クレジットカード番号等の漏えい等の事故を防止するための措置に関する書面

1．「クレジットカード・セキュリティガイドライン」（以下「セキュリティガイドライン」という。）の対象となる国際ブランドが付帯したクレジットカードの取り扱いの有無

回答欄 （どちらかに〇を記入）	有　・　無

2．クレジットカード番号等を取り扱っている自社システムの概要図を提出すること。（システムの運用を外部に委託している場合には、委託している部分を明示し、その委託先の名称を記載すること。）

（記載上の注意）

資料上部に「2．概要図」と記載のこと。

3．自社システム（委託しているシステムを含む。）において講じているクレジットカード番号等の漏えい等の事故を防止するための措置の内容及び実施状況を上記2．の概要図を用いて説明すること。（必要に応じこれらを説明する資料を提出すること。）

（記載上の注意）

上記1.のセキュリティガイドラインの対象となるクレジットカード番号等を取り扱っている場合においては、セキュリティガイドラインに掲げられた措置(PCIDSS 準拠)又はそれと同等以上の措置の該当性を説明すること。外的脅威による情報漏洩リスクを極小化する観点から、少なくともインターネットや専用線等で外部に接続しているシステムについては当該措置の実施状況を説明すること。（別紙参照）

なお、準拠に向けた具体的な計画及び取り組み状況についても説明すること。

4．PCIDSS の準拠状況について、下記のいずれかの書面を提出すること。

① PCIDSS 準拠証明書（Attestation of Compliance :AOC）

② PCIDSS 自己問診及び準拠証明書

提出書面	

５．下記のいずれかに応じた措置その他自社で独自に講じている措置がある場合には当該措置の内容を記載するとともに、これを説明する書面を提出すること。ただし、PCIDSSに準拠している場合には、これらについての記載及び書面の提出は特段必要ない。

① 金融機関等コンピューターシステムの安全対策基準・解説書
（公益財団法人金融情報システムセンター（FISC））

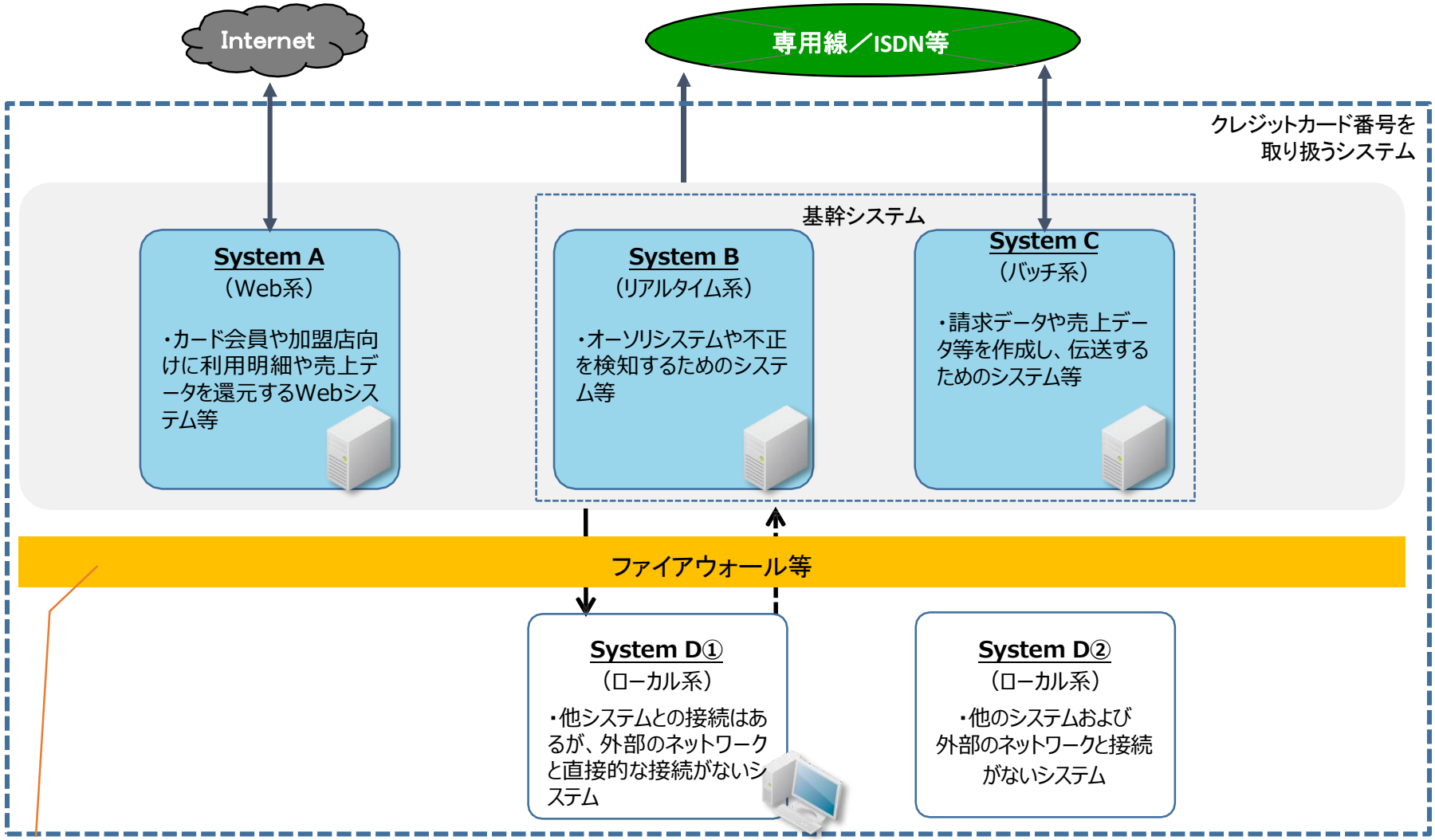
② 情報セキュリティマネジメントシステム（ISMS）適合性評価制度認証基準
（一般財団法人日本情報経済社会推進協会（JIPDEC））

③ 信用分野における個人情報保護に関するガイドライン
（個人情報保護委員会・経済産業省）

措置の内容 （講じているものに☑）	□ ①　□ ②　□ ③ □ その他の措置 （　　）
提出書面	（注）内部監査報告書、外部の専門家による評価報告書がある場合には、これを添付すること。

以上

システム構成例（イメージ）



・ファイアウォール等によりセグメント化され、ローカル系のシステムから外部に接続しているシステム（System A~C）への接続は、限定された宛先、通信のみを許可する設定となっている。

：外的脅威による情報漏洩リスクを極小化する観点から、セキュリティガイドラインに掲げられた措置（PCIDSS準拠）又はそれと同等以上の措置が求められる範囲