図 1-5-b 国家サイバーインテリジェンスの全体像

サイバーインテリジェンスの策定範囲を図 1-5-c に示す。オープン・ソース・インテリジェンスにあたる部分は当然であるが、さらに日本ならではのクローズド・ソース・インテリジェンスまでが策定範囲である。

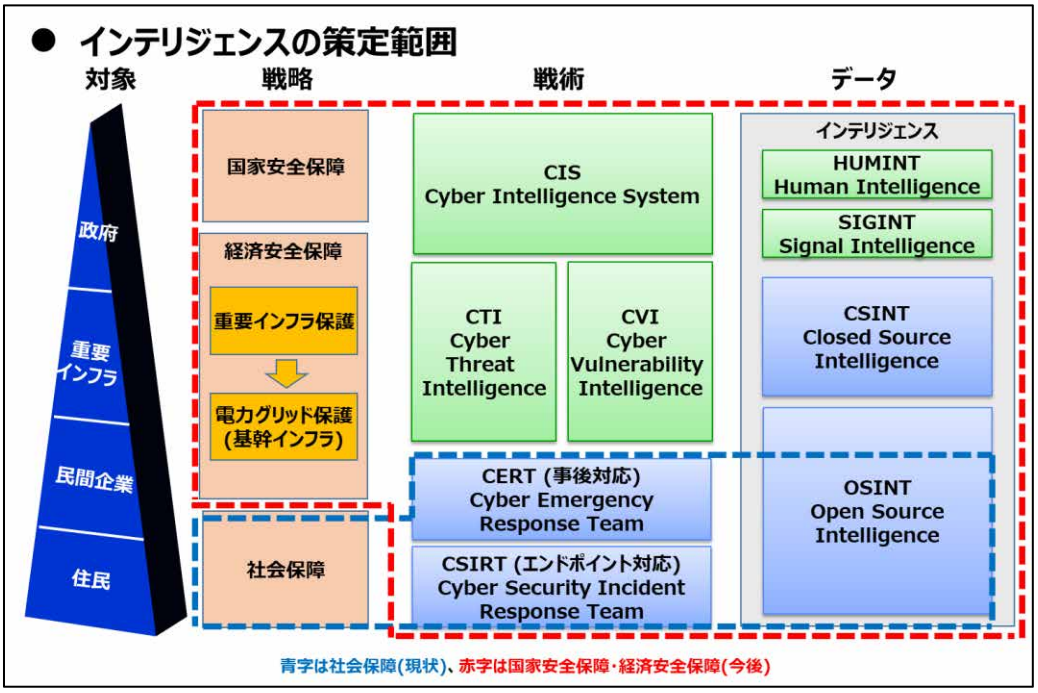

図 1-5-c サイバーインテリジェンスの策定範囲

サイバーインテリジェンスシステムが果たす機能の全体を図 1-5-d に示す。インテリジェンスを活用しての、政策提言、国際連携、安全保障の調査・分析の機能を持つべきである。

