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

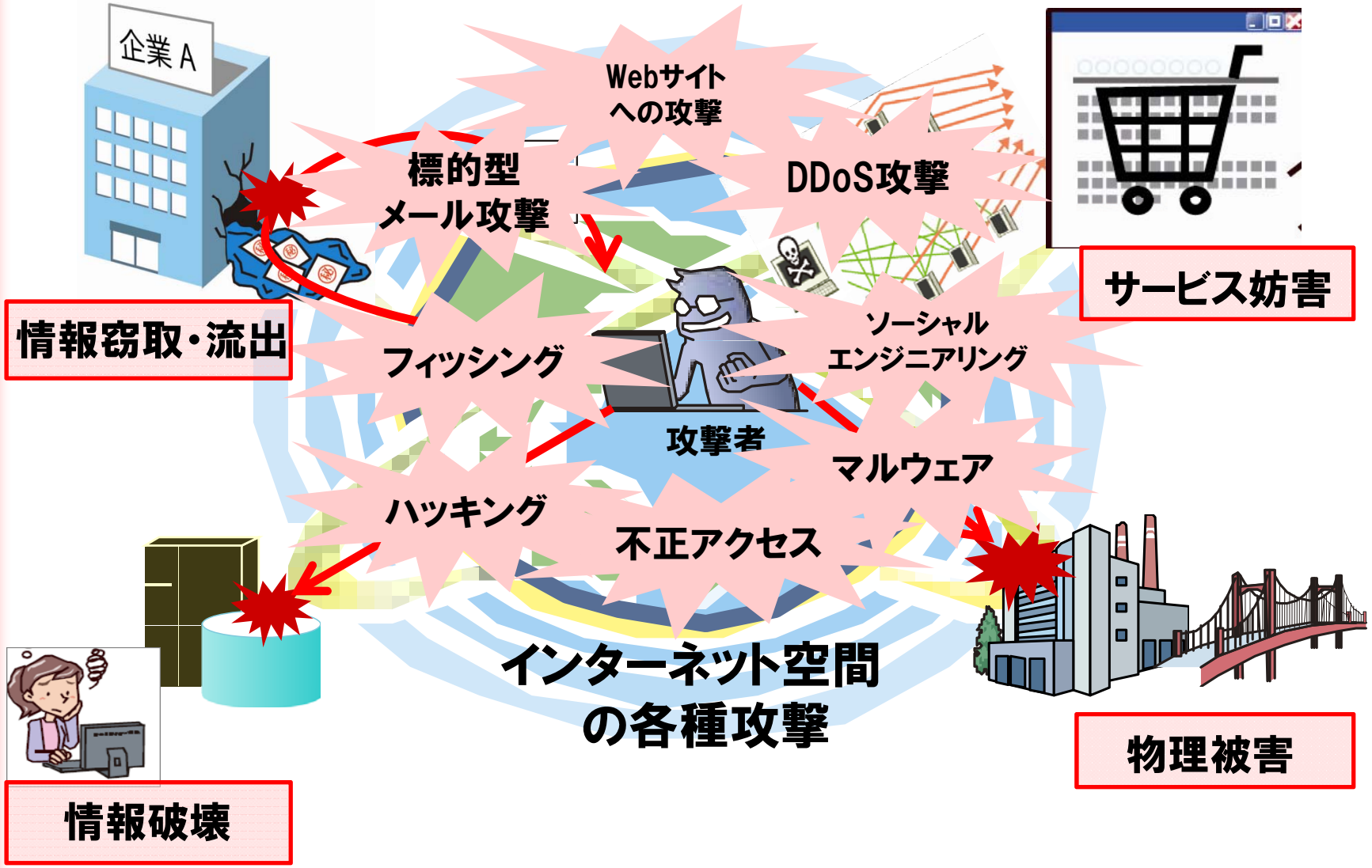
2013年1月25日

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"

