JP-LINKの技術仕様

1 はじめに

1.1 概要

JP-LINKは組織間でセキュアな通信を可能にするシステムである。このドキュメントでは、JP-LINKコアの技術的なアーキテクチャについて説明する。

目的は、JP-LINKとそのコンポーネントの概要を説明することである。
コンポーネントとプロトコルの詳細な説明は別のドキュメントから確認できる。

1.2 設計目標

以下に、JP-LINKの主な設計目標および設計意図を示す。

JP-LINKは分散されている:
データは組織間で直接交換される。仲介者はいない。 2つの組織が安全な接続を確立している場合、データの継続的な交換は、組織と組織間のネットワークの可用性のみに依存する。

データの所有権:
JP-LINKはデータの所有権の変更を行わない。データ所有者(サービス・プロバイダ)は、どのユーザーがどのサービスにアクセスできるかを制御する。

可用性(主要な検討事項):
プロトコルはシステムにボトルネックがひとつもないように設計されている。さらに、単一障害点になるコンポーネントはない。

JP-LINKで処理されたすべてのメッセージ:
デジタル証拠として利用できる。技術的ソリューションは、eIDAS [EIDAS]のデジタルシールに対する要件に準拠しなければならない。これは、セキュア署名作成デバイス(SSCD)に対するサポートを意味する。

すべての通信は[SOAP(今後REST対応)]プロトコル:
使用するサービスコールとして実装される。サービスは[WSDL]言語で記述される。

クロスボーダー・サービス:
組織は、JP-LINKの別のインスタンスに属する組織が提供するサービスを呼び出すことが可能である。

セキュリティ・プロトコルのカプセル化:
セキュリティ対策とセキュリティ・プロトコルは標準のコンポーネントにカプセル化されている。組織は、データ交換のためにセキュリティ関連の機能を実装する必要がない。

標準化:
JP-LINKは、組織の間の通信プロトコルを標準化することを目指す。これにより、組織は、追加のプロトコルを実装することなくさまざまなサービス・プロバイダに接続することができる。JP-LINKコアはプロトコル変換、データ変換を行わない。必要に応じて、これらの変換は組織の情報システムによって実行される。

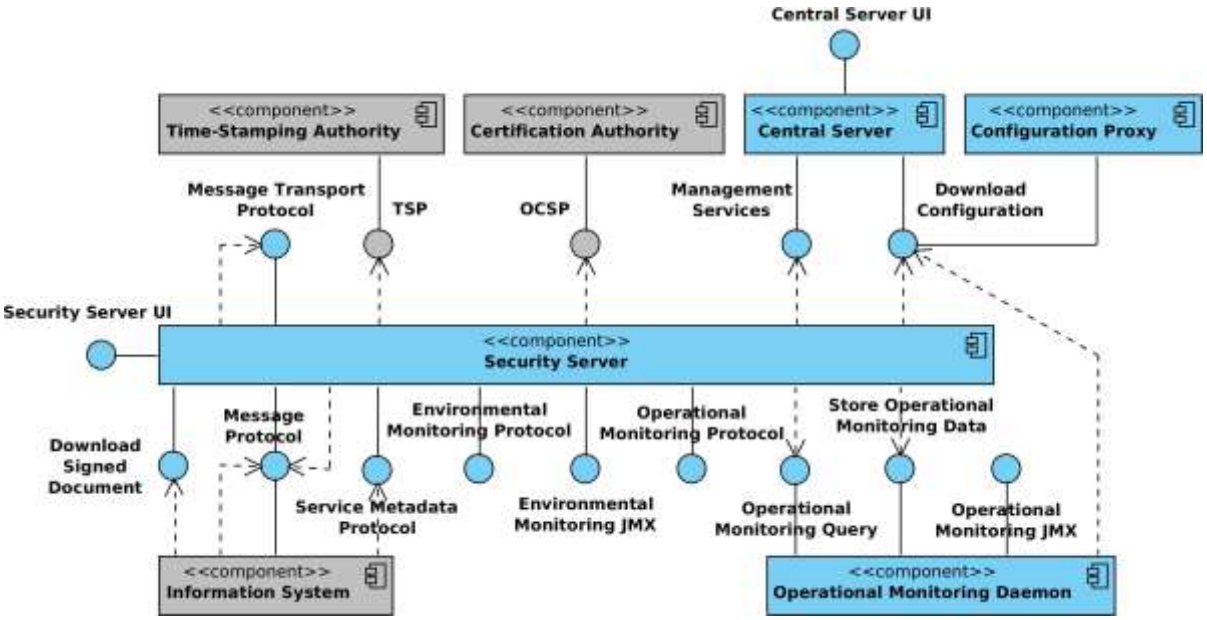
既定の役割なし:
組織がJP-LINKインフラストラクチャに参加すると、追加の登録作業なく、サービス・クライアントとサービス・プロバイダの両方として行動できる。

