High Secure Zone, Secure Zone への接続は禁止。IDS 検知機能を装備する。 |
| VPN 機能 | ファイアウォール配下 | VPN の接続先・接続元を制御する。 | リモートアクセスの、通信路を暗号化する。合意のある拠点のみ通信を許可する。外部プロキシ機能を中継させる。 |
| 外部プロキシ機能 | DMZ | 外部からのアクセスに対する接続処理を行う。他のゾーンへの代理通信を行う。 | High Secure Zone, High Secure Zone へのアクセス制御、フィルターをおこなう。セキュリティパッチなどの更新機能を有するとよい。メールのウィルスチェックを行う。 |
| ゲートウェイ機能 | ゾーン接続点 | High Secure Zone, Secure Zone, DMZ の通信を制御する。レイヤ 4 以上で処理可能であることが望ましい。 | アクセスコントロール、ウィルスチェック、スクリーニング等を行う。 |

| 経路 | 説明 | サービス・事例 |
|---|---|---|
| 拠点内のゾーン間通信 | ゲートウェイ機能で IP レベル・アプリケーションレベルでの通信制御を行う。High Secure Zone へは内部プロキシ機能による代理通信を行い、直接的な接続を避ける。 | 拠点内のデータ移行・更新 |
| 他拠点からの DMZ への接続 | ファイアウォール機能で IP アドレス・ポートレベルでの制御を行う。<br>公開するサイトの閲覧拠点を限定する。 | 地域連携などの情報提供。タイムスタンプ、VA サービスの提供。パッチの提供。 |
| 他拠点への VPN 接続 | ゲートウェイで接続元のホストを限定する。VPN 装置を経由して他拠点へアクセスする。 | リモート保守、検査データの提供。 |
| 他拠点から VPN 接続 | ファイアウォール機能で VPN 接続元チェックを行う。外部プロキシ機能による代理通信で直接接続をさせない。ゲートウェイでウィルスチェック・経路の制御を行う。 | 検査データの交換。ASP サービスの提供。データの外部保存サービス。 |

(b) NW 設計例

サービスプロバイダは、プロバイダ自身の社内 NW とサービス提供する NW は切り離す。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007




6.構築時の確認事項

6.1 チェックシート

以上の議論を踏まえると、セキュリティ要件をまとめたものが各機関毎のゾーン・ホスト配置・各機器に対するチェックシートになる。ゾーン・ホスト配置・各機器に対するチェックシートを以下に示す。

