オンデマンド VPN（HEASNET 版）

技術仕様書

基本編

Ver1.0

2007 年 2 月 15 日

HEASNET

改版履歴

版数	作成日	作成	記事・備考

目　次

1. 概要 1
1.1 定義 1
1.2 目的 1
1.3 実現機能 1
1.4 構成情報 1
2. サービスポリシー 3
2.1 HEASNET内利用アドレス 3
2.2 ルーティング管理 4
2.3 VPN 5
2.4 証明書の管理 7
2.5 HSの接続許諾管理 10
3. 運用 12
3.1 HNPの運用 12
3.2 HSの運用 12
4. APPENDIX 13
4.1 利用技術 13

1. 概要

1.1 定義

保健・医療・福祉の各分野において、セキュアなネットワーク基盤を効率よく実現することを狙いとし、これを運用するオンデマンド VPN（HEASNET 版）の接続サービスの機能を定義する。

1.2 目的

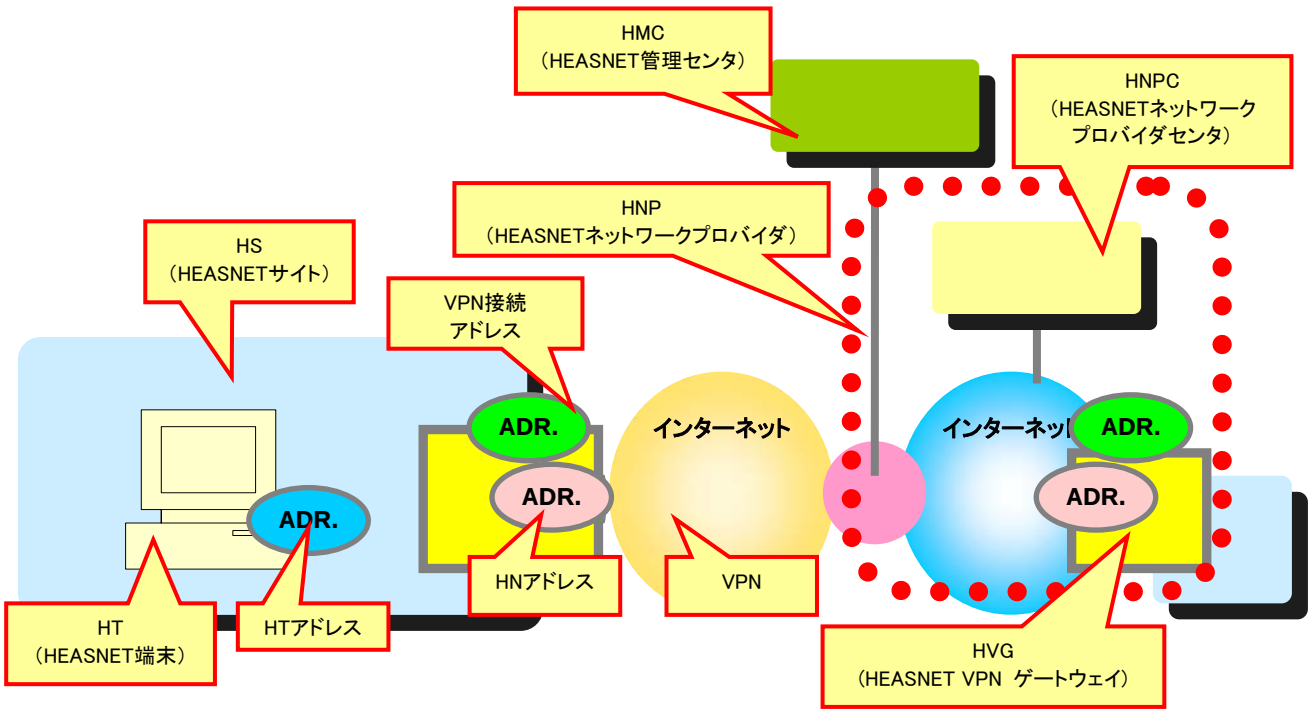
- 医療分野における情報流通の円滑化
- 高セキュリティ、かつ安価で運用性の高いネットワークの提供

