項目	ガイドライン	DoCAN対応内容
【安全対策基準】		
運16 各種資源、システムへのアクセス権限を明確にすること。	2.　不正アクセスが行われた場合の早期発見と原因究明のため、アクセス記録の取得を行うことが必要である。また、正当な権限のない者のアクセスに対しては、アクセス権限がない旨の警告を表示することが望ましい。【技37】	1. セッションログにてアクセス記録の保存可能。 2. DoCANへのアクセス権限のない不正利用者への接続時はエラーを表示。
運17 パスワードが他人に知られないための措置を講じておくこと。	パスワード等の漏洩防止のため、他人に知られないための注意喚起等の措置を講じておくこと。 1.　パスワード等については、以下の事項を使用者に注意喚起する等の対策が必要である。 ・推測されやすいパスワードを設定しないこと ・パスワード等を他人に知られないようにすること ・他人のパスワード等を使用しないこと ・パスワードをメモ等に残した場合、メモ等の盗難・紛失により他人にパスワードが漏洩するおそれがあること また、初期設定されるパスワード等についても推測されやすいパスワードを設定しない等の運用によって、漏洩するリスクを軽減することが必要である。 2.　推測されやすいパスワードとは、例えば以下のようなものがある。 ・桁数の短いパスワード ・IDと同一のパスワード ・生年月日、電話番号、住所(地番)、自分の車のナンバー等の個人の生活に関連した情報 ・自分、および自分の知っている人(配偶者、友人、ペット、有名人等)の名前や愛称 ・123456等の単純な文字列や英字のみのものまたは数字のみのもの ・よく使われる英語の単語 ・上記の逆読みやそれらの組合せ 3.　社内で使用するパスワード等については、長期にわたって同じパスワードを使用し続けることがないよう、適宜変更することとし、変更されないまま一定期間が経過した場合、当該IDを使用不可とする措置を講ずることが望ましい。なお、個人データを扱うシステムにおいては、この措置は必要である。 4.　パスワード等を他人に知られないための技術的対策については【技26】参照のこと。	DoCANは独自のパスワード不要。
運56 外部接続における運用管理方法を明確にすること。	(2) 外部接続の利用管理 社内システムとインターネットとの接続や、出張先からのリモートアクセス等を行う場合以下の点を定め、場合によっては制限を設ける。 1）　利用可能者 2）　利用可能時間	1) 利用者の制限方法は技35参照。 2) DoCANは接続利用時間設定が可能。
	不正アクセスや情報漏洩防止のため、接続記録を取得し以下の監視を行う。 1）　外部から内部への接続監視	セッションログにてアクセス記録の保存可能。

	(4) 認証デバイス紛失時の対応 接続先の本人確認に使用する認証デバイス(アクセストークン、ICカード等)を本人が紛失した際の対応策を定める。	システム管理者によるアカウントの停止が可能。
	(5) セキュリティホール等への対応 外部と接続するサーバーやルーター等に搭載されているソフトウェアについて、セキュリティホール等の情報を収集し、適切なバージョンアップを行うなどの対応策を定める。 なお、不正アクセスや不正プログラム等の対策として、ベンダーから頻繁にセキュリティ対策のための修正プログラムが提供されている。 これらの修正プログラムは、業務やシステムに対する緊急度や重要度を考慮し、適用することが望ましい。	DoCANモジュールのセキュリティパッチは随時コネクトワン社より提供。
技10 プログラム作成段階での品質を確保すること。	3. Webシステムについては、Webアプリケーションの脆弱性対策を考慮してシステムを構築することが望ましい。 (1) 脆弱性の例 現在知られているWebアプリケーションで考慮すべき脆弱性として、以下のようなものがある。 1) SQLインジェクションの脆弱性 2) OSコマンド・インジェクションの脆弱性 3) ディレクトリ・トラバーサルの脆弱性 4) セッション管理機構の脆弱性 5) クロスサイト・スクリプティングの脆弱性 6) CSRF(クロスサイト・リクエスト・フォージェリ)の脆弱性 7) HTTPヘッダ・インジェクションの脆弱性 8) アクセス制御と認可制御の脆弱性 (2) 脆弱性対策の例 実装上の対策として、以下のようなものがある。 