愚かさに対して、神々自身は無駄に争います。  
–箴言26:11  
世界中の人々がカードや電話での支払いを支持して現金を放棄しているため、キャッシュレス決済業界はコロナウイルスの流行の勝者の1つです。  
株式取引から取引決済までのすべてに特化したネットワークがあり、その多くは他の企業にも開放されています。  
このようなシステムは、いくつかの理由でセキュリティエンジニアにとって重要です。  
詐欺のより広い問題に取り組むためにトランザクション処理を理解する必要があります、そしてこの章はあなたにロードマップを与えます。  
CFOの信頼性を確保するには、Gramm-Leach-Bliley、Sarbanes-Oxley、PCI DSSについての会話ができる必要があります。  
第二に、簿記はコンピュータ産業を動かしました。  
バンキングは急速にコンピューティングの最も集中的なアプリケーション領域になり、1960年代から簿記の自動化によって他の企業にも広まりました。  
また、機密性がほとんど役割を果たさないが、レコードの整合性（および一度作成された不変性）が保護される、よく理解された保護モデルも提供します。  
銀行システムは、顧客がお互いを騙したり、銀行を騙したりすることを防ぎます。銀行の職員が銀行やその顧客をだますことを防ぐべきです。そして、それが提供する証拠は、他人が不正行為をしていると誤って非難することで逃れることができないほど十分に良いはずです。  
第3に、50ドルのATMの引き出しであれ、1億ドルの電信送金であれ、トランザクション処理システムは、軍の外で別の分野として商用暗号を開始したアプリケーションでした。  
多くの有益な間違いが最初に行われた（または少なくとも公に文書化された）  
最後に、今世紀に構築したグローバル規模のシステムの多くは、何世紀にもわたってローカルシステムと手動システムで置き換えられたチェックとバランスを回避するように設計されました。  
Uberは、世界中の何千もの町や都市でのタクシー規制を回避することにより、グローバルタクシー会社になることを計画していました。  
この章では、最初に、資産の追跡と破損したスタッフのリスクの管理に使用される簿記システムについて説明します。このような会計システムは、他のあらゆる規模の企業でも使用されています。  
次に、銀行の公の顔であるATMシステムについて説明します。ATMシステムの技術は、ユーティリティメーターなどのアプリケーションにも採用されています。  
次に、非接触型決済、電話決済、オープンバンキングなど、最近の技術進歩に移ります。  
12.2簿記システム  
人々が余剰食糧を生産し始めたとき、彼らはそれを貯蔵し、交換し始めました。  
まず、食品の各単位（羊、小麦、油、...  
 粘土のトークン、またはブラで表現されました。これは粘土の封筒の中に置かれ、倉庫のキーパーのパターンでそれを回転させることによって密封され、次に窯で焼かれました。  
（これは最も古い既知のセキュリティプロトコルである可能性があります。）  
ほぼ同時に、金属インゴットが中間商品として使用されるようになり、しばしば検査員によってブラ内部に封じ込められました。  
ペリクレスのアテネによって、多くの裕福な個人が銀行家として働いていた[772]。  
紀元前3300年（提供：Denise Schmandt-Besserat and Louvre Museum）  
暗黒時代が近づき、貿易が成長し始めると、一部の企業は単一家族が管理するには大きすぎました。  
しかし、会社がオーナーの家族が直接監督する能力を超えて成長するには、経営者を外部から雇わなければなりませんでした。  
歴史家は、12世紀のカイロ[1691]でユダヤ人の商人によって作成された複式の記録を発見しましたが、この主題に関する最初の本は1494年まで表示されませんでした[522]。  
12.2.1複式簿記  
たとえば、企業が顧客に100ドル相当の商品をクレジットで販売する場合、100ドルのクレジットをSalesアカウントに転記し、100ドルの借方をReceivablesアカウントに転記します。  
、および現金勘定から借方記入します。  
 結局のところ、本はバランスがとれている、つまり合計がゼロになるはずです。資産と負債は等しくなければなりません。  
各ブランチのバランスを個別に調整できるように配置します。  
そのため、ほとんどの詐欺では2人以上の共謀が必要であり、この責任分割の原則は、デュアルコントロールまたはマルチパーティ認証（MPA）とも呼ばれます。本は年末に監査されるだけでなく、ランダムな監査もあります。検査官は、通知なしに支店に降りて、スタッフが家に帰る前にすべての本のバランスが取れていると主張することができます。  
リッティは、従業員が彼からお金を盗んだサロン所有者でした。  
National Cash Register Companyを設立したPattersonは、銀行および簿記機器の主要なサプライヤーになっただけでなく、1990年代にMicrosoftが追い出されるまでコンピューター業界を支配していたIBMをスピンオフしました。  
12.2.2銀行での簿記  
1950年代後半から1960年代前半に小切手処理などのアプリケーションを始めて、当時の低速で高価なコンピュータでさえ、店員の軍隊よりはるかに安価であることがわかりました。  
ATMは1970年代に一斉に到着し、1980年代に最初のオンラインバンキングシステムが登場しました。 1990年代には、ウェブベースのバンキングが続いた。  
米国、ヨーロッパ、およびほとんどの先進国の法律では、銀行だけでなくすべての公開会社に効果的な内部統制を持たせ、幹部に責任を持たせることが義務付けられています。  
簿記に使用されるコンピューターシステムは、通常、複式エントリーテーマのバリエーションを実装すると主張していますが、品質はさまざまです。  
たとえば、元帳がすべて1つの単一データベースのビューにすぎない場合、物理的なアクセス権とデータベース編集ツールを持つ誰かがコントロールをバイパスする可能性があります。  
たとえば、ある銀行は住所変更を監査しませんでした。レジ係が顧客の住所を変更し、追加の銀行カードを発行し、再度変更できることがわかるまで[54]。  
従来のコアバンキングシステムにはいくつかのデータ構造があります。アカウントマスターファイルには、各顧客の現在の残高と、おそらく90日間の前のトランザクションが含まれています。システムを通過する途中で現金やその他の資産を追跡する多数の元帳。現金自動預け払い機、窓口、販売店の端末などから受信されたが、まだ元帳に投稿されていないさまざまなトランザクションのジャーナル。誰がいつ何をしたかを記録する監査証跡。  
コアバンキングソフトウェアは、ジャーナルからのトランザクションをさまざまな元帳とアカウントマスターファイルに適用します。  
これは伝統的にバッチ処理で夜通し行われていましたが、リアルタイムのオンライン処理がますます必要になるため、事態はより迅速に失敗する可能性があります。  
銀行（またはその支店）の場合  
そのため、自分のアカウント残高に追加したいプログラマは、アカウントマスターファイルを微調整して空から作成するのではなく、他のアカウントからお金を取得する必要があります。  
さらに、すべてのコードは、内部監査員による精査と、別のテスト部門によるテストの対象となります。  
（それを書いた開発者とは異なるチームが本番システムを実行するという原則は、DevOpsの新しい世界で緊張にさらされています。）  
12.2.3クラーク・ウィルソンセキュリティポリシーモデル  
 [436]。  
より正式には、データを入力できる特別な手順があります。これは、制約のないデータアイテム（UDI）から制約されたデータアイテム（CDI）に変換されます。整合性検証手順（IVP）  
;および変換手順（TP）  
一般的なケースでは、CDIの整合性を維持します。  
 トランザクションが再構築されます。  
、非常に構造化されているため、マルチパーティの承認ポリシーが適用されます。  
システムには、CDIの整合性を検証するためのIVPがあります。 1今日のほとんどのリテールバンキングトランザクションは、電話からの残高照会であり、通常、コアシステムから定期的な更新を取得するフロントエンドによって処理されます。  
2。  
CDIはTPによってのみ変更できます。 4。  
トリプルは、サブジェクトに適切な職務分離ポリシーを適用する必要があります。 6。  
TPを適用するたびに、TPを再構築して特別な追加専用のCDIに書き込むのに十分な情報が必要です。 8。  
システムは特別な主題（つまり、セキュリティ担当者）のみを許可する必要があります  
多くの事柄が言われています。  
監査証跡に加えて、これは通常、デュアルコントロールの場合に必要です。1人のマネージャーだけが承認し、1秒後にサインオフを待つなど、部分的に承認されたトランザクションを追跡する必要があるためです。これは、状態遷移がバランスなどの不変条件を保持する必要があるという考えを捉えていますが、状態遷移は正しいはずではありません。  
第三に、難しい質問が残っています。つまり、不正なスタッフからのリスクをどのように制御するのでしょうか。  
実際、内部統制の設計方法に関する体系的な議論を会計文献で見つけることは困難です。  
これらのリストは、インシデント、恐れ、規制要件に対応して着実に長くなります。  
セクション3.4.4.3で、1990年代に大手4人の監査人がNISTのアドバイスをどのように取得して、人々に毎月パスワードを変更させるかについて話しました。執筆時点（2020）  
しかし、NISTは証拠に直面して数年前にその勧告を撤回し、英国のGCHQはパスワードのエージングに対して企業にも助言しています。  
次のセクションでは、銀行とコンサルタント業、そして最近では大学のガバナンスで炭鉱で働いたときに得た経験を抽出しようとしています。  
12.2.4内部統制の設計  
米国には、スポンサー組織委員会（COSO）があります。  
しかし、自己規制はドットコム時代の過剰を止めることができず、エンロンの崩壊後、サーベンスオクスリー法（SOX）の形で米国議員からの介入がありました。  
SOXはすべての米国の公開企業を規制し、CEOが証明しなければならない財務報告の正確性と完全性について上級経営者に責任を持たせます。内部者詐欺に関する主な情報源である内部告発者の保護。そしてマネージャーに「財務報告のための適切な内部統制構造と手順」を維持する責任を持たせます。  
SOX法のコンプライアンス費用のほとんどは、内部統制によるものと考えられています。  
 1999年には、多くの点で銀行規制を自由化しましたが、セキュリティと完全性の予測可能な脅威から情報を保護するためのセキュリティメカニズムを銀行に義務付けました。  
これらの規制は、内部統制に関する企業方針に対するビッグフォー会計事務所の影響力を強化するのに役立ちました。  
現代のリスク管理システムでは、通常、企業がそのリスクを特定して評価し、リスクを軽減するための統制を構築する必要があります。  
。  
ISA 315は、エラーによるものであろうと詐欺によるものであろうと、組織のアカウントにおける重大な虚偽表示のリスクに焦点を当てています。  
、各アカウントの重要なアサーション（存在など）  
 これらのプロセスに含まれる制御とともに、それらに影響を与えます。  
では、適切な制御をどのように設計するのでしょうか？  
パート3で説明するように、エラーに対する安全性と攻撃に対するセキュリティを保証するには、2つの基本的なアプローチがあります。  
英国の銀行におけるリスクガバナンスの説明については、セクション12.6.3で説明する、2016年のテスコ銀行詐欺に関する金融行為監督機構のレポート[687]を参照してください。  
監査をサポートする場合、財務諸表が依拠する主張に対するリスクに注意を払う必要があります。  
内部統制がセキュリティ体制のすべてではありません。  
デュアルコントロールでは、2つ以上のプリンシパルが連携してトランザクションを承認します。  
。  
保証は特に詐欺の傾向があります。  
偽造または不正に取得された保証を持つ詐欺師は、銀行Bのローンアカウントを略奪するのに時間がかかる可能性があります。警報は、銀行がデフォルトになり、銀行Bが銀行Aにお金を要求したときにのみ発生します。  
職務の分離により、2人以上のスタッフメンバーが補完的な方法でトランザクションに対応します。  
ラインマネージャーが購入を決定し、購入部門に伝えます。そこで店員が注文書を出します。店員は商品の到着を記録します。請求書がアカウントに到着します。会計担当者は、注文書と店舗のレシートを関連付け、小切手を発行します。アカウントマネージャーは小切手に署名します。  
ラインマネージャーは、その内部アカウントの毎月の明細書から借方を取得し、上司がアカウントをレビューして、部門の利益目標が達成される可能性が高いことを確認します。内部監査部門は、いつでも降下して部門の帳簿を監査できます。外部監査人が年に1度来たときに、無作為に選択された部門のサンプルの帳簿をチェックします。モデルは、防止-検出-回復として要約できます。  
検出が遅れる可能性があり、したがって、破損した銀行保証のように、回復が困難になる可能性がある場合は、おそらく二重制御を使用して、予防にさらに努力します。  
ここでの典型的な例は、銀行のレジ係が簡単に現金を受け取ることができるので、家に帰る前に毎日お金を数えます。  
4最近の問題は、2人のマネージャーが共謀したり、1人が他のマネージャーになりすましたりするだけでなく、マルウェアが両方のアカウントを乗っ取ってしまうのではないかということです。  
コントロールは、役割が既存のビジネスプロセスの補完的な部分であり、いくつかのプロセスがそれらをサポートするために何世紀にもわたって進化した場合に最適に機能します。  
スイスの銀行では、ほとんどすべてに2人のマネージャーの署名がありますが、アメリカ人ははるかにリラックスしています。  
これは大学では受け入れられませんが、学界では盗むことがはるかに少なくなります。  
財務管理者、人事部門、弁護士、監査人、システムの人々はすべて、さまざまな方向から問題に立ち向かい、部分的な解決策を提供し、互いの管理目​​標を理解できず、物事は真ん中の穴に落ちます。  
コントロールを文化に適合させ、人々がそれらを使用するように動機づけることが重要です。より良い経営の銀行は、職員を脅迫や誘拐から保護する手段として経営管理策を販売しています。  
儀式となる統制は、その目的が忘れられた、または無関係になった後、何年もの間行われる場合があります。  
親しい同僚の信頼が限られている文化は、維持するのが特に困難です（事業部門にまたがる機能管理がより効果的であるもう1つの理由）  
また、大規模なトランザクションを承認するために複数の銀行に要求するのと同じように、ライブシステムで実行するコードを承認するために複数のエンジニアに要求することもできます。  
まず、多くのインターフェースが単一障害点を提供します。  
注意して、監査可能にすることができます5。  
そして、その状態を管理する必要があるので、仕事をするために完全なアクセスを必要とする信頼できるシステム管理者が常にいます。  
少なくとも信頼の場所は、ソースコードのレビューフェーズに移行するにつれて変化する可能性があります。  
ATMシステムは週末にダウンし、ATMチームのオンコールエンジニアが自宅からライブシステムにアクセスしてバグを修正します。  
最後に、あなたのトップエンジニアが監査人よりもはるかに知識が豊富で、本当に望んでいたとしても悪いことをすることは避けられません。  
sysadmin 5昔の銀行システムがIBMオペレーティングシステムMVS上に構築されました。これにより、監査者が監視していたアクティビティを見つけることを除いて、sysadminは何でも実行できるようになります[224]。  
彼らが捕まるのは、1日か2日後にバランシングコントロールがアラームを鳴らしたときであり、お金を送金する銀行のマネーロンダリングコントロールは、彼らが非常に逃げるのを止めます。  
持ち帰りは、ノウハウとアクセスを分離するため、予防-検出-復旧モデルに沿った機能的制御が共有制御よりも重要であることが多いことです。  
また、分離できるノウハウの量には制限があります。  
同じ分析がビジネスプロセス自体にも当てはまります。  
実際の銀行では、信頼しなければならない30人または40人を見つける可能性があります。CEO、チーフディーラー、トップシステム管理者、その他多数です。  
二重管理に関する最後の発言は、組織の境界面で脆弱になるということです。  
一部の組織は、署名にどれだけの信頼を得ているかを競合他社に示すのを嫌がります。  
12.2.5何がうまくいかない  
平均的な会社からの盗難のほとんどは内部関係者によるものであり、自動化によってインシデントがより稀で大きなものになっているようです。  
12.2.5.1インサイダー詐欺  
典型的な違反は、数千ドルの損失を伴う軽微な横領でした。  
年に数百の窓口を失うことは、ビジネスを行うためのコストにすぎませんでした。  
スタッフが顧客の個人情報を販売することは、スタッフが顧客にセキュリティの質問を案内してレコードにアクセスする必要があるため、現在も困難です。注目に値するインサイダーのケースには以下が含まれます。  
彼は、ターゲット企業を発見した2人のスタッフを倒しました。通常、アカウントが100万ポンドを超える中規模企業です。  
これを行う前に、彼は彼らとしてログオンし、5桁の多額の支払いのバッチを設定していました。  
•HSBCの銀行口座にアクセスするためにAT＆Tが使用するパスワードを変更することを知らない人物と共謀したHSBCのパスワード再設定担当者。  
店員は、内部検査に不合格でパスワードのリセットに雇われていた弱者でした。裁判所は憐れみを取り、彼は5年の猶予を免れた[1569]。  
•2010年代に急成長した銀行詐欺の1つには、中規模企業のスピアフィッシングアカウントスタッフと2、3のスタッフアカウントの乗っ取りが含まれています。  
銀行は大規模なトランザクションに特別な注意を払う可能性があるため、会社が気付く前に、4桁の支払いを何度も行うことがゲームです。  
典型的な攻撃では、50万の純益が得られます。  
12.2.6エグゼクティブ詐欺  
Barings Bankの崩壊は良い例です。マネージャーは不正なトレーダーであるNick Leesonを制御できず、見かけ上の取引の利益で獲得したボーナスを貪欲に盲目にしました。  
6Sopのルールのように、被害者の幹部はひどく過失であったため、コールセンターがCovidの大流行の際に自宅からスタッフを働かせることを難しくしています。  
ベアリングの場合、または株式ファンディングとマクスウェルと同様に、加害者でした。  
エコノミストや会計学の教授は、代理店の問題などの問題を分析します。プリンシパルAはエージェントBを雇って資産を管理し、Bのパフォーマンスをどのように監視および評価できるか知りたいと考えています。  
理論的には、内部統制と内部監査部門は、CEOがジュニアスタッフを追跡するために使用するツールですが、外部監査人は、株主がCEOとシニアエグゼクティブを追跡するために使用するツールです。  
この慣行は、1996年から2004年の間に上場した米国企業に対する230件の企業詐欺の調査で、Alexander Dyck、Adair Morse、Luigi Zingalesによって分析されました[596]。  
ほとんどは、他のインセンティブを持つアクターによって検出されました：従業員による19％、業界規制当局による16％、金融アナリストによる14％、およびメディアによる14％。  
サーベンス・オクスリー法以降、義務付けられた俳優のパフォーマンスはわずかに改善されましたが、それでも全体の半分をわずかに超えました。  
これは、何が起こっているのかを実際に知っているのは支配的な要因であることを示唆しています。  
 内部告発者に報酬を与え、プラスの効果をもたらします。  
 私の経験では、社外取締役はCEOと友好的である傾向があり、監査人はCFO8を変更するために彼らの邪魔をしません。  
大手の監査会社は、クライアントの実際のリスクに関係なく、お気に入りのコントロールの独自のリストをプッシュすることにより、情報セキュリティの世界に悪影響を及ぼす。  
純粋な経済的インセンティブとは別に、上司は上級の同僚が無能であるか不正直であるという証拠に対処するのが難しいと感じています。  
作業。  
バリングスの誰も、彼らのスターディーラーであるニックリーソンが詐欺師であるとは考えたくありませんでした。ポップは銀行に行きました。  
  
