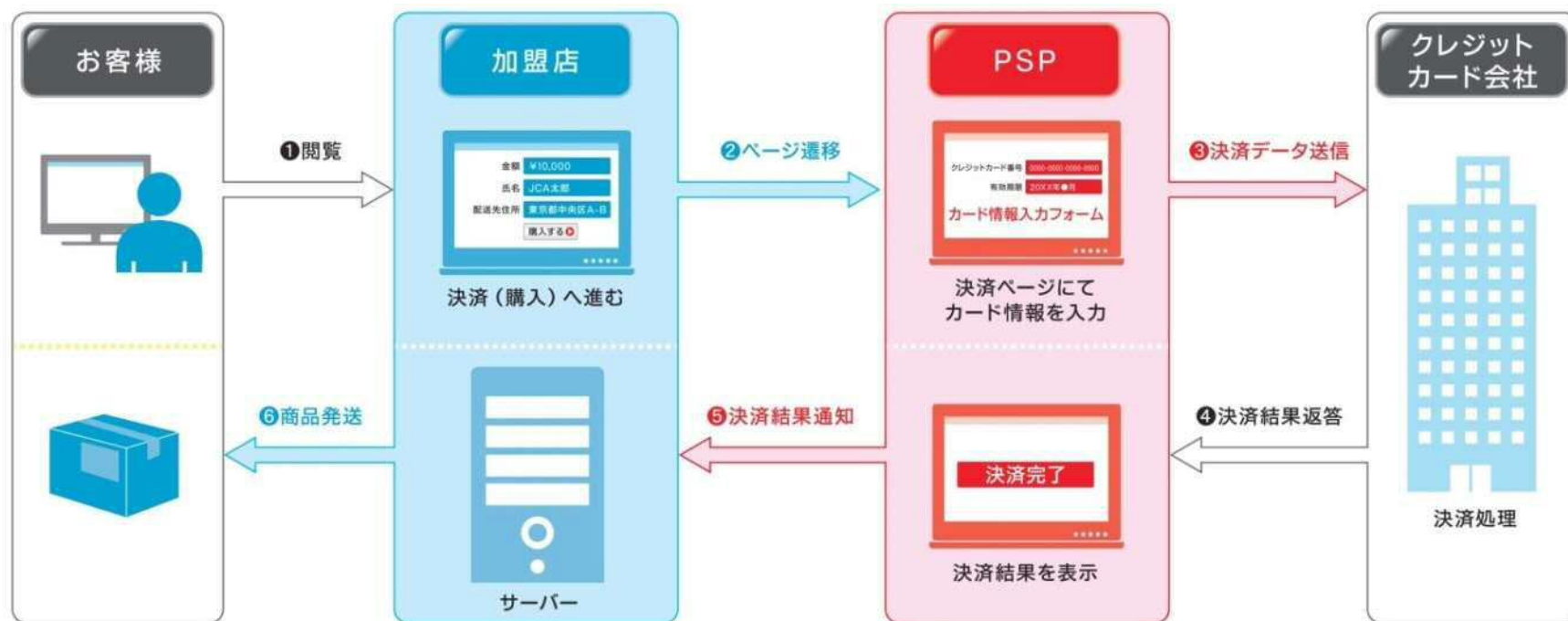


(1) リンク型導入のEC通販からの漏えいイメージ



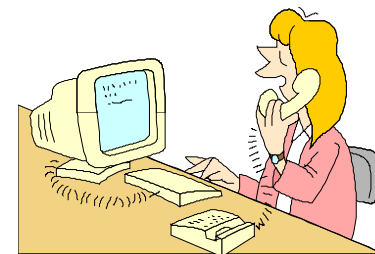
