7.4　利用者のセキュリティ対策

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。

NACCS センターは、利用者のセキュリティ対策が不十分または不適切であると思われる場合には、利用者に対し改善措置を講じるよう指示する。

7.4.1　利用者が行うセキュリティ対策

表 7-4-1　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
	peer to peer 接続	ルータ接続	ゲートウェイ接続		
(1)管理責任者の設置	○	○	○	・NACCSセンターサーバに接続を行う利用者システムの管理責任者を、各事業所ごと及び各ゲートウェイコンピュータ等の設置場所ごとに設置し、NACCSセンターに届け出ること	
(2)ID、パスワードの管理	○	○	○	・上記(1)の管理責任者は、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
(3)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行う~~施し、NACCSセンターに届け出る~~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
(4)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	
(5)社内セキュリティ対策~~の提出※NACCSセンターが必要と認めた場合、提出を求める~~	○	○	○	・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~~講じた~~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	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

				ディパッチ適用等の脆弱性対策等）（ファイアウォール、ユーザー認証等）を行うNACCSセンターに提出すること	
(6)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すし、NACCSセンターに届け出ること	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（※）を参照

（※）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7-4-2　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

~~（注 1）ゲートウェイコンピュータ等の配下のパソコンで通関業務を行う場合、IP アドレス変換は、固定的な IP アドレスから固定的な IP アドレスへの変換でなければならない。よって DHCP サーバのように動的に IP アドレスを当該パソコンに割り当てることは禁止する。ただし、DHCP サーバにおいて静的な変換をする設定（固定的な IP アドレスから固定的な IP アドレスに変換する設定）がなされている場合は、この限りではない。~~

