CSIRT体制

CSIRT体制と効果的なインシデント対応について

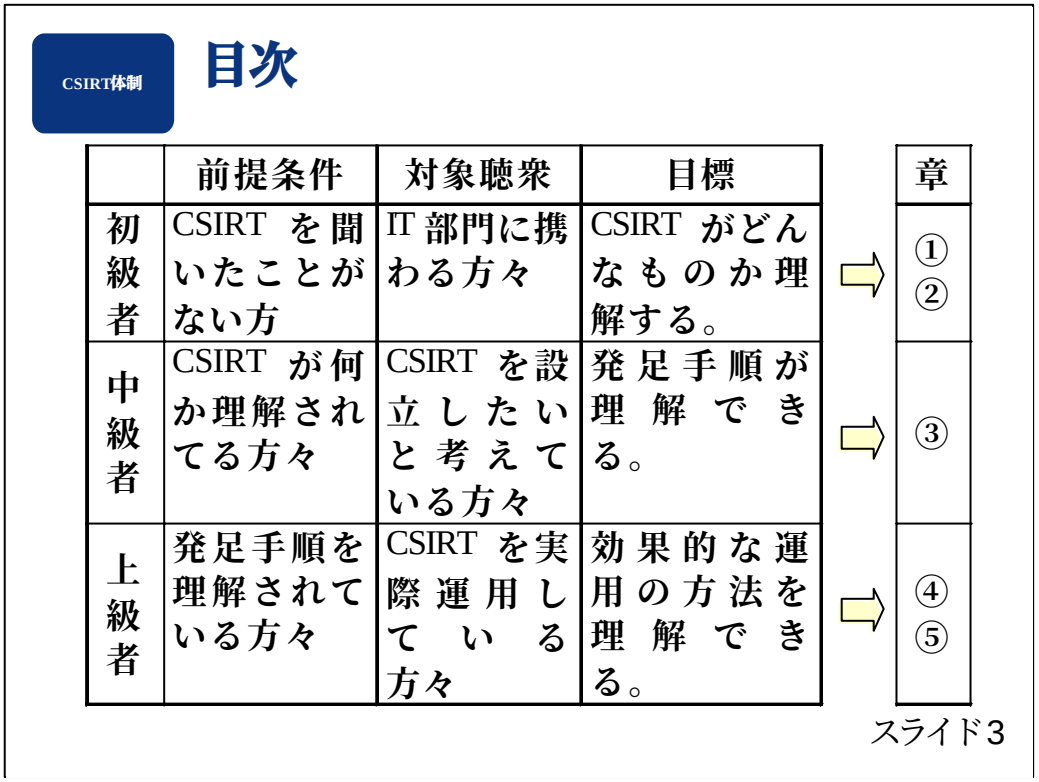
スライド1

CSIRT体制

目次

① インシデント対応の必要性
② インシデント対応のフレームワーク
③ CSIRT発足ガイドライン
④ 各サイトにおける効果的なインシデント対応
⑤ 関係者間の連絡体制
⑥ 関係サイトとの情報交換
⑦ まとめ

スライド2



●このプレゼンテーションは大きく分けて3つのパートから構成されています。

①②章では、CSIRT とは何か、どういう役割があるのか、何をするところなのか
についてご説明いたします。

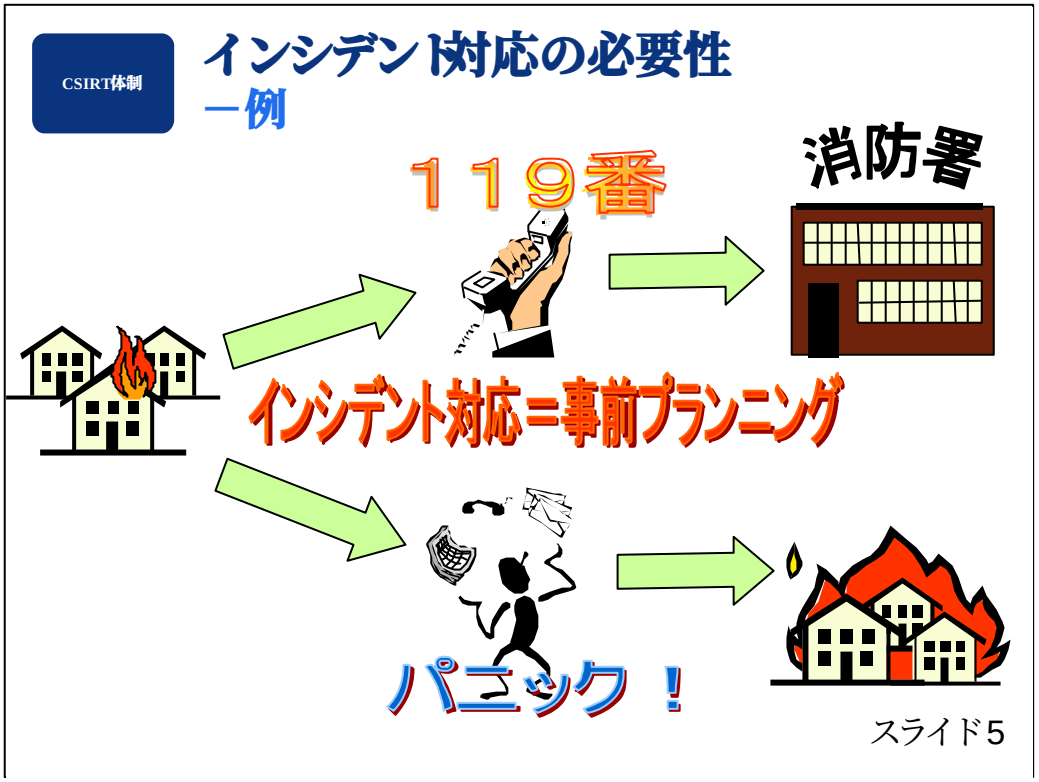
③章ではCSIRT を実際発足する立場の方々のためのガイドラインをご説明いたします。

④⑤章では、CSIRT を運用するにあたっての効果的な運用方法をご説明いたします。

CSIRT体制

①インシデント対応の必要性

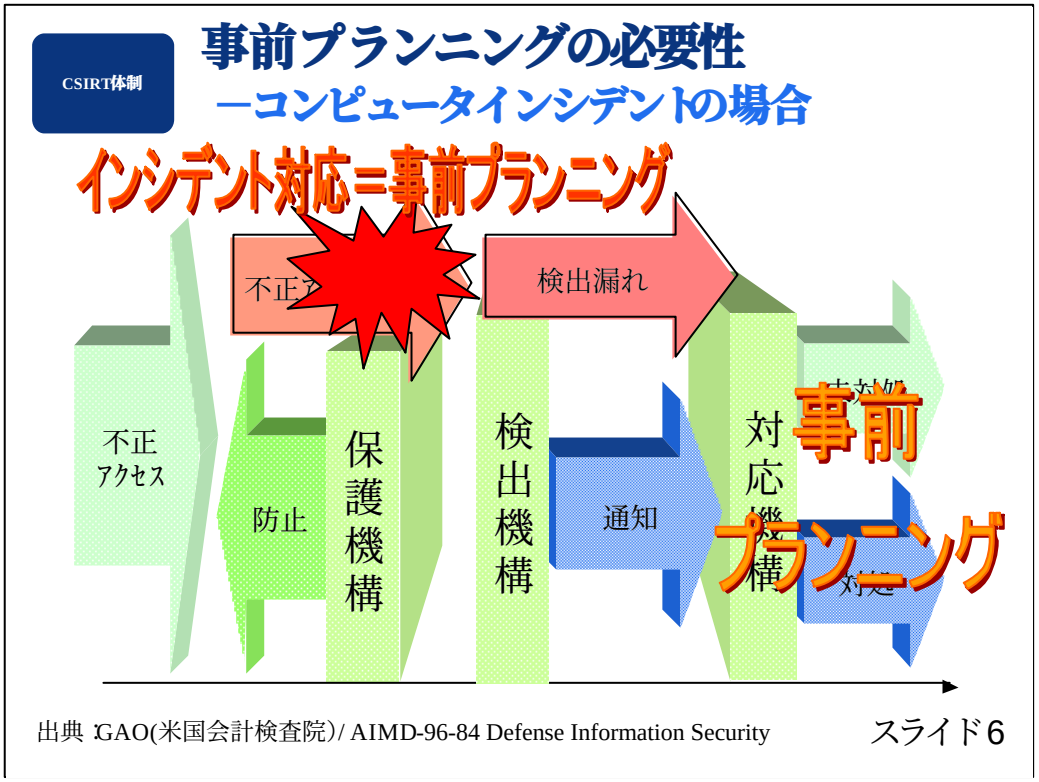
スライド4



●まず始めに、事前プランニングの重要性についてお分かりいただけるよう、身近な例を用いてご説明いたします。

●火事が起きたら、皆様はどう対応しますか？火事の緊急連絡先は皆様ご存知のとおり、119番です。119番に電話すれば消防署に連絡が行くことを私たちは承知しています。しかし、もし、その連絡先が分からなかった場合、もしくは知らなかった場合、私たちはパニックに陥ってしまいます。また何か事件が起きてからその連絡先を調べていたのでは遅すぎます。このような緊急連絡先はあらかじめ知っておく必要があり、またすぐに参照できる所に保存しておくことが重要です。

