



Information-technology
Promotion
Agency, Japan

Network Security Forum 2013
【S6 パネルディスカッション】

最近のサイバー攻撃に対する企業の自己防衛策

2013年1月25日

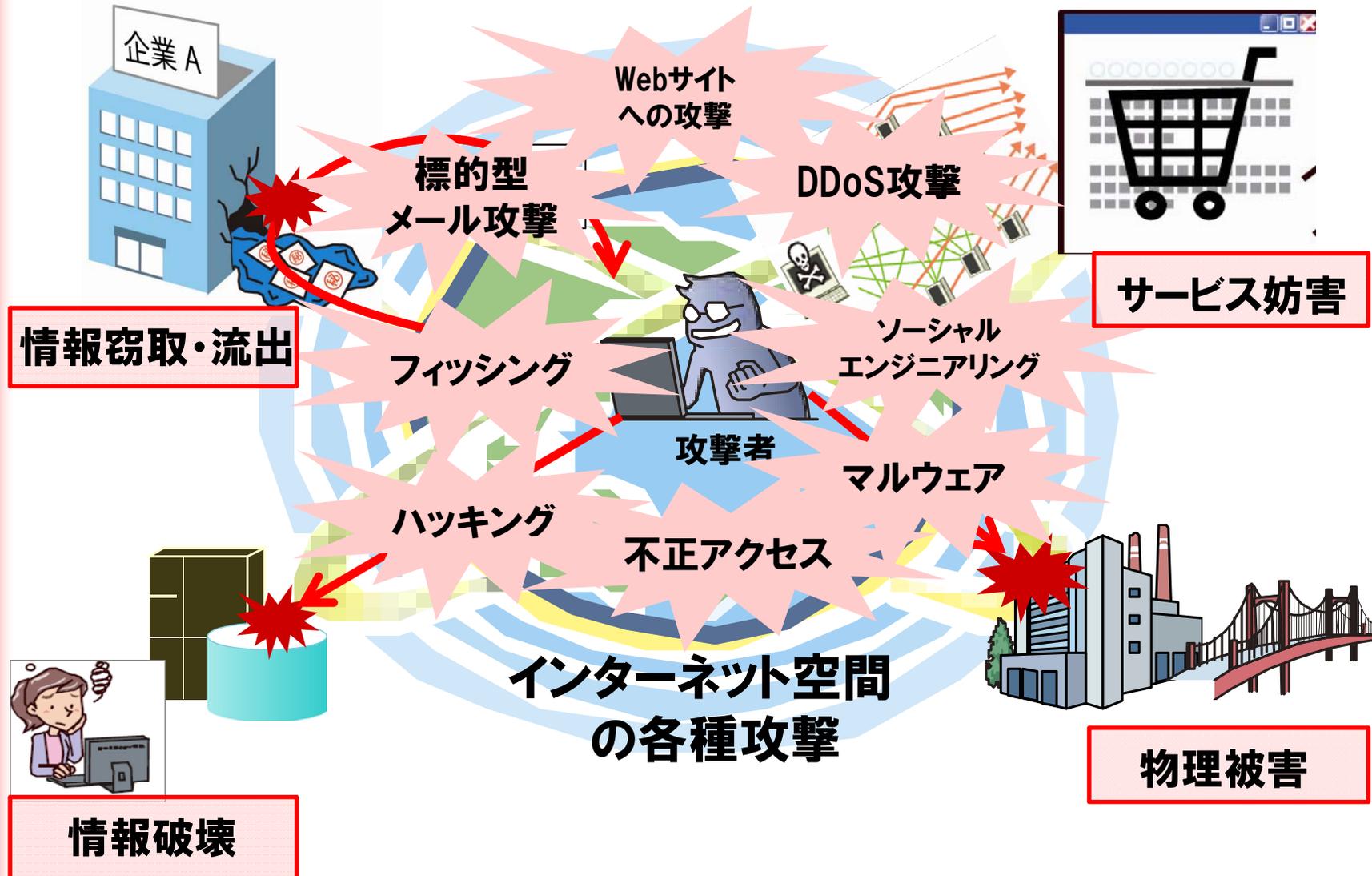
独立行政法人情報処理推進機構

技術本部 セキュリティセンター

情報セキュリティ技術ラボラトリー長 小林 偉昭

企業の視点からの“最近のサイバー攻撃”とは何か 企業をとりまく“最近のサイバー攻撃”

