

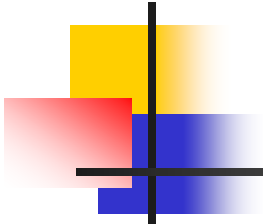
2008年度 TCG専門委員会 活動概要

2009/3/12

(社) 電子情報技術産業協会 TCG専門委員会

委員長 三島 久典

((株) 日立製作所 システム開発研究所)

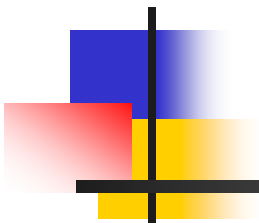


目次

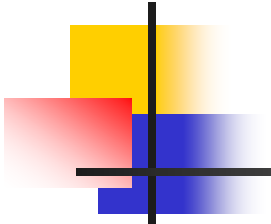
1. TCG専門委員会 活動概要
2. TCG入門
3. 2008年度検討内容
4. 報告書、本日の発表内容

商標、商標登録の記載

- TCGは、Trusted Computing Groupの米国およびその他の国における商標または登録商標です
- Windows Vistaは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です
- その他記載されている会社名、製品名は各社の商標または登録商標です



1. TCG専門委員会 活動概要



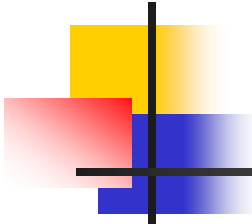
1.1 TCG専門委員会

(1) 構成メンバー(50音順) ～ 10社、20名

インサイトインターナショナル(株)、ウィンボンド・エレクトロニクス(株)、東芝テック(株)、凸版印刷(株)、日本電気(株)、パナソニック(株)、(株)日立グローバルストレージテクノロジーズ、(株)日立製作所、富士ゼロックス(株)、富士通(株)

(2) 活動目標

- ・TCGの仕様の調査、日本のIT業界に与える影響・対応策を検討
- ・TCG技術の積極活用によるセキュリティ技術の向上
 - ⇒ 日本のIT製品の国際競争力向上。2007年度から活動



参考 2007年度の成果

TCG技術は、実は、
既に我々の身近にある

- ・TPM搭載PCは既に普及
- ・OSもTPM対応



既存システムが
TPM搭載PCに置き換わった時
どのようなことが
できるようになるか？



⇒
既存システムへの適用可能性
を追求

トラステッドなシステムの可能性

TCG製品・ソリューション

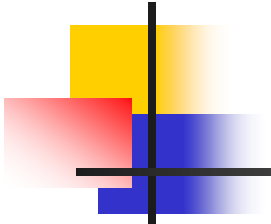
- ・検疫ネットワーク
- ・FDE、HDD暗号機能
- ・トラステッドブート

PC・ネットワーク以外への適用

- ・組込システム
- ・携帯電話
- ・自動車
- ・情報家電

既存業務アプリケーションへの適用

- ・高セキュリティユーザ
 - ・公共インフラ、金融、病院
- ・企業、業種別アプリケーション
- ・学校、教育



1.2 2008年度活動の背景

現状(2008/4～)は、

- ・仕様よりも製品が先行している状況
- ・PC、サーバ以外の製品でも
セキュリティ規格に関する検討が進んでいる
 - ・ストレージ: ATA、ANSI T13、SNIA
 - ・デジタル複合機: IEEE P2600
 - ・携帯電話: OMTP
 - ・ICカード: NFC

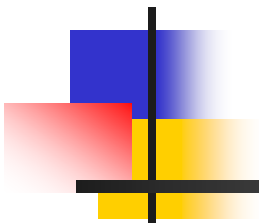
⇒ TCGだけでなく、もう少し範囲を広げてみる

『IT機器におけるセキュリティトレンド、技術動向に関する情報集約』

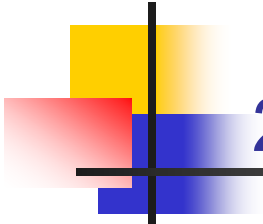
各製品ジャンルごとの、

- ・技術標準: TCG、TCG以外の国際標準、業界標準
- ・製品動向

について報告書としてまとめる



2. TCG入門



2.1 TPMとTCG

TPM (Trusted Platform Module)

