Optimal Remoteセキュリティホワイトペーパー

株式会社オプティム

Ver 1.0

2022/2/17

目次

オプティム セキュリティポリシー

情報セキュリティ基本方針

株式会社オプティム（以下、「当社」という。）は、ITを利用するお客様をサポートするためのテクノロジー・サービス、そしてビジネスモデルを創造することを目的とした事業を展開してまいりました。本事業にて提供する当社サービスは、ネットそのものを空気のように絶対不可欠なものであるにもかかわらず、まったく意識する必要のない存在に変えていくことから、お客様に簡単・安心して利用していただくために、情報セキュリティを取り組むことは、当社の重要なミッションです。よって当社はこれらのミッションを達成することを目的に、情報セキュリティ基本方針を策定し、以下事項を推進してまいります。

1.（情報セキュリティマネジメントシステム（ＩＳＭＳ）の構築）

当社は、当社のサービスに関わる情報資産の重要性を役員、従業員一同が認識し、情報資産の保護のため、情報資産の盗難、改ざん、破壊、漏洩、不正アクセス行為等に対し、組織的、技術的に適切なＩＳＭＳを構築いたします。

2.（情報セキュリティマネジメント体制）

当社は、情報セキュリティを推進していく全社的機関として情報セキュリティ委員会を設置し、全社レベルで情報セキュリティの状況を正確に把握し、必要な対策を迅速に実施できるよう積極的な活動を行います。