■ 各種の攻撃はあるがされて困る結果は何か

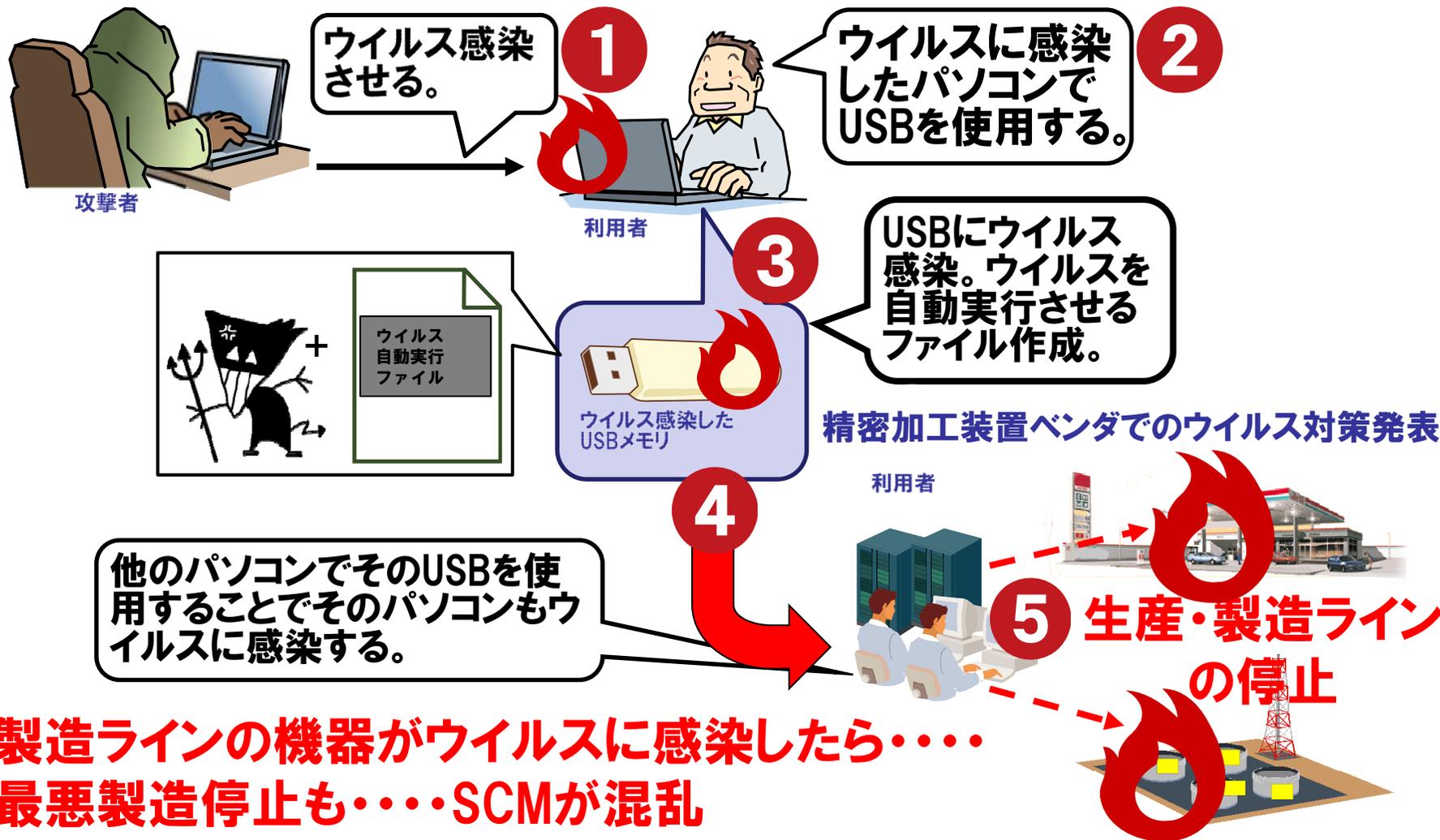


企業の視点からの"最近のサイバー攻撃"とは何か

想定される脅威例(SCM攻撃): **自分に関係ないはだめ!!**

IPA

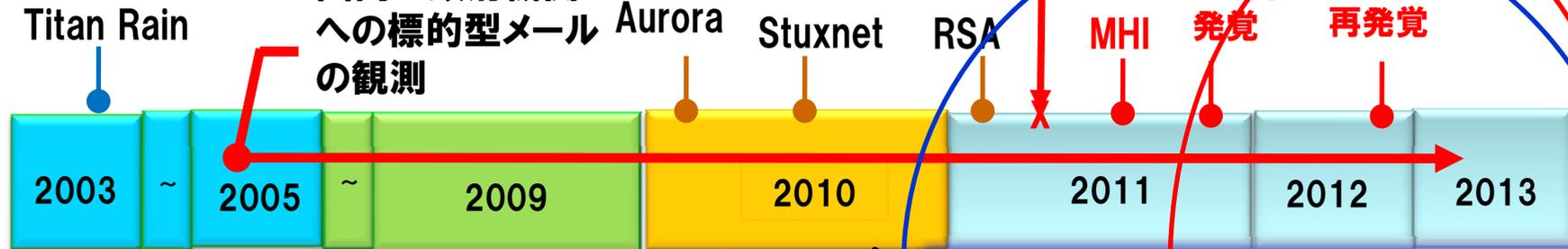
「もし起きたら」を考えた対策を(BCP的発想を)



公共機関は何かをしてくれるのか

官民連携情報共有(PPP : Public-Private Partnership) 推進 IPA

