資料７

将来予測に関する委員ご意見

2【高齢者、社会的弱者への対応】

2［ ３ ］高齢者や初心者用に開発された基本的機能のみのパソコン
3［3－5］社会的弱者に配慮した情報セキュリティ技術

4【開発支援／開発環境標準化】

4［ ３ ］セキュリティの作り込みによる次世代製品の国際競争力の強化
5［3－5］ソフトウェア開発のありかた　→　低コストな形式手法
6［5-10］IT サービスシステムのオートメーション化

7【セキュリティ対策の要件、リスクの評価・可視化】

7［ ３ ］社会システムにおける IC カードセキュリティの影響
8［ ３ ］IT 社会システムにおけるプライバシ保護技術
9［3－5］市場・ビジネス環境の変化への対応速度の向上
10［ ５ ］セキュリティ対策の国内統一フレームワークの構築

11【IT インフラ】

11［3－5］SaaS の高度化
12［3－5］電化製品のネットワーク化
13［ ５ ］クラウドコンピューティングの次の利用形態
15［5-10］大規模環境ネットワーク
16［5-10］ＰＣグリッド上での仮想サーバ（物理サーバレスの環境）

17【将来技術像】

17［ ３ ］情報セキュリティ分野の情報大爆発への対応（“情報セキュリティ大航海”システム）
18［3－5］セキュリティパッチ
19［ ５ ］マルウェアフリーを実現するコンピューティング環境
20［１０］情報のポータビリティ、リロケータビリティ

21【将来サービス像／社会像】

21［ ３ ］携帯電話の将来利用イメージ
22［3－5］ネットワークの高速化に伴う個人、企業データの集中管理
23［ ５ ］ヒューマノイドハニーポット
24［5-10］高度道路交通システム（ITS: Intelligent Transportation System）とセキュリティ事象を含む事故への対応
25［5-10］意図や悪意を測る
26［5-10］社会サービスへの応用
27［5-10］さまざまな分野における電子化・ネット化と脅威分析
28［5-10］個人情報プロファイルの安全な集中管理・提供
29［5-10］オンライン取引における個人認証のしくみ
30［１０］社会の変移
31［１０］交通機関の電子制御化

【高齢者、社会的弱者への対応】

磯村委員

対象・領域	将来ビジョン（ 製品　サービス ビジネス　ライフスタイル ） 技術像（　　） その他（　　）
予測時期	３年後　５年後　１０年後
記述の対象	高齢者や初心者用に開発された基本的機能のみのパソコン
予測内容	情報弱者と言われ、情報化のメリットを体験できない層に向け、例えば基本的に必要な情報を入手し、発信するだけの機能でも、使いやすさ、覚えやすさを最優先にしたパソコン。セキュリティ対策、バージョンアップなども、登録のみで自動的に行われ、製造元、あるいはサービス提供先が使用者の補助、援助をする。（携帯電話での類似思考商品あり） 商品の存在と広報、指導によって情報弱者といわれる層を出来るだけ少なくする。
予測を実現するために必要とされる技術	おそらく技術的には可能と思われるが、コストや営業的観点から、また製品に対する責任の考え方から、実用化されていないのではないかと思われる。
情報セキュリティ技術上の課題（または、研究テーマ）	一般には利用者の責任とされるセキュリティ対策を、製品に付与し、製品、あるいはサービス提供側ができるだけ負担する。それらが登録等で自動的に行われる際のセキュリティ対策がどこまでできるのかわからないが、限界があれば商品の使用に対する指導の中で補助していく。
備考	

【高齢者、社会的弱者への対応】

山田委員

対象・領域	将来ビジョン（ 製品　サービス　ビジネス　ライフスタイル ） 技術像（　　）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	社会的弱者に配慮した情報セキュリティ技術
予測内容	社会的弱者としての非健常者や感覚の衰えた高齢者に配慮した IT 社会、セキュリティ対策が今後ますます必要になってくる。
予測を実現するために必要とされる技術	技術開発要素は高度ではなく、既にある技術の標準化を図ることが重要。 現在普及が広がりつつあるバイトメトリクス認証（指紋、静脈等）は、四肢障害、高齢者になると困難な場面や認識率が低下するケースがあり、これらに対応する技術やデータの蓄積が必要。
情報セキュリティ技術上の課題（または、研究テーマ）	（１）バイオメトリクス認証のためのデータ蓄積については、ドイツと韓国が進行。ただし高齢者や非健常者については、蓄積されていない模様。バイオメトリクス認証・評価技術の開発（認証方式、生体情報の劣化を想定した認証・評価方式)、データの蓄積（ﾃﾞｰﾀﾍﾞｰｽ化）などを行う。 （２）アクセシビリティは、技術の開発よりむしろ標準化の推進が必要。
備考	・我が国は、世界で最も高齢化が進んでいる。(平均寿命は日本 82 才で世界１位。ドイツ 79、アメリカ 78、韓国 76) ・アクセシビリティのうち、視聴覚・四肢・発声等の低下や障害へのパソコン対応は、一部の民間企業で、既に活動が行われつつある。認知症状 （例）MATvp（Microsoft Assistive Technology　Vendor Program）

