



基本仕様書 第15.0.3版



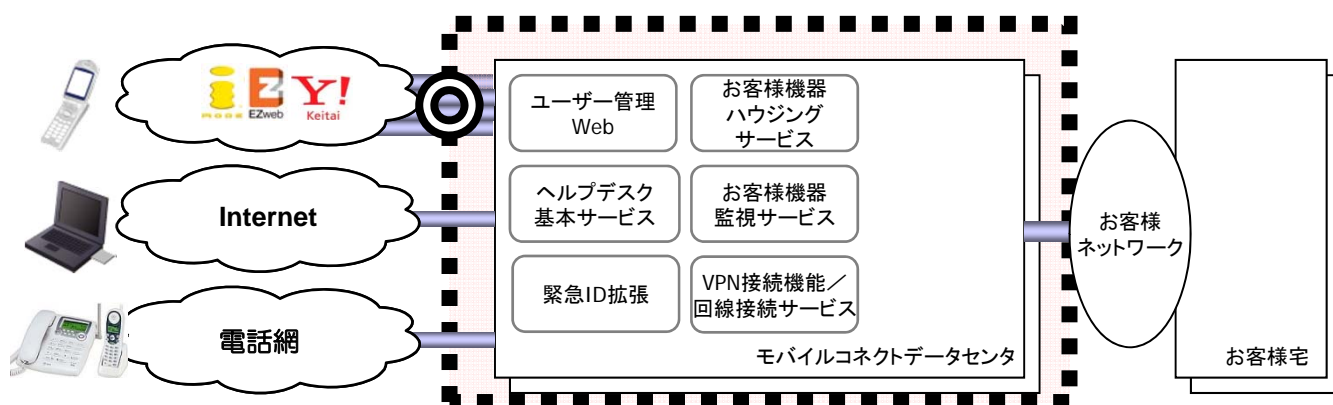
NTTコミュニケーションズ株式会社
2016年8月8日

モバイルコネクトサービス仕様-1

モバイルコネクトサービス
基本仕様書(第15.0.3版)

モバイルコネクト基本サービス

サービス提供範囲

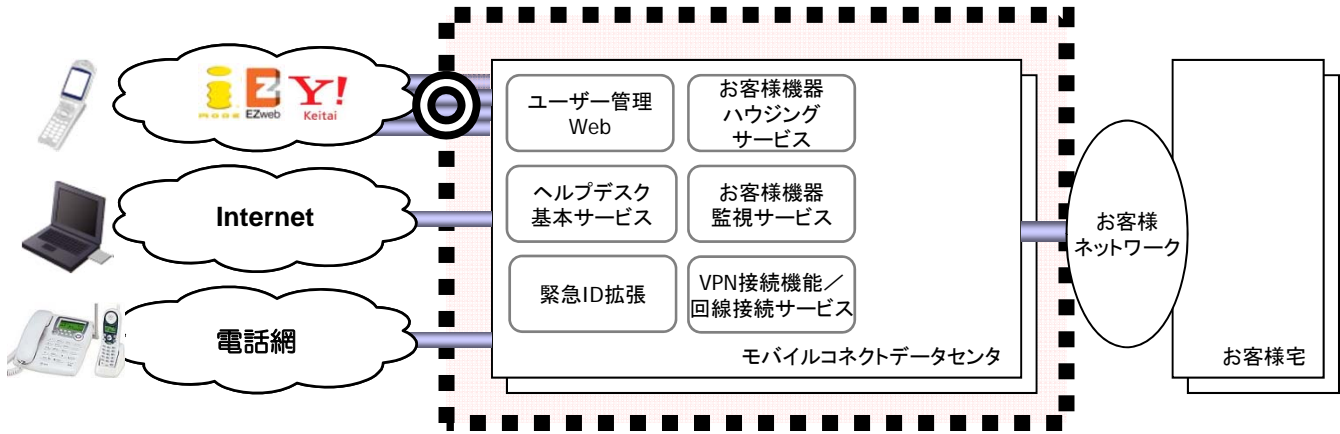


提供機能

項目	概要
ユーザー管理Web	お客様の管理者(企業管理者)がモバイルコネクトサービスの各種利用に関する設定を行なうためのWebサービスです。企業管理者の追加はオプションサービスとなります。
サービス管理	ご契約サービスの管理を行なう機能です。 ・モバイルコネクト認証サービスの動作に関する設定を行なうことができます。
ユーザー管理	ご契約サービスを利用する利用者のユーザーアカウント管理を行う機能です。 ・ご契約ID数の範囲内で、ユーザーアカウントの登録、変更、削除等ができます。 ・ユーザーへの通知メールの送信、アカウントロック、解除等のメンテナンスができます。
グループ設定	ユーザーアカウントの管理をグループ別に行う機能です。 ※本サービスはオプションサービスとなります。一部、グループ毎に選択できないサービスがあります。 ※特定のグループに限定したアカウント操作権限をもつグループ管理者の設定も可能です。
アクセスログ	ご契約サービスの利用者のアクセスログを提供する機能です。 ※一部、アクセスログの提供ができないサービスがあります。
ダウンロードサイト	VPNクライアントソフトソフトウェア及びプロファイル情報などを掲載したサイトを提供します。 ※本サービスはオプションサービスとなります。 ※「ケータイタイプグループウェア」、「スマートフォンタイプグループウェア」サービスは対象外となります。
ポータルサービス	「初期画面」と「トップメニュー画面」をカスタマイズできる機能です。 ※本サービスはオプションサービスとなります。ご利用サービスによって、利用できるポータル機能が異なります。
CSVファイル自動アップロード	CSVファイルを、お客様宅ファイルサーバから自動取得し、ユーザー管理Webにアップロードする機能です。また、登録されたデータに基づき、各種メール通知を行ないます。 ※本サービスはオプションサービスとなります。一部のCSVファイルの登録による設定ができないサービスがあります。
お客様機器ハウジングサービス	お客様ネットワークを収容するモバイルコネクトのネットワーク機器と接続されるお客様ネットワーク機器をモバイルコネクトデータセンタに設置及び保管します。また、お客様ネットワーク機器までのEtherケーブルをご用意します。 ※本サービスはオプションサービスとなります。
お客様機器監視サービス	モバイルコネクトデータセンタと接続するために設置されるお客様のネットワーク機器をPing監視します。お客様宅のネットワーク機器に対しても、Ping監視することができます。 ※本サービスはオプションサービスとなります。
VPN接続機能	既に弊社VPNサービスをご利用いただいている場合、モバイルコネクトデータセンタとお客様ネットワークを接続する回線を個別に設置せずに、モバイルコネクトサービスをご利用いただくことができます。 ※本サービスはオプションサービスとなります。
回線接続サービス	既に弊社VPNサービスをご利用いただいている場合、モバイルコネクトデータセンタとお客様ネットワークを接続する回線を個別に設置せずに、モバイルコネクトサービスをご利用いただくことができます。 ※本サービスはオプションサービスとなります。
緊急ID拡張	緊急グループの利用IDの認証実績分を月単位で集計し、通常利用時の認証利用料単価を特定料率で従量課金いたします。※「SSL-VPN マルチアクセス・ライト」にのみ適用可能です。

モバイルコネクト基本サービス

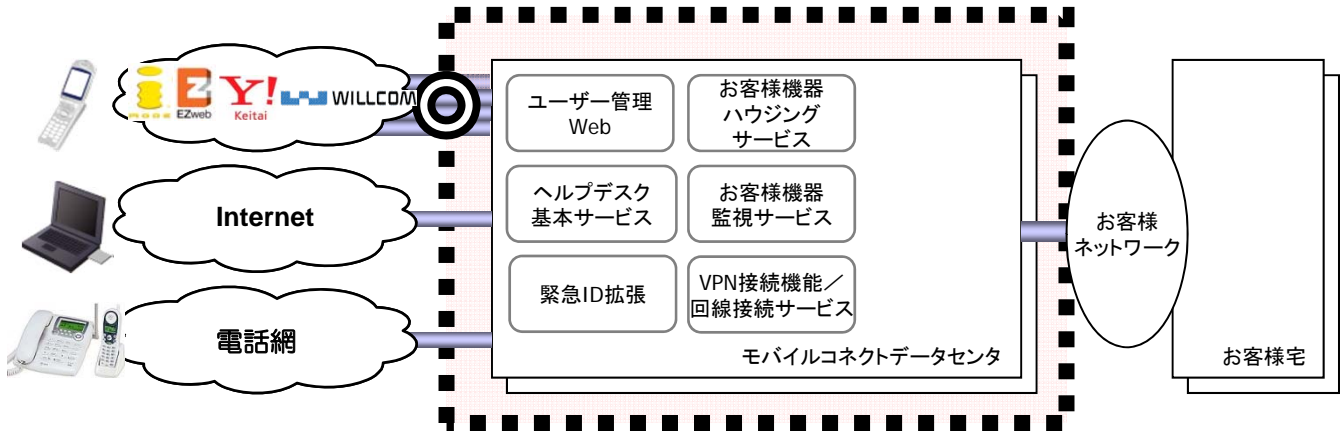
サービス提供範囲



ご利用条件		
項目	概要	
ユーザー管理Web	端末条件	【対応OS/対応ブラウザ】 「ご利用条件/対応OS」をご確認ください ※64bitブラウザを除く ※TLS 1.0のみ対応 【インターネット】 エンドユーザー管理用に、インターネットに接続可能なPCが必要です。 【留意事項】 ※端末1台につき、1ブラウザでの動作を保証します。 ※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の[戻る]ボタン等の操作は保証対象外となります。) ※端末や通信状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外となります。
	ユーザー管理Web用クライアント証明書	企業管理者がユーザー管理Webへアクセスする際、PCのクライアント証明書(ペリサイン認証)と固定パスワードによる認証を行ないます。従って、ユーザー管理Webを利用されるPCへクライアント証明書インストールして頂く必要があります。証明書の有効期限は発行より1年のため、期限切れ前に更新のお願いをさせていただきます。
	CSVファイル自動アップロード	お客様宅にFTPサーバーを設置していただきます。FTPサーバはパッシブモードに設定して下さい。アクティブモードではご利用になれません。 お客様宅のFTPサーバからファイルを取得してアップロード処理を行う実行頻度、時刻は、下記とします。 実行頻度:1日1回 実行時刻:毎日23時～6時の間に実行 ※ただし、メンテナンス作業実施日については、実行されない場合があります。 ※複数のお客様の処理を行うため、上記時間帯の中で実効時間に変更される場合があります。
	グループ管理者	グループ管理者には次の制限事項があります。 ※for メール管理機能をご利用になれません。 ※for グループウェアの管理機能をご利用になれません。

モバイルコネクト基本サービス

サービス提供範囲



ご利用条件		
項目		概要
お客様ハウジングサービス		モバイルコネクトネットワーク機器とお客様ネットワーク機器のI/Fは、10Base-T・100Base-TX/全二重・半二重/Autoネゴシエーションよりお客様にご選択いただきます。コネクタ形状はRJ-45となります。モバイルコネクトサービスのご利用に関連の無い機器は設置できません。
お客様機器監視サービス		モバイルコネクトのご利用に関連のない機器の監視はできません。
VPN接続機能	接続先	UniversalOne、統合VPNがご利用になれます。
	利用可能サービス	ケータイアクセス、SSL-VPN Webアクセス、Radius連携サービス、SSL-VPNマルチアクセス、SSL-VPNマルチアクセス・ライト、IPSecアクセス、クローズドネットワークアクセス、ケータイタイプ for グループウェア、スマートフォンタイプ for グループウェア
回線接続サービス	接続先	UniversalOne、統合VPNがご利用になれます。
	利用可能サービス	ケータイアクセス、SSL-VPN Webアクセス、Radius連携サービス
緊急ID拡張	利用可能サービス	SSL-VPNマルチアクセス・ライトのみご利用可能なオプションです。 基本ID数とは別に、5,000IDを上限として、最大で基本ID数の5倍までご利用可能です。

モバイルコネクト基本サービス

提供機能・ご利用条件		
項目		概要
サービス運用	システム構成	機器・ネットワークの冗長構成 ※ユーザー個別設置機器及び一部の機器、NWは冗長構成とならない場合があります。
	ネットワーク	各携帯電話事業者ネットワークからの閉域接続回線、インターネット接続回線及び公衆電話網回線は、外部の各種サービスを利用しております。従って、各種サービス提供者の障害、メンテナンス等により、モバイルコネクトサービスの全部または一部が提供できない場合があります。
	データセンタ設備	弊社データセンタへ機器を設置
	機器監視	機器の障害/リソース状況の24時間365日監視
	不正侵入・不正アクセス対策	システム、ネットワーク、ファシリティ等のセキュリティ対策とセキュリティ技術者の運用により、不正侵入・不正利用、盗聴・改竄等の対策
ヘルプデスク基本サービス	対応時間	24時間 365日対応
	故障受付窓口	モバイルコネクトヘルプデスク TEL:0120-127-703 E-mail:mc-help@ntt.com
	対応言語	日本語
	対応者	企業管理者様からのお問合せ
	事前登録	企業管理者様の事前申請が必要です
	サービス内容	モバイルコネクトを導入されたお客様の業務が円滑に進むよう、ヘルプデスクにて運用面をバックアップします。 ・企業管理者様からのモバイルコネクトに関する問い合わせ受付 ・企業管理者様からの故障受付および一次切り分け ・企業管理者様に対するサービス停止(故障、定期メンテナンスなど)連絡(E-mailのみ)
エンドユーザ問い合わせサービス	対応時間	平日9:00～17:30 (日本時間)※24時間365日の対応も可能
	故障受付窓口	モバイルコネクトヘルプデスク TEL:0120-127-703 E-mail:mc-help@ntt.com
	対応言語	日本語
	対応者	エンドユーザからのお問合せ
	サービス内容	・モバイルコネクトエンドユーザ様(利用者様)からのモバイルコネクト操作問い合わせ受付 ・モバイルコネクト利用者様からの不具合受付
ユーザー管理代行サービス	対応時間	平日9:00～17:30 (日本時間)※24時間365日の対応も可能
	故障受付窓口	モバイルコネクトヘルプデスク TEL:0120-127-703 E-mail:mc-help@ntt.com
	対応言語	日本語
	対応者	エンドユーザからのお問合せ
	サービス内容	エンドユーザ問い合わせサービスに加えて、以下の業務を実施します。 ・利用者情報の登録・変更・削除 ・モバイルコネクト利用者様のアカウント関連業務 ・アカウントロック解除 ・アクセスログのダウンロード ・ポータル画面作成依頼及びテスト(オプションサービスをご利用の場合)
オプション	サービス内容	日本語および英語で24時間365日対応します。 対象:「エンドユーザ問い合わせサービス」および「ユーザー管理代行サービス」
Bizマネージドセキュリティサービス MDM ヘルプデスク	サービス内容	「Bizマネージドセキュリティサービス MDM」に関するヘルプデスク基本サービスを提供します。 ※モバイルコネクトをご利用のユーザと同一のユーザが「Bizマネージドセキュリティサービス MDM」をご利用される場合に限りです。 ※エンドユーザ問い合わせサービス、ユーザー管理代行サービスはご利用頂けません。

※「エンドユーザ問い合わせサービス」、「ユーザー管理代行サービス」は、「ケータイタイプ「グループウェア」、「スマートフォンタイプ「グループウェア」サービスでは対象外となります。

モバイルコネクト基本サービス

ご利用条件/対応OS

OS			モバイルコネクト 認証サービス		SSL-VPN Webアクセス (スマートフォン for Web /forメール ※2	SSL-VPN Webアクセス for Web /forメール	SSL-VPN マルチアクセス	SSL-VPN マルチアクセス・ライト	
			MCOP 認証	機体 認証				Pulse Secure	Any Connect
Android	2.3~3.x		○	○	○	-	×	×	×
	4.0~5.x		○	○	○	-	○	○	○
	6.0		○	○	○	-	×	○	○
iOS		6.0~9.3	○	○	○	-	○ ※3	○	○
Windows ※1	Vista (SP2)	IE9	○	○	-	○	○	○	○ ※5
	7(SP1)	IE11	○	○	-	○	○	○	○
	8.1	IE11	○	○	-	○	○	○	○
	10	IE11	○	○	-	○	×	○ ※4	○ ※5

