オンデマンド VPN（HEASNET 版）

相互接続仕様書

（網間接続編）

第 2.0 版

2017 年 5 月 23 日

HEASNET 技術委員会

改版履歴

版数	作成日	作成	記事・備考
1.0	2008/01/04		初版
2.0	2017/05/23		2.4 章、2.5 章 IPsec の IKE のバージョン、暗号化アルゴリズム、証明書プロファイルを変更

目　次

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、異なる通信事業者を接続するための相互接続機能について定義する。

1.2 目的

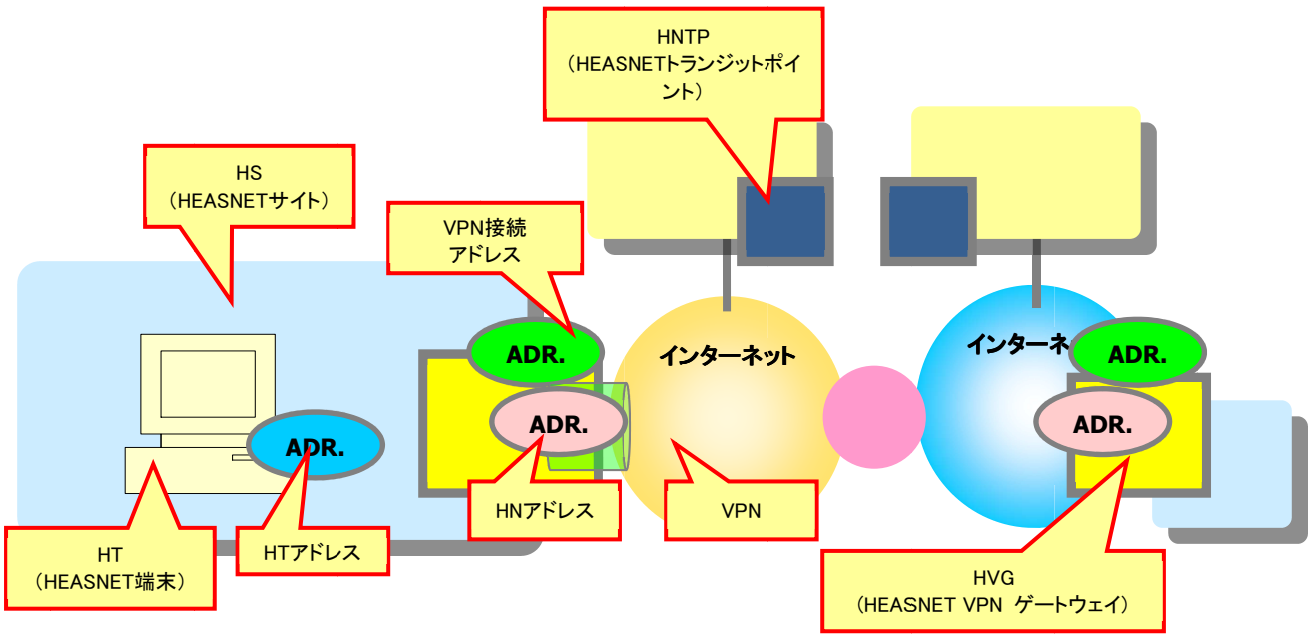
- 相互接続に必要となる事業者間の接続インタフェースを定義
- 医療分野におけるネットワークサービス利用者への接続性と利便性向上

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、以下の相互接続機能を提供する。

① HNP-A の HS-A から HNP-B の 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 が他の事業者の 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、他の事業者の 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 構成図



■ 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
■ 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
■ HNTP(HEASNET トランジットポイント)
:網中継型の相互接続において HNP 間を接続するゲートウェイ

2. サービス仕様

2.1 相互接続関連情報

事業者間で交換される相互接続関連の情報を定義する。

2.1.1 事業者間で交換されるメッセージ

相互接続における情報交換は、以下の要件を満たすものとする

- 相互認証を行う
- 暗号化通信など安全な経路上で行う

各 HNP 間で交換される情報は、以下の 3 つのフェーズに分類される 。

- サイト登録フェーズ
  - 自 HNP に対して相互接続拠点としてサイト登録（更新/削除も含む）された場合に、相互接続先の HNP に対して、サイト登録を要求する
- 接続管理フェーズ
  - 接続要求先が相互接続拠点の場合には、対象となる HNP との管理サーバ間で接続要求を交換する
- 通信開始/終了フェーズ
  - 通信開始/終了の要求先が相互接続拠点の場合には、対象となる HNP の管理サーバ間で通信開始/終了要求を交換する

