お使いのPCが安全でないことを非常に喜んでください。つまり、購入したPCに侵入して、必要なソフトウェアをインストールできるということです。  
–ジョン・ギルモア  
  
著作権はデジタル時代の非常に論争の的となっている問題の1つであり、デジタル著作権管理（DRM）の開発を促進しました  
1990年代と2000年代のハリウッドとテクノロジー業界の間の大きな争いでした。 2010年までにそれは本質的に解決されました。  
技術的には、世界はCDやDVDなどのローカルメディア（多くの人々が共有していたもの）から音楽やビデオを楽しむことから移行しました  
、ブロードバンドストリーミングサービスへのサブスクリプション管理がかなり簡単です。  
反射について、私はそれを編集して2020年から見られるようなコンテキストを与えることにしました。  
DRMは引き続き使用されています。電子ブック、iPhoneのFairplayシステムでは曲のコピーが難しくなり、ブラウザーのHTML5ではNet ﬂ ixビデオのコピーが難しくなります。  
 スマートフォンを根付かせるマルウェアからバンキングやその他のアプリを守るために使用されます。  
この章を割く私の最後の理由は、著作権戦争が私たちの共有セキュリティ文化の一部になったことであり、参加するのに若すぎる場合でも、私たちの灰色ひげが燃えていることを理解するのが役立つことがあります。  
 聖書を英語で印刷したことで火がついた  
著作権と検閲の間のリンクは、テクノロジーによって不明瞭になることが時々ありますが、再び現れる傾向があります。  
ISPが、顧客が著作権で保護された素材をダウンロードできないようにするフィルターをインストールせざるを得ない場合、これらのフィルターを使用して、不適切な素材をブロックすることもできます。  
インターネットが普及するにつれ、音楽および映画業界はデジタルコピーの販売を失うことを恐れ、恋人法（1998年のアメリカのDMCA、およびヨーロッパの一連のIP指令）についてロビー活動を行いました。著作権を強制する。  
これらの法律の表向きの標的は、1990年代からWindows Media Playerなどの製品で使用されたDRMであり、2017年以降、HTML5に準拠したブラウザーで音楽やビデオのコピーを制御するために使用されていました。  
メディアコンテンツをレンダリングするアプリは、これらを順守すると信頼されています。  
DRMは現在、この本の第2版が発表された2008年よりも関連性が低くなっていますが、後で説明するいくつかのアプリケーションがあります。  
エンクレーブやTPMなどの信頼できるハードウェア、またはリバースエンジニアリングされるとすぐにパッチが適用されるクローズドソースのサンドボックスがない限り、DRMをオープンソースソフトウェアと互換性を持たせることは困難です。  
DRMによって台無しになることを警告し、耳を傾けませんでした。  
ただし、DRMは深刻なプライバシーの問題を引き起こしましたが、それはストリーミングではなくなっていません。  
  
著作権の保護は、長年、映画、音楽、書籍の出版業界に執着してきました。  
19世紀にさかのぼると、写真の発明が本の出版業を破壊するという警告がありました。 18回目は、出版社が大量のリテラシーを生み出し、売り上げを伸ばしていることを再確認するまで、公共の貸出図書館を閉鎖しようとすることを目撃した。一方、16番目に、活字活字印刷の発明は、王子や司教からクラフトギルドまで、その日のほとんどの力によって破壊的であると考えられました。  
しかし、1980年代からPCとゲームのソフトウェア市場でDRMにつながった著作権問題の大部分が広まったため、ソフトウェアの保護について検討することから始めます。  
24.2.1ソフトウェア  
IBMは1960年代に、ユーザーが自分で作成したプログラムを共有できるようにする計画を立てました。  
しかし、研究で使用されたソフトウェアは広く共有されていました。）  
コンピュータを所有しているほとんどすべての組織は大規模で、好意的でした。彼らのソフトウェアは熟練したメンテナンスを必要とする傾向がありました。  
そこで、ソフトウェアではなくサービスを購入しました。  
1960年代にミニコンピュータが登場したとき、ソフトウェアのコストはかなり高くなった。  
そもそも、ハードウェア、ソフトウェア、メンテナンスなどの完全なオーダーメイドシステムを販売していたため、海賊行為はそれほど問題になりませんでした。  
当時最も一般的な著作権争いは、プログラマーがあなたの会社を去って競合他社に加わったときであり、彼らのコードは突然あなたの多くの機能を手に入れました。問題は、彼がコードを一緒に持っていったのか、再実装したのかということでした。たとえば、ソフトウェアがアセンブラで記述されていたため、人々が初期のIBM PCのROMからソフトウェアをコピーしたかどうかをめぐる訴訟では、レジスタのプッシュとポップの順序が決定されました。  
詳細1暗号解読者のウィリアム・フリードマンと彼の妻エリゼベスは、ベーコンがシェイクスピアを書いたかどうかを解明するために、環境大富豪に雇われました。  
コード様式測定は依然として研究の活発な分野です[370]。  
そこで、在庫管理のためにミニコンピューターを購入した（または、局のサービスで時間を契約した）会社が  
一方、マシンのインストールベースは、ソフトウェアの共有がたまにしか発生しないほど大きくなりました。  
一般的なのは、プロセッサのシリアル番号を確認することでした。もう一つは時限爆弾でした。  
WXYZ –テクニカルサポートにご連絡ください。」  
（そうでない場合は、営業担当者を派遣します。）  
1970年代後半から80年代前半にマイクロコンピュータが登場して大衆市場が生まれたとき、ソフトウェアの著作権侵害が本当に問題になり始め、ソフトウェア会社がインストールして実行するための技術サポートを必要としない製品を出荷し始めました。  
マイクロソフトが設立された1年後の1976年にビルゲイツからの有名な公開書簡があり、彼はすべてのマイクロコンピュータユーザーの10％未満がBASICに支払ったと不満を述べました[722]。  
" 彼は尋ねた。  
彼の書簡は次のように締めくくっています。「10人のプログラマを雇い、優れたソフトウェアでホビーマーケットを混乱させることができる以上に、私を満足させるものはありません。」フェアプレーへのアピールはこれまでのところまで進んでおり、業界は次にミニと初期のマイクロの主な違いに取り組みました。マイクロはプロセッサーのシリアル番号がありませんでした。  
1。  
最も単純なのはシリアル番号だけでした。最も一般的に実行されるのは、単純なチャレンジ/レスポンスプロトコルです。一部のトップエンドデバイスは、実際に計算の重要な部分を実行しました。  
初期の非常に一般的な戦略は、単純なコピーに抵抗する方法でソフトウェアをPCのハードディスクにインストールすることでした。  
標準のユーティリティを使用して製品をハードディスクからコピーした場合、不良セクターはコピーされず、コピーは機能しません。  
[1001]。  
ただし、一般的には、コピーの保護とマスターの保護を区別する必要があります。多くの場合、必要に応じてバックアップ用にコピーを作成できるようにする必要がありますが、コピーのコピーを作成することはできません（これはコピー生成制御と呼ばれます）。  
3。  
4。  
平均的なPCに一意の識別子がいくつあるかは、驚くべきことです。ディスクコントローラのイーサネットアドレスとシリアル番号は、より明白なものにすぎません。  
これらの防御のほとんどに対して機能する一般的な攻撃は、デバッガーを使用してソフトウェアを通過し、コピー保護ルーチンに対して行われたすべての呼び出しを削除することです。  
ソフトウェアのライセンスされたコピーを持っている人でさえ、バックアップがより簡単で、一般に信頼性が高いことが多いため、保護されていないバージョンを手にすることがよくあります。  
 しかし、この軍拡競争は、もしあなたがそのようなことをしなければ、デバッガを持つ子供たちは常にあなたの計画をいつか壊してしまうことを皆に教えました。  
ベンダーは心理的手法も使用しました。  
これは、偽の名前で登録されたコピーを海賊版で配布することを阻止するものではありませんが、正当なユーザーが同僚にカジュアルなコピーを提供することを阻止します。  
これらは著作権マークの例です。これについては後で詳しく説明します。  
•初期のMicrosoftソフトウェア（Multiplan、WordまたはChart）  
次に、プログラムディスクをゴミ箱に移動します。次に、フロッピーディスクのゼロを追跡し、「rrnt、rrnt、rrnt」に移動します。  
ゲーム市場はハードウェア保護に移行し、最終的には独自のカートリッジでソフトウェアが販売されるクローズドアーキテクチャのコンソールが主流となりました。  
これにより、ハードウェア保護を使用してアフターマーケットを制御するアクセサリ制御が可能になりました。これは、プリンターを販売する企業などに採用されました。  
