資料３

NISC National Information Security Center

平成24年度の情報セキュリティ月間について

普及啓発の目的

情報通信技術の活用を促進するため、全ての国民が情報通信技術を安心して利用できるようにする。

そのために

情報セキュリティに係る取組を、特殊なものとしてではなく、一般常識、マナー、あるいは社会的習慣として広く国民全体に定着させる。

国民・利用者がITリスクを認識し、自発的に情報セキュリティ対策を実施することができるようにする。

平成23年度情報セキュリティ月間の重点テーマ等

キャッチフレーズ

○ 「知る、守る、続ける」をキャッチフレーズとした

知る 安全・安心・便利なインターネット環境を構築するためのポイントを知る

守る 情報セキュリティの脅威から身を守る

続ける 移り変わる情報セキュリティ上の脅威に対して対策を続ける

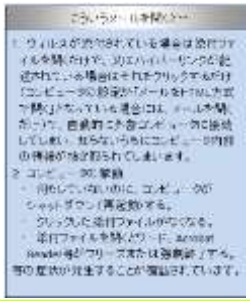
対策のポイント

○ 特に取り組んでほしい対策として、情報セキュリティ対策3か条の実施を訴えた

- 不審なサイトやメールにアクセスしない
- パソコン等は常に最新のセキュリティ状態に
- 個人情報等の重要な情報の扱いは慎重に

重点テーマ

○ 内閣官房の活動としては、不審メール対策を重点テーマとした



平成23年度情報セキュリティ月間の評価

○キャッチフレーズについては、若干抽象的な概念を用いているが情報セキュリティの確保に関する要点を短く表現したもので妥当であったと認識。また、対策のポイントについても、対象が取るべき行動を集約しており、適切であったと認識。

○また、内閣官房による活動としては、「不審メール対策」をテーマとした政府インターネットテレビ番組の作成、ホームページの作成等を集中的に実施し、一定の効果があったと理解。

○他方、「不審メール対策」そのものがどちらかといえば企業における対策が主となるため、個人の関心の盛り上がりを欠いた。

今年度の情報セキュリティ月間の重点テーマ等

○キャッチフレーズ及び対策のポイントについては、スマートフォンの一層の普及など、昨今の状況変化を踏まえてもなお有効と考えられ、継続的に同じことを主張することが重要であるという視点から、今年度も同じものを採用してはどうか。

○他方、重点テーマについては、昨年度の評価を踏まえ、今年度は、対象を個人と企業に分割して設定し、関係者はそれぞれの得意な方を中心に普及啓発活動をすることとしてはどうか。

