補足事項 1

稼働中の医療情報ネットワークの実例検証

< 目　　次 >

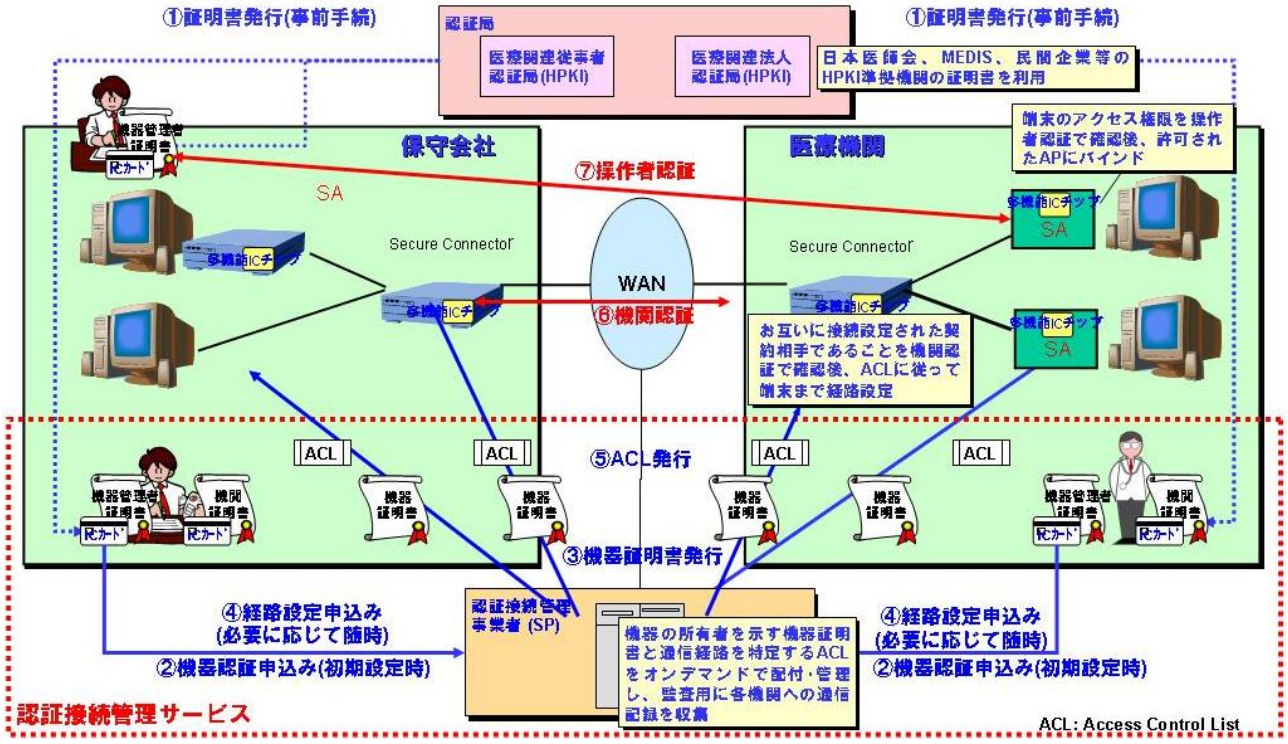
1.適用技術仕様

1.1 HEASNET仕様

HEASNET 仕様は、「オンデマンド VPN(HEASNET 版) 技術仕様書 基本編」(HEASNET, 2007 年 2 月 13 日, ver.1.0)を参照のこと。

1.2 NTT-PC仕様

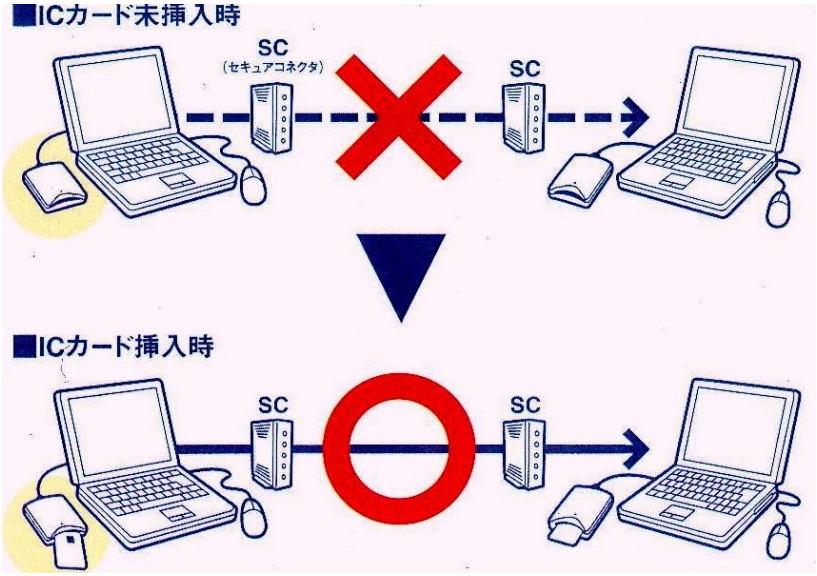
HEASNET 仕様に基いて NTT-PC 社が実装している技術のシステムイメージを以下に示す。



