JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

JNSAにおけるセキュリティ情報流通に関する取り組み

武智　洋

情報流通検討委員会

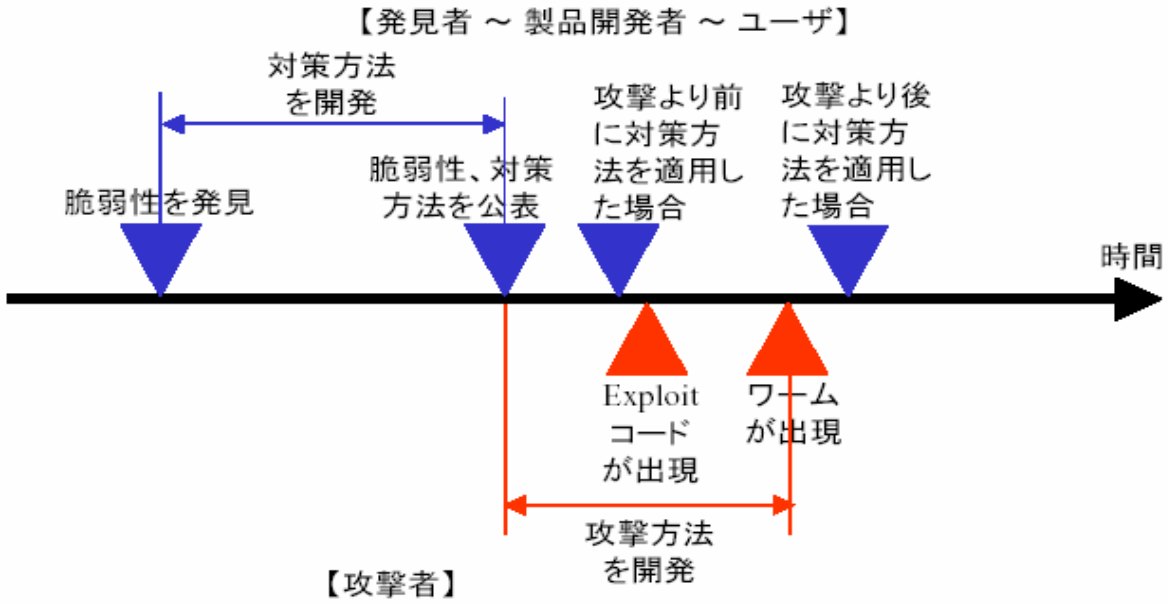
2004年5月18日

セキュリティ情報流通の必要性

- SlammerやBlaster、先日はSasserなど、エンドユーザのみならずISPなどのネットワークにも大きな被害をもたらす大規模インシデントが次々と発生
- エンドユーザのインシデント対応遅れにより、被害が拡大
- 脆弱性公表に関する調整が不十分
  - 特に、エンドユーザへの対応が不十分
    （迅速、正確、わかりやすく）
- 脆弱性に関する研究・発見・対策策定の多くを海外に依存
- 脆弱性に関する情報の取り扱いについて、国内の指針やガイドラインが存在しない

脆弱性の特性

- 情報の適切かつ慎重な取扱いが必須
  - 放置や、対策がない段階での暴露は攻撃に悪用され、大きな被害をもたらす危険がある
- 脆弱性公表から攻撃方法出現までの期間が短縮している
  - 対策方法自体が攻撃方法開発のヒントになる要素を持っている



大規模インシデントに対する対応

- ソフトウェアなどの脆弱性関連情報や対策情報を集積公表し、広く末端のエンドユーザまでに情報を流通させて、日本国全体でインシデントを回避できるような対策を取る仕組みを作る
- 現状の対応組織
  - IPA/JPCERT
  - インターネットセキュリティ対策推進協議会

IPAとJPCERT/CC

- 「情報システム等の脆弱性情報の取扱いに関する研究会」からスタート

  http://www.ipa.go.jp/security/fy15/reports/vuln_handling/

- 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（案）」等を制定
  - 5月28日までパブリックコメントを受付中

    http://www.meti.go.jp/feedback/data/i40430cj.html

- 目的
  - 政府による「情報セキュリティ総合戦略」（平成15年10月発表）の提言に沿って、脆弱性と闘うIT業界の取り組みがより円滑かつ効果的に進むよう、国がそれを補完し支援する官民連携のしくみを構築し、ITユーザの被害発生を阻止することをめざす。