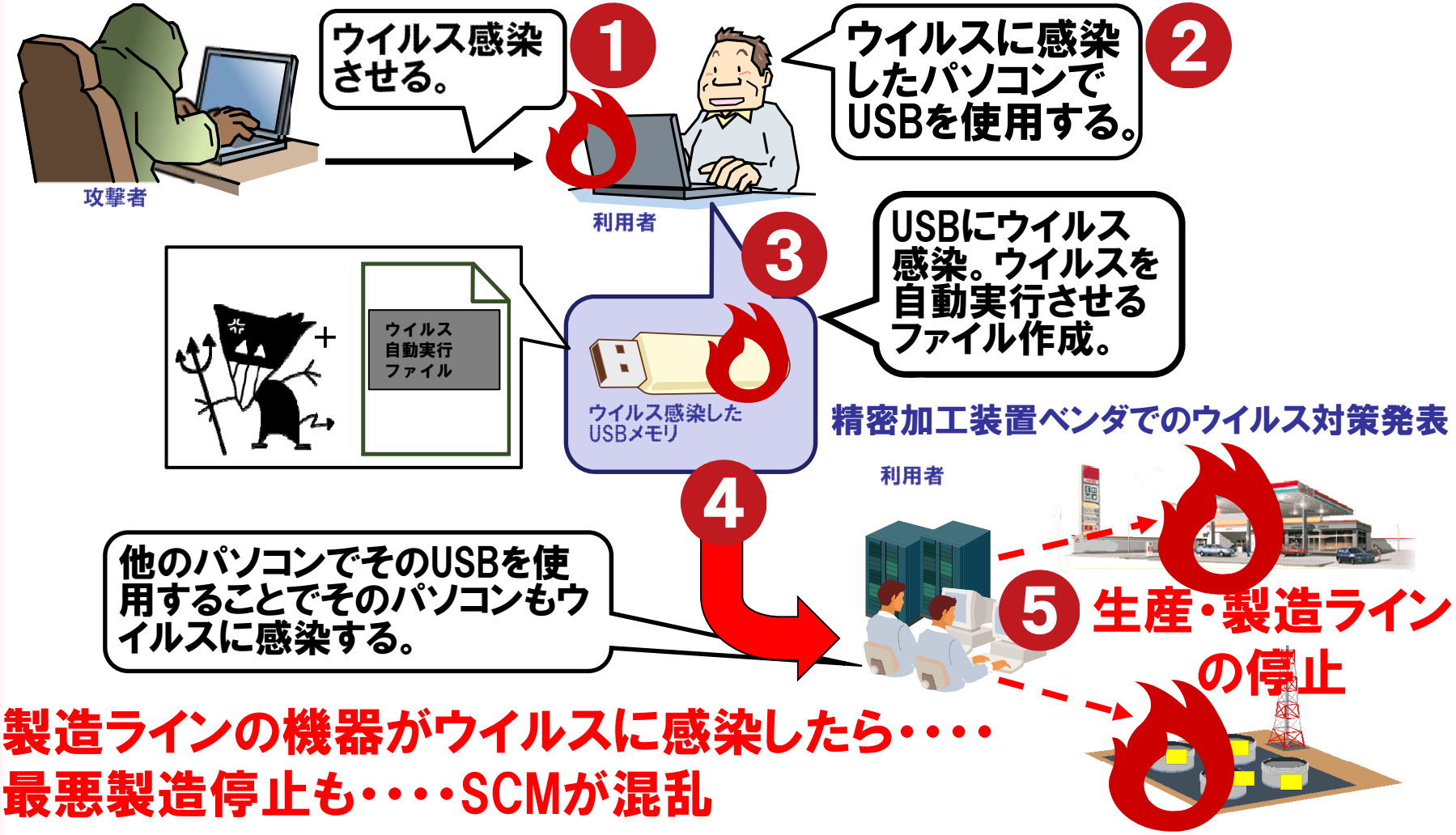
■ 各種の攻撃はあるがされて困る結果は何か



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):自分は関係ないはだめ!!