○　具体的なテーマとしては、例えば以下はどうか

- 個人向け
  「スマートフォンのセキュリティ対策」
  又は「　　」
- 企業向け
  「不審メール対策」
  又は「情報漏えい対策」

今年度の情報セキュリティ月間の取組

次回会合までに、皆様の取組のご提案をお待ちしております。

- イベントを開催する
- 番組で取り上げる
- 記事を掲載する
- Webサイトで特集を組む
- メールマガジンで取り上げる　等

検討スケジュール

・8月（本日）
平成24年度情報セキュリティ月間に向けた基本テーマについての意見交換

・10月
平成24年度情報セキュリティ月間における取組事項の提案及び意見交換

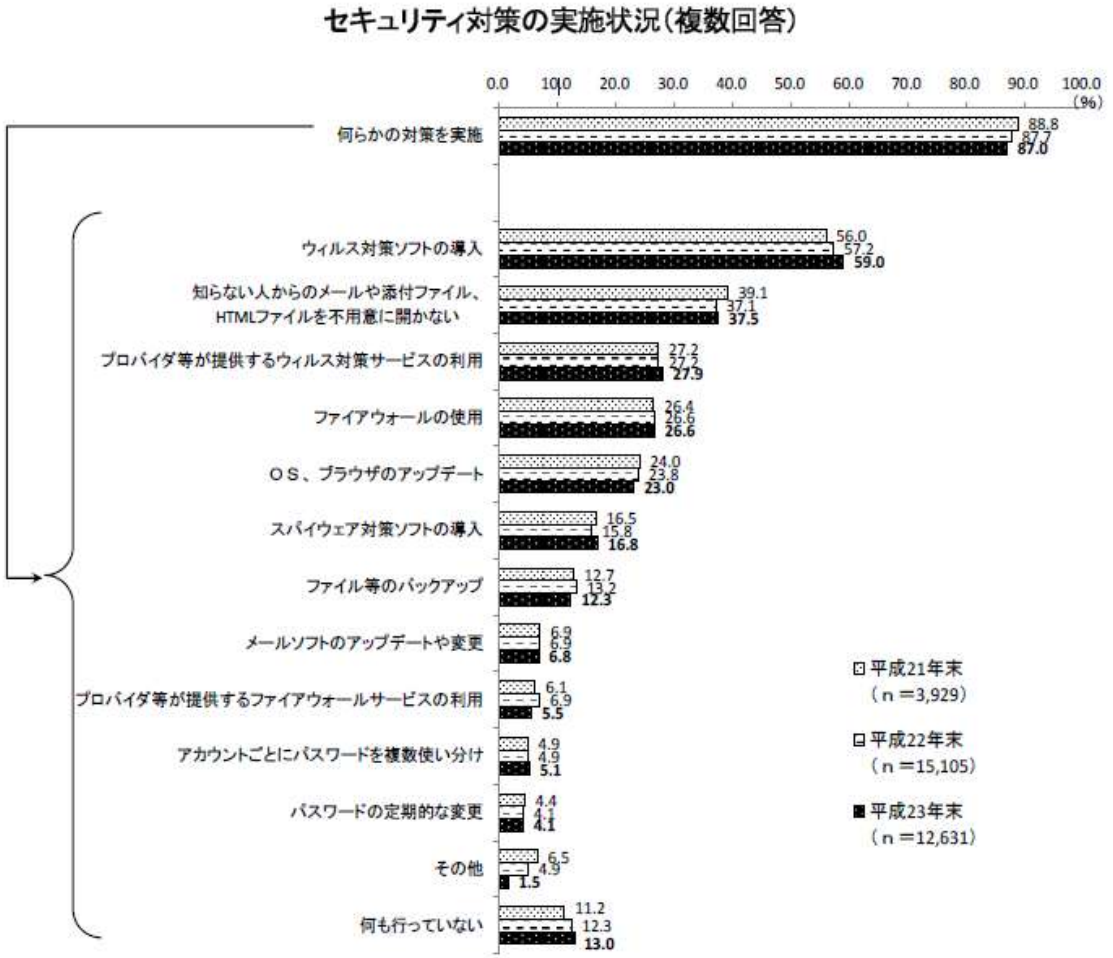
・12月
平成24年度情報セキュリティ月間における取組事項の集約

※随時メーリングリストを活用した意見交換を行う

参考資料

情報セキュリティ対策の実施状況（世帯）

インターネットを利用している世帯において、何らかのセキュリティ対策を実施している世帯の割合は87.0%である。何らかのセキュリティ対策を実施している世帯における対策内容をみると、「ウィルス対策ソフトの導入」が59.0%と最も多く、次いで、「知らない人からのメールや添付ファイル、HTMLファイルを不用意に開かない」（37.5%）、「プロバイダ等が提供するウィルス対策サービスの利用」（27.9%）となっている。

