CDI-CIRT 詳細文書

CDI-CIRT Definition

バージョン 1.2
Version 1.2

2009 年 3 月 26 日
March 26th, 2009

株式会社サイバーディフェンス研究所
Cyber Defense Institute, Inc.

目次
Agenda

1. 文書情報
Document Information

1.1 更新日
Date of last update

バージョン 1.2：2009 年 3 月 26 日更新
Version 1.2, published 2009/03/26.

1.2 修正通知の配布先
Distribution List for Modifications Notifications

更新のお知らせは、CDI-CIRT のウェブサイト（http://public.cirt.jp/）のトップページに提示される。
Notifications of update are submitted to the top page of CDI-CIRT's web site at http://public.cirt.jp/.

1.3 本文書の場所
Locations of this document

CDI-CIRT 詳細の文書の現バージョンは、CDI-CIRT のウェブサイトで入手可能である。
The current version of this CDI-CIRT Service description document is available from the CDI-CIRT web site:

http://public.cirt.jp/

1.4 本文書の認証
Authenticating this document

この文書の PDF バージョンは、CDI-CIRT の PGP キーでデジタル署名されている。その署名は、次のウェブサイト上のドキュメントの横に置かれている。
The PDF version of this document has been digitally signed with the CDI-CIRT PGP key. This signature can be found alongside document, on the web site;

http://public.cirt.jp/

2. 連絡先情報
Contact Information

2.1 チーム名
Name of the team

正式名称：サイバーディフェンス研究所 サイバーインシデントレスポンスチーム
Official name: Cyber Defense Institute Cyber Incident Response Team

略称：CDI-CIRT
Short name: CDI-CIRT

2.2 所在地
Address

CDI-CIRT
〒101-0041
東京都千代田区神田須田町 2-2-5 CTN ビル 4 階

CDI-CIRT
Cyber Defense Institute, Inc.
CTN Building, 4th Floor, 2-2-5, Kanda Suda cho,
Chiyoda-ku, Tokyo, 101-0041
JAPAN

2.3 タイムゾーン
Timezone

日本時間
Japan Time (GMT +0900 throughout the year)

2.4 電話番号
Telephone number

03-5209-4336（CDI-CIRT を呼びだしてください。）
+81-3-5209-4336 (as for the CDI-CIRT)

2.5 ファックス番号
Fax number

03-5209-4338（一般の FAX です。）
+81-3-5209-4338 (this is *not* a secure fax)

2.6 E メール
Email

cirt @ cyberdefense.jp
このメールアドレスは、CDI-CIRT のメンバに同報されるものである。
This is a mail alias that relays mail to the human(s) on duty for CDI-CIRT.

2.7 PGP 鍵
PGP Keys

cdi-cirt <cirt @ cyberdefense.jp>

目的:
このキーは、CDI-CIRT と機微な情報（インシデント、脆弱性、質問等）をやり取りするために使用するためのもの。また、やり取り時には、このキーで署名する。
Purpose:
This key is to be used for any confidential communication with CDI-CIRT: communicating incident, vulnerabilities, questions, ... This key will also sign any communication.

Key ID: 0x56B9EDBC
Key Type: DSA-1024
Key Fingerprint: C1C0 542D 9D7B 8176 3348 DB8D 46FF F37E 56B9 EDBC

2.8 チームメンバ
Team members

ディレクター: **飯沼 勇生**
CDI-CIRT Director: **Jack Iinuma**

<iinuma @ cyberdefense.jp>
Key ID: 0xA19CC16D
Key Type: DSA-1024
Key Fingerprint: B304 2521 912B B960 A1D4 D3A0 B8F5 6286 A19C C16D
Expertise: General Security, Cyber Exercise, Security Consultant, Product

代表者／コーディネーター: **名和 利男**
Representative/Coordinator: **Toshio Nawa**

<nawa @ cyberdefense.jp>
Key ID: 0x79A178CA
Key Type: DSA-1024
Key Fingerprint: 5086 9036 0BEB 4A24 89FC 9D35 230A 311B 79A1 78CA
Expertise: Incident Response, Cyber Exercise, Security Training, Security Affair

メンバ: **小林 真悟**
Member: **Shingo Kobayashi**

<kobayashi @ cyberdefense.jp>
Key ID: 0xCDABEDD5
Key Type: DSA-1024
Key Fingerprint: DBE8 5CF0 AB43 7264 5A94 5030 6F3D 00F9 CDAB EDD5
Expertise: MBA, Security Service

メンバ: **ラウリ コルツパルン**
Member: **Lauri Korts-Parn**

<lauri @ cyberdefense.jp>
Key ID: 0x3F51F95B
Key Type: DSA-1024
Key Fingerprint: D300 A6CC 61C9 18B1 A295 623A 2187 618A 3F51 F95B
Expertise: Unix, Windows, Network, Vulnerability Scanning, Forensic, Security Training

メンバ: **松野 真一**
Member: **Shinichi Matsuno**

<matsuno @ cyberdefense.jp>
Key ID: 0x7A230896
Key Type: DSA-1024
Key Fingerprint: 90B3 E8D9 EE39 0F3D DC74　CE69 9F8B 2283 7A23 0896
Expertise: Unix, Windows, Network, Vulnerability Scanning, Security Consulting

2.9 連絡窓口
Point of Contacts

推奨する連絡手段は、E メールである。もし、E メールが難しい場合は、月曜日から金曜日までの業務時間に電話が可能。
Preferred method is by email. If not by email, telephone during office hours, from Monday to Friday.

3. 憲章
Charter

3.1 ミッションステートメント
Mission Statement

CDI-CIRT の基本的な達成目標は、次の通り。
The basic goal of CDI-CIRT is as follows;

- サイバーディフェンス研究所及びそのクライアントにおけるサイバーセキュリティ（コンピュータ、ネットワーク、情報、インターネットに関する包括的なセキュリティの概念）のレベル向上に寄与すること
  To contribute to the progress of the security level of the cyber (computer / network / information / internet) security in Cyber Defense Institute and its clients.

CDI-CIRT のミッションは、次の通り。
The mission of CDI-CIRT is as follows.

