第９章 セキュリティ方式

９．セキュリティ方式

9-1 セキュリティ要件

インターネットを介したシステムにおいては、サーバへの不正侵入防止や機密情報の漏えい防止などのセキュリティ対策を行うことが必要となる。
セキュリティ要件を以下に記す。

- 公開されたデータを照会、更新できる Party は許可与えられた Party であること（アクセス制御対応）
- Data Pool（DP）間、Registry 間通信は、電子署名による認証と併せて、やり取りされる全てのデータに対して暗号化が行なわれていること（データ認証&暗号化対応）
- 不正侵入対策が施されていること
- ウィルス対策が施されていること
- ログ追跡、監査追跡が行なわれていること

これらセキュリティ要件を満たす為の、セキュリティ管理方式を以下に示す。

9-2 セキュリティ管理方式

9-2-1 インターネット上にアクセスする為の基本的なセキュリティ対策

① ファイアーウォールによるアクセス制御
不正アクセスを防止する為、ファイアーウォールにてアクセス制御を行い、通信要件のポートのみアクセスさせる。
ファイアーウォールは、堅牢性を高める為、多段階構成を考慮する。

② サーバ OS 関連セキュリティパッチ対策
サーバ OS 関連の脆弱性対策として、最新のセキュリティパッチを適用する。

③ ウィルス対策
ウィルス対策として、各サーバにウィルスソフトを導入する。

9-2-2アプリケーションにおけるアクセス制御

① ドキュメント単位のアクセス制御

GLN ごとにドキュメント単位でのアクセス制御を、アプリケーションにて行う。

- Data Recipient（DR）として検索を行える商品は、全ユーザーに公開されたパブリック商品もしくは公開先として指定されたプライベート商品のみとする。
- Data Source（DS）として Catalogue Item を登録・参照する際は、ユーザー自身が登録した内容のみを対象とする。

② クライアント認証

Data Pool（DP）～ Data Recipient（DR）、Data Source（DS）接続の際は、クライアント認証を実施する。WEB インタフェースの場合は、WEB サイトにログインする際に、ログイン情報として『会社コード』、『ユーザーID』、『パスワード』の入力を要求し、クライアント認証を行う。

クライアント認証が正常に行えた場合のみ、アクセスを許可する。

9-2-3通信の暗号化

① EDIINT AS2 による通信の暗号化
データ受信時に信頼できる Data Pool（DP）または Local Registry（LR）からのデータ送信であることを認証する。また通信されるデータに対して暗号化を行う。

EDIINT AS2 は、メッセージを暗号化、署名する仕組みを持ち、それは S / MIME 形式で実装されている。いわゆる公開鍵方式の実装方法をとるため、複数の相手との鍵情報の共有も容易になっている。メッセージレベルの暗号化となっているため、ネットワークやサーバ環境への依存性が少ない。

