ソフトウエア等脆弱性関連情報取扱基準とガイドラインの概要説明

平成16年7月

経済産業省
情報セキュリティ政策室
川口修司

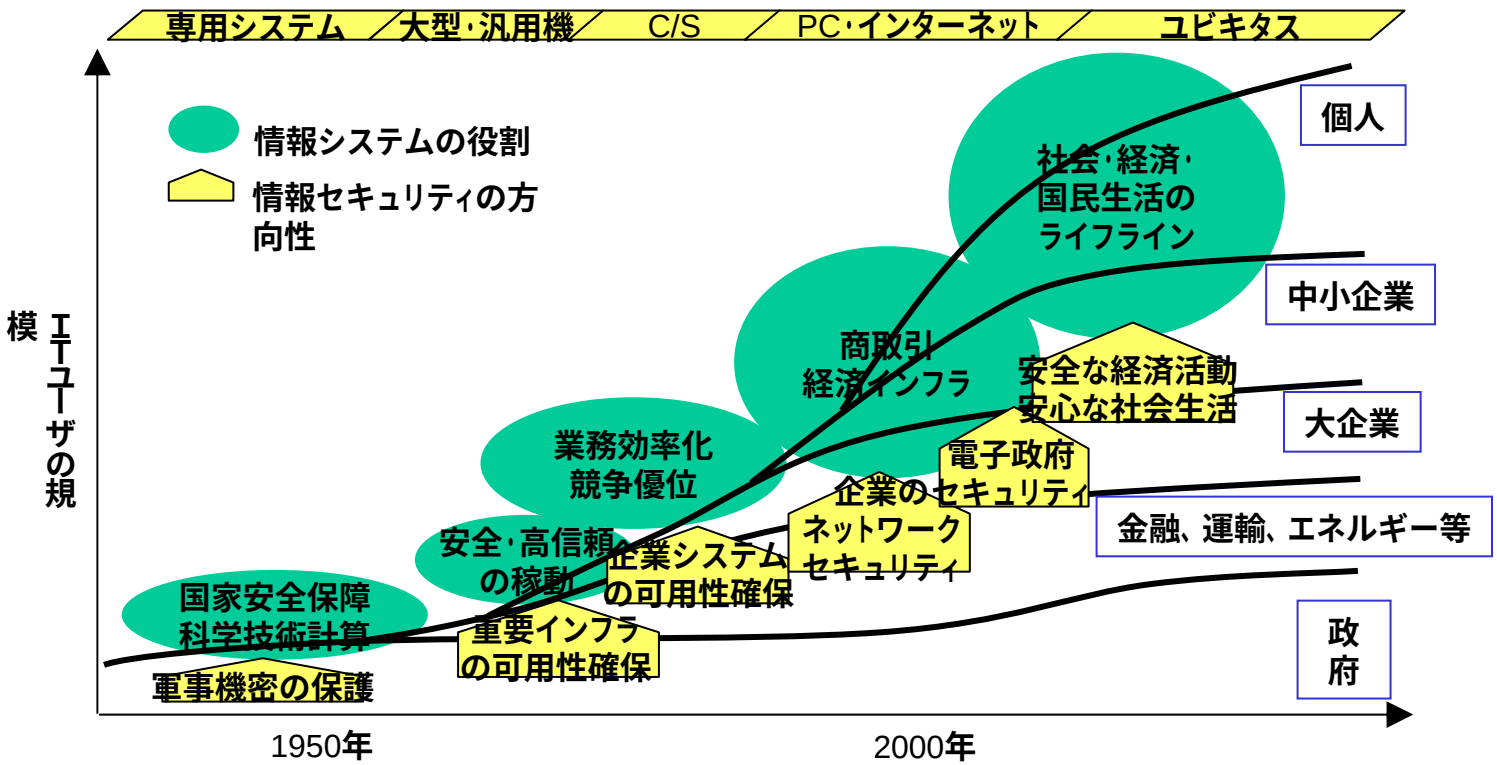
1．経済産業省の情報セキュリティ政策の基本方針

～「情報セキュリティ総合戦略」～

基本認識～経済・社会の「神経系」となったIT

■ 経済・社会の「神経系」となったITと新次元のリスク

- ITはここ近年急速に発展・普及し、**「経済・社会の『神経系』」**に。
- また、情報システムは複雑化し、これまでになかった新次元のリスクに直面。



情報セキュリティ政策の流れ

METI 経済産業省

インターネット幕開け　　電子商取引離陸　　ニューエコノミー／IT革命

クリッパーチップ構想（米）　　暗号輸出規制の緩和

暗号政策ガイドライン（OECD）　　ＡＥＳ選定　　国際標準化

COCOM解散　　ワッセナー成立　　米国サイバーセキュリティ戦略

ＣＣアレンジメント（→ISO/IEC１５４０８）

セキュリティ・マネジメント（ISO/IEC１７７９９）

ＥＵ個人情報保護指令案　　ＥＵ電子署名指令案

電子政府イニシャチブ　　2003.4　　「総合戦略」

ハッカー対策行動計画／サイバーテロ対策行動計画

大規模プラントセキュリティ対策　　NIRT創設

セキュリティ技術開発支援　　暗号技術評価（CRYPTREC）

JPCERT/CCの創設支援　　セキュリティ評価認証開始

IPAセキュリティセンター　　電子署名・認証法

ウィルス等対策基準改訂　　ISMS適合性評価制度

情報セキュリティ監査

対症療法的対応
次々と明らかになる水道管の漏水箇所にパテを当てて回るような取り組み

抜本的見直し
配管全体を再設計

情報セキュリティ総合戦略（2003年10月10日発表）

～世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上～ METI 経済産業省

- 3つの戦略と42の具体的施策項目の提示
- http://www.meti.go.jp/policy/netsecurity/strategy.htm

基本目標　***世界最高水準の「高信頼性社会」の構築***

戦略1　***しなやかな「事故前提社会システム」構築（高回復力・被害局限化の確保）***

→「情報セキュリティに絶対はない」との前提の下で、事故の回避（予防）・被害局限化・回復の最適化を図った対応の徹底化

戦略2　***「高信頼性」を強みとするための公的対応の強化***

→「高信頼性」を強みとするため、国家的視点から、技術基盤・制度基盤両面にわたる公的対応を強化

戦略3　***内閣機能強化による統一的推進***

「脆弱性に対処するためのルールと体制の整備」

（経済産業省「情報セキュリティ総合戦略」より抜粋）

METI 経済産業省

3．3．2．企業･個人における新たな事前予防策

（1）官民連携した脆弱性対応体制の整備

①脆弱性に対処するためのルールと体制の整備

