



AWS EC2 のインストールの前提条件

この章は次のトピックで構成されています。

- [概要](#) (1 ページ)
- [Amazon EC2 設定](#) (1 ページ)
- [ホスト VM の要件](#) (4 ページ)
- [TCP および UDP ポートの要件](#) (10 ページ)
- [IP アドレスの制限](#) (15 ページ)
- [サポートされる Web ブラウザ](#) (17 ページ)

概要

この章では、各 Crosswork コンポーネントをインストールするための一般的な前提条件（VM 要件、ポート要件、アプリケーション要件など）およびプラットフォーム固有の前提条件について説明します。

他の統合コンポーネントまたはアプリケーション（WAE、DHCP、TFTP サーバーなど）の運用に必要なデータセンターリソースについては、このドキュメントでは取り上げていません。詳細については、各コンポーネントのインストールマニュアルを参照してください。

Amazon EC2 設定

このセクションでは、Amazon EC2 に Crosswork Network Controller をインストールする際に構成する必要がある設定について説明します。

Crosswork は、Amazon Elastic Compute Cloud (EC2) に展開できます。Amazon EC2 は、Crosswork アプリケーションをホストするためにクラウドでコンピューティングリソースを提供する Web サービスです。

Crosswork は、CloudFormation (CF) テンプレートを使用して Amazon EC2 に展開されます。CloudFormation プロセスは、クラスタを構築する手動の手順よりも高速でエラーが発生しにくいですが、クラスタの展開の詳細を含む CloudFormation テンプレートを準備するために必要なスキルを持っている必要があります。

Crosswork とそのコンポーネントを AWS 環境にインストールするには、次の前提条件を確認して満たす必要があります。



注目 このセクションで説明する要件のほとんどは AWS の概念であり、Crosswork だけが課すものではありません。

表 1: AWS 前提条件と設定

要件	説明
VPC とサブネット	<p>仮想プライベートクラウド (VPC) は、Crosswork インターフェイス (管理、データ) および Crosswork Data Gateway (管理、データ、デバイス) インターフェイスの専用サブネットで作成および構成されます。</p> <p>すべてのサブネット間で直接 IP 接続が必要です。</p>
エンドポイント	<p>次のパラメータを使用して、VPC にエンドポイントが作成されます。</p> <ul style="list-style-type: none"> • サービス名 : 展開するリージョン (可用性ゾーン) の EC2 サービス。 • プライベート DNS 名 : 有効 • エンドポイントタイプ : インターフェイス • [サブネット (Subnets)]で、インストールに使用する予定の管理サブネットを指定します。Crosswork VM と Crosswork Data Gateway VM に異なる管理サブネットを使用している場合は、両方の管理サブネットを指定して、エンドポイントが両方のサブネットにアクセスできるようにしてください。 <p>重要 インターフェイスのサブネットは、ネットワークロードバランサ (NLB) と競合しないようにする必要があります。</p> <p>エンドポイントの設定方法については、AWS のドキュメントを参照してください。</p>
IAM ロール	<p>Identity and Access Management (IAM) で、関連する権限ポリシーを使用してロールが作成されます。IAM ロールは、短期間有効なログイン情報を持つ、特定の権限を持つ ID です。信頼するエンティティがロールを引き受けることができます。</p> <p>(注)</p> <ul style="list-style-type: none"> • Crosswork ロールに必要な最小限の権限は、ec2:DescribeNetworkInterfaces、ec2:AssignPrivateIpAddresses、および ec2:UnassignPrivateIpAddresses です。 • ロールの信頼ポリシーには、"Action": "sts:AssumeRole" 条件が必要です。