1) 入力データを元に処理(SQL、スクリプト、シェル等)をアプリケーションで生成し実行する場合は、意図しない処理が実行されないような、各脆弱性に対応した適切な実装を行う。追加的対策として、入力項目および入力パラメータについて、の属性やデータ長、制御文字の有無等の確認を行い不正なデータを排除することも望ましい。 2) ユーザーを特定する情報は推測困難なものとし、暗号化を施して送受信するなど漏洩しない方法で受け渡しする。また、なりすましの予防としてユーザーを特定する情報の発行をログイン成功後にするなどの実装を行う。 3) データベースやシステムファイル等の重要な資源に対し、適切なユーザー認証機能や認可制御を設けて必要最小限の権限・アクセスのみを許可するような実装を行う。	1，DoCANとしては各脆弱性対策は実施済み。 2，Webアプリケーションの脆弱性対策は、DoCANが接続する既存の接続Webシステムに準じる。

技13 パッケージ導入にあたり、ソフトウェアの品質を確保すること。	1.　業務システムパッケージ導入時の品質確保の具体的事例として、以下のようなものがある。 (参考1) 契約により、販売者と購入者の責任を明確にすべき例として、以下のようなものがある。 ・パッケージのソフトウェアを使用する装置等の使用条件 ・ソフトウェアについてのバグ(欠陥)その他の瑕疵を発見した場合の責任所在 ・障害発生時の支援体制 ・メンテナンスの範囲、期限等(脆弱性の修正パッチの提供を含む) (参考2) パッケージ購入にあたり、留意すべき事項として、以下のようなものがある。 特にクライアントサーバー・システムの場合、インストールする機器ごとにOSのバージョンやハード要件等の環境が相違することもあるため十分に留意すること。 1. オペレーティングシステムのバージョンレベルの確認 パッケージのソフトウェアが動作可能なオペレーティングシステムであることを確認するものである。 2. アプリケーションパッケージ間の連係時のバージョンレベルの確認 すでに導入しているアプリケーションパッケージとの連係や、同時に購入する複数のパッケージ間の連係について、バージョンレベルの確認を行うものである。 3. 最大利用記憶容量等の必要資源の確認 自社システムの記憶容量等がパッケージのソフトウェアを稼働させるのに十分であることを確認するものである。 4. コード体系の確認 自社システムとパッケージのソフトウェアにおけるコード体系の整合性を確認するものである。 5. 機密保護への対応 機密保護等のセキュリティ機能がパッケージに組み込まれていること。また、必要に応じてカスタマイズが可能であること。 6. コンピュータウイルスのチェック 購入パッケージそのものにコンピュータウイルスが潜むケースもあるため、導入時のウイルス	1. DoCAN利用規約により下記項目の責任範囲を明確化。 ・使用条件 ・サポートの責任範囲 ・サポート窓口／対応時間 2，セキュリティ機能は必要に応じてカスタマイズ可能。
技26 暗証番号・パスワード等は他人に知られないための対策を講ずること。	1.　端末機における漏洩防止として、暗証番号・パスワード等は、他人に知られないように、非表示、非印字、記号などへの置換え、覗き見防止等の対策を講ずることが必要である。また、媒体上に暗証番号・パスワード等をそのまま記憶させない等の対策を講ずることが必要である。	1. DoCANブラウザ起動時に接続する既存Webシステムのパスワード入力値はDoCANブラウザが「＊」表示。 2. DoCANブラウザがクライアント端末へのパスワードの記憶禁止。

	2.　暗証番号・パスワードの利用等にあたっての安全対策上の機能としては、例えば以下のようなものがある。 (1) 暗証番号・パスワードにはNULLまたは少ない桁数を認めない機能 (2) 暗証番号・パスワードの使用に有効期間を設定し、有効期限近接時は、事前に変更要求を行う機能 (3) パスワードの変更にあたって前回もしくは以前と同一のパスワードの使用を認めない機能 (4) 特定の予測可能なパスワード(自分の会社名等)や不適切なパスワードを排他的に定義することができる機能 (5) アクセスの都度、アクセスに使用するパスワードを変更するワンタイムパスワードの機能	DoCANは独自のパスワード不要。
