7.5 netNACCS 処理方式、WebNACCS 処理方式及び ebMS 処理方式

以下の方法により対処する。

7.5.1 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。

7.5.2 通信のセキュリティ対策等

netNACCS 処理方式、WebNACCS 処理方式、及び ebMS 処理方式では、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。

netNACCS 及び WebNACCS 利用の端末においては、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。

netNACCS 処理方式及び WebNACCS 処理方式で採用する通信の暗号化等の概要は、次の図のとおり。

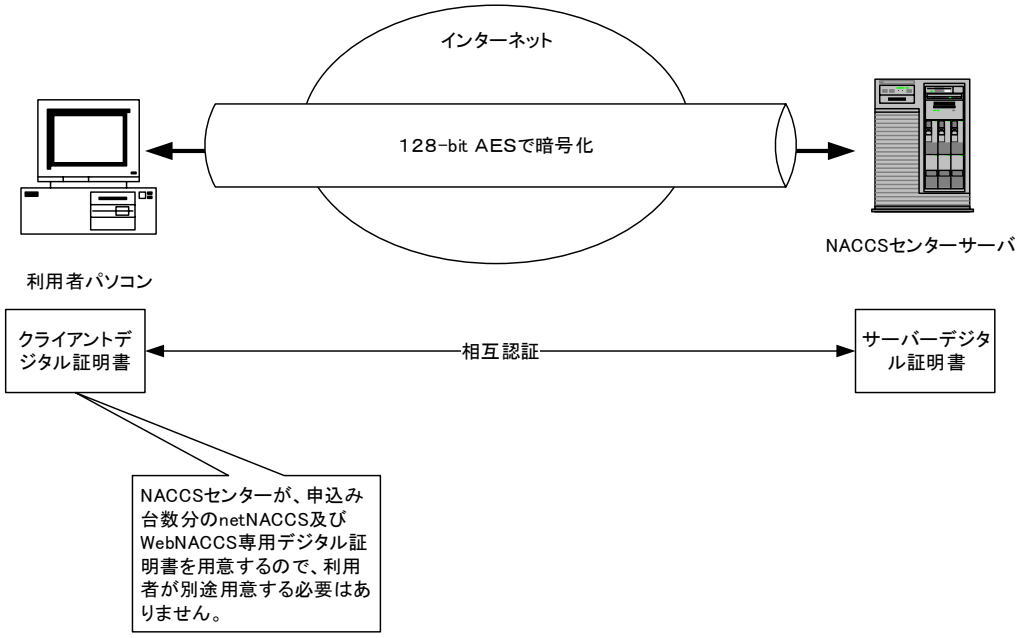

図 7-5-1　netNACCS 処理方式及び WebNACCS 処理方式で採用する通信の暗号化等の概要

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 netNACCS 処理方式、WebNACCS 処理方式及び ebMS 処理方式では、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、インタラクティブ処理方式（パソコン用パッケージソフト）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。

