クラウド環境における法律問題（２）
ーアクセスコントロールに対する各国の法整備ー

IT企業法務研究所（LAIT）セミナー

２０１２年４月１２日

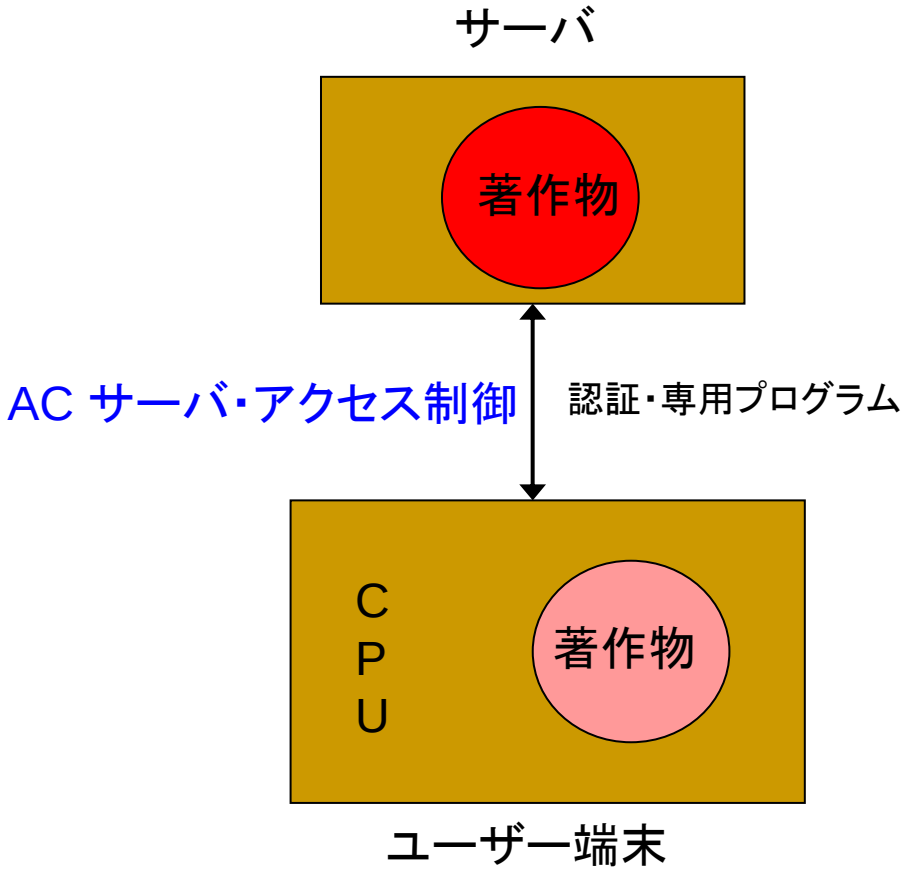
インフォテック法律事務所
弁護士　山 本　隆 司

前回の復習と今回の課題(1)