- アラート（注意喚起）及びサイバーインシデントにかかるインシデントのハンドリング及びコーディネーションの拠点となり、サイバーディフェンス研究所及びそのクライアントを支援すること
  To be the center for alert and cyber security related incidents handling and coordination, helping Cyber Defense Institute and its clients.

- サイバーディフェンス研究所及びそのクライアントのサイバー（コンピュータ及びネットワーク等）システムに影響を与える脅威に対して、迅速かつ的確に対応すること
  To respond to threats that affect Cyber Defense Institute and its clients' cyber system in a fast and efficient manner.

3.2 サービス対象
Constituency

CDI-CIRT は、サイバーディフェンス研究所の中に設置されています。CDI-CIRT のサービス対象は、サイバーディフェンス研究所及びそのクライアント（官公庁、金融企業、ウェブポータル事業者等）である。
CDI-CIRT is part of Cyber Defense Institute. The constituency of CDI-CIRT is the entire Cyber Defense Institute and its clients (Government agencies, banks, web-portal providers and etc).

次は、サービス対象の説明である。
The following information is about target constituency.

項目 Title	説明 Definition
サービス対象のタイプ Type of constituency	親組織内部、顧客基盤 Internal to Host Organization and customer base
サービス対象の詳細 Description of constituency	サイバーディフェンス研究所全体及びそのクライアント Entire Cyber Defense Institute and its clients
サービス対象を表すインターネットドメイン　かつ／或いは　IP　アドレス情報 Internet domain and/or IP address information describing the constituency	- cyberdefense.jp - cirt.jp - vul.jp - dumbtech.jp
サービス対象が在住する国 All countries in which constituency members are located in	日本 Japan

表　1 CDI-CIRT　のサービス対象について
Table 1 Definition of CDI-CIRT's constituency

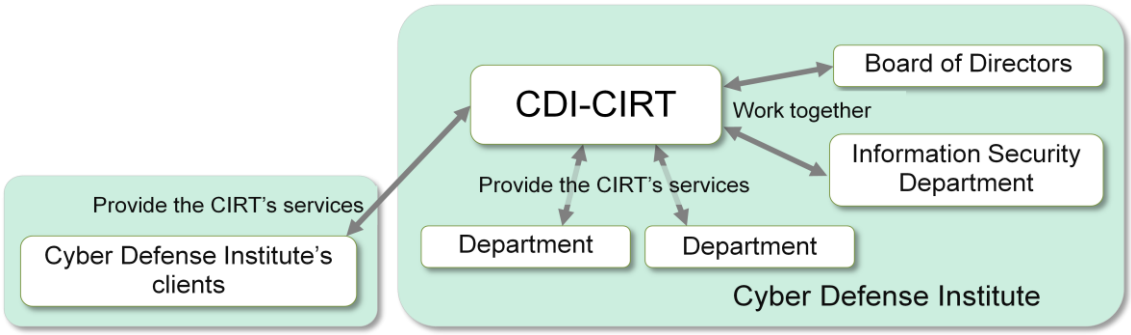

図　1 CDI-CIRT　のサービス対象の概要
Figure 1 Overview of CDI-CIRT's constitutency

3.3 支援組織
Sponsoring organization

CDI-CIRT　は、サイバーディフェンスにおける　組織内　CSIRT（コンピュータ・セキュリティ・インシデント・レスポンス・チーム）の環境整備を目的として、サイバーディフェンス研究所の取締役の意思決定により設置されている。
CDI-CIRT is founded based on the decision by the Board of Directors in Cyber Defense Institute to improve environment of an internal CSIRT (Computer Security Incident Response Team) in Cyber Defense Institute.

3.4 権限
Authority

CDI-CIRT　の権限は、CDI-CIRT　のミッションを達成するための意思決定やアクションをとるため、サービス対象と共有されている。
The authority of CDI-CIRT is shared with the constituency, taking with them the necessary decision and actions to fulfill CDI-CIRT's mission.

4. ポリシー
CDI-CIRT Policies

4.1 インシデントタイプとサポートレベル
Types of incidents and level of support

CDI-CIRT は、サービス対象において発生するサイバーセキュリティに関するインシデントのすべてに対して取り組む権限が与えられている。
CDI-CIRT is authorized to address all types of cyber security related incidents which occurs at its constituency.

CDI-CIRT は、サービス対象からの要求に基づいて活動する。或いは、サービス対象が、サイバーセキュリティに関するインシデントに巻き込まれた場合に、(CDI-CIRT 自ら)活動する可能性がある。
CDI-CIRT may act upon requests of one of its constituents or may act if one of its constituents is involved in a cyber security related incident.

CDI-CIRT によるサポートのレベルは、インシデントや事象のタイプと重要性、対象のタイプ、影響を受けるユーザーコミュニティ、そしてその時の CDI-CIRT の稼働可能状況によって異なる。しかしながら、すべてのケースに対し、1営業日以内に対応する。CDI-CIRT メンバは、次の優先度順に従って割り当てられる。
The level of support given by CDI-CIRT will vary depending of the type and severity of the incidents or issue, the type of constituent, the size of the user community affected and the CDI-CIRT's resources at the time, though in all cases some response will be made within one working day. Resources will be assigned according to the following priorities, listed in decreasing order:

1. 人間の物理的安全に対する脅威
   Threats to the physical safety of human beings.

2. あらゆる経営情報システムやバックボーンネットワーク基盤の一部におけるルートやシステムレベルの攻撃
   Root or system-level attacks on any Management Information System (MIS), or any part of the backbone network infrastructure.

3. マルチユーザー或いは特定使途の大規模な公的サービス機器に対するルートやシステムレベルの攻撃
   Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.

4. 制限されている信用サービスのアカウントやソフトウェア、特に、機密情報を含む経営管理システムやシステム管理者のために使用されるシステムに対するセキュリティ侵害
   Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.

5. 上記 1. から 3. のシステム等に対する DoS 攻撃
   Denial of service attacks on any of the above three items.

6. サイバーディフェンス研究所を起因とする、他のサイト(場所)における上記の攻撃等
   Any of the above at other sites, originating from Cyber Defense Institute.

