

コンテンツセキュリティ・ガイド

コンテンツビジネスを支える技術

日本ネットワークセキュリティ協会
コンテンツ・セキュリティ ワーキンググループ
2003 年 3 月作成

目次

はじめに	1 ページ
------	-------

[現状の把握]

1. コンテンツの不正蓄積と不正流通の流れ	2 ページ
2. コンテンツ不正蓄積と不正流通の実態	3 ページ

[問題と対策]

3. コンテンツ不正流通対策1 「DRM(デジタル著作権管理) システム」	4 ページ
4. コンテンツ不正流通対策2 「透かし技術と監視システム」	5 ページ
5. コンテンツ不正流通対策3 「リージョンコード管理システム」	6 ページ
6. コンテンツ不正流通対策4 「不正侵入検知・予防システム」	7 ページ

[今後の取り組み]

7. 今後のコンテンツ流通技術 「セキュリティ技術の組み合わせ」	8 ページ
----------------------------------	-------

はじめに

ブロードバンド回線の普及とともに、インターネット上でのコンテンツ流通が盛んに行われるようになってきた。インターネットの普及と利用の高度化に伴い、コンテンツビジネス全体に対する脅威も無視できない影響範囲で広がってきている。それがコンテンツの不正蓄積やコンテンツの不正流通だ。これらはコンテンツビジネスの根底に大いに影響を及ぼしつつある。

本ガイドでは、デジタル社会におけるコンテンツビジネスへのセキュリティ的影響範囲と取り組みに関してまとめたものである。

より良いコンテンツビジネスが成長する基盤としてインターネットを含むネットワークが多く活用され、安全・安心にすごせる社会形成を推進する意味でも本ガイド作成されている。

謝辞:

本ドキュメント作成にあたりレビューを頂いた多くの方にお礼申し上げます。

1. コンテンツの不正蓄積と不正流通のしくみ

コンテンツ流通に対する脅威には、コンテンツの不正蓄積と不正流通の二つの側面がある。

これら二つが複合した形でコンテンツ流通に対する脅威が増大している。

コンテンツの不正蓄積は、ウェブサーバーやストリーミングサーバーなどからデジタルコンテンツをデータとして蓄積する手法と、映画やビデオなど映像情報から MPEG エンコーディングなどを行いデータとして蓄積する手法がある。いずれの手法でも最終的にはデータとして蓄積されることになる。インターネット上のストリーミングに関して、一時期「データは蓄積されないでコンテンツは保護される」と世の中に認知されていたが、現在はストリーミングのデータであっても、その内容をデータとして蓄積できるツールが既に多数流通している点に注意が必要である。

