補足資料1

技術戦略専門委員会（第16回会合）における委員意見の整理

重点化して推進すべき研究対象分野（委員ご意見の整理）

攻撃者

攻撃の解析

- 攻撃者を特定する技術
- マルウェアの挙動分析技術
- DoSアタックの影響分析技術
- Spamを中継しているISPの判定技術など

情報システム

・ソフト
・ハード
（ネットワーク）

ディペンダブルな情報システムの開発

- 組み込みデバイスのセキュアなソフトウェア更新技術
- ディペンダブルなクラウドの構成技術
- 無線アドホックネットワークのセキュアな利用技術など

利用者

利用者の対応力（マネジメント技術等）

- ICT環境の変化に対応した情報セキュリティ指針
- セキュリティ投資に対す効果の定量化技術
- 社会科学的側面を考慮したマネジメント技術など

重点化分野に関する主なご意見（1）

【攻撃の解析】

- 海外からのサイバー攻撃は深刻な状況であり、将来を見据えた体系的な研究開発（経済合理性に基づく攻撃者の行動分析、ディシジョンツリー分析等を用いてトータルなリスク低減を図る仕組みなど）が必要。
- 攻撃者が有利な状況を変えるためには「敵の全貌」を知ることが不可欠。そこで、悪意のある攻撃者だけでなく、意識的あるいは無意識のうちに悪者に協力している者を分析対象に加えて、彼らのコストを増大させる方法を整えることが必要。
- コストの大きさは罰則と関係するため、広義のトレースバック技術（攻撃者を特定する技術、マルウェアの挙動分析技術、Spamを中継しているISPの判定技術など）の研究を推進すべき。
- 国家機密の情報漏えい対策など、国家存立の基盤の保持に係わるような研究開発は、政府が率先して研究開発を行なうべき。

No.	研究対象分野(研究開発課題)	概要(キーワード)
1	トレースバックのための国際観測拠点の設置とデータ解析	広義トレースバック（発信元の特定だけでなく、マルウェアの挙動分析、DoSアタックの影響分析、Spamを中継するISPの判定など）のためのデータ解析、国際的な観測データ収集スキームの構築
2	高度に重要な情報の管理技術	機微情報の管理技術及び重要情報の漏えい事案の対処（トレースバック等）方法
3	悪意の利用者のゲーム理論	攻撃者及び協力者（無意識の協力者を含む）の行動要素（悪事への投資規模と期待する効果など）の分析、悪意の利用者の全貌把握（比較制度分析のような、全体の見取り図を知るためのモデル手法）

重点化分野に関する主なご意見（2）

【ディペンダブルな情報システムの開発】

- 社会インフラの安全な運用の一翼を担う情報システムは、新たな攻撃手法の先を読んだディペンダブルな情報システムとすべき。
- 次世代の社会システムは、リアルとサイバーの結びつきが今まで以上に強まったシステムになると想定される。この社会システムを構成するセンサーやアクチュエータなどの組込みデバイスには高い信頼性が求められるため、組込み系のディペンダブルなソフトウェア開発技術を確立すべき。
- ディペンダブルなソフトウェア開発を行なうためには、ソフトウェアの機能安全を計測する技術、機能安全を保証する枠組み、ネットワークで安全にソフトウェアの更新をするフレームワーク等の研究開発を推進すべき。
- 国際的な相場観や法制度が係わるクラウドコンピューティングのセキュリティは、政府が率先して検討すべき。

No.	研究対象分野(研究開発課題)	概要(キーワード)
1	ディペンダブル情報システムの構築	ディペンダブル（可用性だけでなく、セキュリティやプライバシー面の信頼性を合わせ持つ）ソフトウェア開発技術、ソフトウェアの柔軟性・拡張性とディペンダブルを両立するセキュアなソフトウェア更新フレームワーク
2	ネットワーク化された組み込みデバイス(センサー、アクチュエータ)のセキュリティパッチ適応スキーム	組み込みデバイスに対する統一的かつ安定的にセキュリティ向上の機能（ソフトウェア）を安全に書き換える技術及びフレームワーク
3	組み込みシステムにおけるセキュリティ	組み込みシステムの脆弱性対処としてのソフトウェア更新フレームワーク
4	無線ブロードバンド環境におけるセキュリティ技術	端末相互間のリンクが不確実な無線アドホックネットワークのセキュアな利用技術及び、無線周波数帯の効率的な利用技術
5	クラウド化、大規模化に伴うセキュリティ	セキュリティ及びプライバシー面の信頼性を備えたクラウドの構成方法、クラウドセキュリティの可視化

重点化分野に関する主なご意見（3）

【利用者の対応力（マネジメント技術等）】

- 利用者側の組織のマネージメントにおいては、人の心理や組織の感情を考慮することが必要であり、社会科学的な側面（人的・組織的な側面）を考慮したマネジメント技術、情報セキュリティに係わる人のモチベーションを高める仕組みを検討すべき。
- 経営層に情報セキュリティ対策を理解させるうえで、情報セキュリティの指針を示すことや、情報セキュリティ投資に対する効果を定量化する仕組みが必要。
- 国家存続に係わるような情報漏えいが発生したときの対処方策（文書が漏出することも想定し、予め公開／非公開を部分的にコントロールできる技術的な対策を講じておくことなど）を検討しておくべき。
- 市場参加者に適切なインセンティブを与えることは、情報セキュリティの研究開発を推進するうえでも重要なポイント。

No	研究対象分野(研究開発課題)	概要(キーワード)
1	レジリエントな高信頼性組織体制の構築	セキュリティ・インシデントのコーディネーション（意思疎通、情報共有のあり方）体制、社会科学的な側面（人的・組織的な側面）を考慮したマネジメント技術
2	BCM (Business Continuity Management)における情報セキュリティ対応策の策定	BCPのベストプラクティス（脅威に対する事前対策、脅威が顕在化した場合の対応、脅威を排除し正常化するベストプラクティスなど）の明示化
3	新しい社会システムにおける情報セキュリティのあり方	ICT環境の変化（クラウドコンピューティング、利用端末の多様化、個人情報などの社会意識問題など）に対応した情報セキュリティ指針の策定
4	文書中の重要事項の公開/非公開手法	文書が漏出することも想定し、例えば文書ファイルを多重レイヤー構造として、重要文書中の重要事項のレイヤーを暗号化しておくなど、公開／非公開を部分的にコントロールできる技術
5	ROSI (Return On Security Investment)の可視化	セキュリティ投資対効果の定量化及び標準策定

戦略に盛り込むべきことに関するご意見

- 「日本は世界で一番安全なネット環境である」といった分り易いメッセージが必要。
- 情報セキュリティ（個人情報の匿名化など）を確保することによって、新しい価値やサービスを創出できる（イノベーションを創造する）ことを主張すべき。
- イノベーションの創造を促進するためには、現場の情報共有を推進することが必要であり、これにはトップが責任（情報漏えい等の責任）を適切にシェアすることが必要。
- 研究開発・実用化・普及の各段階において、触媒の役割を果たす仕掛け（インセンティブの付与）が必要。
- ディペンダブルなソフトウェアの作り方の指針やテスト方法について、国が責任分解の基準を定めるべき（民間に任せると、過剰な対応を取る可能性がある）。
- サイバー攻撃を仕掛けて来る「ならず者」を追いつめるためには国際連携が必要。