# 業務指示書

## ミャンマー国サイバーセキュリティにかかる情報収集・確認調査

第１　指示書の適用

本指示書は独立行政法人国際協力機構(JICA)（以下「機構」という。）が実施する標記業務のうち、民間コンサルタント等（以下「コンサルタント」という。）により実施する業務に関する内容を示すものです。コンサルタントはこの業務指示書及び貸与された資料に基づき、本件業務に係るプロポーザル等を機構に提出するものとします。

なお、本指示書の第２「業務の目的・内容に関する事項」、第３「業務実施上の条件」は、この内容に基づき、コンサルタントがその一部を補足又は改善し、プロポーザルを提出することを妨げるものではありません。

本指示書に係る質問期限：２０１５年６月３日　　１２時　まで

問合せ先：調達部契約第一課　　大野 忠伸　　Ono.Tadanobu@jica.go.jp

質問に対する回答：　２０１５年６月８日　までに機構ホームページ上に行います。

第２　業務の目的・内容に関する事項ーーーーー別紙のとおり

第３　業務実施上の条件ーーーーーーーーーーーーー別紙のとおり

第４　共同企業体の結成並びに補強の可否等

業務の規模が大きく、一社単独では望ましいレベルの業務従事者を確保することが困難であるか、又は業務の内容が広範にわたるため、業種又は分野ごと得意な社同士で共同企業体を結成することが望ましい案件について、競争を促進するために、必要最低限の範囲で共同企業体の結成を認める場合があります。

（各項目の（　）に○を付したものが、指示内容です。）

１　共同企業体の結成の可否

（　）認めません。

（　）認めます。

（○）認めます。ただし業務主任者（総括）は、共同企業体の代表者の者とします。

（　）　者までの共同企業体の結成を認めます。ただし業務主任者（総括）は、共同企業体の代表者の者とします。

（　）協力準備調査、その他先に行われた調査参加コンサルタント

は、構成員にはなれません。

注１）資格停止期間中のコンサルタントは、構成員になれません。
注２）共同企業体構成員との再委託契約は認めません。
注３）共同企業体の結成にあたっては、結成届をプロポーザルに添付し、プロポーザルに共同企業体結成の必要性を記載してください。

２　補強の可否

自社の経営者若しくは自社と雇用関係にある（原則、当該技術者の雇用保険や健康保険の事業主負担を行っている法人と当該技術者との関係をいう。複数の法人と雇用関係にある技術者の場合、主たる賃金を受ける雇用関係があるものをいう。）技術者の他業務従事状態から望ましいレベルの業務従事者を確保することが困難であるか、又は自社では確保が困難な担当分野である場合、自社と雇用関係のない技術者の「補強」を認める場合があります。

（各項目の（　）に○を付したものが、今回の指示内容です。）

（　）全ての業務従事者について、補強を認めません。

（○）以下の要件で、補強を認めます。

1）共同企業体でプロポーザルを提出する場合は、代表者及び構成員ともに、現地業務に従事するそれぞれの業務従事者数（通訳団員の配置を認める場合はそれらを除く）の１／２まで補強を認めます。

2）共同企業体を結成しない場合に限り、現地業務に従事する全業務従事者数（通訳団員の配置を認める場合はそれらを除く）の３／４まで補強を認めます。

【業務主任（総括）について】

（　）業務主任者（総括）については補強を認めません。

（○）業務主任者（総括）について補強を認めます。ただし、業務主任者が補強の場合には、副業務主任者（副総括）の配置は認めません。

【その他の業務従事者について】

（　）次の団員については補強を認めません。

（　）協力準備調査、その他先に行われた調査参加コンサルタント

からの補強は認めません。

注１）共同企業体を結成する場合、その代表者または構成員となる社は他社の補強になることは認めません。
注２）複数の社が同一の者を補強することは、これを妨げません。
注３）資格停止期間中のコンサルタントからの補強は認めません。
注４）評価対象業務従事者の補強にあたっては同意書をプロポーザルに添付してください。
　　評価対象外業務従事者については、契約交渉時若しくは補強を確定する際に同意書を提出してください。
注５）補強として参加している社との再委託契約は認めません。
注６）通訳については、補強を認めます。

3　外国籍人材の活用

（各項目の（　）に○を付したものが、今回の指示内容です。）

（　）外国籍人材の活用を認めます。

（○）業務主任者を除き、外国籍人材の活用を認めます。ただし、当該業務全体の業務従事者数及び業務従事人月のそれぞれ２分の１を超えない範囲において認めます。

（　）業務主任者を除き、外国籍人材の活用を認めます。ただし、当該業務全体の業務従事者数及び業務従事人月のそれぞれ４分の１を超えない範囲において認めます。

注）外国籍人材とは以下に該当する人材とします。
・プロポーザルを提出する法人に在籍する外国籍の人材で、常用の雇用関係を有するもの又は嘱託契約を締結しているもの
・プロポーザルを提出する法人の外部からの補強として当該業務に従事させる外国籍の人材。

第５　プロポーザルに記載されるべき事項

１　コンサルタントの経験、能力等

（１）類似業務の経験

（２）業務実施上のバックアップ体制等

（３）その他参考となる情報

注）類似業務：サイバーセキュリティ関連業務

２　業務の実施方針等

（１）業務実施の基本方針等

（２）業務実施の方法

（３）作業計画

（４）要員計画

（５）業務従事者毎の分担業務内容

（６）現地業務に必要な資機材

（７）実施設計・施工監理体制（無償資金協力を想定した協力準備調査の場合のみ）

（８）その他

注１）（１）と（２）を併せた記載分量は、 15ページ以下としてください。

注２）（４）要員計画について、評価対象外業務従事者の氏名及び所属先の記載は不要とし、契約交渉時、または遅くとも各業務従事者の作業開始時期までに双方で打合簿により確定するものとします。
なお、評価対象外業務従事者についての補強や外国籍人材の活用等については、契約交渉時、もしくは業務実施過程において、業務指示書で定める制限が遵守されていることを確認するものとします。

３　業務従事予定者の経験、能力等

業務にかかる総括責任者として、業務主任者（総括）を業務従事者の中から指名してください。なお、業務主任者に代えて、業務主任者と副業務主任者（副総括）を業務管理グループとして配置することを認める場合があります。