我が国では、情報システムの脆弱性やコンピュータウイルス、ワーム等の詳細を把握し対策を講じるための情報を収集し分析する体制が弱く、米CERT/CC やウイルスワクチンソフトベンダ などの情報を基に危険性を判断しているのが現状である。そのため、国内を中心に使用されるソフトの脆弱性への対応や急速に広がるコンピュータウイルス感染の被害を食い止める緊急対応を行うことが難しい。

そこで、政府とIT事業者 が中心となって、情報システムの脆弱性情報を集積するためのルールを構築し、それを分析する体制を整備する。具体的には、

1) 不正アクセスやコンピュータウイルス感染等の被害通報の受付
2) ネットワークのトラフィック観測に基づく異常予測
3) 脆弱性の通知と公開に関する一連の手続きルールの明確化（IT事業者や研究者等が発見した製品･システムの脆弱性の通報の受け付け、製造元もしくはサービス提供者の対処、一定期間後の公開等）
4) 脆弱性及びウイルス、ワーム等の危険性を検証･解析する体制
5) 脆弱性及びウイルス、ワーム等の危険性を警告･公表する体制

が必要である。

特に、電子政府の拡大に対応し、通報されたシステムの脆弱性やコンピュータウイルス、ワームの危険性について迅速に検証･解析する体制を、政府として整備することが重要である。中でも、オープンソース のツールや製造元が倒産した製品のように責任を負うべき事業者が明確でない場合の対応、ネットワーク全体に障害をもたらすような緊急性が高く社会的影響の大きい問題への対応等について、本体制の持つ役割は重要である。

ソフトウエアの脆弱性の傾向

- 対策方法の公表からExploitコードが出現するまでの時間が短縮化
  → ウイルス・ワームの登場から動き出すのでは間に合わない

脆弱性番号	脆弱性・対策方法の公表		Exploitコード出現		ウイルス等の攻撃発生
MS02-039	2002/7/29	2ヵ月	2002/9/25	4ヵ月	2003/1/25 SQL Slammer
MS03-026	2003/7/17	10日	2003/7/27	16日	2003/8/12 Blaster
MS03-039	2003/9/11	4日	2003/9/15	5ヵ月	2004/2/11 Welchia.B
MS03-043	2003/10/16	3日	2003/10/19	?	?
MS03-049	2003/11/12	1日	2003/11/13	2ヵ月	2004/2/11 Welchia.B
MS04-007	2004/2/11	3日	2004/2/14	?	?
MS04-011	2004/4/14	11日	2004/4/25	6日	2004/5/1 Sasser

急速に短縮化

我が国に必要な取り組み

脆弱性の特性

- 不正アクセスやコンピュータウイルス等の攻撃に脆弱性が悪用されるケースが増加し、被害拡大のスピードはユーザが対処可能なレベルを遙かに超える
- 関係者内で適切に共有され対策がなされるべき脆弱性情報が、適切に扱われず放置されたり暴露されることで、大きな被害をもたらす危険性
- 脆弱性の公開から攻撃方法の出現までの期間が短縮

我が国の問題

- 脆弱性に関する研究・発見の大半は海外に依存
- ウェブアプリケーションの場合、偶然脆弱性に気づいた人も不正アクセス禁止法の疑いを恐れ放置したり暴露する可能性
- 脆弱性の問題は、IT業界の自律的な改善が進みにくい