システムの特徴を資料から抜粋する。

(1) 簡単にオンデマンドに張れるVPN

IP-Members は、2 階層 PKI モデルに基づいて SC(セキュアコネクタ)に内蔵されたセキュアチップに秘密鍵や接続先の PKI 証明書やアクセス制御リストを格納しており、さらに認証接続管理サーバと連動してこれらの鍵の管理や接続設定を行っています。これにより、面倒な作業を行わず、高セキュリティなオンデマンド VPN がいつでも簡単に構築することが可能です。



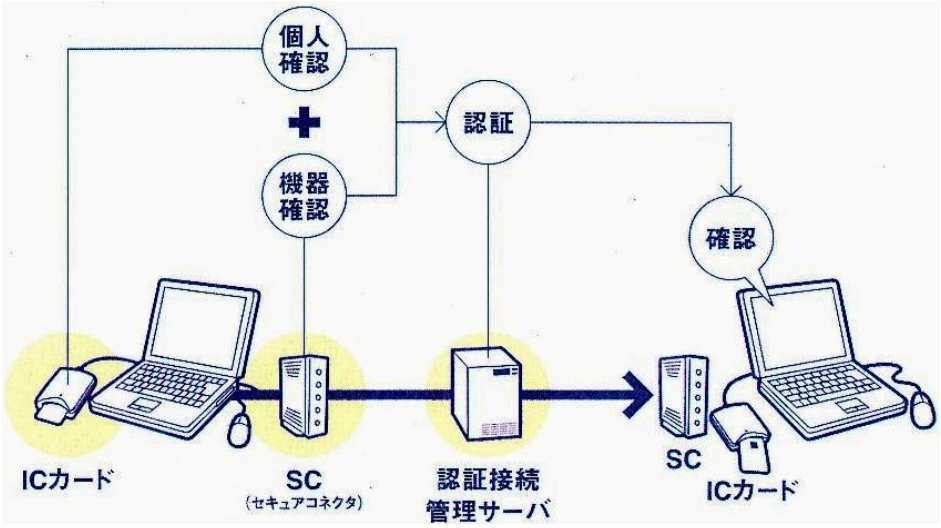
(2) 操作者及び機器の限定で万全のなりすまし対策

【操作者の特定】

操作者の個人情報を基に発行された PKI 証明書を IC カードに格納して IP-Members で利用できるため、ネットワークを利用する操作者の特定が容易にできます。

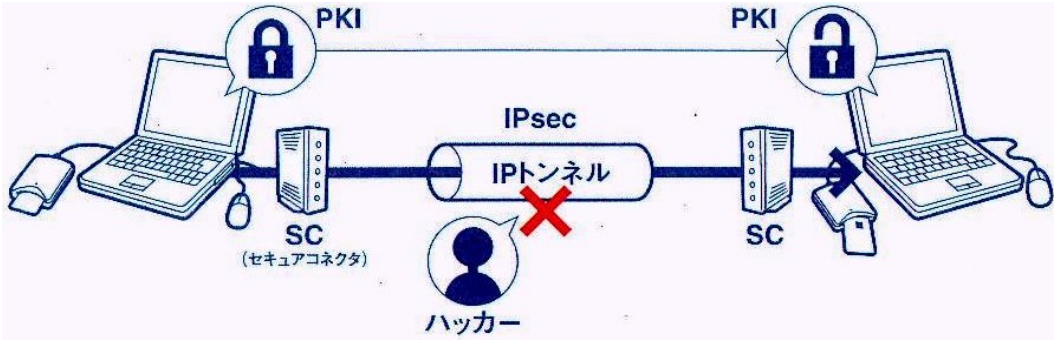
【機器の限定】

SC 内蔵のセキュアチップには、「機器証明書」が入っているため、不正なルータの介入を阻止することができます。LAN 内の端末に認証接続管理サーバからエクストラネット用の IP アドレスを自動付与し、SC が端末の MAC アドレスも管理するため、機器のなりすましも行えません。



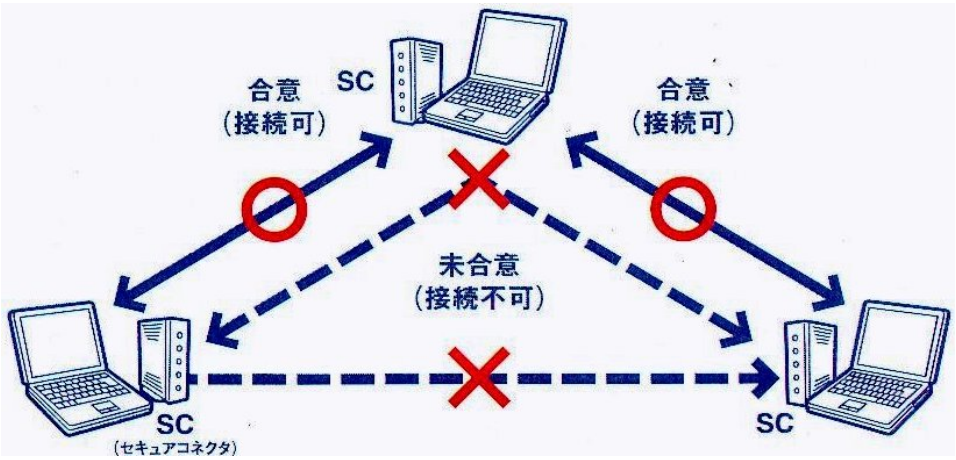
(3) IPsec+IKE+PKI方式による認証

セッション単位に IKE で PKI 認証して暗号化の鍵交換するオンデマンド VPN 接続を行っており、さらに IPsec を利用して通信経路で暗号化やメッセージ認証等のハッカー対策を行っていますので、インターネットのどのような経路を通過してもハッカーの攻撃や暗号解読作業が困難になります。このため、マルチキャリア、マルチ ISP でもメッシュ型接続が可能になります。



