Vol.2018-AVM-103 No.14
2018/11/30

[招待講演] 放送・コンテンツ配信・放送通信連携におけるセキュリティ

小川　一人†

† 日本放送協会　〒157–8510 東京都世田谷区砧 1–10–11
E-mail: †ogawa.k-cm@nhk.or.jp

あらまし　デジタル放送の普及，インターネットのブロードバンド化，モバイル端末，タブレット PC，スマートフォンの高性能化，普及に伴い，デジタル音声，デジタル映像等のデジタルコンテンツを取り巻く環境は著しく変化している．これらの環境に合わせて種々のセキュリティ技術が必要となっている．ここでは，放送・コンテンツ配信・放送通信連携サービスに関わるセキュリティ技術を紹介する．

キーワード　放送，コンテンツ配信，放送通信連携，セキュリティ

[Invited Talk] Security Technologies for Broadcasting, Content Distribution, and Integrated Broadcast-Broadband Services

Kazuto OGAWA†

† Japan Broadcasting Corporation　1–10–11 Kinuta, Setagaya-ku, Tokyo, 157–8510 Japan
E-mail: †ogawa.k-cm@nhk.or.jp

Abstract　Distribution environment for audio and video content has changed dramatically, such as digital broadcasting service is widespread, the bandwidth available in the Internet access has been increasing, mobile terminals, tablet PCs and smart phones have been growing rapidly. According to this trend, variety of security technologies is required. I introduce some technologies used in broadcasting services, content distribution services over the network, and integrated broadcast-broadband services.

Key words　Broadcasting, Content distribution, Integrated broadcast-broadband services, Security technologies

1. はじめに

2000 年にデジタル放送が開始され，2011 年のアナログ停波により全放送がデジタル化された．さらに，2018 年 12 月 1 日には 4K8K スーパーハイビジョン放送が開始される．また，インターネットのブロードバンド化，メモリデバイスの低価格，高密度化，パーソナルコンピュータ（PC），携帯端末の普及に伴い，デジタル音声，デジタル映像等のデジタルコンテンツを取り巻く環境は著しく変化している．

環境の変化に伴い，放送サービスの形態が多様化し，各種のセキュリティ技術が必要となっている．本稿では，放送・コンテンツ配信，さらには，放送通信連携に関するリスクと対策技術の一部を紹介する．

2. 放送サービス用セキュリティ技術

本章では，放送用のセキュリティ技術，限定受信方式 (CAS) [1], [2] を紹介する．

今年の 12 月に開始される 4K8K 放送と既存のデジタル放送の CAS の基本構造は同じである．但し，4K8K 放送では使用する暗号方式が Multi2 [3] から AES [4] になったこと，新たな多重化方式 MMT に対応する変更があること，セキュリティ用のモジュールがカードではなく IC チップになること等が既存のデジタル放送とは異なる．以下では，4K8K 放送に焦点を当てて紹介する．

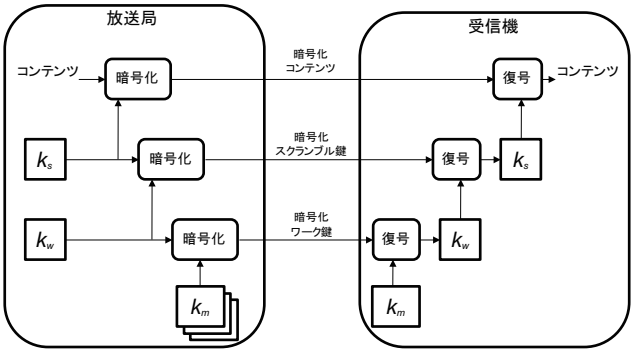

図 1　放送システム

図 1 に電波産業会で規格化された [2] デジタル放送のコンテンツ保護のための CAS のブロック図を示す．このシステム

は，放送されるコンテンツを視聴（Access）できる利用者を条件により（Conditional）制限することができる，という意味で Conditional Access System（CAS）と名付けられている．

