



Information-technology
Promotion
Agency, Japan

情報セキュリティ月間 キックオフ・シンポジウム 参考資料

2013年2月1日

独立行政法人情報処理推進機構

技術本部 セキュリティセンター

調査役 加賀谷 伸一郎

「スマートフォン の 利活用 とセキュリティ対策」

関連資料

急増するスマートデバイス向けウイルスIPA

※特にAndroid向けウイルス



出典: AV-TEST

<http://www.av-test.org/en/tests/mobile-devices/android/>

SNSやメールで不正アプリサイトへ 誘導する事例(2012年9月)



Facebookの
某コミュニティに
投稿されていた、
不正アプリサイト
へのリンクを
含んだ投稿

SNSやメールで不正アプリサイトへ 誘導する事例(2012年9月)

IPA

※Androidの事例

Subject:スマホの電池切れを解消！便利アプリを紹介[APP マグ]

Date:2012/09/24 11:30

To:●●@i●.jp

今回はアプリを紹介します。

電池バッテリー改善アプリ

<http://●.net/●/◆◆.html>

スマホの電池切れを解消する、画期的なアプリが出ました。
このアプリを入れるだけで、朝充電して帰宅まで充電が不要になりました。
有料版や無料版を数多く試してきましたが、
今のところこのアプリが「ベスト」です。
バージョンアップの期間中だけ、無料でダウンロードが可能です。
今すぐ試してみてください！

安心スキャン

<http://●.net/●/▼.html>

一番最初に入れたいウイルス対策アプリ。
軽い動作と、常に最新のウイルス対策パターンをダウンロードします。
無料でさくっとスキャン出来るのは魅力的。
定期的に行えば安心ですね♪

* =====* APPSマグ *

◆編集・発行:便利アプリを紹介！APPマグ

◇配信停止・配信先の変更 <http://●.net/●/>

◆Copyright(C) 2011-2012, APPSマグ

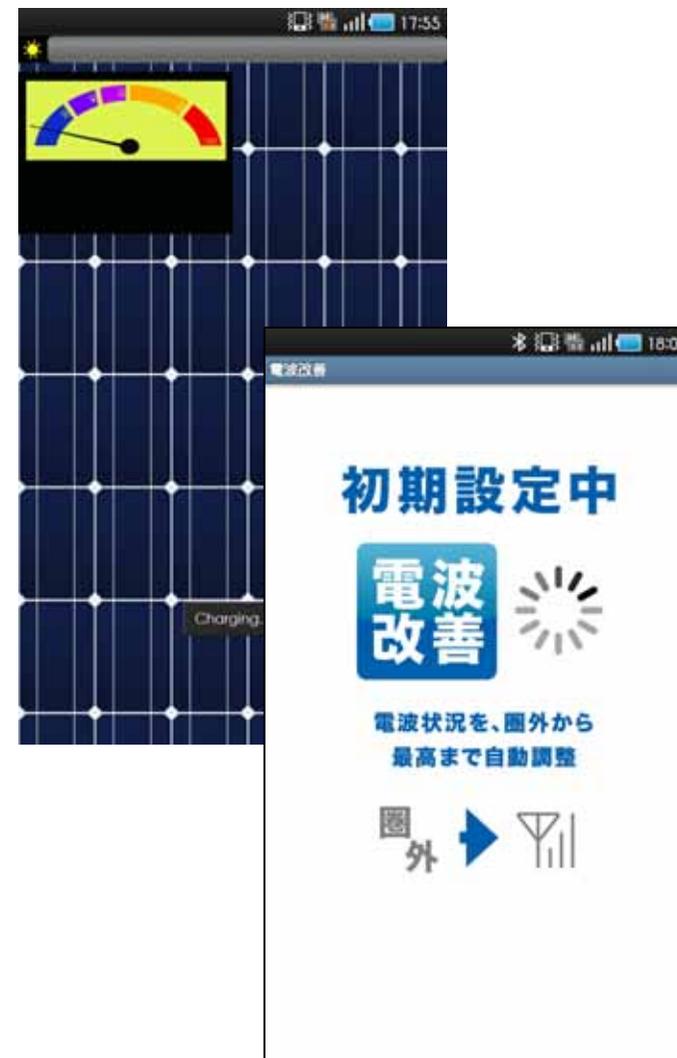
◇本メールマガジンの著作権はAPPSマグに帰属します。、
記事の無断転載は堅くお断りします

リンクをタッチすると、不正アプリが
置かれているサイトに飛ばされる！

SNSやメールで不正アプリサイトへ 誘導する事例(2012年9月)



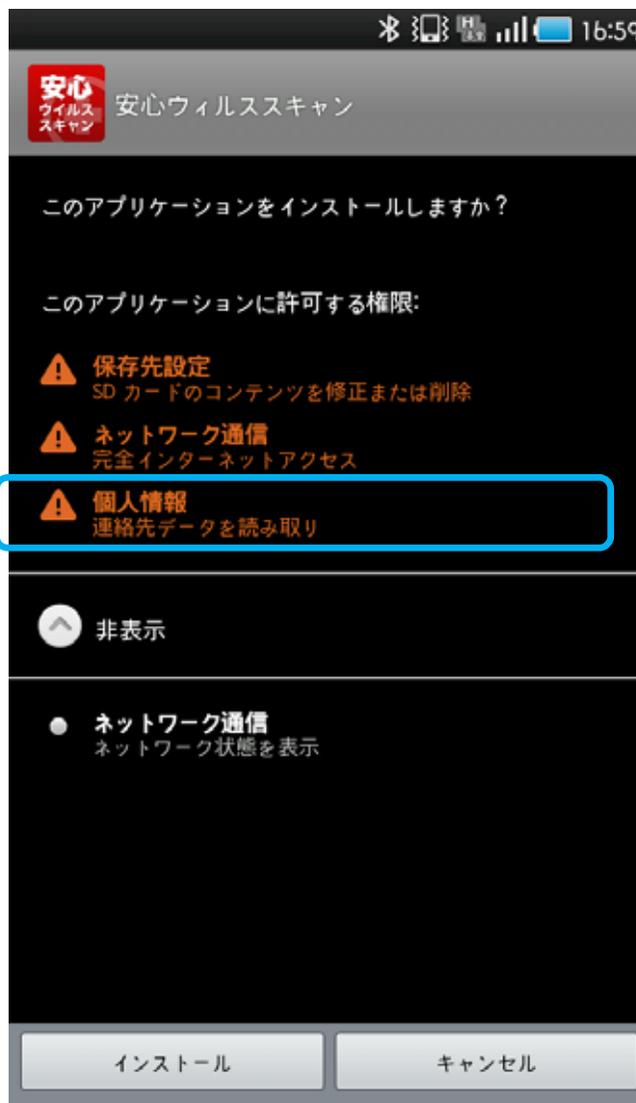
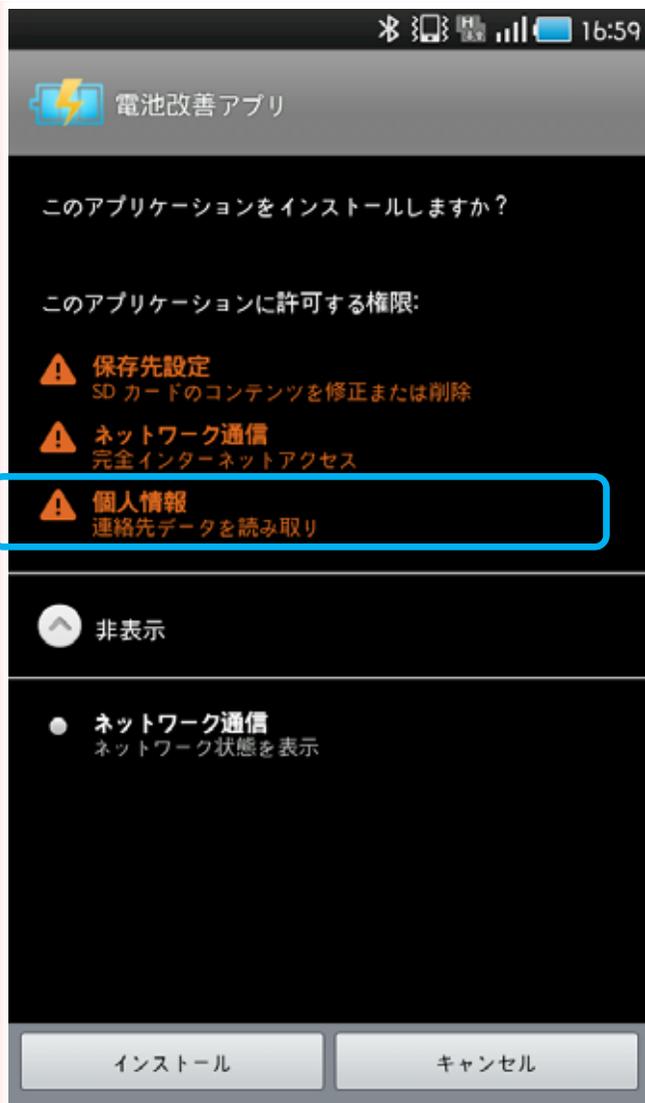
※Androidの事例



SNSやメールで不正アプリサイトへ 誘導する事例(2012年9月)

IPA

※Androidの事例



インストール時、
「連絡先データを読み取り」の許可
を求めてくる！

スマホ内から情報が送られている様子 **IPA**

①: 実際に悪意ある攻撃者に送られている情報

original:

```
test = 1%3A%E3%81%84%E3%81%B1 %E6%AC%A1%E9%83%8E%3A999-  
9999%3Ajiro.t01c%40virus.ipa.go.jp%2F2%3A%E5%B1%B1%E7%94%B0  
%E5%A4%AA%E9%83%8E%3A888-8888%3Ayamada.taro.t01c%40virus.ipa.go.jp%2F
```

decode:

```
test = 1:いば 次郎:999-9999:jiro.t01c@virus.ipa.go.jp/2:山田 太郎:888-  
8888:yamada.taro.t01c@virus.ipa.go.jp/
```