	(6) 新規ユーザーの初回ログオン時に、初期設定されたパスワードからユーザー自身のパスワードに強制的に変更をうながす機能	(6)DoCANは独自のパスワード不要。
	(7) ソフトウェアキーボードを使用し、キーロガーによる暗証番号・パスワードの盗取を防止する。 なお、ソフトウェアキーボードは画面キャプチャーや暗号化前の電文を盗取するようなタイプのスパイウェアの対策にはならないことに留意する必要がある。	(7)キーロガー、画面キャプチャーや伝聞盗取機能を含むマルウェア感染可能性のある端末ではDoCANブラウザの起動禁止。
	(9) 暗証番号の登録・変更時に推測されやすい暗証番号の登録を認めない機能	(9)DoCANは独自のパスワード不要。
技29 伝送データの漏洩防止策を講ずること。	1. データ伝送時に盗聴された場合にもデータの内容がわからないようにするため、重要なデータについては、暗号化することが望ましい。特に個人データを伝送する場合には、暗号化・パスワード設定等データ伝送時に盗聴された場合にもデータの内容がわからないようにするための対策を講ずることが必要である。 2.　暗号の使用にあたっては、CPU負荷の増大、業務処理遅延等の影響にも留意して、信頼のおける適切な技術を選択することが必要である。なお、適用する技術は、情報処理技術の発展とともにその強度が変化することに留意するとともに、その使用にあたっては、複数の方式を適切に組み合わせて使用することが望ましい。 (参考2) 1. インターネットバンキング等における暗号技術はSSL(Secure Socket Layer)プロトコルが一般的になっている。SSLの暗号鍵は、数種類の鍵長が選択可能であるが、安全性を考慮すると128ビット以上の鍵長を使用することが望ましい。	1，DoCAN独自認証部分は暗号化通信対策済み。 2，Webサーバ接続時のSSL暗号仕様はDoCANが接続する既存のWebシステムに準じる。

技35 本人確認機能を設けること。	1.　コンピュータシステムの不正使用およびネットワーク拡大による種々の端末を使用した不特定多数の者からの不正アクセスを防止するため、正当な権限を保有した本人であるか、もしくは正しい端末に接続されているかなど、接続相手先の正当性を確認することが重要である。 3.　本人確認の方法として、以下のようなものがある。 (1) 広義のパスワード ・暗証番号 ・ID・パスワード ・イメージ連想 ・ワンタイムパスワード ・チャレンジ・レスポンス方式　等 (2) 暗号利用 ・共通鍵方式 ・公開鍵方式 ・電子署名 ・認証機関が発行する電子的な証明書　等 (3) バイオメトリクス(個人の身体的特徴を識別情報とした本人確認技術) ・指紋 ・声紋 ・掌紋 ・網膜パターン ・虹彩 ・筆跡 ・顔　等 (4) 所有物 ・磁気カード(キャッシュカード、オペレータカード、役席カード 等) ・ICカード ・パスワード生成機 ・携帯電話の識別番号　等 (5) これらの併用	DoCANの本人確認は下記手段にて行う。 (1)広義のパスワード ・アクティベーションコード ・既存システムのID・パスワード認証成否監視 (2)暗号利用 ・認証機関発行の電子証明書（SSL)利用 (4)所有物 ・端末の固有識別番号 (5)上記の併用
	4.　端末確認の方法として、以下のようなものがある。 (1) 端末ID確認 (2) 電話番号確認 (3) コールバック (4) 認証機関が発行する電子的な証明書等による接続先サーバーの認証 (5) IPアドレス等で利用場所を制限する方式	DoCANは以下の方式で端末確認を行う。 (1)端末の固有識別番号
	5.　本人確認のために使用される手段の管理運用方法については、以下の基準を参照のこと。 【技26、運16、運17、運18、運39、運51】	技26、運16、運17、運18、運39、運51項目参照。

	6.　たとえ端末の操作や画面の情報が盗取された場合でも、当該情報だけではなりすまされる可能性が少ない方式とすることが望ましい。	DoCANは以下の方式で端末確認を行う。 (1)端末の固有識別番号