IT業界の対策策定の取り組みがより円滑かつ効果的に進むよう、政府がそれを補完し支援していくことが必要

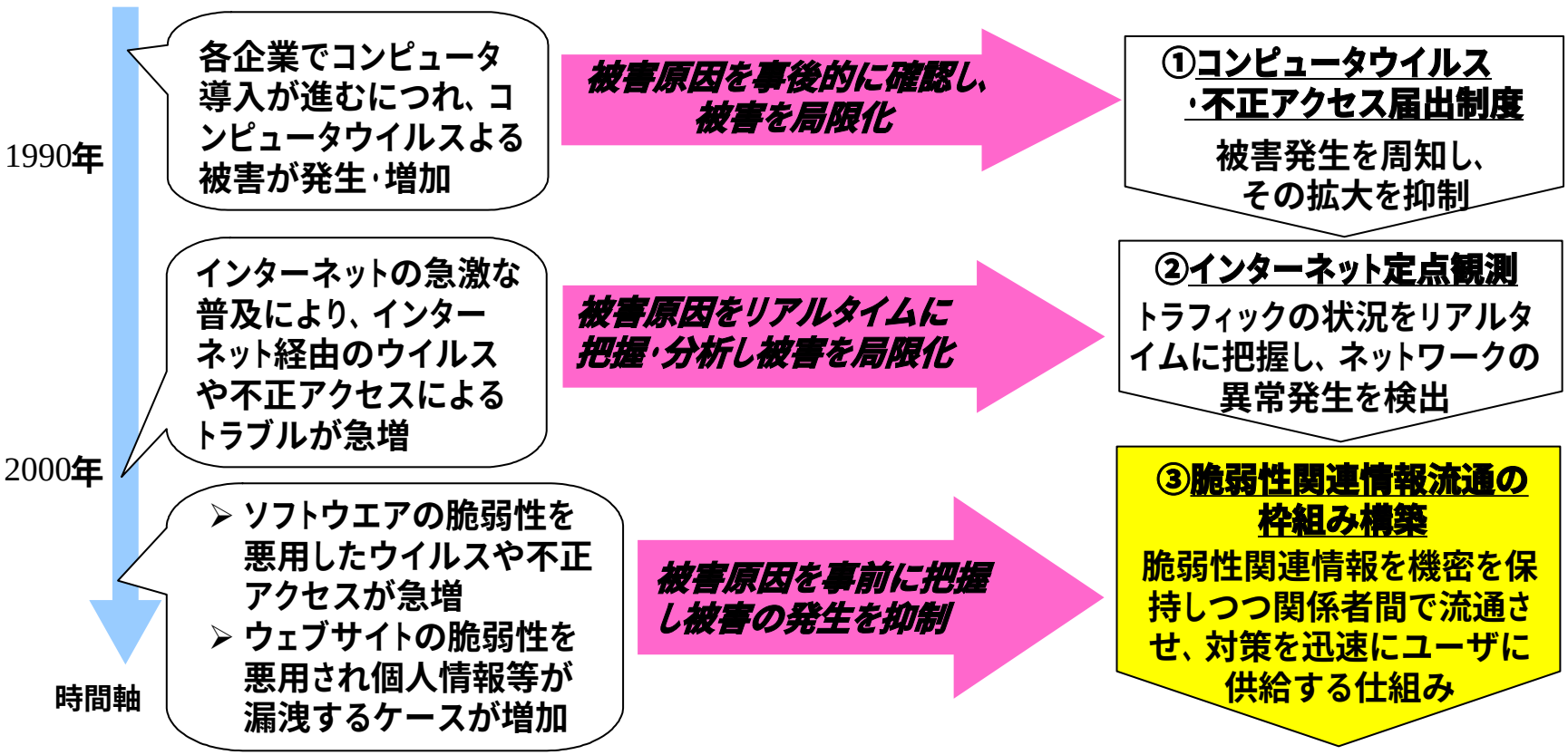
「情報セキュリティ早期警戒体制の拡充・強化」としての位置付け

経済産業省では、コンピュータ・セキュリティ上の問題に関し、早期にトラブルや予兆を発見・公表することで、その被害を局限化するための仕組み作りに取り組んできた。

①コンピュータウイルス・不正アクセス届出（IPA 1990年～、JPCERT/CC 1996年～）
②インターネット定点観測（JPCERT/CC 2003年11月～）

しかし、脆弱性の悪用により、被害拡大のスピードがユーザの対処可能なレベルを遙かに超える状況となったことから、被害の発生を抑制する方向に着手。

③脆弱性関連情報流通の枠組み構築（IPA・JPCERT/CC 2004年～）



2．脆弱性関連情報流通の枠組み構築に向けた取り組み

～「情報セキュリティ早期警戒パートナーシップ」の創設～

「情報セキュリティ総合戦略」策定後の経緯

METI 経済産業省

03/11 ～ 04/03

➢ **独立行政法人情報処理推進機構（IPA）主催の研究会が基本枠組みとルール案を提言（4/6発表）**

http://www.meti.go.jp/policy/netsecurity/vulnerability.htm
http://www.ipa.go.jp/about/press/20040406.html

04/04/30 ～ 04/05/28

➢ **経済産業省がIPA提言をもとに告示案をパブリックコメントへ**

http://www.meti.go.jp/feedback/data/i40430cj.html **意見募集**
http://www.meti.go.jp/feedback/data/i40706aj.html **結果報告**