要件	説明
キーペア	キーペア（VM へのログインに使用される秘密キー）が作成および構成されます。
配置グループ	<p>クラスタ戦略の配置グループが作成されます。</p> <p>クラスタ配置グループでは、インスタンスは単一の可用性ゾーンに論理的にグループ化され、ネットワーク遅延が短く、ネットワークのスループットが高いというメリットがあります。</p> <p>この要件は、Crosswork クラスタインスタンスを起動する場合にのみ必要です。</p>
IP アドレス	<p>Crosswork クラスタ：単一の NIC を使用する場合、展開されるノード（ハイブリッドまたはワーカー）ごとに1つの IP アドレス（IPv4 または IPv6）と、仮想 IP（VIP）アドレスとして使用される1つの追加の IP アドレスが必要です。デュアル NIC を使用する場合（1つは管理ネットワーク用、もう1つはデータネットワーク用）、展開される各ノード（ハイブリッドまたはワーカー）の管理およびデータ IP アドレス（IPv4 または IPv6）と、管理およびデータ仮想 IP（VIP）アドレスとして使用される2つの追加 IP アドレスが必要です。</p> <p>たとえば、単一の NIC を備えた3つの VM クラスタの場合は4つの IP アドレスが必要であり、デュアル NIC を備えた3つの VM クラスタの場合は8つの IP アドレス（管理ネットワーク用に4つ、データネットワーク用に4つ）が必要です。</p> <p>Crosswork Data Gateway：管理トラフィックとデータトラフィック専用の IP アドレス。デバイス アクセス トラフィックの IP アドレスは、『Cisco Crosswork Network Controller 5.0 Administration Guide』の「Create a Crosswork Data Gateway Pool」のセクションで説明されているように、Crosswork Data Gateway プールの作成時に割り当てられます。</p> <ul style="list-style-type: none"> IP アドレスは、Cisco Crosswork Data Gateway がインストールされるネットワークのゲートウェイアドレスに到達できる必要があります。到達できない場合、インストールは失敗します。 この時点では、IP の割り当ては永続的であり、再展開しない限り変更できません。詳細については、シスコ カスタマー エクスペリエンス チームにお問い合わせください。
セキュリティグループ	許可するポートまたはトラフィックを指定するには、セキュリティグループを作成して構成する必要があります。

要件	説明
インスタンスタイプ	<p>インスタンス展開のリソースプロファイル。AWS インスタンスタイプは、「導入の計画」に記載されている VM リソースとネットワーク要件に準拠するように選択する必要があります。</p> <ul style="list-style-type: none"> • Crosswork クラスタ : <ul style="list-style-type: none"> • デモまたはラボ用の展開には、m5.4xlarge を選択します。 • 実稼働の展開には m5.8xlarge を選択します。 • Crosswork Data Gateway (実稼働およびラボ用展開) : <ul style="list-style-type: none"> • 標準 : m5.4xlarge を選択 • 拡張 : m5.8xlarge を選択
CloudFormation (CF) テンプレート	<p>インストール中にアップロードする必要がある Crosswork コンポーネントの CF テンプレート (.yaml) ファイル。詳細については、CF テンプレート画像の抽出を参照してください。</p>
Route53DomainName	Route53 DNS ホストゾーン用に構成されたドメイン名。
ユーザーデータ	手動インストール手順中に指定する必要がある VM 固有のパラメータスクリプト。
ホストゾーン ID	<p>ホストゾーン ID には、ドメイン名 (Route53DomainName) を指定する必要があります。</p> <p>ネットワークロードバランサ (NLB) の展開には、事前定義された Route53 ホストゾーンが必要です。</p>

ホスト VM の要件

このセクションでは、Crosswork クラスタと Crosswork Data Gateway を展開するための VM ごとのリソース要件について説明します。

- [Crosswork クラスタ VM の要件](#)
- [Crosswork Data Gateway VM の要件](#)

Crosswork クラスタ VM の要件

Crosswork クラスタは、ハイブリッド構成で動作する 3 つの VM またはノードで構成されます。これは、標準的なネットワークでアプリケーションをサポートするために必要な最小限の設定です。必要に応じて、ネットワークの要件に合わせて、または他のアプリケーションの導入に

合わせて、後でワーカー構成に VM やノード（最大2つのワーカーノード）を追加して展開を拡張できます（各 Crosswork Network Controller パッケージの VM 数についての詳細は表 1 を参照）。お客様のニーズに最適な展開に関するガイダンスについては、シスコのカスタマーエクスペリエンス チームにお問い合わせください。

次の表は、VM ホストごとのネットワーク要件を説明しています。

表 2: ネットワーク要件 (VM ごと)