1.3 実現機能

HEASNET を提供する事業者（以下、HNP：HEASNET Network Provider）は、HEASNET に参加するサイト（HS：HEASNET Sight）に対し、以下の機能を提供する。

① HS-A から HS-B に対して、インターネット上で VPN（仮想通信網）を設定する機能
② HS が他の HS に対して、許可した VPN の接続先を選択できる機能
③ HS に属す端末（以下、HT：HEASNET Terminal）の通信を、他の HS の中の許可された HT 同士のみ通信可能なよう制限する機能

1.4 構成情報



■ HNP(HEASNET ネットワークプロバイダ)
:HEASNET 仕様の VPN サービスを提供するプロバイダ
■ HNPC(HEASNET ネットワークプロバイダセンタ)
:HNP を運用するセンタ機能
■ HMC(HEASNET 管理センタ)
:HEASNET 内で中立的に必要な機能を提供するセンタおよび HEASNET の各機関を登録/認定するセンタ
■ HS(HEASNET サイト)
:HNP に参加する拠点
■ HT(HEASNET 端末)
:HEASNET を利用する端末
■ HVG(HEASNET VPN ゲートウェイ)
:HNP と直接接続され、HNP 上で外部と通信を中継する通信機器
■ HT アドレス
:HT が直接内部で通信するアドレス
■ HN アドレス
:HNP 内での通信に利用されるエクストラネット用のアドレス(VPN 内部アドレス)
■ VPN 接続アドレス
:VPN の構成に必要なインターネットアドレス

2. サービスポリシー

2.1 HEASNET 内利用アドレス

2.1.1 HN アドレス規定

アドレスとしては、以下のいずれかを使用することとする。

- IPv4 プライベートアドレス
- IPv4 グローバルアドレス
- IPv6 グローバルアドレス

2.1.2 HS アドレス

アドレスとしては、以下のいずれかを使用することとする。

- IPv4 プライベートアドレス
- IPv4 グローバルアドレス
- IPv6 グローバルアドレス

2.1.3 HT アドレス

アドレスとしては、以下のいずれかを使用することとする。

- IPv4 プライベートアドレス
- IPv4 グローバルアドレス
- IPv6 グローバルアドレス

2.2 ルーティング管理

2.2.1 ルーティング情報

- 事前に, HS 内で HT を一意に特定し通信可能にするための情報(例:HN アドレス, VPN 接続アドレス+HT アドレス)を, HNP に登録する必要がある。
- HNPは登録された情報元に、HSの要求に応じて通信先のルーティング情報をHVGへ設定を行う。
- 設定の方式は接続される HNP が選択してよい。

