アザラシは、そのブリーフケースを携行している人と同じくらい優れています。  
– MARC WEBER TOBIAS  
  
多くのコンピューターシステムは、保護の重要な側面を保証するために、安全な印刷、パッケージング、シールにある程度依存しています。  
シールと不正開封防止パッケージは、一般的に信頼できる配布に役立ちます。つまり、製品が工場から出荷されてから改ざんされていないことをユーザーに保証します。  
暗号がどれほど洗練されていても、アザラシの敗北はシステムの敗北となります。  
エンジニアをホスティングセンターに入れる前にエンジニアのIDを精査している場合は、IDを目で見て、電子的に読み取ることをお勧めします。  
•一般的に、認証情報を改ざん防止するよりも改ざん証拠を改ざんするほうが現実的な目標かもしれません。誰かがスマートカードを解体してキーを取り出した場合、詳細な試験に合格するものに再構築することはできません。  
これらの印刷およびシーリングテクノロジーの直接的な応用とは別に、現代のカラースキャナーとプリンターを使用して良好な偽造品を簡単に作成できることで、新たな可能性が開かれました。  
これらには、偽造に使用されている対応スキャナーおよびプリンターを停止する透かし、および自動販売機で偽造を検出できるようにすることができる目に見えない著作権マークが含まれます[830]。  
そのため、デジタルの世界と「面白いインク」の世界はますます近づいています。  
16.2歴史  
銀行システムに関する章では、メソポタミアの新石器時代の倉庫管理者が農産物の領収書として使用した粘土板、つまり水疱が簿記システムの起源である方法について説明しました。  
古代地中海と中国では、印鑑が文書の認証に使用されました。  
 [825]。  
19世紀まで、手紙は封筒には入れられず、何度も折り重ねられ、ホットワックスと印鑑リングを使って封印されました。  
その他、以前の重要性の痕跡は、重要な文書に貼られた会社の印鑑と公証人の印鑑、および一部の国の国家元首が法律のアーカイブコピーに適用する国の印章、および一部のヨーロッパ諸国での電子署名の要求において存続します。 -EUのeIDAS規格に準拠する性質。  
ゆるい商品からパッケージ商品への移行、およびブランドの重要性の高まりにより、品質管理が向上する可能性だけでなく、悪意のある人々が商品を改ざんする可能性のある脆弱性も生まれました。  
これにより、多くのメーカーが製品を不正開封防止に向けることができました。  
これは、香水やたばこから航空機用スペアパーツ、医薬品に至るまで、高価値のブランド品の偽造を防止するためのはるかに大きな市場の一部にすぎませんでした。  
残念ながら、ほとんどのアザラシはまだかなり簡単に倒せます。  
したがって、最初にセキュリティ印刷を検討する必要があります。  
  
1800年代初頭のナポレオンによるヨーロッパへの紙幣の導入、および無記名証券やパスポートなどのその他の貴重な文書の導入は、捕食者と被食者の共進化の特徴の多くを示すセキュリティプリンターと偽造者の間の戦いを開始しました。  
 攻撃者を助け、次にカラー印刷とスチールエッチング（1850年代）  
近年、カラー複写機と安価なスキャナーは、ホログラムや他の光学的可変デバイスによって対抗されてきました。  
時々、紙幣の設計者は、タイタニックエフェクトに屈して、最新のテクノロジーを信じすぎて、特定のトリックにあまりにも多くの信頼を置いています。  
これらのノートには、ウィンドウスレッドがあります。これは、幅1 mm程度で、8 mmごとに紙の表面に届く、紙を貫通する金属ストリップです。  
これを複製するのは難しいと考えられていました。  
彼らは安価なホットスタンピングプロセスを使用して紙の表面に金属ストリップを置き、次に白いインクを使用してその上に固体バーのパターンを印刷して、予想される金属パターンを見えるようにしました。  
英国の紙幣は現在、オーストラリアで先駆的なプロセスであるプラスチックに移行されています。  
16.3.1脅威モデル  
大まかに言って、脅威は主要な組織（ある国が別の紙幣を偽造しようとしているなど）からのものである可能性があります。、自宅やオフィスにある機器を使用するアマチュアに。  
多くの紙幣の高品質の偽造品を製造する方法についての知識が印刷業界で広まっていましたが、これはプロの偽造品のレベルを高めると考えられていたかもしれません。  
