資料２－５

研究会の検討の方向性及び取りまとめ方法について（案）

総務省 情報通信政策局
情報セキュリティ対策室
2007年12月5日

（1）基本的考え方

- **検討対象**

【論点1】

次の2つに分類して、検討してはどうか。

①現在の情報通信環境における脅威・課題への対応

現在の情報通信環境における主な情報セキュリティ脅威・課題及びその対策の現状を整理。

現状において、対策が不十分な項目や、もっと効果的な対策を講ずべき項目など（課題）を検討。

②近い将来における情報通信環境における脅威・課題への対応

今後3年から5年後といった近い将来における情報通信環境、及びその移行過程における環境の変化を捉え、主な脅威・課題を抽出・整理。

それら脅威・課題への対策を検討。

上記の2方向から、主な情報セキュリティ脅威・課題及びその対策を可能な限り網羅性をもって導出するとともに、特に重点的に取組む課題を選定。

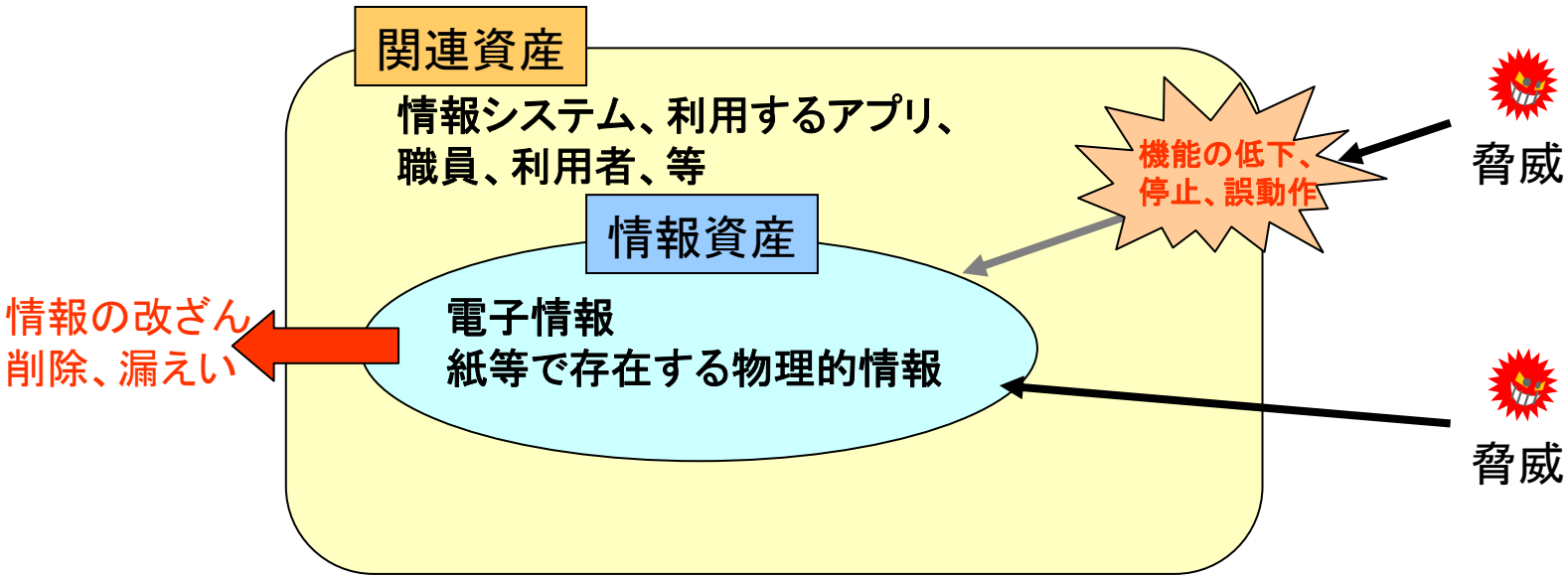
- 情報資産と関連資産（情報セキュリティ脅威から守るべき資産）

【論点2】

情報資産及び関連資産を次のように捉えて良いか。

– 情報資産：企業情報、個人情報（データそのもの）

– 関連資産：ハードウェア資産、ソフトウェア資産、サービス資産、人的資産



- **守るべき資産に対する主な脅威の分類**

【論点３】

情報セキュリティに関する主な脅威を、次のとおりに分類して検討してはどうか。

ア）**ボットウイルス等マルウェアによる脅威**

（ワーム型感染のウイルスによる脅威）

イ）**ソーシャルエンジニアリングを駆使した脅威**

（フィッシング等、人間の行為、行動の弱点、盲点等をついてマルウェアに感染させたり、情報を盗み出す脅威）

ウ）**内部脅威**（人為的ミス、意図的な犯行等）

エ）**外部脅威**（外部からの不正アクセス、自然災害等）

	脅威の個別具体例（手法及び目的）	
ボットウィルス等マルウェアによる脅威	（手法） •ソフトウェアの脆弱性を攻撃（ワーム型感染） （目的） •ハードウェアクラッシュ •ソフトウェア改ざん・削除・誤動作 •サービス不能化攻撃	•情報の削除・改ざん・不正入手 •スパムメール発信 •フィッシングメール発信 •ウィルス感染メール発信　等
ソーシャルエンジニアリングを駆使した脅威	（手法） •なりすまし電話・メール、トラッシング スキミング、ショルダーサーフィン •リバースソーシャルエンジニアリング （トロイの木馬等） •フィッシング（Web Spoofing）	•多段型Webマルウェア感染 •ターゲットアタック（高度な成りすまし） （目的） •不正に情報を入手 •マルウェアの感染
内部脅威	•職員による設定・操作ミスによる機能低下・停止・誤動作 •職員による情報の削除・改ざん・漏えい（意図的・非意図的） •セキュリティポリシーの不備	•委託先管理不備による情報漏えい （セキュリティマネジメントの不備による） •盗聴 •盗難
