情報セキュリティ技術の研究開発課題

R&D on Information Security Technology

キーワード 情報セキュリティ技術、システム技術、社会技術、研究開発

１．調査の目的

日進月歩で進歩・変化する情報技術（ＩＴ）は、我が国の主要な社会基盤を形成しつつあり、その影響は、経済、文化、生活など広い範囲に及んでいる。

このような情報技術は、我々の生活に利便性や快適性をもたらしてくれる反面、セキュリティの確保、情報格差の拡大といった問題が顕在化している。

特に近年、インターネットやコンピュータリソースのオープン化、さらにはモバイル通信など新しいメディアの登場により、情報セキュリティ技術もこれに連動して進歩していく必要がある。

本調査研究は、以上のような情報技術の発展動向や社会動向を踏まえて、将来にわたって安全な情報インフラを構築し、国として取り組むべき中長期的な研究開発課題を体系的に明らかにしようとしたものである。

検討に際しては、慶応義塾大学の土居範久教授を主査とする「情報セキュリティ技術に関する研究会」を開催するとともに、内外の有識者へのインタビュー、インターネットを含む文献サーベイなどを行い、未来工学研究所でそれらの結果をとりまとめた。

２．調査研究成果概要

（１）研究開発の現状と課題

情報セキュリティ技術をさらに具体的に分類したものが、表１および表２の情報セキュリティ技術体系である。

我が国における情報セキュリティ技術の研究開発の特徴的な傾向は、以下のようにまとめられる。

○要素技術の研究開発は、産官学において多様な取組みが行われており、中でも暗号技術関連の研究は、我が国は高い実力を示している。

○セキュアネットワークやセキュアソフトウエアなどシステム技術のセキュリティ対策は、全般的に取組みに遅れがある。

○特に、今後の急速な進展が予想されるモバイルネットワークやＶＰＮ、さらには

グリッド・コンピューティングなどの新しい情報技術分野のセキュリティ対策が遅れている。

○要素技術からシステム技術までにわたるレイヤを越えたセキュリティ対策は、ほとんど手付かずの状態である。

○内外の脅威からシステムを防衛する「予防対策」に比して、被害を受けた後の修復や再構築など「事後対策」に関連する研究開発はまだ少ない。

○組織内部からの脅威（インサイダー攻撃）への対策およびそれに関連した技術開発は、現状ではほとんど実施されていない。

○人間や社会とのインターフェースを考慮した社会技術面からのアプローチは、テーマが学際的であること、研究の歴史が浅いこともあり、研究手法自体がまだ確立していない。

○安心して利用できるセキュリティための条件（守秘性や完全性の保持）と、ユーザのいつでも簡単に利用できる条件（利便性や可動性）のバランスをとることが重要である。

（２）研究開発の推進方策

上記の研究開発課題を実現するためには、以下のような推進方策が考えられる。

（１）ソフトウエア分野など新たな研究分野で若手研究者の独創的アイデアの活用

（２）自然科学者（情報系技術者）と人文・社会学者との連携研究チーム編成

（３）俯瞰型（トップダウン型）研究（例；「人にやさしいセキュリティ技術」、「サイバーセキュリティ社会の総合的分析」）

（４）情報セキュリティ技術開発の研究拠点（日本版ＩＩＩＰ）

（５）最新の情報セキュリティ技術導入のための社会実験プログラム

（６）海外研究機関との研究成果交流・ジョイント研究

表1 我が国における情報セキュリティ技術の研究開発概況 (1/2)

技術分類				開発段階			研究開発の方向性の例
大項目	中項目	小項目	具体的内容例	理論	開発	実用	
要素技術	識別・認証技術	1)記憶による方法	ﾊﾟｽﾜｰﾄﾞ、暗証番号等			◎	＞マルチモーダル認証技術 ＞リアルタイム認証技術
		2)持ち物による方法	IDカード、ｽﾏｰﾄｶｰﾄﾞ等		○	◎	＞プライバシー保護への配慮 （プライバシー侵害を不可能にする技術）
		3)生体的特徴による方法 （バイオメトリクス）	指紋・虹彩・声紋・筆跡照合		◎	○	＞容貌による認証 ＞入手・複製困難なバイオメトリクス
	アクセス管理技術	1)アクセス制御技術	ファイアウォール		○	◎	＞インテリジェントファイアウォール ＞高速ファイアウォール ＞ファイアウォールの階層化・セグメンテーション化
		2)不正アクセス検知・追跡技術	侵入検知システム（IDS）		◎	○	＞リアルタイム追跡技術
			ログ管理・解析技術 安全なログ保管技術		○ ○	○	＞ソフトウェアエージェント
		3) コンテンツフィルタリング	フィルタリングソフトウェア		○	○	
	守秘技術	1)暗号技術	共通鍵暗号		○	◎	＞超高速暗号技術 ＞楕円曲線暗号 ＞情報論的に安全な方式(量子暗号等) ＞暗号と人のインターフェース ＞暗号モジュール化技術
			公開鍵暗号（RSA） 次世代公開鍵（AES）		○ ◎	◎	
		2)暗号安全性評価技術	差分解読・線形解読他		○	○	
		3)通信秘匿技術	暗号鍵回復技術	○	◎ ○	○	＞暗号ブレイク対応技術 ＞暗号解読技術 （暗号技術の悪用への対応） ＞暗号強度評価技術
	完全性保持技術	1)電子透かし技術	共通鍵的な電子透かし		◎		＞公開鍵的な電子透かし
		2)電子署名技術	デジタル署名・電子捺印		○	○	＞署名のヒューマンインターフェース

