WG3－2

HITACHI
Inspire the Next

情報家電機器認証技術

2005年　2月17日

株式会社 日立製作所
手塚　悟

HITACHI
Inspire the Next

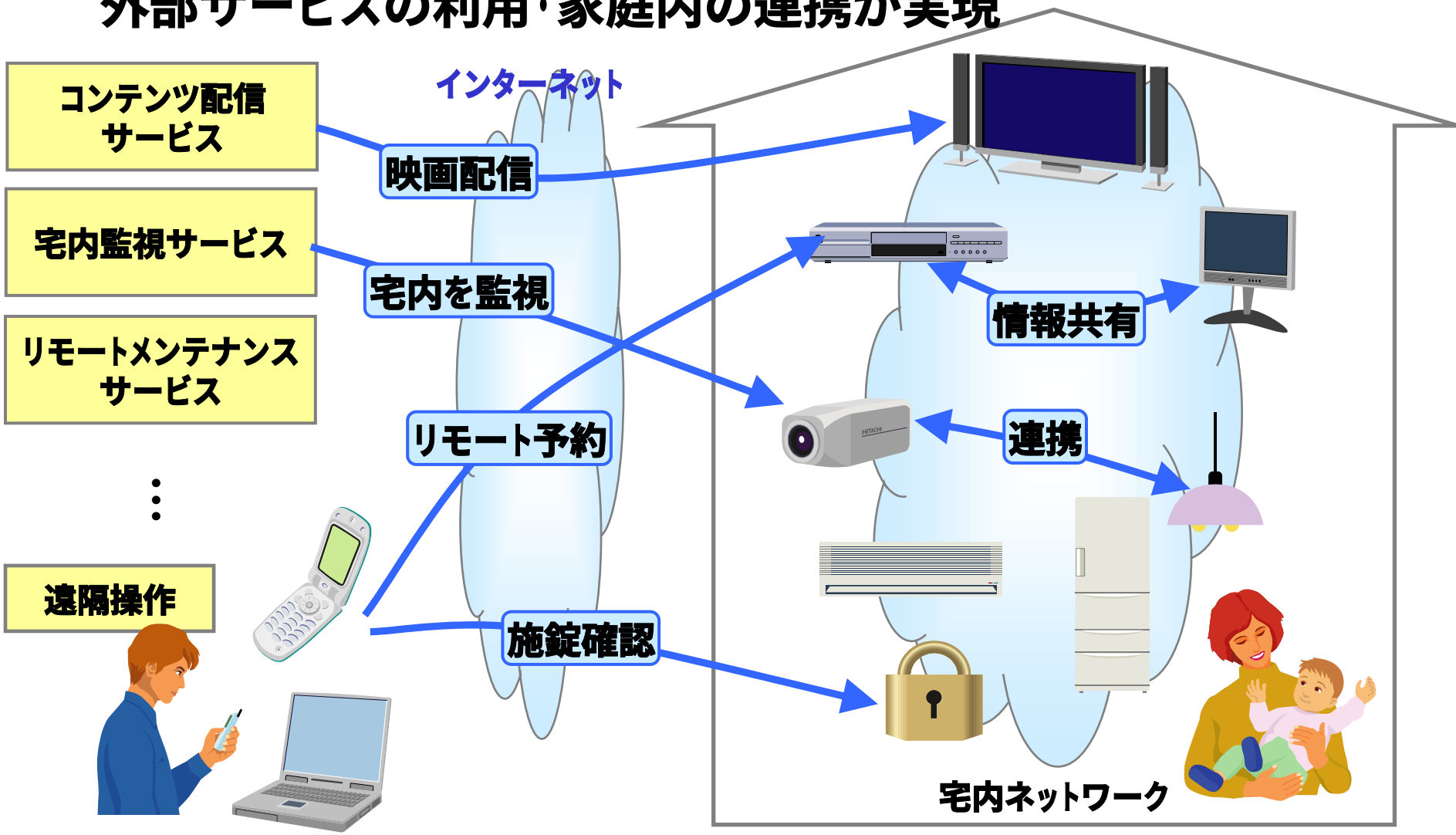
目 次

HITACHI
Inspire the Next

目 次

1.1. 情報家電がつくるユビキタス社会

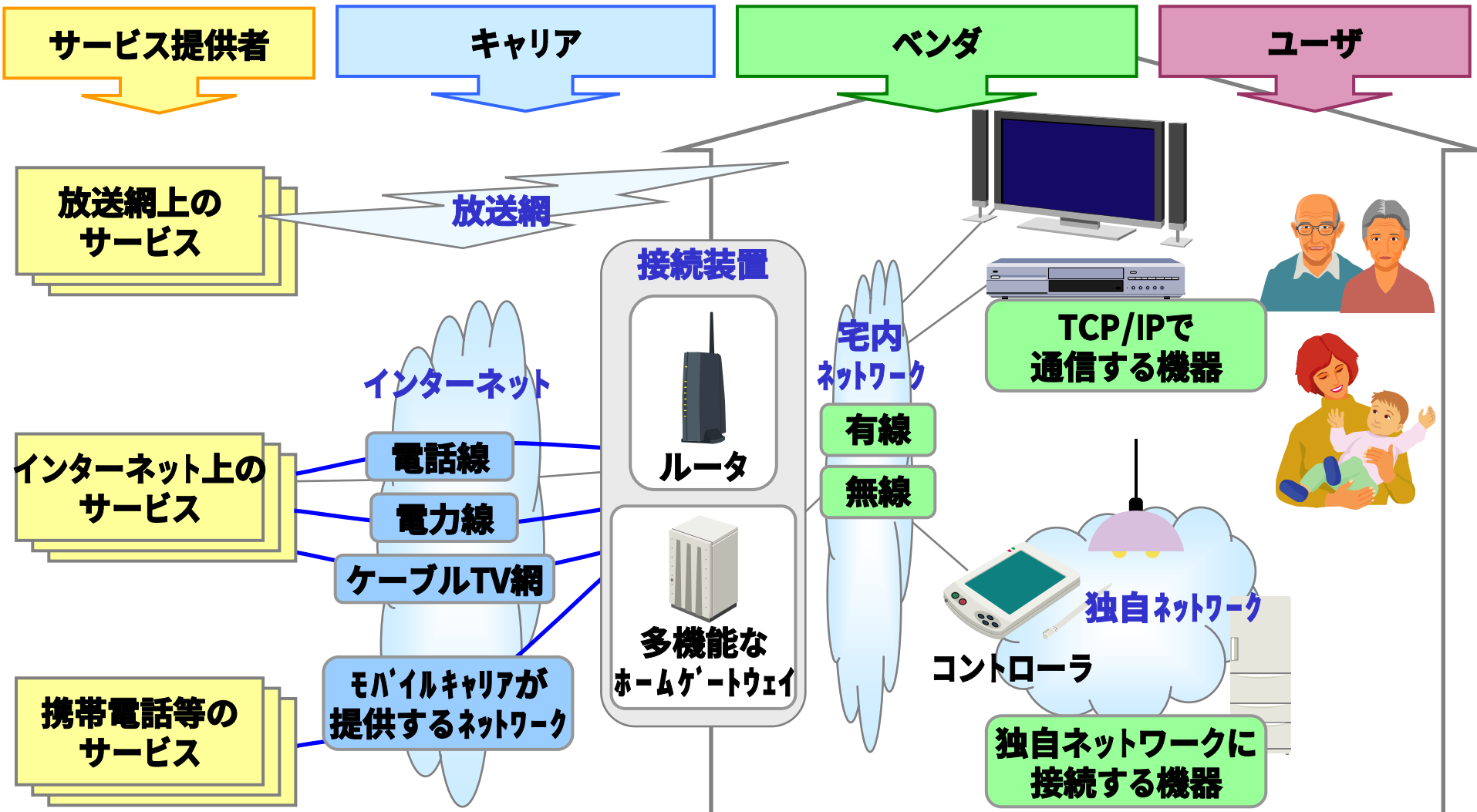
様々な家電がネットワークに接続し、外部サービスの利用・家庭内の連携が実現



1.2. 情報家電を実現するシステムの構成

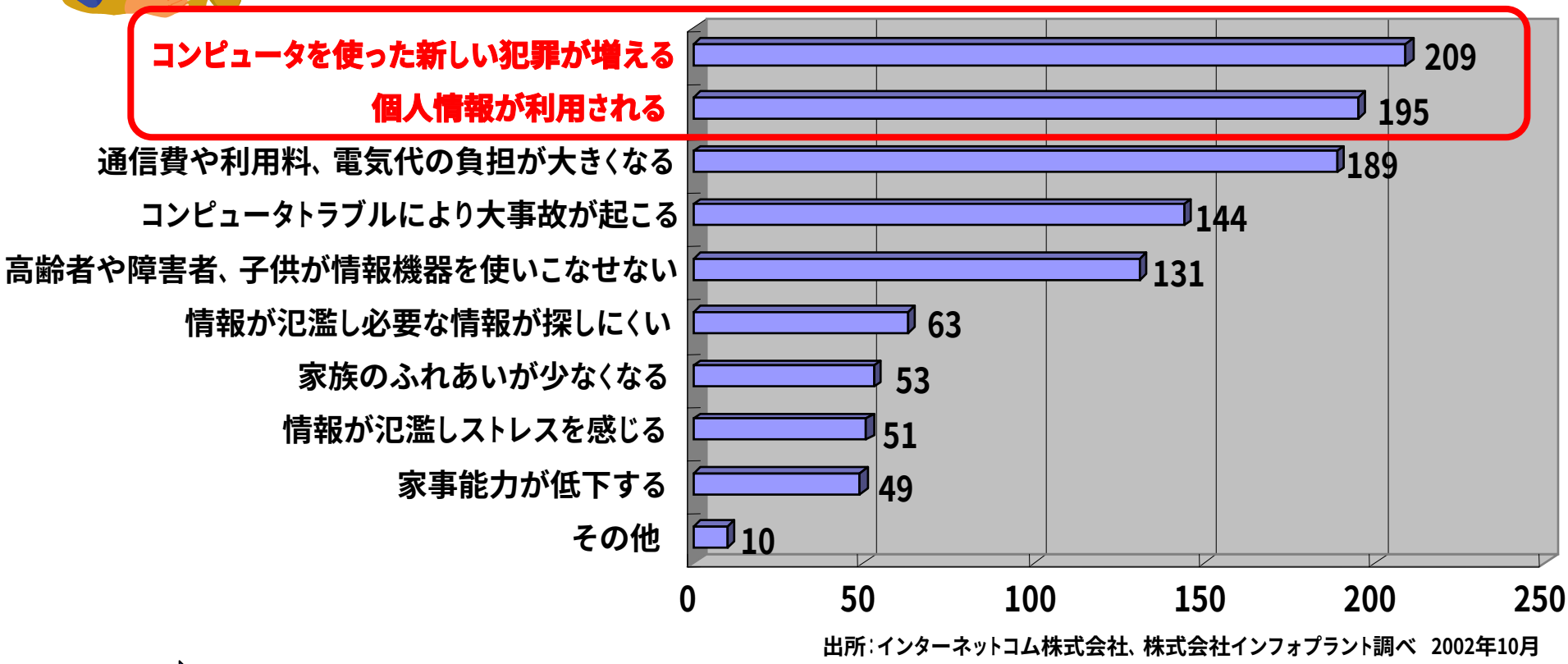
HITACHI
Inspire the Next

家電業界だけでなく、さまざまな業種が参加
電力線や ﾎｰﾑｹﾞｰﾄｳｪｲの利用など、ネットワーク構成もさまざま



1.3. 情報家電とユーザの意識

生活が便利になるメリットはあるが、セキュリティ面が不安

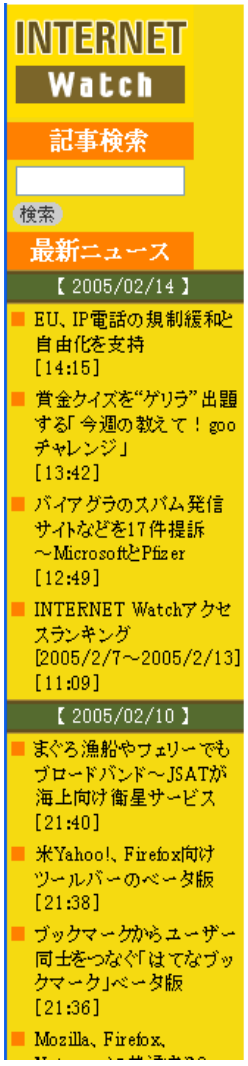


出所：インターネットコム株式会社、株式会社インフォプラント調べ　2002年10月

情報家電の普及には、セキュリティ対策が重要

1.4. 情報家電のセキュリティに関するニュース①

情報家電が“踏み台”になる危険性
（２００４年１０月　INTERNET Watch）



東芝、HDD搭載DVDレコーダ「RD」シリーズが“踏み台”になる危険性
～セキュリティ設定「あり」に変更を呼びかけ

東芝は、同社のHDD搭載DVDレコーダ「RD」シリーズに、外部からの不正アクセスにより“踏み台”にされる危険性があると警告した。対象は「RD-XS40」「RD-X3」「RD-XS31」「RD-XS41」「RD-XS41KJ-CH869」「RD-X4」「RD-X4EX」「RD-XS43」「RD-XS53」「RD-XS34」といった「ネットdeナビ」対応の10機種。該当機種のセキュリティ設定を初期状態の「なし」から「あり」に変更するよう呼びかけている。

東芝によるとネットdeナビ対応のRDシリーズでは初期状態で、外部からユーザー名やパスワードの入力不要でアクセスできる設定になっている。そのため、外出先からDVDレコーダにアクセスできるようルータの設定を変更している場合などでは、不特定のPCから不正にアクセスされ、RDシリーズをプロキシサーバーとして経由し、コメントスパムなどのデータを送信させられてしまう可能性があるという。

東芝は対策として、ソフトを最新版にバージョンアップすることとセキュリティ設定を「あり」に変更することを呼びかけている。セキュリティ設定を「あり」にすることで、外部からアクセスする際にユーザー名とパスワードの入力が必要になり、不正アクセスを防げるようになる。