二つの認証レベル:
JP-LINKコアは、組織レベルでの認証とアクセス制御を処理する。エンドユーザ認証は、サービス・クライアントの情報システムによって実行される。

2 システム・コンポーネント

図1は、JP-LINKの主要なコンポーネントとインターフェイスを提示する。 JP-LINKコアの一部ではないコンポーネントは、灰色の背景で表示する。 コンポーネントとインターフェイスについて、以降のセクションで詳しく説明する。

図1 JP-LINK論理構成図



2.1 センター・サーバ

センター・サーバ(詳細については別ドキュメントを参照)は、JP-LINKメンバーとセキュリティ・サーバのデータベースを管理する。さらに、センター・サーバにはJP-LINKインスタンスのセキュリティ・ポリシーが含まれている。セキュリティ・ポリシーは、次の項目からなる。

- 信頼できる証明局のリスト
- 信頼できるタイムスタンプ局のリスト
- OCSP応答の最大許容期間などの調整可能なパラメータ

メンバー・データベースとセキュリティ・ポリシーは、HTTPプロトコル(3.2セクションを参照)を介してセキュリティ・サーバで利用可能になる。この分散されたデータ・セットが、グローバル・コンフィギュレーションを形成する。

コンフィギュレーション(グローバルコンフィグレーションファイル:GCF)の配布に加えて、センター・サーバは、セキュリティ・サーバ・クライアントの追加や削除などの管理タスクを呼び出すためのインターフェイスを提供する。これらのタスクは、セキュリティ・サーバのユーザー・インターフェイスから呼び出される。管理サービスは標準のJP-LINKサービスとして実装され、センター・セキュリティ・サーバを通じて提供される。詳細については、セクション3.6を参照。

2.2 セキュリティ・サーバ

セキュリティ・サーバ(詳細については別ドキュメントを参照)は、情報システムの間のサービスコールとサービス応答を仲介する。セキュリティ・サーバは次のJP-LINKのセキュリティ面のインフラをカプセル化する。署名および認証のためのキーの管理、セキュアなチャネルを介したメッセージの送信、デジタル署名付きのメッセージのために証明の作成、タイムスタンプ(セクション3.8を参照)とロギングなど。サービス・クライアントとサービス・プロバイダ情報システムに対して、セキュリティ・サーバはSOAPに基づくプロトコルを提供する(セクション3.1を参照)。このプロトコルは、クライアントとサービス・プロバイダ共通であり、セキュリティ・サーバをアプリケーションに対して透過的にする。

一台のセキュリティ・サーバは複数の組織をホストすることができる(マルチテナント)。セキュリティ・サーバを管理する組織はサーバの所有者であり、ホストされる組織はセキュリティ・サーバのクライアントである。

セキュリティ・サーバは、2種類のキーを管理する。認証用の証明書は、セキュリティ・サーバに割り当てられ、他のセキュリティ・サーバ(セクション3.3を参照)との暗号化されたセキュアな通信チャネルを作成するために使用される。署名用の証明書は、セキュリティ・サーバのクライアントに割り当てられ、交換されたメッセージに署名するために使用される。キーは、ディスク(ソフトウェアトークン)またはSSCD？のいずれかに格納できる。

