持続可能性ソフトウェア設計を構築するには2つの方法があります。  
もう1つの方法は、複雑にして、明らかな欠陥がないようにすることです。  
私たちは何かが間違っているときにのみ報酬を受け取り、私たちはいつでも何か間違っているものを見つけることができます。  
–ウィンストンチャーチル  
この本では多くの資料を取り上げましたが、その一部はかなりトリッキーです。  
これらは保証の問題です-システムが機能するかどうか。その従順なコンプライアンス–これについて他の人々をどのように満足させるか。そして持続可能性–それがどれだけ長く働き続けるか。  
 どのようにしてセキュリティと安全のケースを保険会社に販売しますか？  
 2020年の新機能は持続可能性です。  
当時の重点はCommon Criteriaのようなテストおよび評価スキームにありました。  
保証はもはや静的ではありません。  
電話やラップトップなど、ソフトウェアが含まれていてオンラインだったものがありましたが、ソフトウェアは月に1回パッチが適用されるため、ある程度安全でした。  
今、私たちは車と医療機器をオンラインに置くことを始めたので、それらもオンラインでパッチを当てられなければなりません。  
前の章で説明したように、ソフトウェア開発ライフサイクルはDevOpsになり、次にDevSecOpsになりました。システムのオンラインコンポーネントは継続的な統合を使用して維持されますが、フィールドのコンポーネントは定期的なアップグレードが必要です。  
しかし、「十分」をどのように定義しますか？  
 あなたは間違ったものを守る人々にどのように対処しますか？  
 あまりにも多くのシステムは、アラートの経験豊富な専門家が使用するように設計されていますが、一般の人々には扱いが難しいか、エラーに耐えられません。  
10年前のセキュリティエンジニアリングでは、上司、クライアント、および（必要な場合）を説得するために証拠をどのようにまとめたかについての評価に関して、保証についてよく話しました。  
。  
Common Criteriaなどのサードパーティの評価スキームは、これらのリスクをより透明にして軽減するはずでしたが、特に公共部門や銀行などの規制された業界では、責任の盾として機能することになりました。  
評価はコンプライアンスによって推進されました。  
詳細は業界ごとに異なります。  
一般的なビジネスシステムには、Big Four監査会社によって設定されたポリシーと、PCIによる支払いシステムがあります。  
この本の冒頭の図1.1で、インセンティブ、ポリシー、メカニズム、および保証に基づいたセキュリティエンジニアリングのフレームワークを示しました。  
多くの場合、これらは正式な保証プロセスの範囲外ですが、セキュリティポリシーを定義する必要がある環境の最も重要な部分です。  
本のパートIIの多くをさまざまなアプリケーションのセキュリティポリシーの調査に費やしました。  
•保証とは、システムが特定の方法で失敗しない可能性の推定です。  
それは伝統的に評価についてでした–合意されたセキュリティポリシーとメカニズムの強さを考慮して、製品が正しく実装されたかどうか。  
 故障までの平均時間を定量化できますか？  
システムにパッチを適用する期間と勤勉さはどれくらいですか？  
ほとんどのシステム障害には重大な人間的要素があります。  
個々の製品にまたがっています。事故の一般的な理由は、製品ごとにユーザーインターフェースが異なることです。この問題については後で説明します。  
（いくつかの例外があります。簿記システムはエラーと詐欺の両方に対処するように設計されています。）  
多くの脆弱性は、セキュリティメカニズムが理解しにくい、または手に負えないために発生します。  
顧客とベンダーは、バリューチェーンの複数のポイントで異なるものを求めています。  
保証ゲームが行われるのは、この危険な風景です。  
コードやドキュメントの開発と同様に、動的なプロセスでもあります。  
したがって、保証は、1回限りのプロジェクトとして行われるものから、継続的な進化の別の側面に着実に変化しています。  
  
製品評価は、セクション8.3.3で説明したレモン市場の問題に取り組みます。顧客が品質を測定できない場合、悪い製品は良い製品を追い出します。  
錠前鍛造に関する1853年の本は、強盗がそれらをすでに知っていたという理由で貿易の「秘密」を明らかにすることを正当化しました。無知だったのは錠前屋の顧客だった[1895]。単にブランド名に依存する場合は、ベンダーはセキュリティエンジニアを雇うのではなく、広告を購入することもできます。  
以前の章では、さまざまな製品が評価および認定される静的セキュリティ標準のいくつかの例について説明しました。  
それは50年前にコンピューターのセキュリティが始まった場所だったかもしれませんが、コンピューターが至る所に行き着くにつれて、他の業界にも目を向ける必要があります。  
電力の送配電については、セクション23.8.1ですでに説明しました。  
現在、トラックと車の両方に運転支援用の複数のシステムがあり、インターネットに接続されているため、重要なセキュリティと安全要件があります。  
これについては、いくつかのケーススタディで説明します。  
  
米国の保険業界は1894年に共同試験所を設立し、電球の火災リスクを警戒しました。それは1901年に火災安全およびその他の規格を開発する非営利団体であるUnderwriters ’Laboratoriesとして組み込まれ、1913年にセキュリティ製品の承認を開始しました[1916]。  
評価者は一定の予算を費やしてフローを探し、レポートを作成します。その後、ラボはデバイスを承認するか、デバイスを拒否するか、いくつかの変更を要求します。  
リスクの1つは慣性です。標準が進歩に追いついていない可能性があります。  
セクション13.2.4で、バンピングツールがどのように改善されたかを説明しました1 20代後半から30代前半に私は銀行で働きました。私が銀行間セキュリティ標準委員会に行ったとき、その部屋にいたのは約4人だけでした私たちが話していたのは、そのうちの1人はIBMの出身でした。  
2010年までに大きな脅威となり、ピックも改善しました。  
ドイツなど一部の国の保険研究所は、攻撃が改善するにつれて認定を取り下げる用意ができています。アメリカでは、彼らはおそらく訴えられるのを恐れて、気が進まないようです。  
  
安全基準は、重大な事故やスキャンダルに対応して、一度に1つの業界で出現する傾向があります。  
アメリカで最も売れている薬は、硫酸とテレビン油の希薄溶液であることがわかりました–製造するのに本当に安価でありながら、人々がそれが彼らにとって良いことであると信じられるほど十分に味わいがありませんでした[2050]。  
FAAは後に、グランドキャニオン上での2つの旅客機間の1956年の墜落で2人の飛行機に乗っていた128人全員を殺害した後、アイゼンハワー大統領によって設立されました[684]。  
Ralph Naderの著書「Unsafe at Any Speed」が議会に全国高速道路交通安全局（NHTSA）の設立を促すまで、ベンダーは自動車をシートベルトではなくクロムで装飾することを競いました。  
ヨーロッパは、1985年に製造物責任指令に国内法のパッチワークを調和させ、業界セクターごとに規制と安全機関を追加しました。  
たとえば、自動車の場合、ヨーロッパでは通常、独立したラボによる安全性テスト2が必要ですが、アメリカではそうではありません。しかし、ヨーロッパでは「業界の規範」が作成され、米国の裁判所が不法行為の不法行為の事例を評価するため、ほとんどの米国のベンダーも米国のモデルを個別にテストしています。  
EUの全体的な安全戦略は、業界のワーキンググループやロビイストとの交渉により一連の基準を進化させ、7〜10年ごとにそれらを更新することです。  
おもちゃなどの危険性の低い商品には自己認証が必要です。ベンダーは製品に「CE」マークを付けて、関連するすべての規格に準拠していることを表明します。  
ドイツでは、それがT¨UVです。  
製品が事故を引き起こす;また、自動車のブレーキから産業用圧力バルブまで、幅広いコンポーネントに使用されています。  
28.2.3医療機器の安全性  
たとえば、医療機器の安全性については、アメリカとヨーロッパの両方で長い間論争が続いています。  
原因は、ユーザビリティの問題として表面化したソフトウェアのバグでした。オペレーターがマシンのパラメーターをあまりにも早く編集すると、マシンが危険な状態になり、患者に非常に多くの放射線を照射する可能性があります。  
