

**コネクテッドテレビ
(インターネット接続テレビ)
の最新動向
～CES2011報告～**

CES : Consumer Electronics Show

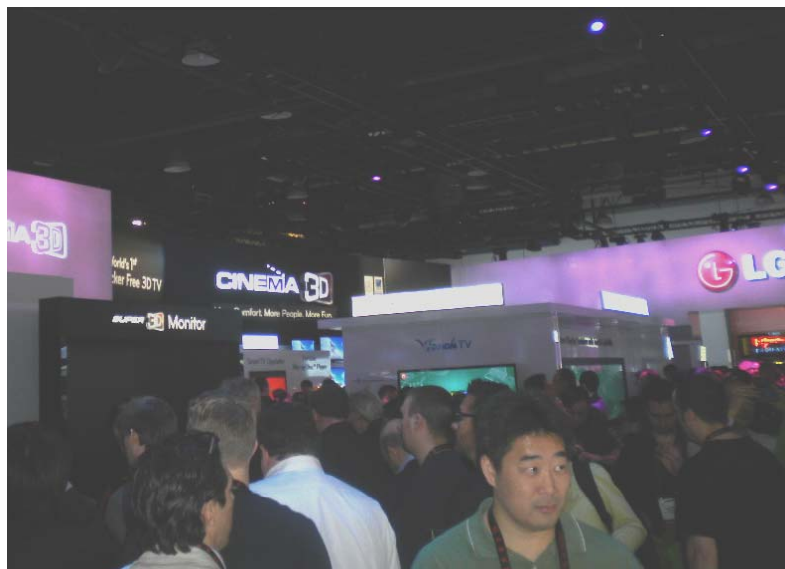
独立行政法人情報処理推進機構 (IPA)
セキュリティセンター
情報セキュリティ技術ラボラトリー長 小林 偉昭
2011. 2. 24

CES2011概要



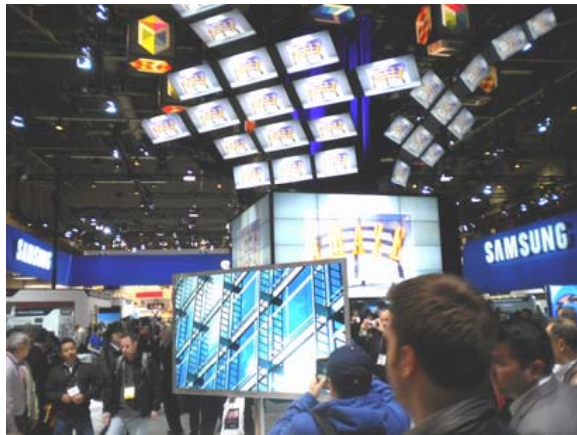
CES : Consumer Electronics Show

1967年に初回が開催され、毎年米国ネバダ州ラスベガス市で開催されている。全米家電協会CEA: The Consumer Electronics Associationが主催し、130カ国以上から12万人以上の参加者が見込まれている。2,500以上の出展社が20,000件以上の新製品を展示するCESは、消費者エレクトロニクス業界にとっての世界最大規模の国際会議及び展示会。



インターネットにつながるテレビと自動車 IPA®

3Dに加えて、コネクテッドTV(インターネットテレビ)



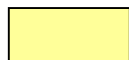
インターネットに繋がる自動車は、ホットスポットへ



2010グローバルTVブランド トップ20 IPA®

日本と韓国ブランドがグローバルTV産業で継続強い 出典: CE Magazine at CES

順位	ブランド名	順位	ブランド名
1	SAMSUNG	11	VIZIO
2	LG	12	KONKA
3	SONY	13	CHANGHONG
4	PANASONIC	14	HITACHI
5	HISENSE	15	SANYO
6	TCL	16	HAIER
7	SHARP	17	JVC
8	PHILIPS	18	FUNAI
9	TOSHIBA	19	LOEWE
10	SKYWORTH	20	METZ



:コネクティドTV出展社

テレビの映像をどこでもいつでも



テレビに加え、スマートフォン、タブレットが主流になるか



テレビでインターネットの映像を楽しむ



Built in Wi-Fiで、簡単にYouTube他の利用

出典パネルから: YouTube, Netflix, HuluPlus, Amazon on Demand, Sony's Qriocity, Gameloft, Napstar, MLB, NBA, NHL, Facebook, CinemaNow, Vuda, Alphaline



Web-ready TV 視聴映像例



出典:VISION January/February 2011

	Amazon	Blockbuster	Cinema Now	Netflix	Pandora	Vudu	YouTube
LG			○	○	○	○	○
PANASONIC	○			○	○		○
SAMSUNG		○	○	○	○		○
SHARP				○	○	○	○
SONY				○	○		○
TOSHIBA	○			○	○	○	
VIZIO		○	○	○	○	○	○