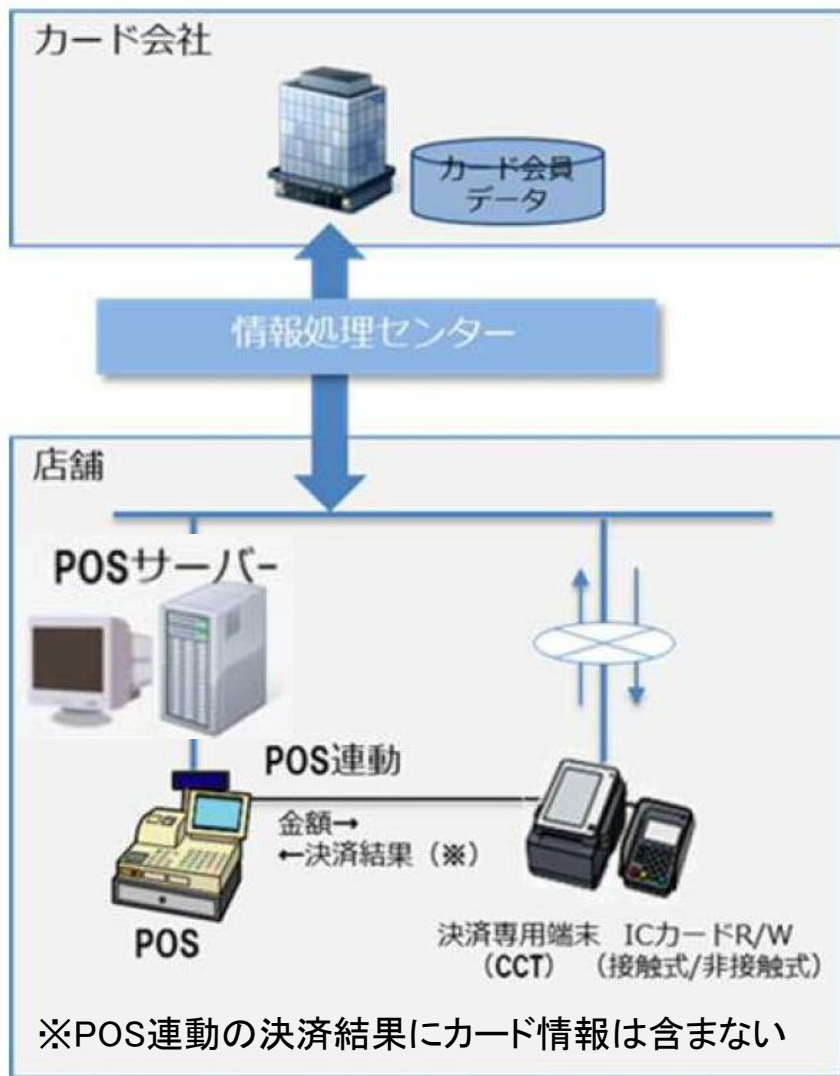
出典:クレジットカード・セキュリティガイドライン【3.0版】のP20より