ご利用条件/対応OS

OS			Radius 連携	クロスド ネットワークアクセス	スマートフォンタイプ for グループウェア ※2	for SaaS	ユーザー管理Web ※6
Android	2.3~3.x		-	-	○	○	-
	4.0~5.x		-	-	○	○	-
	6.0		-	-	○	○	-
iOS		6.0~9.3	-	-	○	○	-
Windows ※1	Vista (SP2)	IE9	○	○	-	○	○
	7(SP1)	IE11	○	○	-	○	○
	8.1	IE11	○	○	-	○	○
	10	IE11	○	○	-	○	○

※1 すべてIE64bitブラウザを除きます。

※2 携帯電話の端末対応条件は、各サービス仕様をご参照ください。

※3 スマートフォン利用(SD)において、iOS7.xはEdge Client 2.0.8以降はご利用いただけません。

スマートフォン利用(SD)において、iOS9.xはEdgeClient ver2.0.9をご利用の場合、モバイルコネクトアプリ認証後、Edge Clientが起動せずVPN接続が不可となる場合がございます。回避策として、モバイルコネクトアプリ認証前に事前にEdgeClientアプリをタップし、アプリを起動した上でモバイルコネクト認証を実施頂くと正常に接続可能となりますので、本回避手順を実施の上接続頂くことを推奨致します。

※4 2016年7月~9月、お客様SSL-GW機器毎にVerUPを行います。VerUP後はWindows10が利用可能です。

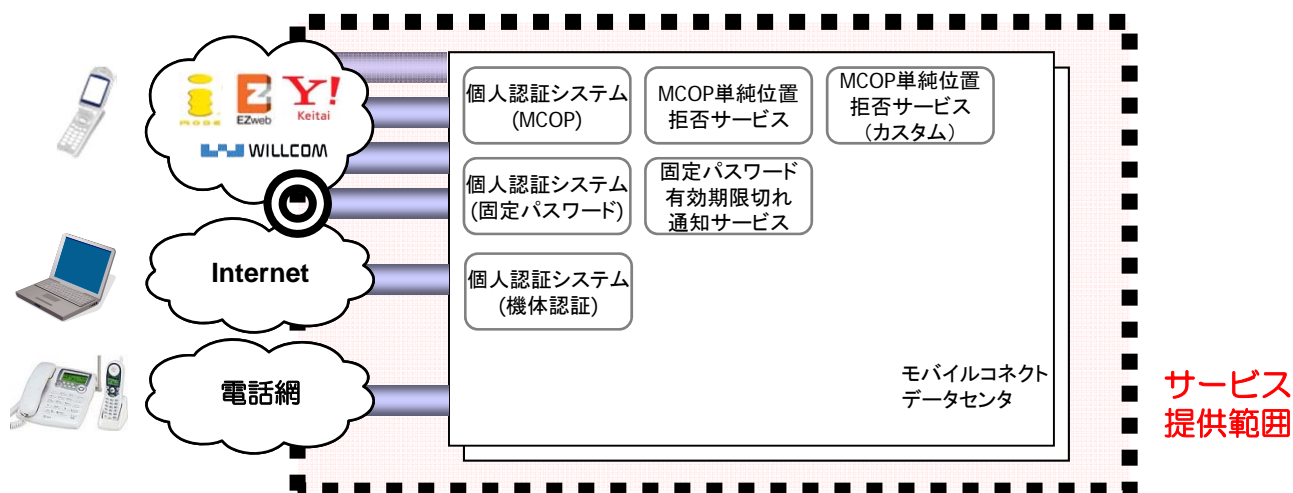
※5 2016年7月~9月、お客様SSL-GW機器毎にVerUPを行います。ただし機器仕様によりWindows10対応を行うとWindowsVistaが利用出来なくなることから、ご希望のお客様より提供を行います。

WindowsVistaはマイクロソフト社が2017年4月11日にサポート終了予定です。モバイルコネクトについても同日を持ってサポート終了予定です。

※6 IE10以降ご利用時はブラウザの互換表示設定に追加して頂く必要がございます。

「安否確認/一斉通報サービス」については、各サービス仕様をご確認ください。

モバイルコネクト認証サービス



提供機能

項目	概要
アプリケーション (認証)	MCOP認証
	MCOP単純位置拒否サービス
	MCOP単純位置拒否サービス (カスタム)
	固定パスワード認証
	固定パスワード有効期限切れ通知サービス
	機体認証

ご利用条件

項目	説明
利用可能サービス	MCOP認証
	固定パスワード認証
	機体認証
端末条件	機体認証 (PC)
	対応OS
	対応ブラウザ
	留意事項
	その他

モバイルコネクトサービス仕様-3

モバイルコネクトサービス
基本仕様書(第15.0.3版)

ケータイアクセス／for Web／for メール

サービス提供範囲



提供機能		
項目	概要	
社内メール連携	お客様社内にあるメールサーバと連携し、メール送信、受信、転送、返信、署名、アドレス帳(オプション)、新着メール通知(オプション)機能を提供するサービスです。	
	連携サーバ追加	連携するメールサーバが複数台ある場合、メールサーバ(IPアドレス)を1台単位で追加するサービスです。
	アドレス帳	モバイルコネクトデータベースに登録したアドレス帳をご利用いただくサービスです。
	新着メール通知	利用者があらかじめ設定した条件のメールが新規に届いている場合、指定のメールアドレスへ通知するサービスです。
コンテンツ連携	お客様のWebアプリケーションと連携するサービスです。	
	連携メニュー追加	コンテンツ連携するメニューが複数リンクある場合、モバイルコネクトトップメニューに1メニュー単位で追加するサービスです。
	シングルサインオン	コンテンツ連携時に、連携先コンテンツに利用者のログイン情報を受け渡す事により、コンテンツアクセス時に認証を行わずに利用する事ができるサービスです。
	URL変換	お客様のWebコンテンツが絶対パスや絶対URLで記述されている際に、特定文字列を指定した文字列に変換し、通信を可能にするサービスです。 具体的には、 ・連携アプリケーションに絶対URL、絶対パス記述が存在する場合 ・Cookieの払い出しがdomain/path指定されている場合 ・複数サーバで同一のCookie名を使用している場合 にURL変換サービスが必要となります。
グループウェアコネクト	モバイル端末(携帯電話ブラウザ)を利用して、お客様社内内で運用中のグループウェアを社外から安全に利用することができるサービスです。	
	新着メール通知機能	利用者があらかじめ設定した条件のメールが新規に届いている場合、指定のメールアドレスへ通知するサービスです。
	独自DB追加サービス (Notes版のみ)	Dominoサーバ上の業務DBを連携機能に追加します。 カスタマイズが発生する為、詳細についてはご相談ください。
	英語化オプション (Notes版のみ)	Notes英語版に対応し、ユーザインターフェースを英語化致します。
ポータルサービス	企業管理者様にて、携帯電話向けの初期画面とトップメニューの文言のカスタマイズを行うことができるサービスです。	
機体番号認証サービス	各携帯電話本体に格納されているユニークな機体番号を認証情報としてログインを制御することができるサービスです。	
	パスワード認証スキップ	本人認証のMCOPまたは固定パスワードをスキップすることができるサービスです。
TEL Directory	電話番号、メールアドレス等のデータをネットワークにて格納する、ネットワーク電話帳機能を持つサービスです。	
ネットワーク	携帯キャリアからの専用線での接続	
セキュリティ対策	本人認証	・MCOP方式 (Mobile Connect One-time Password) ・固定パスワード ・機体番号認証
	セッション管理	ユーザ毎にURL単位でコントロール
	侵入防止対策	Firewall、セキュリティ管理システム
	盗聴改ざん対策	・携帯キャリアからの専用線接続 ・SSL対応 (i-mode)
その他	ユーザー管理Web	インターネット環境でPKI認証による接続
	耐障害性性能	ユーザ情報データベース、Webサーバ、ネットワーク機器は全て冗長構成

モバイルコネクサービス仕様-3

モバイルコネクサービス
基本仕様書(第15.0.3版)

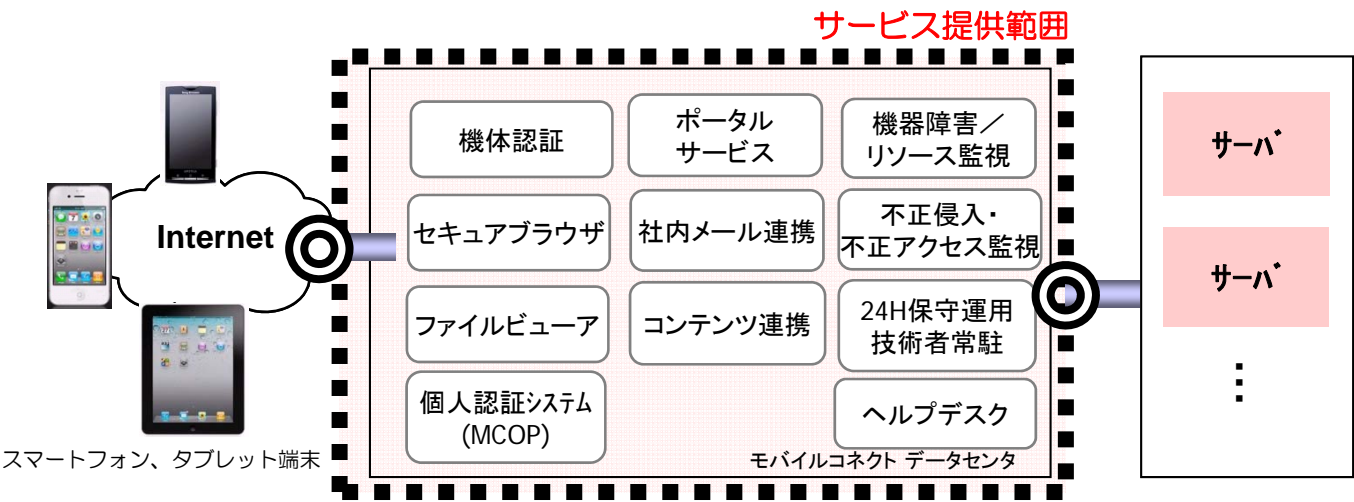
ケータイアクセス／for Web／for メール

ご利用条件		
項目	説明	
端末対応条件		NTTドコモ:i-mode対応端末(HTML機) au:A5000/C5000/C3000/A1100シリーズ以降の端末(HDML機は非対応) Softbank Mobile: Yahoo!ケータイ対応端末(但し、C2型端末及びモトローラ社製702MO、702sMOは非対応) WILLCOM: HTML対応端末
	留意事項	※端末1台につき、1ブラウザでの動作を保証します。 ※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の「戻る」ボタン等の操作は保証対象外となります。) ※端末や通信状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外となります。
社内メール連携		お客様のメールサーバが、POP3・IMAP4・SMTPに対応していること。
	連携サーバ追加	メールサーバの登録数はPOP3・IMAP4・SMTP合わせて20サーバまで。 ※1ユーザで複数サーバ・複数プロトコルの利用はできません。 ※POP3の場合、メールサーバのメッセージ並び替え順を昇順に設定する必要があります。 ※メールの対応文字コードは、iso-2022-jp、shift_jis、euc_jp、utf-7、utf-8となります。
	アドレス帳	登録件数は100件まで
	新着メール通知	お客様のメールサーバ(POP3)が、RFC2076で定めるSTATUS情報を返す仕様であること。
コンテンツ連携		相対パスで記述されたhttp通信のアプリケーションで、利用する端末で参照可能な言語で記述されていること。 【絶対パス、絶対URLで記述されたアプリケーションであればURL変換サービスが必要となります。】
	シングルサインオン	お客様Webコンテンツ側へGETもしくはPOSTによりログイン情報を引き渡した際に、お客様側で認証を行う機能があること。
	URL変換	・圧縮コンテンツなどのバイナリデータ、JavaScriptなどで動的に生成されるコンテンツ内のソースについてはURL変換を行うことが出来ない場合があります。 ・ソース内の記述を変換する文字列として指定できる文字コードは「ASCIIコード」のみになります。 ・変換元の文字列は大文字、小文字の区別は出来ません。
グループウェアコネク		・グループウェア条件 Notes対応版: Domino Server R6.5.x、R7.0.x、R8.0.x、R8.5.x (ただし、R6.5.xの新規受付は終了しております。) Exchange対応版: Exchange 2000、2003、2007、2010(SP1)Server対応。(ただし、2000の新規受付は終了しております。) ※グループウェア上で扱われる文字コードがShift-jisへ文字コード変換できるものであること。 ※一部の機種依存文字(NEC 特殊文字(13 区文字)、NEC 選定IBM 拡張文字(89-92 区文字)、IBM 拡張文字(115-119 区文字)等)は非サポートとなります。 ※グループウェアコネクサーバからお客様Exchangeサーバへの認証方式について Exchange2007以前ではNTLM認証、基本認証への対応となります。Exchange2010ではダイジェスト認証、基本認証への対応となります。(EWS仮想ディレクトリ設定において、ダイジェスト認証(もしくは基本認証)と合わせて匿名認証を、有効にする必要があります。)
機体番号認証サービス		・機体番号認証サービスのみのご利用はできません(本人認証のMCOPまたは固定パスワードとあわせてのご提供となります)なおパスワード認証スキップ(オプション)をご利用の場合は、本人認証のMCOPまたは固定パスワードをスキップすることが可能です。 ・1モバイルコネクユーザアカウントにつき1台の機体番号のみ認証情報として登録できます ・端末対応条件(上記ケータイアクセス共通端末対応条件に加えて) NTTドコモ:i-mode対応HTMLバージョン3.0以降のブラウザを搭載した携帯電話のみ対応。 (SO210i、SH251i、SH251iS、D503i、D503iS、N2001、N2002、SH900iは非対応) au:A5000/C5000/C3000/A1100シリーズ以降の端末(HDML機不可) Softbank Mobile: Yahoo!ケータイ対応端末(但し、モトローラ社製702MO、702sMO、及びJ-SH53は非対応) TU-KA: WAP2.0対応端末(XHTML機) WILLCOM: HTML対応端末 * 端末種別にかかわらずフルブラウザを利用しての機体番号認証サービスはご利用できません。
TEL Directory		・TEL Directoryのみのご利用はできません。(同ID数のケータイアクセスご契約が必要) ・認証は、MCOP認証をご利用いただきます。(固定パスワードとの組み合わせは不可) ・1IDあたり、電話帳500件まで登録可能です。 ・利用者ID、電話帳データの登録・メンテにつきましては、お客様にて実施いただきます。 ・ヘルプデスク(ユーザー管理代行サービス)をご利用の場合、TEL Directoryサーバへの各種登録・管理作業(利用者ID登録、電話帳データ登録作業等)は対象外となります。 ・端末対応条件(携帯)・・・ケータイアクセスの端末対応条件に従います。 ・端末対応条件(PC)・・・以下のいずれかの端末 【対応OS】Windows Vista (SP2)、Windows 7 (SPなし) ※全てのOSに対し64bitOSを除く 【対応ブラウザ】Internet Explorer 7.0、8.0 (ActiveXが動作する環境であること) ※IE7.0、8.0を利用する際は、別途、モジュール適用及び設定が必要になる場合があります。 【他】ブラウザのActiveXの動作許可設定、Admin権限が必要です。 ・TEL Directory設備の保守上必要な場合に、メンテナンス工事を実施することがあります。
利用条件	NTTコムデータセンター～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になれます。 (一部の回線品目でご利用にならない場合があります。) 注: 一部回線品目ではVPN装置もしくはルーターが必要になります。
	最小ご利用者数	1ユーザ

モバイルコネクトサービス仕様-4

モバイルコネクトサービス
基本仕様書(第15.0.3版)