2.2.2 動的ルーティングプロトコルの利用

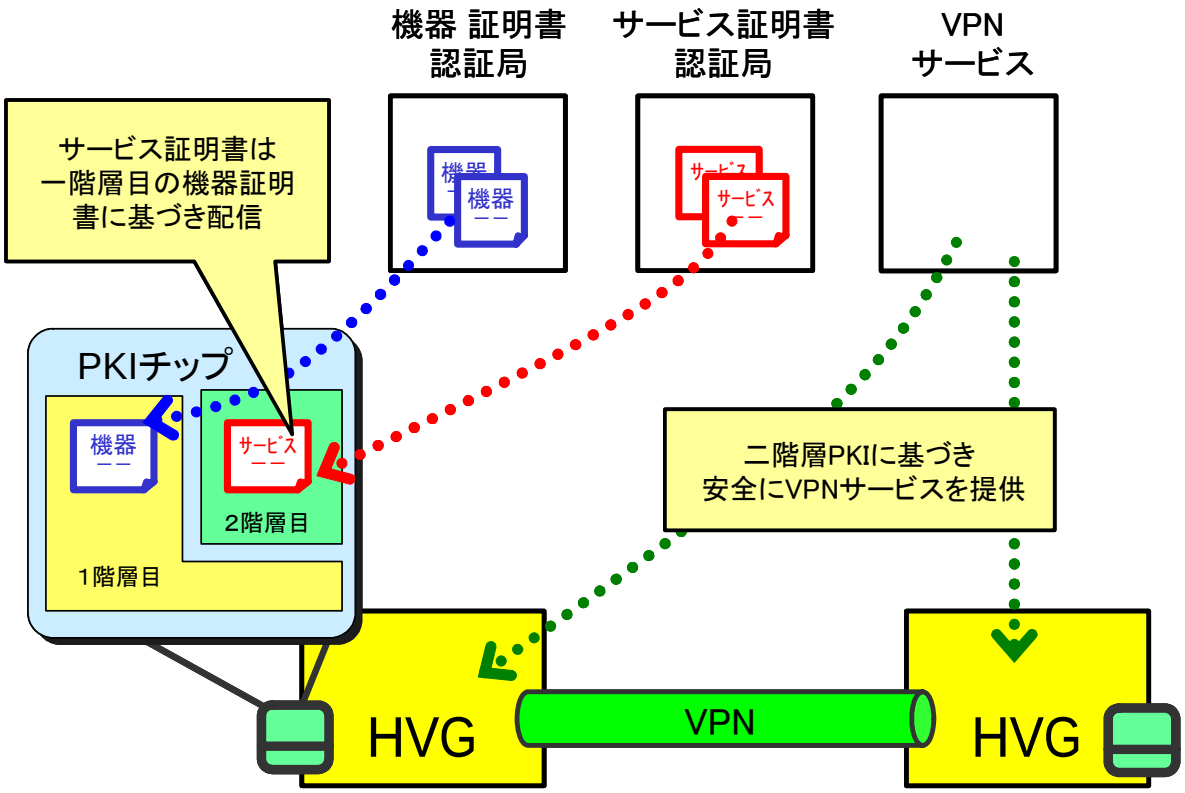
- HS 間の動的経路プロトコル(RIP, OSPF など)は、HS の責任の下に利用しても良い。

2.3 VPN

HEASNET に接続される HS がインターネットを経由して通信する際、通信の保護のため VPN を利用する。HNP は以下で規定する VPN の仕様を規定する。

2.3.1 VPN プロトコル

HS 同士の拠点間通信には、IKE による自動鍵交換と IPsec による暗号化方式を利用する。VPNを設定する際に必要なサイトでの接続情報は、二階層 PKI を用いて配布するものとする。



2.3.2 暗号化方式

暗号化方式としては、以下のいずれかの方式の利用を規定する。

(1) IKE 暗号化アルゴリズム　　:ﾄﾘﾌﾟﾙ DES、または CBC ﾓｰﾄﾞ AES-128、または CBC モード AES-256

(2) IKE ハッシュアルゴリズム　　:SHA-1

(3) IPsec 暗号化アルゴリズム　　:ﾄﾘﾌﾟﾙ DES、または CBC ﾓｰﾄﾞ AES-128、または CBC モード AES-256

(4) IPsec ハッシュアルゴリズム　　:SHA-1

(5) IKE Diffie-Hellman グループ　　:ｸﾞﾙｰﾌﾟ2（離散対数 1024 ﾋﾞｯﾄ）、またはｸﾞﾙｰﾌﾟ 14（離散対数 2048 ﾋﾞｯﾄ）

2.3.3 鍵交換における認証方式

以下のいずれかの方式の利用を規定する。

(1) デジタル署名方式

(2) 事前共有鍵方式

2.4 証明書の管理

HEASNET では VPN の管理のため電子証明書を用いた PKI 認証を行う。以下に証明書の利用について規定する。

2.4.1 証明書の種類

HEASNET では以下の二つの証明書を利用し、サービスを提供する。
① 機器証明書
HVG の機器を特定するために、一意に発行される。
② サービス証明書
HEASNET のサービス利用を特定するために、サービスに応じて発行される。

