TTC標準草案
(Draft TTC Standards)

セキュリティ専門委員会

2021年12月

新規標準の制定について（JT）

- 近年、標的型攻撃やランサムウェアによる二重の脅迫などサイバー脅威が多発しており、企業や組織の活動全体に大きな影響を与え続けている。さらには、DXが加速する中、社会的あるいはビジネス的な環境変化や、国内外の法規制など、外的な変化がもたらすリスクへの対応も重要となってきており、組織レベルでの戦略的なセキュリティ対応を実現するフレームワークが求められている。

- このようなフレームワークとしてITU-T 勧告X.1060が発行された。この勧告には、日本発のサイバーセキュリティの知見として、政府や各省庁、民間セキュリティ団体（ISOG-J等）の政策やノウハウが取り入れられている。そのため、官民の両面において、これまでのセキュリティ施策との整合を保ちながら、さらなる発展的なフレームワークとして、国内でも組織的なサイバーリスク対策への活用が期待される。

JT標準

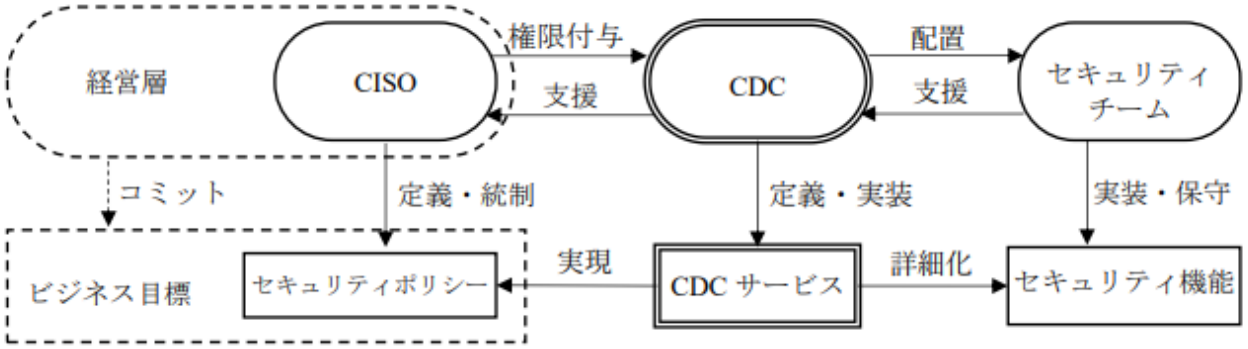
- セキュリティ専門委員会は、国内の組織的なサイバーセキュリティの発展、普及啓発のため、以下のITU-T勧告をベースとするTTC標準の制定を提案する。

		標準類	版数	タイトル
1	新規	X.1060	1	サイバーディフェンスセンターを構築・運用するためのフレームワーク

付録
JT標準のベースとなるITU-T勧告の概要

JT-X1060:サイバーディフェンスセンターを構築・運用するためのフレームワーク

組織レベルでの戦略的なセキュリティ対応を実現するための存在としてサイバーディフェンスセンター（CDC）の位置づけを定義し、CDCが実践すべき構築、マネジメント、評価の3プロセスをフレームワークとして規定する。



