記載例　（様式１）

年　月　日

一般社団法人全国銀行資金決済ネットワーク　御中

〒XXX-XXXX

会社所在地：東京都千代田区大手町 99-99-99

会社名：　株式会社○○○○○○○○

所属部署・役職：　●●●●部長

氏　名：　全銀　太郎

法人番号：○○○○○○○○○○○○○

担 当 者：　全銀　次郎

電話番号：　03-XXXX-XXXX

メールアドレス：　yyyy@zzzzz.jp

役職は担当部長以上で、氏名も併せてご記入ください。

法人番号は取得している場合のみご記入ください。

全銀 EDI システムクライアント証明書に係る定期報告

全銀 EDI システムクライアント証明書の管理に関して、下記のとおり報告いたします。

記

１．クライアント証明書の管理状況について（該当するものに✓をつける）

☑問題なし（適切に管理を行っている）
☐問題あり（適切な管理がなされていない）

以下の全ての項目を満たす場合に「問題なし」に✓をつけてください。
1. 発行されたクライアント証明書を悪用していないか。
2. 発行されたクライアント証明書を他へ転用していないか。
3. アクセス制御（※）などのセキュリティ対策を実施し、クライアント証明書を適切に管理しているか。
※端末操作者のアクセス制御に係る留意事項については、次ページをご参照ください。
4. 発行されたクライアント証明書の有効期限を把握しているか。

２．上記１で「問題あり」とご記入された理由

３．申込先金融機関名（金融機関が複数の場合は全てご記入）

全銀銀行

（注）(1) 報告対象は、当該年度（4 月～3 月）分となります。
(2) 一般社団法人全国銀行資金決済ネットワーク（以下「全銀ネット」という。）は、必要に応じて、内容についてヒアリングを実施させていただく場合があります。
(3) 全銀ネットは、ご記入いただいた個人情報を「クライアント証明書に関するご連絡」の目的にのみ使用いたします。

以　上

端末操作者のアクセス制御に係る留意事項

企業クライアント（※）は、セキュリティの観点から不特定多数の利用者での運用を防止するために、許可された利用者のみが操作可能なように本人認証を実施して、利用を制限すること。

本人認証はワンタイムパスワード、生体認証などさまざまな実現方式が想定されるが、企業クライアントで定めるセキュリティ要求レベルを満たす方式を採用すること。ただし、以下の（１）から（３）相当のセキュリティレベルは担保すること。なお、これは企業クライアントのソフトウェアに求める認証であり、本システムとの接続に使用するものではない。

（１） ログイン機能

パスワードは入力画面上マスキングされ、ログイン ID とパスワードにより利用者の認証を実施すること。またクラッキング対策として、指定回数以上の入力ミス時は当該ログイン ID をロックし、その旨を利用者に通知すること。

（２） ログイン情報の管理

企業クライアントは、利用者へ払い出すログイン ID、およびパスワードを管理すること。なお、ログイン ID とパスワードは当該ソフトウェア以外アクセス不可能な DB、システム管理者の権限を持つユーザ以外アクセス不可能な領域へのファイル格納、あるいは暗号化ファイルと改ざんチェックなどを用いて管理すること。

（３） パスワードとその変更

企業クライアントは、企業が定めた期間において、企業への注意喚起、ならびに変更が可能であること。なお、パスワードは推測されやすいもの（例えば、6 桁未満のパスワード、単純な文字列、単一属性（英字のみなど））は避けること。

※企業クライアントとは、企業が本システムを利用するにあたり使用するシステムのことをいう。