アマチュアは以前は軽微な迷惑であると考えられていましたが、1997年または1998年以降、アメリカで発見された偽造のほとんどを占めてきました。  
彼らが作成した紙幣は、銀行の窓口を通過するには十分でないことがよくありますが、暗くて騒々しいナイトクラブなどの場所で発声されます。  
一次検査は、一般の人や店の新しいレジ係など、訓練を受けていない経験の浅い人が行う検査です。  
少し怪しげな感じの紙幣を受け取った場合、共犯者になるか、それとも報告する手間をかけるかを判断するのに十分なほど注意深く見ずに、紙幣を渡そうとします。 2。  
この人は、紫外線ランプ、化学試薬を備えたペン、さらにはスキャナーとPCなどの特別な機器を持っている場合があります。  
3次検査とは、製造業者の研究所または紙幣発行銀行で行われる検査です。  
 充実した設備とサポートを用意します。  
一次検査を過ぎて偽造品を入手することは通常簡単ですが、製品と検査プロセスが適切に設計されている場合、三次検査を過ぎてそれを入手することは通常不可能です。  
現場の副検査官がどのような偽造品を検出できるかについての主な制限は、必要な機器の大きさとコストに関係しています。  
16.3.2セキュリティ印刷技術  
これは紙幣やパスポートのスクロール作業によく使用されます。 •凸版は、インクが隆起したタイプに転がり、次にページに押し付けられ、くぼみを残します。  
したがって、表面と裏面の印刷を正確に調整できます。パターンを前面と背面の一部に印刷できるので、ノートをライトに近づけると完全に一致します（シースルーレジスタ）。  
これを再現することは、安価なカラー印刷装置では難しいと考えられています。  
; •文書の裏書き、または写真の封印に使用されるゴム印。 •写真のシールや、偽造のコストを押し上げるための銀行カードにも使用されるエンボス加工とラミネート。  
それらは、製造時に厚みを変えることにより、紙に挿入されるより半透明な領域です。  
•オーストラリアで最初に導入された最新のプラスチック製のメモでは、さまざまな機能をシースルーウィンドウに埋め込むことができます。 •視野角に応じて緑色から金色に変化する光学的に変化するインク。 •磁気、フォトクロミック、またはサーモクロミックの特性を持つインク。 •拡大鏡を必要とする米国の紙幣へのマイクロ印刷、紫外線、赤外線、または磁気インクでの印刷など、特別な機器でのみ表示される印刷機能（これらの最後のものは米国の紙幣の黒印刷で使用されます）  
ホログラムは通常、光学的に生成され、フィルムの背後にある固体のオブジェクトのように見えますが、キネグラムはコンピュータによって生成され、わずかに異なる角度からいくつかの驚くほど異なるビューを表示することがあります。 •ディテールなどのスクリーントラップは適切にスキャンするには暗すぎ、適切なサイズのディテールを含むエイリアスバンド構造は、一般的なスキャナーやコピー機のドット分離で干渉効果を形成します。 •デジタル著作権マーク。フーリエ変換を直接マイクロプリントすることによって隠された画像から、カラーコピー機、スキャナー、またはプリンターによって認識されて停止させる独自のスペクトラム拡散信号までさまざまです。  
100ドルの法案の設計については、[1367]を参照してください。また、どの特徴がどの証拠を提供するかを分析した偽造紙幣の研究については、[1936]を参照してください。  
古い手法の多く、および新しい手法のいくつかは、一次検査に合格する方法で模倣できます。  
。  
1988年にシェイクスピアーのホログラムが英国の銀行カードに導入されたとき、私は銀行の代表として工場を訪れ、業界が第2の供給源を要求していたため、予備のプレートセットを大規模なセキュリティ印刷会社–そして、彼らのこの競合他社は、許容できるホイルを製造することはまったくできませんでした。。  
 しかし、7年後にシンガポールを訪れたとき、私は同様の（しかしより大きな）を購入しました  
これは明らかに、彼が望めば英国の銀行カードを偽造できるというメーカーの自慢でした。  
ポリマー紙幣が英国に導入されたとき、2016年には5ポンド紙幣、2017年には10ポンド紙幣が導入されました。  
ある被害者は、「近くを見るとビッグベンが欠けていて、シリアル番号の一部と女王の顔が剥がれているのがわかりました。  
