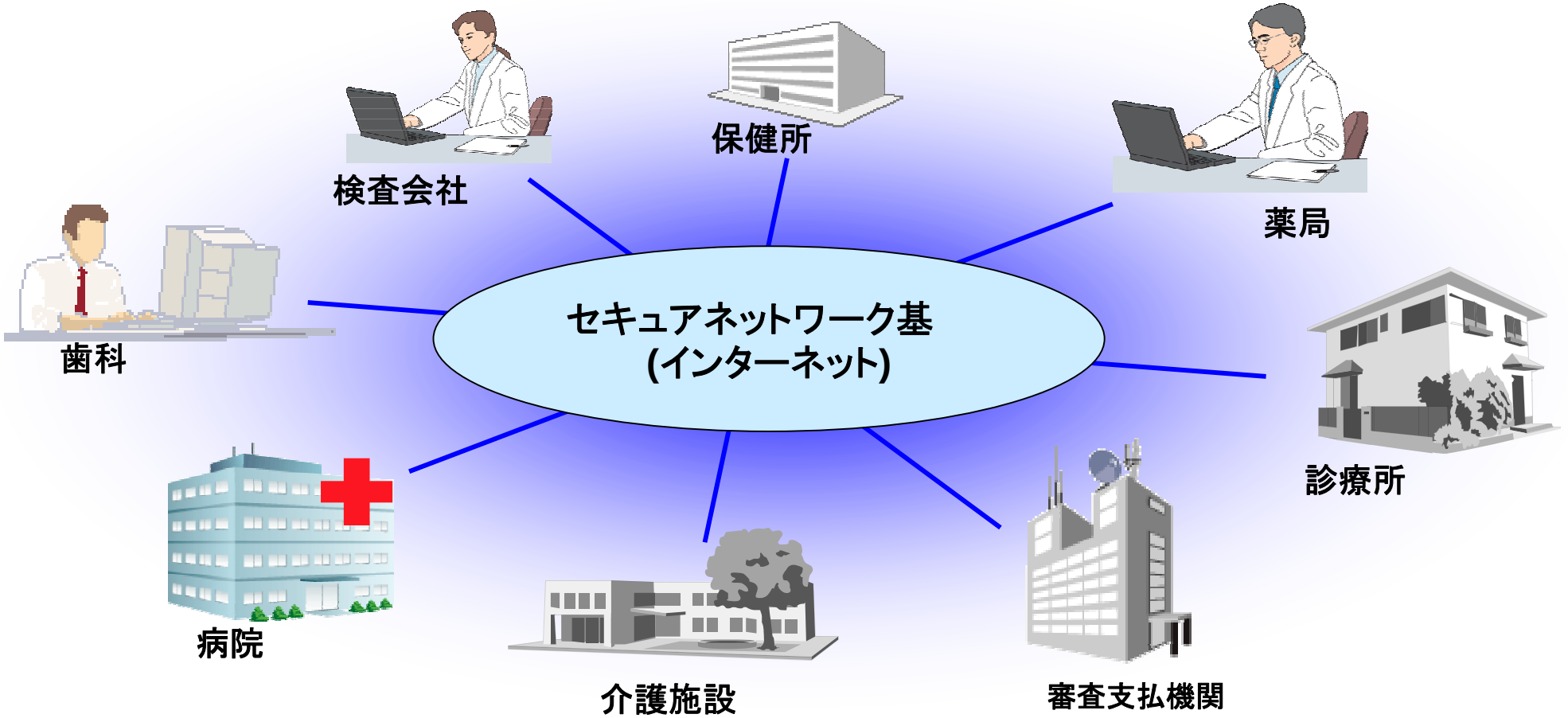
厚生労働省
「医療情報システムの安全管理に関するガイドライン第2版」概要紹介と適用のための技術要件および チェックシート概要について

平成19年11月14日

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
HEAlthcare information Secure NETwork consortium
(HEASNET)

Copyright© 2007 HEASNET

HEASNETは、大山永昭東京工業大学像情報工学研究施設教授を会長として、セキュアネットワーク基盤を介して、国民に対し多様なヘルスケアサービスを提供し、安心・安全で暮らしやすい社会を実現することを理念として、平成17年2月4日に設立



Copyright© 2007 HEASNET

セキュアネットワーク基盤の整備に関する活動

- セキュアネットワーク基盤実現のための標準フレームワークの提起
- 相互接続などの標準インタフェース提起・公開
- 登録センタ間等の連携モデルの検討
- HPKI、公的個人認証、民間認証との連携を検討
- 既存 VPN方式等との連携を検討
- セキュリティポリシ等の運用ガイドラインの提起
- 保健・医療・福祉分野の各種アプリケーションとの連携を検討

普及啓発に向けた活動

- セキュアネットワーク基盤を活用したサービスの普及促進活動

Copyright© 2007 HEASNET

医療情報システムの安全管理に関するガイドラインの改訂点

【大きな変更点】
- ●ネットワーク利用の安全管理の全面改定　(6．9→6．10)
- ●災害等の非常時の対応(6．9)を新設
- ●ISMSの考え方を明確に導入(6．2他)
- ●7章の電子保存の要求要件の根拠をE文書法厚生省令および関連通知に変更
  (内容は変化なし)
- ●8章(外部保存)のオンライン部分を6．10を明に参照するように変更
- ●アクセスログ検査を運用規程で定める項として明示

6．10　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
- ●責任分界点の明確化
  - ●送り手・受け手の責任分界点
  - ●通信を形成するプレーヤの責任分界点
- ●医療機関等における留意事項
  - ●情報の送信が終了するまでは内容の真正性に関して送り手の医療機関等に責任がある
  - ●盗聴　⇒　暗号化
  - ●改ざん　⇒　電子署名
  - ●なりすまし　⇒　人・組織・機器の認証
- ●選択すべきネットワークのセキュリティの考え方
  - ●ネットワークサービスの種類、オープンネットワーク適用における留意事項
    (医療情報システムの安全管理に関するガイドライン実装事例に関する報告書)

Copyright© 2007 HEASNET

医療分野におけるネットワークのニーズ

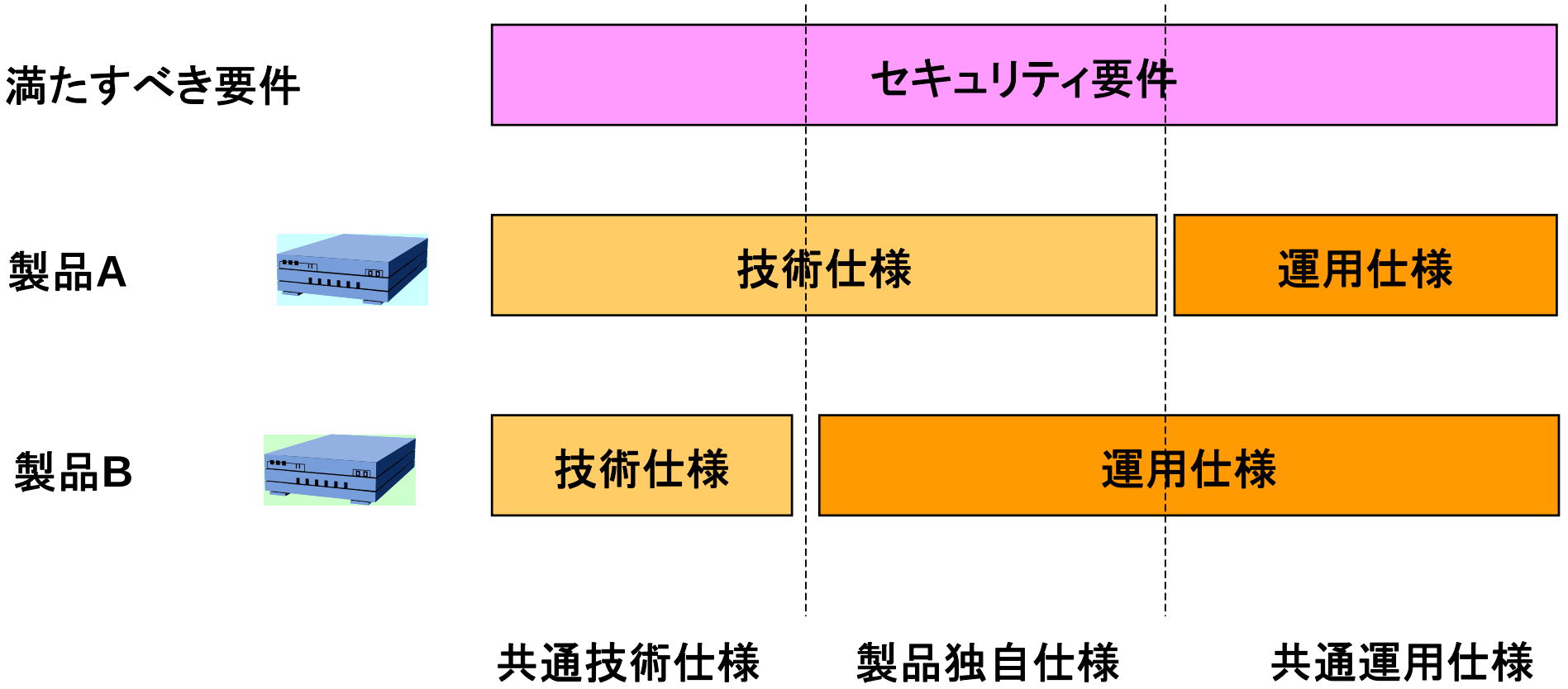
- 医療機関としてどこまで、ネットワーク内のセキュリティを担保すべきか責任の範囲が不明瞭である
- 医療機関ネットワークにおいてどのような脅威やリスクが想定されるのか、またその対策についての基準が明確には示されていない

- IETFが発行するRFCを網羅的に分析・類型化して31のリスクに体系化
- オンデマンドVPNは、31のリスクの発生要因と対処技術を考慮して、それを満足する様に仕様の策定を実施

医療分野におけるネットワークセキュリティチェックシートの作成

Copyright© 2007 HEASNET

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。



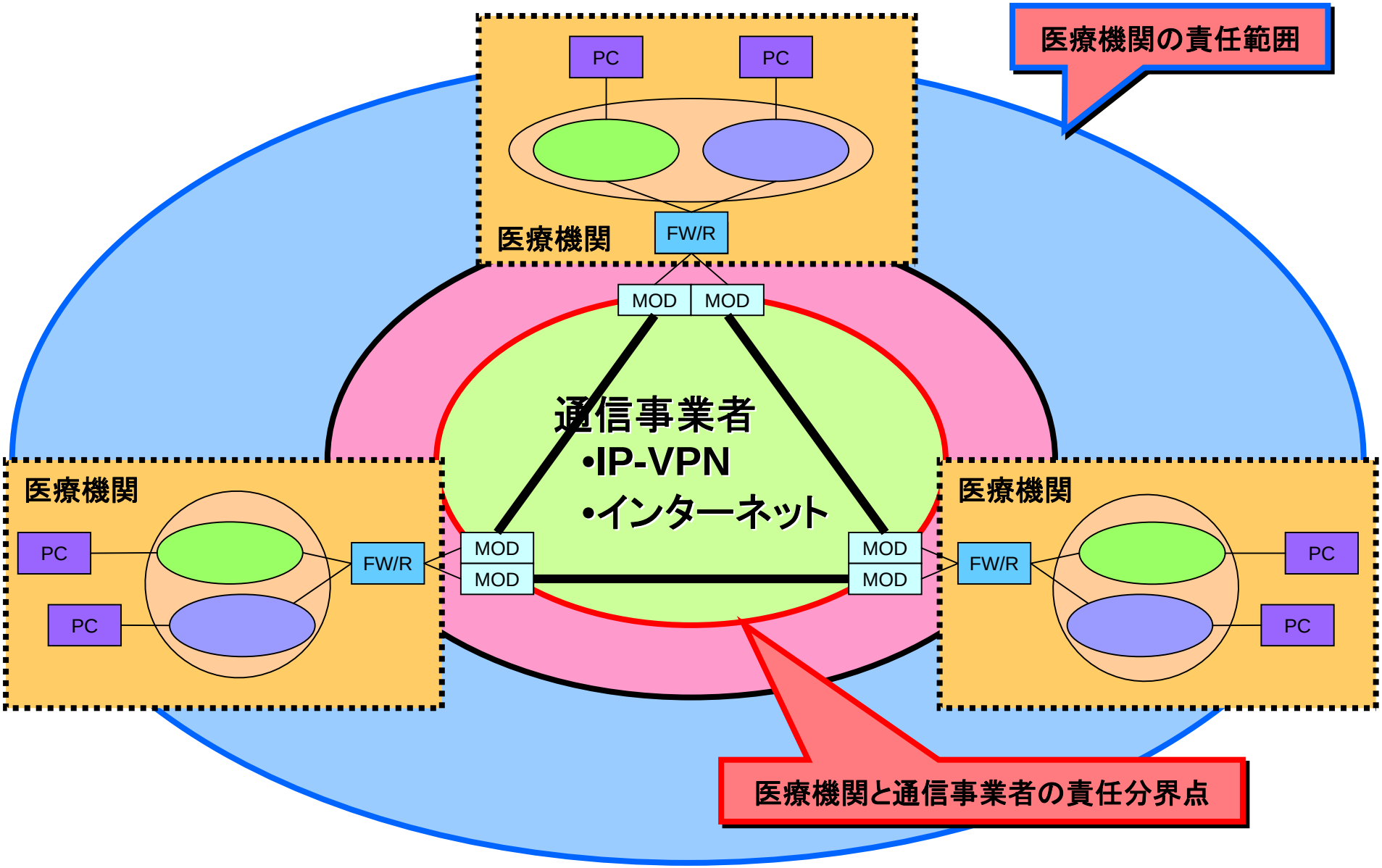
Copyright© 2007 HEASNET

各種ガイドラインがカバーする対象範囲の整理

ガイドライン ＼ 対象範囲	ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	セキュアネットワーク基盤の運用(その他)	利用者
厚生労働省GL (レセプト)				■
厚生労働省GL (医療情報システム)				■
RFC4107他	■		■	
NICSS 運用ガイドライン	■	■		
NICSS セキュリティ要件	■	■		
JAHIS標準				■
JIRAガイドライン				■