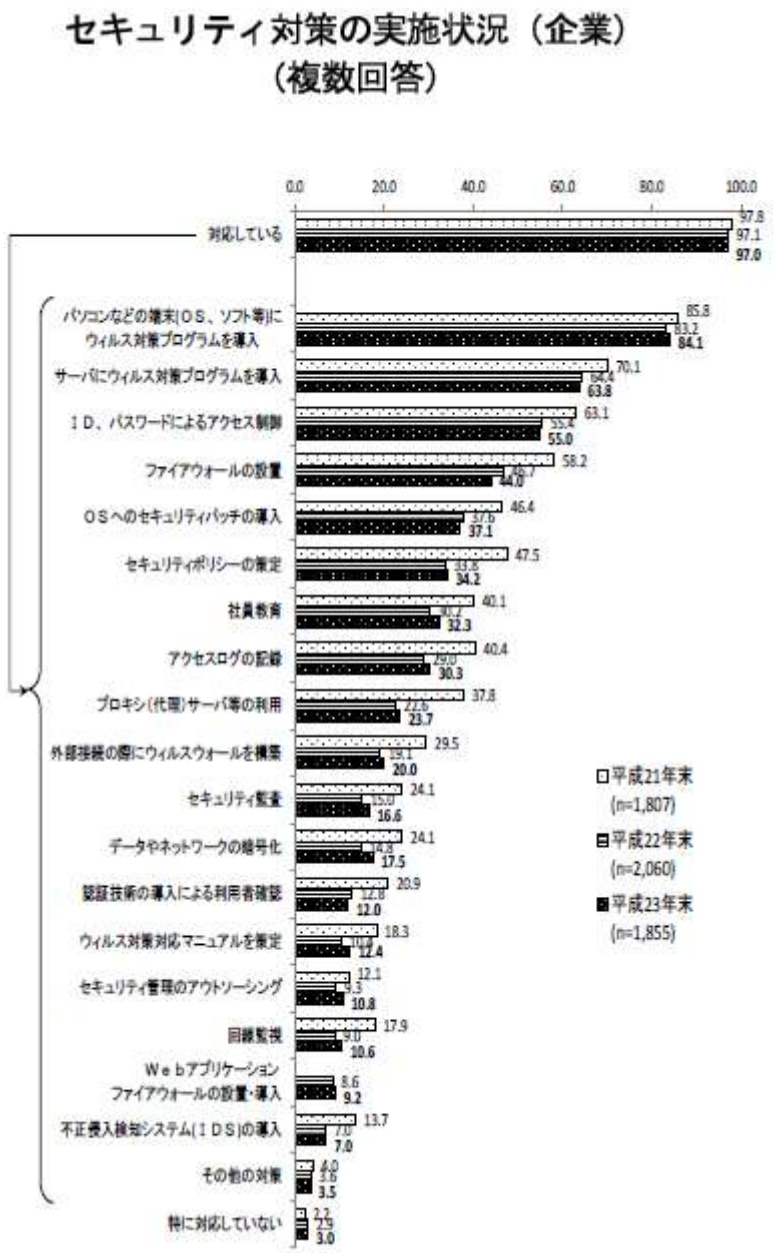


総務省「平成23年通信利用動向調査」平成24年5月

情報セキュリティ対策の実施状況（企業）

インターネット、企業内LAN等を利用する企業のうち何らかのセキュリティ対策を実施している企業の割合は、97.0%であった。

主な対策内容としては、「パソコンなどの端末（OS、ソフト等）にウィルス対策プログラムを導入」が84.1%と最も多く、次いで、「サーバにウィルス対策プログラムを導入」（63.8%）、「ID、パスワードによるアクセス制御」（55.0%）となっている。



総務省「平成23年通信利用動向調査」平成24年5月

情報セキュリティに関する脅威の動向

IPAの「2012年版 10大脅威（2012年3月22日）」では、標的型攻撃が1位、個人向けの脅威としてはスマートフォンやタブレットを狙った攻撃が6位に位置づけられている。

