

InfoTrace 360

サービス仕様書

2026年2月9日
株式会社ソリトンシステムズ

目次

はじめに.....	3
1. サービスの概要	3
1-1. サービス提供条件.....	3
1-2. 通知	3
1-3. サービスシステム内に保持するお客様データ	3
2. サービスのセキュリティ	5
2-1. 通信の暗号化	5
2-2. ユーザー認証	5
2-3. 証明書.....	5
2-4. ユーザーID とパスワード	5
2-5. データの暗号化	6
3. サービス導入時の確認事項.....	6
3-1. サービス指定ソフトウェア.....	6
3-2. 使用する通信	6
3-3. ログスポット提供サービスに関する留意事項	6
3-4. ログダウンロードオプションに関する留意事項.....	7

はじめに

本書は、株式会社ソリトンシステムズ（以下、当社）が提供する InfoTrace 360 サービス（以下、本サービス）の技術的な情報を記載したものです。本書の内容は、サービスの変更その他に伴い更新する場合があります。常に最新の版をご参照ください。

1. サービスの概要

本サービスは、InfoTrace Mark II Client により収集した証跡ログ、システム情報・インベントリ情報を分析/可視化する機能を提供します。また、「USB デバイス制御オプション」により USB デバイス制御機能を利用できます。「ログダウンロードオプション」「ログスポット提供サービス」により証跡ログを提供します。

本サービスでは、お客様管理者が Web ブラウザを使用して本サービスの各管理画面にアクセスする Soliton Cloud Service Portal（以下、SCSP と表記）を提供します。SCSP では、下記の機能を使用できます。

1) Soliton Cloud Service Portal（以下、SCSP と表記）

本サービスの各管理画面にアクセスするポータル Web サイトです。各管理画面へのアクセス時に安全な認証を行う機能を提供します。

2) クライアント管理

InfoTrace Mark II Client をインストールしたコンピューターのシステム情報・インベントリ情報を管理と USB デバイスの制御機能を提供します。また、InfoTrace Mark II Client のインストーラー、マニュアルなどの各資料を提供します。

3) 360 ダッシュボード

各種解析レポートを作成します。分析した情報を約 90 日間保管します。

1) HiQZen（オンラインストレージサービス）

ログダウンロードオプションまたは、ログスポット提供サービスをお申込みの際に、証跡ログを提供します。

1-1. サービス提供条件

本サービスは下記の条件で提供します。

項目	内容
提供エリア	日本国内
データ保管先	日本国内のデータセンターにて保管・運用
サービス提供時間	24 時間 365 日、但しメンテナンスによる停止あり
稼働監視	24 時間 365 日、但しメンテナンス中は対象外
ライセンス	InfoTrace 360 サービス実施要領別紙「10.ライセンス」を参照

1-2. 通知

障害やメンテナンスに関する通知を下記の通り行います。

通知の種類	通知する条件	通知目標時間	通知方法
障害	サービス停止、性能低下などの影響が広範に生じた場合に通知	障害検知から 120 分以内	サービスポータル またはメール
メンテナンス	サービスへの影響を伴うメンテナンスを行う場合に通知	原則 10 日前まで	メール
緊急メンテナンス	緊急メンテナンスの実施時	なるべく早く	メール

1-3. サービスシステム内に保持するお客様データ

本サービスのシステム内には、下記のデータを保持します。

データの種類	説明
設定データ	サービスシステムが動作するための設定情報です。お客様管理者、サービ

	ス利用者が本サービスに設定した内容が保存されます。設定可能な項目はマニュアルをご参照ください。
組織情報	下記の情報をお客様より提供頂き、当社でサービスシステムに設定することで、360 ダッシュボードに組織情報を表示できます。 <ul style="list-style-type: none">・ 氏名・ 役職・ 会社名・ 組織名・ メールアドレス
台帳管理	お客様管理者が下記の情報を当社のサービスシステムに設定することで、クライアント管理にてコンピューターのインベントリ情報と自由に設定できる資産項目を紐づけて CSV ファイルとして出力することができます。 <ul style="list-style-type: none">・ 資産項目・ インベントリ情報
証跡ログ、インベントリ情報	InfoTrace Mark II Client が収集し、サービスシステムにアップロードする情報です。下記の内容が含まれます。 <ul style="list-style-type: none">・ コンピュータ名・ 端末 ID・ 操作内容・ PC のモデル・ OS バージョン・ IP アドレス・ MAC アドレス・ ドライブ情報・ USB デバイス・ ログイン名・ インストールアプリケーション・ Windows Update 適用状況
システムログ	サービスシステムが記録するログです。端末 ID、InfoTrace Mark II Client のバージョン・状態に関する内容が含まれます。