●CISRTはよく消防署に例えられます。消防署には、火事疑惑もしくは発生した場合のための緊急連絡先が用意されています。（119番に電話をすれば、消防署に連絡できることを皆知っています。）それと同じように、CSIRTもコンピュータセキュリティインシデント疑惑もしくは発生した場合の電話番号や電子メールアドレスなどの緊急連絡先を持っています。この連絡先はあらかじめ知っておく必要があります。火事が起きてから消防署の電話番号を調べていては、遅すぎます。同じように、CSIRTの連絡先も侵害が起こる前に用意しておく必要があります。消防署とCSIRTの類似点は他にもあります。緊急に対応することは彼らの提供するサービスの一部です。同じぐらい大切なことは、まず第一に緊急事態が起きないよう防ぐことです。そのために、消防署は火事に対する安全指導を提供しています。同様にCSIRTでも技術的情報を提供したり、教育やトレーニングを実施しています。



●出典：GAO(米国会計検査院)/ AIMD-96-84 Defense Information Security

●それでは、なぜCSIRT（Computer Security Incident Response Team：コンピュータ・セキュリテイ・インシデント・レスポンス・チーム）が必要かについてお話しします。

●現在、インターネットの発達と普及に比例するように、コンピュータ・セキュリティ・インシデントの数も増えてきました。今まではローカルな問題に留まっていたかもしれませんが、インシデントの範囲も世界にまで発展するようになってしまいました。このような状態になると、とても1サイトでは対応しきれなくなり、複数のサイトを巻き込んでしまうケースも多いです。これらのインシデントに適切かつ迅速に対応するためにCSIRTが設立されました。

●しかし、CSIRTの存在理由が明確になっていない場合、財源や管理に対するサポートに欠け、チームの停止につながってしまいます。もし、サービス対象がそのチームを必要としなかったら、その効果は最小限に留められてしまいます。従って、CSIRTはコンピュータセキュリティに関するなにか問題が起こる前に、用意されているべきで、また人々に認識されるよう公表されているべきなのです。

CSIRT体制

インシデント対応のフレームワーク
ー用語の定義

- CSIRTとは？
- サイトとは？
- POC（Point Of Contact :連絡窓口）とは？

スライド7

●CSIRT（Computer Security Incident Response Team)とは？

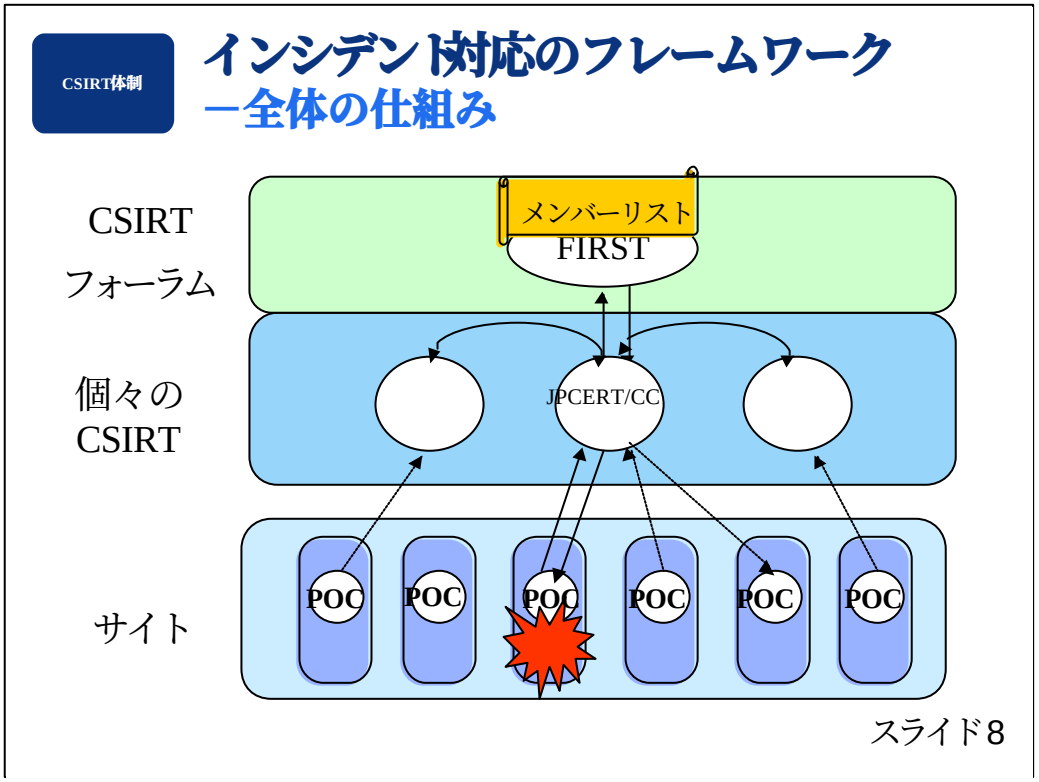
定められた範囲内のサイトに関するセキュリティインシデントについて、
基本的なサービス（トリアージ、インシデント、要求）を用意する事により、
チームはコンピュータセキュリティインシデントに対応するための定義された
サポートを提供します。これらのサービスを提供するのが、CSIRT
（Computer Security Response Incident Team)です。コンピュータセキュリティ
の分野において、CSIRTをしばしば単にIRTと呼ぶこともあります。

●Site（サイト）とは？

コンピュータやネットワーク関連資源を持つあらゆる組織体を意味します。
地理的な位置、組織体の管轄、またはネットワークアドレスの単位で
グループ化されたコンピュータシステムに適用されます。サイトは、典型的には、
共通の管理下にあるネットワークのことをいいます。

● POC（Point of Contact:連絡窓口）とは？

セキュリティ侵害もしくは問題に備えて、多くの組織体では人々に警告したり、
適切な対応をとることができるPOC（連絡窓口）を設けています。この窓口
が明確でないと、侵害が起きた際にどこに連絡してよいのか分からず、
外部へ重要機密が漏れてしまう危険性もあります。ゆえに、適切なPOCを
持ち、適切な人材によって運用されることが重要です。



