7.3　各種セキュリティ対策

7.3.1　NACCSセンター側のセキュリティ対策

NACCS センター側のセキュリティ対策としては、ファイアウォールや不正アクセス検出装置等を設置し、これらの設定及び運用において現時点で想定されうる最善の対策を講じる。

7.3.2　通信のセキュリティ対策等

インタラクティブ処理方式(netNACCS)、WebNACCS 処理方式及びインタラクティブ処理方式(netAPI)では、送受信電文の盗聴・改ざん・なりすまし等への対策として、HTTP の暗号化においてデファクトスタンダードとなっている TLS を採用する。なお、NACCS センターが提供するクライアントデジタル証明書の導入を必須とする。

（参考）TLSについて

TLSとは、Transport Layer Securityの略で、SSLを元に標準化したインターネットで安全に通信を行うための暗号化通信プロトコルである。

（参考）SSLについて

SSLとは、Secure Socket Layerの略で、米国Netscape Communications Corporationが開発した、インターネットで安全に通信を行うための暗号化通信プロトコルである。Webサーバと Webブラウザの間でやりとりするデータを暗号化することができるので、個人情報など第三者に漏洩すると問題があるデータの通信に向いており、Webブラウザベースではデファクトスタンダードとして広く認知されている。SSLは、暗号化に関する複数の構成要素から成り立っている。

インタラクティブ処理方式(netNACCS)、WebNACCS処理方式及びインタラクティブ処理方式(netAPI)で採用する通信の暗号化等の概要は、次の図のとおり。

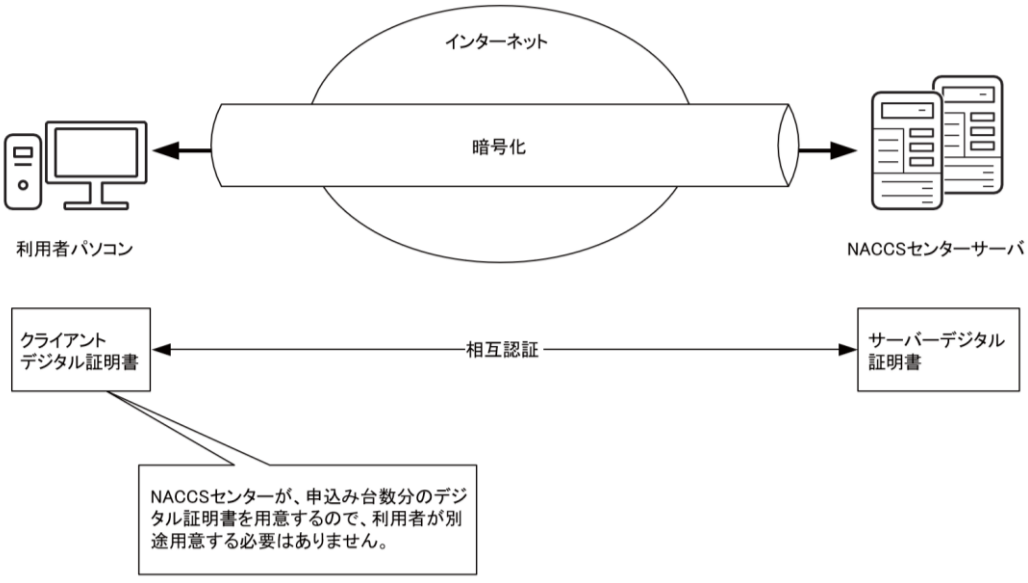

図 7-3-1　採用する通信の暗号化等の概要

なお、暗号化の方式については、今後のセキュリティの状況を踏まえて随時見直すこととする。

さらにインタラクティブ処理方式(netNACCS)、WebNACCS処理方式及びインタラクティブ処理方式(netAPI)では、NACCSセンターが発給・管理を行う利用者コード、識別番号、利用者パスワードを用いて、利用者が業務処理を行う資格があるかどうかのチェックを行う。