CAS では，図 1 に示された 3 つの暗号化（復号）のブロックで暗号技術が使用される．例えば，コンテンツ（番組）は共通鍵暗号アルゴリズム AES(デジタル放送では Multi2) で暗号化 (復号) される．暗号化の鍵にはスクランブル鍵 k_s が使用される．すなわち，k_s を知ることができる受信機のみがコンテンツを視聴・利用できる．

k_s は番組属性情報等と合成された Entitlement Control Message (ECM) と呼ばれる情報として受信機に送られる．この際，k_s はワーク鍵 k_w を暗号化鍵として暗号化される．すなわち，k_w を保存している受信機のみが k_s を復号できる．k_w は放送事業者と視聴者の間の契約情報とともに合成され，Entitlement Management Message (EMM) と呼ばれる情報を生成し，CAS 用 IC 固有のマスター鍵 k_m を用いて暗号化され，CAS 用 IC に送られる．コンテンツを視聴するためには，これらの 3 つの鍵 k_m，k_w，k_s が正しく使用されることが必要である．

なお，4K8K 放送用の規格では，CAS の安全性確保のため，CAS を更新することも考慮している．

有料放送では，視聴者と放送事業者間で契約が成立した場合，新しい契約情報と k_w が EMM として送られ，CAS 用 IC に保存される．そして，保存された契約情報によって，CAS 用 IC からの k_s 出力が制御される．すなわち，番組の復号が制御され，視聴制御が可能になる．放送区域の制御も同様な方法で行われ，地域毎に k_w を使い分けることで，放送区域の制御が可能になる．

なお，EMM や ECM には改ざん検出部が含まれており，コンテンツの発信元の正当性を確認できる．

3. コンテンツ配信用セキュリティ技術

ネットワークを用いたコンテンツ配信の大きな特徴に双方向性がある．結果として，危惧しなければならないリスクはサーバにもクライアントにも存在する．すなわち，ネットワークを用いたサービス全般と同じリスクがある．そこで本章ではネットワークを用いたサービスにおいて考えなければならないリスクと対策を紹介する．

3.1 ネットワークセキュリティ

ネットワークセキュリティの中から利用者を悪意あるサイトへ導く Drive-by Download 攻撃，ネット上の経路情報を変更する経路ハイジャック攻撃とその対策を紹介する．

3.1.1 Drive-by Download 攻撃とその対策

Drive-by Download 攻撃とは，攻撃者がある Web サイトを改ざんし，その Web サイトを訪れた利用者を攻撃者が管理するサイトに誘導（リダイレクト）する攻撃である．具体的には，後述するインジェクション攻撃等の攻撃を使って，攻撃者がある Web サイトに侵入し，その内容を改ざんする．多くの Web サイトでは，利用者の入り口になるサイトがあり，そこから別のサイトにリダイレクトする仕組みになっている．そのリダイレクト先を攻撃者の管理する Web サイトに設定（改ざん）する．利用者の画面上は全く変更されず，行先だけが変更されるので，注意していなければ攻撃に気づくことはない．また，悪質なサイトであることを隠すために，表面的には正規のサイトと同じような動作を行うように設定されている．そして，Web サイトを訪れた利用者の端末にマルウェアをダウンロードし，インストールさせる．

具体的には，Exploit Kit [5] と呼ばれる攻撃プログラムが使用され [6]〜[8]，Flash player, Explorer, Silverlight 等の脆弱性を利用するとともに，JavaScript を難読化して通常の動作と見分けがつかないだけでなく，悪質サイトの場所が一読ではわからなくなっている．

脆弱性をなくすためにアプリケーション，ブラウザ等を逐次更新することは利用者が可能な対策である．Microsoft や Google では検知した悪質サイトの URL ブラックリストを作っている [9], [10]．さらに，悪質サイトを検知する研究も盛んである [11], [12]．

3.1.2 経路ハイジャック攻撃とその対策

インターネット上のパケットは宛先情報に基づいて正確に宛先に届けられなければならない．しかし，設定ミスが生じ経路が誤ることがある．例えば，1997 年には AS7007 として知られるルータの設定ミス [13] によるパケットの大量誤送信，2008 年には動画サイト Youtube へのアクセスの遮断 [15]，2015 年にはインドでの設定ミスが経路ハイジャックへとつながり全世界に影響を与えた事件 [16] 等が報告されている．