図28.1：–明らかに同じモデルの2つの輸液ポンプ（写真はHarold Thimbleby提供）  
致命的な事故の多くは、ユーザビリティの失敗です。  
緊急治療室には、さまざまなユーザーインターフェイスを備えた、半ダース以上の異なるベンダーからの機器がある場合があります。輸液ポンプは車と同じくらい多くの人を殺し、その数は英国では数千人、米国では数万人にのぼります[1878]。  
 まあ、標準があります。  
それでは、なぜこの基準が適用されないのですか？  
単なる書類審査です3。  
この3比較として、同僚と私が小さな店や家などの重要度の低いリスク用に設計された盗難警報機の評価を手伝ったとき、私たちの予算は2週間でした。  
2つの異なるデバイスが同じ製品として販売されているという事実は、コンプライアンスコストを最小限に抑えるための一般的な戦略です。  
これは多くの分野をカバーする重要な進歩ですが、使いやすさは大きなフィールドです。  
エンジニアが使用できるいくつかの評価手法について説明していますが、「医療機器の種類に関する不十分な経験」は、使用エラーの原因となる可能性のある要因のリストの1つの箇条書きにすぎません。  
数値入力のみでの安全性は複雑な分野です[1879]。すべてのベンダーはおそらく、その専門家や他の何十もの技術についても専門家を訓練する必要がありますが、多くのベンダーは、彼らがうまくやれると思うほどのことはしません。  
しかし、看護師が競合他社の機器のさまざまなインターフェースを使用するときに生じる混乱が、本来あるべき程度に真剣に受け止められるかどうかは不明です。  
これは、欠陥のある乳房インプラントに関するスキャンダルに続いて、2017年にヨーロッパ全体に導入され始めました[233]。  
2020年5月、新しいEU医療機器規制（2017/745）  
そして2020年6月、英国議会は、大臣がBrexitの後に既存の規制を修正できるようにする医薬品および医療機器法を可決しました。  
英国の国民健康保険内では、安全専門家としてのキャリアを築くのは困難です4。  
輸液ポンプが車と同じくらい多くの人、または米国では銃と同じくらい多くの人を殺す場合、彼らは交通安全と銃の制御についてであるので、なぜ人々はもっと努力しないのですか？  
地元の病院では、そのような事故はおそらく1か月に1人未満の死者であり、輸液ポンプの人はとにかくかなり病気になる傾向があるので、それらの多くは気づかれません。  
営業担当者との素敵なランチの後、6ダース以上の異なるサプライヤーから。  
（例外は、人々が実際に敵意に非常に敏感であるため、安全障害にセキュリティの角度がある場合です。  
 ユーザーインターフェイスの標準化は、事故とその原因がより明確になる業界でより適切に管理されます。  
車のコントロールは今やかなり標準的で、右側がアクセル、中央がブレーキ、左側がクラッチです。  
しかし、それはかつてずっと悪かった。  
平均的な現代のドライバーは、そのような車をレンタルロットから出すのに苦労するでしょう。  
28.2.4航空安全  
パイロットは事故報告に注意を払い、飛行中の各タイプの飛行機で訓練する必要があります。  
看護師が同様に各輸液ポンプの型格を取得する必要がある場合、それは実際のお金がかかり、病院の幹部が注意を払い、最終的にベンダーはボーイングをフォローし、多くの命を救うことができます。  
ボーイングが1997年にマクドネルダグラスを買収して以来、大型航空機を製造する唯一の米国企業となったため、連邦航空局はボーイングを支援する役割を果たしてきました。  
買収のさらに有毒な影響は、マクドネルダグラスの幹部が引き継いだことであり、同社は本社をシアトルからシカゴに移動し、エンジニアではなく、すでに1つのエンジニアリング会社を破壊し、現在その目標を持っている金融関係者によって運営されていました。新しい独占から最大の利益を搾り出すことでした。  
その後インドネシアとエチオピアで2回の墜落事故が発生し、346人が死亡しました。  
ボーイングは、エアバスの最新モデルと競合するために、737の燃料効率をより速くする必要があり、これは、より大きなエンジンを意味し、さらに前方に取り付ける必要がありました。そうしないと、機体を再設計して、それは規制目的のための新しい飛行機であり、証明するのにはるかに長い時間がかかっただろう。  
 これを補正するために飛行制御コンピューターに  
実装エラーは、不正な迎角入力があると、飛行機がパイロットをヨーク上で約50kg引っ張って飛行機のレベルを維持する必要がある体制に入る可能性があることでした。その結果、ボーイングは適切な故障モードと影響分析を行わず、ソフトウェアの動作はパイロットマニュアルに記載されていませんでした。  
ボーイングは、多くの警報が一度に鳴るコックピットの緊急事態の混乱に対処するパイロットの能力に満足していました[1055]。  
FAAは、既知のすべての米国に緊急耐空性指令を送信することにより、墜落に対応しました。  
;ただし、2つのセンサーの不一致をパイロットに警告する警告灯は、車のサンルーフのように航空会社のオプションになっており、MCASを無効にできるスイッチの操作が直感的でなくなった[155]。  
パイロットは苦情を記録し、1つはマニュアルを「犯罪的にほぼ不十分」であると説明しました[139]。しかし、FAAはそのような苦情を航空会社の運航にのみ関連すると見なし、世界的な安全性の危険について分析していませんでした[664]。  
ボーイング社は、2020年3月までに187億ドルの売上を失いました。  
2020年8月に承認された修正には、ソフトウェアの変更だけでなく、MCASが両方の迎角センサーを読み取り、飛行ごとに1回だけ、スティックの力が制限されて展開されるようにする必要があります。ただし、手順の変更により、両方のセンサーが飛行前にチェックされます。パイロットトレーニングの更新。規制の変更により、ボーイングではなくFAAが製造後に各飛行機をチェックするようになりました[592]。  
心理学、インセンティブ、制度、権力も重要です。  
時間の経過とともに、リスク評価とリスク削減のために設計された対策は工業化され、コンプライアンスの問題になりがちであり、企業は最小コストで合格することを求めます。  
優れたエンジニアになりたい場合は、関連する可能性のあるシステム全体のあらゆる側面を理解する必要があります。  
28.2.5オレンジブック  
これについてはセクション9.4で触れました。ここでは、米国国防総省がこれを介して促進しようとしているマルチレベルのセキュリティモデルについて説明しました。  
インセンティブに関しては、保険と同様に、それは集団的依拠当事者スキームでした。  
C1は、アクセス制御システムがあることを意味しました。 C2は、慎重に構成された商用システムに対応しています。  
トップバンドで、A1は正式な検証の要件を追加しました。  
 システムの評価クラスは、システム上で処理できる情報の広がりを決定しました。  
オレンジブックが作成されたとき、国防総省は、市場が小さすぎるために高保証のコンピュータに高額を支払うと考え、セキュリティ標準が市場を拡大することを望んでいました。  
政府のユーザーは、いくつかの製品を評価してもらいたいでしょう。 NSAはそれを行うために人々を割り当てます。従来の公務員の注意と遅延を考えると、これには2〜3年かかる可能性があります。製品が成功した場合、評価済み製品リストに加わります。法案は納税者が拾った。  
他の政府も同様の考えを持っていました。  
、彼らの防衛請負業者が米国の供給業者と競争するのを助けるための共有スキーム。  
 しかしベンダーによって。  
請負業者は、商業的に認可された評価機関（CLEF）として承認を得ることができます  
それは決して起こらなかった。  
その理由は、標準よりもはるかに広く深いものです。  
  
20世紀に米国政府によって推進された2番目の評価スキームは、暗号化プロセッサの耐タンパー性を評価するためのNISTのFIPS 140スキームでした。  
1994年に発売され、現在も勢力を維持しており、米国の暗号化機器の顧客に支持されています。  
1つ目は、ソフトウェアではなく暗号化デバイスのハードウェアをカバーし、FIPS 140で評価された多くのデバイスをカバーしていることです（最高レベルでも）。  
セクション20.5で説明されているように、下位互換性のために、弱いアルゴリズム、レガシー動作モード、脆弱なAPIが銀行標準化団体によって義務付けられています。  
