情報化時代の大きな幸運は、閉じ込められた顧客の大規模なインストールベースで使用される独自のアーキテクチャを確立している企業の手にかかっています。  
  
– EARL BOEBERT  
法律は、コモンズからガチョウを盗む男性または女性をロックしますが、誰がガチョウからコモンズを盗む大悪役を解き放ちます。  
8.1はじめに  
実際、セキュリティメカニズムは多くの場合、意図的に責任をシフトするように設計されており、さらに深刻な問題につながる可能性があります。  
しかし、複数の所有者がいる複雑なシステムで生じる悪意のあるインセンティブは、セキュリティエンジニアにとって経済的な問題をより重要かつ微妙なものにします。  
私たちが得る結果は、通常、市場の均衡であり、驚くほど安定していることがよくあります。  
マクロレベルでは、スマートフォンがラップトップに置き換わり、社会がソーシャルネットワークに移行し、サーバーがクラウドに移行するなど、テクノロジーは完全に変化しましたが、サイバー犯罪のパターンは2010年代を通じて非常に安定しています。  
一般に、インセンティブがない限り、人々は行動を変えません。  
しかし、市場は失敗する可能性があります。コンピュータ業界は、当初から独占に悩まされてきました。  
セキュリティ経済学は、2000年代初頭以来、学問分野として急速に発展してきました。  
たとえば、プログラマーとテスターに​​よる作業の最適なバランスはどれですか。  
 また、サイバー犯罪のコストやそれに対する最も効果的な対応など、多くの重要な政策問題を分析することもできます。  
また、公的活動と私的活動のバランスについての質問もあります。保護活動のどれだけを個人に任せるべきか、そしてどれだけベンダー、規制当局、または警察が負担すべきか？  
この章では、最初に、古典的な経済モデルで独占を分析する方法、情報商品とサービス市場がどのように異なるか、ネットワークの影響と技術的なロックインによって独占が起こりやすくなる方法について説明します。  
次はゲーム理論です。これにより、人々が協力するのか競争するのかを分析できます。また、オークション理論により、インターネットの大部分を牽引している広告市場の仕組みと、それがどのように失敗するかを理解できます。  
また、システムの信頼性が本来よりも低い理由、つまり、脆弱性が多すぎる理由、およびサイバー詐欺師が巻き込まれない理由も理解できます。  
8.2古典経済学  
これまでセキュリティに適用されてきた部分は、主にミクロ経済学、ゲーム理論、行動経済学に基づいています。  
私の目的は、経済学に関するチュートリアルを提供することではなく、基本的な言語とアイデアを理解して、安全保障経済学について話し合うことです。  
1776年、アダム・スミスの古典的な「国民の富」[1788]は最初のドラフトを提供しました。彼は自由市場における合理的な自己利益が進歩にどのようにつながるかを説明しました。  
彼の有名なフレーズで、「私たちが夕食を期待できるのは、肉屋、醸造者、またはパン屋の慈善からではなく、彼ら自身の興味に対する彼らの配慮からです。」同じメカニズムがファーマーズマーケットや小規模な工場から国際貿易まで拡大します。  
JevonsとMengerからの洞察の1つは、競争の激しい市場で平衡状態にある財の価格は、生産の限界コストであるということです。  
価格が下がった場合、これらの鉱山は閉鎖されます。それが上がった場合、さらに多くの限界地雷が開くでしょう。  
（また、今日の多くのオンラインサービスが無料である理由についての洞察も得られます。情報を複製するための限界コストがほぼゼロであるため、多くのオンラインビジネスはそれを販売できず、他の方法でお金を稼ぐ必要があります。広告から。  
 19世紀の終わりまでに、アルフレッドマーシャルは、商品、労働力、資本の市場での需要と供給のモデルを、均衡ですべての過剰な利益が奪われ、経済が効率的に機能している。  
経済学への関心の多くは、これらの条件の1つ以上が満たされていない状況に由来しています。  
エコノミストはこれらの外部性を呼びます、そしてそれらはポジティブまたはネガティブのいずれかです。その結果、研究者は彼らの仕事の利益を完全に捉えることができず、理想よりも少ない研究しか得られません（経済学者は、理想的な量の研究の4分の1しかしないと考えています）。  
負の外部性の例は環境汚染です。石炭を燃やすと、家を暖めることでプラスの効果が得られますが、隣人は臭いや灰のマイナスの影響を受けますが、誰もがCO2排出量の増加というマイナスの影響を共有しています。  
1人のプレーヤーが市場の清算価格よりも多く請求する十分な力を持っている場合、または共通の問題を解決する力を誰も持っていない場合、市場だけでは問題を解決できない可能性があります。  
それでは、さらに詳しく見ていきましょう。  
8.2.1独占  
大学の町にアパートの市場があり、学生の収入が異なるとします。  
 少なくとも1000は、少なくとも月額1000ドルを支払う準備ができています。  
図8.1：アパートの市場したがって、多くの競合する家主が1000のアパートを賃貸している場合、市場清算価格は、需要曲線と垂直供給曲線の交差点、つまり$ 1000になります。  
独占的な家主が需要曲線を調べたところ、賃貸しているアパートが800室しかない場合、それぞれのアパートで月額1400ドルを稼ぐことができます。  
（経済学者は、彼の「収益ボックス」は図8.1のEDGOではなくボックスCBFOであると言います。）  
これは明らかに非効率的であり、イタリアの経済学者Vilfredo Paretoはこれを形式化するための巧妙な方法を発明しました。  
ここでは、独占者が誰かに1つの空のアパートを低価格で貸し出し、彼と彼らの両方をより良い状態にすることができるため、割り当ては効率的ではありません。  
 そして完璧な独裁政権（王は多くを得る）  
どちらの場合も、誰かを悪化させることなく、誰かをより良くすることはできません！しかし、ここで説明されている単純な独占は、この非常に弱い意味でも効率的ではありません。  
 1つの可能性があります。もし彼がすべての人に異なる価格を請求できる場合、彼は各学生の家賃を彼らが支払う準備ができている正確に設定することができます。  
同じ学生が以前と同じようにアパートを取得しますが、彼らのほとんどすべてがより悪い状態にあります。  
差別的な独占者は、すべての消費者余剰を抽出することに成功しています。  
あなたが彼の価格を値下げすることを期待しているイスタンブールのカーペット売り手は、最初の、ビジネスの、そして牛のクラスの座席を売っている航空会社がそうであるように、このゲームをしている。  
市場支配力は、商人が独占者であることへの近さの尺度です。独占の下では、商人は価格設定者であり、完全な競争の下では、市場が確立するどんな価格でも受け入れなければならない価格担当者です。  
情報の非対称性は、いくつかの方法でそれらを助けることができます。  
そのため、商人は固定価格を表示するよりも、せりふを好むかもしれません。  
価格比較サイトのおかげで、乗客は基本価格についての良い情報を持っていますが、満席に割引を行う場合、広告エコシステムからの情報を使用してそのオファーをターゲットにできる可能性があります。  