7. あらゆる種類の広域的な攻撃 (例:スニッフィング攻撃、IRC ソーシャルエンジニアリン

グ攻撃、パスワードクラッキング攻撃）
Large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks.

8. 個人ユーザーカウントに絡む脅威、嫌がらせ、犯罪行為
Threats, harassment, and other criminal offenses involving individual user accounts.

9. マルチユーザーシステム上の個人ユーザーカウントへのセキュリティ侵害
Compromise of individual user accounts on multi-user systems.

10. デスクトップシステムへのセキュリティ侵害
Compromise of desktop systems.

11. 偽装と不当表示、そして、ローカル・ルールと規則のセキュリティに関する違反（例：ネットニュースと E メールの偽装、IRC ポットの不正使用）
Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. netnews and e-mail forgery, unauthorized use of IRC bots.

12. 個人ユーザーカウントに関する DoS 攻撃 （例： メールボム）
Denial of service on individual user accounts, e.g. mailbombing.

他のインシデントについては、確認できる重要性と範囲に従って優先付けがされる。インシデントの関連する重要性は、CDI-CIRT の裁量によって決定される。
Other types of incidents will be prioritized according to their apparent severity and extent. The relative severity of incidents will be assessed at CDI-CIRT's discretion.

エンドユーザーに対して直接のサポートが全く与えられないわけではない。エンドユーザーは、システム管理者、ネットワーク管理者、本部の支援部署に連絡するはずである。CDI-CIRT は、その管理者等に対してサポートをする。
Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The CDI-CIRT will support the latter people.

CDI-CIRT は、サイバーディフェンス研究所とそのクライアントにおけるシステム管理者の専門的知識には、実に様々なレベルがあることを理解しており、CDI-CIRT は、それぞれの方に対して適切なレベルで、情報や支援の提供を試みるが、CDI-CIRT は、その場でシステム管理を教育することができなく、システム管理者に代わって、システム保守をすることもできない。大抵の場合、CDI-CIRT は、適切な施策を行うために必要となる情報先を提供する。
While the CDI-CIRT understands that there exists great variation in the level of system administrator expertise at Cyber Defense Institute and its clients, and while CDI-CIRT will endeavor to present information and assistance at a level appropriate to each person, the CDI-CIRT cannot train system administrators on the fly, and it cannot perform system maintenance on their behalf. In most cases, The CDI-CIRT will provide pointers to the information needed to implement appropriate measures.

CDI-CIRT は、サイバーディフェンス研究所とそのクライアントに対して、可能性のある脆弱性を、継続的に伝えることになっている。可能であれば、彼らが作為的に侵害される前に、脆弱性のような情報を伝える。
The CDI-CIRT is committed to keeping the Cyber Defense Institute and its clients informed of potential vulnerabilities, and where possible, will inform them of such vulnerabilities before they are actively exploited.

CDI-CIRT は原則として、被害者か被疑者にかかわらず、サービス対象がインシデントに巻き込まれた報告を受け入れる。

The CDI-CIRT will in principle accept any incidents reports that involves an incident with one of the constituent, either as victim or as suspect.

個人ユーザーからのインシデント報告は、優先度を低くなる。また、この報告は、個人ユーザーに対して責任を持つセキュリティの権限を持つ方に委ねられる。
Incidents reports from individual users will be given a low priority and will be deferred to their responsible security authority.

4.2 連携、相互関係、情報開示
Co-operation, Interaction and Disclosure of Information

CDI-CIRT からの情報の流れにおいて、サービス対象の組織のポリシーで概説されているところすべて、及び、尊重すべきところにおいて、法的及び倫理的な制約があるが、CDI-CIRT は、インターネットを構築した協調精神に対する責務を認識し、それに貢献する意図表明をする。そのため、私どものサービス対象と、必要に応じて、近隣のサイトのメンバのアイデンティティを守るために適切な施策をとるが、別の面では、CDI-CIRT は、他者にするセキュリティインシデントの解決と予防に関する支援をする際、制限を受けずに情報を共有する。
While there are legal and ethical restrictions on the flow of information from CDI-CIRT, all of which may also be outlined in Policies at the organizations of its constituency, and all of which will be respected, CDI-CIRT acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighboring sites where necessary, CDI-CIRT will otherwise share information freely when this will assist others in resolving or preventing security incidents.

次のパラグラフにおいて、「影響を受けた当事者」とは、正当な所有者、オペレーター、そして関係するコンピュータ設備のユーザーのことである。CDI-CIRT からの守秘義務を全く気にかけない侵入者のような、施設を不正目的で使用する正規ユーザーや、無許可のユーザーのことではない。「影響を受けた当事者」は、守秘義務に対する法律上の権利を持っているかどうかは分からない。もちろん、そのような権利は存在することが期待されている。CDI-CIRT は、法律上の義務がある場合はいつでも、第三者や監督省庁に対して情報を公開する場合がある。しかしながら、場合によっては、CDI-CIRT は、周囲の事情のようなものが、明確に確立するまでは、このアクションは遅延させる場合がある。例えば、裁判所の命令などがある。このような場合は、 CDI-CIRT は、常に、影響を受ける人或いは組織に対して通知をする。
In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from CDI-CIRT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist. CDI-CIRT may release information to any third party or to governing authorities whenever there is a legal obligation to do so. However, CDI-CIRT may in some cases delay this action until such a circumstance has been established irrevocably, e.g. by court order. CDI-CIRT will in such cases always notify the affected persons or organizations.

公開が必要とみなされる情報は、次のように分類される:
Information being considered for release will be classified as follows:

- 個人のユーザー情報は、特定のユーザーに関する情報であるが、場合によっては特定のアプリケーションの情報でもある。これらは、法律、契約、及び／或いは、倫理上の信用情報とみなすべきものである。
  Private user information is information about particular users, or in some cases,

particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons.

- 個人のユーザー情報は、以下に示されること以外、CDI-CIRT の外部において識別可能なフォームで公開されることはない。ユーザーを識別することが困難にするものであれば、情報を制限なく公開することができる。（例えば、侵入者によって書き換えられた.cshrc ファイルを見せることや、特定のソーシャルエンジニアリング攻撃のデモをすることなど）
  Private user information will be not be released in identifiable form outside CDI-CIRT, except as provided for below. If the identity of the user is disguised, then the information can be released freely (for example to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).