3.（法令等の遵守）

当社は、当社が取り組む情報セキュリティに適用される法令、その他の規範・契約を遵守いたします。

4.（情報資産の保護）

当社は、保有及び運用管理する全ての情報資産を、機密性・完全性・可用性の視点から重要性を認識するとともに、リスクアセスメントを行い適切な情報資産の保護を行います。

5.（情報セキュリティ社内教育・研修の実施）

当社は、情報資産を扱う役員、従業員一同が、情報資産の重要性を認識するために、情報セキュリティに関する社内教育・研修を実施し、本基本方針の徹底を図ります。

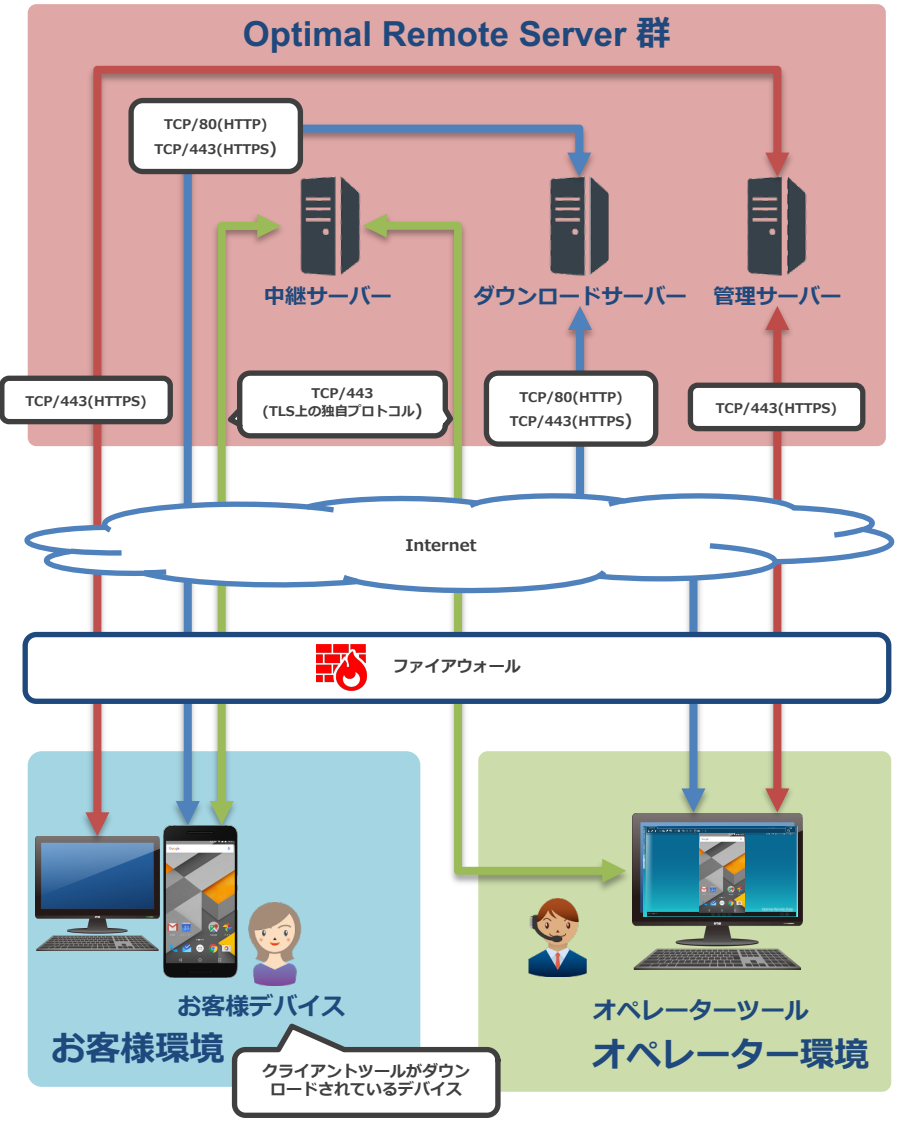
6.（情報セキュリティインシデントの対応）

当社は、万一、情報セキュリティ上のインシデントが発生した場合、またはその予兆があった場合、迅速な原因究明を行い最小限の被害に食い止める最善の策を講ずるとともに、予防及び維持改善に努めます。

7.（ＩＳＭＳの継続的見直し）

当社は、情報資産の適正な管理・運用のため、本基本方針及び関連する社内規程、管理体制を定期的に見直し、改善を図ってまいります。

システム概要



- Optimal Remoteのシステムはサポートを実施するオペレーターが利用する「オペレーターツール」、サポートを受けるお客様が利用する「クライアントツール」およびインターネット上のサーバーで構成されます。
- サーバーはオペレーターとお客様の接続を管理する「管理サーバー」、オペレーターとお客様の接続を中継する「リレーサーバー（中継サーバー）」とクライアントツール・オペレーターツールの配信を行う「ダウンロードサーバー」の3種類があります。
- 管理サーバー、ダウンロードサーバー、中継サーバーともに冗長化しています。
- 本サービスはファイアーウォールを介してインターネットに接続しています。

Protocol and Port

Server	Port (Protocol)	用途
ダウンロードサーバー	TCP/80(HTTP) TCP/443(HTTPS)	クライアントツールのダウンロード、オペレーターツールのバージョンアップ
管理サーバー	TCP/443(HTTPS)	オペレーター管理、ログ管理サイト オペレーターツールでのログイン 受付番号発行 オペレーターとお客様のペアリング サポート時間などログの保存
リレーサーバー(中継サーバー)	TCP/443(TLS上の独自プロトコル)	オペレーター・お客様間の画面転送、遠隔操作

- 商用環境の設定変更は常にレビュー後に実施します。
- サーバーとネットワークは常に別の拠点から監視しており、後で分析可能な状態です。
- 問題が発生すると電話とEメールにて担当者に通知され、復旧作業を開始します。
- OSとミドルウェアの脆弱性情報を常に監視しており、緊急度と重要度に応じてパッチを適応しています。
- 情報セキュリティインシデントは定義されたフローに則って処理します。

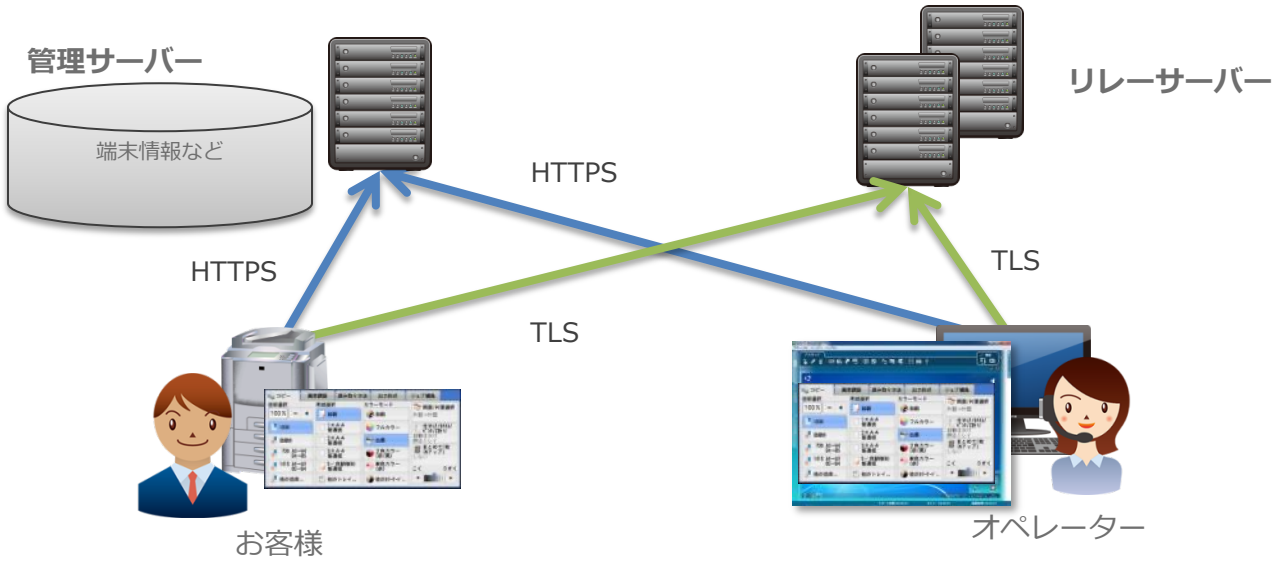
監視項目(代表的なもの)