なお、帳票の取り出しにおいては、NACCSパッケージソフト(インタラクティブ処理方式)と同様に、利用者コード、識別番号、及びパスワードによるアクセス資格のチェックを行う。

7.3.3 利用者が行うセキュリティ対策

利用者は、NACCS センターサーバとの接続に際し、NACCS センターが定めたセキュリティ対策に関する内容を遵守し、利用者が講じたセキュリティ対策の内容について NACCS センターに報告しなければならない。利用者が遵守するセキュリティ対策の内容は、以下のとおりとする。

表 7-3-1　利用者が遵守すべきセキュリティの内容

内容	接続形態			遵守内容	備考
	ルータ接続	ゲートウェイ接続（netAPIを含む）	netNACCS WebNACCS		
(1)ID、パスワードの管理	○	○	○	・管理責任者は、NACCSにおいて利用する各種ID、パスワードの管理を行うこと	災害その他やむを得ない理由による在宅勤務・サテライトオフィス勤務での利用等、システム利用契約の申込み時にNACCSを利用することとした事業所以外で各種ID、パスワードを使用することとなった場合も、当該事業所の管理責任者が適切に管理すること
(2)ウィルス対策	○	○	○	・NACCSと接続する全てのコンピュータに対し、市販のウィルスチェックソフトの導入及び適切な頻度でのバージョンアップを施し、ウィルスに感染した場合は、NACCSセンターに速やかに届け出ること	市販のウィルスチェックソフトには、OSに組み込まれたウィルス対策ソフト（Microsoft Defenderウィルス対策等）も含む
(3)利用者側のシステム構成の提出	○	○		・NACCSセンターサーバに接続を行う利用者側のシステムに係る次のものをNACCSセンターに届け出ること ①システム構成図 ②使用する機器の構成リスト	

内容	接続形態			遵守内容	備考
	ルータ接続	ゲートウェイ接続(netAPIを含む)	netNACCS WebNACCS		
(4)社内セキュリティ対策の提出	○	○	○	・NACCSに関連する社内システム(サーバ・ネットワーク機器・クライアント端末等)に適切なセキュリティ対策(主体認証機能、アクセス制御機能、暗号化機能、セキュリティパッチ適用等の脆弱性対策等)を行うこと	NACCSセンターが必要と認めた場合、社内セキュリティ対策の提出を求める
(5)履歴（ログ）の管理		○		・ゲートウェイコンピュータ等からNACCSセンターサーバに接続した接続者を特定するため、利用者は、その送受信内容の履歴（ログ）を管理する仕組みを構築し、NACCSセンターの求めに応じて提出できるようにすること	NACCSセンターが必要と認めた場合、履歴（ログ）の提出を求める 履歴の管理方法については、次ページの（注）を参照

（注） 履歴（ログ）の管理（ゲートウェイ接続）

ゲートウェイ接続における履歴（ログ）の管理方法を次のとおり定める。

① 保存すべき履歴（ログ）の内容
NACCS センターサーバと送受信する電文の項目のうち、次の項目とする。

表 7-3-2 ゲートウェイ接続を行う利用者が保存すべき履歴（ログ）の項目

送信／受信 ＼ 項目	送信時	受信時
利用者コード	○	○
識別番号	○	－
業務コード	○	○
年月日時分秒	○	○

○・・・必要　　－・・・不要

② 保存すべき期間
履歴（ログ）の保存期間を 1 年間とする。

③ 保存場所及び保存方法
履歴（ログ）の保存場所及びその方法については利用者の自由とするが、NACCS センターの提出依頼に迅速に対応可能な状態でなければならない。