要件	説明
ネットワーク接続	<p>実稼働環境への展開では、管理ネットワーク用とデータネットワーク用のデュアルインターフェイスを使用することを推奨します。</p> <p>最適なパフォーマンスを得るには、管理ネットワークとデータネットワークでは 10 Gbps 以上で設定されたリンクを使用する必要があります。</p>
NTP サーバー	<p>使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体で Crosswork アプリケーションの VM クロック、デバイス、クライアント、およびサーバーを同期するために使用するものと同じ NTP サーバーである必要があります。</p> <p>インストールを試行する前に、NTP サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。</p>
DNS サーバー	<p>使用する DNS サーバーの IPv4 または IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバーと同じである必要があります。</p> <p>インストールを試みる前に、DNS サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。</p>
DNS 検索ドメイン	<p>DNS サーバーで使用する検索ドメイン (cisco.com など)。検索ドメインは 1 つのみ設定できます。</p>
バックアップ サーバ	<p>Cisco Crosswork は、SCP を使用して、システムの設定を外部サーバーにバックアップします。SCP サーバーのストレージ要件は若干異なりますが、少なくとも 50 GB のストレージが必要です。</p>

- Cisco Crosswork インフラストラクチャおよびアプリケーションは、Kubernetes によって管理されるコンテナの分散型集合体として動作するように構築されています。コンテナの数は、アプリケーションが追加または削除されると変わります。
- Crosswork プラットフォーム インフラストラクチャでは、デュアルスタック構成はサポートされていません。したがって、環境のアドレスはすべて IPv4 または IPv6 のいずれかである必要があります。

Crosswork Data Gateway VM の要件

ここでは、Crosswork Data Gateway をインストールするための一般的なガイドラインと最小要件について説明します。

- [Crosswork Data Gateway の展開タイプの選択](#) (6 ページ)
- [Crosswork Data Gateway VM の要件](#) (6 ページ)

Crosswork Data Gateway の展開タイプの選択

次の表に、各 Crosswork 製品に Crosswork Data Gateway をインストールするために使用する必要がある展開プロファイルのリストを示します。



- (注) Crosswork Data Gateway の VM リソース要件はタイプごとに異なり、変更することはできません。したがって、要件が変わった場合は、Crosswork Data Gateway を再展開して、あるタイプから別のタイプに移動する必要があります。詳細については、『[Cisco Crosswork Network Controller 5.0 Administration Guide](#)』の「[Redeploy a Crosswork Data Gateway VM](#)」のトピックを参照してください。

表 3: Crosswork Data Gateway の展開タイプ

Cisco Crosswork 製品	Crosswork Data Gateway の展開
Crosswork Network Controller (Crosswork Active Topology と Crosswork Optimization Engine の組み合わせ)	オンプレミス標準
Crosswork 最適化エンジン	オンプレミス標準
Crosswork ゼロタッチプロビジョニング	オンプレミス標準
Crosswork Change Automation	オンプレミス拡張
Crosswork Health Insights	オンプレミス拡張
Crosswork Service Health	オンプレミス拡張

Crosswork Data Gateway VM の要件

Crosswork Data Gateway の VM の要件を次の表に示します。

表 4: オンプレミス アプリケーションの *Crosswork Data Gateway* 要件

要件	説明
データセンター	VMware 「 VMware vCenter のインストールの前提条件 」を参照してください。

要件	説明			
インターフェイス	最小値：1 最大値：3 Cisco Crosswork Data Gateway は、次の組み合わせに応じて、1 つ、2 つ、および 3 つのインターフェイスのいずれかで展開できます。			
	(注) Crosswork クラスタで 1 つのインターフェイスを使用する場合は、Crosswork Data Gateway で 1 つのインターフェイスのみを使用する必要があります。Crosswork クラスタで 2 つのインターフェイスを使用する場合は、ネットワークの要件に応じて、Crosswork Data Gateway で 2 つまたは 3 つのインターフェイスを使用できます。			
	NIC の数	vNIC0	vNIC1	vNIC2
	1	<ul style="list-style-type: none"> 管理トラフィック 制御/データトラフィック デバイス アクセストラフィック 	—	—
	2	管理トラフィック	<ul style="list-style-type: none"> 制御/データトラフィック デバイスアクセストラフィック 	—
3	管理トラフィック	制御/データトラフィック	デバイス アクセストラフィック	

