

# 将来の社会ビジョンと技術像の検討の進め方

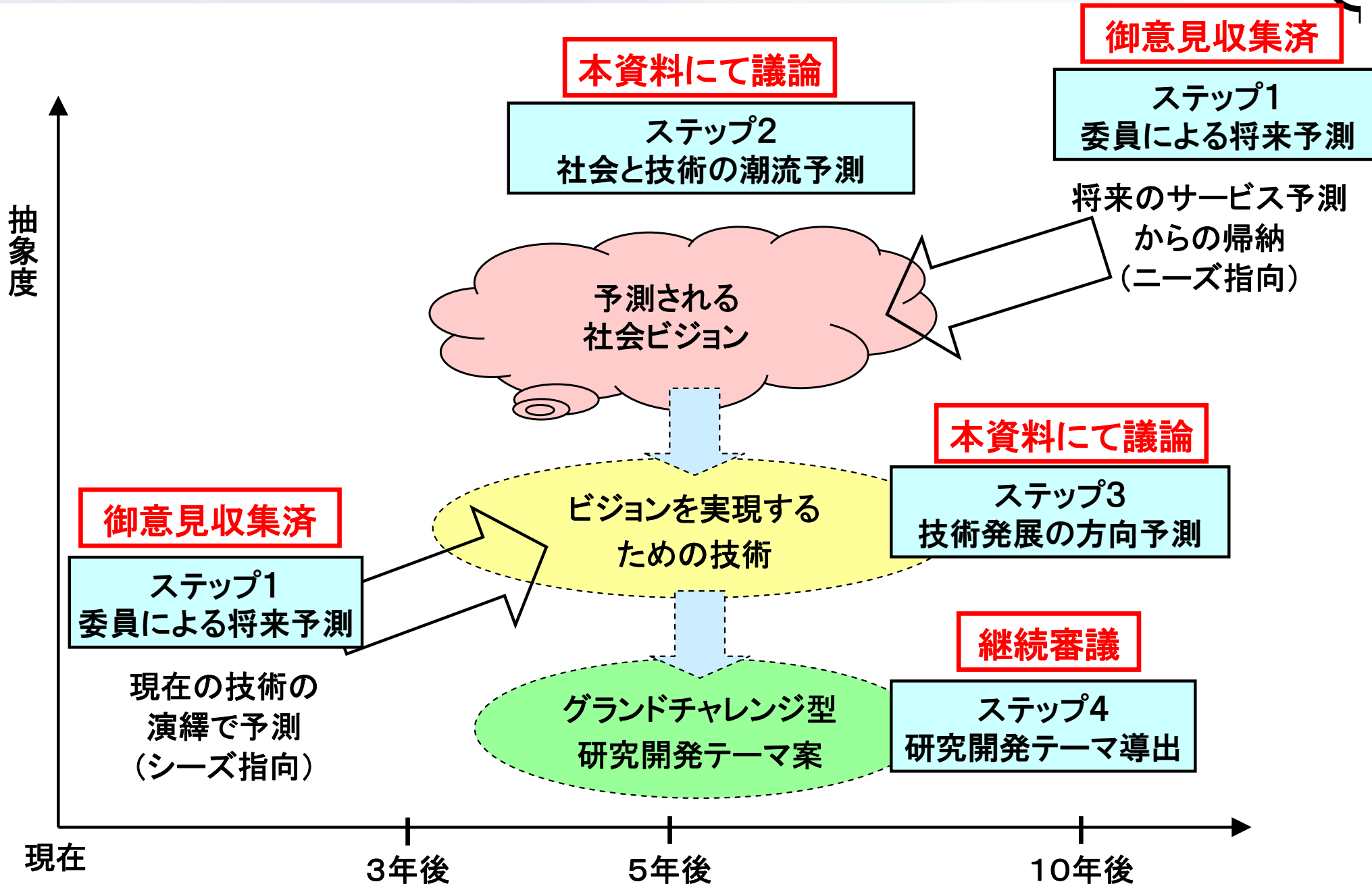
事務局案