②: ①をIPAが目で見えてわかるように変換した内容

最新の不正アプリ(2013年1月)-1



最新の不正アプリ(2013年1月)-2

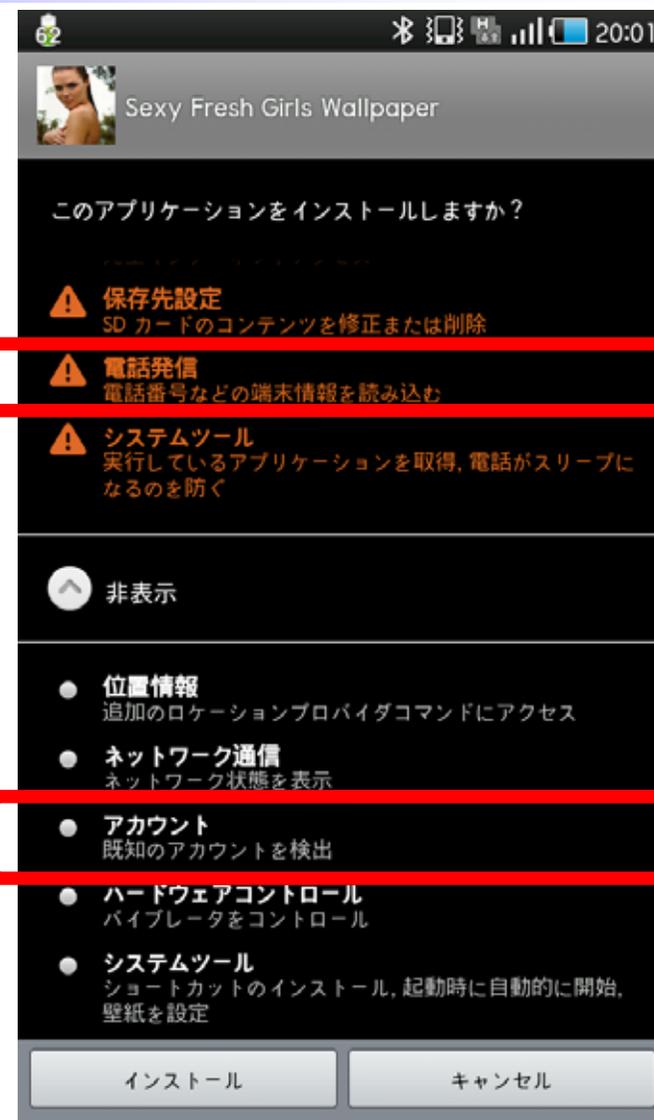
ウェブブラウザの画面なのに、あたかも公式マーケットであるGoogle Playの画面に酷似！

公式マーケットに存在した不正アプリの特徴(2012年4月)

項番	特徴	アプリ配布場所における名称	インストール後の名称
1	有名なアプリ、ほかのスマートフォンOSで人気のアプリ名を含む	ウォーリーを探せ the Movie	ユーチューブ動画
		うまい棒をつくろう! the Movie	youtube動画まとめ
		ギャングハウンド the Movie	グラビア動画
		スヌーピーストリート the Movie	笑える動画
		チャリ走-the Movie	ようつべ動画まとめ
		ひよ盛り the Movie	面白動画まとめ
		メガ盛ポテ the Movie	芸能動画
		空手チョップ! The Movie	ニコニコ動画まとめ
		大盛モモ太郎 the Movie	youtube動画
		桃太郎電鉄the Movie	ようつべ動画
		魔界村騎士列伝 THE MOVIE	暇つぶし動画
		連打の達人 the Movie	ユーチューブ動画まとめ
2	個人的嗜好をくすぐる文字列を含む	FC2動画まとめ the Movie	怖い動画
		けいおん-K-ON!動画	アニメ動画
		スク水動画まとめ	美人動画
3	実用性を感じさせる文字列を含む	3D視力回復 THE MOVIE	泣ける動画

電話帳の内容を盗むものだった

公式マーケットに存在した不正アプリの実例(2013年1月)



スマートフォンのセキュリティ対策



スマートフォンを安全に使用するための6か条

- 1 スマートフォンをアップデートする。
- 2 スマートフォンにおける改造行為を行わない。
- 3 信頼できる場所からアプリケーション(アプリ)をインストールする。
- 4 アンドロイド端末では、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。
- 5 セキュリティソフトを導入する。
- 6 スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

※詳細の解説については、以下のページを参照してください。

<http://www.ipa.go.jp/security/txt/2011/08outline.html>

アプリインストール時の注意

- 公式マーケットにあるアプリでも、念のため、アプリに許可する**権限**や、**評判**を読み取る！



パスワードを教えるてはいけません！！ IPA



スマホよく
わかんない...



このアプリ入れて
設定してあげる！



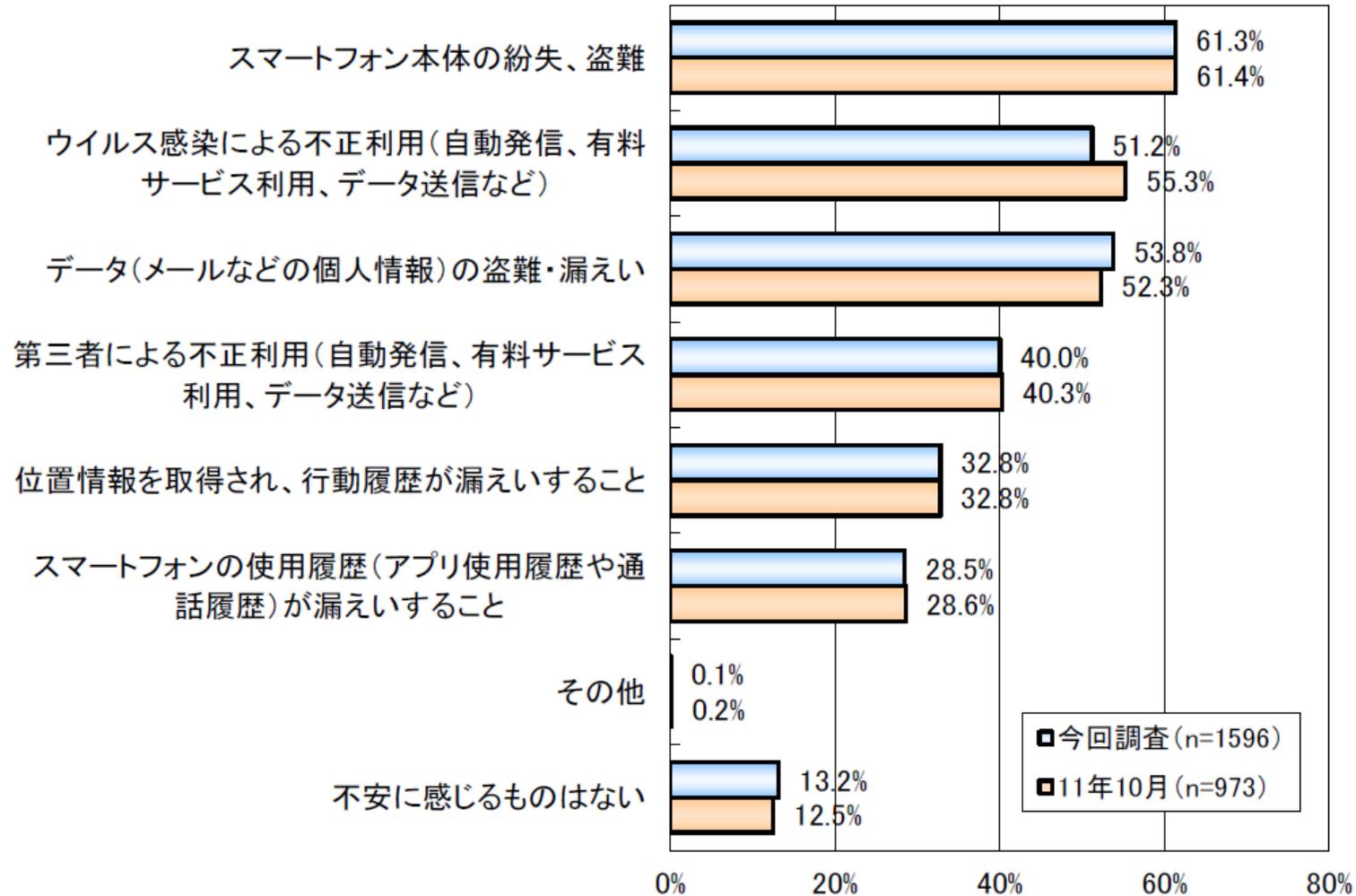
- ・セキュリティアプリ
- ・ID、パスワード登録
- ・各種設定



今どこにいるかな・・・
このアプリ入れちゃおうかな・・・

スマートフォン利用時の不安要素

※対象：現在スマートフォンを利用している人



出典：IPA「2012年度 情報セキュリティの脅威に対する意識調査」報告書

<http://www.ipa.go.jp/security/fy24/reports/ishiki/>

スマホ: 端末ロックの落とし穴

Android



スマートフォンでの写真撮影に注意！

某フリーソフト (Windows用)

画像ファイル

画像ファイルに含まれる情報を基に地図上に位置表示！！

メーカー	Apple
機種	iPhone 4S
著作権者	
撮影日時	2012/02/24 12:16:02
最終更新日	2012/02/24 12:16:02
画像サイズ	3264X2448
経度・緯度	北緯35度43分48.6秒 東経139度44分59.4秒
GoogleURL	maps.google.co.jp/maps?geocode=&q=35.7301666
コメント	

一般利用者向けの啓発資料



http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/

一般利用者向けの啓発資料



IPA Channel: 情報セキュリティ普及啓発映像コンテンツ
<http://www.youtube.com/user/ipajp/videos?view=1>

