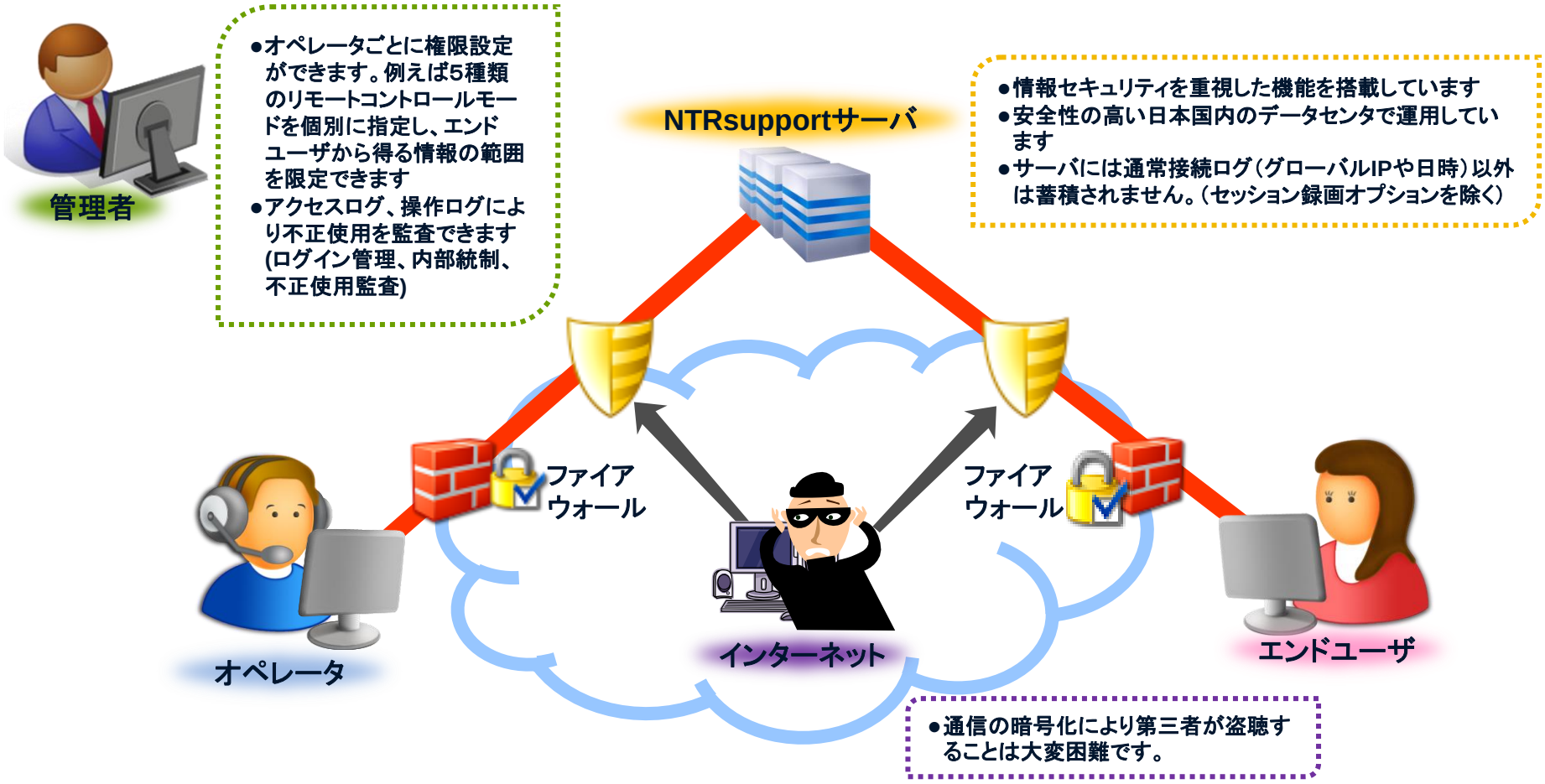
NTR global

NTRsupportの情報セキュリティ

株式会社インターワーク

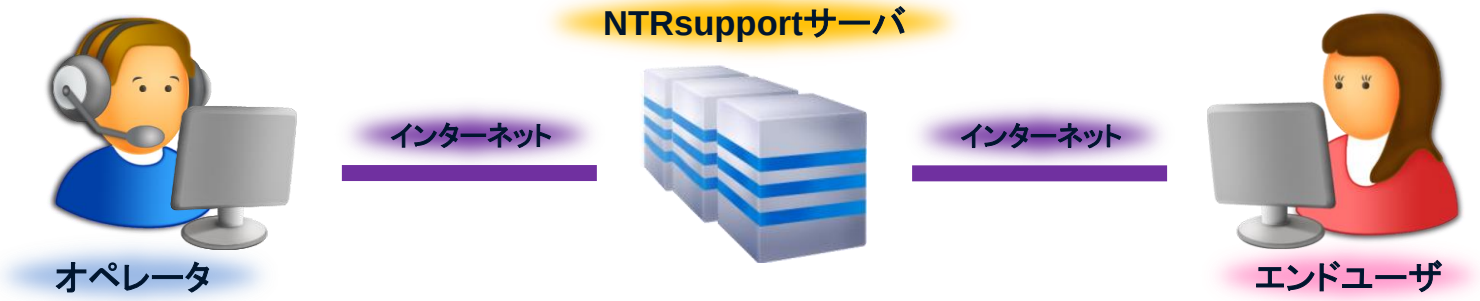
NTRsupportの情報セキュリティ　概要

NTRsupportは皆さまにご安心してお使いいただけるよう、機能の細部に至るまでセキュリティに配慮しております。
256ビットAES暗号化により通信を保護し、リモートコントロールはエンドユーザが承認操作するまで開始されません。
また、管理者機能でサポートオペレータの権限設定やログの出力により、セキュリティポリシーに沿った細かい設定が可能です。



NTRsupportの情報セキュリティ【顧客のコンピュータを管理する】

オペレータがエンドユーザの画面を見て、操作を行うモードですが、ユーザのPCを再起動した後にそのままログイン画面から自動で再接続が可能です。さらに、オペレータもしくはユーザによるタスクトレイからの切断操作がない限り、リモート接続を継続させることが出来ます。



- ●オペレータの操作により、エンドユーザPCの任意のアプリケーションを起動したりOS設定を変更できます。その過程すべての画面をオペレータは見ることができます
- ●エンドユーザPCの再起動あるいはログオフした後にそのまま再接続が可能です
- ●画面キャプチャにより、エンドユーザPCの画面を画像として保存ができます
- ●ファイル転送機能により、エンドユーザPCの任意のファイルを取得できます。エンドユーザPCに任意のファイルを送信できます
- ●オペレータPCの情報はエンドユーザには一切送られません