ビジネスソフトウェアベンダーは、ドングルから、チップから船まですべてを設計するために使用されるCADソフトウェアなどの高価値製品のライセンスサーバーに移行しました。  
しかし、ベンダーは一般に、いくつかの理由により、技術的な手段を使用して大衆市場の製品を保護することをやめました。•保護は迷惑でした。  
ソフトウェア保護技術は、バックアップとリカバリの邪魔になります。また、異なるベンダーのソフトウェアに互換性がなくなり、場合によっては同じマシンに常駐できなくなります。  
 •多くのベンダーは、ソフトウェアがユーザーにライセンスされているかどうかを心配する必要がないことを望んでいました（その場合、ユーザーはソフトウェアを新しいマシンに移行できました）。  
。  
両方を処理できるメカニズム（ドングルとライセンスサーバーなど）  
•コンピュータウイルスの到来により、企業のお客様はソフトウェアの衛生管理に投資する必要が生じたため、カジュアルなコピーを簡単に容認することはできませんでした。  
•個人ユーザーが製品をたまにしか使用せず、支払うのではなく捨てることが多いため、嫌がらせをすることで得られるお金はあまりありませんでした。  
ツールの海賊版を入手して気に入った人は、通常のコピーを購入するか、雇用主に購入を勧めるでしょう。  
いつか彼らはそうするでしょう。  
彼らは中毒になり、次の10年間にどのように収集するかを何らかの形で考え出します」[755]。  
たとえば、ツールの場合、ボーランドは1983年にターボパスカルを発売して業界を揺るがしました。  
Borlandの製品の価格は49.95ドルで、技術的にはMicrosoftの製品より優れており、サードパーティ製品と同じくらい優れたマニュアルが付属していました。  
 「高く積み上げて安く売ること」は、より収益性の高いビジネスモデルであることがわかりました。  
ソフトウェアは主に著作権法によって保護されています。ソフトウェア（または本、曲）を書くとき  
詳細は国によって異なりますが、著作権侵害は、商業規模で行われた場合にのみ犯罪になる傾向があります。  
ただし、大規模なユーザーに対しては、著作権の行使は価値があります。  
1988年、マイクロソフトはIBMの足跡を残して業界をリードし、貿易組織（米国のビジネスソフトウェアアライアンスなど）を設立しました  
これに続いて、中小企業にも脅迫的な手紙を送り、著作権の行使に関する会社のポリシーの詳細を要求する嫌がらせを行います。  
1993年、イギリスのスカンソープにあるソフトウェア会社の取締役が、英国のコンピューター誤用法に基づき、システムに「不正な変更を加えた」という刑事上の有罪判決を受けました。  
しかし、このメカニズムを使用して係争中の請求書の支払いを強制したとき、裁判所は彼が行き過ぎだと判断し、最終的に犯罪歴を残しました[455]。  
Officeに加えて、ネットワーク管理やその他のタスク用に多くの高価値製品を販売していたため、CADサーバーのようにライセンスサーバーに切り替えました。  
その後、パッチ火曜日が2003年に到着したとき、ライセンスのないソフトウェアで実行するというまさにその考えが狂ったようになりました。  
その後、オンラインで登録された製品のシリアル番号を監視することにより、大規模な商用偽造を検出できます2。  
：購入したり、実行中のバージョンをフリーズしたり、オフラインで使用したりすることはできません。  
それはまさに、ソフトウェア業界が2010年代初頭から収束してきたモデルです。  
ソフトウェアはサブスクリプションで販売され、コピー防止の問題はなくなります。  
24.2.2フリーソフトウェア、フリーカルチャー？  
これは当時の主要なプラットフォームを引き続きサポートし、当初はIBMを意味していました。  
ただし、世界中のほかの学者がハードウェア上で動作するソフトウェアを作成していたため、私たちの学者はIBMメインフレームを望んでおり、ほとんどがFORTRANのような高級言語で記述されていましたが、移植は面倒でした。  
1983年、IBMは自社製品のソースコードの提供を停止し、「オブジェクトコードのみ」のポリシーを導入し、他のベンダーがそれに続きました。  
2年後、MITのエンジニアであるRichard Stallmanは、Xeroxがプリンタードライバーのソースコードを提供しなかったため、新しいXeroxプリンターをローカルメンテナンス契約に統合できなかったときに悩みました。  
、フリーソフトウェアのアイデアを促進しました。  
1つのスローガンは「無料のビールではなく、無料のスピーチのように無料」でしたが、無料のソフトウェアには多くの風味が含まれています。  
 GPLライセンスソフトウェアを適用して利用できるようにするには、誰でもソースを作成する必要があるという特性があります。製品登録を整理したら、Microsoftはドイツで販売されているOfficeのコピーの3分の1が偽造品であり、それらを小さな工場まで追跡しました。ケンブリッジの私たちから道を数マイル進んだところです。彼らは自社製品を誇りに思っており、営業スタッフはそれを使用して他のソフトウェア会社からCD複製ビジネスを獲得しようとしました。  
1988年、カリフォルニア大学はUnixのBerkeleyディストリビューションを、制限の少ないBSDライセンスの下でリリースしました。これにより、誰でも任意の目的でソフトウェアを使用できます。  
独自のソフトウェアベンダーは、彼らが採用しているエンジニアによって書かれたコードの著作権を取得できます3。しかし、ボランティアによって維持されているプロジェクトはどうですか？  
1990年代を通じて、それぞれのメリットについて多くの議論がありましたが、どちらのアプローチも広く使用されています。  
アクセスコントロールの章で述べたように、LinuxはAndroidが構築されたプラットフォームでしたが、FreeBSDはOSXとiOSに進化しました。  
ソフトウェアと文化の両方は、多くの個人の適応的かつ累積的な貢献を伴います。  
DJは他の人からトラックをリッピングし、新しいコンポジションにまとめます。  
法律は、コミュニティよりも大きな企業利益のために書かれる傾向があるため、これは常にこれをうまく扱うとは限りません。  
アカデミアは私たちがお互いの仕事の上に構築する場所でもあり、私たちが仕事にお金を払う人の数ではなく、私たちの仕事を使用する人の数から私たちが認識を得るというさらにひねりがあります。  
これは出版社との真の緊張を生み出します。  
私たちは、論文を発表するために学術誌と署名しなければならない著作権契約を無視する傾向がありました。または、注意して契約の「独占的」条項を取り消しました。 。  
アンドリュー・オドリズコは、米国が  
米国など一部の国では、従業員が作成したプログラムの著作権を所有していますが、その他の国では、雇用契約の中でそれを期間にする必要があります。請負業者もまた別の問題です。  
書面による合意があることは本当に賢明です。  
 さらに、年間1億ドルのマーケティング数学（ジャーナルや会議に費やされた費用、および雑誌出版社が利益を上げるために数学者が費やした未払いの労働力）  
出版物が完全にオンラインになり、すべての論文がすべての人に読めるようになった場合、おそらく実際の数学に費やされる金額が増える可能性があります。  
。  
彼は、デジタルテクノロジーではコピーの限界コストがゼロであるため、「情報は無料でありたい」と述べた（スチュワートブランドに帰属）  
アイデアの物理的なコンテナ（本、CD）の両方  
彼は、実際の効率や一般的な社会的同意では保護できなくなったものを力で保護しようとする企業の法務部門に対して警告し、米国が著作権コンプライアンスを貿易協定に書き込んだことについて、「理想的には、法律はすでに発展した社会的合意を批准しています。」彼は、情報化時代のきめ細かさと連携するビジネスモデルを開発するよう企業に求めました。  
彼は他の業界がビットのバンドルを販売するよりもライブパフォーマンスとサービスのモデルを探究することを提案しました[170]。  
本、雑誌、音楽、および映画についての議論（これから間もなく戻る）とはまったく別のことですが、共有インフラストラクチャおよびツールの必要性の認識が高まりました。  
たとえば、1994年にNetscapeが最初の人気のあるWebブラウザーを利用可能にした後、Microsoftは独自のブラウザーであるInternet ExplorerをWindowsで無料で提供することでそれらを殺し、インターネットインフォメーションサーバーと呼ばれる製品でサーバー側で独占を確立しようとしました。 1995年に発売されました。  
これは、これまでに作成された最も重要なソフトウェアの1つであった可能性があります。これは、MicrosoftがWebの初期の段階でリンクの両端を制御できなかったため、抽出できる独自のものに変えることができなかったためです。家賃。  
（代わりに、私たちは彼らと政策闘争をしているかもしれませんが、その間に多くの革新が起こりました。）  