幹部はまた、何かが彼らの会計システムで体系的に間違っているかもしれないと信じたがらないかもしれません。  
ここで検討する価値のある事例は、英国の郵便局会計システムの失敗です。  
それらを制御するために、郵便局はHorizo​​nと呼ばれる会計システムを構築しました。これには複数のバグがあり、多くのフランチャイズ店に借りていない金額が請求されました。  
最終的に、587人の郵便局長が郵便局を訴え、2019年12月に謝罪と5,800万ポンドを勝ち取りました。  
これは、私の知る限りでは、会計システムが積極的な訴訟で適切なテストを受けた最初で唯一のケースです。  
ちなみに、フランチャイズ店の損失総額は数億ドルに上るようです。彼らはおそらく5800万ポンドの和解のうち1100万ポンドを獲得し、残りは弁護士と訴訟をバンクロールしたヘッジファンドに送られます。  
彼女は最終的に去った。  
  
ほとんどの会計システムの失敗はそれほど目立たないものですが、金融機関や他の企業の経営能力に大きな影響を与える多くの失敗があります。1。  
ソフトウェアエンジニアはこれを技術的負債と呼んでいます。つまり、変更はより遅く、より高価になり、障害からの回復は複雑になる可能性があります[41]。  
たとえば、2012年6月、Natwest Bankの650万人の顧客が数週間サービスを中断し、ソフトウェアのアップグレードが失敗し、元に戻す必要がありました。  
銀行は4200万ポンドを調達した[686]。その後、2008年の事故で破産したため、主に英国政府が所有していました。  
ですから、マネーセンターの銀行を閉鎖するという破局的な失敗の恐れは現実のものです。  
若い男として、私はいくつかのそのようなプロジェクトに取り組みました：彼らは彼らの爪を噛む瞬間を持っています。  
私たちは同様のプロジェクトのリスクを、食物連鎖のさらに下に突き止めます。  
私たちはそれをインストールした会計事務所を訴え、何が問題だったかの詳細なレポートを公開しました[691]。  
このシステムはまだ何年も経った今でも、使用するのが面倒であり、なぜ興味深いのかもしれません。  
私たちの教授は週に1〜2時間使用するかもしれませんが、店員はいつもそれを使用するので、もっと気にします。  
したがって、簿記システムが、バランスと整合性の基本的なクラーク・ウィルソンの特性を強化する標準コアを使用していても、まだ多くの問題があります。  
12.2.6.3生態学的妥当性  
また、それらが外部の現実に対応していることを確認する必要があります。  
記録された資産と在庫の20％が存在しないことが判明しました。  
監査人は、会社の上司について問い合わせることなくマッケソン口座を受け入れていました。彼らは、在庫の確認、顧客との売掛金の確認、または会社内での職務の分離について考えることに失敗しました[1616]。  
CEOのTino de Angelisのケネディ。  
内部告発者が詐欺についてそれを告げた後、アメリカン・エキスプレスの株式は50％下落しました。 $ 58mを失った。  
 すべての大手企業を監査するという要件は、すべての主要な金融スキャンダルで監査企業を巻き込みました。  
また、一部の支払いおよび簿記アプリケーションで現在宣伝されているブロックチェーンシステムの1つの問題は、数学的構造が一貫性とコンセンサスを保証する一方で、言及された資産が健全であるか、存在するかについての情報がまったくないことです。  
セクション20.7でこれに戻ります。  
決済サービス会社であり、ポルノサイト、オンラインカジノ、および通常の銀行では触れられない他の商人へのカード決済の処理を開始していました。  
しかし、2020年6月、ドイツ銀行（時価総額は約200億ドルのドイツ最大の銀行）を買収しようとしていました。  
（EYは3年間、銀行の明細書を銀行員に確認することができず、会社自身が提供する「スクリーンショット」を使用していました[1834]）。  
それを使用して支払いを処理する一連の最先端の新興企業は取引を停止し、ドイツ内外の何百万人ものカード所有者が自分のお金にアクセスできなくなっていました。  
さらに悪いことに、Financial Timesが2019年にWirecardの疑わしい会計慣行の分析を発表したとき-そのドバイ子会社には顧客がいないようであり、1つのフィリピンの子会社の住所は小さなバス会社であり、別の会社は自宅だったと指摘した引退した船員の1人で、シンガポールの子会社の内部告発者は本を調理するように命じられていたと報告している[1283] –ドイツの規制当局BaFinは会社を調査するのではなく、ジャーナリストの犯罪捜査を開始し、空売りを禁止した会社の株式の[610]。  
これは、ヨーロッパの歴史上最大の詐欺の1つであり、見かけ上の株主価値だけでなくe200bnを破壊し、ドイツの金融規制に対する国民の信頼も失墜させました。  
マッケソンとロビンスのレッスンがどれだけ注意されていなかったかを見るのは驚くべきことでした。海外の現金残高をチェックすることは本当に監査101である必要があります。  
  