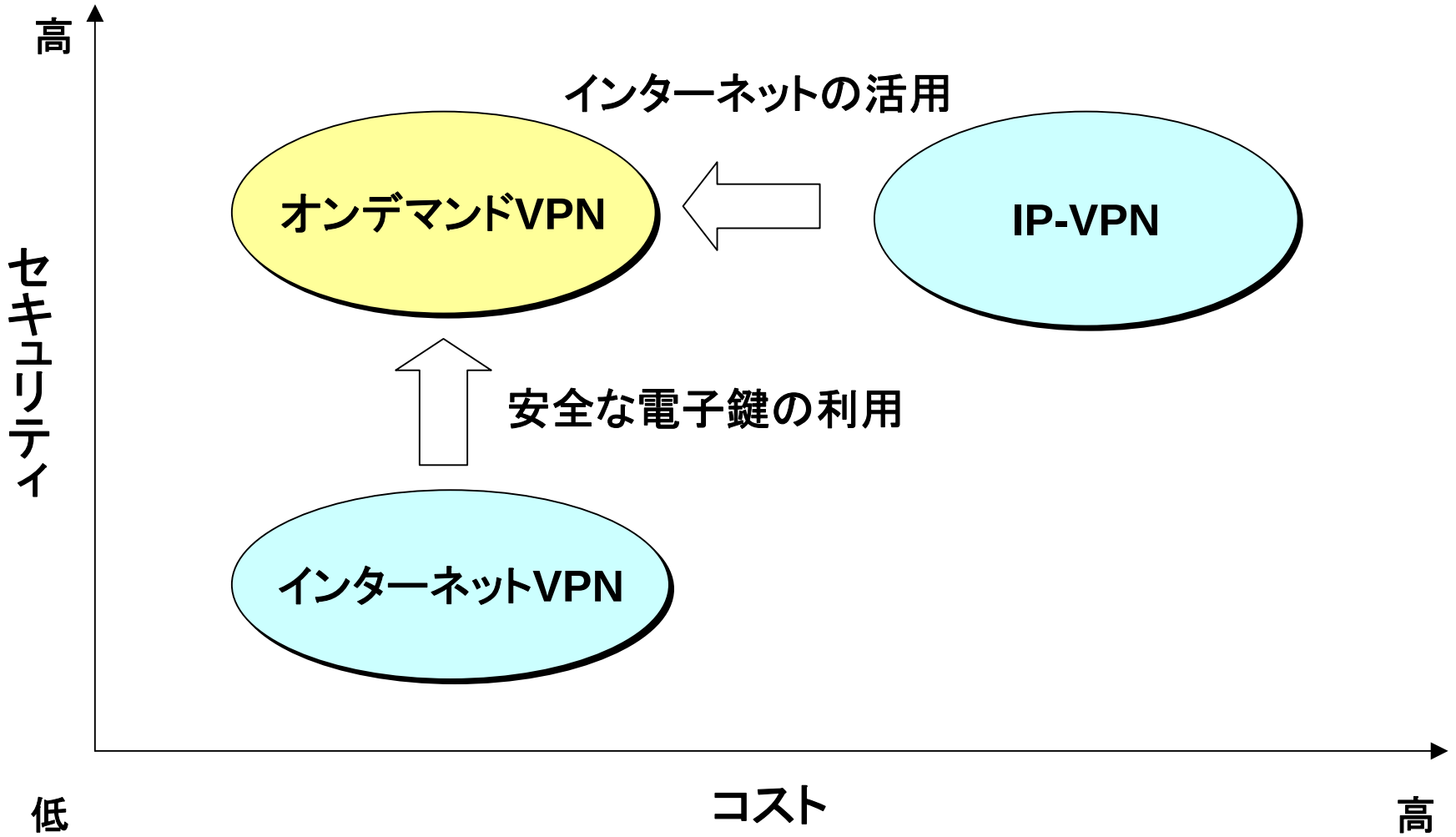
Copyright© 2007 HEASNET

ネットワーク基盤と責任分界点



Copyright© 2007 HEASNET

HEASNETの提唱するオンデマンドVPN

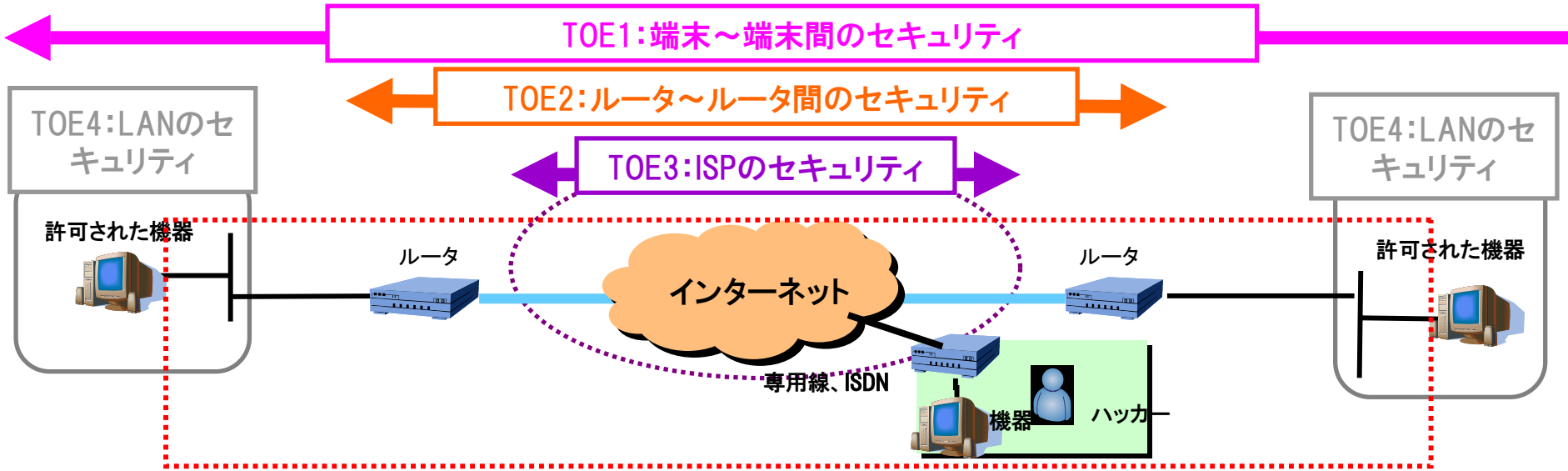


Copyright© 2007 HEASNET

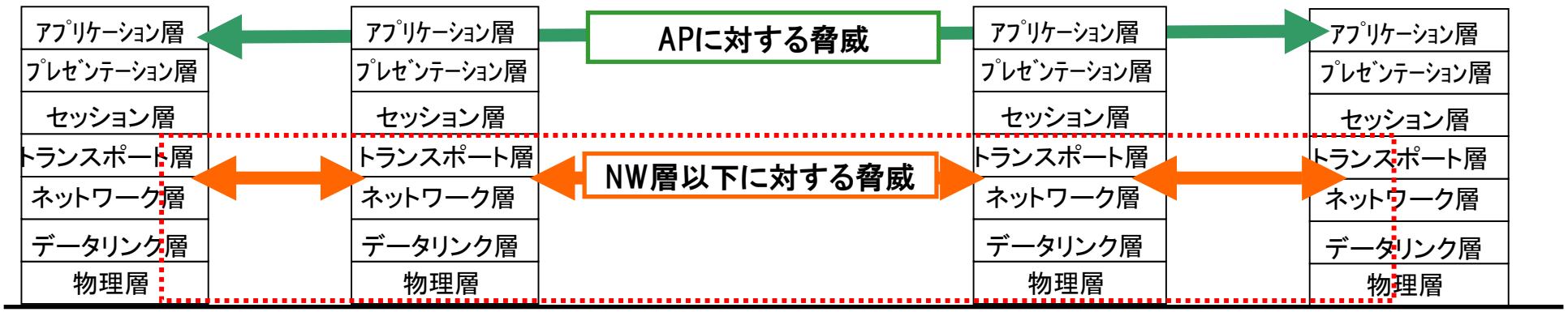
検討範囲

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。

「ネットワークの範囲」の観点



「ネットワークの階層」の観点

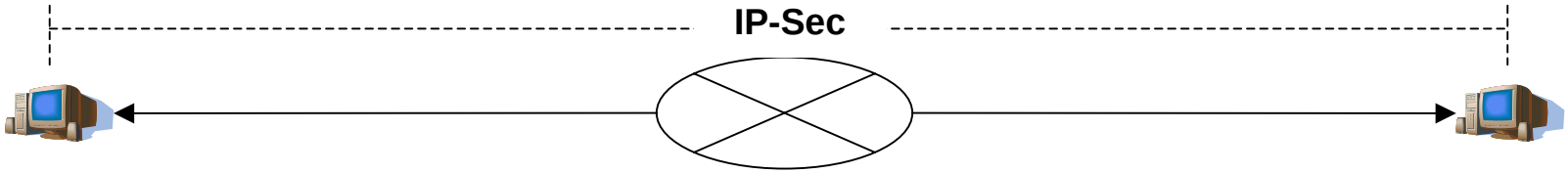


Copyright© 2007 HEASNET

AP層のセキュリティ対策

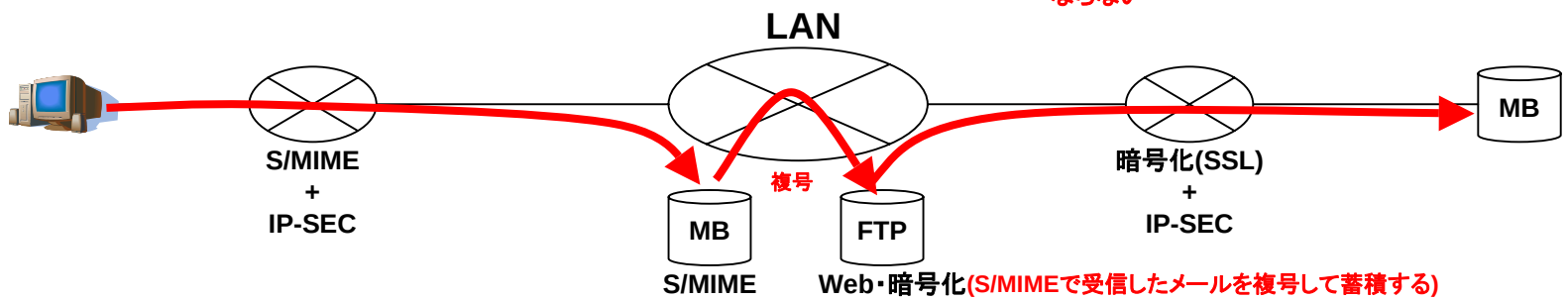
AP層ではユーザがネットワークの脅威とは別にそれぞれが暗号化や改ざんに対する対策を個別に打って脅威から医療情報を守る。