ここではこの公開鍵、および、秘密鍵の方式に関して記述する。

S / MIME の実装では証明書を利用するが、証明書の利用方法は以下のようになる。

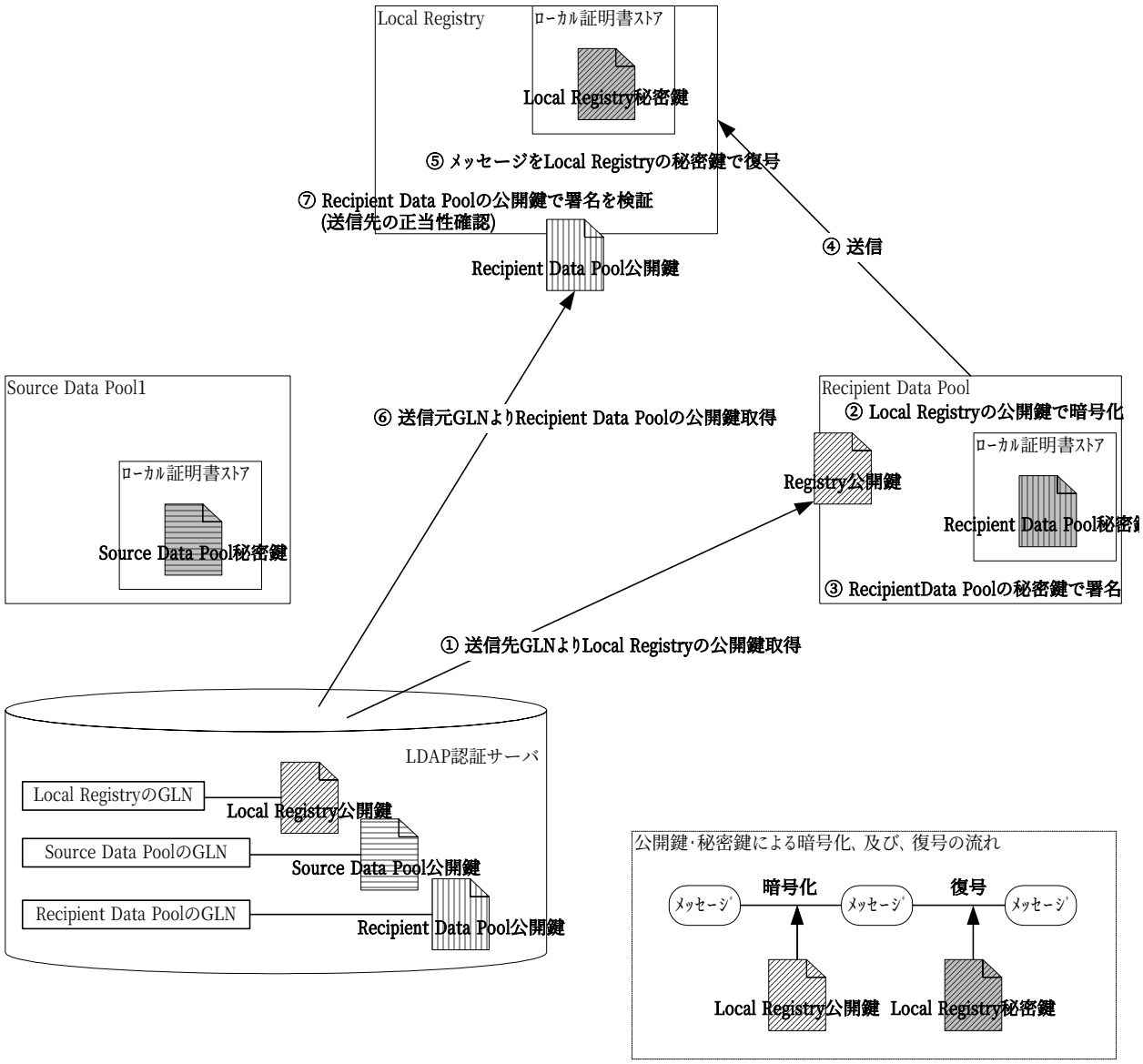
1) 送信側が受信側の公開鍵証明書を利用してメッセージを暗号化する
2) 送信側が自分の秘密鍵証明書を利用してメッセージに署名する
3) 受信者はメッセージから署名した証明書（送信側の公開鍵証明書になる）を抽出する
4) 受信者は自分の秘密鍵証明書を利用してメッセージを復号する
メッセージから抽出した送信者の証明書と公開されている送信者の公開鍵証明書を比較し、一致するかどうかを確認する

S / MIME 実装に必要な秘密鍵は、証明書ストアを利用し、自サーバのローカル鍵ストアに格納する。

公開鍵の管理は、LDAP サーバを使用して管理する。公開鍵を LDAP 認証サーバ上に GLN と対応付けたユーザー情報として登録し、様々なデータプールから検索、取得が可能なようにする。

以下に、公開鍵 / 秘密鍵の処理方式概要を記す。

図表 9-1：公開鍵 / 秘密鍵処理方式概要



② SSL 通信によるの暗号化（WEB インタフェース）

WEB インタフェースの場合､WEB サーバと WEB ブラウザ間の電文は SSL 通信にて暗号化を行う。

認証局より 128 ビットのサーバ証明書を取得し、サーバにセッティングし、通信を行う。

9-2-4ロギング

セキュリティ対策として、監査証跡の為のログ管理が必要となる。今回のシステムでは、各種アクセスログ取得およびアプリケーションでのログ取得を行う。

（1）サーバアクセスログ

監査証跡、不正アクセス時の解析の為、サーバへのアクセス履歴を取得する。

※ サーバログイン履歴ログ、通信ログ、WEB アクセスログなど

（2）GDS（Global Data Synchronisation）メッセージ（受信データ）の更新アクセス履歴

データ改ざん時の解析の為、Catalogue Item データの更新時間や、Catalogue Item、Publication、Subscription に対する追加、更新、削除の際に発生する送受信データを保存・管理する。Party 情報についても同様。

また、バックアップデータとしても取得する。