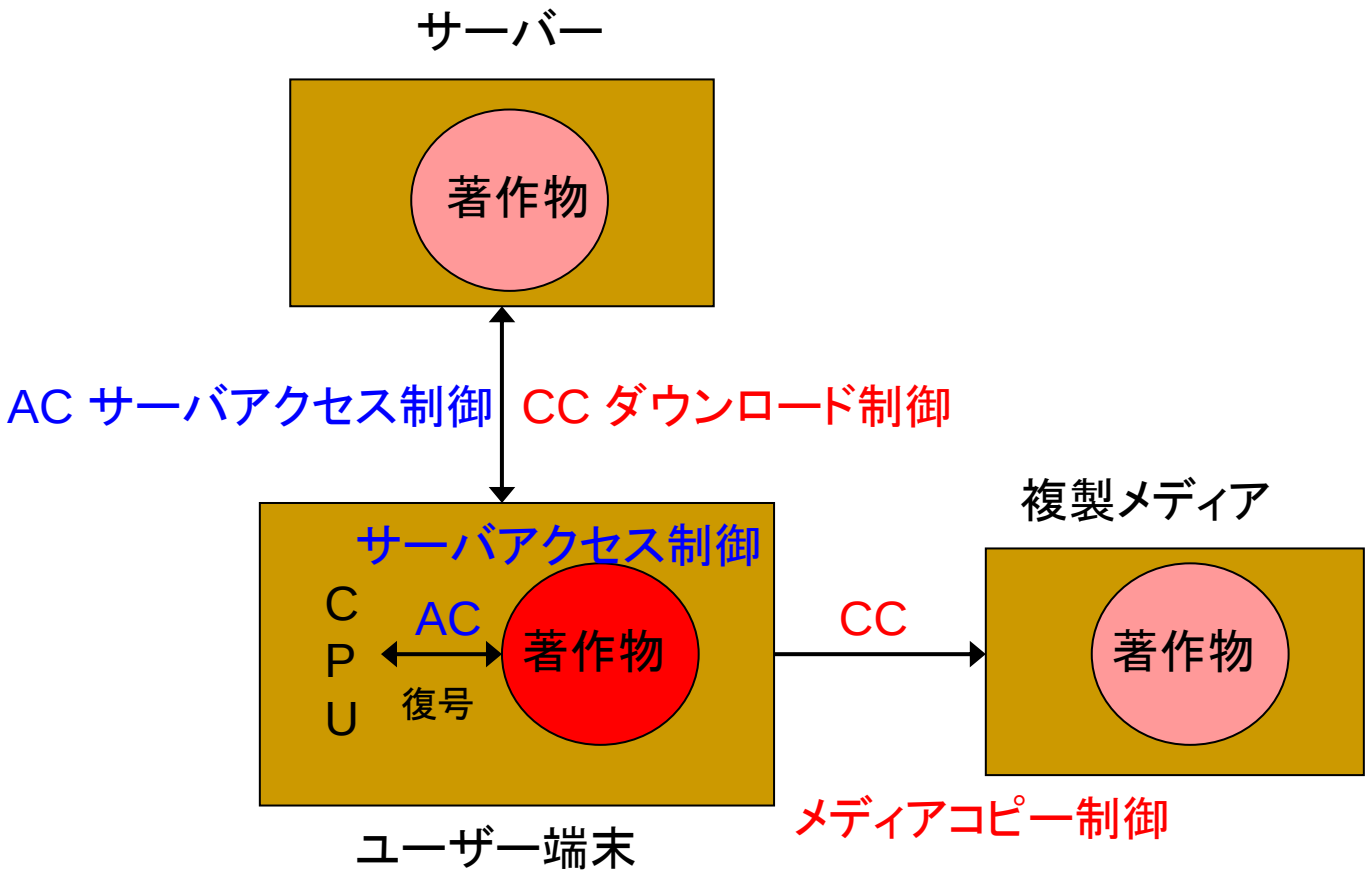
- 7つの利用形態

- 6つの要素技術
- 6つの技法
- 3つの固有問題

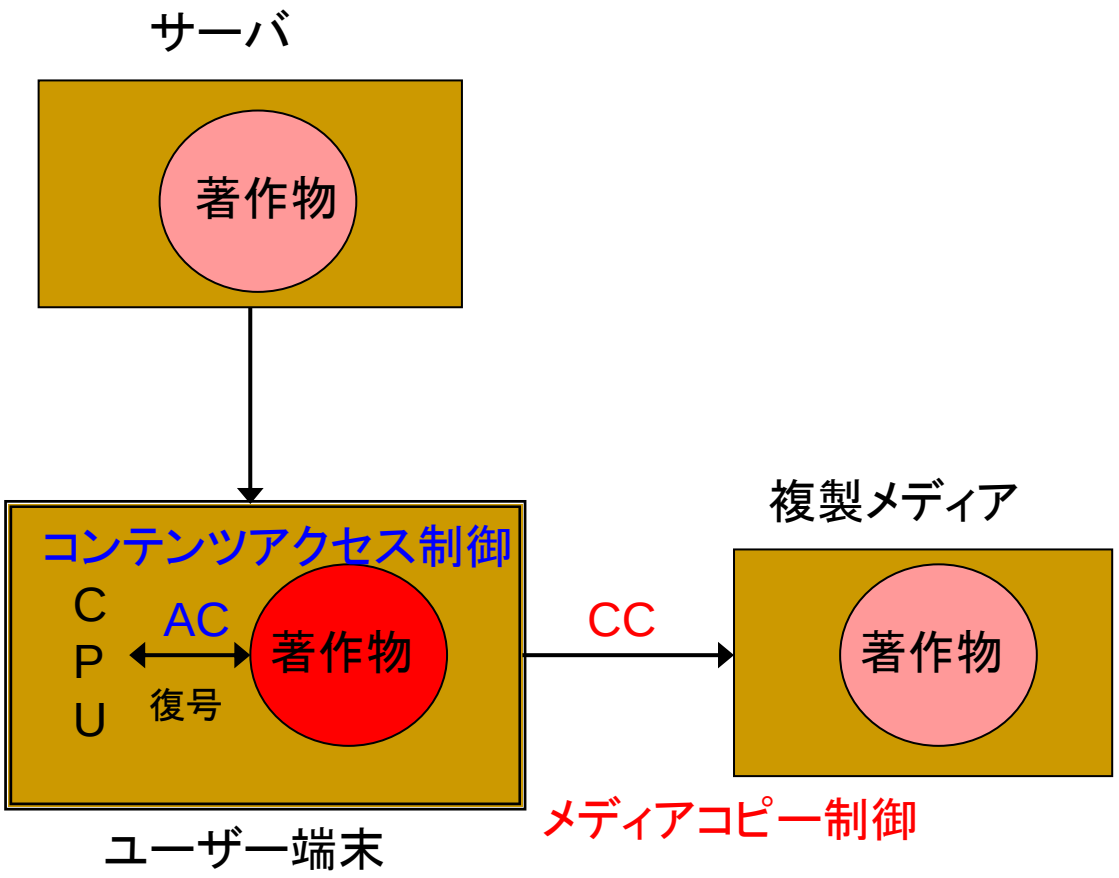
１－１　サーバ･アクセス制御



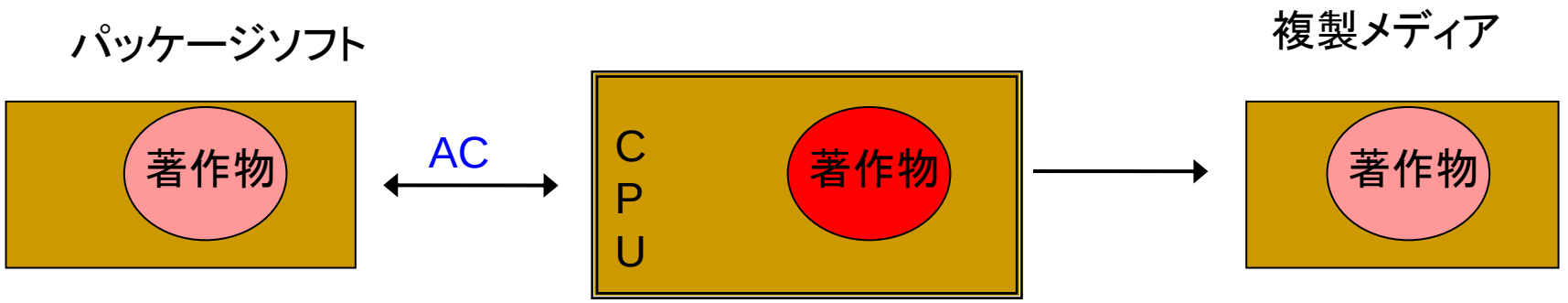
１－２　ダウンロード制御


サーバー
著作物
AC サーバアクセス制御
CC ダウンロード制御
複製メディア
サーバアクセス制御
C
P
U
AC
著作物
復号
CC
著作物
メディアコピー制御
ユーザー端末