    （経済産業省のホームページからの引用 http://www.meti.go.jp/policy/netsecurity/vulnerability.htm）

- 平たく言うと
  - 国の組織として、脆弱性関連情報の受付、公表、重要インフラへの情報提供、公表ルールの策定、などをおこなう

脆弱性関連情報の種類と取扱い方針

IPA, 2004

区別して考える必要

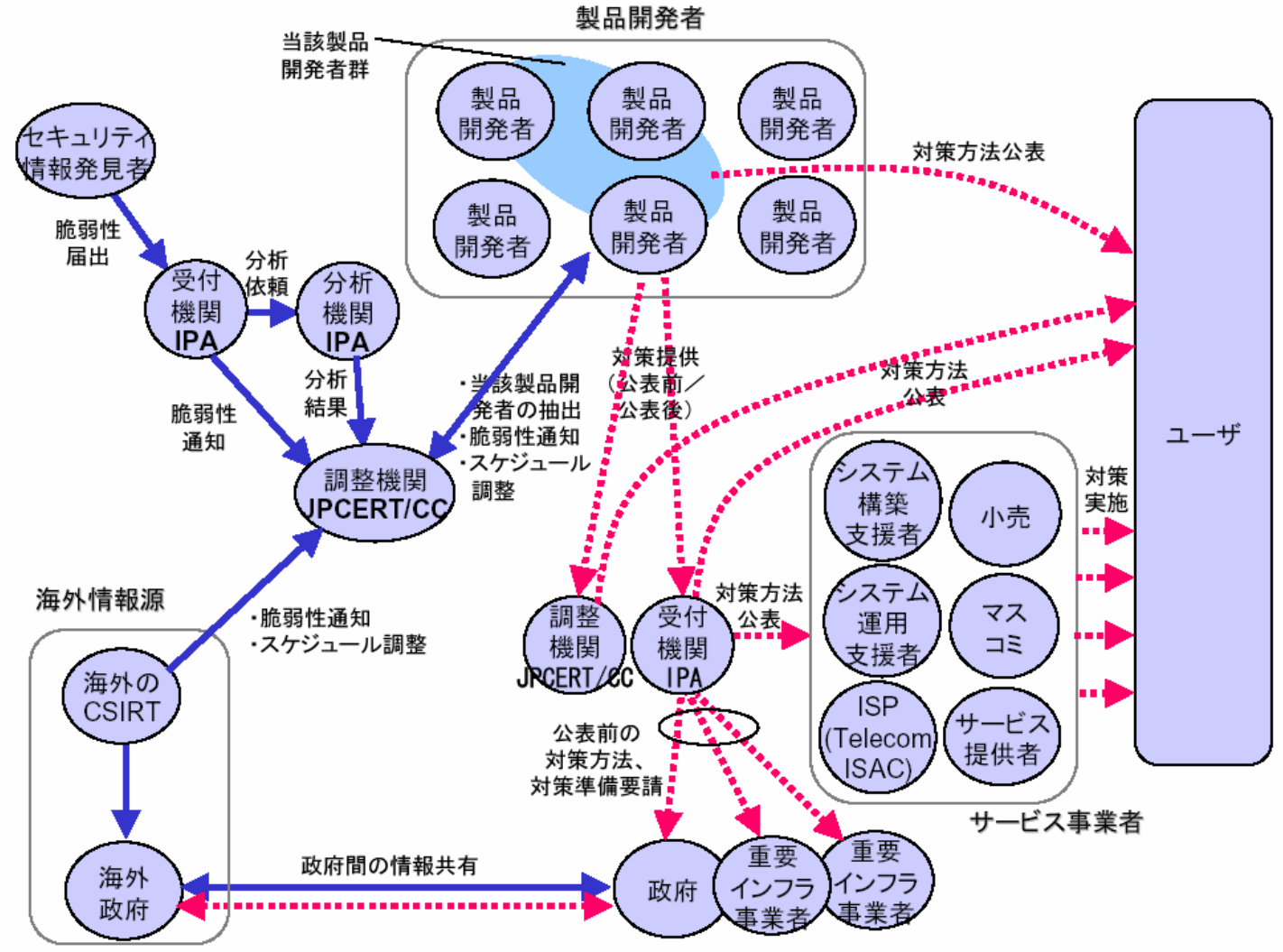
情報の種類		内容	取扱い方針
脆弱性関連情報	脆弱性	ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。 ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。	対策方法が公表されるまでは原則として**公表しない**。
	攻撃方法	脆弱性を悪用するプログラム、コマンド、データ及びそれらの使用方法。	**公表しない**。
	検証方法	脆弱性が存在することを調べるための方法。	**公表しない**。
対策方法	回避方法	脆弱性を修正するのではないが、それが原因となって生じる被害を回避するための方法。 ワークアラウンドと呼ばれる。	公表後**迅速にユーザに流通させる**。
	修正方法	脆弱性を修正する方法。パッチ。	公表後**迅速にユーザに流通させる**。