04/07/07

➢ **経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」の制定**

http://www.meti.go.jp/policy/netsecurity/vulhandlingG.htm

04/07/08

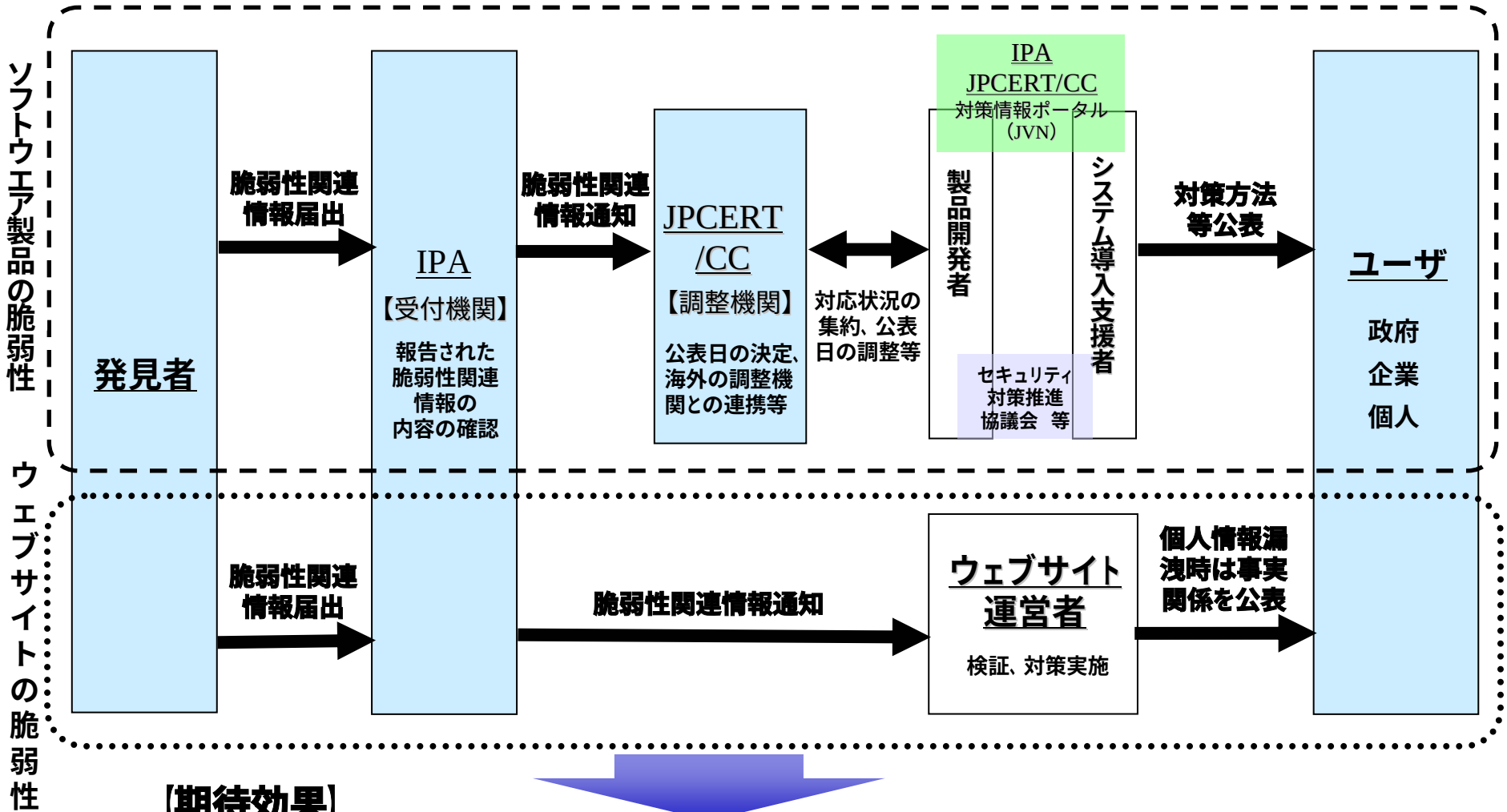
➢ **情報セキュリティ早期警戒パートナーシップの運用開始**

http://www.meti.go.jp/policy/it_policy/press/0005399/index.html

- 経済産業省告示の施行
- IPA及びJPCERTコーディネーションセンター（JPCERT/CC）において、脆弱性関連情報の取り扱いを開始
- IPA, JPCERT/CC, 社団法人電子情報技術産業協会（JEITA）, 社団法人情報サービス産業協会（JISA）, 社団法人日本パーソナルコンピュータソフトウェア協会（JPSA）, 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が連名で「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」を発表

脆弱性関連情報流通の基本枠組み ～「情報セキュリティ早期警戒パートナーシップ」

METI 経済産業省



【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脆弱性関連情報の放置・危険な公表を抑制
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

告示とパートナーシップガイドラインの位置づけ

【ソフトウエア等脆弱性関連情報取扱基準】

- 経済産業省が告示として制定［官］
- 脆弱性関連情報の流通に関する基本枠組み
- 第三者が脆弱性関連情報を発見し、受付機関に届け出た際の、関係者に求める行動基準