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

(1) 大規模機関型　チェックシート

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| 1. 通信形態 | | | | |
| 1-1<br>接続相手の確認 | 1-1-1<br>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「大規模機関型　チェックシート」の項目を満たしていますか？ | | | 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。<br>本資料「2.2 セキュリティに関するガイドライン」 |
| | 1-1-2<br>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」の項目を満たしていますか？ | - | | |
| | 1-1-3<br>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」の項目を満たしていますか？ | - | | |
| 2. 通信ポリシー | | | | |
| 2-1<br>中継の確認 | 2-1-1<br>アクセス回線または中継回線に共用型ネットワークが使用されていますか？ | WAN 機能 | | はい：<br>共有型ネットワークを経由している場合、事業者が検知できないデータの盗聴、改ざんなどのハッキング手法が知られており、セキュリティに関する脆弱性があるため、オープンネットワークとして扱いユーザ側で通信に関するセキュリティを担保する必要がある。<br>本資料「4.1 WAN の定義」<br>いいえ：オープンネットワークを使用しない。専用線・ISDN などを利用する。<br>本チェックシート「2-3 接続処理の確認」に進む。 |
| 2-2<br>オープンネットワークの利用した拠点間の接続 | 2-2-1<br>同一法人以外の複数拠点と接続する場合，不正な中継を禁止していますか？ | VPN 機能 | | オープンネットワークを利用した拠点間の接続をした場合、同時に複数の拠点と接続が可能になる。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。<br>本資料「5.1 法人間の接続における留意点」 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 2-2-2<br>IKE でユーザ認証を行っていますか？ | VPN 機能 | | オープンネットワークにおける脅威（盗聴・侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。<br>本資料「4.2 脅威への対処技術」 |
| | 2-2-3<br>IKE の認証は公開鍵または自動鍵配送機能を持った共通鍵方式ですか？ | VPN 機能 | | |
| | 2-2-4<br>セッション毎に共通鍵を自動決定していますか？ | VPN 機能 | | |
| | 2-2-5<br>IPSec による暗号化を行っていますか？ | VPN 機能 | | |
| | 2-2-6<br>IPSec でメッセージ認証を行っていますか？ | VPN 機能 | | |
| 2-3<br>他拠点との接続処理 | 2-3-1<br>接続先拠点と通信に関して合意がなされていますか？ | - | | 接続先拠点を文書・口頭などで合意を行い、サービス内容・運用形態等を確認し不正利用を防ぐ |
| | 2-3-2<br>他拠点への接続先をアドレス・ポート等で制限していますか？ | VPN 機能<br>／プロキシ機能 | | 接続先拠点と通信に関して合意がなされている接続先 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を防ぐ。他拠点で提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 2-3-3<br>他拠点からの接続元をアドレス・ポート等で制限していますか？ | VPN 機能<br>／プロキシ機能 | | 接続先拠点と通信に関して合意がなされている接続元 IP アドレスのみ接続を許可し、合意のなされていない他拠点から自拠点への不正なアクセスを防ぐ。自拠点で提供するサービスポートのみを許可し、サービス不正利用・侵入等を防ぐ。 |
| | 2-3-4<br>ロギングによりアクセス監視（接続先・接続元）を行っていますか？ | VPN 機能<br>／プロキシ機能 | | ログは、発信元・アクセスポイント・アクセスされた場所の 3 箇所で取る必要がある。本項目は発信元・アクセスポイントのロギングになる。<br>本資料「2.2 (3)SPC 要件」 |
| 3. 拠点内のセキュリティ | | | | |
| 3-1<br>ホストの配置 役割 | 3-1-1<br>電子カルテ検査データ等の重要なデータを処理蓄積 | High Secure Zone | | 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適切なゾーンに配置をする。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | する機能は High Secure Zone に配置していますか？ | | | 本資料「5.3.1 通信モデルの定義」 |
| | 3-1-2<br>業務用端末インターネット接続用端末は Secure Zone に配置していますか？ | Secure Zone | | |
| | 3-1-3<br>情報公開外部サービス等の機能は DMZ に配置していますか？ | DMZ | | |