セキュリティ・サーバは最新のグローバル・コンフィギュレーションと証明書有効性情報をダウンロードしてキャッシュする(セクション3.7を参照)。キャッシングは、ダウンロード元が利用できない場合でもセキュリティ・サーバの動作を可能にする。

セキュリティ・サーバには、実行中のプロセス、使用可能なディスク容量、インストール済パッケージなどの環境情報を監視するモニタリング・コンポーネントが含まれている。モニタリング・コンポーネントは、環境モニタリング・サービス(セクション3.11)およびモニタリングJMXインターフェイス(セクション3.12)、を介してこのデータを発信する。

2.3 情報システム

情報システム(IS)は、JP-LINKを介してサービスを使用および/または提供する。

サービス・クライアントISの場合、セキュリティ・サーバはすべてのJP-LINKサービス(セクション3.1を参照)のエントリーポイントとして機能する。クライアントISは、特定のJP-LINKインスタンスの要件に準拠したユーザー認証およびアクセス・コントロール・メカニズムを実装する。エンドユーザの身元は、SOAPメッセージに含まれてサービス・プロバイダに通知される。クライアントは、JP-LINKメタデータプロトコル(セクション3.4を参照)を利用して、JP-LINKメンバーおよび利用可能なサービスを発見できる。

サービス・プロバイダ情報システムはSOAPサービスを実装し、JP-LINKで利用可能にする。このためには、サービスはJP-LINKメッセージ・プロトコル(セクション3.1を参照)に従わなければならない。サービスは、WSDL言語で実装されたサービス記述を含まれなければならない。

2.4 タイムスタンプ局

タイムスタンプ局は、特定の時点におけるデータの存在を証明するタイムスタンプを発行する。タイムスタンプ局はセクション3.8で記述されたタイムスタンプ・プロトコルを実装しなければならない。

JP-LINKはバッチのタイムスタンプを使用する。これにより、タイムスタンプ・サービスの負荷を軽減する。負荷はJP-LINKを介して交換されるメッセージの数には依存せず、システム内のセキュリティ・サーバの数に依存する。

2.5 認証局

認証局(CA)は、セキュリティ・サーバ(認証用証明書)とJP-LINKメンバー組織(署名用証明書)に証明書を発行する。すべての証明書はセキュリティ・サーバに格納される。CAは、[PKCS10]に従った証明書署名リクエストを処理しなければならない。

CAは、証明書有効性情報をOCSPプロトコル(セクション3.7を参照)を介して配布しなければならない。セキュリティ・サーバはOCSP応答をキャッシュすることによってOCSPサービスの負荷を軽減し、可用性を向上させる。 OCSPサービスの負荷は、発行された証明書の数に依存する。

2.6 コンフィギュレーション・プロキシ

コンフィギュレーション・プロキシは、コンフィギュレーション配布プロトコルのクライアント部分とサーバ部分の両方を実装する(セクション3.2参照)。コンフィギュレーション・プロキシはコンフィギュレーションをダウンロードして保管し、ダウンロード可能にする。したがって、コンフィギュレーション・プロキシを利用して、追加のコンフィギュレーション・ソースを作成し、センター・サーバの負荷を軽減することにより、システムの可用性を向上させることができる。

2.7 運用モニタリング・デーモン

運用モニタリング・デーモンの主な機能は、JP-LINKセキュリティ・サーバの運用データを収集し保存することである。また対応するインターフェイスを介して外部のモニタリング・システムに利用可能にする。

3 プロトコルとインターフェイス

3.1 JP-LINKメッセージ・プロトコル

JP-LINKメッセージ・プロトコルは、JP-LINKセキュリティ・サーバと通信するために、サービス・クライアントおよびサービス・プロバイダの情報システムによって使用される。