【開発支援／開発環境標準化】

山田委員

対象・領域	将来ビジョン（ 製品 サービス ビジネス ライフスタイル ） 技術像（セキュアな製品開発） その他（ ）
予測時期	３年後 ５年後 １０年後
記述の対象	セキュリティの作り込みによる次世代製品の国際競争力の強化
予測内容	3～5 年後には、デジタル家電等のデバイスを通じてインターネットを利用する人口が、無視できない割合となるものと推測。これらのデバイスがインターネットに接続されることで、PC が直面した、セキュリティ上の脅威や問題に直面することが予想。自動的に設計→製造段階でのセキュリティの確保が大きな課題となる。
予測を実現するために必要とされる技術	**「セキュアな開発手法の定着（セキュア開発の現場力の確立・向上）」** 製品のセキュリティの作り込みについては、様々な開発技法が提案されているが、現場レベルで利用可能なものはない。 （加えて、セキュア開発を担当する技術者は極めて少数であり、また各企業に分散しているため、情報交換や議論を通じた現場力の向上をはかる事が難しい。） 現場でのセキュアな開発手法を定着させるためには、以下のようなマネジメント的な（ソフト的な）開発技術が必要。 ・そもそもなにが問題となっているかを明らかにする ・必要とされる開発手法や、その周辺の手法・技術を開発する ・それらの手法や技術の普及と定着を図る
情報セキュリティ技術上の課題（または、研究テーマ）	**「製品ライフサイクルを見据えた、セキュリティの組み込み」** コーディングレベルの規約などのセキュリティ開発技術は提案されているが、経営的な視点を含んだ製品ライフサイクル全般を見据えた手法は提案されておらず、そのような手法を研究する。このような研究テーマは、理論的な面に加えて、ケーススタディを積み重ねないと確立できない。 現場力の確立・向上のため、多くの企業の開発者の参画により、具体的な製品開発の現場に即した手法の開発実証が不可欠であり、プロジェクト形成と実施においてはこれがキーとなる。
備考	日本製品が高いセキュリティレベルを持つことができれば、従来からの品質に対するイメージとあいまって、日本製品のブランディングと国際競争力を更に高めることが可能。

【開発支援／開発環境標準化】

松並委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	ソフトウェア開発のありかた　→　低コストな形式手法
予測内容	**　ソフトウェアの低価格化が進む。品質悪化が深刻な社会問題となる。品質を技術により解決すべく、「形式手法によるソフトウェア開発技術」が重要技術となる。形式手法は高度な設計手法であるため、同時に「形式手法の人材育成」も重要なテーマとなる。** **　ただし現実的なコスト範囲内で実施可能な形式手法である必要がある。そのためには完璧な品質までは必要無く、セキュリティ脆弱性と重大な欠陥を防ぐことができれば十分（エンドユーザーが納得できてビジネスも成立するバランス）である。（低コストなまま完璧な品質となってしまうのは大歓迎。）**
予測を実現するために必要とされる技術	・セキュリティ脆弱性と重大な欠陥が何なのか？コスト削減してよい線引きライン ・現実的なコスト範囲内で実現可能なソフトウェア開発の形式手法。おそらくソフトウェアの要件・設計の形式記述手法と、そのセキュリティ観点による自動レビュー技術（要件・設計の自動検査技術）。 ・自然言語→形式記述言語へのある程度の自動変換技術。目視レビューによる確認が必要でもよい。
情報セキュリティ技術上の課題（または、研究テーマ）	・人材育成／教育を効率よく実現する手法の研究
備考	

【開発支援／開発環境標準化】

加藤委員

対象・領域	(将来ビジョン)（ 製品 サービス ビジネス ライフスタイル ） 技術像（ ） その他（ ）
予測時期	３年後 (５年後) １０年後
記述の対象	IT サービスシステムのオートメーション化
予測内容	**現在一般的に IT サービスを提供するためのシステムは要件定義から運用にいたるほぼすべての業務を人的リソースに頼っている状態が続いている（産業革命前の家内制手工業状態）。IT システムは年々複雑化、巨大化しており、システムライフサイクル全般において、機械による支援が不可欠となりつつある。今後様々な IT システムがコンポーネント化され、自動制御されることで低コストかつ迅速なサービス提供ができるようになる。（単純なサービス化は小回りが効かない。柔軟に、迅速に、低コストでシステムを組むことができるようになることで国際的にも競争力を付けたい。）**
予測を実現するために必要とされる技術	・IT システムの標準化（部品化） ・IT システムの設計自動化、構成自動化技術 ・IT システムの障害自動復旧技術（免疫、治癒能力）
情報セキュリティ技術上の課題（または、研究テーマ）	・ 機能不備によるシステムの暴走を止める手段が必要 ・ 障害自動復旧を阻止するような攻撃への対処
備考	標準化、自動化による IT 業界の産業革命が必要。不完全な製品のバグ出しが我々の仕事ではないし、機械に振り回されるのもおかしい。仕事を右から左へ移しても何の改善もない。機械を使うことで作る人も使う人も、みんなが楽できて初めて技術は進歩したと言えるのでは！？

