

# 海外のセキュリティ対策の動向について

---

2007.2.14(水)

JPCERT/CC コーディネーションセンター

早期警戒グループ

情報セキュリティアナリスト 名和 利男

# アジェンダ

---

- そもそも“対策”とは？
  
- 海外のセキュリティ対策の概観
  - コミュニティの活発な活動
  - テクニカルトレーニング
  - 対応体制の Dry run(予行演習)
  
- セキュリティ対策に必要なテクニック  
「アドバイザリー(注意喚起)を出す際の注意喚起」

そもそも“対策”とは？

# そもそも“対策”とは？

---

## □ “対策”

- 好ましくない事態の出現を解決するために取る、また、相手の態度や事件の成行きに応じて取る、手段・方策。

*(新明解国語辞典, 第五版(C)三省堂 より)*

## □ みなさんにとって、何が「好ましくない事態」なのか？

- これまでのトラブルやインシデントの対応で困った経験から思い描いてみてください。

## □ どんな「解決手段や方策」があるのか？

- 「相手の態度や事件の成行きに応じて」ということを念頭において、思い描いてください。

# 海外のセキュリティ対策の概観

# 海外のセキュリティ対策の概観

- すべての対策に係る活動の基盤は、“信頼(Trust)”
  
- 海外のセキュリティ対策の動向を概観すると...
  1. コミュニティの活発な活動
    - インシデント対応に必要な国際間連携、最新のインシデントや対策技術に関する情報共有などの活動が見られる。
  2. テクニカルトレーニング
    - インシデント対策に必要なノウハウや技術の習得や、各種ツールを活用した分析手法などが顕著に見られる。
  3. 対応体制の Dry run(予行演習)
    - インシデントへの対応体制の構築後、意図どおりに機能するかのテストと、関連するルールの適合性や、担当者の習得度合いを測るために活用されている。