一部の作家は自分の作品が誰にでも使用されることに満足しているので、BSDスタイルのライセンスを選択してください。他の人たちは、自分たちの作品をクローズドプロプライエタリ製品に組み込むのではなく、コモンズに留めておきたいので、GPLを好みます。学者は一般的に、私たちがクリエイターとして認められている限り、私たちのものを使用することを望んでいます。これにいくつかの秩序をもたらすために;これにより、これをパラメータ化したライセンスセットが利用可能になり、作業の使用方法を指定できます。  
これらのライセンスは現在、ソフトウェア以外で広く使用されています。  
本の代金を払っていただければ幸いですが、最新バージョンが遅れてオンラインになったとしても、誰でも利用できるようにしたいと思っています。  
。  
サービス会社は、侵害されたコンテンツを知らされたときに削除することになっています。実際には、境界を取り締まるのは難しく、インセンティブは悪意のあるものです（セクション230が偽造品の広告を掲載するときにそれらを保護します[1830]）。  
後で、この章と第26章でこれに戻ります。  
1つはフリーミアムです。製品のベーシックバージョンを配り、プレミアムバージョンを販売します。  
 もう1つは、ソフトウェアを無料で配布し、サービスの販売、広告、またはスパイウェアとして機能し、ユーザーに関するデータを販売することで収益を上げることです。  
ソフトウェアにおけるこれらのモデルの成功は、コンサルティングからのLinux業界と広告からのGoogleであり、他のオンラインビジネスに同様のアプローチを提案しました。  
ワーナーのハリウッドを率いたスタジオは、通常の金色のパラシュートなしで幹部を解雇した。彼らはもはや宇宙のマスターではなく、電話会社のビデオ制作部門の従業員になっていました。  
認識できる形で残っている唯一のスタジオはディズニーであり、サブスクリプションへの移行を早期に管理しました。おそらく、スティーブジョブズを筆頭株主およびメインボードディレクターにすることで助けられました。  
  
1800年には、イギリスには8万人の読者しかいなかった。それまでのほとんどの本は、深刻な哲学的または神学的な本でした。  
教育を受けたクラスはぞっとさせられました、そして、プリンターが図書館が彼らの売り上げを奪うことを恐れていました。  
人々が最初に図書館から借りた本を購入したため、本の売上は急増しました。  
人々はソフトウェアよりもずっと長い間音楽をコピーしてきました。  
（その結果、彼の作品の多くは後世に失われました。）  
多くの国で、これらは法律に裏打ちされた独占になった。私たちの大学のコンサートホールで演奏するには、Performing Rights Societyに徴収する必要があります。  
多くの曲は孤児的な作品であり、作曲家の相続人が不明であるため、社会はお金を維持するか、既知の作曲家の間で共有することができます。  
。  
 オーディオカセットへの課税。著作権者に分配される。  
ビートルズのレコードサージェントペッパーには20KHzのスポイラートーンが含まれており、理論的にはテープの21KHzバイアス周波数と組み合わせて、音を台無しにする1KHzホイッスルを生成する必要があります。  
しかし、実際にはこれは問題ではありませんでした。  
その後、1980年代にソニーウォークマンの登場でカセットが大物になり、コピーはあったものの、レコーディングされたカセットの売り上げが大きくなり、音楽業界は一掃されました。  
以前は、デジタルオーディオはそのサイズによって保護されていました。非圧縮音楽のCDは650Mbになる場合があります。  
1998年までに、MITのネットワークトラフィックの約40％がMP3トラフィックでした。  
これにより、権利管理業界が成長しました。  
  
ビデオカセットの初期の歴史は、オーディオカセットの歴史の再現でした。  
家庭用VCRの記録回路を混乱させるために偽の同期パルスを追加したMacrovisionシステムなど、コピーを防ぐために粗悪な技術的対策が取られましたが、これもまた簡単に敗北することが判明しました。  
もう一度、図書館は出版社の友人であることがわかりました。ビデオをレンタルできることで、人々はVCRを購入するようになり、お気に入りの映画を所有したいという欲求を刺激しました。  
ビジネスモデルが変化したため、映画のリリースはビデオの販売を宣伝するだけでした。  
これにより、問題が産業用の模造品になりました。  
より興味深い技術的保護メカニズムが放送有料テレビ機器に組み込まれました。  
オペレーターがポーランドで映画を上映する権利しか購入していなかった場合、衛星フットプリント内のドイツ語またはロシア語の視聴者が見ないようにブロックする必要があります。  
ほとんどのオペレーターは、ボクシングの試合などの特定のイベントに追加料金を請求できるようにしたいと考えていました。24.2.4.1典型的なシステムアーキテクチャ  
。  
それらは実装するのに十分簡単でしたが、敗北するのも簡単でした。それらを壊すことは暗号解読を含まず、オシロスコープと持続性だけでした。  
これらには、VideocryptやNagravisionなどのシステムが含まれ、通常3つのコンポーネントがありました。•ステーションのサブスクリプション管理サービスは、発信ビデオを暗号化し、さまざまなエンタイトルメント管理メッセージ（EMM）を埋め込みます  
 その中で、スマートカードなどのアクセストークンを加入者に発行します。 •セットトップボックスは、ケーブルまたは衛星信号をテレビが処理できるものに変換します。  
これは、ECMを解釈し、セットトップボックス内のデスクランブル回路にキーを提供することによって行われます。  
システムがハッキングされるたびにセットトップボックス自体を交換しなければならない場合、経済性はそれほど魅力的ではありません4。  
カードはECMを解読して両方の制御メッセージを取得します（「スマートカード番号123356、加入者は支払いを行っていません。通知があるまで機能しません」など）。  
次に、セットトップボックスは制御ワードを使用して、ビデオストリームとオーディオストリームをデスクランブルします。  
  
1990年代初頭に低コストで利用できるチップの制限により、ハイブリッドシステムは通常、転置暗号を画像要素に適用することによってビデオをスクランブルしました。  
これは、制御バイトによって決定されたポイントでビデオをカットし、左半分と右半分を入れ替えることにより、一度に1行のビデオをスクランブルします（図24.1）。  
しかし、4Nowのセットトップボックスのコストは数ドルであり、送料が大部分を占めるため、スマートカードはマザーボードにはんだ付けされるだけで、ハックが発生した場合はボックス全体が交換されます。  
これは1995年にMarkus Kuhnによって最初に行われ、大学のスーパーコンピューターを使用してリアルタイムで行う必要がありました。  
2000年までに、PCでこれを行うことが可能になりました[1824]。  
ハイブリッドシステムは、開発途上国の一部のステーションで依然として使用されています。また、海賊の生活を不便にする頻繁なキーの変更もあり、その問題は顧客が解読するときにキーを顧客に配布することです。  
これらのデジタルシステムは同じ原理で動作します。暗号化ハードウェアを備えたセットトップボックスと、ECMからコンテンツキーを解読する個人キーを保持するスマートカードです。  
現在のデジタルビデオブロードキャストシステムについては、次のセクションで説明します。  
 十分な長さ。  
図24.2 –スクランブルされたビデオフレーム図24.3 –処理されたビデオフレーム  
コントロールワードのストリームを使用してブロードキャストビデオのスクランブルを解除できるセットトップボックスの数を考えると、次の問題は、有料の顧客だけがコントロールワードを取得できるようにすることでした。  
ただし、使用可能な帯域幅は通常、1秒あたり約10 ECMでした。  
お客様のスマートカードがECMを解釈します。  
 –カードに保持されているマスターキーを使用して一連のECMで計算され、コントロールワードとしてセットトップボックスに提供される：CW = MAC（K; ECM1、ECM2、ECM3、ECM4）  
カードを改ざん防止できる場合は、準拠したデバイスのみがマスターキーKにアクセスでき、必要に応じて自殺する必要があります。  
 最初の攻撃はプロトコルに対するものでした。  
他の人々はスクランブルされたプログラムをビデオ録画し、後でそれを解読することができます[1255]。  
そのような機器を持っている愛好家は、ブロッカー、カードに宛てられたECMがカードに配信されないようにするプログラムを含む他の攻撃を発見しました。この方法では、オペレーターがサービスをキャンセルすることなくサブスクリプションをキャンセルできます[1255]。  
約0.5秒ごとに、スマートカードはセットトップボックスに新しいコントロールワードを提供し、これが次のように機能するキーストリームジェネレーターに読み込まれます。  