プロトコルは、クライアントISまたはサービス・プロバイダのセキュリティ・サーバによって開始される同期RPCプロトコルである。

JP-LINKメッセージプロトコルは、HTTP(S)上のSOAP　であり、サービス・クライアントと呼び出されたサービスを識別するために、追加ヘッダー・フィールドを追加する。

このプロトコルはメッセージ転送プロトコルと共に、JP-LINKデータ交換のコアをなす。関係するコンポーネントが利用できない場合、データ交換は不可能になる。JP-LINKアーキテクチャは、冗長性により関連するコンポーネントの可用性を向上させる。

3.2 コンフィギュレーション・ダウンロード・プロトコル

コンフィギュレーション・クライアントは、生成されたグローバル・コンフィギュレーション・ファイルをセンター・サーバからダウンロードする。

コンフィギュレーション・ダウンロード・プロトコルは、センター・サーバによって提供される同期プロトコルである。セキュリティ・サーバやコンフィギュレーション・プロキシなどのコンフィギュレーション・クライアントによって使用される。

プロトコルはHTTPとMIMEマルチパート・メッセージに基づいている。コンフィギュレーションは、変更から保護するためにセンター・サーバによって署名される。通常、コンフィギュレーションはいくつかの部分からなる。このプロトコルにより、コンフィギュレーション・クライアントはコンフィギュレーションが変更されたかどうかを確認し、変更された部分のみをダウンロードすることができる。

JP-LINKセキュリティ・サーバ(および運用モニタリング・デーモン)は、それぞれのコンフィギュレーション・ソースから定期的に更新されるグローバル・コンフィギュレーションのローカルコピーを保持する。このキャッシュされたグローバル・コンフィギュレーションの有効期間は、コンフィギュレーション・クライアントがローカルコピーを更新するように設定されている期間よりも長くなっている。セキュリティ・サーバはキャッシュされたグローバル・コンフィギュレーションの有効期間中、動作可能である。ただし、有効期限切れのグローバル・コンフィギュレーションは、セキュリティ・サーバ管理者の管理機能を厳しく制限し、セキュリティ・サーバが受信リクエストを処理することを禁止する。したがって、設定されたコンフィギュレーションの有効期間内に、インターフェイスの短い停止時間は許容される。

3.3 メッセージ転送プロトコル

JP-LINKメッセージ転送プロトコルは、セキュリティ・サーバによってサービス・リクエストとサービスレスポンスを交換するために使用される。プロトコルは、サービス・クライアントのセキュリティ・サーバによって開始される同期RPCプロトコルである。

プロトコルはHTTPSに基づき、相互のTLS認証を使用する。クライアントおよびサービス・プロバイダISから受信されたSOAPメッセージは、署名やOCSP応答などの追加のセキュリティ関連データと共にMIMEマルチパート・メッセージにラップされている。

このプロトコルはJP-LINKメッセージ・プロトコルと共に、JP-LINKデータ交換のコアをなす。関係するコンポーネントが利用できない場合、データ交換は不可能になる。JP-LINKアーキテクチャは、冗長性により、関連するコンポーネントの可用性を向上させる。

3.4 サービス・メタデータ・プロトコル

JP-LINKサービス・メタデータ・プロトコルは、サービス・クライアント情報システムによって使用され、JP-LINKインスタンスに関する情報を収集することができる。特に、プロトコルを使用して、JP-LINKメンバー、これらのメンバーによって提供されるサービス、およびWSDLサービスの説明を発見することができる。

このプロトコルは、サービス・クライアントISによって開始される同期RPCプロトコルである。

情報サービスの中には、クライアントISの実装を単純化するためのHTTP(S)GETリクエストとして実装されるものがある。他の情報サービスは、標準なJP-LINKサービスと呼ばれている(セクション3.1を参照)。

サービス・メタデータ・プロトコルはクライアントISコンフィギュレーションの場合に使用される。そのため、そのスループットおよび遅延の実装コンポーネントの可用性はJP-LINKの動作にとって致命的ではない。