- 侵入者の情報は、侵入行為に関すること以外は、個人のユーザー情報と同義である。
  Intruder information is similar to private user information, but concerns intruders.

- 特定の識別可能な情報を伴う侵入者の情報は、一般に公開することはないが、システム管理者とインシデントの追跡活動をする CISRT と、制限なく情報交換する。ただし、刑事責任があるために、その情報が公記録になる場合は、この限りではない。
  While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRT's tracking an incident.

- 個人のサイト情報は、特定のシステム或いはサイトの技術情報である
  Private site information is technical information about particular systems or sites.

- 以下に示されること以外、問題があるサイトの許可がない状態で公開することはない。
  It will not be released without the permission of the site in question, except as provided for below.

- 脆弱性の情報は、修正及び回避策を含めた、脆弱性或いは攻撃に関する情報である。脆弱性の情報は、制限なく公開されるが、不特定多数の人に公開される前に、関係するベンダーに通知し、働きかけるようなあらゆる努力をする。
  Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds. Vulnerability information will be released freely, though every effort will be made to inform and work with the relevant vendor before the general public is informed.

- 当惑させる情報には、インシデントが発生したという宣言と、その伝達範囲と重要性に関する情報を含んでいる。当惑させる情報は、サイト、及び、特定のユーザー或いはユーザーグループと関係する場合がある。
  Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users.

- 当惑させる情報は、いかに示されること以外、問題を持つサイト或いはユーザーの許可なく、公開することはない。
  Embarrassing information will not be released without the permission of the site or users in question, except as provided for below.

- 統計情報は、特定可能な情報が取り除かれた、当惑させる情報である。統計情報は、CDI-CIRT の裁量によって公開される。
  Statistical information is embarrassing information with the identifying information stripped off. Statistical information will be released at the discretion of CDI-CIRT.

- 連絡先情報は、CSIRT のセキュリティ連絡担当者へ連絡手段を説明するものである。連絡先情報は、サービス対象のメンバに対して、制限なく公開される。ただし、実際とは異なると要求してきた連絡担当者等や、CDI-CIRT に、この情報を露出させることが適切でないと信じるに足りる理由がある場合は、この限りではない。
  Contact information explains how to reach Security Contact Persons and CSIRT's. Contact information will be released freely to members of the constituency, except where the contact person or entity has requested that this not be the case, or where CDI-CIRT has reason to believe that the dissemination of this information would not be appreciated.

CDI-CIRT からの情報を受領する可能性のある主体は、次のように分類される:
Potential recipients of information from CDI-CIRT will be classified as follows:

- サービス対象の管理層のメンバは、 守秘義務の責任及び説明責任の性質を有するため、管理すべき範囲で発生したコンピュータセキュリティインシデントをハンドリングを促進させる必要がある情報は何でも受領するはずである。
  Because of the nature of their responsibilities and consequent expectations of confidentiality, members of the constituency's management are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.

- サービス対象のメンバであるセキュリティ連絡担当者も、その職責に基づいき、機密情報の扱いを委ねられる。しかしながら、CDI-CIRT メンバのような人でない限り、セキュリティ連絡担当者は、調査を事実調査の支援或いは所有するシステムを安全にするために十分な、最小限の機密情報を受け取るべきである。
  Security Contact Persons at organizations that are members of the constituency are also, by virtue of their responsibilities, trusted with confidential information. However, unless such people are also members of CDI-CIRT, they will be given only that confidential information which they must have in order to assist with an investigation, or in order to secure their own systems.
  サービス対象範囲のユーザーは、CDI-CIRT とは出来るだけ少ないやり取りにすべきである。そのかわり、必要ならば、主となる連絡窓口は、ユーザーが所属する組織のセキュリティチームがなるはずである。そこが、CDI-CIRT と同様な連絡をする。
  Users within the constituency should have as little interaction with CDI-CIRT as possible. Instead, their primary point of contact should be their parent institution's security team, that in turn would contact CDI-CIRT if necessary.

- サービス対象全体は、情報開示の許可が与えられた影響を受けるところを除き、制限された情報を受け取ることはない。インシデントをサービス対象全体に対してインシデントを報告する CDI-CIRT には、いかなる義務も負うことはない。しかしながら、報告をするという選択肢を選ぶ場合がある。特に、CDI-CIRT が、影響を受けるに至った流れについて、影響を受けるところにすべてに対して通知すると思われる。
  The constituency community will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general community. There is no obligation on the part of CDI-CIRT to report incidents to the community, though it may choose to do so; in particular, it is likely that CDI-CIRT will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

- 社会全般は、制限された情報を受け取ることはない。現実的に、社会全般に対してコミュニケーションをとる特段の努力が図られることない。しかしながら、CDI-CIRT は、あらゆる観点から見て、サービス対象全体に対して提供した情報は、実際には、一般社会に提供する情報であることと、結果からみると、その情報をよく吟味していることを認めている。

The public at large will receive no restricted information. In fact, no particular effort will be made to communicate with the public at large, though CDI-CIRT recognizes that, for all intents and purposes, information made available to its constituency community is in effect made available to the community at large, and will tailor the information in consequence.

- コンピューターセキュリティコミュニティは、一般社会と同じ要領で取り扱われる。CDI-CIRT のメンバは、ニュースグループ、full-disclosure リストである「bugtraq」を含むメーリングリスト、そして、カンファレンス等の、コンピューターセキュリティコミュニティでのディスカッションに参加するか場合があるが、そのようなフォーラムは、一般社会として取り扱う。脆弱性を含むような技術的な話題が、あらゆるレベルで議論されるかもしれないが、CDI-CIRT の経験から得られた例示は、影響を受けたところが識別されないように隠ぺいされる。
  The computer security community will be treated the same way the general public is treated. While members of CDI-CIRT may participate in discussions within the computer security community, such as newsgroups, mailing lists (including the full-disclosure list "bugtraq"), and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from CDI-CIRT experience will be disguised to avoid identifying the affected parties.