2.1.2 相互接続関連 ID

各 HNP 間で交換される情報については、以下の通りフォーマットを規定する。

項目	フォーマット	例
HNPのID	P-{[A-Z0-9]8桁}	P-PROVIDE1
HSのID	S-{[A-Z0-9]最大16桁}	S-HOSPITAL00000001
HTのID	T-{[A-Z0-9]最大16桁}	T-TERMINAL00000001
管理サーバ間で交換されるメッセージのID	RS[YYMMDDhhmm]{[A-Z0-9]2桁}	RS0708101704A1

2.2 HEASNET 利用アドレス

2.2.1 HNP 間アドレス

(1) HNTP 間アドレス規定

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

2.2.2 HNP 内アドレス

(1) 相互接続用仮想 HS アドレス

アドレスとしては、HEASNET で一意な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) 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

(3) 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

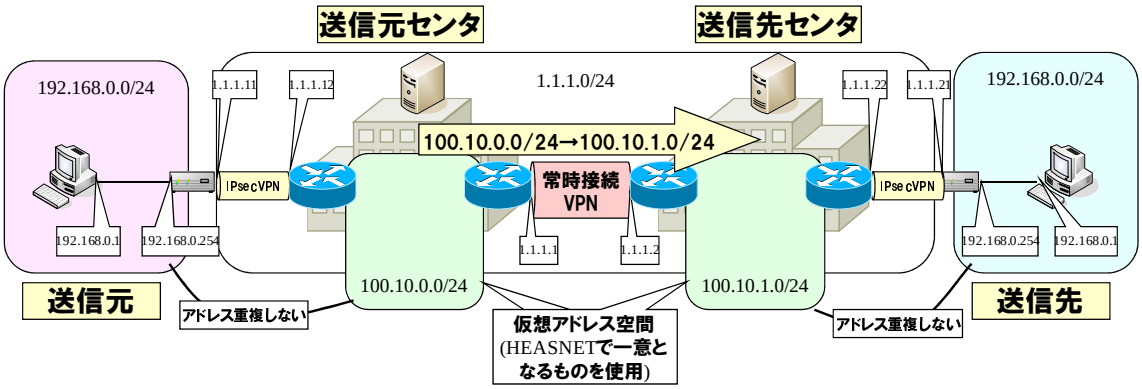
(4) HT アドレス

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

(5) アドレス重複回避

- 仮想アドレス空間は、事業者間の相互接続時にアドレス重複が起きないように HEASNET 内で一意となるアドレスブロックを利用する。
- 事前にセンタ間では、相互通信する端末に割り当てた仮想アドレスの変換を行う。
- 常時接続 VPN に流す前のパケットに対するアドレスの変換方法は、各センタで決定する。



2.3 ルーティング管理

相互接続時における経路情報の管理・交換に関する仕様を規定する。

2.3.1 HNP 内ルーティング情報

- 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。

(1) 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。

2.3.2 HNP 間ルーティング情報

静的に設定する。経路情報は事前に通知する。

2.4 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。

2.4.1 HNP 内での VPN 仕様

(1) HEASNET ネットワークプロバイダ内ルータ IKE パラメータ

1) サポートする鍵交換手法	IKEv2
① 相互認証方式	RSA 電子署名認証方式
(ア) 証明書の形式	X.509 バージョン 3(2.5.2 章参照)
② 暗号化アルゴリズム	AES-128 CBC モード
③ 疑似乱数関数	AES-XCBC-PRF-128
④ Diffie-Hellman グループ	2048 ビット MODP グループ(グループ 14)
⑤ PFS(Perfect Forward Secrecy)	有効
2) サポートするセキュリティプロトコル	ESP
① 暗号化アルゴリズム	AES-128 CBC モード
② 認証アルゴリズム	AES-XCBC-MAC-96