- ●リモートコントロールの承認を行うと、オペレータがエンドユーザPCの操作を行えるようになり、エンドユーザ画面をオペレータと共有します
- ●任意のファイルをオペレータは取得でき、ファイルを送信される(書き換えられる)こともあります

NTRsupportの情報セキュリティ【顧客のコンピュータを操作する】

オペレータがエンドユーザの画面を見て、操作を行うモードです

- オペレータの操作により、エンドユーザPCの任意のアプリケーションを起動したりOS設定を変更できます。その過程すべての画面をオペレータは見ることができます
- 画面キャプチャにより、エンドユーザPCの画面を画像として保存ができます
- ファイル転送機能により、エンドユーザPCの任意のファイルを取得できます。エンドユーザPCに任意のファイルを送信できます
- オペレータPCの情報はエンドユーザには一切送られません

- リモートコントロールの承認を行うと、オペレータがエンドユーザPCの操作を行えるようになり、エンドユーザ画面をオペレータと共有します
- 任意のファイルをオペレータは取得でき、ファイルを送信される(書き換えられる)こともあります

NTRsupportの情報セキュリティ【顧客の画面を見る】

オペレータがエンドユーザの画面を見るモードです

- エンドユーザの画面を見ることができます
- 画面キャプチャにより、エンドユーザPCの画面を画像として保存ができます
- 見ることができるのは、エンドユーザが操作した画面だけです
- オペレータPCの情報はエンドユーザには一切送られません
- 閲覧のみで、ファイル転送は行えません。

- リモートコントロールの承認を行うと、エンドユーザ画面をオペレータに閲覧させます
- デスクトップ画面以外の情報をオペレータに送ることはありません
- オペレータから操作されることはありません