障害調査に必要な場合、下記の情報を InfoTrace Mark II Client が収集しサービスシステムにアップロードする方法により取得することができます。情報収集中は、管理画面にて対象の端末の状態が「診断情報取得中」に代わります。アップロードされたデータは利用者がアクセスできない領域に一時保管され、収集後すみやかにサービスシステム上から削除します。

データの種類	説明
システム情報	Windows のシステム情報
イベントログ	Windows のイベントログ
Soliton 製品詳細情報	導入されている当社製品一覧および構成情報
証跡ログ	InfoTrace Mark II Client がその時点で保持している証跡ログ
サービス稼働情報	サービスシステムで指定したサービスプロセスの稼働状態
ファイルプロパティ	サービスシステムで指定したファイルのプロパティ情報
レジストリ値	サービスシステムで指定したレジストリの値
ユーザーダンプ	プログラムがクラッシュした時にそのプロセス状態を保存するファイル

2. サービスのセキュリティ

2-1. 通信の暗号化

下記、本サービスに対する通信は暗号化が行われます。

- ・ エージェントからの当社クラウドサービスへのデータ通信
- ・ 管理画面（360 ダッシュボード、クライアント管理、HiQZen）アクセス用のクライアント証明書取得
- ・ SCSPへの接続

2-2. ユーザー認証

SCSP 及び管理画面への接続には認証が必要です。認証の方式は下記の通りです。

接続の種類	認証の方式
SCSPへの接続	下記の二要素による認証 ・メールワンタイムパスワードまたは、Soliton Authenticator 認証 ・ユーザーID、パスワード
管理画面（360 ダッシュボード、クライアント管理、HiQZen）	・クライアント証明書（TLS クライアント認証） ・SAML（SCSPへのログイン情報を参照するので、各管理画面へのアクセス時には認証画面は表示されません）
HiQZenへの接続	ユーザーID とパスワードによる認証

2-3. 証明書

お客様管理者の端末（PC 等）には、本サービスで発行するクライアント証明書をインストールする必要があります。証明書の仕様は下記の通りです。

項目	内容
証明書発行枚数	1 契約あたり 1 枚まで
証明書の取得方法	アカウント通知メールに記載されたリンクから p12 ファイルをダウンロードして取得
証明書の失効	問い合わせフォームから証明書の再発行をお申込みください。元の証明書を失効し、新しい証明書を再発行します。作業には時間を要することがあります（目安：1～3 営業日）。
証明書の更新	証明書の有効期限が切れる約半年前に、証明書の更新案内をメールで送付します。案内に従い、証明書のダウンロードとインポートを行ってください。

2-4. ユーザーID とパスワード

管理アカウント

項目	内容
用途	SCSPへのログイン SCSP からは、クライアント管理画面、360 ダッシュボード、HiQZen 等にアクセスできます。
発行方法	当社で ID を発行し、申し込み時に指定頂いたメールアドレスにアカウント通知を送付します。パスワードは初回アクセス時にお客様自身で設定して頂きます。設定手順はアカウント通知に記載の案内を参照してください。
パスワードポリシー	SCSP は 8～64 文字、大文字/小文字/数字/記号から 3 種類以上です。

2-5. データの暗号化

本サービスシステム内のデータはすべて暗号化されています。

3. サービス導入時の確認事項

本サービスの導入に際しては、下記の条件をご確認ください。

3-1. サービス指定ソフトウェア

本サービスを使用する PC に下記のソフトウェアをインストールする必要があります。

サービス指定ソフトウェア名	機能
InfoTrace Mark II Client	インストールした PC からデータを取得し、サービスシステムに送信します。本サービスにより管理するすべての端末にインストールする必要があります。
Soliton Authenticator	ユーザーの指紋、顔、PIN などスマートフォンのセキュリティを利用して本サービスへのログインを行うスマートフォンアプリです。

InfoTrace Mark II Client がサポートする OS、サポート対象バージョンに関して下記の情報をご確認ください。

InfoTrace 360 クライアント動作環境

https://www.soliton.co.jp/products/category/product/pc-security/infotrace_360/?tab=03

3-2. 使用する通信

本サービスの利用に必要な通信は下記の通りです。必要な通信が行えるようにファイアウォールの設定変更等を行って頂く必要があります。

通信元	通信先	ポート、プロトコル
PC (InfoTrace Mark II Client)	アカウント通知に記載の通信先 「クライアント接続先」	443/tcp
管理端末	アカウント通知に記載の通信先 「管理画面アクセス先」 「ログダウンロード接続先」	443/tcp
管理端末	i360-01-ec-s2.soliton-ods.jp i360-01-wb-s2.soliton-ods.jp i360-01-logdls2.soliton-ods.jp secure.okbiz.okwave.jp www.soliton.co.jp	443/tcp