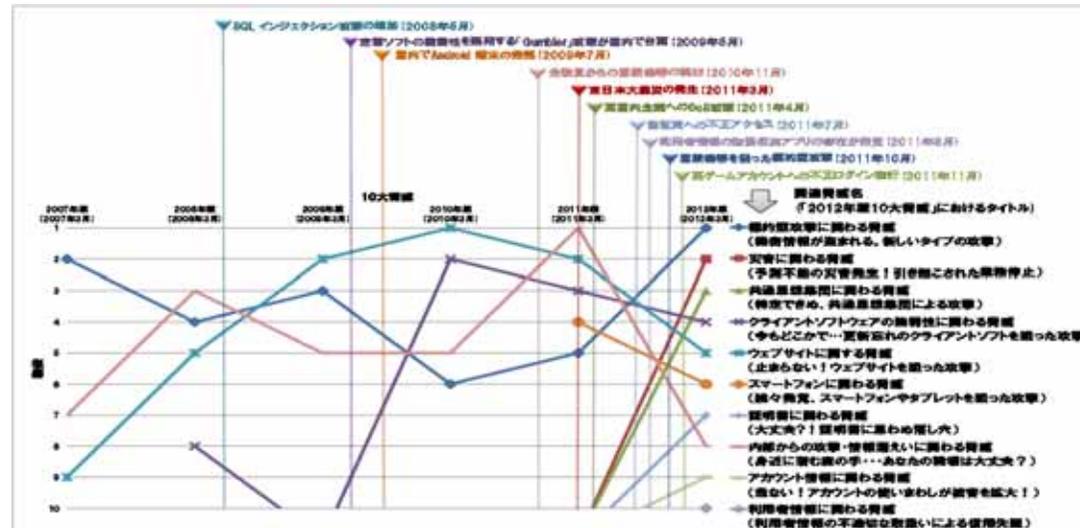
「企業等における サイバー攻撃対策」

関連資料

10大脅威から見る脅威の変遷

2012年
10大脅威

IPA

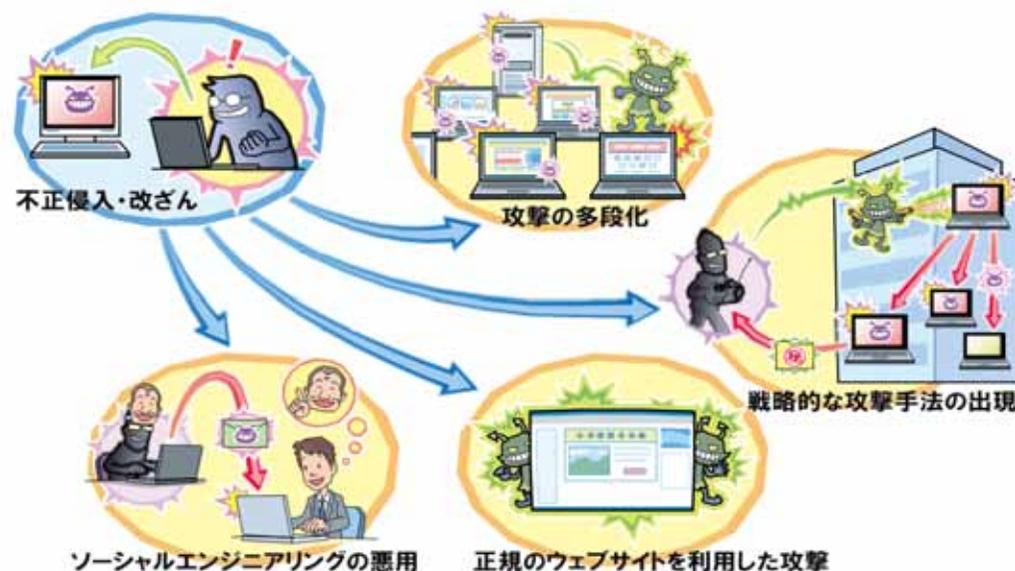


● 傾向

- 新しいデバイス・サービスの出現により新たな脅威が生まれる
 - スマートフォン、クラウドサービスの浸透など
 - ⇒ **定期的なセキュリティ対策の見直しを**
- 長い間、脅威と認識されながらも対策が進まない脅威の存在
 - 情報漏洩、標的型攻撃、ウェブサイト攻撃、Clientソフトへの攻撃
 - ⇒ **常に発生する脅威に対する対策コストの予算化を**

1. 攻撃手法の変化

～「1つの脆弱性＝1つの攻撃」から人を騙すテクニックや洗練した手法が登場～



● 近年の傾向

- 複数の攻撃を駆使した多段型の攻撃に
- 正規のウェブサイトを使った攻撃。利用者は攻撃に気付けない
- システム的な弱点だけでなく、人の心理面をつくソーシャルエンジニアリング
- 複数の攻撃を戦略的に使う攻撃手法の出現

2. システム環境の変化

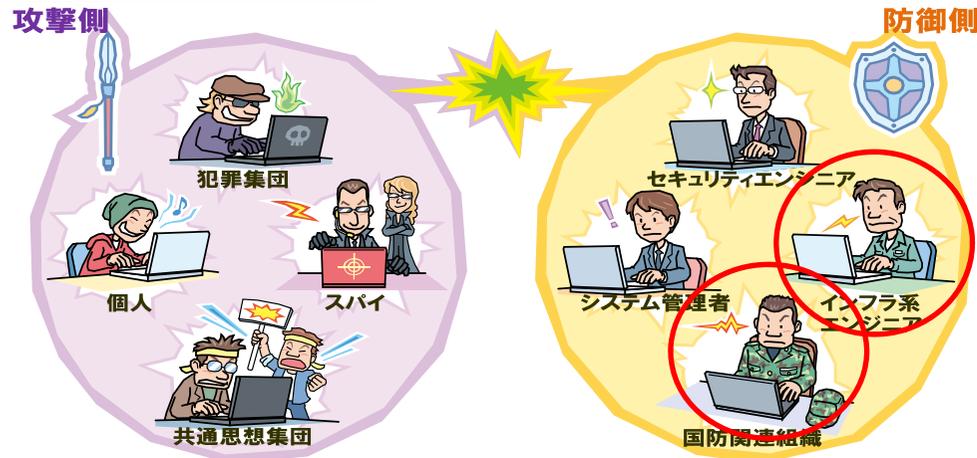
～システム環境の変化により、新たな脅威が生じる～



- システム環境の変化により下記のような脅威が発生
 - － ネットワークに接続する新たなデバイスの登場
 - 外部から攻撃を受ける脅威に晒される状態
 - 個人に紐づく情報を保持するスマートフォンは、攻撃への影響が大きい
 - － 制御系システムのオープン化
 - クローズド⇒オープン化 になったことにより情報システムと似た環境に
 - 攻撃者にとって攻撃しやすい環境になってきた
 - － クラウドの台頭により、データ管理の考え方が変わる

3. 情報セキュリティを取巻く構図の変化IPA

～一企業の情報セキュリティ対策からナショナルセキュリティへ～



● 防御側の構図の変化

－ 制御系・組込み系システムへの拡大

- 制御・組込系システムが攻撃対象に含まれてきた
- 制御系エンジニアにも、セキュリティ対策が求められるようになった
- 情報系システムだけの問題で無くなってきている

－ ナショナルセキュリティとしての対応

- 米国国防省は、サイバー空間を陸、海、空、宇宙に次ぐ第5の新たな戦場と宣言
- サイバー攻撃が軍事活動、経済活動的な意味合いに変化してきている
- 政府機関や軍需関連産業まで巻き込んだ防衛体制となりつつある

4. 攻撃によるインパクトの変化

～一企業の不祥事だった問題が社会的問題に～

IPA



- インシデントが発生した際の組織に与えるインパクトも増大している
 - － 機密情報が窃取されることで…。
 - 知的財産…模倣品出現⇒市場での競争力の低下⇒企業収益の低下
 - 国家機密情報…外交上のアドバンテージを奪われる⇒国益に影響
 - 長期的な視点で考えると、将来の利益や国益が奪われる大きな問題
 - － 情報の大量流出(メガリーク)することで…。
 - 大手ゲームメーカーの例では、1ヶ月近くサービスを停止せざるをえない状況
 - ブランドイメージの大幅な低下、営業利益にも影響
 - 一企業の不祥事的な扱いから社会的な問題に
 - － 社会インフラを狙った攻撃
 - 海外では、工場プラントや鉄道システムが攻撃により一時停止した事例がある
 - 社会インフラが攻撃を受けた場合、我々の社会生活にも大きく影響する
ex.電力供給停止、鉄道停止、工場停止 etc

【1位】機密情報が盗まれる!?

新しいタイプの攻撃

2012年
10大脅威

IPA



● 脅威

- 組織の機密情報が窃取されてしまう
- 攻撃に気付けない。有効な対策方法がない

【1位】機密情報が盗まれる!?

新しいタイプの攻撃

- **事例1:衆議院への攻撃**

- 衆議院議員1人のパソコンで、ウイルス付きのファイルを開いたことでウイルスに感染
- ネットワークを經由して感染範囲が拡大しサーバとパソコン計32台がウイルスに感染した。
- 全議員約480人のIDとパスワードが流出し、最大15日間にわたってメールが攻撃者に見られていた可能性

- **事例2:三菱重工業へのサイバー攻撃**

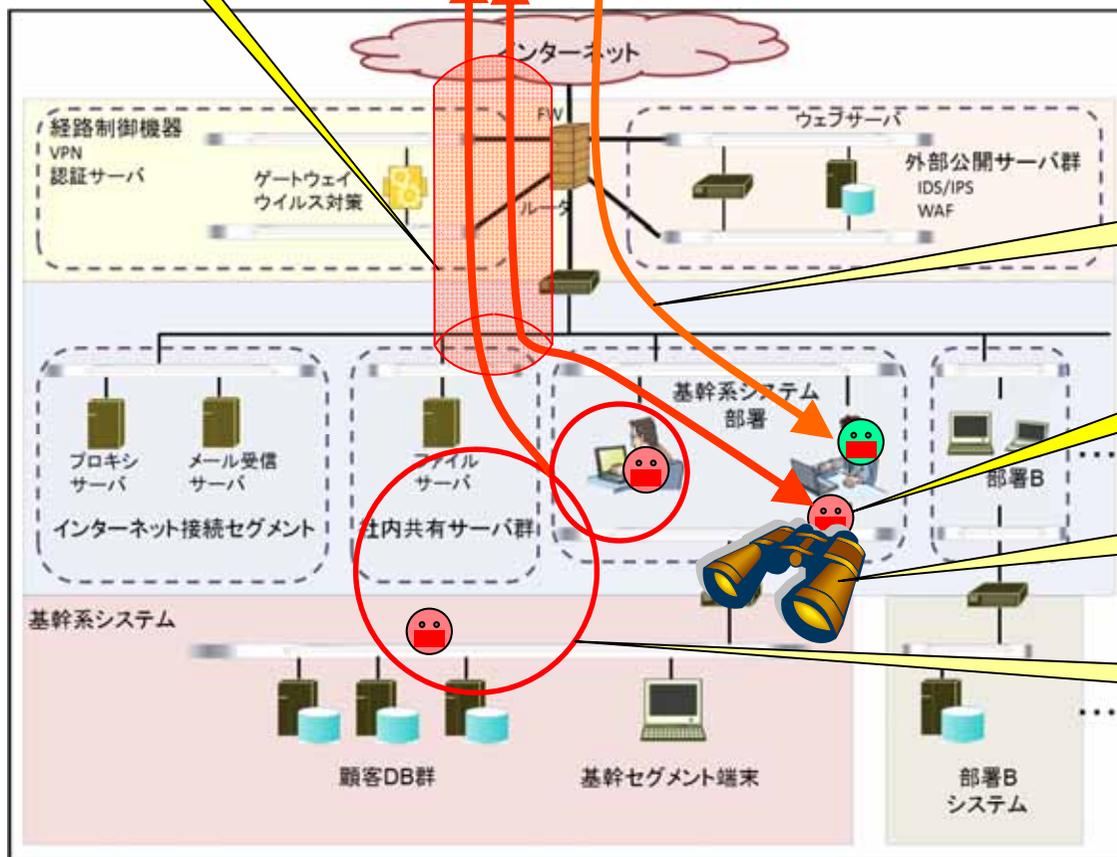
- 外部からの標的型攻撃メールにより、システム内部に侵入したとされている
- 本社のほか工場、研究所など国内11拠点にあるサーバ45台と従業員が使用していたパソコン38台の感染が確認された

【1位】機密情報が盗まれる!?

