クラウド環境における法律問題（1）
―コンテンツに対する技術的保護手段―

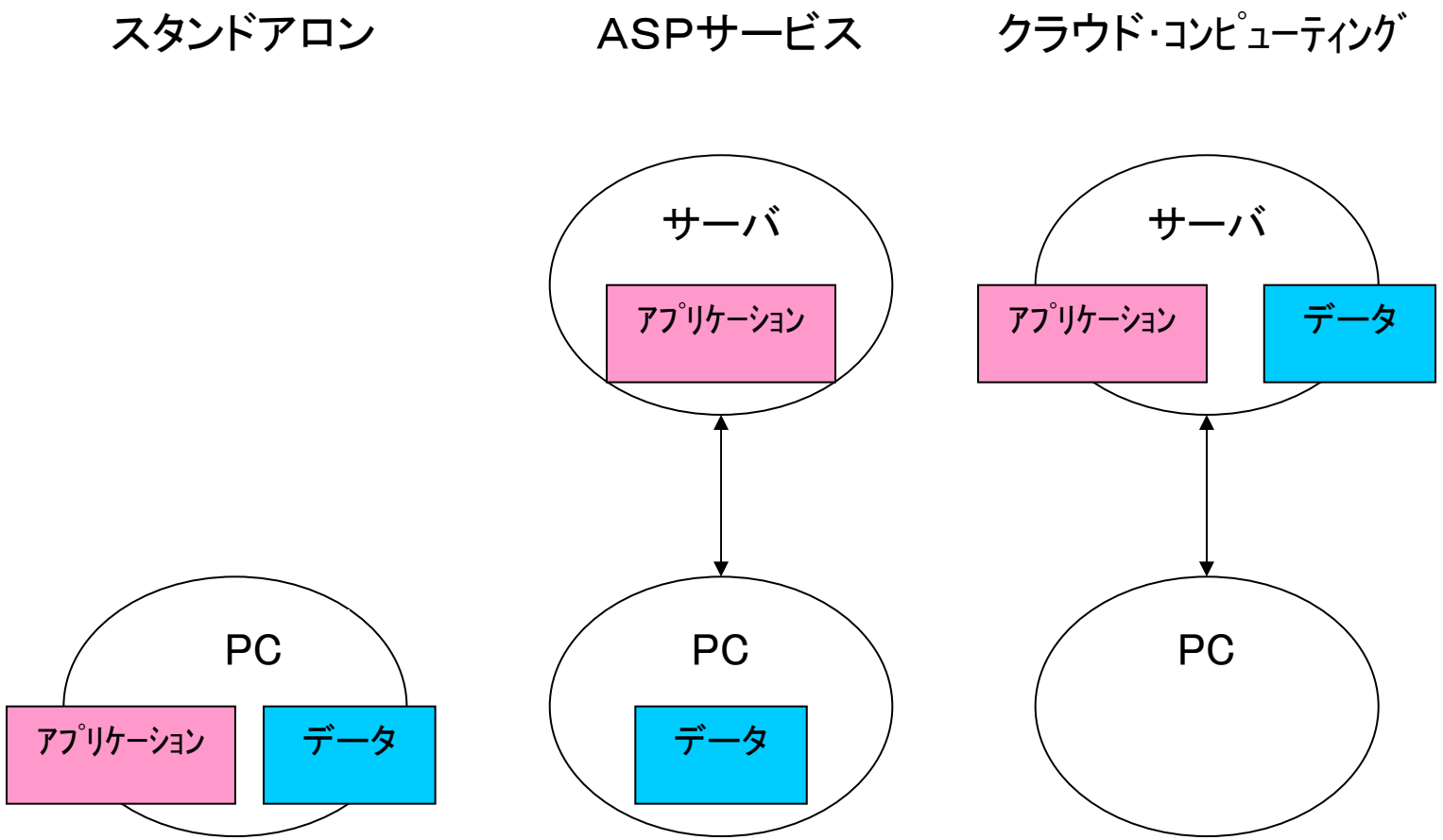
IT企業法務研究所（LAIT）セミナー

2012年3月22日

インフォテック法律事務所

弁護士　山 本　隆 司

クラウド・コンピューティングの概念



米国・国立標準技術研究所（NIST）の勧告（2011．09）

勧告された定義：

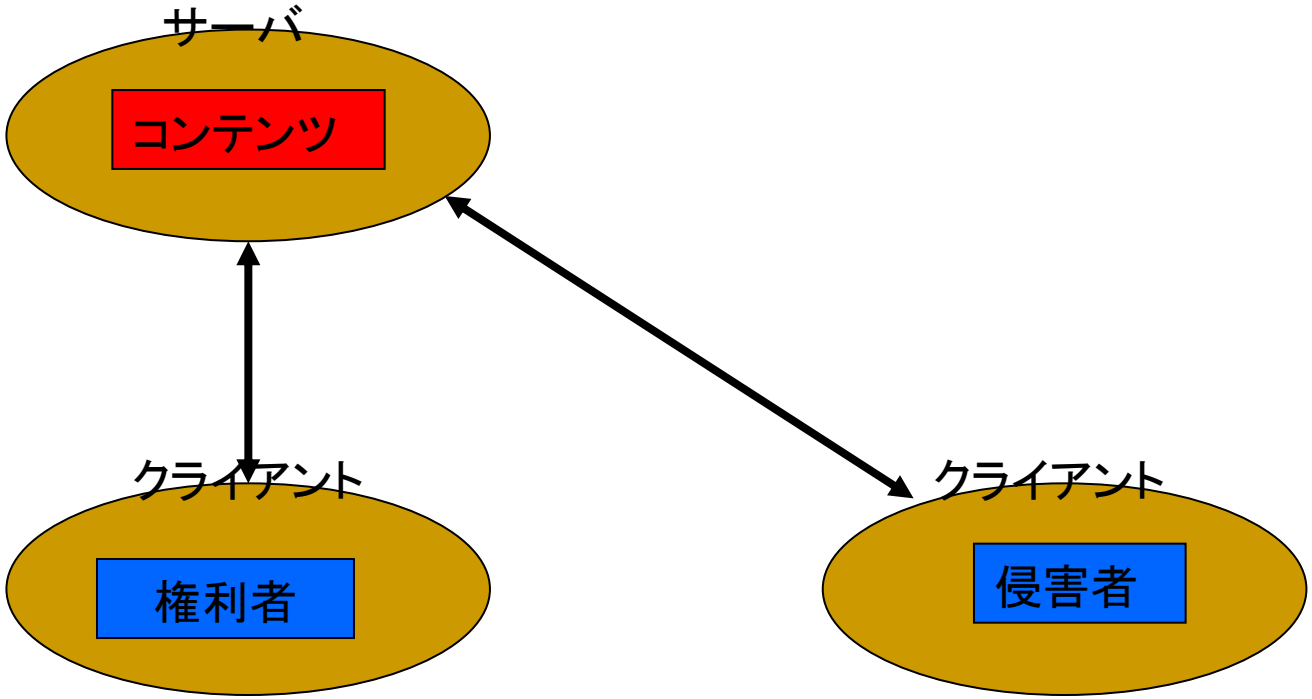
「クラウド・コンピューティングは、環境設定可能なコンピュータ資源（たとえば、ネットワーク、サーバ、ストレージ、アプリケーションおよびサービス）を共用する場へ、どこからでも便利にオンデマンドでネットワークアクセスすることを可能にし、またこれを最小限の管理作業とサービス・プロバイダによる介入で迅速に提供することを可能にするモデルである。」