（１）業務管理グループ

業務主任者と副業務主任者の配置計画を併せて業務管理グループを提案する場合、その配置の考え方、両者の役割分担等の考え方等について記載願います

（各項目の（　）に○を付したものが、指示内容です。）

（○）業務管理グループ（副業務主任者の配置）を認めない。

（　）業務管理グループ（副業務主任者の配置）を認める（ただし、副業務主任者を補強とすることは認めない）。副業務主任者は 名を上限とする。

注）業務管理グループを認める全案件（業務指示書にて総括を1号以上としている案件を除く）においては、業務管理グループとしてシニア（46歳以上）と若手（35～45歳）が組んで応募する場合、３点の加点を行います。（「第９　プロポーザルの評価」参照）。

（２）評価対象業務従事者の経験、能力等

【業務主任者（業務主任／サイバー戦略）】

（業務管理グループにおける副業務主任者（副総括）も同様の項目）

１）類似業務の経験：サイバー戦略

２）対象国又は同類似地域：ミャンマー 及び全途上国での業務の経験

３）語学力（語学は認定書（写）を添付）：英語

4）業務主任者等としての経験
5）学歴、職歴、取得学位、資格、研修受講実績等（照査技術者については必要資格の認定書（写）を必ず添付して下さい。）
6）特記すべき類似業務の経験（類似職務経験を含む。）

【業務従事者：担当分野　セキュリティ対策計画】
1）類似業務の経験：セキュリティ対策計画
2）対象国又は同類似地域：ミャンマー 及び全途上国での業務の経験
3）語学力：語学評価せず
4）学歴、職歴、取得学位、資格、研修受講実績等（照査技術者については必要資格の認定書（写）を必ず添付して下さい。）
5）特記すべき類似業務の経験（類似職務経験を含む。）

【業務従事者2】

業務従事者は想定していません。

第６　プロポーザルの提出手続き等

１　プロポーザルの提出期限、提出場所、提出物
（１）期限：　2015年6月12日　　１２時
（２）場所：本機構本部１階　調達部受付
（３）提出物：プロポーザル　正１部　　写 ４部
　　見積もり　　正１部　　写 １部（次項第７参照）

２　プロポーザルの無効
次の各号のいずれかに該当するプロポーザルは無効とします。
（１）提出期限後にプロポーザルが提出されたとき
（２）提出されたプロポーザルに記名がないとき
（３）同一提案者から２通以上のプロポーザルが提出されたとき
（４）プロポーザル提出者（共同企業体構成員を含む）が全省庁統一資格結果通知書を取得していない、またはJICAの事前の資格審査を受けていないとき
（５）既に受注している案件、契約交渉中の案件及び選定結果未通知の案件と業務期間が重なって同一の業務従事者の配置が計画されているとき
（６）機構が定める「独立行政法人国際協力機構契約競争参加資格停止措置規程」（平成20年規程（調）第42号）に基づく資格停止を受けている期間中である者又は当該者が構成員となる共同企業体からプロポーザルが提出されたとき（なお、プロポーザルの提出後であっても本指示書第８．２による審査結果の通知前に資格停止を受けたものを含みます。）
（７）虚偽の内容が記載されているとき
（８）前号に掲げるほか、本指示書又はコンサルタント契約関連規程に違反したとき

第７　見積価格及び内訳書

本件業務を実施するのに必要な経費の見積り（消費税を含まない）及びその内訳書正１部と写１部を密封して、プロポーザルとともに提出して下さい。見積書の作成に当たっては「コンサルタント等契約における見積書作成ガイドライン」を参照してください。
（URL：http://www.jica.go.jp/announce/manual/guideline/consultant/quotation.html）

（各項目の（　）に○を付したものが、指示内容です。）

（各項目の（　）に○を付したものが、指示内容です。）

（　）本業務における一般業務費の見積りについては、定率化方式とし、一般業務比率の上限は、

（　）契約全体が複数の契約期間に分かれるため、各期間分及び全体分の見積りをそれぞれに作成して下さい。

（　）第２、第３で記載した事項のうち下記については、分けて見積って下さい。

（　）現地の治安状況が不安定であることから、業務従事者に対し、戦争保険（戦争危険担保特約）あるいはこれに相当する保険を付保することができます。付保する場合は、その経費を見積もって下さい。

（○）航空運賃及びエクセス料金については、別見積りとしてください。

航空運賃を見積る場合には、ZONE-PEX運賃を上限の単価として見積りを行って下さい。「業務実施契約等における正規割引航空運賃の利用について／通知(PR)第9-27004号」によりビジネスクラスの利用が認められる業務従事者の渡航については、ビジネスクラス正規割引運賃までを上限の単価として見積りを行ってください。

なお、実際の航空券の手配にあたっては、上記見積額を上限としつつも、業務実施上の必要による経路の変更、予約の変更等の必要な緊急時の対応も考慮しつつ、より効率的であるとともに経済的な航空券の手配に努めてください。

（　）航空運賃及びエクセス料金については、別見積りとしてください。

航空運賃を見積る場合には、エコノミークラス普通運賃と制限付エコノミークラス（Y2）を比較のうえ、より安価な運賃を上限の単価として見積りを行って下さい。「業務実施契約等における正規割引航空運賃の利用について／通知(PR)第9-27004号」によりビジネスクラスの利用が認められる業務従事者の渡航については、ビジネスクラスの正規運賃までを上限の単価として見積りを行って下さい。

注）外貨交換レートは以下のレートを使用して見積もってください。
（MMK1 = 0.112 円 , US$1 = 118.96 円 , EUR1 = 131.21 円）

第８　プレゼンテーション

プロポーザルを評価する上で、より効果的かつ適切な評価をおこなうために、業務主任者等から業務の実施方針等についてプレゼンテーションを求める場合があります。

（各項目の（　）に○を付したものが、指示内容です。）

（○）プレゼンテーションは実施しません。

（　）プロポーザル評価の一環として、以下の要領でプレゼンテーションを行っていただきます。その際、

（　）業務主任者がプレゼンテーションを行ってください。ただし、業務主任者以外に１名の出席を認めます。

（　）業務主任者又は副業務主任者、若しくは両者が共同してプレゼンテーションを行ってください。なお、業務主任者または副業務主任者のみがプレゼンテーションを行う場合は、業務主任者または副業務主任者以外に１名の出席を認めます。

（１）実施時期：　　～

（各社の時間は、プロポーザル提出後、別途指示します。）

（２）実施場所：独立行政法人国際協力機構　　会議室

（3）実施方法：

1）一社あたり最大、プレゼンテーション10分、質疑応答15分とします。

2）機材を使用する場合は、コンサルタント等が準備するものとし、プロポーザル提出時、使用機材リストを調達部契約第一課・第二課まで報告するものとします。

（以下、各項目の（ ）に○を付したものが、指示内容です。）

（ ）テレビ会議システムによる上記（2）の実施場所以外からの出席を認めません。

（ ）テレビ会議システムによる上記（2）の実施場所以外からの出席を認めます。その場合は、上記（2）の実施場所以外でのテレビ会議システムの準備はコンサルタント等が行うものとし、プロポーザル提出時、接続先等（接続先名、ISDN番号、使用機器のメーカー名・銘柄、担当者のアドレス・電話番号）を調達部契約第一課・第二課まで報告するものとします。