１－３　配信コンテンツ･アクセス制御



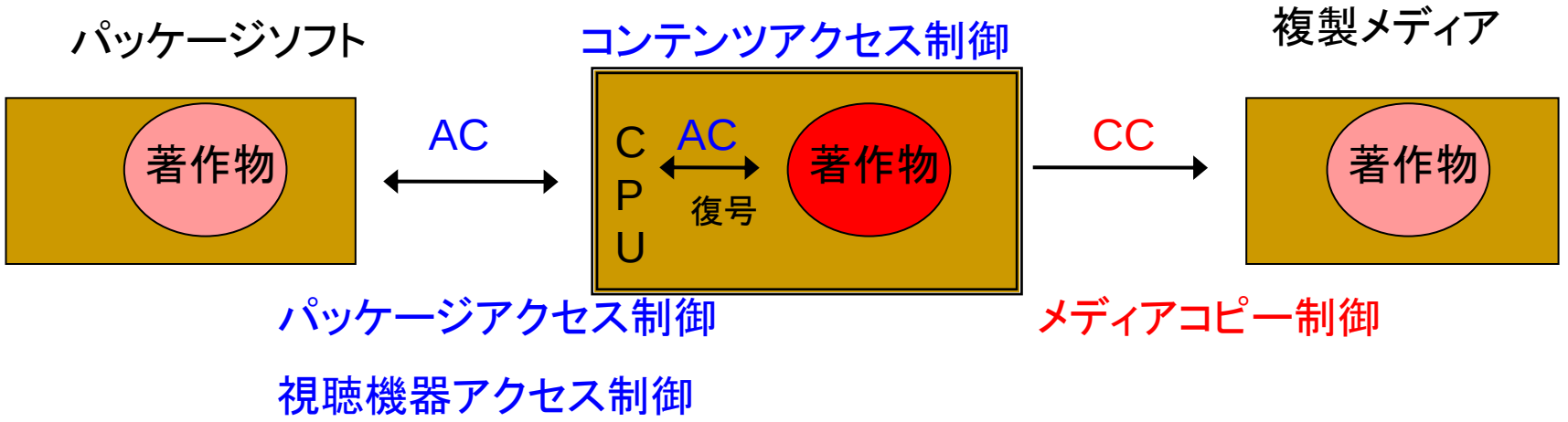
２－１　パッケージ＝機器・アクセス制御



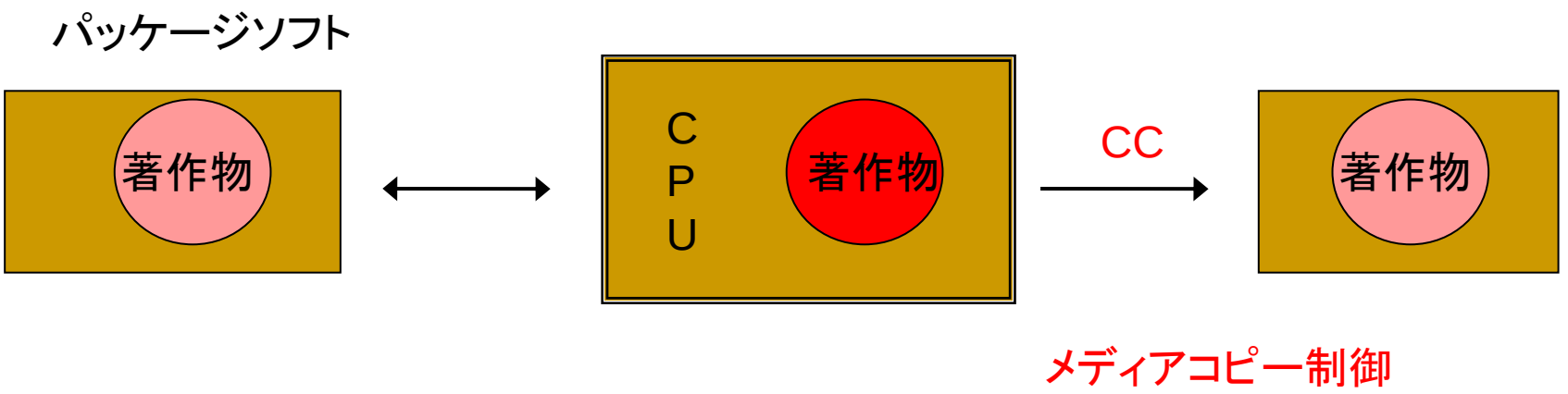
パッケージアクセス制御

視聴機器アクセス制御

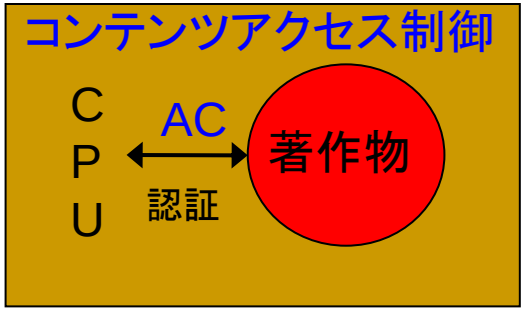
２－２　パッケージコンテンツ･アクセス制御



２－３　パッケージソフト･コピー制御



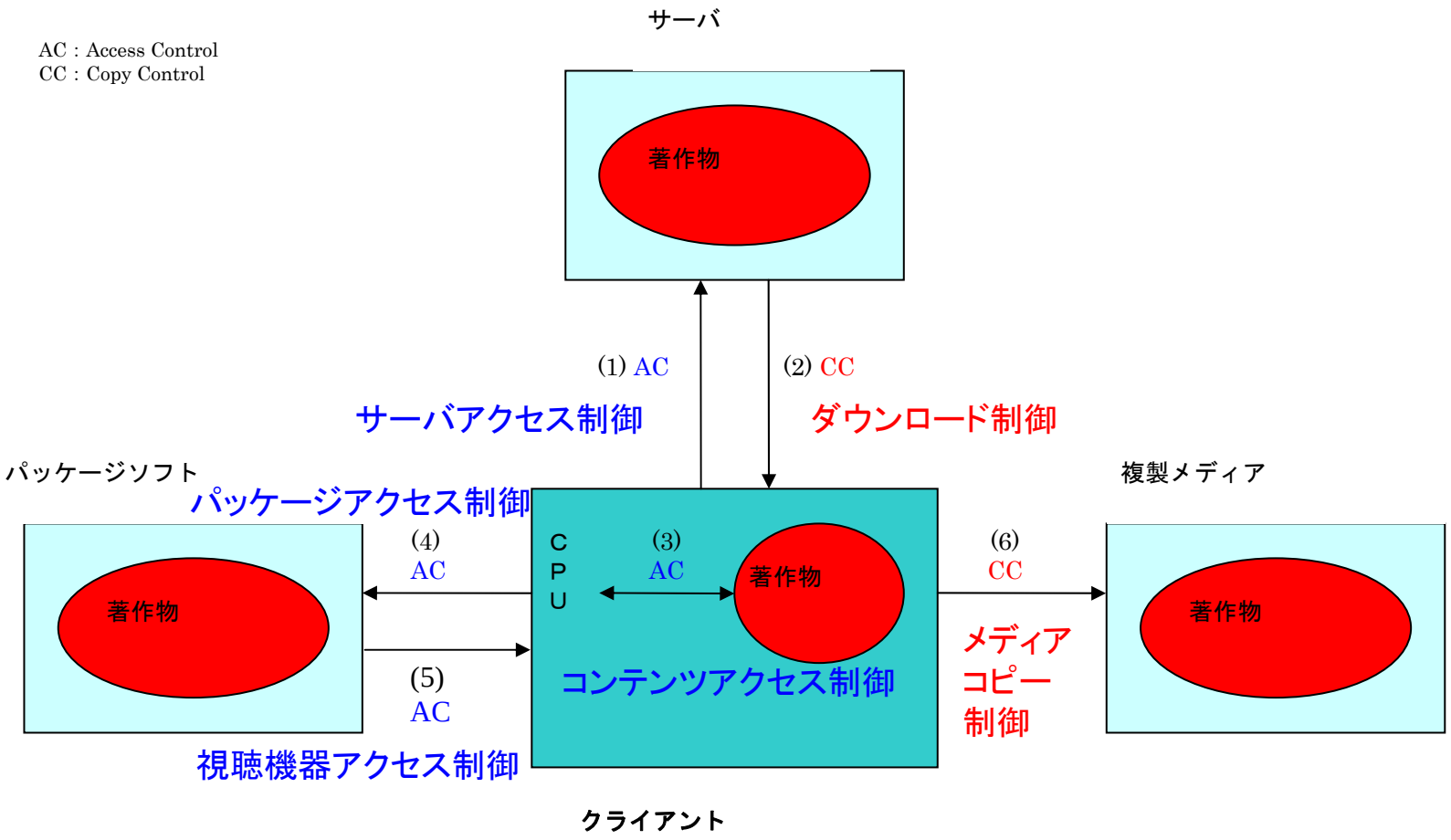
３　システム内コンテンツアクセス制御



ユーザー端末

前回の復習と今回の課題(2)

- 7つの利用形態
- 6つの要素技術
- 6つの技法
- 3つの固有問題


サーバ
AC : Access Control
CC : Copy Control
著作物
(1) AC
サーバアクセス制御
(2) CC
ダウンロード制御
パッケージソフト
パッケージアクセス制御
複製メディア
(4)
AC
C
P
U
(3)
AC
著作物
(6)
CC
著作物
著作物
(5)
AC
コンテンツアクセス制御
メディア
コピー
制御
視聴機器アクセス制御
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	―	―	○	○
	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･アクセス制御	認証	パッケージソフト	―	―	―	○
		暗号化	PS２、CSS、Blu-ray	△	○	―	○
		誤作動信号加	CCCD	―	―	―	○
	視聴機器アクセス制御	認証	DS、PS2	―	○		
CC	ダウンロード制御	認証	WM DRM、iTune、RealPlayer	―	―	―	○
	メディア･コピー制御	専用プログラム	WM DRM、iTune、RealPlayer	―	―	―	○
		専用機器	B-CAS、DirecTV 、CSS、Blu-ray	―	―	―	○
		コンテンツ付加信号	マクロビジョン、SCMS	○	○	―	○

前回の復習と今回の課題(3)

- 7つの利用形態
- 6つの要素技術
- 6つの技法
- 3つの固有問題

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	―	―	○	○
	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･アクセス制御	認証	パッケージソフト	―	―	―	○
		暗号化	PS２、CSS、Blu-ray	△	○	―	○
		コンテンツ付加信号	CCCD	―	―	―	○
	視聴機器アクセス制御	認証	DS、PS2	―	○		
CC	ダウンロード制御	認証	WM DRM、iTune、RealPlayer	―	―	―	○
	メディア･コピー制御	専用プログラム	WM DRM、iTune、RealPlayer	―	―	―	○
		専用機器	B-CAS、DirecTV 、CSS、Blu-ray	―	―	―	○
		コンテンツ付加信号	マクロビジョン、SCMS	○	○	―	○

前回の復習と今回の課題(4)