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。

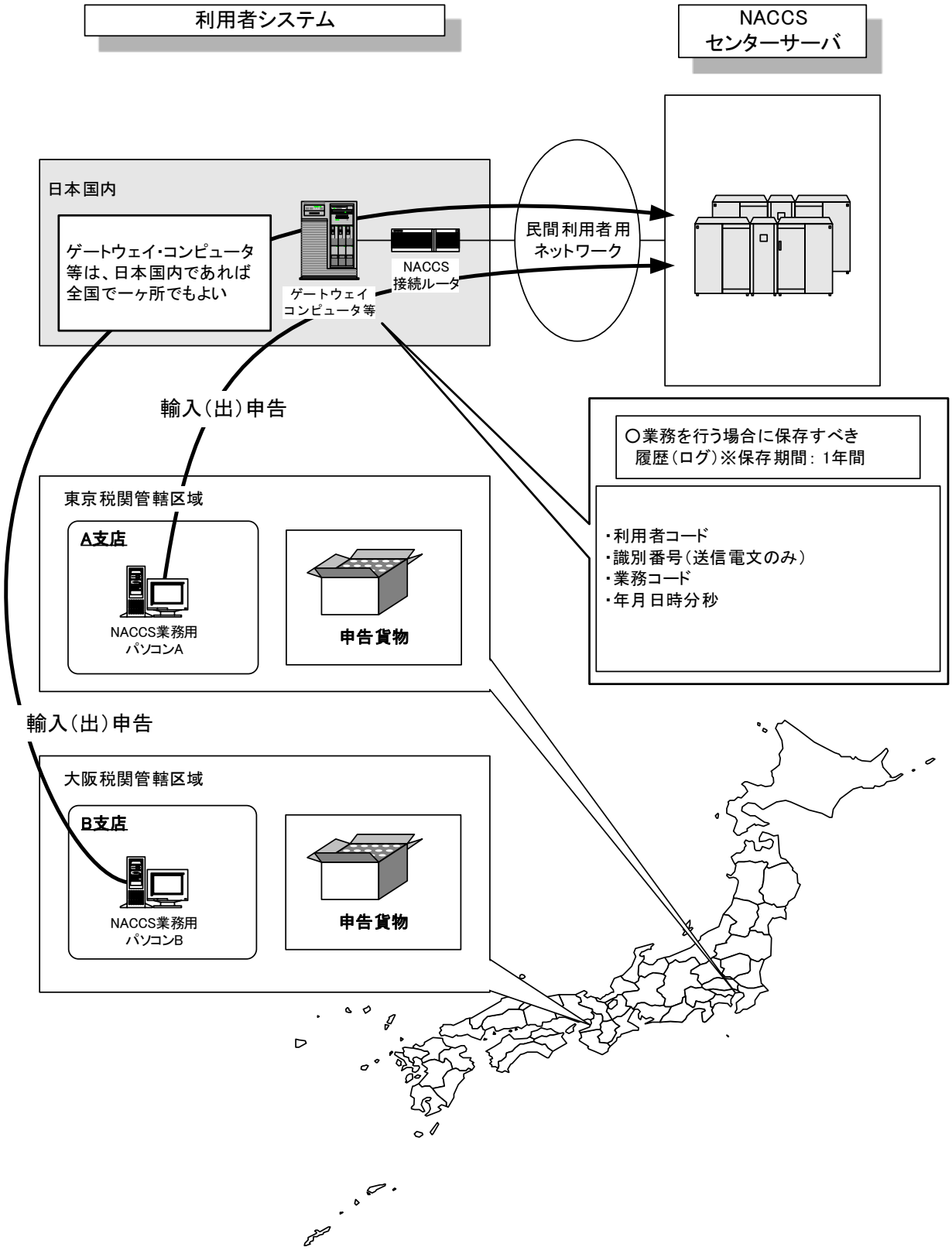


図7-4-1 ゲートウェイコンピュータの配下のパソコンで、輸入（出）申告等業務を行う場合の履歴（ログ）

~~業務を行ったパソコンを特定するために業務サーバ（プロキシサーバ等）及びゲートウェイコンピュータで、以下のとおりログを取得することとする。~~

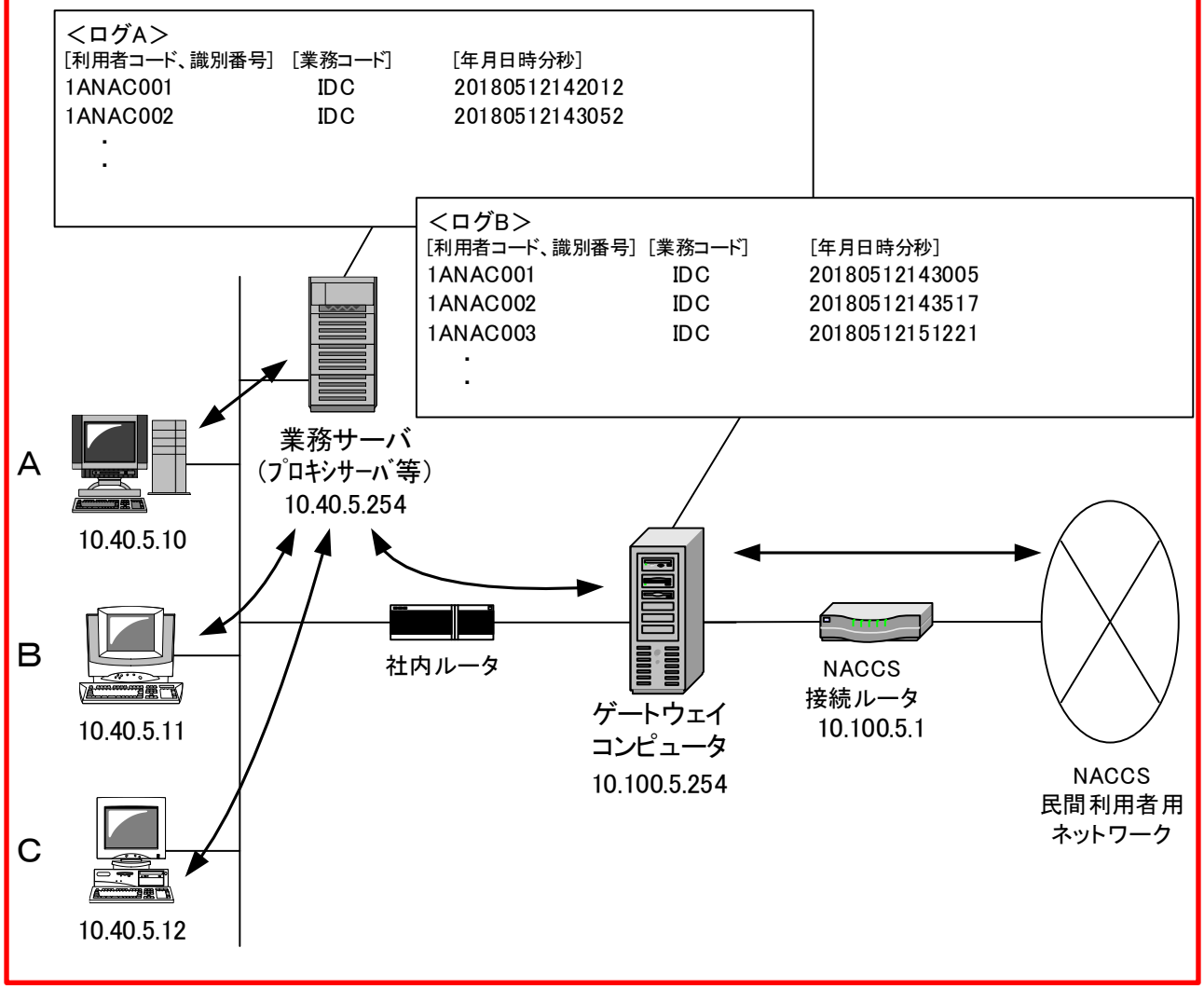


図 7-4-2 【削除】 ~~業務を行うパソコンから業務サーバ（プロキシサーバ等）を介し、電文を送信する場合の履歴（ログ）管理~~

7.4.2　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

①　~~LAN10BASE-T/100BASE-TX/1000BASE-T~~ポートの利用

Peer to Peer 接続、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 ~~LAN10BASE-T/100BASE-TX/1000BASE-T~~ポートは、NACCS 接続専用として設定するため、この ~~LAN10BASE-T/100BASE-TX/1000BASE-T~~ 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。）