条件等は、以下のとおりです。

a）本邦以外の場所より、ISDN回線を用いてコンサルタント等からJICA-Netに接続し、指定された実施日時にテレビ会議実施が可能な場合は、認めます。

b）JICA在外事務所のJICA-Netを使用しての出席は認めません。ただしJICA在外事務所主管案件の場合は、当該主管事務所からの出席を認めます。

c）接続にかかる費用は、コンサルタント等の負担とします。ただしJICA在外事務所主管案件で、当該主管事務所より出席する場合は、この限りではありません。

## 第9　プロポーザルの評価

### 1　プロポーザルの評価基準

本件業務では別紙のプロポーザル評価表に従いプロポーザルの評価（技術評価）を行います。

業務管理グループにおける副業務主任者（副総括）は業務主任者（総括）と同様の項目・基準で評価を行います。

注）業務管理グループを認める全案件（業務指示書にて総括を1号以上としている案件を除く）においては、業務管理グループとしてシニア（46歳以上）と若手（35～45歳）が組んで応募する場合（どちらが総括でも可）、一律3点の加点（若手育成加点）を行います。なお、45歳以下でも上位格付認定により1号以上となる場合は「シニア」とみなし、「若手」と組んだ場合は加点対象とします。（年齢は当該年度（公示日の属する年度。再公示の場合は再公示日の属する年度。）4月1日時点での満年齢とします。）ただし、「1．コンサルタント等の法人としての経験・能力」、「2．業務の実施方針」、「3．業務従事予定者の経験能力」の合計が70点未満の場合は、加点は行いません。

技術評価及び若手育成加点の結果、各プロポーザル提出者の評価点について第1順位と第2順位以下との差が僅少である場合に限り、第7により提出された見積価格を参考として交渉順位を決定します。

具体的には、技術評価点及び若手育成加点の合計の差が第1位の者の点数の2.5%以内であれば、見積価格が最も低い者に価格点として最大2.5点を加点し、その他の者に最低見積価格との差に応じた価格点を加点します。

（1）評価対象とする業務従事者の担当分野

業務主任／サイバー戦略

セキュリティ対策計画

（2）評価対象とする業務従事者の予定人月数

5.00 M／M

### 2　評価結果の通知

提出されたプロポーザルは当機構で評価・選考の上、　２０１５年７月２日(木)　までにプロポーザルを特定し、各プロポーザル提出者に契約交渉順位を通知します。

3　評価結果の公表

評価結果については、以下の項目を機構ホームページに公開することとします。

（1）プロポーザルの提出者名

・契約交渉順第１位の者の名称のみを公開し、第２位以下の者の名称は非公開とする。

（2）プロポーザルの提出者の評価点

・以下の評価項目別小計及び合計点を公表する。

①コンサルタント等の法人としての経験・能力

②業務の実施方針等

③業務従事予定者の経験・能力

④若手育成加点＊

⑤価格点＊

＊④、⑤は該当する場合のみ（若手育成加点及び価格点については「第９ プロポーザルの評価１ プロポーザルの評価基準」参照）。

・基準点に達しない者については「基準下」とのみ記載する。

## 第１０　その他

1　配布・貸与資料

機構が配布・貸与した資料は、本件業務のプロポーザルを作成するためのみに使用することとし、複写又は他の目的のために転用等使用しないで下さい。

2　プロポーザルの報酬

プロポーザル及び見積書の作成、提出に対しては、報酬を支払いません。

3　プロポーザルの目的外不使用

プロポーザル及び見積書は、本件業務の契約交渉順位を決定し、また、契約交渉を行う目的以外に使用しません。

4　プロポーザルの返却

不採用となったプロポーザル（正）及び見積書（正）は、各プロポーザル提出者の要望があれば返却しますので選定結果通知後２週間以内に受け取りに来て下さい。また、不採用となったプロポーザルで提案された計画、手法は無断で使用しません。

5　虚偽のプロポーザル

プロポーザルに虚偽の記載をした場合には、プロポーザルを無効とするとともに、虚偽の記載をしたプロポーザル提出者に対して資格停止措置を行うことがあります。

6　プロポーザル作成に当たっての資料

プロポーザルの作成にあたっての参考情報は以下のとおりです。

（1）「プロポーザル作成ガイドライン」：

ＪＩＣＡホームページ「調達情報」中「調達ガイドライン、様式>>調達ガイドライン コンサルタント等の調達>>コンサルタント等契約におけるプロポーザル作成ガイドライン」

(URL: http://www.jica.go.jp/announce/manual/guideline/consultant/proposal.html)

(ハードコピーでの販売・配布は行っておりません)。

（2）業務実施契約に係る様式：

同上ホームページ「調達情報」中「調達ガイドライン、様式>>様式 コンサルタント等の調達 業務実施契約」

(URL：http://www.jica.go.jp/announce/manual/form/consul_g/index_since_201404.html)

（3）規程：
同上ホームページ「調達情報」中「調達ガイドライン、様式>>規程」
（URL：http://www.jica.go.jp/announce/manual/guideline/common/index.html）
（4）調達ガイドライン（コンサルタント等契約）：
同上ホームページ「調達情報」中「調達ガイドライン、様式>>調達ガイドライン コンサルタント等の調達」
（URL: http://www.jica.go.jp/announce/manual/guideline/consultant/index.html）

7　密接な関係にあると考えられる法人との契約に関する情報公開について

契約先に関する以下の情報を機構ホームページ上で以下のとおり公表することとしますので、本内容に同意の上で、プロポーザルの提出及び契約の締結を行っていただきますようご理解をお願いいたします。なお、案件へのプロポーザルの提出及び契約の締結をもって、本件公表に同意されたものとみなさせていただきます。

（1）公表の対象となる契約相手方取引先（共同企業体を結成する場合は共同企業体の構成員を含む。）
次のいずれにも該当する契約相手方を対象とします。
ア．当該契約の締結日において、当機構で役員を経験した者が再就職していること、又は当機構で課長相当職以上の職を経験した者が役員等(注)として再就職していること
注）役員等とは、役員のほか、相談役、顧問その他いかなる名称を有する者であるかを問わず、経営や業務運営について、助言することなどにより影響力を与え得ると認められる者を含みます。
イ．当機構との間の取引高が総売上又は事業収入の３分の１以上を占めていること