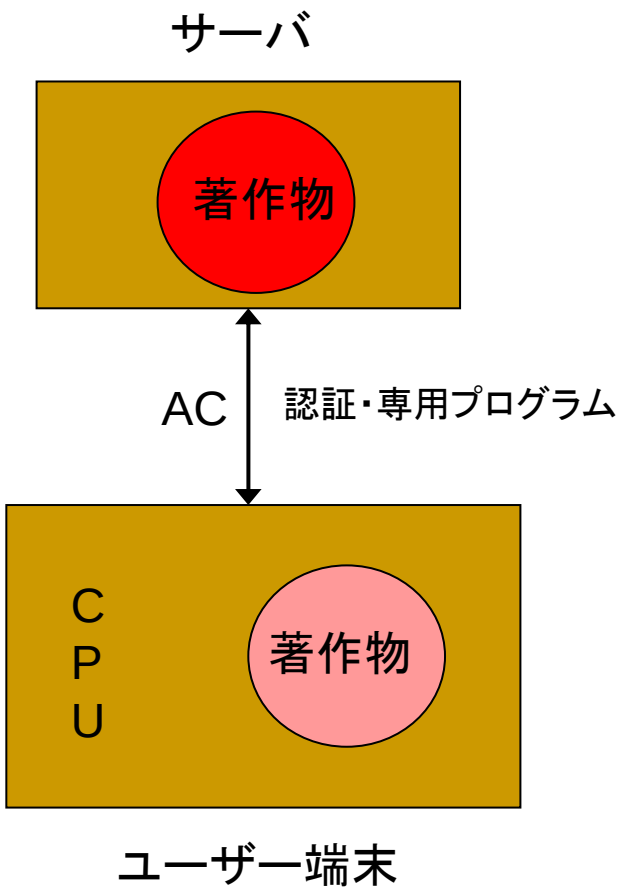
- 7つの利用形態
- 6つの要素技術
- 6つの技法

- 3つのAC固有問題

  既存の支分権では対応できない利用形態
  ・・・著作物使用の対価は、ACで回収

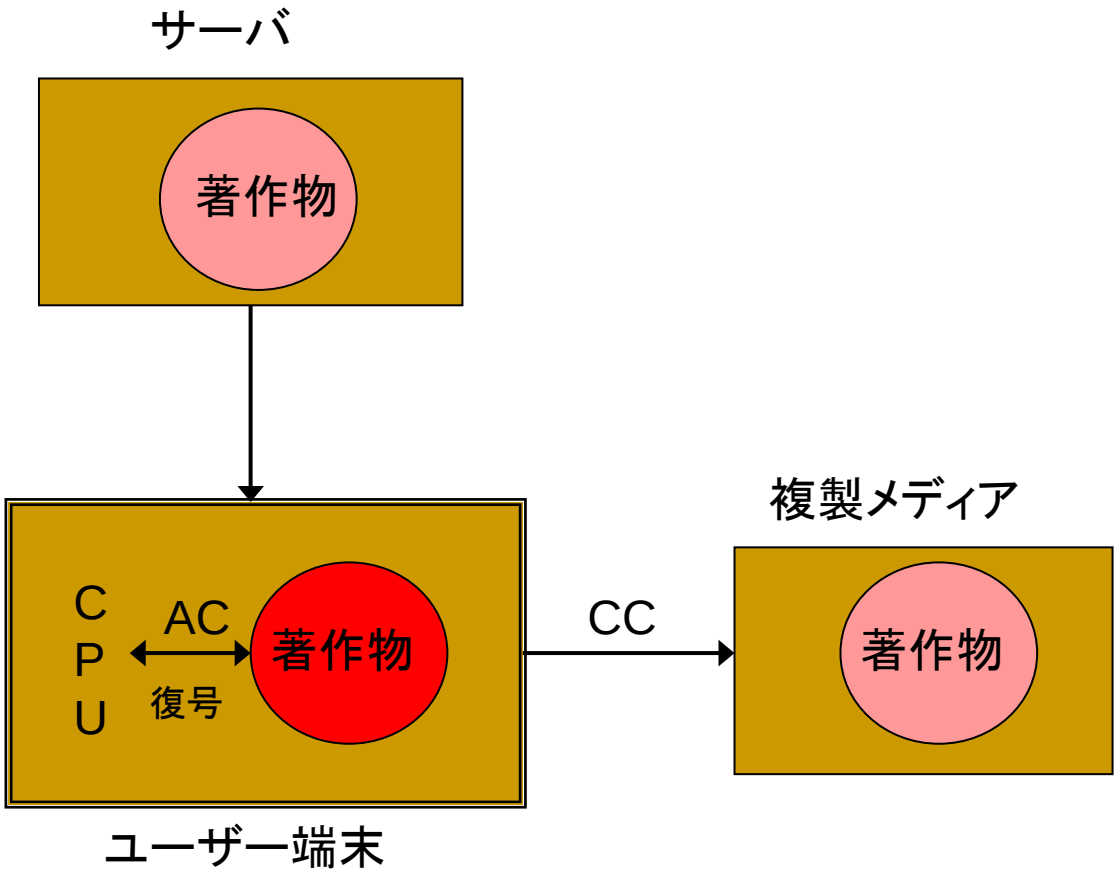
１－１　サーバ･アクセス制御

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



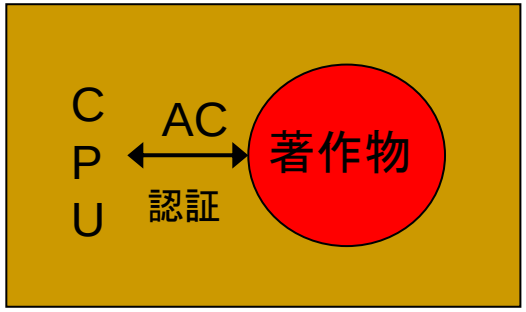
１－３　配信コンテンツ･アクセス制御

- B-CAS
- ケーブルテレビ
- DirecTV事件



３　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

１．日本におけるACの保護

（１）WIPO条約

WIPO著作権条約11条

「締約国は、著作者によつて許諾されておらず、かつ、法令で許容されていない行為がその著作物について実行されることを抑制するための効果的な技術的手段であつて、この条約又はベルヌ条約に基づく権利の行使に関連して当該著作者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。

→著作権を保護する技術的手段（コピー・コントロール）

アクセス・コントロールは侵害から保護すべき支分権が存在しないので、条約上、保護の義務を負わない。

→アクセス・コントロール（アクセス権）を、著作権法で保護する必要があるか、という「そもそも論」

（2）著作権法

- 技術的保護手段の定義（2条1項20号）

  「技術的保護手段　電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法…により、【著作権等】を侵害する行為の防止又は抑止…をする手段…であつて、著作物、実演、レコード、放送又は有線放送…の利用…に際し、これに用いられる機器が特定の反応をする信号を著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、若しくは送信する方式又は当該機器が特定の変換を必要とするよう著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像を変換して記録媒体に記録し、若しくは送信する方式によるものをいう。」

- 回避の定義（30条1項2号）

  「第2条第1項第20号に規定する信号の除去若しくは改変（記録又は送信の方式の変換に伴う技術的な制約による除去又は改変を除く。）を行うこと又は同号に規定する特定の変換を必要とするよう変換された著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像の復元（著作権等を有する者の意思に基づいて行われるものを除く。）を行うことにより、当該技術的保護手段によつて防止される行為を可能とし、又は当該技術的保護手段によつて抑止される行為の結果に障害を生じないようにすることをいう。」

- 規制
  - 私的複製の限界（30条1項2号）
  - 刑事罰（120条の2第1号、第2号）

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	―	―	○	○
	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･アクセス制御	認証	パッケージソフト	―	―	―	○
		暗号化	PS２、CSS、Blu-ray	△	○	―	○
		誤作動信号加	CCCD	―	―	―	○
	視聴機器アクセス制御	認証	DS、PS2	―	○		
CC	**ダウンロード制御**	認証	WM DRM、iTune、RealPlayer	―	―	―	○
	メディア･コピー制御	専用プログラム	WM DRM、iTune、RealPlayer	―	―	―	○
		専用機器	B-CAS、DirecTV 、CSS、Blu-ray	―	―	―	○
		コンテンツ付加信号	マクロビジョン、SCMS	○	○	―	○