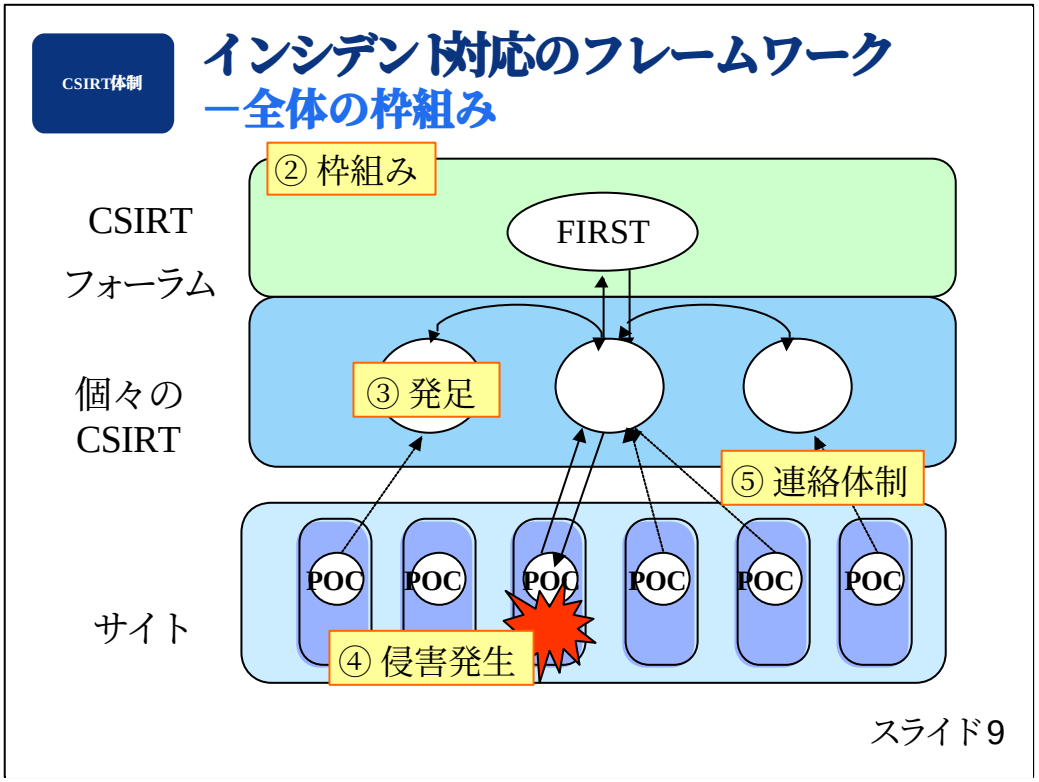
ここでは、インシデント対応のフレームワークの仕組みについて説明致します。

①あるサイトで侵害が発生しました。インシデントの対応方法はそのサイトの定めた対応手順によって異なります。
自分のところだけで処理してしまうサイトもあれば、CSIRTに連絡し、ほかのサイトへの影響を防ぐための対処をするサイトもあります。 図では、日本に存在するCSIRTの具体例として、JPCERT/CCを書いてあります。）

②例えば、国内での対応の場合、侵害を受けたサイトはPOC(連絡窓口)を介し、CSIRTに連絡し、CSIRTはそのサイトに対し侵害に関する情報（他のサイトからも同じようなインシデントの報告を受けているや、その侵害に対する対応策を）伝えます。もし、ほかの関連サイトへの連絡が必要と考えられた場合、インシデント防止また対応のためにCSIRTが対応策または防止策を必要サイトのPOCに連絡します。

③もし、このインシデントが海外にも関連している場合は、CSIRTはFIRSTのメンバーリストを参照し、このインシデントに関わりのある他のCSIRTを割り出します。この際、メンバーのMLにこのインシデントに対する情報を投げ、それに関係のある（自分のサービス対象内でも同じようなインシデントが起きている）他のCSIRTは最初にメールを出してきたCSIRTにその旨を伝えます。そして、その関係するメンバーで協力しあい、情報を交換するなどして、早急の対応をします。

④そして、そのCSIRTが各々の連絡が必要なサイトに対し、インシデントの発生と対応策を伝えます。



●2章ではインシデント対応の枠組みについて説明いたします。全体の仕組みから始まり、CSIRT フォーラムの存在目的、そしてこのインシデント対応のフレームワークができあがった背景についてお話し致します。

●3章では実際CSIRT を発足するにあたって、新しく設立するCSIRT のフレームワークにおいて何を含めたらよいかをご説明いたします。

●4章では各サイトでインシデントが発生した時の対応をどのように事前に用意しておけばよいかご説明いたします。

●5章では関係者間の連絡体制の必要性とその関係者間でどのように連絡が行われるかをご説明いたします。

CSIRT体制

②インシデント対応のフレームワーク

スライド10

CSIRT体制

インシデント対応のフレームワーク
－CSIRTフォーラムの目的

- CSIRT間でコミュニケートする際に起こる言語、時差、国際基準や協定に関する問題を取り除く。
- コンピュータセキュリティインシデントの効率的な防止、探知、復旧におけるIT構成員の協力を促す。
- 起こりうる危険や持ちあがった事件状況の警戒と忠告情報をコミュニケートできる手段を提供する。
- 研究や運用活動を含む、CSIRTフォーラムメンバーの行動や活動を促進する。
- セキュリティ関連の情報、ツール、技術を共有することを促進する。

スライド11

●インターネットの普及により、広範囲に（世界中に）影響を及ぼすインシデントに対応、解決する際に、他のCSIRTと連絡を取り合って、協力を必要とするケースが増えてきています。

●このような複数のCSIRTをまとめる機関（CSIRTフォーラム）があることで、次のようなことが実現できます。

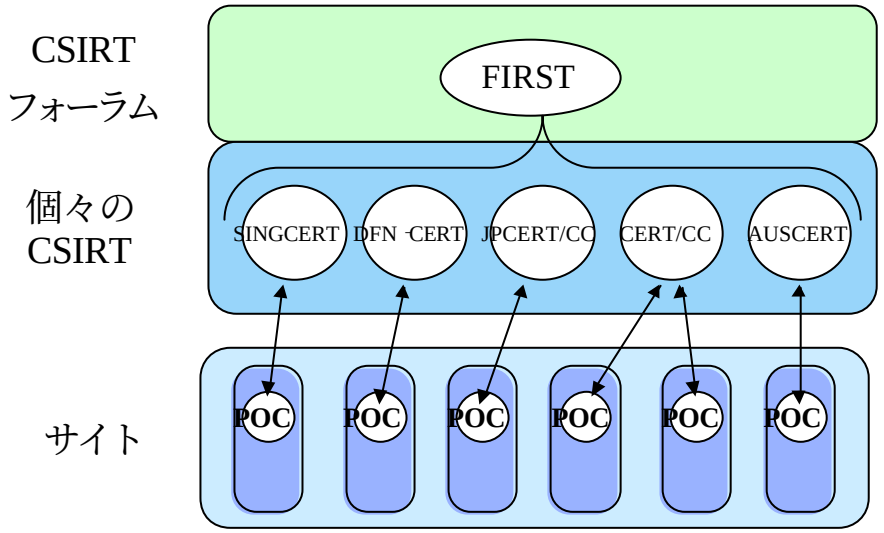
・言語、時差、国際基準や協定に関わる問題を解決します。
・侵害が起きた際にIT構成員の協力を得、効率的にまた迅速に対応できるようにします。
・もし、侵害が起こった際に各CSIRT、各サイトに効率よく、適確にコミュニケートできるような手段、構成が提供されます。
・将来的な侵害を防ぐために、研究や運用活動を促進します。
・情報、ツール、技術を共有することにより、迅速な対応ができ、侵害を適切に対処できます。