外部脅威	•地震等自然災害による機能停止等 •物理的攻撃による機能停止等 •脆弱性をついた不正侵入によるハードウェアクラッシュ、ソフトウェア改ざん・削除・誤動作等（Web改ざん等）	•ID、PWDの不正利用による侵入（なりすまし）による情報の削除・改ざん・漏えい等 •盗聴 •盗難

- **主な情報セキュリティ対策実施主体の分類**

【論点４】

情報セキュリティ対策の主な実施主体を、次のとおりに分類して検討してはどうか。

ａ.利用者（企業等・個人）

ｂ. 情報セキュリティ関連事業者（AVV、情報セキュリティソリューション提供事業者等）

ｃ. 電気通信事業者（ISP、アクセス系、携帯電話系、無線通信系）

ｄ. ＯＳ/アプリケーション/サービス提供事業者

ｅ. 機器開発事業者

ｆ. 政府機関

（2）現在の情報通信環境における脅威・課題への対応

- **現状の情報セキュリティ脅威への対応状況**

【論点5】

P4に示す脅威毎に、各対策実施主体が行っている対策を整理し、その十分性を検討してはどうか。

［例1］	ボットウイルス等マルウェアによる脅威					
その他	・運用ポリシーの設定（主に企） ・監査の実施		・運用の高度化			・ガイドラインの作成等、運用の高度化支援 ・情報セキュリティ対策の普及啓発
アプリケーション/サービス	・ウイルス対策ソフトの適用、サービスの導入（個・企） ・バージョンアップ、パッチの適用 ・企業ネットワーク監視サービスの適用（主に企）	・脆弱性対応 ・ウイルス対策ソフトの提供 ・企業ネットワーク監視サービスの提供	・ウイルス対策サービスの提供	・脆弱性対応		・情報セキュリティ対策の普及啓発
OS/ミドルウェア	・バージョンアップ、パッチの適用			・脆弱性対応		・情報セキュリティ対策の普及啓発
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク	・認証の適用（個、企） ・FW、IDS等対策機器の導入（主に企） ・バックアップ・冗長化（個・企）	・FW、IDS等対策装置の提供			・組み込みシステムの脆弱性対応	・情報セキュリティ対策の普及啓発
ネットワーク（インターネット／公衆網）			・ネットワーク設備の運用・維持管理、緊急対応、事業者連携 ・ネットワーク監視サービスの提供 ・VPN、専用線の提供			・ガイドラインの作成・支援 ・運用の高度化支援
要素技術		・解析・対策技術の高度化	・ネットワーク設備	・設計段階からのセキュリティ対策	・設計段階からのセキュリティ対策	・研究開発の推進
	利用者（企業等・個人）	情報セキュリティ関連事業者（AVV、情報セキュリティソリューション提供事業者等）	電気通信事業者（ISP、アクセス系、携帯電話系、無線通信系）	OS/アプリケーション/サービス提供事業者	機器開発事業者	政府機関

