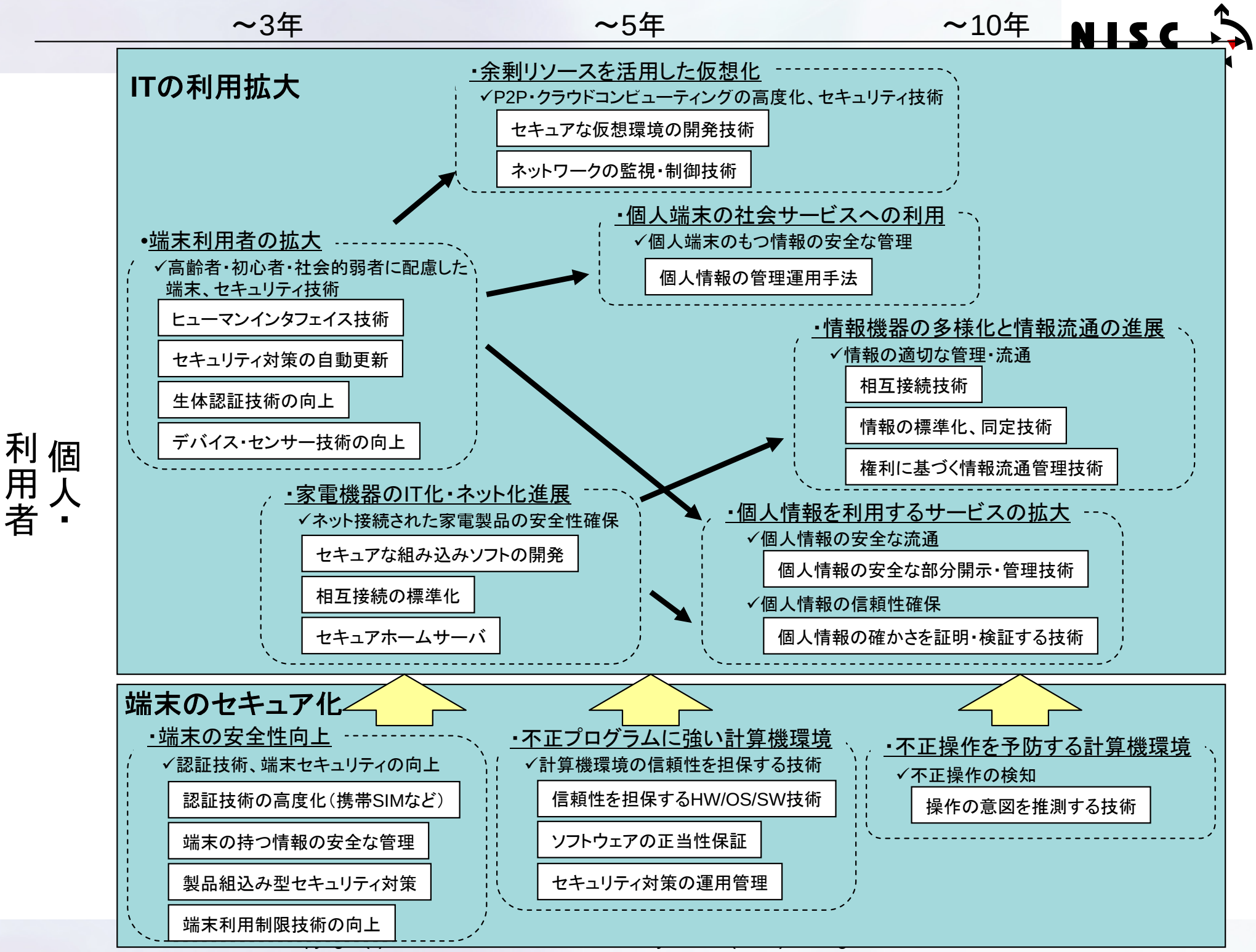
NISC National Information Security Center