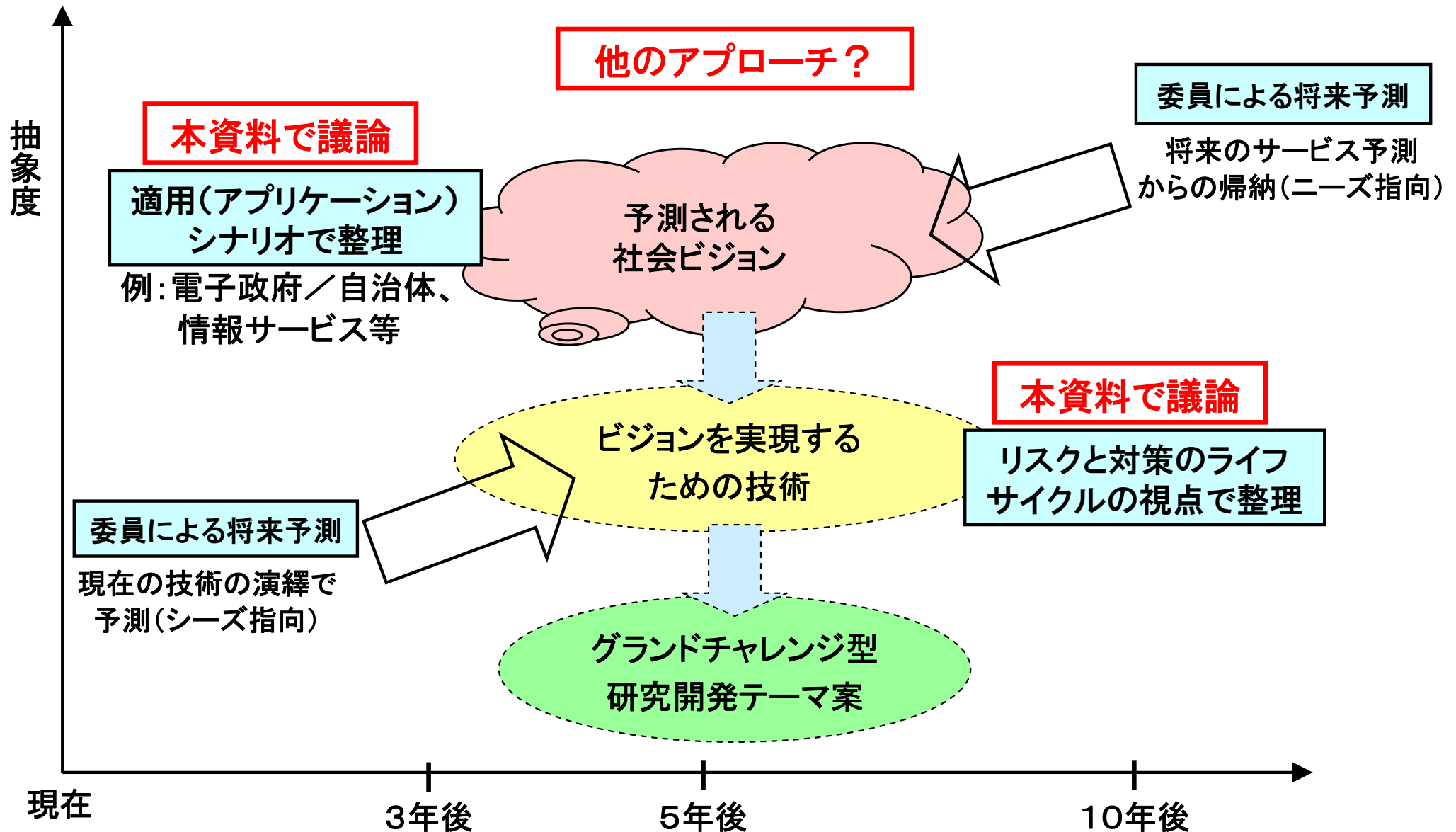
2008年12月19日

内閣官房情報セキュリティセンター(NISC)