JT-X1060 図1　CDCの運営における関係者とその役割

- 図1は、X.1060が定義するサイバーディフェンスセンター（CDC）の組織における位置づけを示している。

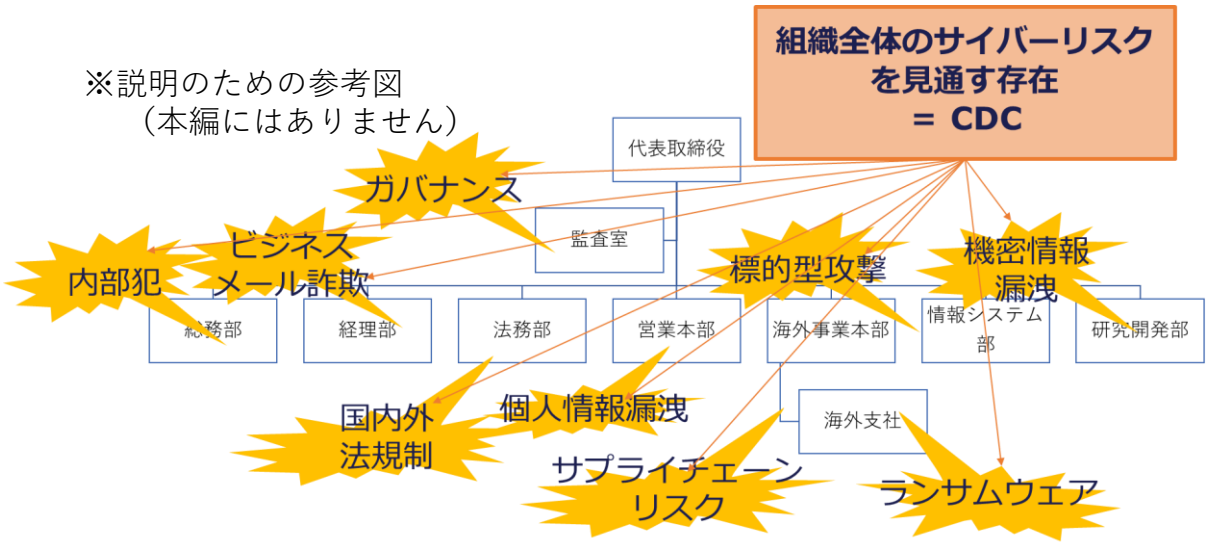
サービスリスト	サービスカタログ	サービスプロファイル	サービスポートフォリオ
構築プロセス			
評価プロセス		**マネジメントプロセス**	
ギャップ分析		**フェーズ**	**サイクル**
アセスメント		戦略マネジメント	長期サイクル
割り当て		運用	短期サイクル
推奨レベル		対応	

JT-X1060 図2

サイバーディフェンスセンターを構築・運用するためのフレームワーク

- 図2は、CDCのフレームワークとして、構築・マネジメント・評価の3プロセスを規定し、それぞれのプロセス内において実施すべきステップをまとめたものである。

具体的なサイバーディフェンスセンターの姿、形
CDC Concept: 既存の組織を包含するより広い概念



- CDCという言葉は新しい概念であるものの、「新たな組織」を持とうという話ではなく、すでに存在する組織が担っている場合もある。
- また必ずしも独立した一つの組織によって営まれるわけではなく、複数の組織に横断的に存在している場合もり、**X.1060で示されるようなサービスが、既に存在し、関係する組織が連携して活動している状態であれば、「その総体がCDCである」と言える。**
- 一般的にセキュリティに関わる組織として**CSIRTやSOCの存在があるが、CDCはそれらをサービスの一部として包含するより広い概念**である。
- 新たな概念としてCDCが必要となったのは、組織活動がデジタル化するにつれ、情報システムへの脅威が、単にシステムへの被害を発生させるだけでなく、経営的な被害や、より物理的あるいは人的な被害までをも引き起こすようになったからである。こういった**情報システムに留まらない、より広い範囲のリスクに対抗するための組織としてCDCの概念が重要**となる。

以降、説明用スライド

X.1060そしてサイバーディフェンスセンターとは？

X.1060のスコープ

- この勧告は、組織がサイバーディフェンスセンター（CDC）を構築、マネジメントするとともに、その有効性を評価するためのフレームワークを提供するものである。このフレームワークは、組織のセキュリティを実現するために、CDCがどのようにセキュリティサービスを決定し、実施すべきかを示している。
- この勧告は、最高セキュリティ責任者（CSO）や最高情報セキュリティ責任者（CISO）など、組織のセキュリティに責任を持つ経営幹部レベル、およびそれを補佐するセキュリティ管理者を対象としている。

サイバーディフェンスセンターとは？

- 定義
  - “CDC is an entity within an organization that offers security services to manage the cybersecurity risks of its business activities.”
  - 「ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体」