| 3-2<br>外部からの脅威 | 3-2-1<br>外部から High Secure Zone, Secure Zone への接続を禁止していますか？ | ファイアウォール | | 起点が外部から、High Secure Zone, Secure Zone への接続を禁止して、改ざんや侵入に対して資産を守る。 |
| | 3-2-2<br>外部からの攻撃（Dos 的攻撃・不正形式パケットなど）を検知できますか？ | ファイアウォール | | DMZ で公開しているサービスに対して、攻撃があった場合、それらのパケットを検知・遮断することで改ざんや侵入などから資産を守る。 |
| | 3-2-3<br>他拠点との接続合意がなされている通信のみを許可していますか？ | ファイアウォール | | 他拠点と接続の合意がとれている通信のみを許可して、不正なアクセスを禁止する。 |
| 3-3<br>High Secure Zone のセキュリティ | 3-3-1<br>接続の起点を High Secure Zone とした Secure Zone DMZ への直接アクセスを禁止していますか？ | ゲートウェイ機能 | | High Secure Zone に格納されている電子カルテ・レセプトなどの重要データの漏洩を防ぐ。 |
| | 3-3-2<br>インターネット接続を禁止していますか？ | プロキシ機能 | | 重要データが格納されているゾーンからの、インターネット接続を防ぐ。 |
| | 3-3-3<br>各ホストでウィルスチェックを行っていますか？ | 各ホスト | | 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。 |
| 3-4<br>Secure Zone のセキュリティ | 3-4-1<br>DMZ、High Secure Zone からの直接アクセスを禁止していますか？ | ゲートウェイ機能 | | DMZ の公開サーバが外部からの不正アクセスにより侵入された場合、被害拡散を防止する。<br>High Secure Zone からの重要データの内部情報漏えい防ぐ。 |
| | 3-4-2<br>インターネットへの HTTP 接続のサイト制限をしていますか？ | プロキシ機能 | | 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・情報漏えいを防ぐ。 |
| | 3-4-3 | プロキシ機能 | | 格納したデータにウィルスが混在されていた場合の、発 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 各ホストでウィルスチェックを行っていますか？ | | | 病・拡散を防ぐ。 |
| 3-5<br>DMZ の<br>セキュリティ | 3-5-1<br>High Secure Zone, Secure Zone への直接アクセスを禁止していますか？ | ゲートウェイ機能 | | DMZ の公開サーバが外部からの不正アクセスにより侵入された場合、High Secure Zone, Secure Zone への被害拡散を防止する。 |
| | 3-5-2<br>各ホストでウィルスチェックを行っていますか？ | 各ホスト | | 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。 |
| 3-6<br>High Secure Zone と<br>Secure Zone 間の通信 | 3-6-1<br>接続の起点を Secure Zone から行い、プロキシ機能を経由していますか？ | プロキシ機能 | | High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。 |
| | 3-6-2<br>プロキシ機能でロギングを行い、アクセスを監視していますか？ | プロキシ機能 | | 「いつ」「だれが」「どこに」接続したかをロギングすることで、不正アクセスが生じた場合の監査を可能にする。 |
| | 3-6-3<br>Secure Zone からの接続をアドレス・ポートで制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 患者データなど重要データのアップデート・閲覧の際、ホストとサービスを制限することで情報漏えいを防ぐ。 |
| 3-7<br>High Secure Zone と<br>DMZ 間の通信 | 3-7-1<br>接続の起点を DMZ から行い、プロキシ機能を経由していますか？ | プロキシ機能 | | High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。 |
| | 3-7-2<br>プロキシ機能でロギングを行い、アクセスを監視していますか？ | プロキシ機能 | | 「いつ」「だれが」「どこに」接続したかをロギングすることで、不正アクセスが生じた場合の監査を可能にする。 |
| | 3-7-3<br>DMZ からの接続をアドレス・ポートで制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 患者向け診断情報提供サービスなどで、High Secure Zone の情報の一部を閲覧・取得する場合、ホストとサービスを制限することで情報漏えい・改ざん等を防ぐ。 |
| 3-8<br>DMZ と Secure Zone<br>間の通信 | 3-8-1<br>接続の起点を Secure Zone から行い、プロキシ機能を経由していますか？ | プロキシ機能 | | DMZ への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。 |