- 5つの基本的特徴
  - オンデマンドのセルフサービス
  - ブロードバンドによるネットワークアクセス
  - 資源の共用
  - 対応時間の弾力性
  - 管理されたサービス
- 3つのサービスモデル
  - ソフトウェアの提供（SaaS）
  - プラットホームの提供（PaaS）
  - インフラの提供（IaaS）
- 4つの利用モデル
  - プライベート・クラウド
  - コミュニティ・クラウド
  - パブリック・クラウド
  - ハイブリッド・クラウド

文化庁調査研究報告書の指摘する著作権問題

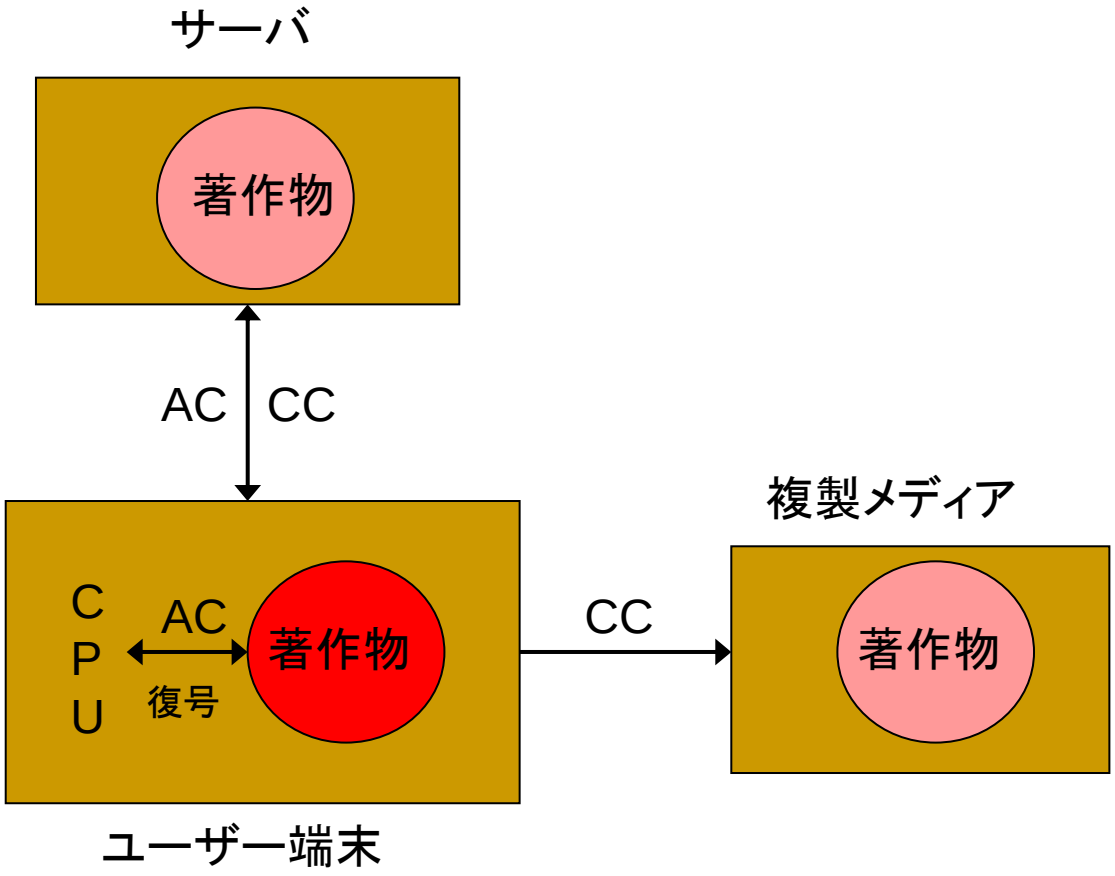
- サーバにコンテンツを複製する行為主体が誰か
- サーバへのコンテンツ複製に、私的複製として30条1項が及ぶか
- サーバは30条1項1号の公衆用設置自動複製機器に該当するのか
- サーバからのダウンロードは、業者による「公衆」送信に該当するか
- 効率化のための技術的複製に著作権法47条の5は及ぶか
- 利用者によるサーバへのアップロードに、著作権法47条の3の適用はあるか

クラウドの特徴に由来する問題点



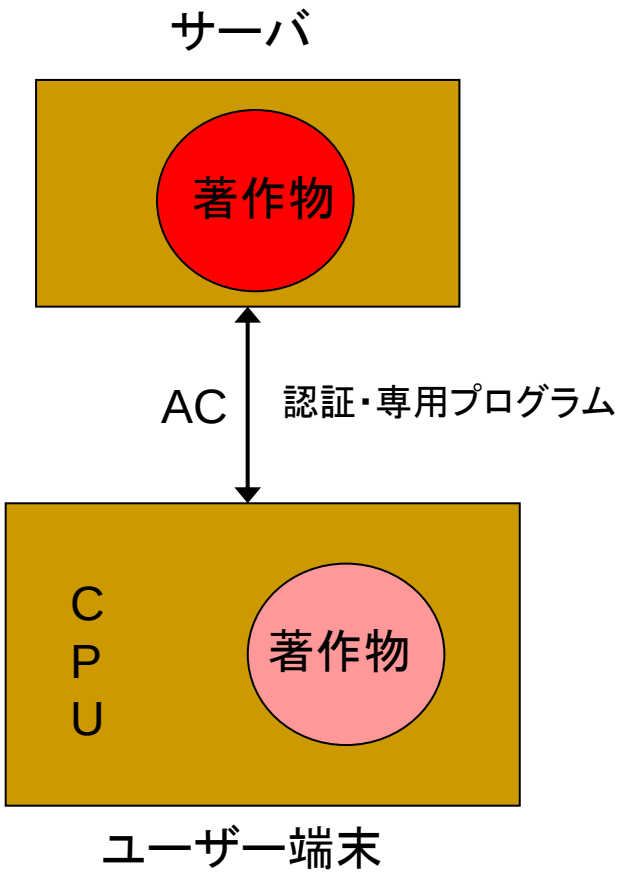
- クラウドの特徴： 利用者とコンテンツの隔地
  →①アクセス・コントロールの法的保護
  ②国際裁判管轄と準拠法