インシデント



対応状況

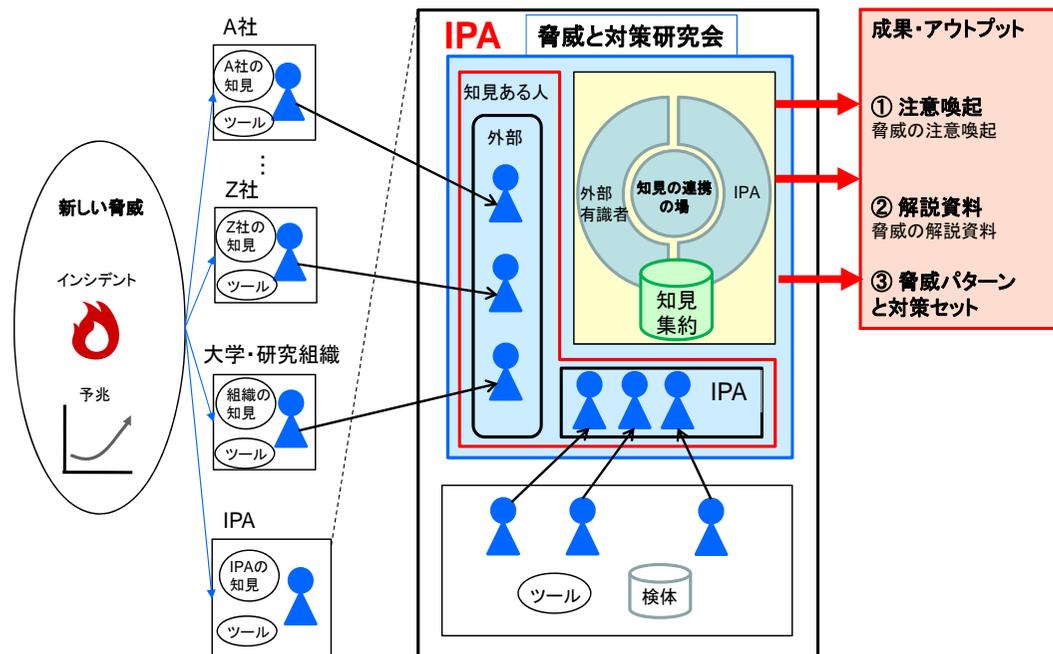


- 10年間攻撃が続いており、被害が食止められていない実情
- 2年間(2010, 2011)で、攻撃による被害が顕在化してきた

公共機関は何かをしてくれるのか IPA「脅威と対策研究会」の活動



- IPA「脅威と対策研究会」(2010.12 ~) オープンな情報共有の場
 - 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および対策の検討等を行う