●またCSIRTフォーラム（FIRST）の意義として次のことがあげられます。

・公正な審議の上でメンバーが決定されるので、メンバーは信頼できます。
・お互いよい関係を築くことで、協力し合え、情報の交換が信頼関係の上で行えます。

CSIRT体制

インシデント対応のフレームワーク
―世界規模のCSIRT体制

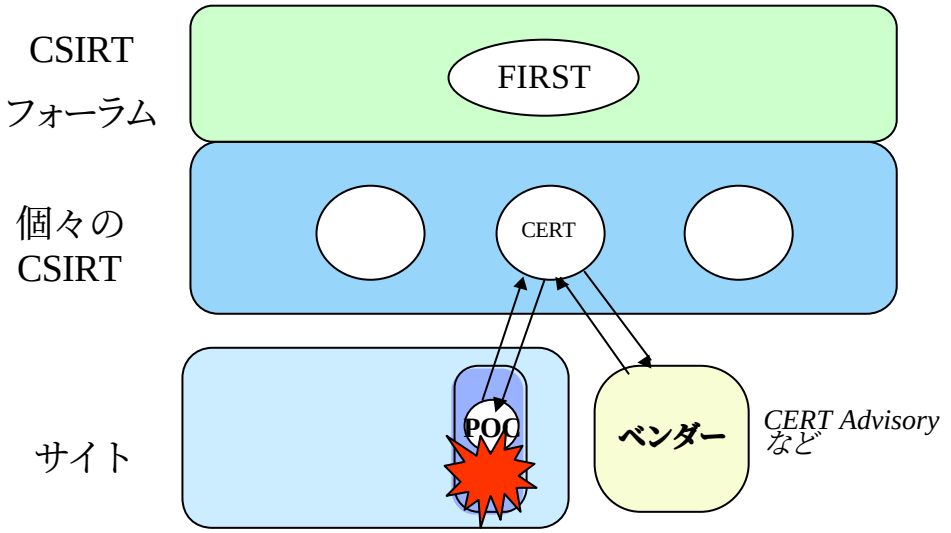


スライド12

●世界規模のCSIRT体制が出来あがったのには、次のような背景があります。
●1980年後半、ARPANET という新しいコンピュータネットワーク施設が世界にまたがって活動するようになり、このネットワークが発達し、改善されるにつれて、たくさんのサイトが利用するようになりました。
●しかし、1988年11月に“Internet Worm”というコンピュータセキュリティインシデントが発生しました。ARPANETはこのインシデントによって多大な被害をこうむりました。また、この事件への対応は孤立していて、調整のとれていないものでした。
●その結果、重複する調査や研究などで、非効率的だったため、コンピュータインシデントへの対応を取りまとめ、情報の共有を取りまとめるセンターが必要という結論に達し、CSIRT（Computer Security Incident Response Team)を結成しました。
（例として、JPCERT/CCやCERT/CCが挙げられます。）
●このCSIRTチームが世界各国で結成され、インシデント解決のためや情報交換のためにコミュニケーションをとる際、言語、時差、国際基準や協定に関する問題に直面しました。その問題を解決するために、CSIRTフォーラムが結成されました。
（例として、アメリカのFIRSTなど)
●CSIRTフォーラムはコンピュータセキュリティ問題とその回避策を扱うために個々のCSIRTの自発的な共同作業のネットワークから成っています。
●CSIRTフォーラムは、参加組織がインシデント情報を共有情報の開示に関する契約を元に、情報を交換し、共通の問題を解決し、将来に向けての戦略をたてるフォーラムの場を提供します。

CSIRT体制

インシデント対応のフレームワーク
ーベンダーとの連携



スライド13

●ここでは、ベンダーとの連携について説明致します。

●CERTは必要な場合、ベンダーに連絡します。連絡を必要とする場合というのは、あるサイトでインシデントが発生し、それがベンダーの製品に関係のありそうな場合、CERTが各ベンダーに連絡し、そのベンダーの製品に脆弱性があるかどうかを確認します。もし、そのベンダーが自社の製品に脆弱性があると考えた場合CERTに連絡し、CERTがCERT Advisoryによって、他の一般の人々に伝えます。

●ベンダーはFIRSTのメンバーでなくてもよいが、FIRSTのメンバーになれます。メンバーであったほうが、CSIRTが連絡する際に簡単になり、また信頼性も高まります。

CSIRT体制

③CSIRT発足ガイドライン

スライド14

CSIRT体制

CSIRT発足ガイドライン

- 新しくCSIRTを設立するために必要なフレームワーク
  - 何を……ミッションステートメント
  - 誰に対して……サービス対象(Constituency)との関係
  - 位置付け……組織内の位置付け
  - 誰と……外部との関係

スライド15

●CSIRTのフレームワークは個々のCSIRTによって異なります。既存のCSIRTのフレームワークを使って新しいCSIRTを設立しようとしても、自らのニーズや目的に当てはまりません。各チームはそれぞれ固有の基準と運用ガイドラインを定義する必要があります。新しくCSIRTを設立する際、明確にしなくてはならない点がいくつかあります。

●何を：
まず、CSIRTを設立するためのミッションステートメント。ここにおいて、何をなんのためにするのかというCSIRTの全般的なゴールと目的の明確化させます。

●誰に対して：
次に、誰に対してサービスを提供するのか、どのようなサービス対象から成っているのかを定義し、どのようにしたら信頼を獲得できるかについて定義します。一般的な英単語としては、Constituencyは「構成要員」として訳されていますが、ここではCSIRTがサービスを提供する「サービス対象」として使われます。（constituency=supported customer-base)

●位置付け：
また、CSIRTを設立するにあたって、組織内においてどのような位置付けにあるのかを定義する必要があります。

●誰と：
最後に外部との関係を整理し、定義する必要があります。他のCSIRTや機関との関係をどう持つのかを明確化することが大切です。

CSIRT体制

CSIRT発足ガイドライン
ー何を

- ミッションステートメント
  - 明確かつ簡潔なものを作成する。
  - チーム目標を明確にする。
  - 全般的なゴールと目標へのフォーカスを提供する。

スライド16

●既存のCSIRTの多くは、彼らのゴールや目標の明確な理解が欠けているか、相互作用する主体にその情報を効果的にコミュニケートできていません。

●ミッションステートメント：
ミッションステートメント（使命の表明）は、提供されるサービスの性質や範囲、ポリシーと手続きの定義、サービスの品質を含む、サービスと品質のフレームワークを設立するのに絶対的です。

●ステートメントを作る際に気をつけなくてはならない事は、ステートメントは明確かつ簡潔な表現で、数行程度にまとめるのが望ましいといえます。

●ステートメントはチームが何を達成しようとしているのかの基礎的な理解を提供し、さらに重要なことには、CSIRTの全般的なゴールと目的を集中させることです。

●サービス対象の定義とこのサービスと品質のフレームワークを合わせると、全てのCSIRTの活動を促し、その活動範囲を決定します。

CSIRT体制

CSIRT発足ガイドライン
―誰に対して

- サービス対象について
  - サービス対象の定義
  - サービス対象との関係
  - CSIRTをサービス対象へ促進
  - サービス対象の信頼獲得

スライド17

●運用の過程において、どのCSIRTも広い範囲の主体と相互作用します。CSIRTがサービスを提供する特定のコミュニティの中で最も重要なのは、彼らのサービス対象です。

●サービス対象：
サービス対象とは、CSIRTによるサービスを受けている特定のユーザ、サイト、ネットワークや組織のことを指します。CSIRTは効果的にそのサービスを提供できるように、サービス対象によって認識されるよう努めなくてはなりません。

●CSIRTがやるべき必須の仕事の1つは、彼らのサービス対象を定義し、両者の関係をそのサービス対象に定義し、それからCSIRTをそのサービス対象に促進し、“仕事をきちんとする（doing the job right）”ことによって信頼を得ることです。

CSIRT体制

CSIRT発足ガイドライン
―サービス対象

CSIRT Type	*Nature of Mission*	*Type of Constituency Served*
International Coordination Center	・他の CSIRT と協力することから、グローバルの観点からみたコンピュータセキュリティの脅威に対する知識基礎を獲得する。 ・CSIRT 間での“相互的な信用関係（Web of Trust）”を作り出す。	世界各国の CSIRT
Corporation	組織の情報基盤のセキュリティを向上させ、侵害によるダメージの脅威を最小限に留める。	システム管理者およびネットワーク管理者と組織内のシステムユーザ
Technical	与えられた IT 製品のセキュリティを向上させる。	製品のユーザ

出典: Handbook for Computer Security Incident Response Teams/ Software Engineering Institute

スライド18

●この表は違うタイプのCSIRTがどのように異なったミッションを遂行し、異なったサービス対象にサービスを提供するかを示します。

●CSIRT のタイプ別にそれぞれ説明致します。まず、一番大きいのが国際的な規模のCSIRTフォーラム。CSIRT フォーラムは各国を代表するCSIRT（CERT、JPCERTなど）を対象にサービスを提供しています。コンピュータセキュリティインシデントの範囲がグローバルになっている今、世界各国のCSIRTが協力することにより、“相互的な信用関係（Web of Trust）”を作り出し、情報、知識の共有をはかり、インシデントの早期発見、解決、また予防を促進します。

●次に、組織レベルのCSIRTがあります。組織レベルのCSIRTはその組織のシステム管理者およびネットワーク管理者と組織内のユーザにサービスを提供します。組織の情報基盤のセキュリティを向上させることによって、侵害による組織へのダメージを最小限に押さえれるよう、働きかけます。

●最後に、技術レベルのCSIRTとして、製品のユーザに対して、サービスを提供します。IT製品のセキュリティを向上させることによって、外からの侵害を防ぎます。

CSIRT体制

CSIRT発足ガイドライン
ー位置付け

- 組織内の位置付け
  - 組織内における位置
  - CSIRTの役割
  - 各グループの相互関係

スライド19

●組織内の位置付け：
CISRTの基礎的なフレームワークのなかで、チームが何を目標としているか（ミッションステートメント）、誰のために（サービス対象）を定めるだけでなく、CSIRTの“根本（Roots）”である親組織における位置を厳密に定義する必要があります。

●CSIRTの親組織における位置はその定義したミッションに深く連結していて、そのサービス対象にも少し関係してきます。

●運用ガイドラインを確立し始める前に、その組織的な環境およびサービス対象の情況下での、全面的なリスク管理の中におけるCSIRTの役割を決定することが重要です。また、その役割について、経営陣（マネージメント）によってサポートされていることと、関係する主体全てによって理解されていることは絶対的です。