# 1. コミュニティの活発な活動

## □ APCERT と TF-CSIRT

**TF-CSIRT**

<http://www.terena.org/activities/tf-csirt/>

**APCERT**

<http://www.apcert.org/>

# 1. コミュニティの活発な活動

## □ APCERT と TF-CSIRT

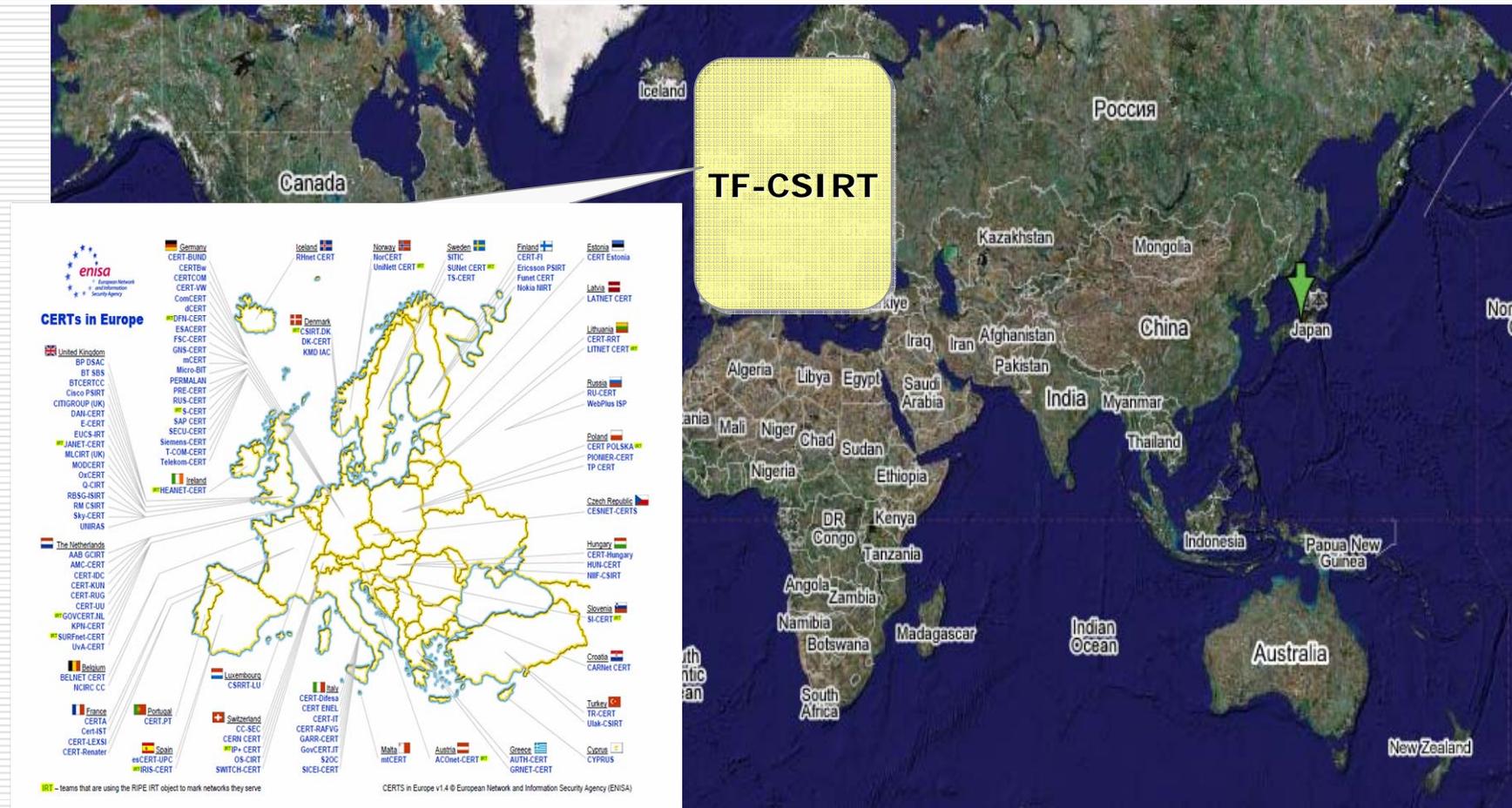


TF-CSIRT

- TF-CSIRT は、ヨーロッパの研究グループ (TERENA) の 1 Task Force として 2000年に設立
- 主な活動概要
  - CSIRT Start kit サイトの提供  
<http://www.terena.org/activities/tf-csirt/starter-kit.html>
  - Trusted Introducer for CSIRT in Europe  
フォーラムに参加する条件を既存メンバの推薦や「信頼性」によるレベル分け、年に3回のミーティング
  - CHIHT - Clearinghouse of Incident Handling Tools (<http://chiht.dfn-cert.de/>)  
インシデントハンドリングに必要なツールやガイドラインなどの情報を収集している。
  - IODEF - Incident Object Description and Exchange Format  
異なる CSIRT 間においてインシデントに関する情報をやり取りするための共通データフォーマットを構築
  - RTIR – Request Tracker for Incident Response WG  
インシデントハンドリングに役立つ Web アプリ (<http://bestpractical.com/rtir/>)