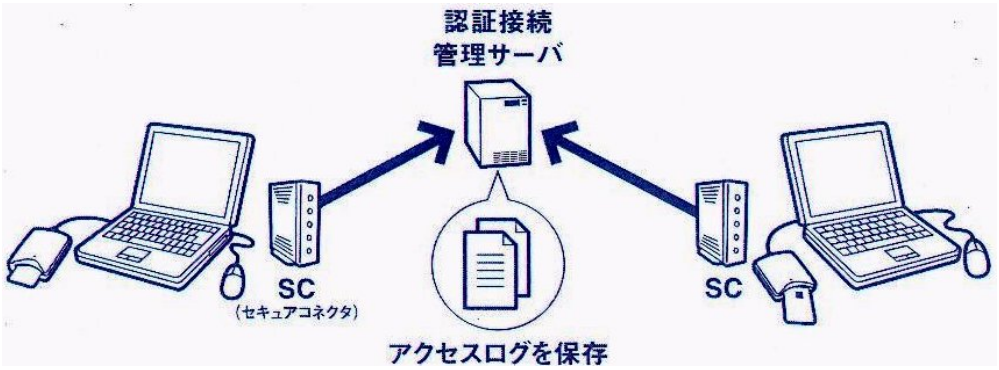
(4) アクセスコントロール

従来の静的なネットワーク構成では、1)企業間の通信ポリシー設定に多大なリソースを消費する、2)コストを下げるために通信ポリシーを簡易にしてネットワークにセキュリティホールが発生し易い、などの問題がありました。IP-Members は、最も厳しい通信ポリシーをベースに双方の合意形成に沿ってアクセス制御や鍵の管理を行うため、厳密なアクセスコントロールにより未合意の接続先からアクセスや接続先の異なる VPN 間での渡りは不可能になります。



(5) IP-Membersにおける監査ログ

IP-Members は、定期的に時刻合せをしたタイマと PKI 証明書に基づいた情報から作成したログを認証接続管理サーバに保管しています。これらのログは、内部統制やシステム監査等の要件に合った監査ログとして使用可能で、IC カードにより操作者が特定されるので、ネットワークを利用した操作者のトレースも容易に行えます。このため、「いつ、誰が、どこから、どこへ」アクセスした、といった精緻な情報を下に問題発生の原因分析が簡単に行え、早期の問題解決を可能にします。



① グローバルIPアドレス

SCのWAN側ポートには固定IPアドレスを付与する。初期設定後のアドレス変更は不可。

→グローバルIPとSC内チップとの紐付けることで経路を確保。

② サービス用指定IPアドレス

SCのLAN側ポート・PC(サービス対象機器)はサービス用指定IPアドレス(10.x.x.x)を付与する。既存NWとは別セグメントであり独立に存在する。

→Secure LAN。既存IPアドレスとの調停を図る。

③ MACアドレス

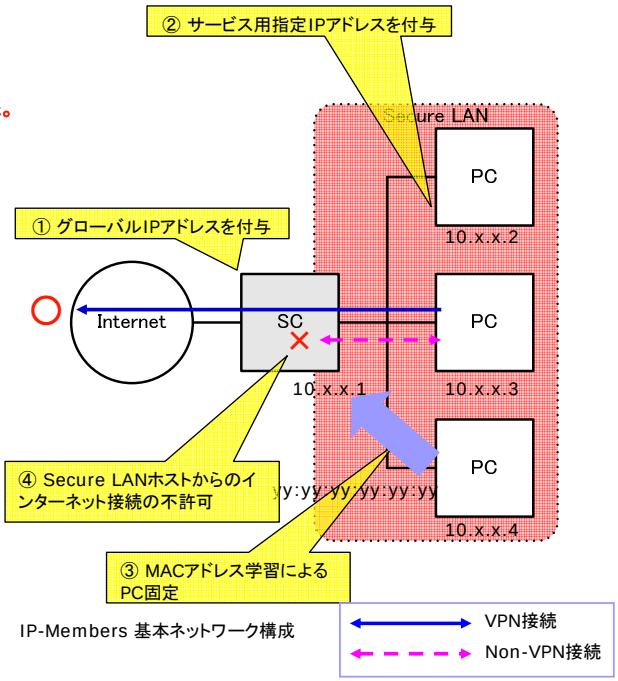
PC初回接続時、SCのMACアドレス学習によって機器固定をする。サービス対象機器の取替えは不可。