TCGで仕様が標準化されたセキュリティチップの名称

TCG (Trusted Computing Group)

「信頼できる(Trusted)」コンピューティングのための仕様検討を行う、ベンダーコンソーシアム／標準化団体の名称



(実は)既に我々の身近にある

TPM : Infineon, Winbond, Atmel, STMicro等が出荷

PC : 2005年以降、ほとんどのPCベンダがTPM搭載モデルを発表

OS : Windows Vista はTPM対応

2.2 TPM (Trusted Platform Module)

TPMの機能

- ・暗号機能
 - 公開鍵暗号(RSA)
 - ハッシュ(SHA1)、MAC(HMAC)
 - 乱数生成
- ・メモリ(揮発・不揮発)
- ・カウンタ、タイマ

TPMの用途

- ・データ(鍵)の暗号化
 - ⇒ PC内部のデータの漏洩を防ぐ
- ・データの署名
 - ⇒ データの中身が他人に改ざんされるのを防ぐ
- ・高度な認証
 - ⇒ 機器が正当なものかどうか
 - 機器内部の各ハードウェア(CPU、メモリ、HDD等)やソフトウェア(OS、アプリ等)が正当なものかどうか

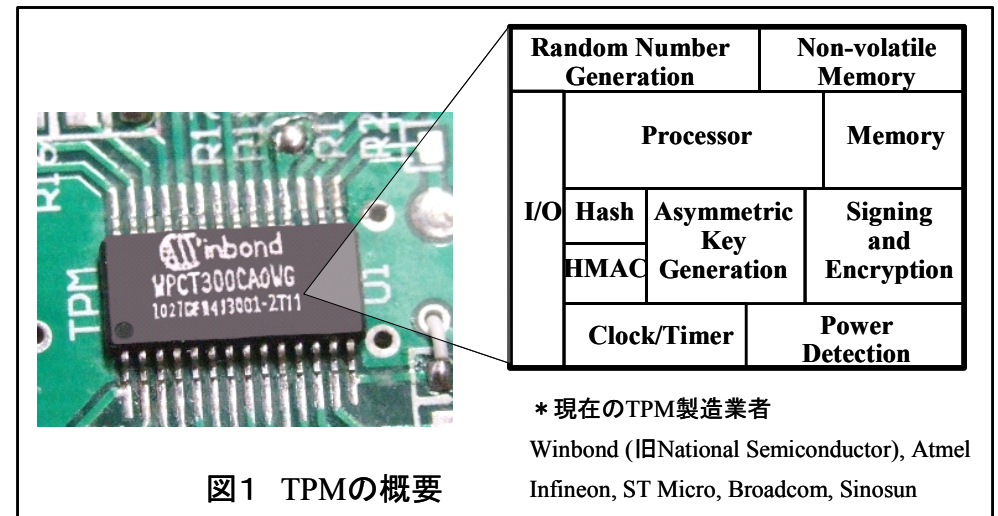
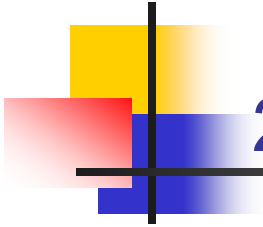