基本枠組みを支える役割分担

IPA, 2004

対象	受付	調整	分析･対策策定	公表	情報利用
ウェブアプリケーションの脆弱性	■IPA ･一次受付 ･スクリーニング ･受理／不受理通知 ･当該ウェブサイト運営者への通知 ･統計データ化	―	■当該ウェブサイト運営者 ･脆弱性の検証 ･対策の実施 ･IPA へ完了報告 ←（IPA が必要と判断した場合、当該ウェブサイト運営者の許可を得て分析）	■当該ウェブサイト運営者 ･個人情報漏洩の可能性がある場合には事実関係を公表 ■IPA ･統計データの集積･公表	■ウェブサイト運営者 ･統計データを踏まえ、ウェブアプリケーションの脆弱性の実態について把握
ソフトウェア製品の脆弱性（発見者からの届出）	■IPA ･一次受付 ･スクリーニング ･受理／不受理通知 ･統計データ化	■JPCERT/CC ･配信先の抽出･通知 ･公表スケジュールの管理 ･IPA の分析成果を当該製品開発者に提供	■当該製品開発者 ･対策方法の策定（ワークアラウンド、パッチ、ver-up 等） ■IPA ･脆弱性分析（影響範囲の検証、リスク分析、脆弱性検証ツールの作成等）	■当該製品開発者 ･スケジュールに沿って対策方法を公表 ■IPA、JPCERT/CC ･対策方法を公表 ･IPA がDB 登録 ･IPA が統計データを集積･公表 ■インターネットセキュリティ対策推進協議会 ･一般ユーザへの対策適用を促す	①製品開発者 ･JPCERT/CC から脆弱性関連情報の提供を受けて自社製品への影響を検証、報告 ･機密保持が前提 ②政府･重要インフラ事業者 ･IPA から公表前の対策方法や準備要請情報の提供を受けて対処 ･機密保持が前提 ③システム構築者/運用者、ISP(Telecom-ISAC Japan) ･公表後の対策方法を受けてユーザに対策実施 ･JNSA 等の活動と連携 ←IPA のDB を活用
ソフトウェア製品の脆弱性（海外CSIRT からの連絡）	―	■JPCERT/CC ･海外CSIRT からの受信 ･配信先の抽出･通知 ･公表スケジュールの管理 ･IPA の分析成果を当該製品開発者に提供 ･情報源への報告			