1．ネットコンテンツの技術的手段



1－1．サーバ･アクセス制御

- クラウド(SaaS)
- オンラインサービス
- Davidson事件
- MDY事件
- CAPTCHA



クラウド会計サービスにおける技術的手段

- 保護される著作物：　サーバ上の会計処理ソフトウェア
- 著作物の利用方法：　利用者は、料金を払い、インターネット経由で業者のサーバに接続して、サーバ上のソフトウェアを利用し、作成したデータをサーバ上に保存する。会計処理プログラムは、サーバ側において実行され、クライアント側にダウンロードされる必要はない。
- 技術的手段：　サーバへの接続に対してユーザ認証（AC)
- 回避方法：　ユーザ認証に必要なIDおよびパスワードを盗み出す。

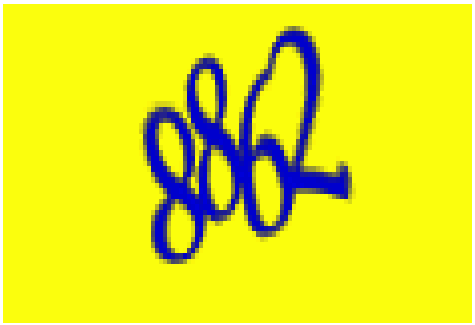
オンライン・ゲームにおける技術的手段

MDY Ind., LLC v. Blizzard Ent., Inc., 97 USPQ2d 1001 (9th Cir. 2010)

- 保護される著作物: オンライン・ゲームWoW
- 著作物の利用方法: 利用者は、月額使用料を払い、インターネット経由で業者のサーバに接続して、ゲームを利用する(SaaS) 。利用者は接続するために、クライアント・ソフトをパソコンにインストールする。
- 技術的手段:
  - サーバへの接続に対してユーザ認証する(AC)
  - 「Warden」プログラムでbots利用があれば接続を切断する(AC)
- 回避方法: 被告は、利用者に回避プログラムを提供した。それは、botsを発見されないようにWardenの探索をかいくぐる。
- 判決: アクセス・コントロール回避装置等の禁止(1201条(a)(2))違反を認めた。

CAPTCHAにおける技術的手段

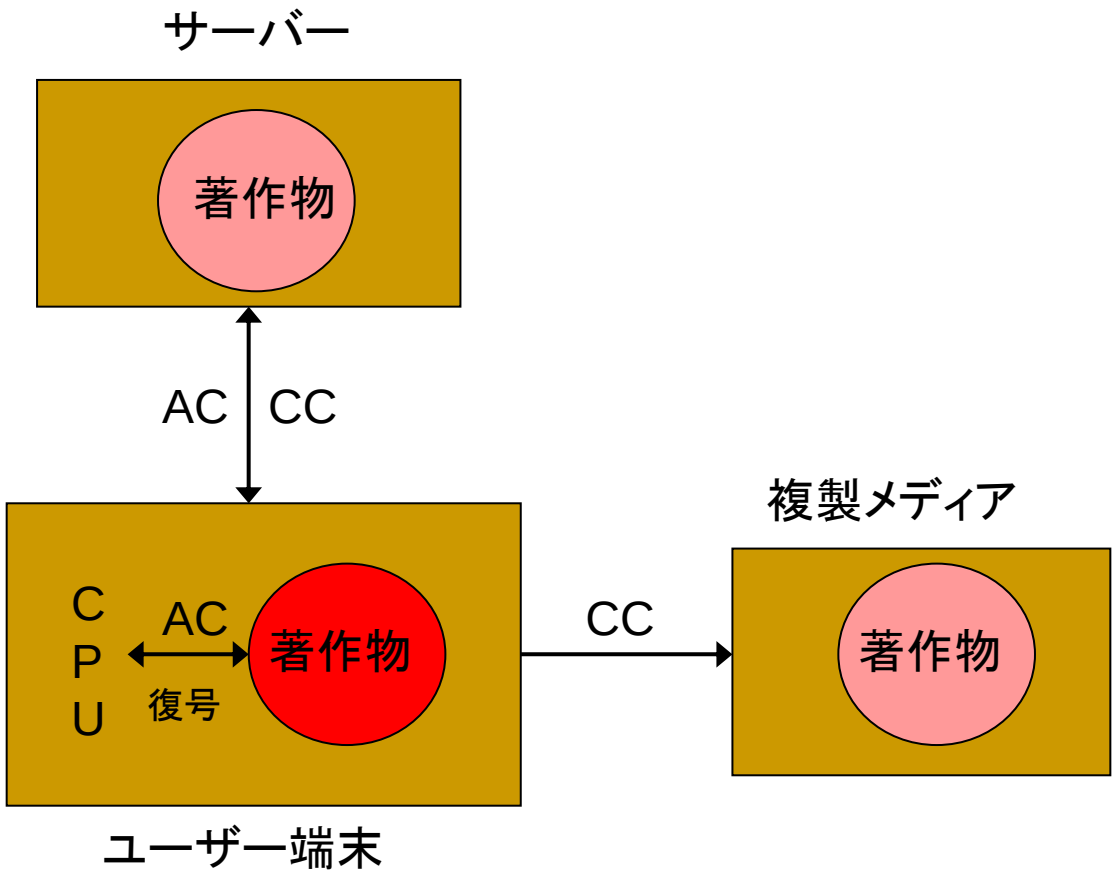
Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F Supp 2d 1096 (CD Cal. 2007)



- 保護される著作物： ウェブサイト上のコンテンツ
- 著作物の利用方法： ウェブサイト上において、そのコンテンツにアクセスしようとする利用者に対して、文字を読み取ってこれをタイプ入力することを要求する。正しく入力された場合に、利用者に、そのコンテンツにアクセスしダウンロード等の利用を許す。すなわち、自動アクセス装置でウェブサイト上のコンテンツを機械的・自動的に複製することを禁止する。
- 技術的手段： 文字の読み取り入力を要求する（AC)
- 回避行為： 被告は、CHAPTCHAを回避し自動でアクセスできる装置TBATを販売した。
- 判決： 1201条(a)(2)違反

1－2. ダウンロード制御＋コピー制御

- WM DRM
- Fair Play
- Real Player
- Acrobat eBook
- pdf



Windows Media DRMにおける技術的手段

- 保護される著作物： 配信コンテンツ
- 著作物の利用方法： 配信業者は、MSからシステム使用のライセンスを受けて、コンテンツを暗号化したファイルに変換し、これをネットで配信する(PaaS)。その配信を受けた利用者は、Windowsに標準搭載されているWindows Media Playerで、ファイルを復号して視聴できる。
- 技術的手段：(配信業者が有料で配信する場合）
  - 利用ソフトがWM Playerであるかを認証する（AC）
  - 料金支払者にのみ（AC）ダウンロードを許す（CC）
  - コンテンツを暗号化する（AC）
  - WMPは、他の媒体への複製を禁止する機能（CC）
- 回避方法： 暗号解読および暗号窃取による回避プログラムであるFairUse4WNがインターネットに流された。MSは、著作権侵害でJohn Doe訴訟を提起したが、身元確認が取れずに、訴えを取り下げた。