（3）不正競争防止法

① 技術的制限手段の定義（2条7項）

「電磁的方法（・・・）により影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を制限する手段であって、視聴等機器（・・・）が特定の反応をする信号を影像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式又は視聴等機器が特定の変換を必要とするよう影像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式によるものをいう。」

② 規定の方法

2条1項10号（一般的制限）

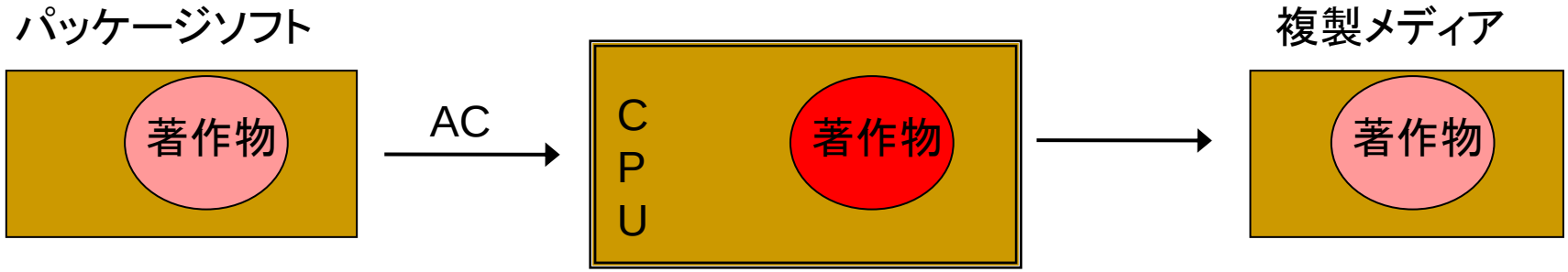
2条1項11号（選択的制限）

③ 制度趣旨

・・・コンテンツ提供事業者の保護のために、技術的手段の解除という行為に違法性を認める。

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

（4）不正アクセス禁止法

① 「不正アクセス行為」に対して、一年以下の懲役又は五十万円以下の罰金を課す（3条1項、8条）。

② 不正アクセス行為の定義
「一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為…
　二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報…又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為…
　三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為 」

③ 制度趣旨
　電気通信上の犯罪の防止および電気通信に関する秩序維持を目的とする。著作物というコンテンツの保護は目的ではない。

東京地裁平成17年3月25日判決

- アクセス制御機能のある他人のサーバに、プログラムの瑕疵や設定の不備（セキュリティホール）がなければ、IDとパスワードなしにはアクセスできないところ、被告人は、セキュリティホールを利用してID・パスワードなしに無断で当該サーバからデータをダウンロードした。
- 裁判所は、プログラムの瑕疵や設定の不備（セキュリティホール）がなければアクセスできない場合にはアクセス制御機能があるコンピュータに該当すると判示し、不正アクセス禁止法違反として、被告人を懲役8月、執行猶予3年の刑に処した。

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	―	―	○	○
	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･アクセス制御	認証	パッケージソフト	―	―	―	○
		暗号化	PS２、CSS、Blu-ray	△	○	―	○
		誤作動信号加	CCCD	―	―	―	○
	視聴機器アクセス制御	認証	DS、PS2	―	○		
CC	**ダウンロード制御**	認証	WM DRM、iTune、RealPlayer	―	―	―	○
	メディア･コピー制御	専用プログラム	WM DRM、iTune、RealPlayer	―	―	―	○
		専用機器	B-CAS、DirecTV 、CSS、Blu-ray	―	―	―	○
		コンテンツ付加信号	マクロビジョン、SCMS	○	○	―	○

2. 米国におけるACの保護

（1）1992年家庭内録音法（著作権法1001条以下）

- SCMS（連続コピー制御システム）の義務づけ（1002条(a)）
「何人も、以下に適合しないデジタル音声録音装置またはデジタル音声インターフェイス装置を輸入し、製造しまたは頒布してはならない。
(1) 連続コピー制御システム。
(2) 連続コピー制御システムと同一の機能的特徴を有し、かつ、当該方式の連続コピー制御を使用する装置と連続コピー制御システムを使用する装置との間で、著作権および世代の状況に関する情報を正確に送信し、受信しかつ作用することを要するもの。
(3)　その他、商務長官が無断の連続コピーを禁止されたシステムであると証明するもの。」

- SCMS回避装置等の禁止（1002条(c)）
「何人も、第(a)項に定めるシステムの全部または一部を実行するプログラムまたは回路を忌避し、迂回し、除去し、無効にし、その他回避することを主たる目的または主たる効果とする装置を輸入し、製造しまたは頒布し、またはかかる目的または効果を有するサービスを提供しもしくはその提供申出を行ってはならない。」

（2）DMCA（1976年著作権法1201条）

① アクセス・コントロールの回避行為禁止 (a)(1)
② アクセス・コントロールの回避装置取引禁止 (a)(2)
③ コピー・コントロールの回避装置取引禁止 (b)(1)

(a)(2) AC回避装置	(b)(1) CC回避装置
(a)(1) AC回避行為	著作権侵害行為

①アクセス・コントロールの回避行為禁止

1201条(a)(1)

「(A) 何人も、本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避してはならない。…」

回避:「著作権者の許諾なく、スクランブルがかかっている著作物のスクランブルを解除し、暗号化された著作物の暗号を解除し、またはその他技術的手段を回避し、迂回し、除去し、無効にしもしくは損壊すること」(1201条(a)(3)(A))

著作物へのアクセスを効果的にコントロールする:「当該技術的手段がその動作の通常の過程において著作物へのアクセスを行うには、著作権者の許諾を得て情報を入力しまたは手続もしくは処理を行うことを必要とする場合」(1201条(a)(3)(B))

②アクセス・コントロールの回避装置取引禁止

1201条(a)(2)

「何人も、以下のいずれかに該当するいかなる技術、製品、サービス、装置、部品またはそれらの一部分を製造し、輸入し、公衆に提供し、供給しまたはその他流通させてはならない。

(A) 本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避することを主たる目的として設計されまたは製造されるもの。

(B)本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避する以外には、商業的に限られた目的または用法しか有しないもの。

(C)本編に基づき保護される著作物へのアクセスを効果的にコンロールする技術的手段を回避するために使用することを知っている者またはこれに協力する者によって販売されるもの。」

③コピー・コントロールの回避装置取引禁止

1201条(b)(1)

「何人も、以下のいずれかに該当するいかなる技術、製品、サービス、装置、部品またはそれらの一部を製造し、輸入し、公衆に提供し、供給しまたはその他流通させてはならない。

(A) 著作物またはその一部分に対する本編に基づく著作権者の権利を効果的に保護する技術的手段により施される保護を回避することを主たる目的として設計されまたは製造されるもの。

(B)著作物またはその一部に対する本編に基づく著作権者の権利を効果的に保護する技術的手段により施される保護を回避する以外には、商業的に限られた目的または用法しか有しないもの。

(C)著作物またはその一部に対する本編に基づく著作権者の権利を効果的に保護する技術的手段により施される保護を回避するために使用することを知っている者またはこれに協力する者によって販売されるもの。」

④適用除外等

- AC保護の適用除外（a(1)(B)-(E)）・・・AC固有
- 著作権の権利制限との関係（c）・・・AC＋CC
  「（1）本条のいかなる規定も、著作権侵害にかかる本編に基づく権利、救済、制限または抗弁(フェア・ユースを含む)に影響を及ぼさない。」
- 非営利の図書館等に対する免責（d）・・・AC固有
- 政府の情報収集行為に対する免責（e）・・・AC＋CC
- リバース・エンジニアリングに対する免責（f）・・・AC＋CC
- 暗号化研究に対する免責（g）・・・AC固有
- 未成年者の保護のための免責（h）・・・AC固有
- 個人識別情報の保護のための免責（i）・・・AC固有
- セキュリティ検査に対する免責（j）・・・AC固有
- 放送局による一時的固定物の作成に対する免責（112条a(2)）・・・AC固有