要件	説明
	<ul style="list-style-type: none"> • 管理トラフィック：インタラクティブコンソールにアクセスする場合、およびサーバー間で制御/データ情報を渡す場合に使用されます（たとえば、Crosswork アプリケーションから Crosswork Data Gateway）。 • 制御/データトラフィック：Cisco Crosswork Data Gateway と Crosswork アプリケーション、および他の外部データ接続先間でデータと設定を転送します。 • デバイス アクセス トラフィック：デバイスにアクセスする場合、およびデータを収集する場合に使用されます。 <p>(注) セキュリティポリシーにより、他の vNIC で受信された vNIC のサブネットからのトラフィックはドロップされます。たとえば、3 vNIC モデル設定では、すべてのデバイス トラフィック（着信および発信）がデフォルトの vNIC2 経由でルーティングされる必要があります。Crosswork Data Gateway は、vNIC0 および vNIC1 経由で受信されたデバイス トラフィックをドロップします。</p>
IP アドレス	<p>使用するインターフェイスの数に基づいて、1つまたは2つの IPv4/IPv6 アドレス。</p> <p>仮想 IP (VIP) アドレスとして使用する 1つの追加 IP アドレス。アクティブなデータゲートウェイごとに、一意の VIP が必要です。</p> <p>詳細については、表 1の「Interfaces」のセクションを参照してください。</p> <p>(注) Crosswork はデュアルスタック構成をサポートしていません。したがって、環境のすべてのアドレスは IPv4 または IPv6 である必要があります。</p> <p>3-NIC 展開では、インストール時に管理インターフェイス (vNIC0) および制御/データインターフェイス (vNIC1) の IP アドレスを指定する必要があります。デバイス アクセス トラフィック (vNIC2) の仮想 IP アドレスは、『Cisco Crosswork Network Controller 5.0 Administration Guide』の「Create a Crosswork Data Gateway Pool」のセクションで説明されているように、Crosswork Data Gateway プールの作成時に割り当てられます。</p>

要件	説明
NTP サーバー	<p>使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体でデバイス、クライアント、およびサーバを同期するために使用する NTP サーバと同じでなければなりません。NTP IP アドレスまたはホスト名がネットワーク上で到達可能であることを確認します。到達可能でない場合、インストールは失敗します。</p> <p>また、Crosswork アプリケーションと Cisco Crosswork Data Gateway VM を実行する ESXi ホストには NTP が設定されている必要があります。そうでない場合、最初のハンドシェイクが「certificate not valid」エラーで失敗する可能性があります。</p>
DNS サーバー	<p>使用する DNS サーバーの IPv4 または IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバーと同じである必要があります。インストールを試みる前に、DNS サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。</p>
DNS 検索ドメイン	<p>DNS サーバーで使用する検索ドメイン (cisco.com など)。検索ドメインは 1 つのみ設定できます。</p>

TCP および UDP ポートの要件

Crosswork クラスタポートの要件

次の TCP および UDP のポート番号は、データセンター管理者が展開した外部ファイアウォールまたはアクセスリストのルールを通過できるようにする必要があります。NIC の展開によっては、これらのポートが一方のみの、または両方の NIC に適用される場合があります。



(注) Crosswork クラスタポートにより、双方向の情報フローが可能になります。

表 5: Crosswork クラスタが使用する外部ポート

ポート	プロトコル	用途
22	TCP	リモート SSH トラフィック
111	TCP/UDP	GlusterFS (ポートマッパー)
179	TCP	Calico BGP (Kubernetes)
80、443	TCP	EC2 API へのアクセス。