●危機（リスク）管理におけるそれぞれの役割に関係なく、各グループは自分たちの責任がどのような相互関係をもっているのか、また、孤立してしまわないように、他のグループとどのようにして協調しあうのかを理解しなくてはなりません。

CSIRT体制

CSIRT発足ガイドライン
―誰と

- 外部との関係
  - **他のCSIRTとの関係**
  - **CSIRT間における階層構造**
  - 法執行機関（警察など）
  - 報道機関

スライド20

●外部との関係として考えられるのが、4つあります。他のCSIRTとの関係、CSIRT間における階層構造、法執行機関との関係、そして報道機関との関係です。

●他のCISRTとの関係：
CSIRTの活動範囲はインターネットであり、ゆえに世界です。CSIRTがサービスを提供しているたくさんのサービス対象が世界各国に散らばっており、またどんどんと増加しています。従って、各CSIRTが相互作用して問題を解決していかなければ成りません。この協調し調和しあうことが、CSIRTの枠組みの中心になります。

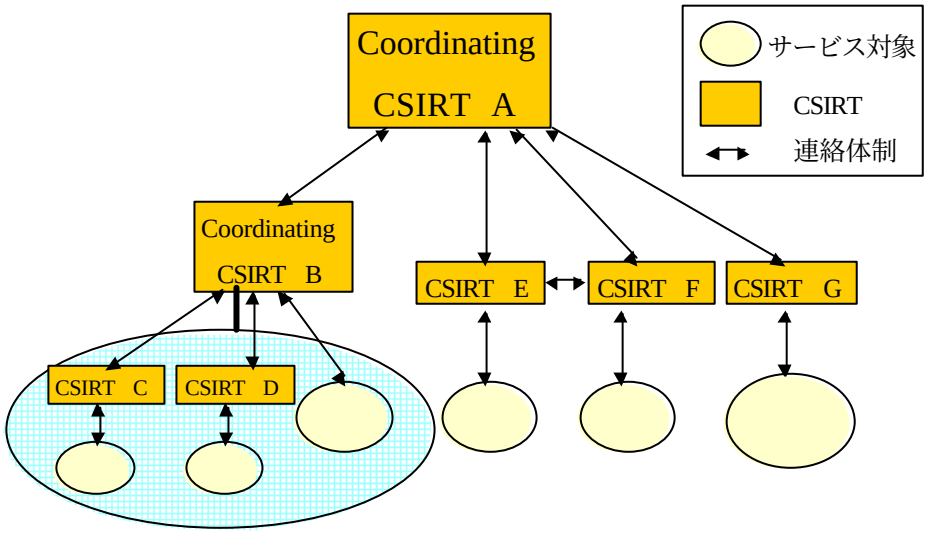
●CSIRT間において階層構造がみられるところもあります。あるチームははっきりとしたサービス対象にサービスを提供するところもあれば、CSIRTのグループをまとめる役割の上で、サービスを提供するチームもあります。

●形式的な階層構造を持ったCSIRTも存在します。例として、USミリタリーにおいて、米陸軍、空軍そして海軍はそれぞれのサービス対象にサービスを提供し、米国防総省がさまざまなUSミリタリーチームのチーム調和の手助けを行います。

●しかしながら、この構造は確実な階層ではなく、たいていの場合、形式ばっていなく、任意のものです。この形式ばらない構造は、信用できる他のCSIRTとの情報共有をすばやく、かつ効果的にでき、その他のチームとはもう少し注意を払いながら、情報のやり取りを行える、という柔軟性が利点とされています。

CSIRT体制

CSIRT発足ガイドライン
－CSIRTとサービス対象の関係図



スライド21

●いくつかの活動において、多くのチームは直接関係のあるチームと連絡を取りあって、Coordinating CSIRTには連絡をする必要がないと判断してしまうチームもあります。しかし、Coordinating CSIRTは自分のドメインにおける全てのレベルの活動についての全般的な概要をつかむため、また、他のチームに関連した活動があるかについて警告を発するために、全ての活動の連絡を受けることを要求します。

●CSIRT間において、可能なピアの関係はたくさんあります。

●他のCSIRTをまとめる役割を担っているチームはCoordinating CSIRTと考えられます。
→例えば、この図において、CSIRT AとBを両方ともCoordinating CISRTとしています。
→CSIRT BはCSIRT CとDをまとめている他に、別のサービス対象に直接
サービスを提供しています。
→反対にCSIRT Aは他のCSIRTからなるサービス対象しかいません。
しかし、CSIRT EとFが直接コミュニケーションを取り合っているので、CSIRT Aの下にあるCSIRTは階層ではなくなります。

CSIRT体制

CSIRT発足ガイドライン
ー誰と(続き)

- 外部との関係
  - 他のCSIRTとの関係
  - CSIRT間における階層構造
  - **法執行機関（警察など）**
  - **報道機関**

スライド22

●次に残りの二つの関係についてご説明致します。
●法執行機関：
法執行機関は警察や他の捜査機関（アメリカのFBIなど）を意味します。CSIRTとそのサービス対象たちは位置するローカルの法律や規制に対し、敏感である必要があります。この法律は国や地域によって異なります。しかし、不正アクセス禁止法違反等の犯罪の可能性がある場合は、それを法執行機関（警察や関係機関）に報告するかどうかを検討します。また同様に法執行機関より、情報の提供を求められた場合に協力する範囲や条件をCSIRTのポリシーに定めておくことが望ましいです。

●日本における不正アクセス行為の禁止等に関する法律
公布：平成11年8月13日号外法律第128号（総理・法務・通商産業・郵政大臣署名）
施行：平成12年2月13日
最終改正：平成11年12月22日号外法律第160号
施行：平成13年1月6日

●報道機関：
報道機関を通して社会にコンピュータセキュリティインシデントについて伝えることは有効です。しかし、その際、いつ、誰に、どれだけの情報を公表するかを考えることが重要です。気をつけなくてはならないのは、報道機関に注意を払ってばかりで、インシデントの処理を後回しにしないことです。いつでも無事にインシデントを解決することが第一であることを忘れないで下さい。

CSIRT体制

④各サイトにおける効果的なインシデント対応

スライド23

CSIRT体制

各サイトにおける効果的なインシデント対応

1. 侵害対応のポリシーと手続きの確立
2. 侵害対応の準備
3. 侵害情報の分析
4. 侵害について認識する必要のある当事者への伝達
5. 侵害関連情報の収集と保護
6. 侵害を隔離(contain)するための短期的な処置
7. 侵害者からのアクセス手段の根絶(eliminate)
8. システムの通常運用への復帰
9. 教訓の認識と実装

スライド24

●すなわち、これらの項目は：

1. 侵害に対応するためのポリシーと手続きを確立する。
2. 侵害に対応する準備をする。
3. 侵害を特徴付けるため、入手可能なすべての情報を分析する。
4. 侵害とその拡大を認識しておく必要のある当事者とコミュニケートする。
5. 侵害に関連する情報を集め、保護する。
6. 侵害を隔離するために短期的解決策を適用する。
7. 侵害者のアクセス手段を根絶する。
8. システムを通常の運用に復帰する。
9. 学んだセキュリティの教訓を識別し、実装する。

CSIRT体制

⑤関係者間の連絡体制

スライド25

CSIRT体制

関係者間の連絡体制
―連絡体制の必要性

- インシデントが発生した際の連絡体制

- 関係者間の連絡体制の必要性

スライド26

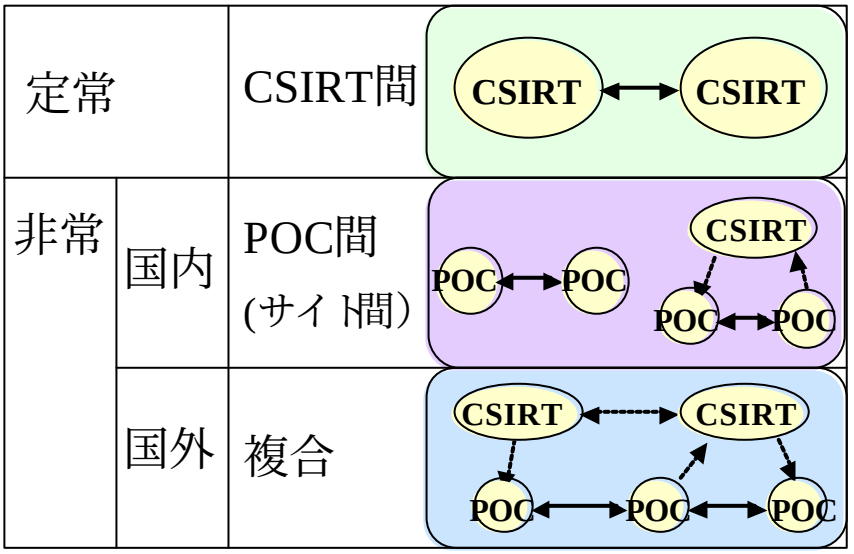
●多くのコンピュータセキュリティインシデントはローカルなコミュニティ外で発生し内部のサイトに影響を与え、また他のはローカルコミュニティ内で発生し、ホストや外部のユーザに影響を与えます。従って、セキュリティインシデントを扱う際に、複数のサイトや他の複数のCSIRTも関係してきます。このようなインシデントを解決していくには、個々のサイトとCSIRT間の、また、CSIRT間の協力が必要となります。

