日本シーサート協議会、JPCERT/CC共催
第1回連携ワークショップ
～脆弱性ハンドリングとインシデントハンドリングへの対応～

ワークショップ開催の趣旨説明
～シーサートPoCの重要性～
PoC: Point of Contact

日本コンピュータセキュリティ
インシデント対応チーム協議会
運営委員長　寺田真敏
2015年10月14日

目次

日本シーサート協議会の加盟チーム数も100チームとなりました。加盟チームの増加、各シーサートの機能の差異などから、外部の組織からの脆弱性情報や、インシデント通知等を受けた場合の対応について、各シーサートの対応が異なることが予想されます。多くのシーサートが連携を通して問題解決を図っていくためには、シーサート活動の暗黙知(慣習)、特に、「脆弱性ハンドリング」「インシデントハンドリング」暗黙知(慣習)についての相互理解が重要です。本イベントでは、～脆弱性ハンドリングとインシデントハンドリングへの対応～と題し、シーサート活動の暗黙知(慣習)に対する理解を深める場としたいと考えています。

- 協議会活動にあたっての心構え
- 企業におけるシーサートの役割
- 脆弱性ハンドリングとインシデントハンドリング

1 協議会活動にあたっての心構え

- 日本シーサート協議会では、『協議会の会合、メーリングリスト等』の活動において、チャタムハウスルールを適用しています。

Chatham House Rule

The Chatham House Rule reads as follows:

> *When a meeting, or part thereof, is held under the* **Chatham House Rule**, *participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.*

出典　http://www.chathamhouse.org/about/chatham-house-rule

1 協議会活動にあたっての心構え

- 日本シーサート協議会では、『連絡窓口担当者(PoC: Point of Contact)の役割』を次のように定義しています。

✓ シーサート(含む、日本シーサート協議会)間の連携において、
実効的な調整担当者であること。
  - ➢ チームEmailのメンバに登録されていること。
  - ➢ チームサイトURLの問合せ窓口から確実に連絡が届くこと。

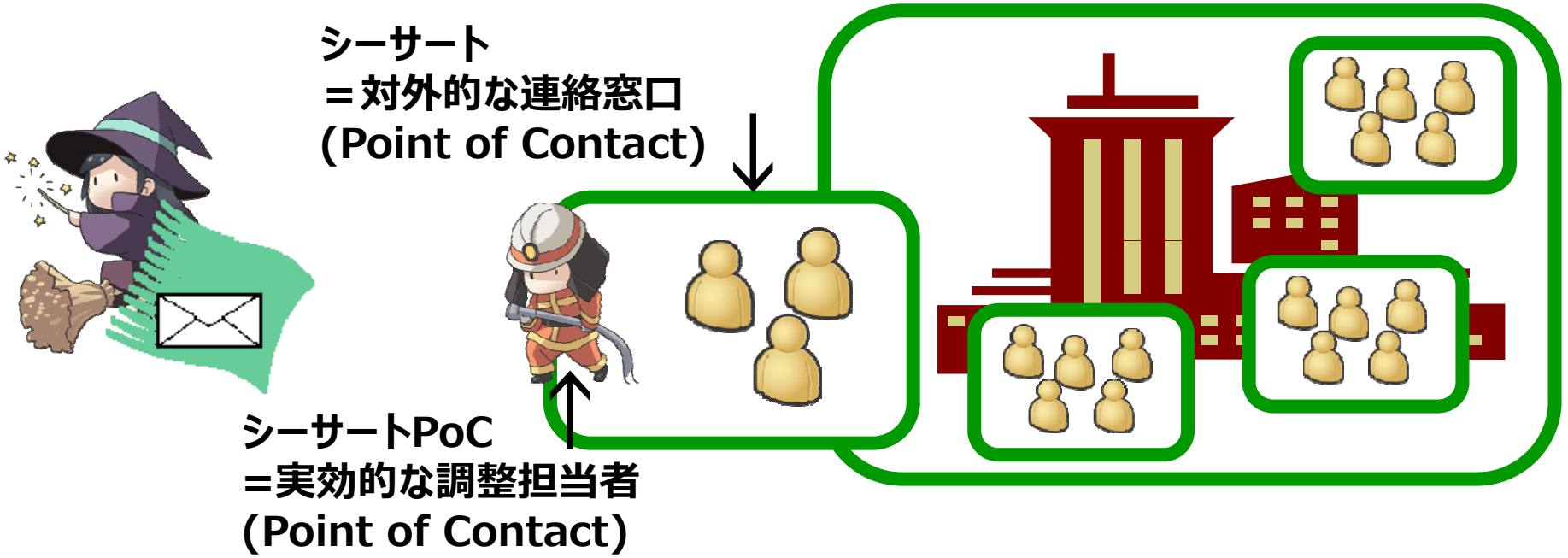
✓ 日本シーサート協議会においては、加盟チームの代表者であること。
  - ➢ 加盟チームの代表者、実効的な調整担当者という立場から、
日本シーサート協議会の総会議決権を行使すること。