	7.　ID・パスワードを用いて携帯電話の識別番号を金融機関に登録する方式においては、ID・パスワード漏洩時に、第三者の携帯電話の識別番号を、不正に登録されるリスクがあるため、登録時には異なる認証を用いることが望ましい。	DoCANは下記手順にて端末の登録を行う。 1. システム管理者による端末固有識別番号の登録 2. アクティベーションコードを使用したユーザーによる端末固有識別番号の登録
技36 IDの不正使用防止機能を設けること。	1.　システムやデータへのアクセス権を不正使用される危険性を考慮し、不正使用を防止するための機能を組み込むことが必要である。また、暗証番号等についても、同様に不正使用を防止する機能を整備することが必要である。(暗証番号の不正使用防止策については【技45】参照。) 2.　具体的な方法として、例えば以下のようなものがある。 (1) ログオン中のタイムアウト システムにログオンしたまま一定時間操作が行われないIDを、強制的にログオフもしくは画面をロックする。	操作されないと判断される一定時条件（画面ロックへの移行時、他のアプリ切替時など）下で、DoCANのセッションを終了させる。
	(2) 使用されていないIDの使用停止 一定期間システムに対してアクセスがないIDは、使用停止とする。	DoCANが接続するWebシステムの機能に準じる。
	(3) ユーザーにログオン履歴情報を提供する システムへのログオン時、ユーザーに以下の情報を提供する。 ・前回のアクセス日付、時刻、状況 ・前回ログオン以降、ログオンが連続失敗していた場合、そのアクセス状況	DoCANが接続するWebシステムの機能に準じる。
	(4) パスワード入力失敗の回数制限 パスワードの入力を一定回数失敗した場合は、当該IDを一時的に使用不可とする。	(4)DoCANブラウザ起動時の接続Webに対し一定回数のログオン失敗時にはDoCANブラウザ設定値を初期化し一時的に使用不可とする。
	(5) パスワードを他人に知られないための対策を講ずる。 パスワードを他人に知られないための対策としては、【技26】参照のこと。	(5)技26参照。
	(6) 総当り攻撃(ブルートフォース攻撃)への対策を講ずる。 単にパスワード入力時のリトライ制限を設けるだけでなく、認証方式の特性を分析し、総当り攻撃が可能となるリスクに対応する。例えば想定されるリスクとして、パスワードを固定しユーザーIDを次々変化させてログオンを繰り返すことによるパスワードのリトライ制限の回避が考えられる。	(6)DoCANブラウザ起動時の接続Webに対し一定回数のログオン失敗時にはDoCANブラウザ設定値を初期化し一時的に使用不可とする。
	(8) エラーメッセージからの推測を防止する。 エラーメッセージの文面からパスワード等を推測できないようにする。	(8)エラーメッセージ上に認証失敗要素詳細を明記せず。
	(9) ログオン後は画面に必要な場合を除きIDを表示しない。 ログオン後は画面に必要な場合を除きIDを表示しないことで、覗き見での漏洩を防止する。	(9)DoCANが接続するWebシステムの機能に準じる。
	(10) プログラム等にID・パスワードを記述しない。 パスワード変更が必要な際に容易な対応ができるよう、プログラム等にID・パスワードを直接記述しない。ID・パスワードをプログラム等で使用する場合には、別ファイルに記述し、さらに容易に閲覧されないよう、当該ファイルの参照権限を限定する等の対策を講ずることが必要である。	(10)プログラム上にはIDパスワードの記述なし。

技37 アクセス履歴を管理すること。	アクセス状況を管理するため、システムやデータへのアクセス履歴を取得し、監査証跡として必要期間保管するとともに定期的にチェックすること。 1.　アクセス履歴を取得し監査証跡として保管する必要がある。また、アクセス記録を定期的にチェックして正当なアクセスなのかどうかを調査していることを周知させることによって、不正アクセス行為を牽制することが必要である。 記録として取得する具体的な内容としては、以下のような例がある。 ・ログインとログオフ状況(指示端末、時刻、ID、回線種別、使用したシステムもしくはデータ、行った処理) ・不正なアクセス要求(指示端末、時刻、ID) ・システムによって失効とされたID ・システムにログインしたまま一定時間操作が行われないために、強制的にログオフされたID なお、不正アクセス対策については、以下の基準項目を参照のこと。 ・本人確認機能を設けること【技35】 ・暗証番号、パスワード等は他人に知られないための対策を講ずること【技26】 2.　監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とすることが望ましい。なお、個人データを扱うシステムにおいては、この措置は必要である。 3.　監査証跡、オペレーション記録、運転記録等は、改ざんや不正アクセスを防ぐために、正当なアクセス権限者以外のものから適切に保護される必要がある。 具体的な対策としては、以下のような例がある。 ・暗号化して保管する。 ・書換え不能メディアに記録し、保護された場所に保管する。 ・ネットワーク経由の不正アクセスや改ざんを防止するために、オフライン媒体に記録する。 4.　後日アクセス履歴を参照する場合に備え、複数システムの時刻を、基準となる時刻に同期させておくことが望ましい。 分散システムにおけるシステム間の時間の同期方法としては、NTP(Network Time Protocol)を用いる方法がある。	1. DoCANのセッションログは下記履歴を保存。 ・ログイン：ID、時刻、端末固有識別番号、処理内容 ・不正アクセス、失効IDアクセス（ログイン失敗）：ID、端末 2. 不正アクセスの分析、報告が可能。 3. セッションログはシステム管理者が許可する特定のCDR等書き換え不能メディアへの書き出しが可能。

技43 外部ネットワークからの不正侵入防止機能を設けること。	3. 外部ネットワークからシステムへの不正侵入の防止と早期発見のため、システムへのアクセスを監視し、アクセス履歴のチェックを行うことが必要である。また、サーバー等のセキュリティホール対策を行うことが必要である。【技37、技45、運56】 4. 不正侵入防止策として、例えば以下のようなものがある。 (1) ファイアウォール インターネットと接続する場合はファイアウォールを設置し、インターネットを介した社内ネットワークへの侵入を制限する。 (2) アクセスサーバー ダイヤルアップによるリモートアクセスの受け口にアクセスサーバーを設置する。その際、コールバック、アクセス認証を行うことで、安全性を確保する。 (3) 非武装セグメント(DMZ：De-Militarized Zone) ファイアウォールにより設けられた特別なセグメント上に公開サーバー(外部にホームページなどを公開しているサーバー)を設置し、社内ネットワークへの不正アクセスを防止する。非武装セグメントを設けることにより、外部ネットワークから社内ネットワークを隠蔽するとともに、詳細なアクセス制御が可能となる。 7. 外部ネットワークに接続するネットワークと、接続しないネットワークを物理的に分離したネットワーク構成を検討することも必要である。 8. 本人確認機能等アクセス権限の確認と併せて本項の対策を行うことが重要である。【技35】 9. インターネットに接続する場合のセキュリティ技術は、最新のセキュリティ技術の動向に留意し、その安定性、互換性、実装の容易さなどを適切に評価したうえで採用することが必要である。 10. Webアプリケーションの脆弱性を利用した不正侵入や不正使用の防止策の実施にあたっては、既に発見され、公表されている不正行為(侵入や組込みの手口)の事例は、防御対策、検知対策に対する有益な情報となることが多い。したがって、これらについて記載されている文献や、ガイド等を参考にすることも有用である。【運103】(参考3) 図1 非武装セグメントの構成例	DoCANはファイアウォールににおいて接続元IPアドレス制限を行うか、専用VPN（Co-DoCAN）の利用により、ファイアウォールの外から中への通信を禁止したままにすることにより、不正侵入を防止。
技45 不正アクセスの監視機能を設けること。	不正アクセスを早期に発見するため、アクセスの失敗や不正アクセスを監視する機能を設けること。 1. アクセスの失敗を監視する機能として、以下のものを設けること。 ・アクセスの失敗を記録する機能を設けること。 ・連続した何回かのアクセスの失敗に対しては、強制終了・取引禁止等を行う機能を設けること。	・セッションログにて不正アクセスを記録。 ・指定回数以上のログイン失敗にてアカウント停止。