●サービス対象は自分の属するCSIRTが他のCSIRTや外部の組織とどのように協力し合い、どのような情報が共有されるのか、確実に知っておく必要があります。

●CSIRTのポリシーと手続きが明文化されているステートメントがあると、サービス対象はどのようにインシデントを報告すればよいか、その後のサポートはどのようなものが期待できるか、が理解できます。明確な期待、特にCSIRTが提供できるサービスの制限によって相互作用をもっと効率的にまた効果的にする事ができます。

CSIRT体制

関係者間の連絡体制
－インシデントが発生した際の連絡体制



スライド27

●今日、インターネットの発達により国際的なネットワークが広まっている中、1つのCSIRTによって扱われるインシデントはそのサービス対象外の主体を含む場合が増えています。それゆえ、チームは他のCSIRTやサイトと協力し、相互作用する必要があります。

●大きく分けて3方法の連絡体制があります。

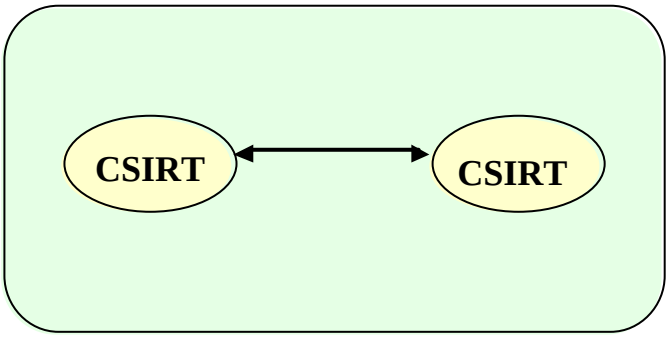
－CSIRT間
－POC間
－複合（複数のCSIRTとPOC間）

●この3方法の連絡体制について、それぞれご説明致します。

CSIRT体制

関係者間の連絡体制
－インシデントが発生した際の連絡体制

• CSIRT間



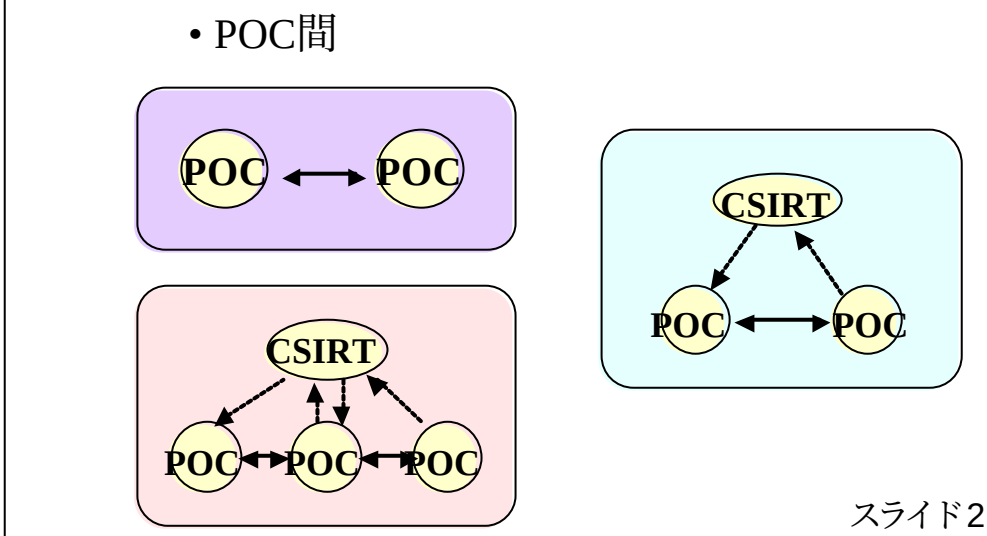
スライド28

●CSIRT間：
インシデントに対応する時以外のCSIRT間の相互作用は、他のチームに意見を求めたり、問題に関する知識を広めたり、1つ以上のCSIRTのサービス対象に影響を与えているセキュリティインシデントを解決するために協力することを含みます。

●このような協力関係を持つ際、CSIRTはこの相互関係に関して、どのような契約を結ぶか考えなくてはなりません。（共有情報の開示などに対して。）

CSIRT体制

関係者間の連絡体制
－インシデントが発生した際の連絡体制



●POC間（Point of Contact):

関係者サイトにインシデントの報告をすることによって、インシデントの解決や拡大を防ぐことができます。インシデントの発生場所によって、アクセス元システムまたはアクセス先システムに問題の所在と内容を伝えることにより、原因を調査し、対応策を考えることができます。早急の対応が、インシデントの早期解決と拡大防止につながります。また、関係者サイトに連絡することで、さまざまな情報が入手でき、再発防止につなげることができます。

●POC間で連絡する方法として、いくつか挙げられます。
①まず1つ目は、直接関係サイトのPOCに連絡を取ってしまう方法です。この方法が一番早くそのインシデント発生場所に連絡をつけ、早急対応につなげることができますが、これはその相手の連絡先が分かっていなければできません。

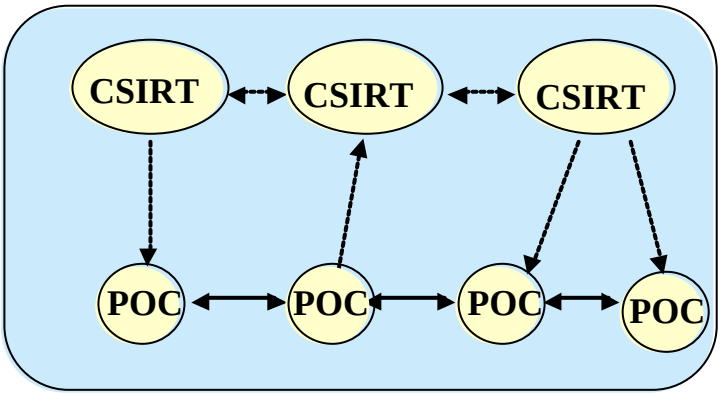
②連絡先が分からない場合、CSIRTを介する連絡方法があります。もし、そのサイトがCSIRTに登録されたメンバーであれば、連絡がｽﾑｰｽに行われます。またそのサイトはCSIRTからインシデントの対応策などのアドバイスを受けることもできます。

③もし、インシデントが3サイト以上の間で起こった際、CSIRTを介すと、その連絡はｽﾑｰｽに行えます。またCSIRTを介すということは、CSIRTが第3者として他のサイトと連絡を取り合えるので、対応を適確に行う事ができます。

CSIRT体制

関係者間の連絡体制
－インシデントが発生した際の連絡体制

• 複合（CSIRTとPOC間）



スライド30

●複合（CSIRT とPOC間）：
複合の連絡体制は複数のCSIRTを介して、複数のPOCに連絡する場合のことを指します。複数のCSIRT を介すということは、たいてい国境を越える場合が多いです。コンピュータインシデントはインターネット上において起こるので、国境という概念はありません。そのため、各国におけるCSIRT間での協力が必要となります。

●自分が属するCSIRT に連絡をすることで、他国の他サイトに連絡をする事ができ、また再発防止にもつながります。しかし、ここで大切なのは、自分が属するCSIRTの連絡先を知っているのはもちろんのこと、そのCSIRT も他のCSIRTの連絡先をあらかじめ知っていて、すぐに参照できるところにあることが重要です。