FairPlayにおける技術的手段

- 保護される著作物： 音楽配信コンテンツ
- 著作物の利用方法： FairPlay音楽配信システムで、利用者は、パソコンにインストールした音楽プレーヤiTunesで、音楽ファイルを購入し、これを5台までのパソコンで再生し、またiPodなどに複製して視聴できる。
  コンテンツはマスター・キーで暗号化される。マスター・キーは利用者ごとに作成されるユーザ・キーで暗号化される。ユーザ・キーは、アップルのサーバにユーザのアカウント情報として登録されるとともに、当該ユーザに送られ、iTunesがユーザのパソコンに作成するキーデータベースに登録される。
  iTunesは、キーデータベースに登録されたユーザ・キーでマスター・キーを復号し、さらにコンテンツをマスター・キーで復号して視聴できる。
- 技術的手段：
  - 利用者ソフトがiTunesであるかを認証する（AC）
  - 料金支払者にのみ（AC）ダウンロードを許す（CC）
  - コンテンツを暗号化する（AC）
  - iTunesは、所定の複製以外の複製を禁止する（CC）
  - iPodもiTunesと同様に暗号化したキーデータベースを持っており、所定の複製以外の複製を禁止する（CC）

Real Playerにおける技術的手段

…*RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311, 5 ILR (P&F) 251 (WD Wash. 2000)

- 保護される著作物： 配信コンテンツ
- 著作物の利用方法： RealProducer、RealServer、RealPlayerから成るストリーミングサービス用のソフトウェア（PaaS）。RealProducerは、コンテンツを独特の形式で圧縮しコード化する（RealMediaファイル）。コンテンツ配信業者は、RealServerでRealMediaファイルを配信すると、利用者は、RealPlayerでしかこれをダウンロードできない。ダウンロードされたRealMediaファイルはストリーミング再生できるが、RealMediaファイルに付されたコピー可否信号がoffになっていればファイルを複製することはできない。なお、音楽配信の初期の頃のシステム。
- 技術的手段：
  - RealServerへの接続に対してRealPlayerを認証する（AC）
  - 料金支払者にのみ（AC）ダウンロードを許す（CC）
  - RealPlayerは、ダウンロードされた音楽ファイルを、コピー可否信号に従ってパソコンに保存するか、再生と同時に消去する（CC）
- 回避方法： RealMediaファイルは暗号化されていないので、適法に他のファイル形式に変更して、他のプレーヤで再生することが可能であった。
- 判決： RealPlayerに成りすましてダウンロードを受け、また RealMediaファイルに付されたコピー可否信号を無視して再生・複製を可能にするプログラムの販売を、1201条(a)(2),(b)違反と認定

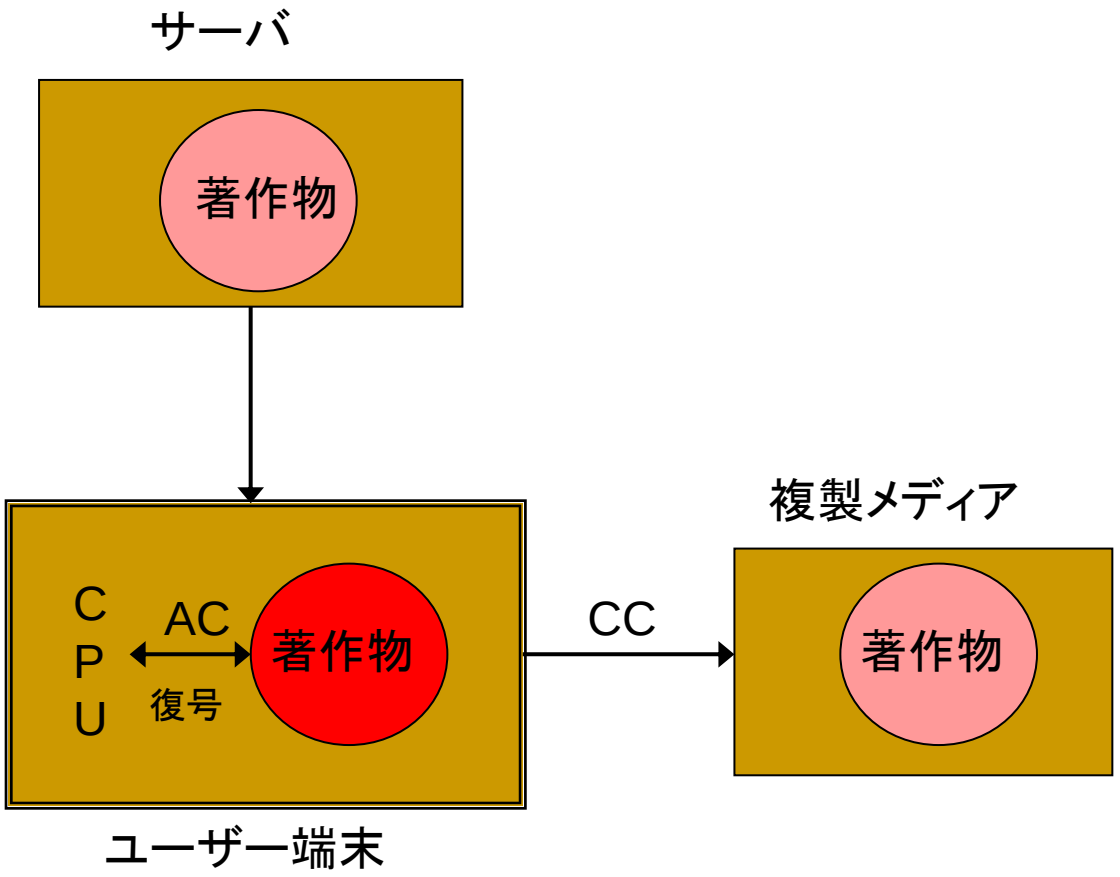
Acrobat eBook Readerにおける技術的手段

…*United States v. Elcom Ltd.*, 203 F Supp 2d 1111 (ND Cal. 2002)

- 保護される著作物: 書籍配信コンテンツ
- 著作物の利用方法: アドビの書籍配信システムのライセンスを受けた配信業者(PaaS)は、書籍を所定formatでデジタル化し(「eBook」)、これを所定Serverで顧客に配信する。配信にあたって、顧客がeBookを複製できるかなどを設定し、eBookの「voucher」として書き込む。顧客は、eBookを所定eBook Readerでダウンロードし、読むだけでなくvoucherに設定された使用ができる。
- 技術的手段:
  - 利用者のソフトがAcrobat eBook Readerであるかを認証する(AC)
  - 有料配信の場合、料金支払者にのみ(AC)ダウンロードを許す(CC)
  - Acrobat eBook Readerは、voucherの設定に従って、複製・送信を禁止する(CC)
- 回避方法: Acrobat eBookファイルはpdfファイル同様に暗号化されていないので、適法に他のファイル形式に変更して、他のプレーヤで再生することが可能である。
- 判決: voucherに付された利用制限を除去するプログラムの販売を1201条(a)(2)と認定