【セキュリティ対策の要件、リスクの評価・可視化】

山田委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	[３年後]　５年後　　１０年後
記述の対象	社会システムにおける IC カードセキュリティの影響
予測内容	社会システムの複数の領域において、多くのシステム（金融、交通インフラ、流通など）が連携し、その媒体として IC カード（モバイル端末などのチップを含む）が利用されている。海外では、類似 IC カードのセキュリティへの攻撃技術の進歩による社会システムへの影響を不安視される事例も発生している（ロンドン、ボストンの地下鉄）。国内においても、IC カードを利用するシステムに起因するトラブルも発生した（JR の例）。 このような現状において、IC カードのセキュリティが全体システムへ及ぼす影響、連携システム間の関連を評価し、社会システム全体のセキュリティを維持するための要件を抽出することが重要である。
予測を実現するために必要とされる技術	① 個別システムのセキュリティ（例：IC カード）と社会全体システムのセキュリティについての連関的な相互関係を評価する技術 ② セキュリティを維持するための IC カード、鍵管理システム ③ 利用者登録、情報管理のためのアイデンティティ管理システム ④ セキュリティブリーチ(＝抜け穴)が発生した場合の、利用者、経営者の反応計測技術（集団行動・個別行動などの行動科学に関するシステム） ⑤ ブリーチの発生を統計的に予測する技術（統計的リスク解析技術） ⑥ 実際にブリーチが発生した場合における危機管理技術
情報セキュリティ技術上の課題（または、研究テーマ）	研究テーマは、上記①～⑥に重複する。 課題としては、協力企業の個別技術の開示が必要となること、市場における経済的な影響も、①において考慮する必要がある可能性があるから、経済分野の専門家、また、④においては社会心理学・行動学の専門家の参画、⑥については、実証的研究が不可欠である。
備考	（カードだけの問題ではないが、）社会的なインフラとなってしまっているカード等のセキュリティブリーチ情報を、専門家等の報告により政府等が認知した際に、その情報そのものをどのように扱うか、という課題がある。不用意な公表は社会の混乱を招く。（欧米の地下鉄のケースでは、司法当局等により、ブリーチ情報の発表が差し止められた。）しかしその脅威が現実に事故につながった場合には、政府等は知っていたのに何も対処しなかったのかと、一般国民やユーザーから批判されてしまうだろう。社会への公表の方法を含めた行政実務的な対処方針、対策の確立が肝要。

【セキュリティ対策の要件、リスクの評価・可視化】

山田委員

対象・領域	将来ビジョン（　製品　[サービス]　ビジネス　[ライフスタイル]　） 技術像（　　）　　その他（　　）
予測時期	[3年後]　　5年後　　１０年後
記述の対象	IT 社会システムにおけるプライバシ保護技術
予測内容	検索ツール、ストリートビューなどの多くの情報提供ツールが誰でも利用可能であり、おそらく膨大な個人に関する情報がネットワーク上でやりとりされている。利用者は、本人が意識することなく本人の情報の断片をネットワーク上へ投入する一方で、このようなデータを収集し、本人の属性情報を関連づけ、その特性を特定できるような技術の実現が容易に予測できる。このような状況で、本人が望むプライバシが保持できるかが不明瞭となる。
予測を実現するために必要とされる技術	例えば、本人の特定はできないが、車体によって識別されたデータが、特定の複数のロケーションへ行動することが識別でき、また特定のロケーションにおける別の識別されたデータが特定の購入実績を持つなどの特性がある場合、本人の“名前”は分からなくても、それぞれの識別情報（車体番号や購入者番号）により、本人の特性情報が明らかにされ得る。
情報セキュリティ技術上の課題（または、研究テーマ）	一般にセキュリティの研究では、防御技術の研究とともに、攻撃技術の研究により、さらに防御技術が進歩するという効果を期待している。本件では、プライバシ暴露技術（データマイニング）を研究することによって、プライバシ保護技術を推進する効果を持つ。 ① データマイニング技術 ② プライバシ保護技術 ③ アイデンティティマネジメント技術 利用者のプライバシ保護に関する意思決定の技術プライバシ保護は、法律上の個人情報保護とは異なる概念であることに留意。従って、まずは④における利用者におけるプライバシ保護に関する意思決定の技術による分析をもとに、①～③の要件を抽出すべき。
備考	法律における個人情報保護と技術とが現実に乖離していることを比較検討できるとよい。

【セキュリティ対策の要件、リスクの評価・可視化】

二木委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　認証技術　　）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	市場・ビジネス環境の変化への対応速度の向上
予測内容	市場、ビジネス環境変化が激しくなり、人間系のみでは対応が困難になることから、企業の主要ビジネス分野ごとにその状況、変化やリスクを可視化し、さらに予測と経営判断を支援するようなシステムが必要になる。（現在の経営支援システムの延長上）
予測を実現するために必要とされる技術	多面的な情報を整理、必要な内容のみを可視化する技術 異常発見のための技術 予測技術
情報セキュリティ技術上の課題（または、研究テーマ）	（セキュリティのみではないが）リスクの数値化、可視化の技術 リスクのシミュレーション技術 セキュリティリスクとその他の経営リスクを、うまく正規化して統合できるような技術（方法論）
備考	

【セキュリティ対策の要件、リスクの評価・可視化】

三河尻委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　〇その他（フレームワーク　　）
予測時期	３年後　　〇５年後　　１０年後
記述の対象	セキュリティ対策の国内統一フレームワークの構築
予測内容	[現状] 現在、国内ではセキュリティが関連する基準が乱立しており、経営者のセキュリティ投資判断を困難にすると共に、運用現場の負荷増大を招いている。 （各基準間の不整合、重複と抜け、解釈の曖昧さ、分かり辛さ等々） [予測] ・投資の遅れ、不足による運用現場の疲弊により、対策の形骸化、リスクの増大が懸念される。 [対策] ・国による統一されたフレームワーク（セキュリティ対策/脅威の一覧）の整備と開示、定期的な見直し。　⇒各基準の段階的な見直し。 [効果] ・対策の「対応要/不要」「対応済/未対応」「残対応」等の統一的、定量的な分析が可能となる。 ・経営上の「投資基準作り」が容易になることで、「セキュリティ投資の全体最適化」「投資の促進」「運用に無理の無い計画的な対策導入」が促進される。結果的にリスクの回避が図れる。 ・フレームワークにより、今後の新規テクノロジー開発の議論において、その網羅性（セキュリティ対策との関連付け）、有効性（脅威との関連付け）を事前に定量的に分析することが可能になり、投資判断基準の整備、投資の促進に繋がる。
予測を実現するために必要とされる技術	・標準化技術 ・体系化技術
情報セキュリティ技術上の課題（または、研究テーマ）	・セキュリティ対策、脅威の統一フレームワークの不在による セキュリティ基盤（運用）の弱体化
備考	DBSC(DataBase Security Consortium)の「DB セキュリティガイドライン」のまとめ方が参考になるかもしれません。