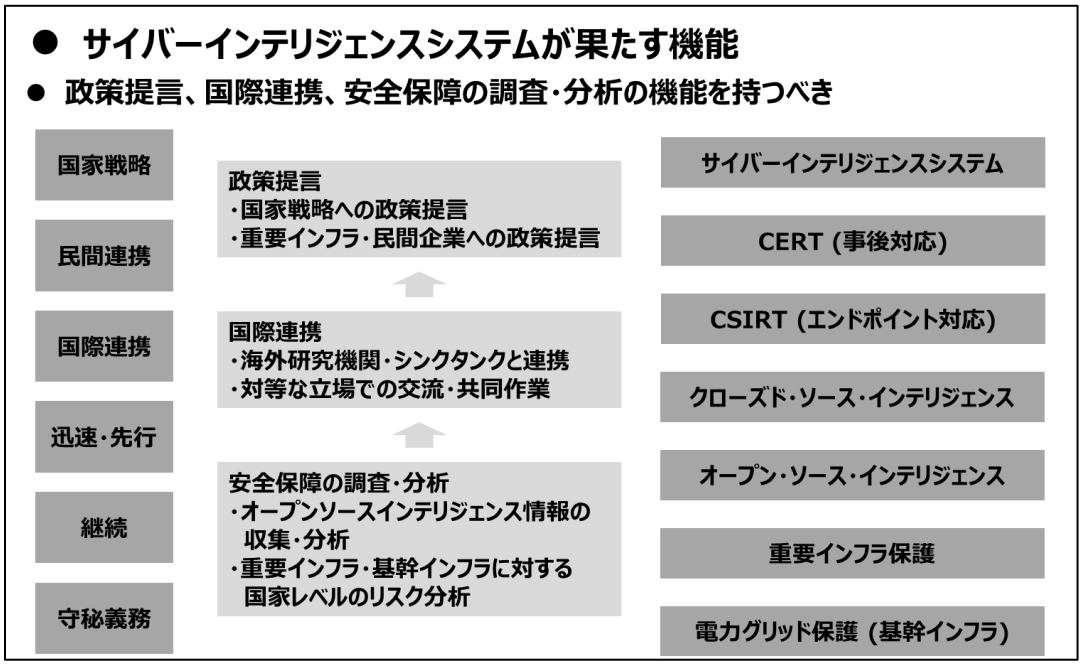

図 1-5-d サイバーインテリジェンスシステムが果たす機能

第２章 サイバーインテリジェンスシステム

第１節 システムの全体像

国家サイバーインテリジェンスの「政府」の階層にあたる、国家サイバーインテリジェンスセンターの全体像を図 2-1-a に示す。国家サイバーインテリジェンスセンターは、「セキュリティクリアランス」「コントロールプレーン」「データプレーン」の３つの階層で構成される。