→PCの不正な付替え・成りすまし防止。導入時に利用する端末を選定する。

④ インターネット接続不可

VPN接続以外のインターネット通信は許可しない。

→不特定多数ネットワーク接続の禁止。SCでフィルターされる。



1.3 NTT-DATA仕様

2.実用事例

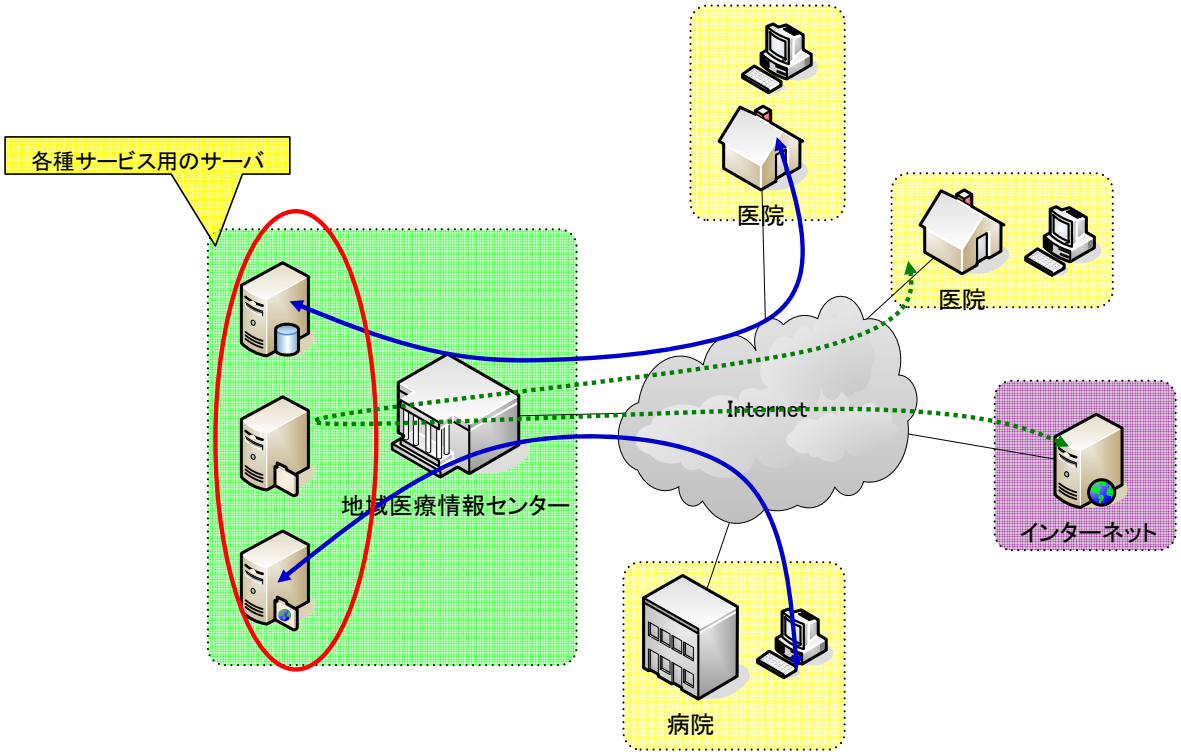
本章では、HEASNET 仕様に基いて実際に運用されている事例を紹介するとともに報告書にあるチェックシートに基いてネットワークセキュリティを評価してみる。

2.1 NTT-PC仕様の事例

2.1.1 K地域連携NW

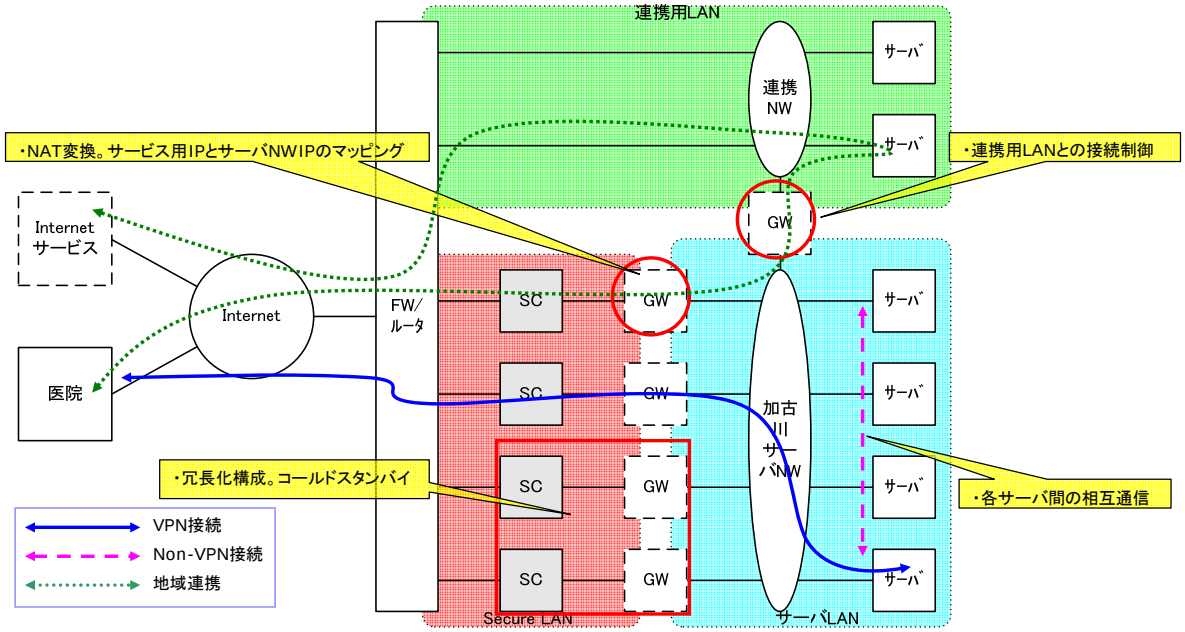
(1) サービス概要

K 地域連携 NW は、情報センターと地域の医療施設が連携するネットワークを構築している。情報センターに共有・サービス用のサーバを構築し、各医院・病院がアクセスする、クライアント・サーバ型を展開している。



