3.4. SSL 証明書

① 本システムと通信する加盟店様システムは、「Security Communication Root CA2」のルート証明書が必要となります。

ポートは 443 を使用致します。

なお、「Security Communication Root CA1」については、署名アルゴリズム SHA-1 の利用停止に伴いご利用できません。

② 本システムがクライアントとなるケース（POST 通信）におきましては、加盟店様は以下 **「表 3.5 対応 SSL 証明書一覧」** に記載の SSL 証明書がご利用可能です。

また、加盟店様システムの SSL 証明書を更新される際は、**必ず事前にテスト環境でご確認ください**。なお、下記に記載のある証明書にて、エラーが発生した際は弊社までお問い合わせください。

表 3.5 対応 SSL 証明書一覧

Verisign	EnTrust	Global Sign
Digi Cert	CERTNM	GTE cybertrust global
GeoTrust	AddTrust	Telesec Global
SECOM	QuoVadis	Sonera
Trust Center	Deutsche Telekom	Sectigo
Thawte	Baltimore	KEYNECTIS
SwissSign	Starfield	AOL
UTN-USERFirst	Cert Plus	Cybertrust
RapidSSL	ACM Certificate	

③ SNI(Server Name Indication)を有効化した状態で本システムより POST 通信を行います。