2012年版 執筆者会が選んだ10大脅威と脅威の変遷

IPA

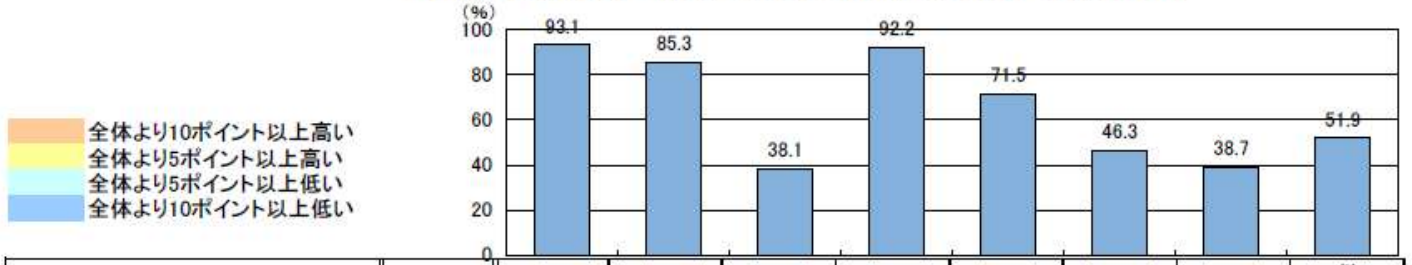
	2012年版10大脅威	2011年	2010年	2009年	2008年	2007年
1位	機密情報が盗まれる!? 新しいタイプの攻撃（標的型攻撃） 定番	5位	6位	3位	4位	2位
2位	予測不能の災害発生！ 引き起こされた業務停止 New	–	–	–	–	–
3位	特定できぬ、共通思想集団による攻撃 New	–	–	–	–	–
4位	更新忘れのクライアントソフトを狙った攻撃 定番	3位	2位	–	8位	–
5位	ウェブサイトを狙った攻撃 定番	2位	1位	2位	5位	9位
6位	スマートフォンやタブレットを狙った攻撃	4位	–	–	–	–
7位	大丈夫 !? 電子証明書に思わぬ落し穴 New	–	–	–	–	–
8位	身近に潜む魔の手・あなた職場は大丈夫？（内部犯行・情報漏洩の脅威） 定番	1位	5位	5位	3位	7位
9位	危ない！ アカウントの使まわしが被害を拡大 定番	–	8位	4位	–	8位
10位	利用者情報の不適切な取扱いによる信用失墜（プライバシーに係る問題） New	–	–	–	–	–

長い間、脅威と認識されながらも解消されない脅威の存在を無視できない。継続的に対策を行うことが組織に求められる

情報セキュリティに関する攻撃・脅威の認知

◆情報セキュリティに関する攻撃・脅威の認知は、『ワンクリック請求』(93.1%)、『フィッシング詐欺』(92.2%)、『スパイウェア』(85.3%)が上位3位。
◆『ボット』『マルウェア』の認知は4割を下回っている。
◆年代別でみると、60代で低い項目が目立ち、「ボット」「マルウェア」は全体を10ポイント以上下回る。
◆習熟度別では、最上級、上級レベルと初級、中級レベルの差が大きい項目が多い。