(2) ネットワーク概要

サーバ用ネットワークと Secure LAN をゲートウェイ(GW)で接続。サーバ相互通信と SC の複数化により冗長性と負荷分散を実現している。



(3) チェック結果

報告書のチェックシートに合わせて各拠点の状況を精査する。

K 情報センター（サービスプロバイダ）

目的対象	項目	機能要素	チェック	備考
1. 通信形態				
1-1 接続相手の確認	1-1-1 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。 本資料「2.2 セキュリティに関するガイドライン」
	1-1-2 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？	-	はい	
2. 通信ポリシー				
2-1 オープンネットワークの利用した拠点間の接続	2-1-1 不正な中継を禁止していますか？	VPN 機能	はい	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。 本資料「5.1 法人間の接続における留意点」
	2-1-2 IKE でユーザ認証を行っていますか？	VPN 機能	はい	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。 本資料「4.2 脅威への対処技術」
	2-1-3 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	はい	
	2-1-4 セッション毎に共通鍵を自動決定していますか？	VPN 機能	はい	
	2-1-5 IPSec による暗号化を行っていますか？	VPN 機能	はい	
	2-1-6 IPSec でメッセージ認証を行っていますか？	VPN 機能	はい	
2-2 他拠点との接続処理	2-2-1 接続先拠点と通信に関して合意がなされていますか？	-	はい	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 他拠点への接続先をアドレス・ポート等で制限していま	VPN 機能	はい	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

	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 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 ／プロキシ機能	はい	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 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 ／プロキシ機能	はい	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。 本資料「2.2 (3)SPC 要件」
3. 拠点内のセキュリティ				
3-1 ホストの配置 役割	3-1-1 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。 本資料「5.3.1 通信モデルの定義」
	3-1-2 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	はい	
	3-1-3 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？	-	はい	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 外部からの脅威	3-2-1 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 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	はい	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 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	はい	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 High Secure Zone のセキュリティ	3-3-1 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 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 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 DMZ のセキュリティ	3-4-1 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	はい	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 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	はい	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 High Secure Zone と DMZ 間の通信	3-5-1 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 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 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 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 内部セキュリティサービス	3-6-1 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 プロキシ機能	はい	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 情報提供サービスの展開	4-1-1 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 各サーバ	はい	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	VPN 機能	はい	オープンネットワークにおける脅威（盗聴・侵入など）から

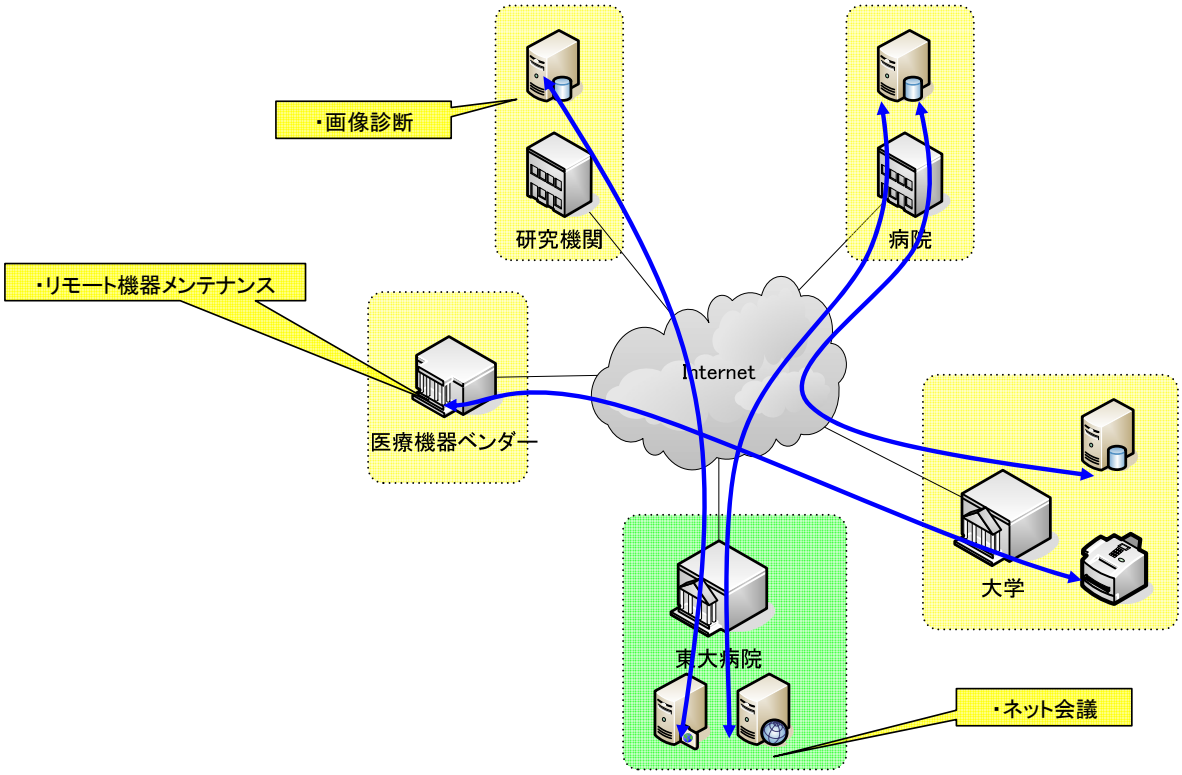
	医療機関向けに情報を公開・提供する場合、通信路を暗号化していますか？			パケットを守るために、それらに対応可能な技術対策を講じる必要がある。 本資料「4.2 脅威への対処技術」
	4-1-3 医療機関向けに情報を公開・提供する場合、ロギングを行いアクセス監視を行っていますか？	プロキシ機能	はい	ログは、発信元・アクセスポイント・アクセスされた場所の3箇所で取る必要がある。本項目は発信元・アクセスされた場所のロギングになる。 本資料「2.2 (3)SPC 要件」
	4-1-4 患者向けに情報を公開・提供する場合、ユーザ認証を行っていますか？	プロキシ機能 各サーバ	-	不正なユーザによるデータの閲覧を防ぐ。
	4-1-5 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 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 インターネット接続サービス	4-2-1 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	はい	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 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	はい	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 外部保存サービス	4-3-1 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 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 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。
	4-3-3 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。 本資料「5.3.1 通信モデルの定義」
4-4 メールサービス	4-4-1 メールのスクリーニングを行っていますか？	メール機能	はい	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 不正なメール転送を禁止していますか？	メール機能	はい	メール転送の踏み台になることを防ぐ。
4-5 リモート保守 サービス	4-5-1 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 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。