オペレータの人為ミスは悪意ある攻撃とは区別するため Mis-Origin と呼ばれることもあるが，Mis-Origin を 0 にすることはかなり困難である．この対策として最も効果があると期待されるのが Origin Validation(OV) である．設定直後にそのアドレスの Validation チェックするものである．IETF の Secure Inter-Domain Routing WG が標準化を進めている [17]．OV は自動化しなければならず，自動で Origin を参照する仕組みが必要である．IETF では Origin にデジタル署名をつける仕組みと，デジタル署名を検証するための仕組みを作り自動化を図った．この実際の効果について，現在検証中である．

3.2 Web セキュリティ

Web サーバに関わるリスクとして，インジェクション攻撃とアドフラウドを紹介する．

3.2.1 インジェクション攻撃

VoD 等のサービスでは，最初に利用者がサーバにアクセスする．そして，利用者が所望するコンテンツをサーバに知らせ，サーバからコンテンツが送られてくる．そのサーバへの攻撃の一つがインジェクション攻撃である．

図 2 にインジェクション攻撃の例を示す．これは Web サイトからパスワードの入力を求められた際のイブによる攻撃を示している．i) は，Web 内部で書かれているプログラムである．入力された“id”と“password”がパスワードデータベースのいずれかのデータと一致する，すなわちデータベース内にこの id と password にマッチする行が 0 行でなければ“accept”し，一致しなければ“reject”する．ii) に示すように，利用者が普通に id と password を入力する場合は通常の処理が行われる．

```
i) Web アプリケーション内の記述
 sql=“select count (*) from users”
   +“where id = ‘”+request[“id”]+”’
    and password = ‘”+request[“password”]+” ’ ”;
 count=execute(sql);
 if(count==0){
  rejcet
 }else{
  accept
 }
ii) 通常のアリスからの入力
 id = alice
 password = zorxu
iii) 攻撃者イブからのリクエスト
 id=alice
 password = ’or‘a’=‘a
```

図 2　インジェクション攻撃

これに対し，攻撃者が iii) のような入力をすると，accept の条件が「パスワードが一致する，もしくは，a=a」となり，いかなるパスワードが入力されても accept される．この対策としては，password の入力に「’」や「=」を受け付けないプログラムにする必要がある．

インジェクション攻撃に類するものは SQL インジェクション，OS インジェクション，クロスサイトスクリプティング，HTTP ヘッダ・インジェクション等多数あり，完全な防御技術はない．このため，現在でも多くのインジェクション攻撃が存在している．これらの攻撃に対しては，Web プログラム毎に適切に対処しなければならない．

3.2.2　アドフラウド

Web コンテンツの閲覧数はカウントできる．この機能を利用し，閲覧数に応じて広告主が Web サイト管理者に代金を支払うモデルがある．このモデルを不正に利用し，広告主に実際の閲覧数よりも多くの閲覧数の代金を請求する詐欺行為がアドフラウドである [14]．

アドフラウドでは，利用者が Web サイトを閲覧する際に，利用者にはわからないようにバックグランドで他のサイトを閲覧する仕組みが組み込まれている．バックグランドであるため，利用者が指定していない他のサイトにアクセスしていることに気づくことは困難である．Web サイトの閲覧はフォアグランドであろうとバックグランドであろうとカウントされる．すなわち，利用者が実際には閲覧していないにも関わらずカウント数がプラスされ，結果として広告主は不要な代金を支払わされる．

広告を掲載している Web サイトの管理事業者が対策に乗り出しているが，リンク先の多いサイトでは全てをチェックすることは困難であるとともに，手口の巧妙化があり，完全な対策は困難となっている．

3.3　マルウェア

PC 等をターゲットにした攻撃も多く存在する．ウイルス，ワーム等のマルウェアがこれである．ウイルスは他のファイル・プログラムにくっついて（寄生して）感染し，寄生したプログラムが動作すると同時に有害な処理を始める．例えば，メールに添付されたファイルを開くことで感染したり，悪意ある URL にアクセスすることで感染する場合がある．これに対し，ファイル・プログラムを介さずに拡散するマルウェアがワームである．Code Red，Nimda，トロイの木馬，WannaCry 等が有名である．ここでは，最近猛威を振るった Microsoft Windows に対するワームである WannaCry の概要を紹介する．