7.5.3　netNACCS処理方式接続例

(1) ダイヤルアップルータ・モデム等で直接インターネットに接続している場合

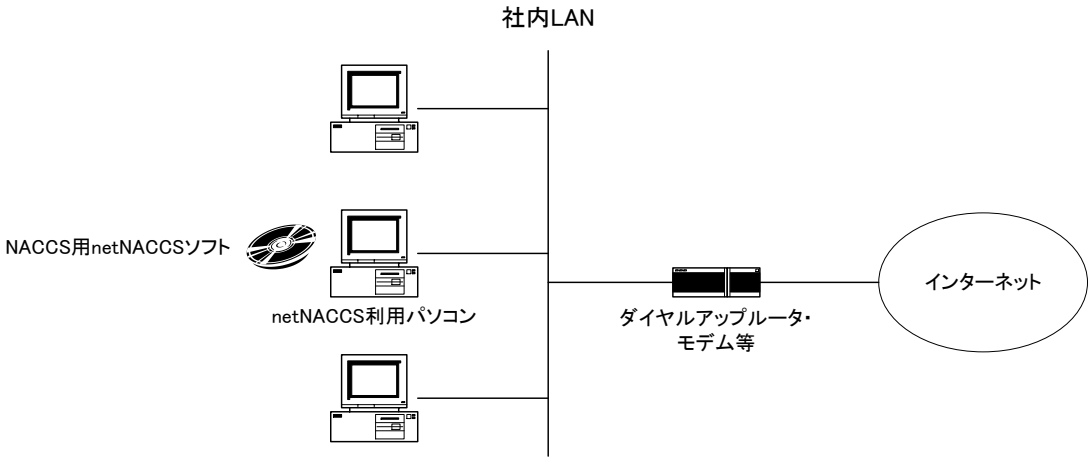

図 7-5-2　ダイヤルアップルータ・モデム等により直接インターネットに接続する例

(2) 社内ファイアウォール経由でインターネットに接続している場合

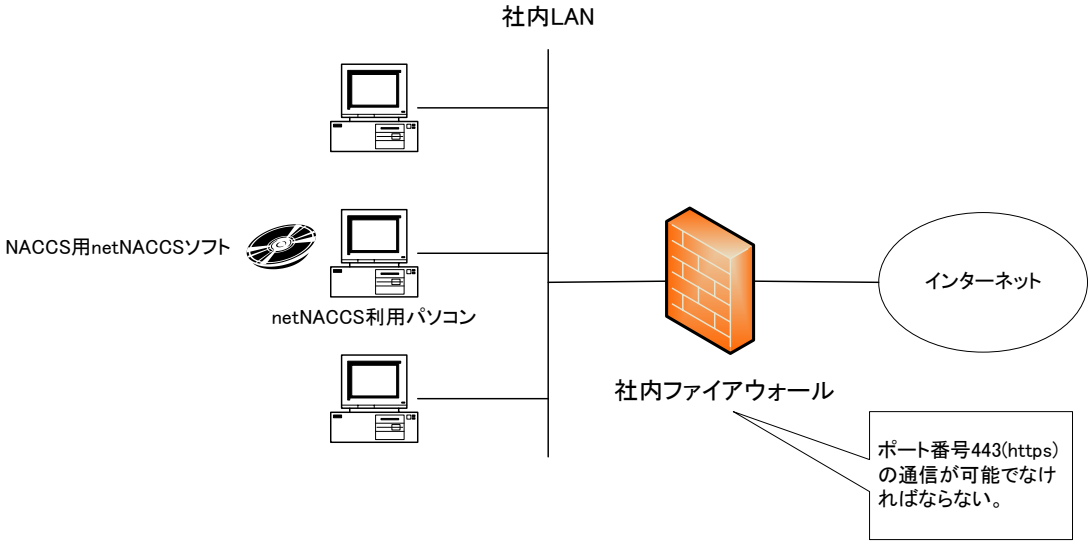

図 7-5-3　社内ファイアウォール経由でインターネットに接続する例

(3) netNACCSソフトとNACCSパッケージソフトを併用する場合

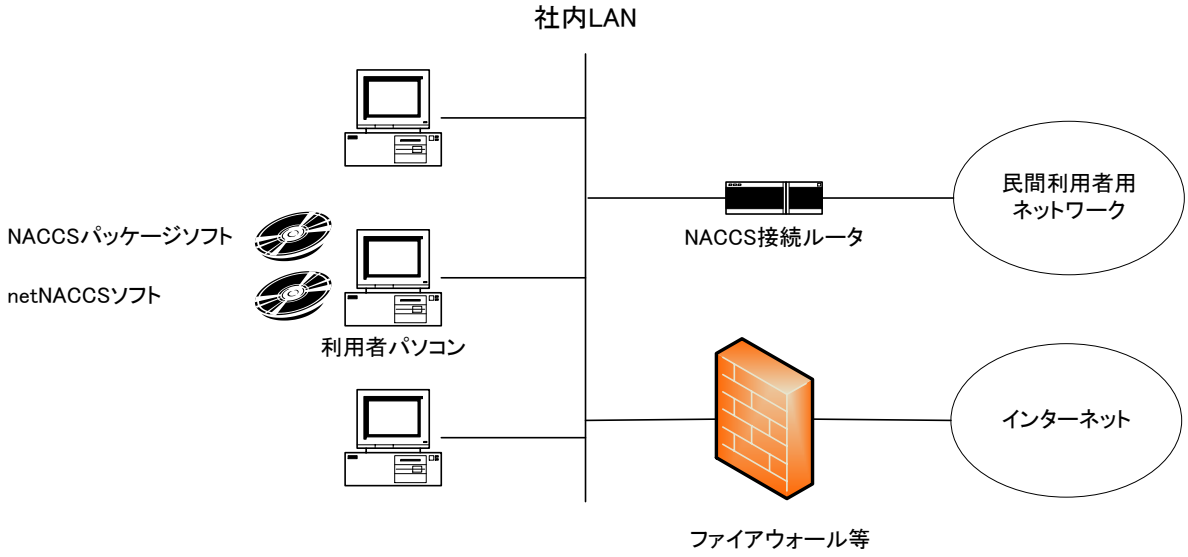

図 7-5-4　netNACCS ソフトと NACCS パッケージソフトを併用する例

(注1) netNACCSソフトとNACCSパッケージソフト（民間利用者用ネットワークに接続してNACCSに接続するパッケージソフト）を1台のパソコンにインストールすることは可能だが、同時に起動して使用することはできない。

(注2) NACCSパッケージソフトとnetNACCSを併用して利用する場合については、「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」を参照のこと。