2.1.2 T大リモート実験NW

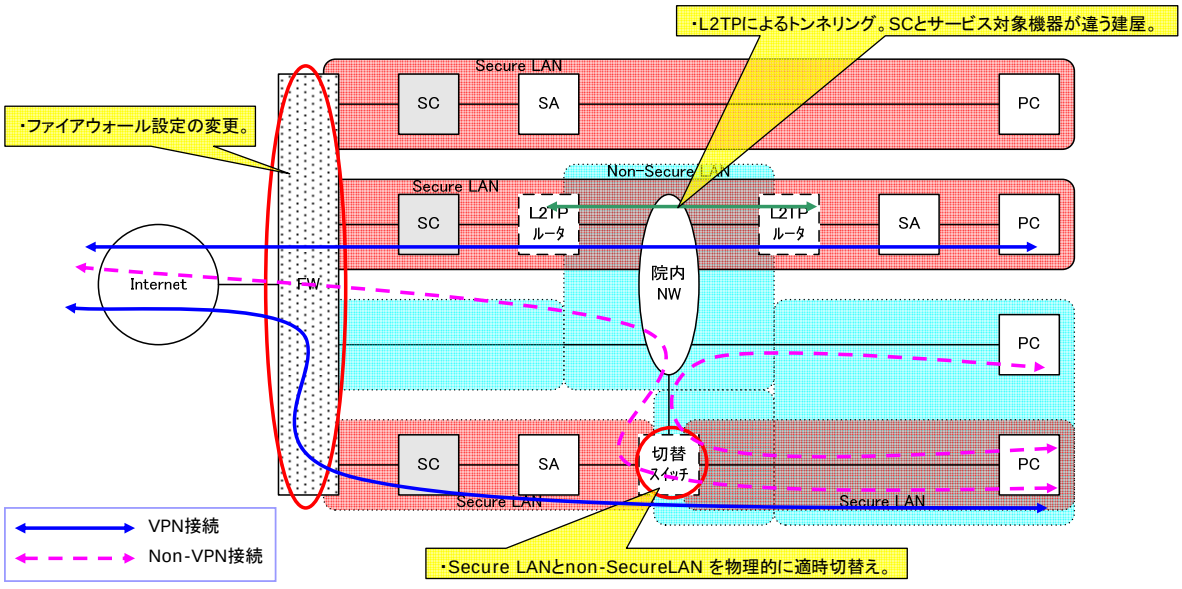
(1) サービス概要

T 大リモート実験 NW は、大学病院・研究機関・医療機器ベンダーが連携するネットワークを構築。ネット会議・画像診断・リモート機器メンテナンスなどのサービスを展開している。



(2) ネットワーク概要

T 大リモート実験 NW は、SC と SA の設置場所が離れているため、L2TP によってトンネリングしている。このため、SC 上位のファイアウォールにトンネル用の設定を変更してある。ネットワークは、物理的にネットワークを切替えるスイッチを用いて、院内ネットワークと Secure LAN を適時切り替えている。



(3) チェック結果

報告書のチェックシートに合わせて各拠点の状況を精査する。

T 大学病院 （大規模機関型）

目的対象	項目	機能要素	チェック	備考
1. 通信形態				
1-1 接続相手の確認	1-1-1 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。 本資料「2.2 セキュリティに関するガイドライン」
	1-1-2 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 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？	-	はい	
2. 通信ポリシー				
2-1 中継の確認	2-1-1 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	はい： 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」 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。 本チェックシート「2-3 接続処理の確認」に進む。
2-2 オープンネットワークの利用した拠点間の接続	2-2-1 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	はい	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。 本資料「5.1 法人間の接続における留意点」

	2-2-2 IKE でユーザ認証を行っていますか？	VPN 機能	はい	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。 本資料「4.2 脅威への対処技術」
	2-2-3 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	はい	
	2-2-4 セッション毎に共通鍵を自動決定していますか？	VPN 機能	はい	
	2-2-5 IPSec による暗号化を行っていますか？	VPN 機能	はい	
	2-2-6 IPSec でメッセージ認証を行っていますか？	VPN 機能	はい	
2-3 他拠点との接続処理	2-3-1 接続先拠点と通信に関して合意がなされていますか？	-	はい	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 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 ／プロキシ機能	はい	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 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 ／プロキシ機能	はい	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 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 ／プロキシ機能	はい	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。 本資料「2.2 (3)SPC 要件」
3. 拠点内のセキュリティ				
3-1 ホストの配置 役割	3-1-1 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	はい	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。 本資料「5.3.1 通信モデルの定義」
	3-1-2	Secure Zone	-	