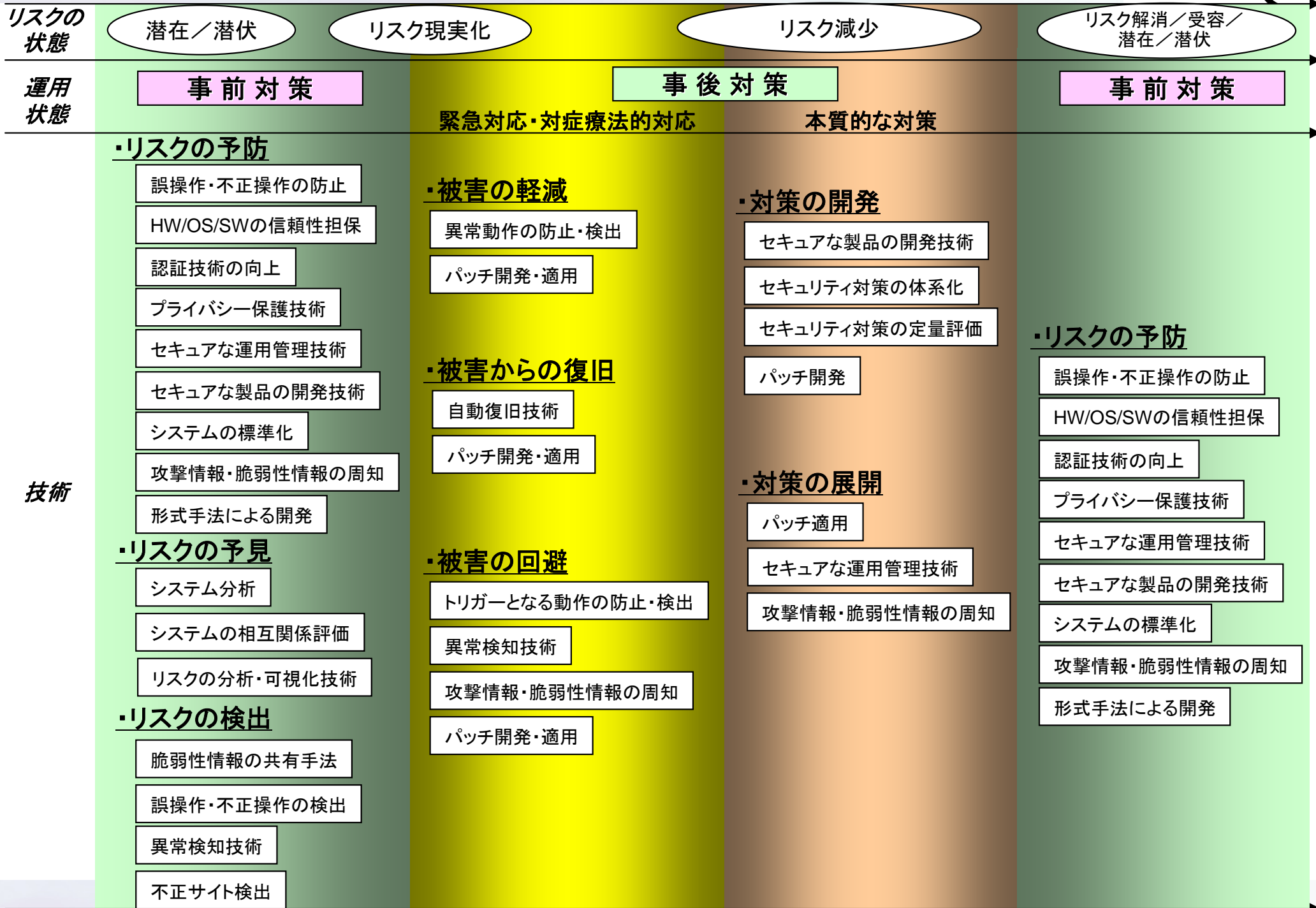
<http://www.nisc.go.jp/>

# 将来の社会ビジョンと技術像を導く検討ステップ





# 必要技術を「リスクと対策のライフサイクル」の視点で整理



- ・適用分野例: 電子政府／自治体、情報サービス等
- ・シナリオの記述方式例: 文章(例えば、委員の将来予測説明を膨らませた形式)、図など

シナリオ『マイクロ・グリッド』(サンプル: 森山委員の「大規模環境ネットワーク」の予測に追記する形で、他の委員のご意見の要素を取り入れて作成)

## (サービス像)

パソコンやAV機器のみならず、いわゆる白物家電と呼ばれる冷蔵庫、給湯器、エアコン、電子レンジ、電灯など、家庭で使用されるほとんどの電気機器がセンサー機能を持ち、ネットワーク化される。各機器は電力消費量など稼動状況、装置の周辺環境などのセンサー情報を、家庭・ビル・地区などの単位で設置されたサーバーに送信。

サーバーは事前の設定や契約(例: 最大電力量)などの条件に基づき、最適な資源(主に電力)配分となるよう、各機器の動作の制御を行う(例: エアコンの設定温度を調整、湯沸かし器の起動を数秒遅らせる、など)。

サーバー同士も互いに通信を行い、家庭レベルのサーバー間で資源を融通したり、上位のサーバーの判断で機器の制御内容を変更し、エリアレベルでの、より最適な資源配分の実現を目指す。

## シナリオ『マイクロ・グリッド』

### (セキュリティに関する実現課題)

機器の使用状況は個人の行動履歴に直結するため、それらの情報を収集し利用することはプライバシー上の問題となることが予想される。各機器からサーバーへの通信やサーバー間通信はもちろん、蓄積された情報の保護や、どのレベルのサーバーにどの粒度の情報を送るべきか(送らないべきか)、いったん受け取った情報を他のサーバーに送る際に情報の粒度をどう調整するか、といった、ポリシーの扱いとそのenforceも課題となる。