なお、インターネットに接続したDVDレコーダが直接グローバルIPアドレスを取得している場合や、ADSLやFTTH、CATVのモデムに直接接続している場合、それらのモデムにハブを経由して接続している場合においても外部からのアクセスが可能になるため、セキュリティ設定の変更が必要だ。

東芝ではセキュリティ設定について、「従来機種では初期状態で無効になっていたが、今後発売する機種に関しては、有効以外に設定できないように変更する」としている。

製品出荷時の設定では、
外部から操作する人物を認証しない為、
不特定の端末からアクセスされ、
DoS攻撃の踏み台にされてしまう危険性あり。

外部からのアクセスに対して
ユーザ名・パスワードで
認証するように設定変更する。

1.5. 情報家電のセキュリティに関するニュース②

CATV海賊版デコーダが出回る
(２００４年１０月　日本経済新聞、NIKKEI NET)

NIKKEI NET
日本経済新聞社

■新聞購読申し込み
■日経のイベント
■ENGLISH

検索　記事　株価

▼ニュース　マネー | IR | IT | 経営 | 住宅 | 生活・グルメ | 学び | 就職 | 転職 | クルマ | C-Style | ウーマン | 日経g

トップ | 主要 | 経済 | 企業 | 株・為替 | 国際 | 政治 | 社会 | スポーツ | 新製品 | リリース | 社説・春秋 | おくやみ

社会　>> 記事一覧

▼トップ　おくやみ

CATV“ただ見”横行

マンションなどでケーブルテレビ（CATV）局の有料番組を無料で視聴できる機器が出回っている。契約者以外は視聴できないように加工された信号を解除してしまう機器で、局側は「機器販売は違法性が高い」と主張。だが、機器の売り手側は「研究目的で適法」と反論し、販売を中止する気配はない。CATVの業界団体は業者に警告する一方、法的措置の検討も始めている。

CATVは局と契約して通常、毎月数千円の料金を支払う顧客しか視聴できないように、映像信号に「スクランブル」と呼ばれる視聴制限処理をして放送。正規契約者にはこれを解除する専用機器をレンタルするなどしている。

問題の機器はスクランブルを解除する機能がある。自室までCATV回線が引き込まれているマンションの住人などが、この機器を取り付ければ、その後は、CATV局側と契約しなくても番組を見ることができる。(07:00)

専用の接続装置でのみ
解除できるはずのスクランブルを、
解除できる不正な機器が出回る。

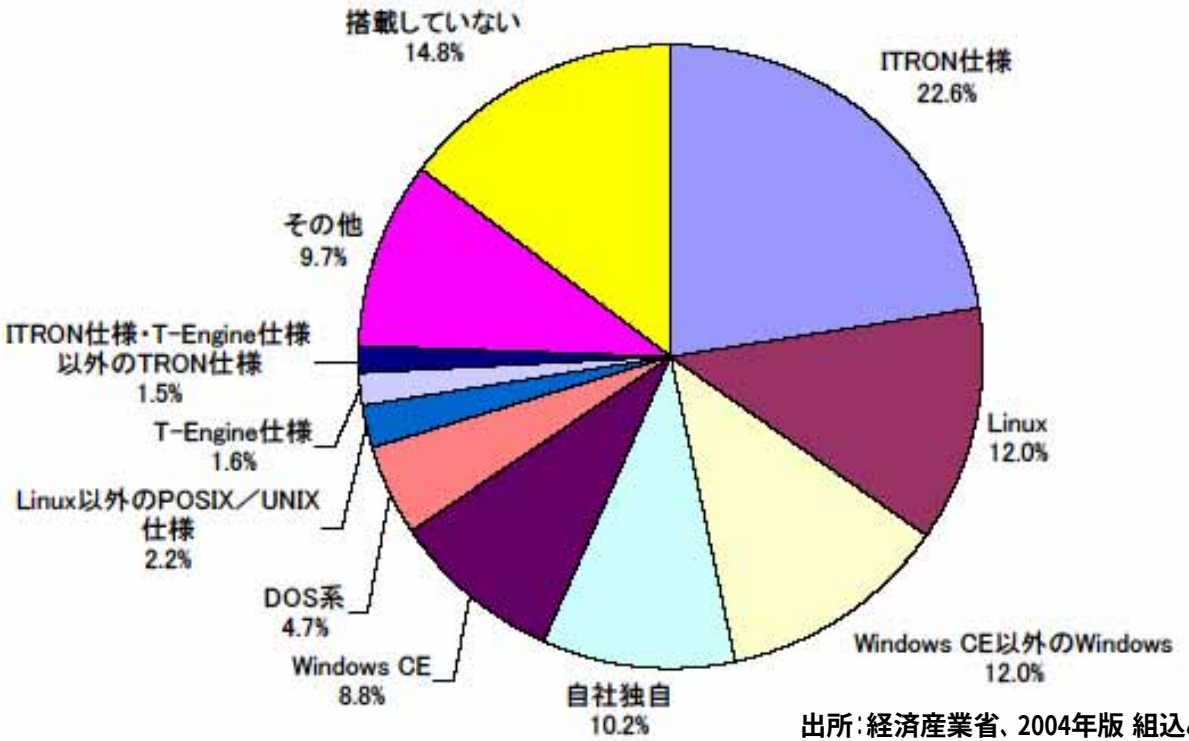
法的手段により、
販売業者への販売差止めを検討中
安全なコンテンツ配信方法が必要