公共機関は何かをしてくれるのか

サイバー情報共有イニシアティブ(J-CSIP)の活動



クローズドな情報共有の場

クローズドな情報共有の枠組みにより、事前対策を加速

J-CSIP: initiative for Cyber Security Information sharing Partnership of Japan

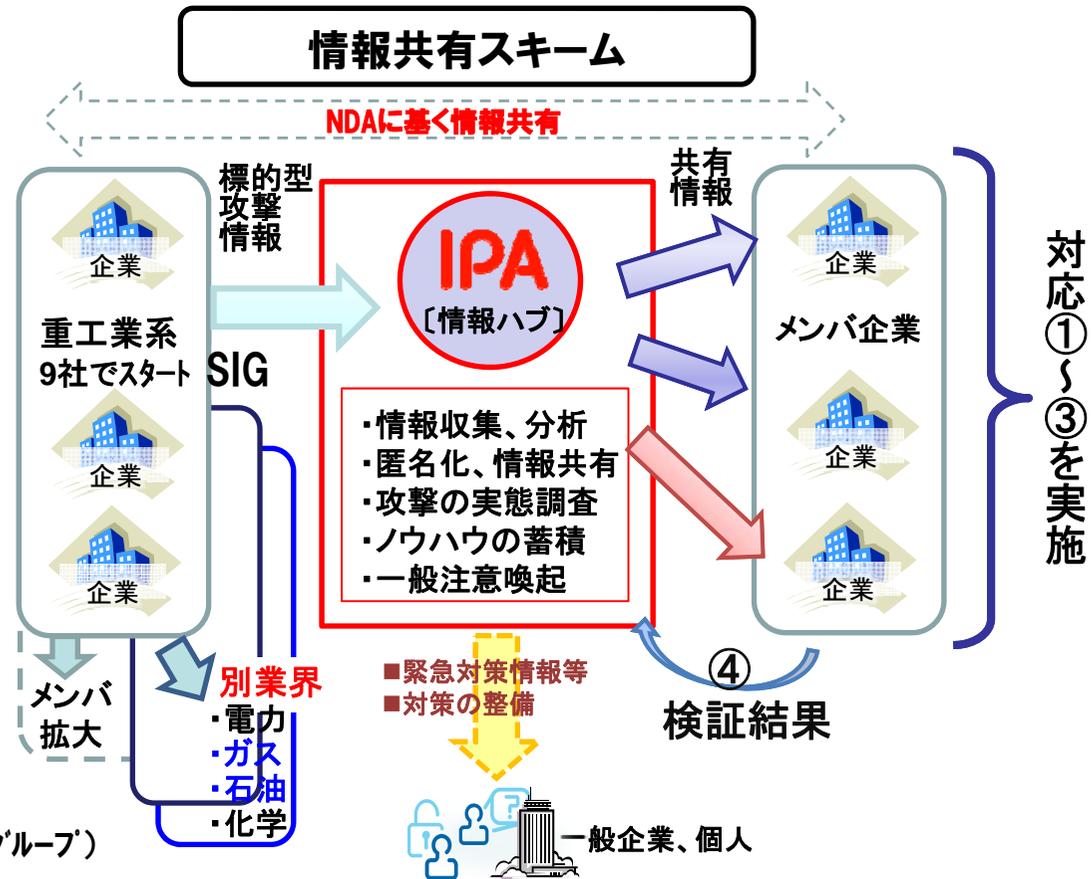
J-CSIPメンバ企業実施項目

標的型メール攻撃からスタート