（3）DMCA立法経緯

- 1995年ホワイトペーパー
  ・・・著作権侵害の文脈でACを捉えている
- 1996年WIPO条約
- 1997年下院コーブル法案→DMCA
- 1997年上院アッシュクロフト法案
  ・・・CC回避装置の禁止のみを規定

（4）DMCAの立法趣旨（上院報告書105-190）

「デジタル著作物を複製し事実上瞬時に世界中に頒布することが容易なので、著作権者は、著作物が大規模盗用から保護される合理的な保障がなければ、著作物をインターネット上で利用可能にすることに躊躇する。前記条約【WIPO著作権条約等】を施行する法律は、かかる保護を与え、かつ、著作権のある著作物のためにグローバルなオンライン市場を可能にするプラットフォームを形成するものである。この保護を提供し、グローバルに著作権のある著作物のオンライン市場を形成する法的基盤を構築する。これは、アメリカの創造的才能の成果物である映画、音楽、ソフトウェアおよび言語著作物をインターネットを介して即座にかつ便利に利用可能にすることを促進する。また、強力な国際著作権標準を定めることによりデジタル形式の著作権のある著作物のための既存のオフラインのグローバル市場の継続的な成長を後押しするものである。」

「法案第1201条(a)(2)および第1201条(b)は、似たような言葉で表現され、似たようなテストを採用しているが、これらは、2つの異なった権利を保護し、2つの異なった種類の装置を対象とするように設計されている。第1201条(a)(2)は、著作権のある著作物へのアクセスを保護するよう設計されている。第1201条(b)は、著作権者の伝統的な著作権の権利を保護するよう設計されている。…

言い換えると、これが、第1201条(a)(1)に規定する回避行為に関する禁止事項と同等の行為に関する禁止事項が第1201条(b)に規定されていない理由である。本法以前は、回避行為が違法とされていなかったため、第1201条(a)(1)の禁止事項は必要である。第1201条(a)(2)の装置制限は、この新たな行為禁止を強化するものである。著作権法は長い間、著作権侵害を禁じていたため、新たな禁止事項は必要なかった。第1201条(b)の装置の制限は、昔から続く侵害禁止を強化するものである。」

	アクセス・コントロール	コピー・コントロール
侵害する装置	1201条(a)(2): AC回避装置の禁止	1201条(b): CC回避装置の禁止
侵害される権利	1201条(a)(1): 無断アクセスの禁止	106条の支分権 :無断複製等の禁止

（５）制限的解釈論・・・チェンバレン判決の乱

- アクセス独自法益説
  →著作権侵害が生じない場合でも、回避は違法
  →フェア・ユースのためでも回避も違法

- 著作権法益説（チェンバレン判決）
  →著作権侵害が生じない場合は、回避は適法
  →フェア・ユースのためなら回避は適法

① Chamberlain v. Skylink (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

「DMCAの回避禁止規定は、1201条(a)、(b)が責任追及の請求原因を創設するものである点に本質がある。それらは、新たな財産権を創設するものではない。DMCAの文言は、回避が著作権侵害でないことを示しており(・・・)、法律の構造はこの点をさらに明確にしている。財産権と責任の区別は決定的に重要である。・・・著作権は財産権であるが、無断回避からの保護のための責任は被告に責任を負わせる請求原因を形成するにとどまる。」
「侵害を助長する方法でアクセス・コントロールを回避する装置を取り引きする被告は、1201条(a)(2)に基づく責任を負いうる。かかる装置を使用する被告は、それが侵害であろうとなかろうと、1201条(a)(1) に基づく責任を負いうる。権利のコントロールを回避する装置を取り引きする被告は、侵害を助長するので、1201条(b) に基づく責任を負いうる。そして最後に、回避装置が侵害を助長しない場合には、被告は1201条の責任を負うことはない。」
「当裁判所の結論によれば、1201条は、著作権法が著作権者に与える保護との合理的関係を有するアクセスの形態のみを禁止するものである。」

…その根拠として、明文解釈には以下の問題があるとする。
ⓐ公衆によるアクセスを違憲的なほど不合理に制限する
ⓑ1201条(c)(1)と矛盾する。…フェア・ユースがアクセス・コントロールによって阻止される事態を生ずる。
ⓒ独禁法に反してアフターマーケット独占を認めることになる。

② MDY v. Blizzard (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。

「当裁判所は、1201条が二つの異なる種類の請求権を創設するものであると理解するのが最善であると考える。第1に、1201条(a)は、保護されている著作物へのアクセスを効果的にコントロールする技術的手段の回避を禁止し、著作権者に当該禁止を執行する権利を与えるものである（コーレイ判決参照）。第2に、また1201条(a)とは対照的に、1201条(b)(1)は、『著作権者の権利』を効果的に保護する技術的手段の回避技術の取引を禁止し、それによって、1201条(b)(1)の禁止は、著作権それ自身を保護する技術の回避を対象とし、著作権法上の既存の排他的権利を保護する権利を著作権者に付与するものである。」

「当裁判所のみるところ、立法経緯は、連邦議会が1201条(a)において伝統的な著作権侵害から独立した新たな回避禁止権を創設し、1201条(b)(1)において著作権者に著作権侵害に対する新たな武器を与えたとの見解を裏付ける。」

「当裁判所は、法律を公平に読むならば（また立法経緯が裏付けるとおり）連邦議会は侵害関連性要件を課すことなく、1201条(a)に基づいて別個の回避禁止権を創設したものである、と結論する。・・・したがって、当裁判所は、侵害関連性要件を課すことを拒否する。」

…Chamberlain判決の論拠に対する反論：

ⓐ公衆によるアクセスは1201条(a)(1)(B)～(D)で合憲的に保護される。

ⓑ1201条(a)(1)が新たな権利の創設と考えれば、1201条(c)(1)と矛盾しない。アクセス・コントロールに対する権利制限は1201条(d)以下に個別に定められている。