2 企業におけるシーサートの役割

- シーサート活動から導かれる企業におけるシーサートの役割
  - 対外的な連絡窓口であること
  - 技術的な問合せに関して対応が可能であること
  - インシデントレスポンス(事後対処)だけではなく、インシデントレスポンスなどの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めていること
  - 部署間を横断した組織体制をとっていること

2 対外的な連絡窓口

- 対外的な連絡窓口が明らかになっていることの利点
  - [通知側] 脆弱性ハンドリングやインシデントハンドリングの通知先を探さずに済む。通知の背景説明を省略できる。通知をたらい回しにされない。
  - [受領側] 通知をトリガに、脆弱性ハンドリングやインシデントハンドリングをベストエフォートで動かし始めることができる。



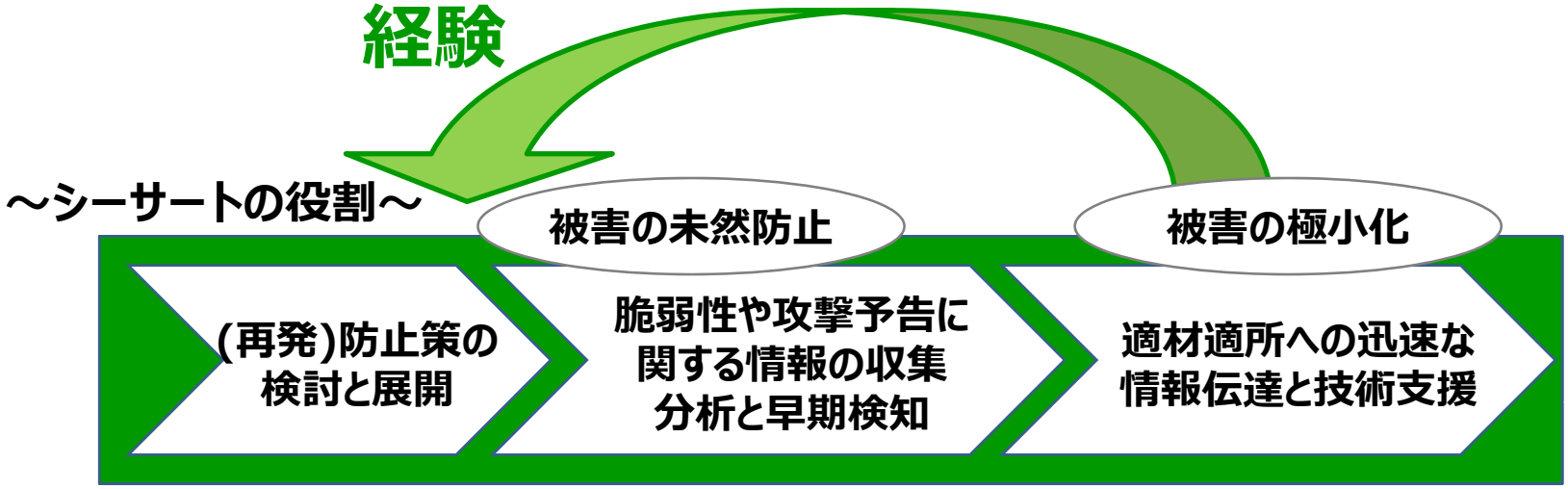
2 技術的な問合せに対応可

- 対外的な連絡窓口が、技術的な問合せに関しても対応可能であることの利点
  - [通知側]脆弱性ハンドリングやインシデントハンドリングの技術的な通知をたらい回しにされない。
- 連絡窓口(シーサート)に期待したい要件
  - 技術的な視点で脅威を推し量り、伝達できること
  - 技術的な調整活動ができること
  - 技術面での対外的な協力ができること

技術的な通知や依頼に対して対処してくれることを
期待しているのであり、必ずしも、シーサート内に技術的な
専門家が必要であるという指摘ではない。

2 インシデントレディネス(事前対処)