内部統制構造が保守的で費用がかかり、効果がない傾向がある主な理由は、理論的には組織が経験に照らしてそれらを開発する一方で、実際にはこの経験は監査人カルテルを通じて中継されるためです。  
内部監査基準の調査があります[？、米国の会計および監査機関のグループ[461]。  
COSOモデルは、内部統制だけでなく、財務報告の信頼性と法規制の遵守を対象としています。  
COSOは、ハードシステム設計の問題よりも企業文化のソフトな側面を強調するため、システムが進化するプロセスを管理および文書化するためのガイドと見なすことができます。  
実際には、監査人はそれを捕捉しました。  
、Certified Information Systems Auditor（CISA）を管理します  
 これはより国際的です[946]。  
より具体的な基準は、米国の上場企業のSarbanes-Oxley、米国の金融機関企業のGramm-Leach-Bliley、米国の医療提供者のHIPAA、個人情報のGDPRなど、特定の部門別規制の監査人の解釈から生まれます。 EU加盟国の居住者の。  
セキュリティ管理に関するISO 27001もあります。  
これらの多くは標準であり、誰もが同意できるため、決して十分ではありません。  
セクション28.2.9でこれに戻ります。  
12.2.7弱点の発見  
あなたも人々と彼らの外部の関係について考える必要があります。  
 支店長は、いとこが偽造した担保に対して経営する危険なビジネスにお金を貸すことができるでしょうか。  
 運用マネージャーはサプライヤーから賄賂を受け取っている可能性がありますか？  
 多くのことがうまくいかない場合があります。  
毎年誘惑に陥るスタッフの1％の古い経験を思い出してください。  
誰があなたに損害を与えることができますか？  
学ぶべき教訓は次のとおりです。  
•顧客やスタッフからの苦情を利用して詐欺やシステム障害を警告する場合は、顧客から連絡を受けたり、彼らに耳を傾けたりするための良い方法があるとよいでしょう。  
•主な露出は会社のスタッフと請負業者にありますので、十分に彼らと話をして、「会社を詐欺したい場合、どうしますか？  
やる気を起こさせる構造がなく、内部告発者にリスクを負わせることなく、人々がお互いを正直に保つことを期待していますか？  
•これらの回避策は当然のことながら脆弱性を生み出すため、人々が準拠できるコントロールをより適切に設計する必要があります。  
リスクは常に残ります。  
特定のシステムが絶対に失敗しないという教義を採用することは非常に悪い考えです。なぜなら、その失敗をアプリオリの確率ゼロに割り当てた場合、証拠がそれをシフトせず、最終的に失敗すると事態が大きく悪化する可能性があるためです。  
経験とは、単なる損失履歴ではなく、邪魔になるコントロールを特定して改善する必要があることを意味します。  
たとえば、パスワードリセット機能を修正して必要なスタッフを減らすか、詐欺エンジンを改善して会社のWebサイトがより少ない買い物かごを拒否するようにできると、取締役会はより簡単にあなたの言うことを聞きます。  
セキュリティ管理に関する国際規格ISO 27001が一部の業界で使用されています。リスクを体系的に分析し、許容できないものに何らかのリスク処理（管理、回避、移転）を施す必要があります。  
多くの企業では、これはとにかくあなたの監査人によって動かされます。  
医療では、HIPAAについて心配する必要があります（セクション10.4を参照）  
  