2.4.2 HNP 間での VPN 仕様

(1) HEASNET ネットワークプロバイダ間中継 GW ルータ IKE パラメータ

1) サポートする鍵交換手法	IKEv2
⑥ 相互認証方式	RSA 電子署名認証方式
(ア) 証明書の形式	X.509 バージョン 3(2.5.2 章参照)
⑦ 暗号化アルゴリズム	AES-128 CBC モード
⑧ 疑似乱数関数	AES-XCBC-PRF-128
⑨ Diffie-Hellman グループ	2048 ビット MODP グループ(グループ 14)
⑩ PFS(Perfect Forward Secrecy)	有効
2) サポートするセキュリティプロトコル	ESP
③ 暗号化アルゴリズム	AES-128 CBC モード
④ 認証アルゴリズム	AES-XCBC-MAC-96

【第 2.0 版策定時の備忘録】
RFC4308 を参考に検討。
・現在主流の IKEv2 を採用し、アルゴリズムは RFC4308 の高セキュリティの Suite VPN-B を採用。
・認証方式は、2.0 版ではデジタル署名認証方式のみとし、1.0 版で併記されていた事前共有方式は削除した。
・相互運用性確保の観点から、AES を 1 種類に特定。Suite VPN-B にあわせる方針とし、AES-128 CBC モードを残し、AES-256 CBC モードを削除。

2.5 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。

2.5.1 認証局の配置

事業者毎に認証局を保持する「分散型」と、事業者共通の認証局を利用する「集中型」に対応する。認証局の取り扱いについては、相互接続するプロバイダ双方で調整する。

2.5.2 証明書フォーマット

HEASNET の相互接続に使用する証明書フォーマットを記載する。

証明書の形式	相互接続 GW 認証用公開鍵証明書	備考
Certficate		
tbsCertificate		
version	3	
serialNumber	設定	同一認証局が発行する証明書内でユニークな値
signature	SHA256WithRSAEncryption	
issuer	設定	
validity	利用する証明書の仕様に準拠する	
subject	C,O,OU,CN は必須	
subjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	2048 ビット	
extension		
keyUsage	digitalSignature	
basicConstraints	cA:FALSE	
subjectDirectoryAttributes	オプション	
certificatePolicies	設定	証明書ポリシの OID
cRLDistributionPoints	設定	
authorityKeyIdentifier	設定	
subjectKeyIdentifier	設定	
subjectAltName	FQDN、USER-FQDN の 2 種を設定	
signatureAlgorithm	SHA256WithRSAEncryption	
signature	設定	

【第 2.0 版策定時の備忘録】
厚生労働省発行の保健医療福祉分野 PKI 認証局 認証用(組織)証明書ポリシ 1.1 版と RFC4945 を参考に検討した。1.0 版から 2.0 版への修正箇所は以下の通り。
・アルゴリズム:SHA1WithRSA から SHA2WithRSA へ変更
・鍵長:1024 ビットから 2048 ビットへ変更
・keyUsage の明確化
・証明書ポリシ(certificatePolicies)、CRL 配布点(cRLDistributionPoints)を必須に変更
・subjectAltName には IPV4_ADDR、IPV6_ADDR を使ってもよいと考えるが、1.0 版を踏襲。
・keyUsage は、RFC では nonRepudiation も設定可だが、証明書ポリシ 1.1 版にあわせた。

2.6　HS の接続許諾管理

HEASNET で異なる事業者間の HS 間の接続においては、合意形成された場合のみ、対象の 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。