レジスタ1のビットの一部は、レジスタ2からビットを選択するマルチプレクサへのアドレスラインとして使用されます。このビットは、キーストリームシーケンスの次のビットになります。  
。  
 マルチプレクサーffi！出力（選択）  
しかし、暗号にはショートカット攻撃があることが判明しました。  
（私は1985年にこの攻撃を発見し、それが暗号に興味を持った理由です。）  
したがって、暗号解読を使用して後者を再構築できます。  
おそらく「アマチュア」攻撃のなかで最も強力なものは、マスターキーの漏洩を利用したものです。中古PCを購入し、好奇心からハードディスクを見て、1回の支払いで完全な加入者管理システムの削除を取り消した人がいたでしょう。埋め込まれたマスターキーを含むTVオペレーター。とにかく、商業海賊はマイクロプロービング技術を使用してスマートカードをリバースエンジニアリングすることに転向し、セクション18.5で私はそれに続く軍拡競争について説明しました。  
したがって、他の防御技術も試されました。  
アイルランドでの海賊に対する訴訟は敗北しました。アイルランドはしばらくの間、海賊がそこからヨーロッパ中の通信販売でカードを販売する避難所になりました。  
1995年半ばまでに、英国の主要衛星テレビ局（Sky-TV）  
したがって、1990年代中頃まで、海賊とオペレーターは技術的対策と対策の戦争に従事していました。  
オペレーターはいくつかを購入して分析し、失敗させるトリックを開発しました。  
 オペレーターはあらゆる種類の狡猾なトリックを考え出しました。  
2つのプラットフォームで異なる答えが得られる計算–意図しないタイミング条件の結果としてのみであっても– KM KG12 KG11 KG21 KG22 KGn1 k1 k2•••ffi•••ffi•••ffi•••ffi図24.5：–海賊カードが無効な制御ワードを配信するように、MACアルゴリズムにバイナリー失効ツリーをフィードします。  
 最初から効率的な失効スキームが設計されていたので、簡単に見ておく価値があります。  
図24.5に示すように、各操作カードは、カードとマスターキーの間のパスにあるすべてのグループキーを認識しています。  
 鍵k2は海賊カードに表示され、取り消す必要があります。その後、オペレーターは他のすべての加入者カードに新しいマスター鍵KMを計算させるパケットのストリームを送信します。  
その結果、1,000万人の顧客がいる場合でも、オペレーターは完全なキー変更を行うために50未満のECMを送信する必要があります。  
しかし、それは箱の中の便利なツールです。  
たとえば、あるケーブルテレビ局が無料のTシャツの特別オファーを放送し、正当な視聴者が0800番の電話番号を見ることを阻止しました。これは彼らに海賊の顧客のリストを得ました。  
有料テレビの海賊は、従来のソフトウェア企業と同様に、市場投入までの時間を成功に依存しています。3週間で99％の正しい偽造品を製造できた海賊は、3か月後に99.9％の偽造品を製造した競合他社を一掃します。  
経済学の理解は、あなたが彼のプラグを抜く前に海賊に相当なユーザー基盤を構築させることが最善であると教えています、これは彼に競争相手を一掃する時間を与え、彼が確立されたら彼のカードをオフにすると彼を破壊するので即時対応よりも多くの潜在的な顧客との信頼性。  
有料テレビ業界は、セキュリティ回復の事前計画を立て、最初は使用されなかったが後でアクティブ化できる可能性がある製品の機能を隠すことを学びました5。  
攻撃者はプロービングステーションでアルゴリズムを単純に読み取ることができず、チップ内の数千のゲートをリバースエンジニアリングする必要があったため、攻撃を行うための技術的能力を備えたラボの数を数に減らしました。  
テントの外に残った人たちは見守られました。  
業界は、主要な商業用海賊を取り締まり、投獄したり、訴訟で溺死させたりして、彼らを廃業させました。  
彼は偽造カードがまだ違法ではなかったアイルランドのフロント会社を通して偽造品を販売しました[1368]。  
イギリス当局は起訴したくなかったため、スカイは私訴を起こし、有罪判決を受けました。  
それから彼は適切な刑務所に行きました。  
  
デジタルビデオ放送（DVB）  
標準は多くの複雑なもので、IPTVと地上デジタルTV、衛星TV、および無料放送サービスと有料TVに関連しています。  
最新の標準であるDVB-T2は、2009年にETSIによって公布されました。  
DVBの条件付きアクセスメカニズムはハイブリッドシステムに似ています。コンテンツは、セクション16.3.1で説明した内容で、必要に応じて一度に開示できる一連のセキュリティ印刷機能全体を含むように、銀行券プリンタが何年も前に学んだ方法について説明しました。  
暗号化には、NDAでのみ利用可能でしたが2002年に漏洩したDVB Common Scrambling Algorithmが使用されています。  
スマートカードは標準化されていません（インターフェースレベルを除く）  
有料テレビは、ケーブルか衛星かに関係なく、米国の世帯の75％で2008年にピークを迎えました。DVDの歴史は、Hollywoodとコンピュータ業界との間のトラブルの警告であり、コピー防止策を講じないことに関する教訓でもありました。  
、後に1996年にデジタル多用途ディスクの名前を変更しました。  
したがって、コンテンツスクランブルシステム（CSS）と呼ばれるメカニズム  
（DVD標準がどのように進化したかについてのストーリーは、ジムテイラーの標準参照[1865]で伝えられています。これには、DVD標準のほとんども説明されています。）  
しかし、ユーザーは、リージョンコーディングをオフにできるDVDプレーヤーを購入することを好みました。  
これにより、DVDが発売された時点で脆弱であることが知られているCSSが残されました[1494]。  
ノルウェーの10代のJon Lech Johansenがアルゴリズムをリバースエンジニアリングし、そのための復号化ソフトウェアDeCSSを作成しました。  
これにより、より広く配布され、ハリウッドは愚かに見えました[1127]。  
ヨハンセンを起訴するノルウェー。  
PCがオープンプラットフォームであることから、別の問題が発生しました。  
体系的なソフトウェア難読化のトリックに関する論文が正式に掲載されました[141]。  
DVDコンソーシアムの理念は、DVDドライバーをLinuxコミュニティで利用可能にすることと一致していませんでした。  
このような状況下で、CSSとDeCSSを設定するのは時間の問題でした。  
私は2001年に次のように書いています。「合理的な人は、もう一度スタジオが最終的に理にかなって、DVDの販売から多くのお金を稼ぐことを期待するかもしれません。  
その後、2007年にHD-DVDとBlu-Rayの間でフォーマット戦争が発生し、どちらも短波長レーザーを使用して情報をより高密度にエンコードしてディスクあたり最大50Gbを提供する、より高密度の光メディアを市場に売り込む試みがありました。  
この本の第2版で説明した。  
それらは、ブロードバンドの成長によって配布メディアとして、またUSBメモリスティックのコストの低下によってストレージメディアとして破壊されました。  
24.3汎用コンピューターのDRM  
これにより、DRMメカニズムが実際の所有権を反映できるようになり、私があなたに写真を販売し、領収書を受け取ったらそれを復号化できるようになりました。さらに、それを他の誰かに渡すと、それがなくなってしまいます。  
元のアプリケーションには、科学雑誌からの新聞や記事の配布[315]が含まれていました。7InterTrustの特許は、20世紀の4つのコンピュータ関連特許のうちの1つであり、9桁の合計額が変わりました。メモリ特許、RSA公開鍵特許、フラウンホーファーMP3特許。  
基本的な問題は、汎用コンピュータであるPCが原則として任意のファイルをコピーして他の任意のコンピュータに送信できることです。アナログコピーとは異なり、コピーは完璧なので、1つのオリジナルから何百万ものコピーが作成される可能性があります。  
音楽業界は、無制限のコピーはビジネスを破壊すると信じていました。コンピュータ業界は、汎用コンピュータではDRMは本質的に不可能であるため、新しいビジネスモデルを採用するほうがよいと彼らに言いました。  
、そしてコンピューター業界がPCと電話で再生できるようにしたい音楽とビデオへのアクセスをまだ制御していました。  
  
Windows Media Player（WMP）  
MP3プレーヤーのサポートからカラオケの歌詞の同期まで、さまざまな機能を備え、音楽の再生、ビデオの視聴、写真の表示を可能にしました。  
、次のように機能します。  
メディアオブジェクトにアクセスするには、オブジェクト識別子、ライセンスキーシード、およびそれを使用して何ができるかを示す権利管理言語の一連の指示で構成されるライセンスを顧客が取得する必要があります。再生回数、CDへの書き込みの可否など。  
ライセンスの取得には登録や支払いが含まれる場合がありますが、バックグラウンドで静かに行われる場合もあります[1558]。  
