資 料 ２－１

我が国の情報セキュリティ戦略について

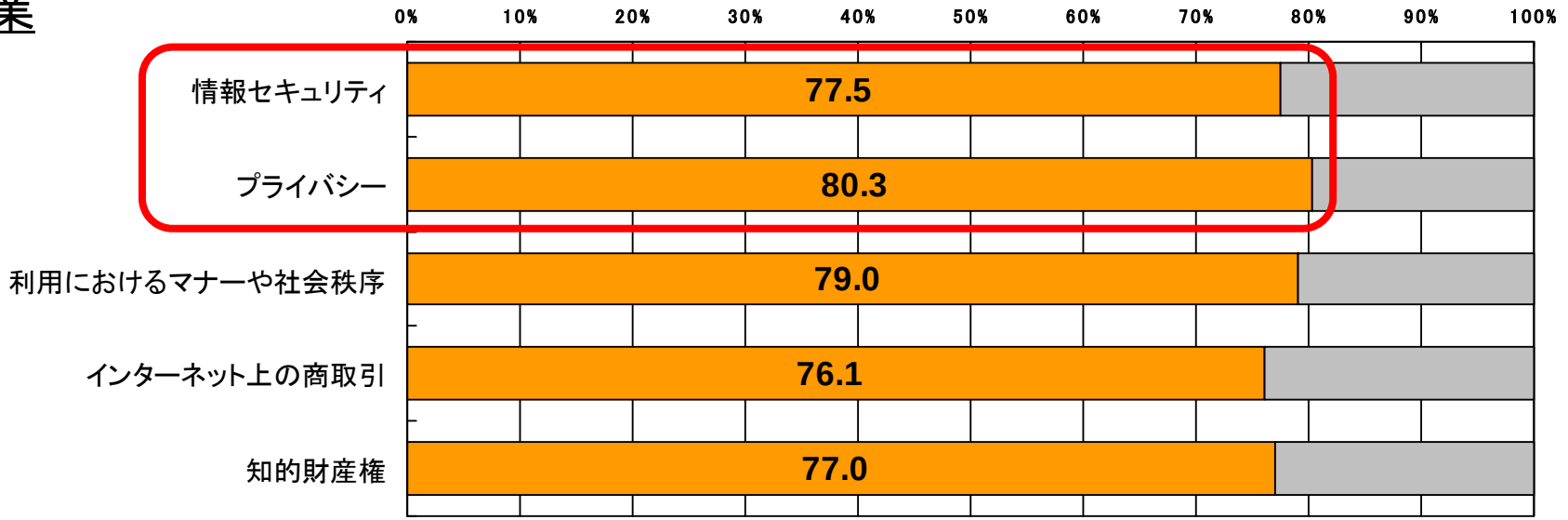
平成２３年４月１３日

内閣官房　情報セキュリティセンター（NISC）

情報通信利用に対する不安感

国民

企業



【出典】平成21年「ユビキタスネット社会における安心・安全なICT利用に関する調査」（総務省）

情報セキュリティ政策と個人情報保護対策

情報セキュリティ政策

すべての国民が情報通信技術を安全・安心に利用できる環境の実現

（参考）**高度情報通信ネットワーク社会形成基本法**（平成十二年十二月六日法律第百四十四号）

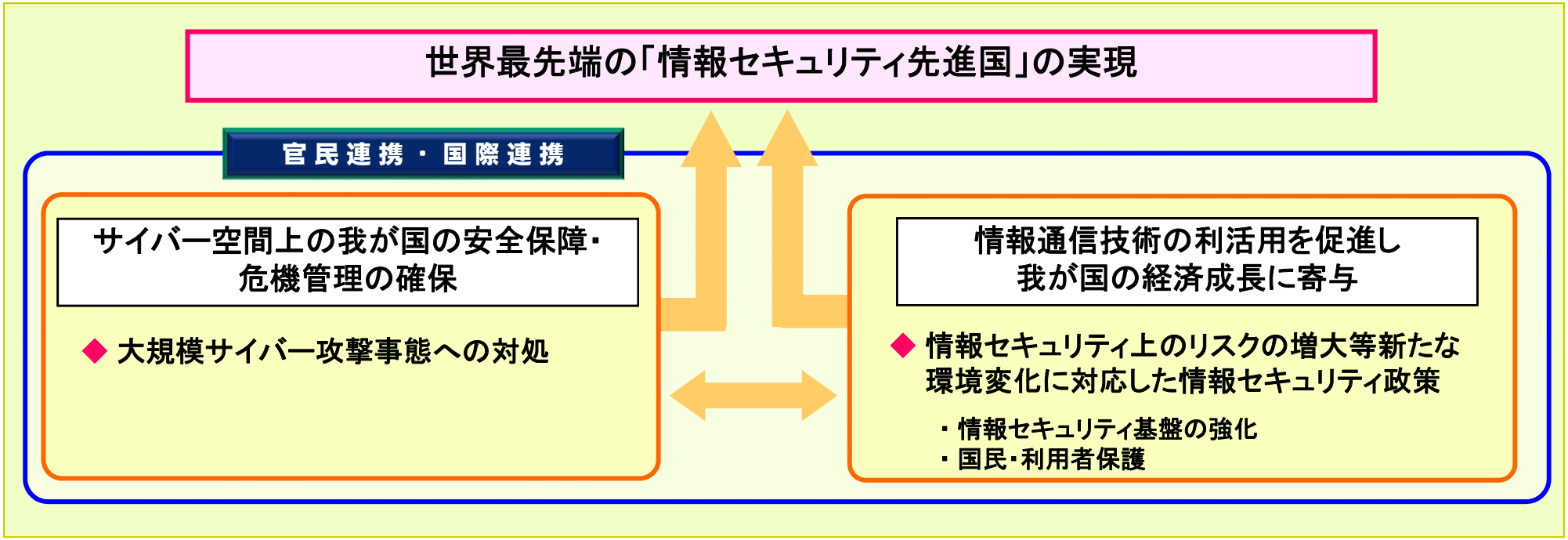
（高度情報通信ネットワークの安全性の確保等）
第二十二条　高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。