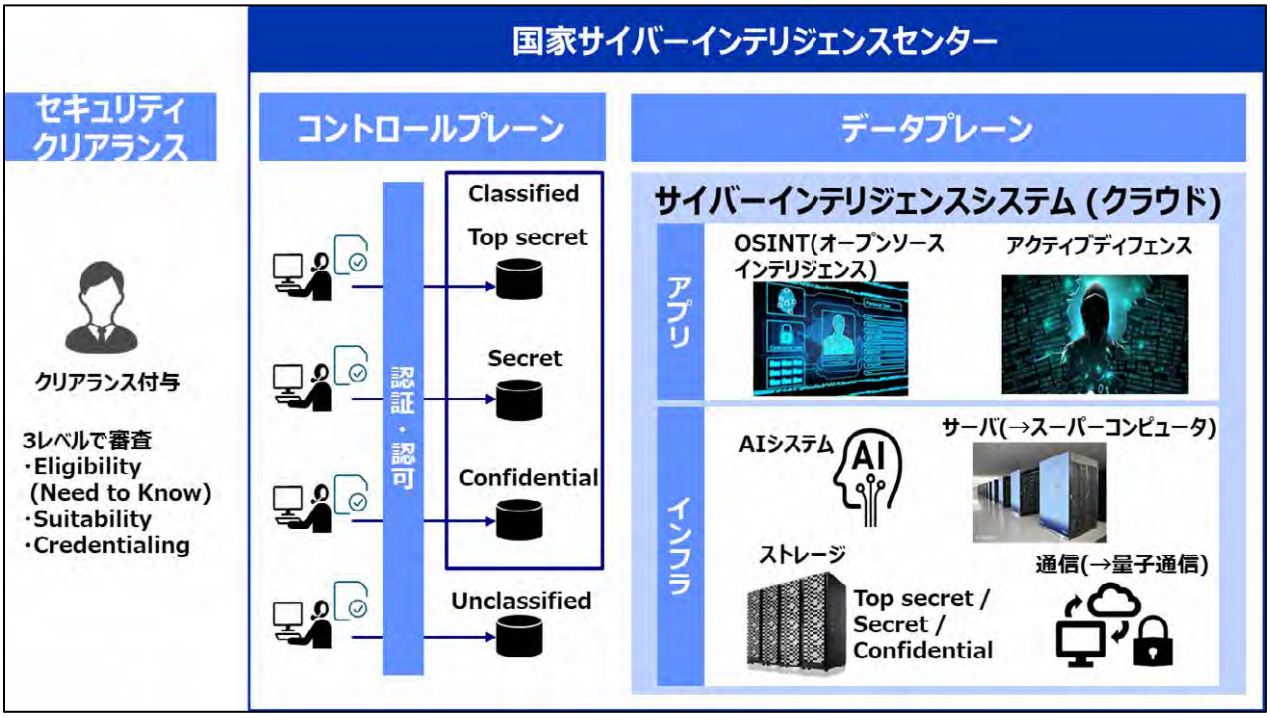

図 2-1-a 国家サイバーインテリジェンスセンターの概要

「セキュリティクリアランス」では、国家サイバーインテリジェンスを扱う権限のある者に適切に権限を与えるとともに、Need to Know の原則にしたがい必要に応じて機密情報を共有すべき人物であることを特定する。セキュリティクリアランスの付与のための審査は、厳格性（Eligibility, Need to Know）、適切性（Suitability）、クレデンシャル付保（Credentialing）のすべての手順を行うことで実施する。とくにクレデンシャル付与では、耐タンパ機能を備えた可搬性のある IC カードなどに、当該人物を物理的およびサイバー的に一意に識別するための情報（多くの場合は X.509 証明書）を格納して、当該人物だけが所有するような形で渡すものである。

「コントロールプレーン」では、クリアランスを与えられた者が、物理的およびサイバー的に認証され、必要なデータにアクセスするための、識別・認証・認可を適用する基盤である。本プレーンは、当該人物が与えられたデジタルアイデンティティのもとに、トップシークレット、シークレット、コンフィデンシャル、

アンクラシファイドの情報にアクセスするための基盤を構成する。

「データプレーン」では、サイバーインテリジェンスシステムを構成し、多くの場合にはクラウドサービスとして提供する。サイバーインテリジェンスシステムは、アプリケーション層とインフラ層とから構成される。アプリケーション層は、サイバーインテリジェンスを、広く流通する OSINT（オープンソースインテリジェンス）から収集し分析するとともに、もし国家がサイバー攻撃を受けた際に攻撃者を特定し反撃可能な能力を示すための、アクティブディフェンスも担う。また、インフラ層は、民間で広く使われるクラウドサービスに比べてさらに「AI システム」「サーバー（スーパーコンピュータ）」「ストレージ」「通信（量子通信）」を備えるものである。

サイバーインテリジェンスシステムの機能および開発項目を以下に示す。

- サイバースレットインテリジェンス（Cyber Threat Intelligence, CTI）
  - データ収集
  - キュレーションと重複排除
  - 機械学習
  - データのエンリッチメント(優先順位つけ)
  - 関連付けと統合
  - 形式(容易に取り込めるような)
  - インテリジェンスレポートと分析

- サイバーバルネラビリティインテリジェンス（Cyber Vulnerability Intelligence, CVI）
  - 倫理的ハッカー(人材管理)
  - ペネトレーション・テスト
  - 脆弱性スキャン
  - バグ・バウンティ(報奨の仕組み)
  - 組織的な脆弱性開示
  - 敵対的レッドチーム(運用)
  - セキュリティ・コントロール評価(適切な実装の確認)
  - セキュリティコードレビュー(ソフトウェアを対象)

- アトリビューション
  - サイバーヒューミント(AI 活用)
  - 犯行自白誘導
  - 犯罪情報の露呈誘導
  - 侵入分析(犯罪グループの証跡)
  - 痕跡からの犯罪者特定
  - データの収集

- クラスタリング
- 動機・意図の特定
- 結果公開

第２節 データプレーン

1. アプリケーション

サイバーインテリジェンスシステムは、2 大インテリジェンスとして CTI と CVI を扱う。

CTI とは、サイバー脅威に関わるインテリジェンスである（図 2-2-a）。CTI が効果的であるとは、「敵に関する情報」「技術環境」「関連性」の共通部分に焦点をあててアクションを施すことである。CTI を形成するには、商用プロバイダのデータソースや、政府系プロバイダーのデータソースからデータを収集し、生データ、処理データ、分析データへと次第にインテリジェンスを濃縮する。CTI の良否を決める評価基準は、「適時性」「精度」「使い勝手の良さ」「カバレージ」「リソース」「（データ処理の）スケーラビリティ」「（機能の）拡張性」「コンテキスト」である。