テクノロジーは、企業を航空会社に似たものにし、小さなカーペット店に似たものにしない傾向があります。情報の非対称性は、平均価格について知っているかどうかに関係なく、システムがあなたについて知っていることと、それがどのようにあなたを固定するかと同じです。  
私たちの例の家主やカルテルのような古典的な独占者は、単にすべての人の価格を押し上げる可能性があり、その結果、消費者余剰が明らかに失われる可能性があります。  
19世紀後半、鉄道会社は、収益性、商品の傷みやすさ、その他の要因に応じて、さまざまな顧客にさまざまな運賃を請求しました。基本的には、支払い能力に応じてすべてを揺さぶっています。  
同じように、電話会社は狂ったように価格差別をしていた。 SMSはかつては音声よりもはるかにコストがかかり、音声はデータよりもはるかに高額でした。  
これはまだ乱闘スペースであり、FCCのトランプ大統領の任命者は以前の多くの正味の中立性の決定を覆しました。  
、顧客の値下げ。  
しかし、テクノロジーにおける独占力については疑いの余地はありません。  
 1990年代に2人（MicrosoftおよびIntel）  
 しかし、それぞれがその分野を支配しています。 ArmはIntelと競合することができましたが、2009年のBing以来、新しい検索スタートアップはありません（市場シェアは低下しています）。。  
EUは、技術違反を犯すために複数回技術専攻を定めてきました。  
  
情報通信産業は、多くの点で従来の製造業とは異なり、最も顕著なのは、これらの市場が世代に非常に集中していることです。  
鉄道でも、運河でもその前にほとんど同じことが起こりました。  
IBMは1960年代と70年代にコンピューター業界を支配し、その後Microsoftが登場して90年代にポールポジションを獲得しました。  
なぜそうなのでしょうか？  
8.3.1情報市場が異なる理由  
しかし、ほとんどゼロの情報については！そのため、オンラインには無料のものがたくさんあります。ゼロはその公正価格です。  
例として百科事典を考えてみましょう。 Britannicaは32巻で1,600ドルのコストがかかりました。その後、MicrosoftはEncartaを49.95ドルで売り出し、Britannicaに安いCD版を生産するように強いました。そして今、無料のウィキペディアがあります[1718]。  
また、無料のサービスや非常に安価なサービスと競争するのは難しく、開始するために必要な設備投資を取り戻すのは困難です。  
第2に、ネットワークの外部性がしばしばあり、それによってネットワークの価値がユーザー数において直線的に増加することはありません。  
2000年代半ば以降、ソーシャルメディアでも同じことが起こりました。当初はソーシャルネットワークを運営する新興企業が40〜50社ありましたが、Facebookが牽引し始めると、突然すべての若者がそこにいなければなりませんでした。そこに友達がいたので、そこにいないと、パーティーの招待状。  
また、2種類のユーザーが集まる両面市場でも運用できます。  
ですから、いったん論文が出ると、それはしばしば地元の独占に成長しました。競合他社が侵入するのは困難でした。  
IBMメインフレームがコンピューティングを支配した1960年代にも同じパターンが見られました。多くのユーザーがIBMを購入したのに対し、多くのユーザーがIBMを購入したのに対し、企業はIBM向けのソフトウェアを開発していたためです。  
もう1つの勝者は1990年代後半のeBayでした。オークションに参加したい人の多くは、より多くの入札者を引き付けるため、最大のオークションを利用したいと思うでしょう。  
第三に、比類のない量のユーザーデータへのアクセスから、多数のA / Bテストを実行してユーザーの優先順位を理解し、システムパフォーマンスを最適化する機能まで、さまざまなサプライサイドスケールエコノミーがあります。 。  
第4に、相互運用性またはその欠如に起因するロックインがしばしばあります。  
これには技術的要素と人間的要素の両方があり、後者がしばしば支配的です。プログラマを再訓練するよりも、ツールを置き換える方が安価です。  
これらの切り替えコストは移行を阻止します。  
これらの4つの機能（限界費用が低い、ネットワークの外部性、供給側のスケールエコノミー、技術的なロックイン）を個別に使用すると、支配的な企業のある産業につながる可能性があります。組み合わせて、彼らはさらに可能性が高くなります。  
 その後、最大の市場シェアを獲得すると予想されるベンダーから論理的に購入します。  
8.3.2ロックインの価値  
 すべての顧客の[1718]。  
LibreOfficeなどの無料プログラムに移行することで、この15,000ドルを節約できるため、この製品のインストール、スタッフの再トレーニング、ファイルの変換などのコスト、つまり総スイッチングコストが15,000ドル未満の場合、 。  
ロックイン、価格設定、および値の間のリンクの例として、価格が10年間でどのように変化したかを考えます。  
2019年にこのエディションを書き始めたとき、スタンドアロンのOfficeが59.99ドルから164ポンドの価格で販売されているのを見ました。  
 大学は、選択するオプションと交渉の良さにもよりますが、シートあたり数十ポンドの費用がかかります。また、Googleは、組織を無料サービスから、ほぼ同じコストの有料G Suiteバージョンに移行しようとしています。  
2020年にこの章を改訂したとき、昨年スタンドアロン製品の約2倍のコストで「ライフタイムキー」を取得できるようになりました。  
ロックインは、なぜ標準戦争と独占禁止法訴訟にそれほど多くの努力が費やされるのかを説明しています。  
。  
このような場合、可能性のある攻撃者は悪意のある外部者ではなく、機器の所有者、または互換性のある製品を作成することによって既存企業に挑戦しようとする新しい企業です。物事を厳しく制限しすぎると、ビジネスにとっても悪影響が出る可能性があります。イノベーションはしばしば増分的であり、新しい企業がキラーアプリケーションを見つけて製品が成功するためです[903]。  
確かに、IBM PCがApple Macよりもオープンだったという事実は、その支配的なデスクトッププラットフォームになる要因の1つでした。  
 そのため、多くの国の法律により、企業は互換性のために競合他社の製品をリバースエンジニアリングする権利を与えられています[1647]。  
クラウドサービスや暗号化などのデジタルコンポーネントを使用して製品をロックダウンするため、競合他社がこれらの製品のリバースエンジニアリングを試みる法的権利を持っている場合でも、実際に成功するとは限りません。  
これらのより複雑なエコシステム戦略については、セクション8.6.4で詳しく説明します。  
8.3.3非対称情報  
私たちは、昔ながらのカーペットトレーダーが自分の店で買い物をする観光客よりも情報の利点を持っていることを話し合いました。しかし、非対称情報の正式な研究は、1970年に「レモンの市場」[34]に関する有名な論文によってキックオフされ、ジョージアケルロフがノーベル賞を受賞しました。  
売り手はどちらがどちらかを知っていますが、買い手は知りません。  
 1500ドルと思うかもしれません。しかし、その価格では、良い車は販売されません。  