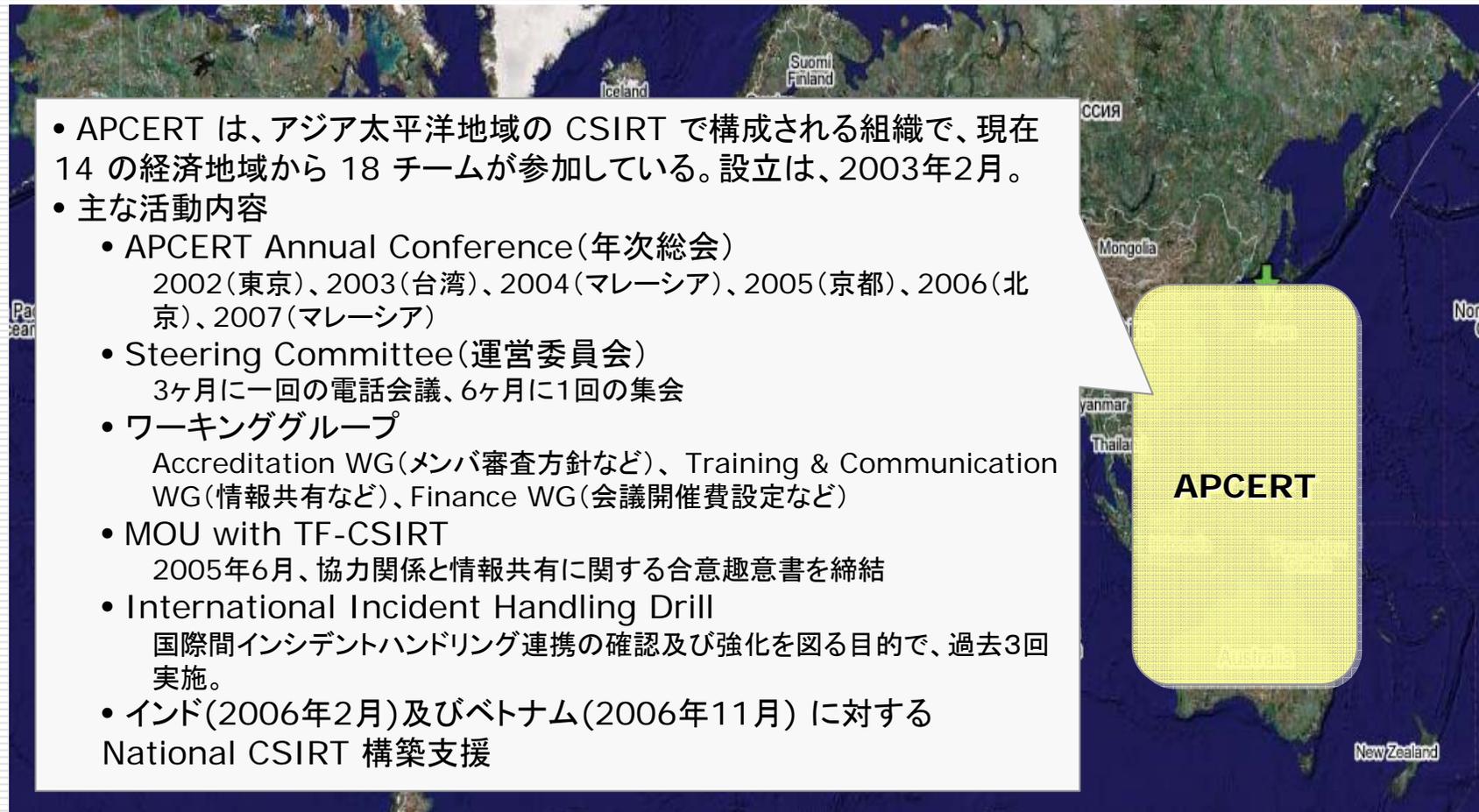
# コミュニティの活発な活動

## □ APCERT と TF-CSIRT



# コミュニティの活発な活動

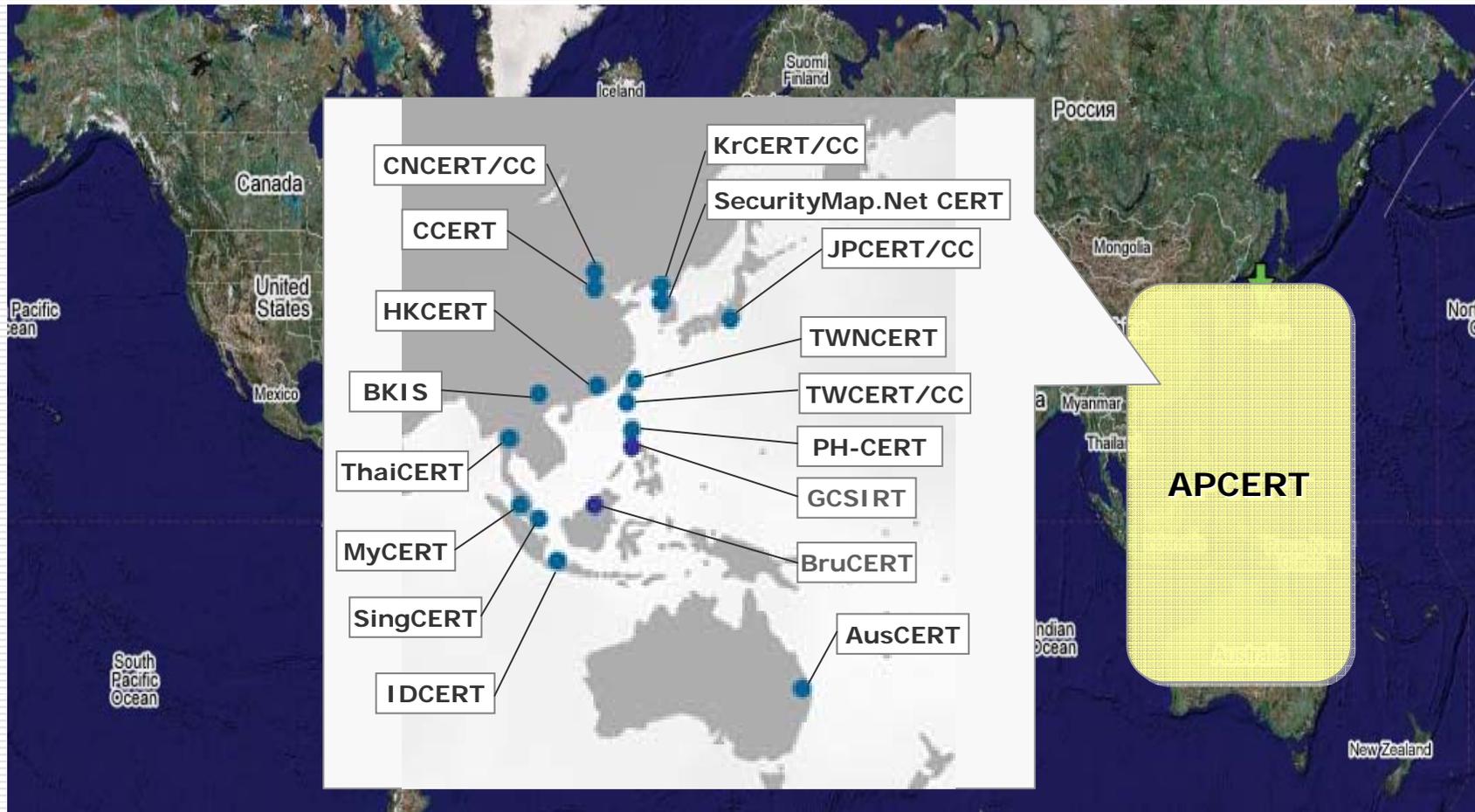
## □ APCERT と TF-CSIRT



- APCERT は、アジア太平洋地域の CSIRT で構成される組織で、現在 14 の経済地域から 18 チームが参加している。設立は、2003年2月。
- 主な活動内容
  - APCERT Annual Conference (年次総会)  
2002(東京)、2003(台湾)、2004(マレーシア)、2005(京都)、2006(北京)、2007(マレーシア)
  - Steering Committee (運営委員会)  
3ヶ月に一回の電話会議、6ヶ月に1回の集会
  - ワーキンググループ  
Accreditation WG (メンバ審査方針など)、Training & Communication WG (情報共有など)、Finance WG (会議開催費設定など)
  - MOU with TF-CSIRT  
2005年6月、協力関係と情報共有に関する合意趣意書を締結
  - International Incident Handling Drill  
国際間インシデントハンドリング連携の確認及び強化を図る目的で、過去3回実施。
  - インド(2006年2月)及びベトナム(2006年11月) に対する National CSIRT 構築支援