- 報道機関も、一般社会の一部としてみなす。CDI-CIRT は、通常、一般社会に対して既知の情報を提供する窓口として以外、コンピュータセキュリティインシデントに関心を寄せる報道機関と直接のやり取りをしない。CDI-CIRT は、報道機関の役割は、一般社会と特にサービス対象全体に対して知らしめるための手段であると認識している。この役割を適切な形で活用するために、CDI-CIRT の渉外担当部署が、報道機関に対する一元化した窓口業務する。
  The press will also be considered as part of the general public. CDI-CIRT will generally not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. However, CDI-CIRT acknowledges the role of the Press as a vehicle to inform the broad public in general and its own constituency in particular. To properly accommodate this function, the CDI-CIRT Public Relations department acts as the focal point in Press contacts.

  サイバーディフェンス研究所の渉外担当部署は、CDI-CIRT の声明が必要になる場合、CDI-CIRT に支援を求める。CDI-CIRT のみが、CDI-CIRT として声明を作成することができる。情報セキュリティの最高責任者、CDI-CIRT のコーディネーター及び監督責任者が、CDI-CIRT に代わって、公式見解を作成する責任がある。このことは、CDI-CIRT のメンバ個人がコンピュータセキュリティのトピック全般に関するインタービューを受け入れることを妨げるようなものではない。現実には、サービス対象全般に対する公的サービスをとして圧力がかけられている。ここで留意すべきことは、すべての CDI-CIRT メンバは、特定のインシデントに関する厳格な守秘義務の責任を持っていることである。
  The Cyber Defense Institute Public Relations department will call in CDI-CIRT in case a CDI-CIRT statement is needed. Only CDI-CIRT can make statements on behalf of CDI-CIRT. The Chief Information Officer, the CERT Coordinator and the Supervising Director are responsible for making public statements on behalf of CDI-CIRT. The above does not affect the ability of individual members of CDI-CIRT to grant interviews on general computer security topics; in fact, they are encouraged to do so, as a public service to the community. Note that all CDI-CIRT members are committed to absolute confidentiality pertaining specific incidents.

- その他のサイトや CSIRT は、コンピュータセキュリティインシデントの調査に関する連携をする際、場合によっては機密情報を委ねる。これは、他のサイトの誠実さが確認された場合

に限りなされるものであり、送付される情報が、インシデントの解決に役立つようなものである場合に限られる。このような情報共有は、多くの場合、CDI-CIRT と十分な付き合いがあるサイト間で実施される。（例えば、日本国内の幾つかの CSIRT は、コンピュータセキュリティインシデント問題について、CDI-CIRT と非公式ではあるが、確立された連携関係がある。）
Other sites and CSIRT's, when they are partners in the investigation of a computer security incident, will in some cases be trusted with confidential information. This will happen only if the other site's bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. Such information sharing is most likely to happen in the case of sites well known to CDI-CIRT (for example, several other Japanese CSIRT's have informal but well-established working relationships with CDI-CIRT in such matters).

セキュリティインシデントの解決のために、ユーザーアカウントの接続元のようなあたりさわりのないような個人に準じた情報は、機密情報とみなすことはせずに、必要以上の事前注意をすることなく、外部のサイトに転送することができる。「侵害情報」については、セキュリティ連絡担当者と CSIRT に制限なく転送する。「当惑させる情報」は、守秘義務が保持できることが確実であることが十分であり、かつ、インシデントの解決に必要である場合に転送することができる。
For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other Security Contact Persons and CSIRT's. "Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential, and when it is necessary to resolve an incident.

- 他の CSIRT とのやり取りにおいて、CDI-CIRT は、他に対して提供する情報は、（非拒否のため）署名する。また、必要があると考えられるときには暗号化をする。詳細は 4.3 章を参照。
  In its contact with other CSIRT's, CDI-CIRT will see to it that the information which is made available to others, will be signed (so as to provide for non-repudiation), and, whenever deemed necessary, crypted. See also 4.3 for more details.

- ベンダーは、あらゆる点で外国の CSIRT とみなしている。CDI-CIRT は、さまざまなネットワーク及びコンピュータ機器、ソフトウェア、並びにサービスのベンダーに、それぞれが提供するプロダクトのセキュリティ向上を働きかけたいと考えている。このようなことに寄与するため、それらのプロダクトで発見された脆弱性は、問題の特定と修正に必要な技術詳細とともに、そのベンダーに報告されるようにする。判明した詳細情報は、影響を受ける主体の許可を得ないでベンダーに与えられない。
  Vendors will be considered as foreign CSIRT's for most intents and purposes. CDI-CIRT wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

- 法執行機関（警察）は、守秘義務に関する事前の取り決めにかかわらず、法執行機関（警察）が調査を目的のために要求する情報など、法に基づいた形での CDI-CIRT から全面協力を受ける。
  Law enforcement officers will receive full cooperation, as permitted by law, from CDI-CIRT, including any information they require to pursue an investigation, notwithstanding the earlier statements made about confidentiality.

4.3 コミュニケーションと認証
Communication and Authentication

CDI-CIRT が取り扱う可能性の高い情報の形態の中で、電話は、暗号化が施されなくとも十分に安全だと考えられる。暗号化されていない E メールは、著しく安全ではないが、機密性の低いデータを送信するには十分である。もし、機密性の高いデータを送信する必要がある場合は、PGP が使用される。ネットワークファイル転送は、このような趣旨で、E メールと同様とみなされる。機密データは転送前に暗号化をすべきである。
In view of the types of information that CDI-CIRT, will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted before transmission.