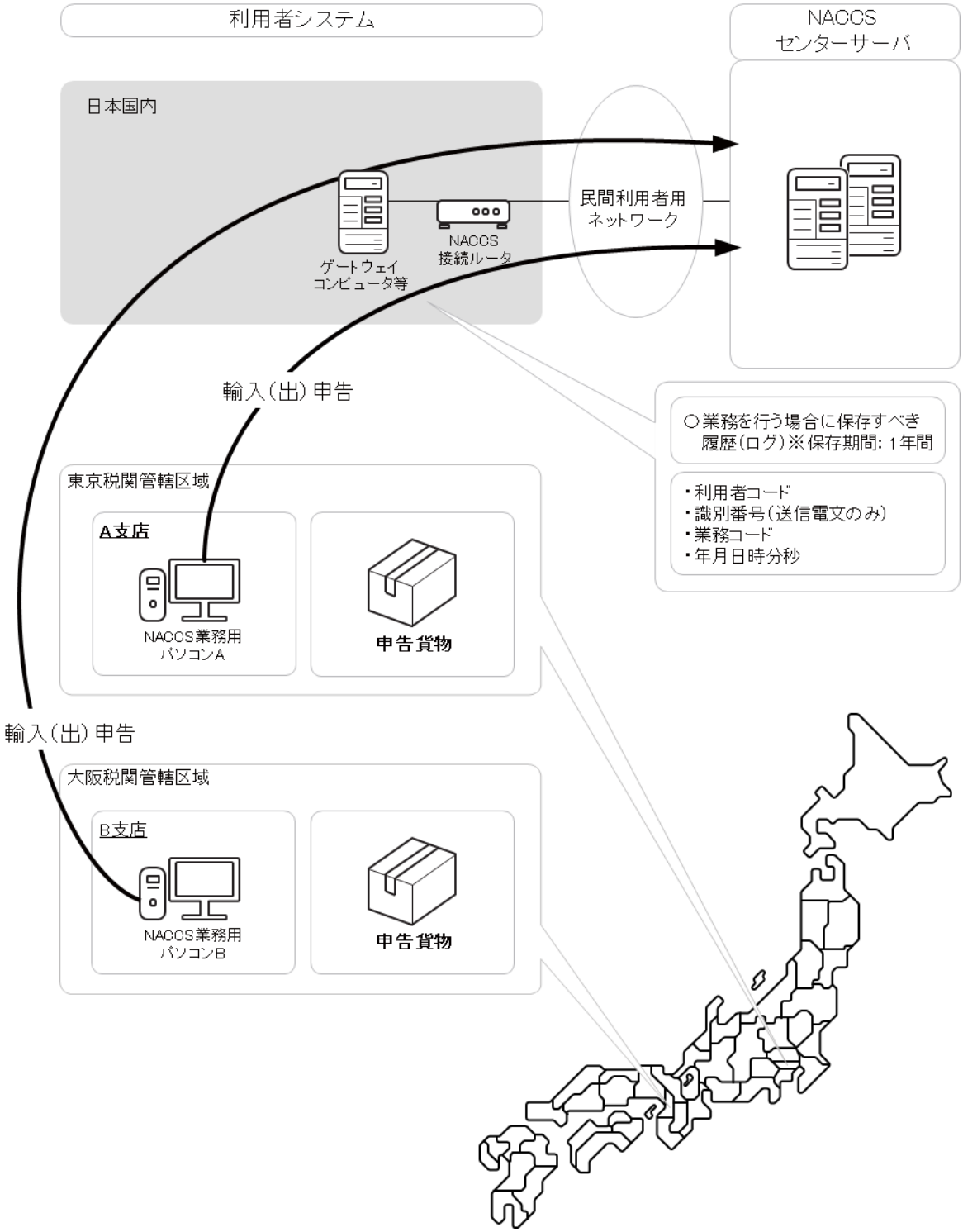

図 7-3-2　ゲートウェイコンピュータ配下のパソコンで
輸入（出）申告等業務を行う場合の履歴（ログ）

7.3.4　社外ネットワークとの接続に関するセキュリティ基準

(1)　NACCS接続ルータの利用に関しての制限

(A)　LANポートの利用

ルータ接続、ゲートウェイ接続において、NACCS 接続ルータの民間利用者システム側の LAN ポートは、NACCS 接続専用として設定するため、この LAN のポートを他の目的に使用することはできない。(「WAN」ポートについても利用不可。)