2つ目は、セクション18.4で説明した歴史的な理由により、FIPS 140-1標準にはレベル3とレベル4の間に大きなギャップがあるということです。  
 レベル3のデバイスの中には壊れにくいものはありません（エポキシをナイフで削り取るだけです）。  
レベル4は非常に難しく、そのグレードを達成したデバイスはごくわずかです。これはFIPS標準では正式な表現がないため、企業は米国外の顧客と話をする際に、代わりにCommon Criteriaに依存することがよくあります。  
28.2.7コモンクライテリア  
1989年のソビエト連邦崩壊後、軍事予算は削減され、将来の敵はどこから来るのかは明確ではありませんでした。  
作業は実質的に1994〜1995年に行われ、ヨーロッパのITSECモデルはオレンジブックアプローチに勝ちました。  
イノベーションは、複数のセキュリティポリシーのサポートでした。  
これは、製品のクラスに対するセキュリティ機能要件と保証要件のセットです。  
オペレーティングシステム、アクセス制御システム、境界制御デバイス、侵入検知システム、スマートカード、鍵管理システム、VPNクライアント、投票機、さらに家庭用ごみ箱が最後に空になった時期を識別するトランスポンダまでの保護プロファイルがあります。  
防衛コミュニティがマルチセキュリティを放棄したのではなく、商業企業が他の目的にもそれを使用することにより、独自の評価システムを主流化しようとしたのと同じくらいです。  
暗号化、放出のセキュリティなど、セキュリティのいくつかの側面が明示的に除外されました（NATO標準が分類されたため）。  
。  
その評価は、スマートカード、ハードウェアセキュリティモジュール、TPM、電子署名デバイスなどの専門的な市場で使用され、セクター別のデューデリジェンスルール（PCIなど）が使用されます。  
 コンプライアンス要件を作成します。  
 – EU諸国の諜報機関の代表からなる委員会。  
英国は2019年に撤退しました。  
28.2.7.1ゴーリーの詳細  
テスト対象の製品は、評価対象（TOE）として知られています  
審査の厳密さは、評価保証レベル（EAL）です。  
商用製品で一般的に得られる最高の評価レベルはEAL4ですが、2020年にはCCで認定された1472のうちEAL6以上で85の製品があり、多くのスマートカードはEAL4 +に評価されます。レベル。  
 それを評価します（適切なものがまだ存在しない場合）  
保護プロファイルは、セキュリティ要件、その根拠、およびEALで構成され、すべてのクラスの製品に対応しています。  
セキュリティターゲット（ST）  
PPを評価して、それが完全で一貫していて技術的に健全であること、およびSTであることを確認できます。  
最終結果は、保護プロファイルの登録と認定製品のカタログです。  
たとえば、FCO\_NROは機能コンポーネントです（したがってF）  
 そしてそれは起源の否認防止（NRO）を指します  
その他のクラスにはFAU（監査）が含まれます  
。  
 •P.Crypt\_Stdなどの組織ポリシー–「暗号規格：暗号エンティティ、データ認証、および承認機能は、ISOおよび関連する業界または組織の基準に準拠している必要があります」•O.Flt\_Insなどの目的–「障害の挿入：TOEは、誤ったデータの挿入による繰り返しのプローブに対して耐性がなければなりません。」•ADO\_DEL.2などの保証要件–「変更の検出：開発者は、TOEまたはその一部をユーザーに配信するための手順を文書化する」保護プロファイルには根拠が含まれるはずです。これは通常、各脅威が1つ以上の目標によってどのように制御されるか、および逆方向で、脅威と環境の想定の組み合わせによって各目標がどのように必要とされるかを示す表で構成されます。  
これにこだわる最も早い方法は、コアCCドキュメント自体を読んでから、いくつかのプロファイルを読むことです。  
たとえば、マネージメントでクリップアートを使用して書かれた自動現金自動預け払い機の保護プロファイルは、「セキュリティポリシーを含めないように選択されており」、1999年に書かれたときによく知られている問題の多くを見逃しています[340]。  
スマートカードの保護プロファイルは、請負業者にNDAを課したり、廃棄物を細断したりすることによってチップ設計の機密性を維持することを強調しますが[650]、実際には、スマートカードに対するほとんどの攻撃は、チップマスクの知識が無関係であるプローブまたは電力分析攻撃を使用しました。この情報は、AVA\_VAN.5の保証要件を超えています。AVA\_VAN.5は、情報機関のトップシークレットシステムのように、開発環境全体をエアギャップにする必要があることを本質的に要求しています。  
スマートカード会社は、HSMや飛び地が市場に侵入することを望んでいません。  
  
この本の第2版が2008年に発表されるまでに、業界の人々はCommon Criteriaについて多くの不満を持っていました。  
HSMなどのデバイスを販売したいスタートアップは、現在、数百万ユーロを費やして、プロセスをナビゲートするために数年の労力を費やす必要があります。  
•次に大きいのは、CCはEmsecや暗号アルゴリズムなどの「技術的な物理的」側面を回避するだけでなく、実際にはユーザビリティを無視することを意味する管理セキュリティ対策を無視することです。  
•保護プロファイルは、スポンサー企業が市場を不正に操作するために設計されています。  
ゲームはしばしば安全でない製品につながります：ベンダーは簡単にできることをカバーするためにPPを書きます。  
セクション20.5で説明されているHSMに対するAPI攻撃を思い出してください。一部の脆弱なHSMはCC認定されており、他のCC認定製品でも同様の障害が見られます。  
セクション26.5.2で、スマートカードを使用して作成されたデジタル署名を企業が認識することを要求するヨーロッパのeIDAS規制について説明し、税務申告書の提出などの相互作用について政府に要求するように勧めました。  
その問題は非常に難しいため、除外され、最終的には、PC内のウイルスやトロイの木馬がスマートカードに送信したものに対する「安全な」署名になります。  
PPは、スマートカードが「セキュアな署名作成デバイス」として機能するように作成されました。 HSMと署名アクティベーションモジュール（SAM）用の他のPPが登場  
HSMとSAMは、適格な署名作成デバイス（QSCD）として評価されます  
ただし、サービスプロバイダーが使用するフロントエンドサーバーソフトウェアは監査のみであり、認証されていません。また、運が良ければ、セクション12.7.4で説明したように、マルウェア対策として携帯電話またはタブレットのアプリにRASPが含まれている可能性があります。 。  
•CCは、特定の開発方法論を想定していないと主張しているが、実際にはウォーターフォールアプローチを想定している。  
そのため、通常のセキュリティ開発ライフサイクル、または毎月のセキュリティパッチを入手する商用製品には対応できません。  
 •基準はテクノロジー主導であり、ほとんどのアプリケーションでは、保護の決定を推進するのはビジネスプロセスです。  
セキュリティは、製品ではなくシステムの特性です。  
システム内の誰も実際に外交上の事件を引き起こさずにこれを公に言うことができないので、修正することはできません。  
•Common Criteriaブランドは十分に防御されていません。  
したがって、サプライヤーは欠陥のある端子を「CC評価済み」として説明し続けることができます。  
•より一般的には、責任については何もありません。「認定での評価結果の使用手順は、CCの範囲外です。」  
そのような装置には、裁判官の共感を得ることから、だまされやすい政府からお金を奪い取ること、頭の周りの人々を強打することまで、あらゆる種類の用途があります。  
  
これらの批判に対処するために、協調的保護プロファイル（cPP）  
アイデアは、EALレベルから安全なデバイスの各クラスの単一の保護プロファイルに移行し、政府および学者からの入力を使用して、業界の企業間の共同作業としてそのプロファイルを開発することでした[462]。  
この結果は、CC Webサイトで評価済み製品のカタログを閲覧することにより、2020年に見ることができます。  
しかし、ヨーロッパ以外では、CCシステムはベンダーの関心に完全に捕らえられています。  
安全なFAXマシンとは何ですか？FAXを暗号化しますか？  
。  