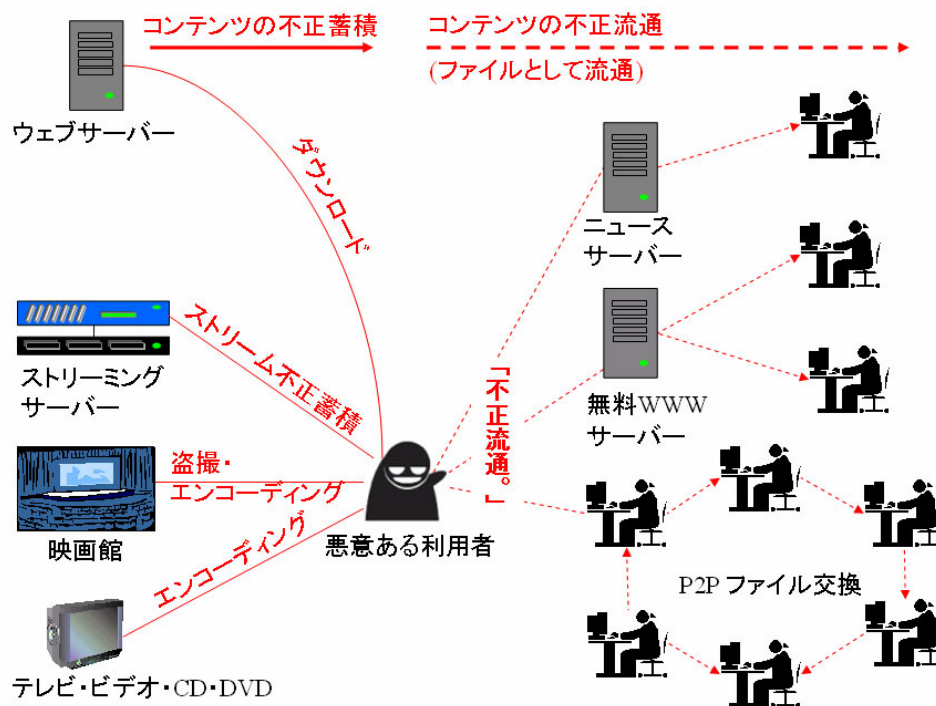


図 1.コンテンツの不正蓄積と不正流通経路

コンテンツ不正流通は、「悪意ある利用者」によってコンテンツの蓄積が行われ、データを二次流通先で共有する。二次流通先は、サーバー（ニュースサーバー、無料 WWW サーバー）や P2P ファイル交換ネットワークが用いられていることが多い。

現在多くの P2P ファイル交換ネットワーク上で、これら不正蓄積されたコンテンツの二次流通が行われていることが確認されている。

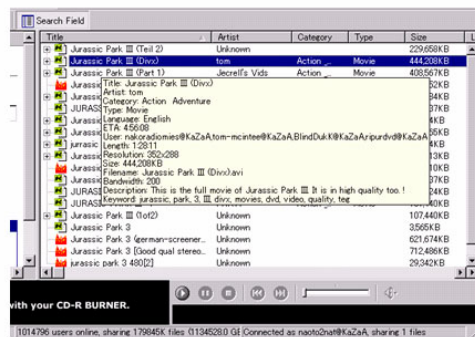
2. コンテンツ不正蓄積と不正流通の実態

コンテンツの不正蓄積と不正流通は、P2P ファイル交換ネットワークを中心に大きな波を作り出している。P2P のファイル共有量は年々増加傾向にあり、ひとつの P2P ファイル交換ネットワークでは 2002 年 12 月時点、ファイル共有データ総量が 2 ペタバイト(DVD 40 万枚相当)を超え、2003 年 3 月現在では 6 ペタバイト(DVD 120 万枚相当)にまで膨張している。

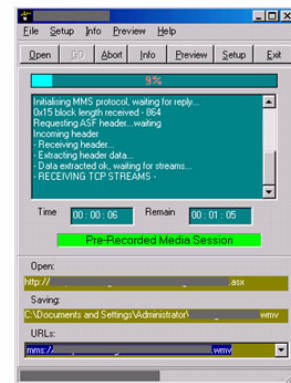
P2P ファイル交換ネットワークで共有される情報の中には、コンテンツを不正に蓄積したものが多く、映画館上映の映像やテレビ・ビデオの映像をエンコーディングしデータ化したもの、インターネット上のストリーミングサイトで流れるデータを不正に蓄積したがファイル共有されているのが目立ってきている。

P2Pで交換されているコンテンツ(例)

(映画) ハリーポッター 秘密の部屋 (日本語字幕).avi
 (映画) バンドオブブラザーズ 03 カンラン攻略 (日本語字幕).avi
 (映画) バンドオブブラザーズ Vol.08「捕虜を捉えよ」(日本語字幕)[58m56s 640x360 DivX5].avi
 (映画) マルホランド・ドライブ (日本語字幕)(2002.02.16) 850230074.avi
 (映画) リング RING 2002米 アメリカ版(SAMPLE版 日本語字幕 DivX).avi
 (映画)60セカンズ (日本語字幕).AVI
 (映画)スターウォーズ エピソードI ファントム・メナス(日本語字幕).mpg
 (映画)タイムマシン The Time Machine (2002米 日本語字幕 640x272).avi
 (映画)少林サッカー(日本語字幕).avi
 [ディズニー映画] ムーラン(日本語吹替版).avi
 [映画 2001] イルマーレ (日本語字幕).avi