ⓒアフターマーケット独占を生じる場合に、独禁法違反を考えればよい。

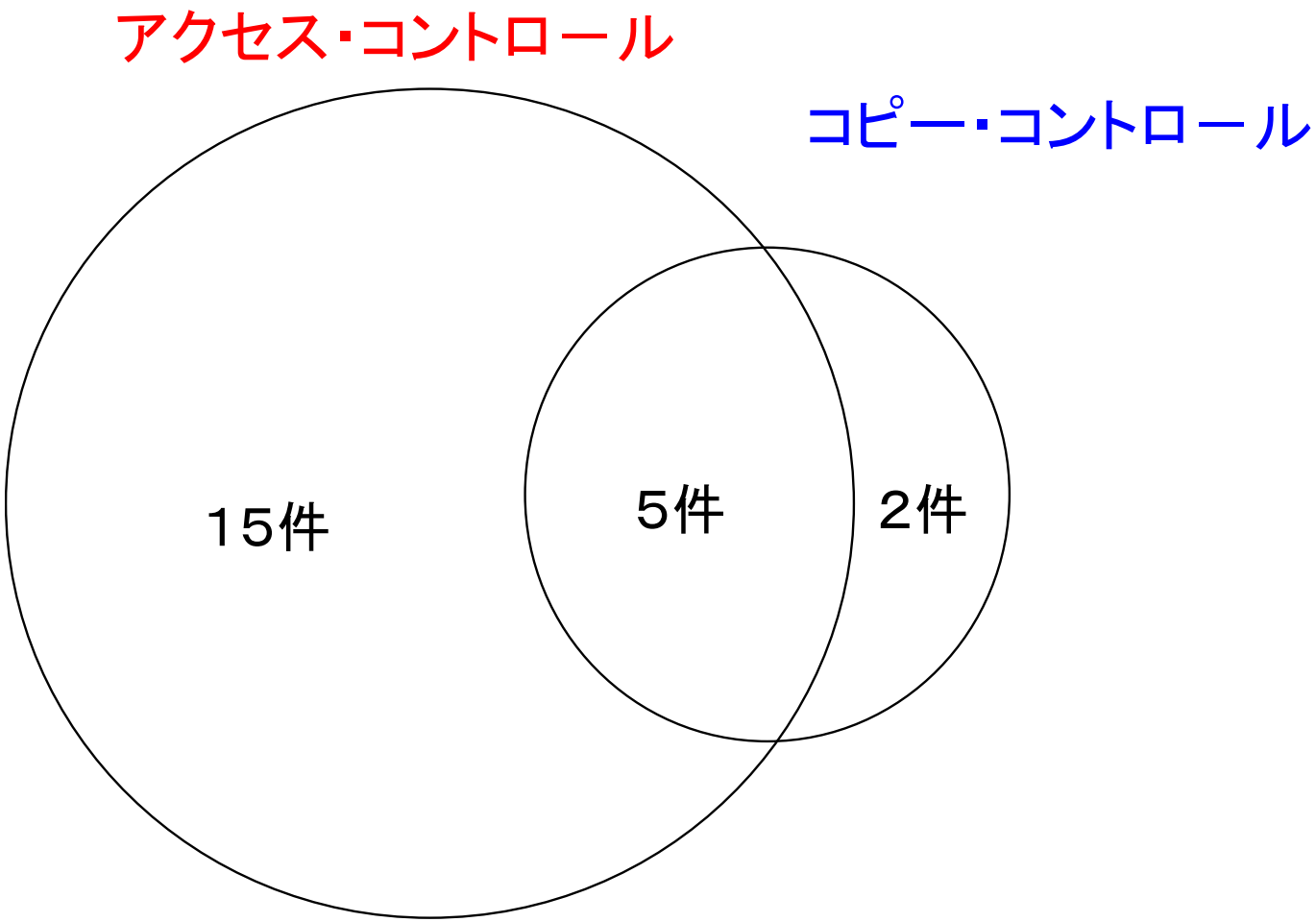
③ Universal City Studios v. Corley (2d Cir. 2001)

- 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←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

「被告の主張によれば、『本条のいかなる規定も、著作権侵害にかかる本編に基づく権利、救済、制限または抗弁（フェア・ユースを含む）に影響を及ぼさない。』と規定する1201条(c)(1)は、著作物の『フェア・ユース』が著作権侵害責任を免除する場合には当該著作物を保護する暗号化技術を回避することも許容するものと読むことができる。当裁判所は、1201条(c)(1)がこのような読み方を許容するものとは考えない。そうではなく、DMCAが著作物を保護するデジタル防護壁の回避（および回避道具の取引）を対象とするものであって、回避後の著作物の使用自体を問題にするものではないことは、単純明白である。1201条(c)(1)は、情報がDMCAに違反する方法で取得したことをもって、当該情報の使用の『フェア・ユース』を禁止するものと解釈されてはならない、ようにするものである。被告のような1201条(c)(1)に対する拡大解釈は、条文の合理的解釈を越えるにとどまらず、この法律の立法経緯からも明らかに排除されるものである（…）。」

アクセス・コントロール裁判例	アクセス独自法益説		著作権法益説	
	フェア・ユース論	要件論	フェア・ユース論	要件論
RealNetworks v. Streambox (WD Wash. 2000)	○	○		
Universal City Studios v. Corley (2d Cir. 2001)	○	○		
Pearl Investments v. Standard I/O (D Me. 2003)	○			
321 Studios v. MGM (ND Cal. 2004)	○			
Comcast v. Hightech Electronics (ND Ill. 2004)	○			
Chamberlain v. Skylink (Fed Cir. 2004)			○	○
Lexmark v. Static (6th Cir. 2004)	○			
DirecTV v. Borow (ND Ill. 2005)	○			
Davidson v. Jung (8th Cir. 2005)	○			
Storage v. Custom Hardware (Fed Cir. 2005)			○	
Auto Inspection v. Flint (ED Mich. 2006)	○			
Sony v. Divineo (N.D.Cal. 2006)	○	○		
Healthcare v. Harding (ED Pa. 2007)	○			
Ticketmaster v. RMG (CD Cal. 2007)			○	
CoxCom v. Chaffee (1st Cir. 2008)	○			
MGE v. GE (5th Cir. 2010)			○→X	
MDY v. Blizzard (9th Cir. 2010)	○	○		

（６）主要裁判例



裁判例	コンテンツ		
	ネット	パッケージ	システム内
RealNetworks v. Streambox (WD Wash. 2000)	１－２		
Universal City Studios v. Corley (2d Cir. 2001)		２－２	
US v. Elcom (ND Cal. 2002)	１－２		
Pearl Investments v. Standard I/O (D Me. 2003)			３
321 Studios v. MGM (ND Cal. 2004)		２－２	
I.M.S. v. Berkshire (SD NY 2004)	１－１		
Comcast v. Hightech Electronics (ND Ill. 2004)	１－３		
Chamberlain v. Skylink (Fed Cir. 2004)			３
Lexmark v. Static (6th Cir. 2004)			３
DirecTV v. Borow (ND Ill. 2005)		２－２	
Davidson v. Jung (8th Cir. 2005)	１－１		
Storage v. Custom Hardware (Fed Cir. 2005)			３
Egilman v. Keller & Heckman (D DC 2005)			３
Macrovision v. Sima (SD NY 2006)		２－３	
Auto Inspection v. Flint (ED Mich. 2006)			３
Sony v. Divineo (N.D.Cal. 2006)		２－２	
Healthcare v. Harding (ED Pa. 2007)	１－１		
Ticketmaster v. RMG (CD Cal. 2007)	１－１		
CoxCom v. Chaffee (1st Cir. 2008)	１－３		
Blueport v. US (Fed Cir. 2008)			３
MGE v. GE (5th Cir. 2010)			３
MDY v. Blizzard (9th Cir. 2010)	１－１		

（7）技術的手段とは

① 技術的手段の性質

(a) 技術的手段として脆弱であっても技術的手段に当たる
…Corley

(b) 回避方法がすでに公知・公用になっていても技術的手段に当たる
…321Studios

(c) すべてのアクセスを制限していなければ技術的手段に当たらない
・・・Lexmark判決の裏口理論

→ (i)玄関も裏口も鍵を掛けてあるときに、鍵を破って侵入… ×
(ii)玄関も裏口も鍵を掛けてあるときに、トイレの小窓から侵入… ×
(iii)裏口にのみ鍵を掛けてあるときに、玄関から侵入 …○
(iv)裏口にのみ鍵を掛けてあるときに、鍵を破って裏口から侵入…○
(v)玄関のみに鍵を掛けてあるときに、裏口から侵入…○

② 技術的手段の種類

- ファイル形式自体は技術的手段ではない
  …RealNetworks、(Healthcare)
- パスワードは技術的手段に当たる
  …Pearl
- secret handshake(認証コード)は技術的手段に当たる
  …RealNetworks、Davidson
- 画像に乱れを生じさせる信号は技術的手段に当たる
  …Macrovision
- 人からのアクセスではなく機械による自動的アクセスを排除するものも技術的手段に当たる
  …Ticketmaster
- ソフトに付された利用状況を監視プログラムは技術的手段に当たる(？)
  …Auto Inspection
- ケーブルテレビの視聴実績データを送信する機能も技術的手段に当たる(？)
  …CoxCom