＜従来のネットワークの検討スコープ＞

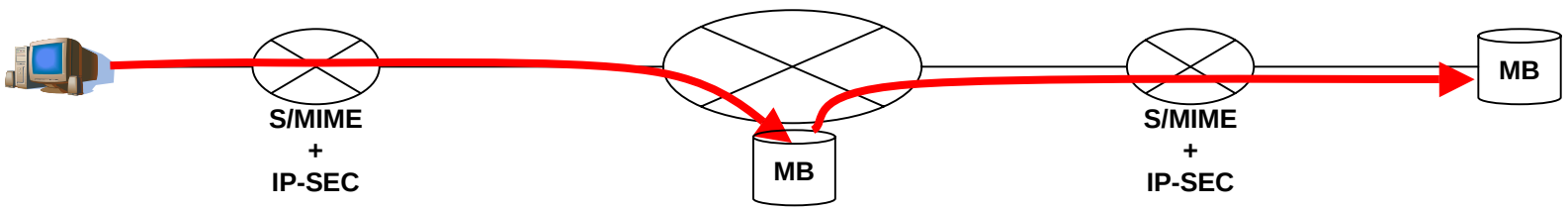


＜今後検討が必要とされるネットワーク構成の例：健診情報等の伝送＞

※ WebサーバやFTPサーバに蓄積されている情報の
※ オブジェクトセキュリティについて考慮しなければ※
ならない



＜今後検討が必要とされるネットワーク構成の例：電子メールによる医療情報の交換＞



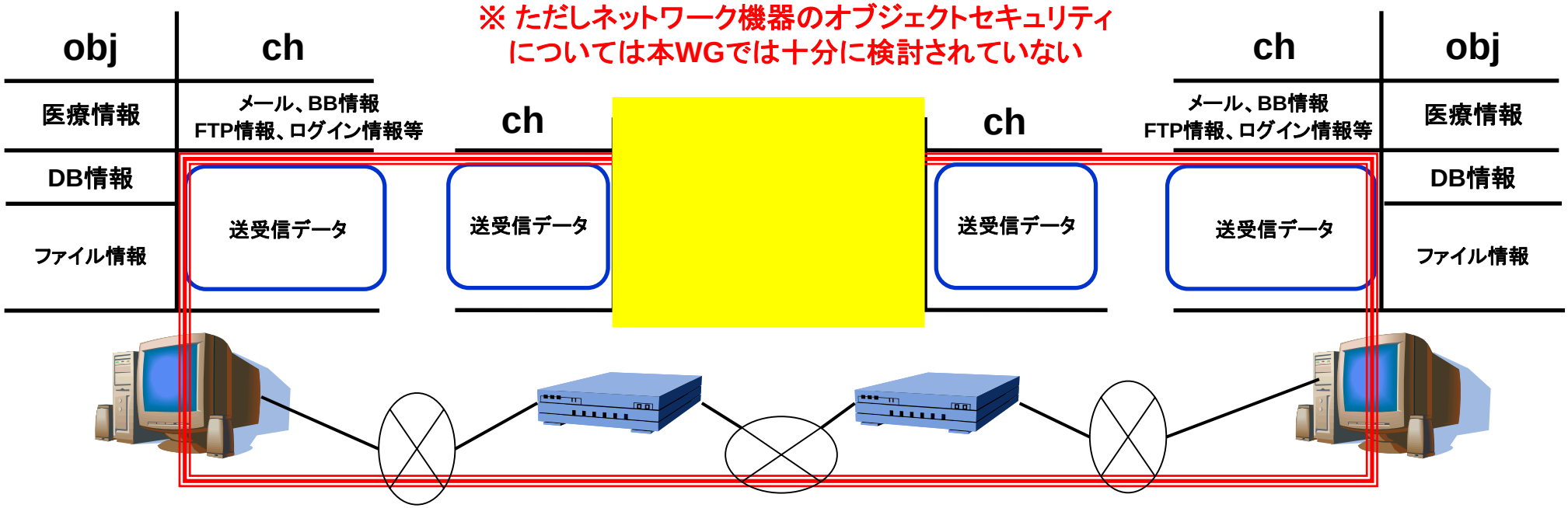
Copyright© 2007 HEASNET

守るべき資産

(1)端末間のチャネル･セキュリティ　⇒ 送受信データ

(2)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

※ ただしネットワーク機器のオブジェクトセキュリティについては本WGでは十分に検討されていない



ネットワークにおいて守るべき資産

Copyright© 2007 HEASNET

ネットワークの脅威

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	共有ﾊﾟｽﾜｰﾄﾞ	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	ﾄﾎﾟﾛｼﾞｰの破壊	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	常用ﾌﾟﾛﾄｺﾙでの攻撃	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	情報の不正ｺﾋﾟｰ	ウイルスには、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。また巧妙なウイルスには、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（IPｱﾄﾞﾚｽ詐称）	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ﾊﾟｹｯﾄ挿入	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。

Copyright© 2007 HEASNET

類型	脅威	解説
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	ｳｲﾙｽ混入後の転送	ウイルスには、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。また巧妙なウイルスには、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。
T20	情報の破壊・書換え	ウイルスには、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。また巧妙なウイルスには、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	ﾒｯｾｰｼﾞ盗聴後再送	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ﾌﾗｯﾄﾞ攻撃	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イ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	ｻｰﾋﾞ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。

Copyright© 2007 HEASNET

チャネル･セキュリティ対策の技術要素

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	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／チャレンジレスポンススキーム	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
		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	IKE v1 用アルゴリズム
			Modular 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 Modular Exponential (MODP) Diffie-Hellman グルー
		鍵配布センター	自動鍵管理（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.509 PKI および CRL プロファイルにおける DirectoryString 処理についての更新
	守秘性	IP暗号ペイロード（ESP）	暗号ハッシュ関数（HMAC-SHA1-96）	RFC4305	ESP および AH についての暗号アルゴリズム実装要
				RFC4303	IP 暗号ペイロード（ESP）
			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）	RFC 3602	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 についての暗号アルゴリズム実装要
				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 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 守秘性 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 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
トラフィックセキュリティ		IPSec	IP暗号化ペイロード（ESP） IP認証ヘッダ 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
				RFC 4301	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
				RFC3631	インターネットについてのセキュリティメカニズム

Copyright© 2007 HEASNET

RFCに基いた脅威と対策の整理

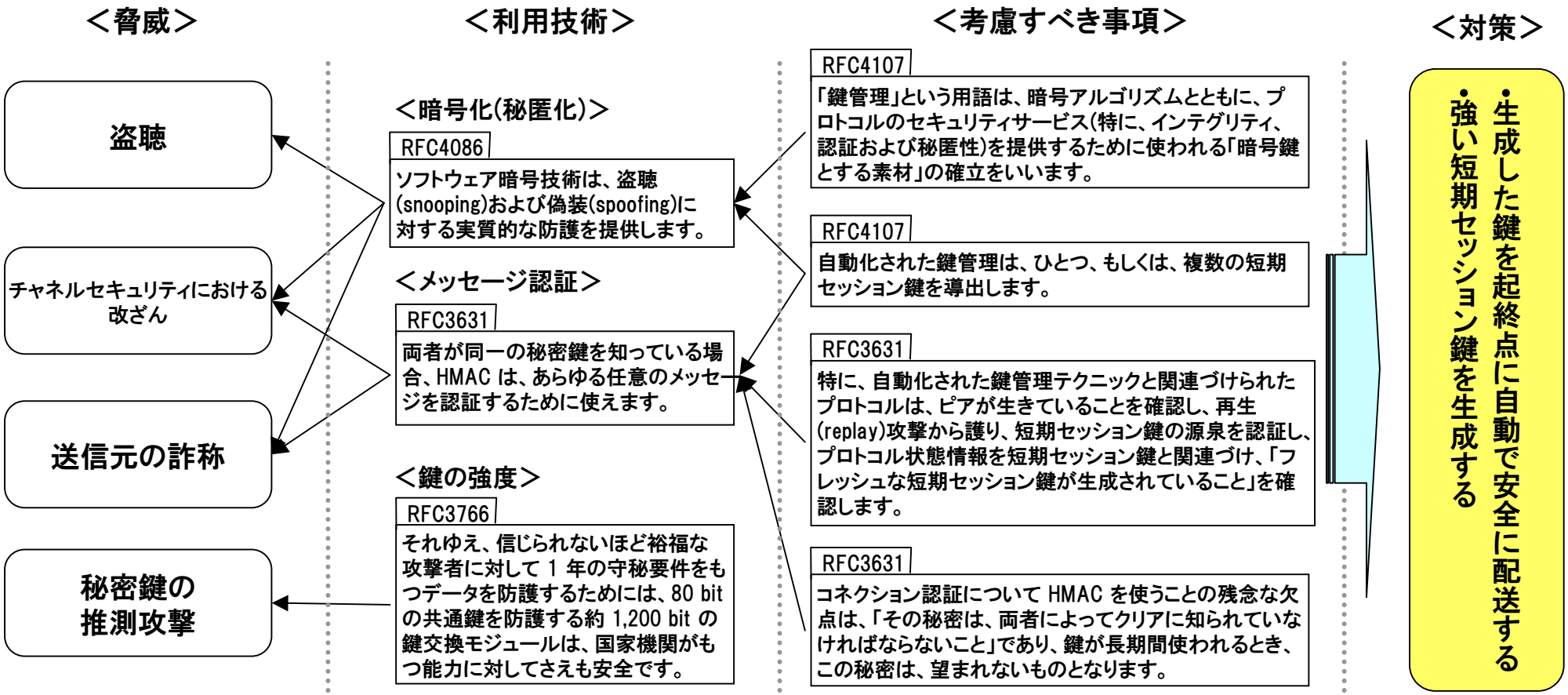
ネットワークへの攻撃と攻撃に対する直接的な対策について整理する。

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）：RFC1704> 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。	<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）：RFC1704> 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。	<RFC2828> $ keyed hash （鍵付ハッシュ） (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。） (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。： ＊鍵付暗号化アルゴリズムに基づく関数。（例： Data Authentication Code 参照。） ＊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）：RFC1704> 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。	<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、相互適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：RFC3552> 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。	<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ー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：RFC3552> 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> 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 ：RFC3552> 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。	<RFC3227> 4.1 カストディの連鎖 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。 下記事項が、文書化される必要があります。 ＊どこで／いつ／誰によって、証拠が発見、収集されたか。 ＊どこで／いつ／誰によって、証拠が対処、検査されたか。 ＊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。 ＊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：RFC3552> 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。	<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。

Copyright© 2007 HEASNET

セキュリティ対策の検討

セキュリティ対策素案を検討するにあたり、守るべき資産、及びネットワーク上の脅威を踏まえ、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。
作成した脅威モデルをもとに、厚生労働省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。



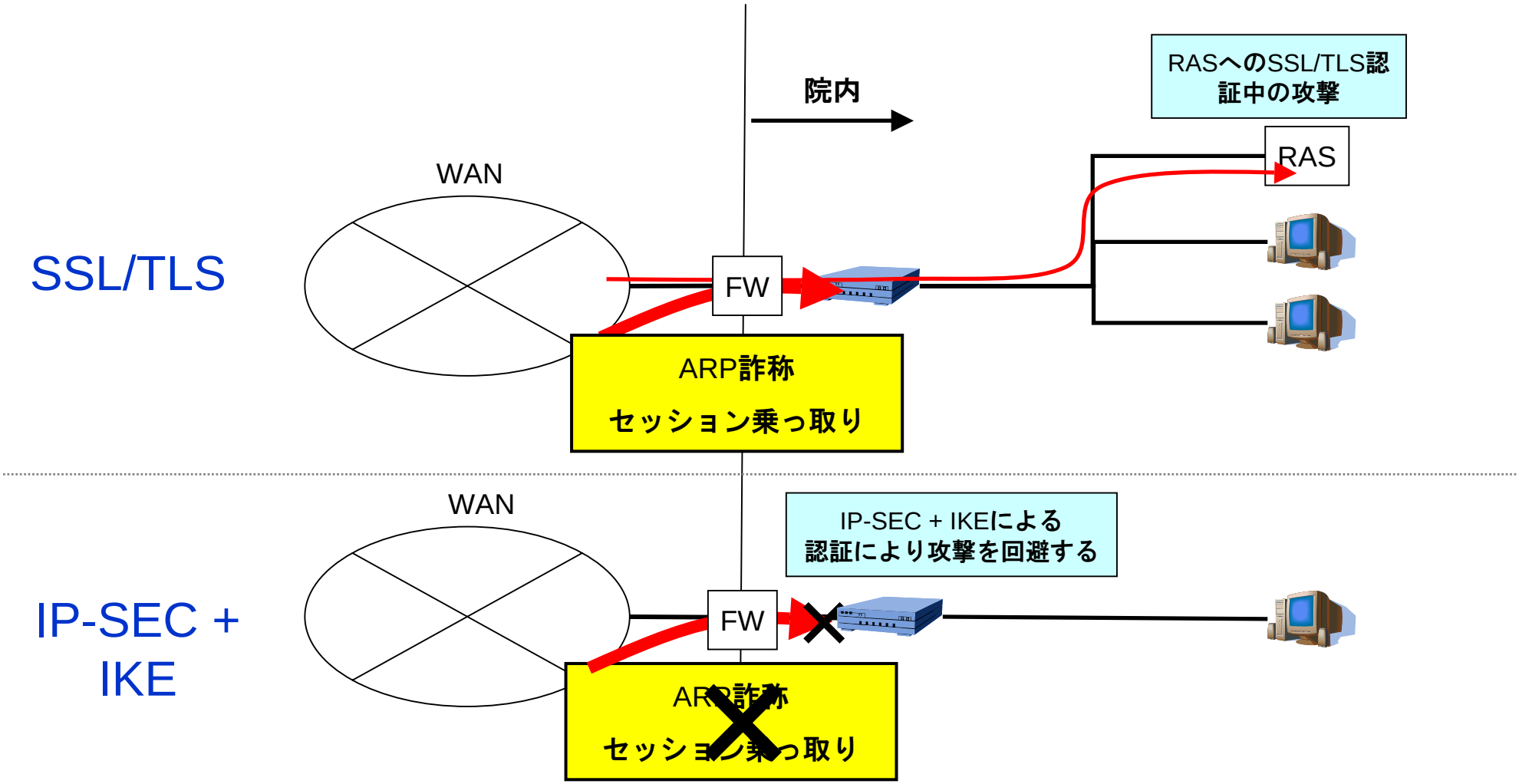
Copyright© 2007 HEASNET

チャネル･セキュリティの脅威と技術対策

評価項目 ＼ 対策					エンティティ間の認証						トラフィックセキュリティ		暗号ペイロード（ESP）	メッセージ認証	否認防止		サービス妨害
					ユーザ／パスワード	ワンタイム	チャレンジ	共有鍵（自動鍵管理）	鍵配布（Kerberos）	証明書	IPSec	IP-VPN			証拠収集	アーカイビング	イングレスフィルタリング
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	×	◎	◎	◎	◎	◎	△	△	◎	×	△	△	△
			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	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
		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	△	△	△	△	◎	◎	△	△	△	△	△	△	◎
				T25. 災害・物理的破壊													
				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													