１－３．配信コンテンツ・アクセス／コピー制御

- B-CAS
- ケーブルテレビ
- DirecTV事件



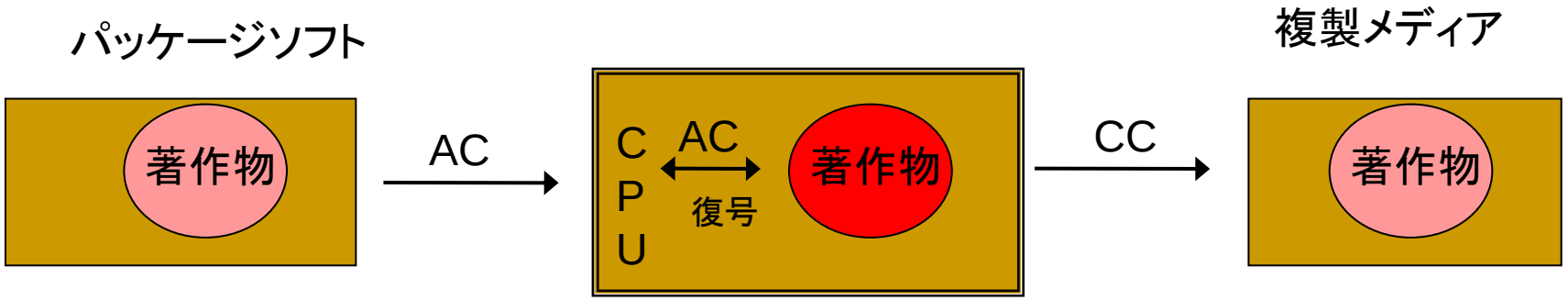
B-CASにおける技術的手段

- 保護される著作物： BS、地デジおよびCS110°のデジタル放送番組
- 著作物の利用方法：
  - 放送信号は暗号化され、無料放送については、規格準拠の受信機器に装着されたB-CASカードに登録された暗号解除キーで、放送信号を復号し、視聴できる（AC）。有料放送については、視聴契約者のみに与えられた暗号化キーがB-CASカードに登録され、これで放送信号を復号し視聴できる（AC）。
  - 規格準拠の録画機器は、複製メディアがCPRM準拠のメディアであることを認証したうえで、放送コンテンツに設定されたダビング10などのコピー制御信号（フラッグ）に従って、メディアにコンテンツを複製することができる（CC）。
  - CPRM準拠のメディアでは、コンテンツが、メディア・メーカーに固有のデバイス・キーとメディア固有のメディアIDで暗号化されて、記録される。メディアのデータを複製しても、メディアIDが異なるのでコンテンツを復号化できない（CC）。
- 技術的手段：
  - 放送コンテンツは暗号化され、視聴できる受信機器および利用者を制限する（AC）。
  - 規格準拠の受信機器は複製を制限する（CC）。
  - 規格準拠の複製メディアは複製を制限する（CC）。
- 回避方法： ー
- ハードウェア製造業者の協力

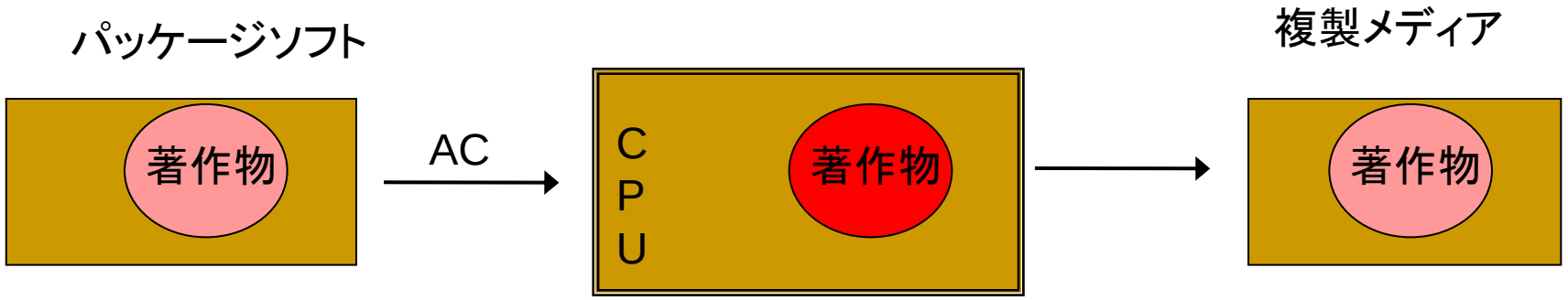
DirecTVにおける技術的手段

- 保護される著作物： CS放送番組
- 著作物の利用方法： 放送事業者は、ライセンスを受けたコンテンツを暗号化して，契約者に有料で配信している。契約者がその放送番組を視聴するには、パラボラアンテナと受信機とアクセスカードを購入する必要がある。アクセスカードには、契約者の契約情報が記録され、視聴料を支払った顧客は、アクセスカードを取り付けた受信機で放送信号を復号化し、視聴できる。
- 技術的手段：
  - 放送信号は暗号化され、規格準拠の受信機器に装着されたアクセスカードに視聴契約者のみに与えられた暗号化キーが登録され、これで放送信号を復号し視聴できる（AC）。
  - 規格準拠の受信機器は、コンテンツの複製を禁止する（CC)。
- 回避方法： 海賊業者の販売するエミュレータをインストールしたコンピュータを前記受信機に接続することによって、アクセスカードがなくても、放送信号を復号することができる。
- ハードウェア製造業者の協力

2. パッケージコンテンツの技術的手段



２－１．パッケージソフト・アクセス制御



- 通常のパッケージソフト
- CCCD
- ニンテンドーDS

多くのパッケージソフトにおける技術的手段

- 保護される著作物： パッケージソフト
- 著作物の利用方法： 多くの場合、認証によるアクセス・コントロールを掛ける。利用者は、パッケージソフトをパソコンに読み込む際にまたはインストールする際に、認証コードの入力を要求される。
- 技術的手段： ソフトの読み込みまたはインストールにコードで購入者を認証する（AC)
- 回避方法： このようなソフトでは、CD-Rなどの丸ごとコピーすることは可能である。したがって、正規品に付いていた認証コード情報を、当該違法複製物の読み込みまたはインストールの際に、入力すれば当該違法複製物の利用は可能になる。