SSL-VPN Webアクセス(スマートフォン)／for Web／for メール



提供機能		
項目		概要
セキュアブラウザ		端末にキャッシュ等のデータを残さない機能です。
ファイルビューア		端末にファイルを保存することなく、office文書やpdfファイルをブラウザで参照できます。 ※クラウドサービス連携のファイルビューア機能は、連携するサービスの仕様に準じます。
スマートフォン動作制御	モバイルコネクト利用時のスマートフォン、タブレット端末の動作を制御します。	
	アプリケーション起動制御	モバイルコネクト利用時のアプリケーション起動リンクから、他のアプリケーションを起動する場合の動作について制御します。
	アクセス制御	連携サーバ以外の外部サイトへのアクセスを制御します。
接続情報		各コンテンツへの接続情報が閲覧可能です。
社内メール連携	お客様社内にあるメールサーバと連携し、メール送信、受信、転送、返信、署名、アドレス帳(オプション)を提供するサービスです。	
	連携サーバ追加	連携するメールサーバが複数台ある場合、メールサーバ(IPアドレス)を1台単位で追加するサービスです。
	アドレス帳	モバイルコネクトデータベースに登録したアドレス帳をご利用いただくサービスです。
コンテンツ連携		お客様のWebアプリケーションまたはクラウドサービスと連携するサービスです。
	連携メニュー追加	コンテンツ連携するメニューが複数リンクある場合、モバイルコネクトトップメニューに1メニュー単位で追加するサービスです。
	シングルサインオン	コンテンツ連携時に、連携先コンテンツに利用者のログイン情報を受け渡す事により、コンテンツアクセス時に認証を行わずに利用する事ができるサービスです。
	URL変換	お客様のWebコンテンツが絶対パスや絶対URLで記述されている際に、特定文字列を指定した文字列に変換し、通信を可能にするサービスです。 具体的には、 ・連携アプリケーションに絶対URL、絶対パス記述が存在する場合 ・Cookieの払い出しがdomain/path指定されている場合 ・複数サーバで同一のCookie名を使用している場合 にURL変換サービスが必要となります。
ポータルサービス		ログイン後に表示するトップ画面にリンクメニューを設ける事ができます。
接続端末 & ネットワーク		Internetに接続されたスマートフォン、タブレット端末
セキュリティ対策	本人認証	・MCOP方式 (Mobile Connect One-time Password) ・固定パスワード ・機体認証
	端末制限	AndroidOS：当社においてRoot化の疑いがあると判断される端末、および、USBデバッグが設定されている端末を検知し、ブロックします。 iOS：当社においてJailBreakの疑いがあると判断される端末を検知し、ブロックします。
	セッション管理	URL単位でコントロール、または、Cookieによるコントロール(選択可能) ※ファイルビューア利用時はCookieによるコントロールのみ利用可能です。
	侵入防止対策	FireWall、セキュリティ管理システム
	盗聴改ざん対策	128bitSSLトンネリング
その他	ユーザー管理Web	インターネット環境でPKI認証による接続
	耐障害性性能	ユーザ情報DB、Webサーバ、ネットワーク機器、変換サーバは全て冗長構成

SSL-VPN Webアクセス(スマートフォン)／for Web／for メール

ご利用条件		
項目	説明	
端末条件	スマートフォンシステム要件	対応OSVer(「ご利用条件/対応OS」参照)・モバイルコネクセキュアブラウザ ※上記搭載端末で動作可能です。但しOSのバージョンや端末固有の問題及びお客様の端末設定、利用状況等によっては一部動作しない可能性があります。 ※iPad touchは対象外です。 ※キャリア/メーカー保証対象外の端末(改造された端末等)はサポート対象外です。
	留意事項	・端末1台につき、1ブラウザでの動作を保証します。 ・OS、端末によって動作が異なる場合があります。 ・端末や通信状況によっては、画面表示に時間がかかる場合があります。
	機体認証	・機体認証は1ユーザにつき5端末利用可能です。 ・機体認証における機体識別情報は変更する場合があります。 ・端末の初期化等の変更を実施した場合、再度、初期設定が必要になります。
	ログイン条件チェック	Android：モバイルコネクで指定するアプリケーションのプロセス、サービスの起動有無をチェックします。アプリケーションの設定内容に関わらず、指定するプロセス、サービスが起動している場合は、起動状態と判断します。 iOS：モバイルコネクで指定するアプリケーションのインストール有無をチェックします。インストールされている場合は、アプリケーションの起動有無、設定内容に関わらず、インストール状態と判断します。 ※ログイン条件については設定したグループに属するSSL-VPNマルチアクセス(SD)にも適用されます。 ※指定するアプリケーションについては変更になる場合がございます。また、指定するアプリケーションの仕様変更や端末固有の問題、お客様の端末設定、利用状況等によっては一部動作しない可能性があります。
	セキュアブラウザ	・一定時間無操作の場合、タイムアウトとなります。 ・キャッシュ等のデータ消去についてはアプリを正常に終了した場合に動作します。 ・初期設定時に標準搭載ブラウザ以外のブラウザをご利用の場合、正常に動作しない可能性がありますので、標準搭載ブラウザにて初期設定を実施ください。 ・スマートフォンアプリケーションの強制停止を行った場合は、正常に動作しない場合があります。 ・URLの表示およびブックマークはできません。
	ファイルビューア	・添付ファイルのページ数制限は最大99ページです。 ・改ページ位置及びページ数がPC閲覧時と異なる場合があります。 ・テキストファイル(拡張子txt)は、文字コードがUTF-8またはShift-JISのファイルのみ正常に閲覧可能です。 ・Excel文書は、シート設定等の条件によっては閲覧できない場合があります。 （データが保護されているページやシート非表示のデータ、印刷できるものを含まないデータなど） ・プリンター印刷時の画像が表示されます。 特にExcelの場合、ページ設定が適切にされていない場合は、内容が途中で切れたような表示になります。 ・マクロは無効になります。 ・書き込み制限がかかったPowerPointファイル(書き込みパスワード又はデジタル署名又は最終版が設定されたファイル)は、(出力用紙サイズに合わせた拡張ができないため、)余計な余白が含まれていたり、出力イメージが出力用紙サイズのフチで切られた画像となることがあります。 ・Microsoftオフィスファイル、PDFファイル、Zipファイルのパスワードがかかったファイルも閲覧可能です。 ・ファイルのパスワードに関する制限は以下になります。 文字数制限:最大64文字 文字種制限:半角英数記号 ・5MBを超過するファイルは閲覧できません。 ・圧縮ファイル内のファイル数は最大100件です。 それ以上のファイル件数がある場合は、「最大表示件数を超過しました。」というダイアログが表示されます。 ・Zipファイル内に階層がある場合も閲覧可能です。ただし、階層数に関わらず、同一フォルダにあるようにファイルはフラットに表示されます。階層は階層パス長259文字まで閲覧可能です。 ・Zipファイル内のZipファイルは閲覧できません。 ・圧縮ファイル作成ツールによっては、ファイルを解凍できない場合もあります。 ・Windows(日本語版)以外のOS、環境(MacやLinux等)で圧縮されたzipファイルは文字化けする、または変換不可な場合があります。 ・圧縮ファイル内のファイル名に、NEC機種依存文字及び一部の記号(～//ー¢&一)等を含むファイルは、正しく解凍出来ない場合があります。また、各種IBM拡張文字(NEC 選定IBM 拡張文字(89-92 区文字)、IBM 拡張文字(115-119 区文字))には対応しておりません。
社内メール連携		Excel(xls、xlsx)、Word(doc、docx)、PowerPoint(ppt、pptx)、PDF(pdf)、テキストファイル(txt)、画像ファイル(jpeg、jpg、png、gif)、Zip(zip) ※上記以外のファイルは閲覧不可(保存も不可)です。
コンテンツ連携		Excel(xls、xlsx)、Word(doc、docx)、PowerPoint(ppt、pptx)、PDF(pdf)、テキストファイル(txt)、Zip(zip) ※上記以外のファイルは閲覧不可(保存は可(セキュアブラウザを利用した場合は保存も不可))です。 ※5MBを超過する圧縮ファイルは閲覧できません。

SSL-VPN Webアクセス(スマートフォン)／for Web／for メール

ご利用条件		
項目		説明
スマートフォン動作制御		モバイルコネクト利用時のスマートフォン、タブレット端末の動作を制御します。
	アプリケーション起動制御	一部コンテンツにおいては制御できない場合があります。
	アクセス制御	一部コンテンツにおいては制御できない場合があります。
接続情報		・サービス提供開始(本機能提供開始日)より5年間の接続情報を保持します。利用者による閲覧は、利用月含む過去4ヶ月分の情報が閲覧可能です。 ・接続情報の集計は以下のとおり実施します。 集計頻度: 1日1回 集計時刻: 毎日0時～9時の間に前日分の接続情報を集計 ※ただし、メンテナンス作業実施日等、実行されない場合があります。 ※複数のお客様の処理を行うため、上記時間帯の中で実効時間が変更される場合があります。
社内メール連携		お客様のメールサーバが、POP3・IMAP4・SMTPに対応していること。 ※1ユーザで複数サーバ・複数プロトコルの利用はできません。 ※POP3の場合、メールサーバのメッセージ並び替え順を昇順に設定する必要があります。 ※メールの対応文字コードは、iso-2022-jp、shift_jis、euc_jp、utf-7、utf-8となります。 ※セキュアブラウザ利用時に新着メール通知サービスはご利用になれません。 ※ファイルアップロード機能は一部の端末ではご利用いただけません。 弊社の動作確認においてはAndroid4.1以上、iOS5.x以下の端末で動作不可であることを確認しています。
	連携サーバ追加	メールサーバの登録数はPOP3・IMAP4・SMTP合わせて20サーバまで。
	アドレス帳	登録件数は100件まで
コンテンツ連携		相対パスで記述されたhttp通信のアプリケーションで、利用する端末で参照可能な言語で記述されていること。 【絶対パス、絶対URLで記述されたアプリケーションであればURL変換サービスが必要となります。】
	シングルサインオン	お客様Webコンテンツ側へGETもしくはPOSTによりログイン情報を引き渡した際に、お客様側で認証を行う機能があること。
	URL変換	・圧縮コンテンツなどのバイナリデータ、JavaScriptなどで動的に生成されるコンテンツ内のソースについてはURL変換を行うことが出来ない場合があります、 ・ソース内の記述を変換する文字列として指定できる文字コードは「ASCIIコード」のみになります。 ・変換元の文字列は大文字、小文字の区別は出来ません。
セキュリティ対策	端末制限	※同一IDで、SSL-VPNマルチアクセス(SD)を併せてご利用される場合は、同様に適用されます。 ※端末固有の問題やお客様の端末設定、利用状況等によっては一部動作しない可能性がございます。
利用条件等	NTTコムデータセンター～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になれます。 (一部の回線品目でご利用になれない場合があります。) 注: 一部回線品目ではVPN装置もしくはルーターが必要になります。
	最小ご利用者数	1ユーザ

モバイルコネクトサービス仕様-5

モバイルコネクトサービス
基本仕様書(第15.0.3版)

SSL-VPN Webアクセス／for Web／for メール

サービス提供範囲



提供機能		
項目		概要
社内メール連携		お客様社内にあるメールサーバと連携し、メール送信、受信、転送、返信、署名、アドレス帳(オプション)を提供するサービスです。
	連携サーバ追加	連携するメールサーバが複数台ある場合、メールサーバ(IPアドレス)を1台単位で追加するサービスです。
	アドレス帳	モバイルコネクトデータベースに登録したアドレス帳をご利用いただくサービスです。
	新着メール通知	利用者があらかじめ設定した条件のメールが新規に届いている場合、指定のメールアドレスへ通知するサービスです。
コンテンツ連携		お客様のWebアプリケーションと連携するサービスです。
	連携メニュー追加	コンテンツ連携するメニューが複数リンクある場合、モバイルコネクトトップメニューに1メニュー単位で追加するサービスです。
	シングルサインオン	コンテンツ連携時に、連携先コンテンツに利用者のログイン情報を受け渡す事により、コンテンツアクセス時に認証を行わずに利用する事ができるサービスです。
	URL変換	お客様のWebコンテンツが絶対パスや絶対URLで記述されている際に、特定文字列を指定した文字列に変換し、通信を可能にするサービスです。 具体的には、 ・連携アプリケーションに絶対URL、絶対パス記述が存在する場合 ・Cookieの払い出しがdomain/path指定されている場合 ・複数サーバで同一のCookie名を使用している場合 にURL変換サービスが必要となります。
ポータルサービス		ログイン後に表示するトップ画面にリンクメニューを設ける事ができます。
接続端末 & ネットワーク		Internetに接続されたPCデバイス ※携帯電話ブラウザからの接続にはケータイアクセスのお申込が必要です。
セキュリティ対策	本人認証	・MCOP方式 (Mobile Connect One-time Password) ・固定パスワード ・機体認証
	セッション管理	URL単位でコントロール、またはCookieによるコントロール(選択可能)
	侵入防止対策	FireWall、セキュリティ管理システム
	盗聴改ざん対策	128bitSSLトンネリング
その他	ユーザー管理Web	インターネット環境でPKI認証による接続
	耐障害性性能	ユーザ情報DB、Webサーバ、ネットワーク機器、変換サーバは全て冗長構成
ご利用条件		
項目		説明
端末条件	クライアントPCシステム要件	【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 ※TLS 1.0のみ対応 【その他】上記以外はお客様コンテンツの必要要件に準じます
端末条件	留意事項	※端末1台につき、1ブラウザでの動作を保証します。 ※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の[戻る]ボタン等の操作は保証対象外となります。) ※端末や通信状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外となります。

SSL-VPN Webアクセス／for Web／for メール

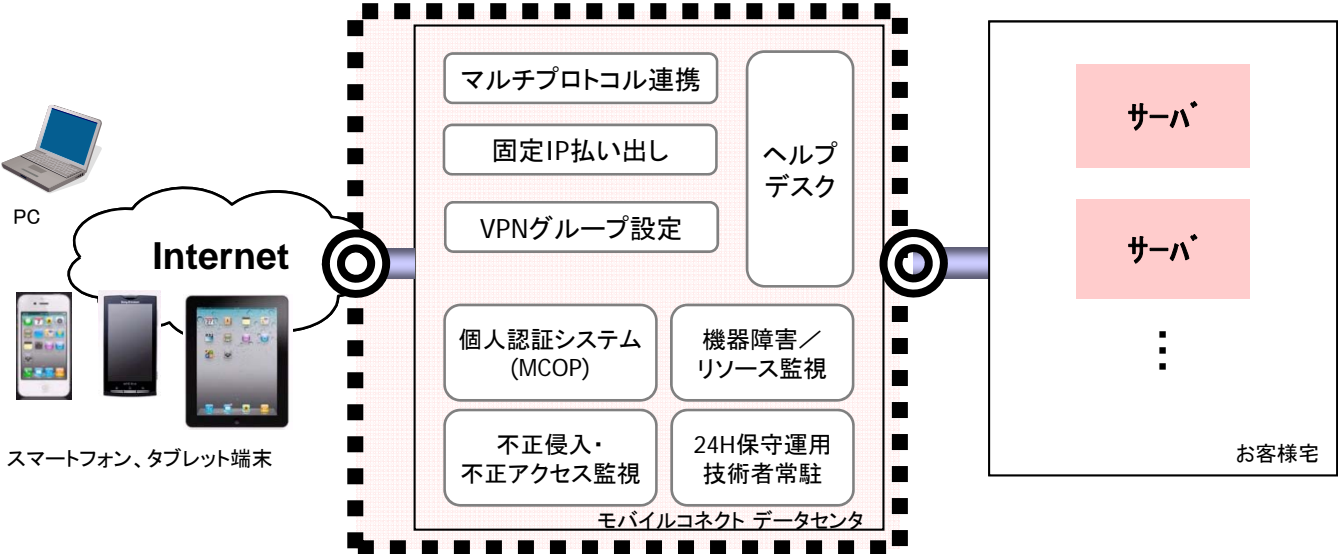
ご利用条件		
項目		説明
社内メール連携		お客様のメールサーバが、POP3・IMAP4・SMTPに対応していること。 ※1ユーザで複数サーバ・複数プロトコルの利用はできません。 ※POP3の場合、メールサーバのメッセージ並び替え順を昇順に設定する必要があります。 ※メールの対応文字コードは、iso-2022-jp、shift_jis、euc_jp、utf-7、utf-8となります。
	連携サーバ追加	メールサーバの登録数はPOP3・IMAP4・SMTP合わせて20サーバまで。
	アドレス帳	登録件数は100件まで
	新着メール通知	お客様のメールサーバ(POP3)が、RFC2076で定めるSTATUS情報を返す仕様であること。
コンテンツ連携		相対パスで記述されたhttp通信のアプリケーションで、利用する端末で参照可能な言語で記述されていること。 【絶対パス、絶対URLで記述されたアプリケーションであればURL変換サービスが必要となります。】
	シングルサインオン	お客様Webコンテンツ側へGETもしくはPOSTによりログイン情報を引き渡した際に、お客様側で認証を行う機能があること。
	URL変換	・圧縮コンテンツなどのバイナリデータ、JavaScriptなどで動的に生成されるコンテンツ内のソースについてはURL変換を行うことが出来ない場合があります、 ・ソース内の記述を変換する文字列として指定できる文字コードは「ASCIIコード」のみになります。 ・変換元の文字列は大文字、小文字の区別は出来ません。
利用条件等	NTTコムデータセンタ～お客様との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になれます。 (一部の回線品目でご利用になれない場合があります。) 注：一部回線品目ではVPN装置もしくはルーターが必要になります。
	最小ご利用者数	1ユーザ