新しいタイプの攻撃 ~ 攻撃の特徴 ~

ウイルスを使って深部に空けたバックドア（裏口）を用いて攻撃基盤を構築し、システムをハッキング

初期潜入に成功後、バックドアを設置まで素早く数分。その後はバックドアを使ってマルウェアの機能を拡張し、攻撃基盤を構築。



事前調査

初期潜入段階

攻撃基盤構築段階

システム調査段階

攻撃最終目的(窃取)の遂行

【1位】機密情報が盗まれる!?

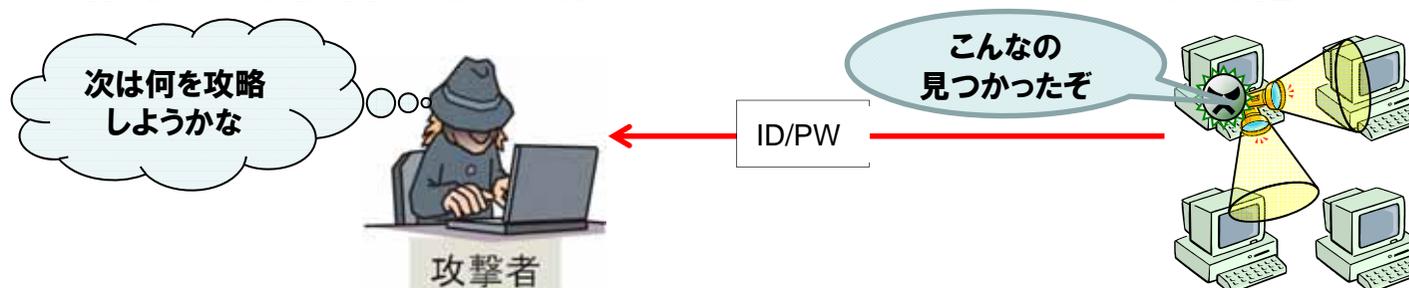
新しいタイプの攻撃 ~ 対策の難しさ ~

● 攻撃が検知できない

- ウイルスの通信は、HTTPなどオフィス環境で使用する通信と同じため、攻撃を検知することができない

● 攻撃者がシステムの状況に応じて攻撃方法を変える

- 攻撃者が送り込むウイルスがスパイ活動を行い、内部のシステム状況に応じて、攻撃を仕組んでくる
- アカウント・パスワード情報などのセキュリティを確保する上で前提となる情報が攻撃者の手に渡り、**セキュリティシステムが無効化される**



● 巧みなソーシャルエンジニアリング

- 事前調査段階で窃取した情報が標的型メールとして使用されるため、**標的型メールと気付けない**

【1位】機密情報が盗まれる!?

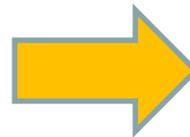
新しいタイプの攻撃

- 対策

- 外部からの脅威をブロックする「**入口対策**」
- 情報が外部に持出されない為の「**出口対策**」



詳細はこちら

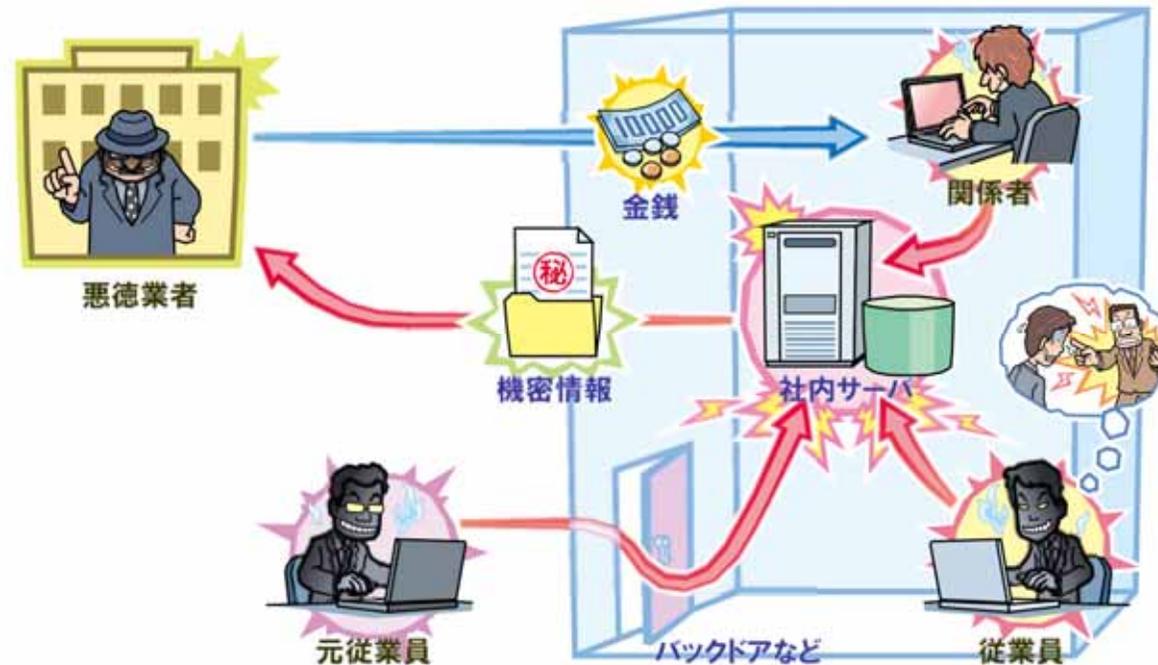


<http://www.ipa.go.jp/security/vuln/newattack.html>

【8位】身近に潜む魔の手・・・ あなたの職場は大丈夫？

2012年
10大脅威

IPA



● 脅威

- 組織内部の人による故意の情報流出や業務妨害
- 関係者による犯行が行われた場合、影響範囲が大きい
- 内部情報を知っている人による、人為的な犯行である為、完全な対策を実施することは難しい

【8位】身近に潜む魔の手… あなたの職場は大丈夫？



- **事例1：国内通信会社のデータ改ざんによる営業妨害**
 - － 業務委託先の元社員により、基地局とネットワークセンターを結ぶATM 伝送装置の回線設定データが改ざんされる事件が発生
 - － 携帯電話サービスが対象地域で利用しにくい状態になり、約7万2,700人の利用者が影響を受けた
- **事例2：国内クレジット会社の顧客情報の漏えい**
 - － 国内クレジット会社では、最大約16万人分の顧客情報が不正に持ち出され、売却された可能性が高いことが判明した
 - － 過去に保険代理店事務に関わる委託をしていた関係者からの犯行
- **事例3：ソーシャルゲームにおけるデータ改ざん**
 - － ソーシャルゲームのサーバに元派遣社員が不正アクセスして約130万人が利用するゲームを改ざん
 - － 元派遣社員は、任期満了で退社する際に、サーバ内に不正アクセス制限を解除できるプログラムを仕込んでいた

【8位】身近に潜む魔の手… あなたの職場は大丈夫？

- **対策1:「物理的対策」と「システムの対策」**
 - － 重要な情報が保存されている場所や操作を行う場所への入場を制限するなどの「物理的対策」
 - － 重要システムへのアクセス制限を行う「システムの対策」
- **対策2:職務権限の分離**
 - － 作業実施者と承認者を分けることにより、不正を行いにくくする環境を構築する
 - － 運用を形骸化させないためにも、定期的に運用状況のチェックや見直しを行うことが重要
- **対策3:情報漏えい発生時の事後対応の計画**
 - － 問題が発生時にいかに早く通常業務に戻せるかが事後対応の鍵となる
 - － 情報漏えいを起こした際の事後対応も事前に計画しておく必要がある

【8位】身近に潜む魔の手・・・ あなたの職場は大丈夫？

- 対策例 ～IPAテクニカルウォッチ
『組織の内部不正防止への取り組み』に関するレポート～

(出典)5 カテゴリ 25 分類は、社会安全研究財団：「環境犯罪学と犯罪分析」 P191 を参考とし、
セキュリティ対策の例を IPA 作成

- 犯行を難しくする
- 捕まるリスクを高める
- 犯行の見返りを減らす
- 犯行の挑発を減らす
- 釈明させない

詳細はこちら



5 カテゴリと 25 分類	IT セキュリティ対策の例
犯行を難しくする	
対象を防御的に強化する	スクリーンロック、アクセス制御、パスワードポリシー、物理チェーンロックなど
施設への出入りを制限する	登録者のみの入場、手荷物検査など
出口の検査	登録者のみの退場、手荷物検査、メールや秘密パスの検査
犯罪者をそらす	通路、出入り口の閉鎖、金属探知機
道具や武器を制御する	非登録の PC/USB メモリの持ち込み禁止、携帯電話禁止、メール・ネットの利用制限・禁止
捕まるリスクを高める	
監視者を増やす	複数人での作業環境、特権階級の分散化、個人情報売買の監視、防犯ベル
自然監視を補佐する	守りやすい空間設計、オフィスのフリースペース化、投書箱による密告者のサポート
匿名性を減らす	IC カードや社員証バッジの携帯、名前が判明可能な ID による管理
現場管理者の利用	CCTV(監視カメラ)の設置、機密情報への複数人での操作、アクセスログの監視
フォーマルな監視体制を強化する	侵入等警報装置、警備員
犯行の見返りを減らす	
標的を隠す(存在がわからない)	電子ファイルのアクセス権限の設定、電子機器の保管手法
対象を排除する(存在をなくす)	電子ファイルのアクセス権限の設定、紙の廃棄、溶解処理
所有物の特定	PC に登録シールをつける、ファイルや紙データに管理 ID を付ける
市場を阻止	情報売買の規制、許認可等
便益を与えない	ファイルの暗号化、情報にノイズや電子すかしなどを挿入
犯行の挑発を減らす	
欲求不満やストレスを減らす	職場での円滑なコミュニケーションの推進、適切な人事・作業管理など
対立(紛争)を避ける	職場での円滑なコミュニケーションの推進、適切な人事・作業管理など
誘惑や興奮の低減	職場での円滑なコミュニケーションの推進、適切な人事・作業管理など
仲間からの圧力を緩和する	職場での円滑なコミュニケーションの推進、適切な人事・作業管理など
模倣犯を阻止する	インシデントの手口の公表を慎重にする、インシデントの証跡を残さないなど
釈明させない	
規則を決める	情報セキュリティポリシーの策定、管理・運用策の策定、就業規則、雇用契約など
指示を掲示する	情報セキュリティポリシーの掲示、管理策の掲示、就業規則の掲示など
良心に警告する	ルール順守への自己サイン、持ち出し厳禁等の表示
遵守を補佐する	PC/USB 持ち出し手続きの簡素化、シュレッダーの設置など
薬物・アルコールを規制する	職場での飲酒禁止、アルコールなしの行事