1.6. 情報家電におけるセキュリティの課題

ライフサイクル	セキュリティの課題
製造	オープンアーキテクチャ化による脆弱性
設置	初期設定の複雑化による設定ミス
利用	PCと異なる利用方法 → 宅内へのPush型アクセスが増加
	PCと同様の脅威 ＋ 情報家電特有の脅威（著作物の不正コピー等）
破棄・転売	家電に残した個人情報の漏洩

1.7. [製造時] オープンアーキテクチャ化による脆弱性

ネットワーク化に伴い、サービスが多様化・複雑化
→ 組み込みソフトウェアの高機能化対応のため、汎用OS利用が増加



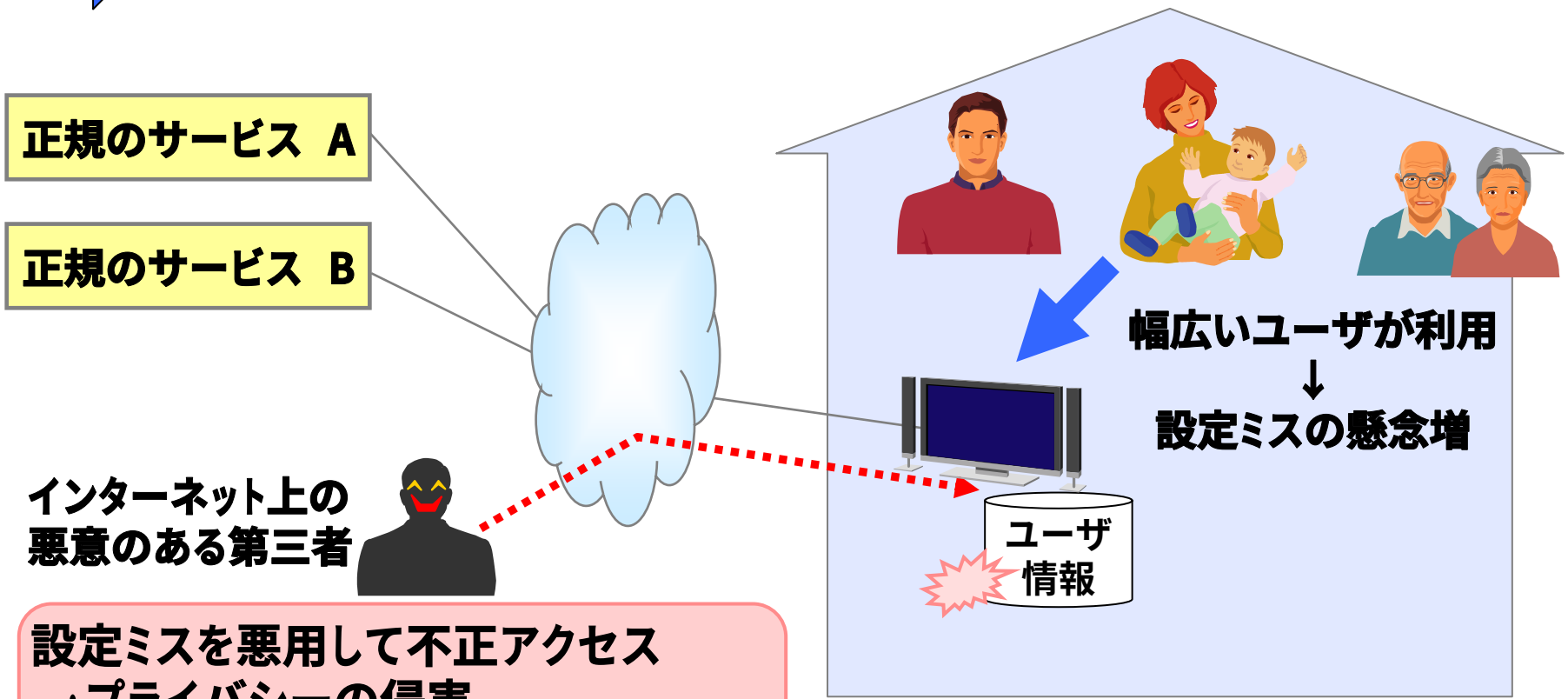
出所：経済産業省、2004年版 組込みソフトウェア産業実態調査 報告書

情報家電でも、PCと同様の脆弱性対策が必要

1.8. [設置時] 初期設定の複雑化による設定ミス

・従来の家電と違い、ネットワーク接続やサービス利用の設定が必要
・高齢者や子供等、幅広いユーザが利用する

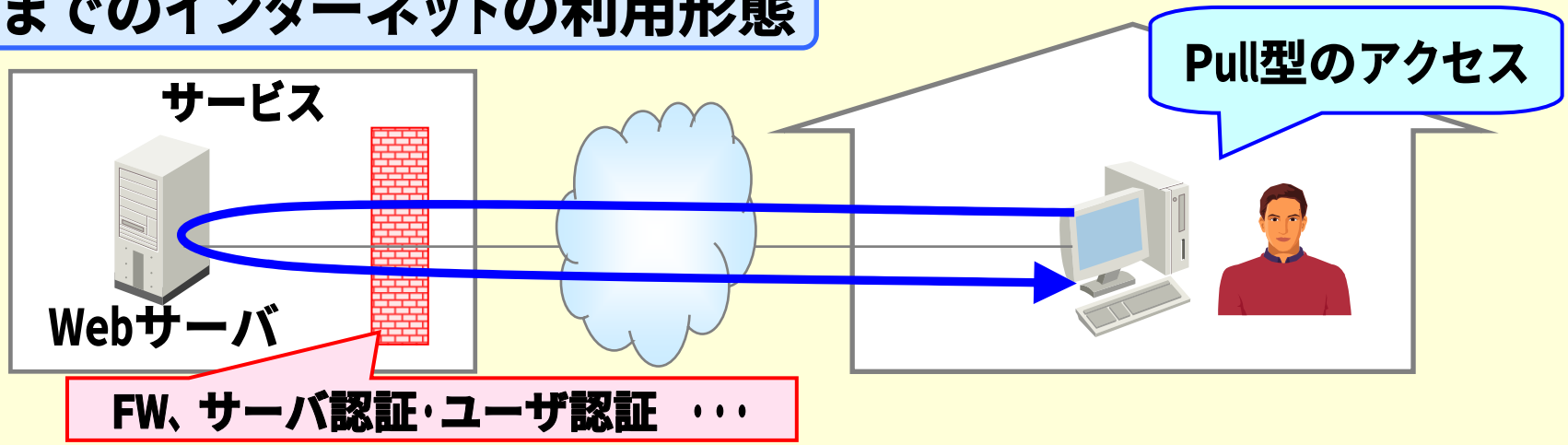
➡ 設定ミスによるセキュリティ脅威が懸念される



設定ミスを悪用して不正アクセス
・プライバシーの侵害
・他の機器への踏み台に　等

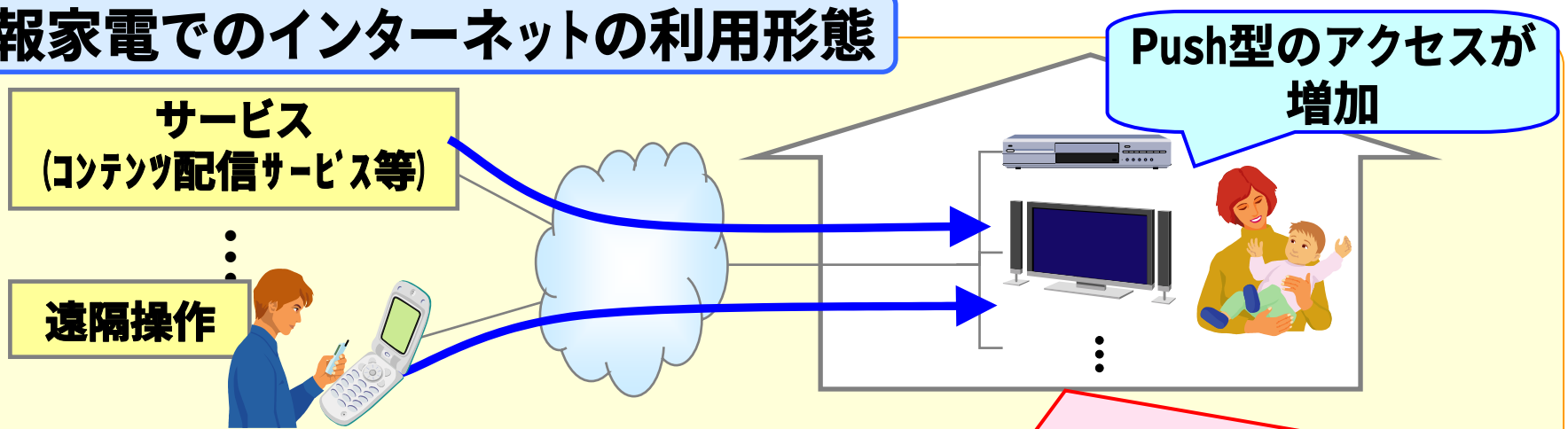
1.9. [利用時] 宅内へのPush型アクセスが増加

今までのインターネットの利用形態



コストをかけられるサービス側（企業・官公庁・ISP等）が対応

情報家電でのインターネットの利用形態



家庭側でのセキュリティ対策が重要になる

1.10. [利用時] PCと同様の脅威＋情報家電特有の脅威

宅外のサービス・機器

コンテンツ配信サービス

コミュニケーションサービス

遠隔操作

不正な機器

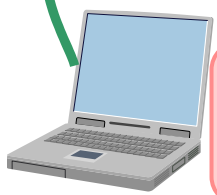
正規の機器になりすまし
・不正にサービスを利用
・著作物の不正コピー　等

ユーザ情報

機器への不正アクセス
・プライバシーの侵害
・他の機器への踏み台　等

インターネット上の
悪意のある第三者

通信データの盗聴・改ざん
・プライバシーの侵害
・不正な遠隔操作　等



不正機器の物理的持込み
・ウィルス感染PCから感染　等

PCで実施していた対策 ＋ 特有の対策 が必要

1.11. [破棄･転売時] 家電に残した個人情報の漏洩

破棄･転売時に情報家電に情報が残ってしまうと、
個人情報･秘密情報が漏洩し、悪用される可能性がある

例：情報家電が保持すると予想される情報

情報家電	個人情報･秘密情報
テレビ電話用TV	アドレス帳、通信料引き落とし口座　など
コンテンツ配信用レコーダ	サービス契約情報、 コンテンツ復号用秘密情報　など
エアコン、照明	利用者の帰宅時間　など
冷蔵庫	冷蔵庫の過去の中身　など