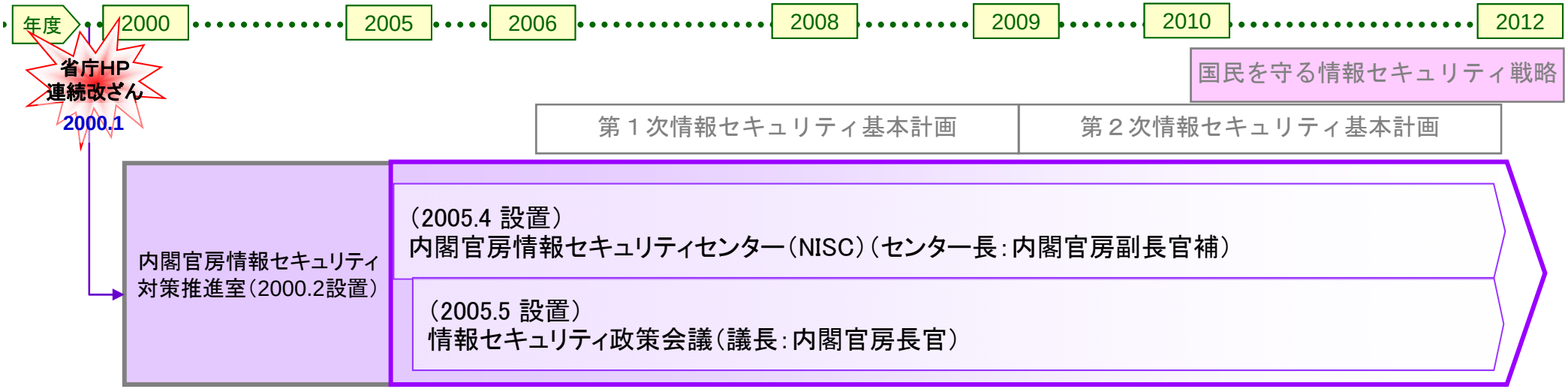
事業者等における対策

	情報セキュリティ対策（※1）	個人情報保護対策（※1）
対象となる情報の範囲	情報全般	個人情報
内容	「機密性」「完全性」「可用性」（※2）の確保	漏えい、滅失又は毀損の防止（利用目的に沿った利用）
事業者等に対する規制	一般法は存在しない	個人情報保護法
法令に基づくガイドライン等	ー ※政府については政府統一基準に沿って、重要インフラについては安全基準等を参考として情報セキュリティ対策を実施	主務官庁が事業等分野ごとにガイドラインを定める
当該分野における規格	情報セキュリティマネジメントガイドライン（ISMS・国際規格）(ISO 27000シリーズ)	個人情報保護マネジメントシステム（Pマーク制度・国内規格）(JIS Q 15001)