# 1. コミュニティの活発な活動

## □ APCERT と TF-CSIRT



# 1. コミュニティの活発な活動

## □ FIRST

**FIRST**  
United States

**FIRST**  
Forum of Incident Response and Security Teams

**Events at Spotlight**

- Joint FIRST and TF-CSIRT Meeting
- March 2007 FIRST Technical Colloquium
- April 2007 FIRST Technical Colloquium

**SEVILLE SPAIN**

**FIRST is the global Forum for Incident Response and Security Teams**

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents - reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:

- access to up-to-date best practice documents
- technical colloquia for security experts
- hands-on classes
- annual incident response conference
- publications and webservices
- special interest groups

Currently FIRST has more than 170 members, spread over the Americas, Asia, Europe and Oceania.

**What's new**

**Tue, 23 Jan 2007**

Four new sponsors for the 2007 FIRST Conference in Seville (17-20-2007)

Google, KVCERT/CC, Cisco and Cymru are now sponsoring our conference. Our thanks to all of our current sponsors for their valuable support. There are still sponsorship opportunities available, please visit the Conference Sponsorship web page.

**Thu, 14 Dec 2006**

Register now for January TC in Budapest, Hungary (15-16-2007)

This Colloquium will be a joint event between FIRST and the TF-CSIRT from 29-31 January 2007, in Budapest (HU). FIRST Members may register online via the FIRST website to attend to the event.

**Fri, 08 Dec 2006**

Information: I CEP Monthly Social Networking Club (19-16-2006)

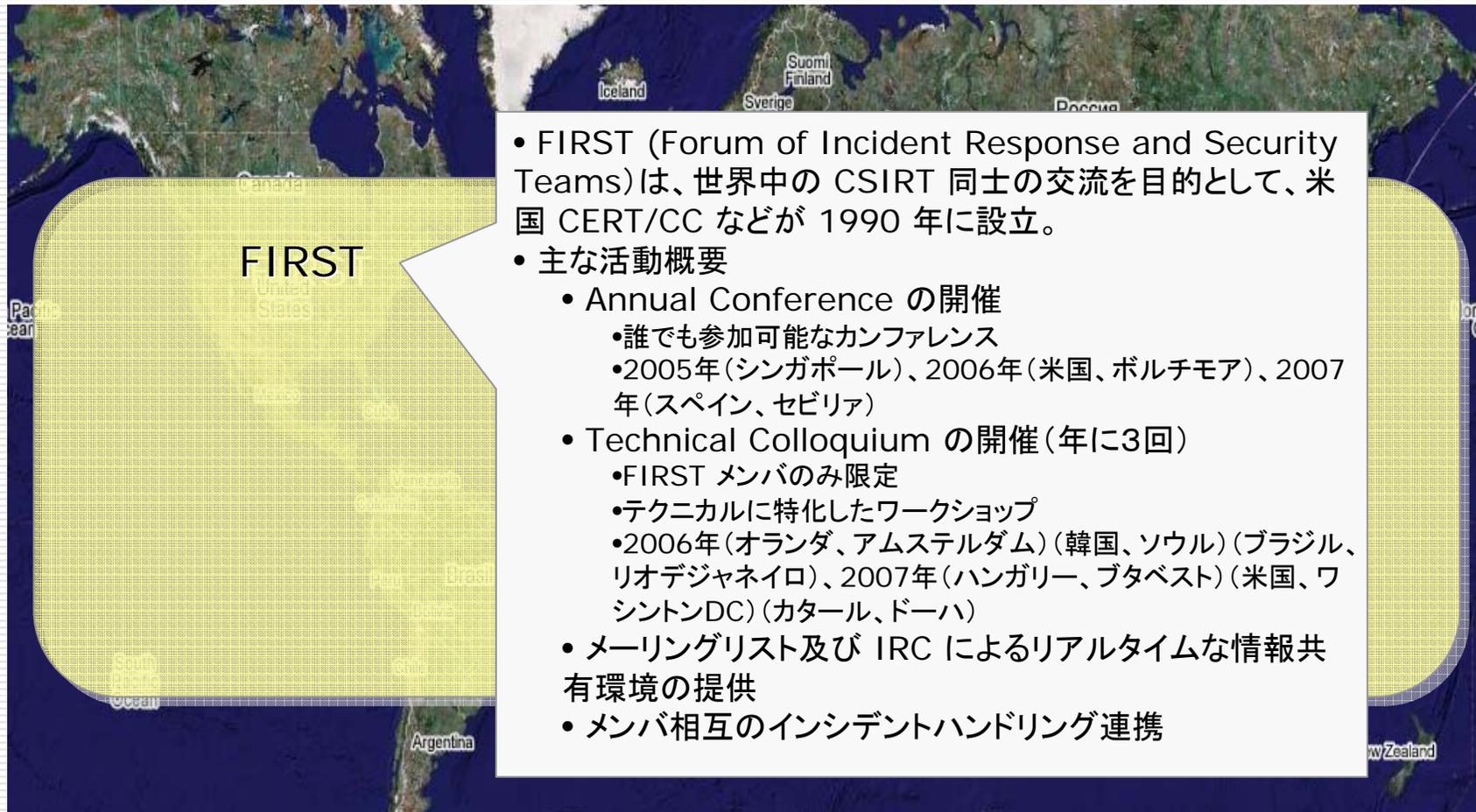
Every last Wednesday of each month members and guests of the CEP meet to catch-up on the latest. The aim is to provide a venue in the City of London, so that we can get together after work and have a chat over some nibbles, wine / beer / water. There are no presentations, speeches, canvassing, pressure, or anything that would spoil a wind-down drink and chat Dates: Every last Wednesday of each month (except December) Time: From 6pm until 8:30pm