NTRsupportの情報セキュリティ【オペレータの画面を共有する】

エンドユーザがオペレータの画面を見て、操作を行うモードです

●オペレータPCの画面をエンドユーザPCに表示します
●オペレータのPCをエンドユーザに操作させることが出来ます
●オペレータPCで表示した画面以外の情報はエンドユーザには一切送られません
●ファイル転送は行えません

●リモートコントロールの承認を行うとエンドユーザPCにオペレータ画面が表示されます。またオペレータのPCを操作することが出来ます
画面キャプチャにより、オペレータPCの画面を画像として保存できます
●オペレータから操作されることはありません
●ファイル転送は行えません

NTRsupportの情報セキュリティ【オペレータの画面を見せる】

オペレータの画面をエンドユーザに見せるモードです

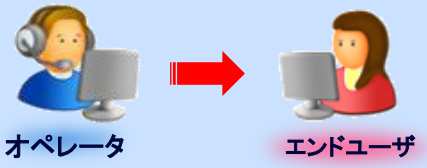
- オペレータPCの画面を、エンドユーザPCに表示します
- エンドユーザから操作されることはありません
- エンドユーザPCの情報は取得できません
- オペレータPCで表示した画面以外の情報はエンドユーザには一切送られません
- ファイル転送は行えません。

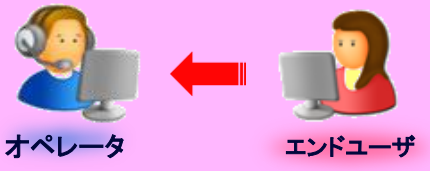
- オペレータPCを見ることができます。
- リモートコントロールの承認を行うと、エンドユーザPCにオペレータ画面が表示されます
- 画面キャプチャにより、オペレータPCの画面を画像として保存できます
- 見ることができるのは、オペレータの操作した画面だけです

NTRsupport5種類の接続モード

NTRsupportはご利用シーンに合わせて5種類の接続モードが選択できます

顧客のコンピュータを管理する	オペレータがエンドユーザの画面を見て、操作を行うモードですが、ユーザPCを再起動後、そのままログイン画面から自動で再接続が可能です。さらに、オペレータもしくはユーザによるタスクトレイからの切断操作がない限り、リモート接続を継続させることが出来ます。
顧客のコンピュータを操作する	オペレータがエンドユーザの画面を見て、操作を行うモード
顧客の画面を見る	オペレータがエンドユーザの画面を閲覧するのみ
オペレータの画面を共有する	エンドユーザがオペレータの画面を見て、操作を行うモード
オペレータの画面を見せる	オペレータの画面をエンドユーザに見せるモード





【NTRsupportのセキュリティ機能】

情報漏洩の防止やセキュリティに関係する機能はどのようなものがありますか？

セキュリティに関係	
エンドユーザの承認	エンドユーザが承諾をするまでは、リモート接続を開始しません
エンドユーザの識別	セッション割当機能では、正しい数字(セッション番号)を入力した相手としかリモートコントロールを開始しません
ファイル転送の事前承認	エンドユーザの承諾がなければ、ファイルを転送できないように設定が可能です
アプリケーション選択機能	アプリケーション選択機能を使うと、指定したアプリケーションの画面だけをオペレータに操作＋閲覧させることができます。アプリケーション選択機能を常時必須にした運用も可能です
ログ・操作記録	管理者は、管理者機能により各種レポートを出力できます

リモートコントロールやファイル転送機能の暗号化の方式は？

- 256bit AES暗号を採用しています
- オペレータ⇔NTRsupportサーバ、エンドユーザ⇔NTRsupportサーバのいずれもが暗号化通信の対象です
- ログ、操作記録も暗号化して保存しています

5種類のリモートコントロールモードとは？

- 「顧客のコンピュータを管理する」、「顧客のコンピュータを操作する」、「顧客の画面を見る」、「オペレータの画面を有する」、「オペレータの画面を見せる」の5種類です

オペレータが権限外の操作をすることを防ぐ機能はありますか？

- 管理者は、オペレータIDごとにリモートコントロールモード(5種類)、アプリケーション選択機能を設定できます

オペレータPCの情報がエンドユーザに見られる/コピーされる危険性はありますか？

- オペレータが、オペレータPCの画面を意図的に見せたり、オペレータPCのファイルを意図的に転送した場合だけエンドユーザは情報を受け取れます。エンドユーザの操作でオペレータPCの情報を見る/コピーするといった機能はありません