（2）公表する情報
契約ごとに、物品役務等の名称及び数量、契約締結日、契約相手方の氏名・住所、契約金額とあわせ、次に掲げる情報を公表します。
ア．対象となる再就職者の人数、再就職先での現在の職名、当機構での最終職名（氏名は公表しない。）
イ．契約相手方の直近の財務諸表における当機構との取引高
ウ．総売上高又は事業収入に占める当機構との間の取引割合
エ．一者応札又は応募である場合はその旨
（3）当機構の役職員経験者の有無の確認日
当該契約の締結日とします。
（4）情報の提供
契約締結日から1ヶ月以内に、所定の様式にて必要な情報を提供頂くことになります。

8　本体事業からの排除
以下、各項目の（　）に○を付したものが、指示内容です。）
（　）本件受注コンサルタント（ＪＶ構成員及び補強を含む。）は、本業務（協力準備調査）の結果に基づき当機構による無償資金協力が実施される場合は、設計・施工監理契約以外の役務及び財の調達から排除される（その場合は、受注コンサルタント等が製造、販売する資機材も排除される）見込みです。
（　）本件受注コンサルタント（ＪＶ構成員及び補強を含む。）及びその関連会社／系列会社（親会社を含む。）は、本業務（詳細設計）の結果に基づき当機構による有償資金協力が実施される場合は、施工監理業務（調達補助を含む。）以外の役務（審査、評価を含む。）及び財の調達から排除されます。

9　案件の延期又は中止について
治安の急変等により案件が延期又は中止になることがありますので、予めご留意ください。

以　上

# プロポーザル評価表
## ミャンマー国サイバーセキュリティにかかる情報収集・確認調査

| 評価項目 | 配点 | |
|---|---|---|
| 1．コンサルタント等の法人としての経験・能力 | (10.00) | |
| （1）類似業務の経験 | 6.00 | |
| （2）業務実施上のバックアップ体制等 | 4.00 | |
| 2．業務の実施方針等 | (30.00) | |
| （1）業務実施の基本方針の的確性 | 14.00 | |
| （2）業務実施の方法の具体性、現実性等 | 12.00 | |
| （3）要員計画等の妥当性 | 4.00 | |
| （4）その他（実施設計・施工監理体制） | | |
| 3．業務従事予定者の経験・能力 | (60.00) | |
| （1）業務主任者の経験・能力／業務管理グループの評価<br>（本案件では副業務主任者の配置（業務管理グループ）を認めません。） | (40.00) | |
| | 業務主任者のみ | 業務管理グループ |
| ①業務主任者の経験・能力　業務主任／サイバー戦略 | (40.00) | (　　) |
| ア）類似業務の経験 | 16.00 | |
| イ）対象国又は同類似地域での業務経験 | 4.00 | |
| ウ）語学力 | 6.00 | |
| エ）業務主任者等としての経験 | 8.00 | |
| オ）その他学位、資格等 | 6.00 | |
| ②副業務主任者 | (　－　) | (　　) |
| カ）類似業務の経験 | － | |
| キ）対象国又は同類似地域での業務経験 | － | |
| ク）語学力 | － | |
| ケ）業務主任者等としての経験 | － | |
| コ）その他学位、資格等 | － | |
| ③体制、プレゼンテーション | (　　) | (　　) |
| サ）業務主任者等によるプレゼンテーション | | |
| シ）業務管理体制　（今回は評価の対象としません） | － | |
| （2）業務従事者の経験・能力：セキュリティ対策計画 | (20.00) | |
| ア）類似業務の経験 | 14.00 | |
| イ）対象国又は同類似地域での業務経験 | 2.00 | |
| ウ）語学力 | | |
| エ）その他学位、資格等 | 4.00 | |
| （3）業務従事者の経験・能力： | (　　) | |
| ア）類似業務の経験 | | |
| イ）対象国又は同類似地域での業務経験 | | |
| ウ）語学力 | | |
| エ）その他学位、資格等 | | |
| （4）業務従事者の経験・能力： | (　　) | |
| ア）類似業務の経験 | | |
| イ）対象国又は同類似地域での業務経験 | | |
| ウ）語学力 | | |
| エ）その他学位、資格等 | | |
| （5）業務従事者の経験・能力： | (　　) | |
| ア）類似業務の経験 | | |
| イ）対象国又は同類似地域での業務経験 | | |
| ウ）語学力 | | |
| エ）その他学位、資格等 | | |
| 総合評点 | [100.00] | |

## 第２　業務の目的・内容に関する事項

### １．業務の背景

インターネットの急激な普及に伴い、サイバーセキュリティに関する対策の必要性は日増しに高まっている。特に、政府機関や民間企業などを標的とした、不正なウェブサイト改ざん、機密情報の外部流出、重要システム強制停止等を行うサイバー攻撃による被害事例が国際的に増加している。わが国においても 2011 年に重工業企業など防衛・インフラ関連産業や衆参両院、中央省庁が相次いでサイバー攻撃を受けていたことが発覚し、政府として官民情報連携強化などによるサイバーセキュリティ対策の強化に乗り出している。

わが国は、2008 年日・ASEAN 経済大臣会合「アジア知識経済化イニシアティブ」及び 2009 年より継続実施中の「日 ASEAN 情報セキュリティ政策会議」の枠組みにおいて、我が国およびミャンマーを含む ASEAN における安心安全な情報通信技術（以下、「ICT」という。）利用環境の構築に向けた取り組みを実施している。ミャンマーにおいては、情報通信については主に、通信・情報技術省（以下、「MCIT」という。）が主管しており、MCIT は 2014 年よりアジア開発銀行の協力をうけ、ミャンマー電子政府マスタープランの作成を進めており、電子政府の利用環境としてもミャンマー国内におけるサイバーセキュリティ対策についての重要性認識が向上してきている。

係る状況において、ミャンマー政府は 2010 年にサイバーセキュリティ対策の情報収集、対策支援、各種調整機関としてミャンマーComputer Emergency Response Team（以下「mmCERT」という。）を設立した。2013 年にはサイバーセキュリティの推進機構として国家サイバーセキュリティ運営委員会を設立し、同国のサイバーセキュリティ対策の強化に取り組んできた。さらに、2015 年 4 月に新たにミャンマー政府内のサイバーセキュリティ対策を一手に担うべく IT サイバーセキュリティ局が通信・情報技術省配下に設立された。