CDI-CIRT に提供される情報を信頼する前に、或いは、機密情報を展開する前に信頼関係を構築する必要が場面で、妥当なレベルの信頼があるかどうか、相手の身元確認や実情を確認する。サービス対象内、よく知られた近隣のサイト内、そして信頼のおける人からよく知られている委託先については、それらを確認するには特に問題はない。そうでない場合については、FIRST メンバの検索、WHOIS 情報及び他のインターネット登録情報の活用し、折り返し電話や返信メールで相手が偽物出ないことを確認するなどの、適切な手段を使用する。信頼しなければならないデータのある受信メールは、その作成者の身元確認や、デジタル署名（特に、PGP がこれを実装しているもの）によって確認される。
Where it is necessary to establish trust, for example before relying on information given to CDI-CIRT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within the constituency, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

4.4 親組織の ISMS 認証
ISMS certification of parent organization

CDI-CIRT の親組織であるサイバーディフェンス研究所は、2008 年 8 月、国際標準 ISO/IEC 27001:2005 と日本規格 JIS Q 27001:2006 に準拠した ISMS 認証を取得した。この認証範囲は、サイバーディフェンス研究所全体に適用されている。
Cyber Defense Institute, which is the host/parent organization of CDI-CIRT, obtained Information Security Management Systems (ISMS) certification under the international standard ISO/IEC 27001:2005 and the Japanese national standard JIS Q 27001:2006 in August, 2008. The scope of certification applies to Cyber Defense Institute on a company-wide basis.

この認証の概要は、次の通り。
The overview of this certification is as follows.

取得した認証 Obtained Certification	ISO/IEC 27001:2005, JIS Q27001:2006
認証番号 Certificate Number	700956
登録日 Date of Registration	2008 年 8 月 27 日 August 27th, 2008
認証機関 Certification Agency	ビューロベリタス株式会社 Bureau Veritas Japan Co., Ltd.
登録機関 Registration Agency	財団法人 日本情報処理開発協会 JIPDEC (Japan Information Processing Development Corporation)
認証有効期間 Certificated Valid Until	2011 年 8 月 26 日 August 26th, 2011

表 2 認証の概要
Table 2 Overview of the Certification

認証範囲: IT サービスおよび IT セキュリティビジネスの情報セキュリティマネジメントシステム。クライアントから受領される、及び、サイバーディフェンス研究所によってクライアントに提供される情報資産とみなされるものすべてを含む。
Scope of Certification: Information security management system of IT service and IT security business. This includes all identified information assets received on behalf of clients and provided for the clients by of Cyber Defense Institute.

この組織のポリシーに基づき、CDI-CIRT は、そのサービスに関する補足的なポリシーに準じる。
Based on this organizational policy, CDI-CIRT complies some additional policy concerning CDI-CIRT's services.

5. サービス
Services

5.1 事後対応サービス
Reactive Services

このサービスは、CDI-CIRT メンバやサービス対象のメンバによって認知された、発生後のインシデントに対して必要な対応措置がとられるものである。これは、短期間な取り組みである。
These services are offered in reaction to an occurring incident, be it detected by CDI-CIRT member or a constituency's members. They focus on short-term issues.

5.1.1 注意喚起と警報
Alerts and Warnings

CDI-CIRT は、一般に言われるような発生攻撃、セキュリティ脆弱性、警告に関する情報と、問題解決のための活動において推奨される短期間の行動方針をサービス対象に提供する。
CDI-CIRT will provide its constituency with information about ongoing attacks, security vulnerabilities, alerts in the general sense, and short-term recommended course of action for dealing with the resulting problems.

5.1.2 インシデントハンドリング
Incident Handling

CDI-CIRT は、技術的かつ組織的な見地によるインシデントハンドリングで、サービス対象を支援する。特に、次のインシデントハンドリングにおける局面を重要視して、支援或いはアドバイスを提供する。
CDI-CIRT will assist its constituency in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident handling.

インシデント・トリアージ
Incident Triage

- 実際に発生したインシデントを評価する
  Assessing whether indeed an incident occurred.
- インシデントの影響範囲を決定する
  Determining the extent of the incident.

インシデントレスポンス・サポート
Incident response support

CDI-CIRT は、電話、E メール、Fax、或いは書面を通じて、攻撃の被害者に対して、インシデントからの復旧に関する支援や相談などを実施する。これには、次のサービスがある。
CDI-CIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve;

- 収集されたデータの解釈について技術的解釈
  technical assistance in the interpretation of data collected,
- 連絡先情報の提供
  providing contact information, or
- 回避策及び復旧策に関する助言の回答
  relaying guidance on mitigation and recovery strategies.

このサービスには、上記で説明した直接的、オンサイトのインシデントレスポンスは含まない。その代わりに、CDI-CIRT は、サイトの担当者の復旧活動に役立つ情報を提供する。
It does not involve direct, on-site incident response actions as described above. CDI-CIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

オンサイトのインシデントレスポンス
Incident response on site

場合によっては、CDI-CIRT は、サービス対象に対して、インシデントからの復旧を支援するために、有料で直接的なオンサイトの支援を提供する。電話や E メールによるインシデントレスポンスサポートの提供だけではなく、CDI-CIRT 自ら、影響を受けたシステムを分析し、システムの修復や復旧を直接実施する。
In some cases, CDI-CIRT provides direct, on-site assistance to help constituents recover from an incident for a fee. The CDI-CIRT itself physically analyzes the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email.

インシデントレスポンス・コーディネーション
Incident response coordination

- 可能ならば、インシデント（脆弱性のエクスプロイト）の一次的原因の決定
  If possible, determining the initial cause of the incident (vulnerability exploited);
- 関係する他のサイトとのやり取りの促進
  Facilitating contact with other sites which may be involved;
- 可能ならば、適切な法執行機関（警察）とのやり取りの促進
  Facilitating contact with appropriate law enforcement officials, if necessary;
- 他の CSIRT に対する報告
  Making reports to other CSIRTs;
- 可能ならば、ユーザーに対するアナウンスメントの作成
  Composing announcements to users, if applicable.

インシデントハンドリングプロセスの概要は、次の図の通り。
The outline of the incident handling process is the following diagram.