	2. 不正アクセスの監視機能の使用例として、以下のようなものがある。	
	(5) 他人が不正にアクセスしたかを利用者が確認できるために、表示器等に、前回アクセス日時を表示する。 (6) 不正アクセス等の異常を検知した場合には、セキュリティ管理者など、あらかじめ定められた者に自動的に通知する。	(5)前回アクセス情報表示などはDoCANが接続する既存Webシステムに準じる。 (6)アラート機能のついたファイアウォールやIDSなどとの組み合わせは可能。
	(7) Webサイトを外部に公開している場合は、侵入検知システム(IDS：Intrusion Detection System)や専用ソフトウェア等により、改ざんやサービス妨害攻撃(DoS攻撃：Denial of Service)等の不正アクセスを自動監視または早期に検知する。	(7)汎用の不正アクセス監視ツールとの組み合わせ可能。

技49 コンピュータウイルス等不正プログラムへの防御対策を講ずること。	3. 防御策としては、以下のようなものがある。 (1) コンピュータウイルスの侵入 1) 抗ウイルスソフト(ワクチンソフト)の導入 抗ウイルスソフトは、端末・サーバーへの導入のほか、外部ネットワークと内部ネットワークを接続するゲートウェイ等に導入し、データ送受信の都度チェックする仕組みとすることが望ましい。 抗ウイルスソフトを有効とするには、最新のウイルスパターンファイルを利用することが必要であり、そのための仕組みを構築することが望ましい。 2) ファイル管理の実施 出所が不明のプログラムは導入しない、ダウンロードしたファイルや電子メールの添付ファイル等は必ずウイルスチェックを行う、オリジナルプログラムにはライトプロテクトをかける等の対策が必要である。 予防、検査の機能を持つ抗ウイルスソフト(ワクチンソフト)を導入し外部より入手したファイルおよび媒体は、必ず検査する。 なお、抗ウイルスソフトで使用するウイルスパターンファイルは定期的に更新し、最新のものを利用することが重要である。	1)2)DoCANはクライアント端末のウィルスの検疫状態を監視し問題がある場合はDoCANを許可しない。 監視例) ・すでに感染している場合 ・検疫ソフトが導入されていない場合 ・定義ファイルの更新が一定期間されていない場合
	(2) 不正アクセスによるプログラムの改ざん 1) アクセス管理の実施 ファイルに対するアクセス制御機能を設けること。【技31】 本人確認機能を設けること。【技35】 IDの不正使用防止機能を設けること。【技36】 2) 不正侵入防止機能の導入 外部ネットワークからの不正侵入防止機能を設けること。【技43】 3) 不正アクセスの要因除去 ・ID、パスワード等の漏洩防止 暗証番号、パスワード等が他人に知られないための対策を講ずること。【技26】 蓄積データの漏洩防止策を講ずること。【技28】 伝送データの漏洩防止策を講ずること。【技29】 ・OS等のセキュリティホールへの対応 ・Webアプリケーションの脆弱性への対応 Webアプリケーションの脆弱性に関する監査(評価)を、定期的あるいはシステム変更時に実施することが効果的である。	技31、技35、技36、技43、技26、技28、技29の各項目参照
	(3) 不正プログラムの組込み 開発の各段階において、十分な検証を行い、システムに不正プログラムを組み込ませないことが必要である。 ・プログラム作成段階での品質を確保すること。【技10】 ・パッケージ導入にあたり、ソフトウェアの品質を確保すること。【技13】	技10、技13参照。
【METI情報セキュリティ管理基準】		