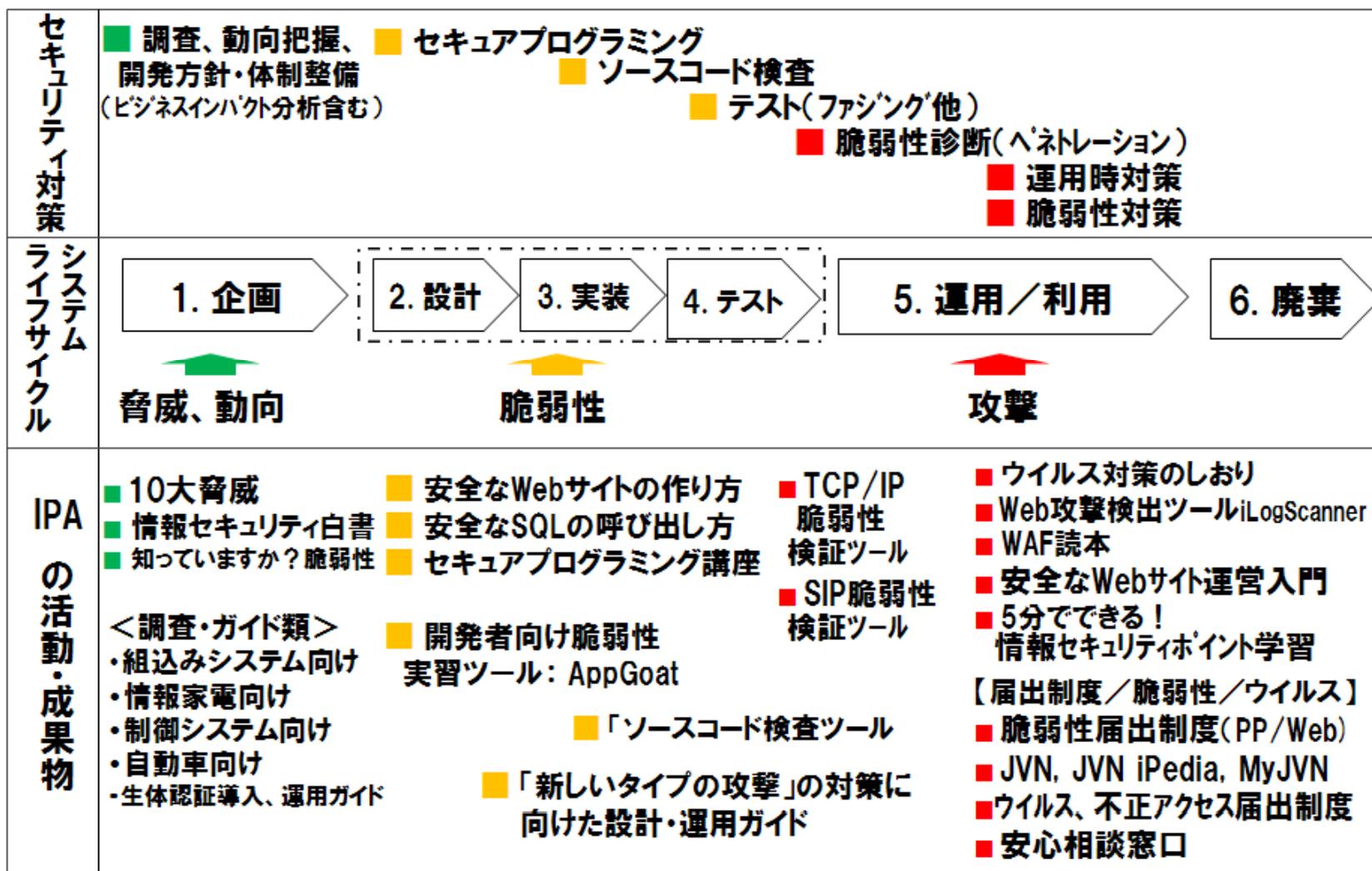
- ① 組織内への注意喚起・初動対策
⇒ メール開封を回避
- ② メールサーバのアーカイブの検証
⇒ 攻撃痕跡検証
- ③ 防御対策
⇒ メールフィルタのチューニング、FWパラメータ設定等

- ④ 検証結果のフィードバック ⇒ 再度の情報共有
 - ✓ 該当メール、類似メールの検出有無
 - ✓ 開封の有無
 - ✓ 被害の有無

SIG: Special Interest Group (業界毎の情報共有グループ)