これが、新しい車を購入すると、ディーラーの駐車場から2度目に車を運転したときに、20％が価格を下回る理由です。  
ユーザーが良いことと悪いことを区別できない場合は、最も安いものを購入することもできます。  
（最近、マルウェア作成者はリリース前にすべての利用可能な製品に対してコードをテストするため、AVを購入する理由ははるかに少なくなっています。代わりにパッチシステムに焦点を当てる必要があります。  
 隠された情報と隠されたアクションをさらに区別することができます。  
これは、自分が悪いドライバーであることを知っている人々がボルボを購入して殺される可能性が低くなるためか、ボルボの人々が安全で速く運転できると信じているためですか？  
両方の効果はセキュリティにおいて重要であり、特定のケースでは両方が組み合わさることがあります。  
これは、義務的なシートベルト法が全体の命を救うのではなく、単に車の乗員から歩行者や自転車に死者を移動させる傾向がある理由も説明しています[19]。  
。  
  
ポジティブな外部性の興味深いケースは、彼らがそれを望んでいるかどうかに関係なく、誰もが同じ量の何かを得るときです。  
エコノミストはこれらの公共財を呼び、正式な定義はそのような物品は非競争的であるということです（私がそれらを使用することはあなたにとってより少ないという意味ではありません）  
。  
公共財は、国防と同様に政府によって直接供給されるか、または特許や著作権に関する法律などの間接的なメカニズムを使用して、人々に一時的な独占権を与えることで発明、書籍、音楽を制作するよう促すことができます。  
。  
私の家の屋根には対空砲はありません。航空防衛の脅威は少数の関係者から来ており、政府の行動によって最も効率的に対処されます。  
 確かに強い外部性があります。安全でないマシンをインターネットに接続する人々は、悪意のある人物がボットネットを構築することを可能にするため、他の人にコストを投じることになります。  
それで私たちはそれについて何をすべきですか？  
セクション2.3のサイバー犯罪の簡単な調査では、マルウェアの作成者、スパマーなどが商業化するにつれて、多くの脅威が統合されていることに気付きました。  
 攻撃：1つの主要なDoS for-hireプロバイダーがあるようです。  
脆弱性を発見した研究者に報酬が支払われ、ソフトウェアが含まれている企業に課された罰金によって支払われる、より穏やかな政府の対応を想像する人もいます。  
しかし、皮肉屋は実際に起こることは脆弱性がサイバー武器メーカーに売られ、政府がそれらを備蓄し、それを備蓄することであり、業界はNotPetyaのように付随的損害の支払いをすることを指摘するでしょう。  
 これはゲーム理論につながります。  
8.4ゲーム理論  
それは、私たちが協力するときと、戦うときです。  
あなたは何か有用なものを作り、それを交換します。または、必要に応じて、力を入れて、投票箱などを持ちます。  
それらを研究および分析するために使用できる主なツールは、ゲーム理論です。独立した意思決定者間の協力と対立の問題の研究です。私たちは戦略ゲームに興味があり、詳細の多くを抽象化して決定の核心に到達しようとします。  
これを図7.2のように記述します。ボブアリスH T H -1,1 1、-1 T 1、-1 -1,1図7.2 –一致するペニーテーブルの各エントリは、最初のアリスの結果、次にボブの結果を示しています。  
 アリスはペニーを失い、ボブはペニーを得る。  
多くの場合、このようなペイオフマトリックスを作成することで、ゲームをすばやく解くことができます。  
：Bob Alice左上1、2 0、1下2、1 1、0図7.3 –支配的な戦略の均衡ゲーム理論では、戦略はゲームの状態を取り、move1を出力するアルゴリズムにすぎません。  
各プレイヤーには支配的な戦略があります。他のプレイヤーが何をするかに関係なく、最適な選択です。  
これを支配的な戦略均衡と呼びます。  
アリスの選択がボブの場合に最適である場合、およびその逆の場合、2つの戦略はナッシュ均衡にあると言います。  
支配的な戦略の均衡がグローバルな最適である一方で、それらをローカルのオプティマのように考えることができます。  
8.4.1囚人のジレンマ  
それは、1950年に米国とソ連の国防費に関連してランド社の科学者によって最初に研究されました。ランドは、核戦争における可能な戦略について考えるために支払われました。  
銀行強盗を計画している疑いで2人の囚人が逮捕されました。  
片方だけが自白した場合、彼は自由になり、もう一方は強盗の陰謀のために6年の猶予があります。  
 ペイオフマトリックスを次に示します。ベンジーが告白するつもりなら、私も6年ではなく3年になるはずです。そして、彼がビジネスと政治において、一連の動きによって独占権力や軍事的優位性などの権力を獲得する手段である戦略に行く場合、ゲーム理論上の意味は、問題を扱いやすくするために、やや単純化されたバージョンです。  
Benjyも同様に推論します。  
これは単なるナッシュ均衡ではありません。それは支配的な戦略均衡です。  
しかし、待ってください、彼らが静かにしておくことに同意した場合、彼らはそれぞれ1年を過ごすでしょう、それは彼らにとってより良い結果です！実際の戦略（deny、deny）  
（これが、「最高」について論じるだけでなく、「パレート効率」や「支配的な戦略の均衡」などの概念を持つことが有用である1つの理由です。）  
 まあ、ゲームが一度だけプレイされ、これが町で唯一のゲームである限り、解決策はありません。  
正しく機能するため、これは十分に公正であると考えるかもしれません。  
肥満や中毒などの自制心さえ、未来の自分との協調の失敗と見ることができます。  
ゲーム自体を変更できる場合にのみ、これを変更できます。  
実際には、囚人のジレンマゲームは、均衡がより効率的な別のゲームに変換するようにルールまたはコンテキストを変更することによって変更されます。  
8.4.2繰り返される進化的なゲーム  
そしてもちろん、彼らが協力するインセンティブがあるかもしれません。  
1970年代に、ボブアクセルロッドは、人々が囚人のジレンマを何回もプレイするかについて考え始めました。  
彼は全体として最良の戦略の1つが一生懸命であることに気づきました。つまり、ラウンド1で協力し、その後の各ラウンドで、前のラウンドで相手がしたことを相手に行います[147]。  
たとえば、ノイズが存在する場合、プレイヤーは（欠陥、欠陥）に閉じ込められる傾向があります  
したがって、この場合は、他のプレーヤーを時々「許す」のに役立ちます。  
彼らは、あなたが攻撃的で従順な個人、「鷹」と「鳩」の混合集団がいる場合にどうなるかを考えました。鷹は鳩から餌をとります。そして、タカの戦い、死のリスクがあります。  
すると、ペイオフマトリックスは図7.6のようになります。HawkDove Hawk vffic 2、vffic v、0 Dove 0、vv 2、vドミナント戦略、ただしc> vの場合（ファイトが高すぎる）  
v =（1 ffi p）  
言い換えれば、集団内に攻撃的で従順な個人を共存させることができ、攻撃的個人の割合は攻撃的コストの関数になります。戦闘が危険であるほど、戦闘に参加する個人の数は少なくなります。しかし、社会が均衡に移行するには、何世代もかかります。  