技術発展の潮流予測について

2009年1月26日

内閣官房情報セキュリティセンター（NISC）
http://www.nisc.go.jp/

参考資料1


～3年
～5年
～10年
NISC
個人・利用者
ITの利用拡大
・余剰リソースを活用した仮想化
✓P2P・クラウドコンピューティングの高度化、セキュリティ技術
セキュアな仮想環境の開発技術
ネットワークの監視・制御技術
•端末利用者の拡大
✓高齢者・初心者・社会的弱者に配慮した端末、セキュリティ技術
ヒューマンインタフェイス技術
セキュリティ対策の自動更新
生体認証技術の向上
デバイス・センサー技術の向上
・個人端末の社会サービスへの利用
✓個人端末のもつ情報の安全な管理
個人情報の管理運用手法
・情報機器の多様化と情報流通の進展
✓情報の適切な管理・流通
相互接続技術
情報の標準化、同定技術
権利に基づく情報流通管理技術
・家電機器のIT化・ネット化進展
✓ネット接続された家電製品の安全性確保
セキュアな組み込みソフトの開発
相互接続の標準化
セキュアホームサーバ
・個人情報を利用するサービスの拡大
✓個人情報の安全な流通
個人情報の安全な部分開示・管理技術
✓個人情報の信頼性確保
個人情報の確かさを証明・検証する技術
端末のセキュア化
・端末の安全性向上
✓認証技術、端末セキュリティの向上
認証技術の高度化（携帯SIMなど）
端末の持つ情報の安全な管理
製品組込み型セキュリティ対策
端末利用制限技術の向上
・不正プログラムに強い計算機環境
✓計算機環境の信頼性を担保する技術
信頼性を担保するHW/OS/SW技術
ソフトウェアの正当性保証
セキュリティ対策の運用管理
・不正操作を予防する計算機環境
✓不正操作の検知
操作の意図を推測する技術

「個人・利用者」に係る潮流予測の例

安心・安全な利用者環境（PC端末）の実現

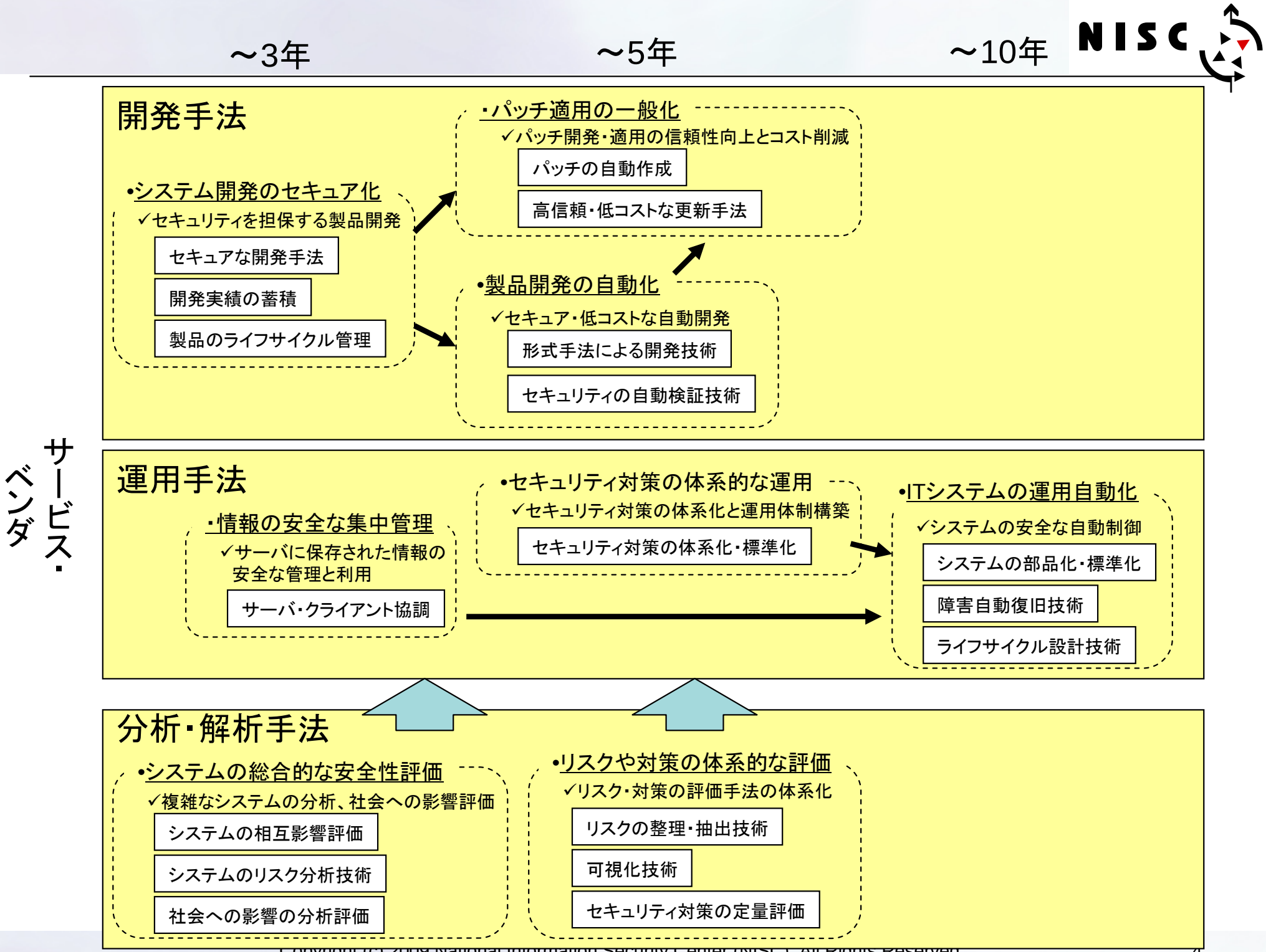
ITの利用拡大に対応するための技術と端末の安全性を向上させる技術の進展により、一般の利用者が適切な安心感をもって利用できる計算機環境を実現する。
（個人情報を無頓着に提供したり、逆に注意を払いすぎるあまり必要以上に不便な使い方をする、といったことのない状態）