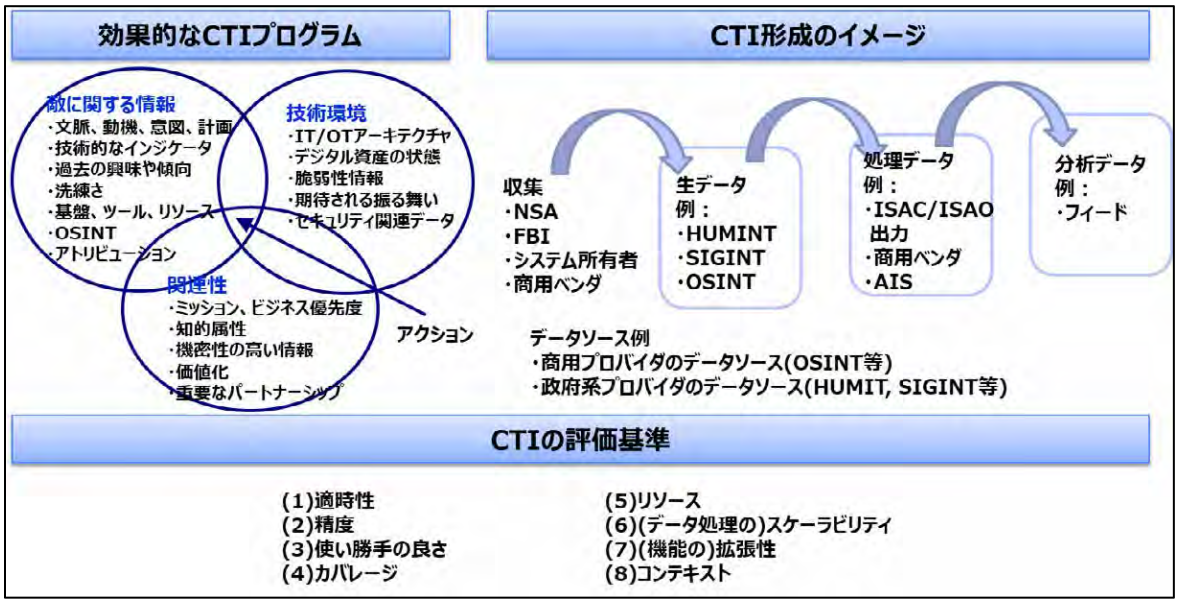

図 2-2-a サイバースレットインテリジェンス（CTI）の概要

CVI とは、サイバー脆弱性に関わるインテリジェンスである（図 2-2-b）。CVI が効果的であるとは、脆弱性を悪用することの容易さと、脆弱性を悪用した場合の影響の大きさの共通部分に焦点をあててアクションを施すことである。CVI を形成するには、公開データベースや商用サービスサイトなどからデータを収集し、生データ、処理データ、分析データへと次第にインテリジェンスを濃縮する。CVI の良否を決める評価基準を以下に示す。

- 特定された脆弱性がシステム固有のものか、意図的な脅威アクターや不注意によってシステムに導入されたものか
- 既知の脆弱性が存在するか
- 個々のステークホルダーが、自らが管理・支配するシステムの脆弱性を明らかにすることに消極的な場合があることの理解
- 特定の脆弱性についてのペネトレーション・テストやネットワーク評価の結果を含める
- 評価対象のシステムのベンダーやサプライヤーが新規で未試験であるか