一方で、サイバーセキュリティ分野については、法令、組織、人材育成等のバランスのとれた強化、および、官民双方の協力が不可欠であるが、ミャンマー政府のサイバーセキュリティに係る包括的な戦略、政府組織間や官民の役割整理、現状の対策整備状況、および強化方針が明確となっていない。

今後、ミャンマーがサイバーセキュリティ向上に取り組むに際し、対応を強化すべき事項や優先度を整理し、わが国による支援可能な分野を明らかにする必要がある。そのため、同国のサイバーセキュリティに係る包括的な基礎情報の収集を目的とし、本件調査を実施する。

### ２．業務の概要

（１）調査の目的

ミャンマーのサイバーセキュリティについて、サイバーセキュリティに係る戦略、政策、関連官庁および民間企業等のサイバーセキュリティ対策の現状、当該分野の課題等について情報を収集・確認するとともに、サイバーセキュリティに係る協力ニーズを把握・分析した上で、わが国 ODA による支援内容の方向性を確認することを目的とする。

（２）調査の対象
ミャンマー国　ネピドー、ヤンゴン

（３）本邦主要関係機関
NISC、JPCERT/CC

（４）相手国主要関係機関
通信・情報技術省（MCIT）、郵便電気通信局（PTD）、ミャンマー郵電公社（MPT）、IT サイバーセキュリティ局、mmCERT、科学技術省（MOST）、教育省（MOE）、ミャンマーコンピューター開発委員会、国家サイバーセキュリティ運営委員会、ミャンマーコンピューター連盟

## ３．業務の範囲

本業務は、「２．（１）調査の目的」を達成するため、「４．実施方針及び留意事項」を踏まえつつ、「５．業務の内容」に示す事項の調査を行い、「６．成果品等」に示す報告書等を作成し、JICA に提出する。

## ４．実施方針及び留意事項

（１）本調査の目的に係るミャンマー関係機関への説明
本調査の目的等については、JICA が予めミャンマー政府に対して説明、調整を行う。コンサルタントは同説明・調整内容に基づき、調査を行うこと。

（２）調査内容等の確認プロセス
本調査は、JICA 社会基盤・平和構築部や JICA ミャンマー事務所と意見交換を十分に行いながら進めるものとする。特に以下の段階において、JICA 関係者が出席する会議を開催し、内容を確認することとする。

１）インセプション・レポート作成時（JICA 社会基盤・平和構築部）
２）現地調査開始時
（JICA ミャンマー事務所、在ミャンマー日本大使館及びミャンマー国政府関係者）
３）現地調査終了時
（JICA ミャンマー事務所、在ミャンマー日本大使館及ミャンマー国政府関係者、JICA 社会基盤・平和構築部（TV 会議にて参加を想定））
４）ドラフト・ファイナル・レポート作成時（JICA 社会基盤・平和構築部）
５）ファイナル・レポート作成時（JICA 社会基盤・平和構築部）

（３）本邦関係機関とのアポイントメント
本調査の実施に際し、本邦関係機関へのヒアリングも想定するが、必要なア

ポイントメントの取り付けは、原則コンサルタントが行うことを前提とする。

（４）相手国関係機関とのアポイントメント

本調査の実施に際し、相手国関係機関との必要なアポイントメントの取り付けは、原則コンサルタントが行うことを前提とするが、JICA ミャンマー事務所は、ミャンマー情報通信省等その他の関係諸機関へ調査内容・実施スケジュールを通知し、調査協力を依頼するとともに、必要に応じ、各機関との初回のアポイントメント取り付けを行い、円滑な調査実施のための協力を行う。

（５）民間企業に対する調査

ミャンマー民間企業に関する調査はミャンマーコンピューター連盟を通じ調査するものとするが、コンサルタントにてミャンマー現地企業への調査協力の取り付けが可能である場合には、調査対象案として提案すること。

２社以上を対象に日系ミャンマー進出民間企業へのヒアリングを行うことを想定しており、必要なアポイントメントの取り付けは原則コンサルタントが行うことを前提とする。

（６）セキュリティアセスメント及び脆弱性診断の対象

セキュリティアセスメントの対象は省庁内の１組織（MCIT 内の組織を想定）を対象とする。また脆弱性診断の対象は、電子行政システム及び政府系 WEB サイトの各々１システムを対象とする。現地調査前にミャンマー政府と評価対象確定に係る調整、確認が必要となるため、想定される事前、現地、事後の先方作業（ヒアリング対応や情報提供、ソフトウェアのインストール等）、および評価に必要となる確認期間等は提案にて提示すること。

（７）想定される支援内容及びその前提

情報通信セクターに係る現状、相手国の要望、事業規模等を踏まえ、適切な支援内容を検討すること。また、ミャンマーは ICT 分野に係る基礎的なインフラ（電気、通信設備等）にも課題があるため、協力内容の検討に際し、前提となるインフラ整備等がある場合には当該前提条件についても検討すること。

（８）支援内容の範囲

先方のサイバーセキュリティに関する要望の全てをわが国 ODA により支援することは困難なことから、先方要望を踏まえ、重要度や緊急性、維持管理能力等を確認の上、適切な協力範囲を検討すること。また、支援内容の範囲は ODA による支援のみならず、政策レベルの連携案から、裾野レベルの支援案についても検討の範囲とする。

（９）開発課題との関連およびわが国の優位性

支援内容については、当該支援による裨益が想定される組織、開発課題についても検討を行うこととする。また支援内容に関し、わが国独自の優位性の有無についても検討すること。

## ６．業務の内容

### （１）本邦関連機関の活動内容の確認

NISC、JPCERT/CC 等にヒアリングを行い、相手国関係機関と実施しているサイバーセキュリティに関する現状の取組状況、及び課題を確認する。

### （２）インセプション・レポートの作成

ミャンマーにおける、ICT 分野の基礎情報、およびサイバーセキュリティに関連する政策、ガイドライン、関連組織、人材育成等の現状について、文献情報を中心に収集・分析・検討を行い、調査の全体像を把握した上で、調査の基本方針、方法、工程、手順、実施スケジュール、実施体制、要員計画等を含むインセプション・レポート及び質問票（英文）を作成する。

### （３）インセプション・レポートの説明・協議

JICA が派遣する調査団員と協力し、インセプション・レポート（調査方針、調査計画、便宜供与依頼事項等）を先方政府関係者に説明し、調査の協力を依頼するとともに、内容を協議・確認する。