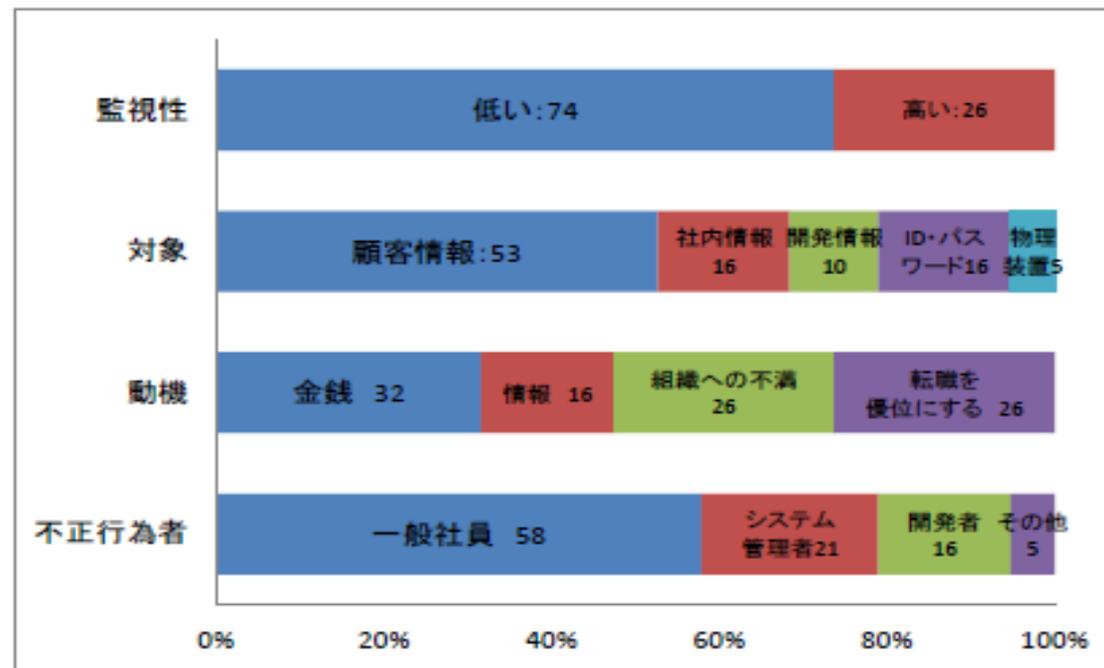
<http://www.ipa.go.jp/about/technicalwatch/pdf/120315report.pdf>

【8位】身近に潜む魔の手・・・ あなたの職場は大丈夫？

- **内部不正の状況**

～IPAテクニカルウォッチ

『組織の内部不正防止への取り組み』に関するレポート～

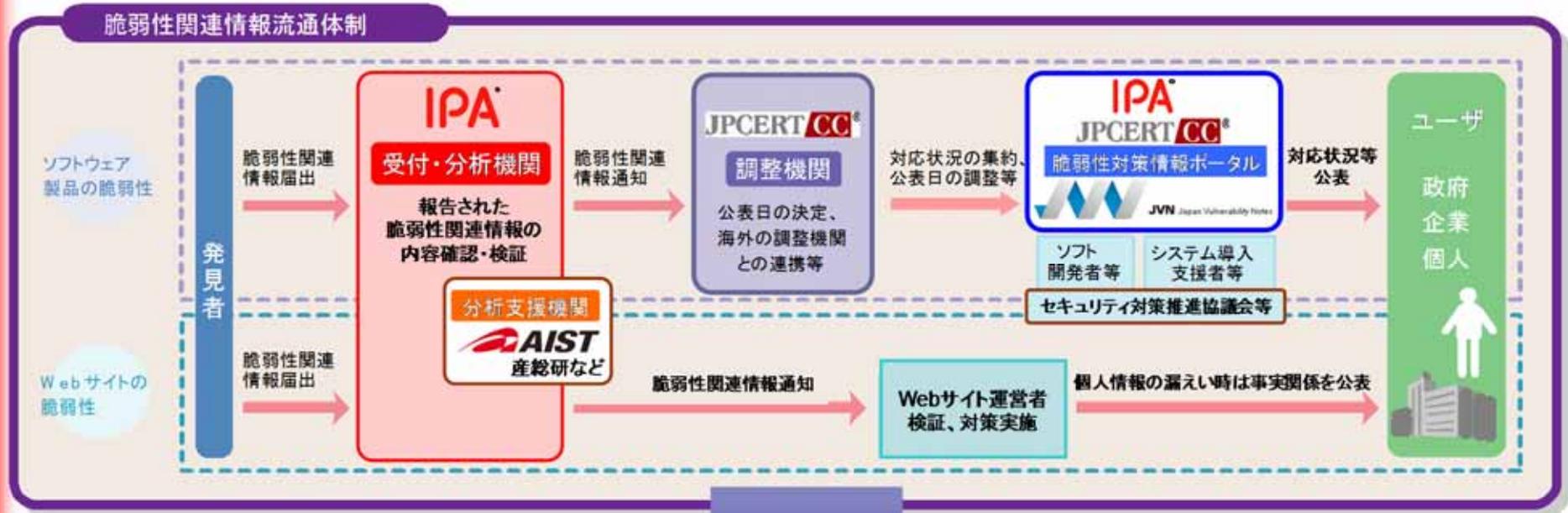


- 顧客情報や社内情報が窃取される状況にある
- 金銭や組織への不満が動機に挙げられている

脆弱性対策(1)

～脆弱性届出制度の運営～

2004年7月に経済産業省が「ソフトウェア等脆弱性関連情報取扱基準」(平成16年経済産業省告示第235号)を公示し、「情報セキュリティ早期警戒パートナーシップガイドライン」に則り運用を行っている。



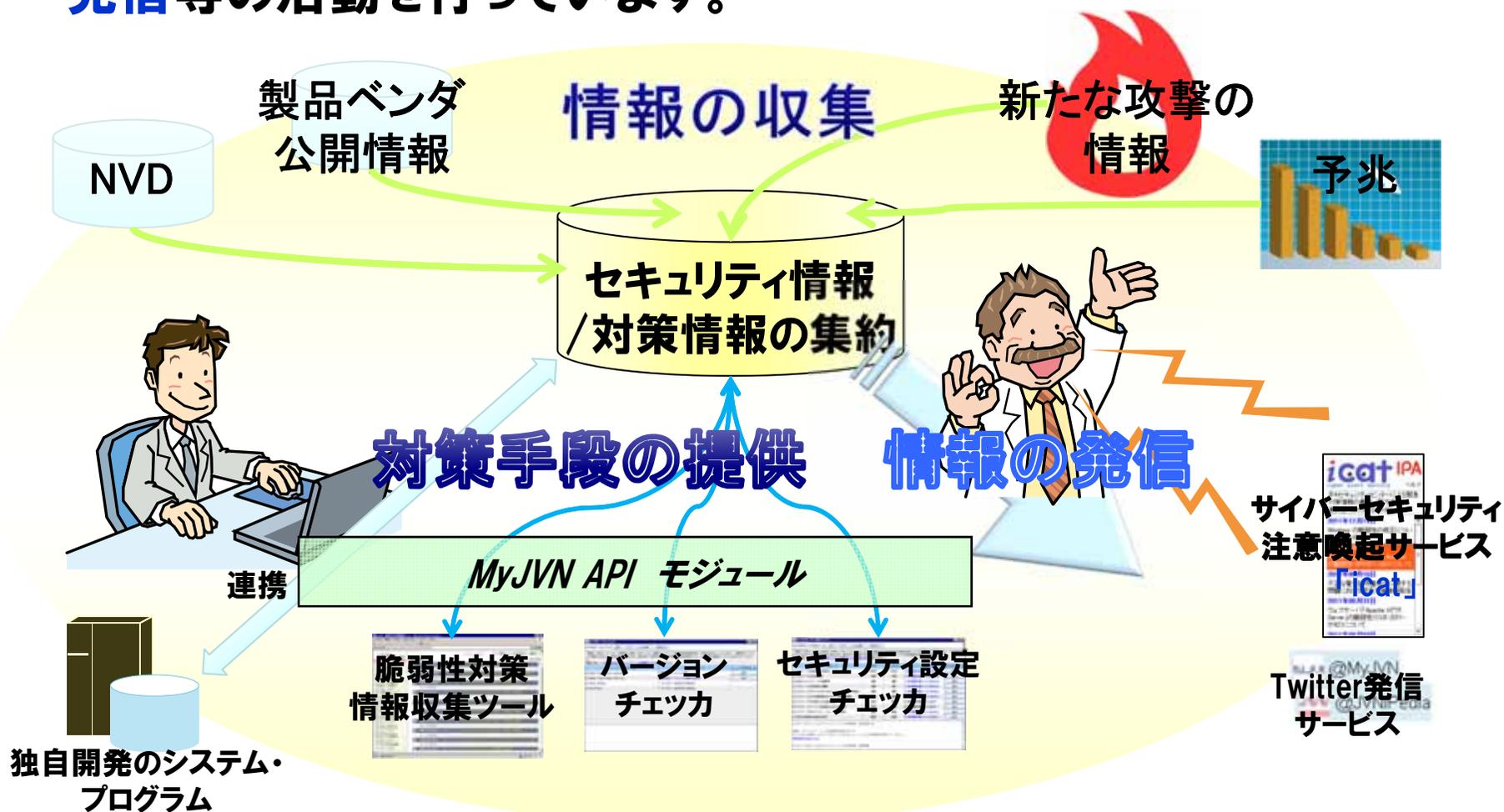
【期待効果】

- ①製品開発者及びウェブサイト運営者による脆弱性対策を促進
- ②不用意な脆弱性関連情報の公表や脆弱性の放置を抑制
- ③個人情報等重要情報の流出や重要システムの停止を予防