② 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

① 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。

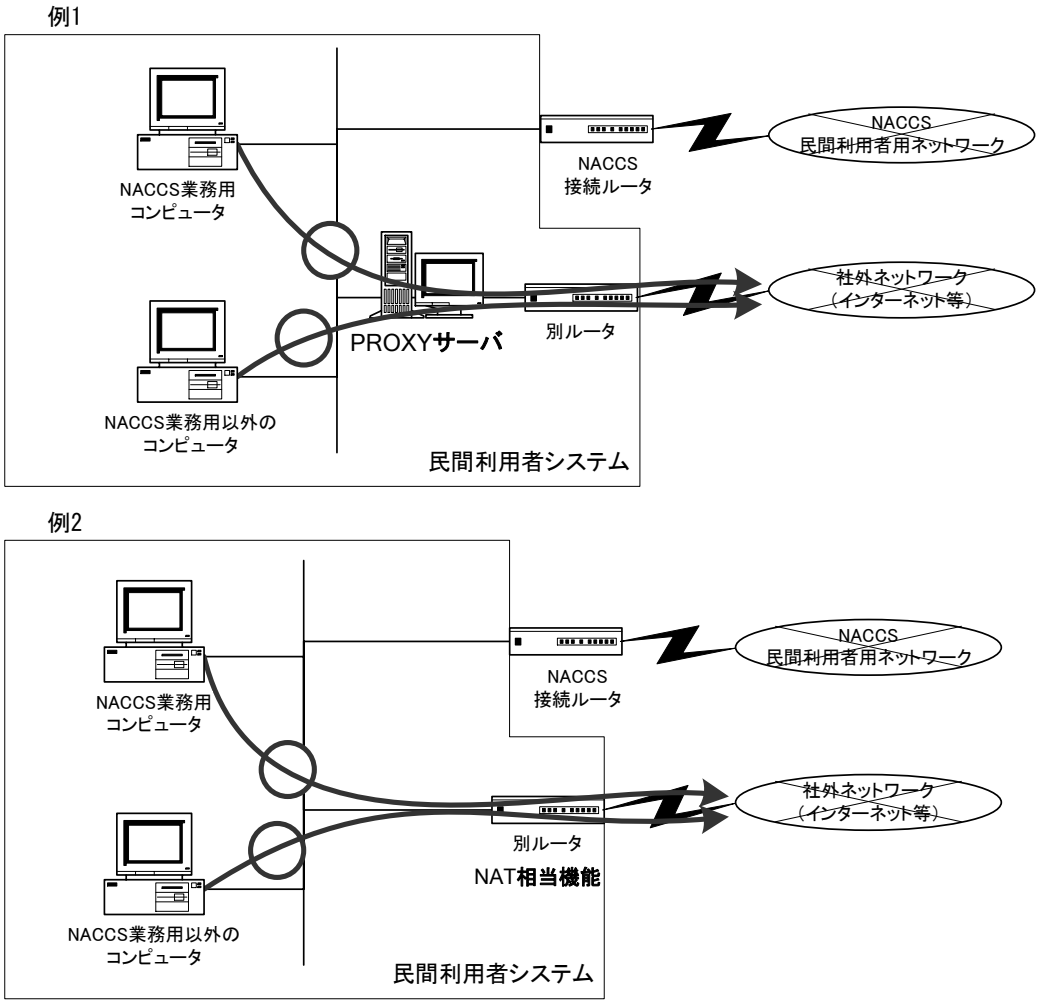


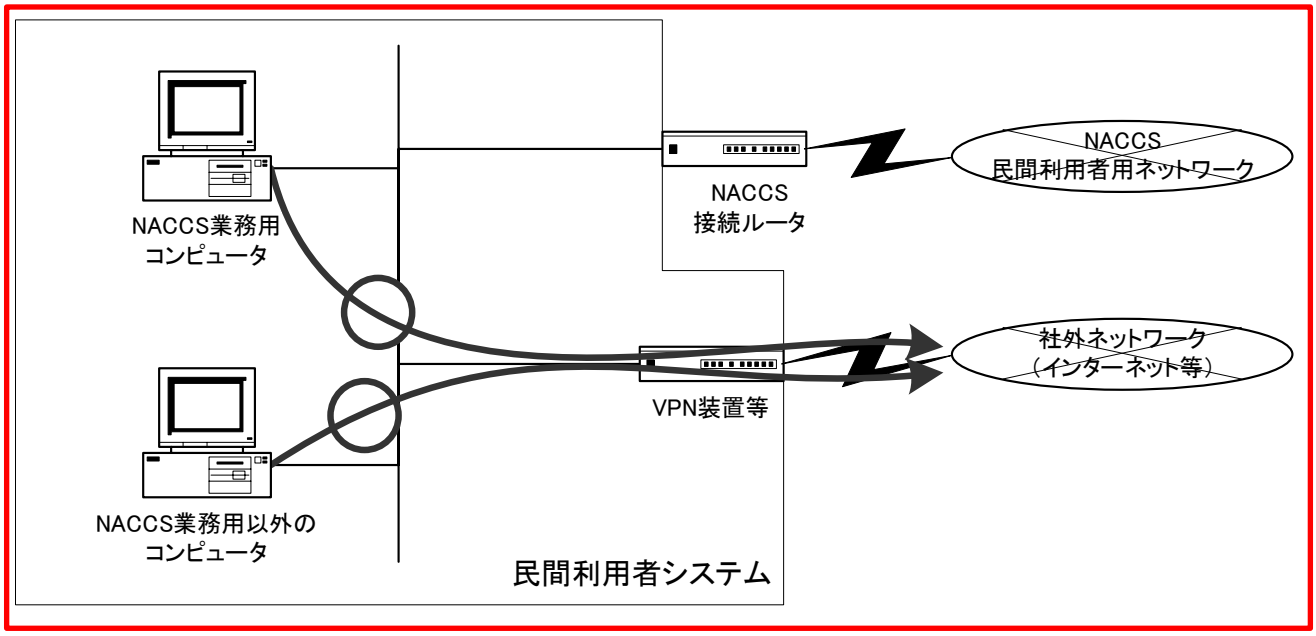
図7-4-3　社外ネットワークとの接続が認められる例（例1、例2）

② 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。

~~イ．NACCS 業務用コンピュータと、~~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~~をモデム、TA（DSU）等を用いてリモート接続することを、原則として禁止する~~。