| | 3-8-2<br>プロキシ機能でロギングを行い、アクセスを監視していますか？ | プロキシ機能 | | 「いつ」「だれが」「どこに」接続したかをロギングすることで、不正アクセスが生じた場合の監査を可能にする。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 3-8-3<br>Secure Zone からの接続をアドレス・ポートで制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | DMZ の公開サーバなどの情報をアップデートする際、ホストとサービスを制限することで、情報漏えい・改ざん等を防ぐ。 |
| 3-9<br>内部セキュリティ<br>サービス | 3-9-1<br>セキュリティパッチなどの更新機能を拠点内に装備していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 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を対策を行う。 |
| 4. サービス運用例 | | | | |
| 4-1<br>情報提供<br>サービスの展開 | 4-1-1<br>医療機関向けに情報（診療記録、検査データ、診療サマリ、健診データ等）を公開・提供する場合、接続先・接続元の制限を行っていますか？ | プロキシ機能<br>各サーバ | | 接続先拠点と通信に関して合意がなされている接続先・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。提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 4-1-2<br>医療機関向けに情報を公開・提供する場合、通信路を暗号化していますか？ | VPN 機能 | | オープンネットワークにおける脅威（盗聴・侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。<br>本資料「4.2 脅威への対処技術」 |
| | 4-1-3<br>医療機関向けに情報を公開・提供する場合、ロギングを行いアクセス監視を行っていますか？ | プロキシ機能 | | ログは、発信元・アクセスポイント・アクセスされた場所の 3 箇所で取る必要がある。本項目は発信元・アクセスされた場所のロギングになる。<br>本資料「2.2 (3)SPC 要件」 |
| | 4-1-4<br>患者向けに情報を公開・提供する場合、ユーザ認証を行っていますか？ | プロキシ機能<br>各サーバ | | 不正なユーザによるデータの閲覧を防ぐ。 |
| | 4-1-5<br>情報サービスにおいて High Secure Zone の情報を提供する際、プロキシ機能を使用して外部ユーザから遮蔽していますか？ | プロキシ機能<br>各サーバ | | 外部からの High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。 |
| 4-2<br>情報提供<br>サービス（医療機関向 | 4-2-1<br>医療機関向けの情報（診療記録、検査データ、診療サマリ、健診データ等）の提供サービスを利用する場合、 | プロキシ機能<br>各サーバ | | 接続先拠点と通信に関して合意がなされている接続先・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 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| け）の利用 | アクセスするホストを限定していますか？ | | | ぐ。提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 4-2-2<br>医療機関向けの情報（診療記録、検査データ、診療サマリ、健診データ等）の提供サービスを利用する場合、取得したデータは High Secure Zone に格納していますか？ | ゲートウェイ機能 | | 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適切なゾーンに配置をする。<br>本資料「5.3.1 通信モデルの定義」 |
| 4-3<br>外部保存<br>サービスの利用 | 4-3-1<br>外部保存サービスプロバイダが起点の接続を禁止していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 自拠点からのアップロードのみの接続を行うため、サービスプロバイダからの接続は禁止し不正アクセスを防ぐ。 |
| | 4-3-2<br>外部保存を利用するホストは High Secure Zone から接続していますか？ | ゾーン | | 業務端末などが配置されている Secure Zone からの外部保存サービスプロバイダへの不正なアクセスを防ぐ。 |
| 4-4<br>メールサービス | 4-4-1<br>メールのスクリーニングを行っていますか？ | メール機能 | | スパムメール・ウィルス添付メール等から内部を守る。 |
| | 4-4-2<br>不正なメール転送を禁止していますか？ | メール機能 | | メール転送の踏み台になることを防ぐ。 |
| 4-5<br>リモート保守<br>サービスの利用 | 4-5-1<br>外部からの医療機器への接続をリモート保守サービスのみに制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | リモート保守を行うサービスプロバイダによる、不正アクセスを防ぐ。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