Contact | Copyright © 1995 - 2006 by FIRST.org, Inc. View this page as a member

<http://www.first.org/>

# 1. コミュニティの活発な活動

## □ FIRST



FIRST

- FIRST (Forum of Incident Response and Security Teams)は、世界中の CSIRT 同士の交流を目的として、米国 CERT/CC などが 1990 年に設立。
- 主な活動概要
  - Annual Conference の開催
    - 誰でも参加可能なカンファレンス
    - 2005年(シンガポール)、2006年(米国、ボルチモア)、2007年(スペイン、セビリア)
  - Technical Colloquium の開催(年に3回)
    - FIRST メンバのみ限定
    - テクニカルに特化したワークショップ
    - 2006年(オランダ、アムステルダム)(韓国、ソウル)(ブラジル、リオデジャネイロ)、2007年(ハンガリー、ブタベスト)(米国、ワシントンDC)(カタール、ドーハ)
  - メールングリスト及び IRC によるリアルタイムな情報共有環境の提供
  - メンバ相互のインシデントハンドリング連携

# 1. コミュニティの活発な活動

## □ FIRST 2007 Annual Conference ! (2007.6.17-22)

**SEVILLE JUNE 2007 SPAIN**  
19th Annual **FIRST** Conference

PRIVATE LIVES AND CORPORATE RISK: digital privacy - hazards and responsibilities  
**June 17- 22, 2007**  
**Melia Sevilla Hotel**  
**Seville, Spain**

**PROTECTING PRIVATE and PERSONAL INFORMATION**  
**PREVENTING FRAUD, THEFT and ACCIDENTAL LOSSES**  
**PRESERVING CORPORATE REPUTATION**

Privacy is the genie in the bottle for all data-holding organizations - once out, whether through crime or carelessness, private and personal information is out for ever, and has a power to do harm which is almost incalculable. In the wake of losses and thefts which have exposed millions of customers to fraud and identity theft, states in America and governments in many other countries are legislating or plan to legislate to compel corporates and other data-holders to report publicly all violations of digital privacy. The impact on reputation for those "named and shamed" may be catastrophic, and the risk to revenues and even to survival will be profound. New threats to privacy are emerging every day, and at the same time, tensions are rising between governments who want to harvest and store data about individual citizens and use it to oversee and steer behavior, and corporates who collect data from and about citizens who are also customers. Already, brands which have been exposed by the media for "stopping" customers or "hacking" behavior have suffered serious blows to their reputations. **Understanding these complex issues and being adequately prepared in case of exposure will be crucial if organizations are to navigate successfully all the trials that digital privacy is posing, and by joining the FIRST Global Computer Security Network conference in Seville, June 17-22, 2007, you will learn:**

- How privacy breaches most commonly occur - and security measures you can take to lessen the risks
- What to do if a privacy breach does occur - guidelines for Incident Response Teams
- How to communicate to stakeholders and the public to minimize damage to reputation and credibility after a privacy breach
- Orwell's "1984" - Past history or present tension? The challenges to individual liberties that are now unfolding as we grapple with big brother around the globe.

*If these are concerns you share, then you should attend the 19th Annual FIRST Conference, "Private Lives and Corporate Risk" in Seville, Spain, June 17-22, 2007. Sponsored by FIRST, this conference brings together security professionals from the global incident response community who are seeking answers to a raft of questions like those above.*

**Who Should Attend?**  
 You do not need to be a member of FIRST to attend the 19th Conference. Any incident response and security team or security professional who has responsibility for representing how an organization responds to digital security incidents should attend. And the conference will also be of interest to:

- **Technical Staff** who determine security policies, measurements and implement solutions
- **Policy and Decision Makers** with overall security responsibilities
- **Law Enforcement Staff** who are involved in investigating cyber crimes
- **Legal Counsels** who work with policy and decision makers in establishing security policies
- **Senior Managers** directly charged with protecting their organizations
- **Government Managers and Senior Executives** who are responsible for protecting Government systems and networks/critical infrastructures.

Past participants at conferences have included IT managers, system and network administrators, software and hardware vendors, security solutions providers, ISPs, telecommunications providers and general computer and network security personnel.