人々が電子詐欺について考えるとき、巧妙なロシアのハッカーが銀行のコードを破り、無数のドルの電信送金をタックスヘイブンに送るハリウッドのシーンをよく想像します。  
まず、銀行間での送金に使用されるシステムについて説明し、次に個人または販売者を問わず、銀行の顧客が使用するシステムについて説明します。  
12.3.1電子商取引の電信の歴史  
しかし、それははるかに遡ります。  
、セマフォ（動く腕の位置を使用して文字と数字を通知する）  
陸上システムは一連のビーコンタワーに沿ってメッセージを送信し、海軍システムはそれらを船間で中継しました。  
彼らが1836年に発見されるまでの2年間、2人の銀行家がオペレーターに賄賂を渡して、安全な距離から観測できる送信の誤りを犯すことにより、株式市場の動きを密かに知らせました。  
Bookiesは、結果を待って最初にそれを聞いたことを期待するのではなく、時計で「時間を呼び出す」ことを学びました。彼は1842年に議会を説得して、ワシントンからボルチモアまでの実験線に資金を提供しました。  
これは、1990年代後半のインターネットブームのように、さまざまな意味でありました。  
電報は、国内市場の創出にも使用されました。  
この期間の歴史は、eコマースの概念と問題のほとんどがビクトリア朝時代によく知られていることを示しています[1818]。  
 彼らが信頼できるかどうかはどうやって分かりますか？  
 19世紀の答えは信頼できる仲介者でした。主に、参照、保証、信用状を使用してビジネスのリスク管理を支援した銀行です。  
まず、セクション5.2.4で前述したように、ほとんどのテストキーシステムは暗号解読に対して脆弱でした。多数のトランザクションを観察した人は、徐々に鍵となる資料を見つけ出すことができます。  
秘密のテーブルは金庫に保管され、2人の店員が一緒に座ってテストを行い、チェックしました。しかし、スタッフが同時に許可されていないメッセージのテストを実施するのを止めることは何も実際にはありませんでした。  
手動暗号化を使用すると、各トランザクションはキーボードで少なくとも3回入力されます。テストが手動で計算されたテレックスルームでトランザクションを出力する支払銀行のコンピュータに1回入力します。次に、もう一度テレックスを受信銀行に送信します。受信銀行は手動でテストをチェックします。その後、その銀行が3度目に自分のコンピュータにそれを供給した。  
確かに、支払いは銀行のコンピュータから別の銀行のコンピュータに直接流れる可能性がありますか？  
12.3.2 SWIFT  
 1970年代には、加盟銀行間で支払い指示を送信するための、より安全で効率的で制御可能なメカニズムを提供します。  
これは世界中で毎日数兆ドルを出荷するために使用されており、そのデザインは、船の貨物の所有権を証明する船荷証券など、他の多くの種類の資産にタイトルを処理するシステムにコピーされています。  
銀行は、従業員が銀行取引を偽造できるほどにSWIFTを信頼したくありませんでした。  
 機密保持のための暗号の民間使用を禁じます。  
最後に、銀行は銀行間取引に対して監査可能な二重統制を実施できなければなりませんでした。  
メッセージの信頼性は、メッセージ認証コード（MAC）を計算することにより保証されました。  
鍵は、二国間鍵交換を使用して管理されていました。銀行が海外で関係を築くときはいつでも、それを交渉した上級管理職は、面談でも会議でも、相手の番号と鍵を交換していました。その後、お互いの自宅の住所に郵送する。  
。  
このように、SWIFTはメッセージ認証に関与しませんでした。使用されている認証アルゴリズムが適切である限り、スタッフは誰もトランザクションを偽造できませんでした。  
かなり早く、攻撃が発見され、[1545]で公開されました。  
SWIFT自体は認証に対して信頼されていませんでしたが、否認防止サービスを提供しました。  
 それらはログに記録してSWIFTに転送しました。SWIFTもログに記録し、国のRGP経由で受信者に送信しました。  
したがって、トランザクションを不正に拒否したい銀行家は、ローカルのSWIFTアプリケーションとその周囲のコントロールだけでなく、異なる国の2つの独立した請負業者を倒さなければなりません。  
機密性はオプションのアドオンでした。  
専用回線の両端にあるデバイス間で鍵が手持ちされていました。  
10ある国では、ラインエンクリプターをインストールしようとした銀行が、数時間後にラインにノイズが現れるのを発見しました。  
銀行は、地元のスパイが暗号化を容認しないことを認識し、あきらめました。  
通常の操作方法は、3人のスタッフがSWIFTトランザクションを行うことです。1人は入力、1人はチェック、1人は承認です。  
そのため、入室管理を通過した偽の支払い指示は、翌営業日に警告を発するはずです。  
12.3.3何がうまくいかない  
1990年代半ば、MACアルゴリズムへの攻撃が公開された後、公開鍵メカニズムを追加することで機能が強化されました。SWIFTIIは引き続き双方向の鍵交換を使用しましたが、公開鍵暗号とMAC自体を使用して通信相手銀行間でMAC鍵を共有しましたデジタル署名によって保護されています。公開鍵暗号化の採用によってもたらされた信頼の集中化とはまったく別–中央の認証局がそうでない場合に、銀行に属しているとして鍵を誤って認証する可能性がある–少なくとも1つの初期展開で512ビットを採用米国による公開鍵  
双方向の鍵交換は、暗号化メカニズムが独自仕様である新しいシステムに2009年に置き換えられました。  
暗号が強化され始め、デフォルトで機密性が提供されるようになると、政治的な議論が生じました。  
これはプライバシーを意識したヨーロッパ人との対立を引き起こしましたが、最終的にオバマ大統領がブッシュ大統領を引き継いだ後、EUは米国財務省がスウィフトで召喚状に仕えることができる条約に合意しました[341]。  
犯罪者（政府とは対照的）  
銀行のプログラマが偽のメッセージを処理キューに挿入することは時々起こりますが、ビジネスプロセスを理解していないため、通常は失敗します。  
これらのアカウントは11チェッカーが受取人と金額を変更できるため、これは実際にはデュアルコントロールであり、トリプルコントロールではありません。システム側で職務の分離を維持できない限り、インターフェイスを維持するプログラマーは常にシステムを攻撃できます。あまりにも。  
残高と与信限度の両方があり、支払いは1つまたは複数のコルレス銀行を経由する必要がある場合があるため、大規模な支払いでは、資金を利用できるようにするために人間の介入が必要です。  
そのため、スイスの銀行に開設した口座に偽の取引をこっそりやっているナイーブなプログラマーは、現金を集めようとするときに逮捕されます。  
彼らは、Dridexマルウェアを使用して銀行スタッフの資格情報を盗み、ニューヨークの連邦準備制度にある銀行の口座から8100万ドルをフィリピンに送金する4つのトランザクションを注文し、そのうち1800万ドルしか回収されなかったようです。残りは地元のカジノで洗濯されました。  
これは実際にはSwiftに対する攻撃ではなく、バングラデシュ銀行自身のSwiftシステムへのゲートウェイに対する攻撃でした[858]。  
実際、ほとんどの重大な詐欺では、技術的な攻撃ではなく、手続き上の脆弱性が悪用されています。  
彼はスイスのロシア政府機関から大量のダイヤモンドを購入することに同意することにより、規制を回避しました。  
彼は米国の銀行休暇の直前に取引をすることによって脱出するために余分の時間を与えました。  
彼がヨーロッパでそれらを隠し、米国に戻って詐欺の調査を手伝っていたなら、彼はそれを回避したでしょう。そのまま彼は逃げて捕まった。  
当時、南アフリカ政府は2つの為替レートを運用しており、1つの銀行では、各取引に適用されるレートを決定する責任を負うマネージャーがロンドンの金持ちと共謀しました。  
この2週間後、中央銀行は警察ラウンドを送った。  
そこで、彼は邪悪なアパルトヘイトシステムをどのように詐欺したかについてマスコミに自慢しました。  
これはおそらく、私が知っている唯一のケースであり、perpが数百万ドルで済んだだけでなく、自慢しなければなりませんでした。  
ある国の企業が別の国の企業へのローンを保証するよう銀行に依頼するのはよくあることです。  
しかし、その時点では現金は変わりませんので、バランス調整は機能しません。  
貸し出し銀行がローンが酸っぱくなったことに気づき、保証を要求しようとしたときにのみ、偽造品が発見されます。  
教訓は、デュアルコントロールを打ち負かす可能性のあるものすべてに警戒することです。  
それは、システム管理、インターフェース、または共有制御暗号の技術的な問題だけではありません。コアはビジネスプロセスの設計です。  
通常、適切な分割制御には機能の分離が必要です。そのためには、その社会的および経済的コンテキストでアプリケーションを本当に理解する必要があります。  
12.4自動預け払い機  
このストーリーには少なくとも4つのコンポーネントがあります。最初の現金自動預け払い機（ATM）  
ATMは、20世紀で最も影響力のある技術革新の1つでした。  
彼は1939年にニューヨークに自分の「Bankamat」マシンをインストールするようにシティコープを説得しましたが、彼らは6か月後にそれを撤回し、「マシンを使用したのは少数の売春婦とギャンブラーだけで対処したくなかった窓口担当者の対面 '[1743]。世界銀行によると、現在240万台を超えるマシンがあり、10万人あたり41台です[2041]。  
つまり、ATMは、現代の商用暗号化と小売決済技術を地面から取り除く「キラーアプリ」でした。  
12.4.1 ATMの基本  
カードの磁気ストリップにはPAN：PINキーが含まれていますKP：FEFEFEFEFEFEFEFE DESの結果{PAN} KP：A2CE126C69AEC82D {N} KP 10進数：Natural PIN：オフセット：カスタマーPIN：図12.3：–銀行カードを生成するIBMの方法は、お客様のプライマリアカウントにPINを入力します番号（PAN）  
「PINキー」と呼ばれる秘密キーは、PANを暗号化し、それを10進数化して切り捨てるために使用されます。  
オフセットには暗号化機能はありません。顧客が自分のPINを選択できるようにするだけです。  
PINを使用する最初のATMでは、各ATMにPINキーのコピーが含まれ、各カードにはオフセットとプライマリアカウント番号が含まれていました。  
初期のATMもまたオフラインで運営されていました。現金引き出し限度額が1週間あたり500ドルの場合、カードにカウンターが置かれていました。  
2003年以降、磁気ストリップにはスマートカードチップが追加され、続いて2012年から非接触型決済が行われました。これらの機能強化については、後のセクションで説明します。  
ハードウェアセキュリティモジュール（HSM）と呼ばれる暗号化プロセッサ  
1。  
、銀行のスタッフが自分のPIN以外のPINを見ることはありません。  
2。  
数日間隔で郵送されます。  
端末マスターキーは、2つの印刷されたコンポーネントの形式で各ATMに提供されます。これらのコンポーネントは、別々の人によって支店に運ばれ、ATMの背面キーボードで入力され、組み合わされてキーを形成します。  
 バンクとVISAなどのネットワークスイッチとの間にマスターキーを設定するために使用されます。  
ATMがPIN検証をローカルで実行する場合、PINキーは端末マスターキーで暗号化され、ATMに送信されます。  
5。  
このPIN変換機能は、完全にHSM内で実行されます。  
ATMネットワークは急速にSwiftよりも桁違いに大きくなりました。  
20,000の銀行間で鍵交換または金融決済を双方向で行うことは不可能だったため、各銀行はVISAなどのスイッチング組織によって提供されるスイッチに接続し、これらのスイッチのHSMがトラフィックを変換します。  
スイッチは信頼されているため、何か問題が発生した場合、結果は深刻になる可能性があります。  
あるケースでは、スイッチマネージャーは正義から逃亡し、別のケースでは、スイッチでのY2K関連のソフトウェアアップグレードが失敗し、その結果、ある国のカード所有者は、1日か2日の間、たとえお金を引き出しても、彼らの口座は空でした。  
1980年代にATMネットワークとセキュリティシステムを設計したエンジニア（そのうちの1人）  
セキュリティモジュールの購入が遅れている多くの銀行を心配しました。  
暗号化アルゴリズムが十分に強力であるか、改ざん防止HSMが十分に改ざん防止であるか、およびキーの生成に使用される乱数ジェネレーターが十分にランダムであるかどうかについて悩みました。  
何よりも、修理業者が銀行のPINキーを手に入れ、何百万ものカードの再発行を強制し、電子バンキングにおける公の信頼を破壊するのではないかと心配しました。  
最終的に終末が起こりました。  
どういうわけか、それはメモリースティックにコピーされました。 CEOにもコピーがありました。  
2018年3月から2019年12月までに、5600万ルピア（340万米ドル）  
2019年2月、中央銀行はPostbankに1200万枚のカードをすべて再発行するように命じました。  
ただし、過去50年間のPINベースの支払いカードに対する数百万の詐欺は、非常に多様であることが判明しました。  
12.4.2何がうまくいかない  
カード詐欺の相次ぐ波があり、そこで脆弱性が発見され、悪用され、最終的に修正されました。  
1990年代初頭の最初の波は、初期の磁気ストリップカードシステムの不十分な実装と管理を悪用しました。  
彼は偶然に「暗号化の置き換え」のトリックを発見したときに始めました。彼は銀行カードの口座番号を妻の口座番号に変更し、彼のPINを使用して彼女の口座からお金を引き出すことができることに気付きました。  
これは、彼の銀行が暗号化されたPINをアカウント番号にリンクせずにカードの磁気ストリップに書き込んだために発生しました。当時のほとんどの銀行は伝票に完全な口座番号を印刷していましたが、カードは他の正しい情報がなければ機能しました。  
彼（およびその他）の約2000人の犠牲者  
銀行は、それぞれのケースで事実が異なると主張してこれを打ち負かし、被害者が追求する専門知識を持っていなかった何千もの小さな請求のケースにそれを分割しました。  
ルーマニアなどの犯罪者がATMスキミング機器の設計を開始し、オンラインで販売したため、詐欺は最終的に世界中に広がりました。  
1990年代初頭の実際の「ファントム撤退」のほとんどは、次の3つの原因の1つを持っているように見えました。•単純な処理エラーは、紛争の定常的なバックグラウンドノイズを引き起こします。  
エラー率が100,000分の1の場合、それは多くの論争です。  
追跡したエラーの原因の1つは、銀行のサーバーから確認メッセージを受信する前にネットワークがダウンした場合、大手銀行のATMがトランザクションを再度送信することでした。定期的に、サーバー自体がクラッシュし、開いているトランザクションを忘れて、借方が重複していました。  
（私たちはこれらのカードを「ディレクターズカード」と呼んでいましたが、それらが銀行のディレクターに発行されたと冗談を言っていました。）  
たとえば、1992年2月にケンブリッジに引っ越したとき、私の銀行は1通ではなく2通のカードとPINを郵便で送り、侵入者が私たちのアパートのブロックの郵便を手に入れてそれを解体してから数日後に到着しました貴重品を探しています。  
主な修正は、コールセンターに電話をかけるか、Webサイトにアクセスしてカードを使用できるようにすることでした。  
ATMサービススタッフがATM内に盗聴器を取り付けて顧客カードとPINデータを記録するケースが時折ありました。1ケースは、1990年代に不正なインサイダーが盗んだカードのPINを一度に£50で処理したケースです。  
インサイダー詐欺は、法律のように顧客に詐欺の代金を支払わせることが一般的である英国のような国では特に一般的であり、銀行が支払った米国のような国ではまれでした。英国の銀行スタッフは、顧客の苦情を注意深く調査しないことを知っていました。  
•1980年代半ばにニューヨークで最初に報告されたのは、ATMキューに立って、顧客のPINを観察し、破棄されたチケットを受け取り、データをブランクカードにコピーするという肩を並べるトリックでした。そしてそれは1990年代半ばにベイエリアでまだ働いていました。  
ビジュアルコピーは簡単に停止できます。現在の標準では、チケットにアカウント番号の最後の4桁のみを印刷します。1990年代初頭から、カードには3桁のカード検証値（CVV）があります。  
ただし、CVVは常にチェックされるわけではありません。  
1980年代に販売された1つのATMには、特定の14桁のシーケンスがキーボードで入力されるたびに、利用可能な最低額の10枚の紙幣を出力する「テストディスペンス」コードがありました。  
マシンを使用するすべての銀行は、テストディスペンストランザクションを無効にするパッチを急いで出さなければなりませんでした。  
•コンビニエンスストアで使用されている一部の種類のATMは、実際には20代を払っていたときに、1ドル札を分配していたと考えるように再プログラムできます。オンラインマニュアルに印刷されているデフォルトのマスターパスワードが必要です。  
マシンをリースした店舗の所有者は、この脆弱性について知らされておらず、タブを手に取り残されました[1539]。  
実験として、妻は1993年に目撃者として私たちの銀行の支店に行って、PINを忘れたことを伝えました。  
誰も彼女を知らなかった、そして彼女が提供したすべての身元は私たちの銀行カードと彼女の小切手帳であった。  
（その銀行は後に2008年に破綻した。）  
詐欺師は、おそらく古いビデオカセットからのテープのループをATMの喉に差し込み、被害者を待ちます。  
詐欺師はそれを取得し、被害者のPINを確認できた場合は買い物に行きます。  
一部の銀行は気にしません。そのような詐欺の被害者の1人は、銀行のロビーで、銀行の内部にまっすぐ行き、不満を述べましたが、関与したくないスタッフに騙されました。  
•ハイテクモードの操作では、偽の端末またはスキマーを使用してカードおよびPINデータを収集していました。  
1993年、2人の悪者が実際のATMとそのソフトウェア開発キットを購入し、カードデータとPINを盗むようにプログラムし、コネチカット州のバックランドヒルズモールに設置しました[988]。セクション4.5で触れましたが、ガレージのPOS端末のタップを使用して、オランダのユトレヒトでカードとPINデータを収集しました。そして1994年に、ロンドンの詐欺師は偽の銀行支店全体を設置した[943]。  
2015年までに、ルーマニアのギャングがメキシコの観光スポットで100台のATMを操作し、月額2,000万ドルを盗んだ[1094]。  
•2010年代半ば以降、詐欺師がATMをハッキングして、空になるまで請求書を出し続ける「ジャックポッティング」攻撃が時折見られました。  
•インサイダーがバックエンドシステムのサーバーの1つに到達したとき、またはサーバーの1つが安全に失敗したときに、不正が発生することがあります。  
 または適切なPINを使用している顧客で無制限の当座貸越を実行できる（残高照会プロセスが失敗した場合）  
9/11がATMネットワークに損傷を与えた後、地方自治体信用組合はニューヨークの顧客に物事が修正されるまで残高を確認せずにお金を引き出せるようにすることを決めました。  
1980年代にATMセキュリティシステムを設計するときに最初に間違えたのは、顧客（銀行のシステム設計者、実装者、テスター）がセキュリティを使用できないことを心配する必要があるときに、犯罪者が賢いことを心配することでした。私たちが設計したシステム。  
数学は興味深いので、セキュリティ専門家は暗号に注意を向けますが、専門家ではない人が実際に使用できるツールを作成するなどの「退屈」なビットにはそれほど注意を向けません。  
また、最近の支払いネットワークには非常に多くのユーザーがいるため、あまりにもあいまいすぎてテストに捕らえられない脆弱性が発見される可能性を期待する必要があります。  
ATMの場合、偽端末攻撃は最終的に大きな時間を費やしたものです。  
2005年頃から、東ヨーロッパで製造されたスキマーは地下市場で販売され、ATMの喉に取り付けて磁気ストリップを読み取り、小さなカメラやキーボードオーバーレイを使用してPINをキャプチャするように設計されています。  
救済策は磁気ストリップカードからチップカードに移っていますが、これには15年以上かかり、その間、磁気ストリップ詐欺には多額の費用がかかりました。  
重要な要素は、2.3で説明したように、犯罪者が専門化して組織化し始めたことです。  
12.4.3インセンティブと不正  
歴史的なケースでは、ジャッド対シティバンクの銀行の顧客であるドロシージャッドは、異議のあった引き出しは行わなかったと主張し、シティバンクは、そのシステムは安全であったため、実行したに違いないと述べた。  
米国連邦準備制度はこの見解を「規制E」に組み込んでおり、顧客による詐欺行為を証明できない場合は、銀行がすべての係争中の取引の払い戻しを要求しています[639]。  
他の国（イギリス、オランダ、ノルウェーなど）では、銀行は何年もの間、ATMシステムは間違いがないと主張して逃亡しました。  
ストーンと彼の追随者がATM詐欺のために投獄され始めたとき、この立場はイギリスでいくらか損なわれました、そして、いくつかのかなり不愉快な事件がありました。  
ジョンマンデンはケンブリッジシャー州ボッティシャムに拠点を置く地元の警察の巡査の一人でした。彼のビートには、私が当時住んでいたロードの村が含まれていました。  
彼は声明を求め、彼が作成を思い出さなかった合計460ポンドの6つの引き出しを見つけ、不満を述べた。  
裁判中に、彼らのITがやや手に負えないものであることが判明しました。係争中の取引は適切に調査されていませんでした。また、ソフトウェアはアセンブラで作成されているため、ATMシステムはバグに悩まされないなど、あらゆる種類の野生の主張をしていました。  
彼は1994年2月に有罪判決を受け、警察に拘束された。  
弁護側は、銀行のシステムへの平等なアクセスを専門家に要求した。  
事件は崩壊し、ジョン・マンデンは無罪となり、彼は仕事を取り戻した。  
彼女に対する訴訟は2008年1月に崩壊した。  
それは敵対的な専門家による検査に耐えることができなければなりません。  
これは、ATMカメラをインストールすることによって提供された可能性があります。これらはニューヨーク州では反強盗対策として必須でしたが、イギリスでは使用されませんでした。  
12.2.6.1項で述べた郵便局の訴訟が最終的に銀行のシステムを徹底的に調査し、高等法院で信頼できないと非難されるまでには、さらに25年かかります。12.5クレジットカード  
1950年代にDiners Clubが発明してから何年もの間、クレジットカードは、ほとんどの銀行によって、価値の高い顧客を引き付けるための損失リーダーとして扱われていました。  
英国では、80年代半ばから、クレジットカードビジネスが突然非常に収益を上げました14。  
 これは、小さな商人の場合は通常2％弱の商人割引を差し引いた後に支払います15。  
各トランザクションには2つのコンポーネントが含まれます：承認、カードを販売者に提示し、商品を提供するかどうかをすぐに知りたい場合の承認と、別のシステムを経由して販売者にお金を受け取る決済（多くの場合2つか3つ）数日後。  
  