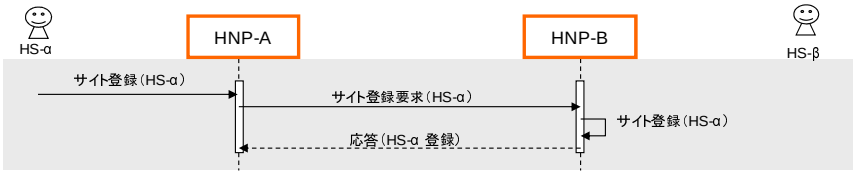
2.6.1　サイト登録

(1)　HNP 内でのサイト登録

各 HNP 独自で実施する

(2)　HNP 間でのサイト登録情報の連携

自 HNP に対して相互接続拠点としてサイト登録（更新/削除も含む）された場合に、相互接続先の HNP に対して、サイト登録を要求する。



カテゴリ	メッセージ	内容大枠	内容詳細		説明
共通	HEASNETの管理サーバ間のメッセージの定型	メッセージ宣言 <heasnet-ctl>	メッセージID：messaged-id を <heasnet-ctl> の属性値として持つ		・メッセージIDは、リクエスト側にとっての一意の値とする。 ・応答側は、リクエスト側が指定したメッセージIDを指定する。
	プロバイダ識別情報	HNP情報 <hnp>	接続元HNPのID <from-id>		HEASNET内で一意のHNPのID
			接続先HNPのID <to-id>		HEASNET内で一意のHNPのID
リクエスト	サイト-端末登録要求 <hs-register-req>	HS情報 <hs>	HSのID <id>		HEASNET内で一意のHSのID
			HT情報 <ht>	HTのID <id>	HEASNET内で一意のHTのID
				HTのアドレス <address> ・IPv4 <ip><v4> もしくはIPv6<ip><v6>	HEASNET内で一意のHTの仮想IPアドレス
	サイト-端末変更要求 <hs-update-req>	HS情報 <hs>	HSのID <id>		HEASNET内で一意のHSのID
			HT情報 <ht>	HTのID <id>	HEASNET内で一意のHTのID
				HTのアドレス <address> ・IPv4 <ip><v4> もしくはIPv6 <ip><v6>	HEASNET内で一意のHTの仮想IPアドレス
	サイト-端末削除要求 <hs-delete-req>	HS情報 <hs>	HSのID <id>		HEASNET内で一意のHSのID
			HT情報 <ht>	HTのID <id>	HEASNET内で一意のHSのID
				HTのアドレス <address> ・IPv4 <ip><v4> もしくはIPv6 <ip><v6>	・HEASNET内で一意のHTのID ・IDとして、HS内の全HTを意味する"ANY"を指定可とする
応答	応答 <heasnet-ctl-reply>	正常応答 <ok/>	HTのアドレス <address> ・IPv4 <ip><v4> もしくはIPv6 <ip><v6>		HEASNET内で一意のHTの仮想IPアドレス
		異常応答 <heasnet-ctl-error>	エラータイプ <error-type>		・フォーマットエラー：format-error ・データ内容エラー：data-error
			エラーメッセージ <error-message>		内容は特に規定しない。

2.6.2　合意形成

(1)　HNP 内の合意形成

各 HNP 独自で実施する

(2)　HNP 間の合意形成情報の連携

接続要求先が相互接続拠点の場合には、対象となる HNP との管理サーバ間で合意要求を交換する

カテゴリ	メッセージ	内容大枠	内容詳細		説明
共通	HEASNETの管理サーバ間のメッセージの定型	メッセージ宣言 <heasnet-ctl>	メッセージID: messaged-id を <heasnet-ctl> の属性値として持つ		・メッセージIDは、リクエスト側にとっての一意の値とする。 ・応答側は、リクエスト側が指定したメッセージIDを指定する。
	プロバイダ識別情報	HNP情報 <hnp>	接続元HNPのID <from-id>		HEASNET内で一意のHNPのID
			接続先HNPのID <to-id>		HEASNET内で一意のHNPのID
リクエスト	合意要求 <connection-create-req>	接続構成 <connection>	接続元 <from>	・HSのID <hs><id> ・HTのID <hs><ht><id>	・メッセージ送信者にとって自HNP側のHS、HTのID
			接続先 <to>	・HSのID <hs><id> ・HTのID <hs><ht><id>	・メッセージ送信者にとって相手側のHS、HTのID
	合意削除要求 <connection-delete-req>	接続構成 <connection>	接続元 <from>	・HSのID <hs><id> ・HTのID <hs><ht><id>	・メッセージ送信者にとって自HNP側のHS、HTのID
			接続先 <to>	・HSのID <hs><id> ・HTのID <hs><ht><id>	・メッセージ送信者にとって相手側のHS、HTのID
応答	応答 <heasnet-ctl-reply>	正常応答 <ok/>			正常応答
		異常応答 <heasnet-ctl-error>	エラータイプ <error-type>		・フォーマットエラー: "format-error" ・データ内容エラー: "data-error"
			エラーメッセージ <error-message>		内容は特に規定しない。