実際、人類学者は、部族戦争はそのような社会ではかつては風土病であったと信じています。考古学的記録は、州が来るまで、男性と少年の約4分の1から3分の1が殺人で死亡したことを示しています[1132]。  
このような洞察は、ボブアクセルロッドのシミュレーション方法論とともに、道徳哲学者から進化ゲーム理論に関心のある動物行動の学生まで多くの人々を獲得しました。  
多くの霊長類は作り付けの公平感を持ち、浮気していると見られる個人を罰することが判明しました-復讐の本能は社会性を強化するための1つのメカニズムです。  
たとえば、ハトが互いを認識して優先的に相互作用できる場合、ハトはタカに対してより良い結果を得ることができ、いくつかの社会運動およびおそらくいくつかの宗教でさえも自分自身を確立する方法のモデルを与えます[1784]。  
もちろん、tit-for-tatの背後にある基本的な考え方は、かなり前に遡ります。  
最近になって、トーマス・ホッブズは、17世紀にも同様の議論を用いて、国家は王の神権の存在を必要とせず、革命、共和国、憲法への道を開きました。  
同僚と私は進化ゲームを使用して、反政府勢力がどのようにセルに組織化されるかをモデル化しました[1373]。  
たとえば、英国のインターネットサービスには、ローカルループを提供する規制された独占、およびインターネットサービスを家庭に販売する競合小売企業が含まれます。  
 まあ、もし誰かが他の人を打ち負かすとしたら、彼らは皆、彼ら自身の価格を引き下げて脱北者を罰することによって報復するでしょう。  
航空会社が顧客を混乱させるためにあらゆる種類の取引、航空マイルなどを提供するのと同じように、通信プロバイダーも独自の混乱価格を提供しています。  
暗黙の共謀は、会社の幹部が実際に座って固定価格に同意することなく、両方の業界で発生する可能性があります（これは違法になります）  
価格設定がよりアルゴリズム的になるにつれて、弁護士と経済学者の両方がより多くのコンピュータサイエンスを理解する必要があるかもしれません。コンピュータ科学者は、ゲーム理論やオークション理論などの経済分析ツールを理解する必要があります。  
8.5オークション理論  
多くのオンライン活動は、GoogleやFacebookなどの企業が運営する広告オークションによって賄われており、多くのeコマースサイトはオークションとして運営されています。  
彼らはユニークな商品の価格を発見する基本的な方法です。  
以下の5つの従来のタイプのオークションを検討してください。  
英語または昇順のオークションでは、競売人は最低価格で開始し、入札者が1人だけになるまで価格を上げます。  
2。  
これは、花の販売に使用されます。  
ファーストプライスの密閉入札オークションでは、各入札者が1つの入札を行うことができます。  
これは、テレビの権利のオークションに使用されています。政府の契約にも使用され、落札した最低価格です。  
セカンドプライスの密封入札オークション、またはビックリーオークションでは、密封された入札も行われ、最高入札価格が落札されますが、その入札者は2番目に高い入札価格で価格を支払います。  
5。  
これは、いくつかのハイテクスタートアップ間の戦争、訴訟、または勝者総取りの競争のモデルです。  
最初の重要な概念は、戦略的同等性です。  
同様に、イングリッシュオークションとヴィックリーオークションは同じ結果になります（入札単位を法として）  
ただし、2つのペアは戦略的に同等ではありません。  
2番目の重要な概念は、収益の同等性です。  
ここで興味深い結果は、収益の等価性の定理です。これは、理想的な条件下で適切に動作するオークションから同じ収益が得られることを示しています。  
 および独立した評価（入札者間の外部性なし）  
このような状況では、入札者は戦略を調整し、イングリッシュ、オランダ語、および全額オークションはすべて同じ結果になります。  
詳細と例については、Paul Klempererの本[1057]を参照してください。  
すべてのバイヤーが競売に参加する入札リングが存在する場合があります。ここでは、ランクを破るのに2人ではなく1人の脱退者しか必要としないため、ファーストプライスオークションが最適です。  
第3に、エントリの抑止力があります。企業買収の入札者は、他の入札額を上回ると宣言することがよくあります。  
第5に、シグナリングゲームがあります。米国のスペクトラムオークションでは、入札者の入札の最下位桁に郵便番号を入れることで匿名性を破り、彼らが戦う準備ができたエリアの組み合わせを知らせ、競合他社がそこで入札戦争を始めるのを阻止しました。広告オークションは大企業であり、Google、Facebook、およびAmazonは2019年にそれぞれ約500億ドル、300億ドル、100億ドルを稼ぎ、その他の業界は約400億ドルを獲得しています。  
入札者は双方向で価格を支払うことを提案し、プラットフォームは広告の関連性とクリック率に基づいて広告品質をeiと推定します。  
私の広告があなたのクリックの5倍クリックされる可能性が高い場合、10cの私の入札は50cの入札と同じくらい良いという考えです。  
したがって、5倍の広告品質がある場合は、10cで入札し、40cで入札した場合、広告を取得して8cを支払います。  
ただし、落とし穴が1つあります。  
あなたの広告が良いクリックベイトであり、人々がそれらをクリックした場合、あなたはより少なく支払います。  
オークション理論と経験的データはどちらも、プラットフォームの収益を最適化するための推進力がこれまで以上に極端なコンテンツにつながる可能性があることを示しています。フィルターバブルの影響。これはユーザーの操作によるものではありません[40]。  
実際、イギリスでは、テレビなどの選挙広告やタバコなどの他のカテゴリは許可されていません。  
また、ソーシャルメディアが極端なコンテンツを宣伝する唯一の方法は広告の価格設定ではありません。元Google社員のTristan Harrisが説明したように、プラットフォームのレコメンダーアルゴリズムは、サイトでの滞在時間を最大化するように最適化されています。つまり、フィードやフォロワーをスクロールするだけでなく、不安や怒りに偏っています。  
これはすべて、経済学と心理学の境界で厄介な政治問題を引き起こしますが、オークション理論などの経済的ツールを使用して、それらを取り除くことができます。  
8.6セキュリティと信頼性の経済性  
しかし、1945年以降、核兵器は国の生存を経済力から切り離すと考えられ、経済学と戦略研究の分野はバラバラになりました[1238]。  
2000年頃、私たちの多くは、一見して不合理であるように見える永続的なセキュリティ障害に気づきましたが、さまざまなアクターが直面しているインセンティブをより注意深く見たときに、それは理解し始めました。  
Hal Varianは、ベンダーが期待するほどウイルス対策ソフトウェアに多くのお金をかけなかった理由を調査しました[1943]。  
当時、私はこの本の初版を書いていましたが、インセンティブ問題として問題の多くを説明すると、説明がはるかに説得力のあるものになることがわかりました。そのため、本の最終的な編集から学んだことを「情報セキュリティが難しい理由–経済的展望」という論文にまとめました。  
彼らが登場するまでに、9/11攻撃が起こり、人々はセキュリティに関する新しい見方を探していました。  