※IPA: 独立行政法人 情報処理推進機構、JPCERT/CC: 有限責任中間法人 JPCERT コーディネーションセンター、産総研: 独立行政法人 産業技術総合研究所

脆弱性対策(2)

- IPAではセキュリティ情報の収集、対策手段の提供、情報の発信等の活動を行っています。



サイバーセキュリティ注意喚起サービス icat



http://www.ipa.go.jp/security/vuln/icat.html

迅速なセキュリティ対策情報の入手により、**ユーザへの対策適用を促進**します。
IPAから発信する緊急対策情報を、リアルタイムで企業や団体のウェブサイト上に表示します。



サイバー攻撃への対応(1)

～ 様々な分野の専門家が集結した研究会の発足～

● IPA「脅威と対策研究会」(2010.12～)

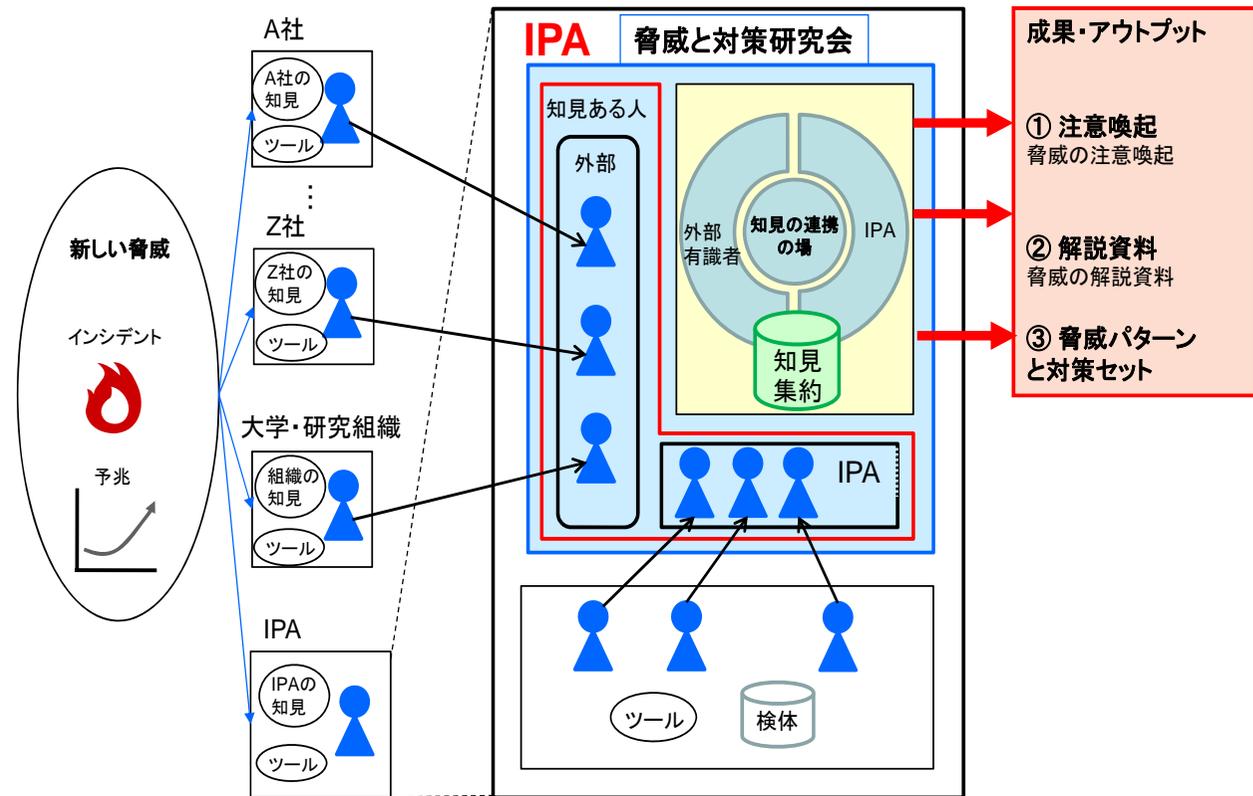
- SIベンダ、セキュリティベンダ、大学関連等の有識者で構成
- 「新しいタイプの攻撃」に関する攻撃の特徴の分析、対策の検討等を行う

研究会アウトプット

2010年12月公表:
IPA テクニカルウォッチ
『新しいタイプの攻撃』に関するレポート

2011年8月公表:
「新しいタイプの攻撃」の対策に向けた
設計・運用ガイド

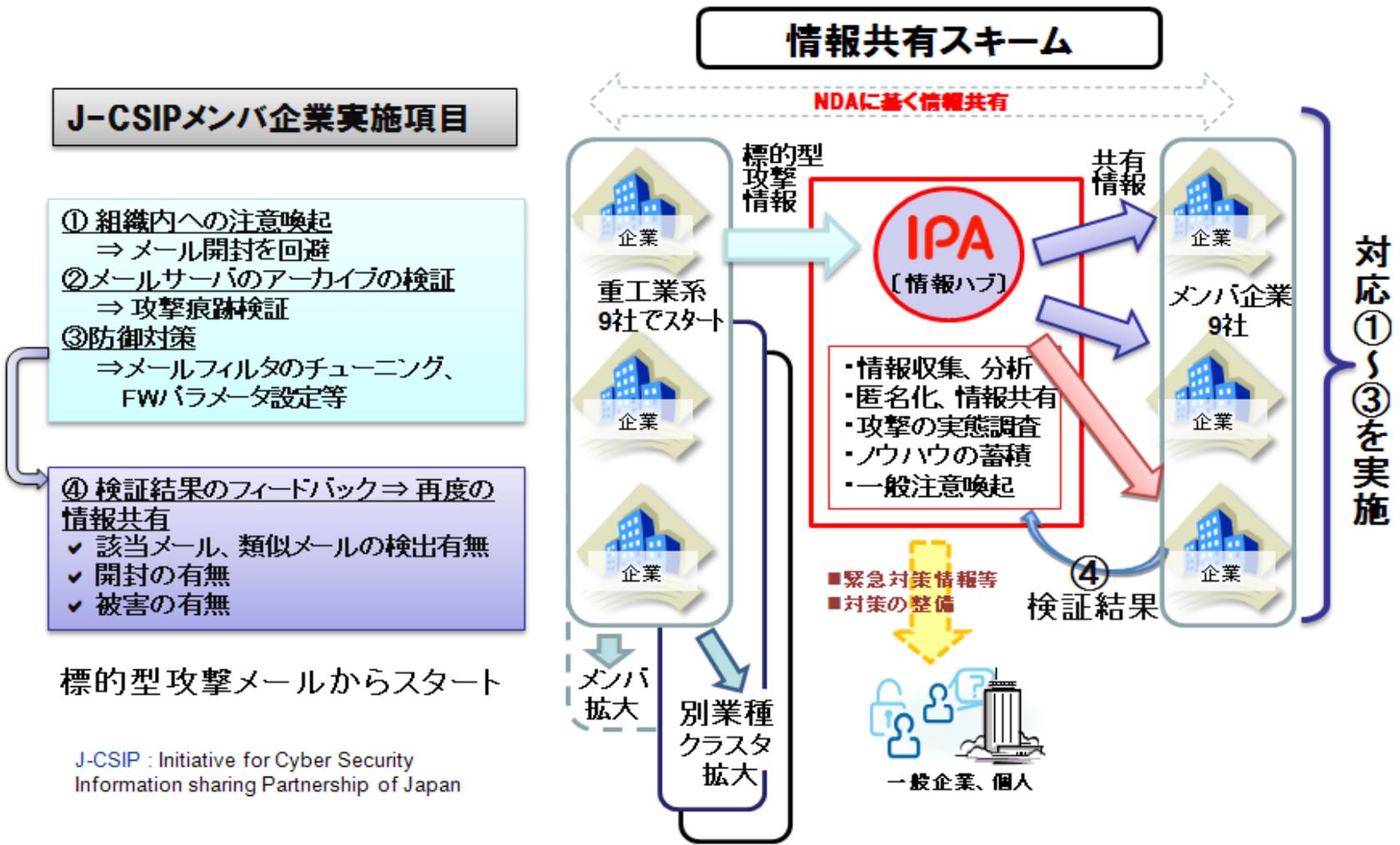
2011年11月公表:
改訂第二版の公開



サイバー攻撃への対応(2)