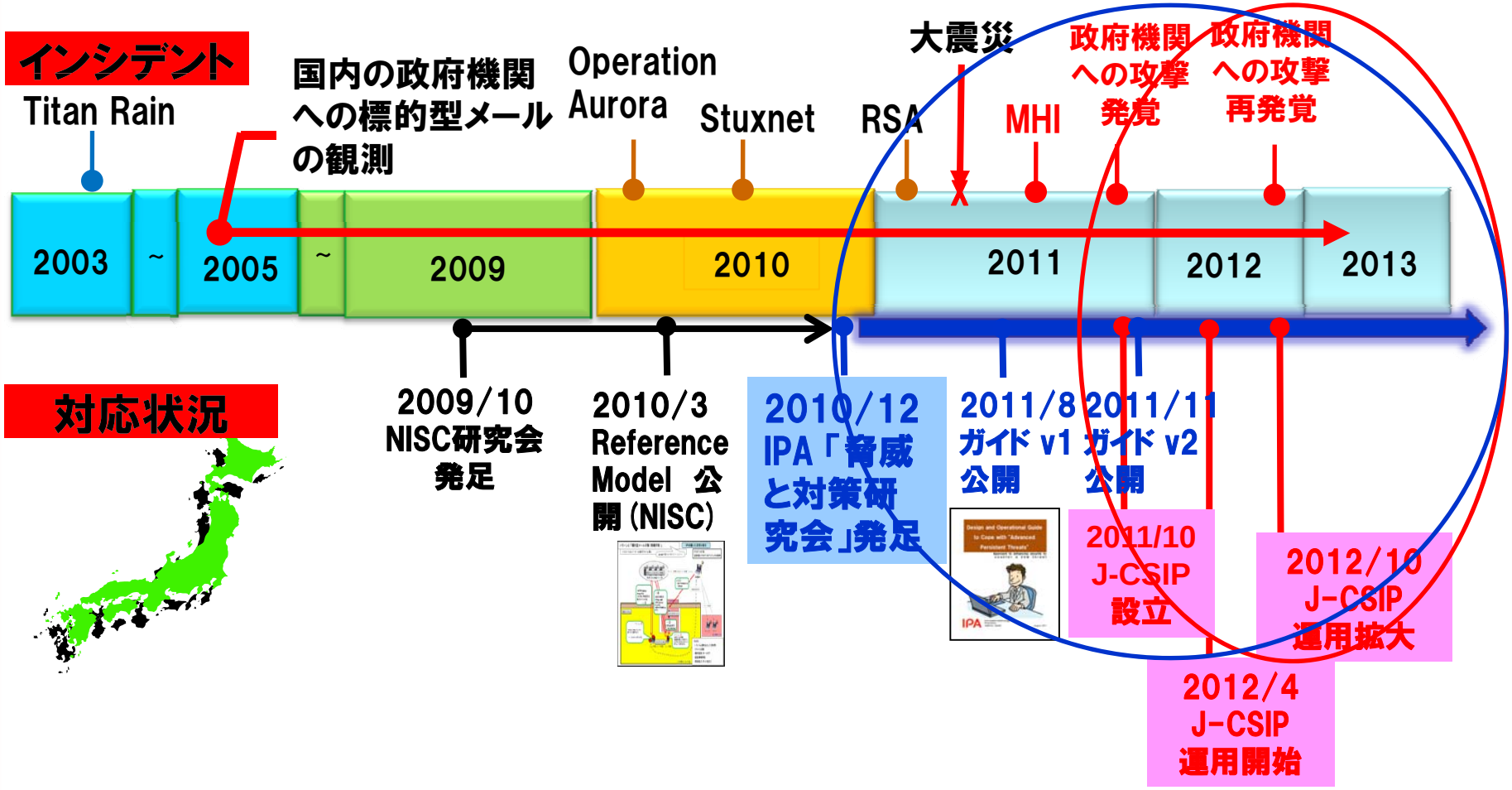
「もし起きたら」を考えた対策を(BCP的発想を)