3-3. ログスポット提供サービスに関する留意事項

ログスポット提供サービスは、InfoTrace 360 のオプションメニューの一つです。360 ダッシュボードでは確認できない 90 日以上前のインシデントの情報を確認したい場合、インシデントに関する証跡ログを内部で保管する必要がある場合などに、本オプションを使用して証跡ログをお客様の手元にダウンロードできます。※ 本オプションの利用に際しては、本契約とは別途費用がかかります。証跡ログの提供は SCSP からアクセスできる HiQZen にて提供します。

※サービスシステム内には、過去 1 年分の証跡ログを保持しています。

ログスポット提供サービスは、以下の種類があります。お客様の目的に合わせてお申し込みください。

オプション名称	端末数	期間	申し込み時に必要な情報
ログスポット提供サービス	全端末	最大で連続する 30	必要な期間の最初と最後の日付 (た)

30 日分		日間	だし、30 日以内であること)
ログスポット提供サービス 1 年分	お客様指定の 1 端末	サービスシステム内 に保持している全期 間（過去 1 年間）	対象となる端末の管理 ID (TMID) とコンピューターネーム

4) ログスポット提供サービス利用の流れ

申込時にいただく「ログスポット提供サービス利用申請書（以下、利用申請書）」にて、対象のオプション名称を指定してください。当社が利用申請書を受理してから 10 日以内を目標にログのアップロードを開始します。アップロードが完了後、当社からお客様へメールにて通知しますので、証跡ログをダウンロードしてください。以下の注意事項についても、ご承知おきください。

- アップロード完了の通知は、InfoTrace 360 本契約の「アカウント送付先」に登録されているメールアドレスに対して行います。
- ダウンロード期限はアップロード完了日から 30 日後です。期限を過ぎると HiQZen から自動的に削除されます。
- 対象の証跡ログの量が多い場合は、アップロードに時間がかかる場合があります。

5) 提供時のファイル形式について

SCSP にログイン後、「その他の機能」 - 「HiQZen」から HiQZen の画面にアクセスできます。提供するデータの詳細な形式は下表を参照してください。

項目	ログスポット提供サービス 30 日分	ログスポット提供サービス 1 年分
提供ファイル 数と形式	申込み数量毎に 30 ファイル（1 ファイル 1 日分、それぞれ ZIP 圧縮形式）を提供します。	申込み数量毎に 1 ファイル（ZIP 圧縮形式） を提供します。
HiQZen の格納 フォルダ名	/it360-log/ご契約サポート ID	/it360-log/ご契約サポート ID
提供するログ のファイル名	YYYY-MM-DD_SP.zip ※YYYY-MM-DD は、証跡ログの収集日です。	TMID_AllData_YYYY-MM-DD.zip ※TMID は、端末固有に割り当てられた一意 の識別番号（ハイフンで区切られた英数 32 文字）です。 ※YYYY-MM-DD は、証跡ログの提供日です。
ファイル解凍 後のディレク トリ構造	/コンピューターネーム/zip ファイル群	/YYYY-MM-DD/ zip ファイル群 ※YYYY-MM-DD は、証跡ログの収集日です。
zip ファイル群 のファイル名	TMID_証跡ログ送信日時 15 行-英数字 32 行.zip	TMID_証跡ログ送信日時 15 行-英数字 32 行.zip
zip ファイル群 解凍後のファ イル名	証跡ログ送信日時 15 行.log	証跡ログ送信日時 15 行.log

3-4. ログダウンロードオプションに関する留意事項

ログダウンロードオプションでは、InfoTrace Mark II Client により収集した証跡ログを HiQZen にてダウンロード提供します。本サービスの料金とは別途、契約中のライセンス数に応じた費用がかかります。

1) 証跡ログの提供タイミング

ログは 1 日 1 回、1 日前（前々日の午前 5 時から前日の午前 5 時まで）の証跡ログを HiQZen にアップロードします。

※ログのアップロードは1契約ごとに順次処理するため、アップロード完了時刻は不定です。

※ダウンロードできる期限は、アップロードが完了した日より30日間です。

※証跡ログを何も受信していない日は、ログファイルがアップロードされません。

2) 提供するログの仕様

InfoTrace Mark II Clientにより収集した全クライアントの証跡ログ1日分を1つのファイルに圧縮したデータを提供します。詳細な形式は下表を参照してください。

項目	形式
HiQZenの格納フォルダ名	/it360-log/ご契約サポートID
提供するログのファイル名	YYYY-MM-DD.zip ※YYYY-MM-DDは、証跡ログの収集日です。
ファイル解凍後のディレクトリ構造	/YYYY-MM-DD/コンピューター名/zipファイル群
zipファイル群のファイル名	TMID_証跡ログ送信日時15桁-英数字32桁.zip ※TMIDは、端末固有に割り当てられた一意の識別番号(ハイフンで区切られた英数32文字)です。
zipファイル群解凍後のファイル名	証跡ログ送信日時15桁.log