【IT インフラ】

二木委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	SaaS の高度化
予測内容	**ASP もどきの SaaS から、本来の SaaS へ。サービスコンポーネントの標準化による「切り売り」サービスと、それらを束ねてユーザインターフェイスを短期間に開発出来るツールが普及。ユーザは、外部で提供されるサービスコンポーネントと自社開発のサービスを自由に組み合わせてシステムを構築可能に。開発・運用コスト、開発期間、メンテナンス性が大幅に向上**
予測を実現するために必要とされる技術	・高効率かつ安全な XML/Web サービス ・ビジネスロジックの標準化とコンポーネント化 ・使いやすく汎用的なＵＩデザイナ
情報セキュリティ技術上の課題（または、研究テーマ）	・（既存の Web/Web サービスセキュリティ対策の延長上にある？） ・サービス提供元への DoS/DDoS 対策
備考	

【IT インフラ】

森山委員

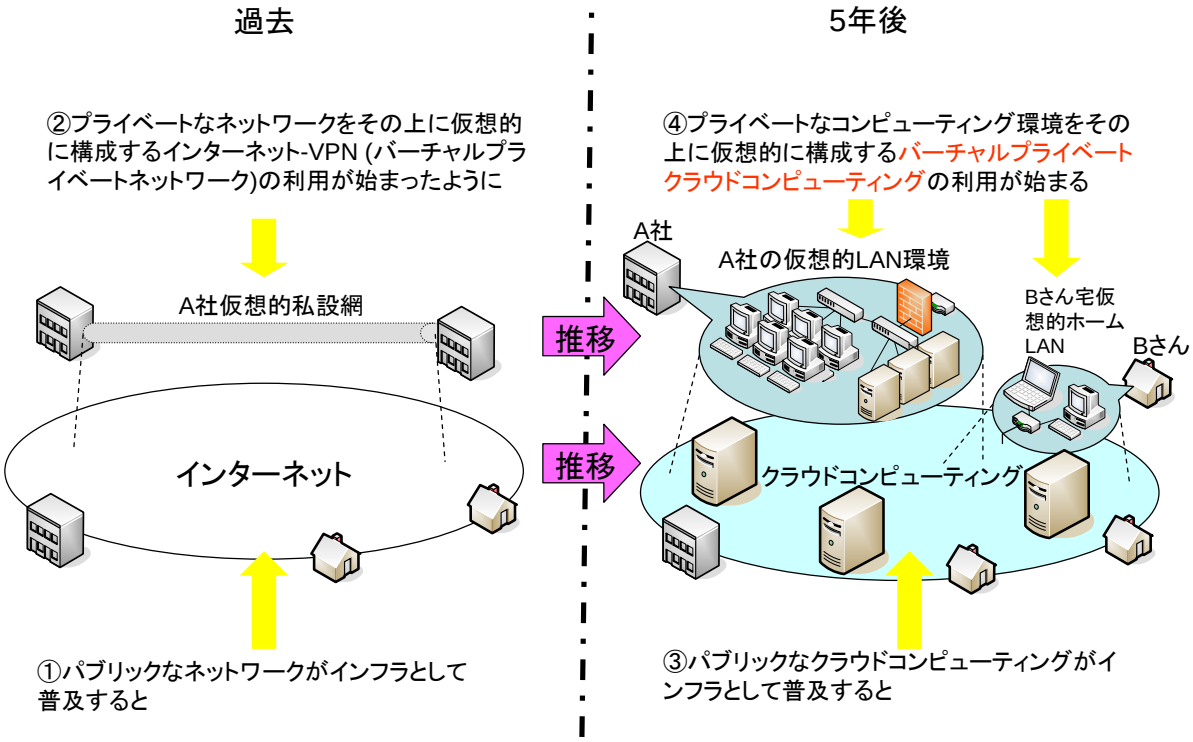
対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　　５年後　１０年後
記述の対象	電化製品のネットワーク化
予測内容	ありとあらゆる家電製品がインターネットを介して、ネットワークに接続される世の中が次第に具現化されてくる。例えば、エコーネットのような団体（http://www.echonet.gr.jp/1_echo/index.htm）においても、家電製品をつなぐための標準化が行われているように日本が先導をきって、この分野の検討が行われている。また、その際、接続される家電製品に特に制約がなく、家庭用コンロから、エアコン、暖房機、掃除機、洗濯機、鍵等々あらゆるものに及ぶと思われる。 あらゆる家電がネットにつながると想定し、構成する各機器、サーバ等々を如何にセキュリティ脅威から、守れるか、また、守るか等が必要になってくる。
予測を実現するために必要とされる技術	エコーネットのような組込み技術、ホームサーバ、センタサーバ等々
情報セキュリティ技術上の課題（または、研究テーマ）	アーキテクチュア？、組込み技術、
備考	この分野は、日本がリードする分野だと思われ、セキュリティ対策を万全の体制で進めることは、日本の将来に向けても有益と考える。