**Conference Location**  
 The 19th Annual FIRST Conference will be held at the **Hotel Melia Sevilla**, Doctor Pedro de Castro, 1, Sevilla 41001, Spain.

A block of rooms is being held for conference attendees at a discount rate of 110.00 €/night/line and 122.50 €/night/line.

These rates will be honored three days before and three days after the official meeting dates, based on availability. To receive the discount rate, you must make your reservation prior to May 15, 2007, and mention that you are attending the **FIRST Computer Security Conference**. Reservation requests received after May 15, will be accepted on a space and rate availability basis. To make your reservation, please contact the hotel prior to May 15, 2007.

**Melia Sevilla Hotel**  
 Phone: +34 95 442 26 11  
 Fax: +34 95 442 16 08

**Join the Global Computer Security Network Today!**  
 The upcoming conference promises to be the best ever: record attendance is expected. So here is one event you don't want to miss: take advantage of early registration and our hotel discounts - **Sign up today!**  
 For more information about FIRST go to [www.first.org](http://www.first.org)  
 For questions about the conference, email: [First2007@first.org](mailto:First2007@first.org)  
 To register for the conference, go to <http://www.first.org/conference/2007>  
 Complete and submit the registration form.

**Sponsorship Opportunities**  
 In an effort to attract registrants at an affordable fee, FIRST Org, Inc., a not-for-profit corporation, solicits conference sponsorships at varying levels. We seek sponsoring organizations that support the mission of FIRST and are committed to improving computer security around the world. Sponsors may receive discount registration fees. For more information visit [www.first.org](http://www.first.org).

**Call for Papers**  
 The FIRST program committee solicits original contributions on network security for refereed paper presentations, tutorials, invited talks, and panel discussions. Past topics have included creating and managing CSIRTs, computer vulnerability, triage/detection, computer forensics, and case studies. Presenters may receive discount registration fees. For more information, visit [www.first.org](http://www.first.org) or write [first2007chair@first.org](mailto:first2007chair@first.org). The deadline for submissions is November 15, 2006.