CCCDにおける技術的手段

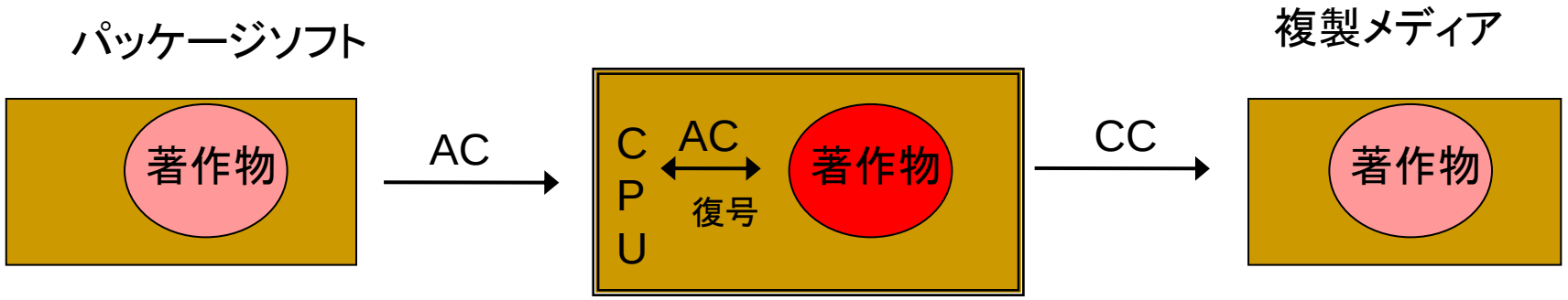
- 保護される著作物： 音楽CDコンテンツ
- 著作物の利用方法： CCCDは、CDに埋め込まれた誤り訂正符号を意図的に壊す。CDでは毎秒数回の読み取り誤りが発生するが、再生機器は、符号によって読み取り誤りを訂正することができる。しかし、符号がなくても、オーディオ用CDプレーヤでは、誤り補正機能によって人間の耳で聞いて不自然ではない程度にごまかして再生される。他方、パソコンのCD-ROMドライブでは、データそのものを読み出そうとするので、符号がなければ正しく読み出すことができなくなる。
- 技術的手段： 音楽CD上の情報を破壊することによってパソコンによる読み取りを禁止する（AC)
- 回避方法： アナログ信号に復号した音楽をコンピュータに音声入力してデジタル化することが可能であり、またWindows Media Player11では再生に失敗した場合、アナログモードに切り替えて再生・複製が可能である。

ニンテンドーDSにおける技術的手段

…東京地判平成21年2月27日（R4 Revolution for DS事件）

- 保護される著作物：　①DSカードに収録されたゲームソフトか、②DS本体のシステムプログラム
- 著作物の利用方法：　DS本体にDSカードを挿入すると、DS本体のシステムプログラムは、DSカードに記録された特定信号を検知し、DSカードに記録されたゲームソフトを実行する。なお、ゲームソフトは暗号化されておらず、これを他の媒体に複製して、パソコン等で利用することはそれ用のOSさえあれば可能である。
- 技術的手段：
  DS本体がDSカードに記録された特定信号を検知することによって、正規ソフトを認証する（AC）
  →DS本体のシステムプログラムを保護
- 回避方法：　R4 Revolution for DS装置は、特定信号を記録しており、ゲームソフトを収録したmicroSDカードを装着できる。これをDSカードのスロットに挿入することによって信号を生じさせ、当該ゲームソフトをDS本体で実行することができる。

２－２．パッケージソフト・アクセス／コピー制御



- ソニーPS2
- CSS
- Blu-ray

ソニー・プレイステーションにおける技術的手段

Sony Computer Ent. Am., Inc. v. Divineo, 457 F. Supp.2d 957 (N.D.Cal. 2006)

- 保護される著作物: ①CD-ROMに収録されたゲームソフトと、②コンソールのシステムプログラム
- 著作物の利用方法: PlayStationのゲーム・コンソールで、暗号化されたゲームソフトを収録したCD-ROMを起動すると、コンソールは正規ゲームソフトのCD-ROM書込欄外に埋め込まれた特定信号を検知し、ゲームソフトを実行する。すなわち、①正規CD-ROMに収録されたゲームソフトはパソコンなどでは復号キーがないので実行することはできない。また、②正規ゲームソフトのCD-ROMをCD-Rなどに複製しても当該特定信号まで複製できないので、コンソールは、これを読み込んで実行することをしない。
- 技術的手段:
  - コンソールは、特定信号を検知して正規ソフトであることを認証する（AC）→コンソールのシステムプログラムを保護
  - 正規コンソールだけが正規ソフトに掛けられた暗号を復号できる（AC）→CD-ROMのゲームソフトを保護
  - 正規ゲームソフトのCD-ROMをCD-Rなどに複製しても当該特定信号まで複製できない（CC）→CD-ROMのゲームソフトを保護
- 回避方法: 正規コンソールが認証信号を検知しなくてもゲームソフトを読み込み実行するプログラムを収録するmod chipなどを、正規コンソールに装着することによって、無断複製ゲームソフトを収録するCD-Rでも正規コンソールが読み込み実行することとなる。
- 判決: mod chipの販売に1201条(a)(2)違反を認定

CSSにおける技術的手段

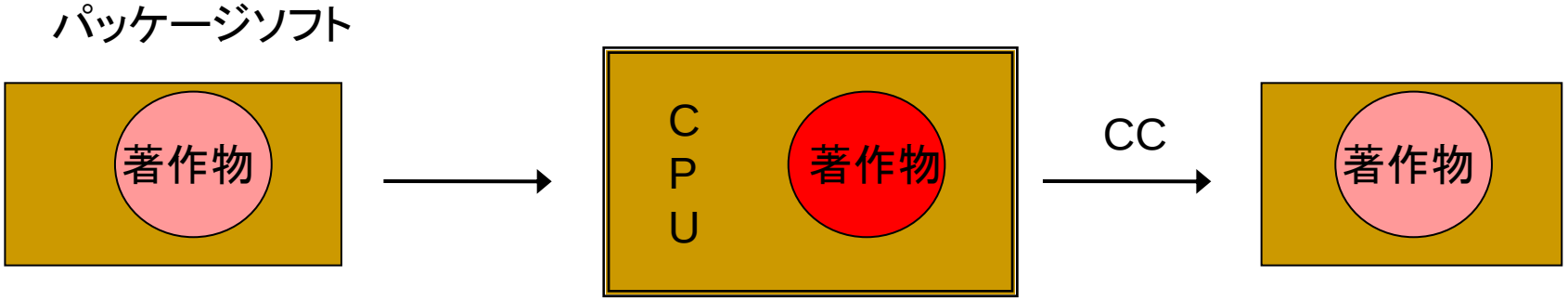
…*Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001)

- 保護される著作物： DVDに収録された映画コンテンツ
- 著作物の利用方法： DVDに収録された映画コンテンツは、暗号化（コンテンツ←タイトル・キー←ディスク・キー←ディスク・キー←マスター・キーで暗号化）されている（CSS）。規格準拠の再生機器（マスター・キーを内蔵）で暗号化された映画コンテンツを復号し、視聴できる。暗号化された鍵情報がDVD-ROM書込欄外に収録され、これを丸ごとDVD-R等にコピーしてもディスク・キー情報までは複製されないので、DVD-R等への丸ごとコピーを防止できる。
- 技術的手段：
  - 規格準拠の再生機器でなければ暗号を復号できない（AC）。
  - 暗号化された鍵情報をDVD-ROM書込欄外に収録して、丸ごとコピーを防止する（CC）。
  - 規格準拠の再生機器は複製を禁止する（CC）。
- 回避方法： 再生装置に格納されたマスター・キーを探し出すことができれば、コンテンツに掛けられた暗号を解読して復号化することができる。
- ハードウェア製造業者の協力
- 判決： 回避プログラムのサイト掲載およびリンクに1201条(a)(2)を認定