その年の後半には、2020年までに正式な20ポンド紙幣の発売が予定されていなかったにもかかわらず、進取的な悪者たちは20ポンド紙幣を手放していました。  
1つの防御が完全に打ち負かされた場合（金属箔の機械的なコピーを作成することが容易になる場合など）  
。  
保護、美学、堅牢性の間には複雑なトレードオフがあり、ビジネスの焦点も変化する可能性があります。  
ドキュメントを適切に検討するように人々を訓練することの難しさについて手書きで書くことに多くの時間が費やされ、大ざっぱなものなどの製品の一般的なユーザーが実際にそれが許容できるかどうかを無意識のうちに決定する方法を研究することに十分な注意が払われなかった。  
ここまでの教訓は[1935]です。•セキュリティ機能は、製品に関連するメッセージを伝える必要があります。  
紙幣のコミュニティは、セキュリティのユーザビリティに多くの注意を払ってきた、私たちの貿易の数少ない専門分野の1つであるため、この作業はより幅広い注目に値します。  
 パスポートなど、紙幣以外の書類については、国の政治環境や、それが使用される社会の慣習に関する問題もあります[1293]。  
紙幣の場合、理論では、公には宣伝されない20の機能を備えた紙幣を設計することになります。  
やがて、これらは偽造者に知られるようになります。  
最終的に、それらがすべて公開されると、そのノートは発行が中止され、置き換えられます。  
自動販売機を盗んで解体し、ソフトウェアを読み取って、現在使用されている小切手の完全かつ正確な説明を得る泥棒。  
したがって、中央銀行が製造業者に第2レベルの電子透かし（またはその他）の秘密の多項式を伝えるとき  
したがって、障害は手動システムの場合よりも突然かつ完全になる可能性があり、機能の寿命、死亡、および再生のサイクルは、以前よりも速く変わります。  
製品のパッケージ化では、典型的なビジネスモデルは、フォージェリーのサンプルが発見されて実験室に運ばれ、そこで科学者がそれらの違いを発見することです。おそらくホログラムが正しくない可能性があります。  
これらのキットがかさばって高価である場合、設置できるキットの数は少なくなります。  
プラスチック製品のシュリンクラップに個々の微視的な紫外線バーコードを印刷するなどのアイデアは、検証に必要な顕微鏡、ラップトップ、およびオンライン接続のコストが原因で失敗することがよくあります。  
金融商品、特に小切手では、改ざんはコピーや偽造よりもはるかに大きな問題です。  
被害者は正当に小切手を発送しますが、小切手ははるかに大量に変更され、すぐに入手できる家庭用溶剤を使用することがよくあります。  
しかし、レーザープリンターのトナー（およびタイプライターの修正リボンなどの簡単なもの）を取り除くためのトリックのため、保護は完全ではありません。  
進取的な悪意者の1人は、インクを簡単に取り外せるように特別に選択されたペンを被害者に見せました[8]。  
これは非常に大量の場合を除いて精査を不可能にします。  
ただし、手書きの署名では、許容可能なエラー率での自動検証は最新技術を超えています（セクション17.2で説明します）。  
企業の将来は、支払いを銀行振込に移行することです。ここでの早期採用者であるドイツは、2000年代初頭までに小切手詐欺を大幅に抑制しました。  
もちろん、ドキュメントの変更は銀行の問題だけではありません。  
名前の変更、写真の置き換え、またはページの追加と削除。  
  
サプライチェーンのセキュリティには、パッケージングとシールの問題が含まれます。  
用途は、医薬品から貨物コンテナ、投票箱までさまざまです。  
  
一部のシステムは、基板材料にランダムな変動を追加します。これらはスウェーデンの銀行カード、韓国のテレホンカード、​​私の大学の一部の建物の入国管理カードで使用されていました。  
多くの武器や素材には独特の表面があります。紙の表面については、例として図16.1を参照してください。  
パターンはレーザースペックル技術を使用して測定され、ログに記録されるか、機械読み取り可能なデジタル署名としてデバイスに添付されます[1749]。  
レーザースペックルを使用して紙を認証し、表面の粗さを折り目、乾燥、落書き、さらには焼けに強いコードにエンコードすることもできます[332]。  
  