アプリケーション選択機能とはなんですか？

- パソコンで稼動している特定アプリケーションのウィンドウだけを相手側に閲覧、操作することが出来る機能で、おもにセキュリティ用途で利用するものです

リモートコントロール中に不審を感じたら、通信を遮断できますか？

- オペレータまたはエンドユーザどちらからも、クローズボタンをクリックすることで即時にリモートコントロールを終了することができます。(「顧客のコンピュータを管理する」はタスクトレイ上のアイコンからの終了となります)

【NTRサーバの安全性】

NTRsupportサーバの運用場所、運用体制はどこですか？
- 日本国内では、NTTコミュニケーションズ社のクラウドサーバで運用しています
- サーバは、開発元であるASG社（アメリカ）のサービス専用で利用しており、それ以外の用途に兼用していません
- データセンター、ASG社のいずれも、24時間体制でサーバ監視を行っています

NTRサーバが不正アクセスされる危険性はありませんか？
- サーバのセキュリティ設定を厳重にすることで不正アクセスを防いでいます
- サーバのセキュリティパッチを適用して、セキュリティホールを塞いでいます
- NTR管理者は、ログイン記録や操作記録をチェックすることで、後日の監査を行っています
- サーバを設置しているデータセンターは入退出管理などの対策を行っています
- 仮にサーバが不正アクセスされても、ID/Passwordやその他のオペレータ/エンドユーザのデータは暗号化して記録しており、容易には解読できないようにしています

NTRsupportの安全性を外部監査していますか？
- ASG社が、定期的にNTRsupportのASPサービス、NTRソフトウェア(サーバ、exe、ActiveX)の外部監査を受けて安全性を確認しています

サポート担当者やエンドユーザがニセのNTRsupportサーバと通信するフィッシングの危険性はありませんか？
- 証明書(GoDaddy社)によりサイト認証を行っているので、通所はフィッシングの危険性はありません

ASG社は、パスワードや通信記録の暗号を解読できますか？
- できません。パスワードや通信記録の暗号を解くには、お客様の解除キーが必要です
- 解除キーも暗号化してサーバに保存されており、ASG社でも解読できません

ASG社は、通信内容を解析できるのではないですか？
- ASG社では、厳格な社内運用ルールで不正行為を禁止し、外部監査を受けて安全性を確保しています
- 例外的に、技術的トラブルの解析のために、お客様の許可を得た上で通信内容を保存することがあります

NTRsupport 情報セキュリティFAQ【NTRサーバの安全性】

NTRsupportサーバを経由するのみというが、本当に情報は蓄積されないのですか？

- 「オペレータの画面を見せる」、「オペレータの画面を共有する」ではエンドユーザPCの情報をオペレータは一切取得できません
- 「顧客のコンピュータを管理する」、「顧客のコンピュータを操作する」、「顧客の画面を見る」ではエンドユーザPCの情報を取得可能です。
  オペレータPCでの情報の蓄積が可能ですので、運用ルールにより情報保護対策が必要です
- ファイル転送を行なった際はファイルそのものを蓄積することはなく、移動のパスのみを記録します
- 管理者が通信記録を取得するよう設定した場合のみ、NTRサーバは通信内容を保存します
- セッション録画オプションが有効とした場合のみ、リモートセッション中の画面情報を動画として保存します
- オペレータPC/エンドユーザPCの通信内容は暗号化されているので、第三者が盗聴してもそのままでは内容を解読できません

オペレータ側がエンドユーザPCの情報を絶対に取得できないという保障はありますか？

- 「オペレータの画面を共有する」、「オペレータの画面を見せる」ではエンドユーザPCの情報を一切取得できません
- 「顧客のコンピュータを管理する」、「顧客のコンピュータを操作する」、「顧客の画面を見る」では取得可能ですので、運用ルールによりオペレータの
  管理を行う必要があります

リモート中にネットワークに侵入される危険性はありませんか？　回避方法はありますか？

- NTRsupportが原因となる侵入は、通常はありません
- オペレータPCがウイルスに感染すると危険性がゼロとはいえませんので、オペレータPCでは常にウイルス対策ソフトを動作させてください

【不正使用の防止】

第三者の不正使用を防ぐ仕組みは、どのようなものを備えていますか？

- 管理者、オペレータはID/Password認証によるログインが必要です
- ログインを受け付けるIPアドレス、MACアドレスを指定することで、特定の場所や端末でなければ利用できないよう設定が可能です
- ログイン記録や操作記録をチェックすることで、管理者により後日の監査が可能です