【IT インフラ】

伊藤委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　５年後　１０年後
記述の対象	クラウドコンピューティングの次の利用形態
予測内容	インターネットが広まりインターネット VPN が出たように、クラウドコンピューティングが広まった後、プライベートなネットワークコンピューティング環境をクラウド上に仮想的に構成する VPCC（Virtual Private Cloud Computing）が登場する。SaaS、クラウドコンピューティングと仮想化技術が連携することで、任意のプライベート計算環境をクラウド上に間借りする柔軟性の高いオンデマンドコンピューティングが可能になる。 例）コンシューマは、PC、バックアップサーバ、BB ルータを LAN 接続した個人専用の環境をクラウド上に仮想的に構成し、旅行先からも利用できる。 例）X 社の社内システムはクラウド上に仮想的に独立した環境として実現される。そこには A 社 CRM の SaaS、B 社会計管理の SaaS が仮想的な専用サービスとして表現され、独自開発した在庫管理システムと連結されている。処理能力はオンデマンドで増減可能で、支社用やバックアップ用インスタンスの複数配備もクラウド上で環境をコピーするだけで可能。このようなプラットフォームにオープン化された携帯電話も組み込まれ、利用のモビリティも高い。
予測を実現するために必要とされる技術	- ネットワークコンピューティングの論理モデル - コンピューティングレイヤ構成技術(ホストとネットワークの総合的な仮想化技術) - 計算リソース管理技術、セキュリティ技術 - セマンティック Web/SaaS データ構造の標準､クラウドで動作する仮想 SOA
情報セキュリティ技術上の課題（または、研究テーマ）	- コンピューティングレイヤ構成技術(暗号化/アイソレーション等) - 仮想環境下での不正アクセス監視、防御技術 - セキュリティ処理を組み込んだ論理的ネットワークコンピューティングモデル - クラウドで動作する仮想 SOA
備考	

クラウドコンピューティングの次の利用形態



【IT インフラ】

森山委員

対象・領域	将来ビジョン（　製品　(サービス)　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　(５年後)　１０年後
記述の対象	大規模環境ネットワーク
予測内容	今後、各装置の省電力化、センサー装置の進展、各装置のネットワーク化、環境問題の深刻化等が進むにつれ、資源の有効利用、効率化、無駄な生産抑制、需給調整等が必要になってくると思われる。これを防ぐ意味でも、各データを集め、有効に活用することが重要になる可能性がある。このような環境系を基とした大規模なデータを収集、活用することにおいて、そのセキュリティを守りつつ、個人情報等に配慮しつつ、活用するために、セキュリティ技術が必要である。このように国家規模で、データを吸い上げ、活用する仕組みを作った場合の、各構成要素並びに、それを防御する仕組みが必要。
予測を実現するために必要とされる技術	組込み技術、省電力化、ホームサーバ、センタサーバ等々？
情報セキュリティ技術上の課題（または、研究テーマ）	アーキテクチュア？、組込みセキュリティ、ミドルウェアのセキュリティ？
備考	

【IT インフラ】

二木委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（高度な仮想分散処理技術）その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	ＰＣグリッド上での仮想サーバ（物理サーバレスの環境）
予測内容	**現在のＰＣグリッドコンピューティングの延長上に、グリッド上に仮想サーバを構成し、クライアントＰＣの余剰リソースを使いながら高い冗長性をもったサービスを提供するような形が確立する。これにより、小規模なデータベースやアプリケーションサーバは不要になり、バックエンドの大規模ストレージや特殊なサービスのみが専用サーバで提供されるようになる。**
予測を実現するために必要とされる技術	Ｐ２Ｐ技術の高度化（高度なノード制御、管理機構の充実など） サービスコンポーネント単位の並列化技術と開発環境 （仮想「サーバ」ではなく、仮想「サービス」？） ネットワーク分散を前提とした仮想化プラットホーム
情報セキュリティ技術上の課題（または、研究テーマ）	Ｐ２Ｐネットワークのセキュリティ監視、制御技術 （個々のノード乗っ取り、マルウエア対策を含む） サービス妨害対策
備考	

【将来技術像】

山田委員

対象・領域	将来ビジョン（　製品　[サービス]　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	[３年後]　　５年後　　１０年後
記述の対象	情報セキュリティ分野の情報大爆発への対応 （“情報セキュリティ大航海”システム）
予測内容	・情報セキュリティ分野でも、情報大爆発に対応する必要に迫られると推測。 ・また、海外の悪質なサイトにおいて、インターネットショッピングサイトなどから顧客情報を詐取するための方法に関する情報が表示・流通されている中で、現実に、我が国のオンライン販売会社が被害を受ける事故が発生しており、今後、国や公的機関がこのような状況に対処することが必要。
予測を実現するために必要とされる技術	（１）インターネット上の情報の高度利用システムの開発、構築 インターネット上に散在・変容・増加している情報セキュリティ関係の情報を、政策立案・対策実施・評価に資するように、自動的に構造解析し、時系列解析する技術。 （２）インターネット上の攻撃情報の収集・監視・注意喚起システムの構築 （（１）の適用ケースの一つとして） インターネット上に散在し、日々現われては消え、姿を変えていく、攻撃情報等の取扱いサイトやブログなど監視し、情報を収集・分析し、必要があれば攻撃対象組織に注意喚起を行うための、サイトの時空関分析技術。
情報セキュリティ技術上の課題（または、研究テーマ）	・技術的には、文部科学省特定領域研究「情報爆発」領域で開発された技術の適用となる。情報セキュリティ分野では、攻撃者は頻繁にサイトを変えるため、それらを動的に追従し、または悪意を持った者の行動の予測が可能となるような検索技術が必要。 （経済学、心理学、行動科学的知見の結合も必要） ・また、情報セキュリティ関連情報は日本語だけのサイトを監視しても意味がないため、（１）は世界の主要言語、（２）は中国、ロシア、アラビア、東欧系言語でも監視・分析できるようにすることが重要。
備考	・将来想定される cyber　war への技術的対処にもつながり得る。 ・“情報セキュリティ大航海”システムができれば、これをアジア等他国にも利用してもらうことができる。情報セキュリティ分野における国際貢献・協力の有力な玉とすることも可能。