・受付機関、調整機関を指定

【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】

- IPA，JPCERT/CC，JEITA，JISA，JPSA，JNSAが連名で公表［民］
- 第三者が脆弱性関連情報を発見し、IPA に届け出た際の、関係者に係る自らの役割や推奨される事項を示した指針
- 法律専門家の見解をもとに発見者、製品開発者、ウェブサイト運営者の法的論点を整理

基本的な思想は共通

官民連携したソフトウエア等の脆弱性関連情報流通の枠組み
～「情報セキュリティ早期警戒パートナーシップ」を支える基盤

告示とパートナーシップガイドラインの全体構成

【ソフトウエア等脆弱性関連情報取扱基準】

- ◆ 趣旨
- ◆ 定義（用語、関係者）
- ◆ 適用範囲

- ◆ ソフトウエア製品の脆弱性
  - ・発見者基準
  - ・受付機関基準
  - ・調整機関基準
  - ・製品開発者基準

- ◆ ウェブアプリケーションの脆弱性
  - ・発見者基準
  - ・受付機関基準
  - ・ウェブサイト運営者基準

受付機関、調整機関の指定

IPA, JPCERT/CC を指定

【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】

- ◆ 位置づけ
- ◆ 用語の定義と前提
- ◆ 適用範囲

- ◆ ソフトウエア製品の脆弱性
  - ・発見者の対応
  - ・IPAおよびJPCERT/CCの対応
  - ・製品開発者の対応

- ◆ ウェブアプリケーションの脆弱性
  - ・発見者の対応
  - ・IPAの対応
  - ・ウェブサイト運営者の対応

- ◆ 付録（ガイドラインにのみ記載）
  1. 発見者の法的な論点
  2. 製品開発者の法的な論点
  3. ウェブサイト運営者の法的な論点

基本枠組みや関係者の行動基準

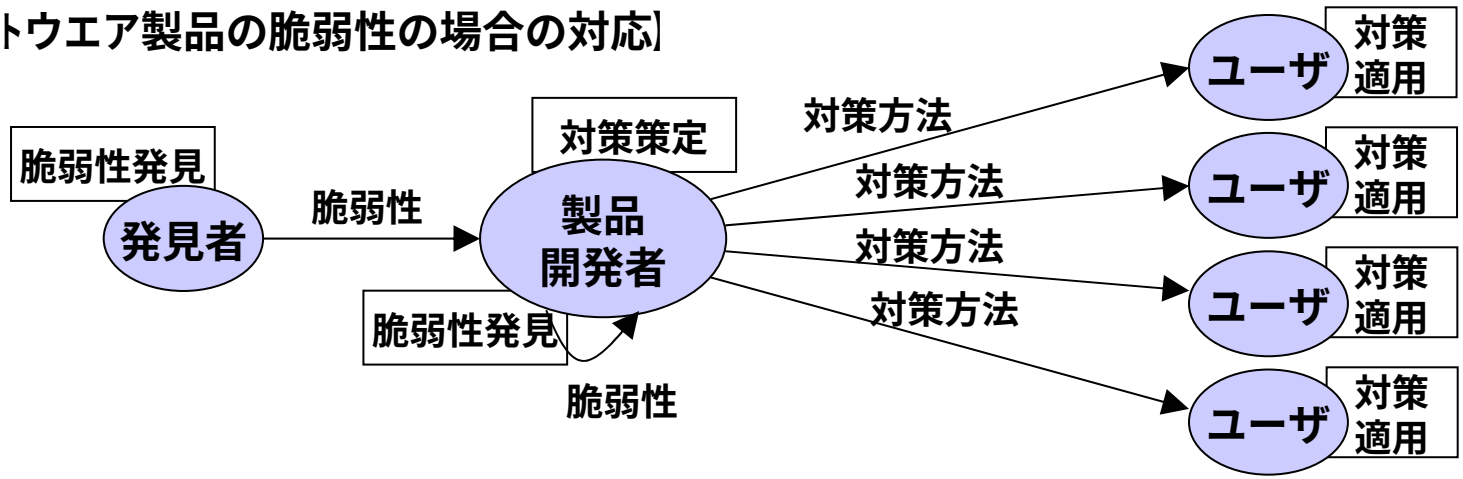
自らの役割や推奨事項を示した指針