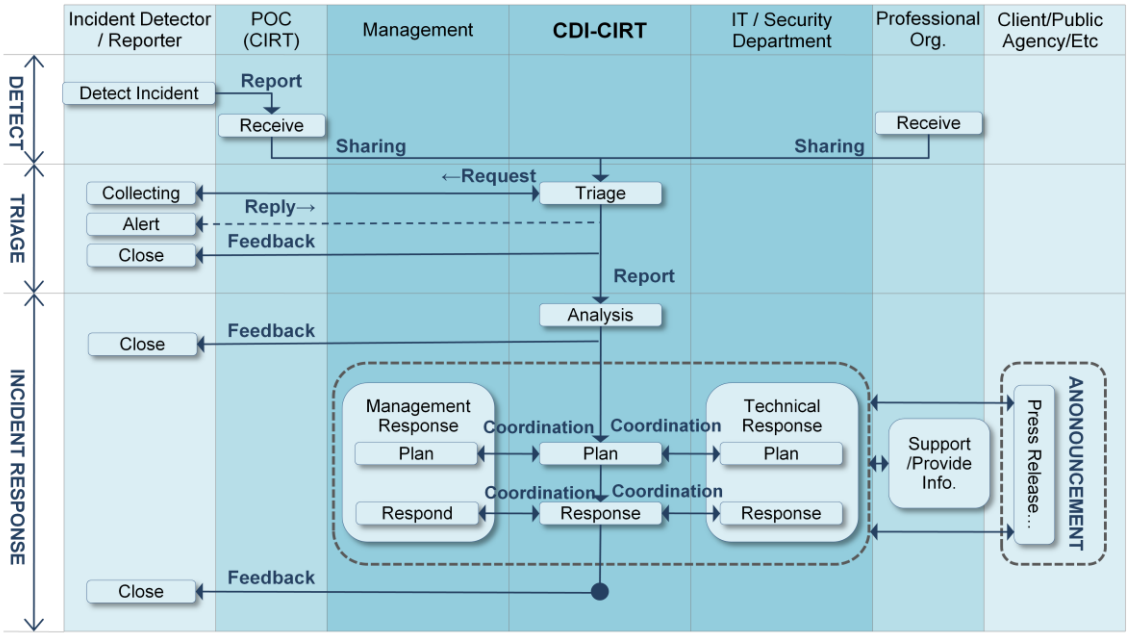

図 2 CDI-CIRT のインシデントハンドリングプロセス
Figure 2 Incident Handling Process of CDI-CIRT

5.1.3 アーティファクトハンドリング
Artifact Handling

アーティファクトとは、プローブ或いは攻撃されているシステムやネットワークに巻き込まれている可能性のあるシステムで発見されたファイルや対象物である。アーティファクトの例としては、ウィルス、トロイの木馬、ワーム、エクスプロイトスクリプト、ルートキットがある。
An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks, or that can be used to defeat security measures. Examples of artifacts are viruses, Trojan horse programs, worms, exploit scripts, rootkits, ...

フォレンジック分析
Forensic analysis

CDI-CIRT は、システム上で発見されたるアーティファクトを技術的な調査及び分析をする。この分析には、次が含まれる。
CDI-CIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include;

- ファイルタイプとアーティファクトの構造の分析
  identifying the file type and structure of the artifact,
- 新しいアーティファクトと、既存のアーティファクトや同じアーティファクトの他のバージョンとの類似点と相違点の確認
  comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or
- アーティファクトの目的や機能を見出すためにリバースエンジニアリングや逆アセンブル
  reverse engineering or disassembling code to determine the purpose and function of the artifact.

5.2 事前対応サービス
Proactive Services

このサービスは、インシデント発生後、その発生抑止と影響の軽減をねらいとする。これは、中長期間な取り組みである。
These services aim to prevent incidents from happening and reduce their impact when they occur. They focus on medium- to long-term issues.

5.2.1 アナウンスメント
Announcements

- アナウンスメントは、次を含む。
  Announcements include
- 侵入注意喚起
  Intrusion alert;
- 脆弱性の警戒
  vulnerability warnings;
- セキュリティアドバイザリ
  security advisories.

このアナウンスメントは、新しく発見された脆弱性や浸入ツールのような、中期から長期的な影響を伴う新しい攻撃物について、サービス対象に対して通知をするものである。アナウンスメントは、サービス対象が、エクスプロイトの被害に合う前に、新しく発見された問題に対して、システムやネットワークを防御させることができる。
These announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

5.2.2 技術監視
Technology Watch

CDI-CIRT は、将来的な脅威を特定するため、新しい技術開発、不正侵入行為、及び関連する同行を監視及び観察する。対象とするテーマは、法制度、社会或いは政治的情勢、そして、新興テクノロジーにまで広げる。
CDI-CIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies.

このサービスには、サービス対象のシステムやネットワークのセキュリティに関連する情報を引用するような科学、テクノロジー、政治問題、そして政府関連の分野における、セキュリティのメーリングリスト、セキュリティのウェブサイト、そして、時事ニースと学術論文が含まれる。
This service involves reading security mailing lists, security Web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks.

このサービスの成果は、中期及び長期的なセキュリティ問題に着目したアナウンスメント、ガイドライン、或いは、提言（勧告）となるかもしれない。
The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues.

5.2.3 セキュリティ監査
Security Assessments

このサービスは、適用すべきその組織或いは他の業界標準によって定められた要求事項に基づき、組織のセキュリティインフラの詳細な検査及び分析を提供する。
This service provides a detailed review and analysis of an organization’s security infrastructure, based on the requirements defined by the organization or by other industry standards that apply.

5.2.4 セキュリティツールの構築
Development of Security Tools

CDI-CIRT は、サービス対象に対して、特有のツールの設定サンプル、或いは、メール、DNS 或いは、ウェブサーバのような広く使われるツールのセキュアな設定サンプルを提供することにより、セキュリティに関係するツールの設定を支援する。
CDI-CIRT helps its constituency to configure security-related tools by providing sample configuration of typical tools, or sample secure configuration of widely-used tools, like mail, DNS or web servers.

5.2.5 セキュリティ関連情報の展開
Security-Related Information Dissemination

このサービスは、サービス対象に対して、セキュリティ向上に役立つような、分かりやすく、かつ、見つけやすい収集情報を提供する。次のような情報が含まれる。
This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- CSIRT のための報告ガイドライン及び連絡先情報
  reporting guidelines and contact information for the CSIRT
- 注意喚起、警報、及び 他のアナウンスメントのアーカイブ
  archives of alerts, warnings, and other announcements

- 現在のベストプラクティスに関するドキュメント
  documentation about current best practices
- 一般的なコンピュータセキュリティガイダンス
  general computer security guidance
- ポリシー、プロシージャ、及び チェックリスト
  policies, procedures, and checklists
- パッチ開発および流通情報
  patch development and distribution information
- ベンダーのリンク情報
  vendor links
- インシデント報告に関する現在の統計と動向
  current statistics and trends in incident reporting
- 全体的なセキュリティ施策の向上につながる他の情報
  other information that can improve overall security practices

5.3 セキュリティ品質管理サービス
Security Quality Management Services

このサービスは CSIRT/CERT の専門性を活用したものであり、長期的な取り組みである。
These services leverage the CSIRT/CERT's expertise and focus on long-term issues.