※1　情報セキュリティ政策が関係するのは、このうち情報通信技術に関係するもの
※2　機密性確保・・・漏えい等の防止、完全性確保・・・改ざん等の防止、可用性確保・・・データ破壊等の防止

すべての国民が情報通信技術を安全・安心に利用できる環境の実現





情報セキュリティ政策の枠組みと推進体制

内閣官房を中心に関係省庁も含め横断的な体制を整備

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）

本部長　内閣総理大臣
副本部長　内閣特命担当大臣（科学技術政策）
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（８人）

（事務局）
内閣官房IT担当室
室長（官房副長官補（内政））

情報セキュリティ政策会議　（2005年５月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　内閣府特命担当大臣（科学技術政策）
構成員　国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣

閣僚が参画

小野寺　正	KDDI株式会社代表取締役会長
黒川　博昭	富士通株式会社相談役
土屋　大洋	慶應義塾大学大学院准教授
野原　佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	首都大学東京法科大学院教授
村井　純	慶應義塾大学教授

重要インフラ専門委員会　技術戦略専門委員会　CISO等連絡会議

（事務局）
内閣官房情報セキュリティセンター　（NISC）

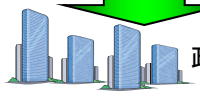
センター長（官房副長官補（安危））
副センター長（内閣審議官）２名
内閣参事官６名
情報セキュリティ補佐官（アドバイザー）３名

その他の関係省庁
重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）
その他
文部科学省（セキュリティ教育）　等

協力

協力４省庁
警察庁　（サイバー犯罪の取締り）
総務省　（通信・ネットワーク政策）
経済産業省　（情報政策）
防衛省　（国の安全保障）


重要インフラ事業者　等


政府機関（各府省庁）


企業


個人

「国民を守る情報セキュリティ戦略」の概要（平成22年5月11日情報セキュリティ政策会議決定）

現状の課題

大規模なサイバー攻撃事案等の脅威の増大

✓重要インフラ等、国民生活に直結するサービスの情報通信技術への依存による脅威の増大
✓国境を越えたサイバー攻撃が現実化（米韓大規模サイバー攻撃（昨年7月））
✓ガンブラーウイルス等、年々新たなウイルスが出現。攻撃手法も高度化・多様化

社会経済活動の情報通信技術への依存度の増大

✓情報家電、電子タグなどあらゆる機器がネットワークに接続
✓ 約8割の国民が情報セキュリティに不安感

急速な技術革新の進展

✓ クラウド・コンピューティング技術、IPv6への移行
✓ 暗号の危殆化につながるコンピュータの能力向上

グローバル化の進展

✓ 国境を越えた瞬時の情報流通
✓ 各国の個人情報保護・情報セキュリティ制度の調和

- *重要インフラ等の国民生活に直結するサービスの情報通信技術への依存の高まりにより、脅威（ITリスク）は着実に増大*
- *情報セキュリティ上の攻撃手法が多様化・高度化・複雑化しており、従来の取り組みでは対応が困難*
- *各国でも戦略的な取り組み（＊）を実施*

（＊）米国
・サイバースペース政策レビュー（60日レビュー）
・「サイバーセキュリティ調整官」を設置し、国家的取組みを強化
・「2010 Cybersecurity Enhancement Act 」（2010年2月）

課題に対応する
新戦略の必要性

「国民を守る情報セキュリティ戦略」

国民を守る情報セキュリティ戦略（2010～2013）

第2次基本計画（2009～2011）

（＊）第2次情報セキュリティ基本計画を包含し、今後4年間の重点的な取組み

基本的な考え方（取組みの重点化）

① サイバー攻撃の発生を念頭に置いた政策強化・対処体制整備
② 新たな環境変化に対応した政策の確立
③ 受動的な対策から能動的な対策へ

➢ ITリスクを克服し、安全・安心な国民生活を実現
➢サイバー空間の安全保障・危機管理政策の強化と情報通信技術政策の連携
➢安全保障・危機管理及び経済の観点に国民・利用者保護の観点を加えた3軸構造の総合的な政策（特に、国民・利用者の視点を重視した政策の推進）
➢ 国際連携の強化

安全・安心な国民生活を実現

サイバー空間上の我が国の安全保障・危機管理の確保

情報通信技術の利活用を促進し、我が国の経済成長に寄与

実現すべき成果目標

2020年までに、インターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境 （高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現