2.4.2 機器証明書

HVG に搭載する機器証明書は以下の形態で利用する。

- 機器証明書は機器証明書発行機関が発行する

2.4.3 サービス証明書

サービス証明書は以下の形態で利用する。

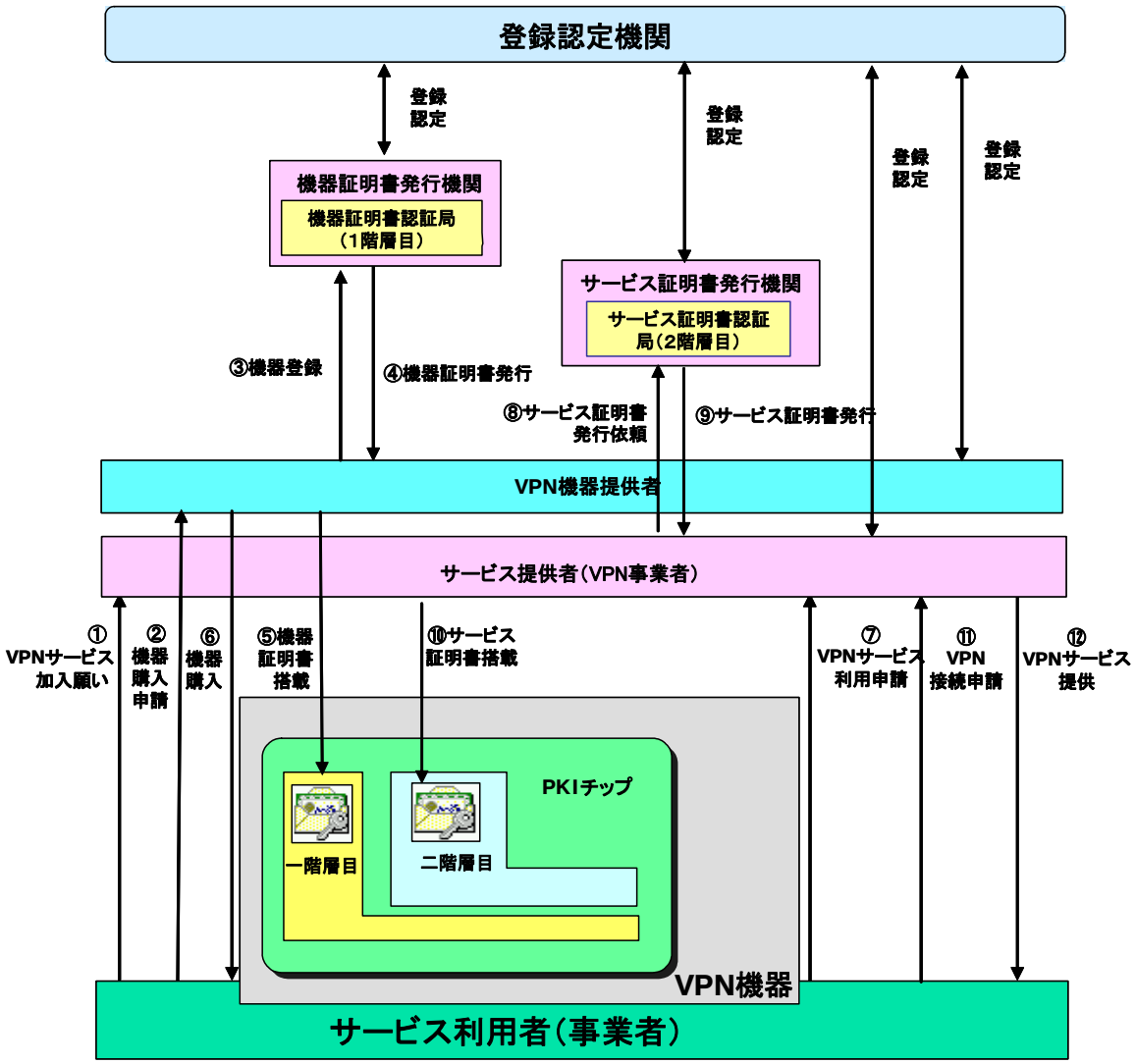
- VPN で利用するサービス証明書はサービス証明書発行機関が発行する

2.4.4 証明書の利用

HNP は以下の機能を提供しなければならない。
- HNP は HVG の特定のために、HVG に対して機器証明書を配布する
- HNP は VPN 接続の管理のため、機器証明書を基にしてサービス証明書を発行する
- VPN 接続の許可/不許可を認証するために、サービス証明書を利用し認証する

2.4.5 VPN サービスの申請手順例

申請者(サービス利用者)が VPN サービスを利用するまでの申請手順例を示す。本手順は、機能的な観点での手順であり、実際のサービスにおいては、個々の申請手順は、簡略化される。



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、HMC(HEASNET 管理センタ)の登録認定機関に、事業者、機関登録を行い、認定を受ける。

① 申請者は、サービス提供者に VPN サービスの加入申請を行う。
② 申請者は、VPN 機器提供者に VPN 機器購入申請を行う。
(VPN サービス加入申請と VPN 機器購入申請は、同時に行われる可能性はある。またサービス提供者が VPN 機器を代行提供(販売)する事はある。)
③ VPN 機器提供者は、申請者が購入予定の VPN 機器を、機器証明書発行機関に登録する。
④ 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。
⑤ 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。

⑥ 申請者は、機器証明書が搭載された VPN 機器を購入（入手）する。
⑦ 申請者は、サービス提供者に、VPN サービス利用申請をする。
⑧ サービス提供者は、申請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。
⑨ サービス証明書発行機関は、サービス提供者に、申請者用のサービス証明書を発行する。
⑩ サービス提供者は、サービス証明書を、申請者の VPN 機器の IC チップの2階層目に搭載する。
⑪ 申請者は、VPN 接続申請を、サービス提供者にする。
⑫ サービス提供者は、申請者に対して、VPN サービスを提供する。
（VPN サービスを提供する為に、接続用証明書または、事前共有鍵を配布する）