5.3.1 リスク分析
Risk Analysis

CDI-CIRT は、リスク分析やアセスメントの付加価値を提供できる。
CDI-CIRT may be able to add value to risk analysis and assessments.

5.3.2 セキュリティコンサルタント
Security Consulting

CDI-CIRT は、事業継続における最善のセキュリティ施策にんするアドバイスやガイダンスを提供できる。
CDI-CIRT can provide advice and guidance on the best security practices to implement for constituents' business operations.

5.3.3 啓発向上
Awareness Building

CDI-CIRT は、ベストプラクティスの説明と事前注意に関するアドバイスを提供するために、必要と考えられる、記事、ニュースレター、及び、あらゆる情報源を通じて、サービス対象全体に対して、セキュリティ啓発を向上することを狙う。CDI-CIRT は、サービス対象者に最新の情報を提供するために、ミーティングやセミナーを開催することがある。
CDI-CIRT will aim to increase security awareness among its constituents population through articles, newsletters, and any information source deemed necessary, in order to explain security best practices and provide advice on precautions to take. CDI-CIRT can also schedule meetings and seminars to keep constituents up to date.

5.3.4 トレーニング
Training

CDI-CIRT は、ワークショップ、トレーニングコース、或いは、チュートリアルのようなセミナーを通じて、コンピュータセキュリティ問題に関する情報を提供する。
CDI-CIRT will provide information about computer security issues through seminars; workshops, courses, or tutorials.

5.3.5 製品評価或いは認証
Product Evaluation or Certification

CDI-CIRT は、プロダクトのセキュリティと、CDI-CIRT 或いは 組織的なセキュリティ施策に対する適合性を確認するために、ツール、アプリケーション、或いは その他のサービスにおけるプロダクト検証を実施する場合がある。
CDI-CIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CDI-CIRT or organizational security practices.

6. インシデント報告フォーム
Incident reporting form

可能な限り、インシデント報告フォームを使用してください。この文書の電子版は、CDI-CIRT のウェブサイト上にある。
As far as possible, please use the following Incident Reporting Form. An electronic version of the document can be found on CDI-CIRT's web site.

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

バージョン 1.2
version 1.2
2009 年 3 月
March 2009

CDI-CIRT インシデント報告フォーム
CDI-CIRT Incident Reporting Form

このフォームは、インシデント情報収集を容易にするように作成されました。もし、インシデントに巻き込まれたと思いました、可能な限り、以下のフォームをすべて埋めて、次のアドレスに送信してください。
The following form has been developed to ease gathering incident information. If you believe you have been involved in an incident, please complete - as much as possible - the following form, and send it to:

cirt@cyberdefense.jp

もし、メールを送信することができない場合は、次の番号に FAX してください。
If you are unable to send email, please fax it to:

+81-3-5209-4338

このフォームは、CERT/CC のインシデント報告フォーム バージョン 5.2 に準じています
This form is an adaptation of CERT/CC's incident reporting form, version 5.2.

報告者の連絡先及び組織情報について
Your contact and organizational information

1. 名前
   name.....:

2. 組織名
   organization name.....:

3. 事業分野の種別（銀行、教育、電力、自治体など）
   sector type (such as banking, education, energy or public safety).....:

4. E メールアドレス
   email address.....:

5. 電話番号
   telephone number.....:

6. その他
   other.....:

影響を受けたシステム（別々のホストに対する重複情報も可）
Affected Machine(s)
(duplicate for each host)

7. ホスト名と IP アドレス
   hostname and IP.....:

8. タイムゾーン
   timezone.....:

9. ホストの目的或いは役割（出来るだけ詳細にお願いします）
purpose or function of the host (please be as specific as possible).....:

攻撃元（別々のホストに対する重複情報も可）
Source(s) of the Attack
(duplicate for each host)

10. ホスト名と IP アドレス
hostname or IP.....:

11. タイムゾーン
timezone.....:

12. やり取りはありますか？
been in contact?.....:

インシデントについて（複数インシデントの重複情報も可）
Description of the incident (duplicate in case of multiple incidents)

13. 発生日時
dates.....:

14. 攻撃手段
methods of intrusion.....:
.....
.....

15. 関与しているツール
Tools involved.....:
.....
.....

16. ソフトウェアのバージョン
Software versions.....:
.....
.....

17. 浸入ツールの活動
Intruder tool output
.....
.....

18. 悪用された脆弱性
Vulnerabilities exploited
.....
.....

19. その他の関連情報
Other relevant information
.....
.....

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEAREIAAYFAknLI8cACgkQRv/zfla57bxGxACfeuxEJ5juZ09OLDNwRo0zZ7XH
60wAn2JVKhu2M0ceqAJHQ6d6NZlsrfBY
=JALJ
-----END PGP SIGNATURE-----

7. 免責条項
Disclaimer

資料、告知、注意喚起の準備には、あらゆる予防策が取られる。含まれる情報の使用によって生じる誤り、不作為、或いは損害に関して、CDI-CIRT は責任を負わない。
While every precaution will be taken in the preparation of information, notifications and alerts, CDI-CIRT assumes no responsibility for errors, omissions, or for damages resulting from the use of the information contained within.

8. 参考文献
Bibliography

Expectations for Computer Security Incident Response - IETF, RFC 2350, BCP21
June 1998
by Neville Brownlee and Erik Guttman
http://www.ietf.org/rfc/rfc2350.txt

Handbook for Computer Security Emergency Response Teams (CSIRTs) - CMU/SEI
2nd Edition, April 2003
by Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajcek
http://www.cert.org/archive/pdf/csirt-handbook.pdf