Copyright© 2007 HEASNET

トラフィックセキュリティを提供する対策として、「SSL/TLS」と「IP-SEC＋IKE」が有効な対策として考えられるが、下記に示すように攻撃の種類によっては、「IP-SEC＋IKE」では防げるが、「SSL/TLS」では防げない攻撃が存在する。



Copyright© 2007 HEASNET

チャネル･セキュリティ対策

現状において、利用可能な技術要素を組合わせたチャネル･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。

脅威	技術要素
待ち伏せ攻撃	<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。
積極的な攻撃	<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。
再生攻撃	<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。
ﾄﾎﾟﾛｼﾞｰ破壊	<RFC2196> 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ー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。
同一ﾘﾝｸ判別	<RFC3552> 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。
否認防止	<RFC3227> 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。
サービス妨害	<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。

IP-SECの認証ヘッダ(AH)と IP 暗号ペイロード(ESP)の2つのトラフィックセキュリティプロトコルの利用、および暗号鍵管理手法とそのプロトコルの利用によって達成する

この文書の執筆時点では、HMAC-SHA-1-96 に対する実際の暗号攻撃は存在しない。

「鍵管理」という用語は、暗号アルゴリズムとともに、プロトコルのセキュリティサービス(特に、インテグリティ、認証および秘匿性)を提供するために使われる「暗号鍵とする素材」の確立をいう

IKEv2：暗号用に 3DES/AES-128、 HMAC 用にHMAC-SHA-1-96 をサポートする

IP-SEC(ESP/AH) + IKE + HMAC-SHA-1-96

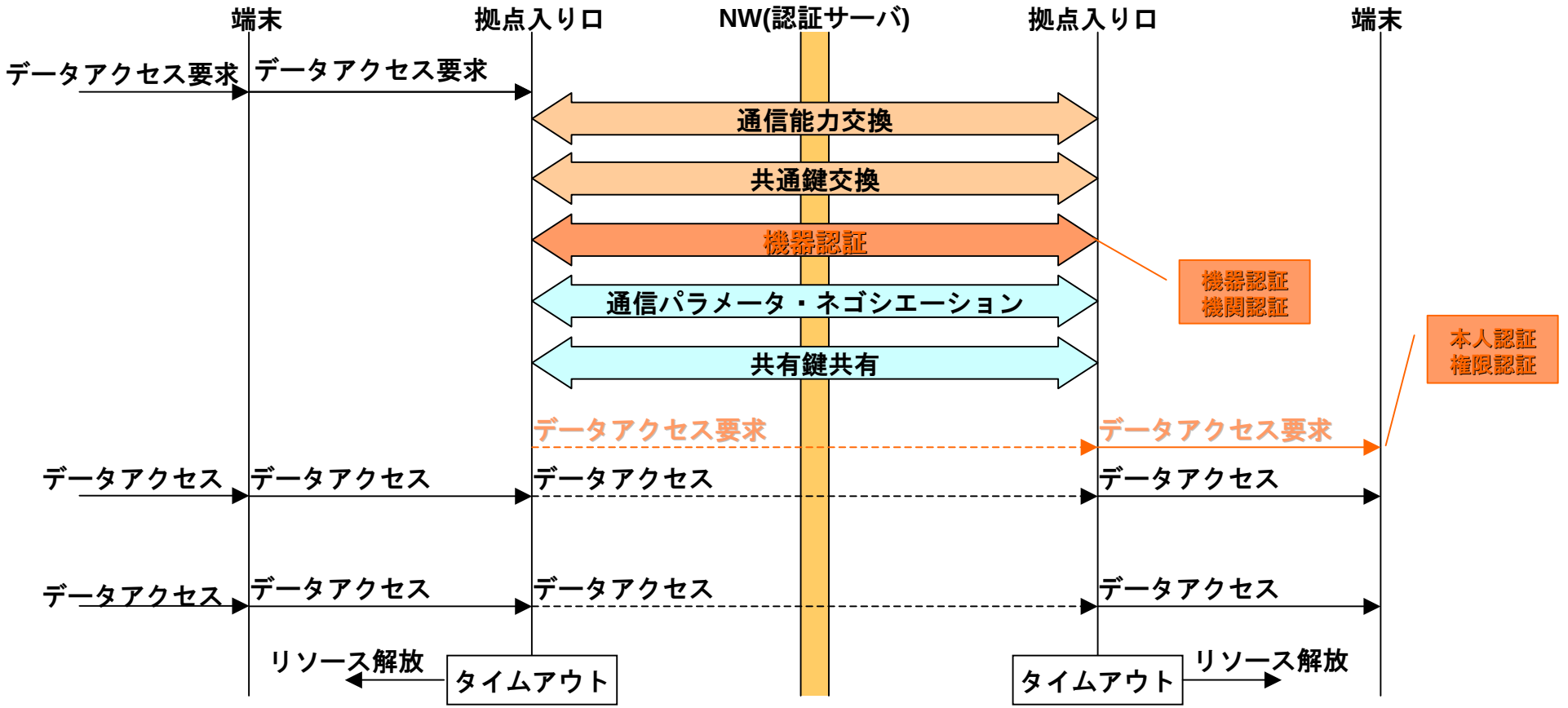
TTLの検証

証拠収集とアーカイビング

イングレスフィルタリング

Copyright© 2007 HEASNET

- 認証方式として、ID・パスワード(ワンタイムを含む)方式や共通鍵方式の脆弱性は指摘されているが、最も安全な公開鍵方式についても、認証対象の識別方法に対する安全な方式が未確立
- 端末間VPNは拠点の入り口がセキュリティホールになるため、拠点入り口での認証が重要(拠点間VPNは、複数の端末間でパスを共有する可能性があるため、拠点の機関認証が最低条件)
- なりすまし対策に関する端末間での通信は、リソースアクセスの権限認証を含めてユーザ認証が必須だが、ユーザや機器のなりすましを防ぐ手段が未確立



Copyright© 2007 HEASNET

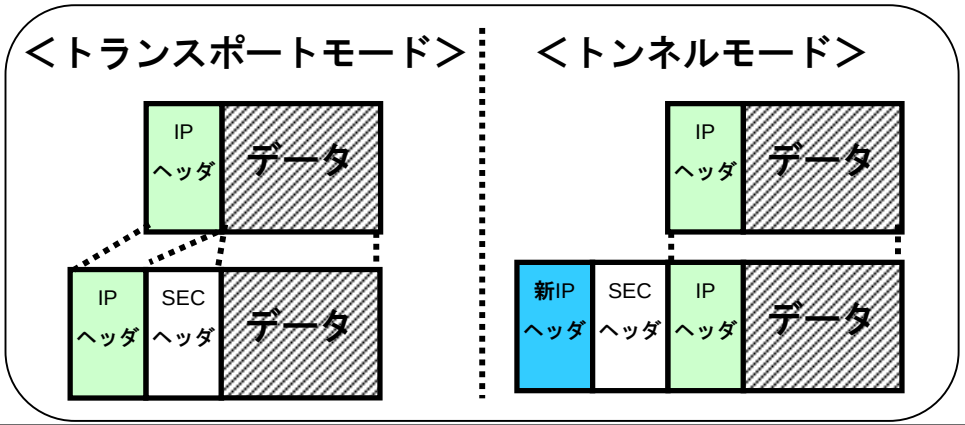
IP-SEC

トラフィックセキュリティを確保するためには、IP-SECが有効な技術である。IP-SEC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)

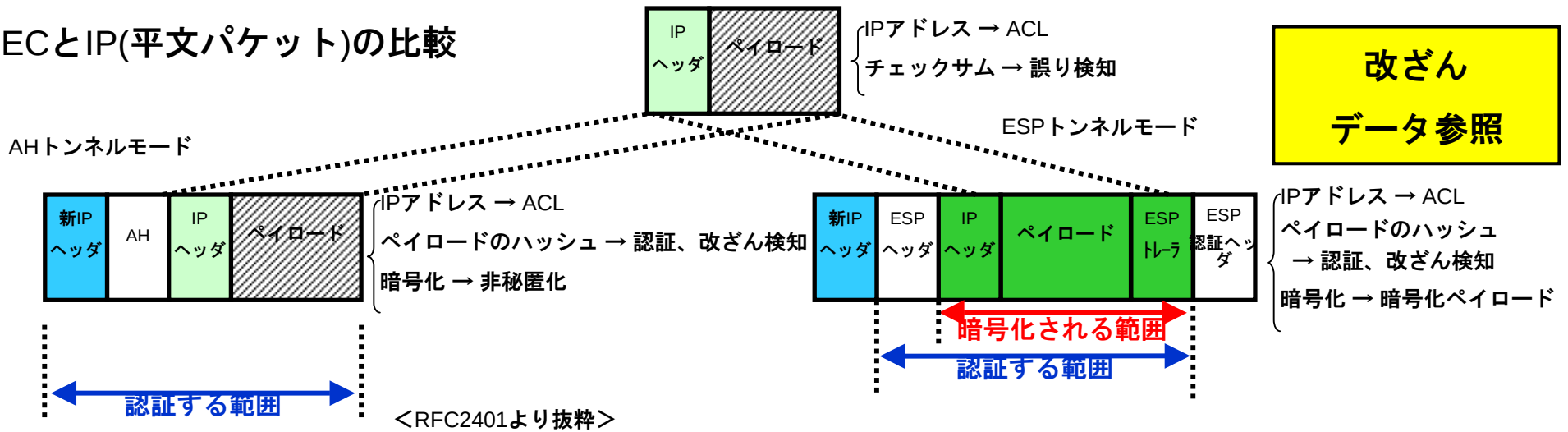
[IP-SECのモード]

トランスポート・モード：
元のIPデータグラムのデータ部だけが保護対象

トンネル・モード：
元のIPデータグラム全体が保護対象



IP-SECとIP(平文パケット)の比較

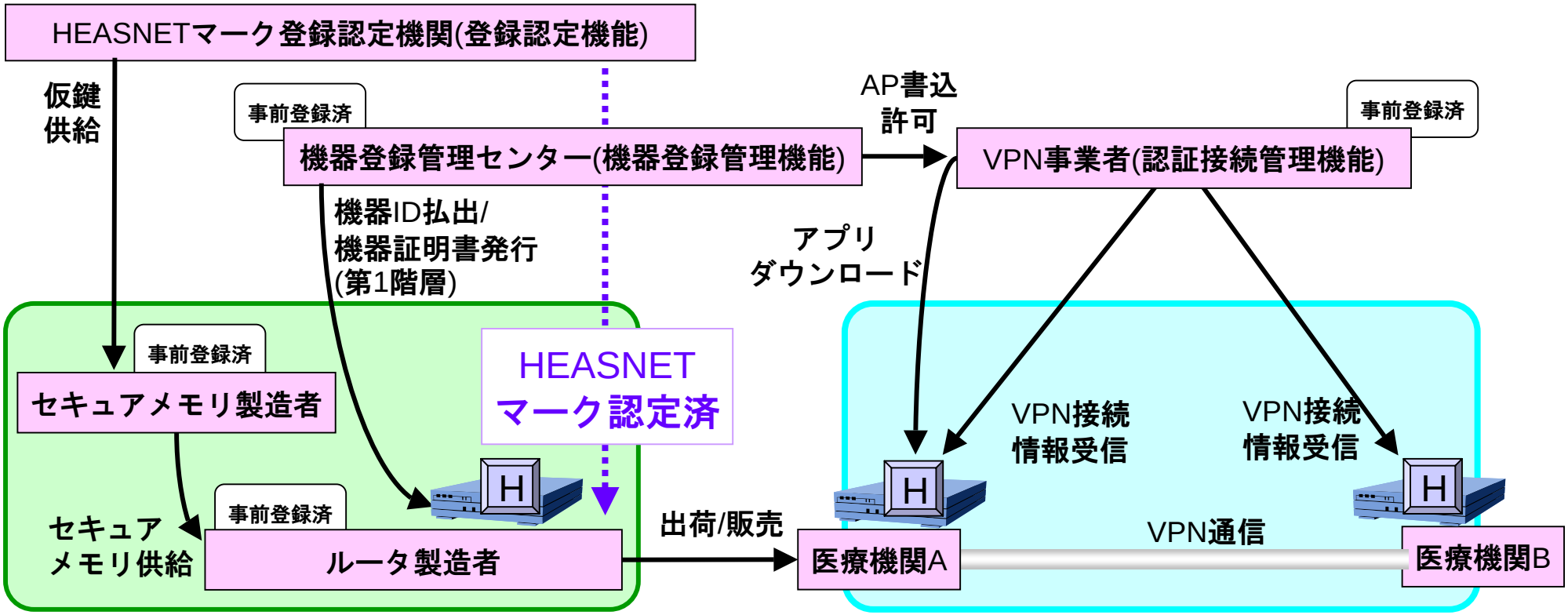


＜RFC2401より抜粋＞

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)。

Copyright© 2007 HEASNET

ネットワーク機器のなりすまし対策



①セキュアメモリの正当性を確認
②電子署名付の機器情報を書込
③機器登録管理センターに機器情報を登録
④機器ID、鍵ペア、機器証明書を格納

①１階層目の証明書の保護
②２階層目の証明書を格納
③アプリのダウンロード
④VPN接続要求
⑤VPN接続パラメータの取得
⑥VPN接続パラメータをもとにIKEによる鍵交換
⑦交換したセッション鍵による暗号化通信開始
⑧通信が終了次第通信切断、セッション鍵削除