（後で、私たちは患者の安全の失敗がしばしば同様の根を持っていることを発見しました。）  
ネットワーキングの研究者たちは、オークション理論を使用して、戦略を証明できるルーティングプロトコルを設計し始めました。  
マイクロソフトは標準の経済性について考えていました。  
浮上し始めた絵は、システムのセキュリティが失敗したというものでした。システムを保護しているのは、失敗のコストを被った人々ではないからです。  
言い換えると、セキュリティはしばしば権力関係です。特定のシステムでそれが何を意味するかを制御するプリンシパルは、多くの場合、それを使用して自分の利益を前進させます。  
しかし、主題を真剣に研究し始めると、それだけではないことに気づきました。  
8.6.1なぜWindowsはそれほど安全ではないのですか？  
マイクロソフトの支配的な市場での地位にもかかわらず、なぜWindowsはそれほど安全ではないのですか？  
特にMicrosoftには真の競争相手がいないため、コモディティプラットフォームで行われた同等の取り組みが見られないのはなぜですか？  
そのようなレースでは、1990年代のマイクロソフトの哲学–「火曜日に出荷してバージョン3までに正しくする」–は完全に合理的な行動です。  
セキュリティはアプリケーションの邪魔になり、とにかくレモン市場になりがちです。  
次に、セキュリティを強化するかもしれませんが、顧客のロックインを最大化するように設計したり、デジタルメディアなどの新しい市場の補完者にアピールしたりするように誘惑されます。  
製品は最初は安全ではなく、時間の経過とともに改善されますが、新しいセキュリティ機能の多くは、ユーザーと同じくらいベンダーの利益になります。DOSはまったく保護されておらず、マルウェア市場を立ち上げました。 Windows 3とWindows 95は恐ろしいものでした。 Windows 98の方がわずかに優れていました。そしてセキュリティの問題により、最終的に2003年にビルゲイツはすべてのエンジニアが安全なコーディングコースを終えるまで開発を中止することを決定し、Microsoftの顧客をいらいらさせました。  
悪用可能な脆弱性の数と寿命は、Windowsのその後のリリースを通じて減少し続けました。  
Peter Gutmannが指摘するように、プレミアムビデオコンテンツの保護には、ユーザーのクレジットカード番号の保護よりもはるかに多くの労力が費やされました[842]。  
素敵な新しいプリンターを39.95ドルで購入し、わずか数か月後に、それぞれ19.95ドルで2つの新しいプリンターカートリッジが必要だという嫌悪感を見つけます。  
アプリケーション開発者から見ると、ロックインに基づく標準競争のある市場は、このように見えます。  
貧困層の消費者の観点からすると、「貧しい人々の安全、それから誰かの安全」と表現することができます。  
支配的な地位を確立するために競争するとき、ベンダーは製品を設計するように誘惑され、セキュリティ管理のコストのほとんどがユーザーに捨てられます。  
これは、1990年代半ばにMicrosoftとNetscapeがブラウザ市場の優位を争うために採用されました。  
それでも、ユーザーのコンプライアンスコストをダンプすることは、当時は完全に理にかなっています。 SETなどの競合するプロトコルは、オンラインで商品を購入したいすべての顧客に証明書を発行するコストを銀行に課し、コストが高すぎます[524]。  
不良品や商品に対してもネットワーク効果があります。  
感染するWindowsマシンの数が増えるだけで、2010年代–奇妙な均衡につながり、ラップトップにもっとお金を払う用意ができている人々は、ソフトウェアをあまり実行していなかったとしても、より安全なマシンを持つことができます。  
（そこでは、Appleのアプリストアのより厳しいポリシーが市場シェアよりも重要になっています。）  
8.6.2パッチ適用サイクルの管理  
脆弱性を発見した場合、それを公開する必要があります。これにより、ベンダーはパッチを適用しなければならなくなりますが、そうするまで何ヶ月も人々にさらされる可能性がありますか？  
 この議論は長い道のりを戻ります。序文で述べたように、ビクトリア朝の人々はロックピッキングに関する本を出版することが社会的責任であるかどうか悩み、結局それは[1895]であると結論付けました。  
安全保障経済学は、この種の問題を議論するための理論的および定量的フレームワークの両方を提供します。  
しかし、現実の世界は実際にそうですか？  
 これは大きな政策論争につながりました。  
Ashish Aroraや他の人々は、公開によりベンダーがより迅速にバグを修正したことを示すデータで対応しました。攻撃は当初増加しましたが、報告された脆弱性は時間とともに減少しました[133]。  
つまり、適切な状況では、ソフトウェアは牛乳よりもワインのようになり、年齢とともに向上します。  
 いくつかのさらなる制度的要因は、協調的開示とも呼ばれる、責任ある開示に賛成して議論を解決するのに役立ちました。それにより、人々はベンダーまたはサードパーティにバグを報告し、パッチが利用可能になるまで一定期間機密を保ち、その後、記者に信用を与えます彼らの発見のために。  
これにより政府が参加しました。  
3番目に、スマートソフトウェア会社は独自のバグ報奨金プログラムを開始したため、セキュリティ研究者はバグを直接販売し、CERTやiDefenseなどの仲介者を排除できました。  
Zerodiumのように、バグを購入して国家の俳優や、国家にも販売するサイバー兵器のサプライヤに販売する企業が登場しました。 iPhoneなどのプラットフォームのゼロデイエクスプロイトは、100万ドル以上で販売できるようになりました。  
たとえば、2012年に、オープンソースプロジェクトに脆弱なコードを故意に寄付したボランティアの最初のケースに遭遇しました3。これは、広く使用されているプラ​​ットフォームへの道が見つかれば、6桁の利益が見込めることを期待しています。  
2014年、Abdullah AlgarniとYashwant Malaiyaは脆弱性市場を調査し、より活発な研究者にインタビューしました。好奇心と経済的インセンティブの組み合わせにより、開発途上国の多くの有能な若者が引き寄せられ、責任を持って開示する人もいれば、脆弱性市場を利用してお金と認識を得る人もいれば、より多くの金を売って黒人帽子を売る人もいます。一部はベンダーにバグを提供しますが、適切に処理されない場合は代わりに悪者にバグを提供します。ああ、そしてバグハンターの多くは数年後に引退します[38]。  
脆弱性のライフサイクルには、現在、その発見だけでなく、おそらく諜報機関や他のブラックハットの俳優による秘密の使用も含まれています。その後、おそらく他の黒い帽子が、最終的には白い帽子によって、その再発見が行われました。パッチの発送;そして、パッチを適用しなかったユーザーに対するさらなる悪用。  
Linuxの脆弱性は、ラボ内のサーバーやお子様のRaspberry Piに影響を与えるだけではありません。  
これが、責任ある開示が調整された開示としてブランド変更されている理由です。  