(2) 小規模機関型　チェックシート

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| 1. 通信形態 | | | | |
| 1-1<br>接続相手の確認 | 1-1-1<br>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「大規模機関型　チェックシート」の項目を満たしていますか？ | - | | 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。<br>本資料「2.2 セキュリティに関するガイドライン」 |
| | 1-1-2<br>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」の項目を満たしていますか？ | - | | |
| | 1-1-3<br>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」の項目を満たしていますか？ | - | | |
| 2. 通信ポリシー | | | | |
| 2-1<br>中継の確認 | 2-1-1<br>アクセス回線または中継回線に共用型ネットワークが使用されていますか？ | WAN 機能 | | はい：<br>共有型ネットワークを経由している場合、事業者が検知できないデータの盗聴、改ざんなどのハッキング手法が知られており、セキュリティに関する脆弱性があるため、オープンネットワークとして扱いユーザ側で通信に関するセキュリティを担保する必要がある。本資料「4.1 WAN の定義」<br>いいえ：オープンネットワークを使用しない。専用線・ISDN などを利用する。<br>本チェックシート「2-3 接続処理の確認」に進む。 |
| 2-2<br>オープンネットワークの利用した拠点間の接続 | 2-2-1<br>同一法人以外の複数拠点と接続する場合，不正な中継を禁止していますか？ | VPN 機能 | | オープンネットワークを利用した拠点間の接続をした場合、同時に複数の拠点と接続が可能になる。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。<br>本資料「5.1 法人間の接続における留意点」 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 2-2-2<br>IKE でユーザ認証を行っていますか？ | VPN 機能 | | オープンネットワークにおける脅威（盗聴・侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。<br>本資料「4.2 脅威への対処技術」 |
| | 2-2-3<br>IKE の認証は公開鍵または自動鍵配送機能を持った共通鍵方式ですか？ | VPN 機能 | | |
| | 2-2-4<br>セッション毎に共通鍵を自動決定していますか？ | VPN 機能 | | |
| | 2-2-5<br>IPSec による暗号化を行っていますか？ | VPN 機能 | | |
| | 2-2-6<br>IPSec でメッセージ認証を行っていますか？ | VPN 機能 | | |
| 2-3<br>他拠点との接続処理 | 2-3-1<br>接続先拠点と通信に関して合意がなされていますか？ | - | | 接続先拠点を文書・口頭などで合意を行い、サービス内容・運用形態等を確認し不正利用を防ぐ |
| | 2-3-2<br>他拠点への接続先をアドレス・ポート等で制限していますか？ | VPN 機能<br>／プロキシ機能 | | 接続先拠点と通信に関して合意がなされている接続先 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を防ぐ。他拠点で提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 2-3-3<br>他拠点からの接続元をアドレス・ポート等で制限していますか？ | VPN 機能<br>／プロキシ機能 | | 接続先拠点と通信に関して合意がなされている接続元 IP アドレスのみ接続を許可し、合意のなされていない他拠点から自拠点への不正なアクセスを防ぐ。自拠点で提供するサービスポートのみを許可し、サービス不正利用・侵入等を防ぐ。 |
| | 2-3-4<br>ロギングによりアクセス監視（接続先・接続元）を行っていますか？ | VPN 機能<br>／プロキシ機能 | | ログは、発信元・アクセスポイント・アクセスされた場所の 3 箇所で取る必要がある。本項目は発信元・アクセスポイントのロギングになる。<br>本資料「2.2 (3)SPC 要件」 |
| 3. 拠点内のセキュリティ | | | | |
| 3-1<br>ホストの配置 役割 | 3-1-1<br>電子カルテ検査データ等の重要なデータを処理蓄積 | High Secure Zone | | 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適切なゾーンに配置をする。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | する機能は High Secure Zone に配置していますか？ | | | 本資料「5.3.1 通信モデルの定義」 |
| | 3-1-2<br>業務用端末インターネット接続用端末は Secure Zone に配置していますか？ | Secure Zone | | |
| 3-2<br>外部からの脅威 | 3-2-1<br>外部から High Secure Zone, Secure Zone への接続を禁止していますか？ | ファイアウォール | | 起点が外部から、High Secure Zone, Secure Zone への接続を禁止して、改ざんや侵入に対して資産を守る。 |
| | 3-2-2<br>他拠点との接続合意がなされている通信のみを許可していますか？ | ファイアウォール | | 他拠点と接続の合意がとれている通信のみを許可して、不正なアクセスを禁止する。 |
| 3-3<br>High Secure Zone のセキュリティ | 3-3-1<br>接続の起点を High Secure Zone とした Secure Zone への直接アクセスを禁止していますか？ | ゲートウェイ機能 | | High Secure Zone に格納されている電子カルテ・レセプトなどの重要データの漏洩を防ぐ。 |
| | 3-3-2<br>インターネット接続を禁止していますか？ | プロキシ機能 | | 重要データが格納されているゾーンからの、インターネット接続を防ぐ。 |
| | 3-3-3<br>各ホストでウィルスチェックを行っていますか？ | 各ホスト | | 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。 |
| 3-4<br>Secure Zone のセキュリティ | 3-4-1<br>インターネットへの HTTP 接続のサイト制限をしていますか？ | プロキシ機能 | | 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・情報漏えいを防ぐ。 |
| | 3-4-2<br>各ホストでウィルスチェックを行っていますか？ | プロキシ機能 | | 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。 |
| 3-5<br>High Secure Zone と Secure Zone 間の通信 | 3-5-1<br>接続の起点を Secure Zone から行い、プロキシ機能を経由していますか？ | プロキシ機能 | | High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。 |
| | 3-5-2<br>プロキシ機能でロギングを行い、アクセスを監視していますか？ | プロキシ機能 | | 「いつ」「だれが」「どこに」接続したかをロギングすることで、不正アクセスが生じた場合の監査を可能にする。 |
| | 3-5-3<br>Secure Zone からの接続をアドレス・ポートで制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 患者データなど重要データのアップデート・閲覧の際、ホストとサービスを制限することで情報漏えいを防ぐ。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| 3-6<br>内部セキュリティ<br>サービス | 3-6-1<br>セキュリティパッチなどの更新機能を拠点内に装備していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 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を対策を行う。 |
| 4. サービス運用例 | | | | |
| 4-1<br>情報提供<br>サービス（医療機関向け）の利用 | 4-1-1<br>医療機関向けの情報（診療記録、検査データ、診療サマリ、健診データ等）の提供サービスを利用する場合、アクセスするホストを限定していますか？ | プロキシ機能<br>各サーバ | | 接続先拠点と通信に関して合意がなされている接続先・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。提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 4-1-2<br>医療機関向けの情報（診療記録、検査データ、診療サマリ、健診データ等）の提供サービスを利用する場合、取得したデータは High Secure Zone に格納していますか？ | ゲートウェイ機能 | | 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適切なゾーンに配置をする。<br>本資料「5.3.1 通信モデルの定義」 |
| 4-2<br>外部保存<br>サービスの利用 | 4-2-1<br>外部保存サービスプロバイダが起点の接続を禁止していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 自拠点からのアップロードのみの接続を行うため、サービスプロバイダからの接続は禁止し不正アクセスを防ぐ。 |
| | 4-2-2<br>外部保存を利用するホストは High Secure Zone から接続していますか？ | ゾーン | | 業務端末などが配置されている Secure Zone からの外部保存サービスプロバイダへの不正なアクセスを防ぐ。 |
| 4-3<br>リモート保守<br>サービスの利用 | 4-3-1<br>外部からの医療機器への接続をリモート保守サービスのみに制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | リモート保守を行うサービスプロバイダによる、不正アクセスを防ぐ。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