【将来技術像】

松並委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	セキュリティパッチ
予測内容	**家電などのメーカーは価格競争の果てに製品販売売上から、サービス売上へと収益源をシフトする。ほぼすべての製品はネット化され、何かのサービスの端末と化する。** **ネット化された製品はセキュリティの脅威にさらされることとなる。セキュリティパッチのダウンロードが日常化・自動化し、パッチ「配布」のコストは下げられる。しかしパッチ「開発」のコストが目立つようになる。パッチの共通化・自動作成によるコスト削減がニーズとなる。**
予測を実現するために必要とされる技術	・Update サーバーの DoS 攻撃防御（回避）技術→P2P による Update か？ ・形式手法によるソフトウェア開発が進めば、パッチの自動作成も可能か？
情報セキュリティ技術上の課題（または、研究テーマ）	
備考	

【将来技術像】

伊藤委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） （技術像）（コンピューティング環境）　　その他（　　）
予測時期	３年後　（５年後）　１０年後
記述の対象	マルウェアフリーを実現するコンピューティング環境
予測内容	現在の PC 環境では，誰もがソフトウェアを開発でき，誰もがそのソフトウェアをインストールし利用することができる．これはマルウェアに対しても全く同じことが言えるため，正規のソフトウェアとマルウェアを確実に見分ける術は存在せず，ヒューリスティックな判断に任されている． 一方，永遠のビギナーを含む多くのユーザには，ここまでの自由度は必要とされておらず，ある決められたソフトウェアやＮＷのみが利用できれば問題ない．こうしたユーザには，【認証なきプログラムを利用できないコンピューティング環境】が適している．これにより，いかなるソーシャルハッキング手法を用いても，マルウェアを動作させることできない状態を作り出すことができる．
予測を実現するために必要とされる技術	同アーキテクチャの実現には，現状の TPM(Trusted Platform Module)相当の技術に加え，それに対応する OS，ソフトウェアなどが必要となる．また，正規のソフトウェアを認証する機関の設置やその運用体制も必要となるであろう．
情報セキュリティ技術上の課題（または、研究テーマ）	「データがプログラムに化ける」類の脆弱性は，一過性である（発見後，対処されれば解決する）ものの，ソフトウェアの認証機構を破綻させるため，その対処は重要な課題となる．具体的には，ソフトウェア開発プロセス・脆弱性発見・パッチマネージメント等の洗練化が課題として挙げられる．また、損なわれる利便性への対応が必要である．
備考	

【将来技術像】

加藤委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　その他（　　）
予測時期	３年後　５年後　１０年後
記述の対象	情報のポータビリティ、リロケータビリティ
予測内容	**現在はデータ（情報）、デバイス（処理装置）、ストレージ（記憶媒体）が比較的密な結合性を持っている（例 1:音楽配信、例２：電子マネー）。そのため扱う情報の種類が増えるとデバイスの種類が増えるという事態が発生しており、今後情報量が増えるに従って利便性は著しく損なわれていく。しかし、今後の情報処理技術や情報通信技術の進歩によりそれらの結合性が疎なものとなり、データのポータビリティが向上する。ユーザは自分が権利を所有するデータの扱いをデバイスやストレージに制限されることなく、自分の意思により自由に行うことができる。**
予測を実現するために必要とされる技術	・ データモデリングによる「情報」の標準化 ・ 現状の DRM とは異なる「権利」に基づいた「情報」の管理技術 ・ 情報を一意に特定する技術（コピーか本物か？） ・ 属性がまったく異なる莫大な情報の保存技術
情報セキュリティ技術上の課題（または、研究テーマ）	・ なりすまし等による情報窃盗等 ・ 物理的特徴が無い「情報」だけで本物とニセモノをどれだけ見分けられるか
備考	つまり、自分に所有権のある情報は自分の好きに扱いたいということです。 今はお金を払って入れ物を買っているのかデータを買っているのかわからない。

【将来サービス像／社会像】

伊藤委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　５年後　　１０年後
記述の対象	携帯電話の将来利用イメージ
予測内容	携帯電話は現在のいわゆるスマートフォンと融合し、W-CDMA などネットワークを使った高機能な「携帯電話」に進化し普及する。 ・　携帯電話は分散型コンテンツストレージになる。現在携帯電話で撮った写真などのコンテンツを他人と共有するにはメールでのプッシュ送信が主流だが、将来自端末の公開フォルダに入れるだけで、サーバを経由せず友人や家族と P2P のオンデマンド式で共有できるようになる。 ・　音声からはじめ様々メディアが利用できるようになる。例えば、一台の携帯電話で複数の異なる電話サービスを契約し、多数の電話番号の同時利用や、他人の携帯電話を借りてログインすれば自分の電話番号がすぐ使えるほどのポータビリティが実現できる。また、電話番号は国への依存がなくなるため、安価に国際ローミングもできる。 ・　SIM カードを利用した回線認証は活用され、従来のパスワードを用いた WEB サービス認証の代わりになり、セキュリティは向上される。
予測を実現するために必要とされる技術	・　携帯電話ネットワーク帯域の拡大 ・　バッテリーの消費を抑える方式
情報セキュリティ技術上の課題（または、研究テーマ）	・　携帯電話から個人情報流出の防止 ・　携帯電話の場合、DoS、fuzzing、不正アクセスなどのセキュリティ対策強化が必要 ・　SPIT 対策：迷惑電話を受けやすくなる可能性がある ・　ＩＰ技術の匿名性が高くなる、詐欺を防ぐための発信者特定技術が必要
備考	