電子署名システムを販売したい企業は、EAL4と見なされるcPPの下でそれらを評価することができ、ほとんどの顧客は、それと古いルールの下で行われたEAL4 +評価との違いを見分けることができません。  
28.2.8「最大の自己満足の原則」  
あなたが10代の明るい人なら、一流の大学に申し込んで二流の学位を取得するリスクがありますか、それとも地元の大学に行ってスターになるべきですか？スタートアップのために資金を調達する場合、ビジネスエンジェルから資金を得るのか、それとも有名なベンチャーファンドを買収するのか。  
そして、国家でさえ認証ゲームをします。  
そのようなゲームに対処するためのオプションは何ですか？  
彼らのモデルは3段階のゲームであり、スポンサーは認定者を選択し、認定者は製品を調査し、おそらくいくつかの変更を要求し、最終的にエンドユーザーは購入するかしないかを決定します[1143]。  
ほとんどの場合、最大の自己満足の原則が優先されます。所有者は単一の認証者からの承認を求め、製品を改善するように彼らに求めようとする試みに抵抗します。  
1つの例は、製品を持続可能なものとして認定するためにNGOが競合する場合です。そこでは、認定者はスポンサーよりもユーザーの結果を重視しており、目的の物件は単一のスポンサーによって強く管理されていません。  
スポンサー、認証者、ユーザー以外のプレーヤーがいる場合、状況はさらに複雑になります。  
ある会社がいくつかの新製品を発明し、それを一部の顧客に販売しています。  
彼らは、発明者に彼らの確立された供給者、または少なくとも第二の供給者に製品を認可することを望むかもしれません。  
企業は、ロイヤルティのシェアを最大化するために、特許を取得するために長く困難な交渉を行っています。これはしばしば、7Tiroleが2014年のノーベル賞を受賞した恐ろしい基準になり、これだけでなく、市場支配力と規制に関する他の多くの研究に貢献しました。  
。  
。  
 ベンダーが数日しかかからないセキュリティ評価の費用を支払う場合（そして今ではパンデミックのためにリモート監査を許可します）  
要するに、産業戦略は、独占やカルテルほどには優れた製品を最適化しません。  
。  
セキュリティ認証の複雑さはおおよそ（a）です。  
 スポンサーは、ベンダー、顧客、依存者、またはこれらのいずれかの団体である場合があります（c）  
 複数の認定機関があり、さらにそれらの間に政治がある場合もあります。  
物事を理解するには、実際のケースを詳細に検討する必要があります。  
イブが法廷でボブから返金を請求したとき、評価はどのように変化しますか？  
チャーリーが自分のシステムにサインオフした場合、この議論はさらに強力になります。  
そのため、アリスはチャーリーを満足させるために必要なだけ努力します。  
現実の結果として、ペイメントカードブランドがチャーリーの役割を引き継ぐためにPCIを設定した。  
。  
Docusignなどのオンラインサービス署名プロバイダーによるロビー活動によって、彼らも参加しました。  
（一部のEU諸国での納税申告を行うには、そのようなサービスで署名してもらう必要があり、税理士の手数料にさらに20ユーロを追加します。）  
 興味深いケーススタディは、Webサイトを認証するTrust-eスキームのBen Edelmanによるものです。  
逆選択により、このスキームは質の悪いシグナルになりました。弱いベンダーは自社のWebサイトを認定しましたが、有名な消費者ブランドは気にしませんでした[612]。  
しかし、業界のロビーは「テープを切る」ことについて話したいと思っていますが、政府が支援する安全またはセキュリティ基準または機関の全面的な廃止に満足している人はどれくらいいますか？  
多くの規制制度は、新興企業が現職者に容易に挑戦できないようにするための堀として、また責任の盾として機能します。  
  
Brexit以来、イギリスとヨーロッパは分岐しています。  
 欧州ネットワークと情報セキュリティ機関（ENISA）を強化する  
ENISAは専門知識の中心として行動し、銀行、航空、エネルギー、通信、およびデータ保護機関の分野の規制当局と連携します。  
後でこれに戻ります。  
「競合する、または重複する国家のサイバーセキュリティ認証スキームの重複を回避し、デジタル単一市場で事業を展開するためのコストを削減する」のに役立つはずです[655]。  
私が2020年に書いているように、詳細はまだ検討中ですが、意図は、EU加盟国のスポンサー機関が、ベンダーが規格への適合を自己評価し、責任を負うことを必要とする「基本」から3つのレベルで認証を実行することです準拠については、セキュリティ機能の検証を伴う「実質的」を通じて、ENISAがSOG-ISから現在EAL4以上で評価されているスマートカード/ HSM /電子署名キットの監視を引き継ぐことを伴う「高」へしかし、2017年までに、基準はセキュリティにとって必要でも十分でもないという結論に達し、GCHQは2019年からスポンサーとして撤退しました。  
それは長い間独自の国家製品認証スキームを持っていました、現在は商業と呼ばれています8ドーナツの私のスパイの1人は言っていますそれは値する:-)  
ですが、現在CPA認証を維持している唯一の消費者向け製品は、セクション14.2.4で説明したスマートメーターです。  
旅行の方向は、英国の国家インフラのための重要な機器を開発している企業にとっても、より一般的にも、製品ではなくプロセスを検討することです。  
12.2.4で説明したセキュリティ管理のISO 27001標準はすでに存在していました。これは高価であり、大手の会計事務所によって収入源になっており、CCと同じくらい役に立たないものです。  
監査人は企業が彼らに言うことに依存する必要があり、そのシステムを保護する方法を知らない企業は彼らがそうしないとき、単に「私たちはXのための素晴らしいプロセスを持っている」と言うでしょう。  
 そして、なぜ政府はそのような税金を課すべきなのでしょうか？  
その目標は中小企業でしたが、その下で実際に認定された最初の企業は、企業のデューデリジェンスにすべてのタッセルを追加したいと考えた銀行や電話会社などの大企業でした。  
最初の章で、企業の世界では、信頼できるシステムは保険会社にとって受け入れられるものであることが多いと述べました。  
 さて、Bitsightは民間セクター向けにMugshotを実行しますが、企業のシステムを攻撃する代わりに、最新のパッチが適用されていないサーバーの数と、目に見える他の侵害の指標の数を数えることにより、企業のサイバーセキュリティリスクを評価します。  
これはラーナー・チロールモデルでは理にかなっています。Bitsightは、エリート大学のように、競合他社に先んじるよう動機付けられているためです。  
たとえば、サービス会社は現在、学校での旗揚げ競技会を後援することに消極的です。 Bitsightクローラーが、そのような演習のターゲットとしてセットアップしたIPアドレススペース内の脆弱なシステムを検出した場合、Bitsightの評価を10％以上カットし、実際のビジネスにコストをかける可能性があります。  
次のセクションでは、障害分析、バグ追跡、製品間の依存関係、オープンソースソフトウェア、および開発チームの観点から、信頼性メトリックをさらに詳しく見ていきます。  
28.3信頼性の指標とダイナミクス  
多くの場合、それは開発チームの機能であることがわかっています。セクション27.5.3で機能成熟度モデルについて説明しました。  
その過程で、フィードバックを提供し、プロセスとツールを常に改善することで、彼らがどれだけうまくやっているかを測定し、それを改善します。  
 これには主に2つの側面があります。テストとバグ修正によりシステムが時間の経過とともに信頼性が高まることによる信頼性の向上、およびバグが見つかった場合と修正されない場合の脆弱性の開示です。  
28.3.1信頼性成長モデル  
テスターがシステム内の単一のバグを見つけようとしている最も単純なケースでは、合理的なモデルはポアソン分布です。t統計的にランダムなテストの後でバグが検出されない確率pは、p = effiEtで与えられます。影響を与える可能性のある入力の割合について[1175]  
しかし、広範な経験的調査により、大規模で複雑なシステムでは、t番目の検定が失敗する可能性はeffiEtではなく、定数kのk / tに比例することが示されています。  
これは、IBMメインフレームオペレーティングシステムのバグ履歴で最初に文書化され[18]、他の多くの調査で確認されています[1198]。  