1.12. セキュリティ対策と認証の重要性

OS･ソフトウェアの脆弱性	･外部サービスから、家電に修正プログラムを配布 ↑認証により配布すべき機器を特定
機器への不正アクセス	･家電が、宅外のサービス･機器を認証
正規の機器になりすまし	･宅外のサービス･機器が、家電を認証
通信データの盗聴･改ざん	･家電～宅外サービス間の通信の暗号化、署名 ↑認証情報を利用することで、より強固な対策が可能
宅内への不正機器持込み	･宅内ネットワーク接続時の認証、検疫
破棄･転売時の情報漏洩	･家電が、利用者を認証 ･家電破棄時に保存情報消去

セキュリティ対策には、認証が重要

HITACHI
Inspire the Next

目 次

2.1. 身の回りにある通信技術と認証方法

現在、多く利用されている通信技術の認証方法に関して整理する

(1) SSL-VPN
(2) デジタル放送（B-CASカード）
(3) UPnP
(4) Bluetooth
(5) リモート番組予約サービス
(6) ECHONET

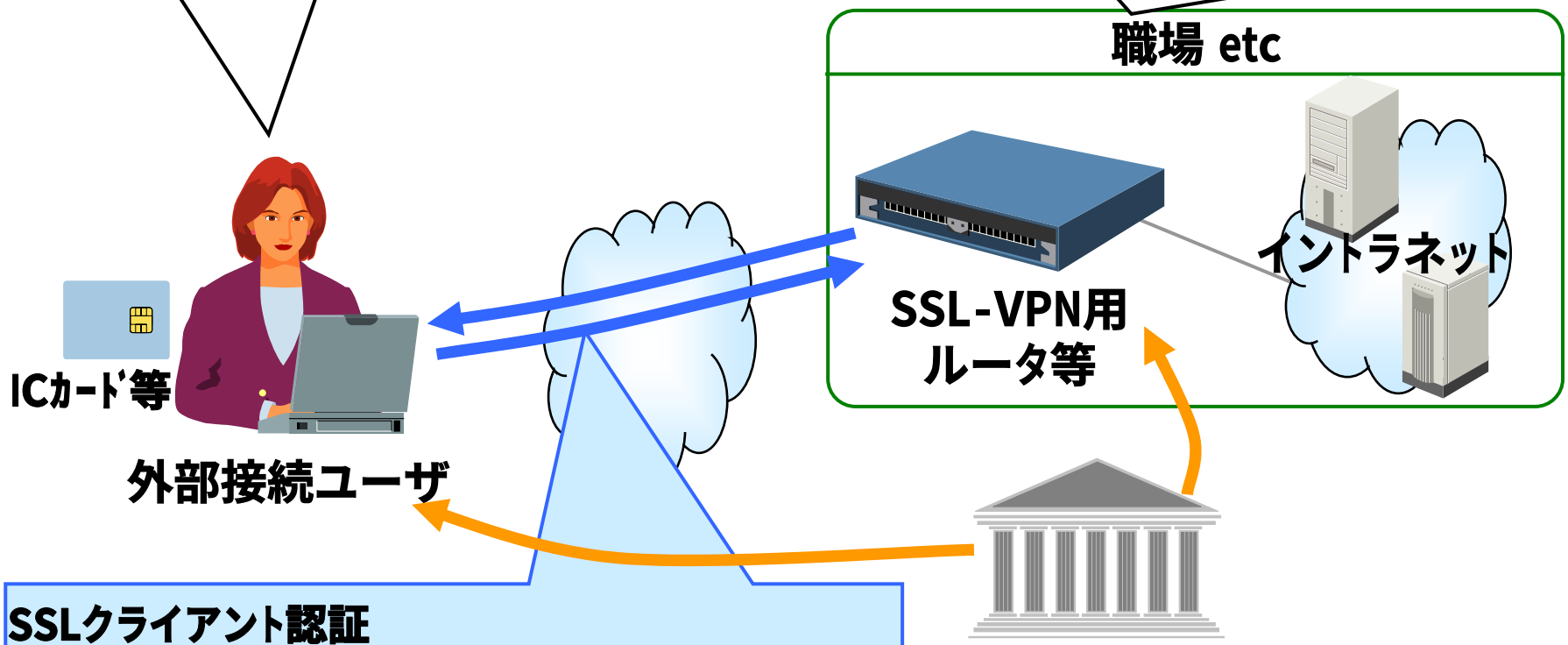
・ECHONETは、ECHONETコンソーシアムの登録商標です。
・Bluetoothは、The Bluetooth SIG Inc.の登録商標です。

2.2. SSL-VPNでの認証

HITACHI
Inspire the Next

職場にアクセスしたい

社員だけを接続させたい



SSLクライアント認証
①サーバ内に保存された
　サーバ証明書をもとに、サーバの真正性を認証
②ICカード内のユーザ証明書や、
　PC内に保存されたユーザ証明書をもとに、
　ユーザの真正性を認証