(B)　コンソールポートの利用

コンソールポートは、NACCS センターが NACCS 接続ルータの設定を行う際に使用するためのポートであり、利用者はいかなる機器も接続してはならない。

(2)　NACCS接続ルータを使わないで社外ネットワークと接続する場合の制限

(A)　社外ネットワークとの接続がLAN接続の場合（ネットワークとネットワークの接続）

社外ネットワークとの接続がある場合は、全て NACCS センターのセキュリティ対策の審査を受ける必要がある。

社外ネットワーク(他社ネットワーク、インターネット等)との接続が認められる例は、以下のとおり。

(例1) 利用者側でPROXYサーバ等を設置することにより、社外ネットワークから利用者コンピュータにアクセスできない仕組みが施されている場合。

(例2) 社外ネットワークとの接続用ルータ（NACCSセンターが提供するルータとは別）の機能としてNAT相当機能（IPアドレス変換機能）を有し、社内ネットワークを外部から隠すように設定されている場合。

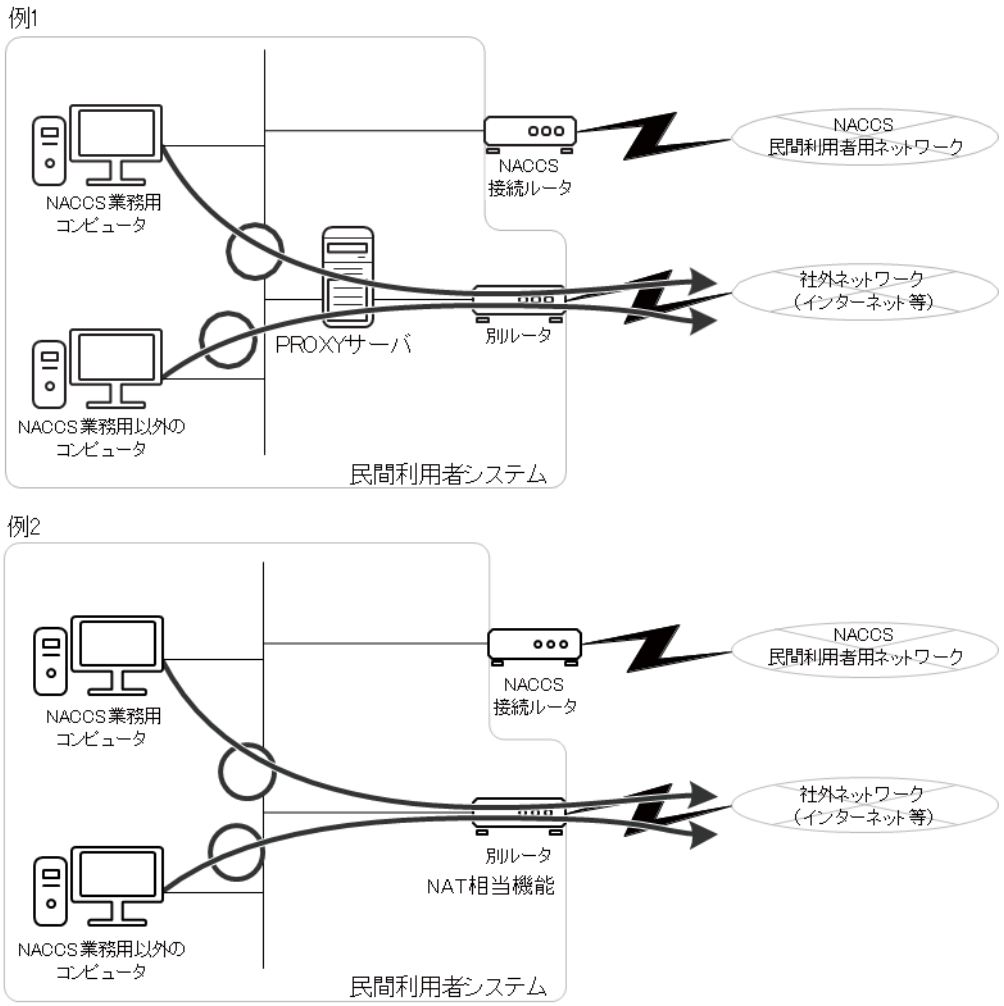

図 7-3-3　社外ネットワークとの接続が認められる例（例 1、例 2）