タグの一意性はその製造の副作用である可能性がありますが、ほとんどのシールは、セキュリティ印刷されたタグをターゲットオブジェクトに固定することによって機能します。  
不正開封防止パッケージの特定のケースでは、取り付けは工業プロセスの一部です。それは、ポップアップボタンまたはブレークオフ蓋付きの加圧容器である可能性があります。  
 引き離した。  
ただし、ほとんどの製品では、実装はかなり貧弱です。  
鋭利なナイフを取り、セルフシールの封筒に入ってくる次のいくつかの文字を試します。  
しかし、この期待される改ざんの証拠は、通常、人々が封筒のフラップを身体から引き戻すことによってそれらを開くことを前提としています。  
（一部の接着剤は、最初にヘアドライヤーを使用して柔らかくするか、または凍結により壊れやすくする必要があります。）  
どちらの方法でも、慎重に調べたときにわずかにしわくちゃに見える封筒が得られるでしょう。  
この攻撃は通常、一次検査に対して機能し、おそらく三次検査に失敗し、二次検査に合格する可能性があります。とにかくポストでしわが発生します。  
悪名高い例は、スイスとオーストリアで使用されているビネット、または高速道路通行料ステッカーです。  
フロントガラスからステッカーを剥がして別の車で使用する場合、フロントガラスにくっつくインクと一部のインクが付属します。  
これは現在犯罪になっており、あなたが捕まった場合[1468]に罰金が科せられます。  
16.4.3 PINメーラー  
昔は、PINメーラーはマルチパートのステーショナリーとインパクトプリンターを使用していました。封筒を開封し、PINが押されていた伝票を引き出すと、PINが手に入ります。  
アイデアは、目に見える証拠を残さずにアザラシを移動することができないのと同じように、この文房具では、目に見える証拠を残さずに秘密を抽出することはできないということです。  
フィルムの後ろには、紙のダイカットタブがあり、背景を覆い隠してPINを表示できます。  
初期の製品は、それらを光にかざすことで読み取ることができるため、光は約10度の角度で表面から見えました。不透明なトナーは、光沢のある接着フィルムに対してはっきりと現れました。  
もう1つは熱伝達でした。メーラーの上に白紙を置き、アイロンをかけます。  
この研究は2004年に銀行業界に報告され、最終的に2005年に発表された[284]。  
それでも今日まで、PINが読みやすいメーラーを入手しています。  
詐欺師は、新しい銀行カードを受け取っていることを知っていて、郵便物を盗むことができる場合、カードとPINの両方を手に入れます。  
家族が誤ってPINを学習するのを妨げることがあります。同様に、タブを引き裂かずにPINを読み取り、多額のお金を引き出して、それをしなかったと主張する顧客がたまにあるかもしれません。メーラー。  
このような動作の原動力はおそらくコンプライアンスです。インパクトプリンターの時代に進化したカードスキームルール、監査手順、保険検査を再考するのは面倒です。  
16.5全身の脆弱性  
地元のプールでは、混雑時にはリストバンドを付けた水泳選手を出して混雑を管理しています。  
バンドはワックス紙でできています。  
（一部の空港で使用されている手荷物シールに似ています。）  
お金をかけたくない場合は、各バンドを使用できます。図16.2：–ローカルスイミングプールのリストバンドシールを一度、別の方向から交互に引っ張って、穏やかに外し、写真のようになります。  
重要なのは、シールを2度固定することによってシールに加えられた損傷は、単純なユーザーが1度固定した場合の影響と簡単に区別できないことです。それにもかかわらず、リストバンドシールは目的に完全に適合しています。  
また、シーズンチケットも購入しているので、いつでも外に出て新しいリストバンドを入手できます。  
顧客は敵です。シールを貼るのはお客様です。シールの再利用の効果は、ランダムな破損の効果と区別がつきません。未使用のシールは市場で購入できます。偽造シールも低コストで製造できます。効果的な検査は不可能です。  
   
軍事システムでは、敵は不忠実な兵士、またはあなたの装備を妨害しようとする反対側の特殊部隊です。  
投票機では、ほとんどの攻撃は選挙当局から行われます。  
典型的なビジネスアプリケーションは、会社がその製品の一部の製造を下請けする場合であり、請負業者が合意したよりも多くの商品を生産することを恐れています。  