具体的な取組

● *強力なリーダシップの下、総合的な政策推進体制を確立し、官民の役割の明確化、官民連携を強化*

1　大規模サイバー攻撃事態への対処態勢の整備等

サイバー攻撃事態への対処態勢の整備

・平時からの対策と事案対処の連携強化

➢対処態勢の整備
- ・初動対処態勢の整備
- ・初動対処訓練の実施
- ・官民連携の推進
- ・サイバー攻撃に対する防衛分野での体制強化
- ・サイバー犯罪の取締り　等

➢平素からの情報収集・共有体制の構築・強化
- ・対処に資する情報収集・分析・共有体制の強化
- ・諸外国等との情報共有体制の構築・強化

2　新たな環境変化に対応した情報セキュリティ政策の強化

国民生活を守る情報セキュリティ基盤の強化

➢政府機関等の基盤強化
- ・各府省の最高情報セキュリティ責任者（CISO）の強化
- ・政府横断的な情報収集・分析システム（GSOC）の強化
- ・政府統一基準の見直し、政府機関情報システムの対策強化
- ・共通番号制に対応した情報セキュリティ対策の検討　等

➢重要インフラの基盤強化
- ・分野横断的な官民連携体制の強化
- ・情報共有体制の強化、サービス提供が確保できるシステム等の検討
- ・事業継続計画（BCP）の充実　等

➢その他の基盤強化
- ・マルウェア対策の充実・強化
- ・クラウド化、IPv6に対応した情報セキュリティ確保方策
- ・中小企業に対する情報セキュリティ対策支援
- ・医療、教育分野等における情報セキュリティ確保方策　等

国民・利用者保護の強化

➢普及啓発活動の充実・強化
- ・情報セキュリティ月間による普及啓発の強化
- ・包括的な普及啓発プログラムの策定

➢情報セキュリティ安心窓口（仮称）の検討
- ・地域NPO法人等の支援
- ・国民・利用者からの相談受付窓口の検討

➢**個人情報保護の推進**
- ・プライバシー保護技術の適切な利用促進
- ・個人情報保護に関するガイドラインの見直し
- ・国際的なフレームワークへの対応　等

➢サイバー犯罪に対する態勢の強化
- ・犯罪取締りのための基盤整備の推進　等

国際連携の強化

➢米国、ASEAN、欧州等との連携強化
- ・日米サイバーセキュリティ会合、日ASEAN情報セキュリティ政策会議等を通じた戦略的連携強化
- ・海外CSIRTの構築支援
- ・新たな二国間関係の構築

➢APEC、ARF、ITU、MERIDIAN、IWWN等の国際会合を活用した情報共有体制等の強化
- ・国際会議への積極的な参加を通じた情報共有体制の強化

➢NISCの窓口機能の強化
- ・情報セキュリティに関するベストプラクティスの共有等
- ・情報セキュリティ政策について諸外国等と連携強化　等

技術戦略の推進等

➢情報セキュリティ関連の研究開発の戦略的推進等
- ・新たな情報セキュリティ研究開発戦略の策定
- ・高度化・多様化する攻撃等に対応できる技術の実現・普及（「グランドチャレンジ型」研究開発の推進）

➢情報セキュリティ人材の育成
- ・政府、大学、企業等における高度な情報セキュリティ人材の育成

➢情報セキュリティガバナンスの確立
- ・情報セキュリティガバナンスの経営としての位置付け
- ・事業継続計画（BCP）の策定、情報セキュリティ監査　等

制度整備

➢サイバー空間の安全性・信頼性を向上させる制度の検討等
- ・コンピュータウイルス関連の法改正等サイバー犯罪条約の早期締結に向けた検討
- ・機微な情報へのアクセス権限の明確化の検討　等

➢各国の情報セキュリティ制度の比較検討
- ・各国間の法制度等の相違について分析し、情報セキュリティ関連の国際連携のための課題抽出・連携方策の検討を実施

「情報セキュリティ2010」における記述（個人情報保護の推進）

・プライバシー保護技術の適切な利用促進

ア) プライバシー保護技術の適切な利用方法の検討（内閣官房）
大規模な個人情報漏えいを防止する観点から、アクセス権の設定、認証情報の管理、暗号化、匿名化等のプライバシー保護技術の適切な利用方法について検討する。