 約t / kの場合、信頼性はテスト時間とともに直線的に増加します。  
 100万時間[355]。  
k / t動作の理由は[249]で明らかになり、理想的なガスをモデル化するために開発されたMaxwell-Boltzmann統計が統計的に独立したバグにも適用されることを観察することにより、より一般的な仮定の下で証明されました[312]。  
バグが統計的に独立していると想定できる場合は、k / t信頼性の向上が最も可能です。100万時間のMTBFを得るには、100万時間のテストが必要であるというルールは、以下に依存する一定の定数倍までです。コードの初期品質とテストの範囲。これらの統計は、ソフトウェアの進化モデルと選択圧下の生物種の進化との間のきちんとしたリンクを提供します。ここで、「バグ」は適合度を低下させる遺伝子です。  
たとえば、ウサギの集団がヘビに捕食されている場合、それらは速度ではなく警戒のために選択されます。  
進化モデルは、オブジェクトやライブラリなどの再利用可能なソフトウェアコンポーネントから得られる信頼性の向上に関する基本的な制限も示しています。十分にテストされたライブラリは、全体的な失敗率が新しいコードによって支配されることを単に意味します。  
テスターに​​よって測定された障害時間は、プログラムの初期品質、テストの範囲、およびテストの数にのみ依存するため、別の環境でのプログラムのパフォーマンスについて、それ以上の情報はほとんどありません。  
最後に、異なるテスターは、プログラムではなく、並行して作業する必要があります。  
機械がどのように故障するかについて統計的知識を得るので、これは、機械の実証済みの設計に利点をもたらします。  
開発チームによる回帰テストの使用は、新しいビルドごとに数十億のテストケースを一晩で実行できることを意味しました。  
では、信頼性にはどのような制限がありますか？  
簡単な例を見てみましょう。  
アーメドがイラン革命警備隊のために働き、米軍のネットワークに侵入するためのツールを作成するとします。一方、ブライアンはアーメドを止めることを目的としたNSAの男です。  
アーメドはたった半ダースの人々しか持っていないので、彼は年間10,000時間のテストしかできません。  
商業評価ラボ、CERTの内部調査、他のファイブアイズ加盟国との情報共有契約、そして政府のスキームを実行して、電力や通信などの重要な産業にコンサルタントを派遣し、ハッキングの方法を見つけます（失礼しますが、彼らに自分のシステムを保護する方法をアドバイスする）  
これを合計すると、1年間のテストで1億時間に相当します。  
しかし、ブライアンがアーメドのバグのいずれかを発見した確率は10％にすぎず、それらすべてを発見した確率はごくわずかです。  
つまり、攻撃者は熱力学を持っています。  
ただし、この問題を解決するまでに数年を要し、新しい問題が常に発生しています。  
統計トラップを回避する1つの方法は単純さです。これは、第9章で見たように、必須のアクセス制御、マルチレベルのセキュアメールガードなどのアーキテクチャなどのポリシーを意味します。  
これは、セクション27.5.7で説明したように、慎重なネットワーク監視、違反レポート、脆弱性の開示、迅速なパッチ適用を意味します。  
28.3.2敵対的レビュー  
最終的には、システムが実装される前に完了すると、安くなる可能性があります。  
これが、Common CriteriaやISO 27001のように、競合する複数の評価者の1人からベンダーが支払った評価が根本的に破られている基本的な理由です。  
ワイアカードのショートから1億ドルを稼いだヘッジファンドマネージャーのジムチャノスは、次のように述べています。「監査人である人々が私たちに尋ねるとき、私はいつも「誰が気にしますか？  
 敵対的なレビューを行うには、お金または本物のいずれかで攻撃者をやる気にさせることができます。  
 NASAが有人宇宙飛行に使用するプログラム。請負業者は、コードを調査するために雇われ、発見したすべてのバグに対してボーナスを支払いました。  
もう1人はIBMで、ニューヨークとノースカロライナに2つのチームを置き、ケンブリッジとオックスフォードがボートレースに勝とうとするなど、お互いの仕事を壊そうとすることで、長年にわたって暗号技術の主導的地位を維持していました。毎年。  
これはそれらの97％以上を修正します[589]。  
私たちの研究者たちは、物事を壊すことで拍車を勝ち取り、新しいタイプの攻撃を発明することで最高の称賛を得ています。  
ただし、確立されたベストプラクティスは、お金で敵対的なレビューを動機づけることであり、具体的には、ベンダーが脆弱性のレポートに対して大きな報酬を提供するバグ報奨金プログラムを通じてです。  
学術的レビューまたはバグ報奨金プログラムのいずれかを強化する1つの方法は、設計と実装を開き、世界中がバグを探すことができるようにすることです。  
28.3.3フリーでオープンソースのソフトウェア  
 歴史的なコンセンサスは、彼らがそうあるべきだということです。「マーキュリー、または秘密と迅速なメッセンジャー」で、彼は暗号化について次のように論じることを正当化しました。 。  
ビクトリア朝時代には、鍵屋が鍵の脆弱性について話し合うべきかどうかについても議論が交わされました。セクション13.2.4で述べたように、ある本の著者は、鍵屋と強盗の両方が錠を選ぶ方法を知っていて、それは無知な顧客だけだったと指摘しました。  
フリーでオープンソースのソフトウェア（FOSS）  
多くのセキュリティ製品には一般に公開されているソースコードがあり、その1つはおそらくPGP電子メール暗号化プログラムでした。  
オープンソースソフトウェアは完全に最近の発明ではありません。コンピューティングの初期には、ほとんどのシステムソフトウェアベンダーがソースコードを公開していました。  
ユーザーからの激しい批判にもかかわらず、メインフレームソフトウェアの「オブジェクトコードのみ」のポリシー。  
オープンソフトウェアを支持する多くの強力な議論があり、反対のものもいくつかあります。  
第2に、システムが非常に複雑になり、ツールチェーンが非常に長くなるため、バストしようとしているバグが、記述したコードではなく、オペレーティングシステムまたは依存しているコンパイラにあることが多いため、バグもすぐに見つけて、修正するか、自分で修正してください。  
第4に、そのような製品にバックドアを挿入することはさらに困難になる可能性があります（悪用​​されて7つの数字が売れるようになったため、人々は試みに巻き込まれました）。  
最後に、これらすべての理由から、オープンソースは信頼に値します。  
典型的なボランティアはバグハンティングよりもやりがいのあるコードを開発しているため、多くのオープンな製品に対して十分なディフェンダーがいない可能性があります（ただし、バグバウンティがこれをシフトし始めています）。  
次に、セクション28.3.4で述べたように、テストの焦点が異なるため、テスターが異なればバグも異なります。  
実際には、主要な脆弱性が何年も潜んでいます。  
それでは、攻撃者や防御者はもっと助けられるのでしょうか？  
したがって、特定のアプリケーションでオープンアプローチとプロプライエタリアプローチのどちらが最適に機能するかは、そのアプリケーションが、独立した脆弱性などの標準の前提から逸脱しているかどうか、およびその方法に依存します。  
では、利益のバランスはどこにあるのでしょうか。  
セキュリティはこれらすべてのテストに合格しています。  
それでもなお、セキュリティに関する議論が広まり始めています。1999年頃の暫定的な始まりから、米国国防総省は、特に9.5.2項で説明したSELinuxプロジェクトを通じて、オープンソースを採用し始めました。  
重要な一次的な質問は、有能な人々があなたが作ったものをチェックしてテストするのにどれだけの労力が費やされたか、そして彼らが彼らが見つけたすべてをあなたに言うかどうかです。  
そして、重要性が高まっているという2次的な問題があります。ビジネスがLinuxに依存している場合、少なくとも何人かのエンジニアがその開発者コミュニティに関与すべきではないので、何が起こっているのかを知っていますか？  
28.3.4プロセス保証  
システム開発を終えた人なら誰でも知っているように、一部のプログラマーは、他の人よりも桁違いにバグの少ないコードを生成します。  
有能な企業は善良な人々を雇おうとしますが、善良な人々は彼らを大切にし、同胞を雇う企業のために働くことを好みます。  