3.5 署名付きドキュメントのダウンロード

情報システムは、署名付きドキュメントダウンロードサービスを、セキュリティ・システムのメッセージ・ログから署名されたコンテナをダウンロードするために　　利用できる。さらに、このサービスは、署名されたコンテナを検証するために利用できるグローバル・コンフィギュレーションをダウンロードするために便利な方法を提供する。

プロトコルは、ISによって開始される同期RPCプロトコルである。 サービスはHTTP(S)GETリクエストとして実装される。

署名付きドキュメントダウンロードプロトコルは、セキュリティ・サーバに格納されたデータをダウンロードするためにISによって使用される。そのため、そのスループットおよび遅延の実装コンポーネントの可用性はJP-LINKの運用にとって致命的ではない。

3.6 マネージメント・サービス・プロトコル

マネージメント・サービスは、セキュリティ・サーバによって呼び出され、セキュリティ・サーバ・クライアントの登録や認証証明書の削除などの管理タスクを実行する。

管理サービス・プロトコルは、センター・サーバによって提供される同期RPCプロトコルです。サービスはセキュリティ・サーバによって呼び出される。

マネージメント・サービスは、JP-LINKインスタンスを管理する組織が提供する標準なJP-LINKサービス(詳細についてはセクション3.1を参照)として実装されている。例外的には、技術的理由からセンター・サーバによって直接実装される認証用証明書登録サービスである。

一般に、マネージメント・サービスはJP-LINKの運用にとって致命的ではない。従って、その可用性は最優先事項ではない。管理サービスが利用できない場合、セキュリティ・サーバはクライアントと認証用証明書を管理できない。クライアントや証明書を削除するなどのいくつかの操作はマネージメント・サービスを使用せずに、センター・サーバ管理者が手動で行うことができる。マネージメント・サービス操作は緊急を要するサービスではない(セキュリティ・サーバ・ユーザーは明示的に管理リクエストを送信することを選択し、ユーザー・インターフェイスはこの操作が瞬間的であることを暗示しない)。

3.7 OCSPプロトコル

OCSPプロトコル([OCSP]を参照)は、署名用と認証用証明書に関する有効性情報を確認するためにセキュリティ・サーバによって使用される。OCSPプロトコルは、認証局に属するOCSPレスポンダによって提供される同期プロトコルである。

JP-LINKでは、各セキュリティ・サーバは、その証明書に関する有効性情報をダウンロードしてキャッシュする。OCSP応答は、メッセージ転送プロトコルの一部として他のセキュリティ・サーバに送信される(3.3を参照)。これにより、セキュリティ・サーバは、相手が使用するOCSPサービスを発見する必要がなくなる。さらに、この構成は、OCSPサービスへのアクセスが証明書の所有者に制限されているか、料金が課せられているかなどの状況をサポートする。

セキュリティ・サーバは、OCSPリクエストにナンスフィールドを含むことはない。これにより、OCSPサービスは、OCSP応答の事前作成などのさまざまな最適化戦略を採用できる。

OCSP応答は証明書検証のプロセスで使用されるため、OCSPサービスの失敗は実質的にJP-LINKメッセージ交換を無効にする。キャッシュされたOCSP応答をリフレッシュできない場合、セキュリティ・サーバは通信できなくなる。したがって、OCSP応答の有効期間は、OCSPサービスが利用できない最大時間を決定する。ライフタイムはセンター・サーバの所有者によって定義され、JP-LINKのさまざまなインスタンスによって異なる場合がある。

3.8 タイムスタンプ・プロトコル

タイムスタンプ・プロトコル([TSP]を参照)は、交換されたメッセージの長期的な証拠とするためにセキュリティ・サーバによって使用される。セキュリティ・サーバは、すべてのメッセージとその署名を記録する。これらの記録には、長期的な証明のために、定期的にタイムスタンプを付けている。