オペレータがログインに失敗するとどうなりますか？

- 3回のログイン失敗でアカウントが一定時間停止されログインできなくなります。この情報は管理ログに記録されます

内部関係者の不正使用を防ぐ仕組みはありますか？

- 管理者は、(1)オペレータのIDを設定できます、(2)オペレータの操作範囲を限定できます、(3)アプリケーション選択機能で、エンドユーザは、リモートコントロールで取得するウィンドウを制限できます
- 管理者は、オペレータと管理者のログイン記録や操作記録をチェックすることで、後日の監査が可能です
- ASG社内の管理者は、NTR関係者のログイン記録や操作記録をチェックして、監査を実施しています
- ASG社では、定期的にセキュリティの外部監査を受けています

NTRソフトウェア(exe、ActiveX)を組み込んだエンドユーザPCを放置した場合、リモートコントールが勝手に動作する危険性はありませんか？

- ありません。exe、ActiveXのいずれも、起動後に動作を承認するクリックの操作を行わなければリモートコントールを開始しないようになっています

【ウイルス対策】

オペレータPCがエンドユーザPCからウイルスなどを感染させられる危険性はありますか？

- 顧客のコンピュータの操作でエンドユーザPCのファイルをオペレータPCにコピーすると、ウイルス付きファイルを受け取る可能性があります
- オペレータPCにウイルス対策ソフトが導入されていれば、(既知ウイルスであれば)コピーした時点で検出・警告されるので感染には至りません
- 顧客のコンピュータの操作であっても、ファイルコピーの操作を行わなければ、エンドユーザPCからウイルスに感染させられることはありません
- その他のモードでは、エンドユーザPCからウイルスに感染させられることはありません

NTRソフトウェア(サーバ、exe、ActiveX)にウイルスや不正なコードが混入する危険性はありますか？

- NTRソフトウェアはASG社が100%所有権を有するソフトウェアです。開発・提供のすべての段階でASG社が管理しており、不正な第三者ソフトウェアの混入が起こらない体制です
- 開発、運用で利用するサーバ/クライアントPCはセキュリティ対策を実施しています
- 証明書(GoDaddy社)によって、ソフトウェアがASG社提供のもので、なおかつ改変されていないことを確認できます

【運用】

個人情報の漏洩事故に繋がる危険性はないですか？

- 技術面と運用面の2面での考察が必要です。
- 技術面では、NTRsupportのセキュリティ対策機能で漏洩を防ぐ対策を施しています
- 運用面では、NTRsupportを利用する管理者・オペレータのための運用ルール、情報管理ルールを策定して、人的な漏洩が起こらない対策が必要です
- 具体的には、リモートコントールを行うオペレータが、(1)取得してよいエンドユーザPCの情報の範囲、(2)行ってよい操作の範囲、(3)コピーしてよいファイルの範囲を、社内ルールとして定めます。運用時には、管理者はログイン記録、通信記録を定期的に監査します

エンドユーザのファイルを転送できない方式でサポートできますか？

- 可能です。「顧客の画面を見る」、「オペレータの画面を見せる」、「オペレータの画面を共有する」の3種類ではエンドユーザのファイルをコピーできません。
- また、「顧客のコンピュータを操作する」、「顧客のコンピュータを管理する」であってもオペレータのID毎に、ファイル転送機能の利用可否の設定が可能です。

エンドユーザの情報を一切見ない使い方はできますか？

- 可能です。オペレータPCの画面を閲覧させるだけの「オペレータの画面を見せる」を使います。操作方法説明や教育などの用途で利用可能です

導入する際に、ファイアウォール/ルータに穴を空ける必要がありますか？

- 通常はありません。NTRsupportはWWWアクセスを模倣する機能を持っており、Webブラウザができる環境であればファイアウォール/ルータに穴を開ける(特定ポートの通信を新たに許可する)必要はありません
- これは、オペレータ、エンドユーザのいずれにもあてはまります

外部からリモートコントロールされることに危険を感じているユーザに、信頼と安心を与えるにはどのようにしたらよいでしょうか？

- セキュリティを重視した機能を実装しているリモートコントロールソフトを採用していることをお伝えください
- 運用面では、エンドユーザに、明確な運用ルールのもとでサービスを提供しております