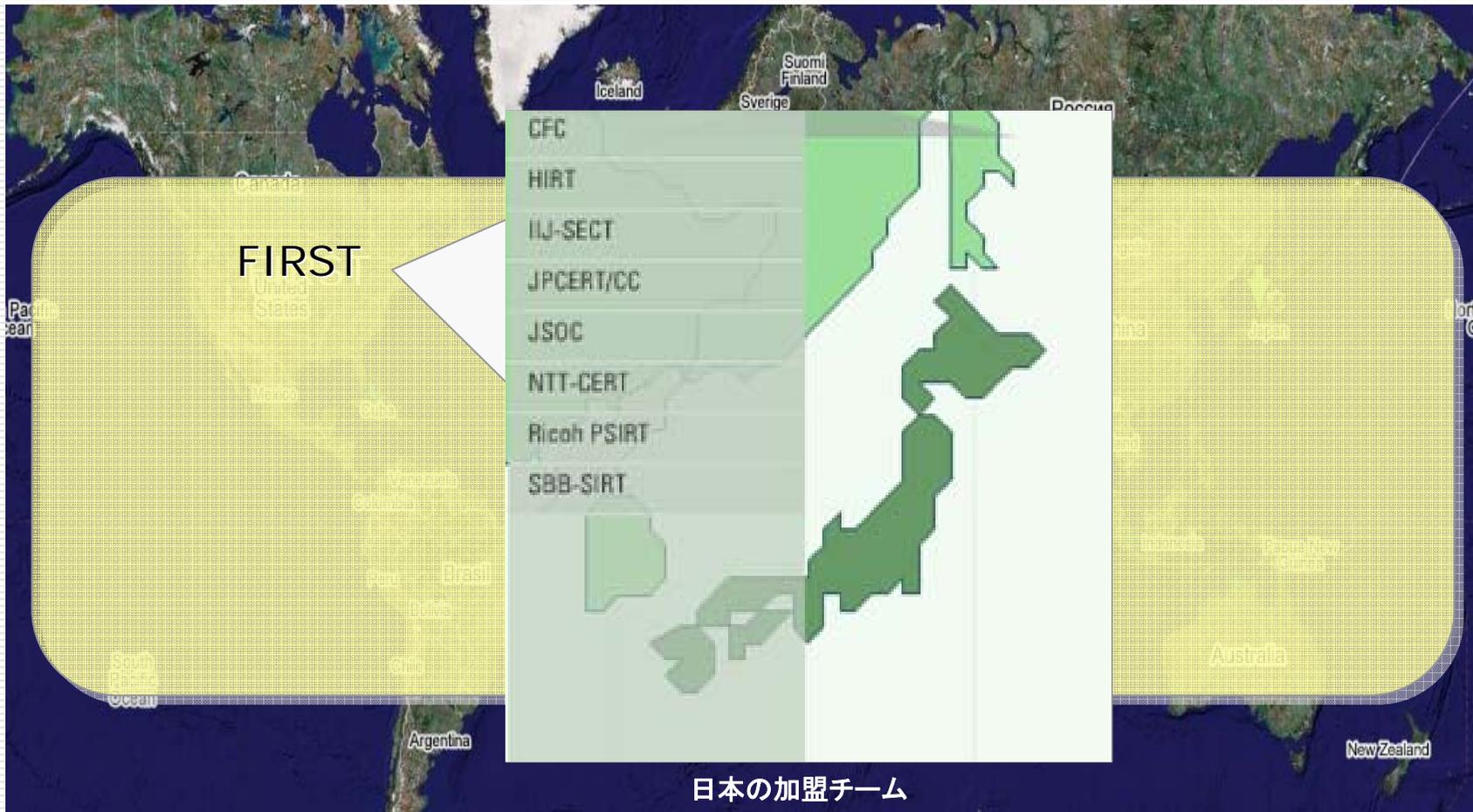
# 1. コミュニティの活発な活動

## □ FIRST



# 1. コミュニティの活発な活動

## □ FIRST



## 2. テクニカルトレーニング

---

### □ 世界中で行われているテクニカルトレーニング

#### ■ 継続的に実施されているトレーニングの例

- 欧州 TERANA の TRANSITS Training
- 米国 CMU の Creating a CSIRT Workshop
- FIRST の Technical Colloquium

#### ■ その他の例

#### □ APEC TEL の 2006 APEC Security Training Course

<http://www.apectel34.org.nz/uploads/Summary%20Report%20of%202006%20APEC%20SECURITY%20TRAINING%20COURSE.pdf>

#### □ G8 の Second Training Conference of the G8 24/7 Computer Crime Network

[http://www.coe.int/t/e/legal\\_affairs/legal\\_co%2Doperation/combating\\_economic\\_crime/3\\_technical\\_cooperation/cyber/G8%2024-7%20agenda%20Rome.pdf](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/3_technical_cooperation/cyber/G8%2024-7%20agenda%20Rome.pdf)

### □ セキュリティ対策に有益な情報のあるサイトの活用

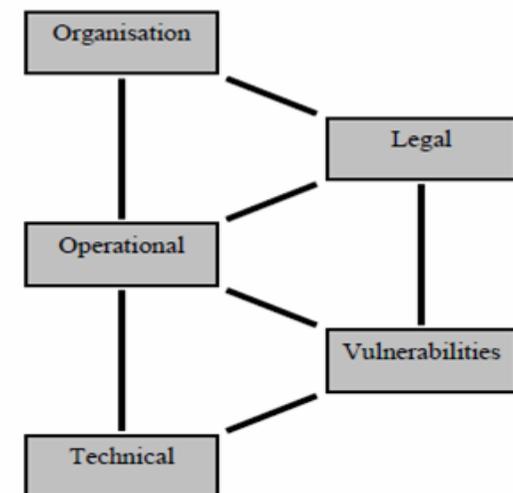
---

## 2. テクニカルトレーニング



### □ 欧州 TERENA の TRANSITS Training

- <http://www.ist-transits.org/>
- CSIRT (Computer Security Incident Response Team) の設立を促進、及び既存の CSIRT の対応能力を向上させることを目的としたヨーロッパのプロジェクト
- 右図の5つのモジュールで構成されたマテリアル
  - 著作権所有者は TERENA
- FIRST メンバであれば、許諾を受けてマテリアルを活用して、ワークショップを開催可能
- これまでのトレーニング開催地の例
  - チェコ(2004年)、フランス(2005年)、ポルトガル(2005年)、ボルチモア(2006年) 韓国(2006年)、ブラジル(2006年)など



TRANSITS Final Report (IST-2001-39118)から引用

## 2. テクニカルトレーニング

### □ 米国 CMU の Creating a CSIRT Workshop

- <http://www.sei.cmu.edu/products/courses/cert/creating-csirt.html>
- CSIRT を構築しなければならない管理者に対する1日コースのトレーニング
- CSIRT 構築の要件定義と計画の作成から、CSIRT の設立に必要なサービスの定義、ポリシー及びプロシージャーなどの立案に役立つ。
- 参加条件は、特にない。
- 費用が、\$1,000 かかる。
- 基本的には米国で開催されるが、米国以外でも開催されることがある。



## 2. テクニカルトレーニング

### □ FIRST Technical Colloquium

- <http://www.first.org/events/>
- インシデントレスポンスチームなどの活動に必要な脆弱性情報、最新のインシデント動向及びツールなどについて情報交流し、Hand-on スタイル(育成型で実践を伴う)で、高度なテクニカルトレーニングを行う。
- 参加者条件は、FIRST メンバであること。
- 参加費用は、基本的にかからない。
- 期間は、基本的に2日間
- これまでの開催地の例
  - オランダ(2006年)、韓国(2006年)、ブラジル(2006年)、ハンガリー(2007年1月)、米国(2007年3月)、カタール(2007年4月)



## 2. テクニカルトレーニング

---

- セキュリティ対策に有益な情報のあるサイトの活用
  - CSIRT Development (CERT/CC)
    - <http://www.cert.org/csirts/>
  - CSIRT Start Kit (TERENA)
    - [www.terena.nl/activities/tf-csirt/starter-kit.html](http://www.terena.nl/activities/tf-csirt/starter-kit.html)
  - Forming an Incident Response Team (AusCERT)
    - <http://www.auscert.org.au/render.html?it=2252>
  - 技術メモ - コンピュータセキュリティインシデントへの対応 (JPCERT/CC)
    - <http://www.jpCERT.or.jp/ed/2002/ed020002.txt>
  - Expectations for Computer Security Incident Response (RFC 2350)
    - <http://www.ietf.org/rfc/rfc2350.txt>