Lexmark v. Static (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

「原告のプリンターを購入した者は誰でも、当該認証コードを利用しようとしまいと、直接にプリンターのメモリーからプリンター・エンジン・プログラムを読むことができ、当該プログラムのデータは解読可能なソース・コードに翻訳することもその後にその複製物を自由に頒布することも可能である。言い換えれば、いかなるセキュリティ装置もプリンター・エンジン・プログラムへのアクセスを保護しておらず、したがって、当該プログラム・コードへのアクセスに当たって回避されなければならないいかなるセキュリティ装置も存在しない。

確かに、認証コードは、プリンターが機能しないようにしてプリンター・エンジン・プログラムを利用できるようにするという『アクセス』の一つの方式を阻止する。しかし、それは、当該著作物の複製物を入手するまたは当該プログラムの文字的要素を利用できるようにするという『アクセス』の他の方式を阻止しない。法律は『本編に基づき保護される著作物へのアクセスをコントロールする』ことと言っており、『本編に基づき保護される著作物』が他方法によってアクセスされうる場合にも当然には適用があるわけではない。玄関のドアに鍵をかけていなければ裏口のドアに鍵をかけてもその家への『アクセスをコントロール』しているとは言えないのと全く同様に、また、家のすべてのドアに鍵をかけても購入者に鍵を渡した後ではその家への『アクセスをコントロール』しているとは言えないのと全く同様に、著作権のある著作物にすでに他の方法でアクセス可能になっているものにDMCAのこの規定を適用することは無意味である。さらに、DMCAは技術的手段に『アクセスをコントロール』することという要件を求めるだけでなくアクセスを『効果的に』コントロールする手段であることを求めている（合衆国法典17編1201条(a)(2)）との事実に着目すれば、この規定がアクセスの一形態のみを制限し、他の方法を広く放置している技術的手段に対して当然には及ぶものではないことは、明らかなように思われる。」

（8）回避とは

- パスワードのランダム入力
- 真正に発行されたパスワードの利用
  - 利用者から借りて利用することは回避に当たらない…IMS
  - 不正に入手して利用することは回避に当たらない（？）…Egilman
- リバースによる認証コードの解析
- 技術的手段であるプログラムの除去
- 他のアクセス方法の付加
  …Divineo（認証信号を読み取らなくともゲームを実行するようなプログラムを付加することは回避に当たる）

3. EUにおけるACの保護

（1）EU指令

- 1991年コンピュータプログラム指令
「コンピュータプログラムを保護するために施された技術的装置を無断で除去または回避することを可能にすることのみを目的とする手段を流通させまたは商業目的で所持する行為」を禁止する（7条（c））。

- 2001年情報社会指令
・・・著作物等について「有効」な「技術的手段」の回避を禁止し（6条1項）、また、「有効」な「技術的手段」を回避する装置の製造と取引を禁止する（6条2項）。

  - 「技術的手段」：「著作権もしくは法令の規定する関連権または96/9/EC指令第3章に規定するスイ・ジェネリス権の保有者の許諾を受けない行為を、著作物その他の保護対象物に関して、通常の操作過程において、禁止または制限するように設計された技術、装置または部品をいう。」（6条3項前段）。

  - 技術的手段が「有効」：「権利保有者が、著作物その他の保護対象物の暗号化、スクランブルその他の変形などのアクセス・コントロールもしくは保護手順または当該保護目的を達成するコピー・コントロールを施すことによって、保護される著作物または保護対象物の使用をコントロールする場合をいう」（6条3項後段）。

（2）ドイツ著作権法

- 69f条
「(1) 権利保有者は、所有者又は占有者に対して、違法に製作され若しくは頒布され又は違法な頒布のために特定された複製物のすべてを廃棄するよう求めることができる。第98条第3項及び第4項は、ここに準用するものとする。
(2) 前項は、技術的なプログラム保護機構の不法な除去又回避を容易にすることに専ら特定された手段について、準用するものとする。」
- 95a条
「(1) この法律に基づき保護を受ける著作物その他この法律に基づき保護を受ける保護対象の保護のために有効な技術的手段は、それを回避する行為が当該著作物若しくは保護対象へのアクセス又はそれらの使用を可能にすることを目的として行われることを、その行為者が知り、又は諸般の事情に照らし知るべきものと認められるときは、権利保有者の同意を得ることなく回避してはならない。」

（3）フランス著作権法

- １２２の６の２条
「ソフトウェアを保護するいずれかの技術的装置の除去又は回避を可能とする手段に関するいずれの広告又は使用説明書も、それらの手段の違法使用が、侵害の場合に規定される制裁を課されるべき旨を記載しなければならない。」
- ３３１の５条
「著作物（ソフトウェアを除く。）の著作権者又は実演、レコード、ビデオグラム若しくは番組の著作隣接権者が許諾していない使用を防止すること、又は制限することに当てられる有効な技術的手段は、この章に規定する条件に従って保護される。」

（4）イギリス著作権法

- 296条
  コンピュータプログラムに適用される「技術的装置の無許諾の除去又は回避を容易にすることを唯一の意図された目的とするいずれかの手段」の販売等および「技術的装置を除去し、若しくは回避することを可能とし、又は補助することを意図される情報」の公表を禁止する。
- 296条のZA
  コンピュータプログラム以外の著作物に適用される有効な技術的手段を、故意または過失で回避する 行為を禁止する。
- 296条のZA
  有効な技術的手段の回避することを目的とする装置等の販売等を禁止する。

4. アクセス権を創設すべきか

（1）アクセス権否定論

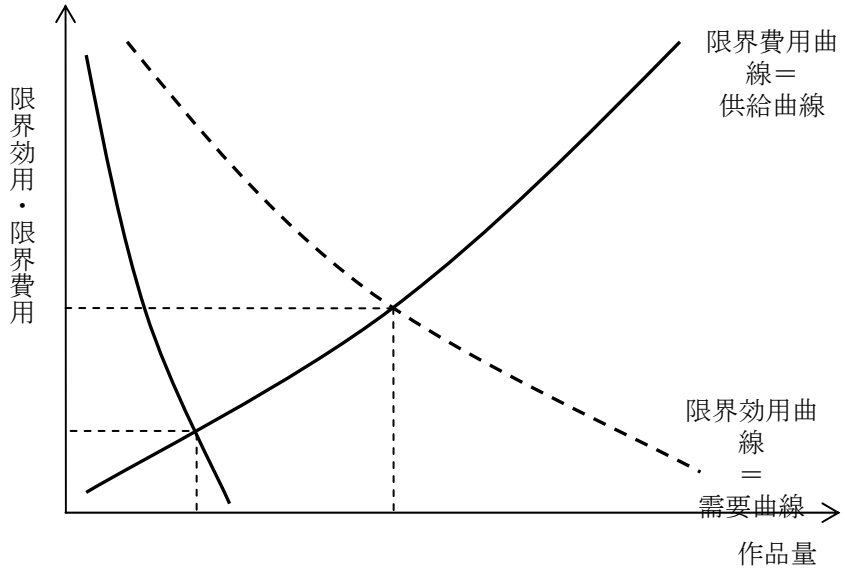
「使用は個人の聖域ないし権利」

しかし、著作権法30条の私的使用には権利性はない。また、著作権法30条は、家庭内での複製は零細であって処罰に値しない、という点に立法趣旨があったが、現在のデジタル化・ネットワーク化の環境下では、もはや当てはまらない。

「使用は個人の聖域ないし権利」はドグマにすぎない。

（2）アクセス権肯定論の主張

著作物の価値を利用する行為（「鑑賞行為」）は、本来、すべて著作権の対象とすべきである。



これまで、著作物へのアクセスを可能にする行為そのものは、既存の支分権から独立して著作権の対象とすべき独自性が存在しなかった。ところが、デジタル化・ネットワーク化の中では、アクセスを既存の支分権から独立して権利化すべき著作物の利用形態（独自性）が登場し、かつDRMによってこれを権利化することも実効的な状況（実効性）になってきた。

http://www.itlaw.jp/lait2.pdf