～官民連携によるサイバー攻撃への対応～

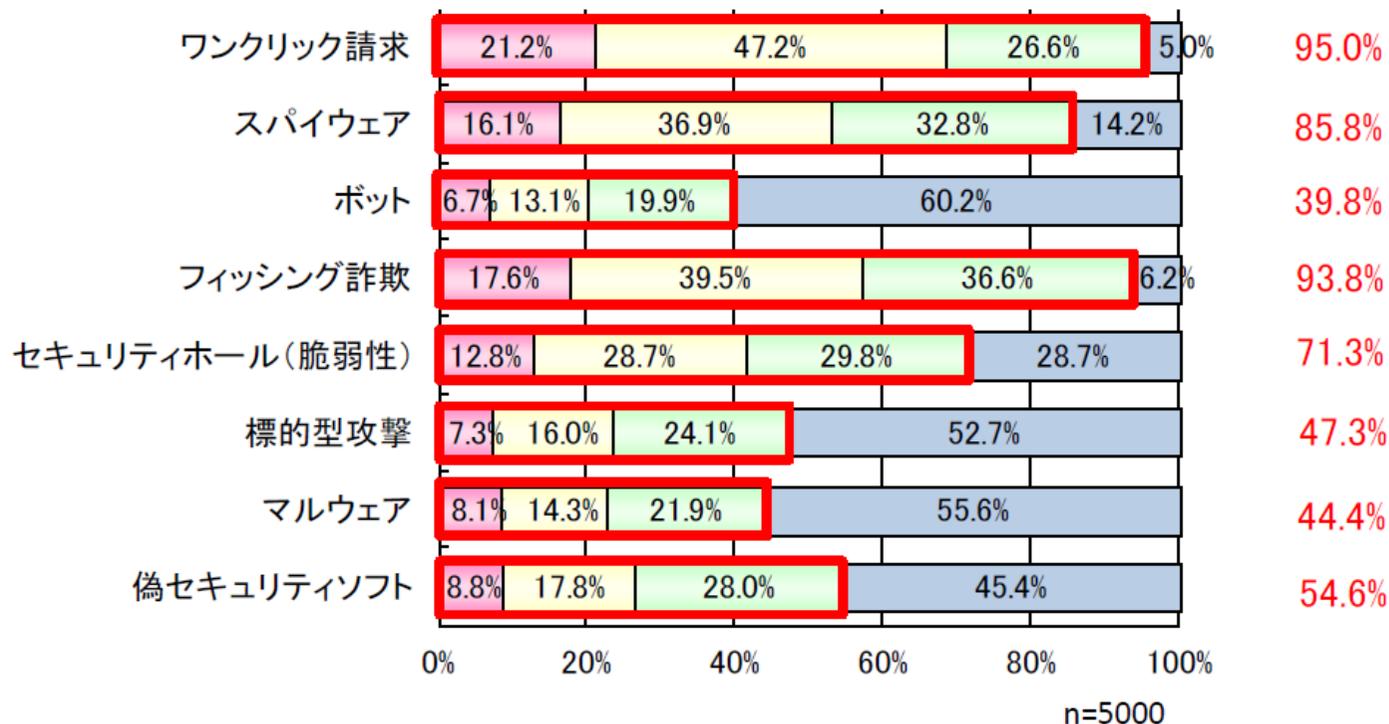
サイバー情報共有イニシアティブ J-CSIP



情報セキュリティに関する 攻撃・脅威の認知



認知・計

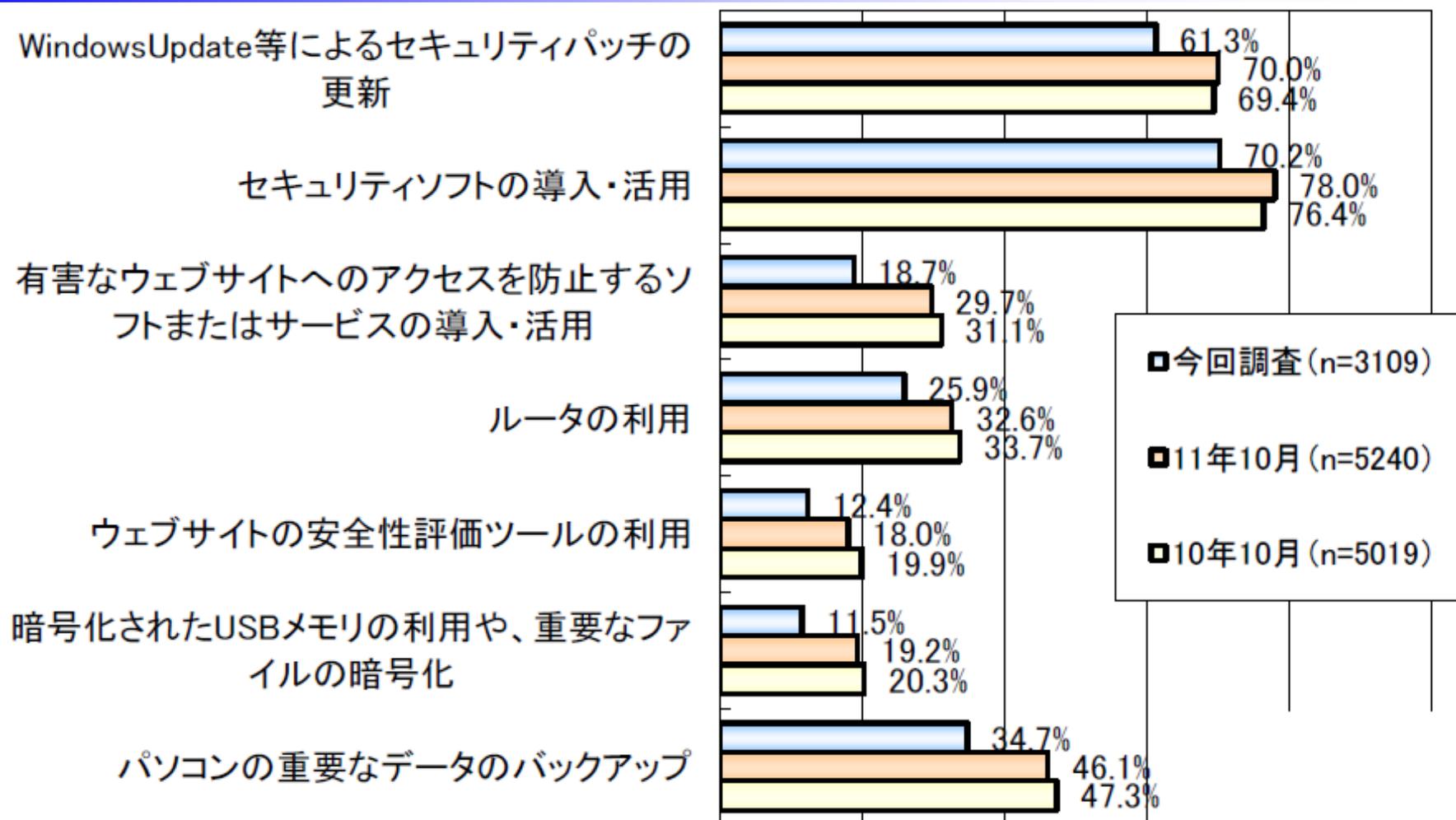


- 詳しい内容を知っている
- 概要をある程度知っている
- 名前を聞いたことがある程度
- 名前も概要も知らない

出典: IPA「2012年度 情報セキュリティの脅威に対する意識調査」報告書

<http://www.ipa.go.jp/security/fy24/reports/ishiki/>

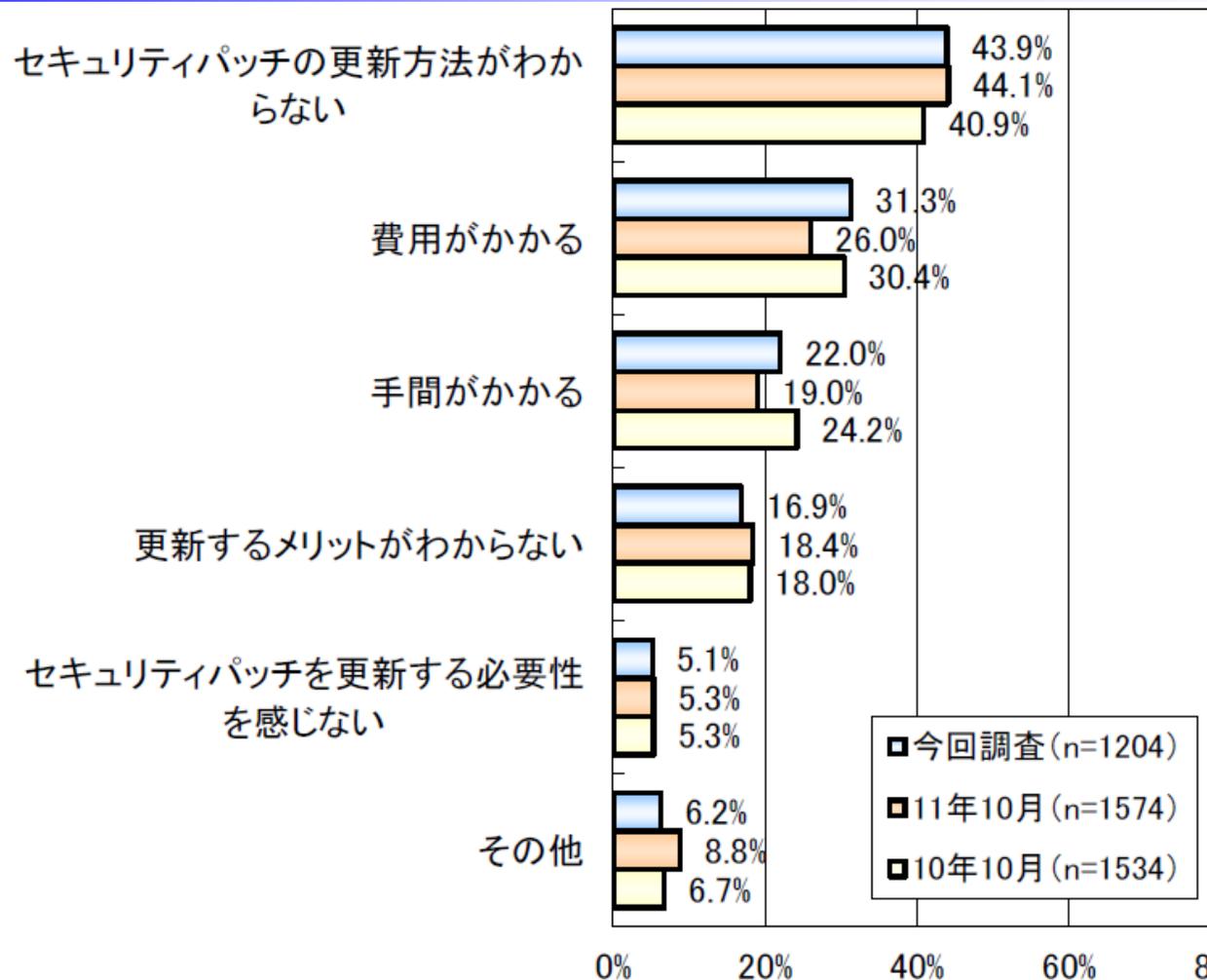
セキュリティ対策の実施状況(抜粋)