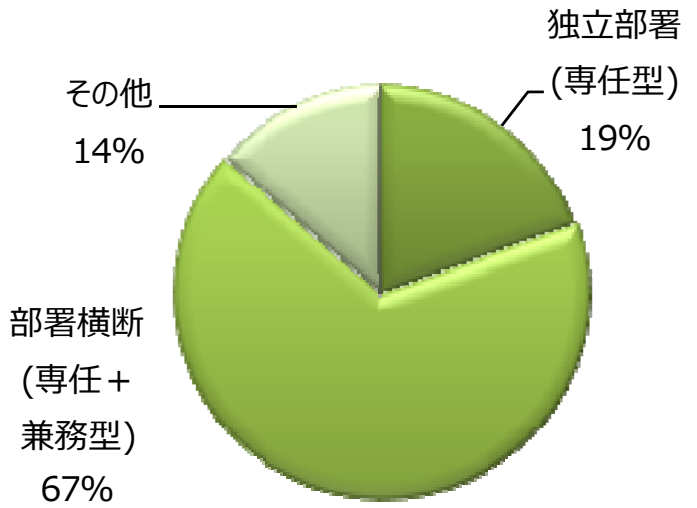
- インシデントレスポンス(事後対処)などの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めることの重要性



- 経験があるからこそ、「問題解決」に向けての想像力も働く。
- 経験ができないならば、他のインシデントレスポンス(事後対処)の疑似体験を通して、「問題解決」に向けての想像力を養う。

2 部署間を横断した組織体制

- シーサート実装の多くは、専任のシーサート要員を抱えた部署を核とした部署横断型
  - 部署間を横断した組織体制の構築、
    すなわち、組織内の横断的な協力体制整備への期待



実装の形態

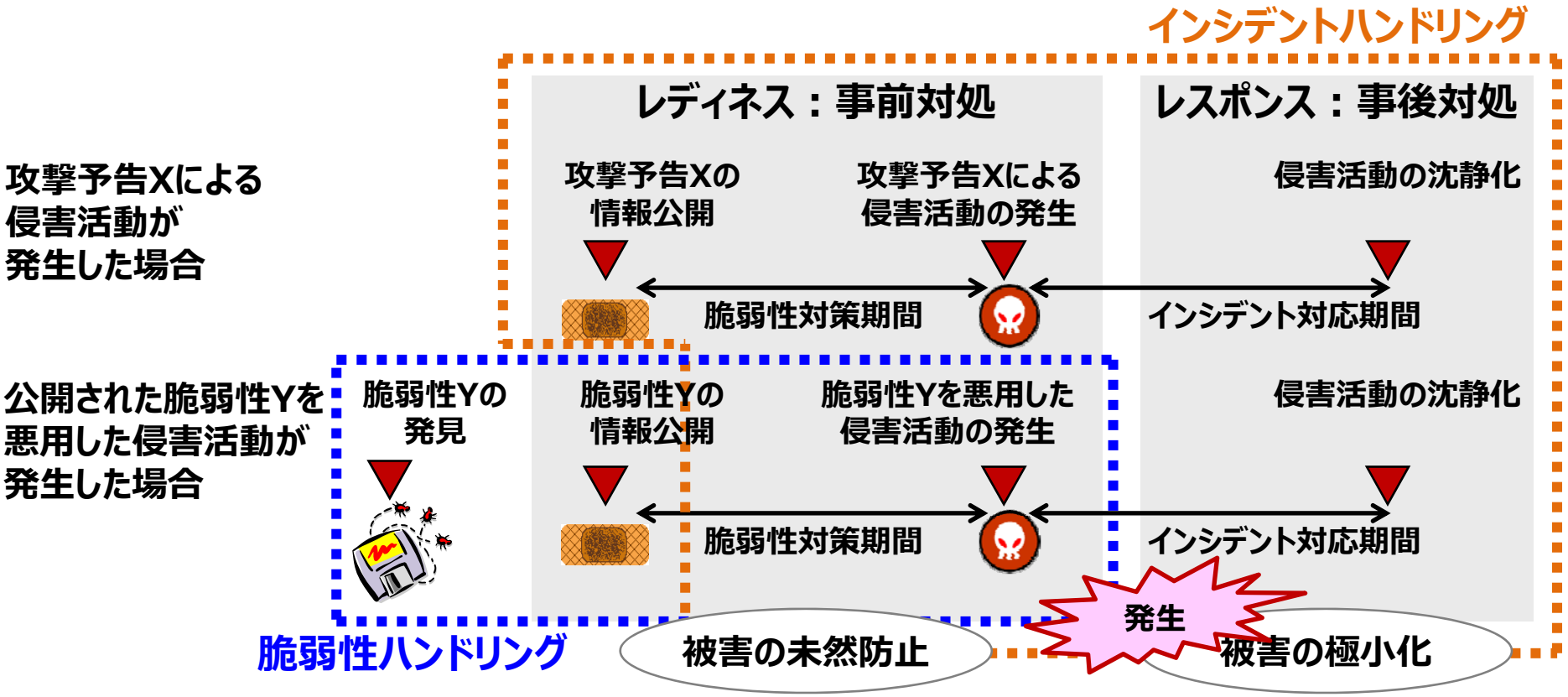
サイバーセキュリティ対策の推進
特定の部署だけが頑張れば良い(お任せ)
モデルから組織全体で頑張る(連帯)モデルへ