そのような詐欺を検出することさえ-それらを法廷に証明することは言うまでもなく-難しい場合があります。  
これらの材料の一部には、シリアル番号がさまざまな方法で埋め込まれている場合があります（ボトルガラスへのレーザー彫刻、UV光の下でのみ表示されるインクを使用したセロハンへの印刷など）  
メーカーのフィールドエージェントがショップでランダムに購入したサンプルのシリアル番号を確認できるオンラインサービスが存在する場合や、パッケージにデジタル署名があり、すべてのさまざまなシリアル番号をリンクしてオフラインチェックを行う場合があります。  
時々、ブランド所有者自身が悪人である場合があります。ブドウ園が誤ってヴィンテージとラベルを付けた場合、実際に買い取られたブレンドされたブドウから作られた追加の1000ケースのワインです。  
シーリングメカニズムは通常、補完的な制御プロセスを念頭に置いて設計する必要があります。  
正規品であると信じて、グレーマーケットで偽造品を購入した販売業者は、犯罪者の意図なしに検査官を騙そうとする可能性があります。  
また、ディストリビューターは完全に暗闇の中にいる可能性があります。偽造品を売っているのは彼のスタッフかもしれない。  
航空会社の倉庫（および飛行機が着陸した後の免税カート）の在庫  
したがって、通常はエージェントが外に出てサンプルを購入することが不可欠であり、密閉メカニズムがこれをサポートする必要があります。  
16.5.2ガンデッキング対策  
セクション14.3.2.2で、トラックスピードリミッターシステムでは、ギアボックスセンサーは、特別なトングで所定の位置に圧着されたリードディスクで校正用ガレージがシールする1本のワイヤーを使用して固定される方法について説明しました。  
これは、アマチュアの彫刻家のクラスに行くよりも簡単なので、アザラシのキャストを取り、ブロンズから一対のシーリングトングを鍛造できます。  
一部の空港では、チェックインキューの近くにある機械を使用してX線検査をした後、受託手荷物にテープシールが貼られています。  
とにかく、空港のセキュリティはとにかくほとんど劇場です。  
大きな問題の1つは、シールを検査することになっているスタッフが実際に検査したかどうかを確認することです。  
したがって、港に到着する何千もの輸送用コンテナのシールを検査することがタスクである場合、スタッフが実際に各コンテナを確認することをどのように保証しますか？  
次に、検査官のタスクは、すべてのインバウンドコンテナーを訪問し、それらが表示する番号を記録することです。  
検査官がいずれかのコンテナから有効なシールコードを返さなかった場合、それが原因かどうかにかかわらず、何かが間違っていることがわかります。  
不注意と腐敗が相互作用します。  
  
完全に無害な理由でシールが破れる可能性がある場合にも、同様の影響があります。  
（トラックの運転手はこれを知っています。）  
彼はそれをテープで留めて、正面から「間違った住所に配送されました」と書き直してもいいでしょう。  
保護目標が製品の大規模な偽造を防止することである場合、偶発的な破損は問題にならない可能性があります。しかし、それが訴追を支援することである場合、自然発生的な封印の失敗は深刻な問題になる可能性があります。  
 値。  
そこで、タグベンダーは自社製品の改ざん防止について壮大なマーケティングの主張をしましたが、法廷で異議を申し立てられたときに、抗弁者によるテストのためにサンプルを提供することを拒否しました。  
  
もう1つの一般的な脆弱性は、シーリング材の供給が管理されていないことです。  
英国では、これらは通常、特別なペンチに挿入され、重要な文書を圧着するために使用された2つの金属エンボスプレートで構成されています。「Microsoft Corporation」のシールを注文するのは少し危険かもしれませんが、あまり知られていないほとんどすべてのターゲットに対してシールを作成するのは簡単です。あなたがしなければならないことは、法律に由来するように見える手紙を書くことだけです。しっかり。  
より深刻な例は、製薬業界がブリスターパックに依存していることであり、ホログラムやカラーシフトインクが追加されていることもあります。  
または、開封時に引き裂くように設計されている宅配業者が使用しているプラ​​スチック製の封筒を検討してください。  