### （４）情報通信分野基礎情報の調査

基礎的な ICT 関連情報の収集を行う。

１）一般情報

人口、人口密度、面積、GNI などの一般的な基礎情報。

２）インターネット関連データ

利用者数、利用者層、伝送方式、接続形態、利用場所、料金、頻度など。

３）サイバーセキュリティ関連の事例・統計情報

ウィルス感染率、被害、インシデント等の概況（事件、被害、手法、トレンド）、統計など。

４）インターネットの利用状況

電子行政手続き、電子商取引、ゲーム、SNS、チャット　等

### （５）サイバーセキュリティに関する現状調査

ミャンマーのサイバーセキュリティに関する現状の取組状況、および将来の計画について詳細な調査を行う。

１）サイバーセキュリティに関連する組織

サイバーセキュリティに関連する省庁や組織、その役割、人員、予算規模などに関する情報を収集する。役割については、法令制定、ガイドライン制定、危機管理、規制、法執行、標準認定・監査、資格認定、研究開発、技術者育成、普及啓発、国際連携など、どの組織が何をスコープに活動しているかを明らかにすること。

（以下の項目の括弧内の例は、日本の場合の組織例）

・政府組織（例：NISC、総務省、経済産業省、防衛省、NPA　等）
・政府に準じる組織（例：IPA、JPCERT/CC、JIPDEC　等）
・業界団体等（例：Telecom-ISAC Japan, JNSA, 重要インフラセプター 等）

・民間企業（国内、外資（コンサルティング、ソフトウェア、機器））
・研究機関（例： NICT　等）
・教育機関（例：情報セキュリティ大学院大学　等）
・政府機関 ICT の構築・管理組織（各省庁の情報システム室、CSIRT、ベンダー 等）

2）サイバーセキュリティ戦略、政策、法令、ガイドライン

サイバーセキュリティに係る戦略、政策、法令、ガイドラインに関する情報を収集し、策定状況と予算規模、政策の強制力、政府の関与度などを調査する。

また、国家開発計画における位置づけや、セキュリティ関連標準やガイドライン策定等に関して国際連携等の取組状況を確認する。

3）重要 ICT システムおよび関連設備

ミャンマー政府が重要と考える構築済、および構築が予定されている ICT システム、およびデータセンター、電子認証基盤等の関連設備に関する情報を収集し、その概要、運用状況、設置拠点、責任組織等を調査する。

4）サイバーセキュリティに関する人材育成

セキュリティに関する技術者育成機関、技術者育成制度、普及啓発活動等に関する情報を収集する。

・技術者養成機関
・人材発掘イベント
・資格認定制度
・政府関係者、企業向け普及啓発活動
・一般利用者向け普及啓発活動（学校教育における情報倫理教育を含む）

5）政府のセキュリティ対策実施機関の活動状況

mmCERT、各省庁の CSIRT 及び、情報システム室等のセキュリティ対策、インシデント対応を行う組織の活動状況、現状の課題、今後の計画、予算状況、支援ニーズ等について情報を収集する。

また、電子行政システムの構築および運用する組織（各省庁の情報システム室、委託先ベンダー等）に関し、システム構築、および運用の体制、システム改修に係る手続き、実施しているセキュリティ対策、現状の課題等について情報を収集する。

6）政府機関の ICT 環境に係るセキュリティアセスメント

関連省庁の１つの組織に対し、ICT 環境についてのセキュリティアセスメントを行う。なお、アセスメントの対象となる項目は下記を含むことを想定しているが、詳細な評価項目、およびアセスメントに際し必要となる情報等については提案において提示すること。

・セキュリティ対策に対する予算規模
・セキュリティポリシー、運用ルール（ISMS、個人情報保護、PC 持出管理、BCP 等）
・エスカレーションルール（インシデントに対する窓口、報告ルール 等）

・セキュリティ対策における人員体制
・コンプライアンス、社員・職員の教育
・情報セキュリティに対する意識
・技術的な対策（異常検知、ファイアウォール、IDS/IPS、DDoS 対策、WAF、WEB Proxy、障害対策、DLP、マルウェア[1]対策、ウィルス対策ソフト 等）

7）政府機関の電子行政システムの脆弱性診断

政府機関の運用している主要な電子行政システムの１つに対して脆弱性診断を行う。なお、脆弱性診断の対象となる項目や、診断に際し必要となる情報等については提案において提示すること。

8）政府機関の WEB サイトの脆弱性診断

政府機関の公開している主要な WEB サイトの１つに対して脆弱性診断を行う。なお、脆弱性診断の対象となる項目や、診断に際し必要となる資料等については提案において提示すること。

また、mmCERT が WEB サイトの脆弱性診断を実施しているため、mmCERT による脆弱性診断の結果がある場合には、合わせて情報を収集し、その内容を確認する。

9）政府機関データセンターの評価

政府機関の所有する主要なデータセンター１つについて評価を行う。なお、評価基準や、評価に際して必要となる情報等については提案において提示すること。

10）その他セキュリティ対策関連設備

政府の保有設備として、電子認証基盤等のセキュリティ対策にかかる設備がある場合には、当該設備の整備状況、サービス・運用、事業継続計画等について情報を収集する。

11）通信事業者のセキュリティ対策

通信事業者のインターネット事業に係るセキュリティガイドラインの有無、セキュリティ対策、運用状況、および事業継続計画等について情報を収集する。
・バックボーン（国際ゲートウェイ、国内基幹網、Internet Exchange）
・アクセスライン、通信局（ファイバー、ADSL、無線等）
・通信設備（通信サービス基盤、NOC、セキュリティ対策機器）

12）中央銀行システムのセキュリティ対策

中央銀行システムに係る、金融機関向けを含むセキュリティガイドラインの有無、セキュリティ対策、運用状況、および事業継続計画等について情報を収集する。また、中央銀行システムの利用に係る ICT 環境やセキュリティ対策についても、関連技術協力プロジェクト等へのヒアリングを通じ可能な限り確認

[1] マルウェア：不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアやコードの総称。Sandbox、パケット監視等の対策がある。

を行う。
・基幹決済系システム
・情報系システム（基幹系以外のシステム）
・オフィス ICT

13）民間企業の動向、ニーズ

現地民間企業および日系ミャンマー進出企業におけるセキュリティ対策状況やニーズ、および民間企業向けセキュリティ関連ビジネスの普及状況を調査する。

**（６）サイバーセキュリティ分野における他国政府・ドナーとの連携・支援**

サイバーセキュリティ分野に係る、他国政府・ドナーからの支援や、脅威やインシデント情報のリアルタイム共有等　連携して進めているプロジェクトなどの情報を収集する。

**（７）他 ASEAN 諸国との状況比較**

調査結果を基に、ミャンマーにおけるサイバーセキュリティに係る対策状況を整理し、「ASEAN 諸国における情報セキュリティ情報収集・確認調査報告書」（2012 年）等の文献情報に基に、他 ASEAN 諸国とのサイバーセキュリティ対策状況の比較を行い、ASEAN 諸国内におけるミャンマーのサイバーセキュリティ対策レベルを確認する。