ルータの製造・出荷にかかわる運用ルール

NICSSフレームワークを参考に、機器の製造・出荷の運用に関する運用ルールを中心に検討する。

ルータのセキュリティ機能

通信時におけるインターネット上の脅威への対応や2階層PKI技術を活用する際に機器に求められる機能を中心に検討する。

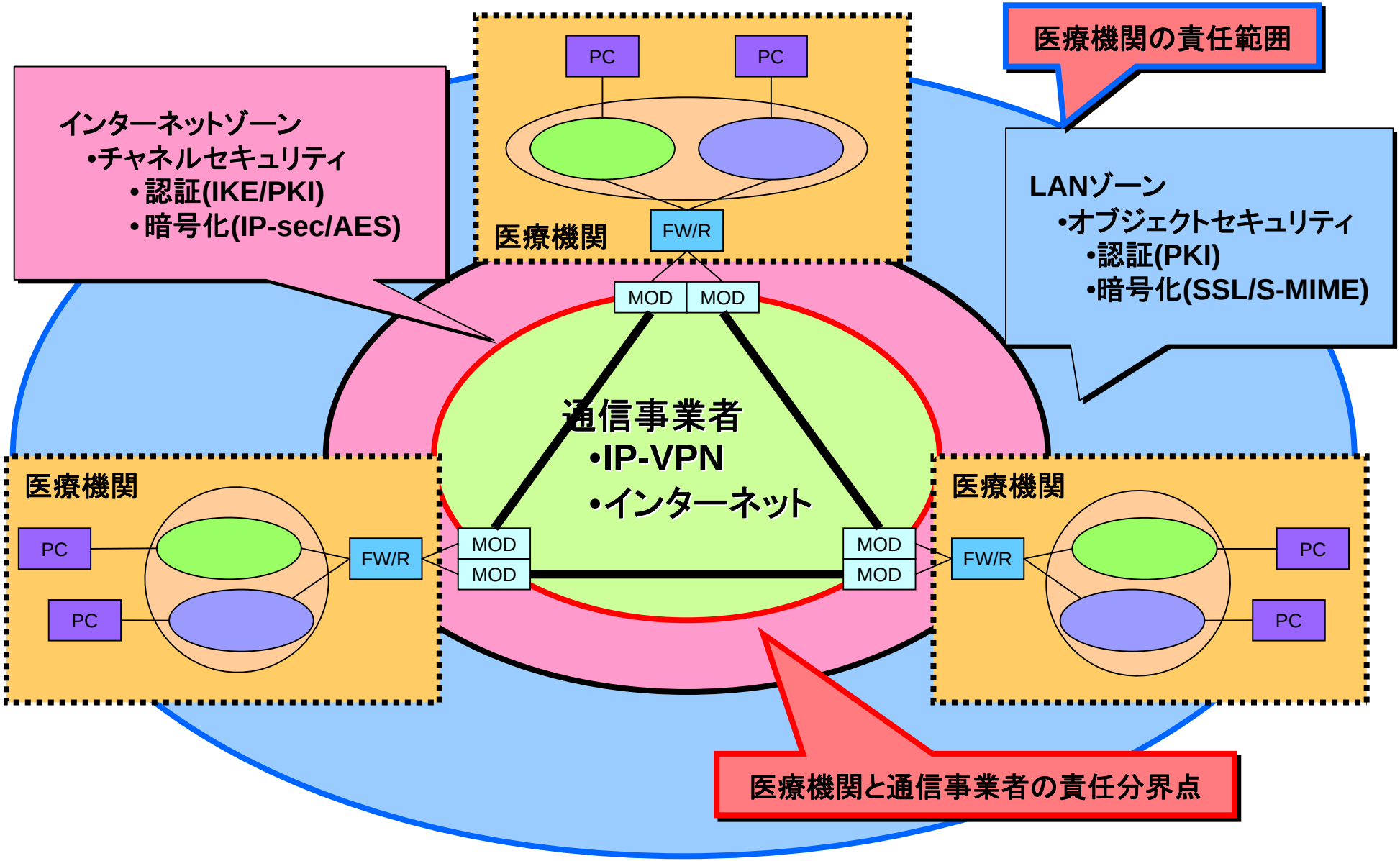
Copyright© 2007 HEASNET

HEASNETの提唱するオンデマンドVPN

比較項目	オンデマンドVPN	IP-VPN(MPLS)	インターネットVPN(IP-SEC)	SSL／TLS-VPN
データの機密性	ネットワーク層(IPプロトコル)	通信事業者が独自に構築した閉域IP網	ネットワーク層(IPプロトコル)	セッション層/トランスポート層(HTTP、FTPなどAPに依存)
品質保証	ベストエフォート型	帯域保証型(サービスにより保証値は異なる)	ベストエフォート型	追加設定不要
拠点追加等の設定変更の容易性	ネットワークで鍵配送	追加設定不要	接続先設定について、各拠点での変更作業必要	追加設定不要
機器認証	2階層PKIの第一階層目の証明書で認証	なし(ISP事業者のIP網の構成自体の信頼性に依存)	拠点の機器による相互認証	サーバ証明書にて認証
利用者認証	2階層PKIの第二階層目の証明書で認証	なし	なし	電子証明書を利用したサーバ・クライアントの相互認証
対象者	キャリアフリー プロバイダフリー	キャリアが限定される	キャリアフリー プロバイダ限定の可能性	キャリアフリー プロバイダ限定の可能性

Copyright© 2007 HEASNET

セキュアネットワーク基盤と責任分界点



Copyright© 2007 HEASNET

異なる法人間でVPN接続を行う際に考慮すべき事項(ガイドライン)として、オンラインレセプトガイドライン、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等の脆弱性、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諸条件を検証する。

①経路分離

②経路制御

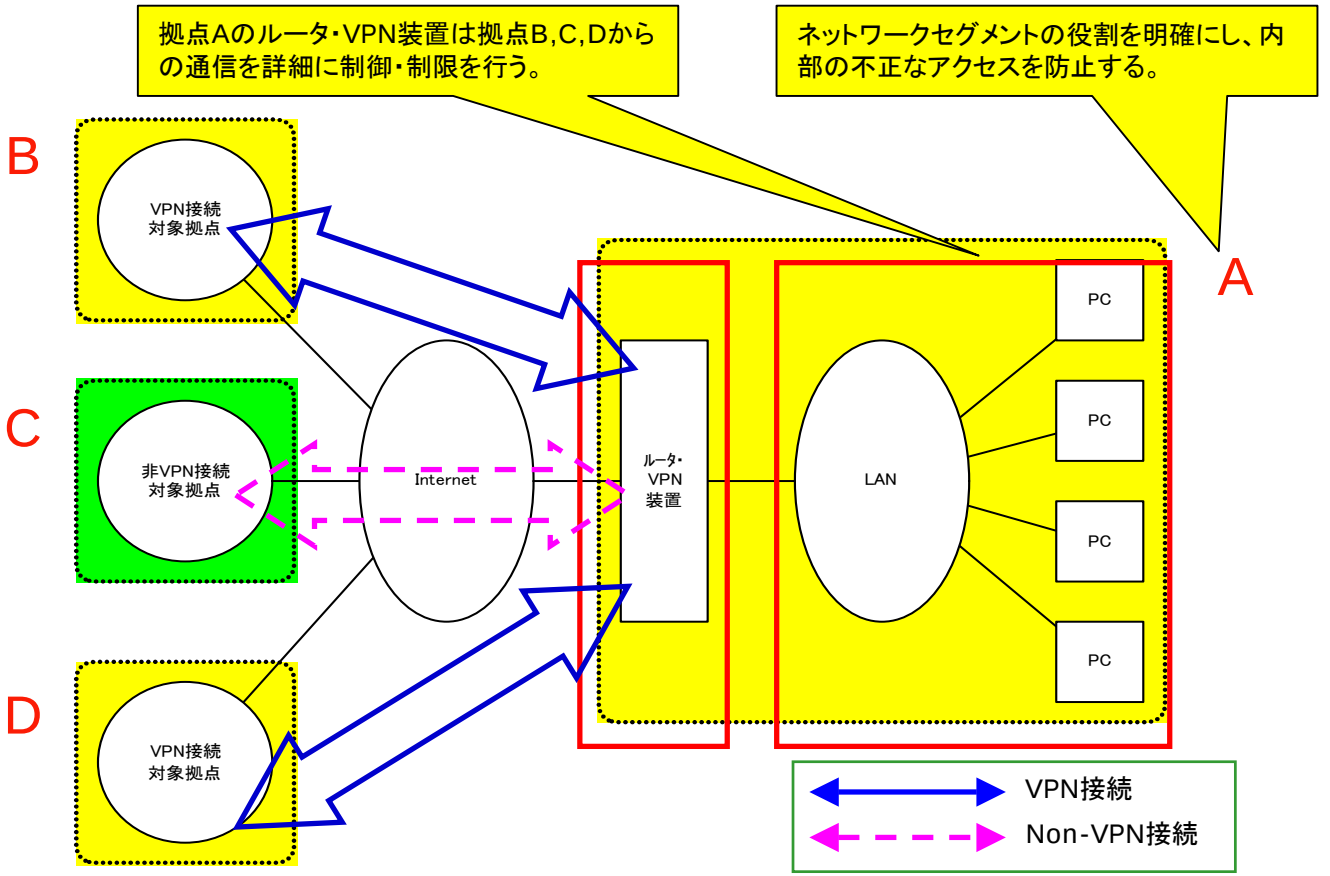
③不正中継禁止

④セグメントの分離

Copyright© 2007 HEASNET

一般的なVPN接続

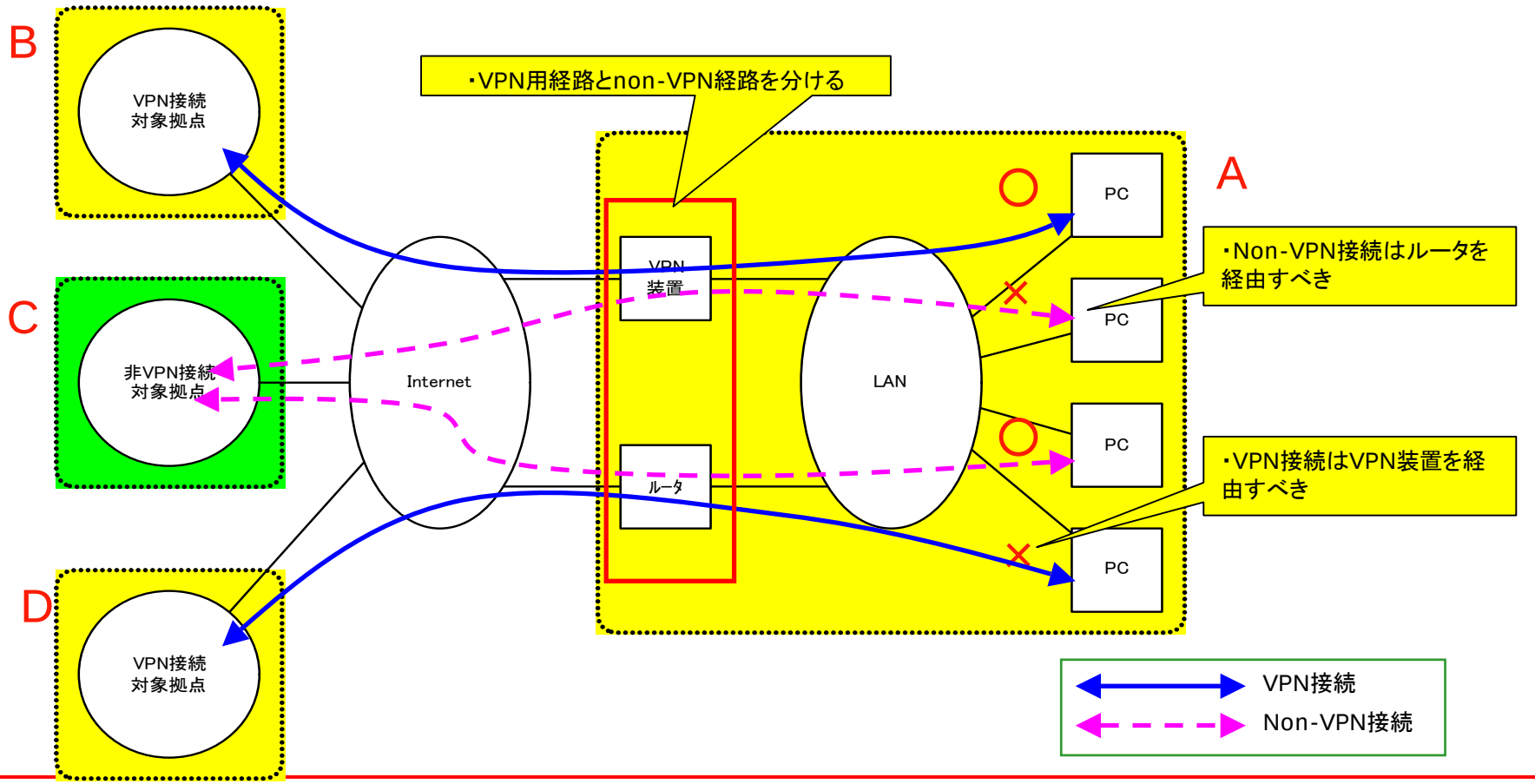
通常、企業で用いられるVPNの接続は拠点間のLAN間VPNである。拠点A,B,D間は基本的に通信が管理されていない。各拠点のVPN装置はローカルリソースとリモート続先のセキュリティを確保するために、経路やセグメントに制御・制限を施す必要がある。