1950年代から1990年代にかけて、クレジットカードのトランザクションは、カードのエンボスを使用してマルチパートフォームに紙の販売ドラフトを作成し、金額を書き込んで、顧客に署名させ、小切手のように処理することによって処理されました。  
各販売者は、ローカルの「ホットカードリスト」に加えて、それを超えるとオンライン認証を呼び出さなければならない取得銀行によって設定された制限を取得しました。  
詐欺師の対応は偽造されたカードの大洪水でした：1989年から1992年の間に、磁気ストリップの偽造は、時折の迷惑行為から詐欺による損失全体の半分にまで成長しました[12]。  
 販売者がカードを検査できなかった取引。  
しかし、主な変更は、商人が紛争のリスクを負うように責任をシフトすることでした。  
、全額が多額の手数料とともに即座にマーチャントに引き落とされます。  
15Debitカードの方が安価で、大手の販売者はクレジットカードの取引でも1％未満で支払うことができます。  
増大するカード偽造とオンライン詐欺に対するVISAの対応は、カード検証値（CVV）でした  
 ストリップの最後に書かれています。  
したがって、MastercardもCVVを採用しました。  
詐欺師はスキミングに移りました–事業者は本物の顧客カードを余分な無許可の端末に通して、磁気ストリップのコピーをつかみ、本物のカードに再エンコードしました。  
 銀行の対応は、不平を言った顧客の購入履歴を相互に関連付けることにより、犯罪ビジネスを特定しようとする侵入検知システムでした。  
あなたはマフィアが所有するビストロでドリンクを飲み、カードを提供し、バウチャーに署名し、料金が請求書に記載されていないときに気付かない場合。  
その時までにビストロのことを忘れてしまい、銀行にはその記録がありませんでした[720]。  
2003年にロシアとウクライナで始まったオンライン犯罪フォーラムの出現により、マルウェアの作成者、ボットネットの遊牧民、フィッシングサイトの運営者、キャッシュアウトの専門家が互いに取引し、仕事をうまくやり遂げることができました。  
フォーラムは、カードクローンを作成するために、マグストリップカードとPINデータを記録する偽の端末とスキマーを提供しました。  
ヨーロッパは2003年から5年にスマートカードを導入し、詐欺師たちは、チップカードからマグストリップカードにデータをコピーして、マグストリップトランザクションをまだ受け入れている端末で使用するデバイスを考え出しました。  
カードにチップが搭載されているかどうかに関係なく、正規の顧客が受け取ることのないカードに関連する多くの詐欺があります。  
存在しているが、アプリケーションを認識していない人の名前で作成されたアプリケーションがあります（銀行では、お金ではなく自分のIDが盗まれたと偽装したい場合、「IDの盗難」と誤って伝えられることがよくあります[1324]）。  
また、詐欺師が不注意に銀行のスタッフにあなたのアカウントの交換用カードを彼らが管理するアドレスに送信する詐欺があります[2013]。  
  
今、私は従来のクレジットカード詐欺からオンラインのさまざまな方法に移り、1987年に警察がオンラインクレジットカード詐欺を調査するのを最初に支援しました。  
当時のホットカードリストには、その国で悪用されていたカードのみが記載されていました。海外のローカルホットカードを使用するということは、銀行が無実の顧客ではなく缶を運ぶことを意味しました。  
暴風雨が彼の家の反対側の川岸を洗い流し、警察が彼を締め出すために建てた皮を露出させました。  
「悪意のあるハッカー」が電子メールやWebフォームを傍受し、クレジットカード番号を100万件収集したため、インターネットでのクレジットカードの使用が詐欺の雪崩につながるのではないかという不安がありました。現実はもう少し複雑です。  
多くのWebサイトが暗号化なしで、または弱い暗号化で何年もの間実行され、本当の問題は盗聴ではなくフィッシングであることが判明しました。  
 問題は暗号よりも心理学です。  
サイトのドメイン名は異なりますが、特に銀行や販売者があらゆる種類のバリアントドメイン自体を使用しているため、ほとんどの一般の人々がそれに気付くことを期待するのは不合理です16。  
VISAには、取引が処理された後、商人がクレジットカードデータを保存することを禁止する規則が長年ありましたが、多くの商人はそれらを無視しました。  
、Payment Card Industry Security Standards Councilによる共同の取り組み17。  
最後に、施行がかじり始め、2007年10月までに、米国全国小売連盟はクレジットカード会社にクレジットカードデータの保存を強制するのをやめるように要求しました（チャージバックの場合にカード番号を一時的に保存することになっていた）  
PCI DSSは、クレジットカード取引を受け入れる企業にとって、今や重要なコンプライアンス要素となっています。これはほとんど提供しません。16。証明書の透明性など、いくつかの技術的な修正が行われました。  
18カード会員データは、ネットワーク経由で暗号化する必要があり、保存時にはファイアウォールとAVで保護する必要があります。デフォルトのパスワードは使用できません。また、セキュリティポリシー、知っておくべきアクセス制御、テスト、2017年以降の安全なソフトウェア開発ライフサイクルが必要です。  
詐欺が発生した場合、銀行は通常、認定されていたとしても、とにかく商人を非難することができるので、賠償責任をカバーします。  
詳細は国によって異なりますが、顧客への通知に実質的な費用がかかり、違反した企業の株価は数パーセント下落する可能性があるため、開示法は違いをもたらしました。  
基本的に、顧客がしなければならないことは、クレジットカード会社に電話して、「私はそれを承認しませんでした」と言って、販売者に請求書を渡すだけです。  
顧客が取引を不正に否認した場合、商人は裁判所を通じてそれらを追跡します。  
そのため、トランザクションを否認する機会が増え、それを回避できます。  
一般的な詐欺は、サイトの「無料ツアー」を提供し、クレジットカード番号を要求することでした。おそらくユーザーが18歳以上であることを確認してから、とにかく請求しました。  
playboy.comのような明らかに大規模で「立派な」Webサイトでさえ、そのような慣行が批判され、ポルノ業界の最下層では、事態はひどいものになります。  
セクション26.5.3でOperation Oreのケースについて説明します。  
銀行は通常、商人にそれぞれ100〜200ドルの手数料を請求し、取引金額を口座から引き落とします。  
チャージバックがおそらく10％を超えると、銀行がサービスを終了する場合があります。  
4つの時計用）  
しかし、それらとの通信販売トランザクションの責任の大部分を残すことは次善の策です：銀行は詐欺のパターンについてより多くを知っています。  
法律が制定されたときに1人のロビイストが別のロビイストを打つか、主要な判例が設定されたときに1つの法務チームが別のロビイストを破って、私たちはそれで行き詰まります。  
すべてのウェブサイトでメインのアカウント番号と有効期限を尋ねる必要がありますが、販売者はカードの裏面に印刷されているCVVとカード所有者の住所からの数字を尋ねることもあります。  
これがVISAカードで機能するのに十分なウェブサイトがあります。マスターカードには中央監視機能があり、推測が約10回失敗すると、それらの番号がホットリストされます（ただし、サービス拒否攻撃につながる可能性があります）。  
別の攻撃は資格情報の詰め込みです。悪意のあるユーザーは、侵害されたWebサイトから数百万の電子メールとパスワードの組み合わせを取得し、価値を引き出すことができる他のサイトで試します。  
  
3Dセキュアは、ペイメントカード業界によって設計されたシングルサインオンシステムです19。  
これは、大規模な決済カードの取引にますます使用されています。  
顧客のオンボーディングは何年もの間ソフトスポットでした。  
。  
また、URLが銀行とは関係のないサイトで銀行のパスワードを入力するのに慣れていました。また、ある銀行では、顧客にATM PINを入力することもできました[1362]。  
 EMV標準として承認された2番目のバージョン。ただし、SMSベースの2要素認証は、セクション3.4.1で前述し、セクション12.7.4で後で説明するように、その耐用年数の終わりに達しています。  
  