③証明書の有効性を保証

2.3. デジタル放送（B-CASカード）での認証

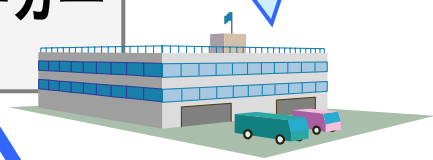
コンテンツ保護ができる
端末にのみ配信したい

② B-CASカードの
同梱を許可

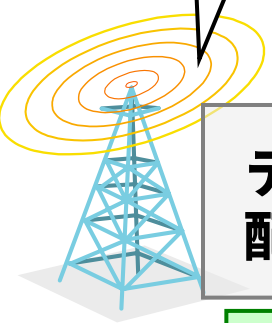
③ B-CASｶｰﾄﾞと対応機器
の関連を保証

B-CASカード
管理団体

家電メーカー

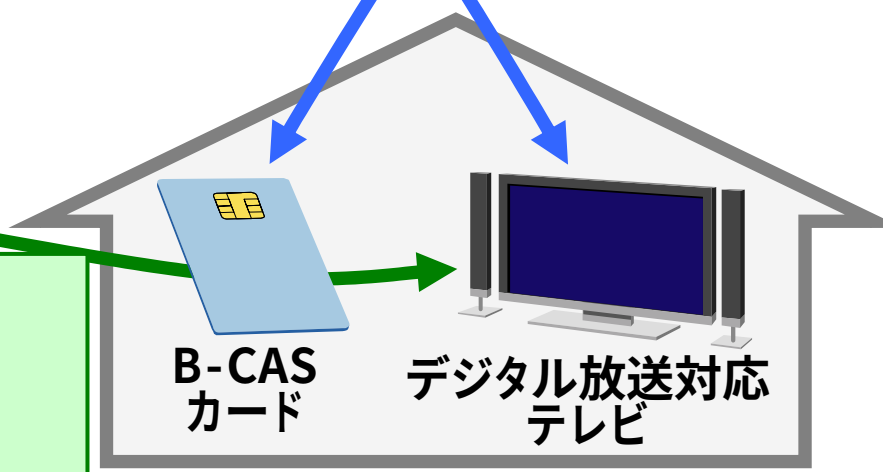


① B-CASカードの
機能を保証



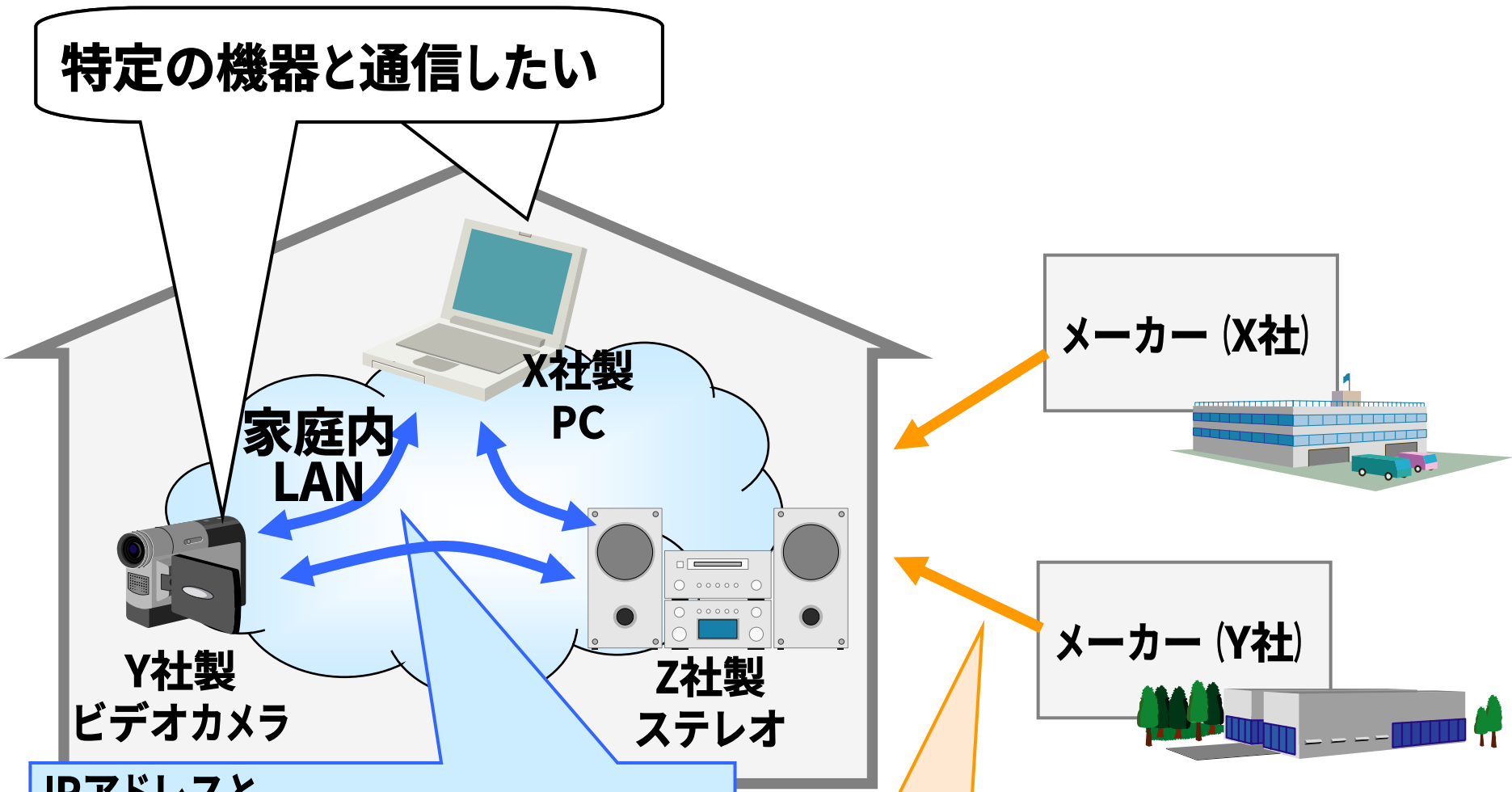
デジタル放送
配信サービス

コンテンツ

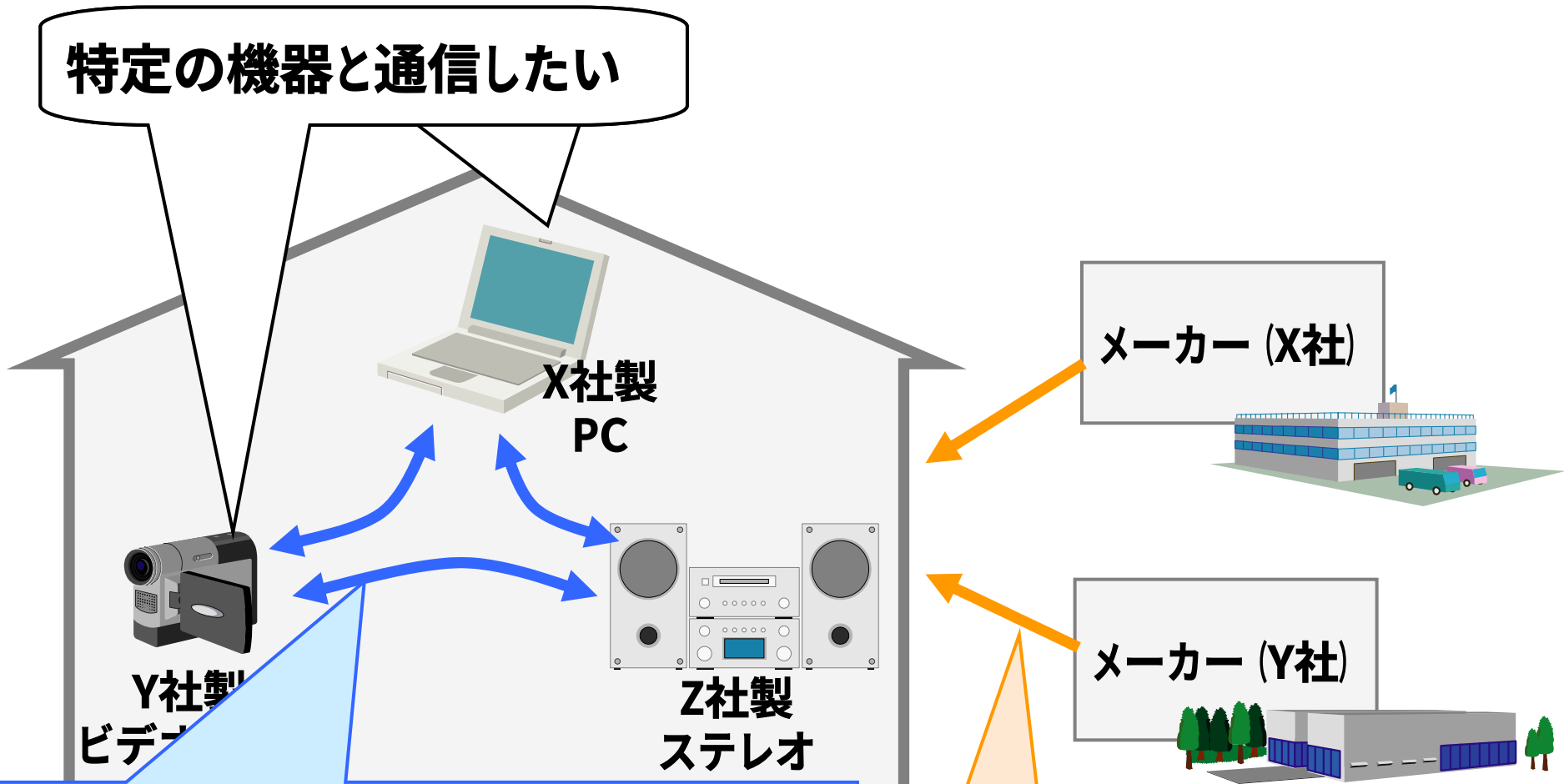


④ B-CASカードでしか
復号できない暗号処理で
コンテンツ配信
→B-CASカードをもとに
サービス契約･機器の機能を認証

2.4. UPnPでの認証



2.5. Bluetoothでの認証



・Bluetooth機器識別番号で
機器を識別
・通信機器間で秘密情報を共有し、
ワンタイムパスワードで機器の真正性を認証

適切な識別番号を
付与して出荷

2.6. リモート番組予約サービスでの認証

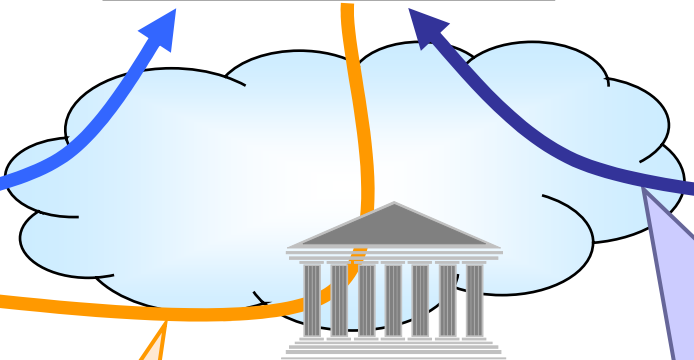
HITACHI
Inspire the Next

特定の機器を操作したい

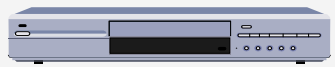
適切な予約指示だけを受信したい

X社
リモート予約ｻｰﾋﾞｽ

外部接続
ユーザ



PKIの認証局



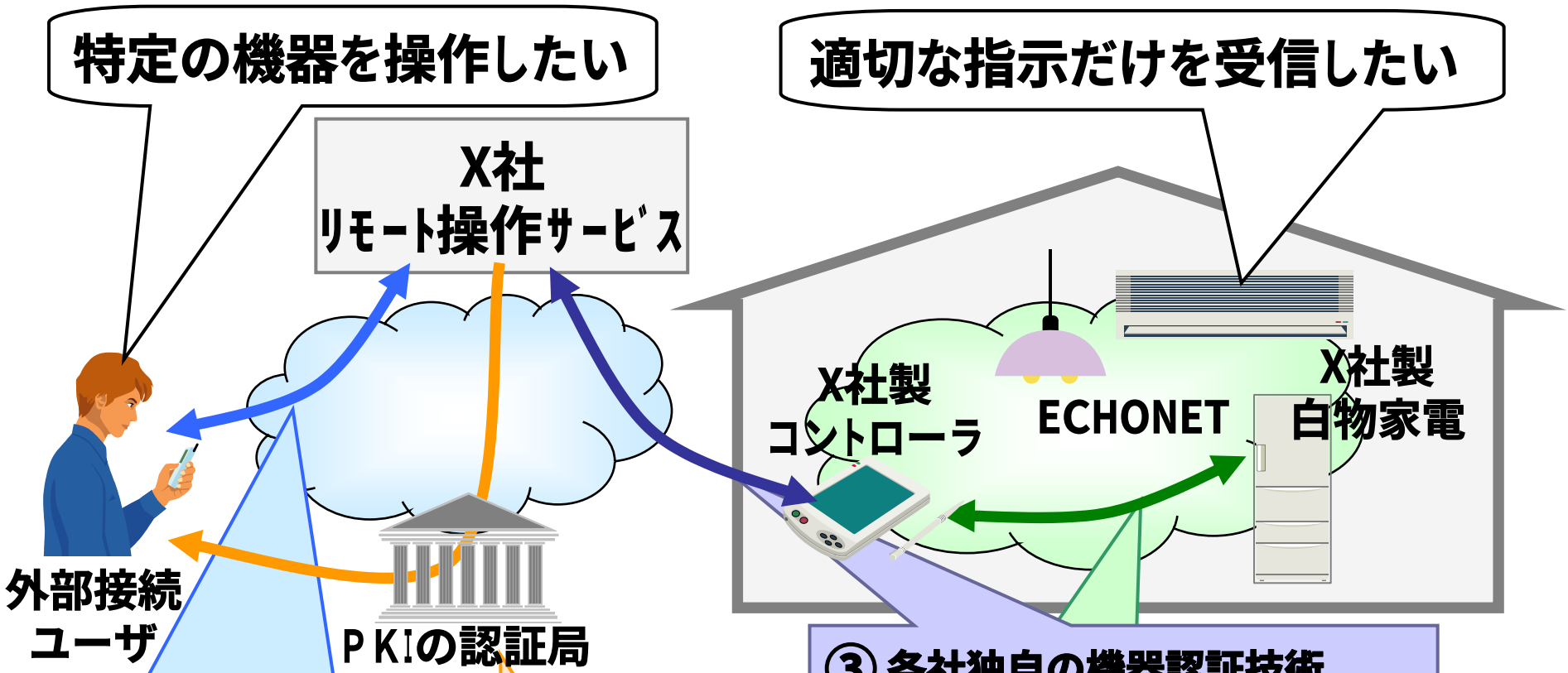
X社