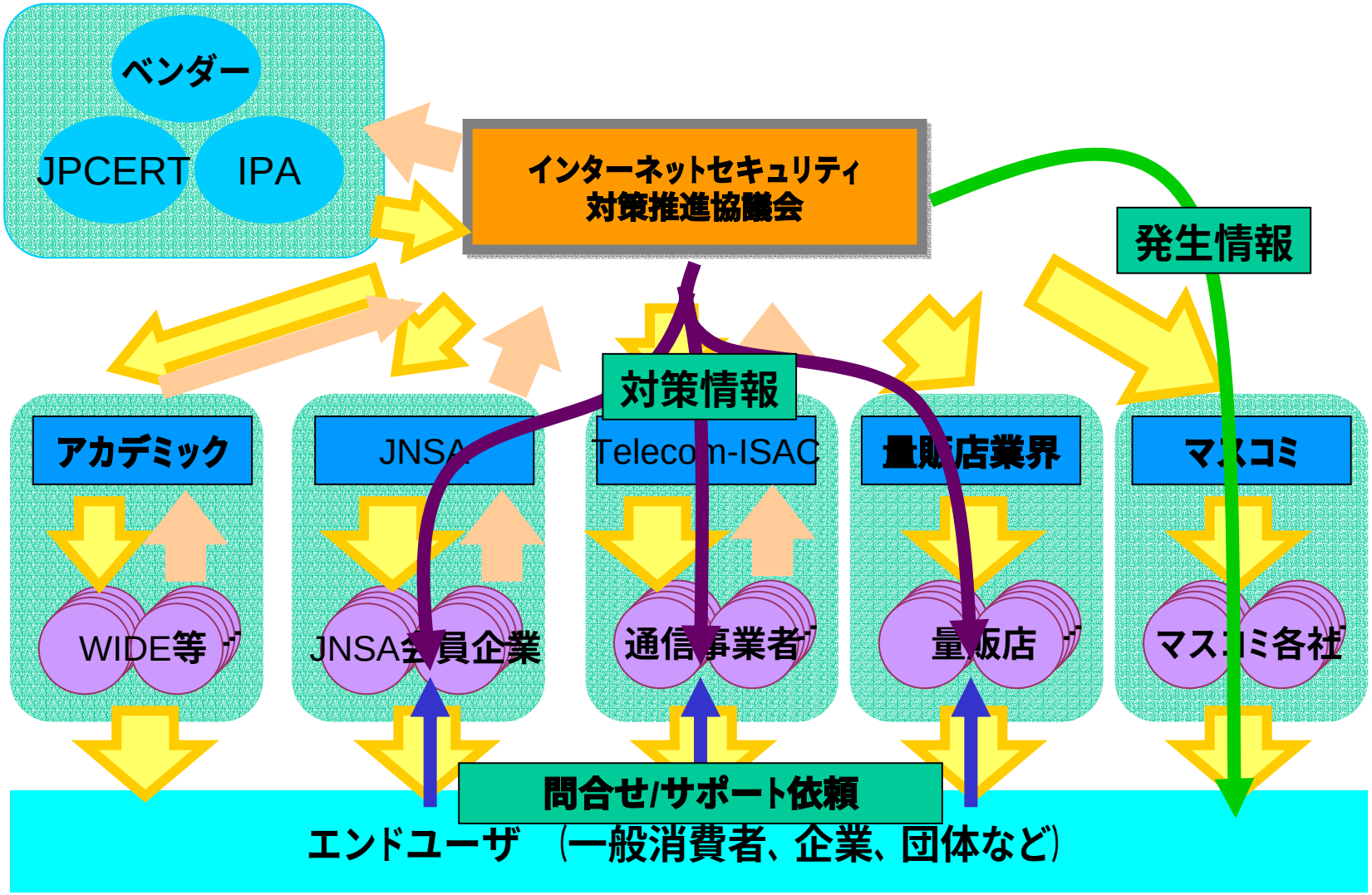
IPA/JPCERTの取り組み



インターネットセキュリティ対策推進協議会

- 2003年10月頃より検討開始
- 2004年2月4日 協議会設立のための準備会発足のアナウンス
- 現在、数十名の設立幹事会
- 目的
  - 会員の顧客等（エンドユーザ）がセキュアになることを目的とし、セキュリティ対策を推進するための各種情報を正確に・早く・わかりやすく会員に提供する。
- 情報を提供する対象
  - セキュリティに関しての知識が少なく、またセキュリティ意識も高くないユーザ
- 提供する情報
  - 修正方法や回避策が明確になっている脆弱性情報や脅威情報に関する対策推奨情報。何をすればよいのか分かる情報として提供する。