6.4 悪意のあるコード及びモバイルコードからの保護	6.4.1.1 悪意のあるコードに対する検知・修復ソフトウェア、セキュリティに対する認識及びシステムへの適切なアクセス・変更管理についての管理策に基づき、悪意のあるコードから保護する 6.4.1.2 認可されていないソフトウェアの使用を禁止する正式な方針を確立する 6.4.1.12 常に情報を収集するための手順(例えば、新種の悪意のあるコードに関する情報を提供するメーリングリストへの登録及び/又はウェブサイトの確認)を定め、実施する 6.4.1.13 悪意のあるコードに関する情報を確認し、警告情報が正確、かつ、役立つことを確実にするための手順を定め、実施する	情報漏洩の恐れのあるソフトウェアが起動している場合はDoCAN認証は許可しない。 また危険なソフトウェアの参考情報はコネクトワン社から定期的に案内される。
	6.4.2.1 モバイルコードが許可されていない動作を実行することから保護するため、論理的に隔離された環境でモバイルコードを実行する 6.4.2.2 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードのいかなる利用も阻止する(例えば、電子メールソフトウェアにて、HTMLメールの表示、モバイルコードの使用又はメールのプレビューを禁止するあるいはマクロ機能のある文書作成ソフトウェアにて、マクロの実行をデフォルトで禁止する又はマクロ実行時に警告を表示する) 6.4.2.3 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードの受取りを阻止する(例は、WEBブラウザの設定で、認可されていないサイトのモバイルコードを実行できない設定を行う、認可されたWEBサイトのモバイルコードだけを実行する設定を行う) 6.4.2.4 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードが管理されていることを確実にする仕組みとして、特定のシステム上で利用可能なように、技術的な手段を作動させる 6.4.2.5 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードが利用可能な資源を管理する 6.4.2.6 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードを一意に認証するための暗号による管理策を利用する	DoCANはクライアント端末のウィルスの検疫状態を監視し問題がある場合はDoCANを許可しない。 監視例) ・すでに感染している場合 ・検疫ソフトが導入されていない場合 ・定義ファイルの更新が一定期間されていない場合
7.7 モバイルコンピューティング及びテレワーキング	7.7.1.2 モバイルコンピューティング方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウィルス対策についての要求事項などを含める	物理保護：クライアント端末にデータ保存を許可しない アクセス制御：ID、パスワード、端末固有識別番号によるDoCAN認証 暗号技術：SSL暗号化通信 ウィルス対策：クライアント端末のウィルス検疫状態を認証時に監視
	7.7.1.5 モバイルコンピューティング設備では、盗難、特にどこか(例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所)に置き忘れたときの盗難から、物理的に保護するよう教育し、重要度の高い、取扱いに慎重を要する及び/又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないよう助言する 7.7.1.6 モバイルコンピューティング設備に保管され、処理される情報について、認可されていないアクセス及び漏えいを防止するため、例えば、暗号技術のような保護を備える	クライアント端末へのデータ保存の禁止により盗難時の情報漏洩を防ぐ。

7.7.1.7 モバイルコンピューティングでは、悪意のあるソフトウェアに対抗する手順を最新のものに保ち、備える	DoCANはクライアント端末のウィルスの検疫状態を監視し問題がある場合はDoCANを許可しない。 監視例） ・すでに感染している場合 ・検疫ソフトが導入されていない場合 ・定義ファイルの更新が一定期間されていない場合
7.7.1.10 モバイルコンピューティングのバックアップは、情報の盗難、喪失などから、十分な保護をする	クライアント端末へのデータ保存の禁止により盗難時の情報漏洩を防ぐ。