シーサートは万能薬ではない。
組織のセキュリティ文化そのもの。

3 脆弱性ハンドリングとインシデントハンドリング

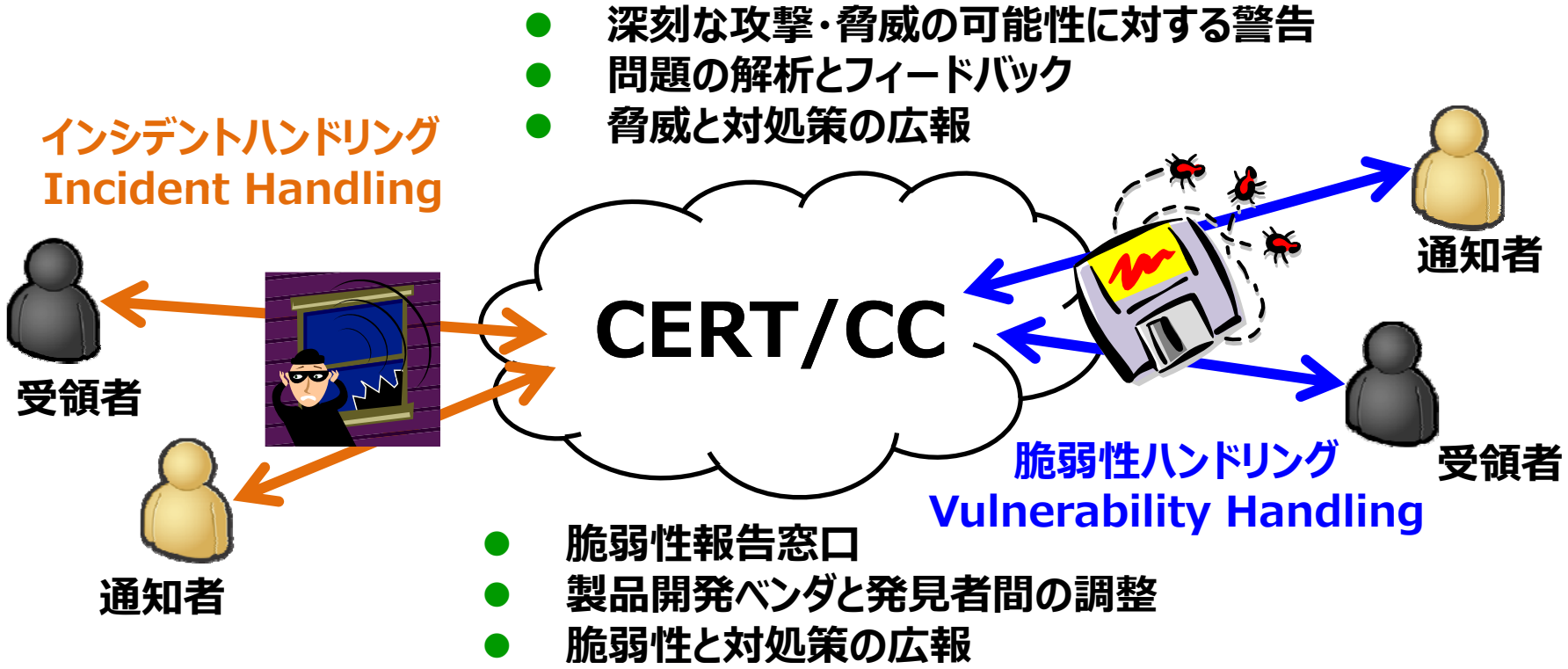
- シーサート連携にあたっては、
  - 自身が該当組織／該当者と直接交渉
  - 調整機関を介して該当組織／該当者と間接交渉

暗黙知(慣習)