P2Pソフトウェア例



ストリームダウンロード
ソフトウェア例

図 2. 実際に交換されていたコンテンツの一部

これら実態の全容は、膨大に広がる P2P ファイル交換ネットワークにより、すべてを把握できていないが、膨大な数であることは前述のファイル共有データ量から容易に想像がつくだろう。コンテンツ流通を取り巻く環境は、以前より指摘がされていたコンテンツのパイラシー行為(海賊行為)を大幅に上回る規模で悪化していつているのは事実である。また、P2P が生み出すトラフィックは、インターネット上で増加傾向にあり、通信事業者の回線設備を圧迫しはじめている点も指摘されて始めている。

3. コンテンツ不正流通対策1 「DRM(デジタル著作権管理) システム」

パイラシー行為に対処すべく、コンテンツ流通機能として DRM(Digital Rights Management: 著作権管理) システム(以下 DRM システム)を導入することが盛んになってきている。DRM システムは、コンテンツを暗号化(パッケージ化)し、利用者個別にライセンスを付与することによって権限管理を行うシステムである。これにより、コンテンツを仮に取得したとしても、ライセンス不一致のため視聴不可となる。

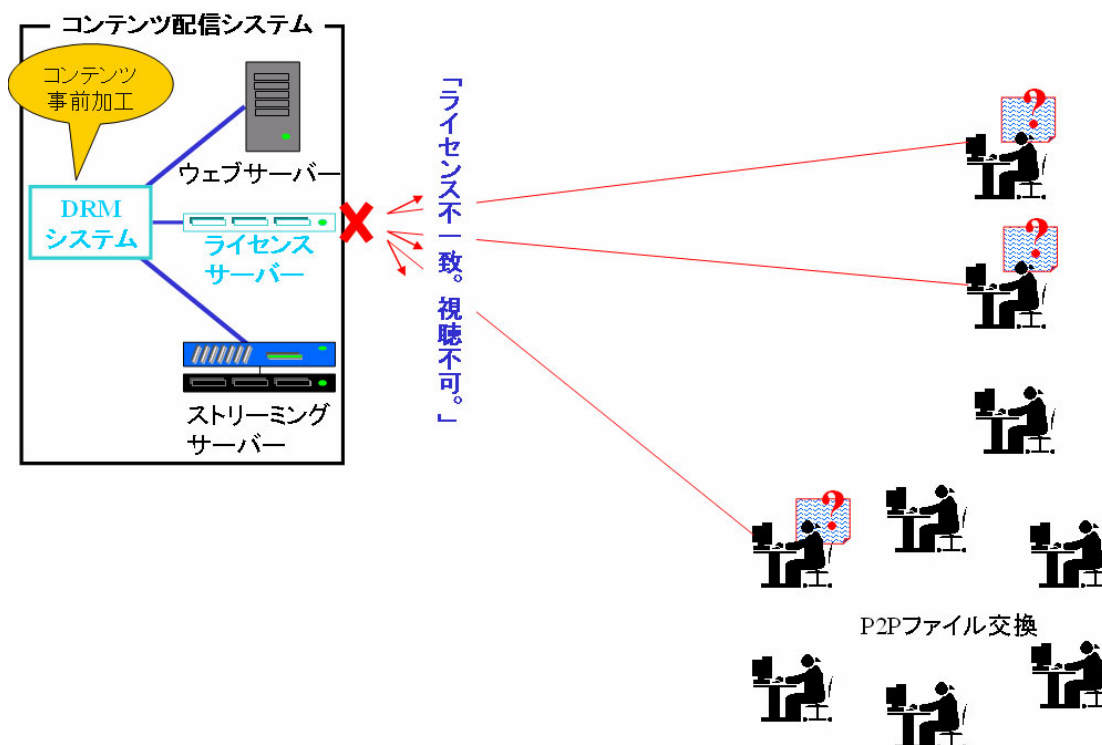


図 3. DRM(デジタル著作権管理) システムの例

DRM システムは、既存のコンテンツ配信システムと連携を図り実現される。主にコンテンツを事前に DRM 対応させ(パッケージ化という)、その情報をライセンスサーバーに登録しておく。利用者毎の個別ライセンスをライセンスサーバーに管理・登録する。利用者のコンテンツ購買行為により、ライセンスサーバー上には権限管理された個別のライセンス情報が蓄積される。このコンテンツのパッケージ化とライセンス管理により、コンテンツ配信の仕組みはそのままに、コンテンツ自身のセキュリティを向上させることができる。

最近のコンテンツ流通ビジネスでは、この DRM 技術導入が進んできている。

4. コンテンツ不正流通対策2 「透かし技術と監視システム」

パイラシー行為の情報掌握手段として、透かし技術と監視システムがある。これはコンテンツ自身へ事前に透かしを刷り込み、不正流通したコンテンツを透かしから判断する。透かし技術は人間の目に見える形ではないため、コンテンツの視聴者にはそれを知覚することは、ほぼ不可能である。