モバイルコネクトサービス仕様-6

モバイルコネクトサービス
基本仕様書(第15.0.3版)

SSL-VPN マルチアクセス

サービス提供範囲



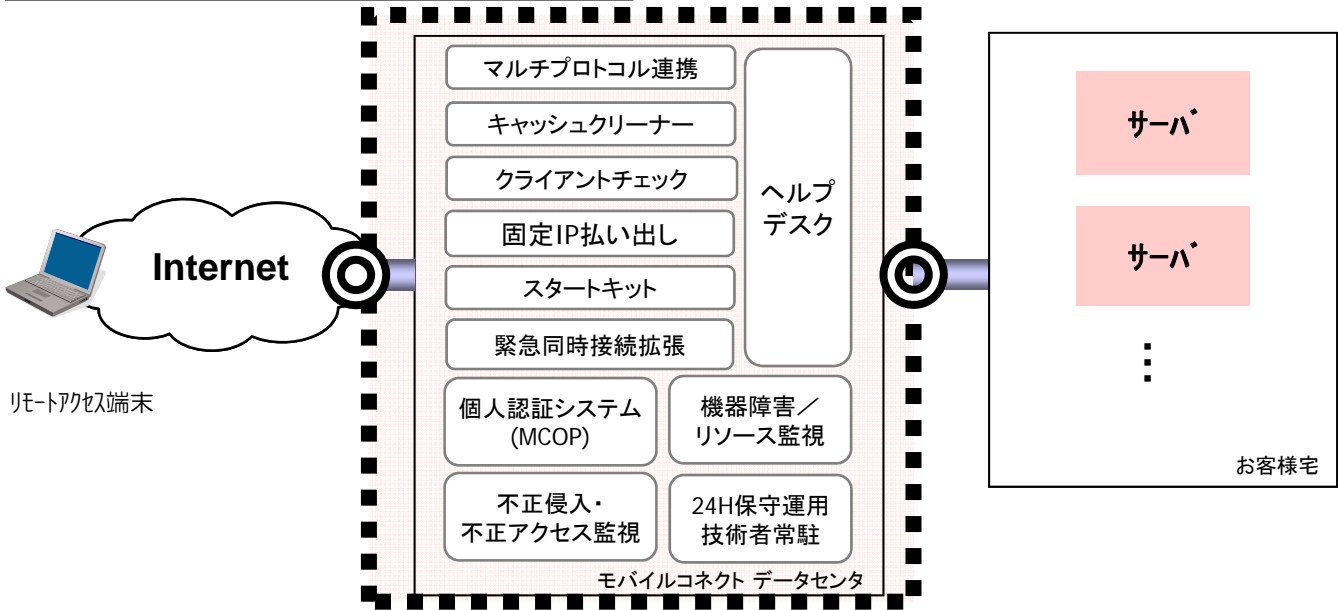
提供機能		
項目		概要
マルチプロトコル対応		お客様のPCからの接続に対して、SSLでの通信(デフォルトUDP/4433。UDP/4433をご利用できない環境ではTCP/443へ自動切替)を提供します。
固定IP払い出し		ユーザIDにIPアドレスをRadiusが固定的に払い出します。
VPNグループ設定		サービス提供時に、VPNグループ設定を実施します。
接続端末 & ネットワーク		Internetに接続されたデバイス (PC、スマートフォン、タブレット端末。携帯電話には対応していません)
セキュリティ対策	本人認証	・MCOP方式 (Mobile Connect One-time Password) ・固定パスワード ・機体認証 (スマートフォンに関しては、SSL-VPNマルチアクセス (SD) のみ対応)
	セッション管理	SSL-VPN装置でコントロール、最大接続時間は480分 (固定)
	侵入防止対策	FireWall、セキュリティ監視システム
	盗聴改ざん対策	128bit SSLトンネリング
耐障害性能		VPN機器 (共有型) は冗長構成 (ACT/STANDBY)
ご利用条件		
項目		説明
端末条件	PC	【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 【他】ブラウザのActiveXの動作許可設定、Admin権限が必要です。 ※Microsoft社のサポートが切れたOS、サービスパック、ブラウザはサポート対象外です。
	スマートデバイス	【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 ・弊社指定のバージョンのEdge Clientを端末にインストールしてご使用ください。Edge Clientのインストールによるトラブルについては責任範囲外とします。Edge Clientの提供元のサポート条件の範囲内でサポートいたします。 ・ただし、利用する端末OS、セキュアブラウザ、Edge Clientの各バージョンの組み合わせ、端末固有の問題、お客様の端末設定、利用状況などによって、一部動作しない場合があります。また、キャリア、メーカー保証対象外の端末 (改造された端末等) はサポート対象外です。 ・iPod Touchはサポート対象外です。
お客様宅側条件		・サーバー条件 ・通信設定条件 ・TCP/UDP通信を行うプロトコル (HTTP, HTTPS, FTP等) に対応。 ・お客様サーバを送信元とするアプリケーション (【例】FTPアクティブモード等) をご利用できません。 ・接続元ネットワークにプロキシサーバがある場合、iOS、AndroidOS搭載端末では本サービスをご利用できません。 ・AndroidOS搭載端末ではお客様社内プロキシサーバ経由の通信をご利用できません。 ・お客様のpacファイルを保存したサーバから、クライアント端末が上記pacファイルを取得できない場合、SSL-VPN通信できません。 ・クライアントへの払い出しIPアドレスと接続するセンタ、拠点のIPアドレスが重複した場合、SSL-VPN通信できません。 ・払い出しIPアドレスのセグメントがVPN機器のお客様側のセグメントと重複した場合、SSL-VPN通信できません。
利用条件	NTTコムデータセンタ～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になります。(一部の回線品目でご利用にならない場合があります。) 注:一部回線品目ではVPN装置もしくはルーターが必要になります。
	・最小ご利用者数 ・最大同時接続数	・1ユーザ ・同時接続ベストエフォート型
	その他	・その他、提供条件の詳細は別に定める「SSL-VPNマルチアクセス (PC) クライアントサーバ要件書」、「SSL-VPNマルチアクセス (SMP) クライアントサーバ要件書」、「SSL-VPNマルチアクセス (SD) クライアントサーバ要件書」に従うものとします。 ・ご利用に際し、お客様端末のCPU、メモリ、ハードディスクを増強していただく場合がございます。 ・最新版のEdgeClientのインストールおよびアップグレードについては弊社からのご案内があるまで実施をしないで下さい。

モバイルコネクトサービス仕様-7

モバイルコネクトサービス
基本仕様書(第15.0.3版)

SSL-VPN マルチアクセス・ライト

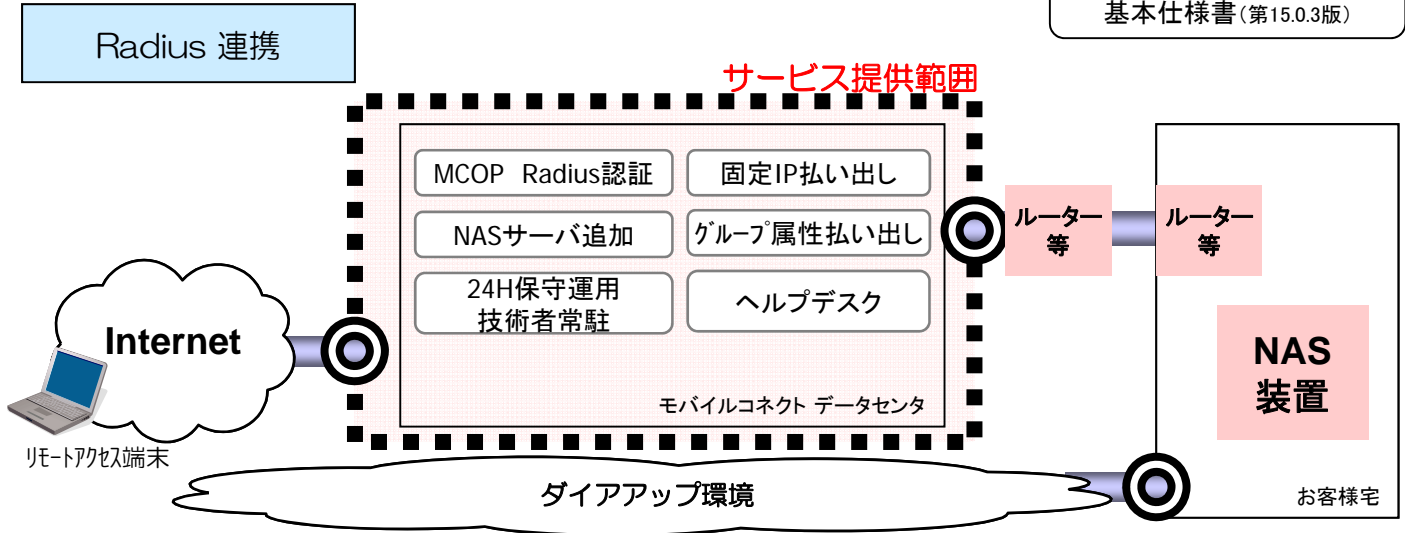
サービス提供範囲



提供機能		
項目		概要
マルチプロトコル対応		お客様のPCからの接続に対して、SSLでの通信(デフォルトUDP/4500。UDP/4500をご利用できない環境ではTCP/443へ自動切替)を提供します。
クライアントチェック		ログイン時にお客様PCのセキュリティ状態をチェックし、条件に応じてログイン可否を自動判断します。
スタートキット		クライアントチェック条件(レジストリ、ファイル)を自動登録できます。(Windows7 64bitを除く)
固定IP払い出し		ユーザIDにIPアドレスをRadiusが自動的に払い出します。
緊急同時接続拡張		通常利用の同時接続数を期間限定(最大8週間)で同時1000まで拡張できます。ただし、同時100,150,250,500が対象です。また3年契約が必須となります。なお、メンテナンス等のために弊社が使用することがあります。使用する際には、事前連絡します。
接続端末 & ネットワーク		Internetに接続されたPCデバイス (携帯電話には対応していません)
セキュリティ対策	本人認証	・MCOP方式 (Mobile Connect One-time Password) ・固定パスワード ・機体認証
	セッション管理	SSL-VPN装置でコントロール
	侵入防止対策	FireWall、セキュリティ監視システム、クライアントチェックオプション
	盗聴改ざん対策	128bit SSLトンネリング、キャッシュクリーン
耐障害性能		VPN機器(個社別)は共用コールドスタンバイ機で冗長構成
ご利用条件		
項目		説明
端末条件		【対応OS/対応ブラウザ】 「ご利用条件/対応OS」参照。 上記以外のクライアント端末のOS、ブラウザは本サービスの対象外とします。 【他】ブラウザのActiveXの動作許可設定、Admin権限が必要です。また、Windows Vista, 7をご利用の場合には、UACの無効化が必要です。 ※Microsoft社のサポートが切れたOS、サービスパック、ブラウザはサポート対象外です。
お客様宅側条件	・サーバー条件 ・通信設定条件	・TCP/UDP/ICMP通信を行うプロトコル(HTTP,HTTPS,FTP等)に対応 ・接続サーバがプロキシ動作をする場合は接続できない場合があります。 ・クライアントへの払い出しIPアドレスと接続するセンタ、拠点のIPアドレスが重複した場合、通信ができません。
利用条件	NTTコムデータセンタ～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になれます。(一部の回線品目でご利用にならない場合があります。)注:一部回線品目ではVPN装置もしくはルーターが必要になります。
	最大同時接続数	同時接続数 10, 25, 50, 100, 150, 250, 500 から選択。
	最大同時接続数の拡張と最低利用期間	同時接続数に変更となる場合は、変更後から最低利用期間が1年となります。なお、長期契約割引を申し込まれている場合は、長期契約割引期間が満了している必要があります。
	その他	・その他、提供条件の詳細は別に定める「SSL-VPNマルチアクセスライトクライアントサーバ要件書」に従うものとします。 ・ご利用に際し、お客様端末のCPU、メモリ、ハードディスクを増強していただく場合がございます。 ・お客様のご判断により、Juniper Installer Serviceをご使用される場合には、弊社サポート対象外となります。

モバイルコネクトサービス仕様-8

モバイルコネクトサービス
基本仕様書(第15.0.3版)



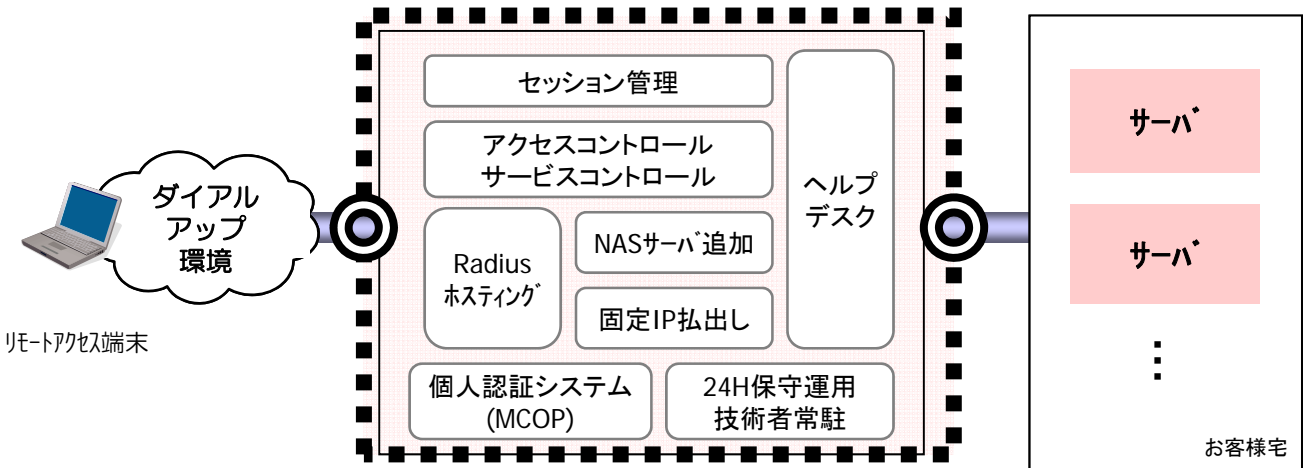
提供機能		
項目		概要
サービス		お客様宅のNAS装置とモバイルコネクトデータセンター内のRADIUSサーバーを連携し、認証サービスを提供します。
NASサーバー追加		連携サーバーが複数台ある場合、サーバーの追加が可能となります。
固定IP払い出し		ユーザIDにIPアドレスをRadiusが固定的に払い出します。
ご利用条件		
項目		説明
端末条件 (チケット取得)	対応OS/ブラウザ	【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 ※TLS 1.0のみ対応 【他】ブラウザのActiveXの動作許可設定、Admin権限が必要です。 ※Microsoft社のサポートが切れたOS、サービスパック、ブラウザはサポート対象外です。
通信方式		Radiusプロトコル
対応アトリビュート		入力アトリビュート(必須) 1 User-Name : ログインユーザー名 2 User-Password : ログインパスワード 4 NAS-IP-Address : NAS装置のIPアドレス *1 32 NAS-Identifie : NAS装置のIPアドレス *2 出力アトリビュート(任意) 8 Framed-IP-Address : IPアドレス 9 Framed-IP-Netmask : サブネットマスク 25 Class : グループ属性 *1 RADIUS認証要求パケットのソースIPアドレスも認証情報として必須 *2 NAS-IP-AddressとNAS-Identifierは、いずれか一つ以上必須。同時に入力された場合、NAS-IP-Addressが優先。
NAS装置条件	認証	PAP認証のみ対応
	アトリビュート	入力アトリビュートはすべて必須 * NAS-IP-AddressとNAS-Identifierは何れか1つ以上必須
	通信ポート	UDP 1812のみの対応
利用条件	最小ご利用者数	1ユーザ

モバイルコネクトサービス仕様-9

モバイルコネクトサービス
基本仕様書(第15.0.3版)