Copyright© 2007 HEASNET

VPN、non-VPN接続の経路分離

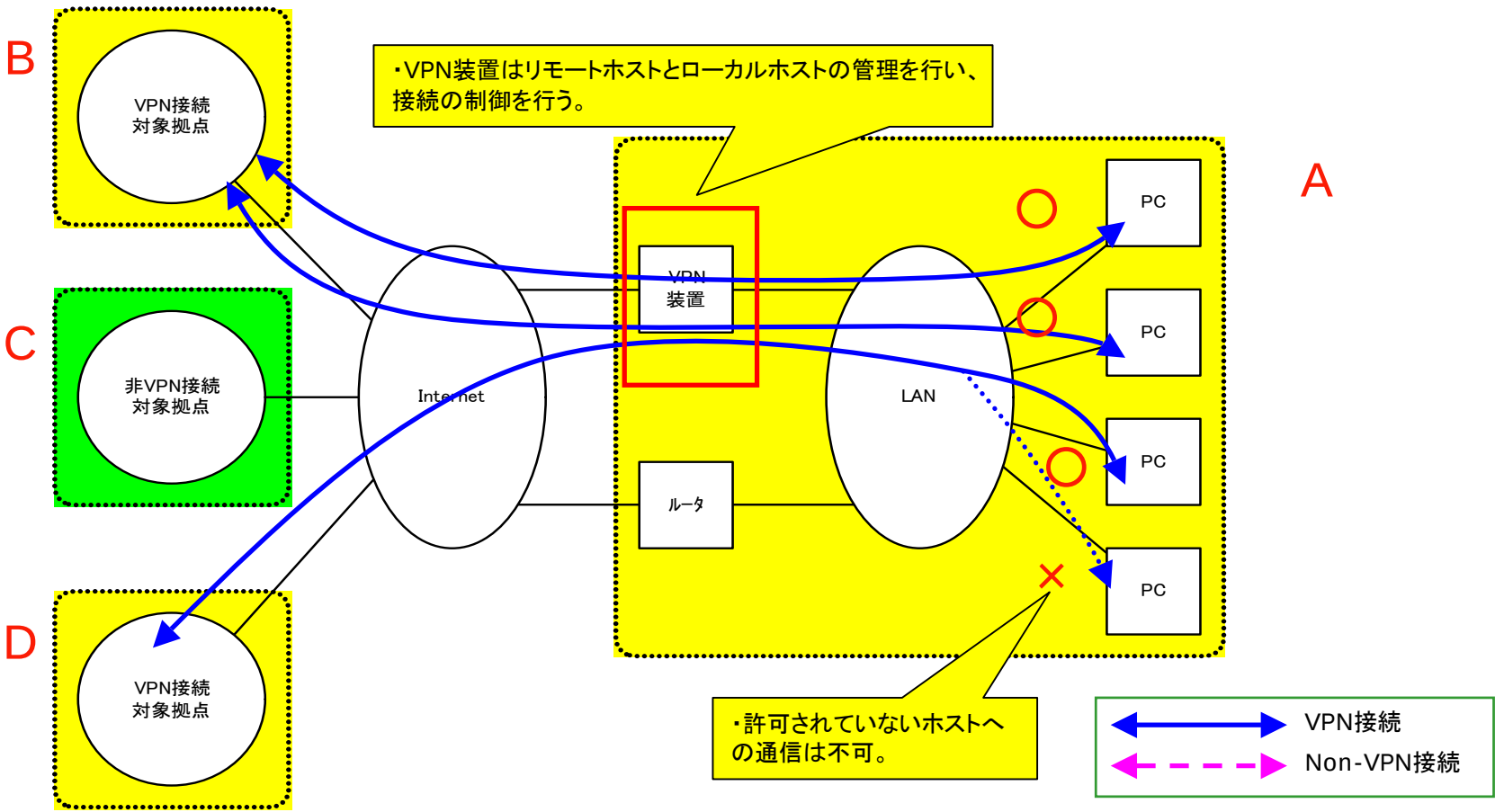
インターネット接続点において、VPN接続とnon-VPN接続とで経路を物理的に分離する。通信ルートを分けることで外部からの不正なアクセスを防止し、VPN接続のセキュアな経路を確保する。



Copyright© 2007 HEASNET

異なるVPN間の経路制御

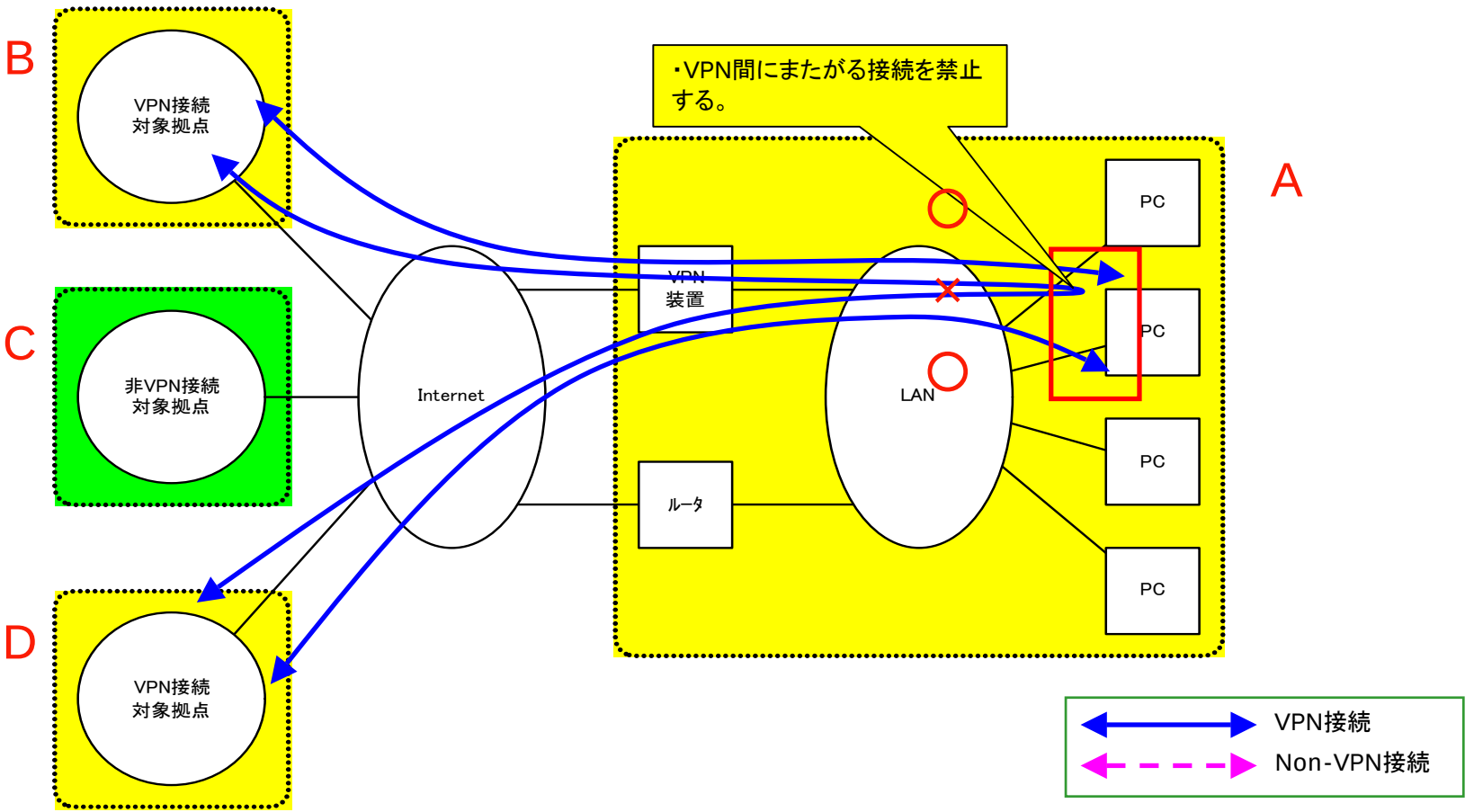
VPN装置においてリモート拠点ホストからの接続を、ローカル拠点のホストまたはIPアドレスレベルで制御し、VPN接続に対して制限を設ける。Peer-to-PeerでVPN接続制御を実現する。



Copyright© 2007 HEASNET

VPN間の不正中継防止

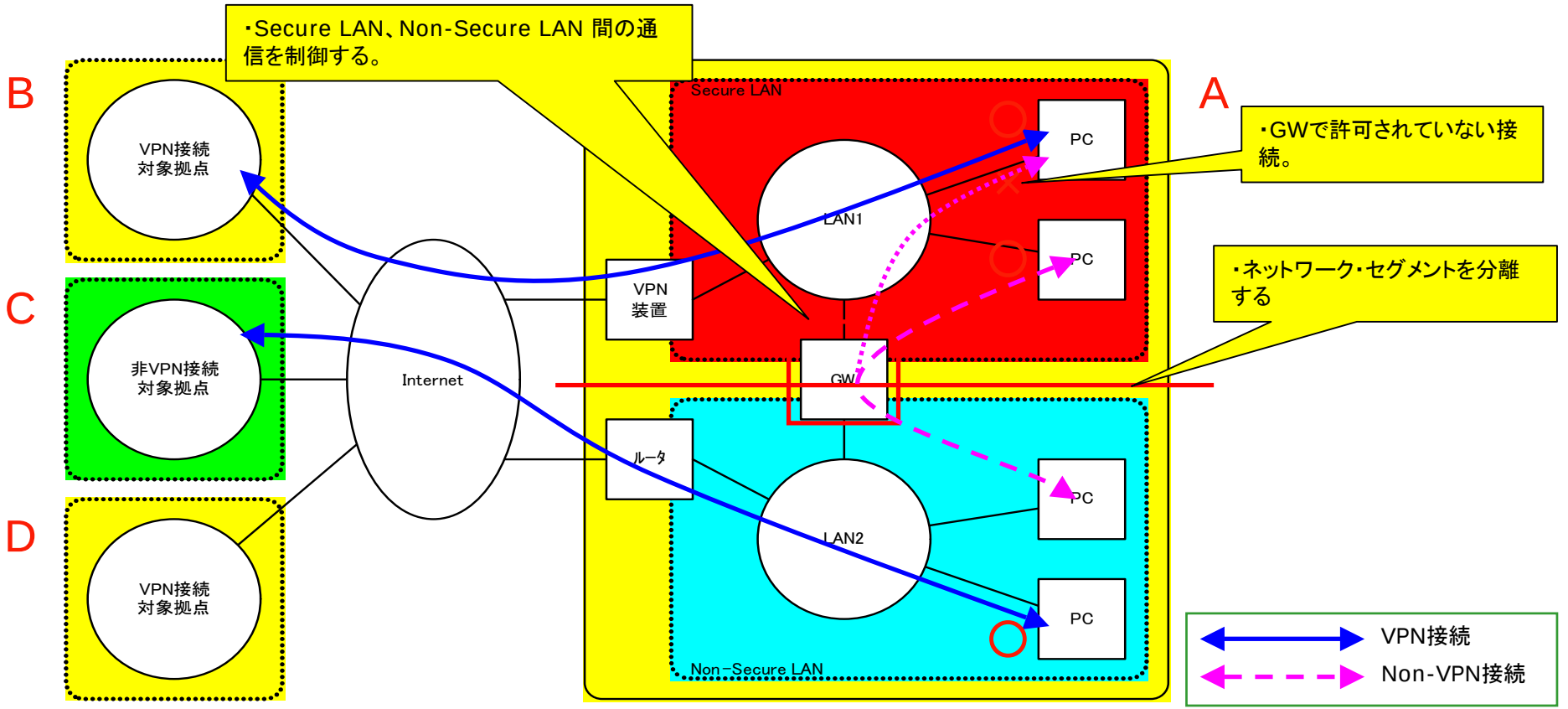
許可されていないVPN接続(B,D間)をある拠点(A)を経由しての接続は不可。不正な中継アクセスを防止する。