(3) サービスプロバイダ　チェックシート

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| 1. 通信形態 | | | | |
| 1-1<br>接続相手の確認 | 1-1-1<br>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「大規模機関型　チェックシート」の項目を満たしていますか？ | - | | 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。<br>本資料「2.2 セキュリティに関するガイドライン」 |
| | 1-1-2<br>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」の項目を満たしていますか？ | - | | |
| 2. 通信ポリシー | | | | |
| 2-1<br>オープンネットワークの利用した拠点間の接続 | 2-1-1<br>不正な中継を禁止していますか？ | VPN 機能 | | オープンネットワークを利用した拠点間の接続をした場合、同時に複数の拠点と接続が可能になる。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。<br>本資料「5.1 法人間の接続における留意点」 |
| | 2-1-2<br>IKE でユーザ認証を行っていますか？ | VPN 機能 | | オープンネットワークにおける脅威（盗聴・侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。<br>本資料「4.2 脅威への対処技術」 |
| | 2-1-3<br>IKE の認証は公開鍵または自動鍵配送機能を持った共通鍵方式ですか？ | VPN 機能 | | |
| | 2-1-4<br>セッション毎に共通鍵を自動決定していますか？ | VPN 機能 | | |
| | 2-1-5<br>IPSec による暗号化を行っていますか？ | VPN 機能 | | |
| | 2-1-6<br>IPSec でメッセージ認証を行っていますか？ | VPN 機能 | | |
| 2-2<br>他拠点との接続処理 | 2-2-1<br>接続先拠点と通信に関して合意がなされていますか？ | - | | サービス提供拠点を文書・口頭などで合意を行い、サービス内容・運用形態等を確認し不正利用を防ぐ |
| | 2-2-2 | VPN 機能 | | サービス提供拠点と通信に関して合意がなされている接 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 他拠点への接続先をアドレス・ポート等で制限していますか？ | ／プロキシ機能 | | 続先 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を防ぐ。他拠点で提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 2-2-3<br>他拠点からの接続元をアドレス・ポート等で制限していますか？ | VPN 機能<br>／プロキシ機能 | | 接続先拠点と通信に関して合意がなされている接続元 IP アドレスのみ接続を許可し、合意のなされていない他拠点から自拠点への不正なアクセスを防ぐ。自拠点で提供するサービスポートのみを許可し、サービス不正利用・侵入等を防ぐ。 |
| | 2-2-4<br>ロギングによりアクセス監視（接続先・接続元）を行っていますか？ | VPN 機能<br>／プロキシ機能 | | ログは、発信元・アクセスポイント・アクセスされた場所の 3 箇所で取る必要がある。本項目は発信元・アクセスポイントのロギングになる。<br>本資料「2.2 (3)SPC 要件」 |
| 3. 拠点内のセキュリティ | | | | |
| 3-1<br>ホストの配置 役割 | 3-1-1<br>電子カルテ検査データ等の重要なデータを処理蓄積する機能は High Secure Zone に配置していますか？ | High Secure Zone | | 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適切なゾーンに配置をする。<br>本資料「5.3.1 通信モデルの定義」 |
| | 3-1-2<br>情報公開外部サービス等の機能は DMZ に配置していますか？ | DMZ | | |
| | 3-1-3<br>サービスプロバイダは、プロバイダ自身の社内ネットワークとサービスを提供するネットワークを切り離していますか？ | - | | サービス用ネットワークと自社ネットワークが連携することは想定されないので、物理的に切り離すことで不正アクセスを防止する。 |
| 3-2<br>外部からの脅威 | 3-2-1<br>外部から High Secure Zone への接続を禁止していますか？ | ファイアウォール | | 起点が外部から、High Secure Zone への接続を禁止して、改ざんや侵入に対して資産を守る。 |
| | 3-2-2<br>外部からの攻撃（Dos 的攻撃・不正形式パケットなど）を検知できますか？ | ファイアウォール | | DMZ で公開しているサービスに対して、攻撃があった場合、それらのパケットを検知・遮断することで改ざんや侵入などから資産を守る。 |
| | 3-2-3 | ファイアウォール | | 他拠点と接続の合意がとれている通信のみを許可して、 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 他拠点との接続合意がなされている通信のみを許可していますか？ | | | 不正なアクセスを禁止する。 |