年代別・習熟度別　情報セキュリティに関する攻撃・脅威の認知

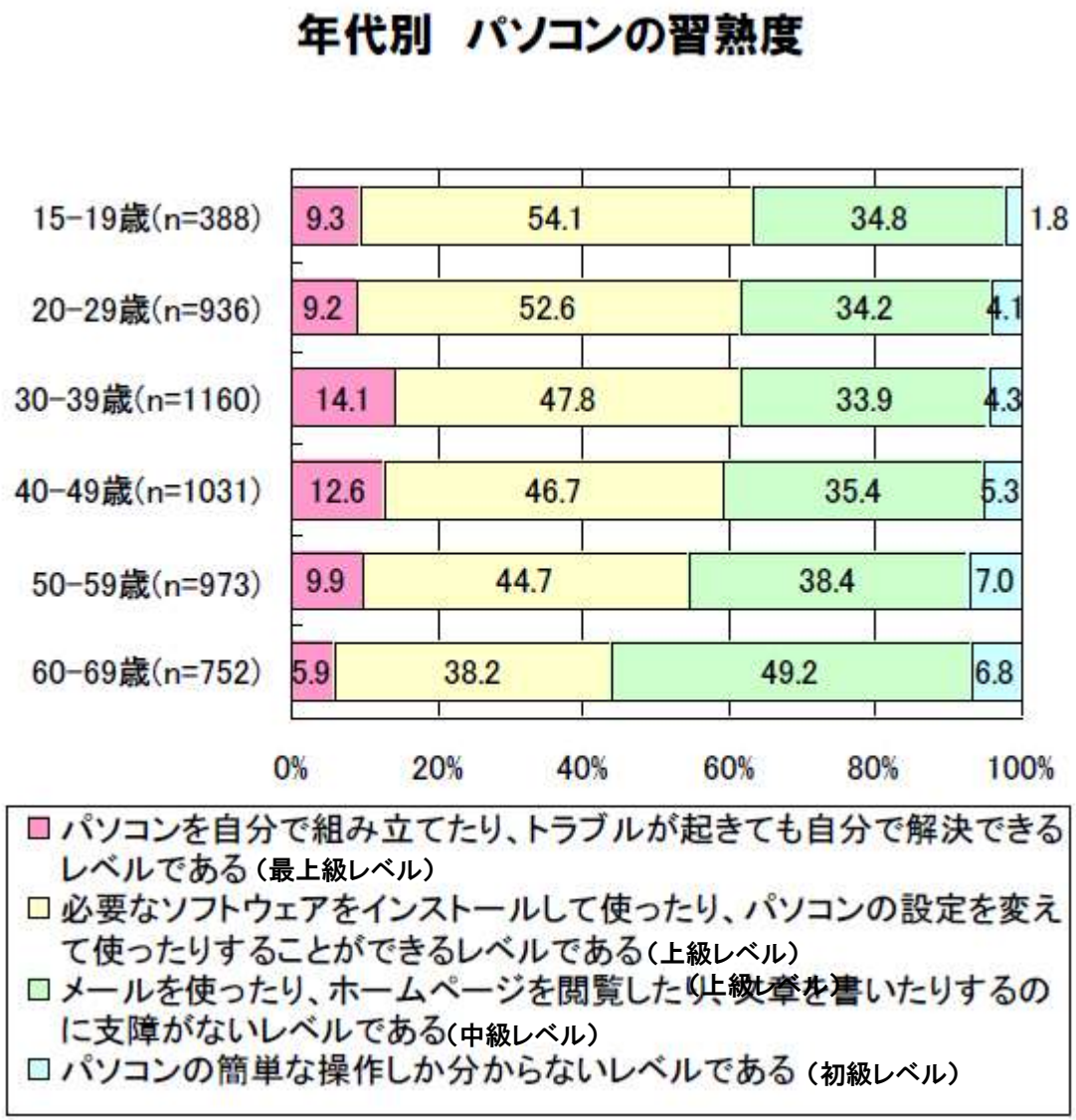


		n	ワンクリック請求	スパイウェア	ボット	フィッシング詐欺	セキュリティホール（脆弱性）	標的型攻撃	マルウェア	偽セキュリティソフト
全体	全体	5240	93.1	85.3	38.1	92.2	71.5	46.3	38.7	51.9
年代別	15-19歳	388	96.4	78.8	42.4	88.4	66.9	38.9	38.1	58.7
	20-29歳	936	96.1	83.5	46.4	90.7	70.7	44.4	45.4	53.5
	30-39歳	1160	94.7	87.5	43.8	93.0	74.3	48.8	47.0	55.0
	40-49歳	1031	93.3	87.6	40.0	94.1	75.1	49.3	40.3	51.4
	50-59歳	973	90.7	86.7	31.2	93.3	71.1	46.4	32.2	48.3
	60-69歳	752	87.5	82.8	23.3	91.3	66.7	44.4	23.8	47.0
パソコン習熟度別	最上級レベル	555	98.6	98.7	80.6	99.2	98.6	86.5	85.3	85.4
	上級レベル	2459	96.3	94.6	47.0	97.2	84.6	55.8	48.3	60.1
	中級レベル	1957	89.8	74.0	18.5	87.6	53.1	26.9	17.1	35.8
	初級レベル	269	75.0	55.8	13.0	67.7	31.6	18.2	12.3	24.9