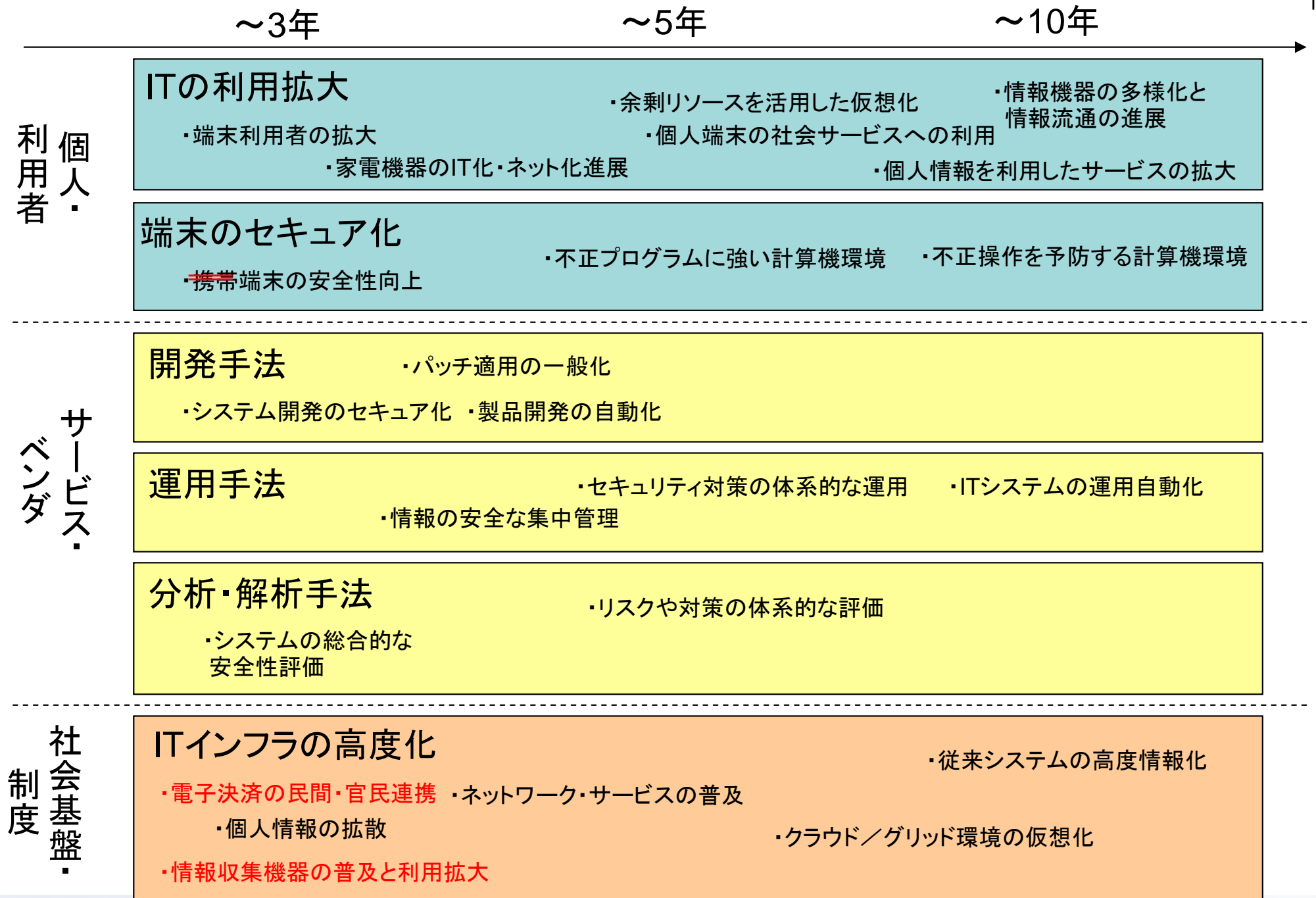
加えて、このようなポリシーの調整によって、プライバシーが保護されていることの「納得感」をどのようにユーザーに提供するかということも課題である。

また、故意に機器のセンサー等を停止するなどしてサーバーの制御を逃れ、不正に資源を利用することの防止や、逆に、センサー故障等の障害が発生した場合でも機器を利用できるようにするための手段の確保や、ある程度自動的に障害から復旧できるようにすることも必要と考えられる。(センサー情報の利用方法として、資源配分だけでなく上記のような故障の予兆を検出することに用いることも考えられる。)

機器自体についても、ネットワークにつながることで外部からの攻撃の影響を受けたり、逆に機器の脆弱性がネットワークに影響を及ぼすようになるため、特に組み込み機器について、安全な機器の開発手法や安全性の検証手法の確立が重要となる。

# 今後10年の社会潮流と 対応する情報セキュリティ技術潮流の予測 (ステップ2:改訂版)

# 委員のご意見に基づく今後10年の社会潮流予測





～3年

～5年

～10年

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  
✓PCグリッド・P2P技術の高度化、セキュリティ技術
- ・個人端末の社会サービスへの利用  
✓個人端末の持つ情報の安全な管理
- ・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
- ・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
- ・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
- ・個人情報を利用するサービスの拡大  
✓個人情報の安全な提供・管理  
✓個人情報の信頼性確保

## 端末のセキュア化

- ・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
- ・不正操作を予防する計算機環境  
✓不正操作の検知
- ・端末の安全性向上  
✓認証技術、端末セキュリティの向上