製造ラインの機器がウイルスに感染したら・・・・
最悪製造停止も・・・・SCMが混乱

BCP : Business Continuity Plan　　SCM : Supply Chain Management

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



- 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

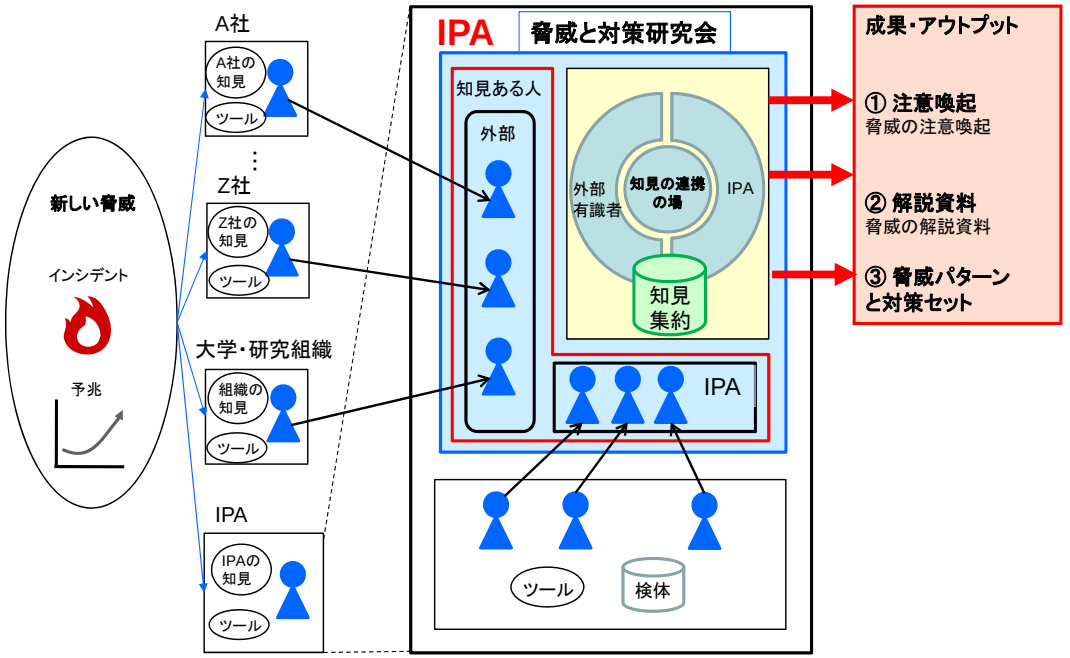
公共機関は何かをしてくれるのか

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

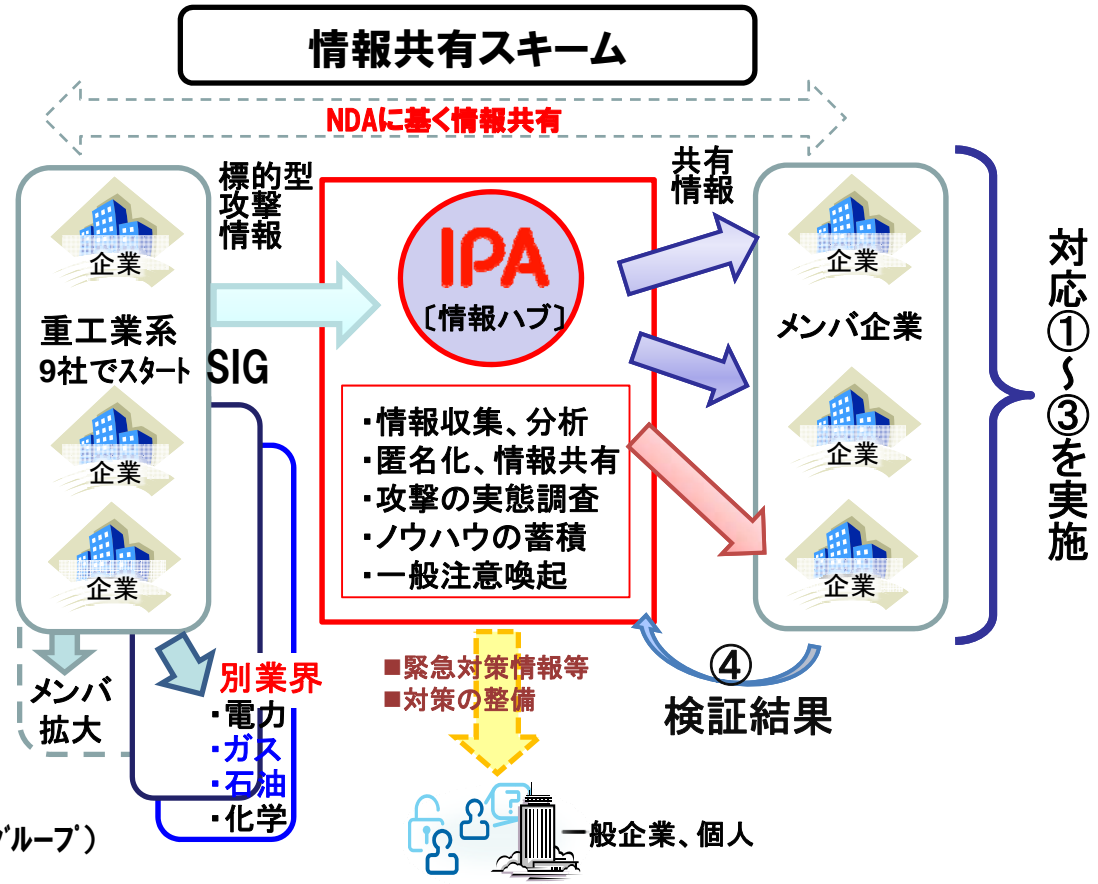
J-CSIP: initiative for Cyber Security Information sharing Partnership of Japan