Copyright© 2007 HEASNET

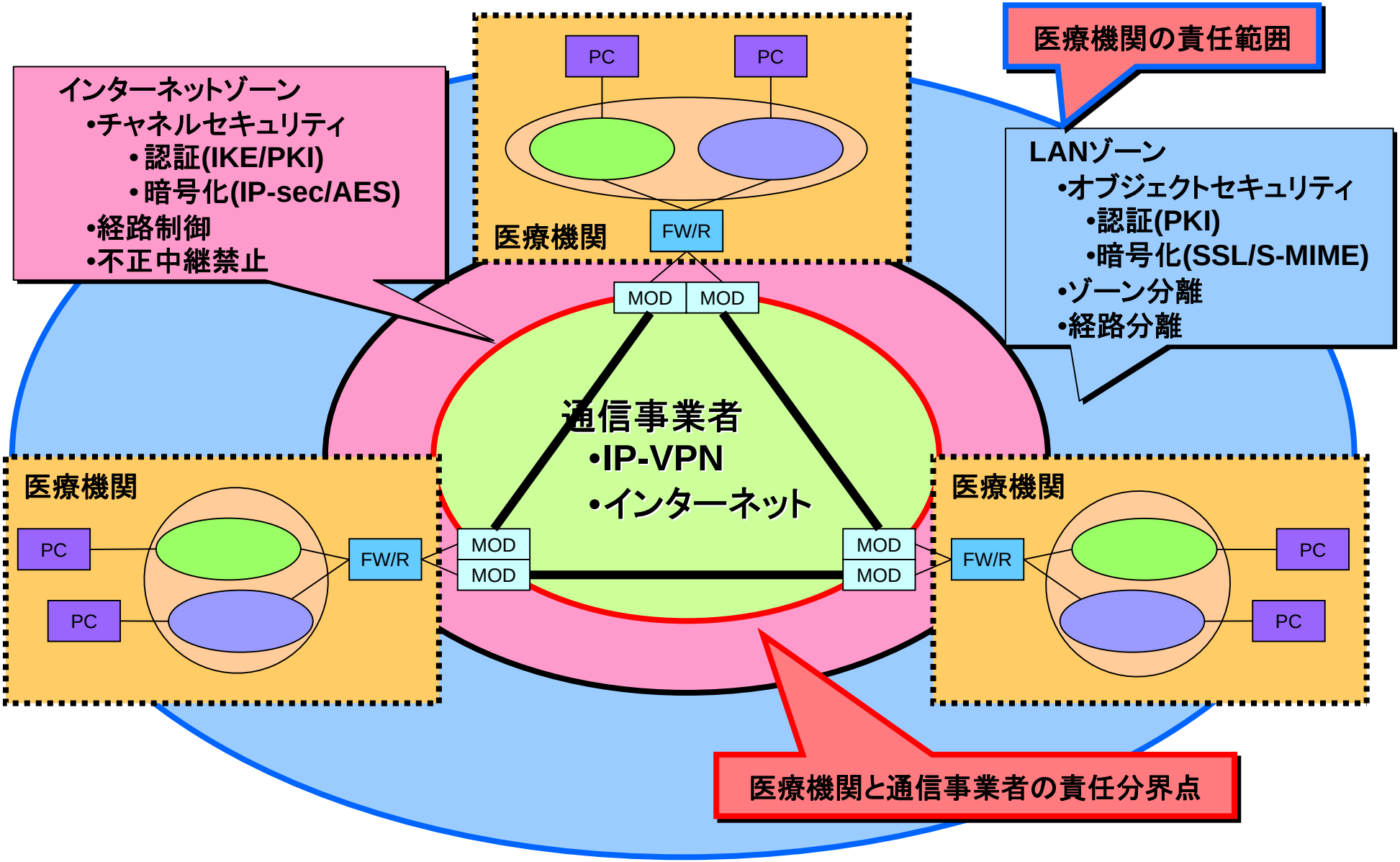
VPN接続とnon-VPN接続の分離

VPN接続専用ネットワーク(Secure LAN)を他のネットワーク(Non-Secure LAN)と分離し、Secure LAN内のPCからはインターネット接続を禁止する。またSecure LAN、Non-Secure LAN 間での通信を制御・制限することで、VPN接続を行うPCをローカルエリアからの不正なアクセスを防ぐ。



Copyright© 2007 HEASNET

セキュアネットワーク基盤と責任分界点



Copyright© 2007 HEASNET

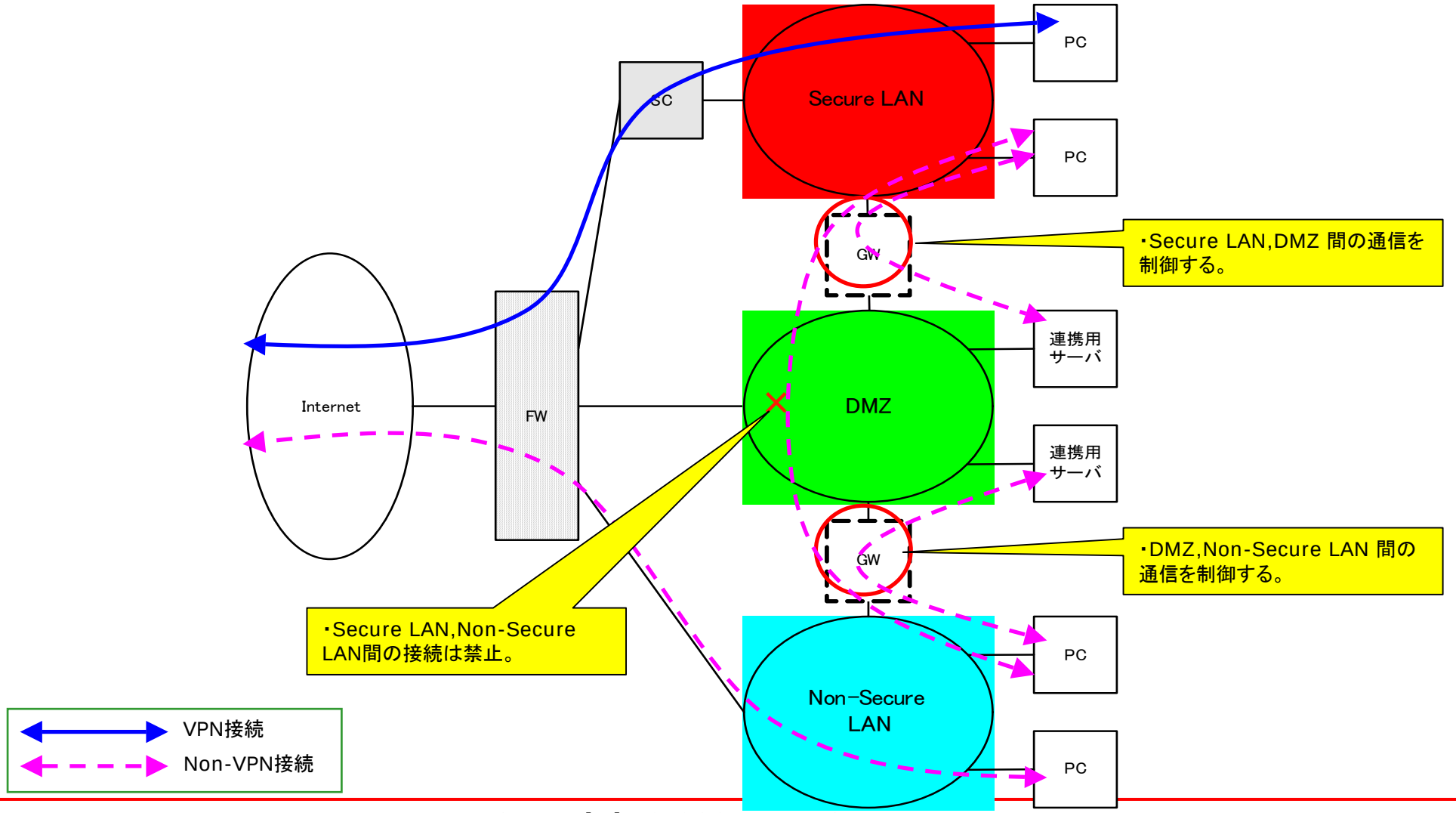
要件の整理・実例の検証から、ネットワークトポロジーのパターンとネットワークセグメントの構成ポリシーを次のように決めた。

ネットワーク･トポロジー
- サービスプロバイダ型
- 大規模機関型
- 小規模機関型

ネットワークセグメント
- High Secure LAN
- Secure LAN
- DMZ

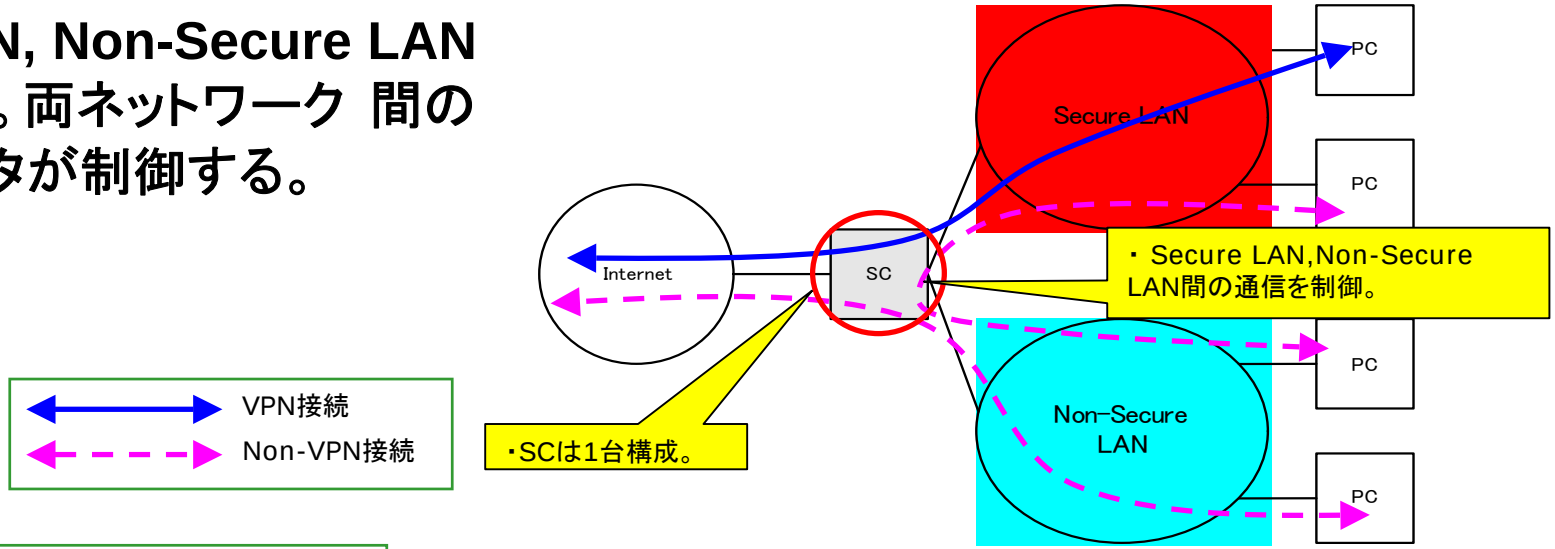
Copyright© 2007 HEASNET

Secure LAN, DMZ, Non-Secure LAN を並列構成にする。各セグメント間の通信はゲートウェイで制御する。

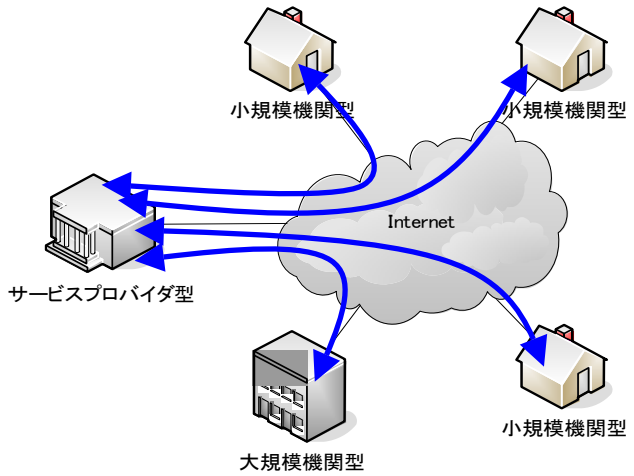


Copyright© 2007 HEASNET

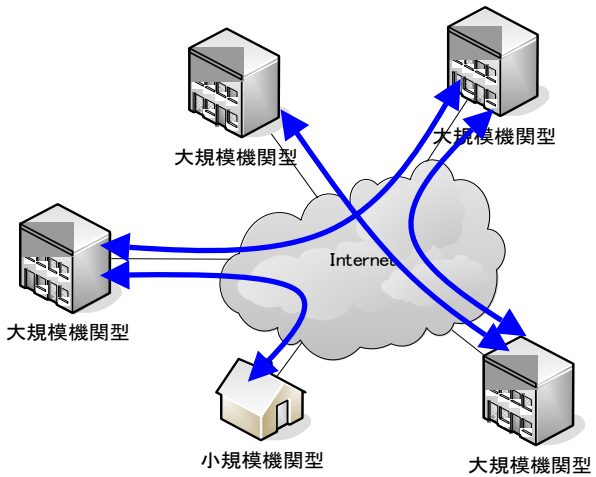
Secure LAN, Non-Secure LAN のみの構成。両ネットワーク 間の通信はルータが制御する。