ポート	プロトコル	用途
500	UDP	IPSec
2379/2380	TCP	Kubernetes etcd
4500	UDP	IPSec
6443	TCP	kube-apiserver (Kubernetes)
9100	TCP	Kubernetes メタモニタリング
10250	TCP	kubelet (Kubernetes)
24007	TCP	GlusterFS
30603	TCP	ユーザーインターフェイス (NGINX サーバーはポート 443 でセキュア接続をリッスンします)
30606	TCP	Docker レジストリ
30621	TCP	FTP 用 (データインターフェイスでのみ使用可能)。ファイル転送に使用される追加ポートは、31121 (TCP)、31122 (TCP)、および 31123 (TCP) です。 このポートは、サポート対象アプリケーションが Cisco Crosswork にインストールされ、FTP 設定が有効になっている場合にのみ使用できます。
30622	TCP	SFTP 用 (データインターフェイスでのみ使用可能)。 このポートは、サポート対象アプリケーションが Cisco Crosswork にインストールされ、SFTP 設定が有効になっている場合にのみ使用できます。
49152:49370	TCP	GlusterFS

表 6: 他の Crosswork コンポーネントが使用するポート

ポート	プロトコル	用途
30602	TCP	インストールのモニタリング用 (Crosswork Network Controller)
30603	TCP	Crosswork Network Controller Web ユーザーインターフェイス (NGINX サーバーはポート 443 でセキュア接続をリッスンします)
30604	TCP	NGINX サーバーのクラシック ゼロ タッチ プロビジョニング (クラシック ZTP) に使用されます。

ポート	プロトコル	用途
30607	TCP	Crosswork Data Gateway のバイタルコレクション
30608	TCP	Data Gateway VM を使用した Data Gateway gRPC チャンネル
30609	TCP	Expression Orchestrator (Crosswork Service Health) によって使用されます。
30610	TCP	Metric Scheduler (Crosswork Service Health) によって使用されます。
30611	TCP	Expression Tracker コンポーネント (Crosswork Service Health) によって使用されます。
30617	TCP	ZTP サーバーのセキュアゼロタッチプロビジョニング (セキュア ZTP) に使用されます。
30620	TCP	ZTP サーバーでプラグアンドプレイ HTTP トラフィックを受信するために使用されます。
30649	TCP	Crosswork Data Gateway の収集ステータスを設定およびモニターします。
30650	TCP	Data Gateway VM で実行されている astack-client を含む astack gRPC チャンネル
30993、30994、30995	TCP	収集されたデータを Crosswork Kafka の接続先に送信する Crosswork Data Gateway。

表 7: Crosswork クラスタが使用する宛先ポート

ポート	プロトコル	用途
7	TCP/UDP	ICMP を使用したエンドポイントの検出。
22	TCP	管理対象デバイスとの SSH 接続の開始。
53	TCP/UDP	DNS への接続
123	UDP	ネットワーク タイム プロトコル (NTP)
830	TCP	NETCONF の開始
2022	TCP	Crosswork と Cisco NSO 間の通信に使用されます (NETCONF の場合)。
8080	TCP	REST API から SR-PCE へ

ポート	プロトコル	用途
8888	TCP	Crosswork と Cisco NSO 間の通信に使用されます (HTTPS の場合)。
20243	TCP	DLM と Cisco NSO 間の通信用に DLM 機能パックによって使用されます。
20244	TCP	Cisco NSO でパッケージのリロードシナリオ中に DLM 機能パックリスナーを内部的に管理するために使用されます。

Crosswork Data Gateway ポート要件

次の表に、Crosswork Data Gateway が正常に動作するために必要なポートの最小セットを示します。

インバウンド：Crosswork Data Gateway は指定されたポートでリスンします。

アウトバウンド：Crosswork Data Gateway は、指定されたポートの外部宛先 IP に接続します。

表 8: 管理トラフィック用に開くポート

ポート	プロトコル	用途	方向
22	TCP	SSH サーバ	着信
22	TCP	SCP クライアント	発信
123	UDP	NTP クライアント	発信
53	UDP	DNS Client	発信
30607	TCP	Crosswork コントローラ	発信