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

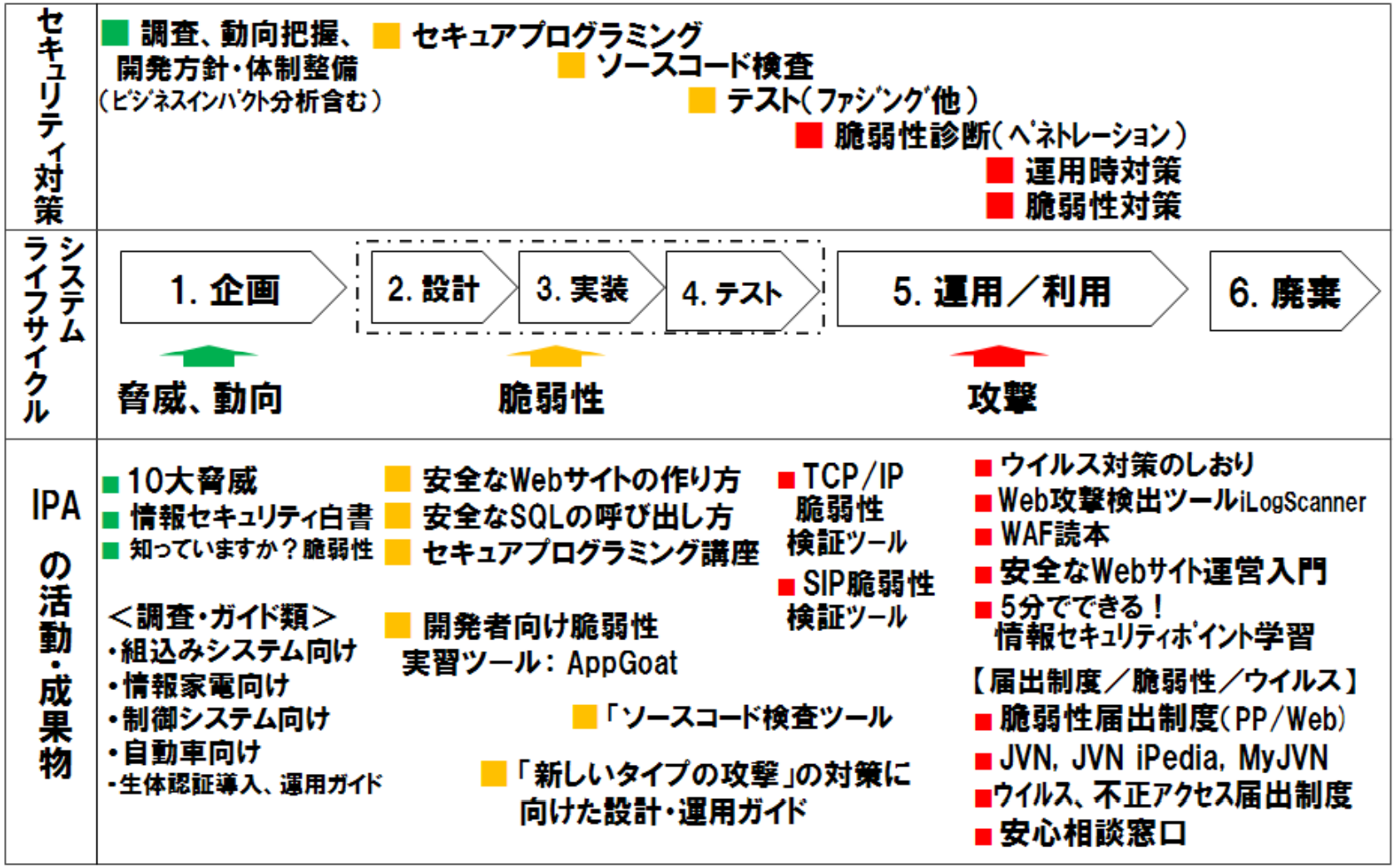
④ 検証結果のフィードバック ⇒ 再度の情報共有
- 該当メール、類似メールの検出有無
- 開封の有無
- 被害の有無