個人情報などの重要度の高い情報を他者に提供するような操作や、マルウェアの起動につながるような操作など、セキュリティ上の危険を伴う操作は、利用者に対し、操作の危険度が明示される等の適切な警告表示や、必要に応じて操作のブロック等が行われる。
利用者も、自身が利用している機器の安全性に対して過度の信頼を置くことなく、状況によりセキュリティ侵害が発生する可能性があることを理解し、上記の警告表示などに対して適切な判断と対応をとれるようになっている。

また、新たな脆弱性や攻撃手法の発生によりセキュリティ侵害が発生する可能性はゼロではないが、利用者に大きな手間をかけたり利便性を大きく低下させることなく、迅速に回復するしくみが確立している。利用者も、セキュリティ侵害が発生した場合でも過度に反応することなく、冷静な対処がとれるようになっている。

『安心・安全な利用者環境（PC端末）の実現』のための要素マップ案

（想定要素）	（想定要件）	（必要と思われる技術・対策）
利用者の啓発	・情報リテラシーの普及 ・リスク教育	誤操作・不正操作の防止
信頼性を担保する HW/OS/SW技術	・セキュリティを作り込むための開発手法 ・新しいリスク対抗するために進化するソフトウェア ・ウイルスなどを自動的に隔離・排除するソフトウェア	攻撃情報・脆弱性情報の周知 リスクの整理・抽出技術 自動復旧技術 セキュリティ対策の定量評価 形式手法による開発 仮想環境のセキュリティ確保
ベンダ側の サポート体制強化	・24時間体制の相談窓口 ・リスクコミュニケーション体制 ・統一的な用語による表示、説明、取扱説明書	攻撃情報・脆弱性情報の周知 リスクコミュニケーション用 エージェントソフトウェア