～3年

～5年

～10年

## 開発手法

・パッチ適用の一般化

✓パッチ開発・適用の信頼性向上とコスト削減

・システム開発のセキュア化

✓セキュリティを担保する製品開発

・製品開発の自動化

✓セキュア・低コストな自動開発

## 運用手法

・セキュリティ対策の体系的な運用

✓セキュリティ対策の体系化と運用体制構築

・情報の安全な集中管理

✓サーバに保存された情報の  
安全な管理と利用

・ITシステムの運用自動化

✓システムの安全な自動制御

## 分析・解析手法

・リスクや対策の体系的な評価

✓リスク・対策の評価手法の体系化

・システムの総合的な安全性評価

✓複雑なシステムの分析、社会への影響評価

サービス・  
ベンダ

～3年

～5年

～10年

社会基盤・  
制度

## ITインフラの高度化

・電子決済の民間・官民連携

✓安全な決済情報流通

・ネットワーク・サービスの普及

✓広範な領域でのセキュリティ対策

・従来システムの高度情報化

✓システムへの社会的信頼感の確保

・個人情報の拡散

✓分散情報におけるプライバシー保護

・クラウド／グリッド環境の仮想化

✓仮想環境上でのサービス提供

・情報収集機器の普及と利用拡大

✓情報利用拡大とプライバシーの両立

# 技術の発展方向予測 (ステップ3:改訂版)

～3年

～5年

～10年

### 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

利用者・個人

### 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管理

製品組み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

～3年

～5年

～10年

### 開発手法

・システム開発のセキュア化  
✓セキュリティを担保する製品開発

- セキュアな開発手法
- 開発実績の蓄積
- 製品のライフサイクル管理

・パッチ適用の一般化  
✓パッチ開発・適用の信頼性向上とコスト削減

- パッチの自動作成
- 高信頼・低コストな更新手法

・製品開発の自動化

- ✓セキュア・低コストな自動開発
- 形式手法による開発技術
- セキュリティの自動検証技術

### 運用手法

・情報の安全な集中管理  
✓サーバに保存された情報の安全な管理と利用

- サーバ・クライアント協調

・セキュリティ対策の体系的な運用  
✓セキュリティ対策の体系化と運用体制構築

- セキュリティ対策の体系化・標準化

・ITシステムの運用自動化

- ✓システムの安全な自動制御
- システムの部品化・標準化
- 障害自動復旧技術
- ライフサイクル設計技術

### 分析・解析手法

・システムの総合的な安全性評価  
✓複雑なシステムの分析、社会への影響評価

- システムの相互影響評価
- システムのリスク分析技術
- 社会への影響の分析評価

・リスクや対策の体系的な評価  
✓リスク・対策の評価手法の体系化

- リスクの整理・抽出技術
- 可視化技術
- セキュリティ対策の定量評価

サーバ  
ベンダ  
サービス

～3年

～5年

～10年

## ITインフラの高度化

### ・電子決済の民間連携・官民連携

✓安全な決済情報流通

複数ポリシーの連携技術

プライバシー保護技術

### ・個人情報の拡散

✓分散情報におけるプライバシー保護

データマイニング技術

ユーザによる個人情報の制御

分散環境でのプライバシー保護技術

### ・情報収集機器の普及と利用拡大

✓情報利用拡大とプライバシーの両立

センシング情報の利活用技術

プライバシー保護技術

### ・ネットワーク・サービスの普及

✓広範な領域でのセキュリティ対策

人材育成

脅威分析・検出

### ・従来システムの高度情報化

✓システムへの社会的信頼感の確保

社会的な合意形成

証跡への対応

システムの安全性・信頼性向上

### ・クラウド／グリッド環境の仮想化

✓仮想環境上での安全なサービス提供

仮想環境のセキュリティ確保

社会基盤  
・  
制度