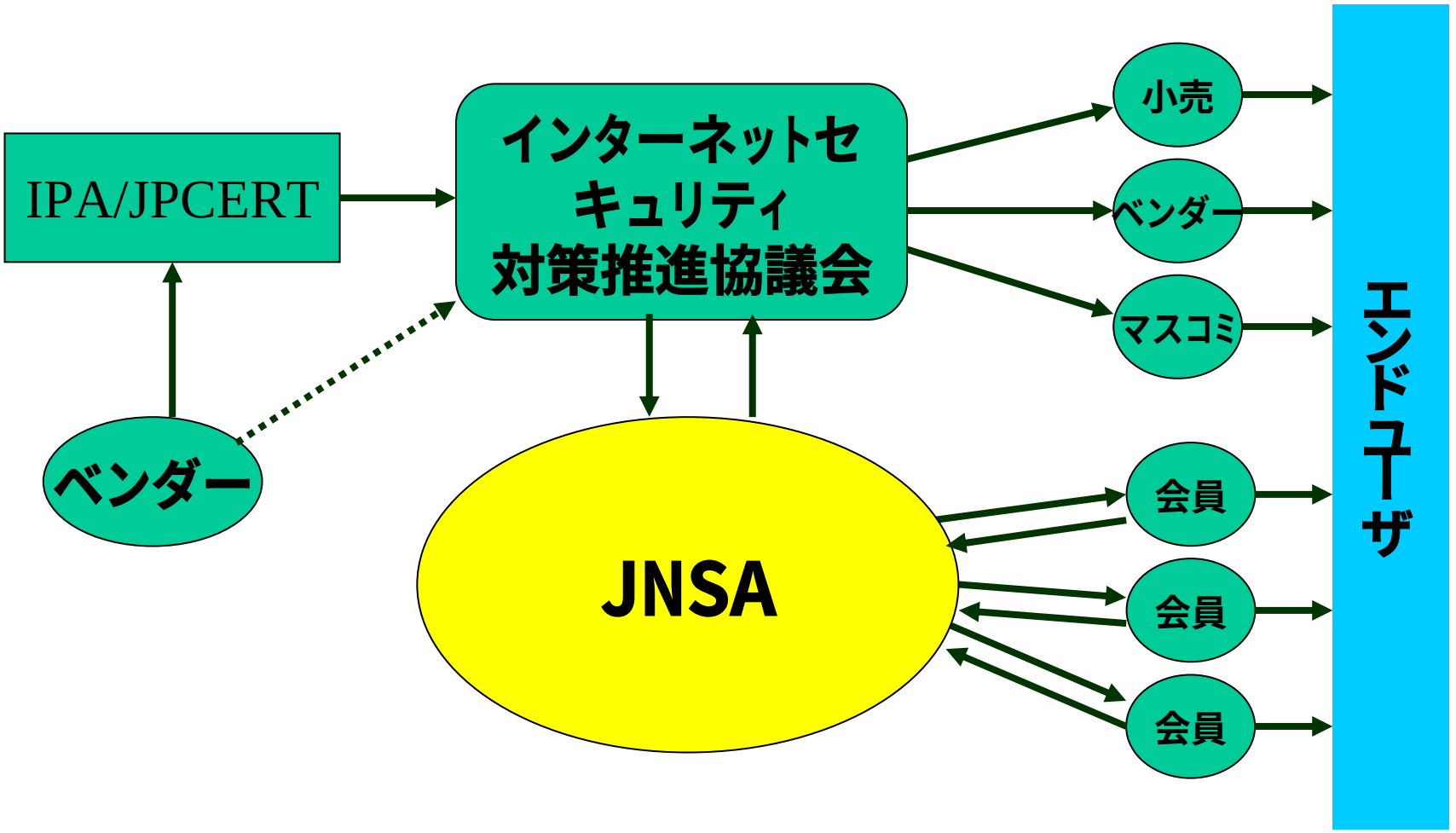
インターネットセキュリティ対策推進協議会の取り組み



JNSA 情報流通検討委員会

- **目的**
  - JNSAにおいて、セキュリティ対策などの情報流通をどのように行うべきかを検討する。
- **概要**
  - JNSA会員への脆弱性情報、対策情報をどのようなルートで、迅速に伝達させるかのルールと仕組みを作る
  - インターネットセキュリティ対策推進協議会の対応
    - Telecom-ISAC Japanとともに事務局として活動
    - 協議会の一会員として、JNSA会員への窓口となる
- **扱う情報**
  - 会員企業が取り扱うｾｷｭﾘﾃｨｿﾘｭｰｼｮﾝの脆弱性情報
  - その対策情報
    - ベンダーから提供されるパッチ情報など
  - 派生情報
    - パッチ等の適用に関する対策影響情報など

JNSAの対応



今後の活動

- インターネットセキュリティ対策推進協議会等との連携
- JNSAとしてセキュリティ情報流通をどのように行うかの検討
- 会員、およびそのエンドユーザに役立つ情報を、迅速、正確、わかりやすい形で提供できるような仕組みづくり