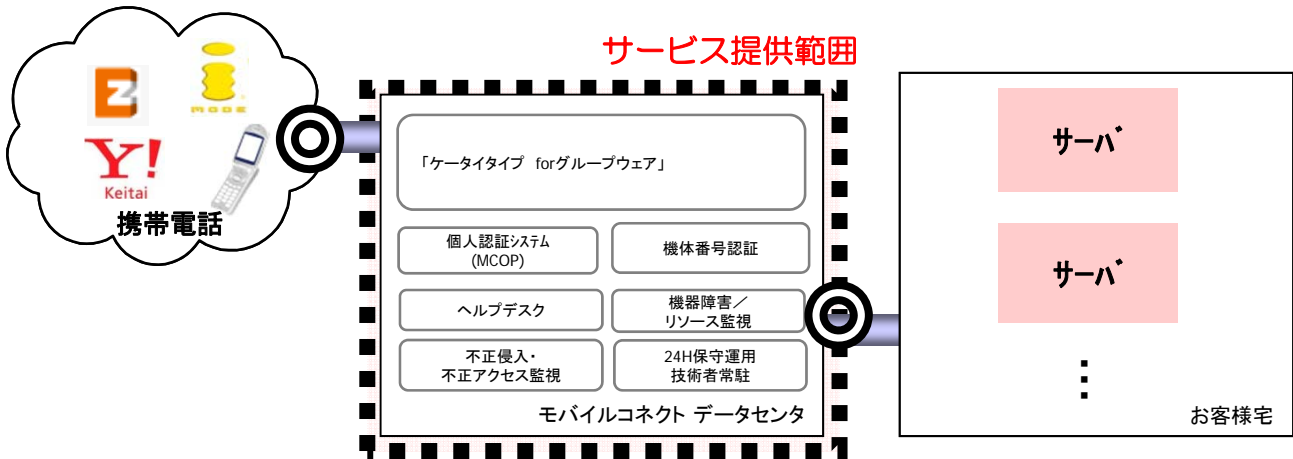
クローズドネットワークアクセス

サービス提供範囲



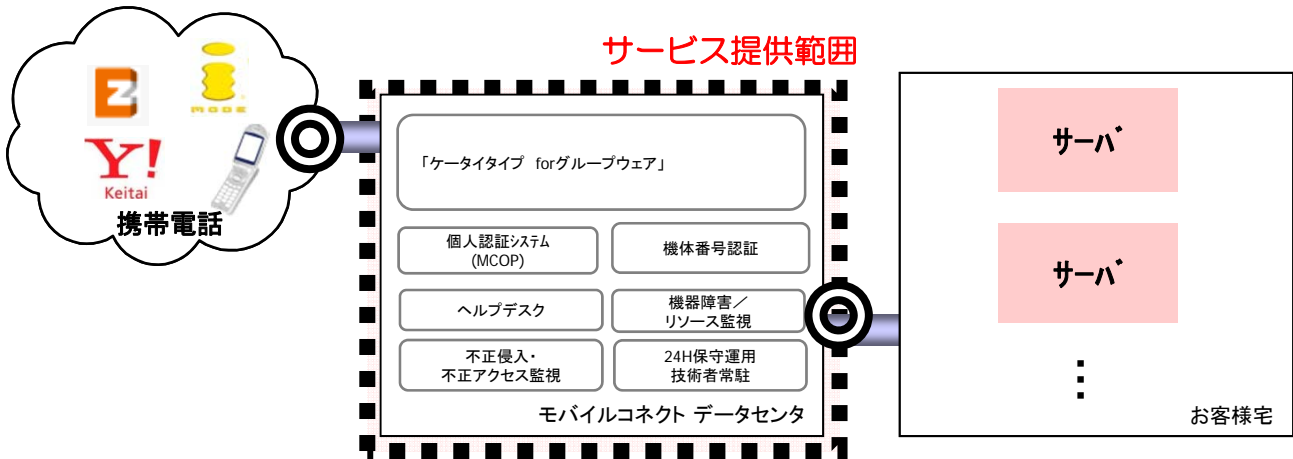
提供機能		
項目		概要
ハイスペックタイプ		ダイヤルアップ環境に対してのRadiusホスティングサービスのご提供と、USMによるMCOP認証、機体認証、アクセス制御を提供するサービスです。
	NASサーバ追加	ダイヤルアップ環境のNASが複数となる場合に対応します。
	固定IP払出し	ユーザに対して固定IPを払いだします。 (ダイヤルアップ環境が固定IP払出しの機能を持つことが前提となります。)
ネットワーク		ダイヤルアップ環境をお客様ごとにモバイルコネクトへ敷設します。 (ダイヤルアップ環境はモバイルコネクトサービス対象外)
セキュリティ対策	本人認証	・固定パスワード[ダイヤルアップ環境へPPP確立時] ・MCOP方式(Mobile Connect One-time Password)[ダイヤルアップ確立後] ・機体認証[ダイヤルアップ確立後]
	セッション管理	MCOP認証後にユーザIDごとにセッション管理を実施
	アクセスコントロール / サービスコントロール	・指定ホストIPアドレスへのアクセス許可 ・指定ホスト、指定ポートへのアクセス許可 ・パケットスルー機能(無条件アクセス許可を指定可能) を指定することが可能
耐障害性能		USM(個社別)は共用コールドスタンバイ機で冗長構成
ご利用条件		
項目		説明
端末条件		【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 Windows Vista Business/Ultimate 日本語版 (SP2)、Windows 7 Professional/Ultimate 日本語版 (SPなし) ※Microsoft社のサポートが切れたOS、サービスパック、ブラウザはサポート対象外です。 【Java】Oracle Sun JRE (Java Runtime Environment) 5.0/JRE6のインストールが必要です。ただし6update4とupdate5は除く。 WindowsVista、Windows7をご利用になる場合には、JRE5.0update21以降のインストールが必要です。 ※32ビット版に限ります。 (参考) Internet Explorer では、アクセスしたWeb ページ上にポップアップ ウィンドウを表示しない設定を行なうことができます。この機能がオンになっていると、「認証アプレット」画面が開けないようになってしまうため、本サービスを利用することができません。ブラウザの設定にてポップアップを許可する設定をしてください。
お客様宅側条件	・サーバ条件 ・通信設定条件	FTPをはじめとするお客様宅内のサーバ側からクライアントにコネクションを行うアプリケーションは、USMのデフォルト設定ではご利用できません。ご利用いただくには弊社担当にご相談下さい。
利用条件	NTTコムデータセンタ～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になります。 (一部の回線品目でご利用になれない場合があります。) 注：一部回線品目ではVPN装置もしくはルーターが必要になります。
	最小ご利用者数	1ユーザ
	最大同時接続数	同時接続200
	その他	その他、提供条件の詳細は別に定める「クローズドNWアクセス提供条件書」に従うものとします。 ご利用に際し、お客様端末のCPU、メモリ、ハードディスクを増強していただく場合がございます。

ケータイタイプ for グループウェア



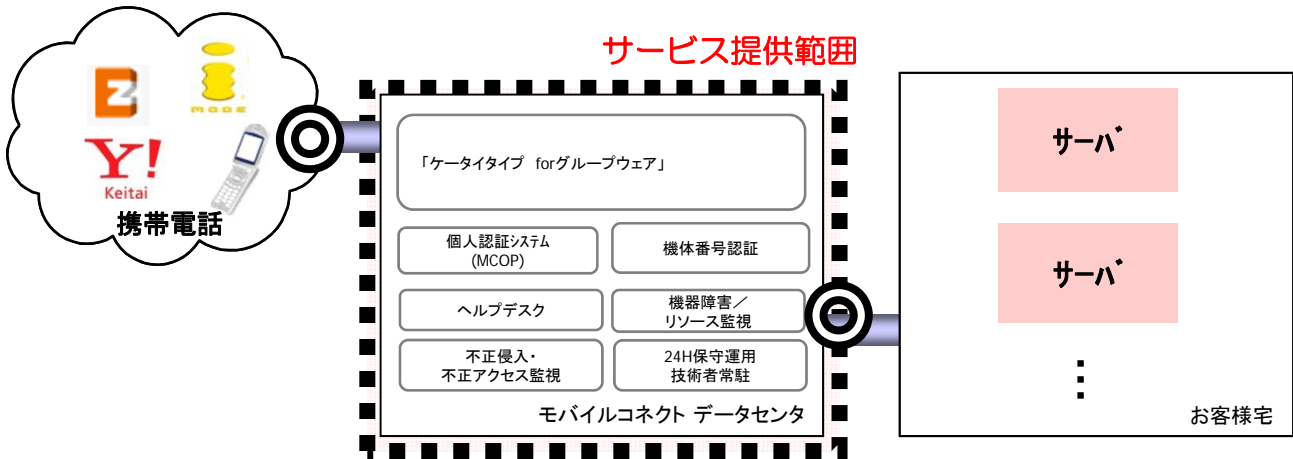
提供機能			
項目		概要	
ケータイタイプ for グループウェア		モバイル端末上で動作する専用アプリを利用して、お客様社内にて運用中のグループウェアを社外から利用することができるサービスです。 ■メール(参照、新規作成／返信／転送、検索、添付ファイル閲覧) ■予定表(参照、登録／削除) ■連絡先(参照、検索) ■グローバルアドレス帳(参照、検索)	
	MCOP認証	認証方式を、MCOP認証に変更することができます。(標準では、認証方式はBASIC認証になります。BASIC認証、MCOP認証の提供機能、利用条件はモバイルコネクト認証サービスに準じます。)	
	機体番号認証	認証方式に、機体番号認証を追加することができます。 (提供機能、利用条件はケータイアクセスサービス 機体番号認証サービスに準じます。)	
ネットワーク		携帯キャリアからの専用線での接続 ※ただしau(BREWアプリ)はインターネット(SSL)接続	
セキュリティ対策	本人認証	・MCOP方式(Mobile Connect One-time Password) ・固定パスワード ・機体番号認証	
	セッション管理	ユーザ毎にURL単位でコントロール	
	侵入防止対策	Firewall、セキュリティ管理システム	
	盗聴改ざん対策	携帯キャリアからの専用線接続	
サービス運用		モバイルコネクト基本サービスに準じます。	
ヘルプデスク		ヘルプデスク基本サービス(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。) ※「エンドユーザ問合せサービス」、「ユーザー管理代行サービス」は対象外です。	
その他	ユーザー管理Web	インターネット環境でPKI認証による接続(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。) ※ダウンロードサイトは対象外です。	
	耐障害性性能	ユーザ情報データベース、Webサーバ、ネットワーク機器は全て冗長構成	
	お客様ハウジングサービス	※本サービスはオプションサービスとなります。(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。)	
	お客様機器監視サービス	※本サービスはオプションサービスとなります。(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。)	

ケータイタイプ for グループウェア



ご利用条件		
項目		説明
端末条件	ケータイタイプ	■NTTドコモ：iアプリ(メガアプリ)が動作可能な端末(対応機種一覧は別紙) ■SoftBank：S!アプリ(MEXA/MIDP2.0)が動作可能な端末(対応機種一覧は別紙) ■au：BREW4.0対応端末であること(対応機種一覧は別紙)
	留意事項	※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の「戻る」ボタン等の操作は保証対象外となります。) ※端末や通信状況、及びNTTコムデータセンター～お客様宅との接続回線帯域、回線利用状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外となります。 ※添付ファイル閲覧は、JPEG形式で変換処理します。 ※添付ファイル閲覧の対応ファイル：Microsoft Office(Excel(xls, xlsx)、Word(doc, docx)、PowerPoint(ppt, pptx))、PDF、TXT、画像ファイル(jpeg,jpg,png,gif) ※パスワード、マクロ付きファイル、ダイアログ表示が設定されたファイルは対象外となります。また、ファイル内容や端末スペックにより、Microsoft Officeで表示した内容と一部異なったり、表示できない場合があります。表示できないページは、専用アプリにて「メモリ不足です」と表示される場合があります。 ※5MBを超過するファイルは閲覧できません。 ※送信、表示可能なメール宛先件数はToとCc、Bcc併せて最大40件です。 ※10,000byte以上の文字のメールは送信できません。 ※表示可能なフォルダは5階層までの最大300件です。フォルダ数の換算には規定のフォルダ(受信トレイ、送信済みアイテムなど)を含みます。 ※表示可能な予定表グループ数は最大20件です。 ※表示可能な予定表グループメンバーは最大50件です。 ※au(Brew)の海外対応機種から海外でサービスを利用することはできません。 ※Notes連携版では、「確認」スケジュールは閲覧できません。 ※Office365連携のグローバルアドレス帳検索では、部署名による検索、部分一致検索、URL/メモの表示ができません。 ※Exchange2013,Office365連携では、宛先を条件としたメール検索ができません。

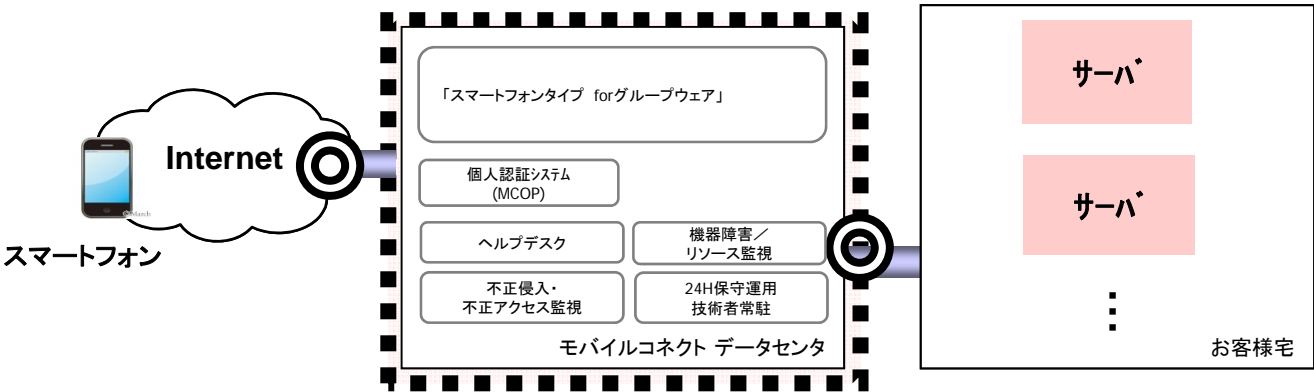
ケータイタイプ for グループウェア



ご利用条件		
項目		説明
対応グループウェア		<p>■Domino Server R7.0.x、R.8.0.x、R.8.5.x、R.9.0.x <条件> ・DIIOPサービスを起動いただき、IOR情報を取得する必要があります。 ・DIIOP(63148:TCP)プロトコルでの接続が可能である必要があります。 ・Domino ServerのDIIOP設定において、弊社払い出しアドレスをDIIOPのサーバアドレスとして設定する必要があります。 ・個人アドレス帳を利用するためには、Domino Serverに同期されている必要があります。 ・本サービスを利用するDominoユーザーにおいて、インターネットパスワードが有効且つ、設定されている必要があります。 ・1ユーザあたり、接続できるDomino Serverは10台までとします。 ・グループウェア上で扱われる文字コードがShift-jisへ文字コード変換できるものであること。 ・メールテンプレートのバージョンがR7未満、あるいはカスタマイズされている場合、機能制約される可能性があります。</p> <p>■Exchange Server 2003(SP2)、2007(SP2、SP3)、2010(SP1、SP2、SP3)、2013(SP1)、Office365(Exchange Online) (ただし、2003の新規受付は終了しております。) <条件> ・ActiveDirectoryサーバへGC(グローバルカタログ)問合せが、許可されている必要があります。 ・以下のプロトコルでの接続が許可されている必要があります。 Exchange2003 ...WebDAV(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) Exchange2007 ...EWS(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) Exchange2010 ...EWS(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) Exchange2013 ...EWS(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) ・1ユーザーあたり、接続できるExchange Server(CASもしくはMB)は10台までとします。 ・Exchangeとの接続認証方式は、基本認証もしくはフォーム認証に対応します。 ・グループウェア上で扱われる文字コードがShift-jisへ文字コード変換できるものであること。 ・Office365(Exchange Online)では、モバイルコネクトデータセンタからインターネット経由にてOffice365にアクセスします。</p>
利用条件	NTTコムデータセンタ～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になれます。 (一部の回線品目でご利用にならない場合があります。) 注:一部回線品目ではVPN装置もしくはルーターが必要になります。
	最小ご利用者数	1ユーザー