2.5　HS の接続許諾管理

HEASNET で異なる HS の間で接続が合意された場合のみ、HS 間でのVPNの接続を許可する。以下にその仕様を規定する。

2.5.1　VPN 通信の設定

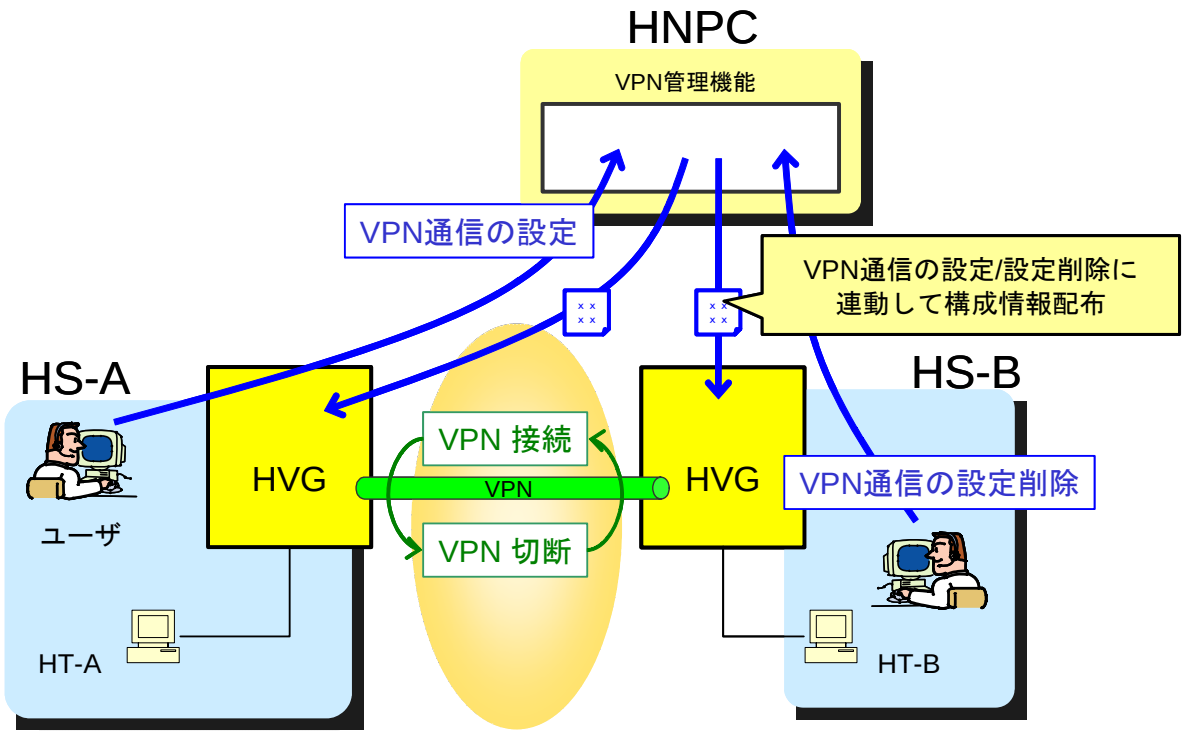
- HS-A と HS-B が互いに許可した場合、その許可情報に従い通信を HS-A－HS-B 間の通信を許可し、VPN の設定をする機能
- HT-A と HT-B、あるいは HS-A もしくは HS-B の管理者が互いに許可した場合、その許可情報に従い VPN の設定をする機能

2.5.2　VPN 通信の設定の削除

- HS-A もしくは HS-B の依頼により、通信の許可が取り消された場合、HVG-A および HVG-B の VPN の許可設定を削除する機能
- HT-A もしくは HT-B、HS-A もしくは HS-B の管理者の依頼により、通信の許可を取り消した場合、HVG-A および HVG-B の VPN の許可設定を削除する機能

2.5.3　VPN の接続/切断

- 上記 VPN 通信の設定において、VPN 可能な設定を行われた HS-A, HS-B に対し、必要に応じて HS-A－HS-B 間で VPN を接続/切断する機能