**（８）サイバーセキュリティに関する課題・対策の検討**

調査結果を基に、ミャンマーにおけるサイバーセキュリティに係る課題、および課題に対する対策を検討する。課題については、以下の項目に留意して検討を行うこと。

・サイバーセキュリティ戦略、法制度、ガイドライン、規制
・サイバーセキュリティ関連機関、体制、予算措置
・政府機関の ICT 環境（ポリシー、組織・体制、技術的対策、運用状況　等）
・重要インフラ設備環境（特に通信事業者、金融機関）
・民間企業の ICT 環境（ポリシー、組織・体制、技術的対策、運用状況　等）
・技術者育成・発掘
・啓発活動

**（９）わが国による支援の内容、および優先項目に係る検討及び提言**

上記（８）およびサイバーセキュリティに係る技術的な特性を踏まえ、わが国による支援の内容、および優先される重点項目を検討し、ロードマップとして整理する。なお、支援内容の検討にあたり、先方政府の要望は踏まえるものの合意の必要はない。

検討の範囲としては、わが国 ODA による協力支援のみならず、政策レベルの連携案から、裾野レベルの支援案（例：国民への啓発活動や、日本推進する取り組み（PRACTICE、JASPER、TSUBAME）等）、および、民間企業の進出等の可能性までを含むものとする。

ODA による協力が望まれる範囲においては、支援により裨益が想定される組織、

開発課題、および支援におけるわが国独自の優位性の有無についても検討を行う。
また、わが国 ODA によるサイバーセキュリティ支援のあり方について、気付きの点、留意すべき点があれば提言として整理する。

(10) ドラフト・ファイナル・レポートの作成

上記の調査・分析・検討結果をドラフト・ファイナル・レポートに取りまとめ、JICA 社会基盤・平和構築部に提出・説明する。

(11) ファイナル・レポートの作成

JICA 各関係者からのコメントを受けて、ドラフト・ファイナル・レポートを修正した上、これをファイナル・レポートとして取りまとめ、JICA 社会基盤・平和構築部に提出・説明する。

## ６．成果品等

次の報告書・成果品を JICA 社会基盤・平和構築部に提出する。なお、以下に示す部数は、JICA へ提出する部数であり、会議等に必要な部数は別途用意すること。最終成果品は、ファイナル・レポートとする。

ファイナル・レポートについては製本することとし、その他の報告書等は簡易製本とする。報告書等の印刷、電子化（ＣＤ－Ｒ）の仕様については、「コンサルタント等契約における報告書の印刷・電子媒体に関するガイドライン」 を参照すること。

（１）報告書

１）インセプション・レポート

記載事項：調査・検討の基本方針、方法、項目、作業計画、要員計画等
提出時期：2015 年 8 月下旬
部数：英文 15 部　和文 10 部（簡易製本）、電子データ

２）ドラフト・ファイナル・レポート

記載事項：調査・検討項目を網羅した調査報告のドラフト
提出時期：2015 年 10 月下旬
部数：英文 8 部　和文 8 部（簡易製本）、電子データ

（２）成果品

１）ファイナル・レポート

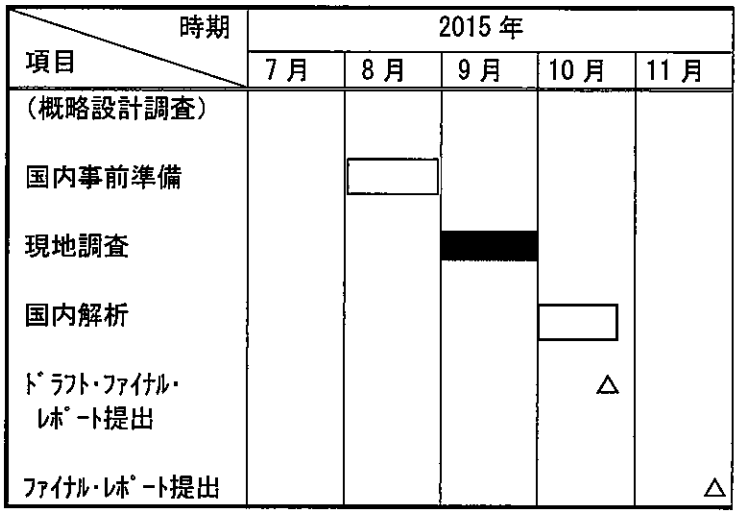
記載事項：調査・検討項目を網羅した調査報告の最終版
（セキュリティアセスメント、脆弱性診断、データセンター評価の詳細結果、および実施時に取得した資料も成果品に含む）
提出時期：2015 年 11 月下旬
部数：英文 10 部 和文 10 部（製本）
英文ＣＤ－Ｒ 3 枚　和文ＣＤ－Ｒ 3 枚

## 第３　業務実施上の条件

### １．業務工程計画

2015 年 9 月上旬より第 1 回現地調査を実施することを想定する。同年 10 月下旬にドラフト・ファイナル・レポートを作成し、同年 11 月下旬までにファイナル・レポートを作成・提出する。

業務内容を考慮のうえ、より適切な工程計画がある場合、プロポーザルにて提案すること。




### ２．業務量の目途と業務従事者の構成（案）

**（１）業務量の目途**

約 7.6 M/M

**（２）業務従事者の構成（案）**

本業務には、以下に示す分野を担当する専門家の配置を想定するが、業務内容及び業務工程を考慮のうえ、より適切な業務従事者構成がある場合、プロポーザルにて提案すること。なお、記載の格付けは目安であり、以下の格付けを超えた格付けの提案も認める。但し、目安を超える格付けの提案を行う場合は、その理由及び人件費を含めた事業費全体の経費節減の工夫をプロポーザルに明記すること。

1）業務主任/サイバー戦略（2 号）
2）セキュリティ対策計画(3 号)
3）セキュリティアセスメント
4）脆弱性診断
5）データセンター評価

**（３）通訳**

本調査には通訳の配置は想定していない。ただし、調査にあたり現地語による対話が必要と想定される場合には、現地での通訳傭上も必要に応じ認める。通訳傭上を希望する場合は、必要経費をプロポーザルに記載するとともに見積りに含