法律専門家の見解に基づく法的論点

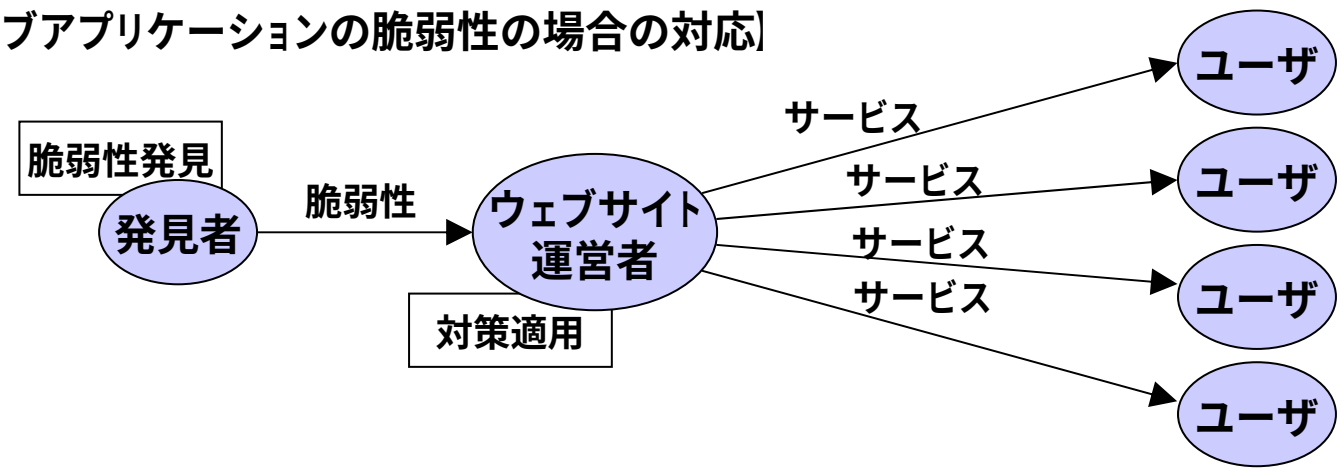
脆弱性とはなにか

「脆弱性」とは、「ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃により機能や性能を損なう原因となり得る安全性上の問題箇所」と定義

【ソフトウエア製品の脆弱性の場合の対応】



【ウェブアプリケーションの脆弱性の場合の対応】



適用範囲の考え方

- 脆弱性が発見される可能性や発見された場合の影響規模を踏まえ、ソフトウエア製品及びウェブアプリケーションを本枠組みの対象とする
- ソフトウエア製品の脆弱性については、**製品開発者**が対策方法を策定
- ウェブアプリケーションの脆弱性については、**ウェブサイト運営者**が対策を適用

・**ソフトウエア製品**：ここではソフトウエア自体またはソフトウエアを組み込んだハードウエア等の汎用性を有する製品とする。
・**ウェブアプリケーション**：インターネット上の各ウェブサイトで稼働するシステム。
・**製品開発者**：ソフトウエア製品を開発した企業もしくは個人。また、ソフトウエア製品の開発、加工、輸入又は販売に関して当該ソフトウエア製品の実質的な開発者と認められる者。
・**ウェブサイト運営者**：そのウェブサイトについて対外的な責任を有する事業者（個人の場合を含む）。依頼されてウェブサイトの作成・運用を代行する事業者や第三者は直接の対象にはならない。

汎用 ⟷ 専用

	汎用ソフトウエアの例	専用システムの例
不特定多数の一般ユーザ向け	・クライアント上のソフトウエア（OS、ブラウザ、メーラー等） ・サーバ上のソフトウエア（DBMS、ウェブサーバ等） ・プリンタ、コピー機 ・ICカード ・PDA	・インターネット上のウェブサイトで稼働しているウェブアプリケーション（電子申請、ネットバンキング等）
特定ユーザ向け	・極めて限定的な層が利用する特定用途アプリケーション	・企業内のカスタムアプリケーション