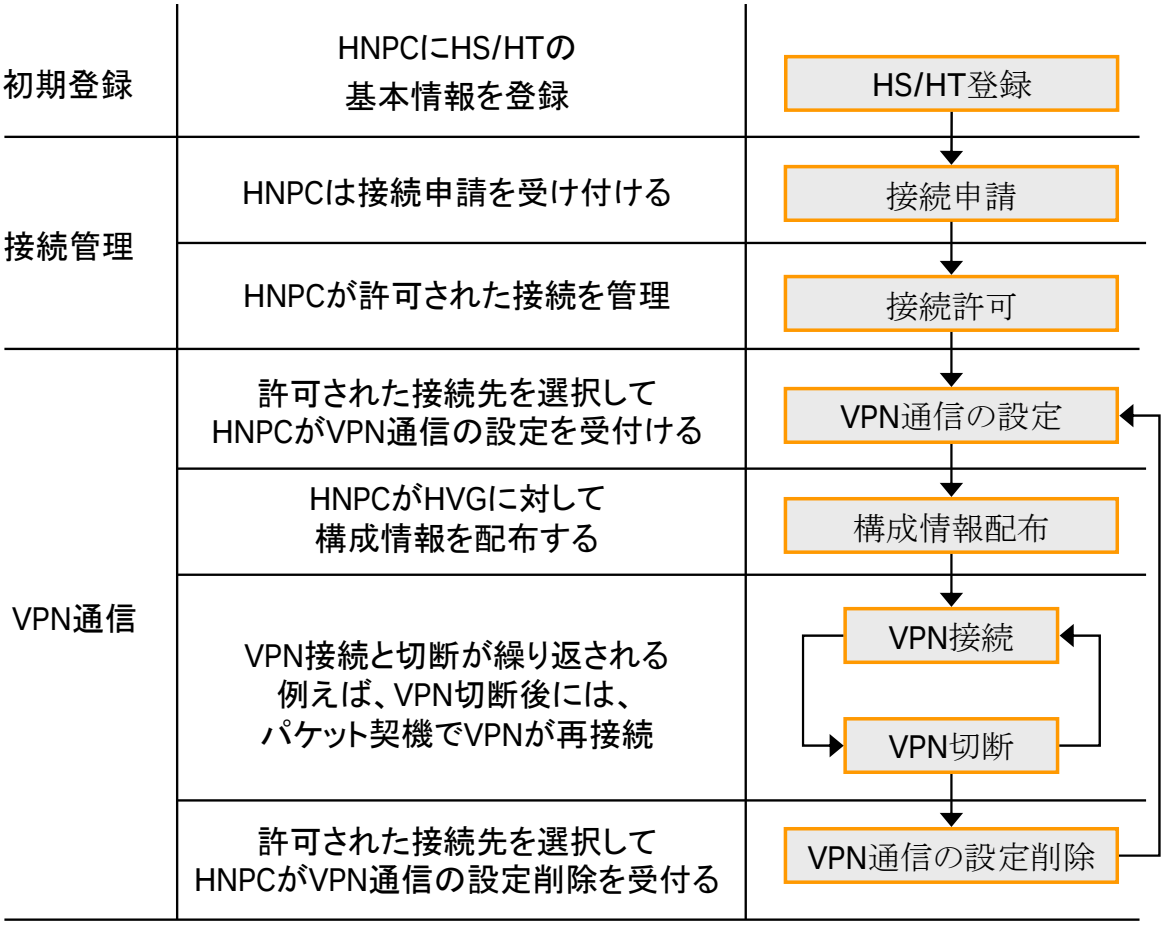
■ VPN の設定/削除

- VPN 設定/削除は、利用者からの依頼に応じて行われる
- VPN の設定された HVG は、VPN の接続/切断処理を開始する

■ VPN 接続/切断

- VPN の接続/切断の契機は、各 HNP で規定する

■ 通信確立の流れ



3. 運用

HEASNET は以下の運用に従い、ネットワークを運用する。

3.1 HNP の運用

- HNP は参加している HS の HN アドレス、HT アドレスを把握していなければならない

3.2 HS の運用

- HS は HEASNET と通信を行うすべての端末を HNP に対し登録する必要がある。
- HS は厚生労働省が規定する**「医療情報システムの安全管理に関するガイドライン」**に遵守した運用を HS 内で行うべきである。