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。）



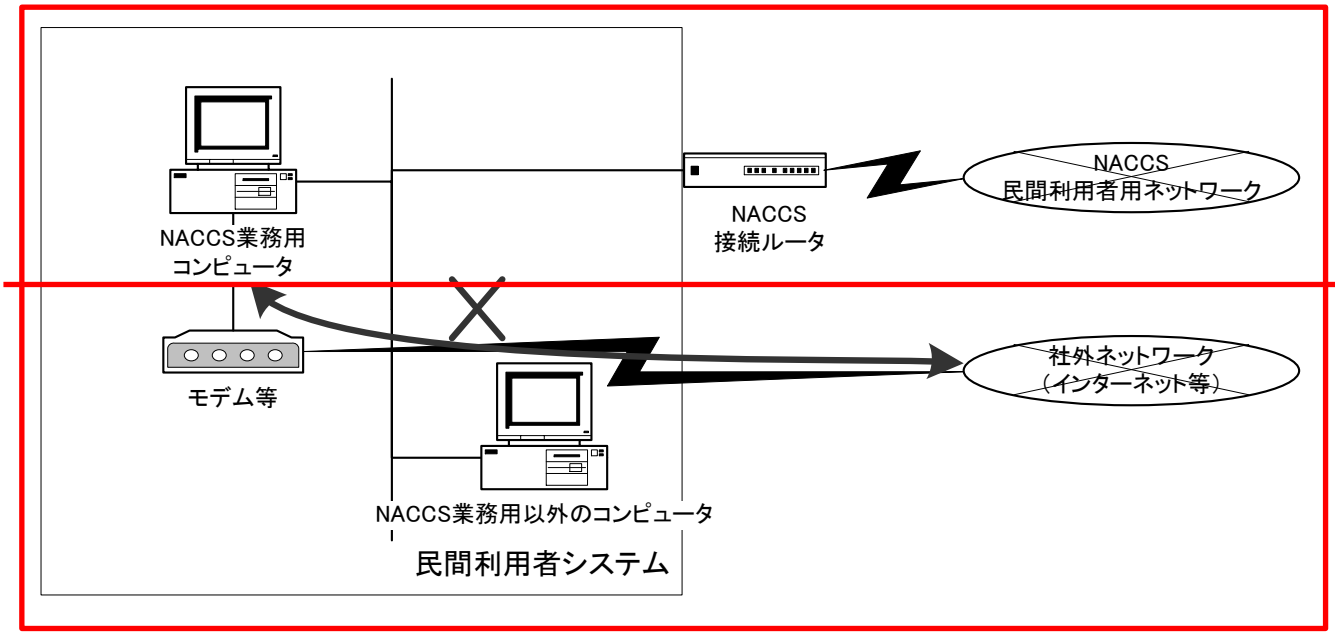


図7-4-4　NACCS業務用コンピュータと社外ネットワークとの接続が認められる禁止例

ロ．NACCS 業務用コンピュータ以外のコンピュータと社外ネットワーク（他社ネットワーク、インターネット等）を、モデム、TA（DSU）等を用いてリモート接続する場合、NACCS 業務用コンピュータには関係ない接続であるため、問題ない。

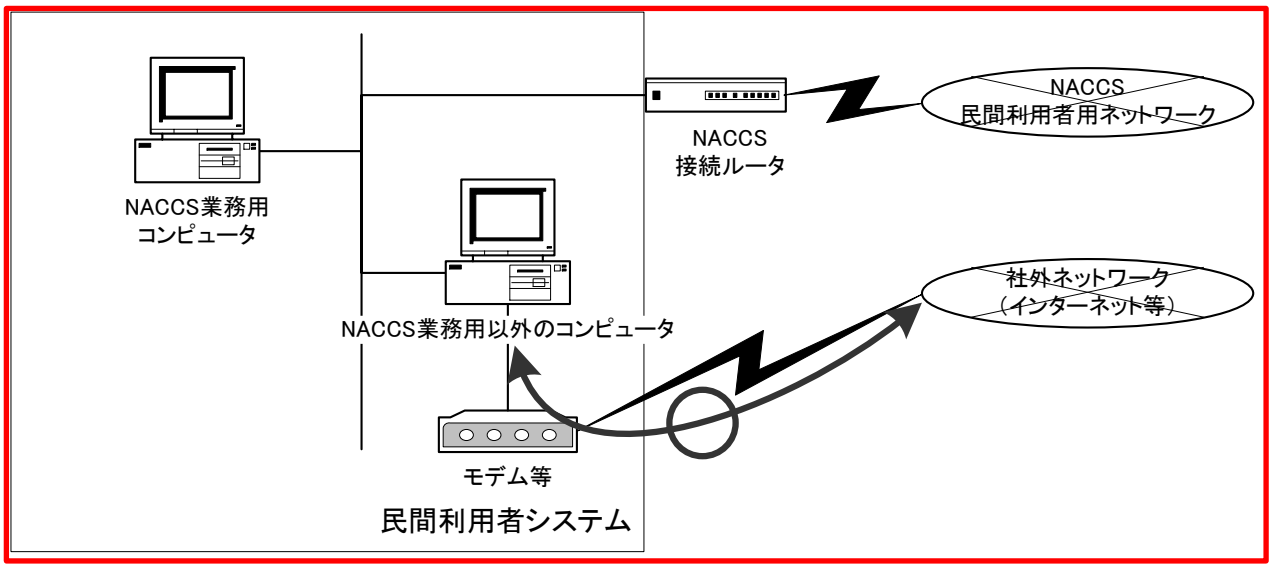


図7-4-5　【削除】NACCS業務用コンピュータと社外ネットワークの接続可能例

表 7-4-3　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		○

○・・・可　　×・・・不可