出典:IPA「2012年度 情報セキュリティの脅威に対する意識調査」報告書

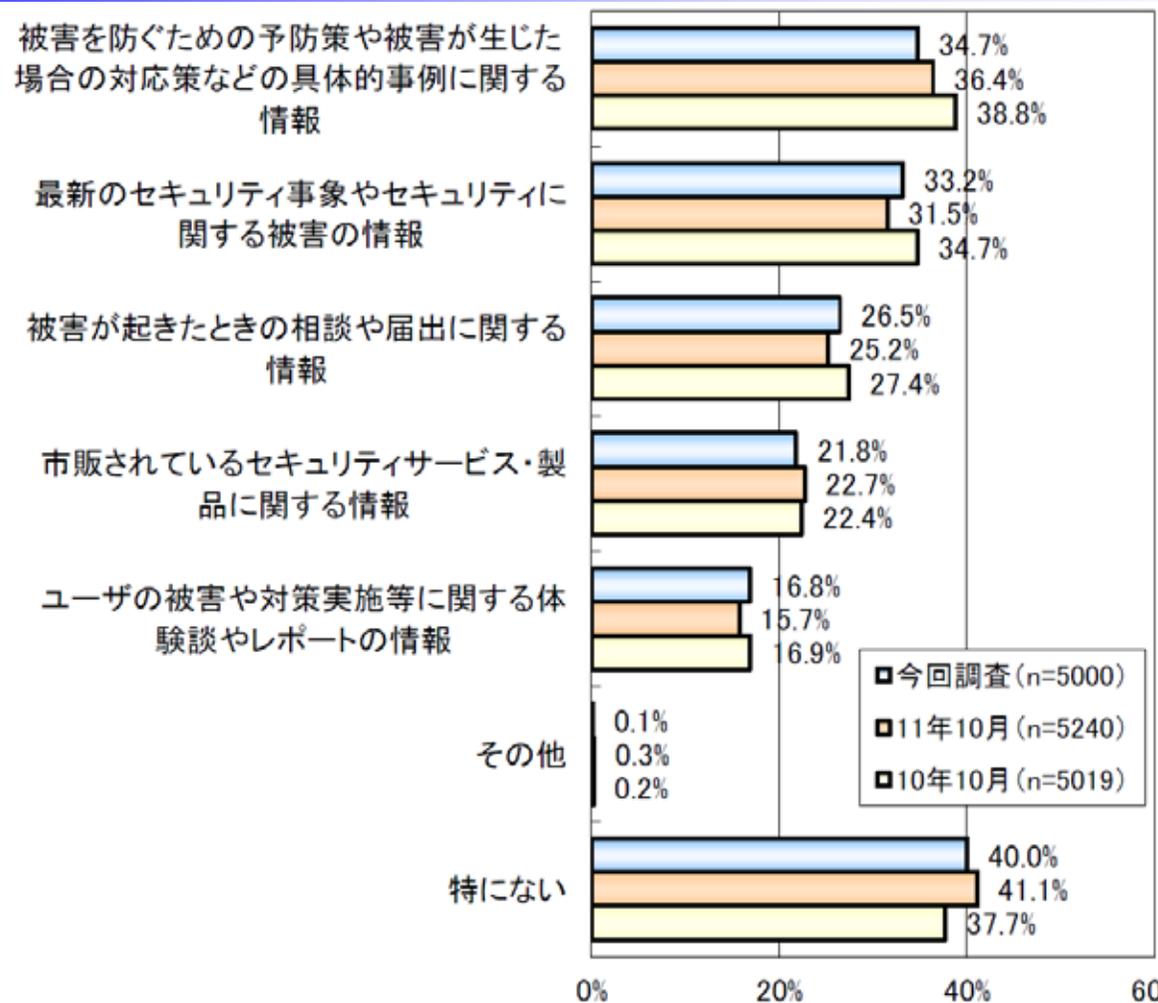
<http://www.ipa.go.jp/security/fy24/reports/ishiki/>

セキュリティパッチの更新をしない理由 **IPA**



出典:IPA「2012年度 情報セキュリティの脅威に対する意識調査」報告書
<http://www.ipa.go.jp/security/fy24/reports/ishiki/>

知りたいセキュリティ情報



出典: IPA「2012年度 情報セキュリティの脅威に対する意識調査」報告書
<http://www.ipa.go.jp/security/fy24/reports/ishiki/>

個人で意識すべき セキュリティ対策の基本



● ウイルス対策ソフトの導入と適切な運用

➤ ウイルス定義ファイルを**最新に保つ**ことが必須！

➤ **統合型セキュリティソフト**がオススメ

(有害サイトのブロック機能やパーソナルファイアウォール機能が有効)

● 脆弱性の解消

➤ OS (Windowsなど)、その他**ソフト全てを最新に**！

➤ こまめな**アップデート**が必須！

(ご参考)「MyJVN バージョンチェッカ」(IPA)

<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>

一歩進んだお勧めの対策

● パーソナルファイアウォールを適切に設定して使用する

- パーソナルファイアウォールを導入し、設定を厳しくして自分が許可したプログラムだけを通信可能とします。
- そうすると、万が一ウイルスに感染してしまっても、そのウイルスが外部と通信することを防ぎ、さらにはウイルスの存在に気付くことができる可能性があります。

MyJVNバージョンチェッカをご活用ください！IPA

MyJVNバージョンチェッカ

実行 終了 全てを選択 選択をクリア 結果出力

「選択」されたソフトウェア製品を「実行」ボタンを押下後ツール下部の内容をい。

クリックするとチェック結果の表示順を切り替えることができます。

あるかをチェックします。「最新のバージョンではありません」と表示された場合には、バージョンを入手してください。利用に関する情報は、MyJVNのウェブページを参照ください。

ソフトウェア製品名 ▲	チェック結果 ▲(×○一順)	結果詳細 ▲
<input checked="" type="checkbox"/> Adobe Flash Player (ActiveX)	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Reader	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> JRE	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Lunascape	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Flash Player (Plug-in)	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Adobe Shockwave Player	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Lhaplus	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Mozilla Firefox	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> QuickTime	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Becky! Internet Mail	— インストールされていないか、対象外のバージョンです	表示
<input checked="" type="checkbox"/> Mozilla Thunderbird	— インストールされていないか、対象外のバージョンです	表示
<input checked="" type="checkbox"/> OpenOffice.org	— インストールされていないか、対象外のバージョンです	表示

チェック結果

詳細情報

表示ボタン

JRE バージョン情報詳細
あなたのPCに現在インストールされているアプリケーションの判定結果は以下の通りです

判定	【インストールバージョン】	【最新バージョン】
×	1.6.0	1.6.0_26 (2011/06/08時点)
○	1.6.0_26	1.6.0_26 (2011/06/08時点)
×	1.5.0_20	1.5.0_22 (2011/08/03時点)
○	1.5.0_22	1.5.0_22 (2011/08/03時点)

バージョンアップ方法は下記のURLを参照ください。
<http://jvndb.jvn.jp/apis/myjvn/vcchecklist.html>

Windows 8
にも対応！

IPA: MyJVN バージョンチェッカ
<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>

IPA・対策のしおり

<p>IPA対策のしおり シリーズ (1)</p> <p>ウイルス対策のしおり</p> <p>コンピュータウイルスから あなたのパソコンを守るには!!</p> <p>IPA</p>	<p>IPA対策のしおり シリーズ (2)</p> <p>スパイウェア対策のしおり</p> <p>気付かぬうちにスパイウェアに 侵入されていませんか?</p> <p>IPA</p>	<p>IPA対策のしおり シリーズ (3)</p> <p>ボット対策のしおり</p> <p>あなたのパソコンは ボットに感染していませんか?</p> <p>IPA</p>	<p>IPA対策のしおり シリーズ (4)</p> <p>不正アクセス対策のしおり</p> <p>大丈夫ですか、 あなたのパソコン? (パソコン利用者向け)</p> <p>IPA</p>	<p>IPA対策のしおり シリーズ (5)</p> <p>情報漏えい対策のしおり</p> <p>企業(組織)で働くあなたへ 7つのポイント!!</p> <p>IPA</p>
<p>IPA対策のしおり シリーズ (6)</p> <p>インターネット利用時の 危険対策のしおり</p> <p>インターネットに接む態度 こんな手口に騙されないで!!</p> <p>IPA 独立行政法人 情報処理推進機構 セキュリティセンター http://www.ipa.go.jp/security/</p>	<p>IPA対策のしおり シリーズ (7)</p> <p>電子メール利用時の 危険対策のしおり</p> <p>電子メールを介したトラブル こんな対策が必要です!!</p> <p>IPA 独立行政法人 情報処理推進機構 セキュリティセンター http://www.ipa.go.jp/security/</p>	<p>IPA対策のしおり シリーズ (8)</p> <p>スマートフォンのセキュリティ <最新回避> 対策のしおり</p> <p>便利な道具 スマートフォン 安全・安心利用のための セキュリティ対策で危険回避!!</p> <p>IPA 独立行政法人 情報処理推進機構 セキュリティセンター http://www.ipa.go.jp/security/</p>	<p>IPA対策のしおり シリーズ (9)</p> <p>初めての情報セキュリティ 対策のしおり</p> <p>個人・家庭向け 「情報セキュリティ」の基礎から 始めてみましょう!</p> <p>IPA 独立行政法人 情報処理推進機構 セキュリティセンター http://www.ipa.go.jp/security/</p>	<p>IPA対策のしおり シリーズ (10)</p> <p>標的型攻撃メール <最新回避> 対策のしおり</p> <p>特定企業・団 体に狙われる 標的型攻撃</p> <p>クラウドサービス 安全利用のすすめ</p> <p>中小企業のみならず 自社のIT環境の改善のために クラウドサービスの導入を検討 するときは、安全についての 確認をしっかり実施しましょう!</p> <p>中小企業のためのクラウドサービス 安全利用チェックシート付</p> <p>IPA 独立行政法人 情報処理推進機構 セキュリティセンター http://www.ipa.go.jp/security/</p>

<http://www.ipa.go.jp/security/antivirus/shiori.html>

IPAが提供する動画コンテンツ

YouTube JP

IPA 情報セキュリティ普及啓発映像コンテンツ
所有者: IPA Channel

▶ すべて再生

共有  Hangout

- 

1 大丈夫？あなたのスマートフォンー安心・安全のためのセ
作成者: ipaip 15,571 回再生

8:55
- 

2 あなたの組織が狙われている！ー標的型攻撃 その脅威と対
作成者: ipaip 8,145 回再生

10:18
- 

3 ワンクリック請求のワナを知ろう！ー巧妙化する手口とそ
作成者: ipaip 1,049 回再生

10:08

YouTube JP

IPA 電車内動画
所有者: IPA Channel

▶ すべて再生

共有  Hangout

- 

1 電車内動画 「インターネット上のID・パスワードに関する情報」
作成者: ipaip 801 回再生

0:23
- 

2 電車内動画 「標的型攻撃メール（なりすまし）の危険性に関する情報」
作成者: ipaip 688 回再生

0:23
- 

3 電車内動画 「スマートフォンのセキュリティに関する情報」
作成者: ipaip 533 回再生

0:23
- 

4 電車内動画 「スマートフォンのセキュリティに関する情報（第2弾）」
作成者: ipaip 793 回再生

0:23
- 

5 電車内動画 「USBメモリ等のウイルスの危険性に関する情報」
作成者: ipaip 769 回再生

0:23
- 

6 電車内動画 「無線LANのセキュリティに関する情報」
作成者: ipaip 816 回再生

0:23

IPA

独立行政法人 情報処理推進機構

Information-technology Promotion Agency, Japan

セキュリティセンター (IPA/ISEC)

<http://www.ipa.go.jp/security/>

★情報セキュリティ安心相談窓口:

TEL: 03(5978)7509 (平日10:00-12:00、13:30-17:00)

FAX : 03(5978)7518

E-mail: anshin@ipa.go.jp