補足資料2

欧米調査に基づく重点分野候補

欧米調査に基づく重点分野候補

研究カテゴリ	重点分野	選定理由
ネットワーク観測防御技術	内部の脅威検知・緩和	FBI/CSI survey では、情報セキュリティの分野の被害のうち70%以上が内部犯行によるといわれている。システムの大規模化、多様化により、内部犯行等の脅威が検知しにくくなっている状況下で、内部脅威の検知に対する要請が高まっている。
セキュアネットワーク構築技術	次世代インターネットインフラのセキュリティ確保	次世代インターネットインフラに関してはその影響の大きさから、広範囲の技術分野における研究開発が必要となる。技術移行、共存や異種システムの相互運用性やスケーラビリティに関する技術が求められる。
セキュアシステム構築技術	セキュア・ソフトウェアエンジニアリング	コンパイラ、ライブラリなど全ライフサイクルにおいて機密性、完全性、可用性の認証が求められている。プログラミング言語、コード分析等のベストプラクティスの組合せが重要である。
	高信頼・証明可能なセキュアシステムとアーキテクチャ	重要インフラ、政府システム、軍事システムでは、高信頼アーキテクチャを実現させるための形式手法やエビデンスベースの手法の応用が求められる。
プライバシー保護技術	サービス・プライバシー保護	ITインフラにおけるプライバシー情報の利用が進展により、リスクが高まっている。プライバシー保護のための原則の開発が求められている。
	信頼できる組込み計算	組込みシステムは多くのプラットフォームが存在し、複雑化している。汎用コンピュータ分野のセキュリティ技術の適用が求められる。
コンテンツセキュリティ技術（データセキュリティ技術）	フォレンジック、トレースバック及びアトリビューション技術	法執行プロセスや手続きはIT技術の進歩に対応していないため、それらに対応したフォレンジック技術が求められている。
セキュリティ評価・マネジメント	敵対行動の予測	敵対行動の予測に基づく対策が効果的である。Red Teaming技術によるメトリクスなどを確立することが求められる。
	メトリクスとリスクベース意思決定	情報セキュリティに関するメトリクス、定量化が未成熟であるために、適切な対策の意思決定が困難な状況である。メトリクスの開発とリスクベースの意思決定が求められている。
	重要インフラ、ネットワーク、情報と制御システムマネジメント	SCADAシステムのリスク評価、コスト見積りに基づく適切な対策レベルの実施が求められている。

【参考資料】予算面における優先分野の推移
（NITRD CSIA予算資料で示された優先分野）

2007

CSIAにおける基盤・応用研究
- ネットワークセキュリティ
- ディペンダブルシステム
- 状況認識・対応
- セキュア分散システム

情報インフラ防護

R&Dのインフラ整備
- テストベッド
- 各種ツール
- 標準
- データ収集・共有

民間支援・技術移行

大分類
- 個別分野
- 個別分野

2008

機能的サイバーセキュリティと情報保証
- 大規模システム防護
- 状況認識アクセス
- 管理・権限・トラストマネジメント
- SW保護

インフラストラクチャ及び領域特化型セキュリティ
- DNSSEC
- セキュアルーティング
- セキュアプロセス管理
- ワイヤレスセキュリティ
- 異種トラフィック　etc

サイバーセキュリティと情報保証の評価
- 脆弱性・マリシャスコード検知
- 各種標準・メトリクス整備
- 自動照合・検証システム

科学的基盤
- セキュアOS
- 暗号化、マルチレベルセキュリティ
- セキュアSWエンジニアリング　etc

2009

機能的サイバーセキュリティと情報保証（短期的）
- OS、暗号化、ID管理
- 状況認識・対応
- オペレーション保証　etc

インフラ及び科学的基盤整備（長期的）
- ポリシベースのセキュリティマネジメント
- 複合NWのセキュリティ
- SWの計算基盤
- 次世代情報システムの開発・保証
- 複雑システムに関する実験的研究etc

社会的問題
- プライバシー
- ITリスクの意識向上
- 連邦政府システムのセキュリティのあり方
- 安全設計、実装、管理、オペレーション
- 次世代のサイバーセキュリティ人材育成

2010

基盤
- サイバーセキュリティ基盤
- 信頼性、セキュリティ等の新たなモデル・ロジック
- Trustworthy なシステム
- セキュアSWエンジニアリング
- 暗号技術、量子暗号　etc.