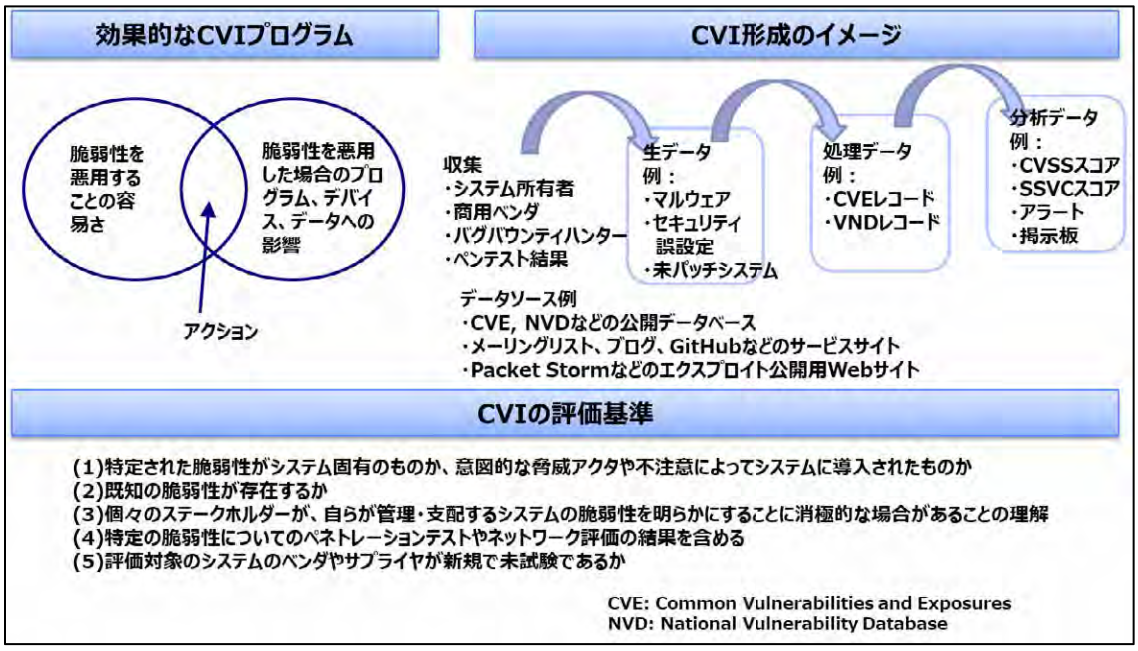

図 2-2-b サイバーバルネラビリティインテリジェンス（CVI）の概要

2. インフラストラクチャ（量子関係を含む）

国家サイバーインテリジェンスシステムは、クラウドサービスとして特に政府クラウドで実現する必要がある。政府クラウドとして実現するためには、一般に広く知られているクラウドサービスのサイバーセキュリティ基準を守るだけでは不足し、国家安全保障に関わる情報を扱えるだけの、高いセキュリティレベルに到達する必要がある。図 2-2-c に示すように、米国ではこのような高いセキュリティレベルは、FedRAMP と呼ばれるクラウドセキュリティ基準のもっとも高いレベル High に位置するものであり、日本の政府クラウドもまた、前記 FedRAMP の High レベルの環境整備が必要である。

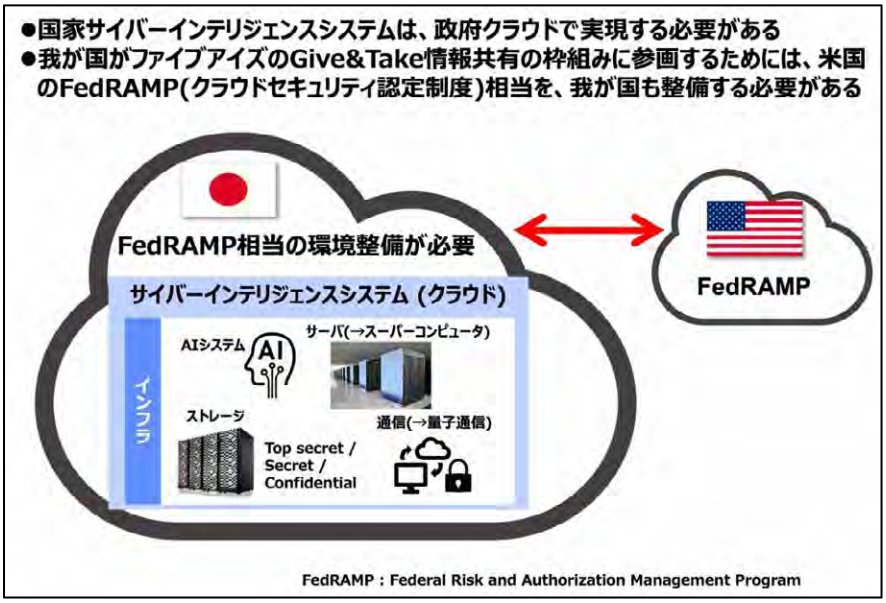

図 2-2-c クラウドサービスの活用イメージ

AI システムは、サイバーインテリジェンスを OSINT 情報からつくるために利用する。AI の活用イメージを図 2-2-d に示す。まず AI システムでは、構造化されたあるいは非構造化な、多種多様で大量に集められた OSINT データを、AI システムが理解できる情報（インフォメーション）に加工する。つぎに集まった情報（インフォメーション）を AI システムが処理し、国家安全保障に資する情報（インテリジェンス）を創出し提示する。