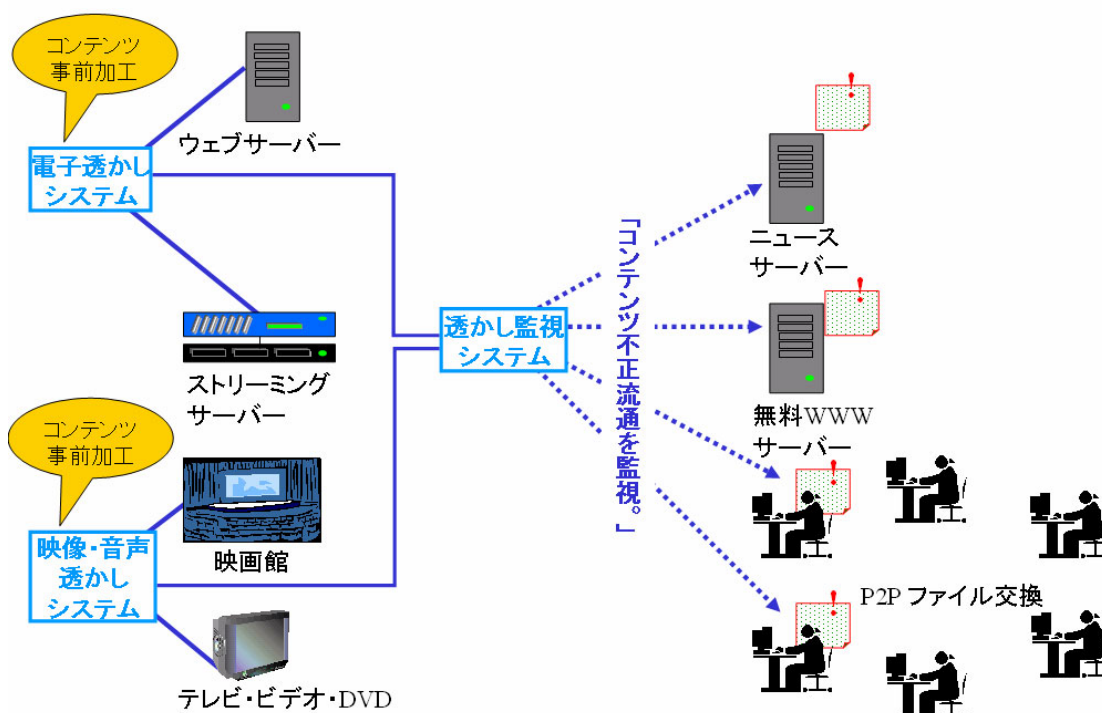


図 4. 透かし技術と監視システム

透かし技術は、デジタルデータにも、アナログデータにも刷り込むことができ、刷り込まれたコンテンツの個別情報(例えば ID)を読み解くことが出来る。

この利用により、「いつ」「どこで」「だれが」「どのように」流通したコンテンツであるかを流通するコンテンツ各個から判断できる。

前述の DRM システムのようなコンテンツ保護の積極的な抑止効果は低い、コンテンツ不正流通の実態掌握と指摘・使用禁止命令等の根拠としては非常有効である。

昨今これら透かし技術を取り入れた著作権管理体制が各組織・各団体により推進が行われている。

5. コンテンツ不正流通対策3 「リージョンコード管理システム」

コンテンツ流通には、コンテンツが持つ権利と権限委譲の関係が色濃く反映される。映画などの配信権がそれにあたる。多くの場合、北米、アジア太平洋、欧州のように各区分けがされたうえで、個別地域での配信権が売買される。