●世界規模に達してるコンピュータの世界はこの縦横のネットワークが重要になってきます。

CSIRT体制

⑥関係サイトとの情報交換

スライド31

CSIRT体制

関係サイトとの情報交換
ー目的

- 調査の依頼
- インシデントの解決、拡大防止
- 再発防止策の検討

出典：JPCERT/CC 技術メモ－関係サイトとの情報交換
http://www.jpcert.or.jp/ed/2000/ed000006.txt

スライド32

●調査の依頼
不審なアクセスがあった場合、そのアクセスが意図的な攻撃とは限りません。
一般的には、アクセス元システムのソフトウェアや設定等に含まれる誤り、操作ミス等や何らかの障害である可能性があります。
従って、まずは問題となるアクセスについて、先方に事実関係の確認を依頼することが先決です。

●インシデントの解決、拡大防止
関係各サイトの管理者（POC)にインシデントが発生した旨を伝えることによって、インシデントの早期解決、また拡大防止につながります。

●再発防止策の検討
関係サイトに連絡を行うことにより、自サイトだけでは入手できない情報の提供を受けられる可能性があります。

CSIRT体制

関係サイトとの情報交換
―連絡先の決定

- サイトへ直接連絡する場合　(例)
  - インターネットレジストリに登録されている連絡先
  - ホストまたはドメインを管理するポストマスタ
  - RFC2142で紹介されているメールアドレス
  - ホストの管理用アカウント
  - DNSのSOAレコードに登録されたメールアドレス
- CSIRTに連絡する場合

出典：JPCERT/CC 技術メモ―関係サイトとの情報交換
http://www.jpcert.or.jp/ed/2000/ed000006.txt

スライド33

●関係サイトに連絡をする際、誰に、どのような方法で、連絡するかを検討しなくてはなりません。連絡先の決定は大きく分けて二通りあります。

●サイトへ直接連絡する場合：
まずはじめにサイトへ直接連絡する場合です。これにはいくつかの方法があります。（別紙参照）

● CSIRTに連絡する場合：
二つ目はCSIRTに連絡する場合です。自サイトもしくは関係者サイトにサービスを提供しているCSIRTがある場合は、連絡します。CSIRTに連絡することによって、インシデントの対応策などの情報を得ることができると同時に、CSIRTもそのインシデントについての分析や他のインシデントとの関連性を見ることができ、以後の再発防止案をたてることができます。

CSIRT体制

関係サイトとの情報交換
―連絡すべき内容

- 連絡を円滑に進めるための情報
- アクセスの事実を調査するための情報
- そのほか有益な情報

出典：JPCERT/CC 技術メモ―関係サイトとの情報交換
http://www.jpcert.or.jp/ed/2000/ed000006.txt

スライド34

●インシデントが発生したことをサイトもしくは CSIRT に報告する際にあらかじめ、報告するべき
内容をまとめておく必要があります。その報告する内容として含むべき項目をいくつか挙げます。

●まず、多くの CSIRT は報告されたインシデントについて、インシデント・レファレンス番号（e.g..CERT#XXXX) を割り当てます。この番号によって一致する、または類似するインシデント
を追跡し、関係ある活動を見分けます。

●次に、円滑に連絡を行うために必要な基本的な情報として自分のサイトの連絡先、また担
当者（POC)を明確にしなくてはなりません。連絡先としては、少なくても電話番号と電子メール
アドレス、できることなら住所、FAX番号、携帯番号などを載せるとよいでしょう。

●アクセスの事実を調査するための情報を提供できるようにします。例えば、巻き込まれたホスト
の情報（ホストネームやIPアドレスなど）があると、関係活動に関しての徴候が分かるかもしれ
ません。また、もっと重要なのは、侵害者の活動の詳細です。利用された弱点を言及し、シス
テムに施された修正やインストールされたソフトウェアについても言及しましょう。また、ログを
参照できればその活動に関係するログも記録しておきましょう。ログはもっと詳しい説明を提供
してくれる場合もあります。