### 3. 対応体制の Dry run(予行演習)

- セキュリティ対策をさまざまな形態で施した後(特に、インシデント対応体制の構築など)、それが以下のポイントでテスト或いは試行している。
  - きちんと機能するかどうか？
  - 関係するルールなどに影響は受けないか？
  - 担当者の習熟度は十分か？
- 予行演習に最適な方法として利用される方法
  - Tabletop Exercise
    - 意思決定者、キーパーソン、インシデントレスポンスを実際にする方が参加
    - ファシリテーター(状況付与兼進行役)の司会によるディスカッション形式
    - シナリオは、実情にあった想定のもの
    - 基本的にはクローズな形で実施し、ディスカッション内容については、公開しない

### 3. 対応体制の Dry run(予行演習)

---

#### □ 海外の状況

- 米国 Cyber Storm (2006.02.06 – 02.10)
  - 米国政府主導による国家レベルの演習で、高度なサイバー攻撃への準備能力を評価する目的で実施。
  - DHS Releases Cyber Storm Public Exercise Report  
[http://www.dhs.gov/xnews/releases/pr\\_1158341221370.shtm](http://www.dhs.gov/xnews/releases/pr_1158341221370.shtm)
- APCERT International Incident Handling Drill (2006.12.19)
  - APCERT 及び APEC TEL 加盟の経済地域から 15 チームが参加し、マルウェアが埋め込まれたサイトを遮断するインシデント対応ドリルを実施
  - JPCERT/CC 報道発表資料  
[http://www.jpcert.or.jp/press/2006/pr\\_1220\\_apcertdrill.pdf](http://www.jpcert.or.jp/press/2006/pr_1220_apcertdrill.pdf)

### 3. 対応体制の Dry run(予行演習)

---

#### □ 国内の状況

- 総務省による「電気通信事業分野におけるサイバー攻撃対応演習」(2007年1月から2月の間に実施)

- 総務省報道資料

- [http://www.soumu.go.jp/s-news/2006/061201\\_4.html](http://www.soumu.go.jp/s-news/2006/061201_4.html)

- 日本政府主導による「重要インフラにおける分野横断的演習」(机上演習)の実施

- 情報セキュリティ政策会議 報道発表資料

- <http://www.nisc.go.jp/conference/seisaku/dai9/pdf/9siryou0302.pdf>

- 関連ニュース記事(2/7 政府、IT障害の机上訓練を実施)

- <http://it.nikkei.co.jp/security/news/index.aspx?n=AT3S07014%2007022007>

---

# セキュリティ対策に必要なテクニック 「アドバイザリー(注意喚起)を出す際の留意点」

## 「アドバイザー(注意喚起)を出す際の留意点」

### □ 誰に対して出すのか？

- 誰のためのものなのかを念頭に入れて、適切な文言を使用すること。
  - システム／ネットワーク管理者に対して？ 一般ユーザーに対して？
- 読者の IT リテラシーなどにばらつきがある場合は、すべての読者が理解できる内容にすること。
  - 難解な言い回しは避ける。
  - 読者にとって馴染みのない専門用語には、注釈をつけるなどの配慮をする。

## 「アドバイザリー(注意喚起)を出す際の留意点」

- どのような内容を含めるべきか？
  - アドバイザリーのステータス
    - 草案版、暫定版、最終版、更新版・・・
  - 脆弱性の対象
    - 基本ソフト、アプリケーション、ファームウェア・・・
  - 被害の種類
    - DoS、不正侵入・・・
  - 脅威の分析
    - 現実に発生中、想定事象・・・
  - 脆弱性或いは不正侵入の検知方法
  - 問題解決方法
    - 運用方法の変更、パッチの適用・・・
  - 修復作業による他の影響

## 「アドバイザリー(注意喚起)を出す際の留意点」

- アドバイザリー配布(公開時)に気をつけるべきことは？
  - 可能な限り、アドバイザリーに署名をつけること。
    - エンドユーザーまでに到達するまでに改ざんされていないことを証明するため。
    - 署名をしたら、必ず検証をする。
  - アドバイザリーに一連番号をつけること。
    - 他のアドバイザリーとの仕分けを容易にできる。
    - ステータス、日時をつける。(国外にも出す／国外から参照される場合は、UTC 表示)
  - アドバイザリーはアーカイブしておくこと。
    - アドバイザリーの更新や削除などの履歴は、読者や発行者にとって有益なことが多い。

# 連絡先

---

## □ JPCERT コーディネーションセンター

- Email: [office@jpcert.or.jp](mailto:office@jpcert.or.jp)
- Tel: 03-3518-4600
- <http://www.jpcert.or.jp/>

## □ インシデント報告

- Email: [info@jpcert.or.jp](mailto:info@jpcert.or.jp)  
PGP Fingerprint : BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
- インシデント報告様式  
<http://www.jpcert.or.jp/form/>