7.5.4　WebNACCS処理方式接続例

(1) ダイヤルアップルーター・モデム等で直接インターネットに接続している場合

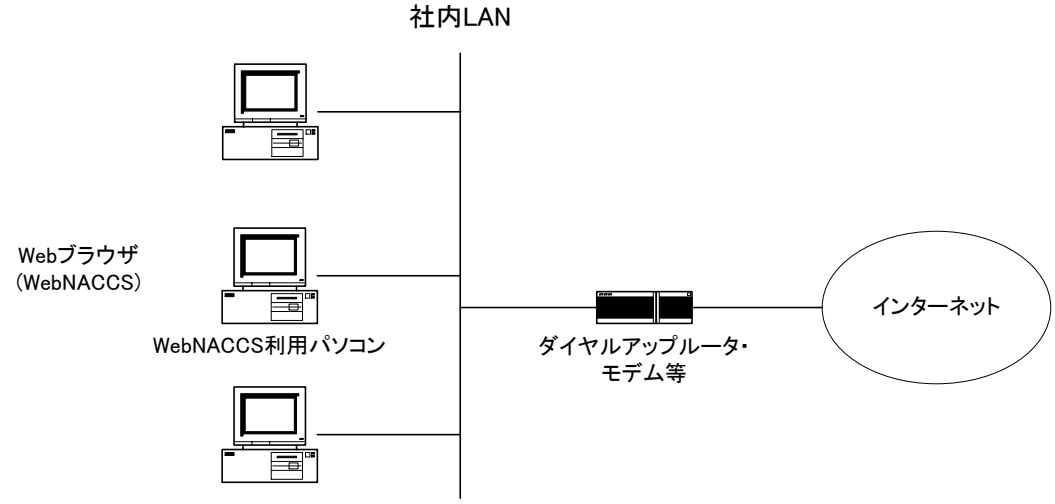

図 7-5-5　ダイヤルアップルータ・モデム等により直接インターネットに接続する例

(2) 社内ファイアウォール経由でインターネットに接続している場合

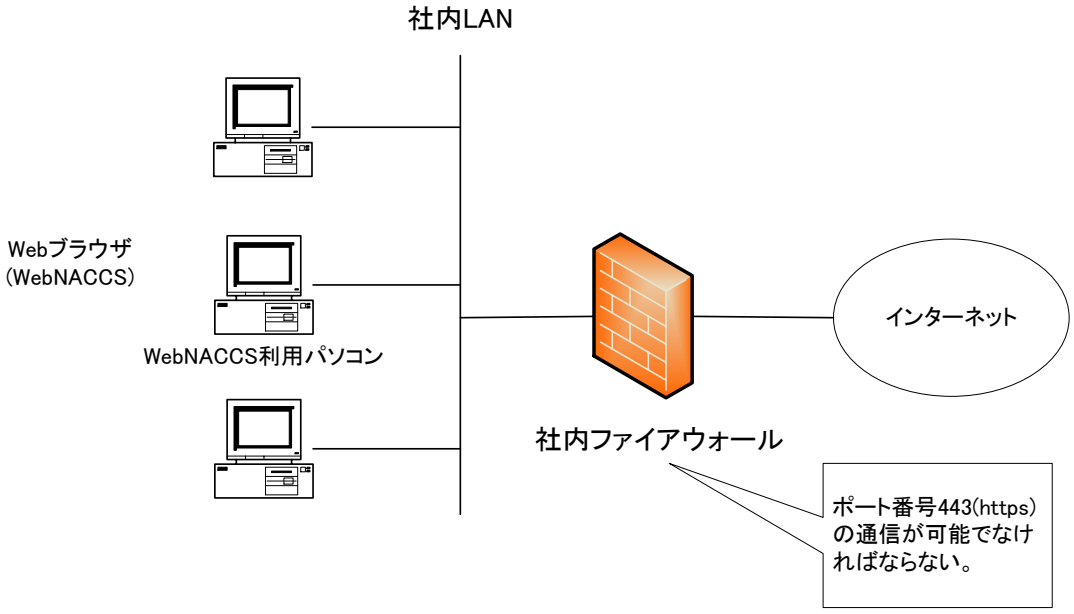

図 7-5-6　社内ファイアウォール経由でインターネットに接続する例