Blu-rayにおける技術的手段

- 保護される著作物: Blu-ray ディスクに収録された映画コンテンツ
- 著作物の利用方法: Blu-ray ディスクに収録された映画コンテンツは、AACSで暗号化されており、規格準拠の再生機器のみが、暗号化された映画コンテンツを復号し、視聴できる。暗号化はDVDよりは複雑な方法で行われている。また、PS2と同様に、特殊な識別子を正規のディスク上に埋め込んでおり(ROM Mark)、再生機器は当該識別子がないディスクを再生しない。さらに、Blu-ray ディスクにプレーヤのプログラムが正常であるかを認証するプログラムを組み込んでおり、正常でないプレーヤによる実行を禁止する(BD+)。
- 技術的手段:
  - AACS:規格準拠の機器のみが暗号を復号する(AC)。
  - BD+:再生機器のプログラムの正常を認証する(AC)。
  - ROM Mark:識別子で正規ディスクを認証する(AC)。
  - 規格準拠の再生機器は複製を禁止する(CC)。
- ハードウェア製造業者の協力

２－３．パッケージソフト・コピー制御



- SCMS
- マクロビジョンACP

SCMSにおける技術的手段

- 保護される著作物： 音楽CDコンテンツ
- 著作物の利用方法： CDの記録部分は多くのトラックに分割されているが、各トラックの末尾に2ビットのコピー制御信号（フラッグ）が付加されており、これでコピー不可、１世代コピー可、コピー無制限を設定する。規格準拠の複製機器は、CDコンテンツに付されたコピー制御信号を読み取って、これに従って複製メディアへコンテンツを複製する。その際に1世代コピー可のコピー制御信号はコピー不可に書き換えられ、2世代以降の複製が禁止される。
- 技術的手段： 規格準拠の複製機器はコピー制御信号に従って複製を制限する（CC）
- 回避方法： 規格に準拠することは義務づけられていないので、CDのコピー制御信号を読み飛ばす複製機器を製造販売することが適法にできる。そもそもパソコンはSCMSを備えていない。
- ハードウェア製造業者の協力

マクロビジョンACPにおける技術的手段

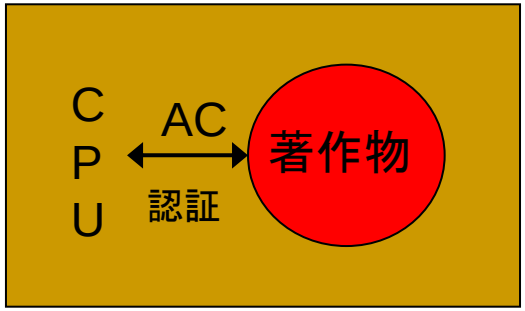
…*Macrovision v. Sima Products Corp.*, (SD NY 2006)

- 保護される著作物： DVDコンテンツ
- 著作物の利用方法： マクロビジョンのACPは、DVDコンテンツに掛ける措置であるが、このアナログ信号がビデオテープなどに複製されると、映像に乱れを生じさせるものである。
- 技術的手段： コンテンツのアナログ信号における不可視部分に情報を付加しておき、アナログ信号の複製によって画質の劣化を生じさせ、これによって複製を防止する(CC)
- 回避方法： ACPにおける信号付加のアルゴリズムを解明して、付加された信号を除去する。
- 判決： ACP除去機器の販売に1201条(b)違反を認定

3. システム内コンテンツの技術的手段

システム内コンテンツ・アクセス制御

- お試しソフト
- Chamberlain事件
- Lexmark事件
- Strage事件
- MGE事件



ユーザー端末

無料お試しソフトにおける技術的手段

- 保護される著作物： ソフトウェア
- 著作物の利用方法： 業者は、利用者に、試用目的で利用期間を制限するプログラムを備えたソフトウェアを、サーバから自由にダウンロードさせる。利用者は、試用期間経過後もこれを継続して利用することを希望する場合には、認証コードを業者から購入し、これを当該ソフトウェアに入力することによって利用期間を延長できる。
- 技術的手段： 試用期間経過後の使用には、所定の認証コードを入力することが必要である（AC）

プリンターカートリッジにおける技術的手段

Lexmark Intl. v. Static Control Components, 387 F.3d 522 (6th Cir. 2004)

- 保護される著作物： プリンターのエンジン・プログラム
- 著作物の利用方法： インク・カートリッジに付されたマイクロチップには暗号化された認証コードが記録されており、プリンターのエンジン・プログラムは、当該マイクロチップ上の暗号化された認証コードを解読し、認証コードが符合しなければ、インク・カートリッジを受け付けない。
- 技術的手段： プリンターは、認証コードでインク・カートリッジを認証する（AC）
- 回避方法： マイクロチップ上の認証コードを解読し、プリンターが受け付ける認証コードを組み込んだ独自のマイクロチップを非正規インク・カートリッジに取り付ける。
- 判決： エンジン・プログラムは「アクセスを効果的にコントロール」していないので、1201条(a)で保護されない

電源の保守プログラムにおける技術的手段

MGE UPS Systems Inc. v. GE Cons. and Ind. Inc., ___F.3d ___ (5th Cir. 2010)

- 保護される著作物： 無停電電源の保守プログラム
- 著作物の利用方法： UPS（無停電電源）の製造販売業者が、その修理スタッフに原告UPS用に開発したソフトウェア・プログラムを使用させている。このソフトウェアには、「dongle」というsecurity keyが付されており、その利用にはUPSに接続してdongleを起動する必要がある。dongleの起動にはパスワードが必要であり、各dongleには利用できる期限と利用できる回数の制限が組み込まれている。
- 技術的手段： security keyによる認証（AC）
- 回避方法： ハッカーがdongleを解除し、dongleを除去したソフトウェアを開発した。
- 判決： その使用に対して1201条(a)(1)違反を認定

ガレージ開閉装置における技術的手段

…*Chamberlain Group, Inc. v. Skylink Tech., Inc.*, 381 F3d 1178 (Fed Cir. 2004)

