NISC National Information Security Center

情報セキュリティ技術に関する将来予測の進め方について

2008年8月28日

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

資料5－3

将来予測の目的及び主な対象分野

１．将来予測を実施する目的

- 政府としての「将来の社会ビジョンと技術像」。
- 政府内で認識を共有するとともに、広く世の中に公表し、情報セキュリティ技術や政策に関する方向性の議論を惹起する。
- 予測された「社会ビジョンと技術像」は、問題提起や提言を行うための前提として用いる。

  予測された「社会ビジョンと技術像」から、新たに登場するであろう情報セキュリティ上の脅威や課題、また、いつ頃、どのような情報セキュリティ対策や技術が必要となるか、などが浮かび上がることを期待。

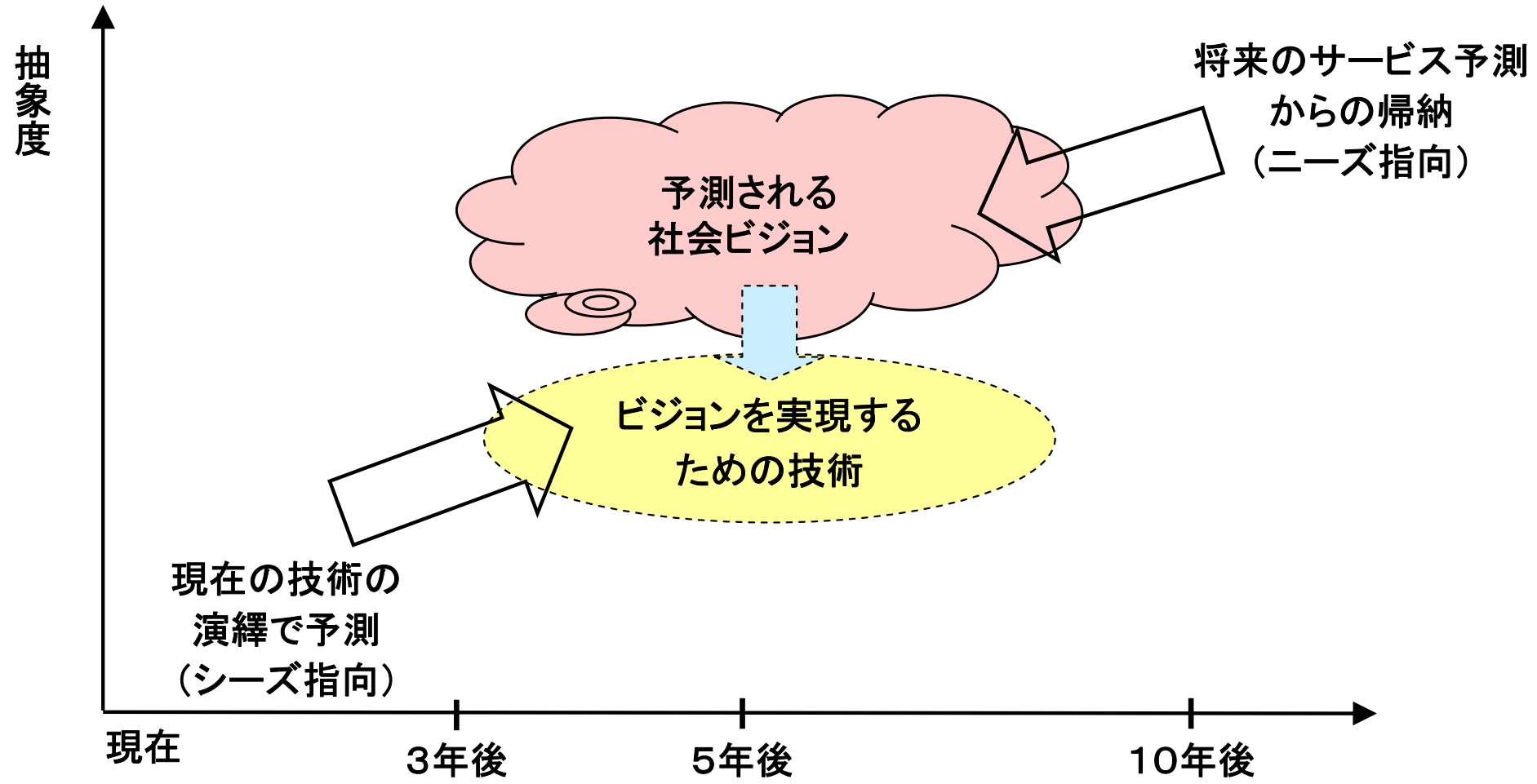
２．将来予測の主な対象分野

- 政府として関心のある、公共性の高い「社会の基盤となるシステムやサービス」。

  （例）電子政府、重要インフラ、災害対策など

将来予測の対象期間

・中長期（3年後、5年後、10年後の3ポイント）とすることが適当か。



将来予測の手法

3. ニーズ・シーズ双方から検討

（1）ニーズ指向アプローチ

- 利用側の視点からアプローチする。
- 将来的に登場するであろう製品、アプリケーション、サービス等を予測し、それらを安全に利用するための情報セキュリティ要件を検討