（略号）AES：Advanced Encription Standard

表２ 我が国における情報セキュリティ技術の研究開発概況(2/2)

技術分類				開発段階			研究開発の方向性の例
大項目	中項目	小項目	具体的内容例	理論	開発	実用	
システム技術	耐力保持技術	1) ウィルス対策技術	ウィルスワクチン		○	◎	＞免疫学的知見の応用
			ウィルス情報自動配信システム		○	◎	＞ウィルス伝播防止技術
	セキュアネットワーク	1) バーチャルプライベートネットワーク（VPN）	セキュアなIP－VPN技術（IPSec、L2TP等）		◎	○	＞高速ＶＰＮ分離技術 ＞ポリシー自動学習アルゴリズム
		2) セキュアなワイヤレスネットワーク	WTLSなど		◎	○	＞Wireless LANs、Home Networks、Wearable Networksのセキュリティ保証
		3) セキュアなグリッド・コンピューティング	ワンステップ認証技術		○		
			最適資源配分		○	○	
	セキュアなソフトウェア	1) セキュアＯＳ	セキュリティ・カーネル	○	○		＞次世代マイクロカーネル
		2) セキュアな言語					
		3) セキュアなアプリケーション					
		4) モバイル ソフトウェアのセキュリティ					＞モバイルソフトウェアの信頼性保証技術
	相互接続性保証	1) システム・インタビリティ	PKI（公開鍵基盤）		○	○	
			複数認証機関の相互運用性の確保		○	○	
	リカバリ・システム	1) 被害予測システム	ウィルス流行警報システム		○		＞複数ＤＢからの情報共有・侵入警報・自動回避システム
			影響シミュレーションモデル	○	○		＞被害限定プログラム
		2) 修復システム	機能代替・切替システム		○		＞自動修復システム
			内部システムセグメント化		○		
			セキュリティホール自動検出		○		
	システムセキュリティ評価	1) システム評価技術	脆弱性・機能強度・対策分析		○	○	＞異分野システムの相互連関分析 ＞セキュアなソフトウエア・アーキテクチャ ＞組み合わせシステムの強度評価
		2) リスクアセスメント技術	コスト・ベネフィット分析	○	○		＞セキュリティ意志決定支援システム
社会技術	個人レベル	1) ハッカー・クラッカーの行動科学的分析	ハッカーの社会心理学的分析	○			＞クラッカーの行動パタン分析
		2) セキュリティユーザインタフェース	安心感の持てるセキュリティシステム		○		
	集団レベル	1) セキュリティとプライバシーの両立	パーソナル情報機器のプライバシー対策	○	○		＞次世代モバイル環境への対応 ＞情報倫理についてのコンセンサス形成手法
		2) 電子コミュニティでの信頼・リスク認知	ＥＣにおける信頼形成要因分析	○			
		3) 電子的コミュニケーションプロセス分析	「噂」の伝播メカニズム分析	○	○		＞チェーンメールのルール解析
		4) 新たな社会的格差の発生	新たな情報格差の発生	○			＞情報リテラシー対策（教育・研修）
	社会レベル～国際レベル	1) セキュリティ相互依存分析	複合システム連関分析	○	○		＞ネットワーク・カタストロフィモデル
			ヘテロなセキュリティシステム	○	○		＞冗長性のある社会システム構築
		2) 総合安全保障としての情報セキュリティ	セキュリティ技術の地政学的分析	○	○		＞総合安全保障における暗号技術の役割
		3) グローバルなＥＣ環境の展開	国際e-ビジネスのセキュリティ対策	○			

（略号）VPN:Virtual Private Network　IPSec:IP Security Protocol　L2TP:Layer 2 Tunnelling Protocol　WTLS:Wireless Transport Layer Security

（注）Blue Tooth:PC，携帯電話，PDAなどをワイヤレスLAN経由でネットワークに接続するためのハードウェア仕様。30～100フィート（9～30メートル）の見通し距離でデータの送受信が