HDDレコーダ

① SSLサーバ認証
・ｻｰﾊﾞ証明書によりｻｰﾊﾞの真正性を認証
・ID・PW等により
外部接続ﾕｰｻﾞの真正性・ｻｰﾋﾞｽ契約を認証

② サーバの証明書の有効性を保証

③ 各社独自の機器認証技術
(ﾚｺｰﾀﾞ内のID・PW　等) により、
ｻｰﾊﾞの真正性、
機器の真正性・特性 (機種など)・
ｻｰﾋﾞｽ契約を認証

2.7. ECHONET ＋ リモートサービス での認証



2.8. 身の回りにある通信技術と認証方法の整理

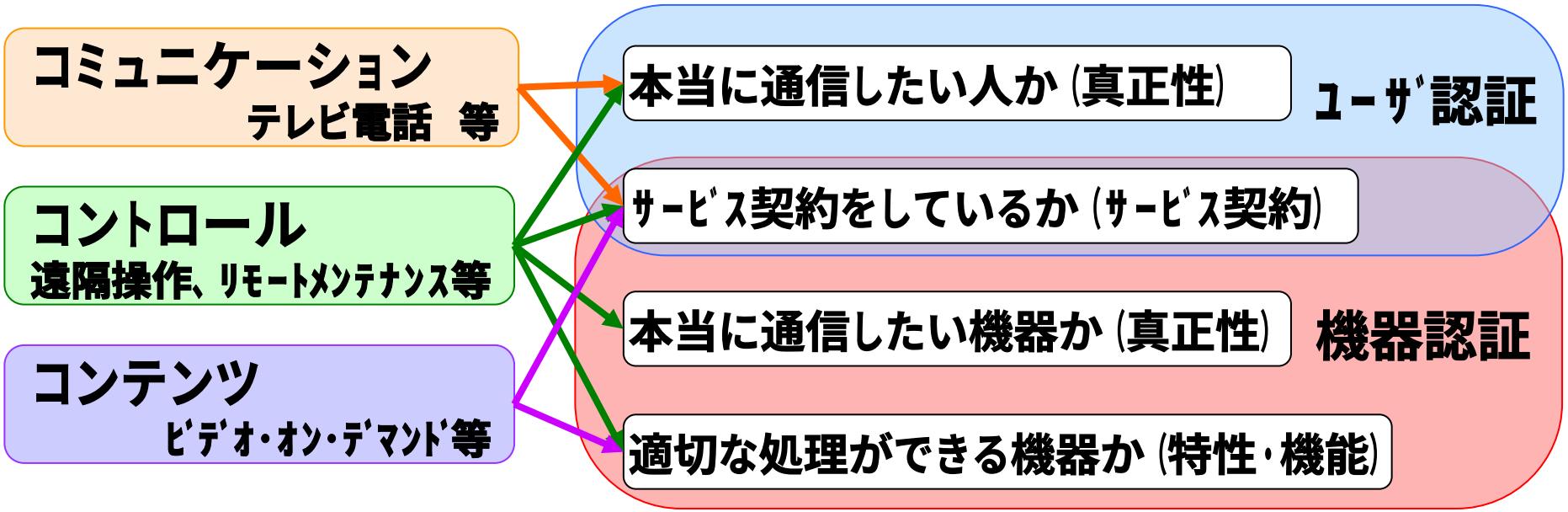
	範囲	対応機器	認証有無	識別 or 認証情報	識別or認証する内容
SSL-VPN	家庭外 →家庭	PC 等	認証	・サーバ証明書 ・ユーザ証明書	・機器（ｻｰﾊﾞ）の真正性 ・ﾕｰｻの真正性
ﾃﾞｼﾞﾀﾙ放送 （B-CASｶｰﾄﾞ）	家庭外 →家庭	テレビ 等	認証	・B-CASｶｰﾄﾞ	・ｻｰﾋﾞｽ契約、機器の特性
UPnP	家庭内	PC、 AV家電 等	識別のみ （認証も 検討中）	・IPアドレス ・UPnP機器識別番号 （UUID）	・機器の真正性
Bluetooth	家庭内	PC、 家電 等	認証	・Bluetooth機器用 識別番号 ・ワンタイムパスワード	・機器の真正性
ﾘﾓｰﾄ番組 予約ｻｰﾋﾞｽ	家庭外 →家庭	ビデオ 等	認証	・サーバ証明書 ・ユーザID,パスワード ・各社固有の 機器特定情報	・機器（ｻｰﾊﾞ）の真正性 ・ﾕｰｻﾞの真正性・ｻｰﾋﾞｽ契約 ・機器（ﾚｺｰﾀﾞ）の 真正性、特性、ｻｰﾋﾞｽ契約
ECHONET	家庭内	白物家電	識別のみ （認証も 検討中）	・ECHONET MACｱﾄﾞﾚｽ ・ECHONET ｱﾄﾞﾚｽ 等 ・各社固有の 機器特定情報	・機器の真正性 ・機器（ｺﾝﾄﾛｰﾗ）の 真正性、特性、ｻｰﾋﾞｽ契約