私自身の経験では、一部のIT部門は遅くて官僚的であり、他の部門は活発です。  
別の問題は、エンジニアの品質が時間とともに低下する傾向があることです。  
もう1つは人口統計です。1990年代初頭のMicrosoftは長時間働いていた若いエンジニアでいっぱいでしたが、10年後、多くの人がストックオプションを現金化して去りましたが、残りはほとんどが家族を獲得してオフィスアワーで働いていました。  
一部の企業はこれに対抗するために、マネージャーがチームの生産性が最低でも10％ほどである必要があるシステムを評価することでこれに対抗しようとしましたが、これが士気に与える影響は恐ろしいものです。人々はコードを書くよりも吸い込むことに時間を費やしています。  
セクション27.5.3で説明した機能成熟度モデルは、優れたマネージャーが優れたチームをまとめ、長期にわたって改善するのに役立つツールの1つです。  
ウォータークーラーチャットからトップリーダーシップまで、企業環境全体が重要です。もちろん、すべての企業がミッションを装っていますが、ほとんどの企業は偽物であり、スタッフはそれらを即座に確認します。  
詳細については、[1937]を参照してください。コンサルタントと監査人の業界全体がこの谷に鼻を持っています。  
せいぜい、漸進的なプロセス改善のためのフレームワークを提供できます。しかし、非常に多くの場合、カオスをより官僚的なカオスに置き換えるだけのボックスティックの練習です。  
保証という意味では、信頼できるサプライヤーです。  
政府の認証機関は差別的であるとは見なされないため、プログラムはボックスティックに縮退します。  
どちらの場合も、コンサルタント会社と監査会社は、手数料収入を最大化するためのプロセスを工業化し、私たちは元の場所に戻ります。  
 高品質の仕事をしている中小企業は、最も差別的な顧客、つまり彼らが何をしているのかを理解するのに十分なほど賢い少数の大企業に販売する場合、一般的にはよりうまくいきます。  
では、ダイナミクスはどうでしょうか？  
 それらは牛乳のようになるのでしょうか、それともワインのようになるのでしょうか[1488]。  
 簡単な答えは、実際の測定を行わなければならないということです。  
製品の機能強化によって新しいバグが導入される割合が、古いバグが検出されて削除される割合と等しい場合は、均衡を見つけることさえできます。  
経験的に、新しいシステムの信頼性は、よりエネルギッシュなバグが発見されて修正されるとしばらく改善されることが多く、その後数年間平衡状態に留まり、コードが複雑になり維持が困難になるにつれて低下します（ソフトウェアエンジニアによっては老化とも呼ばれます）  
ただし、コードを管理している企業がコードから十分な収益を得ており、品質を気にするよう動機付けられている場合、乱雑になりすぎた部分を書き直すことでこれを修正できます。これはリファクタリングと呼ばれるプロセスです。  
モデルはこれまでしかあなたを連れて行くことができません、そしてあなたはシステムが実際の使用でどのように振る舞うかを研究しなければなりません。  
一部のベンダーは、自社製品の失敗に関する大量のデータ（Microsoft、Google、Appleなどのプラットフォーム企業）を収集して分析しますが、選択したデータのみを部外者が利用できるようにし、テクニカルプレスから専門のサードパーティ評価者向けの市場を作ります学者に。  
医療部門は、患者への危害の証拠について悪名高く知られており、その弁護士は過失訴訟を起こすために何年も働かなければならない場合があります。  
最近のほとんどのソフトウェアはプラットフォームではなくアプリケーションであり、デバイス内またはデバイスをサポートすることが非常に多いため、これにより安全性の規制を検討する必要があります。  
28.4安全とセキュリティの絡み合い  
ソフトウェアがあらゆるものに適合し、すべてがクラウドサービスに接続されるにつれて、安全規制の性質は、単純な市販前の安全性テストから、ソフトウェアに定期的にパッチが適用される何年ものサービス寿命にわたってセキュリティと安全性を維持することまで変化しています。  
セクション23.8.1でスマートグリッド、セクション14.2でスマートメーター、セクション13.3でアラームの構築について説明しました。  
安全はセキュリティよりもはるかに多様なテーマです。  
セクション27.3で説明したように、私たちはまだ安全エンジニアから多くのことを学ぶことができ、安全エンジニアもセキュリティについて学ぶ必要があります。  
コロナウイルスの封鎖のおかげで、これらの講義はビデオで公開されています[89]。数年前に講義をオンラインで公開したいと思います。  
EUは最大の市場であり、米国政府よりも安全を重視しているため、EUは数十の業界で世界をリードする安全規制機関です。  
 リモートで悪用される可能性があります。  
2015年にEUが直面している問題は、自動車や飛行機から医療機器、鉄道信号機やおもちゃまで、数十の業界にわたる安全規制をいかに近代化し、必要に応じてセキュリティ規制を導入するかでした。  
この本では、さまざまなセクターでセキュリティがどのように失敗するか、および根本的な市場の失敗の性質について説明しました。  
安全レギュレータはより簡単なようです。  
少なくとも、死亡については、きちんとした統計があると思いますが、優先順位は、さまざまな種類の危害に関する公衆の懸念によって調整されます。  
ただし、ハッカーがWi-Fiを使用して、Hospira Symbiq輸液ポンプのいくつかのモデルによって送達される投与量を潜在的に致命的なレベルに変更できることをハッカーが示したとき、FDAは病院に使用の中止を指示する安全勧告を発行しました[2066]。それについて考えるのをやめると、それはかなり印象的です。  
おそらく人々は、セクション27.3.6で説明した原則を直感的に理解します：偶発的に発生する致命的な事故の100万分の1のチャンスは、対戦相手がそれをトリガーするために必要な入力の組み合わせを設計できる場合、あまり保証されません。  
デバイス障害のわずかなリスクのため、更新には通院が含まれます。  
EUはすでに医療機器の安全性に関する作業を進めており、翌年には医療機器指令を更新して、開発ライフサイクル、リスクの原則を考慮した最先端の技術に従って医療機器ソフトウェアを開発することを要求しました情報のセキュリティ、検証、検証を含む管理」および「デバイスが意図したとおりに機能するのを妨げる可能性のある不正アクセスから可能な限り保護するように設計および製造されている」[653]。  
  
Googleやテスラなどが運転する自動運転車への関心の高まりのおかげで、交通安全は2010年代半ばにセキュリティと安全の融合への関心を高めるのに役立ちました。  
実験車両による初期の事故の最初のニュースは、セクション25.3で説明した敵対的な機械学習とセクション25.2.4で説明したジープチェロキーのハイプロファイルハックに関する画期的な研究と同時に2015年頃に到着しました。  
テロリストはそれらをハッキングして群衆に追いやることができるでしょうか？  
 そして、もし子供たちが携帯電話を使って学校から車を家に呼び寄せることができれば、誰かがそれをハッキングして彼らを誘拐することができるでしょうか？  
 どうする？  
交通安全は、安全規制の大きな成功事例です。  
。  
その影響は、2009年のシェビーマリブと1959年のシェビーベルエアの間の衝突試験の消費者レポートビデオではっきりと見ることができます。  
50年の進歩のおかげで、マリブの客室は無傷のままです。前部のしわくちゃのゾーンがエネルギーの多くを吸収し、シートベルトとエアバッグがダミーの運転手を保持し、人間の運転手が立ち去っていただろう[472]。  
ビデオが示す数十年の進歩には、エンジニアリング、ロビー活動、複数の国にわたる標準設定だけでなく、安全運動家と産業の間の多くの闘争が含まれていました。  
車の安全性には、ドライバーのトレーニング、飲酒運転と過度のドライバーの労働時間に対する法律、そのような行動を取り巻く社会規範の変化、道路交差点の設計の着実な改善などが含まれます。  
これは、自動車がよりスマートに、より接続されるようになるにつれて進化する必要があります。  
セクション25.2で、Googleやテスラなどの企業がこれらのシステムを結合して自動運転を実現するための研究プログラムをどのように推進したかを説明しました。  
一部は悪用される可能性もありました：チャーリーミラーとクリスヴァラセックはジープのパークアシスト機能をハッキングして道路から追い出しました。  