企業は 具体的な自己防衛策として何をすべきか システムライフサイクルに合わせたIPAの活動



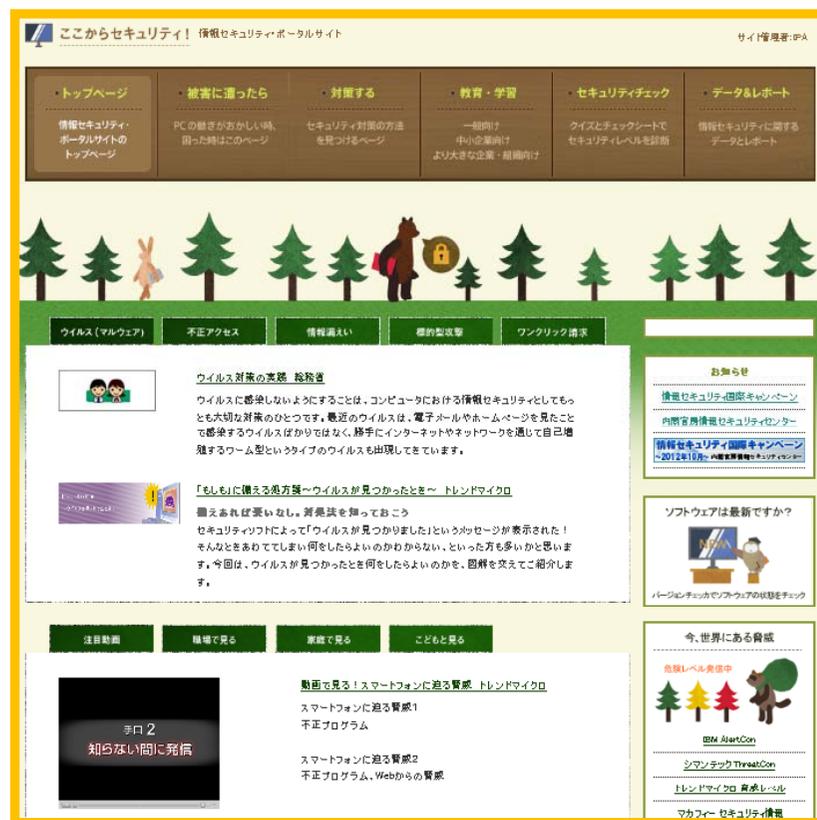
企業は 具体的な自己防衛策として何をすべきか IPAの取組み



■ IPAが提供する情報収集支援

情報セキュリティ・ポータルサイト

官民様々なセキュリティコンテンツを紹介



サイバーセキュリティ注意喚起サービス「icat」

影響度の大きなセキュリティ上の問題について「緊急対策情報」または「注意喚起」としてウェブに埋め込み確認できる



企業は 具体的な自己防衛策として何をすべきか MyJVNバージョンチェッカ



PCを最新の状態に

MyJVN トップページ

MyJVN による
MyJVNとは、セキュリティ上問題となるPCサービスの脆弱性の対策を促進するために、対策情報を積極的に収集した上で、簡単な操作で最新情報に基づいたチェックを行うことが可能に組み込み（フレームワーク）の設計です。MyJVNが提供するセキュリティチェック情報は、お持ちのPCやサーバーにインストールされたソフトウェア製品やシステムの設定が、最新の状態に保たれているかを確認します。ウイルス対策ソフトと合わせて利用することにより最新のセキュリティ対策が可能となります。

一般利用者の方へ
お持ちのPCのソフトウェアが最新か、脆弱な設定（状態）になっていないかを簡単にチェック

システム管理者の方へ
サーバ向けソフトがチェック可能
パッチによるチェックが可能
チェック項目の選択が可能
オフライン環境でも利用可能

開発者の方へ
MyJVNが提供する脆弱性対策情報をWebサイトやアプリケーションから利用可能

クイック起動
MyJVNバージョンチェッカの起動
Windows用

MyJVNバージョンチェッカ
実行

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」することで、最新バージョンで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、表示ボタンを押下後ツール下部の内容を参考にして、ベンダから最新の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)	表示詳細 ▲
<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 Flash Player (Plug-in)	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Shockwave Player	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Becky! Internet Mail	× 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"/> Adobe Reader	○ 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"/> OpenOffice.org	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> VMware Player	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Lunascape	— 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