(3) WebNACCS処理方式とnetNACCSソフトを併用する場合

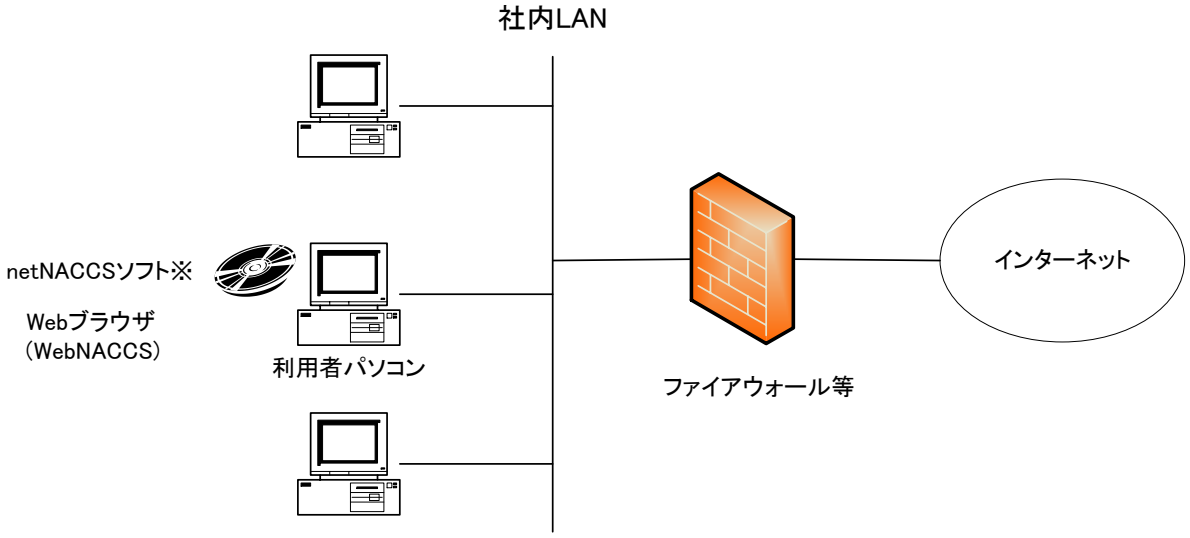

図 7-5-7　WebNACCS 処理方式と netNACCS ソフトを併用する例

(注1) NACCSパッケージソフトとnetNACCSを併用して利用する場合については、「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」を参照のこと。