応用セキュリティ、インフラセキュリティ
- セキュアバーチャル基盤
- 情報共有の保証
- 複合NWのセキュリティ
- ID管理
- セキュリティの自動化
- セキュアプロトコル
- 脆弱性検知、軽減

状況認識・対応
- サイバー攻撃対応
- 高脅威環境におけるオペレーション保証
- セキュリティ事象可視化
- コグニティブセキュリティ

R&Dのインフラ整備
- サイバーセキュリティ実証実験のテストベッドやツール

2011

基盤
- サイバーセキュリティ基盤
- 信頼性、セキュリティ等の新たなモデル・ロジック
- Trustworthy なシステム
- セキュアSWエンジニアリング
- 暗号技術、量子暗号　etc.

応用セキュリティ、インフラセキュリティ
- セキュアバーチャル基盤
- 情報共有の保証
- モバイルセキュリティ
- ID管理
- セキュリティの自動化
- セキュアプロトコル
- 脆弱性検知、軽減
- クラウド
- ヘルスIT
- スマートグリッド

ミッション保証
- あらゆる危機状況で組織ミッションを保証する活動･プロセス
- サイバー戦争防衛

R&Dのインフラ整備
- サイバーセキュリティ実証実験のテストベッドやツール

NITRD：Fed Plan For Cyber Security & Info. Assurance R&Dが強く反映されている。

2012年予算にはNITRD:Cybersecurity Game-Change Research & Development Recommendationsで示された方針が反映されるとしている。

NITRD CSIA予算推移（2006-2011）

NITRD: http://www.nitrd.gov/pubs/bluebooks/index.aspx

【参考資料】FP7におけるセキュリティ関連分野

Challenge 1: Pervasive and Trusted Network and Service Infrastructuresにおいて、セキュリティに直接係わる1～2テーマがObjectiveとしてあげられている。

Challenge 1: Pervasive and Trusted Network and Service Infrastructures

セキュリティ関連分野	総予算	募集テーマ
セキュアで信頼できるインフラ Secure, dependable and trusted Infrastructures (Objective ICT-2007.1.4)	90百万ユーロ	・ネットワークインフラにおけるセキュリティと耐障害性 ・動的・再構成可能なサービスアーキテクチャのセキュリティ及び信頼性 ・トラステッドコンピューティングインフラストラクチャ ・アイデンティティマネジメント及びプライバシー向上ツール ・ロードマップ、標準、メトリクス策定 計23プロジェクトが採択、2010年末で終了。
重要インフラ防護 Critical Infrastructure Protection (Objective ICT-2007.1.7)	40百万ユーロ	・相互接続した交通網またエネルギー網におけるリスクアセスメントと事業継続 ・訓練のためのモデリングとシミュレーション ・相互に接続した交通網またエネルギーインフラの監視における最適化された状況認識 ・重要インフラで発生した危機への初動におけるICTのサポート 計9プロジェクトが採択、2010年末で終了。
Trustworthy ICT (Objective ICT-2009.1.4)	80百万ユーロ	・Trustworthyなネットワークインフラ ・Trustworthyなサービスワークインフラ ・Trustworthy ICTのための技術及びツール 現在実施中。プロジェクト情報は未だ公開されていない。
Trustworthy ICT (Objective ICT-2011.1.4)	80百万ユーロ	・ヘテロジニアスに接続されたサービスとコンピュータ環境 ・信頼性、eIdentity、プライバシーマネジメントインフラ ・データポリシー、ガバナンス 、社会経済的エコシステム ・ネットワーク形成、コーディネーション活動 現在公表されているICT Work Programme 2011-12 において実施予定。

J-BILAT（日本のFP7 窓口）:http://www.j-bilat.eu/documents/seminar/4/presentation_ti.pdf
EU/FP7:http://cordis.europa.eu/fp7/ict/security/fp7_en.htm