株式会社レンタブルワンは、個人情報保護法及びその他の関連法規並びに各ガイドラインを遵守し、弊社が業務上使用するお客様の個人情報を保護することが重要な責務であることを認識し、SSL を導入しております。

（下記内容は、弊社認証局グローバルサインの HP からの抜粋です）

●SSL とは

・Secure Socket Layer の略で、米 Netscape 社が開発したインターネット上で情報を暗号化し、送受信できるプロトコルです。 サーバとクライアント PC 間で機密性の高い情報を安全にやり取りできます。

●SSL 利用の特徴

・**SSL** を利用したページでは、URL が「http://」からではなく「https://」から始まります。「s」はセキュリティを意味しています。 また、インターネットエクスプローラを利用した場合、右下又は右上に鍵のマークが表示されます。

●SSL サーバ情報の見方

・**SSL** 利用の際ブラウザに表示される鍵マークをダブルクリック→プロパティの「証明書」をクリック

●SSL サーバ証明とは

・**SSL** サーバ証明書とは WEB サイトの所有者の情報、送信情報の暗号化に必要な鍵、発行者の署名データを持った電子証明書です。 **SSL** サーバ証明書には主に下記二つの役割があります。

1.証明書に表示されたドメイン（サーバ）の所有者であることの証明

2.ブラウザとウェブサーバ間での **SSL** 暗号化通信の実現

●サーバ証明書の信頼性

・データの送信先を信頼するには、証明書自体が信頼できるものでなければなりません。 **SSL** サーバ証明書は知識さえあれば誰でも発行することができます。そこで証明書に信頼性を持たせるために、信頼のできる第三者認証機関から発行された証明書を使用することが必要になります。

●認証局・ルート証明書

・認証局（CA：Certification Authority）とは電子証明書の登録、発行、失効をおこなう第三者認証機関です。

・ルート証明書とは認証局が自分自身に対して発行した大元の証明書のことをいいます。

●証明書の信頼性の確認方法

・代表的なブラウザでは WEBTRUST という厳しい監査基準を満たした認証局のルート証明書をあらかじめ搭載し、ブラウザの利用を通して意識することなく証明書の信頼性を確認できるようにしています。

●信頼性のない証明書を使用した場合

・信頼性のない（ブラウザにルート証明書がプレインストールされていない）証明書では、ブラウザからセキュリティ警告が発せられます。

●公開暗号基盤（PKI）とは

・Public Key Infrastructure の略で、公開鍵と秘密鍵のキーペアからなる公開鍵暗号方式という技術を利用したセキュリティのシステムのことです。秘密鍵で暗号化したものは公開鍵でしか復号化（解読）できず公開鍵で暗号化したものは秘密鍵でしか復号化できません。 **SSL** サーバ証明書もこの仕組みを利用しています。

●公開鍵とは

・公開鍵と秘密鍵の違いは、公開鍵は広く一般に配布することを目的としているのに対し、秘密鍵は所持者が厳重に管理する必要があります。 公開鍵で暗号化したデータは秘密鍵をもった人にしか復号化できないため、広く一般に公開しても秘密鍵を持った人以外に内容が解読されることはありません。

●SSL 通信の流れ

・**SSL** 暗号化通信は、クライアント側が共通鍵を使って暗号化したデータをサーバ側に送りサーバ側は事前にクライアント側から送られた共通鍵を使ってデータを復号化します。公開鍵、秘密鍵はクライアント・サーバ間で事前に共通鍵を安全に授受するために使用されます。

●**電子署名**

・電子証明書を使用した署名のことで、実社会でのサインや印鑑に相当します。信頼できる認証局の審査を経て発行された証明書を用いることで署名者を明らかにすることができます。また、改ざんの検知をおこなうことができます。

2010 年 2 月 15 日

株式会社レンタブルワン