タイムスタンプ・プロトコルは、タイムスタンプ局によって提供される同期プロトコルである。しかしながら、セキュリティ・サーバは非同期方式でタイムスタンプ・プロトコルを使用する。セキュリティ・サーバは、他のセキュリティ・サーバと交換されたすべてのメッセージを記録する。これらのメッセージは、バッチタイムスタンプを使用して、非同期的にタイムスタンプされる。これは、メッセージ交換の可用性をタイムスタンプ局の可用性から切り離し、メッセージ交換の待ち時間を短縮し、タイムスタンプ局の負荷を軽減するために行われる。

タイムスタンプは非同期で使用されるため、タイムスタンプ・サービスが一時的に使用できなくなっても、JP-LINKメッセージ交換には直接影響与えない。しかし、セキュリティ・サーバが蓄積されたメッセージに一定の期間内にタイムスタンプを付けることができない場合、メッセージ交換の正確な時間を証明することが困難になる可能性がある。このリスクを最小限に抑えるために、タイムスタンプがしばらく失敗した場合、セキュリティ・サーバはメッセージの転送を停止する。メッセージの登録とそのメッセージのタイムスタンプの取得との間の最大許容時間は、センター・サーバの所有者によって定義され、JP-LINKのインスタンスによって大きく異なる場合がある。

3.9 セキュリティ・サーバのユーザー・インターフェイス

セキュリティ・サーバ・ユーザー・インターフェイスは、セキュリティ・サーバ管理者がセキュリティ・サーバを構成および管理するために使用する。

3.10 センター・サーバのユーザー・インターフェイス

センター・サーバのユーザー・インターフェイスは、センター・サーバ管理者がセンター・サーバを構成および管理するために使用する。

3.11 運用モニタリング・データの保存

このプロトコルは、JP-LINKセキュリティ・サーバによって、キャッシュされた運用モニタリング・データを運用モニタリング・デーモンのデータベースに格納するために使用される。このプロトコルは、HTTP(S)を介したJSONに基づく同期RPCプロトコルである。

3.12 運用モニタリング・クエリ

運用モニタリング・クエリ・インタフェースは、JP-LINKセキュリティ・サーバによって運用モニタリング・デーモンから運用モニタリング・データを取得するために使用される。非同期RPCスタイルのJP-LINK運用モニタリング・プロトコルが使用される。

3.13 運用モニタリング・プロトコル

このインターフェースは、外部モニタリング・システムによってセキュリティ・サーバの運用情報を取得するために使用される。このプロトコルは、外部モニタリング・システムによって開始される同期RPCプロトコルである。

3.14 運用モニタリングJMX

このインターフェースは、JMXMPを介してセキュリティ・サーバのローカル運用ヘルスデータを収集するために、ローカル・モニタリング・システム(例えば、
Zabbix)によって使用される。

3.15 環境モニタリング・プロトコル

環境モニタリング・インターフェースは、セキュリティ・サーバのサーバ・プロクシ・インターフェースから環境データのモニタリングに関するクエリに応答する。環境モニタリング・データは、環境モニタリング・サービスによって収集される。

3.16 環境モニタリングJMX

環境モニタリングJMXサービスは、JMXインターフェイスを介して環境モニタリング・データを公開する。環境モニタリング・データは、環境モニタリング・サービスによって収集される。

4 テクノロジー・マトリックス

表1は、JP-LINKで使用されているテクノロジーの一覧と、テクノロジとJP-LINKコンポーネントの間のマッピングを提示する。

表1 JP-LINKのシステム対応表

Technology	Security server	Central server	Configuration proxy	Operational Monitoring Daemon
Java 8	✔	✔	✔	✔
C	✔	✔		
Logback	✔	✔	✔	✔
Akka 2.X	✔	✔		✔
Jetty 9	✔	✔		
JRuby 1.7	✔	✔		
Ubuntu 14.04	✔	✔	✔	✔
PostgreSQL 9.3	✔	✔		✔
PostgreSQL 9.4		✔ [1]		
nginx	✔	✔	✔	
PAM	✔	✔		
Liquibase	✔			✔
upstart	✔	✔	✔	✔
PKCS #11[2]	✔	✔	✔	
Dropwizard Metrics	✔			✔

[1] PostgreSQL 9.4 is used in High-Availability installation of JP-LINK Center server.
[2] The use of hardware cryptographic devices requires that a PKCS #11 driver is installed and configured in the system.