【将来サービス像／社会像】

森山委員

対象・領域	将来ビジョン（　製品　(サービス)　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	(3年後　　5年後)　１０年後
記述の対象	ネットワークの高速化に伴う個人、企業データの集中管理
予測内容	ワイヤレスも含めネットワークが高速化されるとサーバ側に保持されるデータが肥大化される。例えば、アドレス帳のように個々人が持っていた情報をサーバ側で管理するというようになる。このようなことが、今行われている様々なサービスで進展してきた場合、その簡便性を担保しつつ、セキュリティを保つというような相反する要求を保つ手段が必要になってくる。
予測を実現するために必要とされる技術	セキュリティ技術の簡便化、サーバ、クライアントの強調したセキュリティ
情報セキュリティ技術上の課題（または、研究テーマ）	アーキテクチュア？、ミドルウェアのセキュリティ、サーバキュリティ
備考	

【将来サービス像／社会像】

伊藤委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（ハニーポット）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	ヒューマノイドハニーポット
予測内容	従来のハニーポットは受動的に攻撃を待ち受け，攻撃手法の解析やマルウェアの収集に使われてきた．昨今では，ウェブブラウザの脆弱性に対する攻撃の流行に伴い，クライアント型ハニーポットも登場しつつある． 一方，相手が機械か否かを判定する逆チューリングテストといった手法が存在する．現状の機械的に巡回するクライアント型ハニーポットでは，攻撃サイトの手前にこうした逆チューリングテストを設置されると，巡回できない． 将来は，ヒトの思考回路を備え，ヒトが攻撃を受けうるサイトを網羅的に巡回可能なクライアント型ハニーポットの実現が期待される．
予測を実現するために必要とされる技術	人工知能
情報セキュリティ技術上の課題（または、研究テーマ）	逆チューリングテストは，ブログに対するスパムコメントやアカウントの自動登録等への対策として用いられているため，逆チューリングテストの無効化を目指すには，現在それに依存しているサービスにおいて代替となる手段を提供する必要がある．
備考	

【将来サービス像／社会像】

山田委員

対象・領域	将来ビジョン（ 製品　サービス　ビジネス　ライフスタイル ） 技術像（ ）　その他（ ）
予測時期	３年後　５年後　１０年後
記述の対象	高度道路交通システム（ITS: Intelligent Transportation System）とセキュリティ事象を含む事故への対応
予測内容	高度道路交通システム（ITS: Intelligent Transportation System）に関する技術は、「情報提供・警報目的」（現在～3年後）⇒「操作支援目的」（5年後）⇒「自動運転目的」（10年後以降）と進化していくと予測。 悪意のある第３者による違法電波やGPSの情報の操作による事故等の脅威が想定され、関係する機器やシステムの製造段階の瑕疵の有無が問題とされるケースも今後出てくると推測。
予測を実現するために必要とされる技術	日米欧において、単に自動車運転手だけでなく、ITSインフラ提供事業者、カーナビゲーション装置を含むITS装置メーカ、カーナビゲーションへの位置情報、地図などのコンテンツ・プロバイダー等多くの関係者を含めた、技術開発、実証プロジェクトが進んでいる。
情報セキュリティ技術上の課題（または、研究テーマ）	セキュリティ事故の未然防止技術だけでなく、「操作支援目的」⇒「自動運転目的」といっても、明確に切り替わるのではなく、航空機で言うフライト・レコーダーに相当する、言わば“ドライブ・レコーダー”等により、事故の原因が、運転者の運転操作によるものか、自動車を含むITS側によるものかを、事後的に調査できるようにしておくことも必要になる。官（複数省庁）民連携による実証を行い、セキュリティ技術のあるべきスペックと、それを必要。自動車先進国の日本が世界のリーダーシップを取り、日本主導のビジネスモデルも提示。 新しい事故形態と自賠責保険制度、責任所在に関する社会的受容の移行のあり方についての総合研究も重要。
備考	技術、制度、そしてそれらに関する社会的合意形成が必要となる。 （参考）「高度道路交通システム（ITS）と法」（山下友信編）（有斐閣）

【将来サービス像／社会像】

西本委員

対象・領域	将来ビジョン（　製品 (サービス) ビジネス　ライフスタイル　） (技術像（　　）　　その他（　　）
予測時期	３年後　(５年後　　１０年後)
記述の対象	意図や悪意を測る
予測内容	脅威はネットワーク⇒OS⇒サービス⇒アプリケーション⇒コンテンツと、より人間系を騙す方向に変化している。外部の犯罪者もそうであるが内部犯罪も同様と考えられる。その為、変則（アノマリ）行動分析などが叫ばれている。グランドチャレンジではもう一歩先を見据え、操作している人間の意図や悪意を汲み取る技術を確保する必要がある。
予測を実現するために必要とされる技術	キーボード入力、マウス、目線、表情、声などから、本人の意図を汲み取るような技術の開発。セキュリティ上の悪意だけではなく、疲労度合、注意力低下、ストレスなど含め把握することで、本人へのアドバイスやナビゲーションも実施することが可能となる。
情報セキュリティ技術上の課題（または、研究テーマ）	この技術導入により、さらにストレスを抱えてしまう人への対応が課題。
備考	