イ) 情報漏えい対策への取組（経済産業省）
個人情報も含む情報漏えい対策に取り組むため、ファイル共有ソフトによるウイルス感染を防止する等の機能を有する情報漏えい対策ツールを一般国民に提供する。

・各事業分野ごとの個人情報保護に関するガイドラインの見直し

ア) 各事業分野における個人情報保護に関するガイドラインの見直しの検討（内閣官房及び関係府省庁）
2011 年6月を目途に、企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者に対する暗号化等を行うインセンティブの在り方を検討する。

イ) 安全管理措置に係る「電気通信事業における個人情報保護に関するガイドライン」の見直し（総務省）
モバイルPC 等の紛失等に際して、漏えい等が発生した個人情報に対し適切な技術的保護措置が講じられていた場合には、事業者に求められる手続（本人への通知、事実の公表、監督官庁への報告）の一部を緩和すること等をガイドラインに明記する。

・国際的なフレームワークへの対応

ア) 個人情報の保護に関する国際的な取組への対応（消費者庁）
2010 年度においては、OECD 情報コンピュータ通信政策委員会情報セキュリティプライバシーワーキンググループ会合、APEC 電子商取引運営委員会データプライバシーサブグループ会合等に出席し、OECD におけるプライバシー法執行の越境的な課題の検討やAPEC データ・プライバシー・パスファインダー・プロジェクト等の取組を把握し、国際的な協調の観点から我が国として必要な対応・措置を検討するとともに、我が国の個人情報保護関連法制等について国際的な理解を求める。

イ) データプライバシー保護に関する対応策の研究協力に向けた検討（内閣官房）
OECD やAPEC 等の既存の国際的な議論の動向を踏まえつつ、日・ASEAN 情報セキュリティ政策会議等国際会議を通じて、環境の急速な変化に伴う、データプライバシー保護に関する対応策の研究協力に向けた検討を行う。

・個人情報保護法の見直し

ア) 個人情報保護法の見直し（消費者庁及び関係府省庁）
個人情報保護法について、2010 年度以降、法改正も視野に入れた問題点についての審議を踏まえ検討を行う。

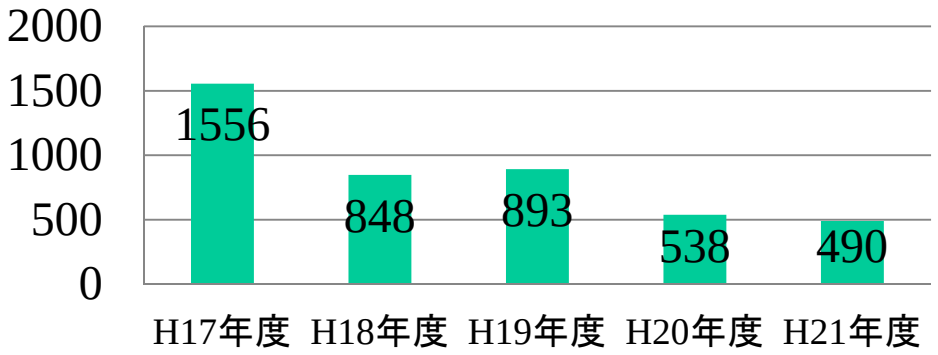
「情報セキュリティ2010」
（2010年7月22日　情報セキュリティ政策会議決定）p.45～p.46
※2010年から2011年にかけて重点的に実施する施策を掲載

サイバー空間の安全性・信頼性向上のための課題等に関する検討会(2011年3月25日・関係部分要約)