※「詳しい内容を知っている＋概要をある程度知っている＋名前を聞いたことがある程度」の値

年代別 パソコンの習熟度

50代以下では上級ユーザの割合が高い。一方、60代では中級ユーザの割合が他年代より高く、上級ユーザを上回る。

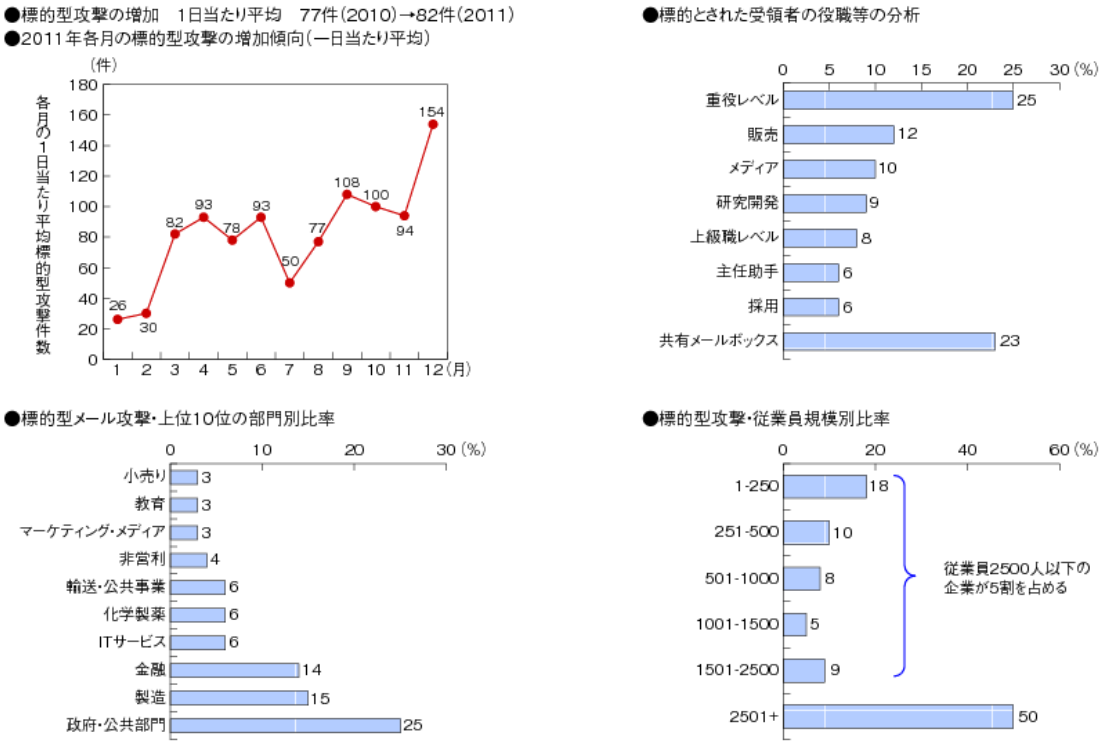


IPA「2011年度 情報セキュリティの脅威に対する意識調査」平成23年12月

標的型攻撃の増加

シマンテック社が2012年(平成24年)4月に公表したレポートによれば、2011年(平成23年)12月には一日平均154件の標的型攻撃が発生しており、その対象は、政府や大企業のみならず幅広い業種や中小企業に及び、職種も広範な範囲に及んでいるとしている。

世界における標的型攻撃の増加



(出典)総務省「情報通信白書」(平成24年)
(INTERNET SECURITY THREAT REPORT 2011Trends(Symantec社)より作成されたもの)