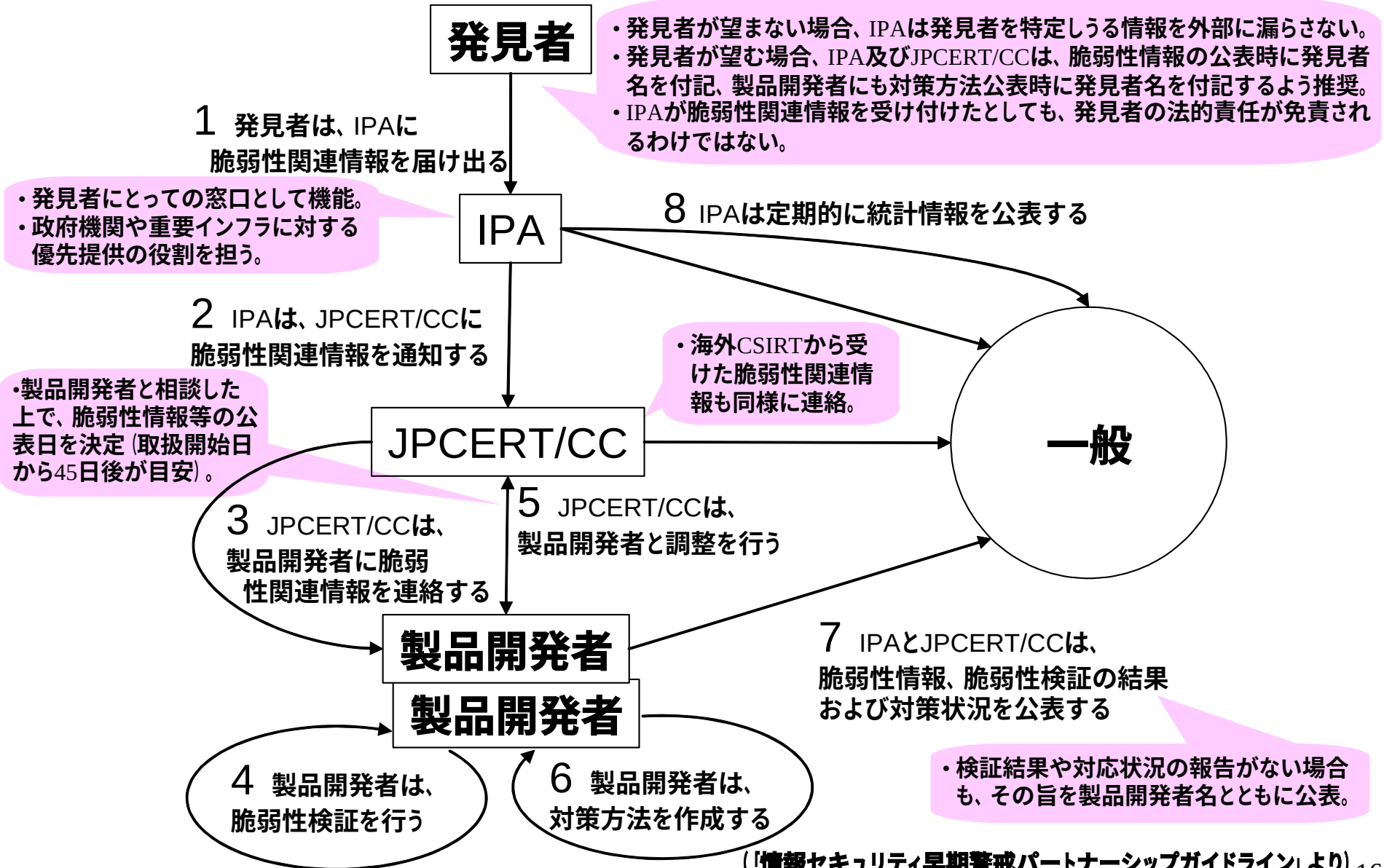
本枠組みの適用範囲

・脆弱性が不特定多数のユーザに発見される可能性
・発見された場合影響範囲が大きい

・脆弱性が発見されにくい
・発見されてもその影響範囲は小さい

ソフトウエア製品に係る脆弱性関連情報取扱

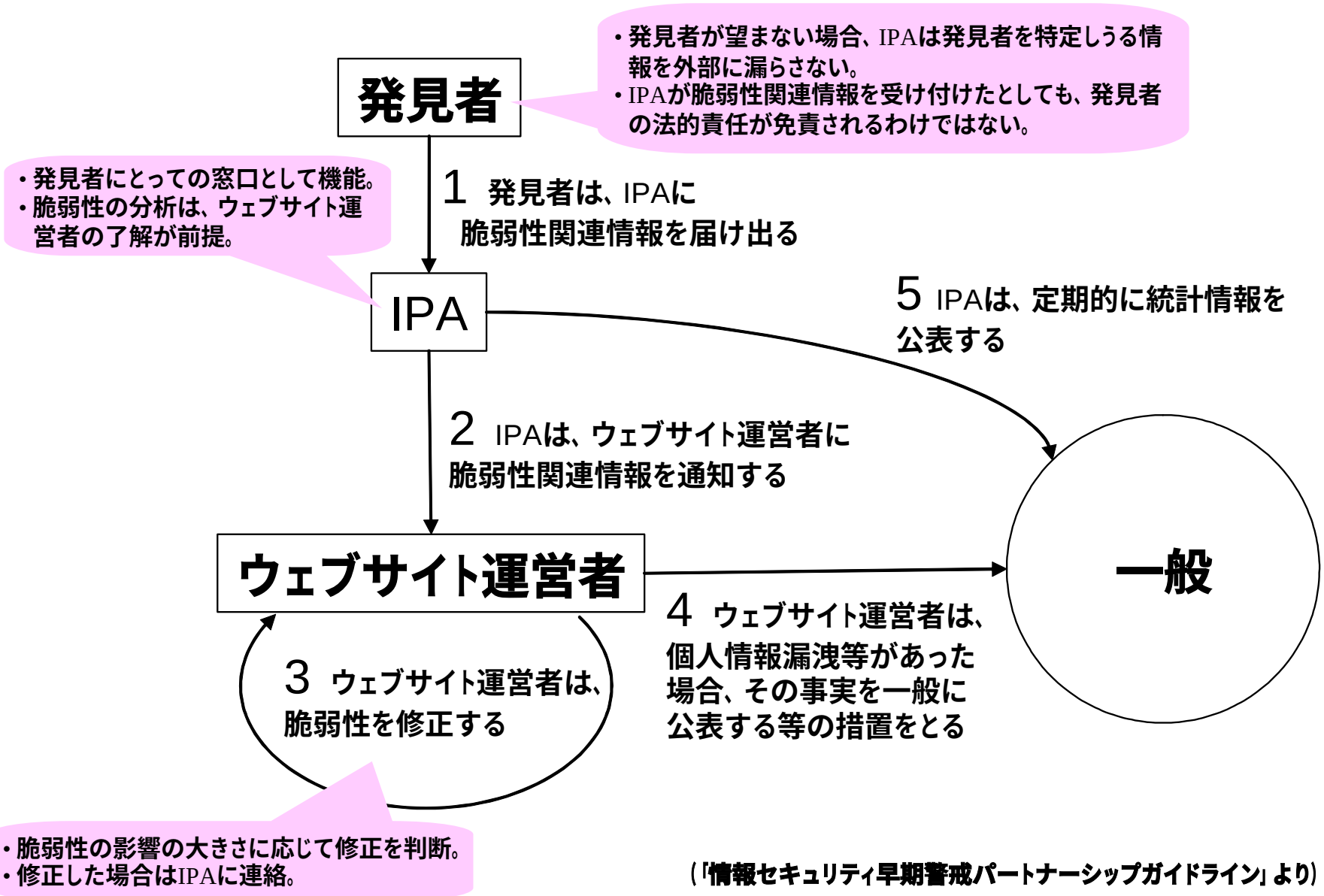
METI 経済産業省



（「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」より）

ウェブアプリケーションに係る脆弱性関連情報取扱

METI 経済産業省



（「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」より）

3．今後の展開

～「情報セキュリティ早期警戒パートナーシップ」の推進～

今後の展開

■ 官民連携した枠組み全体の支持

- 官と民がともに「情報セキュリティ早期警戒パートナーシップ」を支えることを意思表示。
  - ✓ 経済産業省告示（7／7制定）
  - ✓ 関連機関・団体（IPA, JPCERT/CC, JEITA, JISA, JPSA, JNSA）が連名で「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」を公表（7／8発表）

■ 業界側の参加促進

- 「製品開発ベンダーにおける脆弱性情報取扱に関する体制と手順整備のためのガイドライン」
  - ✓ 「製品開発者」の立場で脆弱性関連情報を扱う場合の社内体制や処理手順等のあり方について検討し、これを促進するためのガイドラインを整備。