図1 TPMの概要

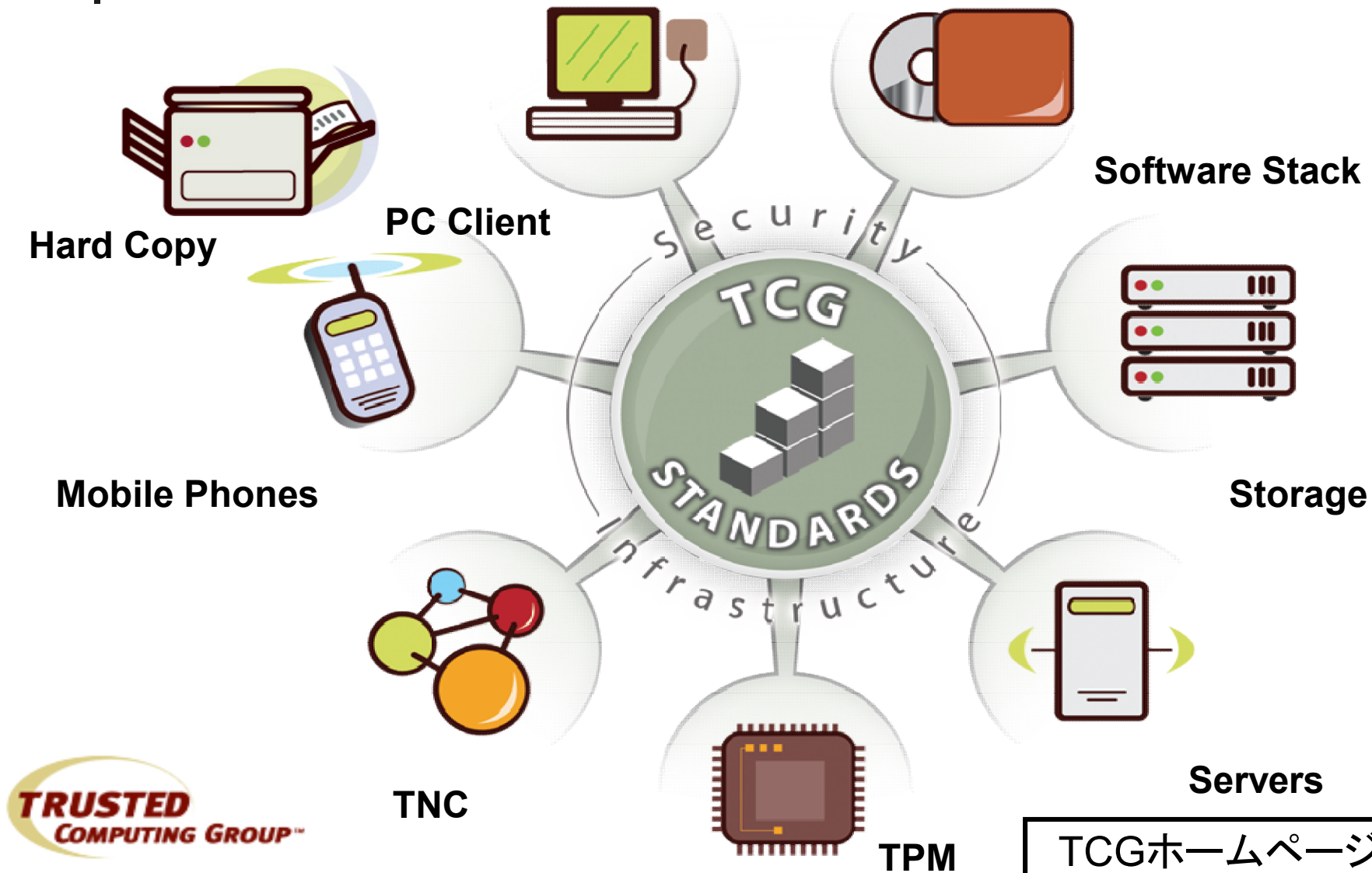
を確認できる



2.3 TCGで定めている仕様

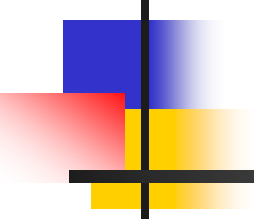
- ・TCGの仕様の全体像
⇒ "TCG Specification Architecture Overview"
Revision 1.4, 2nd August 2007
 - ・TCG仕様
 - ・TPM、PC、サーバ
 - ・インフラストラクチャー
 - ・携帯電話
 - ・ストレージ
 - ・プリンタ
- を公開、または作成中

2.4 Trusted Computing: the “BIG” Picture



2.5 TCG製品・ソリューション

TCG製品		提供機能
検疫ネットワーク		・LAN上PCのソフトウェア構成をチェックし、 <u>不正状態のPCを検出・隔離・治療する</u>
ボリュウム暗号機能	暗号HDD (ハード)	・ <u>HDD自体のボリュウム暗号機能</u> (HDCに暗号機能とセキュア領域を用意、ボリュウム暗号を行う) ⇒ ノートPCが盗難にあっても、ファイルの内容が見れないため、 <u>HDDから情報が漏洩しない</u>
	FDE (ソフト)	・HDのボリュウム暗号を行う(暗号化の手段・専用ハードの有無は問わない) ⇒ ノートPCが盗難にあっても、ファイルの内容が見れないため、 <u>HDDから情報が漏洩しない</u>
トラステッドブート		・IPLからハッシュチェーンを生成、プラットフォーム構成の完全性を保証する ⇒ ウィルスチェックのみでは検出できない <u>ソフトウェアの改変を検知する</u>
デジタル複合機		・電子化されたドキュメントに対するセキュリティ機能 ・ネットワーク利用時のセキュリティ機能