(B) 社外ネットワークとの接続がリモート接続の場合

社外ネットワークとの接続がある場合は、全て NACCS センターのセキュリティ対策の審査を受ける必要がある。

社外ネットワーク（他社ネットワーク、インターネット等）との接続が認められる例は、以下のとおり。

利用者側で VPN 装置等を設置することにより、社内ネットワークのコンピュータと社外ネットワークのコンピュータ、および両コンピュータ間のネットワークに第三者からアクセスできない仕組みが施されている場合。（リモート接続する社外ネットワークのコンピュータにも社内ネットワークのコンピュータに準じたセキュリティ対策を実施すること。）

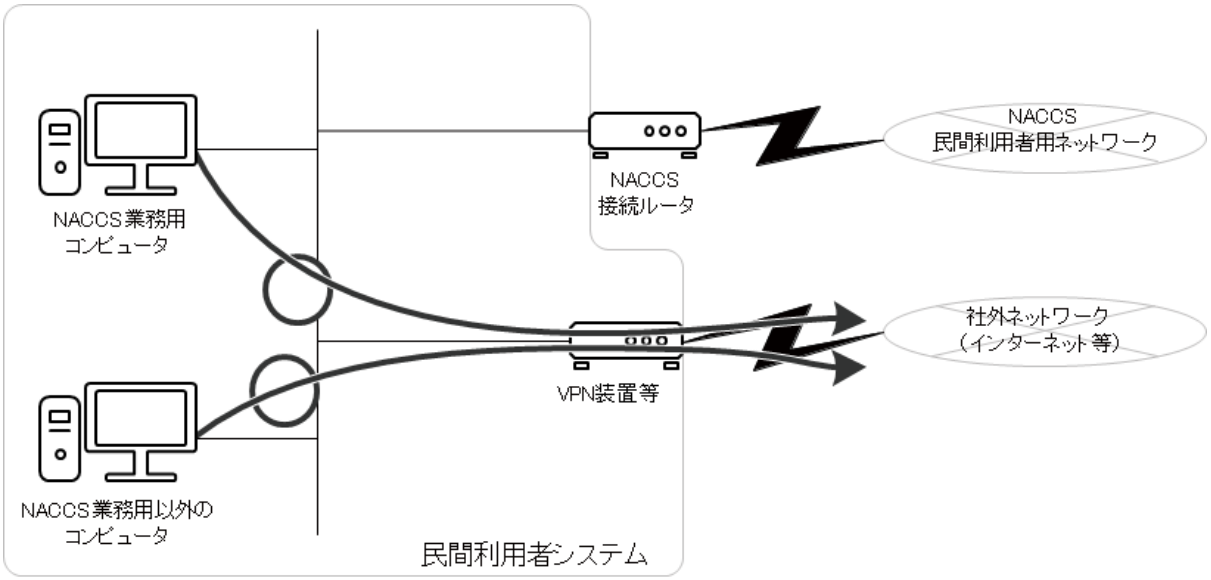

図 7-3-4　NACCS 業務用コンピュータと社外ネットワークとの接続が認められる例

表 7-3-3　NACCS 接続ルータを使わないで社外ネットワークと接続する場合の制限

	LAN接続	リモート接続
NACCS業務用コンピュータ	全てNACCSセンターの、セキュリティ対策の審査を受けること。	
NACCS業務用以外のコンピュータ		