コネクテッドTVでSkypeビデオ対話



Skype Videoコーリング機構：電話機能だけでなくビデオでの対話機能
インターネット電話サービスからビデオコーリングマーケットへ。



Skype内臓TV

Sony, Panasonic,
Samsung

出典：USA TODAY 2011.1.7

国際通信トラフィックでの使用増加。2008年8%、2009年13%、2010年25%に増加。
13.2M人が年内にビデオコーリングを使用想定。2015年に155.1M人使用。軍の家族
や国際人が利用。
家庭(リビング)からモバイル環境での利用へ。2015年にモバイルでのビデオコーリン
グは1B\$へ。Apple iPhone, iPad, iPodTouch用の双方向のビデオコーリングアプリ。

Internet-connected TVのマーケット



出典: VISION誌 TV gets Connected

世界市場:

DisplaySearch社

2014年に118M台以上のConnected TVが売られる予想

iSuppli社

2014年に野心的だが148M台以上

Parks Associates社

2015年で185M台

米国市場:

Forrester Research社

2015年までに43Mの家庭の少なくとも1台が
connected TVとなる

CEA予測

2014年に28.2M台が売られる

①Verizon社Seidenberg CEO基調講演 : 4G LTE (Long Term Evolution)

- ・4G LTEベースのセルラーブロードバンドの実現。3G対応を2月出荷し、年内4Gへアップグレード。
- ・「技術革新(Innovation)サイクルをスピードアップ」、「テレビの第2の黄金時代」を強調し、テレビの映像がPC、タブレット、スマートフォンへオンデマンドで利用可能となる。「TV Everywhere」
- ・モトローラ社のタブレットXoom(Android3.0)は、TV映像をアクセスする方法の一つになる。
- ・4GネットワークでのSkype to Skypeビデオコーリングの推進。

②CEA Shapiro会長 : Innovation

出典:2011International CES DAILY 2011.1.6/7/8

- ・技術革新(Innovation)が、米国経済を立て直す最善の戦略だ。
 - ・Connected TVと高速無線ブロードバンドサービスがそのキー。
 - ・2014年までにインターネット接続のCE製品(消費者向け電子機器)が70%以上になる。
- CE売り上げは、2011年には3.5%増の186B\$となる。

③携帯(Cell phone)マーケット動向 :

ComScore Inc.による調査(2010.8)

出典:THE WALL STREET JOURNAL 2011.1.6

- ・BlackBerry(Research In Motion Ltd.) 35.5%(37.6%からダウン)
- ・Android Smart Phone(Google) 26%
- ・iOS iPhone(Apple) 25%
- Androidはマルチプラットフォーム、iOSはシングルプラットフォーム。今後は？

「情報家電におけるセキュリティ対策 検討報告書」



http://www.ipa.go.jp/security/fy22/reports/electronic/index.html

デジタルテレビに対するセキュリティ対策検討ガイド : 2011年2月1日公開

商品化が先行しているデジタルテレビを対象に、「セキュリティ基準」策定のベースとなる対策検討ガイドを提示。

デジタルテレビにおけるネットワーク接続を含む情報利用機能(7機能)、それらの機能の利用で想定されるセキュリティ上の脅威(16脅威)、脅威群に対するセキュリティ対策(15対策)を明確化し、全体の相関関係(マトリックス)の一覧と解説をまとめている。

＜活用方法＞

デジタルテレビ製品の企画・設計時において、家電メーカーがどのようなセキュリティ対策機能を実装する必要があるかを検討するテンプレートとして、また、既存製品において、どのようなセキュリティ対策が実装されているかのチェックリストとして、利用することが可能です。