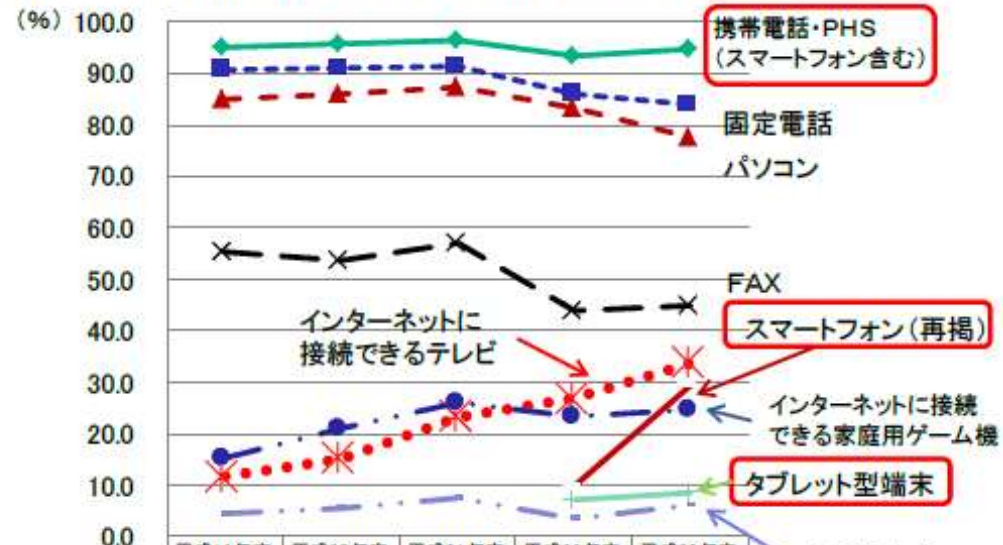
2011 年 11 月までの 12 カ月間、標的型攻撃を受けたシマンテック ドット クラウドの顧客企業は、世界全体で 46.2 社に 1 社の割合でした。しかし、日本だけで見ると、この割合が 9.5 社に 1 社と跳ね上がります。つまりシマンテック ドット クラウドの統計によると、日本企業は世界平均よりもはるかに高い確率で標的型攻撃を受けています。(Symantec社 ホワイトペーパー 日本における脅威の現状 2011年11月 より抜粋)

スマートフォンの世帯保有状況

スマートフォンの世帯保有状況は約30%であり、前年の約3倍と顕著な伸びを示している。

主要情報通信機器の世帯保有の状況

情報通信機器の普及が全体的に飽和状況の中、スマートフォン保有が顕著な伸び。



※無回答を除く

	平成19年末（n＝3,640）	平成20年末（n＝4,515）	平成21年末（n＝4,547）	平成22年末（n＝22,271）	平成23年末（n＝16,530）
携帯電話・PHS（スマートフォン含む）	95.0	95.6	96.3	93.2	94.5
固定電話	90.7	90.9	91.2	85.8	83.8
パソコン	85.0	85.9	87.2	83.4	77.4
FAX	55.4	53.5	57.1	43.8	45.0
インターネットに接続できるテレビ	11.7	15.2	23.2	26.8	33.6
インターネットに接続できる家庭用ゲーム機	15.2	20.8	25.9	23.3	24.5
タブレット型端末				7.2	8.5
その他インターネットに接続できる家電（情報家電）等	4.3	5.5	7.6	3.5	6.2
（再掲）スマートフォン				9.7	29.3

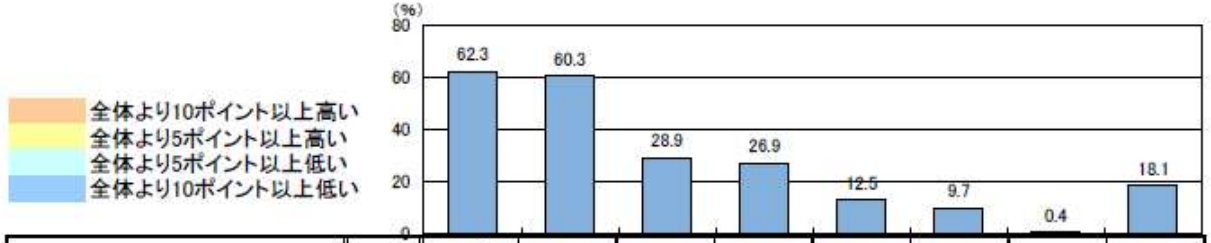
※「携帯電話・PHS（スマートフォン含む）」は、平成22年末以降において、スマートフォンを内数に含む。
平成23年末のスマートフォンを除いた場合の保有率は89．4%である。