【将来サービス像／社会像】

西本委員

対象・領域	将来ビジョン（　製品 (サービス) ビジネス　ライフスタイル　） (技術像)（　　）　　その他（　　）
予測時期	３年後　(５年後　　１０年後)
記述の対象	社会サービスへの応用
予測内容	**社会サービスへの市民の参加** GPS＋電子マネー＋カメラ付き携帯をベースにし、駐車違反通知、防犯活動、道路保全見回り、災害時見回りなどの社会サービスの一部を、訓練を受けた一般の市民が実施することで、シルバー世代や学生などの非生産世代を有効活用することで費用削減を図ると共に、参加者は社会貢献を通じた生きがいと社会への責任と安心を得ることが出来る。
予測を実現するために必要とされる技術	日本国民の「マイル」のようなものを支えるシステム。
情報セキュリティ技術上の課題（または、研究テーマ）	電子マネーの交換或いは両替ショップ周りに、犯罪が蔓延らないような工夫が必要 大変重要なプライバシー情報を持つので第三者機関を含めた、厳重な運用が必要
備考	

【将来サービス像／社会像】

松並委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　５年後　　１０年後
記述の対象	さまざまな分野における電子化・ネット化と脅威分析
予測内容	**人々の生活のあらゆる「用事」が電子化・ネット化され、速い、安い、旨い（便利）が進む（商店街→大型量販店→ネットナントカ）。** **つまり①利便性の追求（早い、安井、旨い）と同時に②プライバシー・安心・安全が求められ、③低コストも制約条件として課せられる。**
予測を実現するために必要とされる技術	
情報セキュリティ技術上の課題（または、研究テーマ）	・あらゆる分野における、電子化・ネット化がどういう絵姿になるのか、その絵姿におけるセキュリティ上の脅威を明らかにする研究 ・それぞれの分野においてセキュリティを語れる（脅威を発見し、対策を打てる）人材の育成も必要
備考	この研究成果の「絵姿」から将来サービスを実現するための技術（とその技術を実現する研究テーマ）がわかる。 「脅威」からも同様に、必要なセキュリティ対策ための技術（とその技術を実現する研究テーマ）がわかる。

【将来サービス像／社会像】

松並委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　５年後　　１０年後
記述の対象	個人情報プロファイルの安全な集中管理・提供
予測内容	**人々の生活のあらゆる「用事」が電子化・ネット化され、速い、安い、旨い（便利）が進む（商店街→大型量販店→ネットナントカ）。** **人々の生活がもっと忙しくあわただしくなり、日々の「用事」を「超効率化」することが大きなニーズとなる。**
予測を実現するために必要とされる技術	・引っ越しの際の住所変更がワンストップでできる技術。 ・自分の個人情報プロファイルの一部だけを取引相手に提供する技術
情報セキュリティ技術上の課題（または、研究テーマ）	それでいて、複数の取引相手に個別断片的に提供した情報を集めて個人プロファイル全体を再構成できない仕組みが必要
備考	

【将来サービス像／社会像】

松並委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　５年後　　１０年後
記述の対象	オンライン取引における個人認証のしくみ
予測内容	**人々の生活のあらゆる「用事」が電子化・ネット化され、速い、安い、旨い（便利）が進む（商店街→大型量販店→ネットナントカ）。** **しかし貧富の差が激しくなり、個人 ID の転売が多発し、悪意あるオンライン取引の後、たとえ個人を特定できたとしても、その個人に賠償能力がなく、単に個人を特定できる現在の個人認証の仕組みだけでは、世の中の経済活動の安定を維持できなくなる。**
予測を実現するために必要とされる技術	・個人の賠償能力もオンライン取引時にわかる認証の仕組み ・匿名による個人認証の仕組みであって、賠償能力を提示できる技術 （成人であることの匿名認証に似ている？）
情報セキュリティ技術上の課題（または、研究テーマ）	
備考	顧客の賠償能力がない場合のオンライン取引のお店側向けの保険サービスもあってもよい。

【将来サービス像／社会像】

西本委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　(ライフスタイル)　） (技術像)（　　）　　その他（　　）
予測時期	３年後　　５年後　　(１０年後)
記述の対象	社会の変移
予測内容	**従前の、実社会と仮想社会の位置づけが逆転する。** **実社会：実生活、仮想社会：仮想生活** **⇒ 実社会：仮想（理想）生活　仮想社会：実生活** **買物、家族や社会との関わりが逆転する** **仕事も納税も仮想社会で、実社会ではボランティアや優しい平和な社会**
予測を実現するために必要とされる技術	グランドチャレンジによる、実生活が営める仮想社会の構築が必須 仮想社会において匿名性を担保した日本国民（日本政府の保護対象）の識別技術 識別した保護対象の保護技術（恐らくエージェントプログラム）の開発
情報セキュリティ技術上の課題（または、研究テーマ）	行動する人間の特性（年齢、嗜好、性格、気分など）に合わせた保護が必要 保護対象の違法行動に対する保護原則
備考	制度的課題の方が大きいかも知れないが、現場の成長にひきづられるのではないか。

【将来サービス像／社会像】

森山委員

対象・領域	将来ビジョン（　製品　サービス　ビジネス　ライフスタイル　） 技術像（　　）　　その他（　　）
予測時期	３年後　　５年後　　１０年後
記述の対象	交通機関の電子制御化
予測内容	公共交通、家庭の車に至るまで、全ての交通手段が電子制御され、集中管理された社会において、その運行、安心、安全を守るためのセキュリティ技術。
予測を実現するために必要とされる技術	制御技術、特殊なネットワーク？、各構成要素のセキュリティ
情報セキュリティ技術上の課題（または、研究テーマ）	アーキテクチュア？、組込みセキュリティ、ミドルウェアのセキュリティ、サーバセキュリティ、交通機関の内部ネットーワークのセキュリティ
備考	