これをインターネット上でも反映するシステムが求められている。しかし、インターネット上で確固たる地域識別に利用可能であろう情報は IP アドレスブロックのリスト程度でしかない。しかし IP アドレスブロックの割り当ては、地域とはまったく無関係に配布されている現状は、把握しなくてはならない事実である。

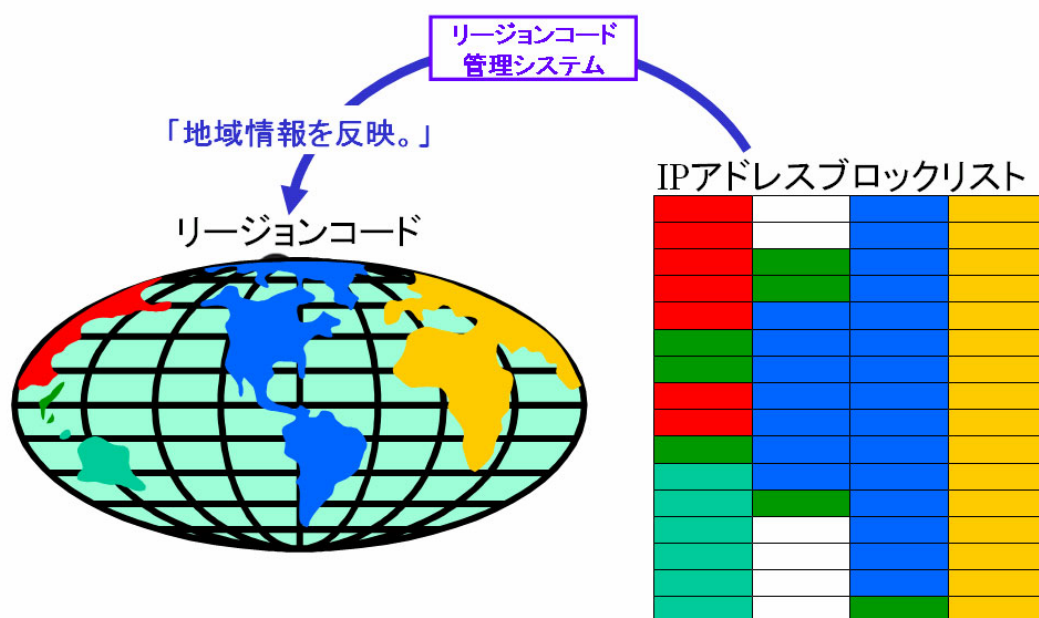


図 5. リージョンコード管理システムの例

そのためインターネット上では、ビデオや DVD などで行われるリージョンコードのように、すぐさま識別できない。このため、インターネット上でリージョンコードに該当するような仕組みを実現することが求められている。リージョンコード管理システムでは、各国各組織に割り当てられた個別の IP アドレスブロックと所有者、想定される利用地域を組み合わせ、地域を特定する情報の基礎とする仕組みだ。これにより、配信権にかかわる権利処理などをよりスムーズに行うことができるだろう。