人々は1990年代半ばからより優れた金融侵入検知に取り組み始めました。現在では、カードを提示しないトランザクションを受け入れるあらゆるサイズのすべてのWebサイトに、各トランザクションを受け入れるか拒否するかを決定する詐欺エンジンがあります。  
どちらの場合も大きな問題は誤検知です。  
彼らが盗まれたカードをテストして泥棒がまだ生きているかどうかを調べることを提案したので、小さなトランザクションは警報を発していました。  
最新の機械学習技術により、このようなメカニズムの煩わしさはわずかに軽減されました。19「Mastercard SecureCode」、「VISAによって検証済み」、「Amex SafeKey」、「Discover ProtectBuy」など、さまざまなブランドがあります。  
より説得力のあるのは、既知の誤用のパターンを探すプロジェクトです。  
そのサービスに加入している銀行は、カードが盗まれた、PINが間違っている、アカウントが空であるなどの理由で、取引が拒否された場合にそれを通知します。  
詐欺師が1枚以上の盗んだカードをATMに持っていくと、3〜4枚のカードでリストの一番上に移動し、FICOのサービスに加入している銀行が発行したカードを拒否します。  
現在、世界の銀行の40％以上がカード発行量で加入しています。  
英国のウェブサイトは、その詐欺エンジンのために、提供されている買い物かごの4％を拒否する可能性があります。  
優れた詐欺エンジンの中核は、よく理解されている一連の脅威ベクトル（不正なIPアドレス、同じIPアドレスからのログオンが多すぎるなど）に基づいてトランザクションストリームから抽出された数十の信号である傾向があります。  
。  
信号は、SVMまたはベイジアンネットワークのどちらを使用するかではなく、設計の最も重要な部分であるように見えます。  
詐欺エンジンがどのように失敗するかについて、テスコ銀行に対する2016年の詐欺に関する規制当局の報告は、スタッフが詐欺検出ルールに対して「十分なスキル、注意、勤勉さ」を実行し、「十分な厳密さ、スキルで攻撃に対応すること」に失敗したことを発見しましたそして緊急性」[687]。  
チップカードについて説明したら、セクション12.6.3でこのケースについてさらに説明します。  
12.6 EMV支払いカード  
カード決済は複雑かつ多様になりました。それらを理解する最良の方法は、それらの進化を追跡することかもしれません。  
ドイツ人は、スマートカードが1968年にHelmutGr¨ottrupとJ¨urgenDethloffによって発明され、カード用のカスタムICを提案して特許を取得したと考えています。日本は、1970年に国村有村による特許を指摘した。一方、1973年にカードにメモリチップを提案したフランスのクレジットRoland Moreno、および1977年にマイクロプロセッサの追加を提案したMichel Ugon  
ノルウェーは2番目で、1986年からいくつかの銀行がチップカードを発行しています。  
VISAとMastercardの間には特許がありました。  
それはすべて良い学習経験でした。  
そのため、銀行は最終的に1990年代後半に集まり、基準を打ち出しました。  
12.6.1チップカード  
それらは、当初、Europay、Mastercard、VISAによって開発され、その後、標準を維持および拡張するためにEMVCoをセットアップしました。  
米国とシンガポールでは、チップカードが署名付きで使用されるようになり、システムは「チップと署名」と呼ばれています。  
すべてを理解するために、PIN付きのEMVカードを使用してショップから商品を購入するための基本的なプロトコルから始めましょう。  
 または、プライマリアカウント番号（PAN）で構成されるターミナル  
次に、端末は、予測不可能な数またはナンスN、日付t、および要求された支払い金額Xを、カード所有者が入力したPINとともに送信します。  
 これはメッセージ認証コード（MAC）です  
各メッセージには、後で説明する追加のデータdiがいくつかあります。  
 T ffi！ C：N、t、X、d2、PIN C ffi！ T：d3、MACKCB（d3、T、N、t、X）  
販売者はこれを確認できないため、20のリスクも受け入れる必要があります長期キーKCBは、トランザクションごとに派生一意キーを生成するために実際に使用されます（DUKPT、発音されたダックプット）  
私はこのようなオフラインの支払いを省略したり、支払いネットワークを介してカード発行銀行にトランザクションを送信したりしています。  
 カード用。  
EMVには多くのオプションがあり、その一部は個別または組み合わせて危険であり、支払いシステムを構築するための構築キットと考えることができ、非常に安全または非常に安全でないシステムを構築できます。一連の詐欺が安全性の低いバージョンを悪用したため、物事は2005年から17年にかけて着実に強化されました。  
  
多くの国で2011年までのデフォルトのEMVバリアントは、静的データ認証（SDA）でした  
これは、公開鍵暗号化を実行できない安価なカードを使用していたため、カードの公開鍵KCはなく、PINは平文でカードに送信されます。  
端末は証明書とデジタル署名を検証しますが、MAC21を検証する方法はありません。  
まず、一般に悪用される脆弱性は、磁気ストリップカードとの後方互換性でした。  
当初、これらはローカルATMで使用されていたため、切り替え中の信頼性と互換性のために、磁気ストリップ処理にフォールバックします。  
このマグストリップのフォールバック詐欺の波は、図12.4の黄色の線で見ることができ、2006年から2010年の間に急増しています。  
ケンブリッジにある私たちの地元のBPガレージへの攻撃には、PINをキャプチャするために天井に取り付けられたCCTVカメラとカードデータを取得するための盗聴が含まれていました。 200人以上の地元住民が、自分たちのカードのコピーがタイのATMで使用されていることを発見しました。  
21このように、銀行は好きなアルゴリズムを使用できますが、デフォルトは、最後のブロックに対してtriple-DESを使用したDES-CBC-MACでした。  
23英国では、900,000のショップターミナルと50,000のATMがあります。  
 年間合計（百万ポンド）  
メンテナンスエンジニアになる。  
英国のショップとオランダの銀行は、箱から出してすぐに新しいデバイスを設置しました。これにより、すぐに顧客のデータをカラチのサーバーにSMSで送信し始めました[1729]。  
したがって、同僚と私はPINパッドのサンプルを調査したところ、そのような攻撃は簡単であることがわかりました。  
シリアルデータ信号を伝送する直径1 mmのビアは、外部のマークを残さずにプラスチックの穴から挿入できる曲がったペーパークリップを使用して簡単にアクセスできることがわかりました。  
そのようなデバイスの「共通基準評価」は価値がないことが判明しました。失敗の政治的および組織的理由については、セクション28.2.7.2で説明します。  
フランスは「イエスカード」を使った攻撃の波に見舞われました。  
 正規のカードの証明書を使用してEMVプロトコルに参加するが、MACのランダムな値を返す[179]。  
図12.5：–スマートカードデータを傍受するために、Ingenicoの隠されたコンパートメント壁の穴を通して硬いワイヤーを挿入します。  
問題の別のファミリーは、認証方法に関係しています。  
、それは補足データd1とd2で共有します。  
「認証なし」がオプションであることは意外に思われるかもしれませんが、PINパッドのないパーキングメーターなどのデバイスをサポートする必要があります。  
カードと端末の両方に、さまざまな方法の金額制限を設定するリスク管理ロジックを含めることができます。  
中間者デバイスを使用すると、多くの攻撃が可能になります。  
カフェのジャーナリストが1人の学生が運営するTILLにケーキ5ポンドを支払うと、トランザクションは、本を購入するのを待っている書店に残っていた別の学生が持っていた偽カードに中継されました。 50。  
テーマには多くの面白いバリエーションがあります。  
詐欺の規模は国によって大きく異なります。これは、EMVの実際的なセキュリティは、状況要因と実装の詳細に依存することを教えています。さまざまな種類のスキマー攻撃、そして–いつものように–インセンティブ。  
 EMV展開中の目印は「責任のシフト」でした。  
その場合、ヨーロッパのほとんどの銀行は単に顧客を非難しました。「あなたのカードが使用され、PINも使用されたので、あなたには責任があります。」したがって、理論上、詐欺は銀行の問題ではなくなった。  
切り替え期間中にメールから盗まれた多くのカードのおかげで、詐欺は最初に増加しました。商人が詐欺の代償を払うので、EMV端末ができるまで銀行はロールアウトを急ぎました。  
最大の変化は、通信販売とオンライン詐欺の急増でした。  
詐欺行為の数値は、露骨な操作を行わない限り、さらに高かったでしょう。  
適切な詐欺の報告は2015年にのみ再導入されました25。銀行はまた、カード詐欺を調査する小さな警察ユニットの資金の多くを引き継いだので、彼らは起こり得るそのような起訴をある程度制御することができます。  
12.6.1.2 ICVV、DDAおよびCDA  
24のCVVは、商人と銀行の間で長年の悪循環につながりました。  
2007年から2015年にかけて、他のすべてと同様にオンラインに移動し、オンライン部分が適切にカウントされていなかったため、犯罪は着実に減少しました。  
ボリスジョンソンは、2019年に彼女に代わる立場に立ったとき、2008年から16年にかけてロンドン市長であったときに犯罪が発生したと主張しました。  
チップ内のカードデータが磁気ストリップのバージョンと異なる（磁気ストリップATMトランザクションで読み取られる）  
。  
。  
動的データ認証（DDA）  
最初はドイツで使用され、2011年からヨーロッパ全体で使用されました。  
暗号化は2つの機能に使用されます。  
。  
これにより、スキマーがPIN26を収集するのを防ぎます。  
複合データ認証（CDA）  
カードもMAC上の署名を計算することを除いて、DDAに似ています。  
これは、トランザクションデータを公開鍵に関連付け、PIN検証が実行されたという事実に関連付けます。つまり、銀行がトランザクションデータにPIN検証フラグを含めるオプションを選択した場合です。  
  
2009年に、いくつかの詐欺被害者から、カードが盗まれ、銀行で払い戻しを拒否された取引で、PINが使用されたと主張しながら、PINが侵害されてはならないと主張しながら、信用できる苦情がありました。  
一部の国の銀行ではPINを使用していません。これは通常、規制当局が責任の移行を許可しなかったためです。英国の一部の銀行では、顧客がPINを拒否し、代わりに米国式のチップと署名カードを入手することを許可しています。  
ただし、カードフラグは26独自のものです。カードデータはまだ明確ではないため、悪意のある人物は、カード発行者がCVVをチェックしないことを期待して、目視でPINを収集し、マグストリップフォールバックを試みることができます。一部の銀行はまだそうしていないようです。  
2011年5月にフランスで4人の犯罪者が逮捕され、最後の控訴が尽きた後、法医学レポートが2015年にHouda Ferrariらによって公開されました。  
ギャングは、40枚の変更されたカードを使用して、7,000件を超えるe600,000件のトランザクションを盗み、そのうち25件は警察に押収されました。  
。  
 [77]。  
ただし、カードまたはマーチャント端末のいずれかが英国以外の銀行から発行された場合でも、攻撃は機能する可能性があります。  
これらは非常に薄いスマートカードで、厚さが約180ミクロンで、上部と下部に接点があります。  
オーバーレイは、古典的な中間者として機能します。  
。  
12.6.2プレプレイ攻撃  
彼は前の晩、スタッフが疑わしいと思っていたレストランで食事をしていたので、自分のカードがコピーされたのではないかと考えました。  
そこで彼は私たちに連絡を取り、トランザクションログを要求するようにアドバイスしました。  
DDA / CDAカードの場合、EMVの認証ステップはT ffi！です。 C：T、N、t、X、d2、{PIN} KC C ffi！ T：d3、MACKCB（d3、T、N、t、X）  
 明日はそのマシンで動作します。  
それらのほぼ半分がカウンターを「予測不可能な数」として使用していることがわかりました。  
次に、EMV仕様に戻り、端末のテストルーチンでは、テスターが3つの「予測不可能な数値」を引き、それらが異なることを確認するだけでよいことがわかりました。  
 次のデータポイントは、スコットランドの船員がバルセロナの観光通りであるランブラス通りのバーで飲み物を注文した2012年9月に来ました。  
彼は気を失い、翌朝目が覚め、その日遅くにLloyds Bankの彼の口座にe3,300の10の借方が当たっていたことが判明しました。  
彼は私たちを雇った弁護士に指示し、銀行から取引ログを入手しました。  
これは技術的な操作の明らかな証拠であり、船員は彼のお金を取り戻しました。  
同じ端末が使用される場合、「予測不可能な数」を生成するのは端末であるため、攻撃が容易になります[282]。  
英国では、ボーンマスのラップダンスクラブの顧客が2014年に、スタッフが彼を酔わせ、13回の取引で7,500ポンドを請求したと訴えました[334]。  
これは、酒に酔った顧客を売春婦にする単純なケースではなく、プレイ前の攻撃を示唆しています。地方自治体が関心を示し、クラブは6か月間「保護観察」されました。2020年、ロンドンのクラブは実際に顧客に複数の請求を行った後にライセンスを失い、数万人の犠牲者が出ました[1341]。  
端末はさまざまな方法で危険にさらされる可能性があります：貧弱な乱数ジェネレーターを除いて、ベンダーはソフトウェアのパッチに失敗する可能性があり、最近ではオペレーターがそれらでアプリを実行することさえできます27。  
プレイ前の攻撃を行うヒモは、被害者の飲み物を急上昇させることが多いようです。酔っぱらいを麻酔し、銀行口座を略奪している間、売春宿のソファーで眠らせておくと、遅かれ早かれ、そのうちの1人が嘔吐物を吸い込みます。  
前年には、同様の失敗に対して40万ポンドが支払われました[2039]。  
あなたがポケットにたくさんの現金を持っているなら、あなたはおそらく町の悪い部分に入らないでしょう。  
支払いカードはこの慎重な反射を覆い隠し、私たちが穏やかで冷静なときよりもはるかに多くを過ごせるようにします。  
たとえば英国政府は、カジノでのクレジットカードの使用を禁止したところです。  
  