| 3-3<br>High Secure Zone のセキュリティ | 3-3-1<br>接続の起点を High Secure Zone とした DMZ への直接アクセスを禁止していますか？ | ゲートウェイ機能 | | High Secure Zone に格納されている電子カルテ・レセプトなどの重要データの漏洩を防ぐ。 |
| | 3-3-2<br>インターネット接続を禁止していますか？ | プロキシ機能 | | 重要データが格納されているゾーンからの、インターネット接続を防ぐ。 |
| | 3-3-3<br>各ホストでウィルスチェックを行っていますか？ | 各ホスト | | 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。 |
| 3-4<br>DMZ のセキュリティ | 3-4-1<br>High Secure Zone への直接アクセスを禁止していますか？ | ゲートウェイ機能 | | DMZ の公開サーバが外部からの不正アクセスにより侵入された場合、High Secure Zone への被害拡散を防止する。 |
| | 3-4-2<br>各ホストでウィルスチェックを行っていますか？ | 各ホスト | | 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。 |
| 3-5<br>High Secure Zone と DMZ 間の通信 | 3-5-1<br>接続の起点を DMZ から行い、プロキシ機能を経由していますか？ | プロキシ機能 | | High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。 |
| | 3-5-2<br>プロキシ機能でロギングを行い、アクセスを監視していますか？ | プロキシ機能 | | 「いつ」「だれが」「どこに」接続したかをロギングすることで、不正アクセスが生じた場合の監査を可能にする。 |
| | 3-5-3<br>DMZ からの接続をアドレス・ポートで制限していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 患者向け診断情報提供サービスなどで、High Secure Zone の情報の一部を閲覧・取得する場合、ホストとサービスを制限することで情報漏えい・改ざん等を防ぐ。 |
| 3-6<br>内部セキュリティサービス | 3-6-1<br>セキュリティパッチなどの更新機能を拠点内に装備していますか？ | ゲートウェイ機能<br>プロキシ機能 | | 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を対策を行う。 |
| 4. サービス運用例 | | | | |
| 4-1<br>情報提供サービスの展開 | 4-1-1<br>医療機関向けに情報（診療記録、検査データ、診療サマリ、健診データ等）を公開・提供する場合、接続先・接 | プロキシ機能<br>各サーバ | | 接続先拠点と通信に関して合意がなされている接続先・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 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 続元の制限を行っていますか？ | | | ぐ。提供しているサービスポートのみを許可し、サービス不正利用・侵入を防ぐ。 |
| | 4-1-2<br>医療機関向けに情報を公開・提供する場合、通信路を暗号化していますか？ | VPN 機能 | | オープンネットワークにおける脅威（盗聴・侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。<br>本資料「4.2 脅威への対処技術」 |
| | 4-1-3<br>医療機関向けに情報を公開・提供する場合、ロギングを行いアクセス監視を行っていますか？ | プロキシ機能 | | ログは、発信元・アクセスポイント・アクセスされた場所の3 箇所で取る必要がある。本項目は発信元・アクセスされた場所のロギングになる。<br>本資料「2.2 (3)SPC 要件」 |
| | 4-1-4<br>患者向けに情報を公開・提供する場合、ユーザ認証を行っていますか？ | プロキシ機能<br>各サーバ | | 不正なユーザによるデータの閲覧を防ぐ。 |
| | 4-1-5<br>情報サービスにおいて High Secure Zone の情報を提供する際、プロキシ機能を使用して外部ユーザから遮蔽していますか？ | プロキシ機能<br>各サーバ | | 外部からの High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。 |
| 4-2<br>インターネット接続サービス | 4-2-1<br>業務・サービス上必要なサイトのみ接続の許可をしているか？ | プロキシ機能 | | 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・情報漏えいを防ぐ。 |
| | 4-2-2<br>インターネット接続サービスを提供するユーザの認証をしていますか？ | プロキシ機能 | | サービスを提供しているユーザを認証することで、不正なユーザによる侵入・情報漏えいなどを防ぐ。 |
| 4-3<br>外部保存サービス | 4-3-1<br>外部保存サービスを提供するユーザの認証をしていますか？ | プロキシ機能<br>各サーバ | | サービスを提供しているユーザを認証することで、不正なユーザによる侵入・情報漏えいなどを防ぐ。 |
| | 4-3-2<br>データの格納時の DMZ から High Secure Zone への通信はプロキシ機能経由で行い、外部・ユーザから遮蔽されていますか？ | プロキシ機能 | | 外部からの High Secure Zone への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。 |