3 脆弱性ハンドリングとインシデントハンドリング

- 脆弱性ハンドリングとインシデントハンドリングは、1988年インターネットワーム事件を契機に設立されたCERT/CCの活動がベースとなっている



3 脆弱性ハンドリング

- 通知者⇒(調整機関)⇒受領者
  - 製品／Webサイトの脆弱性を発見したので通知したい

    ⇒ シーサート組織と直接連絡をとる。
    http://www.nca.gr.jp/member/
    ⇒ 情報セキュリティ早期警戒パートナーシップを活用する。
    http://www.ipa.go.jp/security/vuln/report/

3 脆弱性ハンドリング

- **通知者⇒(調整機関)⇒受領者**
  - **届出様式**

ソフトウエア製品脆弱性関連情報届出様式
1. 届出者情報
2. 脆弱性関連情報
   1) この脆弱性関連情報の入手先
   2) 脆弱性を確認したソフトウエア等に関する情報
   3) 脆弱性の種類
   4) 再現手順
   5) 再現の状況
   6) 脆弱性により発生しうる脅威
   7) 回避策
   8) 検証コード
   9) その他
3. 当該ソフトウエアの海外での利用状況について
4. IPA以外の組織への届出について
5. 今後の連絡について
6. その他

ウェブアプリケーション脆弱性関連情報届出様式
1. 届出者情報
2. 脆弱性関連情報
   1) 脆弱性を確認したウェブサイトのURL
   2) 脆弱性の種類
   3) 脆弱性の発見に至った経緯
   4) 脆弱性であると判断した理由
   5) 脆弱性により発生しうる脅威
   6) ウェブサイトの連絡窓口
   7) その他
3. IPA以外の組織への届出について
4. 今後の連絡について
5. その他

3 インシデントハンドリング

- 通知者⇒(調整機関)⇒受領者
  - 製品／Webサイトの脆弱性を発見したので通知したい
  - マルウェアに感染していると思われるパソコンを検知したので通知したい
  - DoS攻撃元になっていると思われるパソコンを検知したので通知したい
  - 不正なサイトに誘導するWebサイトを発見したので通知したい
  - マルウェアを配信しているWebサイトを発見したので通知したい
  - フィッシングメールを受信したので通知したい
  - 攻撃予告サイトを発見したので連絡したい、など

  ⇒ シーサート組織と直接連絡をとる。
  http://www.nca.gr.jp/member/
  ⇒ 調整機関として、JPCERT/CCを活用する。
  https://www.jpcert.or.jp/form/
  https://www.jpcert.or.jp/ics/ics-form.html

3 インシデントハンドリング

- **通知者⇒(調整機関)⇒受領者**
  - **届出様式**

コンピュータセキュリティインシデント報告様式
1. 連絡先
2. この報告の目的
  2-1 JPCERT/CC の対応について
    1: 情報提供、2: 質問
    3: 関係サイトへの連絡を希望、4: その他
  2-2 具体的なご要望
3. 発生したインシデントの概要
  3-1 アクセス元に関する情報
    IP アドレス、ホスト名など:
  3-2 インシデントの内容、発見方法、対処などについて
  3-3 インシデントが発生したシステムについて
    IP アドレス 又は ホスト名:
    プロトコル 又は ポート:
    関連ソフトウェア:
    ハードウェア/OS:
    発生日時:
    タイムゾーン(時間帯):

制御システム・セキュリティ・インシデント報告様式
1. 連絡先
2. この報告の目的
  2-1 JPCERT/CC の対応について
    1: 情報提供、2: 質問
    3: 関係サイトへの連絡を希望、4: その他
  2-2 具体的なご要望
3. インシデントの情報
  3-1 インシデントが発生したシステムに関する情報
    システムの呼称・名称:
    制御対象となる設備・施設:
  3-2 インシデントの内容、状況について
    関連するOS・ソフトウエア・ハードウエア:
    発生日時:
    タイムゾーン(時間帯):
    インシデントの内容、発見方法、対処状況など

ご清聴ありがとうございました。

シーサートPoCの役割は、実効的な調整担当者というだけではありません。いざというときの脆弱性ハンドリングとインシデントハンドリングのためには、日頃から、シーサート活動の暗黙知(慣習)に対する相互理解を深め、普及させておくことが重要です。

シーサート同士の積極的なコミュニケーションを図ることによって、より良いセキュリティ対応を考え、そして、実現していきます。

シーサートに関して： csirt-pr@nca.gr.jp
加盟に関して： nca-sec@nca.gr.jp

http://www.nca.gr.jp/