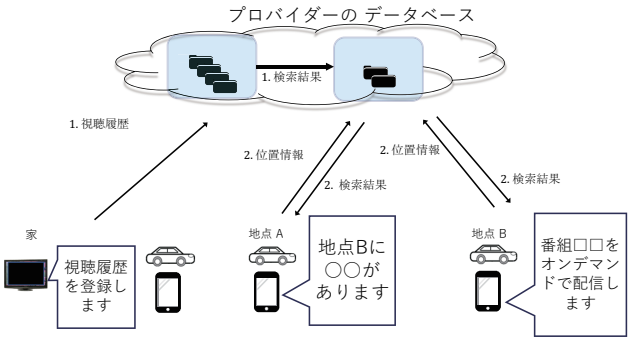

図 3　自動車・携帯端末・テレビ連携サービス

WannaCry は PC 内のファイルを暗号化し，所有者に読めなくした上で，その復号のための金銭を要求するメッセージを表示する．WannaCry の感染源は不明であるが，その活動内容は多く報告されている．基本活動を大雑把に述べると，感染拡大と攻撃の 2 つに分けられる．

感染拡大： Port445/TCP が開いている PC を探し，Port445 が開いている PC に対し，ファイル共有プロトコルである SMB 通信を利用して悪意あるパケットを送付し，不正な DLL を埋め込む．
攻撃： DLL は，コマンド＆コントロール（C&C）サーバに接続し，端末内のファイルを暗号化する．壁紙にメッセージ “Ooops, your important files are encrypted.” を出し，復号のための代金を要求する．

感染拡大はプローブと呼ばれる操作で，脆弱性のある部分 [18] を検査する．攻撃では不正な DLL により PC が乗っ取られ，種々の被害が生じる．C&C サーバとの接続は匿名通信が使われ，C&C サーバの特定を困難にしている．

WannaCry では暗号化と壁紙の書き換えが行われたが，DLL によりどのような処理も実行できる．このような DLL を受け取る脆弱性をなくすことが根本的な解決策である．Microsoft ではパッチ [18] を出し対策している．

4.　放送通信連携サービスセキュリティ

放送通信連携サービスに関連するセキュリティ技術の研究を紹介する．

4.1　自動車・携帯端末・テレビ連携サービス

放送通信連携サービスの 1 つとして，ユーザの視聴した放送番組の視聴履歴に基づいて，ユーザの嗜好に合わせたお勧め番組等をレコメンドするサービスがある．さらに，通信機器とし

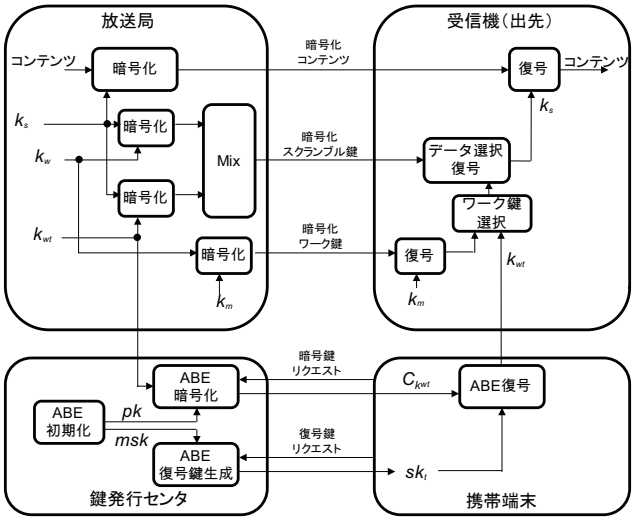

図 4　放送用秘密鍵持ち出しシステム

てスマートフォン等を所有して移動可能な環境でユーザの位置に応じたサービスが考えられている．このサービスの重要な課題の一つが，視聴履歴等の個人情報の保護である．そこで，個人情報を保護しつつ，利用者の居場所に合ったレコメンドサービスを享受できるセキュアなシステムが提案された [19]（図 3 参照）．

システムでは，データを暗号化したままでキーワードによる検索を可能とする属性ベース検索可能暗号や，検索結果を検証可能な属性ベース検索可能暗号が応用され，視聴者の視聴履歴や位置情報等の個人情報を保護したままでデータを効率的に利用することが可能である．