3. 2008年度検討内容

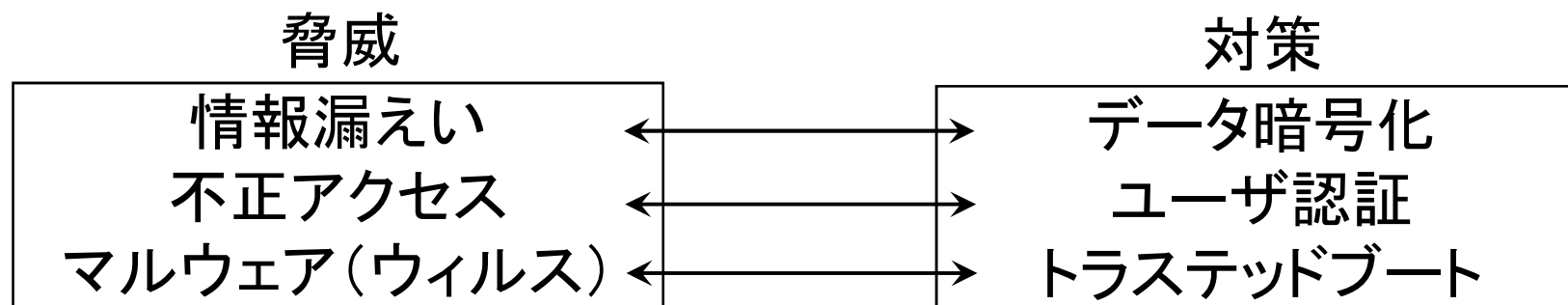
3.1 現状分析:現在のITシステムの利用形態

現在のITシステムの代表的な利用形態

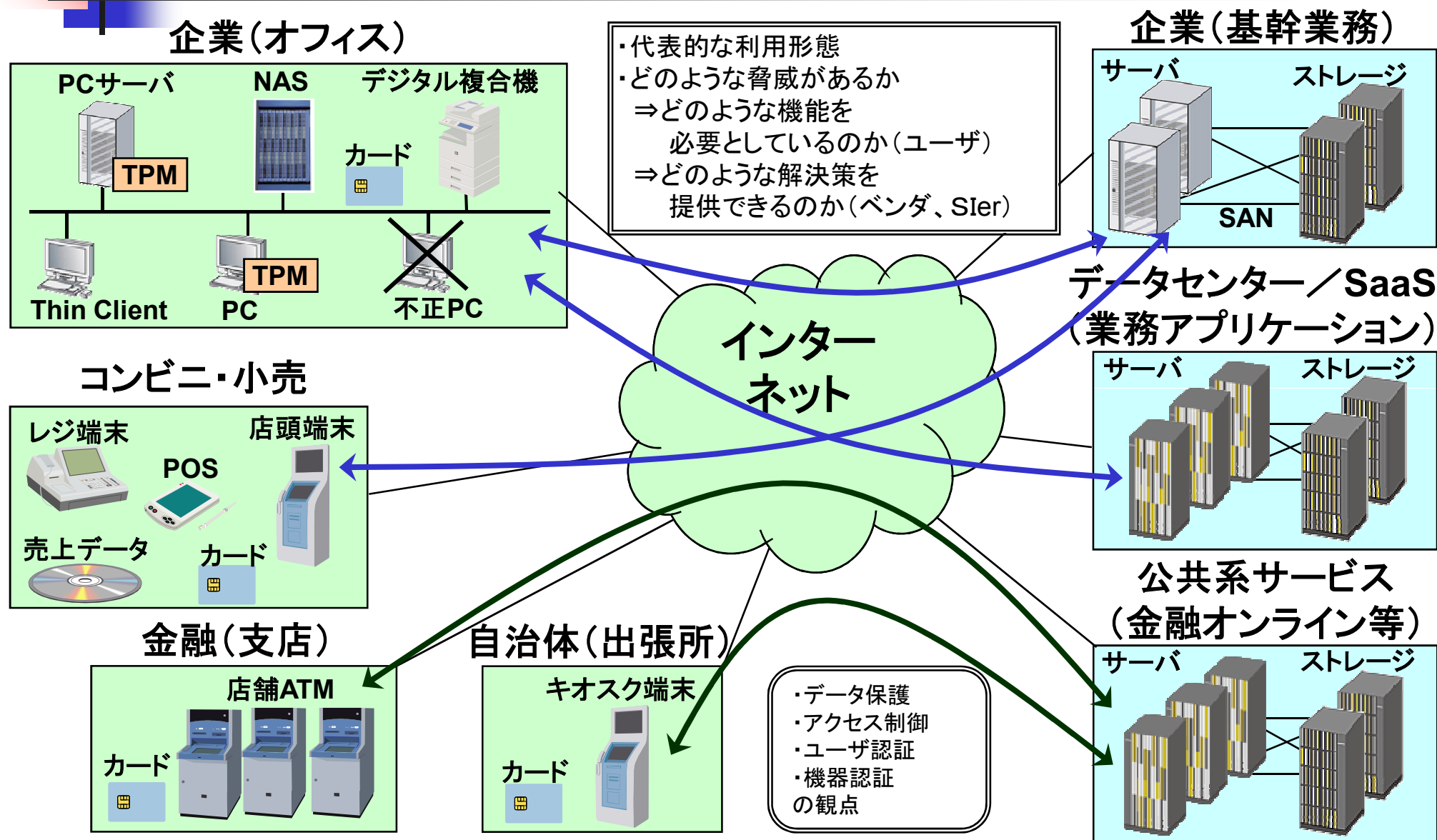
エンタープライズ系(企業ユース)