めること。

## ３．参考資料

### （１）貸与資料

以下の資料をJICA社会基盤・平和構築部（担当：古川）03-5226-8129から貸与可能。

・ASEAN諸国における情報セキュリティ情報収集・確認調査報告書（2012年）

### （２）閲覧資料

以下の資料をJICA社会基盤・平和構築部（担当：古川）03-5226-8129において閲覧可能

・ミャンマーからの無償資金協力「Security Operation Center Project」の正式要請書

### （３）参考

・国際電気通信連合（ITU）によるICTに関する各種調査結果
URL：http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

・mmCERTによる各種報告資料
URL：http://www.mmcert.org.mm/node/26

## ４．JICAからの参加団員の構成と現地調査行程（案）

JICAからの調査参加については以下のとおり想定している。

### （１）現地調査

１）団員構成：総括
　　計画管理

２）調査行程：約7日間

３）目的：
相手国関係機関との協議及び現地調査を通じ、調査の目的・方針等を始めとした双方の合意事項などに関するミニッツを取りまとめる。

## ５．機材

本調査では、コンサルタントが調達する機材は特に想定していないが、現地調査に機材が必要な場合は、プロポーザルに記載するとともに見積りに含めること。

## ６．現地再委託

本調査において現地再委託は想定していないが、現地再委託が適当と思える業務がある場合には、その内容についてプロポーザルにて提案した上で、当該業務について経験・知見を豊富に有する機関・コンサルタント・ＮＧＯ等に再委託して実施することを認める。

現地再委託にあたっては、「コンサルタント等契約における現地再委託契約手続きガイドライン」（2012年4月）に則り選定及び契約を行うこととし、委託業者の業務遂行に関しては、現地において適切な監督、指示を行うこと。プロポーザルでは、

可能な範囲で、現地再委託対象業務の実施方法と契約手続き（見積書による価格比較、入札等）、価格競争に参加を想定している現地業者の候補者名並びに現地再委託業務の監督・成果品の検査の方法等、具体的な提案を行うこと。

また、現地再委託にかかる費用についてはプロポーザルに記載するとともに見積りに含めること。

## 7．その他留意事項

### （1）業務主任の総括団員への同行

現地調査に関し、業務主任は総括団員の滞在期間中に原則として総括団員の調査に同行することとするが、その他の団員は業務の効率を考慮し、別行動にて調査実施することを妨げない。

### （2）ビザ取得およびミャンマー内移動許可

現地調査に必要なビザ取得のための招聘状発出およびミャンマー内の移動許可にかかる手続きはJICAにて支援する。

### （3）安全管理

現地作業期間中は安全管理に十分留意する。当地の治安状況については、JICAミャンマー事務所などにおいて十分な情報収集を行うとともに、現地作業時の安全確保のための関係諸機関に対する協力依頼及び調整作業を十分に行う。また、同支所と常時連絡がとれる体制とし、特に地方にて活動を行う場合は、当地の治安状況、移動手段等については同事務所及び支所と緊密に連絡をとるよう留意する。また、現地作業中における安全管理体制をプロポーザルに記載する。

### （4）不正腐敗の防止

本調査の実施にあたっては、「JICA不正腐敗防止ガイダンス（2014年10月）」の趣旨を念頭に業務を行うこと。なお、疑義事項が生じた場合は、不正腐敗情報相談窓口またはJICA担当者に速やかに相談するものとする。

以上

# 略語表

| 略語 | 英語 | 日本語訳 |
|---|---|---|
| ADSL | Asymmetric Digital Subscriber Line | 上り(アップリンク)と下り(ダウンリンク)の速度が非対称(Asymmetric)な高速デジタル有線通信技術 |
| BCP | Business Continuity Plan | 事業継続計画 |
| CERT | Computer Emergency Response Team | コンピュータ緊急対応チーム |
| CSIRT | Computer Security Incident Response Team | コンピュータセキュリティインシデント対応チーム |
| DDoS | Distributed Denial of Service attack | 第三者のマシンに攻撃プログラムを仕掛けて踏み台にし、その踏み台とした多数のマシンから標的とするマシンに大量のパケットを同時に送信する攻撃 |
| DLP | Data Loss Prevention | 情報漏えい防止システム及び対策 |
| GNI | Gross National Income | 国民総所得 |
| ICT | Information Communication Technology | 情報通信技術 |
| IDS/IPS | Intrusion Detection Systems/Intrusion Prevention Systems | 不正侵入検知システム、不正侵入防止システム |
| IPA | Information-technology Promotion Agency, Japan | 独立行政法人　情報処理推進機構 |
| ISMS | Information Security Management System | 情報セキュリティマネジメントシステム、セキュリティ対策の国際標準の一つ |
| JASPER | Japan-ASEAN Security Partnership | ASEAN各国向けのセキュリティ対策に関する総合的な技術協力プロジェクト |
| JIPDEC | Japan Information Processing Development Center | 一般財団法人　日本情報経済社会推進協会 |
| JNSA | Japan Network Security | 特定非営利活動法人　日本ネットワークセキュリティ協会 |
| JPCERT/CC | Japan Computer Emergency Response Team Coordination Center | 日本コンピュータ緊急対応チーム<br>各国CERTと連携し、日本のサイバーセキュリティ対策の情報収集、対策支援、各種調整を実施 |
| MCIT | Ministry of Communications & Information Technology | 通信・情報技術省 |
| mmCERT | Myanmar Computer Emergency Response Team | ミャンマーコンピュータ緊急対応チーム |
| MOE | Minister of Education | 教育省 |
| MOST | Ministry of Science and | 科学技術省 |
| MPT | Myanmar Posts and Telecommunications | ミャンマー郵電公社 |
| NICT | National Institute of Information and Communications Technology | 国立研究開発法人　情報通信研究機構 |
| NISC | National center of Incident readiness and Strategy for Cyber | 内閣サイバーセキュリティセンター |
| NOC | Network Operation Center | ネットワークオペレーションセンター |
| NPA | National Police Agency | 警察庁 |
| ODA | Official Development Assistance | 政府開発援助 |
| PDT | Post and Telecommunications Department | 郵便電気通信局 |
| PRACTICE | Proactive Response Against Cyber-attacks Through International Collaborative | サイバー攻撃予知即応プロジェクト |
| SNS | Social Networking Service | ソーシャルネットワークサービス(Facebook等) |
| TSUBAME | TSUBAME Project | アジア・太平洋地域インターネット定点観測可視化プロジェクト |
| WAF | Web Application Firewall | WEBサイト改ざん防止システム |