早急に取り組むべき課題	背景及び 解決策
情報セキュリティ事故が起こった際に、被害の発生・拡大を防止するための対策の実施を促す制度設計が必要である	● 企業等による個人情報の漏えいは、繰り返し発生しているが、情報セキュリティ対策の観点からは、これを完全にゼロにすることは困難であると言わざるをえない。 ● 個人情報漏えいについては、二次被害の防止等の観点から、本人への連絡、公表、主務官庁への通知が求められてきたところであるが、現在では、暗号化等の技術的手段によっても、情報漏えい時の二次被害の防止等を図ることができるようになっている。 ● いわゆる「漏洩」が発生した場合に行うべき対応として、本人通知や公表等に加えて暗号化等の技術的対策の実施についても選択肢とすることにより、対策の実施を促すことが可能となると考えられる。 → **上述の観点から、個人情報保護に係る主務省庁のガイドライン等が検討されていくことが望まれる。**
クラウドコンピューティングにより海外にデータが移転する可能性がある	● クラウドコンピューティングにおいては、データがどのサーバに存在するかを容易に確認することができず、国境をまたぐクラウドコンピューティングを利用した場合、特段の対策を講じない限り、異なる法制度や個人情報保護制度を有する国にデータが移転することとなる。(さらに、事業者の倒産リスクやカントリーリスク等もある。) → **特に公的分野において個人情報等の重要なデータを処理する部門においてクラウドコンピューティング事業者が提供するサービスを利用する際には、クラウドコンピューティング事業者が適切に情報セキュリティ対策を講じていることを委託元において確認するとともに、適切なリスクアセスメントを行うことが重要。**
情報セキュリティやプライバシーに関わる分野について、近年、次々と新たな課題が生じてきている	● 欧米では、「プライバシーを予め考慮しシステムや手続きを設定すべき」との考え方(Privacy by Design)、「行動ターゲティング広告において自らが追跡されることを許可するかどうか消費者が選択することができるようにする」との考え方(Do not track原則)、情報を「忘れてもらう権利」(Right to be forgotten)等の議論が行われている。 ● 情報セキュリティ対策は従来、「機密性」「完全性」「可用性」の確保によるデータの保護という観点が強く、上述の論点は、少なくとも情報セキュリティ政策の観点からは、国内で活発に議論がなされてこなかった。 → **これらの課題は、将来の情報セキュリティ対策にも大きな影響を及ぼしうることから、情報セキュリティ政策担当部局(NISC)においても、プライバシー問題・個人情報保護制度に係る議論の動向を踏まえて政策を立案していくことが重要である。**

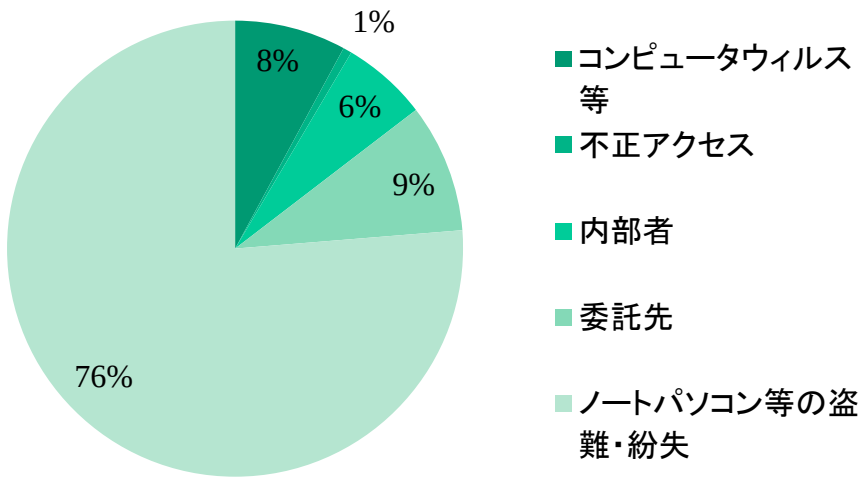
「事故前提社会」における対策の推進

事業者が公表した個人情報の漏えい事案件数



「平成21年度個人情報の保護に関する法律施行状況の概要」
（平成22年8月消費者庁）

重要情報の漏えいの発生原因



「平成21年情報処理実態調査」（平成22年8月12日経済産業省）から作成

電子媒体の漏えいにおいて、暗号化等の情報保護措置がとられていた件数（一部についてのものも含む）
＝約30%

一般的な主務官庁ガイドラインにおける記載例
法違反又は法違反のおそれが発覚した場合の対応
〇影響を受ける可能性のある本人への連絡等
〇事実関係、再発防止策等の公表
〇主務大臣・認定個人情報保護団体への報告
※二次被害の防止、類似事案の発生回避等の観点から、本人への連絡等及び公表等を行うことが望ましいとされている。
（「標準的なガイドライン」（平成20年7月　内閣府）より）

事故発生後に二次被害を防止するための技術的措置の利用が評価される仕組みが必要ではないか

「適切な技術的保護措置」の具体的措置内容の例
① 高度な暗号化措置が講じられていること
② 暗号化された情報及び復号鍵の管理が適切にされていること
③ 個人情報の漏えい等に際し、①及び②の技術的保護措置が有効に実施されていること。
（「電気通信事業における個人情報保護に関するガイドラインの解説」より）