モデルの接続イメージ



各拠点からスター型に接続するタイプ

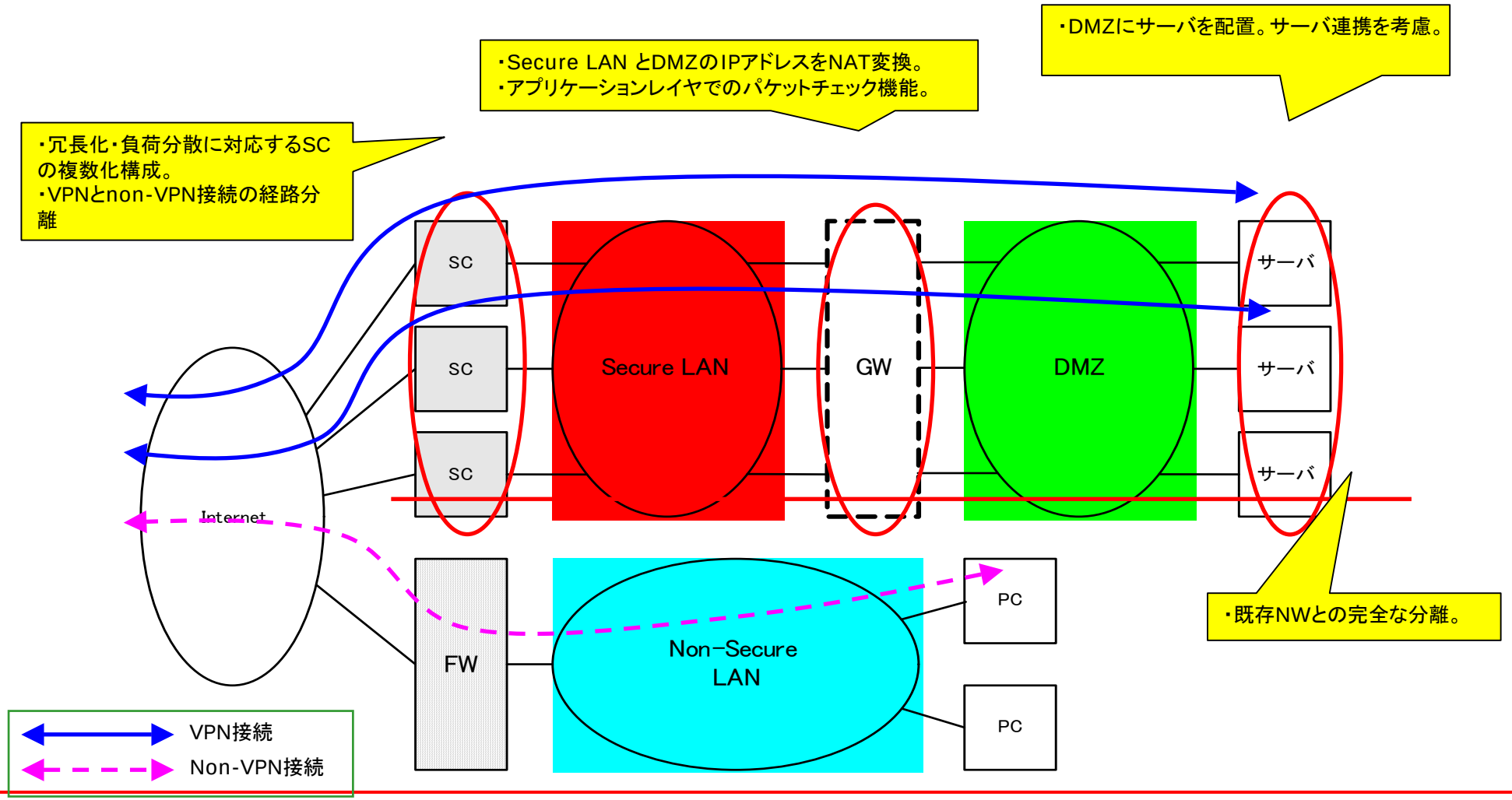


各拠点からメッシュ型に接続するタイプ

Copyright© 2007 HEASNET

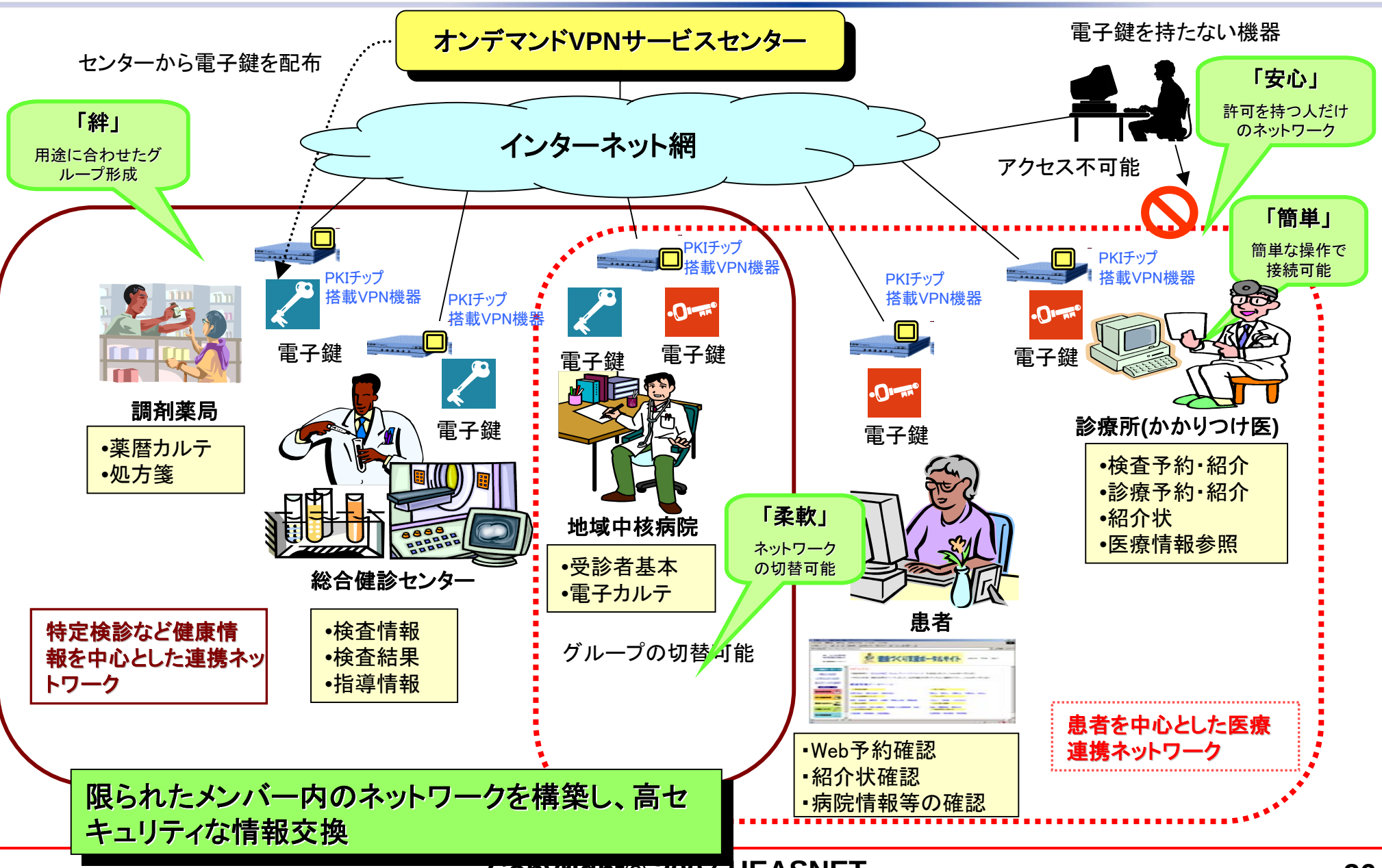
サービスプロバイダ型

Secure LAN と DMZ を縦列構成にする。Secure LAN 上にホストを配置せず、SC VPN接続管理を行いゲートウェイでパケットチェック・DMZ内の通信管理を行う。



Copyright© 2007 HEASNET

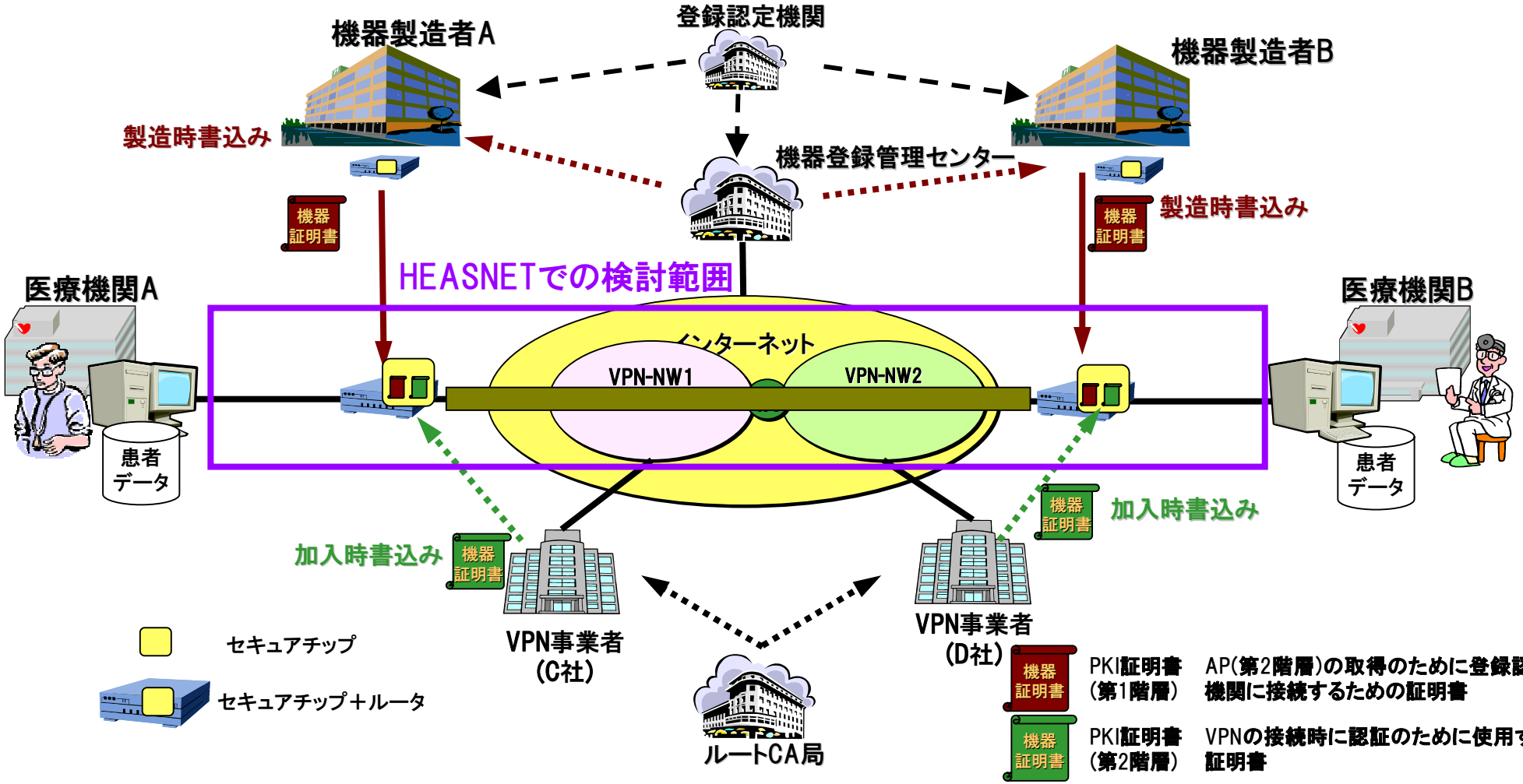
オンデマンドVPNの全体像



Copyright© 2007 HEASNET

インターオペラビリティの確保

HEASNETでは、異なるオンデマンドVPN事業者と契約したユーザ間で、またユーザの同じ端末から複数の医療サービスやメンテナンスが利用できる環境を確保するため、ンターオペラビリティを確保するための相互接続仕様を定義した。



Copyright© 2007 HEASNET

使用目的:
対象となる機関や施設のNWセキュリティの「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」への準拠度を診断する

活用方法:
医療機関の「NW管理者」が責任を持ち、NW全体の設計や構築を行った「ベンダ」や回線事業者、オンラインサービス提供事業者にあたる「SP」と協同でチェックシートを用いて各自の提供できる機能を明確に3者間の責任の分界点や所在を明確にしておくこと

注意点:
機関型式でチェック項目が変わる
(大規模機関型、小規模機関型、SP型)

Copyright© 2007 HEASNET

ご清聴ありがとうございました。

Copyright© 2007 HEASNET