4.2　放送用秘密鍵の持ち出し

放送サービスにおいて，自宅で契約しているチャネルを自宅外で視聴する場合，セキュリティモジュールを持ち歩かなければならない．ただし，既存のデジタル放送であっても受信機やレコーダの構造上，CAS カードの着脱は容易ではない．さらに，4K8K 放送ではカードではなく，IC チップによるセキュリティ機能の実装が図られている．そこで，セキュリティモジュールを持ち出すことなく，電子データとしてテンポラルな鍵を携帯端末に入れて自宅外の受信機でサービスを享受する方法が必要である．文献 [20] では，利用者の属性に応じて復号の制御を可能とする属性ベース暗号を利用したシステムが提案された．システムでは，データの使用制限のために，サービスを享受する場所と日時を属性として指定し，復号制御に利用できる．

図 4 にこのシステムを示す．従来の放送システムに鍵発行センタと携帯端末を追加して組み合わせた．鍵発行センタ内で一時的なワーク鍵 k_{w_t} を属性ベース暗号 (ABE) で暗号化するが，k_{w_t} を利用する位置と時間情報を属性として用いている．暗号化された k_{w_t} を復号するための復号鍵は，現地で通信を通じて受け取る仕組みである．

5. おわりに

放送・コンテンツ配信・放送通信連携におけるセキュリティ技術の最終目的は，不正なコンテンツ利用がなく多くのコンテンツが自由に流通でき，アプリが正しく運用されることである．どちらかと言えば攻撃された後に防御策を考えるセキュリティ技術開発になっているが，これらを一対で研究し，よりよいセキュリティ技術を開発し，コンテンツ・アプリを自由に楽しむ環境を一日でも早く実現したい．

文　献

[1] 電波産業界，「デジタル放送におけるアクセス制御方式」，ARIB STD B-25.
[2] 電波産業界，「デジタル放送におけるアクセス制御方式（第 2 世代）及び CAS プログラムのダウンロード方式」，ARIB STD B-61.
[3] 宝木，佐々木，「マルチメディア向け高速暗号アルゴリズム Hisecurity-Multi2 の開発と利用方法」，WCIS89-D2，1989.
[4] NIST, “Annoucing the ADVANCED ENCRYPTION STANDARD (AES),” FIPS-197, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.
[5] V. Kotov, F. Massacci, “Anatomy of Exploit Kits,” International Symposium on Engineering Secure Software and Systems，2013.
[6] TREND Micro,「エクスプロイトキットとは」，https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/202/exploit-kit
[7] IIJ,「Security Diary - rig Exploit Kit 観測数の拡大に関する注意喚起」，https://sect.iij.ad.jp/d/2016/10/178746.html
[8] Symantec, “Web Attack: Angler Exploit Kit Website,” https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=26992
[9] Microsoft,「SmartScreen フィルター機能」，https://support.microsoft.com/ja-jp/help/17443/windowsinternet-explorer-smartscreen-filter-faq
[10] Google, “Google Safe Browsing,” https://developers.google.com/safe-browsing/’
[11] 笠間，神薗，井上，「Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案」，コンピュータセキュリティシンポジウム（CSS）2013.
[12] F. Howard, “Exploring the Blackhole Exploit kit - Naked Security,” https://nakedsecurity.sophos.com/exploring-the-blackhole-exploitkit/
[13] NANOG, “7007 Explanation and Apology,” https://seclists.org/nanog/1997/Apr/444
[14] NHK クローズアップ現代，「追跡！ネット広告の“闇”」，2018.09.04，NHK 総合.
[15] B. Martin A., “Pakistan hijacks youtube,” Renesys Blog, Feb (2008).
[16] A. Toonk, “Large scale BGP hijack out of India,” http://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/
[17] IETF Secure Inter-Domain Routing WG, “Secure Inter-Domain Routing,” http://datatracker.ietf.org/wg/sidr/charter/
[18] Microsorf,「マイクロソフト　セキュリティ情報 MS17-010」, 2017, https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx
[19] 梶田，小川，大竹，「属性ベース検索可能暗号の移動体向け放送通信連携サービスへの応用」，SCIS2018, 4A2-1, 2018.
[20] K. Ogawa, S. Tamura, and G. Hanaoka, “Key Management for Versatile Pay-TV Services,” Security and Trust Management (STM) 2017, LNCS 10547, Springer-Verlag, pp.3-18, 2017.