(注) SCP ポートは調整できます。

表 9: デバイス アクセス トラフィック用に開くポート

ポート	プロトコル	用途	方向
161	UDP	SNMP コレクタ	発信

ポート	プロトコル	用途	方向
1062	UDP	SNMP トラップコレクタ (注) これはデフォルト値です。この値は、インストール後に Cisco Crosswork UI から変更できます。詳細については「 Configure Crosswork Data Gateway Global Parameters 」を参照してください。	着信
9010	TCP	MDT コレクタ	着信
22	TCP	CLI コレクタ	発信
6514	TLS	syslog コレクタ	着信
9898	TCP	これはデフォルト値です。この値は、インストール後に Cisco Crosswork UI から変更できます。詳細については「 Configure Crosswork Data Gateway Global Parameters 」を参照してください。	
9514	UDP		

ポート	プロトコル	用途	方向
サイト特定 デフォルトポートは、ベンダーによって XR、XE とは異なります。プラットフォーム固有のマニュアルを確認します。	TCP	gNMI コレクタ	発信

表 10: 制御/データトラフィック用に開くポート

ポート	プロトコル	用途	方向
30649	TCP	Crosswork コントローラ	発信
30993 30994 30995	TCP	Crosswork Kafka	発信
サイト特定	サイト特定	Kafka と gRPC の接続先	発信

IP アドレスの制限

Crosswork クラスタでは、内部通信に次の IP 範囲が使用されます。これは変更できません。そのため、これらのサブネットは、ネットワーク内のデバイスやその他の目的のために使用できません。

Crosswork クラスタを分離して、すべての通信がクラスタ内にとどまるようにすることをお勧めします。また、アドレス空間が、外部統合ポイント（デバイスへの接続、Crosswork がデータを送信する先の外部サーバーへの接続、NSO サーバーへの接続など）と重複していないことも確認してください。



(注) これは、クラスタのインストールとスタティックルートの追加に適用されます。

表 11: 保護された IP サブネット

IP タイプ	サブネット	備考
IPv4	172.17.0.0/16	Docker サブネット (インフラストラクチャ)
	169.254.0.0/16	リンク ローカルアドレス ブロック
	127.0.0.0/8	ループバックアドレス
	192.88.99.0/24	予約済み。以前はリレーサーバーが IPv6 over IPv4 を実行するために使用されました
	240.0.0.0/4	将来の使用のために予約済み (以前はクラス E ブロック)
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	現在のネットワーク、送信元アドレスとしてのみ有効
IPv6	2001:db8:1::/64	Docker サブネット (インフラストラクチャ)
	fdfb:85ef:26ff::/48	ポッドサブネット (インフラストラクチャ)
	fd08:2eef:c2ee::/110	サービスサブネット (インフラストラクチャ)
	::1/128	ループバックアドレス
	fe80::/10	リンク ローカル
	ff00::/8	IPv6 マルチキャスト
	2002::/16	予約済み。以前はリレーサーバーが IPv6 over IPv4 を実行するために使用されました
	2001:0000::/32	Terredo トンネルとリレー
	2001:20::/28	ORCHID で使用され、IPv6 ではルーティング不可です
	100::/64	破棄プレフィックス。Crosswork ゼロタッチプロビジョニングに適用されない特定のユースケースで使用されます
	::/128	未指定のアドレス。ホストに割り当てることはできません
	::ffff:0:0/96	IPv4 マッピングされたアドレス
	::ffff:0:0:0/96	IPv4 変換されたアドレス

サポートされる Web ブラウザ

インフラストラクチャのインストール後に Crosswork UI にアクセスするには、検証済みのブラウザのいずれかを使用することをお勧めします。

表 12: サポートされる Web ブラウザ

ブラウザ	バージョン
Google Chrome (推奨)	92 以降
Mozilla Firefox	70 以降

推奨される表示解像度は 1600 x 900 ピクセル以上（最小：1366 x 768）です。

サポートされているブラウザを使用することに加えて、Crosswork アプリケーション内の地理的マップにアクセスするすべてのクライアントデスクトップは、[mapbox.com](https://www.mapbox.com) のサイトにアクセスする必要があります。Cisco Crosswork が外部サイトにアクセスすることを望まないお客様は、マップファイルをローカルにインストールすることを選択できます。

次に行う作業：

以下のインストールワークフローに戻ります。[AWS EC2 への Cisco Crosswork Network Controller のインストール](#)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。