（3）近い将来における情報通信環境における脅威・課題への対応

- **情報通信環境の変化及びその過程の整理**

【論点6】

情報通信環境の変化及びその過程を、次頁のとおりに整理してはどうか。
その上で、脅威・課題を抽出し、対策を検討してはどうか。

- 3年から5年の近い将来：電気通信ネットワークのIP化、端末の高機能化等、多くの環境変化の要因は、成熟期を迎えるのではなく、進展・普及過程にあり、情報通信環境は常に変化が継続している状況。

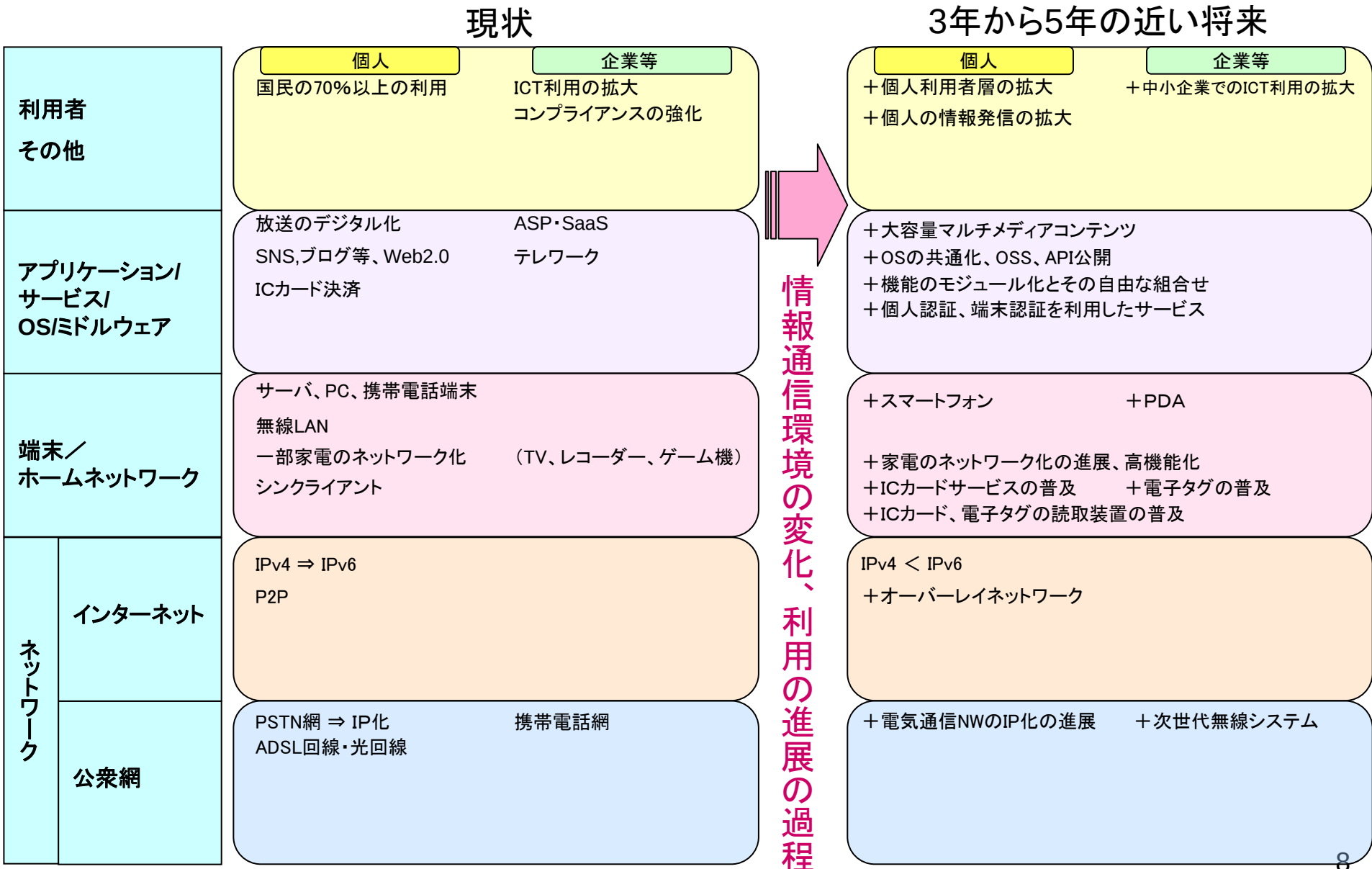
（情報通信環境）

2010年　　：次世代ネットワーク
2010年度　　：ブロードバンド・ゼロ地域の解消
2015年～20年：新世代ネットワークの実用化を目途
2025年　　：イノベーション25の実現

（情報セキュリティ関連）

2009年　　：次期情報セキュリティ基本計画が開始予定

NGN、端末の高機能化等、全ての環境変化の要因は、成熟期を迎えるのではなく、進展過程にあり、情報通信環境は常に変化が継続している状況にある。



（4）アンケート結果等で挙げられた主な脅威・課題、対策等

（現状の脅威・課題、対策等）

- 情報セキュリティ対策を実施すべき主体が抱える問題点（p10）
- 継続して発生する情報セキュリティ脅威・課題（p11）
- 主要な現状課題への対策（p12）

（近い将来における変化の要因、脅威・課題、対策等）

- 情報通信環境の変化の主な要因（p13）
- 情報通信環境の変化等による情報セキュリティ脅威・課題（p14-p15）
- 情報通信環境の変化等によって生じる脅威・課題への対策（p16-p17）

（アンケート結果等から）

- **情報セキュリティ対策を実施すべき主体が抱える問題点**
  - 利用者（企業）：問題が起きて、はじめてリスク分析や管理策の不備に気付く事が多い
  - 利用者（個人）：利用者層が広がり、年少者や高齢者がインターネットを利用することになることから、こうした利用者に情報セキュリティ対策を託すことは難しいのではないか
  - 情報セキュリティ関連事業者：優秀なセキュリティ技術者が不足していないか
  - 電気通信事業者：制度との関係で対応可能範囲が不明確（正当業務行為の範囲等）
  - OS／アプリケーション／サービス提供事業者：サービスに見合った必要な対策が講じられているか不明確ではないか