総務省「平成23年通信利用動向調査」平成24年5月

スマートフォンのセキュリティ対策の実施状況

◆現在実施している情報セキュリティ対策は「OSのアップデート」(62.3%)、
「信頼できる場所からアプリをインストールする」(60.3%)が上位。
◆現在実施している情報セキュリティ対策を年代別でみると、20代で低い対策が目立つ。
◆習熟度別にみると、習熟レベルが高いほどセキュリティ対策の実施率も高い傾向。

スマートフォンのセキュリティ対策の実施状況



		n	OS（オペレーティングシステム）のアップデート	信頼できる場所（公式サイト）からアプリをインストールする	アプリをインストールする前にアクセス許可を確認する（Android のみ）	セキュリティソフトの導入	リモートロック等の不正利用防止機能	データ（個人情報等）の暗号化による紛失時の対策	その他	特にない
全体	全体	973	62.3	60.3	28.9	26.9	12.5	9.7	0.4	18.1
年代別	15-19歳	89	64.0	56.2	25.8	20.2	13.5	12.4	1.1	16.9
	20-29歳	282	55.3	55.0	28.4	20.9	11.0	9.9	0.4	22.7
	30-39歳	267	65.2	62.9	30.7	29.6	14.6	8.6	0.7	15.7
	40-49歳	185	65.4	64.3	28.1	34.1	12.4	7.6	－	16.2
	50-59歳	109	66.1	61.5	32.1	28.4	12.8	12.8	－	17.4
	60-69歳	41	63.4	68.3	22.0	29.3	7.3	9.8	－	14.6
パソコン習熟度別	最上級レベル	178	82.6	70.2	38.2	38.2	27.0	19.1	1.1	5.1
	上級レベル	537	67.0	63.1	29.4	27.4	11.4	8.4	0.2	15.3
	中級レベル	233	39.5	49.8	21.9	18.5	5.6	6.0	0.4	30.5
	初級レベル	25	28.0	28.0	16.0	16.0	－	4.0	－	56.0

（※初級レベルはn数が30未満のため参考値）

スマートフォン情報セキュリティ3か条

（利用者が最低限取るべき情報セキュリティ対策）

スマートフォンは、アプリケーションを活用することで、様々な機能を自由に追加できる便利な携帯電話です。しかし自由さの反面、その中には危険なアプリケーションが混じっている場合もあります。利用者自身で情報セキュリティ対策を取ることが必要です。

盗難・紛失対策や他人による不正利用防止対策など、従来の携帯電話と同様の対策が必要です。さらにスマートフォンにおいては、次の３つの対策が大切です。

1．ＯＳ（基本ソフト）を更新

スマートフォンは、ＯＳの更新（アップデート）が必要です。古いＯＳを使っていると、ウイルス感染の危険性が高くなります。更新の通知が来たら、インストールしましょう。

2．ウイルス対策ソフトの利用を確認

ウイルスの混入したアプリケーションが発見されています。スマートフォンでは、携帯電話会社などによってモデルに応じたウイルス対策ソフトが提供されています。ウイルス対策ソフトの利用については、携帯電話会社などに確認しましょう。

3．アプリケーションの入手に注意

アプリケーションの事前審査を十分に行っていないアプリケーション提供サイト（アプリケーションの入手元）では、ウイルスの混入したアプリケーションが発見される例があります。ＯＳ提供事業者や携帯電話会社などが安全性の審査を行っているアプリケーション提供サイトを利用するようにしましょう。インストールの際にはアプリケーションの機能や利用条件に注意しましょう。