セクション25.2で、自動運転車のセキュリティへの影響について説明しました。  
テスラの「オートパイロット」では、運転手に注意を払い、ハンドルを握ったままにして、事故を未然に防ぎます。  
2020年でさえ、より優れた自動操縦システムは高速道路で車をほぼ無事に運転できますが、小さな道路では不安定になり、環状交差点で混乱し、草の瀬を駆け抜けます。  
 アンチロックブレーキシステム（ABS）のテスト  
次に緊急ブレーキアシスト（EBA）がありました  
緊急停止しようとしています。  
これは単純なアルゴリズムですが、ドライバーの意図を推測しようとしているため、評価が困難です。  
 最近追加されたのは自動緊急ブレーキ（AEB）です。  
従来のロジックとディープニューラルネットワークに基づくマシンビジョンシステムの両方を使用する複雑な処理により、前方にあるすべてのものを理解しようとしているため、これはさらに困難です。  
車線維持支援とアダプティブクルーズコントロールを追加すると、高速道路で車をうまく運転できます。  
 そして、私たちが完全な自律性に移行する場合、リスクと脅威の分析には、人間社会で発生する多くの悪いことを含める必要があります。  
ただし、実際の数値は物議を醸しています。  
テスラが主張したように、車両の自動操縦機能がアクティブ化された後のエアバッグ展開の40％の減少ではなく、完全なデータは、100万マイルの移動あたりの0.76展開から1.21への57％の増加を示しました[1565]。AEBで懸念されていたのは、ウサギがその前を走っているときに車が急ブレーキをかけると、後面衝突が増える可能性があることでした。  
オートパイロットを搭載したテスラと同様の値のプラグインハイブリッドメルセデスを保証するのにどれくらいの費用がかかるかをオンラインで確認すると、ほぼ同じ答えが得られます（ただし、より多くの保険会社がメルセデスに入札します）。  
しかし、保険数理コストは公共政策の唯一の推進力ではありません。  
哲学者は倫理について心配し始めました：歩行者を殺すか運転者を殺すかの選択が与えられた場合、自動操縦はその運転者を保護しますか？  
マシンビジョンの進歩は非常に速いため、今では5年前のハードウェアでは実行できなくなったシステムでは、まったく新しいビジョンユニットを5年ごとに販売しなければならないことを想像できます。  
 私たちが進化して敵対的な活動に敏感になるにつれて、人々はセキュリティの脅威についてもより心配します。  
クレス[1921]が含まれています。日本では、トヨタとホンダに対するサイバー攻撃に続き、自動車業界のサプライチェーン全体のベースライン要件[1243]。  
ブリュッセルでは、当局は規制エコシステムがどのように対処できるかについて心配し始めました。  
。  
 中にはエンジニアがいない人もいます。弁護士と経済学者だけです。  
 当局は、2015年にディーゼルゲートの排出スキャンダルが発生した後、フォルクスワーゲンが排出ガステストをだますためのソフトウェアを車にインストールしたことが判明した後、業界の保証を信頼することに消極的になりました。  
脅威モデルは、もはや外部のハッカーではなく、ベンダー自体を含みました。  
彼らは何をする必要がありましたか？  
28.4.2安全とセキュリティ規制の近代化  
欧州の機関が安全性、プライバシー、消費者保護および競争をサポートするためにサイバーセキュリティの専門知識を必要としていることは明らかでした。  
 これを解決するために、「エイリアンレバレット、リチャードクレイトンと私は、医療機器、自動車、配電という、私たちがある程度知っている3つの産業を研究しました。  
完全なレポートには、ISO、IEC、NISTなどの組み込みデバイスの安全性/セキュリティ標準の既存のパッチワークの広範な分析が含まれています。  
使いやすさはいくつかの点で重要です。  
一部の国では、67歳以上の運転手に医療を受けるか、運転免許試験を再度受けるよう要求するとともに、シートベルトとエアバッグを強く要求しています。  
車のセキュリティは、テロリストがリモートで車を乗っ取って、歩行者に車を運転できるかどうかだけではありません。  
 見知らぬ人によって、または（可能性が高い）彼女が誘拐されるかもしれない  
 そして、エンジニアが彼女の安全を心配する必要があるのは誰ですか。自動車会社、配車会社、政府のどれですか。  
どのようにしてヨーロッパとアフリカに加え、日本、韓国、オーストラリアの自動車製造国を組み込みますか？自動車の3つの標準化ゾーンの1つであり、その他は南北アメリカと中国です。  
 これは、最低限の標準を設定することだけでなく、セキュリティの考え方を標準化団体、規制当局、試験施設、およびエコシステム内の他の多くの場所に組み込むことの問題でもあります。  
「英国の標準指」が誤って電化製品に突き刺されて、創造的な悪意の観点から考えることができるかどうかを注意深くチェックして作業するテストエンジニアを獲得することは難しいでしょう。  
 私たちはいくつかの推奨事項を考え出しました。  
最終的には、特に自動車のオートパイロットが致命的なクラッシュを引き起こした場合の責任をめぐる紛争がある場合、事故の調査において自動車データの使用を規制する法律が必要になります。  
 データがなければ、学習システムを構築することはできません。  
これは、上記のセクション28.2.9で説明したように、技術標準ETSI EN 303 645 V2.1 [646]によって部分的に達成されるように設定されています。  
ただし、ETSI規格に準拠していなくても、ロッテルダムの税関職員はおもちゃのコンテナを中国に送り返すことができません。  
  
別の勧告は、ヨーロッパは政策立案者を支援するためにヨーロッパ安全保障局を設立すべきであるというものでした。  
 これは、EUの政府機関間でのセキュリティ侵害の報告を調整しましたが、ヨーロッパの機関間の競合他社を望まない英国とフランスの情報機関によるロビー活動の結果、クレタ島に追放されました。2019年のサイバーセキュリティ法はこれを公式化した[655]。  
ENISAが時間とともにその能力と影響力を構築し、新しい安全基準がセキュリティにも適切な注意を払うことを期待してください。これには、少なくとも適切な開発ライフサイクル（推奨事項の1つ）が含まれます。  
セキュリティテクノロジーが実際に機能するには、機能だけでは不十分であり、テストや学習のインセンティブにも同じことが言えます。  
つまり、規制当局は製品のテストからシステム全体の保証に移行する必要があります（これが私たちの最終的な推奨事項でした）。  
  
私たちのレポートが長期的に見て最も深刻であると特定した問題は、製品の静的度が大幅に低下していることです。  
自動車のメカニズムには、セキュリティテストと安全性テスト、および更新を処理する手段が必要です。  
OEMとモバイルネットワークオペレーターが一緒に行動することができないため、ほとんどの2年前の電話にはパッチが適用されません。  
 自動車業界は6年以上にわたってソフトウェアのパッチ適用に対して責任を負うことを望まなかったため、これは政治的な戦いを開始しました。  
 ただし、新車の埋め込み炭素コスト（製造中に排出されるCO2の量）は、生涯の燃料燃焼とほぼ同じです。  
現在、廃車時の自動車の平均年齢は約15歳です。それを6つに減らすと、環境コストは許容できなくなります。  
ヨーロッパの機関で非常に準備の整った聴衆を見つけました。  
修理する権利の活動家は、循環型経済で家電製品を再利用できるようにキャンペーンしていました。テック企業が「セキュリティ」メカニズムを使用して修理を防止しようとしたり、修理を違法にしようとして乱用したりすることに腹を立てていました。  
消費者権利団体は、スマートデバイスの寿命が衝撃的に短いことを警告し始めていました。ベンダーがサーバーの保守を停止した1年後に、それが冷ややかなレンガに変わったことを知るためにのみ、「スマート冷蔵庫」に余分に費やすことができました[933]。 。  
以前は電球が長持ちしていました。生誕200周年の光は、1901年からリバモアで燃え続けています。  
政府は押し戻しました。フランスは2015年に製品寿命を短くすることを違法とし、Appleが2017年に古いiPhoneの速度を落とすためにソフトウェアアップデートを使用してユーザーに新しいものを購入するように促したことを認めた後、起訴されました。  
（これは5億ドル[966]の米国の集団訴訟を解決しました。）  