  - 機器開発事業者：サービス提供後の脆弱性等への迅速な対応、情報システムのセキュアプログラミング技法への対応等が不十分ではないか
  - 政府機関：効率的な取締り、国際的に迅速に問題解決できる体制等が不備ではないか

（アンケート結果等から）

- **継続して発生する情報セキュリティ脅威・課題**

【ボット等】

- ボットによる様々なサイバー攻撃が発生（ボットウイルス作成、ボットネット構築、ボットネットを利用した攻撃の実施が分業化、DDos脅迫事件の発生）
- 海外から日本への攻撃（日本から海外への攻撃）が継続（インシデントの国際化）
- P2P等での違法・有害情報、ウイルス等の拡散

【ソーシャルエンジニアリング】

- ソーシャルエンジニアリング手法の高度化、脅威の潜行化　（ターゲットアタック、スピアメールを発端にしたウイルス感染、情報搾取活動）
- フィッシング等による情報漏えい等が継続

【内部脅威】

- 企業等における情報漏えいの継続

【外部脅威】

（アンケート結果等から）

- **主要な現状課題への対策の充実**

【ボット等】
- 問題のあるWebサイトや通信の取締り、法制度の整備
- 国際的な連携に基づく情報共有・問題解決の体制
- 基本的ウイルス対策の徹底
- セキュリティ対策を考えたソフトウェア、システムの設計・製作

【ソーシャルエンジニアリング】
- ソーシャルエンジニアリングを駆使した、或いは複合型の新しい攻撃の発見及び解析手法、情報共有体制の強化
- 問題のあるWebサイトや通信の取締り、法制度の整備
- 国際的な連携に基づく情報共有・問題解決の体制
- 基本的ウイルス対策の徹底

【内部脅威】
- 企業における情報システム管理・人的管理の徹底

【外部脅威】

（アンケート結果等から）

- **情報通信環境の変化の主な要因**

【利用者、その他】

- インターネットの更なる普及促進（利用者数（個人、中小企業等）の増加）
- インターネットの利用形態の変化⇒情報資産の企業レベルでの外部集中と個人レベルでの分散
  （ASP・SaaS等のネットワークを通じたアプリケーションサービスの利用。SNS・ブログ等個人の情報発信機会の増加。PCだけではなく、携帯電話等でのインターネットの利用の増加、等）
- 現在海外で生じている情報セキュリティインシデントが、我が国でも時間差で同様の事案が発生する可能性