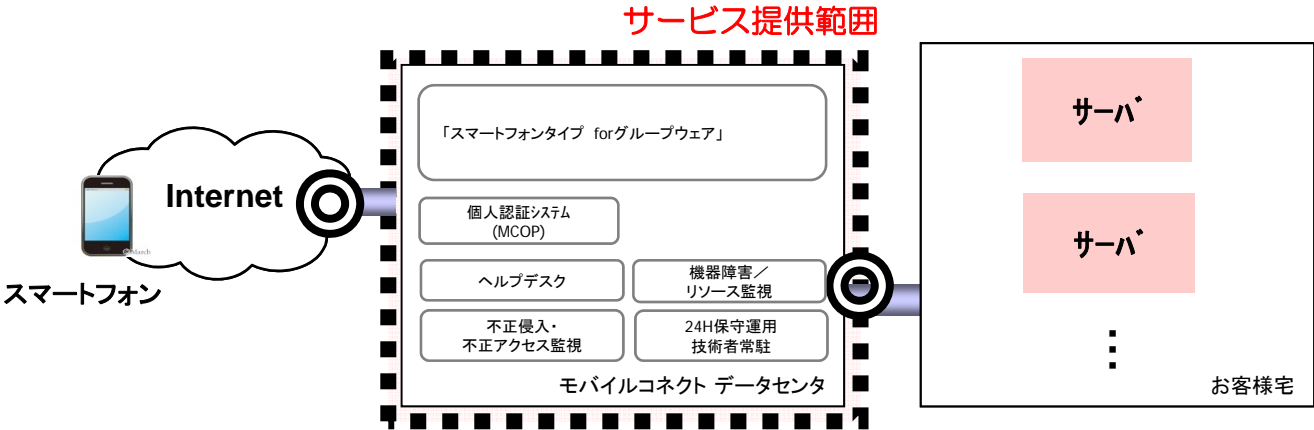
スマートフォンタイプ for グループウェア

サービス提供範囲



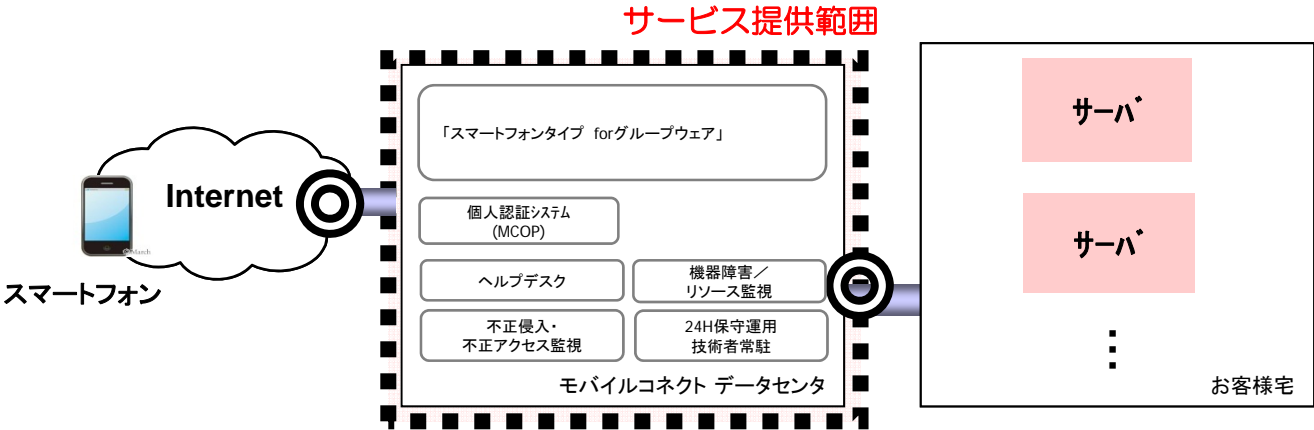
提供機能		
項目		概要
スマートフォンタイプ for グループウェア		モバイル端末上で動作する専用アプリを利用して、お客様社内にて運用中のグループウェアを社外から利用することができるサービスです。 ■メール(参照、新規作成／返信／転送、検索、添付ファイル閲覧※) ■予定表(参照、登録／削除) ■連絡先(参照、検索) ■グローバルアドレス帳(参照、検索)
	MCOP認証	認証方式を、MCOP認証に変更することができます。(標準では、認証方式はBASIC認証になります。BASIC認証、MCOP認証の提供機能、利用条件は、モバイルコネクト認証サービスに準じます。)
スマートフォン動作制御		モバイルコネクト利用時のスマートフォン、タブレット端末の動作を制御します。
	アプリケーション起動制御	モバイルコネクト利用時のアプリケーション起動リンクから、他のアプリケーションを起動する場合の動作について制御します。
	ショートカット	モバイルコネクトTOPページの「新規作成」、「受信トレイ」、「予定表」、「連絡先」、「グローバルアドレス」のショートカット表示を制御します。
	アクセス制御	メール本文中の連携サーバ以外の外部サイトへのURLリンク化について制御します。
接続情報		各コンテンツへの接続情報が閲覧可能です。
ネットワーク		インターネット(SSL)接続
セキュリティ対策	本人認証	・MCOP方式(Mobile Connect One-time Password) ・固定パスワード ・機体認証
	端末制限	AndroidOS：当社においてRoot化の疑いのあると判断される端末、および、USBデバッグが設定されている端末を検知し、ブロックします。 iOS：当社においてJailBreakの疑いのあると判断される端末を検知し、ブロックします。
	セッション管理	ユーザ毎にURL単位でコントロール
	侵入防止対策	Firewall、セキュリティ管理システム
	盗聴改ざん対策	128bitSSLトンネリング
サービス運用		モバイルコネクト基本サービスに準じます。
ヘルプデスク		ヘルプデスク基本サービス(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。) ※「エンドユーザ問合せサービス」、「ユーザー管理代行サービス」は対象外です。
その他	ユーザー管理 Web	インターネット環境でPKI認証による接続 (提供機能、利用条件は、モバイルコネクト基本サービスに準じます。)
	耐障害性性能	ユーザ情報データベース、Webサーバ、ネットワーク機器は全て冗長構成
	お客様ハウジングサービス	※本サービスはオプションサービスとなります。(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。)
	お客様機器監視サービス	※本サービスはオプションサービスとなります。(提供機能、利用条件は、モバイルコネクト基本サービスに準じます。)

スマートフォンタイプ for グループウェア



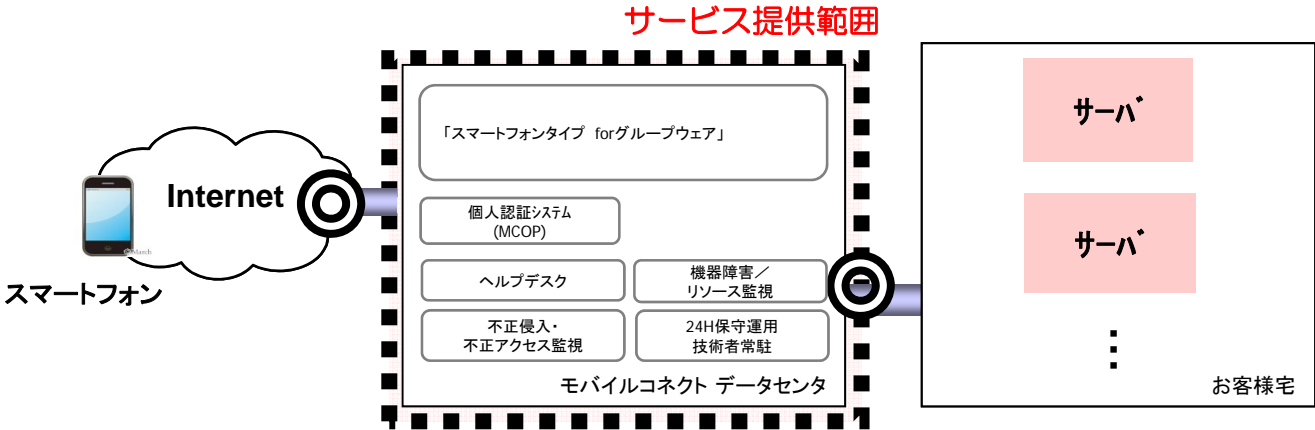
ご利用条件		
項目	説明	
端末条件	スマートフォンタイプ	【対応OS/対応ブラウザ】 「ご利用条件/対応OS」参照 Black Berry OS (4.6、5.0) 搭載端末 (BlackBerryBold、BlackBerryBold9700のみ)
	留意事項	※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の「戻る」ボタン等の操作は保証対象外となります。) ※端末や通信状況、及びNTTコムデータセンター～お客様宅との接続回線帯域、回線利用状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外となります。 ※添付ファイル閲覧は、JPEG、PDF形式のいずれかの形式で変換処理します。PDF形式で変換処理する場合は、Microsoft Office (Excel (xls、xlsx)、Word (doc、docx)、PowerPoint (ppt、pptx)) およびPDFのみPDF形式となります。なお、AndroidでPDF形式での変換処理を利用する場合は、別途RECOMOT INC.提供のアプリ (PdfViewerService) をインストールする必要があります。 ※添付ファイル閲覧の対応ファイル: Microsoft Office (Excel (xls、xlsx)、Word (doc、docx)、PowerPoint (ppt、pptx))、PDF、TXT、画像ファイル (jpeg、jpg、png、gif)、Zipファイル ※Microsoft Office、PDF、Zipのパスワード付きファイルに対応します。 ※マクロ付きファイル、ダイアログ表示が設定されたファイルは対象外となります。また、ファイル内容や端末スペックにより、Microsoft Officeで表示した内容と一部異なったり、表示できない場合があります。表示できないページは、専用アプリにて「メモリ不足です」と表示される場合があります。 ※5MBを超過するファイル (Zipファイル含む) は閲覧できません。 ※Zipファイルのパスワードに関する制限は以下になります。 文字数制限: 最大32文字 文字種制限: 半角英数記号 ※Zipファイル内のファイル数は最大10までです。 ※送信、表示可能なメール宛先件数はToとCc、Bcc併せて最大40件です。 ※10,000byte以上の文字のメールは送信できません。また、返信、転送時に8,192byte以上の文字の引用はできません。 ※表示可能なフォルダは5階層までの最大300件です。フォルダ数の換算には規定のフォルダ (受信トレイ、送信済みアイテムなど) を含みます。 ※表示可能な予定表グループ数は最大20件です。 ※表示可能な予定表グループメンバーは最大50件です。 ※Notes連携版では「確認」スケジュールは閲覧できません。 ※Office365連携のグローバルアドレス帳検索では、部署名による検索、部分一致検索、URL/メモの表示ができません。 ※Exchange2013、Office365連携では、宛先を条件としたメール検索ができません。
	機体認証	・モバイルコネクトスマートフォンアプリケーションと同時にご利用の場合のみ、ご利用可能です。 ・機体認証は1ユーザにつき5端末利用可能です。 ・機体認証における機体識別情報は変更する場合があります。 ・端末の初期化等の変更を実施した場合、再度、初期設定が必要になります。
	ログイン条件 チェック	Android: モバイルコネクトで指定するアプリケーションのプロセス、サービスの起動有無をチェックします。アプリケーションの設定内容に関わらず、指定するプロセス、サービスが起動している場合は、起動状態と判断します。 iOS: モバイルコネクトで指定するアプリケーションのインストール有無をチェックします。インストールされている場合はアプリケーションの起動有無、設定内容に関わらず、インストール状態と判断します。 ※ログイン条件については設定したグループに属するSSL-VPNマルチアクセス (SD) にも適用されます。 ※指定するアプリケーションについては変更になる場合がございます。また、指定するアプリケーションの仕様変更や端末固有の問題、お客様の端末設定、利用状況等によっては一部動作しない可能性がございます。

スマートフォンタイプ for グループウェア



ご利用条件	
項目	説明
スマートフォン動作制御	モバイルコネクト利用時のスマートフォン、タブレット端末の動作を制御します。
	アプリケーション 起動制御
	ショートカット
	アクセス制御
対応グループウェア	<div>■Domino Server R7.0.x、R.8.0.x、R.8.5.x、R9.0.x <条件><ul style="list-style-type: none">・DIIOPサービスを起動いただき、IOR情報を取得できる必要があります。・DIIOP(63148:TCP)プロトコルでの接続が可能である必要があります。・Domino ServerのDIIOP設定において、弊社払い出しアドレスをDIIOPのサーバアドレスとして設定する必要があります。・個人アドレス帳を利用するためには、Domino Serverに同期されている必要があります。・本サービスを利用するDominoユーザーにおいて、インターネットパスワードが有効且つ、設定されている必要があります。・1ユーザーあたり、接続できるDomino Serverは10台までとします。・メールテンプレートのバージョンがR7未満、あるいはカスタマイズされている場合、機能制約される可能性があります。</div> <div>■Exchange Server 2003(SP2)、2007(SP2、SP3)、2010(SP1、SP2、SP3)、2013(SP1)、Office365(Exchange Online) (ただし、2003の新規受付は終了しております。) <条件><ul style="list-style-type: none">・ActiveDirectoryサーバへGC(グローバルカタログ)問合せが、許可されている必要があります。・以下のプロトコルでの接続が許可されている必要があります。 Exchange2003・・・WebDAV(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) Exchange2007・・・EWS(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) Exchange2010・・・EWS(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP) Exchange2013・・・EWS(HTTP(80:TCP)もしくはHTTPS(443:TCP))、LDAP GC(3268:TCP)・1ユーザーあたり、接続できるExchange Server(CASもしくはMB)は10台までとします。・Exchangeとの接続認証方式は、基本認証もしくはフォーム認証に対応します。・Office365(Exchange Online)では、モバイルコネクトデータセンタからインターネット経由にてOffice365にアクセスします。</div>
接続情報	<ul style="list-style-type: none">・サービス提供開始(本機能提供開始日)より5年間の接続情報を保持します。利用者による閲覧は、利用月含む過去4ヶ月分の情報が閲覧可能です。・接続情報の集計は以下のとおり実施します。 集計頻度:1日1回 集計時刻:毎日0時～9時の間に前日分の接続情報を集計 ※ただし、メンテナンス作業実施日等、実行されない場合があります。 ※複数のお客様の処理を行うため、上記時間帯の中で実効時間が変更される場合があります。

スマートフォンタイプ for グループウェア



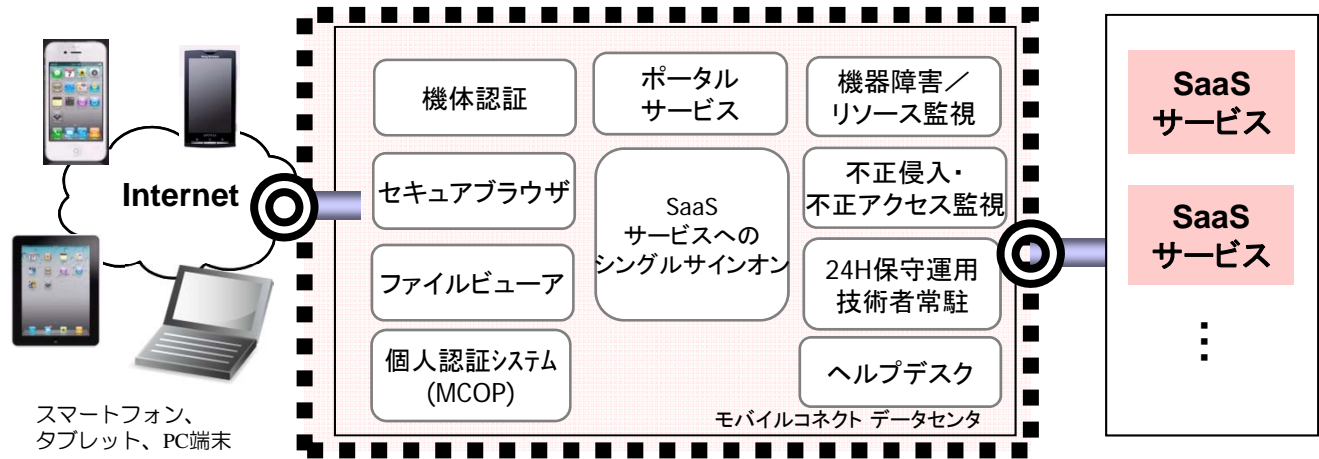
ご利用条件		
項目		説明
セキュリティ対策	端末制限	※同一IDで、SSL-VPNマルチアクセス (SD) を併せてご利用される場合は、同様に適用されます。 ※端末固有の問題やお客様の端末設定、利用状況等によっては一部動作しない可能性がございます。
利用条件	NTTコムデータセンター～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になれます。 (一部の回線品目でご利用にならない場合があります。) 注:一部回線品目ではVPN装置もしくはルーターが必要になります。
	最小ご利用者数	1ユーザ