また、数千の脆弱性があり、そのうち数十は犯罪者が使用するエクスプロイトキットに毎年出現します（一部は間違いなく高価値の標的に対して一度だけ使用されるため、防御システムに知られることはありません）。  
CVE番号で索引付けされた携帯電話のブラウザーの脆弱性で使用される3Webkitの重複する複数のエコシステムを調査する必要があります。侵害指標（IoC）の概要  
これらの生態系の間には部分的な相関関係がありますが、データには一般的にノイズが多く含まれています。  
  
紛争理論の創始者である故ジャック・ヒルスレイファーは、洪水防御壁がそれぞれの洪水壁の一部を維持していた個々の家族によって建設された島であるアナキアの物語を語った。  
彼はこれを、ミサイル攻撃に対する防御が単一の最良の防御射撃に依存する都市と比較しました[906]。  
これは、異なる政治システムにつながる可能性があります。  
中世後期のヨーロッパの残りの多くでは、王や首領が自分たちの軍隊を率いて敵を殺し、土地を占領しました。最強の王が最大の帝国を築き、これが武装勢力の数を最適化する封建制度につながりました。  
この最後のケース、総和は戦争の現代モデルです。私たちは税金を支払い、政府は兵士を雇います。  
、最も弱いリンクよりも効率的です（最も弱いリンクを介して誰もが脆弱になります）  
情報セキュリティは、3つのモードすべての興味深い組み合わせです。  
 ソフトウェアの脆弱性テストは、すべての努力の合計に依存する場合があります。  
より多くのエージェントが追加されると、システムは総和の場合には信頼性が高くなりますが、最も弱いリンクの場合には信頼性が低くなります。  
 プログラマー;マイクロソフトは、2000年代初頭に、ソフトウェアエンジニアよりもテストエンジニアの方が多かったことを発見しました。  
 ゲーム理論と情報セキュリティに専念。  
たとえば、ほとんどのソーシャルネットワークは、他のノードへのリンク数が比較的多い比較的少数のノードへの接続が必要です[1994]。  
米英軍も同様に、イラク戦争中の反乱鎮圧作戦で高度に接続された人々を標的にしました（そして、スンニ派地域での社会崩壊は、ISISの出現を助けました）。  
そのようなモデルはまた、反乱軍がセルを形成することは、繰り返しの断頭攻撃に対する自然で最も効果的な反応であることを示唆しています[1373]。  
RainerB¨ohmeとTyler Mooreは、そうでない場合に何が起こるかを調査しました。人々が私的な利益のみをもたらす防御メカニズムを使用する場合、最も弱いリンクモデルは、ぶら下がる実の1つになります。  
要するに、あらゆる時代の紛争の技術は、存続し繁栄できる制度の種類を規定しているため、政治に深い微妙な影響を与える可能性があります。  
タイラームーア、アランフリードマン、アリエルプロカッチャは、防衛ミッションと攻撃ミッションの両方を備えたNSAなどの国家機関が脆弱性を開示して、それらを修正または備蓄できるかどうかを調査しました。彼らは、他人にかかる社会的コストを無視できれば、備蓄するだろうと結論付けた[1338]。  
  
技術的なロックインは、支配的な企業の市場につながる要因の1つであり、ソフトウェア企業は30年以上にわたって数十億ドルを費やして、顧客が立ち去るのを難しくし、競合他社が簡単に欠陥を見つけられるようにしています。  
1990年代までに、SAMBAがAppleとの相互運用性を確立するまで、Microsoftが他のオペレーティングシステムをLANから除外しようとしたため、この問題はネットワーク互換性に移行していました。 1993年の独占禁止法訴訟の結果、MicrosoftはWindows契約を利用したブロックを阻止しました。同様のメカニズムは、隣接または補完的な商品やサービスの市場を管理するために使用されます。例としては、インクカートリッジをプリンターに結び付けることや、デジタル著作権管理（DRM）があります。  
初期の安全保障経済論の論文で、Hal Varianは2002年に、その自由な使用は競争にダメージを与える可能性があると指摘しました[1944]。  
 これにより、画面では読むことしかできず、印刷することはできず、月末までしかWord文書をメールで送ることができました。  
上記のセクション8.3.2の例を考えてみてください。企業には100人のスタッフがいて、それぞれにPCをインストールして、150ドルでOfficeをインストールしています。  
 LibreOffice、トレーニング、ファイルの変換など。  
現在、IRMはその時に離陸できませんでした。アメリカの企業はそれがロックインプレーであることをすぐに理解し、ヨーロッパ政府はTrusted Computingイニシアチブが小規模な企業を除外し、Microsoftがメカニズムを機能させることができなかったという事実に反対しましたVistaで適切に。  
別の側面は、DRMと音楽に関するものです。  
無許可のピアツーピアのファイル共有がクリエイティブ産業を破壊するというハリウッドの主張は、常に揺らいでいました。 2004年の調査では、ダウンロードが音楽業界全体の収益に悪影響を与えないことが示されましたが[1457]、後半の調査では、ダウンローダーが実際にさらにCDを購入することが示されました[50]。  
。  
サプライチェーンの力が音楽のメジャーからプラットフォームに移ったため、プラットフォーム（現在はApple、Google、Amazon、Spotify）  
これは経済分析の予測力の印象的な実証です。  
これについては、セクション24.5で詳しく説明します。  
同様に、クラウドベースのサービスへの移行は、ソフトウェアを盗む人がほとんどいないことを意味します。  
ただし、クラウドへの移行により、ロックインはより複雑な問題になり、生態系および個々の製品のレベルで運用されています。  
では、ロックインはどこにあるのでしょうか？  
すべてのデータをいつでもダウンロードできますが、別のプラットフォーム（MicrosoftやAppleなど）に再インストールしてください  
同様に、IT企業でSlackやSplunkなどのツールの使用を開始すると、移行を困難にするあらゆる種類の方法でそれらをカスタマイズすることになります。  
今では、補完的な資産を購入または構築するように、または機能全体をアウトソーシングするように顧客を誘導することにより、全員がロックインゲームをプレイしています。  
これらのケースの2番目のように、実行可能な競争がない場合、実際のポリシーの問題があります。  
カルテルによる生態系全体の制御は新しいものではありません。ジョシュアスペクトは、カーギルやアーマーなどの大手食品会社が鉄道によって開かれた両面市場の支配権を獲得し、穀物エレベーターなどのインフラストラクチャを購入して電力を統合し、小規模農家に気候リスクを投じ、組合主催者を運営した歴史を語っています町から出て、政治家に動物の権利の活動をテロリズムとして定義する「ag-gag」法を通過させさえした[1808]。  
実際、過去20年間で世界経済全体がより独占的になり、ITは産業集中の成長の多くを説明しているようです[234]。  
 公益事業などの自然独占の規制当局は、ロビー活動によって長期にわたって捕らえられる傾向がある一方で、独自のダイナミックを持っています。  
情報産業のダイナミクスは、これらの既存の問題の多くを悪化させ、効果的な競争をさらに困難にする可能性があります。  