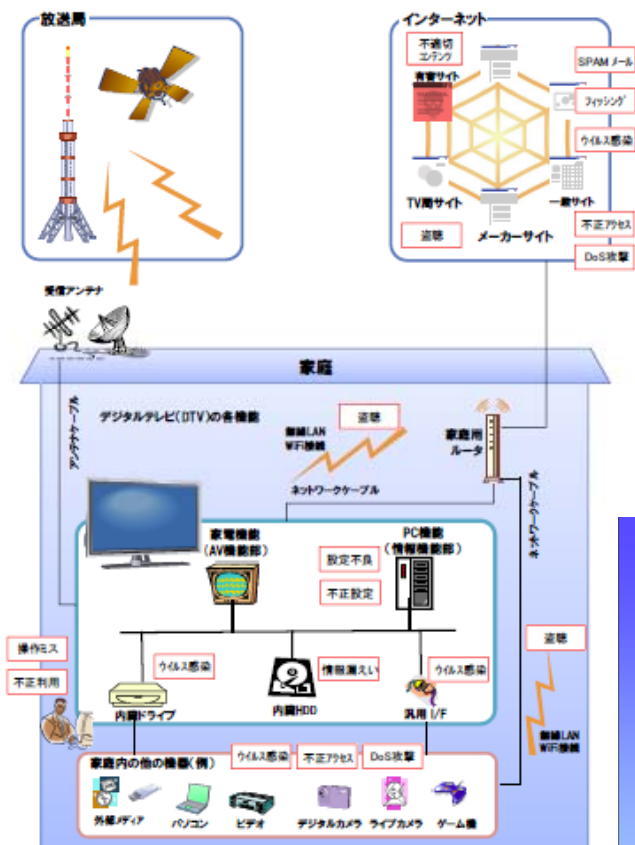


表2. デジタルテレビの機能レベルに応じた脅威/対策一覧

○ 対策として有効、△ 対策として一部有効、(空欄) 該当脅威の対策でない

機能	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	脅威	対策	
10	取扱い説明書																						
14	フィルタリング																						
10	URL 向け																						
12	データ消去ツール																						
11	コンテンツ暗号化																						
10	サーバ(接続先)																						
9	ユーザ(対サービス)																						
8	認証																						
7	ソフトウェア																						
6	機器																						
5	通信暗号化 (VPN含む)																						
4	IDS/IPS																						
3	アンチウイルス																						
2	ファイアウォール																						
1	脆弱性(セキュリティ)対策																						
対策	脅威	媒体	ユーザ操作	操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作	ユーザ操作
	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威
機能	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威
	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威	脅威
A1	外部																						
A2	内部																						
B	基本機能																						
C1	LAN																						
D1	インターネット																						
D2	接続																						

○ 発生する可能性が高い、△ 発生する可能性がある、(空欄) 発生可能性はない

組み込みシステムのセキュリティへの取組みガイド

http://www.ipa.go.jp/security/fy22/reports/emb_app2010/



16の具体的なチェック項目と4つのレベル

- 「マネジメント」、「企画」、「開発」、「運用」、「廃棄」の**全てのフェーズ**を網羅
- 各フェーズからセキュリティのために重要な計**16項目**を選定し、項目ごとに**4つのレベル**を策定。

組み込みシステムの セキュリティへの取組み ガイド(2010年度改訂版)

16個の具体的なチェック項目により、
自組織のセキュリティレベルを明確にする



Approaches for Embedded System Information Security (2010 Revised Edition)

Know Your Organization's Security Level
by Checking 16 Points



IPA
IT Security Center
September 2010
INFORMATION-TECHNOLOGY PROMOTION AGENCY, Japan

2010年9月
処理推進機構
イセンター

本書の活用法

- **自組織の把握**
- **上位を目指す**
- **よりセキュアな製品**

項目ごとのレベルが一覧できる付録チェック表 (「マネジメント」「企画」フェーズのみ抜粋)

ライフサイクル (マネジメントを含む)		「セキュリティへの取組み」のレベル			
段階(フェーズ)	セキュリティを考慮すべき項目	レベル1	レベル2	レベル3	レベル4
マネジメント	1-1. セキュリティルール (P.13)	・セキュリティルールの策定は行っていない	・セキュリティルールは開発者が自主的に策定している ・セキュリティルールは開発責任者や担当者主導で策定される	・組織としてセキュリティルールを策定し、規則集として明文化している	・組織としてセキュリティルールを策定し、規則集として明文化しており、担当者が規則を順守していることを確認するための手段も規定している
	1-2. セキュリティ教育 (P.15)	・セキュリティ教育は実施していない	・セキュリティに関する分科会(小集団活動)が自主的に活動している ・必要に応じて開発責任者や開発者主導で知識を習得したり、勉強会が行われたりする	・セキュリティ教育が業務に組み込まれている ・セキュリティに関する講習会や研修の受講が奨励される	・セキュリティ教育が業務に組み込まれている ・専門家による研修カリキュラムが義務付けられている
	1-3. セキュリティ情報の収集 (P.17)	・セキュリティ情報は特に収集していない	・開発責任者や開発者主導が必要に応じて情報収集を行っている	・組織として情報収集を行い、収集結果は開発者に伝達される仕組みを構築している	・脆弱性情報ハンドリングに積極的に関与し、脆弱性関連情報の活用に努めている
企画	2-1. 予算 (P.18)	・セキュリティに係る予算は用意されていない	・プロジェクトリーダー(開発責任者)の要求があった場合に、予算確保が容認される ・開発責任者や開発者から要求があった場合に、検討される	・開発プロセスの一つとしてセキュリティ確保のために一定の基準で予算を割り振ることが前提として組み込まれている	・組織にセキュリティ部門等を設置するための予算を確保し、活動する
	2-2. 開発プラットフォーム選定 (P.19)	・コスト優先、納期優先で選定され、セキュリティについてはほとんど考慮されない	・開発時に判明している脆弱性への対策は実施する ・出荷後は特に実施されない ・開発プラットフォームの選定を実施する担当者または部門がない ・その製品の開発責任者や開発者によって脆弱性対策の意識が異なり、組織として統一した取組みはなされない	・組み込みソフトウェアパッケージを利用する場合、販売元からの脆弱性対策プログラム等のリリース情報を監視している ・出荷後の製品に対してもソフトウェアアップデート等によって対策を実施している ・同じ製品を扱う部門内では脆弱性対策への意識が高く、統一した取組みがなされている	・全社的に脆弱性対策を実施している ・出荷後の製品に対してもソフトウェアアップデート等によって対策を実施している ・販売元の脆弱性対策に関するサポート体制について事前に確認を行う ・デバイスや回路構成においてセキュリティを考慮した選定を行っている ・製品のセキュリティを高める目的で、独自のプラットフォームの開発や調達先への改善要求活動などを実施している