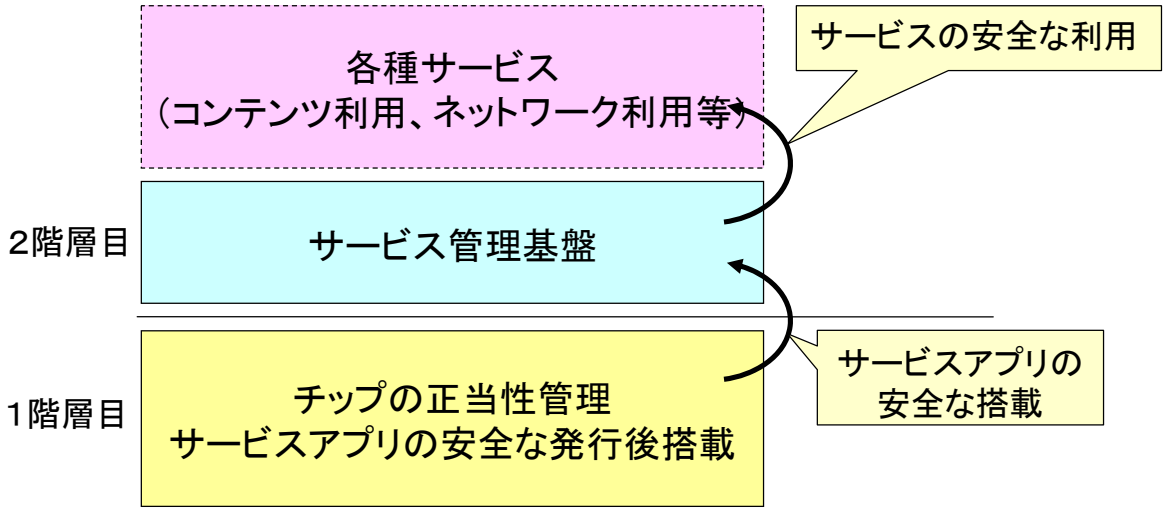
4. APPENDIX

4.1 利用技術

4.1.1 二階層 PKI

*NICSS フレームワークでは、サービスを提供するアプリケーションが、機器の認証を行なうことを想定している。そのため、チップ管理の認証とアプリケーション利用に関する認証を、独立でレベルの異なる鍵で実現する「二階層 PKI」モデルを基本的なコンセプトとしている。以下に「二階層 PKI」モデルのコンセプトを示す。これによって、多様なサービスを便利かつ安全に利用することができる。

- 一階層目: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
- 二階層目:サービス認証
  → サービス提供時に利用される PKI



NICSS: The Next generation Ic Card System Study group

4.1.2 インターネット VPN

通信機器、端末などの機能によりインターネット上に私設仮想回線(VPN:Virtual Private Network)を設定し、インターネットに点在している組織や企業の各部署を接続するためのネットワーク網を構築すること。

インターネットで使われている TCP/IP プロトコルでは、通常はデータの暗号化やユーザー認証などは行なわれていないため、第三者に盗聴されたり改ざんされたりする恐れがあるため、データを送出する前にデータを暗号化して送り、また受信した側のノードでそのデータを復号化して、セキュリティを確保する。この暗号化をユーザーから透過的に行ない、かつユーザー認証によってある特定のユーザーだけしかアクセスできないようにしておけば、公衆回線網を使っても、専用線接続と同じようなセキュリティを保つことができる。

HEASNET では、このVPNを暗号化通信を設定するために IPsec を用い、強固なセキュリティを

実現している。

4.1.3 認証局

本仕様書で規定している証明書発行機関は、以下の説明する認証局と登録局の両方の機能を併せ持つ。

認証局
PKI アプリケーションで利用される公開鍵証明書を発行し、信頼を担うのが認証局（CA：Certification Authority）である。CA の信頼が、PKI システム全体の信頼性の基盤となっている。CA は、以下の役割を持つ。
① 利用者の公開鍵に対して電子署名をし、公開鍵証明書を発行する。
② 申請者が公開鍵・秘密鍵ペアを持つことを保証する。
③ CA は公開鍵証明書に署名するための秘密鍵を持ち、それを管理する。
④ 発行した公開鍵証明書を検証するために CA 自身の公開鍵を公開する。
⑤ 失効リスト（CRL）を発行する。

登録局
登録局（RA：Registration Authority）は、PKI システムの利用者登録を行う。また公開鍵証明書の発行・失効申請を審査する。CA が公開鍵証明書の保持者と公開鍵の関係を保証するのに対して、RA は保持者の身元保証を行う。確実に証明書を発行するのに値する保持者かを、その発行する組織により決められた条件で審査する。RA は、以下の役割を持つ。
① 証明書発行・失効などの資格審査。
② 鍵の一括管理。
③ 公開鍵を開示するためのディレクトリへ証明書の保管。
④ IC カードへの秘密鍵・公開鍵の格納。
⑤ 安全な証明書の配布・鍵配布

以上