分類	項目
サービス監視	別拠点よりサービス毎にHTTP/HTTPSによるサービス死活監視
サーバー死活監視	サーバーごとに死活監視
リソース監視	CPU使用率
	メモリ使用量
	ストレージ空き容量
	プロセス数
	ネットワークトラフィック

- 稼働率
  - 24時間365日の提供を行います。稼働率は計画停止作業を除き99.9%を目標としています。
  - サーバーメンテナンスで停止を伴う場合、1週間前までに通知いたします。
- ソフトウェア更新
  - 本サービスはオープンソースを利用しています。重要なセキュリティ更新が発生した場合重要度に応じて随時更新を実施しています。
- 復旧手順
  - 想定される障害の場合、手順に沿って復旧作業を実施します。
  - 想定外の障害の場合、開発者と連携しながら早急な復旧作業を実施します。

サーバー上のデータ管理

- お客様の端末情報などの情報は管理サーバーに保存されます。
- 共有された画面の情報はリレーサーバーを経由し、リレーサーバー上には情報は残りません。
- 全てインターネット上の通信はTLSによって暗号化されています。
- 全てのデータは毎日遠隔地にバックアップされており、そのデータを利用してサービスを再開できます。



- オペレーターツールの利用には企業コード、ID、パスワードが必要です。
  - パスワードは半角英数字、半角記号を使用し8 文字以上 20 文字以内で設定でき、ハッシュ化して保存されます。
  - パスワードを一定回数間違えるとアカウントをロックする設定が可能です。
- 企業コードはオプティムが管理しています。
- 企業で管理アカウントを発行することができ、管理アカウントによりオペレーターを管理することができます。
- オプティムにおけるサーバー管理
  - サーバー管理およびデータ管理には専用のIDが必要です。
  - IDはID管理基盤で管理されています。
  - 商用環境の管理は限られた社員のみが実施します。
  - 社員の退社や移動で不要になったアカウントは即座に停止されます。

- 商用環境はインターネットデータセンターあるいはインターネットデータセンター上で提供されるIaaS上に構築されています。
- インターネットデータセンターは監視カメラや複数のセキュリティゲートなどが設置されており、地震にも耐えうる建物に設置されています。
- 全てのシステムはファイアウォールの内側に設置しています。

データセンター仕様

	日本	欧州	北米
認証	ISO27001もしくは ISAE3402/SSAE16	ISO27001:2005およびISO9001	SSAE16 SOC-1 Type II
所在地	日本国内	Amsterdam	San Francisco
建物形態	専用建物	非開示	非開示
耐震	震度7を目標として設計	非開示	非開示
無停電電源	有	有	有
給電ルート	特別高圧 本線予備選方式	非開示	非開示
非常用自家発電	有	有	有
消火設備	自動消火設備:有 火災検知システム:有	VESDA	非開示
避雷対策	直撃雷対策:有 誘導雷対策:有	非開示	非開示
入退館管理	入退室記録:7年 監視カメラ保存期間:3ヶ月 個人認証システムあり	監視カメラ:あり 個人認証システム:あり	監視カメラ保存期間:90日

OPTiM

www.optim.co.jp

Optimal Remoteにおけるセキュリティについて