 一方、カール・シャピロのようなシカゴの学校経済学者は反トラスト法のポピュリズムを非難し、大企業が使用する政治的権力への取り組みには反トラスト法が不適切であるため、救済策は特定の危害を対象とすべきであると主張している[1716]。  
欧州競争法では、長年にわたり、企業が1つの市場で支配的な地位を使用して別の市場での地位を確立することを禁じてきたため、大手テクノロジー企業に対する一連の判決を目にしてきました。  
その結果、彼らには範囲の経済があります。あるビジネスで成功すると、別のビジネスでの成功が容易になります。  
この環境では、規制当局はマルチホーミング、スイッチング、相互運用性、データの移植性、アフターマーケットへの影響に注意を払う必要があります。  
セキュリティメカニズムを使用して製品を相互に関連付ける場合、いくつかの非常に具体的なポリシーの問題が発生する可能性があります。欧州連合では最近、新しい物品販売指令（2019/771）によって規則がアップグレードされました  
。  
  
「彼らが見るであろうように、ナンブラインドはあります」と古いスコットランドのことわざに行き、セキュリティエンジニアリングは多くの例を投げかけます。  
2.3節で述べたように、これにより、他のすべてのようにオンラインで移動しているだけであったにもかかわらず、犯罪が長年にわたって減少していると主張することができました。  
しかし、どの銀行家も、彼の顧客の1人がマフィオであることを本当に知りたがっていません。  
•詐欺に関しては、まれな銀行の詐欺パターンを発見することで、決済サービスプロバイダーは、顧客に誤解や嘘をついていると伝えるだけでなく、損失を負わなければなりません。  
•クリック詐欺も同様です。  
最悪の事態を緩和するためにいくつかの作業を行う必要がありますが、市場での地位を独占している場合は、クリック詐欺に取り組むのが難しいほど、収益が少なくなります。  
もちろん、動作を停止させる明らかなバグを微調整する必要がありますが、攻撃者が悪用できるより微妙なバグはどうですか？  
いつでも静的分析ツールを購入できますが、その後、さらに数千のバグが見つかり、出荷日が数か月ずれます。  
。  
取締役はインサイダーの脅威について取締役会と話をすることは昔は困難でした。そのため、一般的なセキュリティマネージャーは、内部統制を構築するための予算を確保するために、「悪質なハッカー」についてのぞっとするようなプレゼンテーションを行います。  
彼らが会社を倒さない限り、エグゼクティブ詐欺はめったに発見されません。その代わりに、毎月パスワードを変更したり、元の紙の領収書を要求したりするなど、煩わしくて無関係な作業が行われます。  
または、セクション2.3.6で説明されている英国での2009年の議会支出スキャンダルを検討してください。  
そのスローガンの作者、当時の内務長官であるジャッキー・スミスは隠すことは何もなかったかもしれないが、彼女の夫は隠した。  
経費サーバに関する情報が彼女の仕事に閣僚の費用がかかる可能性があることを警官が知っていたならば、彼らはおそらくそれを最高機密に分類し、それを金庫に保管しておくべきでした。  
 その陽気なメモで、プライバシーに進みましょう。  
8.6.6プライバシーの経済学  
あなたが通りにいる人々を止めて彼らに彼らの見解を尋ねると、約3分の1はプライバシーの原理主義者であり、マーケティング担当者や他の誰かに個人情報を決して渡さないだろうと言います。約3分の1は彼らが気にしないと言います。約3分の1が真ん中あたりで、開示のリスクとメリットについて実際的な見方をしていると述べています。  
プライバシー強化技術はさまざまな企業から販売されていますが、ほとんどの市場では失敗しています。  
 プライバシーは、関心のあるエコノミストが2000年までに情報セキュリティの1つの側面でした。  
1980年、ジャックヒルスレイファーは、プライバシーを社会からの撤退についてではなく、進化した領土行動から生じる社会の組織化の手段であると論じた独創的な論文を発表しました。財産の内面化された尊重は、自律性をサポートします。  
マーケティング担当者は努力を無駄にしたくありませんが、消費者は無関係なマーケティングの電話に悩まされたくないです。それでも、検索コスト、外部性、その他の要因により、どちらも苛立たしいものです。  
ただし、これまで見てきたように、情報産業は独占につながる市場の失敗に陥りがちであり、支配的で情報集約的なビジネスモデルの急増には別のアプローチが必要です。  
企業は個人の支払い意欲を明らかにするデータを求めてオンラインインタラクションをマイニングします。航空会社の歩留まり管理システムから電気通信価格まで、多くの市場で見られる差別的な価格設定は経済的に効率的かもしれませんが、ますます憤慨しています。  
テレセールス事業者が100人の見込み客に電話をかけ、そのうち3つを保険で販売し、80人を困らせる場合、従来の経済分析は3つと保険会社の利益のみを考慮します。  
ロボコールの長期的な社会的コストはかなりのものになる可能性があります。  
プライバシーのパラドックスは重要な文献を生み出し、少なくとも3つの要因が加わっています。第二に、セクション3.2.5で説明した行動要因が大きな役割を果たします。  
彼女は恥ずかしい質問のリストという形で「プライバシーメーター」を考案しました。スコアは、被験者が怒鳴る前に回答する質問の数でした。  
。  
ゲーマーグループについては、コントロールグループの2倍の喜んで公開しました[987]。  
プライバシーポリシーは通常、最初のページにはありませんが、関係するユーザーが簡単に見つけることができます。通常、ポリシーはanodyneテキストで始まり、不快なものは最後まで残します。そのため、カジュアルな視聴者に警告することはありませんが、警戒する少数派は、サイトを使用しない理由をすばやく見つけることができるため、他のユーザーを停止しません。広告をクリックします。  
では、全体的な効果は何ですか？  
スノーデンの啓示からほぼ2年後の2015年に、ピューリサーチが実施した2つの調査では、米国国民の間で学習した無力感が高まっていることが明らかになりました。  
それでも、成人のわずか6％が、政府機関が自分の記録を秘密にして安全に保つことができると「非常に信頼している」と答え、25％が「ある程度信頼している」と答えた。電話会社とクレジットカード会社の数値は類似しており、広告主、ソーシャルメディア、検索エンジンは大幅に悪化しました。  
これらの緊張は1960年代以降高まっており、米国とヨーロッパの間で大きく異なる複雑なプライバシー規制につながっています。  
  
組織はしばしば明らかに不合理な方法で行動します。  
1918〜19年以降の世紀のヨーロッパと北米における医療サービスの回復力とパンデミックへの備えの衰退は、多くの例の中で最も顕著なものにすぎません。  
悪者が気づくまで、詐欺の発生率が低いと人々は自己満足します。  
その後、それはニュースと経営者のパニックに陥ります。  
したがって、セキュリティエンジニアは、人間の脆弱性が組織の行動を通じて自分を表現する方法を予測する必要があります。  
著名な開業医であるハーブサイモンも、コンピュータのパイオニアであり、CMUでコンピュータサイエンスを設立しました。  
