新しいセキュリティパラダイムのビジネス適用

－ファイアウォールのない世界を目指して－

アブストラクト

1. 研究背景

近年、社会基盤を支える IT に対する脅威は遊戯的なものから金銭詐取や経済テロ、脅迫といったより犯罪性の高いものに移行し、また個人情報保護の観点からもセキュリティに対する要求は急速に高まってきている。

しかしながら、現在、多くのクライアント PC で主流であるソフトウェアのみによるセキュリティ対策では、脆弱性が発見されるたびにパッチ適用といった後追いによる対応をしつづけなければシステムの信頼性を維持できないという問題点をかかえている。

このような状況の中、IT インフラに強固なセキュリティ基盤を簡便・正確・安価に提供することを目指して、国際的な標準化団体 TCG(Trusted Computing Group)により仕様が策定され、世界的に市場浸透してきているセキュリティチップ(TPM:Trusted Platform Module)を適用した IT サービスへの期待が高まっている。(図表 1) 当分科会では TPM のビジネス適用に着目し、研究を行なった。

図表 1　TPM チップと搭載 PC

2. 研究課題と研究の進め方

あまり知られていないが、すでにノート PC への TPM 搭載率は高く、2010 年までには 95%近くになると予想されている。TPM の普及率とその信頼性の高さの観点からシステムで活用してしかるべきであるが、必ずしもビジネス適用が浸透しているとは言えない。そこで TPM をセキュリティ基盤とするソリューションを検討し、新しいセキュリティパラダイム提案を研究の目的とした。

研究を行うにあたり、まず始めに解決しなければならない課題を下記と当分科会では考えた。

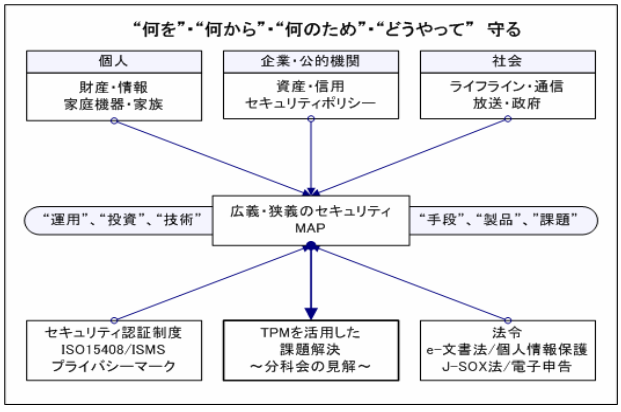
- セキュリティに関する統一的な考え方の指標がない。
- TPM の社会的有用性がアピールできていない。

さらに各企業が対策を講じなければならないビジネス市場での新たな法令・規格・基準への対応・投資の問題に関する調査を行い、ビジネスモデルとしても TPM 搭載の有用性について研究を進めた。

研究手順は以下の通りである。

(1) TPM の機能調査と市場の状況調査
(2) セキュリティベースラインを統一した MAP の作成 (図表 2)
(3) 定量的に安全性を議論するための指標作り
(4) 現状のセキュリティ問題の解決策として、TPM 活用の検討
(5) ビジネス市場を取り巻く、新たな法令対策への TPM 適用の検討
(6) TPM を使用したビジネスモデルの提案
(7) 新しいセキュリティパラダイムの提言

図表 2　本分科会のセキュリティ検討の視点



3. 研究成果

(1) セキュリティＭＡＰ

セキュリティベースラインを統一する資料として、守るべき資産の定義、脅威、組織活動、運用

性の難易度、具体的な製品（ソリューション）を挙げ、対策による効果、現状の問題点調査を行った。また、本分科会のテーマである TPM を現状の問題点の解決策として、どう活用できるかを分科会の見解とした MAP を作成した。

図表 3　セキュリティ MAP

管理資産	脅威	目的	製品	効果	問題	改善策
電子情報 記憶媒体 設備機器 要員 ・	紛失 盗難 ウィルス 改ざん 破壊	漏洩対策 信頼・信用 経営資産 ・ ・	具体的 製品名 ・ ・ ・	守れる対象 ・ ・ ・ ・	守れないもの ・ ・ ・ ・	TPM チップを活用することで新たに守れるもの 高信頼性機器 堅牢な機器 漏洩・改ざん対策