コンシューマー系(一般ユース)

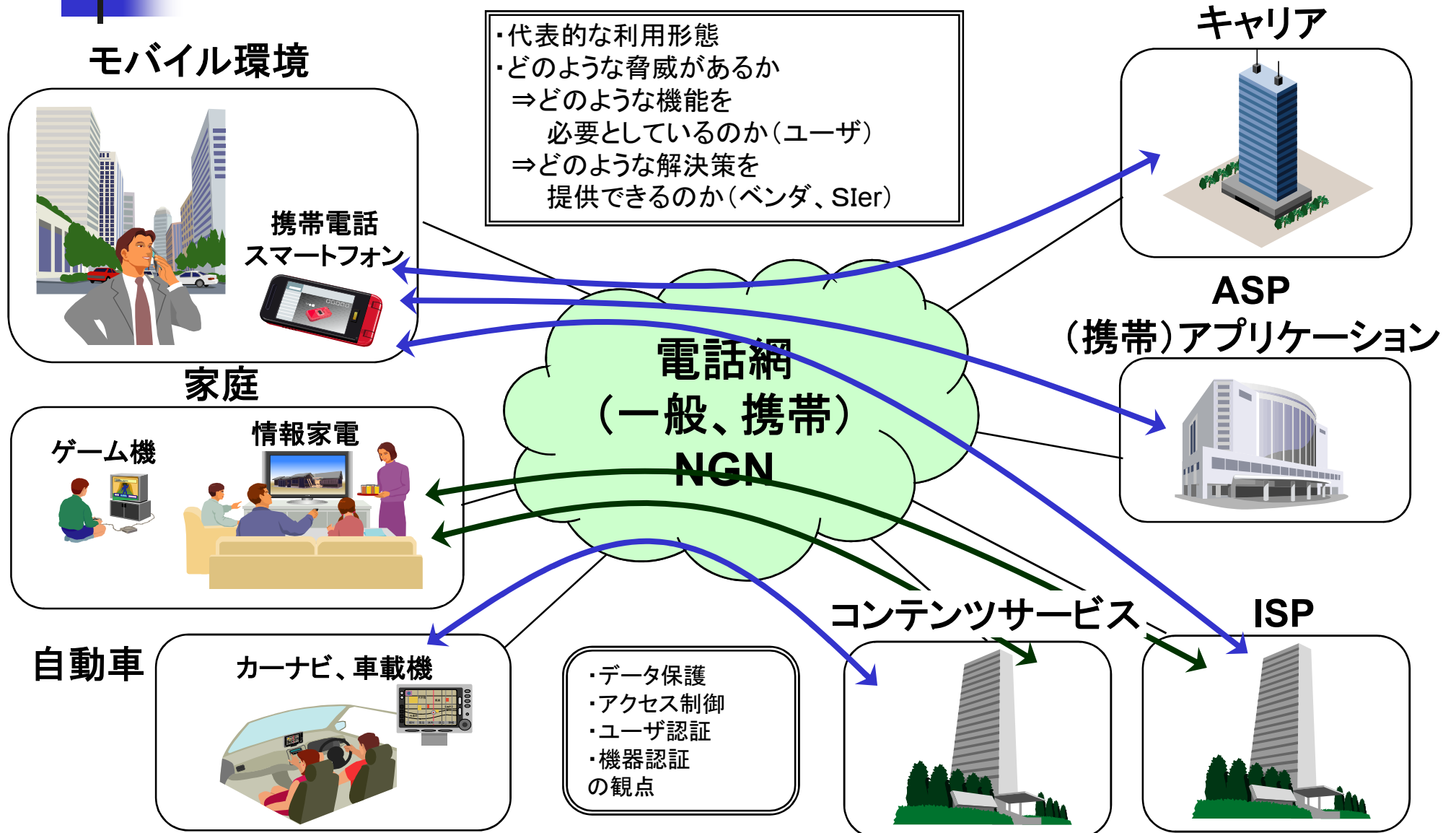
⇒ それぞれの利用環境を眺めると
セキュリティ上の脅威が見えてくる

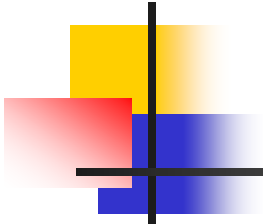


3.2 エンタープライズ系システムの利用形態



3.3 コンシューマー系システムの利用形態





3.4 セキュリティ対策

セキュリティ対策 ⇒ 1. 脅威、2. 構成要素 の2つの切り口

1. 脅威から見た対策

	PC サーバ	ストレージ	デジタル 複合機	ネットワーク 機器	携帯電話	組み込み 機器
データ 漏えい 対策	データ暗号化、ハードディスク暗号					
不正 アクセス 対応	ユーザ認証、機器認証、検疫ネットワーク					
ウィルス マルウェア 対応	アンチウィルス、セキュアブート、トラステッドブート					

TPM(TCG)が提供するセキュリティ対策で、ほぼ全てカバーできる

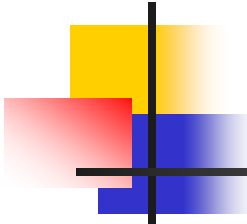
3.5 セキュリティ対策

セキュリティ対策 ⇒ 1. 脅威、2. 構成要素 の2つの切り口

2. 構成要素ごとの対策

	PC サーバ	ストレージ	デジタル 複合機	ネットワーク 機器	携帯電話	組み込み 機器
データ 漏えい 対策						
不正 アクセス 対応						
ウィルス マルウェア 対応						

- ・構成要素ごとに、技術標準・セキュリティ対策あり
- ・全ての構成要素に対して、抜けが無いように



4. 報告書、本日の発表内容について

一般利用者 エンドユーザ向け	情報管理部門向け	開発者、ベンダー向け
目に見える効果 (便利さ、使い勝手)	管理、運用のし易さ コスト	新機能、付加価値 (これまでの問題を解決)

1. 技術、機能の解説

- ・TPMについて
- ・組込システムへの適用
- ・TCG Storage architecture の紹介
- ・デジタル複合機のセキュリティ

2. 開発のための検討材料

- ・TCG IWG仕様における
PKI技術の利用
(TCGにおける機器認証)
- ・開発環境(資料のみ)

3. 新技術・規格の紹介

- ・TCG Mobile仕様とOMTP
- ・PCI-DSS (Payment security)
- ・ICカード: NFCと応用事例(認証デバイス)

4. 導入のための検討材料

- ・鍵管理(資料のみ)