これらの問題のより現代的な分析では、通常、それらをミクロ経済学の枠組みにおける主要機関の問題と見なします。これは会計学の教授の典型的なアプローチです。  
もう1つのアプローチは、公共選択経済学です。これは、ミクロ経済的手法を適用して、政治家、公務員、および公的機関の人々の行動を一般的に調査します。  
シニクスは、官僚機構が非難の可能性を最小限に抑えるような方法で進化しているように見えることに注意します。  
大学の教授たちは互いに懸命に競争している。私たちの顧客は私たちの副首相ではなく、ノーベル賞委員会または同等のものです。  
一方、一部の民間企業は、内部で政府のように振る舞うほどの市場力を持っています（ただし、給与ははるかに優れています）。  
  
システムを攻撃から保護する場合は、攻撃者が誰であるか、何人であるか、どこから来たのか、どのようにして仕事を学び、どのように動機づけているのかを知ることは良い考えです。  
セクション2.3では、サイバー犯罪のエコシステムの概要を示しました。サイバー犯罪のエコシステムをより詳細に調査するために使用できる多くのツールがあります。  
他の経済分野と同様に、興味深い質問とは何かを考え出し、それらに答えるためのデータを収集する反復プロセスがあります。  
犯罪に対する1つのアプローチは、1968年に報酬と罰の観点から犯罪を分析したゲーリーベッカーなどのシカゴ学校の経済学者のアプローチです[200]。  
犯罪が悪い地域に集まっているのはなぜですか？  
 従来の犯罪学者はこのような質問を調査し、犯罪防止における価値の説明を見つけます。最悪の犯罪者は、多くの場合、子育てが不十分であり、薬物乱用やアルコール乱用で複数の剥奪を受け、犯罪のサイクルに引き込まれます。  
批判的な犯罪学者は、法律は貧しい人々を抑圧することによって彼らの力を維持する強力な人々によって作られ、悪い地域は裕福な白人が住んでいる素敵な郊外よりも過度に厳しく非難される可能性が高いと指摘しています。  
1960年代以降、犯罪を抑制するために環境設計を使用することについて、最初は低コストの住宅で、その後あらゆる場所で、かなりの量の研究が行われてきました。セクション13.2.2では、これについて詳しく説明します。  
 彼らの行動を正当化する最小化戦略を持つこと。  
「彼女は私をだましました」と「彼は私を失礼」は典型的なトリガーです。メカニズムについてはセクション3.2.4で説明しました。  
法の反対側にいるハッカーは、とにかく自分たちの行動が正当化されていると感じがちです。結局のところ、ハクティビストは政治活動家であり、サイバー犯罪者は罪悪感を避けるためにさまざまな最小化戦略を使用しています。  
。  
第三に、犯罪への道、犯罪集団の組織、スキルの拡散を理解することが重要です。  
彼らは雨の中で立ち、次のレベルに上がるチャンスのために撃たれる準備ができていました。そこで、近所のボスが3人の女の子と一緒にBMWで運転しました。  
結果を得るために、警察は輸入者のシステム管理者などのチョークポイントをターゲットにする必要があります。  
多くのサイバー犯罪者はゲーマーから始まり、ゲームをだまし、次にゲームの攻略を扱い、次にゲームの攻略をコーディングする方法を学びます。そして数年以内に、より有能なものがマルウェア開発者になりました。  
セクション3.2.4で述べたように、英国国家犯罪庁はGoogleの広告を購入し、イギリスの人々がDDoS for-hireサービスを検索しているときに、そのようなサービスの使用が違法であることを警告しています。  
セクション2.3でサイバー犯罪の全体的なコストについて説明しました。テクノロジーが変化したという事実にもかかわらず、エコシステムは過去10年間で著しく安定していることを指摘しました。今ではラップトップ以上の電話からオンラインに移行し、ソーシャルネットワークを使用して、すべてをクラウドに保管しています。  
（2020年には、その差はさらに顕著になります。ロックダウンを通じて家にいる人がいるため、強盗はさらに減少しています。）  
特定の犯罪に関する研究は、この本のさまざまな場所で報告されています。  
Alessandro Acquistiらは、セキュリティまたはプライバシーの侵害を報告した場合の企業の株価への影響を調査しました[15]。単一の違反は、1週間ほど後に散逸する小さな落ち込みを引き起こす傾向がありますが、二重の違反は、長期的に投資家の信頼を損なう可能性があります。  
ただし、全体として、測定は注意が必要です。  
  
多くのシステムは、技術的な設計ミスによるのではなく、インセンティブが間違っているために失敗します。  
安全経済学は急速に成長し、私たちが「悪天候」だけを考慮していた多くのことを説明しています。  
研究の問題これまで、安全性との関連性について、ミクロ経済学、ゲーム理論、行動経済学の3つの経済学分野が調査されてきました。  
他にどのようなアイデアがありますか？  
最初に、セキュリティと、経済学の他のサブフィールドXについて考えます。  
第三に、金を見つけたら、掘り続けます（例：  
 [78]。  
第4に、（Cambridge Cyber​​crime Centreを介して）大規模なデータセットを学者が利用できるようになりつつある現在、データ主導の研究には多くの範囲があります。  
関連する問題は、個々のセキュリティスタッフの生産性から、機関、特に政府やヘルスケアシステムなどの大規模で複雑な機関内でのセキュリティの仕組みまで、他の分野の調査に役立つ可能性のあるデータを収集する方法です。  
 第5に、自動車や医療機器などの耐久性のある安全が重要なものにソフトウェアとオンライン接続を導入するようになりました。セキュリティと安全性の相互作用について、さらにそのようなシステムにパッチを適用し、何十年もの間走っています。  
セキュリティ経済学に関する現在の研究は、主に情報セキュリティの経済学（WEIS）に関するワークショップで公開されています。  
ワークショップの1つを除くすべてのライブブログがあり、各論文の概要とそのリンクから構成されています。私のブログにアクセスしたり、http：//www.clの私の経済およびセキュリティリソースページから直接リンクしたりできます。 cam.ac.uk/~rja14/econsec.html。  
これはまだ生徒の読書リストにあります。  
Tim Wuの「The Master Switch」は、一般に10年前の観点から、通信および情報産業における独占について論じています[2049]。  
アダム・スミスの古典的な「国々の富の性質と原因への探究」は一見の価値がありますが、ディックターラーの「不作法」は行動経済学の物語です。私がタイラームーアと[110]で書いた分野の調査と、同じくタイラーとの[111]でのより包括的な2011年の調査。  
次に、研究文献に飛び込むために、WEIS会議の論文とライブブログを提案します。  
ジャック・ヒルスレイファーの衝突理論[907]について触れました。もう1つの重要なストランドは犯罪の経済学であり、これはゲイリーベッカー[200]によってキックスタートされ、スティーブレビットとスティーブンダブナーの「フリーコノミクス」[1151]によって一般化されました。  
最後に、サイバー犯罪学に関する研究コミュニティと文献が増えており、Cambridge Cyber​​crime Centerのウェブサイトが妥当な出発点となる可能性があります。