また、サムネイルをこすって磨き落とした粘着テープでフラップを補強した場合、警察とセキュリティサービスが封筒を跡形もなく開くことができないことも「都市の神話」です（最近、銀行から書類を受け取ったこの方法で密封されます）  
これは完全に信じられないことです–警察の研究所がセロテープの接着剤用の魔法の溶剤を発明していなかったとしても、19世紀のツァリスト警察はすでにフォークの棒を使って封をした封筒の中に手紙を巻き取り、引き出して読んでから入れられるようにしました戻る[1001];そこに、そして実際にヨーロッパ中の手紙作家はレターロックを使用しました-彼らが望んでいた改ざん、スリットとシールの複雑なシステムは改ざんを明白にするでしょう[366]。  
会社のロゴが入った封筒を簡単にスキャンし、安価なカラープリンターを使用して複製できることを考えると、これらの前提条件はかなり野心的です。  
これにより、偽造者の仕事がはるかに簡単になります。  
16.5.5正しいものを保護しない  
1980年代後半、銀行が磁気ストリップを読み取る認証端末を導入したため、クレジットカードは偽造に対して脆弱になりました。一方、ほとんどの業者が顧客に署名するためのバウチャーを印刷するために使用したインプリンティングマシンはエンボス加工を使用し、ほとんどの業者は署名済みの銀行に署名しましたまるで小切手であるかのような伝票。  
部分的な変更を伴う攻撃もあります。  
銀行がクレジットカード番号を生成するために使用したアルゴリズムがわかっていた場合、これはカードの残りの部分を平坦化、再印刷、および再エンボス加工するだけであり、これは安価な機器で実行できました。  
いずれにせよ、ホログラムはすべて「これはかつて有効だったカード」であり、ほとんどの銀行は現在それを廃止しています。  
ただし、保護対策を選択するときは、脅威モデルについて非常に明確にする必要があります。それは、偽造、改変、複製、シミュレーション、転換、希釈、置換、または他の何かですか？  
本当に必要なのはタンパーセンシングメンブレンです。これは、小さな侵入でも目に見えて不可逆的に反応します。  
改ざん防止に関する章でそれらについて説明します）。  
16.5.6検査の費用と性質  
新しい紙幣が導入されるとき、それは銀行家にとって心配です。新しい紙幣に誰もが慣れるまでの数週間は、偽造者にとっては大変なことです。  
比較のための本物のサンプルのサンプルがなければ、検査は多かれ少なかれ一次レベルに限定されるので、偽造は簡単です。  
詐欺師は、（発展途上国だけでなく）不正な手段で本物のパスポートとIDカードを頻繁に入手します。  
2006年3月にサンタバーバラで開催された第7回セキュリティシールシンポジウムで、ソニアトルヒージョがやや衝撃的な実験を行いました。  
各被験者は、改ざんされたと思った10製品のうち3製品を正確に選択するように求められました。  
専門家でさえ改ざんを検出できない場合、改ざんが行われていると言われたとしても、平均的な消費者はどのような可能性を持っていますか？  
不正開封防止パッケージの主な目的は、顧客を安心させることです。二次的な目的には、製品の返品、デューデリジェンスの最小化、審査員の賞の規模の縮小が含まれます。  
高級品メーカーのように偽造を真剣に受け止める企業は、紙幣印刷業者が開拓した技術の多くを採用しています。  
親しみやすさは重要です。地元のお金など、頻繁に扱うものに対して「感触」を覚えますが、ファンシーな化粧品や高価なワインのボトルなど、めったに見ないパッケージに問題があることに気づくことはほとんどありません。  
一部の製品はこの目的のために電子機器を取得していますが、すでに電子機器を持っている他の製品はwifiチップを取得しています。これらの番号をRFIDチップで非表示にする代わりに、ベンダーは製品のラベルに番号を印刷できます。また、正規の製品を入手したかどうかを心配している人は、電話で確認することができます。  
たとえば、マイクロソフトが最初にスパイウェア対策ベータを出荷したとき、私はそれを家族のPCにインストールしました。そのPCはWindowsのコピーがすぐに悪であると非難されました。  
私は特に彼らの最初の交渉の立場、つまり私は彼らにもっとお金を送るべきだということを好きではありませんでした。  