また、キーが漏洩したり、キー管理メカニズムが危険にさらされたりしたときに有料テレビのスマートカードを交換できるのと同じように、WMRMのキー管理機能は「個別のブラックボックス」（IBX）で実行されます。  
IBX内部は時々リバースエンジニアリングされました[1693]。  
セクション6.2.5で、2000年代初頭にMicrosoft、Intel、その他の大手企業がTrusted Computing Groupを形成して、DRMをPCアーキテクチャに適切に構築する方法を説明しました。MicrosoftがInformation Rights Management（IRM）を発表  
したがって、DRMはハリウッドだけに利益をもたらすわけではありません。あなたが読むことしかできず、決してコピーすることはできず、1か月後に消えてしまう電子メールを送ることができます。  
ただし、アメリカの企業はロックインを好まなかったため、Microsoftはオペレーティングシステムのメカニズムを機能させることができませんでした。  
その後、WMRMはWindows 10で、新しいMicrosoftの「メディアファイルコピー防止テクノロジー」であるPlayReadyに置き換えられました。  
  
マイクロソフトの製品は、権利管理システムにかなり典型的でした。  
曲を購入すると、ランダムなセッションキーで暗号化されたマスターキーと、iTunesプレーヤーのRSA公開キーで暗号化されたセッションキーが顧客に送信されます。  
Windowsと同様に、保護されたコンテンツのロックを解除する多くのプログラムが時々登場し、AppleはiTunesを正式にアップグレードしました。  
一部の企業の権利管理システムは実に虐待的であり、2005年にソニーのXCPシステムで特に極端な事例が発生しました。  
マイクロソフトはこれをマルウェアとして分類し、Windows Defenderと悪意のあるソフトウェアの削除ツール[1307]によって削除しました。  
ワールドワイドウェブコンソーシアム（W3C）である2012–14年に大きな論争がありました。  
 サンドボックス内のソフトウェアがオンラインライセンスマネージャーと通信するための手段として。  
2017年以降、ブラウザはNet ﬂ ixなどのサービスをサポートするために、Googleの「Widevine」DRMソフトウェアのライセンスを取得する必要があります。  
2020年に、Googleはこの技術をオープンソースのブラウザーに提供することをやめました。それ以降は、すべての新しいブラウザが独自仕様である必要があります。これは、2012–4年の討論中にEFFによって予測されていました[571]。  
Microsoftが運営するDRMが、FISA令状で武装したFBIエージェントがMicrosoftクラウド上のデータにアクセスするのを阻止するかどうかは興味深い問題です。次のスノーデンが出たときに答えがわかるだろう。  
24.3.3ソフトウェアの難読化  
逆アセンブラと時間を手にした子供たちは、そのようなトリックを打ち負かす傾向がありました。そのため、可能な企業は、いくつかの重要な機能をクラウド、信頼できるハードウェア、またはその両方に移動しました。  
。  
多くのAndroid携帯電話がパッチサポートの対象外であり、多くの場合現地の販売代理店に根ざしている開発途上国でAndroidアプリを使用している顧客を保護するためにFacebookで使用されます。  
どちらの場合も、デバイスをルート化する攻撃者から暗号化キーを保護することが目的です。  
改ざん耐性のあるソフトウェアを作成する難読化コンパイラを作成しようとする初期の試みがありました。初期のIntelプロジェクトは[141]で説明されており、初期のソフトウェアDVDプレーヤーで使用されるツールにつながっています。  
理論的なコンピューター科学者は、難読化と区別がつかないことに関する多くの論文を書きました。 2001年のBoaz Barakと同僚による独創的な結果は、強力で持続可能な保護特性を備えた難読化コンパイラを作成できないことを示唆しています[166]。  
マイクロソフトはセキュリティ更新の理念に移行しました。WindowsMedia Playerのキー管理コードはIBXに隠されて移動したため、1か月はWindowsエラーハンドラーに、次は不明なデバイスドライバーに含まれる可能性があります。  
セクション21.3.5で説明したように、マルウェアの本体を復号化するポリモーフィックヘッダーを含むパッカーにコードを実行することで、コードを難読化することがよくあります。  
このようなアプローチは、メンテナの能力とモチベーションが高ければ、適度にうまく機能することがあります。  
メインのセキュリティ研究会議では、難読化に関する論文を科学的知識の蓄積というよりは戦術的な武装競争と見なしているため、それらを受け入れる傾向はありません。  
。  
RASPテスターが2週間試行しても暗号キーを抽出できない場合、それは1か月間試行する誰かに対して何の保証も提供しません8。  
一部の人々はこれのための本当のコツを取得しますが、彼らはあなたのコンプライアンステストラボで働いていないかもしれません！したがって、レモン市場が期待されます。  
一部のツールは、Javaバイトコードを縮小および最適化するときに難読化します。その1つであるProGuardは、Android SDKの一部として配布されます。  
  
ゲームはすべての最初のアプリケーションの1つでした–世界で最初の適切なコンピューターであるEDSACが動作可能になるとすぐに、研究生がゲームを作成していました。彼らは1970年代の家庭用コンピューターブームを牽引し、その結果PC業界が生まれました。ゲームコンソールは、マイクロプロセッサとメモリチップの巨大な市場です。また、ゲームは、コンソールでもPCでも、コンピュータグラフィックスの開発を大きく推進してきました[2056]。  
8個人的に傷跡を負う。  
ちょうど途中までたどり着いたので、同社は顧客に「ケンブリッジではこれを壊すことはできなかった」と自慢しました。  
任天堂がコンソールゲームを家庭に移したとき、ソフトウェアカートリッジやその他のアドオンの販売からコンソールに助成金を支給したので、セクション24.6で後述するように、使用できるアクセサリの制御に多大な労力が費やされました。 PC用のゲームソフトウェアのコピー防止も大きな問題でした。  
ゲームロジックの重要な部分がサーバー上で実行されると、クライアントソフトウェアが配布され、残りの問題は、プレーヤーが不当な優位性を獲得できるかどうかです。  
一部のゲームではコントラクトブリッジなどの共謀が禁止されており、オンラインプラットフォームでプレイしている人々が完全に別のチャネルを使用してチートするのを阻止するのは困難です。  
それでも、いくつかの決定は長年にわたって物議を醸し続けています。プレーヤーは幸運かもしれません。長年一緒にプレーしてきたパートナーは、無意識のうちに無意識のうちにコミュニケーションをとろうとするかもしれません。  
人々のチームを巻き込むアドベンチャーゲームなど、他のゲームでは共謀が必要です。  
多くの場合、子供たちであるプレーヤーは、重要な時に敵チームの主要メンバーを殺すサービスに数ドルを支払います。  
たとえば、戦術的なシューティングゲームでは、成功はゲームのメカニズムではなく、プレーヤーの戦術とシューティングスキルに依存する必要があります。  
たとえば、通常、射撃の決闘では、ネットワークレイテンシが最も低い場合、または最初に移動した場合に有利になると予想されます。  
マイクボンドは、このような異常を潜在的に悪用するプレーヤーを指す「新戦術」という用語を作り出しました[280]。  
これにより、古典的なゲームチートの1つ、つまり、自動化とサポートのために独自のコードを作成することができます。  
 着信ネットワークパケットをインターセプトし、悪意のある人物を特定し、発信ショットを調べ、それらの目的を最適化するプロキシを通じて。  
プロキシとしてパケットストリーム、グラフィックスカード、またはクライアントコードにフックできます。  
ファーストパーソンシューティングゲームは通常、生の位置情報をゲームのすべてのプレーヤーに送信し、ローカルの物理モデルに従ってレンダリングするクライアントソフトウェアに任せているため、このようなハッキングが可能です。  
PunkbusterなどのGuardソフトウェアは2000年から使用されており、アンチウイルス技術を使用して、ゲームコードまたはそれが依存するドライバーにフックしようとする試みを検出しています。  
上記のセクションで説明したように、これは絶え間ない戦いであり、人工ラグなどの一部の手法は完全に処理することが困難です。  
サーバーはまた、プロの橋トーナメントと同様に、イベント後の不正行為を検出するための分析機能を備えています。  
24.3.5ピアツーピアシステム  
人々がコンピュータとブロードバンド接続にCDドライブを持ったら、お気に入りのトラックをコピーして共有することができました。  