	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？			
	3-1-3 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	はい	
3-2 外部からの脅威	3-2-1 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	はい	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 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	はい	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 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	はい	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 High Secure Zone のセキュリティ	3-3-1 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	はい	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 インターネット接続を禁止していますか？	プロキシ機能	はい	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 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	はい	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 Secure Zone のセキュリティ	3-4-1 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。 High Secure Zone からの重要データの内部情報漏えい防ぐ。
	3-4-2 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 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 DMZ のセキュリティ	3-5-1 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	はい	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 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	はい	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 High Secure Zone と Secure Zone 間の通信	3-6-1 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 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 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 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 High Secure Zone と DMZ 間の通信	3-7-1 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	はい	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 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	はい	「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 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 プロキシ機能	はい	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 DMZ と Secure Zone 間の通信	3-8-1 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 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。
	3-8-3 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 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。

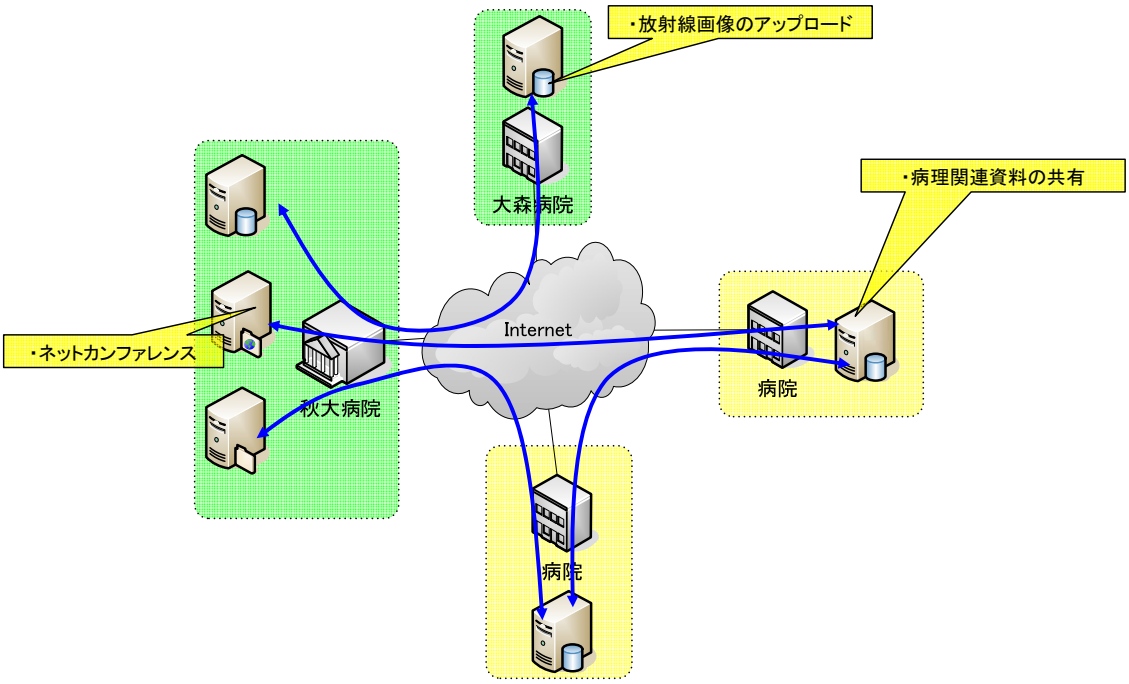
3-9 内部セキュリティ サービス	3-9-1 セキュリティパッチなどの更新機能を拠点内に装備していますか？	ゲートウェイ機能 プロキシ機能	はい	セキュリティパッチなどをインターネット経由で行う際、インターネット通信を許可されていないホスト・ゾーンに対して、パッチのダウンロードを行い必要なホストに配布することでセキュリティホールに対する攻撃の対策を行う。
4. サービス運用例				
4-1 情報提供 サービスの展開	4-1-1 医療機関向けに情報（診療記録、検査データ、診療サマリ、健診データ等）を公開・提供する場合、接続先・接続元の制限を行っていますか？	プロキシ機能 各サーバ	はい	接続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 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	はい	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。 本資料「4.2 脅威への対処技術」
	4-1-3 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	はい	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。 本資料「2.2 (3)SPC 要件」
	4-1-4 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 各サーバ	はい	不正なユーザによるデータの閲覧を防ぐ。
	4-1-5 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 各サーバ	はい	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 情報提供 サービス（医療機関向け）の利用	4-2-1 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 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。
	4-2-2 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、	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。 本資料「5.3.1 通信モデルの定義」

	取得したデータは High Secure Zone に格納していますか？			
4-3 外部保存 サービスの利用	4-3-1 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 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 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 メールサービス	4-4-1 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 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 リモート保守 サービスの利用	4-5-1 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 プロキシ機能	はい	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。