モバイルコネクトサービス仕様-12

モバイルコネクトサービス
基本仕様書(第15.0.3版)

for SaaS

サービス提供範囲



提供機能		
項目		概要
セキュアブラウザ		端末にキャッシュ等のデータを残さない機能です。(Android、iOS端末のみ)
ファイルビューア		モバイルコネクトファイルビューア機能はご利用できません。 ※iOS：OS標準搭載のビューアにより表示します。仕様は該当ビューアの仕様に準じ、サポート対象外となります。 ※PC：PC内のインストール済みアプリケーションによって開きます。仕様は該当アプリケーションの仕様に準じ、サポート対象外となります。
スマートフォン動作制御		モバイルコネクト利用時のスマートフォン、タブレット端末の動作を制御します。
	アプリケーション起動制御	モバイルコネクト利用時のアプリケーション起動リンクから、他のアプリケーションを起動する場合の動作について制御します。
接続情報		各クラウドサービスへの接続情報が閲覧可能です。
SaaSサービス連携		お客様がご利用の次のSaaS(パブリッククラウド)サービスと連携するサービスです。 Salesforce、Cybozu.com、GoogleApps
	連携メニュー追加	SaaSサービス連携するメニューが複数リンクある場合、モバイルコネクトトップメニューに1メニュー単位で追加するサービスです。
	シングルサインオン	SaaSサービス連携時に、連携先クラウドサービスに利用者のログイン情報を受け渡す事により、コンテンツアクセス時に認証を行わずに利用する事ができるサービスです。
ポータルサービス		ログイン後に表示するトップ画面にリンクメニューを設ける事ができます。
接続端末 & ネットワーク		Internetに接続されたスマートフォン、タブレット端末
セキュリティ対策	本人認証	・MCOP方式(Mobile Connect One-time Password) ・固定パスワード ・機体認証
	端末制限	Android：当社においてRoot化の疑いがあると判断される端末、および、USBデバッグが設定されている端末を検知し、ブロックします。 iOS：当社においてJailBreakの疑いがあると判断される端末を検知し、ブロックします。
	セッション管理	Cookieによるコントロール
	侵入防止対策	FireWall、セキュリティ管理システム
	盗聴改ざん対策	128bitSSLトンネリング
その他	ユーザー管理Web	インターネット環境でPKI認証による接続
	耐障害性性能	ユーザ情報DB、Webサーバ、ネットワーク機器は全て冗長構成

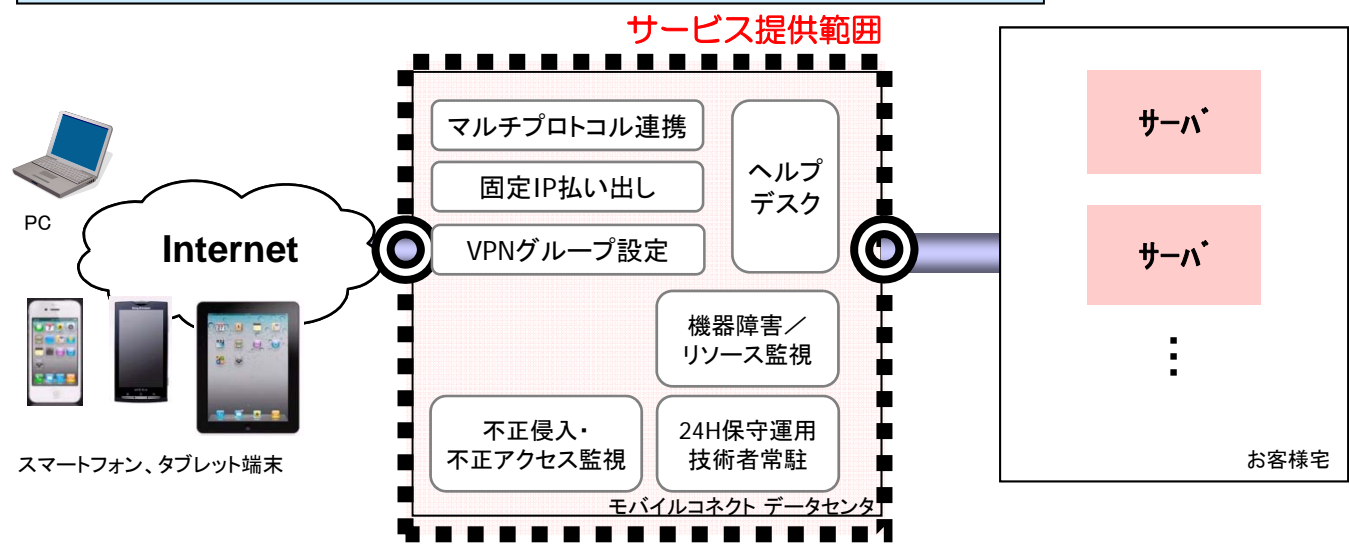
for SaaS

ご利用条件		
項目	説明	
端末条件	スマートフォン PC システム要件	【対応OS/対応ブラウザ】 「ご利用条件/対応OS」参照 ※TLS 1.0のみ対応 ※上記搭載端末で動作可能です。但しOSのバージョンや端末固有の問題及びお客様の端末設定、利用状況等によっては一部動作しない可能性があります。 ※iPod touchは対象外です。 ※キャリア/メーカー保証対象外の端末(改造された端末等)はサポート対象外です。
	留意事項	・端末1台につき、1ブラウザでの動作を保証します。 ・OS、端末によって動作が異なる場合があります。 ・端末や通信状況によっては、画面表示に時間がかかる場合があります。
	機体認証	・機体認証は1ユーザにつき、スマートフォンは5端末、PCは1端末まで利用可能です。 ・機体認証における機体識別情報は変更する場合があります。 ・端末の初期化等の変更を実施した場合、再度、初期設定が必要になります。
	ログイン条件 チェック	Android：モバイルコネクトで指定するアプリケーションのプロセス、サービス起動有無をチェックします。 アプリケーションの設定内容に関わらず、指定プロセス、サービス起動している場合は、起動状態と判断します。 iOS：モバイルコネクトで指定するアプリケーションのインストール有無をチェックします。インストールされている場合は、アプリケーションの起動有無、設定内容に関わらず、インストール状態と判断します。 PC：本機能対象外 ※ログイン条件については設定したグループに属するSSL-VPNマルチアクセス(SD)にも適用されます。 ※指定するアプリケーションについては変更になる場合がございます。また、指定するアプリケーションの仕様変更や端末固有の問題、お客様の端末設定、利用状況等によっては一部動作しない可能性がございます。
	セキュアブラウザ	・一定時間無操作の場合、タイムアウトとなります。 ・キャッシュ等のデータ消去についてはアプリを正常に終了した場合に動作します。 ・初期設定時に標準搭載ブラウザ以外のブラウザをご利用の場合、正常に動作しない可能性がありますので、標準搭載ブラウザにて初期設定を実施ください。 ・スマートフォンアプリケーションの強制停止を行った場合は、正常に動作しない場合があります。 ・URLの表示およびブックマークはできません。
	ファイルビューア	モバイルコネクトファイルビューア機能はご利用できません。 iOS：OS標準搭載のビューアにより表示します。仕様は該当ビューアの仕様に準じ、サポート対象外となります。 PC：PCのインストール済みアプリケーションによって開きます。
スマートフォン動作制御		モバイルコネクト利用時のスマートフォン、タブレット端末の動作を制御します。
アプリケーション 起動制御		一部コンテンツにおいては制御できない場合があります。
その他の制限事項		SaaSサービスの機能において、別ウィンドウや別タブを利用したものは、正常に利用できない場合があります。
SaaSサービス利用時の制限事項		GoogleAppsは、従来のログインID/パスワードによるログインができなくなります。モバイルコネクトを経由したログインのみ有効になります。
接続情報		・サービス提供開始(本機能提供開始日)より5年間の接続情報を保持します。利用者による閲覧は、利用月含む過去4ヶ月分の情報が閲覧可能です。 ・接続情報の集計は以下のとおり実施します。 集計頻度：1日1回 集計時刻：毎日0時～9時の間に前日分の接続情報を集計 ※メンテナンス作業実施日等、実行されない場合があります。 ※複数のお客様の処理を行うため、上記時間帯の中で実効時間が変更される場合があります。
セキュリティ 対策	端末制限(スマートフォンのみ)	※同一IDで、SSL-VPNマルチアクセス(SD)を併せてご利用される場合は、同様に適用されます。 ※端末固有の問題やお客様の端末設定、利用状況等によっては一部動作しない可能性があります。
利用条件等	最小ご利用者数	1ユーザ

モバイルコネクトサービス仕様-13

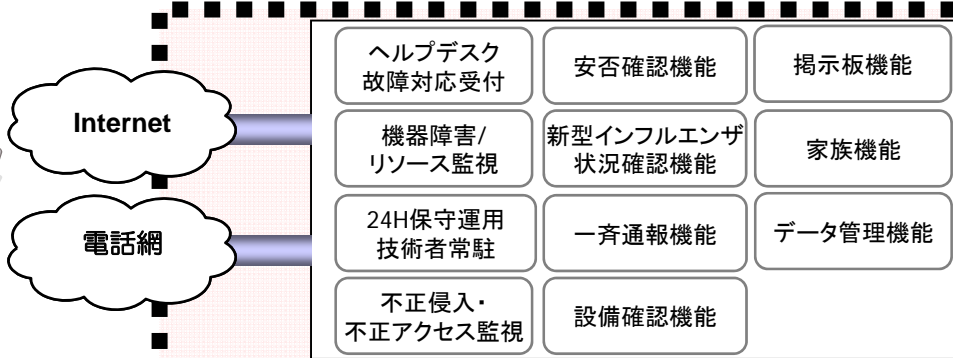
モバイルコネクトサービス
基本仕様書(第15.0.3版)

SSL-VPN マルチアクセス 外部認証連携(ID Federation認証)



提供機能		
項目		概要
マルチプロトコル対応		お客様のPCからの接続に対して、SSLでの通信(デフォルトUDP/4433。UDP/4433をご利用できない環境ではTCP/443へ自動切替)を提供します。
固定IP払い出し		ユーザIDにIPアドレスをRadiusが定期的に払い出します。
VPNグループ設定		サービス提供時に、VPNグループ設定を実施します。
接続端末 & ネットワーク		Internetに接続されたデバイス (PC、スマートフォン、タブレット端末。携帯電話には対応していません)
セキュリティ対策	本人認証	ID Federationサービスが提供する認証をご利用いただけます。 ※モバイルコネクト認証サービス(MCOP認証、機体認証、固定パスワード認証)とは併用出来ません。
	セッション管理	SSL-VPN装置でコントロール。最大接続時間は480分(固定)
	侵入防止対策	FireWall、セキュリティ監視システム
	盗聴改ざん対策	128bit SSLトンネリング
耐障害性能		VPN機器(共有型)は冗長構成(ACT/STANDBY)
ご利用条件		
項目		説明
端末条件	PC	【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 【他】ブラウザのActiveXの動作許可設定、Admin権限が必要です。 ※Microsoft社のサポートが切れたOS、サービスパック、ブラウザはサポート対象外です。
	スマートデバイス	【対応OS/対応ブラウザ】「ご利用条件/対応OS」参照 ・弊社指定のバージョンのEdge Clientを端末にインストールしてご使用ください。Edge Clientのインストールによるトラブルについては責任範囲外とします。Edge Clientの提供元のサポート条件の範囲内でサポートいたします。 ・ただし、利用する端末OS、セキュアブラウザ、Edge Clientの各バージョンの組み合わせ、端末固有の問題、お客様の端末設定、利用状況などによって、一部動作しない場合があります。また、キャリア、メーカー保証対象外の端末(改造された端末等)はサポート対象外です。 ・iPod Touchはサポート対象外です。
お客様宅側条件		・サーバー条件 ・通信設定条件 ・TCP/UDP通信を行うプロトコル(HTTP,HTTPS,FTP等)に対応。 ・お客様サーバを送信元とするアプリケーション(【例】FTPアクティブモード等)をご利用できません。 ・接続元ネットワークにプロキシサーバがある場合、iOS、AndroidOS搭載端末では本サービスをご利用できません。 ・AndroidOS搭載端末ではお客様社内プロキシサーバ経由の通信をご利用できません。 ・お客様のpacファイルを保存したサーバから、クライアント端末が上記pacファイルを取得できない場合、SSL-VPN通信できません。 ・クライアントへの払い出しIPアドレスと接続するセンタ、拠点のIPアドレスが重複した場合、SSL-VPN通信できません。 ・払い出しIPアドレスのセグメントがVPN機器のお客様側のセグメントと重複した場合、SSL-VPN通信できません。
利用条件	NTTコムデータセンター～お客様宅との接続回線	UniversalOne、統合VPNおよび専用線サービスがご利用になります。(一部の回線品目でご利用にならない場合があります。)注:一部回線品目ではVPN装置もしくはルーターが必要になります。
	・最小ご利用者数 ・最大同時接続数	・1ユーザ ・同時接続ベストエフォート型
	その他	・その他、提供条件の詳細は別に定める「SSL-VPNマルチアクセス(PC)クライアントサーバ要件書」、「SSL-VPNマルチアクセス(SMP)クライアントサーバ要件書」、「SSL-VPNマルチアクセス(SD)クライアントサーバ要件書」に従うものとします。 ・ご利用に際し、お客様端末のCPU、メモリ、ハードディスクを増強していただく場合がございます。 ・最新版のEdgeClientのインストールおよびアップグレードについては弊社からのご案内があるまで実施をしないで下さい。 ・基本機能のうちユーザー管理Web、ユーザー管理代行サービスはご利用できません。

安否確認/一斉通報サービス(通常プラン)



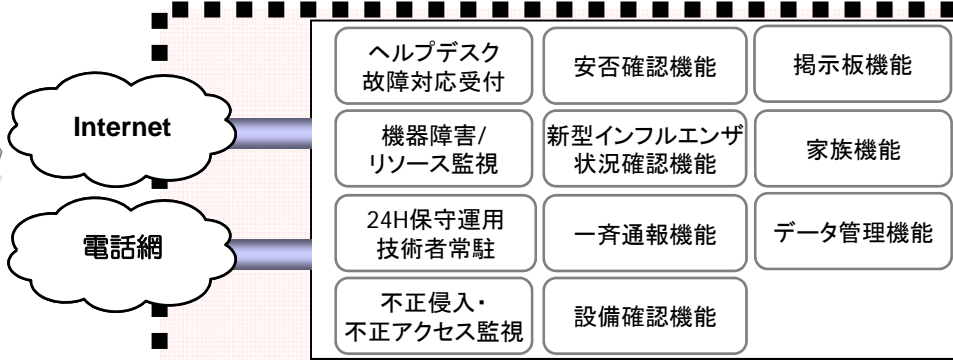
サービス
提供範囲

提供機能		
項目		概要
アプリケーション	安否確認機能	有事の際に社員の安否確認を行う機能です。 ・PC/携帯Web/スマートフォン/電話から登録が可能です。・登録された情報の集計/個別一覧の表示が可能です。 ※電話(音声サービス)のご利用はオプションとなります。
	新型インフルエンザ状況確認機能	新型インフルエンザ発生時の社員の感染や健康状況確認を行う機能です。 ・PC/携帯Web/スマートフォン/電話から登録が可能です。・登録された情報の集計/個別一覧の表示が可能です。 ※電話(音声サービス)のご利用はオプションとなります。
	一斉通報機能	有事の際や日常時に社員への情報伝達・状況確認を行う機能です。 ・PC/携帯Web/スマートフォン/電話から登録が可能です。・登録された情報の個別一覧の表示が可能です。 ※電話(音声サービス)のご利用はオプションとなります。
	設備確認機能	有事の際等に建物や設備の被災状況や復旧状況の確認を行う機能です。 ・PC/携帯Web/スマートフォン/電話から登録が可能です。(電話によるインバウンドでの登録には対応していません)・登録された情報の個別一覧の表示が可能です。 ※電話(音声サービス)のご利用はオプションとなります。 ※添付できるファイルサイズは1ファイルあたり最大3MBまでとなります。1企業あたり登録できるファイルサイズは合計で最大30MBまでとなります。 ※1企業あたりの設備数は100、設備担当者数は300までとなります。
	掲示板機能	有事の際や日常時に管理者が社員へのメッセージを掲載する機能です。 ・PC/携帯Web/スマートフォンでメッセージの登録、閲覧が可能です。 ※添付できるファイルサイズは1ファイルあたり最大500KBまでとなります。 1企業あたり登録できるファイルサイズは合計で最大30MBまでとなります。
	家族機能	社員と家族間のメッセージ共有機能です。 ・PC/携帯Web/スマートフォン/電話でメッセージ共有が可能です。・社員と家族間のメッセージを企業が管理する/しないのポリシーを設定することが可能です。 ※電話(音声サービス)のご利用はオプションとなります。 ※家族は5名まで登録できます。
	データ管理機能	ID情報、社員情報、組織情報、グループ情報等のメンテナンス機能です。 ※文字コードはShif-JISコードの利用となります。
ネットワーク	PC	インターネット(SSL)
	携帯電話(WEB)	インターネット(SSL)
	スマートフォン(WEB)	インターネット(SSL)
	電話	電話公衆網(音声・携帯電話/PHS含む)
セキュリティ対策	本人認証	固定パスワード
	セッション管理	ユーザ毎にURL単位でコントロール
	情報漏えい対策(ネットワーク)	インターネット(SSL)
その他	耐障害性機能	データセンタ/機器の障害・リソース状況の24時間365日監視/機器・ネットワーク等の冗長構成/ロケーションの2拠点構成 ※ユーザー個別設置機器はシングル構成となります。
	2拠点化方式	電話: Active-Active方式 WEB: Active-Standby方式
	ログインURL	http://www.mc-anpi.com
	最小ご利用者数	10ユーザ