法的措置を招くファイルを一元管理するのではなく、Napsterはインデックスを提供して、特定のトラックを望む誰かが他の誰がそれを持っているかを見つけ、共有または取引する準備ができているようにしました。  
次に、GnutellaやFreenetなどのシステムは、検閲耐性システムの世界からアイデアを借りて、法的攻撃によって閉鎖される可能性がある中央ノードなしでネットワークをセットアップしました[439]。  
私は初期の検閲耐性システムであるEternity Serviceの設計者でした。  
事件の主題となったメッセージには、教会の元大臣による宣誓供述書が含まれており、メンバーが完全に発足すると、残りの人類は誤った意識に苦しんでいると告げられた。実際には、イエスは悪者であり、ルシファーは善人でした。  
彼らは多くの管轄区域でこの議論を回避し、最終的にはオランダの裁判所が、そのNGOに「フィッシュマン宣誓供述書」と呼ばれるように発行することを許可することによってそれを阻止しました。これの新しいバージョンはPublius9で、検閲に耐性のある匿名の公開メカニズムも提供していました[1974]。  
裁判所の命令により閉鎖される可能性のあるサーバーがないことは、音楽業界の執行者にとって興味深い問題を引き起こします。  
ピアツーピアシステムを攻撃する1つの方法は、変更されたピアを導入し、他のできるだけ多くのピアに接続して、それらを識別することにより、「ネットワークを歩く」ことです。  
多くの場合、人々は訴訟を起こすのではなく、中止して辞任し、わずかなペナルティを支払うことに同意しました。しかし、2007年10月、ミネソタ州ダルースの連邦陪審は、30歳のジャミートーマスがカザーで素材を共有したことで著作権侵害を有罪とし、事件に関係する24曲それぞれに$ 9,250を支払うよう彼女に命じた。  
、そしてまた、サービス拒否攻撃を行っていることが疑われました（多くの管轄区域ではそうではありません）。  
2007年9月に、音楽業界で「ファイル共有の緩和」に取り組んでいたMedia Defenderと呼ばれる会社は、従業員が自分のメールをGmailに転送し、パスワードが侵害された後、社内メールの数千を漏らしました。  
ピアツーピアシステムもComcastの攻撃を受けたとされています。これは、偽造されたリセットパケットを送信してBittorrent接続を破壊することにより、顧客の接続を破壊したと言われています。  
2020年の状況は、一部の法域では、トレントトロールと呼ばれることもある法律事務所からのこの種の恐喝に苦しんでいます。たとえば、スウェーデンでは、弁護士が家族から大規模な支払いを要求するケースが何万件もあると主張しています彼らの子供たちはいくつかの著作物[1655]をアップロードしました。  
この特定の方法。  
これについては、セクション24.5で詳しく説明します。  
24.3.6ハードウェア設計権の管理  
Armのような企業は、アプリケーション固有の集積回路（ASIC）を設計するかどうかにかかわらず、カスタムチップを製造する企業にプロセッサとその他のコンポーネントの設計をライセンスすることで生計を立てています  
。  
カメラ会社は、FPGAに読み込まれるビットストリームに統合する回路のライセンスを取得します。この回路は、中国の工場で製造した新しいカメラの主要コンポーネントになります。  
2つの失敗モードがあります。カメラ会社が追加の製造を注文してIP所有者に嘘をついた可能性があるか、または中国の工場がカメラ会社をだましている可能性があります。  
今では、製造後にシリアル番号を使用して各カメラをパーソナライズするなど、工場がカメラをだますのを阻止するためにカメラ会社が使用できる技術的メカニズムがありますが、これらはIP所有者をだますことを難しくする可能性があります。  
カメラ会社は、あるモデルのプロセッサまたはフィルターのライセンスを取得し、それを宣言せずに別の安価なモデルに組み込むこともできます。  
また、暗号化されたビットストリームとチップ全体のアップデートを配布することにより、最初の問題に対処するメカニズムを提供するFPGAの販売も抑制します。チップ設計ツールは信頼境界内にあるため、2番目の問題はより困難です。  
科学捜査のためのサイドチャネルの使用がいくつかあります。  
コンポーネントは、電力トレースで適切な信号を生成するように意図的に設計することもできます。  
 これは、著作権マーキングの問題に私たちを連れて行きます。  
24.4情報の隠蔽  
これは主に、MP3オーディオファイルに秘密のメッセージが隠されている場合や、特定の命令が実行される順序でプログラムのシリアル番号が埋め込まれている場合など、他のデータにデータを隠すための手法を指します。  
これらには、透かし、非表示にされている場合とされていない場合があるが削除が難しい著作権メッセージ、非表示のシリアル番号である指紋が含まれます。  
コピーをファイル共有システムにアップロードすると、著作権所有者があなたを訴える可能性があるという考えでした。  
たとえば、AmazonはMP3ダウンロードをマークしていませんでした[852]）。  
Gus Simmons [1745]によって提案された概念モデルは次のとおりです。  
したがって、彼らは無害なカバーテキストで秘密のメッセージを隠すいくつかの方法を見つけなければなりません。  
電子戦争といくつかの類似点があります。  
ウィリーは、著作権マーク検出器を失敗させるような方法でオーディオまたはビデオ信号を壊そうとする海賊と考えることができます。著作権マークを有効にするために非表示にする必要はありません。  
ただし、以下では、非表示の著作権マークに集中します。  
24.4.1透かしとコピー世代管理  
。  
アイデアは、ビデオまたは音楽トラックがマークされていない、「決してコピーしない」、または「一度だけコピーする」とマークされている可能性があるというものでした。準拠しているプレーヤーは、「コピーしない」とマークされたビデオを録画しません。「一度だけコピー」とマークされたビデオを録画すると、マークが「コピーしない」に変わります。  
このように、消費者が利用できるDVDプレーヤーは、ホームビデオの無制限のコピーとテレビ番組のタイムシフトされた視聴を可能にしますが、商業的な著作権侵害のために簡単に悪用されることはありません。  
各ディスクについて、乱数であるチケットXに加えて、コピー制御情報に加えて、リードイントラックのウォブルなどの物理メディアに固有の情報を選択します。  
 そして、h（h（X）  
。  
）  
準拠したマシンにウォーターマークを探しさせ、h（X）が提供されていない限り、トラックを再生することを拒否した場合  
準拠デバイスは、Xが指定されている場合のみマークされたトラックを記録します。その場合、h（X）のみが記録されます  
このようにして、元のメディアの「1回だけコピーする」トラックは、新しいメディアでは「これ以上コピーしない」トラックになります。  
堅牢性は、私たちの旧友、受信機の動作特性、または誤報と見逃した警報のトレードオフを設定するROCなど、多くの要素に依存します。  
お子様の誕生日パーティーで作成した動画でプレーヤーが誤って「コピー禁止」マークを検出した場合、それを視聴するには海賊プレーヤーを購入する必要があります。  
   
情報の隠蔽は、暗号学よりもさらに遡って、カモフラージュにルーツがあります。  
フランシス・ベーコンは、2種類のフォントを交互に使用することにより、1文字につき1ビットで本にバイナリメッセージを埋め込むシステムを提案しました[1513]。  
軍事組織や諜報機関は、トラフィックのセキュリティがコンテンツの機密性よりも重要である場合が多いことを強く認識しており、スパイが使用するマイクロドットから傍受確率の低い無線まで、あらゆる種類のテクノロジーを使用しています。  
著作権マーク、またはステガノグラフィーの場合、埋め込まれたテキストは、マークされたテキストを生成するカバーテキスト、またはステガノグラフィーの場合、ステゴテキストに隠されます。  
ここで、「テキスト」という単語は、「オーディオ」、「ビデオ」などに適宜置き換えることができます。  
•多くの人々が、オーディオまたはビデオ信号の最下位ビットにマークまたは秘密のメッセージを隠すことを提案しています。  
、削除または交換するのは簡単です。  
•より良い方法は、秘密鍵によって決定された1つ以上の場所でマークを非表示にすることです。  
送信者と受信者は、ランダムな場所に穴が切り取られた紙のマスクのコピーを持っていました。  
このトリックは、16世紀にイタリアの数学者カルダンによって再発明され、現在では暗号学者にカルダングリルとして知られています[1001]。  
秘密鍵は、適切な数のピクセルを選択するキーストリームに展開されます。  
実際には、画像内のかなり多数のピ​​クセルでも、目に見える効果なしに、パレット内の同様のピクセルの色に変更することができます[972]。  
カバー画像と埋め込み方法が1％のピクセルを安全に微調整できるような場合は、より良い結果が得られます。  
これらは、エラー修正コードを使用して回復できます。  