SIG：Special Interest Group（業界毎の情報共有ｸﾞﾙｰﾌﾟ）

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

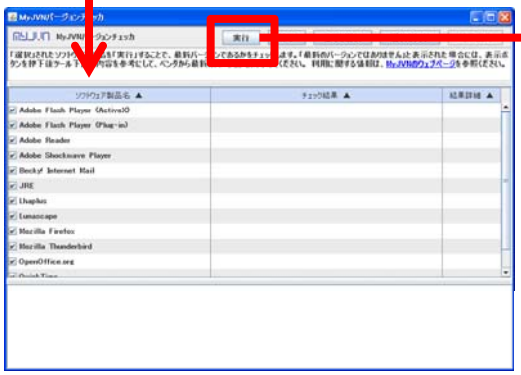
サイバーセキュリティ注意喚起サービス「icat」

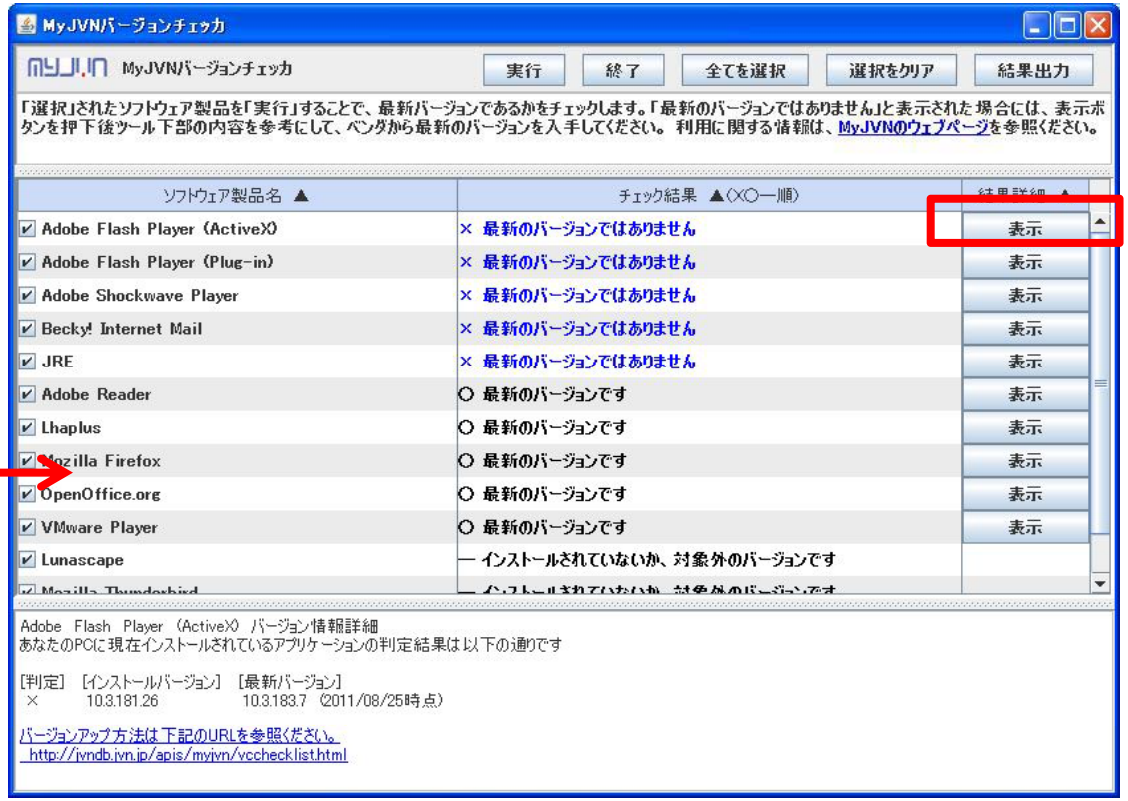
影響度の大きなセキュリティ上の問題について「緊急対策情報」または「注意喚起」としてウェブに埋め込み確認できる