5 配置ビュー

図2は、基本的なJP-LINKインスタンスの配置ビューを示す。実際には、すべてのコンポーネントが冗長性を利用して可用性とスループットを向上させることができる。さまざまなコンポーネントのデプロイメントオプションの詳細は、アーキテクチャ・ドキュメントで説明する。

この図には、組織によってインストールされ、ホストされているコンポーネントも表示されている。監督機関は、センター・サーバとセンター・セキュリティ・サーバをインストールして管理する。コンフィギュレーション・プロキシは、通常、連携されたJP-LINKインスタンスにコンフィギュレーションを配布するために使用されるオプショナル・コンポーネントである。サービス・クライアントおよびサービス・プロバイダ組織は、その情報システムと情報システムをJP-LINKに接続するセキュリティ・サーバをホストする。

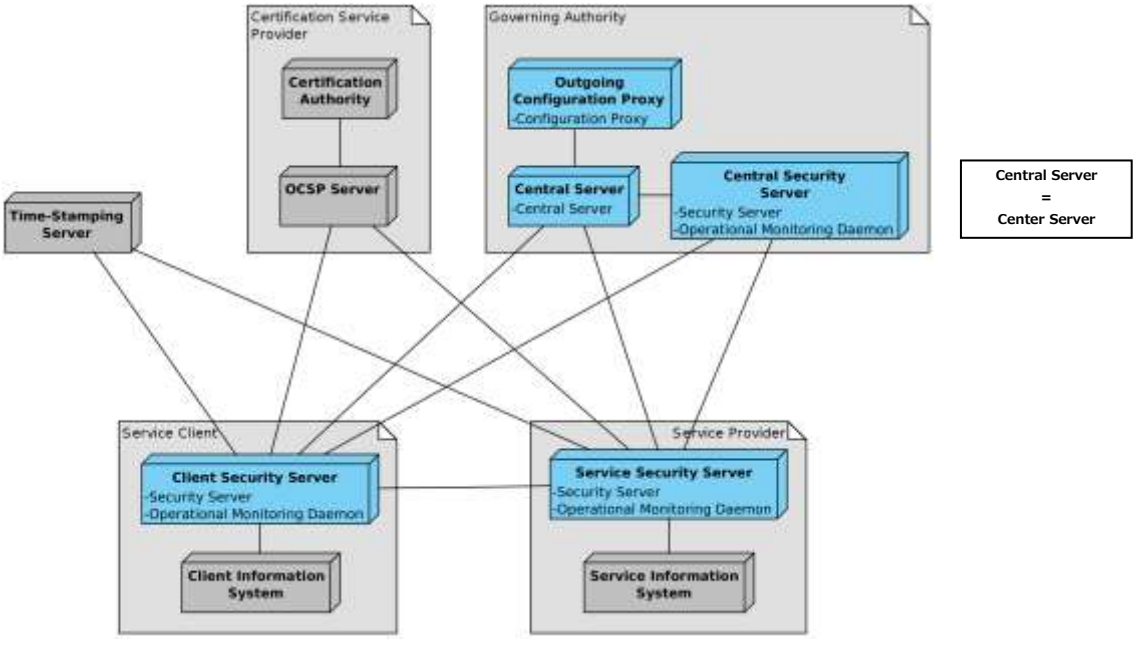


図2 JP-LINKの配置ビュー

用語の定義

EIDAS

EU Regulation No 910/2014 - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

OCSP

X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Internet Engineering Task Force, RFC 6960, 2013.

PKCS10

Certification Request Syntax Standard. RSA Laboratories, PKCS #10.

SOAP

Simple Object Access Protocol (SOAP) 1.1, 2000.

TSP

Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Intenet Engineering Task Force, RFC 3161, 2001.

WSDL

Web Services Description Language (WSDL) 1.1, 2001.