7.5.5 netNACCS処理方式、WebNACCS処理方式及びebMS処理方式利用時の注意事項

(1) netNACCS処理方式及びWebNACCS処理方式のレスポンス

netNACCS処理方式及びWebNACCS処理方式のレスポンスは、使用するインターネット回線の回線速度にも左右されるが、netNACCS処理方式及びWebNACCS処理方式においては、暗号化処理及び認証処理に要する時間、netNACCS処理方式及びWebNACCS処理方式で送受信される電文をNACCSセンターサーバで処理するためにNACCS電文に変換するための時間等、必要なプロセスが多いため、NACCSパッケージソフトを利用（民間利用者用ネットワークを経由してNACCSと接続）する場合と比べてレスポンスが低下するものと考えられる。

(2) インターネット輻輳時のnetNACCS処理方式及びWebNACCS処理方式

現在NACCSセンターが提供している民間利用者用ネットワークでは、ネットワークに輻輳（混雑）が生じた場合においても、NACCSセンターサーバとの接続を保証している。しかし、netNACCS処理方式及びWebNACCS処理方式では、利用者自らが用意するインターネット回線を利用することになるため、NACCSセンターサーバとの確実な接続を保証することはできない。

(3) 電文の消失

netNACCS処理方式及びWebNACCS処理方式は、インターネットによる接続であるため、利用者からの処理要求に対する処理結果電文（画面電文）を利用者が受信中に通信障害が発生した場合には、電文の消失が発生する場合があり得る。

(4) ebMS処理方式のデジタル署名

デジタル署名機能では、X.509準拠のデジタル証明書を用いたXML署名による電子署名の付与及び検証を行う。XML署名には、ebXML Messagingエンベロップ及びペイロードを含むこと。なお、電子署名用証明書は、NACCSセンターより提供されたものを使用すること。

(5) ebMS処理方式に使用するサーバ証明書

ebMS処理方式において、利用者側のサーバに導入するサーバ証明書は、NACCSセンターより提供されたものを使用すること。

(6) その他の留意点

netNACCS処理方式及びWebNACCS処理方式は、インターネットによる接続であるため、netNACCS処理方式及びWebNACCS処理方式に対する不正アクセスやDoS攻撃等を完全に防ぐことは困難である。NACCSセンターとしては、常に最善のセキュリティ対策をnetNACCS処理方式及びWebNACCS処理方式に施しているが、集中的なDoS攻撃を受けた場合、あるいは、重大なセキュリティホールが新たに判明した場合等においては、対策を施す間、netNACCS処理方式及びWebNACCS処理方式を停止せざるを得ない場合もあり得る。

（注）DoS攻撃とは

DoS攻撃とは、「Denial of Service」の略で、サービス拒否攻撃と言われている。例えば、電話回線をつうじて、同一電話番号に対して一斉に電話がかかると、回線がパンクすることがある。それと同じように、インターネット上でも、特定のWebサーバに対し何十万・何百万のパソコンからアクセスが行われた場合、そのWebサーバは、深刻なダメージを受けてダウンさせられてしまう。そのような状態を意図的に作り、特定のサーバをダウンさせようとする手口が、DoS（Denial of Service）攻撃である。

7.5.6　利用者側のセキュリティ対策

netNACCS 処理方式及び WebNACCS 処理方式の利用にあたり、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 7-5-1　利用者が遵守すべきセキュリティの内容

内容	遵守内容	備考
①管理責任者の設置	netNACCS 処理方式及び WebNACCS 処理方式を利用する利用者システムの管理責任者を、事業所ごとに設置し、NACCS センターに届け出ること （但し、既に NACCS センターと利用契約を結び、届け出ている場合は不要）	
②ID、パスワードの管理	上記①の管理責任者は、netNACCS 処理方式及び WebNACCS 処理方式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	netNACCS 処理方式及び WebNACCS 処理方式を利用する全てのコンピュータ(PC を指す)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すこと	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社内セキュリティ対策	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