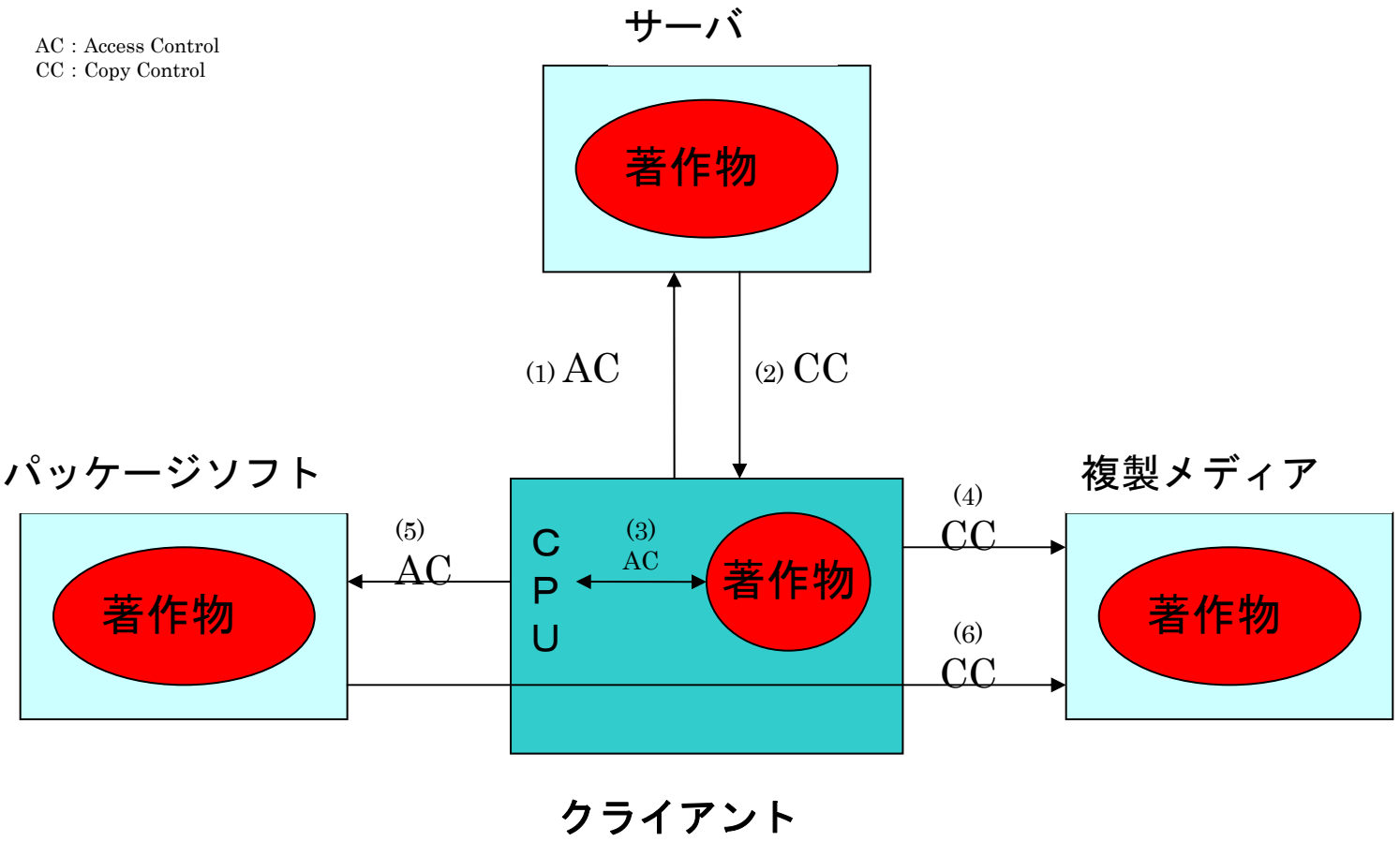
- 保護される著作物： ガレージ開閉システム
- 著作物の利用方法： ガレージ開閉装置は、ガレージのドアに付ける**開閉装置**と、これを遠隔操作する**携帯送信機**とから成る。開閉装置は、組み込まれた受信機が携帯送信機からの特定周波数の信号を受け取ると、信号処理ソフトウェアが開閉モーターに開閉の指示を出す。送信信号（rolling code system）は、固定部分と可変部分に分かれ、固定部分の信号は、発信器に固有のものである。可変部分の信号は、使用する度に変わるものであり、信号が盗用されることを防止するために、受信機が直近に受信した信号と同じ信号に対しては反応しないようになっている。ただし、本件製品は、特定の信号により初期設定モードとなる。
- 技術的手段： 開閉装置は、携帯送信機の発する信号により携帯送信機を認証する（AC）
- 回避方法： 消費者には、破損した携帯送信機の代わりやスペアとして、どの開閉装置にも使える汎用の携帯送信機に対する需要がある。回避行為者は、初期設定モードを生じさせて開閉を可能する携帯送信機を開発した。
- 判決： 1201条(a)(2)違反を否定

倉庫の保守プログラムにおける技術的手段

…*Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F3d 1307 (Fed Cir. 2005)

- 保護される著作物： データ保管倉庫の保守プログラム
- 著作物の利用方法： 原告は、大量のコンピュータデータを保管するテープ・カートリッジ・ライブラリーを製造販売する。原告は、第三者による原告システムの保守業務を阻止するために、コントロール・ユニットがエラーメッセージ「Event Message」を送信するには、パスワードの入力を必要とするプログラム「GetKey」を導入している。
- 技術的手段： パスワードによる認証（AC)
- 回避方法： 被告は、Event Messageを入手して保守作業を行うために、回避装置LEMおよびELEMを使った。LEMは、GetKeyのパスワードを探し当てる装置であった。
- 判決： 1201条(a)(1)違反を否定

技術的手段の要素技術


AC : Access Control
CC : Copy Control
サーバ
著作物
(1) AC
(2) CC
パッケージソフト
著作物
(5)
AC
C
P
U
(3)
AC
著作物
(4)
CC
(6)
CC
複製メディア
著作物
クライアント

技術的手段の機能と法的保護

	技術的手段	要素技術	使用事例	著作権法	不競法	不正ｱｸｾｽ禁止法	米国EU
AC	サーバ･アクセス制御	認証	クラウド、ストリーミング、オンラインゲーム、WM DRM、	―	―	○	○
	配信コンテンツ･アクセス制御	認証	システム内プログラム	―	―	―	○
		暗号化	WM DRM、iTune、B-CAS、	―	○	―	○
	パッケージソフト･アクセス制御	認証	パッケージソフト、DS、PS2	―	―	―	○
		暗号化	PS２、CSS、Blu-ray	―	○	―	○
		誤作動信号加	CCCD	―	―	―	○
CC	ダウンロード制御	認証	WM DRM、iTune、RealPlayer	―	―	―	○
	配信コンテンツ･コピー制御	専用プログラム	WM DRM、iTune、RealPlayer	―	―	―	○
		特定信号･専用機器	B-CAS、DirecTV	―	○	―	○
	パッケージソフト･コピー制御	誤作動信号付加	マクロビジョン	○	○	―	○
		特定信号･専用機器	DS、PS2、CSS、Blu-ray、SCMS	△	○	―	○

http://www.itlaw.jp/lait1.pdf