非接触型決済は、1997年にモービルによって米国で先駆けとなり、2000年代にはロンドンから東京までのさまざまな輸送システムに採用されました。  
バークレイズは同じ年に最初の非接触型銀行カードを発行しました。 VISAとMastercardは、支払い用にEMVの非接触バリアントを開発しました。 Googleは2011年にマスターカードPayPass標準を使用してAndroid Payを発売しました28。  
AppleがApple Payをローンチしたとき、市場は2014年に転落した。  
2020年のコロナウイルスの流行により、現金から非接触型への大規模な切り替えがさらに進み、英国のATMトランザクションは1月の232mから4月の91mに減少し、現金トランザクションは3分の1から10分の1に減少しました。 £30から£45。  
米国では、端末が「予測不可能な数」Nを生成し、カードはKCを使用して、選択されたトランザクションデータの3桁のMACとして動的CVVを生成し、これはNとともにカード発行銀行に送信されます。  
リスクはトランザクション制限によって緩和されます– 2020年には、米国で100ドル、英国で30ポンドです。  
英国とヨーロッパには、ランダムにチェックするために銀行ネットワークに送信される可能性のあるARQCを生成するためにカードが作成されるバリアントがあります。  
ただし、カードから電話への非接触型支払いの延長により、さらに複雑になり、システムが完全に開示されました。Googleで設計のためにいくつかの作業を行いました。  
現在、2つのカードスキームからの競合する提案のマッシュアップがあります。  
他のAndroidフォンは、NFC機能がソフトウェアで提供されるホストカードエミュレーションを使用します。  
多くの場合、電話または他のデバイスがオンライントークン化サービスプロバイダー（TSP）によってtoken30とキーマテリアルでプロビジョニングされるトークン化を使用します  
販売者はトランザクションをTSPに送信します。TSPはHSMで適切な暗号化操作を実行し、トランザクションを顧客の銀行に転送します。  
一部の店舗では、接触型トランザクションを使用して支払いを行った後、別の非接触型カードが入っているターミナルの近くに財布や財布を置いた場合、2回のトランザクションに対して請求される可能性があります。  
マーティン・エムズとニューカッスルの同僚は、これが可能であることを示し、さらに興味深いフローを発見しました。1つの英国の銀行では、PINで推測することさえできました。他のものでは、現金制限は外貨取引で失敗した[628]。  
偽のトランザクションは8,261の顧客アカウントから220万ポンドに達し、最終的な損失はわずか70万ポンドでしたが、攻撃により銀行の週末の作業手順では対応できない詐欺の警告が発生しました。  
この失敗と顧客に生じた苦痛のために、規制当局は銀行に1640万ポンドを提出しました[687]。  
これらの攻撃は、電話、カード、端末の複雑さを悪用します。  
2020年に、David Basin、Ralf Sasse、およびJorge Toroは、トランザクションが盗まれたカードから2台の電話を介して非接触型端末にルーティングされる中間者攻撃の改善を発見しました。これにより、カード所有者は電話自体の認証メカニズムを使用して検証されたという主張を受け入れます。バイオメトリック[182]など。  
。  
30支払いアカウント参照（PAR）があります  
これらが大規模な中間者攻撃につながるかどうかを待つ必要があります。このような手法は、ここで説明する攻撃の多くを阻止する可能性があります。  
 カード選択メカニズムは、反復可能な回答を提供するほど強力ではありません[1287]。  
入口と出口の回転式改札口でウォレットに異なるカードが表示された場合、最大の2倍を支払うことになります。  
 一種の平文の磁気ストリップと強力に暗号化されたPINの古い仮定がその頭でオンになっている場合：SPoCルールは、PINを強力に保護できないデバイスは、関連付けられたカードデータを決して学習してはならないことです。  
 電話に接続し、顧客カードを受け入れます。  
また、電話はカスタマーPINをSCRPに渡し、そこで暗号化されてオンライン検証のために送信されます。  
以下のセクション12.8.1で説明するように、ケニアやバングラデシュなどの国では、電話から電話への直接支払いはすでに何千万もの人々にとって日常的です。  
  
クレジットカードとデビットカードの後、支払いの3番目のスレッドは、PCまたは電話からのバンキングです。  
以前にセクション3.4.4.4で説明したように、スティーブゴールドとロバートシフリーンがプレステルをハッキングしたとき、それはマスコミと銀行家を怖がらせました。  
このシステムでは、指定された口座への支払いのみが可能でした。送金できるのは、自分の口座と、ガスや電力の供給業者など、銀行に通知した口座の間だけです。  
1990年代初頭にはテレフォンバンキングが急速に成長し、1990年代後半から銀行のウェブサイトが続き、その後、フィッシャーマンが到着しました。  
12.7.1フィッシング  
悪者はhttp://www.barqlays.comのような誤植されたドメインからhttp://www.barclays.othersite.comのような欺瞞的なドメインへの粗野なルアーから始めました。銀行の最初の対応は、顧客のせいにすることでした。  
1つのギャングがマルウェアを作成し、別のギャングがボットネットを群がるようになり、ホットマネーを受け入れてそれを洗浄するスペシャリストを見つけ始めました。  
2006年に英国の銀行によって失われた3,500万ポンドのうち、3,300万ポンド以上が単一の銀行によって失われました。  
それで、洗濯屋はそれらを避けることを学びました。  
悪意のあるユーザーは、高速フローなどのトリックで対応しました。フィッシングサイトはボットネットでホストされ、ルアーに答えた各マークは異なるIPアドレスに送信されました。  
2007年5月まで、優先ルートはeGoldでした。これはフロリダから運営されている会社ですが、カリブ海に法定住所があり、規制されていない電子決済を提供していました。  
3番目の選択肢は、ウエスタンユニオンのような電信送金会社でした。フィッシャーマンは、自宅で仕事をし、外国企業のエージェントとして手数料を稼ぐ仕事を提供することでラバを採用しました。  
ロシアや中東でもさまざまな電子マネーサービスが提供されています[75]。  
業界では「ラバ銀行」として知られている、マネーロンダリングが簡単だった銀行は、チェーンの2番目のリンクとしてより長く役立つことを期待して大規模なギャングが顧客を狙うことを避けたため、詐欺の被害はさらに少なくなりました。  
これは、上記のセクション12.2.4で紹介した防止-検出-回復モデルの重要性を強調しています。  
  
2006年に、銀行はEMVに基づく2要素認証標準を発表し、これは翌年に開始されました。  
31は、EMV銀行カードを置くことができる携帯型パスワード計算機で構成されています。  
ログオンするためのワンタイムパスワードを取得したり、ログオンチャレンジに回答したり、通常は受取人の口座番号と金額から一連の数字を認証したりできます。  
 （これは、POSトランザクションに使用されるものとは異なります）  
応答コードは、切り捨てられたMACと切り捨てられたATCです。  
CAPリーダーを利用できるということは、ATMに行かなくてもCCTVで見られる危険なしに、カードを手に持っている強盗がPINを要求して確認できることを意味します。  
  
銀行は、部分的なパスワードの質問から初期の2要素認証スキームまで、さらに複雑な認証メカニズムを使用して単純なフィッシング攻撃を難しくしましたが、一部の悪意のある人は説得に一生懸命に取り組みました。  
他の悪者は、バンキングマルウェアの形で自動化に目を向けました。  
2011年までに、中間者攻撃がブラウザ内攻撃に発展しました：感染したPCのユーザーが銀行口座を使用しようとすると、ブラウザーマルウェアはトランザクションデータを積極的に変更して、見えないものにできるようになります。彼らが許可するものではありません。CAPを使用しない銀行は、代わりに専用の認証デバイス、または電話ベースの第2要素を使用する場合があります。  
12.7.4 2番目の要素としての電話  
確認を送るのは当然のことです、31これはそれを発明したマスターカードのブランド名です。 VISAはそれを動的パスコード認証（DPA）と呼んでいます  
例：「ロシアの不動産LLCに本当に7500ドルを送金したい場合は、ブラウザーで4716と入力してください。」これは、CAPと同じ利点があるように見えますが、ユーザーインターフェイスが優れています。  
ヨハネスブルグの詐欺師の一部は、孤児で脆弱な子供たちの世話をする慈善団体のCFOの電話番号用の新しいSIMを入手し、銀行口座からR90,460を盗みました[1514]。  
セクション3.4.1で説明したように、そのような詐欺は南アフリカからナイジェリアに広がり、2014年から5月頃に米国に広がり、そこで最初にInstagramアカウントを盗み、2018年からビットコイン取引所で人々のアカウントを略奪していました[1092] 。  
2019年の訴訟では、アリゾナ州ツーソンのAT＆T請負業者が、SIMスワップギャングが29人の犠牲者から200万ドルを盗むのを助けました[711]。  
脆弱性には、最近の呼び出しと最近の補充について尋ねることによる人々の認証が含まれ、どちらも攻撃者によって操作される可能性があります[1136]。  
何万ものカスタマーサービス担当者が不注意、ハッキング、SIMスワップギャングから賄賂を受け取る立場にあります。  
また、ドイツとイギリスでは、攻撃者がSS7シグナリングプロトコルを悪用してターゲットの携帯電話をリモートで盗聴し、その方法でコードを盗むケースもいくつかあります[489]（セクション22.1.3で詳しく説明します）。  
中国では、法律により、SIMを購入するには電話ショップに行き、IDを提示する必要があります。インドでは、生体認証チェックが必要であり、電話会社もSIMスワップ詐欺の責任を負います。  
しかし、この本の第2版で2007年に書いたように、「2チャネル認証は、そのセキュリティをチャネルの独立性に依存しています...  
つまり、それは普遍的なものになりつつあり、悪者はそれを破る際に多くの練習をしています。  
 マルウェアがあなたの電話をルート化した場合、それは両方のアプリを乗っ取り、あなたのアカウントを略奪するでしょうか？  
、欧州中央銀行は、ランタイムアプリケーション自己保護（RASP）を使用している限り、2つのアプリは問題ないと考えています。  
ソフトウェアのコピー保護のために1980年代に開発され、デジタル著作権管理のために1990年代に開発されたニーク。  
難読化スキームが解除されるまでにかかる時間を保証することは非常に困難です。いつでも中断が予想されなければならず、そのようなスキームのユーザーは、発生したときにすぐにパッチを適用する準備ができているべきです。  
したがって、キーを抽出したり、RASPメカニズム自体を壊したりする必要はないかもしれません。  
12.7.5責任  
オンラインバンキングへの突入により、多くの銀行は、消費者法や従来の銀行業務と矛盾して、顧客に詐欺のリスクを課す契約条件を採用するようになりました[277]。  
25か国で事業を展開している30の銀行の銀行詐欺の償還条件に関する調査では、多種多様なセキュリティアドバイスが示され、その多くはあいまいで、非現実的であり、さらには矛盾している[201]。  
また、銀行のURLは常に手動でブラウザに入力する必要があるなど、インターネットバンキングで最も煩わしい要求もありました。  
一方、銀行は、一方的な電話をかけた場合でも、セキュリティデータを公開するように顧客に指示するなど、ビジネスプラクティスによって脆弱になるように顧客を訓練しました。  
’あなたは彼らに道に迷うように言いたくてたまらないですが、もしそうした場合、支払いカードを再度有効にしたり交換したりするのは面倒です。  
 攻撃。  
  