(1) リンク型導入のEC通販からの漏えいイメージ



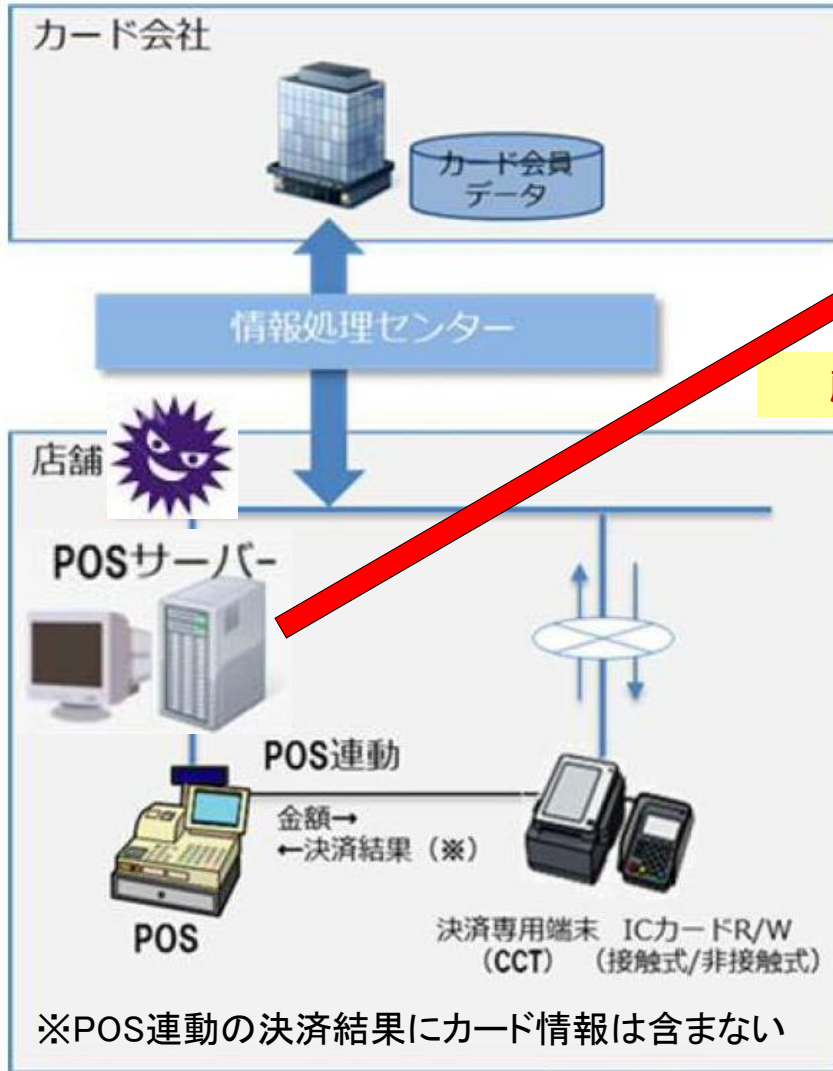
出典:クレジットカード・セキュリティガイドライン【3.0版】のP20より

(2) 非保持化した対面加盟店からの漏えいイメージ



出典:クレジットカード・セキュリティガイドライン【3.0版】のP26より

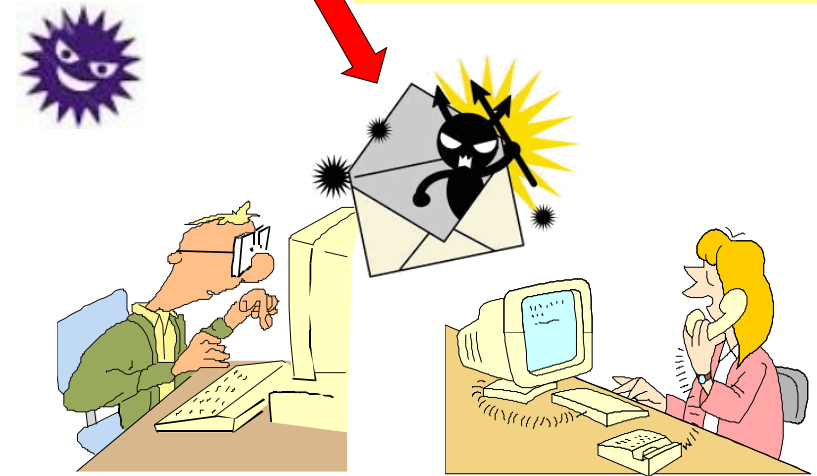
(2) 非保持化した対面加盟店からの漏えいイメージ



フィッシングメールを顧客へ送り、カード情報を入力させて窃取する。

- ・アカウントが凍結されました
- ・お取引情報確認のお願い
- ・異常なアクセスが検出されました
- ・超お買い得セールのご案内

顧客名簿を窃取



EC通販事業者に対しても
同様の手口が考えられる。

出典: クレジットカード・セキュリティガイドライン【3.0版】のP26より

【加盟店に求められる対策】

(P16) 加盟店、特に非対面加盟店ではカード情報の窃取を企図する者の最新の攻撃手口等の情報を踏まえ、**対策実施後も不断に**自社のセキュリティ対策の改善・強化を図る。

【EC 加盟店の対策】

(P19) 非保持化を実現した加盟店であっても、

- ・継続的な情報保護に関する**従業員教育**(標的型メール対策など)や
- ・**脆弱性対策**
- ・**ウイルス対策**
- ・**管理者権限の管理**
- ・**デバイス管理等の基本的なセキュリティ対策**が求められる。



【加盟店側の現状】

- ・カード決済はPCI DSS準拠のPSPと契約した。
 - ・決済端末機はレジを通さず直接にPSPへ送信。
 - ・当社でカード情報を持たず、非保持化は達成した。
- これで割販法はクリアした。



基本的なセキュリティ対策が不足