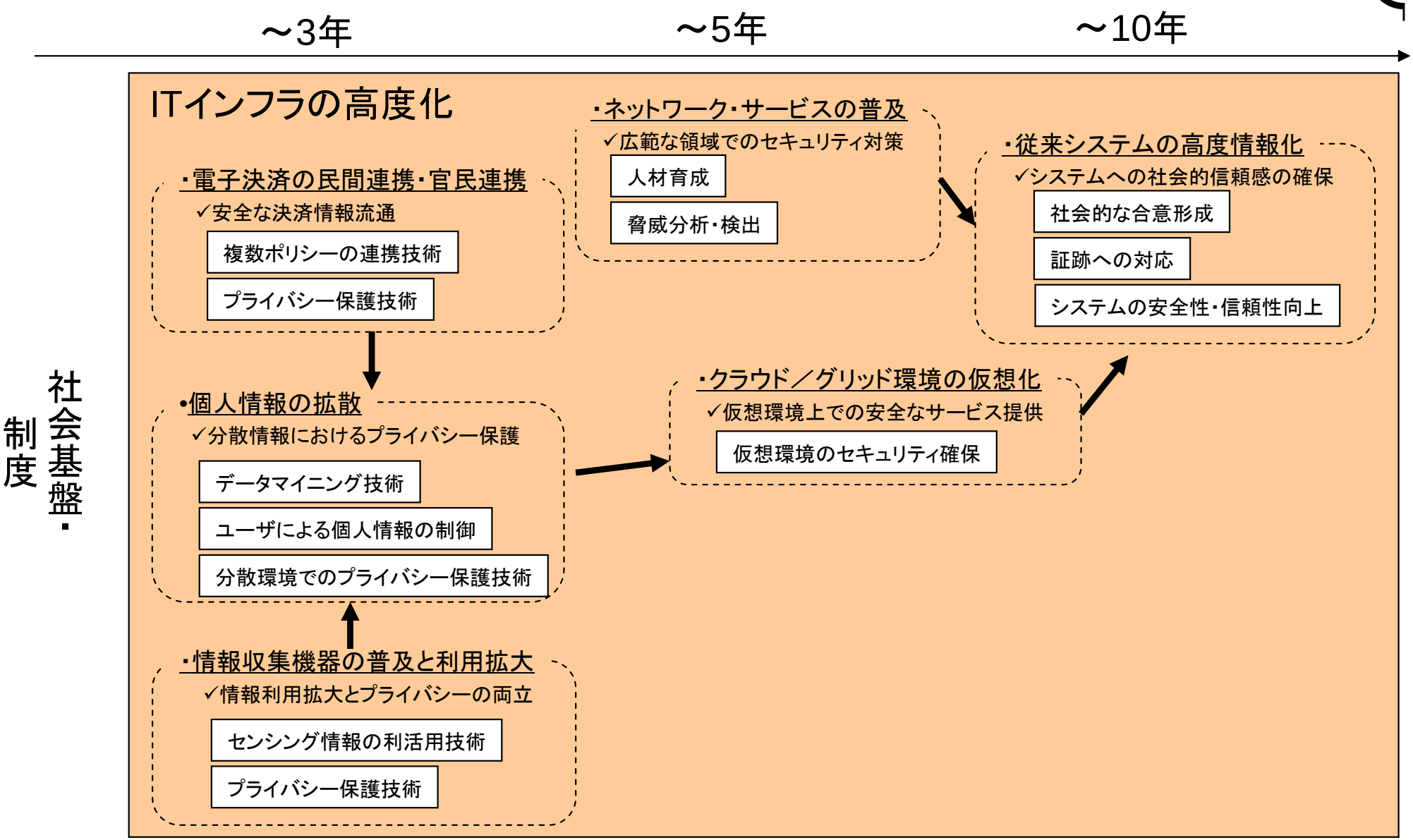
「サービス・ベンダ」に係る潮流予測の例

・自律的にセキュリティを維持するITサービス提供手法の確立

運用中に生じたシステム構成の変更や、システムの内部状態、外部環境の変動に応じてシステムの設定や構成などを変更し、適切なセキュリティを自律的に維持できるようなサービス提供の手法を確立する。

負荷の変動や環境変化に対応して、システム自体が動的かつ自律的に構成を変更しつつサービス提供を行うことが一般的となる。これに伴い、システムは構成変更によって適切なセキュリティが維持できるかどうか自分で判定し、適切なセキュリティを維持するために必要であれば、コンポーネントの設定変更やアップデート、コンポーネントの追加・削除を自律的に実行することができるようになっている。

また、動的にシステム構成が変化するサービスについて、適切なセキュリティが維持されているかどうか、システムの外部から継続的に監視して確認することができるようになっており、システムの自律的な対応だけではセキュリティを維持できない場合には、サービスへの影響を抑えつつ、システムを（外部から）更新することもできるようになっている。



「社会基盤・制度」に係る潮流予測の例

・高い信頼性・可用性とともに適切な安全性を提供可能な仮想サーバの実現

ネットワーク接続された多種多様な計算機の上に、高い信頼性・可用性をもつだけでなく、サービスに応じた適切な安全性が確保できるようなサーバ環境の構築を実現する。

従来、高い信頼性・可用性・安全性が必要なサービスの提供には専用線や専用ハードウェアを用いてシステム構築が行われてきたが、ITインフラの高度化により、汎用的な計算機・ネットワーク上に構築された仮想サーバを利用しても十分な信頼性・可用性・安全性を得られるようになる。

仮想サーバ構築の際には、サーバの構成要素となる資源（計算機・NW等）の安全性を適切に判定し、サービスに必要な安全性に応じた資源の選択が行われる。また、サービス提供において利用者などから取得した情報も、情報の性質によって要求される安全性に応じ、仮想サーバ内で適切な管理が行われる（個人情報を直接扱う処理には高い安全性を持つ特定の計算機だけを利用し、それ以外の処理にはもっと緩い管理がされている多数の計算機を使う、など）。