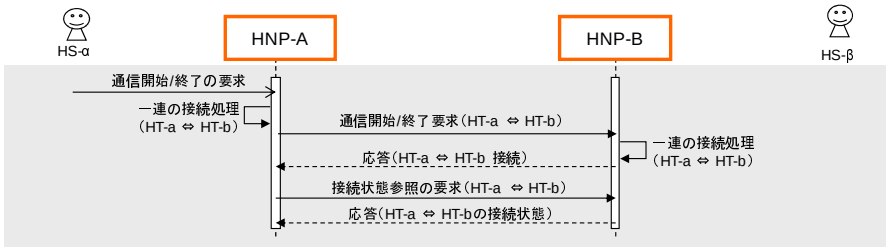
2.6.3 通信開始・終了

(1) HNP 内の通信開始・終了

各 HNP 独自で実施する

(2) HNP 間の通信開始・終了情報の連携

通信開始/終了の要求先が相互接続拠点の場合には、対象となる HNP の管理サーバ間で通信開始/終了要求を交換する



カテゴリ	メッセージ	内容大枠	内容詳細		説明
共通	HEASNETの管理サーバ間のメッセージの定型	メッセージ宣言 <heasnet-ctl>	メッセージID：messaged-id を <heasnet-ctl> の属性値として持つ		・メッセージIDは、リクエスト側にとっての一意の値とする。 ・応答側は、リクエスト側が指定したメッセージIDを指定する。
	プロバイダ識別情報	HNP情報<hnp>	接続元HNPのID <from-id>		HEASNET内で一意のHNPのID
			接続先HNPのID <to-id>		HEASNET内で一意のHNPのID
リクエスト	通信開始要求 <connect-req>	接続構成 <connection>	接続元 <from>	・HSのID <hs><id> ・HTのID <hs><ht><id>	開始要求が相互接続先HNPから受理（正常応答）された場合は、各種通信到達性確保のための設定を行う。
			接続先 <to>	・HSのID <hs><id> ・HTのID <hs><ht><id>	
	通信終了要求 <disconnect-req>	接続構成 <connection>	接続元 <from>	・HSのID <hs><id> ・HTのID <hs><ht><id>	終了要求送信後は、接続時に実施した各種通信到達性確保のための設定を削除する。
			接続先 <to>	・HSのID <hs><id> ・HTのID <hs><ht><id>	
応答	応答 <heasnet-ctl-reply>	正常応答 <ok/>			正常応答
		異常応答 <heasnet-ctl-error>	エラータイプ <error-type>		・フォーマットエラー："format-error" ・データ内容エラー："data-error"
			エラーメッセージ <error-message>		内容は特に規定しない。

3. 運用

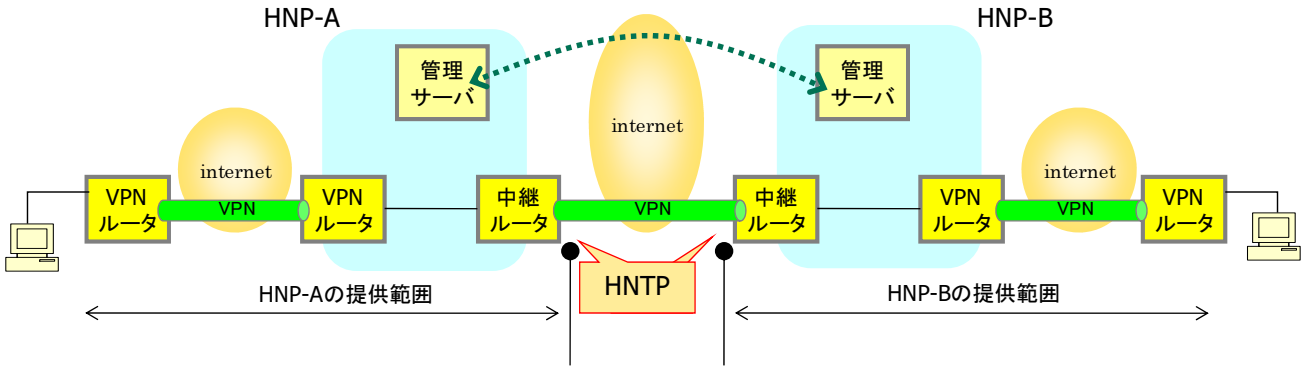
HEASNET は以下の運用に従い、ネットワークを運用する。

3.1 相互接続の運用

■ 相互接続している拠点同士の運用に関しては、相互接続するプロバイダ同士で相互に定めることとする

3.2 責任分解

網間接続における各 HNP の基本提供範囲は、HNTP までとする。



(1) 相互接続における障害

インターネット環境における障害については、互いに協力して切り分けを実施する。
各ユーザからの 1 次対応は、契約している HNP が行うこととする。

(2) 相互接続における賠償

相互接続ユーザ間での接続においては、ユーザが属す HNP が負うこととする。