モバイルコネクトサービス仕様-14

モバイルコネクトサービス
基本仕様書(第15.0.3版)

安否確認/一斉通報サービス(通常プラン)



サービス
提供範囲

ご利用条件

項目		概要
端末条件	携帯WEB	NTTドコモ:i-mode対応機種((モトローラ社製M1000端末、MITSUBISHI社製D2101V端末を除く503i以降) au:EZWeb対応端末(A5000/C5000/A3000/C3000/A1100シリーズ以降) Softbank Mobile:Yahoo!ケータイ 対応機種(モトローラ社製3G端末を除くC3型以降端末) WILLCOM:AirEDGE PHONE各機種(SHARP社製W-ZERO3端末、JRC社製AH-J3001V・AH-J3002V・AH-J3003S・WX220J端末を除く) ※標準ブラウザでのご利用が前提となります。フルブラウザのご利用はサポートしておりません。 (WILLCOM端末からの接続は、ケータイモード設定でのご利用が前提となります。) ※バージョン固有の問題及びお客様の端末設定状況等によっては一部動作しない可能性がございます。
	スマートフォン	WindowsMobile6.5 +標準搭載ブラウザ(IEMobile6) iPhone OS 3/iOS 4/5/6/7 +標準搭載ブラウザ(Safari) (iPad端末含む) Android 1.6/2.1/2.2/2.3/3.0/3.1/3.2/4.0/4.1/4.2/4.3 +標準搭載ブラウザ(AppleWebKit準拠ブラウザ) ※上記搭載端末で動作可能です。但しバージョン固有の問題及びお客様の端末設定状況等によっては一部動作しない可能性がございます。
	PC	ブラウザ:Internet Explorer 7、8、9、10、11(※) ※Internet Explorer 10、11は互換表示の利用が前提となります。
	安否確認専用アプリケーション	iOS 6/7 (iPad端末含む) AndroidOS 4.1/4.2/4.3/4.4 (タブレット端末含む)
	電話	固定電話、公衆電話、携帯電話、PHS ※0AB～J番号以外のIP電話はサポート外となります。 (050番号のIP電話からフリーダイヤルへの接続はできませんのでご注意ください) ※電話(音声サービス)のご利用はオプションとなります。 ※トーン信号(PB信号)に対応している必要があります。 ※国際電話には対応していません。
	留意事項	※1IDにつき、1ユーザの利用を保証します。 ※端末1台につき、1ブラウザでの動作を保証します。 ※システムにログインする際は、ログイン画面を利用してください。 ※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の「戻る」ボタン等の操作は保証対象外となります。) ※端末や通信状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合は保証対象外となります。
その他		<ul style="list-style-type: none"> ・メインサイト被災時にはバックアップサイトをメインサイトとするサイト切り換えを実施いたします。またログインURL(http://www.mc-anpi.com)から、バックアップサイトへアクセスを可能とするためのDNS切り替えを実施します(ただしお客様の環境によってはDNS情報の反映等に時間を要する可能性があります) ・音声サービスは、平常時より、メインサイト・バックアップサイトの両サイトの音声回線のご利用が可能です。 ・CSV自動アップロード機能(オプション)はメインサイトのみの提供となります。メインサイト障害時には本機能のご利用はできません。 ・初動サポート機能は財団法人日本気象協会(以下、気象協会)より、安否確認/一斉通報サービスのデータセンタに対して送付される災害情報データ(震度速報)を元に実行いたします。 ・自動災害登録は震度速報の初報データを元に実行します。このため、記載される内容が最終報の内容とは異なる場合がございます。 ・定期システムメンテナンス及び当社のシステム保守を緊急に行う必要が発生した場合、本サービスの運用を停止することがあります(詳細は「安否確認/一斉通報サービス利用規約」第4章「運用停止」を参照下さい)なおメンテナンス作業前に日本国内の何れかの地域で大規模な地震が発生した場合、原則メンテナンス作業を中止することとします。またメンテナンス作業中に大規模な地震が発生した場合は、より早くサービス復旧ができることを条件にメンテナンス作業の中止または継続を判断します。 ・通常プランからライトプランに変更する場合は、通常プランを解約し、ライトプランへの新規申込が必要となります。この場合、お客様の企業コード等も変更となります。またお客様のデータも引き継がれませんので、お客様にてデータのバックアップを取得いただきますようお願いいたします。 ・本サービスにおける仕様(画面、機能等)は、機能拡張等により変更される場合があります。

モバイルコネクトサービス仕様-14

モバイルコネクトサービス
基本仕様書(第15.0.3版)

安否確認/一斉通報サービス（お手軽導入プラン）



Internet

ヘルプデスク
故障対応受付

安否確認機能

掲示板機能

機器障害/
リソース監視

新型インフルエンザ
状況確認機能

家族機能

24H保守運用
技術者常駐

一斉通報機能

データ管理機能

不正侵入・
不正アクセス監視

サービス
提供範囲

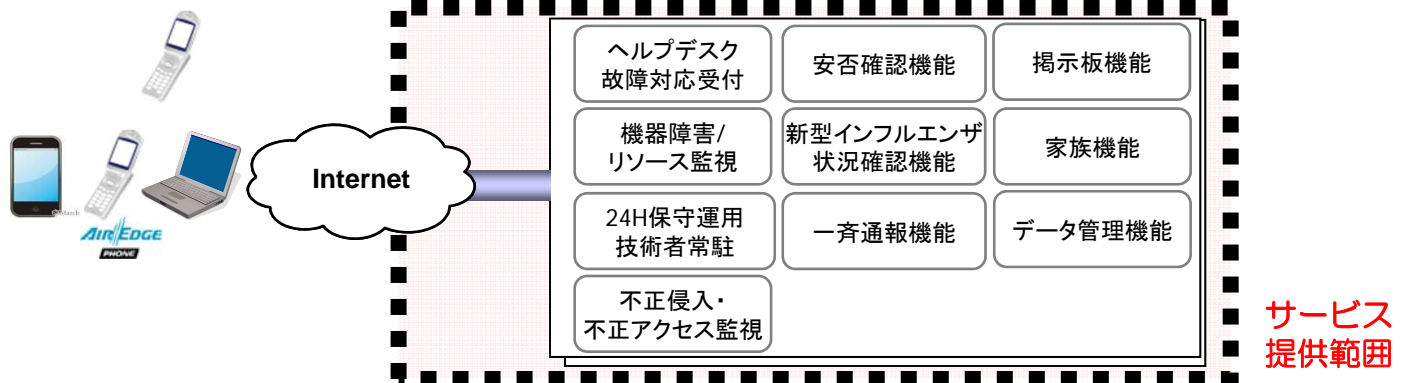
提供機能

項目		概要
アプリケーション	安否確認機能	有事の際に社員の安否確認を行う機能です。 ・PC/携帯Web/スマートフォンから登録が可能です。・登録された情報の集計/個別一覧の表示が可能です。
	新型インフルエンザ状況確認機能	新型インフルエンザ発生時の社員の感染や健康状況確認を行う機能です。 ・PC/携帯Web/スマートフォンから登録が可能です。・登録された情報の集計/個別一覧の表示が可能です。
	一斉通報機能	有事の際や日常時に社員への情報伝達・状況確認を行う機能です。 ・PC/携帯Web/スマートフォンから登録が可能です。・登録された情報の個別一覧の表示が可能です。
	家族機能	社員と家族間のメッセージ共有機能です。 ・PC/携帯Web/スマートフォンでメッセージ共有が可能です。 ※家族は5名まで登録できます。
	掲示板機能	有事の際や日常時に管理者が社員へのメッセージを掲載する機能です。 ・PC/携帯Web/スマートフォンでメッセージの登録、閲覧が可能です。 ※添付できるファイルサイズは1ファイルあたり最大500KBまでとなります。 1企業あたり登録できるファイルサイズは合計で最大30MBまでとなります。
	データ管理機能	ID情報、社員情報、組織情報、グループ情報等のメンテナンス機能です。 ※文字コードはShift-JISコードの利用となります。
ネットワーク	PC	インターネット(SSL)
	携帯電話(WEB)	インターネット(SSL)
	スマートフォン(WEB)	インターネット(SSL)
セキュリティ対策	本人認証	固定パスワード
	セッション管理	ユーザ毎にURL単位でコントロール
	情報漏えい対策(ネットワーク)	インターネット(SSL)
その他	耐障害性機能	データセンタ/機器の障害・リソース状況の24時間365日監視/機器・ネットワーク等の冗長構成/ロケーションの2拠点構成 ※ユーザー個別設置機器はシングル構成となります。
	2拠点化方式	WEB:Active-Standby方式
	ログインURL	http://www.mc-anpi.com
	最小ご利用者数	10ユーザ

モバイルコネクトサービス仕様-14

安否確認/一斉通報サービス（お手軽導入プラン）

モバイルコネクトサービス
基本仕様書(第15.0.3版)



ご利用条件		
項目	概要	
端末条件	携帯WEB	NTTドコモ:i-mode対応機種((モトローラ社製M1000端末、MITSUBISHI社製D2101V端末を除く503i以降) au:EZWeb対応端末(A5000/C5000/A3000/C3000/A1100シリーズ以降) Softbank Mobile:Yahoo!ケータイ 対応機種(モトローラ社製3G端末を除くC3型以降端末) WILLCOM:AirEDGE PHONE各機種(SHARP社製W-ZERO3端末、JRC社製AH-J3001V・AH-J3002V・AH-J3003S・WX220J端末を除く) ※標準ブラウザでのご利用が前提となります。フルブラウザのご利用はサポートしておりません。 (WILLCOM端末からの接続は、ケータイモード設定でのご利用が前提となります。) ※バージョン固有の問題及びお客様の端末設定状況等によっては一部動作しない可能性があります。
	スマートフォン	WindowsMobile6.5 + 標準搭載ブラウザ(IEMobile6) iPhone OS 3/iOS 4/5/6/7 + 標準搭載ブラウザ(Safari) (iPad端末含む) Android OS 1.6/2.1/2.2/2.3/3.0/3.1/3.2/4.0/4.1/4.2/4.3 + 標準搭載ブラウザ(AppleWebKit準拠ブラウザ) ※上記搭載端末で動作可能です。但しバージョン固有の問題及びお客様の端末設定状況等によっては一部動作しない可能性があります。
	PC	ブラウザ:Internet Explorer 7、8、9、10、11(※) ※Internet Explorer 10、11は互換表示の利用が前提となります。
	安否確認専用アプリケーション	iOS 6/7 (iPad端末含む) Android OS 4.1/4.2/4.3/4.4 (タブレット端末含む)
	留意事項	※1IDにつき、1ユーザの利用を保証します。 ※端末1台につき、1ブラウザでの動作を保証します。 ※システムにログインする際は、ログイン画面を利用してください。 ※システム操作はサービス画面内のボタン操作のみを保証します(端末・ブラウザ等の「戻る」ボタン等の操作は保証対象外となります。) ※端末や通信状況によっては、画面表示に時間がかかる場合があります。画面全体が表示される前に、ボタン操作を行った場合の動作は保証対象外となります。
その他	<ul style="list-style-type: none"> ・メインサイト被災時にはバックアップサイトをメインサイトとするサイト切り換えを実施いたします。またログインURL(http://www.mc-anpi.com)から、バックアップサイトへアクセスを可能とするためのDNS切り替えを実施します(ただしお客様の環境によってはDNS情報の反映等に時間を要する可能性があります) ・初動サポート機能は財団法人日本気象協会(以下、気象協会)より、安否確認/一斉通報サービスのデータセンターに対して送付される災害情報データ(震度速報)を元に実行いたします。 ・自動災害登録は震度速報の初報データを元に実行します。このため、記載される内容が最終報の内容とは異なる場合がございます。 ・定期システムメンテナンス及び当社のシステム保守を緊急に行う必要が発生した場合、本サービスの運用を停止することがあります(詳細は「安否確認/一斉通報サービス利用規約」第4章「運用停止」を参照下さい)なおメンテナンス作業前に日本国内の何れかの地域で大規模な地震が発生した場合、原則メンテナンス作業を中止することとします。またメンテナンス作業中に大規模な地震が発生した場合は、より早くサービス復旧ができることを条件にメンテナンス作業の中止また継続を判断します。 ・本サービスにおける仕様(画面、機能等)は、機能拡張等により変更される場合があります。 	

改正履歴

改正年月日	版	備考
2001年09月20日	第 1.0.0版	
2008年02月01日	第 8.0.0版	利用規約別紙から名称変更
2008年05月20日	第 9.0.0版	
2008年09月17日	第 9.0.1版	
2008年10月20日	第 9.0.2版	
2008年10月27日	第 9.0.3版	
2009年02月25日	第10.0.0版	
2009年10月15日	第10.1.0版	
2009年12月01日	第11.0.0版	
2010年02月15日	第11.0.1版	
2010年04月05日	第11.0.2版	
2010年06月08日	第11.1.0版	
2010年08月27日	第11.1.1版	
2010年11月24日	第11.1.2版	
2011年02月23日	第11.2.0版	
2011年03月07日	第11.2.1版	
2011年05月16日	第11.2.2版	
2011年07月01日	第11.2.3版	
2011年11月01日	第11.3.0版	
2011年12月20日	第11.4.0版	
2012年02月15日	第11.4.1版	
2012年02月29日	第11.4.2版	
2012年04月23日	第11.4.3版	
2012年07月24日	第12.0.0版	
2012年10月01日	第12.0.1版	
2012年12月03日	第12.1.0版	
2013年03月22日	第12.1.1版	
2013年04月15日	第13.0.0版	
2013年04月22日	第13.0.1版	
2013年05月17日	第13.0.2版	
2013年06月03日	第13.0.3版	
2013年06月17日	第13.0.4版	
2013年07月08日	第13.1.0版	
2013年10月01日	第13.1.1版	
2013年10月28日	第13.1.2版	

改正履歴

改正年月日	版	備考
2013年11月05日	第13.1.3版	
2013年11月25日	第13.2.0版	
2013年12月18日	第13.2.1版	
2014年02月19日	第13.3.0版	
2014年03月03日	第13.3.1版	
2014年04月01日	第13.4.0版	
2014年04月23日	第13.4.1版	
2014年06月03日	第13.4.2版	
2014年06月30日	第13.4.3版	
2014年8月6日	第13.4.4版	
2014年8月25日	第14.0.0版	
2014年9月8日	第14.0.1版	
2014年9月25日	第14.1.0版	
2014年12月11日	第14.2.0版	
2015年1月23日	第14.2.1版	
2015年4月1日	第14.2.2版	
2015年4月23日	第14.2.3版	
2015年5月7日	第14.2.4版	
2015年8月5日	第14.2.5版	
2015年12月1日	第14.2.6版	
2015年12月24日	第14.2.7版	
2016年3月22日	第15.0.0版	
2016年5月16日	第15.0.1版	
2016年7月1日	第15.0.2版	
2016年8月8日	第15.0.3版	