  - ✓ JEITAにWGを設置。JISAも参加し、連名で7月中旬公表予定。

    → *他団体も本ガイドラインをベースに自らの業界特性に応じた版を策定する方向*
- 窓口担当者向けマニュアル

  製品開発者における脆弱性関連情報の窓口担当者が理解すべき作業事項をJPCERT/CCがマニュアル的に解説。7月中旬公表予定。

■ ユーザ側の対策促進

- 対策情報の受け手であるユーザ企業側の観点から見た問題点や必要な施策についての検討に着手。

「情報セキュリティ早期警戒パートナーシップ」の推進手段

METI 経済産業省

②業界側の参加促進

＜7月中旬発表予定＞

窓口担当者向けマニュアル

【JPCERT/CC】

製品開発者における脆弱性関連情報の窓口担当者が把握すべき作業事項

＜7月中旬発表予定＞

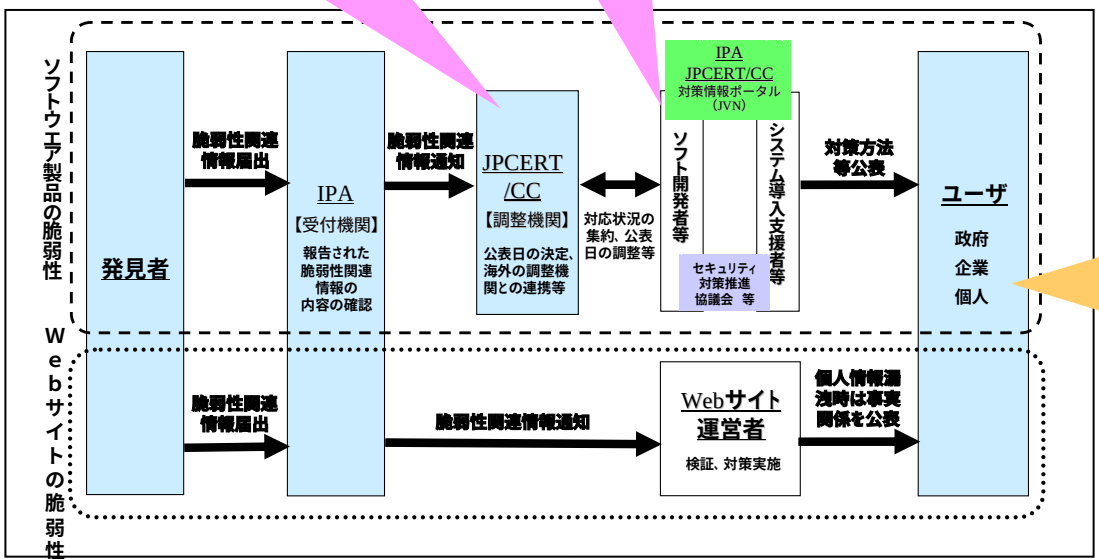
製品開発者向けガイドライン

【JEITA, JISA】

脆弱性関連情報を扱う上で業務プロセスや社内体制等の在り方を提示

波及効果

他の業界団体版ガイドライン



③ユーザ側の対策促進

ユーザ側から見た、脆弱性問題に関する改善方策の検討

①官民連携した枠組みの支持

官

＜7月7日制定＞

ソフトウエア等脆弱性関連情報取扱基準

（経済産業省告示）

脆弱性関連情報の基本枠組みや関係者に求められる行動基準

民

＜7月8日公表＞

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

【IPA,JPCERT/CC,JEITA,JISA,JPSA,JNSA】

枠組みに参加する関係者及び関係業界が、自らの役割や推奨される事項を示した指針