

HULFT-WebConnect セキュリティホワイトペーパー

第三版

2017 年 12 月 11 日

株式会社セゾン情報システムズ

改訂履歴

本紙の改版履歴は以下の通りです。

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

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及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

<http://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（ハードウェア及びオペレーティングシステムの死活監視、CPU 使用率監視）及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、当社の運用担当者及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（Agent、CLI）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、各アクセスポイントの内部では、Web サーバ、AP サーバ、DB サーバにクラスタ構成を適用し、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（Agent、CLI）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 及び Agent 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（HULFT、API/CLI）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 及び 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のアクセス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。対象の運用パターンは Agent、Data Transfer API / CLI、Data Transfer Site を使用したファイル転送（ブラウザ転送）になります。

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及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及び当社の「個人情報保護法に基づく公表事項」(<http://home.saison.co.jp/privacy/>)に従って、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。）、通信の秘密及びプライバシー等を適正に取り扱います。

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、<http://www.hulft.com> をご確認ください。

お客様は本書の情報及び 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。

本書のいかなる内容も、当社、その関係者、サプライヤまたはライセンサーからの保証、代表的な意見、契約、条件を意味するものではありません。お客様に対する当社の責任は利用規約によって規定されています。また、本書は当社とお客様との間の契約に属するものではなく、また、当該契約が本書によって修正されることもありません。

以上