HULFT-WebConnect
セキュリティホワイトペーパー

第 76 版
2024 年 8 月 1 日
株式会社セゾンテクノロジー

改訂履歴

本紙の改版履歴は以下のとおりです。

版数	発行日	改訂内容
1	2015 年 4 月	制定
2	2016 年 8 月	「API の認証・認可」を追加 「機密性」にクライアント種別によるブロック機能を追記
3	2017 年 12 月 11 日	アクセスコントロール」に IP フィルタによる接続制限機能を追加
4	2018 年 8 月 16 日	「可用性」の記載内容を変更
5	2020 年 8 月 17 日	クライアント種別の記載方式を変更
6	2022 年 8 月 1 日	「データの取り扱い」を追加 「通知」の記載内容を変更 表記ゆれの修正
7	2024 年 4 月 1 日	社名の変更 URL の「http」を「https」に修正 「個人情報保護法に基づく公表事項」の URL を変更

この HULFT-WebConnect セキュリティホワイトペーパー（以下「本書」といいます。）は、株式会社セゾンテクノロジー~~情報システムズ~~（以下「当社」といいます。）が提供する HULFT-WebConnect のインフラストラクチャーおよびアプリケーションにどのようなセキュリティ対策を施しているかを紹介するドキュメントです。

クラウドコンピューティング 環境

HULFT-WebConnect はクラウドコンピューティング環境として Amazon Web Services（「AWS」）の Amazon Elastic Compute Cloud（Amazon EC2）を採用しています。クラウドコンピューティング環境のセキュリティ対策については、下記 URL をご確認ください。

AWS Security Center
https://aws.amazon.com/security/

モニタリング

HULFT-WebConnect では自動モニタリングシステムを活用して、インスタンス監視（ハードウェアおよびオペレーティングシステムの死活監視、CPU 使用率監視）およびアプリケーション監視（Web サーバプロセスの死活監視、AP サーバプロセスの死活監視）を実施しています。異常検知時または警戒閾値を越えた場合、当社の運用担当者および開発者にアラート情報をプッシュ通知します。

可用性

HULFT-WebConnect は複数のアクセスポイントを提供しています。HULFT-WebConnect のクライアントは、お客様のご利用環境に応じて自動的に最寄りのアクセスポイントを選択します。最寄りのアクセスポイントが何らかの原因で応答しない場合も、クライアントは接続可能なアクセスポイントの中で最適なアクセスポイントを自動的に選択します。
また、HULFT-WebConnect では、Web サーバ、AP サーバ、DB サーバについて冗長構成をとっており、可用性を確保しています。

機密性

HULFT-WebConnect は通信の機密性を確保するために、HULFT-WebConnect とクライアント間の通信は TLS による経路暗号を常時適用します。
また、登録済みアカウントや接続情報の不正利用を防ぐ目的で、HULFT-WebConnect はアカウントパスワードや接続パスワードをハッシュ化して保持します。

HULFT-WebConnect は、中継転送中のデータをディスクに書き込まず、オンメモリで中継します。さらに、HULFT-WebConnect では予期しない転送相手からのファイル転送を防止するために、接続設定で当該コネクション ID に接続できるクライアント種別を限定したり、中継許可設定（ホワイトリスト形式で中継転送の実行可否のフィルタリングを設定）を行うことができます。なお、中継許可設定はファイル転送の配信側、集信側の双方で設定する必要があるため、配信側のみ設定、または集信側のみ設定するのに比べ、より強固なセキュリティを提供しています。

API の認証・認可

HULFT-WebConnect で公開している Web API および CLI では、API キーによる認証・認可の仕組みを提供しています。API キーには有効期限とアクセス範囲（スコープ）を設定することができます。適用業務に応じて API キーを設定することで、許可されていない情報へアクセスする等の不正操作を防止することが期待できます。

アクセスコントロール

HULFT-WebConnect は当社内外問わず悪意のあるユーザーからの攻撃を防ぐために、事前に許可されたユーザーだけが HULFT-WebConnect の管理サーバにアクセスできる仕組みを導入しています。また、管理サーバへのアクセスを当社内からの通信に特定することで、故意・過失による不正アクセスの可能性を抑制しています。
また、IP フィルタにより接続元 IP アドレスによって HULFT-WebConnect への接続制限を行うことができます。

開発工程におけるセキュリティ対策

HULFT-WebConnect はソースコードの脆弱性を早期に発見するために、開発工程において静的ソース解析ツールおよび疑似攻撃型脆弱性診断ツールによる検証を実施しています。
また、開発環境、ステージング環境、プロダクション環境（お客様がご利用になる環境）をそれぞれ用意し、未検証のアプリケーションをプロダクション環境にデプロイしない仕組みを導入しています。

個人情報

当社は、本サービスの提供にあたり、個人情報保護法、電気通信事業法その他の関係法令および当社の「個人情報保護法に基づく公表事項」（https://~~-~~www.saison-technology.com/privacy-policy~~home.saison.co.jp/privacy/~~）にしたがって、個人情報（個人情報保護法第 2 条第 2 項において定義される情報をいいます。）、通信の秘密およびプライバシー等を適正に取り扱います。

データの取り扱い

当社は、① HULFT-WebConnect サービスの提供、および、② HULFT-WebConnect サービスの改善・向上を目的とした調査、分析のため、以下に列記するデータを取り扱います。これらデータには、お客様が本サービスを通じて送信する文章、画像、プログラムその他一切の情報（HULFT-WebConnect 利用規約 第 9 条第 3 項に定める「本データ」と同義であり、以下「本データ」といいます）は含みません。
なお、「お客様が登録した、転送設定などの情報」および「お客様が使用した、サービス機能の履歴」は、HULFT-WebConnect サービス基盤において暗号化して保持、管理します。

・お客様が登録した、転送設定などの情報
・お客様が使用した、サービス機能の履歴
・サービス稼働中の各種サーバログ

なお、当社は、① お客様の事前の書面による同意、または、② 裁判所の命令、監督官公庁もしくはその他法令・規則の定めに従った要求のいずれかがない限り「本データ」にアクセスしません。また、HULFT-WebConnect は、サービスにおける各機能の中で「本データ」を保持しません。お客様が、HULFT-WebConnect の機能を利用して、「本データ」をオンメモリ中継する際、HULFT-WebConnect は、自身のサービス範囲内でデータの漏えい対策を行います。しかしインターネットの通信網における、HULFT-WebConnect サービス範囲外のデータの漏えい対策はお客様の責任となります。また、「本データ」の性質やお客様の業務内容およびサービスの利用目的に応じたセキュリティ要件（セキュリティ強度レベル等）を決定し、それを実行する責任はお客様自身にあります。したがって、お客様が HULFT-WebConnect サービスをどのように構成し、「お客様が転送するデータ」をどのように扱うかについては、お客様の判断と責任の下でコントロールしていただく必要があります。

通知

本書は情報提供の目的のみのために提供されるものです。本書は、本書の発行日時点での情報を記述しており、これらは事前の通知なく変更される場合があります。最新の情報については、https://www.hulft.com をご確認ください。

お客様は本書の情報および HULFT-WebConnect の使用について独自に評価する責任を負うものとします。これらの情報は明示または黙示を問わずいかなる保証も伴うことなく「現状のまま」提供されるものです。

以上