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





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の取組み

■ IPAが提供する各種報告書・ツール（一部紹介）

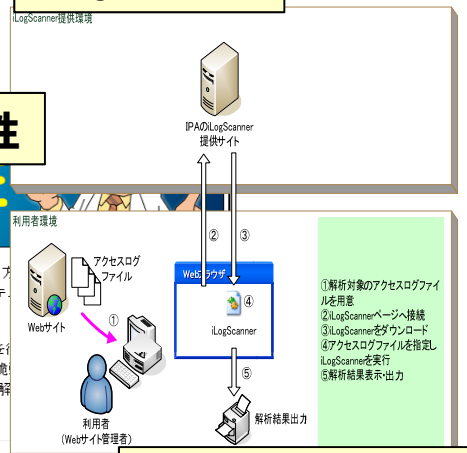
知っていますか脆弱性

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方
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
アニメーションで解説しています。

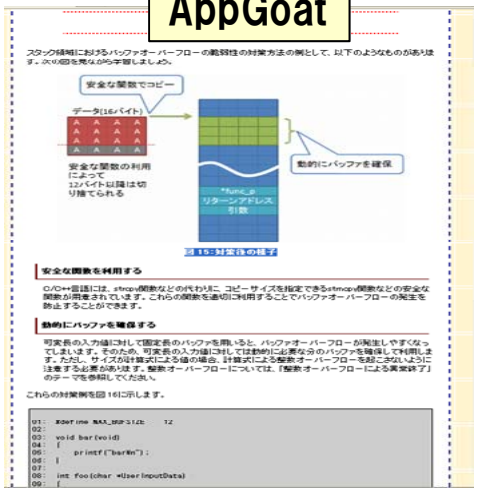
これらの問題は、根本的にはウェブサイトの運営者が対策を
利用者の方も、保険的な対策を取ることで、ウェブサイトの脆
被害を未然に防いだり、抑えることができます。詳細は、各解
い。

- SQLインジェクション
  ～ショッピングサイトの個人情報が盗まれてしまった！～
- 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
  ～SNS で自分の日記が勝手に公開されてしまった！
  て？～
- パス名パラメータの未チェック/
  ディレクトリ・トラバーサル
  ～ウェブサイトの非公開ファイルが漏洩！？～

iLogScanner



AppGoat

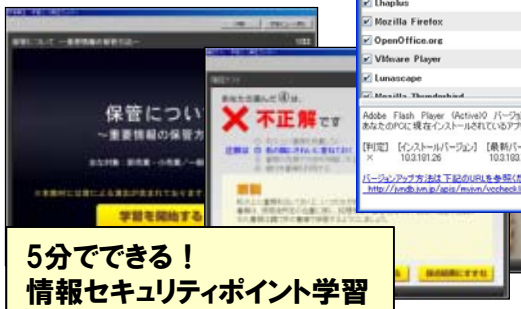


安全なウェブサイトの作り方

MyJVNバージョンチェッカ

ファジング活用の手引き

組込みシステムの報告書



5分でできる！
情報セキュリティポイント学習