(2) 情報漏洩を阻止するバイオメトリック埋め込みＴＰＭの提案と指標値比較

PC 紛失時の情報漏洩技術対策を検討した結果、現在のセキュリティ対策では不完全と考えた。この事は、連日のように個人情報漏洩事件の報道がなされている中、情報漏洩の有無とは関係なく PC の置き忘れまたは盗難そのものが取り上げられていることからも判る。

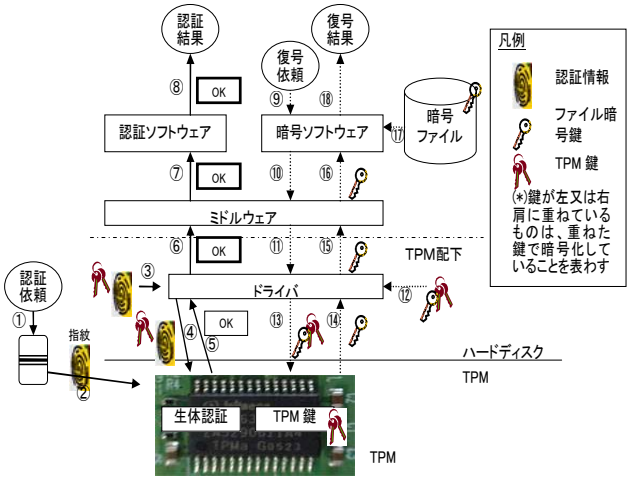
当分科会では、PC が紛失しても情報を守る方法としてバイオメトリック埋め込み TPM 技術の提案行う。(図表 4)

また、当提案の有効性を検証する為に、

・暗号自体が破られたことによる解読
・暗号鍵管理の甘さや運用上の失策による解読
・実装の脆弱性による解読

3 つの視点を加味し、セキュリティ強度を定量的に評価する指標を決め、この指標により、当提案の定量的検証を行った。

図表 4　生体認証を TPM で行う流れと情報の位置



(3) ビジネスモデル提案 ～Ｊ－ＳＯＸも意識して～

実際の運用現場より、「統合監視サービス」、「財務会計 ASP サービス」をモデルケースとして TPM 適用のビジネスモデルを提案した。(図表 5)

① ネットワーク越しでの統合監視サービスにおけるオペレーションの完全な証跡保存による悪意の抑止

② 企業会計における J-SOX 法対応時の問題解決策として「COBIT for SOX」(以下、COBIT) を分析し、TPM を適用することで完全性・正確性・有効性が保たれることを証明した。

これらによって、我々は TPM 適用が非常に有用であると共に、セキュリティの向上と利用者の利便性の向上を図ることができることを確信した。

図表 5 「COBIT」の統制目標に対する TPM 適用 (抜粋)

COBITの統制目標		セキュリティマップとの対応	TPM適用による利点	ASPサービスにおけるユースケース	効果
Ⅲ. サービス提供とサポート(コンピュータ・オペレーションおよびプログラムとデータへのアクセス) 5. システム・セキュリティの保証					
(6)	認証およびアクセス機能の有効性を保つための手続きが存在し、これに従っている。(定期的なパスワード変更など)	電子情報⇒不正アクセス 電子情報⇒人的ミス	本人認証	パスワードの代りに、バイオ認証への移行。バイオ認証データをTPMで管理。	ASPサービス利用時の認証に、TPM＋バイオ認証を利用する。	定期的なパスワード変更などの手続きが不要。
(9)	(必要に応じて)双方の当事者はいずれも取引を否定できないことを担保する統制が存在し、取引の発送または受領の否認防止、発送と受領の証拠を提供するための統制が実施されている。	電子情報⇒改竄 電子情報⇒人的ミス	ロギング	非改竄を標準仕様に基づいた証明可能な、ログ機構により、監査証拠の完全性、正確性、有効性の検証が可能。	連結子会社からのデータ収集の真正性の担保と、個別会計システムとのデータ連携時の正確性を担保するためにTPMを利用する。	親会社への報告した財務データが正しく処理されたことの証明が可能。 個別会計システムからの取得した財務データがすべて取り込まれていることの証明が可能。

4. 提言・まとめ

TPM による相互認証をセキュリティ基盤とする世界は、例えるとすると、互いに隣人同士よく知っており、家に鍵をかけなくても泥棒に入られる恐れがない、一昔前の田舎生活のようなものである。まだまだ課題は多いものの、すべてのネットワーク機器がお互いにお互いを認証しあい、不正な機器はそもそもネットワークに入れない、ファイアウォールのない世界の実現に向けて、当分科会の研究成果が第一歩となれば幸いである。