これらコンテンツ流通ビジネスを支える技術も日本国内において、推進が行われつつある。

6. コンテンツ不正流通対策4 「不正侵入検知・予防システム」

コンテンツ流通を根底から揺るがす懸念も存在している。それはコンテンツ配信システムや DRM システムすべてを標的としたサービス妨害(DoS: Denial of Service Attack)だ。悪意ある利用者が、インターネット上を通じコンテンツ配信システムを停止・乗っ取るといった可能性は常にある。これら行為は通常のコンテンツ流通上の売買行動に紛れて行われる場合が多く、コンテンツ配信システム単体では、すべてを防ぐことは難しい。

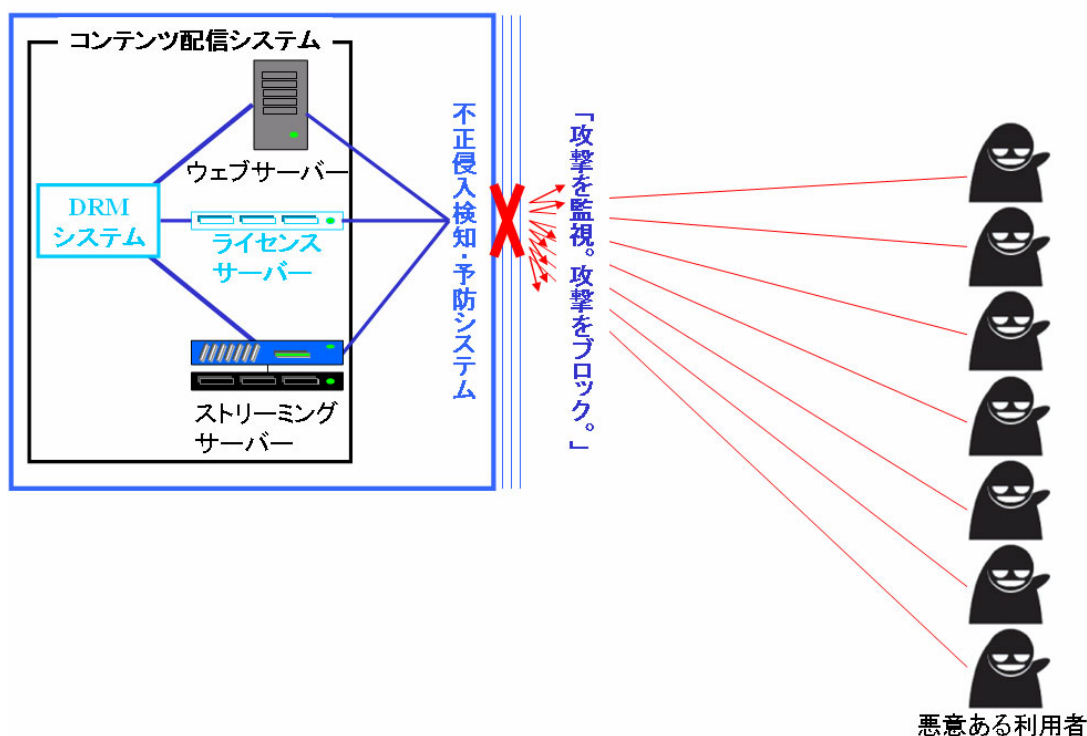


図 6. 不正侵入検知・予防システムの例

これら悪意ある利用者と、その行為を検知し予防するシステムが重要となる。不正侵入検知・予防システムは、IDS (Intrusion Detection System) または IPS (Intrusion Prevention System) と呼ばれ、ネットワークの悪意ある利用者の動向を検知・予防する仕組みとして注目が集まっている。