CSIRT体制

関係サイトとの情報交換
ー脅威

- 盗聴、改竄、妨害
- 情報の漏洩、悪用
- 事実関係の誤認
- 連絡先の不明、不正確、不在
- だまし情報（いたずら情報）

出典：JPCERT/CC 技術メモ－関係サイトとの情報交換
http://www.jpcert.or.jp/ed/2000/ed000006.txt

スライド35

●しかし、インシデントに関する情報交換は、それ自体リスクを伴います。

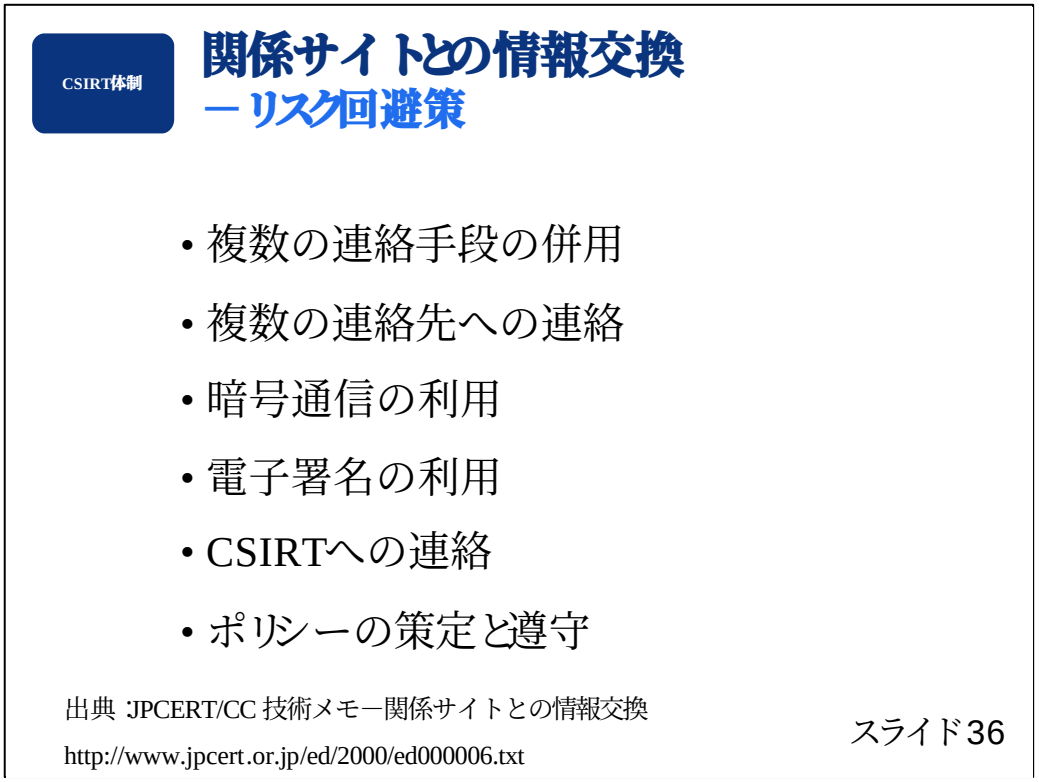
(1)　連絡内容の盗聴、改竄、または妨害をされる可能性があります。

(2)　自サイトに関わるインシデントを外部に知らせることになりますから、もしその知らせた先のサイトが他へ情報を流したり、悪用する可能性もあります。

(3)　例えば、侵害を受けて、ホストの情報（IPアドレスの偽造など）が変えられてしまっていた場合、連絡内容が間違っていることになってしまいます。

(4)　連絡したい人(POC)が不在だったり、明確にされていなかった場合、連絡の遅延につながってしまいます。

(5)　外部からのインシデント情報が悪意に基づく欺瞞情報の可能性もありますし、と同時に自らが報告した内容は欺瞞情報だと思われてしまう可能性もあります。



●前のスライドで紹介した情報交換に基づくリスクですが、それらのリスクを回避する方法がいくつかあります。

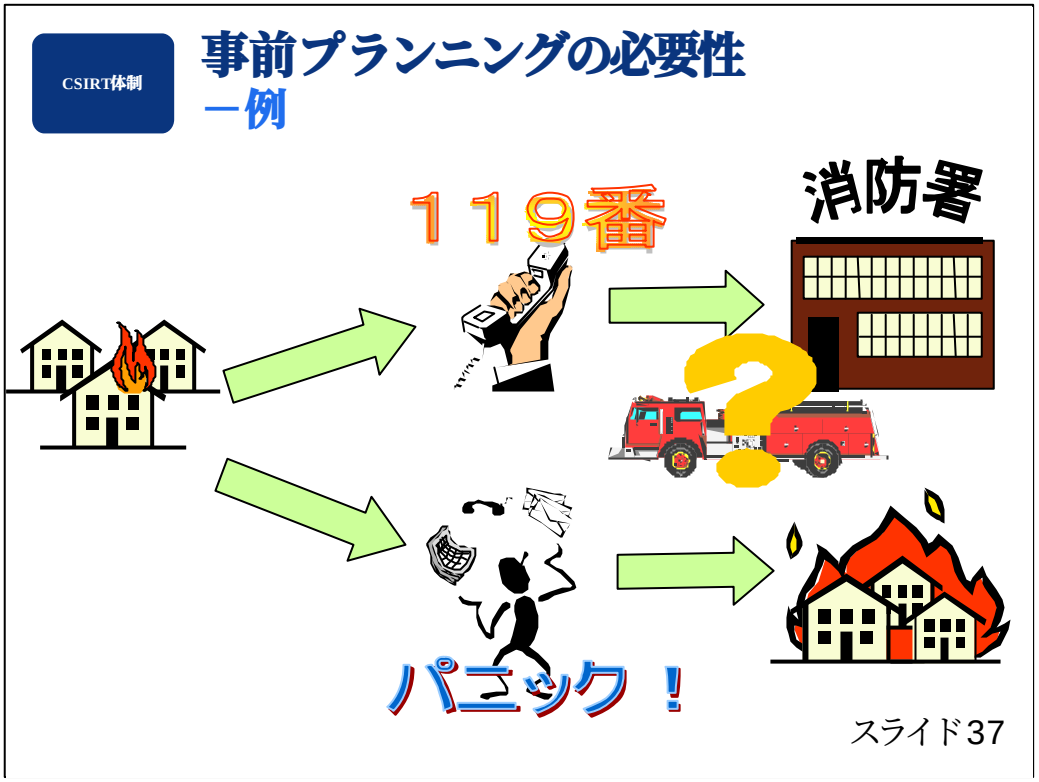
(1) インシデントの報告手段として、電子メールが一般的ですが、 侵害等による影響で使用できない場合、不確かな場合はいくつかの方法を併用して報告します。これによって連絡内容の改竄や妨害をある程度回避することができます。

(2) 複数の関係者サイトに連絡することによって、連絡先の不在などの問題は回避できますが、情報の漏洩の問題に関しては、リスクが高まります。

(3) 連絡内容を暗号化したり、電子署名をつけることによって盗聴や改竄を防止することができます。

(4) CSIRT に連絡することによって、インシデント対応方法やアドバイスを受けることができます。CSIRT に連絡すると、他のインシデントとの関連性をみたり、事実分析を行うので、事実関係の誤認のリスクを軽減することができます。また連絡すべき他の関連サイトの割り出しも、適確に行います。

(5) 想定されるインシデントに対する対応策やそのときの連絡方法、連絡する内容の検討などをポリシーとしてまとめておくことが大切です。また実際インシデントが起きた際、そのポリシーに従って対応するようにします。



●プレゼンテーションの始めにお伝えしましたが、消防署とCSIRTは以下の点において、似ています。双方の重要な役割はそういうインシデント（火事）が発生しないように対策を立てることや、再発防止に努めることです。またサービスを提供する側と受ける側での情報共有や知識共有を通し、調査や研究の重複を減らし、効率化を図ることが可能です。

●ただ、大きく違う点があります。119番に電話して消防署に連絡が行くと、その火事に対応するために消防車がその火事現場に向かい、消火活動を行います。しかし、CSIRTに連絡した場合、以下の点が違います。

①必ずしもCSIRTがそのインシデント発生場所に行くわけではない。
②必ずしも火を消して（インシデントに対応して）くれるわけではない。

これらはCSIRTのポリシーによって異なります。CSIRTはその連絡を受けた際、そのインシデントが発生したサイトに対し、その対応策を伝えると同時に他の関係サイトに連絡したりするのが役割です。

CSIRT体制

まとめ

スライド38

CSIRT体制

まとめ

Ⅰ．CSIRTという言葉の紹介

Ⅱ．インシデント対応の重要性

Ⅲ．CSIRTの発足と連携の必要性

スライド39

CSIRT体制

まとめ

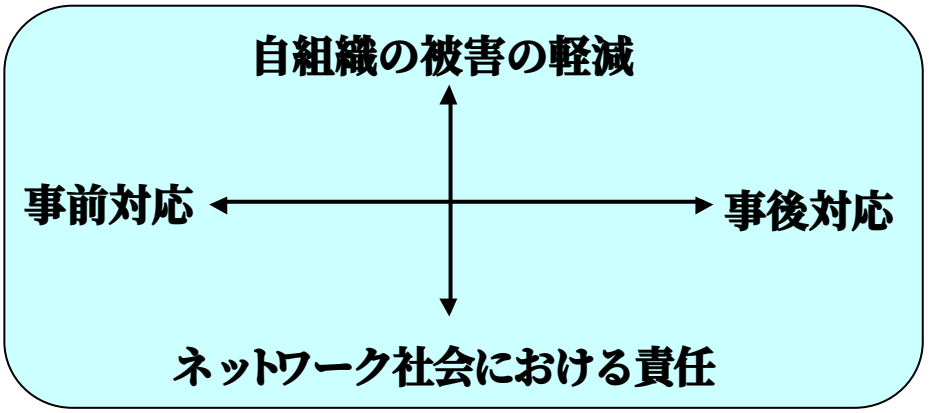
Ⅰ．CSIRTという言葉の紹介

スライド40

CSIRT体制

まとめ

Ⅱ．インシデント対応の重要性



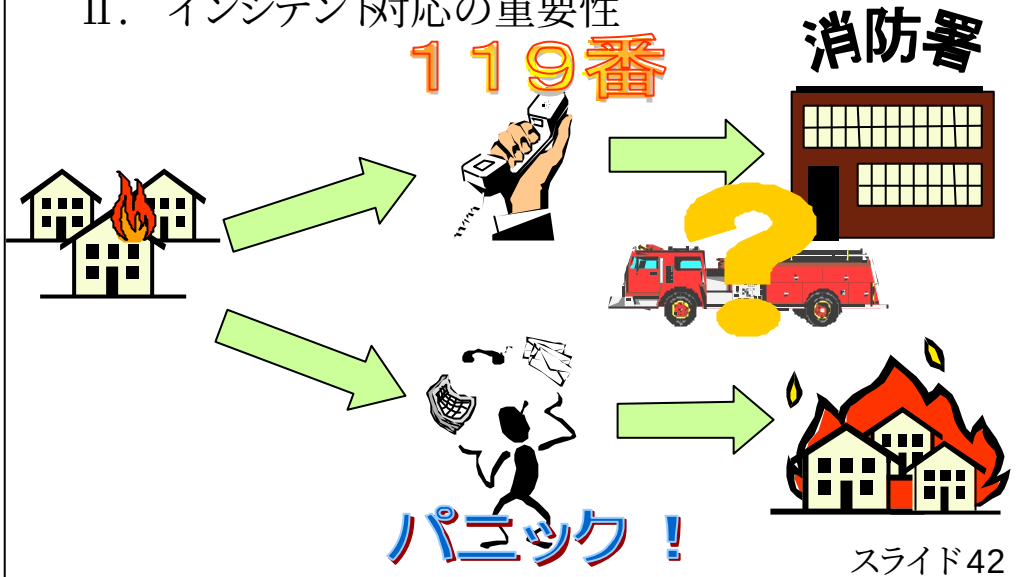
スライド41

●事後対応
●事前対応
●自組織の被害の防止
●ネットワーク社会における責任(踏み台、DDoS対策など）

CSIRT体制

まとめ

Ⅱ．インシデント対応の重要性



スライド42

CSIRT体制

まとめ

Ⅲ．CSIRTの発足と連携の必要性

－CSIRT設立によるインシデント対応

－連携などの効率よい運営による支出の低減

スライド43

●設立は必要ですが、効率のよい運営をしないと支出（人件費も含む）が大きくなってしまいます。そうしないためにも、関係者との協力体制（情報共有）が大切になります。

CSIRT体制

まとめ

Ⅰ．CSIRTという言葉の紹介

Ⅱ．インシデント対応の重要性

Ⅲ．CSIRTの発足と連携の必要性

スライド44