Adobe Flash Player (ActiveX) 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】
× 10.3.181.26 10.3.183.7 (2011/08/25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://vndb.ivn.jp/apis/mvijn/vcchecklist.html>

簡単操作で、インストールしているソフトウェアの最新バージョンの適用状況をチェックできます

■ IPAが提供する各種報告書・ツール(一部紹介)

知っていますか脆弱性

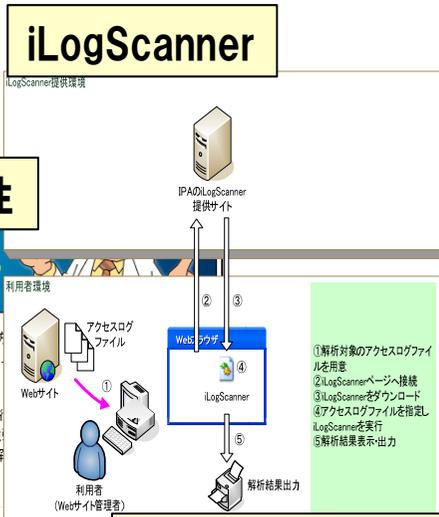


このコンテンツは、ウェブサイトの運営者や一般の利用者の代表的な10種類の脆弱性(ソフトウェア等におけるセキュリティアニメーションで解説しています。

これらの問題は、根本的にはウェブサイトの運営者が対策を、利用者の方も、保険的な対策を取ることで、ウェブサイトの脆弱性を未然に防いだり、抑えることができます。詳細は、各解説を参照してください。

- **SQLインジェクション**
～ショッピングサイトの個人情報盗まれてしまった～
- **クロスサイト・スクリプティング**
～フィッシング詐欺に悪用されてしまった!～
- **CSRF(クロスサイト・リクエスト・フォージェリ)**
～SNSで自分の日記が勝手に公開されてしまった!～
- **パス名パラメータの未チェック/ディレクトリ・トラバース**
～ウェブサイトの非公開ファイルが漏洩!～

5分でできる!
情報セキュリティポイント学習



MyJVNバージョンチェッカ

ソフトウェア製品名	チェック結果 (○×○一順)	結果詳細
Adobe Flash Player (ActiveX)	× 最新のバージョンではありません	表示
Adobe Flash Player (Plug-in)	× 最新のバージョンではありません	表示
Adobe Shockwave Player	× 最新のバージョンではありません	表示
Becky! Internet Mail	○ 最新のバージョンです	表示
JRE	○ 最新のバージョンです	表示
Adobe Reader	○ 最新のバージョンです	表示
Thopos	○ 最新のバージョンです	表示
Mozilla Firefox	○ 最新のバージョンです	表示
OpenOffice.org	○ 最新のバージョンです	表示
VMware Player	○ 最新のバージョンです	表示
Lunasec	○ インストールされていませんが、対象外のバージョンです	表示
Microsoft ThreatDefender	○ インストールされていませんが、対象外のバージョンです	表示

AppGoat

安全な関数でコピー
データ(16バイト)
安全な関数の利用によって、16バイトは切り捨てられる

動的にバッファを確保
動的にバッファを確保

安全な関数を利用する
C/C++言語には、stack overflowなどの脆弱性があり、コピーサイズを指定できるstring関数などの安全な関数を利用することで、これらの脆弱性を回避することができます。

動的にバッファを確保する
可変長の入力値に対して固定長のバッファを用意すると、バッファオーバーフローが発生しやすくなります。そのため、可変長の入力値に対して動的に必要な分のバッファを確保して利用します。サイズが指定された場合、計算式による動的オーバーフローを防ぐように注意する必要があります。動的オーバーフローについては、『動的オーバーフローによる脆弱性』のテーマを参照してください。

安全なウェブサイトの作り方

安全なウェブサイトの作り方 改訂第5版

ウェブアプリケーションのセキュリティ実践とウェブサイトの安全性向上のための取組み

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 2011年4月

ファジング活用の手引き

製品出荷前に機械的に脆弱性をみつけよう

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 2012年3月

組込みシステムのセキュリティへの取組みガイド(2010年度改訂版)

16箇の具体的なチェック項目により、自組織のセキュリティレベルを明確にする

組込みシステムの報告書