紙幣マーキングのために提案されたシステム、パッチワークは繰り返しコードを使用します。キーはピクセルの2つのサブセットを選択します。1つは明度を上げることでマークされ、もう1つは明度を下げることでマークされます。  
これは、微分電力分析を連想させます。キーは、入力データを2つの山に分類する方法を示します。キーが正しかった場合、それらは著しく異なります。  
したがって、一般的な手法は、電子戦[1890]から借用した直接シーケンススペクトラム拡散手法を使用することです。  
•スペクトラム拡散エンコーディングは多くの場合、変換空間で行われ、一般的な形式の圧縮に対してその効果が認識されにくくなり、ロバストになります。  
•一部のスキームは、特定のメディアの特性を使用します。たとえば、テキスト行を300分の1インチ上下に移動して印刷メディアにマークを付けるスキーム[315]や、認識のしきい値を下回る音楽にエコーを追加[225] ]。1990年代後半、著作権マーキングの進歩は非常に速かった。人々は、いくつかのシステムが紙幣やAdobeなどのツールで採用されるまで、他の人々が破ったマーキングスキームを発明した。  
  
この本全体を通して、暗号化分析を時折伴う暗号システムへの攻撃を見てきましたが、多くの場合、誤った仮定に依存し、間違ったもの、プロトコルの失敗、実装のバグを保護していました。  
著作権表示はどちらの点でも違いはありません。  
しかし、これは問題ではありません。  
•いつものように、多くの設計者は、システムのセキュリティは使用中のアルゴリズムではなく、キーの選択にあるべきであるというケルクホフの原則を無視しました。  
•例として、米国で販売されているカラーコピー機は、機械識別コード（MIC）を隠しています。  
1980年代にゼロックスとキヤノンによって導入され、明らかに1つ以上の政府との秘密協定に続いて、その存在は2004年にオランダでの訴訟で明らかにされました。  
MICは直径0.1mmの黄色のドットのパターンで、人間の目にはほとんど見えず、A4カラーコピーで約150回繰り返されます。  
•多くのマークは、信号にノイズを追加するだけです。  
または、いくつかの既知のコンテンツをマーキングシステムに提供し、その入力と出力を比較します。  
•公開鍵暗号と同等のマーキングを開発する試みが行われているため、（たとえば）  
前者は、カバーのオーディオまたはビデオが製造されているときにマークを挿入できる場合、ほぼ実現可能であるように思われます[494]。  
まず、署名を埋め込んですべての画像を認証することはできません。それは、画像が変更されていないことを証明するために変更するためです。  
したがって、主な取り組みは、コンテンツが解読されるときにコンテンツの各インスタンスに異なるマークを付けるメカニズムに投資されました。  
10年以上の間、人々は情報隠蔽ワークショップで新しい情報隠蔽メカニズムを提案し、翌年には機能しなくなりました。  
•最も成功したマーキングのスタートアップ– Digimarc – Web上の知的財産を追跡するサービスをセットアップします。  
これを倒すにはさまざまな方法がありました。  
 [1516]。  
Digimarcはセキュリティ印刷に移行し、そのマーキング技術を偽造検出手段として中央銀行にライセンス供与しました。  
 これにより、最新の機器[2061]を使用したスキャンやコピーができなくなります。  
Digimarcは現在、パッケージを監視し、ラベルシステムを提供しています。  
音声サンプルは、サウンドサンプルをランダムに複製または削除して、聞き取れないジッタを導入することで削除できます。クリックの削除とリサンプリングに使用される手法も、強力なマークリムーバーです。  
わずかな幾何学的な歪みが適用されます。画像がわずかに引き伸ばされたり、ずれたり、シフトしたり、目立たないランダムな量だけ回転したりします。これにより、開発時に存在していたほとんどすべてのマーキングスキームが無効になり、著作権マークの堅牢性の標準ベンチマークとなりました[ 1516]。  
マーク検出アルゴリズムが判明すると、堅牢性を維持するマーキングスキームを設計することは依然として困難です。  
これはストリーミングスポーツイベントにとって非常に重要です。目標を見る前に、隣から歓声が聞こえたくないのです。  
 これを完全に「修正」するために完全に記述される前に、メディアチャンクのダウンロードをサポートするように更新されました。  
これは、代わりに著作権を侵害する素材の直接認識の採用を促進するのに役立ちました。  
著作権所有者は、広告収入の一部を獲得して動画を収益化するか、ブロックするかを選択できます。  
  
1990年代と2000年代に、テクノロジー業界と「知的財産」（IP）の所有者の多くの間で激しい政策論争がありました。  
この反応には、アメリカのデジタルミレニアム著作権法（DMCA）による著作権期間延長からの一連の法律が含まれていました  
技術の取得は、1996年の米国通信品位法（CDA）のセクション230でした  
これにより、ヨーロッパではなく米国での情報サービス企業の成長が促進されました。  
 ISPに著作権を侵害する素材を含むWebサイトの削除を強制する。  
 サブスクライバーが異議申し立てを提出し、著作権所有者のファイルが適切でない限り、14日以内にアイテムを返却するために、実際には多くのISPは訴訟に関与するのではなく、単に顧客のサービスを終了します。Googleへの削除リクエストの半分以上は著作権者の上位16名からのものであり、上位3名は年間10億以上の著作権所有者を抱えており、その多くはGoogleに掲載されていないリンクへのリンクです。  
これは実際にポリシーに影響を及ぼします。Nikeのふりをしている中国の店を検閲することは1つのことですが、白人の至上主義者からの苦情に応じてBlack Lives Matter Peckhamを検閲することはまったく別です。  
 ない技術的なコントロールに置き換えられています。  
多くの活動家は、特許や著作権を、一時的な独占ではなく、不動産や人権などの永続的な自然権として人々に見てもらいたいと望む企業のロビイストが作り出した宣伝用語としてこれに反対しています。  
これは、収益を最大化するためのOrdnance Surveyによる完全に意図的な行為です。  
実際、著作権の規制は、ワシントン州やブリュッセルの議員ではなく、マイクロソフト、アップル、アマゾンで働いているプログラマーによって行われています。  
見事な例の1つとして、Amazonは、顧客のKindleから、ジョージオーウェルの「1984年」と「動物農場」の版を静かに削除しました。  
同時に、著作権法は突然何百万もの人々に関係するようになりました。  
法律がテクノロジーに追いついていないため、法律が許可することと人々が実際に行うことの間のギャップが広がっています。  
 誰も訴えないと優雅に言う。  
、オンラインになりました（曲の電話ビデオクリップが誰かのソーシャルネットワークページに表示されたときのように）  
ジョンテフラニアンは、典型的な法律の教授が1日あたり80を超える著作権侵害を犯し、1,000万ドルを超える法定罰金を科していると計算しています[1866]。  
テクノロジーは施行を可能にし、著作権をますます少数の企業所有者に統合し、社会を収集することでロビーが集中し、貪欲が乱用を引き起こし、摩擦が増大します。  
集金社会の問題についてはすでに触れましたが、これは事実上、税の場であり、金持ちが多くなり、小さな稚魚がそれほど多くないように収益を分配します。これはストリーミングで悪化しており、その支払いはユーザーではなくプレーの機能です。  
、アリアナはキャスリンが取得するものの14倍を取得します[1553]。  
プライバシーの問題もあります。  
（オンライン書店への移行、それからKindleへの移行により、Amazonでも同様の記録が作成されました。）  
カナダのプライバシー委員会の調査では、電子書籍ソフトウェアプロファイリング個人、図書館サービスでのDoubleClick広告、IPアドレスを介して個人を追跡するシステム、ベンダーの表明したプライバシーポリシーと観察された行動の矛盾など、侵入行為の多くの例が見つかりました–第三者への非公開の通信を含む[682]。  
 答えはロビー活動のダイナミクスにあります。  
24.5.1 IPロビー  
歴史はピータードラホスとジョンブレイスウェイト[581]によって語られました。要約すると、ファイザーと他の製薬会社は、音楽と映画業界（海賊版とコピーの削減を望んでいた）と提携しました。  
、およびその他の米国のプレーヤー（ビジネスソフトウェアアライアンスを含む）  
1980年代半ばから、これは主に貿易協定を希望した開発途上国のいじめの問題でしたが、1995年には、貿易関連の知的財産権の側面に関する条約（TRIPS）  
、続いて世界知的所有権機関（WIPO）の2つの条約  
基本的に、米国とEUが集まり、インドやブラジルのようなホールドアウトをいじめました。  