システムに対する悪意ある利用者からの攻撃は、上記システムに対するものだけでなく、コンテンツ自身への攻撃も可能性がある。前述の DRM システムで暗号化されたコンテンツもシステムの脆弱性を用いて、不正利用する試みもすでに存在している。コンテンツ流通ビジネスでは、常にこれらシステムと悪意ある利用者との間でのイタチゴッコが続くことになる。

7. 今後のコンテンツ流通技術「セキュリティ技術の組み合わせ」

コンテンツセキュリティを考えると、コンテンツの保護、監視、配信をバランス機能させることが重要である。セキュリティ技術を取り込んだシステムを組み合わせにより、円滑なコンテンツ流通が実現される。「悪意ある利用者を検知・予防」し、「コンテンツ流通上の権利処理をカバー」した上で「最適なコンテンツ配信を行う」、その上でさらに「不正流通があればそれを監視する」というようにだ。

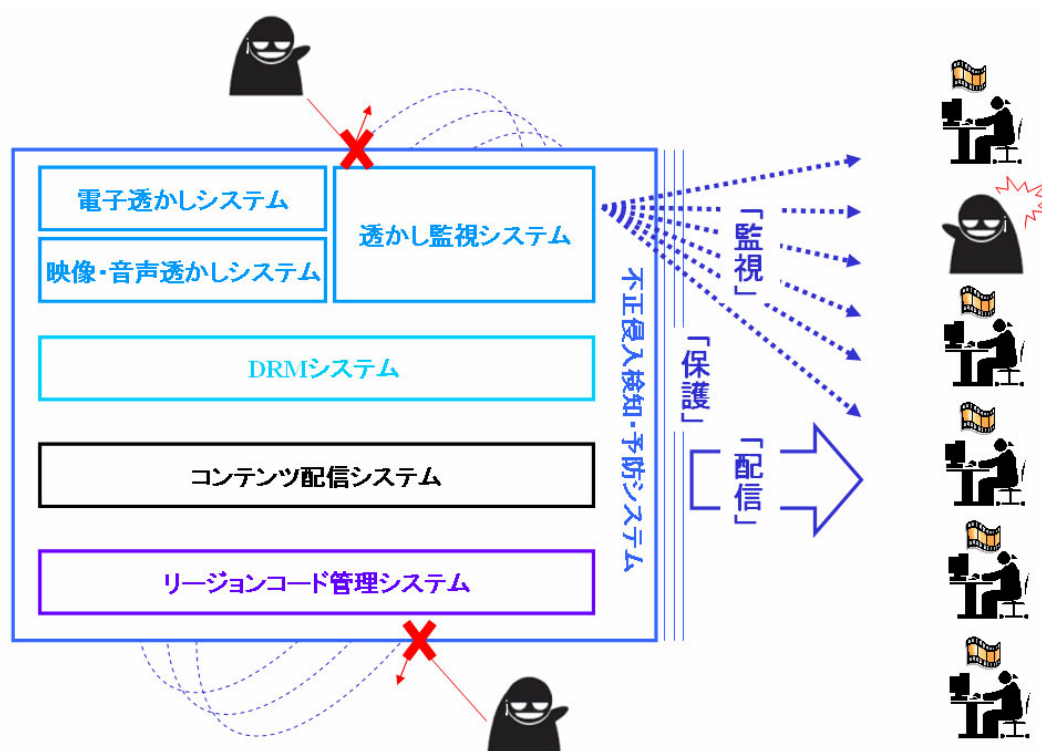


図 7. コンテンツ流通 万全の体制

コンテンツセキュリティ技術は、日進月歩の状況にある。インターネット技術の成長同様に、日々のシステム改善と対策、運用が今後も重要な命題となっていく。コンテンツビジネスを考える上で、これら技術動向を注意深く確認し、取り組んでいくことが望まれている。

以上

2003 年 3 月 / 日本ネットワークセキュリティ協会 コンテンツセキュリティ ワーキンググループ