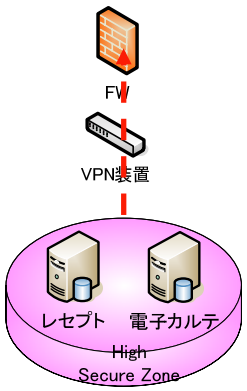
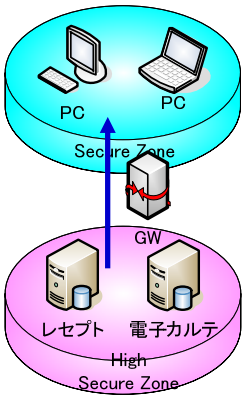
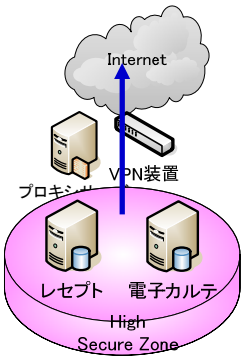
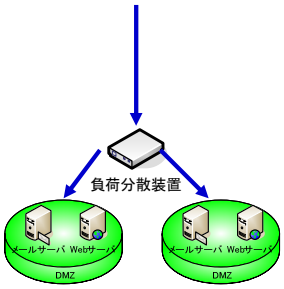
All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

| 目的対象 | 項　　目 | 機能要素 | チェック | 備　　考 |
|---|---|---|---|---|
| | 4-3-3<br>ユーザのデータは High Secure Zone に格納しているか？ | バックアップ機能 | | 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適切なゾーンに配置をする。<br>本資料「5.3.1 通信モデルの定義」 |
| 4-4<br>メールサービス | 4-4-1<br>メールのスクリーニングを行っていますか？ | メール機能 | | スパムメール・ウィルス添付メール等から内部を守る。 |
| | 4-4-2<br>不正なメール転送を禁止していますか？ | メール機能 | | メール転送の踏み台になることを防ぐ。 |
| 4-5<br>リモート保守<br>サービス | 4-5-1<br>リモート保守端末を High Secure Zone に配置し、作業者の認証を行っていますか？ | ゲートウェイ機能<br>プロキシ機能 | | 医療機器へアクセスの際は専門の技術者が接続し、不正なユーザによるアクセスを防止する。 |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007

6.2 付帯要件等

ネットワーク構築の際のユーザ要件と既存 NW との整合方法を整理し、それらの対処内容と運用例について示す。

| 項目 | ファイアウォール | 既存 NW 連携 | インターネット接続 | 可用性 |
|---|---|---|---|---|
| 要件 | VPN 機器の上位にルータが存在する場合、必要なプロトコルの通信許可設定を行わなければならない。 | 既存ネットワーク構成の変更を最小限にし、Secure Zone のホストから Non-Secure Zone 内のホストとの連携をしたい。 | High Secure Zone のホストに対して、Windows Update やウイルスパターンの更新のため、インターネットへの通信をしたい。 | DMZ において、サーバ・ネットワーク機器の冗長化・負荷分散を行いたい。 |
| 対処例・課題 | 一般的な IPSec プロトコルを使用するため変更ルールは容易だが、大規模機関の場合は変更の申請が困難な場合がある。 | 好ましくないが、一部に限りゲートウェイなどで通信を制御しアクセスを許可するホストを限定すべき。 | High Secure Zone からのダイレクトな接続は好ましくない。DMZ を経由しプロキシサーバなどを利用したチェック機構が必須。 | ゲートウェイを複数設置または負荷分散装置を使用することで実現。 |
| イメージ |  |  |  |  |

All Rights Reserved Copyright © 保健福祉医療情報セキュアネットワーク普及促進コンソーシアム 2007