・機器を特定する情報として、規格独自の機器識別番号を利用している
→ 統一的なIDが必要か？

・認証する内容の区別があいまい → 認証内容を整理して検討が必要

2.9. 認証内容の整理（1）

認証したい内容はさまざま。
認証方法（ユーザ認証or機器認証）によって、認証できる内容が変わる



情報家電ではユーザ認証だけでなく、機器認証が必要

2.10. 認証内容の整理（2）

「サービス契約」の認証は、
現状、機器とｻｰﾋﾞｽが1対1で対応づいてｻｰﾋﾞｽ提供しているため、
機器認証によって、実現可能。

<u>今後は、機器が複数のサービスを利用する可能性がある</u>

各社独自の認証により、
機器とサービスが1対1に
対応づく場合は
機器認証で実現可能

- ｻｰﾋﾞｽ契約をしているか（ｻｰﾋﾞｽ契約）
- 本当に通信したい機器か（真正性）
- 適切な処理ができる機器か（特性・機能）

➡ 「サービス契約」の認証は、
他の機器認証の内容と区別して考える必要がある

HITACHI
Inspire the Next

目 次

3.1. 期待される開発内容（1）

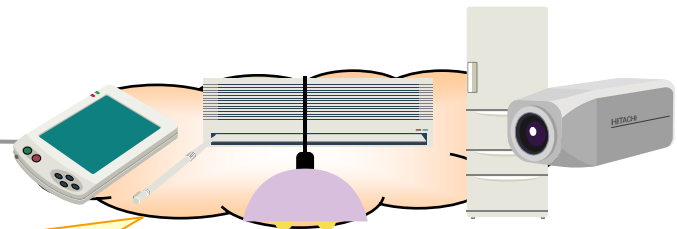
現在は、サービスおよび機器メーカごと利用方法がことなる

➡ 簡単＆安全な設定、操作の共通化が必要

X社向け
リモート予約サービス

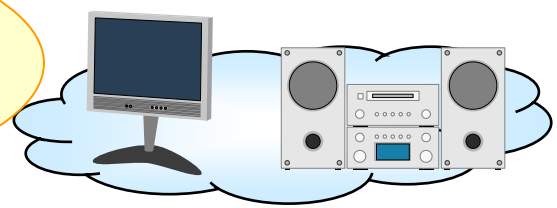
Y社向け
家電操作サービス

X社 ビデオデッキ



ECHONET対応　家電

ECHONETにおいても、基本的な部分での標準化は行われているが、各メーカごとに拡張されており、拡張機能に関する、互換性がない。



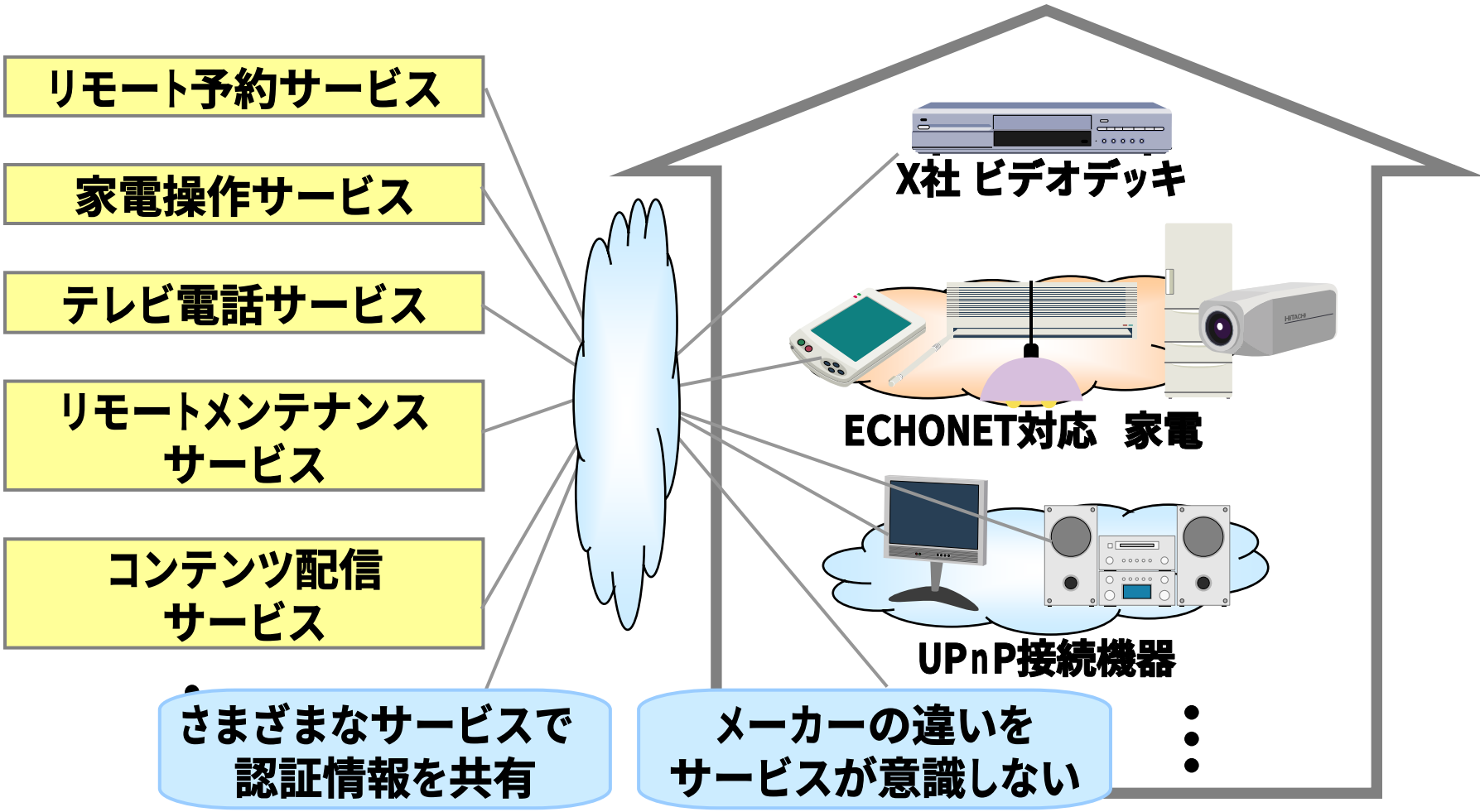
UPnP接続機器

ユーザの声

・サービスが機器メーカー独自のもの（選択肢が少ない）
・たくさんの操作方法に対応しなければならない

3.2. 期待される開発内容（2）

今後は、さまざまなサービスや家電が現れると予想される・・・



3.3. 期待される開発内容（3）

サービスによっては、機器の特性・機能を保証する必要がある・・・

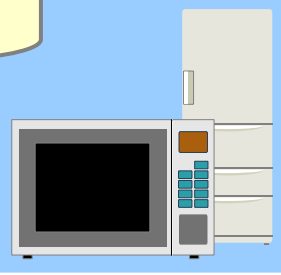
リモート予約サービス
家電操作サービス
テレビ電話サービス

本当に通信したい機器 or 人であることを認証

リモートメンテナンスサービス

修理が必要な機種・機器を特定し、パッチ配布 or 訪問修理

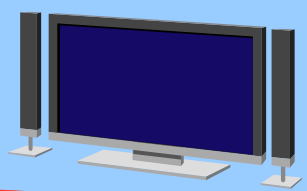
修理が必要な機器であることを認証



コンテンツ配信サービス

ｻｰﾋﾞｽが望むｺﾝﾃﾝﾂ保護機能などを持つか否かを特定し、コンテンツ配信