（例）安全対策として、公共の場所に膨大な数の監視用カメラが設置されて、記録されるようになった場合、プライバシー保護はどうなされるべきか？

（2）シーズ指向アプローチ

- 提供側の視点からアプローチする。
- 現在の技術の延長として、どのような機能、性能のものが登場するかを予測し、その際に必要となるセキュリティ要件を検討

（例）数テラバイトのHDDやメモリが一般家庭に導入された場合、ウイルスチェックを行なうのに、従来のパターンマッチング技術で対応可能か？

将来予測を行なう際の視点(1)

4. 将来予測を行う際の視点や分類例

(1) 領域と粒度

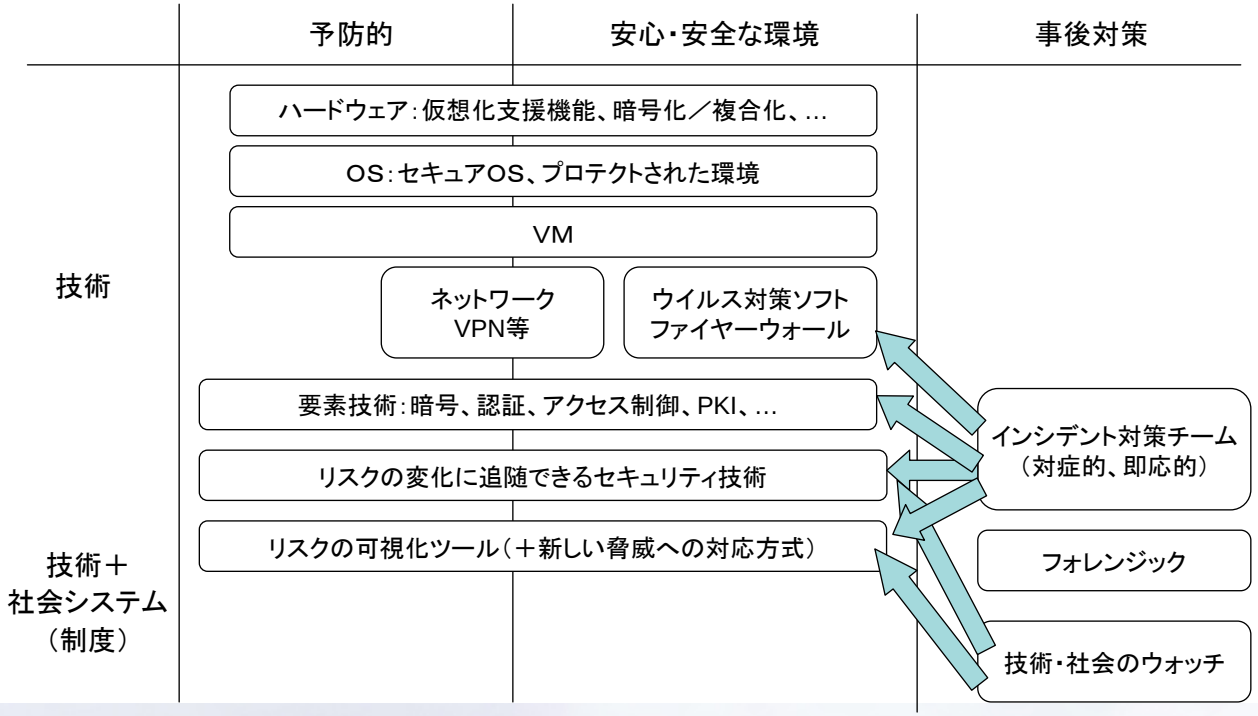
・検討の領域や粒度は細か過ぎない方が適当か。

例えば、領域は大きく「技術」と「制度」といったレベル。さらに、技術に関してもインフラ(ハードウェアとソフトウェア)とサービス(アプリケーション)程度で切り分けるのが、適当か。

(2) フェーズ分け

・予測の対象を、情報セキュリティ対策を行うフェーズで分類することも考えられる。

例えば、「予防的」「安心・安全な環境(ランタイム)」「事後対策」の3つ程度に分ける。



将来予測を行なう際の視点(2)

（3）製品やサービス

・社会環境等の変化に対して、情報セキュリティ製品やサービスがどのように変化、あるいは新しいビジネスが登場するかを想定

（例）ネットワークやストレージの大容量化、SaaS化などに伴って、クライアント用のウイルス対策ソフトの市場が減少した場合、ビジネス領域をどう移していけば、これまでのノウハウを活用し、優位性を維持できるか。

（4）IT利活用のシナリオ

・ニーズ指向アプローチの一つ。

・ITを活用した生活や業務のやり方などが、将来的にどのように変化していくかを予測

（例）全ての業務がオフィス外で可能になった場合（在宅や移動中など）の、セキュリティ対策はどうあるべきか。

（5）その他の検討の視点等

将来予測の方法論として、何か留意点はあるか。