承認済みのプッシュ支払い（APP）  
数字は2017年に収集され始め、33の英国の銀行は英国政府に第72条（2）に「必要に応じて」挿入しました  
ただし、総額は3億5430万ポンドで、リモートでの購入詐欺に次いで2番目であり、残りの合計を上回っています。  
もう1つは、脆弱な高齢者を対象とすることです。  
2日後、息子は訪問し、何が起こったのかを学びました。  
数日後、銀行B（「ミュール銀行」として評判が良かった）  
その犠牲者は幸運でした、しかし多くはそれほどではありませんでした。  
しかし、オンラインバンキングは即時支払いのシステムと組み合わされていたため、詐欺師は5桁、さらには6桁の金額で済むことができました。その結果、大規模な銀行振込を行うことは著しく複雑になりました。  
同様の詐欺も、企業に対して着実に増加しています。  
、彼らは現在、年間数十億ドルの損失を占めています[91]。  
博物館はディーラーを訴えましたが、負けました[506]。  
たとえば、英国の規制当局は銀行に受取人の確認を実装するように命令しました。最初に新しい口座に支払いを行うと、口座名義人の名前を尋ねられ、それが間違っている場合は警告されます[1361]。  
20世紀以来、企業が銀行からの直接支払いを利用してきたドイツでは、企業がレターヘッドに銀行口座番号を印刷することが法的要件でした。  
12.8ノンバンク支払い  
PayPalは、ドットコムブームの時期に出現した多くの電子メールベースの決済サービスプロバイダーの存続者であり、現在では伝統的および新規の決済サービスのポートフォリオを備えた銀行に成長しています。  
彼らは、ビクトリア朝の電信ネットワークで成長したウエスタンユニオン、および低コストの外国為替取引を提供するより近代的な決済サービスプロバイダーと競争します。  
ウエスタンユニオンは、犯罪者が多くの支店のいずれかに送金し、現金で引き出すことができるため、法執行機関にとって特に問題です。  
ビットコインなどの暗号通貨もありますが、一部の規制当局は現在電子マネー規制を免除しており、高度暗号技術の章で説明します。  
  
M-Pesaは、ボーダフォンが2007年に立ち上げたケニアの携帯電話バンキングサービスです。  
200を超える同様のサービスが後発開発途上国で開始され、そのうちの約20で変革を遂げています。現在最大のそのようなサービスはバングラデシュのB-Kashかもしれません。  
M-Pesaは、ナイロビとモンバサの移民労働者が田舎の親戚に家にお金を送る手段として使われるようになりました。  
携帯電話が普及すると、人々は価値を転送する手段として通信時間を購入し始め、そこから実際の価値を転送する小さなステップがありました。  
重要な成功要因は、電話会社が、現金をデジタルクレジットに変換し、また元に戻すことができる数万の販売代理店のネットワークを構築したことです。これは、レガシー銀行とは異なり、最も小さな村に到達するネットワークです。  
  
他の多くの国には、電話による支払いシステムがあるか、電話でかなりうまく機能する広く使用されている独自の支払いシステムがあります。  
2013年まで、これは世界をリードする電話決済システムでした。  
TencentのWeChat Payがすぐ後に続きます。 2020年には、中国のモバイル決済市場のそれぞれ54％と39％を占めていました。  
それらは中国のデフォルトの支払いメカニズムになっており、視覚的な支払いチャネルを使用しています。販売者は、顧客が適切な金額を適切なアカウントに送信するためにスキャンするQRコードを表示します。  
これは、セクション2.2.2で説明した情報主権に対する中国のアプローチと一致しています。  
インドのUPIには、国のAadhaar生体認証カードにリンクされた低コストの電話決済システムもあります。これらの国の支払い層とアイデンティティ層には、いくつかの競合する支払いアプリがあります。  
12.8.3 Sofort、およびオープンバンキング  
1つのアプローチは、ウェブサイトから商品を注文し、販売者の銀行口座の詳細と取引参照番号を取得し、銀行に行って支払い、翌日販売者のウェブサイトに戻って支払いの詳細を入力することでした。  
たとえば、飛行機のチケットを購入するには、「ソフォート」（「即時」）をクリックします  
その後、Sofortはあなたとして銀行にログオンし、銀行の認証チャレンジを提示します。  
次に、航空会社にリダイレクトし、チケットを取得します[79]。  
。  
彼らはドイツ連邦反トラスト局が銀行の利用規約が競争を妨害し、Sofortのような新しいビジネスモデルを除外するように設計されていると主張した後に敗北しました。  
その結果は、EUの2番目の決済サービス指令（PSD2）でした。  
2018年1月以降、銀行は、顧客が要求した場合に標準形式の取引データを他の規制金融機関にリリースするだけでなく、他の機関が顧客のように行動できるようにすることで、システムを開放する必要があります。欠点は、詐欺やマネーロンダリングが銀行口座を開くように急速に移行していることです。  
結局のところ、詐欺やマネーロンダリングに対する従来の制御は、はるかに効果が少なくなるということです。  
私たちは、これがどのように発展するかを待つ必要があります。  
販売者は、顧客が支払い手段をQRコードとして提示するのと同様に、この方法で支払い要求を提示できるため、顧客の電話でオンライン銀行支払いを開始できます。  
ここには革新と収束の余地があるかもしれないので、それがどのように発展するかを待つ必要があります。  
12.9まとめ  
簿記は、機密性ではなく信頼性と説明責任を重視するシステムの成熟した例を示しています。  
実際にうまく機能させることは、高度な機能分離を意味し、その設計には多くの分野からの入力が含まれます。  
支払いシステムは、第1世代のATMシステムでの使用を通じて、暗号の開発において重要な役割を果たしました。スマートカードベースの支払いの採用により、不正の状況は再び変わりました。  
これらは、ハイテクと狡猾さの可能な組み合わせを徐々に探求しており、詐欺緩和への全体論的アプローチの重要性を教えています。  
34Open Bankingは、古いISO 8583標準から新しいISO 20022への移行を意味します。  
研究上の問題私は常に、大きな会計事務所のカルテルを信用していませんでした。1980年代のビッグエイトから現在はビッグフォーまで、3つの合併とエンロンスキャンダルでのアーサーアンダーソンの失敗に続いています。  
その後、私が運営機関または監査委員会に参加したときは、地元の会社を使用することを常に提案しました。それは安価でしたが、変更を得ることができたのは一度だけでした（そして、それは大きな会社から別の会社へ）。  
私が大学の統治機関に勤務したとき、私はこのカルテルに1年間100万人も身を震わせ、見返りに何も提供しないことに我慢しなければなりませんでした。ほとんどの作業はジュニアによって行われました。  
英国政府はそのスキャンダル（そして他の多くの）の後でまだ決定しました  
それがうまくいけば素晴らしいですが、この章で分析されている内部統制の問題か、セクション28.1で取り組む保証の問題かにかかわらず、それがこの本で説明されているほとんどの具体的な問題にどのように影響するかはわかりません。  
よりよく理解する必要があります。  
多くのセキュリティ障害は、両方のユーザー（デフォルトとして危険な選択肢が提供されている）のレベルでのユーザビリティの低下に起因します。  
ので、多くの内部統制の失敗は、実際の組織で実際に使用できるようにするのではなく、監査人の快適さのために設計された管理メカニズムに起因しています。  
 決済システムはかつて非常に保守的であり、1970年代から多くの点でほとんど変更されておらず、メカニズムがATMやHSMからチップカードや携帯電話の暗号化チップに移行するにつれて、絶えず進化しています。  
 と環境の変化（オープンバンキングと同様）  
そのような変化に直面して回復力を維持するには、仕事が必要です。  
アカウントの乗っ取りがますます広がるようになるとしたら、どのような影響がありますか？  
経営幹部が詐欺師であるか、会社が破産している間に取引しているかを検出するのにほとんど役に立たないのに、ほとんどの大企業や大規模大学でさえ、有名だが高価な企業を選ぶのはなぜですか？  
しかし、私たちは何をすべきでしょうか？  
 支払いの速度とファイナリティーを支払者と受取人の両方の既知の立場の関数にするなど、いくつかのスマートな組み合わせはありますか？  
 2020年初頭の状況は、低金利と競争の激化により、リテールバンクは以前よりも収益が少ないため、銀行のセキュリティエンジニアはより少ないリソースでより多くのことを行うよう求められています。  
そのようなインセンティブは、ものをクラウドに移動する方向に押し上げますが、これはさらに問題を引き起こします。クラウドHSMについては、高度な暗号工学の章で後ほど説明します。  
ビデオ会議は、ローンなどの複雑で高額な取引のために、支店内の会議を置き換える必要があります。  
ほかに何か？  
国際決済銀行から利用可能な支払いシステムに関する多くの論文がありますが、私は2020年7月にプレスに行き、サービスの品質とヨーロッパ内での支払いの大部分は30分未満ですが、複数の仲介業者、営業時間、タイムゾーン、資本管理、流動性、古代のテクノロジーの組み合わせにより、アジアとアフリカへの支払いには数時間から数日かかる可能性があると指摘しています[162]。このトピックについては、パート3で再度取り上げます。  
ATM PINを生成および保護するIBMシステムは、[521]や[951]などの多くの記事で説明されており、初期のATMネットワークは[763]で説明されています。  
地下市場の最初の調査は、2007年にJason Franklin、Vern Paxson、Adrian Perrig、およびStefan Savageによって行われました[714]。それでも、焦点は麻薬やマルウェアではなく銀行詐欺にありました。  
同僚と私は、2012年[90]および2019年[91]のサイバー犯罪の大規模な調査に貢献しています。  
大規模なカード詐欺の信頼できるケーススタディについては、テスコ銀行に対するFCAの2018年の判決[687]を参照してください。  
最後に、テロ資金に対する米国の諜報イニシアチブの政治的および法的歴史と、秘密または法的手段によってSWIFTデータを取得するための取り組みについては、David Bullochの論文[341]を参照してください。