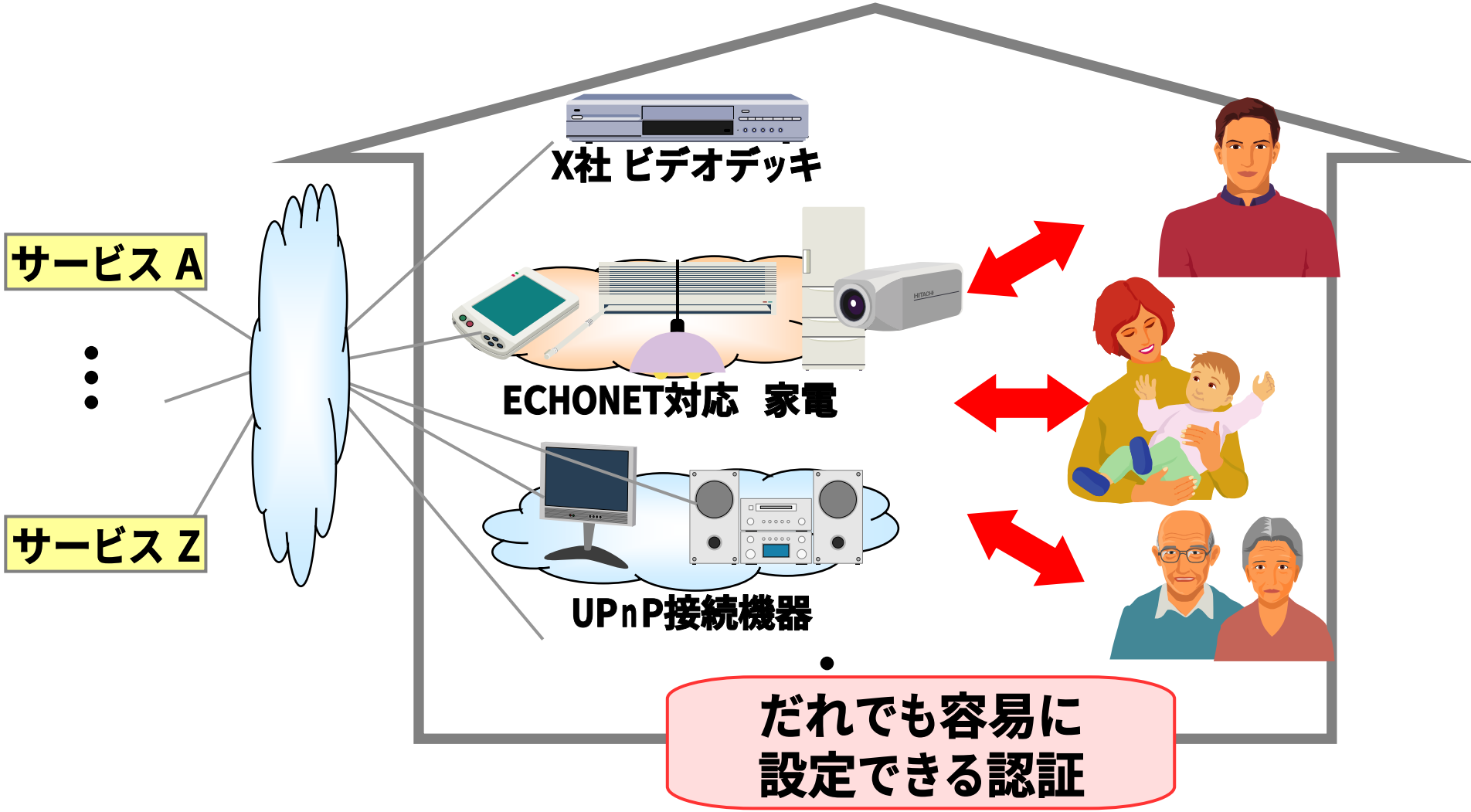
コンテンツ保護が可能な機器であることを認証



機器の特性・機能に関する認証

3.4. 期待される開発内容（4）

今後は、さまざまな人が使うと予想される・・・



3.5. 期待される開発内容（5） 課題

ﾏﾙﾁｻｰﾋﾞｽ、ﾏﾙﾁﾍﾞﾝﾀﾞに対応した機器認証

・共通で使える機器認証が必要。
　システム全体（ベンダ、キャリア、サービス提供者）での協力が重要

機器の特性・機能に関する認証

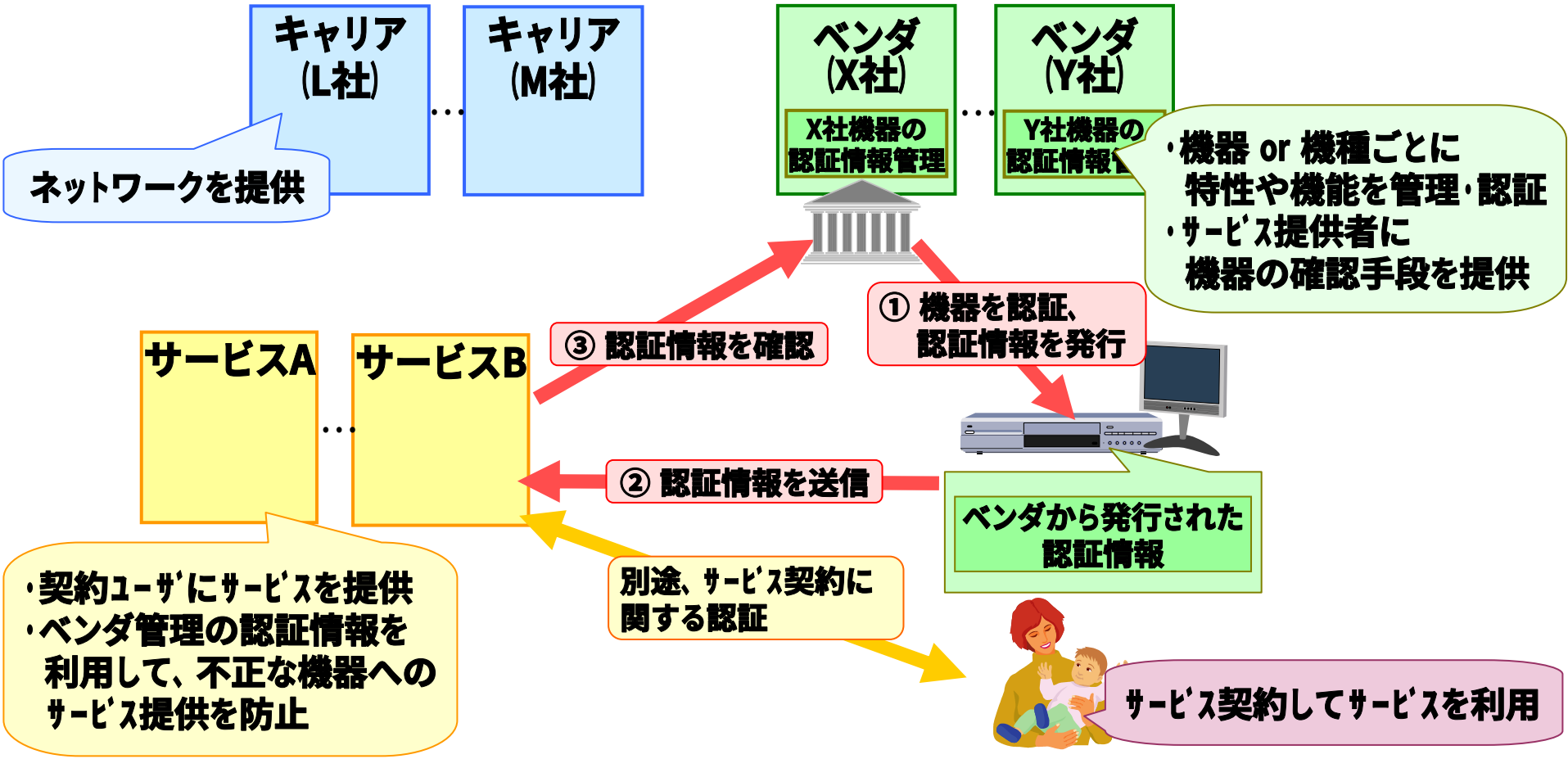
・機器の身元や、特性・機能について、保証する体制が無い

だれでも容易に設定できる認証

・家電は、ユーザインタフェースがPCに比べて乏しい。
・異なるサービスごとに認証が違うと、認証の操作が複雑化

3.6. 機器認証の実現形態の例①
＜ベンダが中心となる認証＞

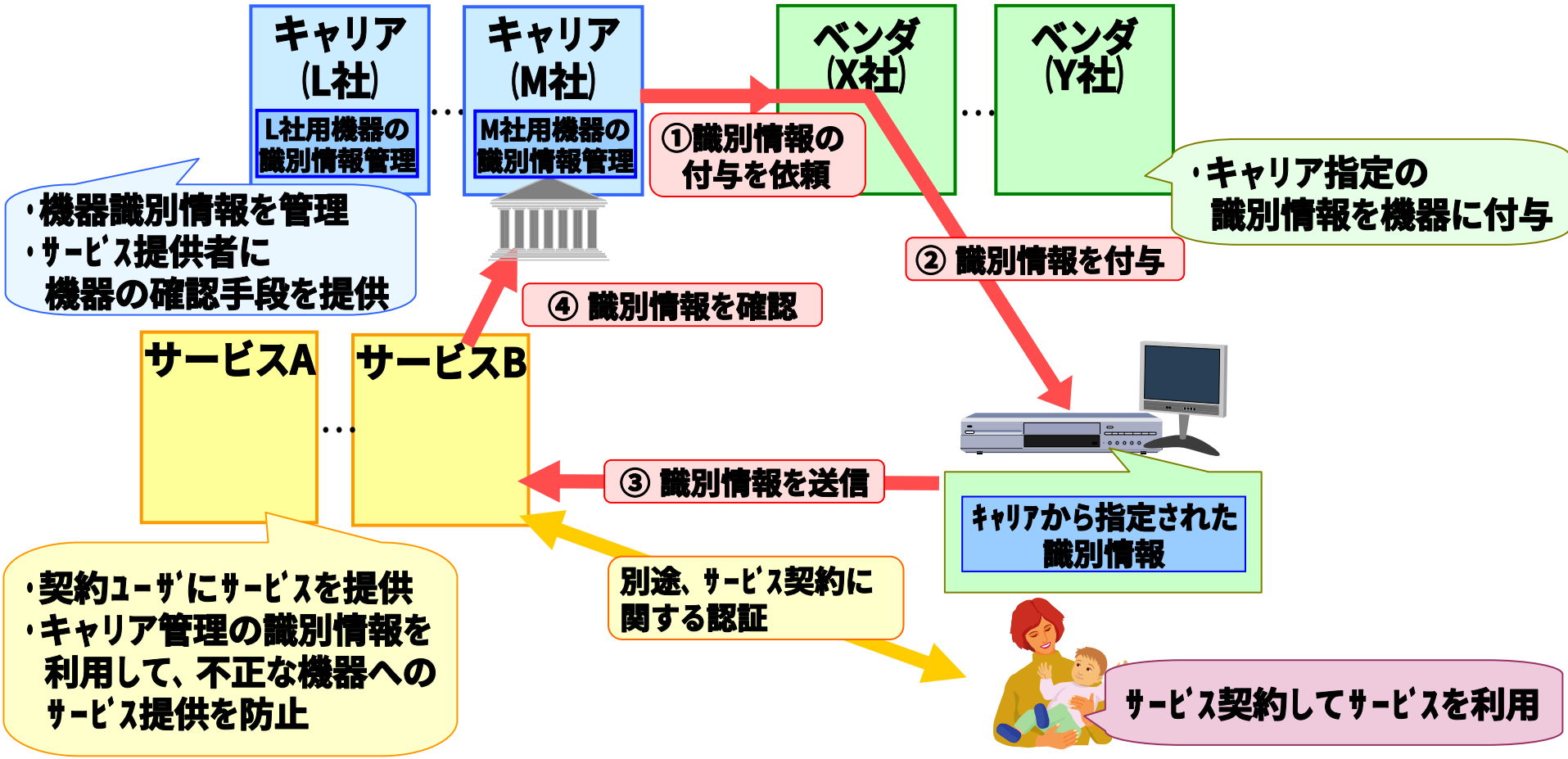
HITACHI
Inspire the Next



・ベンダ間で共通の認証方式が必要
  - 認証情報の付与方法
  - ユーザ、情報家電の負荷が少ない処理方式
・サービスとベンダの連携が必要

3.7. 機器認証の実現形態の例②
＜キャリアが中心となる認証＞

HITACHI
Inspire the Next



・機器識別番号をキャリアが管理する
・サービスとキャリアの連携が必要
・機器識別情報の信頼性を担保する手段が別途必要
　→ベンダによる認証が必要か

3.8. 機器認証の実現形態の例③ ＜サービス提供者が中心となる認証＞

HITACHI
Inspire the Next

キャリア (L社) … キャリア (M社)

ネットワークを提供

ベンダ (X社) … ベンダ (Y社)

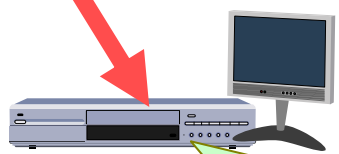
・ｻｰﾋﾞｽから認定を受ける
・機種ごとにｻｰﾋﾞｽ個別の認証情報を付与

① 機器を認定 認証情報を発行

② 認証情報を付与

サービスA … サービスB

ｻｰﾋﾞｽA用認証情報管理 … ｻｰﾋﾞｽB用認証情報管理



③ 認証情報を送信

サービスA用認証情報
サービスB用認証情報

・契約ﾕｰｻﾞにｻｰﾋﾞｽを提供
・サービス自身が管理する認証情報を利用して、不正な機器へのｻｰﾋﾞｽ提供を防止

別途、ｻｰﾋﾞｽ契約に関する認証

ｻｰﾋﾞｽ契約してｻｰﾋﾞｽを利用

・機器はサービスから認定を受けて出荷
・複数のサービスを利用する際に機器のリソース不足が懸念される

3形態ともに、各業種間・業種を超えた合意が必要 ➡ **全体の舵取りが重要**