【アプリ、サービス等】

- ASP・SaaS利用の拡大、サービス試行アーキテクチャの進展（機能のモジュール化）
- 共通OSの利用、APIの公開が促進

（続き）

【端末／ホームネットワーク】

- 携帯電話端末の高機能化（いわゆるスマートフォン、PDAの利用拡大）
- 無線アクセスシステムの多様化（無線LAN利用の増加、次世代無線通信システム）
- 家電製品のネットワーク化（TV、レコーダー、ゲーム機）
- ICカード、RFIDの利用促進

【ネットワーク】

- インターネットプロトコルの変更（IPv4からIPv6へ）
- 電気通信ネットワークのIP化（NGNサービス）

（アンケート結果等から）

- **情報通信環境の変化等による情報セキュリティ脅威・課題**

【利用者、その他】

① 情報セキュリティ意識が必ずしも高いとは言えないユーザーが拡大

② ネットワークを通じたアプリケーションの利用による、情報資産の組織外部への集中

③ 放送波・IPマルチキャストによるウイルスを含む悪意のコンテンツの流布

【アプリ、サービス等】

④ アプリケーションの多様化による、ソフトウェアの脆弱性・不具合が多数発生

⑤ ソフトウェアの共通化により、脆弱性や不具合の影響範囲が拡大

【端末／ホームネットワーク】

⑥ 端末の高機能化により、複数のアクセス経路を持つことで、ウィルス感染経路や拡散経路が多様化

⑦ 家電のネットワーク化により、成りすましや不正アクセスによる外部からの情報資産へのコンタクトの可能性、組込みシステムの脆弱性への対応、PC、サーバー以外での情報資産管理

⑧ ICカード、RFIDの利用に伴う、漏えい電磁波による情報漏えい

（続き）

【ネットワーク】

⑨ IPv6への移行関連： IPSecによるEnd-to-Endの暗号通信により既存のFW等の機器では不正通信が確認できなくなる可能性、匿名アドレスの悪用、端末がNWから直接認識されること、経路制御（ICMPv6）のエラーパケットによるバックドア等

⑩ NGN/電気通信ネットワークのIP化：インターネットとの並存、IP電話における発信番号偽装

（アンケート結果等から）

- **情報通信環境の変化によって生じる脅威・課題への対策**

① 個人の情報セキュリティ対策の徹底

①② 企業における情報資産のリスク分析、必要な管理策実施の徹底

② ASP・SaaS事業者による情報セキュリティ対策の徹底

①⑦ 機器の無線セキュリティ対策のデフォルト設定の徹底

①⑦ HGWの先の個別端末・機器のセキュリティ対策

①⑦⑩ ユーザーの利便性を損なわずに安全性を確保した、NW/プラットフォーム/サービスのレイヤ間、電気通信事業者間/サービス提供者間における共通的な利用者認証スキームの確立

③⑤⑥ 複数の無線IFを通じたマルウェアの感染・拡大行動の抑止対策・機器の修正・機能追加等の確実な対応手法の確立（利用者に頼らない仕組み）

③⑤⑥ コンテンツの真正性を確認した場合にのみ利用できるようにする仕組みの構築

＊）番号は前頁の課題に付した番号。順位付けではない。

（続き）

③⑤⑥⑨⑩ 不正な通信等に対して事業者が情報を共有し連携して対処できる包括的な枠組み・規定の整備

④⑥ 高機能携帯電話等におけるソフトウェアの脆弱性等への対応やサイバー攻撃への耐性強化

⑦⑧ 対タンパ技術の開発

⑧ RFIDの暗号化（安価で強固、実装可能なデバイスの開発）

⑨ IPv6環境でのEnd-to-End接続モデルでのセキュリティ対策

⑨ 現在の情報セキュリティ対策機器等のIPv6対応の徹底

– 情報セキュリティ対策の責任分界点の明確化

他にも考慮すべき環境変化や、検討すべき脅威・課題、対策があるのではないか。ご意見を頂戴したい。