実際に、私はEurostarの電車に乗っていたときにMiraiボットネットがTwitterを停止し、ブリュッセルのセキュリティおよびITポリシー担当者約100人の聴衆に最初の発表を行ったことがわかりました。  
それは行動の必要性を示す完璧な例でした。  
。  
  
この指令は2019年5月に欧州議会を通過し[656]、2021年から施行されます。  
この表現は、商品自体のソフトウェア、商品が接続されているオンラインサービス、およびサービスを介してまたは直接商品と通信できるアプリを対象とするように設計されています。  
それは実際にはどういう意味ですか？  
実際、指令の前文には次のように記載されています。「消費者は通常、少なくとも販売者が適合性の欠如に対して責任を負う限り、更新を受け取ることを期待しますが、場合によっては消費者の合理的な期待がそれを超える可能性があります。特にセキュリティアップデートに関してそうかもしれないように、期間。」多くの国で、自動車は使用を続けるために毎年の路上走行性テストに合格する必要があり、そのようなテストにはソフトウェアが予見可能な将来に最新のパッチが適用されているかどうかのチェックが含まれる可能性が高いことを考えると、セキュリティパッチの要件がよくわかります10年を超えて延長する。  
アメリカの慣行は、安全性に関してヨーロッパに続くことがよくあります。  
28.5.2新しい研究の方向性  
ムーアの法則のおかげで、1960年代以降、コンピューターをほぼ消耗品と見なすようになりました。  
数千、さらに数百万のトランジスタをチップに詰め込んで、より精巧なパイプライン処理とキャッシングをサポートしています。  
10年後のテクノロジーは今日のものとはまったく異なるものになると信じて、独占をすくめました。そのため、市場の競争を市場の競争に置き換えることができます。ムーアの法則は現在、使い果たされています。  
パーティーが終われば、ゴミの片付けを開始する必要があります。  
まだまだあります。  
（最も人気のあるLetsencryptは2021年にロールオーバーされます。）  
コンシューマデバイスでは、暗号を更新可能にするために、ライフタイムを短くする傾向があります。セクション21.6で説明したように、SafariやChromeなどのブラウザーは398日間の証明書の有効期限を強制し始めており、これは頻繁な更新に対するもう1つの強力な動機です。  
建物や土木工学プロジェクトのシステムは、いくぶんハイブリッドです。一部のベンダーは、可能な限り安定して25年間維持されることが期待されるバージョンのLinuxに取り組んでいますが、他のベンダーは、システム全体のより積極的な定期的な更新を求めており、「すべてをクラウドに置く」ように要求しています。  
複数の請負業者や下請業者が、変電所から空調、火災警報器、盗難警報器まで、建物に関する完全なエンジニアリング情報を含むシステムへのオンラインアクセスが必要になると、明らかなリスクがあります。  
それでよろしいですか？  
この適応によって生じた緊張は、今後10年間で政策、起業家精神、研究において重要になると思います。  
 最初のパイロットプロジェクトとして、Laurent Simon、David Chisnall、および私は暗号化ソフトウェアのメンテナンスに取り組みました。  
問題の1つは、OpenSSLなどの暗号化実装に、通常、暗号化操作を一定の時間で実行するように設計されたコードがあるため、使用中のキーが外部のオブザーバーに漏洩せず、キーマテリアルを含むメモリの場所をゼロ化することです。または他の機密データ。これにより、同じマシンの他のユーザーもキーを推測できなくなります。  
それはそれらを離れて最適化し、突然何百万ものマシンすべてが安全でない暗号ソフトウェアを持っています。  
私たちのツールスミスは敵ではなく味方でなければならないので、これを適切に修正するために何が必要かを考え出しました。  
コンパイラに一定時間のコードを実行させ、オブジェクトの削除を適切に保護することは、驚くほどトリッキーであることが判明しましたが、結局、LLVMのプラグインの形で機能の概念実証が得られました[1758]。  
低レベルのコンパイラー内部から中レベルの安全システムに移行すると、自動車業界が直面している大きな課題は、事故データをそこから学ぶことができる利害関係者に提供することです。  
世界中で、年間100万人が亡くなっています。  
ますます、データはベンダーのサーバーと破損した車両にあります。  
緊密に争われた訴訟がある場合、データが要求される可能性がありますが、ベンダーはそれを共有することに消極的であり、通常、裁判所命令が必要です。  
 私たちは学習システムを目指すべきです。  
私たちは更新をプッシュして、それが再び起こるのを止めることができると期待するべきです。  
 航空業界では、事故が監視されており、パイロットや航空管制官などのオペレーターだけでなく、航空機や支援地上システムの設計者にもフィードバックが送られています。  
そこでも、キーは、有害事象を監視し、データを収集するための必須システムです。  
自動車の自律性が高まるにつれ、自動車の学習システムも必然的になっていますが、それだけでは学習しません。  
手始めに、自動車が感知したもの、彼らが何をすることにしたか、そしてその理由からのきめの細かいデータが必要になります。  
現在、EU加盟国は車両規格の市販後調査に責任を負っているので、ほとんど実施されておらず、ディーゼルゲートに続いて欧州委員会に監視権限を与える提案が出されています。  
安全、プライバシー、および管轄権に関する複数の対立する権利に対処する必要があるため、それらは大きく複雑になります。  
テクノロジーが急速に変化している間、私たちはおそらくプライバシーと競争に対するさまざまな害を容認することができました。  
Google+はあまりにも不格好でしたか？  
しかし、ムーアの法則が機能しなくなると、鉄道が19世紀の後半と20分の1の3分の1を支配したのと同じように、現在の支配的な企業はしばらく支配的であり続けるかもしれません。  
独占禁止法に対する考え方を一新する必要があります。法律が今から20年後にどのように見えることを望みますか？  
   
昔、セキュリティエンジニアリングプロジェクトの大きな問題は、いつ完了したかを知る方法でした。  
今、世界は異なります。  
セキュリティの評価と保証のスキームは、さまざまなエコシステムで育ちました。  
安全認証スキームは、ヘルスケア、航空宇宙、道路車両など、さまざまな業界で別々に進化しました。  
すべてが接続性を獲得している今、あなたはセキュリティなしでは安全性を持つことができず、これらのエコシステムは融合しています。  
これは、ソフトウェアライフサイクルの標準を超えて、新しい危険や攻撃からでも迅速に回復できる学習システムの目標に向かって進みます。  
20世紀に戻ると、多くのベンダーが情報セキュリティの権利を手に入れませんでした。  
将来的には、製品が故障したときに合理的に迅速に製品を修正し、妥当な期間、製品を修正することが求められます。  
テクノロジーによって私たちに与えられた安全とセキュリティのコストは、広い意味では、主権の国家的アイデア、そしてより実践的なレベルでは、個人の行動では達成できない目標を集合的行動で達成する人々の能力と緊張が高まります。または市場の力。  
研究の問題上記のセクション28.5.2で説明する持続可能なセキュリティの大きな課題に加えて、保証に関しては他にも多くの未解決の問題があります。  
2番目の問題の束は、安全性とセキュリティの世界がゆっくりと融合しているように、2つの銀河がゆっくりと融合しているように、安全エンジニアとセキュリティエンジニアがお互いの言語を話せないことがわかったためです。互換性のない標準のセット、さらには標準化への互換性のないアプローチ。  
もう1つの大きな機会は、実際に配備されたシステムを改善するための軽量メカニズムです。  
私たちは、開発の隅々まで進んでいる企業から生じる多くの実際の問題を抱えています。  
 また、暗号ライブラリやデバイス権限などのツールのセキュリティユーザビリティ標準を設定する可能性はありますか？  
 さらにもう1つは、展開前と継続的な評価の両方のためのAI / MLシステムのテストです。  
論争の的となる社会問題に触れると、学習システムはどのようになりますか？  
 企業がとるセキュリティ、プライバシー、安全工学の決定が、公の精査と法的異議申し立てに開かれていることをどのように保証するのでしょうか？  
彼らの熱意は、宗教の味さえも持つことができます。