しかし、その後、別のWindowsマシンを購入しませんでした。  
16.6評価方法  
単に尋ねるのではなく、「明白なもの以外の方法でシールを取り除くことはできますか？  
尋ねられるべきいくつかの質問は次のとおりです。•アザラシが偽造されている場合、誰がそれを発見することになっていますか？  
 ベンダーは適切な実験を行って、誤った受け入れ率と誤った拒否率を確立しましたか？  
 そして、これらの検査官（公共または専門家）は、欠陥を見つけて報告する動機はどの程度ありますか？  
 とにかく、敗北とは何か–証拠価値の改ざん、偽造、改ざん、侵食、または商業的信頼性に対する「PR」攻撃？  
 •フィールドでの期間はどれくらいですか。進歩によって敗北が大幅に容易になる可能性はどのくらいありますか。  
 •シールを貼る人は不注意または腐敗しますか。その場合、どのように対処しますか。  
 製品の？  
 汚れ、油、騒音、振動、洗浄、製造上の欠陥の影響についてはどうですか？  
 または、そのようなことが起こった場合、目に見える形で応答するはずですか？  
 •法廷に行く予定の場合、あなた自身（またはベンダー）以外の専門家がいますか  
 答えが「いいえ」の場合、これは良いことですか、悪いことですか？  
 裁判官は彼女を公正な裁判の根拠で解雇しますか-あなたの技術的主張に反論することは彼女が解任する証拠の不可能な負担になるでしょうか？  
 •製品を使用したら、シールはどのように処分されますか？誰かがゴミから古いシールをいくつか回収した場合、気になりませんか？  
ですから、アザラシを申請して確認する人が、忠実かつ効果的に仕事をするかどうかをよく考えてください。動機、機会、スキル、監査、説明責任を分析します。  
 または腐敗しやすい人（トラック会社の事業に勝つことを熱望しているガレージなど）  
最後に、シールの失敗と検査エラー率の起こり得る結果について、クライアント企業とその反対者の観点からだけでなく、無実のシステムユーザーと法的証拠の観点からも検討してください。  
これについてはパートIIIで詳しく説明します。  
16.7まとめ  
。  
シールはセキュリティ印刷に依存することが多く、これについてはほぼ同様のコメントが可能です。  
間違いなく、ナノ粒子から磁性流体、DNAまで、製品の安全性と偽造品の検出のために多くの豪華な新技術が売りに出されるでしょう。しかし、市場が破壊され、システムレベルの問題が無視される限り、彼らは何をするでしょうか？  
 自動検査システムは一方向に進むかもしれません。  
ワクチンなどの一部の製品は、40℃未満に保つ必要があり、温度を監視して障害を特定できるようにするコンテナまたはパレットにロガーが同梱されて出荷されています。  
製薬などの安全が重要な製品を使用する規制産業は、新しいアイデアを試すのに適した場所です。  
偽造品や毒物製品のほとんどは小売レベルで導入され、以前は高度に分散されていました。  
その市場とフルフィルメントサービスは、多くの偽造製品、および政府機関によって安全でないと宣言された製品の流通チャネルで最も懸念されていると報告されており、危険なレベルを含む子供のおもちゃを含む規制当局によって一見ラベル付けされているか禁止されています鉛の[591]。  
おそらく、それはスケールの必然的な影響でしょう。誰もがFacebookにいる場合、それには世界中のゾッと、いじめっ子、過激派が含まれます。また、世界中のすべての商人がアマゾンを使用して製品を出荷する場合、同様のことが期待できます。  
しかし、法律は通常、テクノロジーに15年ほど遅れており、その間も安全な印刷と封印は継続します。ただし、オンライン製品登録への移行が続いています。これは非常に重要な背景資料です。  
。  
独立から南北戦争まで、アメリカ人は政府ではなく民間銀行が発行した紙幣を使用し、偽造が蔓延しました。  
最近、Supernoteの論争がありました。  
米国政府は北朝鮮を偽造したと非難し、これを使用して制裁を課しました。他の人たちは、紙幣は現金の流れを追跡するためにCIAによって作成された可能性が高いと示唆しました。  
それらは、マネーセンターの銀行が使用する計数機以外のすべての検査に合格するように注意深く設計されていました。そして、出来上がったボリュームは、偽造者が生産するよりも少なくとも1桁少なく、設備の支払いのために生産する必要があったでしょう[622]。