こうしたデータからインフォメーションさらにはインテリジェンスを作り出す工程においては、AI システムに限らず、超高速な処理を実現するためのスパコンや、大量のデータを保存するためのストレージや、クラウドサービスにアクセスするまでの通信路を確実に盗聴されないようにするための量子通信を組み合わせることで実現するものである。

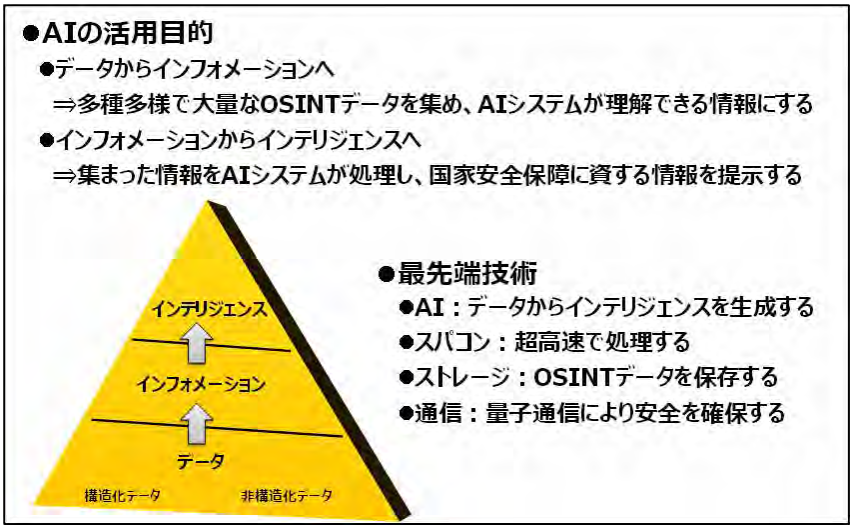

図 2-2-d AI の活用イメージ

ストレージは大容量であることは当然であるが、それだけに限らず、地政学的なバックアップを視野に、パブリッククラウドとセルフソブリンクラウドとの連携を行う（図 2-2-e）。国内におけるセルフソブリンクラウドどうしは大容量回線で接続する。一方、国内のクラウドが物理的に破壊されることが懸念される場合には、パブリッククラウドへのオフライン転送も視野にいれる。オフライン転送の事例としては Amazon Snowball が有名であり、ウクライナ侵攻の際にもウクライナ国内のデータをパブリッククラウドに転送するのに活躍した。

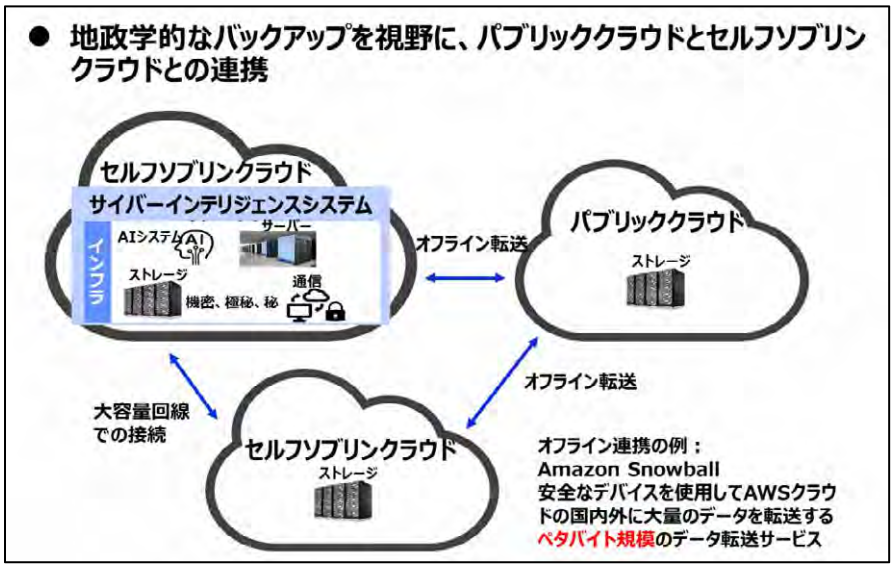

図 2-2-e ストレージとバックアップの活用イメージ

量子通信では、従来からの数学的な安全性に加えて、物理的な安全性を備えた鍵配送や共通鍵暗号の利用が考えられる（図 2-2-f）。