2.1.3 A大学病理診断NW

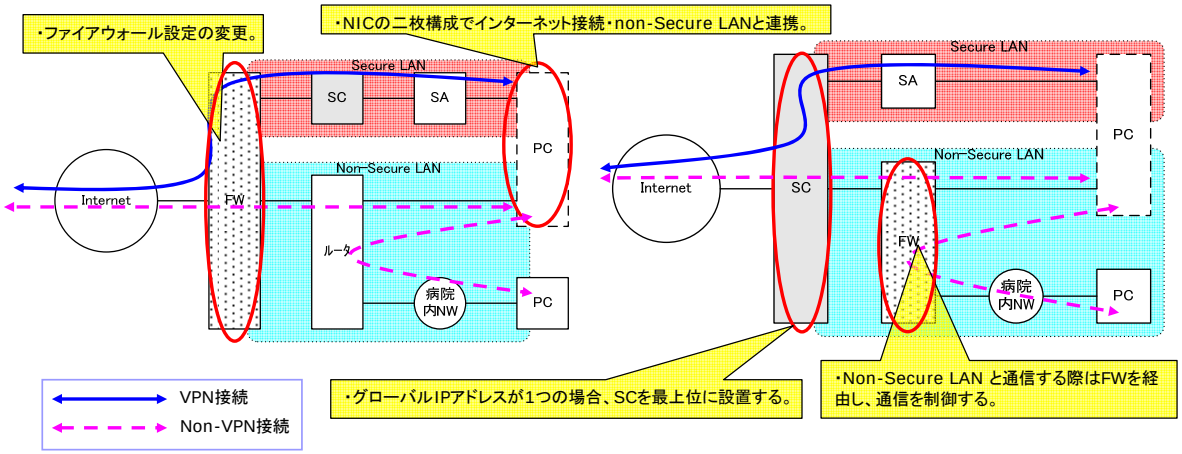
(1) サービス概要

A 大学病理診断 NW は、A 大学病院を中心に県内病院を連携するネットワークを構築している。ネットカンファレンス・診断画像の転送・病理関連資料の共有などのサービスをしている。



(2) ネットワーク概要

A 大学病理診断 NW は、拠点間のサービス形態は T 大リモート実験 NW に類似している。A 大学病理診断 NW は、サービス対象機器にネットワーク・インターフェースを複数装備し、それぞれ High Secure Zone と Secure Zone に接続している。インターネット・Secure Zone 内のホストとの通信の際はファイアウォールを経由し、アクセス制御・ウィルスチェックを行う。大森病院ではグローバル IP アドレスが1つであるため、最上位に SC を設置している。



(3) チェック結果

報告書のチェックシートに合わせて各拠点の状況を精査する。

O 病院 （小規模機関型）

目的対象	項目	機能要素	チェック	備考
1. 通信形態				
1-1 接続相手の確認	1-1-1 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？	-	いいえ	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。 本資料「2.2 セキュリティに関するガイドライン」
	1-1-2 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 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 中継の確認	2-1-1 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	はい： 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」 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。 本チェックシート「2-3 接続処理の確認」に進む。
2-2 オープンネットワークの利用した拠点間の接続	2-2-1 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。 本資料「5.1 法人間の接続における留意点」

	2-2-2 IKE でユーザ認証を行っていますか？	VPN 機能	はい	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。 本資料「4.2 脅威への対処技術」
	2-2-3 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	はい	
	2-2-4 セッション毎に共通鍵を自動決定していますか？	VPN 機能	はい	
	2-2-5 IPSec による暗号化を行っていますか？	VPN 機能	はい	
	2-2-6 IPSec でメッセージ認証を行っていますか？	VPN 機能	はい	
2-3 他拠点との接続処理	2-3-1 接続先拠点と通信に関して合意がなされていますか？	-	はい	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 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 ／プロキシ機能	はい	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 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 ／プロキシ機能	はい	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 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 ／プロキシ機能	はい	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。 本資料「2.2 (3)SPC 要件」
3. 拠点内のセキュリティ				
3-1 ホストの配置 役割	3-1-1 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	いいえ	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。 本資料「5.3.1 通信モデルの定義」
	3-1-2	Secure Zone	はい	

	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？			
3-2 外部からの脅威	3-2-1 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	はい	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 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	はい	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 High Secure Zone のセキュリティ	3-3-1 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	いいえ	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 インターネット接続を禁止していますか？	プロキシ機能	いいえ	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 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	はい	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 Secure Zone のセキュリティ	3-4-1 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	いいえ	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 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	はい	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 High Secure Zone と Secure Zone 間の通信	3-5-1 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	いいえ	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 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	いいえ	「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 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 プロキシ機能	いいえ	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。
3-6 内部セキュリティサービス	3-6-1 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 プロキシ機能	はい	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の対策を行う。

4. サービス運用例				
4-1 情報提供 サービス（医療機関向け）の利用	4-1-1 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 各サーバ	はい	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 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	いいえ	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。 本資料「5.3.1 通信モデルの定義」
4-2 外部保存 サービスの利用	4-2-1 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 プロキシ機能	いいえ	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 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	いいえ	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 リモート保守 サービスの利用	4-3-1 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 プロキシ機能	いいえ	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。

2.2 NTT-DATA仕様の事例

2.2.1 O県遠隔診断

(1) サービス概要

(2) ネットワーク概要

(3) チェック結果

報告書のチェックシートに合わせて各拠点の状況を精査する。

2.2.2 i県遠隔診断

(1) サービス概要

(2) ネットワーク概要

(3) チェック結果

報告書のチェックシートに合わせて各拠点の状況を精査する。