7.7.1.11 モバイルコンピューティングの設備を用いた、公衆ネットワークを経由しての業務情報への遠隔アクセスのために、識別及び認証と適切なアクセス制御機構を備える	DoCANのアクセス認証は下記手段にて行う。 (1)広義のパスワード ・暗証番号 ・ID・パスワード (2)暗号利用 ・認証機関発行の電子証明書（SSL) (4)所有物 ・端末の固有識別番号 (5)上記の併用
7.7.1.13 モバイルコンピューティング設備で、重要度の高い、取扱いに慎重を要する及び/又は影響の大きい業務情報が入っている装置は、可能な場合には、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いる	クライアント端末へのデータ保存の禁止により盗難時の情報漏洩を防ぐ。
7.7.2.2 テレワーキングの場所に適切な保護(例えば、装置及び情報の盗難、情報の認可されていない開示、遠隔地から組織の内部システムへの認可されていないアクセス、設備の不正使用に対するもの)を備える	盗難：クライアント端末へのデータ保存禁止。 開示およびアクセス：ID、パスワード、端末固有識別番号による認証。 不正使用：Winny型ウィルスや情報漏洩ソフトウエアの監視。
7.7.2.6 テレワーキングのための方針、運用計画及び手順に、組織の内部システムへの遠隔アクセスの必要性、通信回線からアクセスし、通信回線を通過する情報の取扱い慎重度及び内部システムの取扱い慎重度を考慮した、通信のセキュリティに関する要求事項の確認を含める	認証機関発行の電子証明書（SSL)。
7.7.2.7 テレワーキングのための方針、運用計画及び手順は、住環境を共有する者(例えば、家族、友人)による、情報又は資源への認可されていないアクセスの脅威を考慮して定める	クライアント端末へのパスワードの記憶禁止。（DoCAN Browser）
7.7.2.11 テレワーキングのための方針、運用計画及び手順は、ソフトウェアの使用許諾に関する取決め(例えば、従業員、契約相手又は第三者の利用者が個人的に所有するワークステーション上のクライアントソフトウェアの使用許諾について、組織が責任をもつことになる場合)を考慮して定める	使用ソフトウェア ・DoCAN Browser（コネクトワン社提供）
7.7.2.12 テレワーキングのための方針、運用計画及び手順は、ウィルスに対する保護及びファイアウォールの要件を考慮して定める	DoCAN認証時にはウィルス検疫ソフトの設定および定義ファイルの更新を監視。

	7.7.2.13 テレワーキングの指針及び取決めに、組織の管理下にない個人所有の装置の使用を許さない場合には、テレワーキング活動のための適切な装置及び保管用具の用意に関する事項を含める	端末固有識別番号が登録された端末からのみDoCAN認証が可能。
	7.7.2.14 テレワーキングの指針及び取決めに、許可した作業、作業時間、保持してもよい情報の分類並びにテレワーキングを行う者にアクセスを認可する内部システム及びサービスの定義に関する事項を含める	アクセス許可時間帯の設定が可能。
	7.7.2.15 テレワーキングの指針及び取決めに、遠隔アクセスを安全にする方法も含め、適切な通信装置の用意に関する事項を含める	一般インターネット回線によるSSL暗号化通信。
	7.7.2.16 テレワーキングの指針及び取決めに、物理的なセキュリティに関する事項を含める	クライアント端末へのデータ保存および外部媒体への保存、印刷を禁止。
	7.7.2.17 テレワーキングの指針及び取決めに、家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引を含める	・クライアント端末へのデータ保存禁止 ・クライアント端末へのパスワード記憶禁止（CBR Secure Brower)
	7.7.2.22 テレワーキングの指針及び取決めに、テレワーキングが終了したときの、権限及びアクセス権の失効並びに装置の返却に関する事項を含める	管理者によるDoCANアカウント停止または削除。
	7.7.2.23 テレワーキング用コンピュータからの接続を受けるネットワーク接続機器(VPN装置、RAS装置など)では、同一の利用者による複数接続を排除する設定を行う	DoCANが接続するWebシステムの機能に準じる。