米国では、1998年のデジタルミレニアム著作権法により、WIPOの要求に応じて著作権保護メカニズムを回避することが違反となりましたが、欧州連合では2001年の著作権指令にも同様の影響がありました。  
他にも多くの目立った事件がありました。たとえば、アメリカのレコード産業協会（RIAA）によって試みられたとき、私は2001年の情報隠蔽ワークショップのプログラム委員会にいました。  
エドはその後、画期的な学問の自由訴訟でRIAAを訴えた[620]。  
次のケースは、Bunnie Huangの著書「Hacking the Xbox」でした。これは、MITの学生として、最初のバージョンのMicrosoftのゲームコンソールの保護メカニズムをどのように克服したかを説明しています[930]。権利管理メカニズムとハッキング防止法によって脅かされている自由の侵害は、多くの国でデジタル権利NGOの成長につながった（他の人たちは「暗号戦争」の結果としてすでにそれを持っていた。セクション26.2.7で詳しく説明します）  
2003〜4年に1つの転換点が訪れました。IPロビーはブリュッセルを通じて、IP施行指令というさらなる措置を講じようとしていたからです。  
今回の措置の反対者たちは、措置が大幅に修正された、十分に強い対立する利害の連合をなんとかして集めることができた。  
IPロビーの過ちは、ヨーロッパのすべての国に、単なる民事ではなく、特許侵害を犯罪とするよう強要しようとしたことでした。  
現在、医薬品の特許保持者は、「常緑化」（しばしば疑わしいデリバティブのクレームを伴う後の特許を提出する）によって特許を延長しようと試みています。ジェネリック医薬品メーカーは、損害を支払う必要がないことをディストリビューターに補償を提供することで対処しています。  
これにより、ジェネリック医薬品メーカーは、スーパーマーケット、自動車部品販売業者、消費者グループとともに、この指令に強く反対しました。  
特許侵害が犯罪になった場合、きっと彼らは彼らの不満を警察に連れて行くでしょうか？  
 テクノロジー企業がサポートを撤回したとき、特許侵害を犯罪とする試みは崩壊しました。  
反対方向に押す別のリッチでパワフルなロビーにぶつかると停止します。  
疑わしい。  
最初の著作権は18年間、次に35年間、その後50年間、作成者の寿命に70年間を加えたものでした。  
（他の皮肉屋は、クリフ・リチャード卿が当時のトニー・ブレア首相をバルバドスの彼の邸宅で休日にさせた後、音楽演奏の著作権期間が50年から70年に延長されたと指摘しました。）  
古い原稿をキュレーションするのと同じように、古いビットをキュレーションするにはお金がかかります。実際、映画業界は最近、デジタル作品をアーカイブすると、古い塩鉱山にマスターコピーを保管しただけの昔は、実際に支払うよりもコストがかかることを発見しました。  
長期的には、ビットストリングが誰にも属さない場合、維持費は誰が支払うのでしょうか？  
 しかし、そのような組織は、一般に、理解の欠如から著作権法に対する過度の防御に至るまで、さまざまな理由でデジタル素材の進歩に失敗しています11。  
Googleは大学図書館の多くの本をスキャンし、最終的には長い訴訟で著者や他の利害関係者との法的和解を得ました12。  
書籍が著作権で保護されている場合、著作権法で許可されているフェアユースとしてスニペットを検索および表示できますが、出版社の同意なしに電子版を販売することはできません。  
 2020年の最新の開発は、書籍出版社（この書籍の出版社であるWileyを含む）による訴訟です。  
パンデミックにもかかわらず、著作権戦争は続いています。  
24.5.2誰が恩恵を受けるのか？  
その年の1月に、GoogleのチーフエコノミストであるHal Varianがベルリンで行われたDRM会議で演説し、より強力なDRMの恩恵を受ける人を尋ねました。  
。  
 音楽業界はそれほどではありませんでしたが（4つの専攻と多くの独立者）  
 経済理論によると、プラットフォームベンダーはもっと勝つべきです。  
次の数年間で、ハルの予測が実現しました。  
音楽のダウンロード– DRMの有無にかかわらず–音楽業界の構造とダイナミクスを変えました。  
前進する唯一の実際的な方法は、物事をオンラインに置いて、誰かが説得力のある異議を唱えたらそれを取り下げることです。  
12The Authors Guild、Inc.  
Google、Inc .; 2015年10月16日（2Dサーキット）  
。  
実際、スマートバンドはインディーレーベルと一緒になり、ストリーミングやその他の収益のシェアが大きくなっています。  
  
暗号化メカニズムと権利管理技術の最も重要で急速に成長している用途の1つは、一般的には付属品の管理です。  
エコノミストは、ジレットの記憶の中で、この戦略を2部構成の価格設定、または単に「かみそりとブレード」モデルと呼んでいます。  
。  
2003年に、有効期限とインク使用量の制御が追加されました[1207]。最近のカートリッジは、物理的にインクがなくなるのを待つのではなく、電子的にディスペンスされるインクの量を制限します。他の業界がこの技術を採用しています。  
いくつかの不満の後、ヨーロッパの規制当局はこれに耐えることを決定しましたが、米国では、問題は法廷で決定されました。  
彼らは最初は勝ったが、2004年に控訴審で敗れた[1157]。  
 Skylinkを訴えた（互換性のあるオープナーを作った）  
これにより、暗号学者のための自由市場を支持する米国の法律が解決しました。これは、DMCAが登場する前の立場でした[1647]。  
さらに多くの例があります。  
何百もの例があります。2020年に私がこの章を改訂しているときに思いついたのは、GE冷蔵庫の浄水器での使用です。  
6か月ごとに新しいフィルターを購入しないかぎり、必要かどうかにかかわらず、フィルター水オプションは自動的にオフになることがわかりました。  
アクセサリの制御に問題はありますか？  
インクカートリッジに高い利益率があるが、プリンターの市場が競争的である場合、競争により、プリンターの価格が下落し、高価なカートリッジを補うことができます[1942]。  
その後、気が変わった。  
たとえば、John Deereは、修理を認定ディーラーに限定するロックをトラクターに取り付けているため、技術者がスペアパーツを承認するために$ 230の呼び出しと1時間あたり$ 135を支払う必要があることで、農家の間で大きな憤慨を引き起こしています[1070]。  
トラクターの場合、修理権法が必要な緩和策の1つになる場合があります。  
ウォーターフィルターカートリッジを月に6回交換するのが良い例です。約5年間使用しています。  
「スマート冷蔵庫」を購入した場合のもう1つの一般的な結果は、ベンダーが話しているサーバーの保守を停止すると、数年後に冷ややかなレンガになることです。  
covidのパンデミックは、アクセサリーコントロールの他の副作用を示しています。  
市場をリードする3M人工呼吸器とそれらを駆動するバッテリーには認証チップが搭載されていたため、200ドル以上でバッテリーを販売でき、5ドルで製造できました。  
この場合の修正は確かに競争でした。  
運が良ければ、3Mは彼らが乱用した支配的な市場での地位を失うことになりますが、パンデミックの初期の数か月間に十分な個人用保護具を持っていなかった臨床スタッフに実際のコストがかかりました。  
  
不正コピーからのデジタルコンテンツの技術的保護は、技術的にも政治的にも邪悪な問題です。  
音楽業界自体が犠牲者の1人だったというのは正しかったかもしれませんが、継続する問題を解決するものではありません。  
研究の問題2020年の著作権に関する厳しい問題の多くは、技術的な問題ではなく、政策の問題です。  
ソフトウェアの難読化については、Bjorn De Sutterとその同僚[555]が主催した、このテーマに関する2019年のDagstuhlセミナーのレポートから始めることができます。  
彼らはあなたのPCからどのような情報を収集し、どこに送信しますか？  
 さらに読むカーンは、いつものように、良い歴史的背景の読み物です[1001]。  
情報の非表示については、カッツェンバイサーとプチコラスの本[1023]とジェシカフリドリッヒの本[724]があります。  
著作権とオープンカルチャーに関するポリシーの問題についての原則的な議論については、Pam Samuelson [1646、1647]とLarry Lessig [1144、1145]から始めることができます。  
あなたが学者なら、何百万もの科学的論文をオンラインに置き、出版社の弁護士に拘束された後に自殺したアーディンスワーツの悲劇と、Sci-Hubを巡る長期にわたる戦いについて読むべきです。これにより、著作権を無視して科学論文をすべての人が利用できるようになります。  
パブのセッションで音楽を再生する場合、アイルランド音楽著作権機構に関する論争に興味があるかもしれません。  
ここに例はヨーロッパのデジタル権利（EDRi）の見解です  
著作権は、目的に適合し、クリエイターが予測可能で、「柔軟で信頼できる」ものになるように根本的に改革する必要があります。