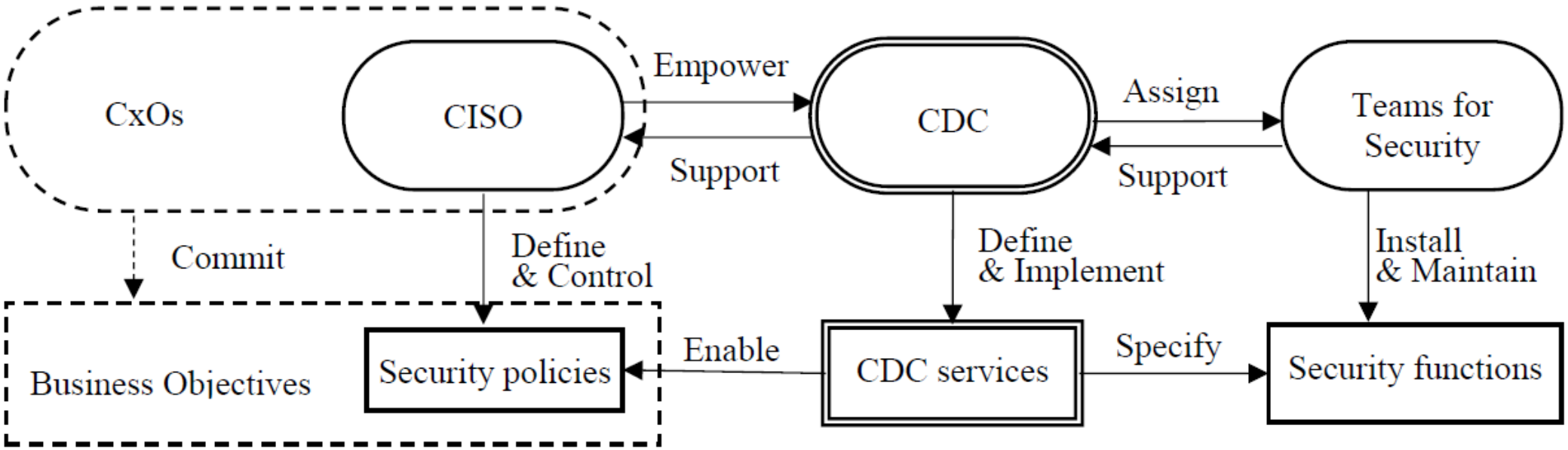


Figure 1 – Stakeholders and their roles for CDC operation

サイバーディフェンスセンターとは？CDC in the organization

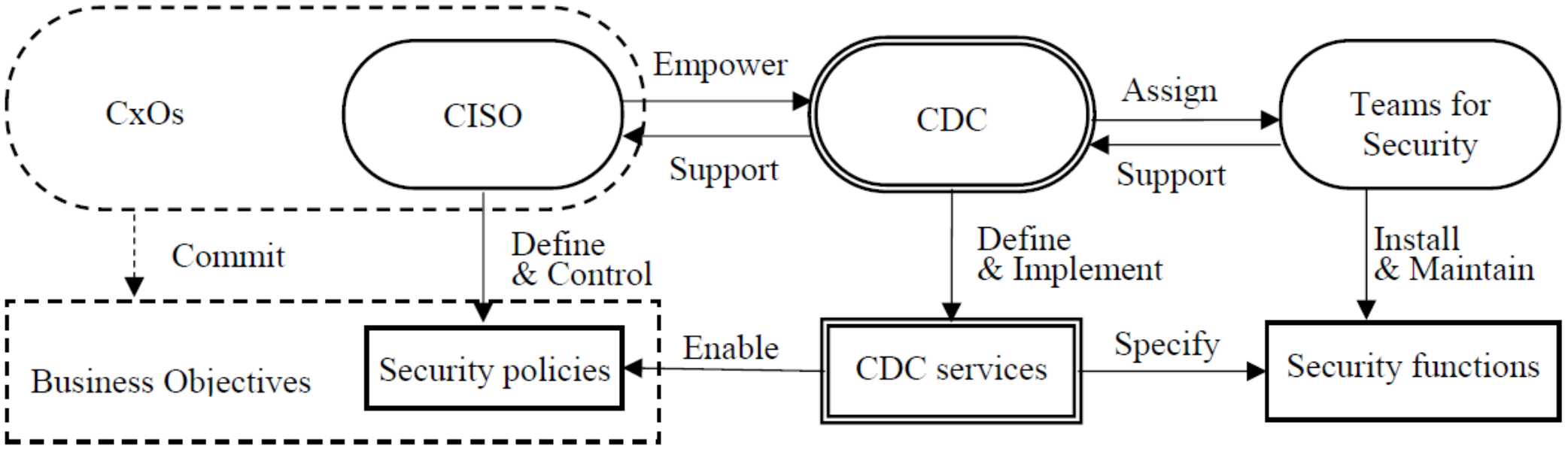


Figure 1 – Stakeholders and their roles for CDC operation

経営層が
ビジネス目標を定める

CISOはその目標におけるリスクをマネジメントするために、セキュリティポリシーを策定・監督する

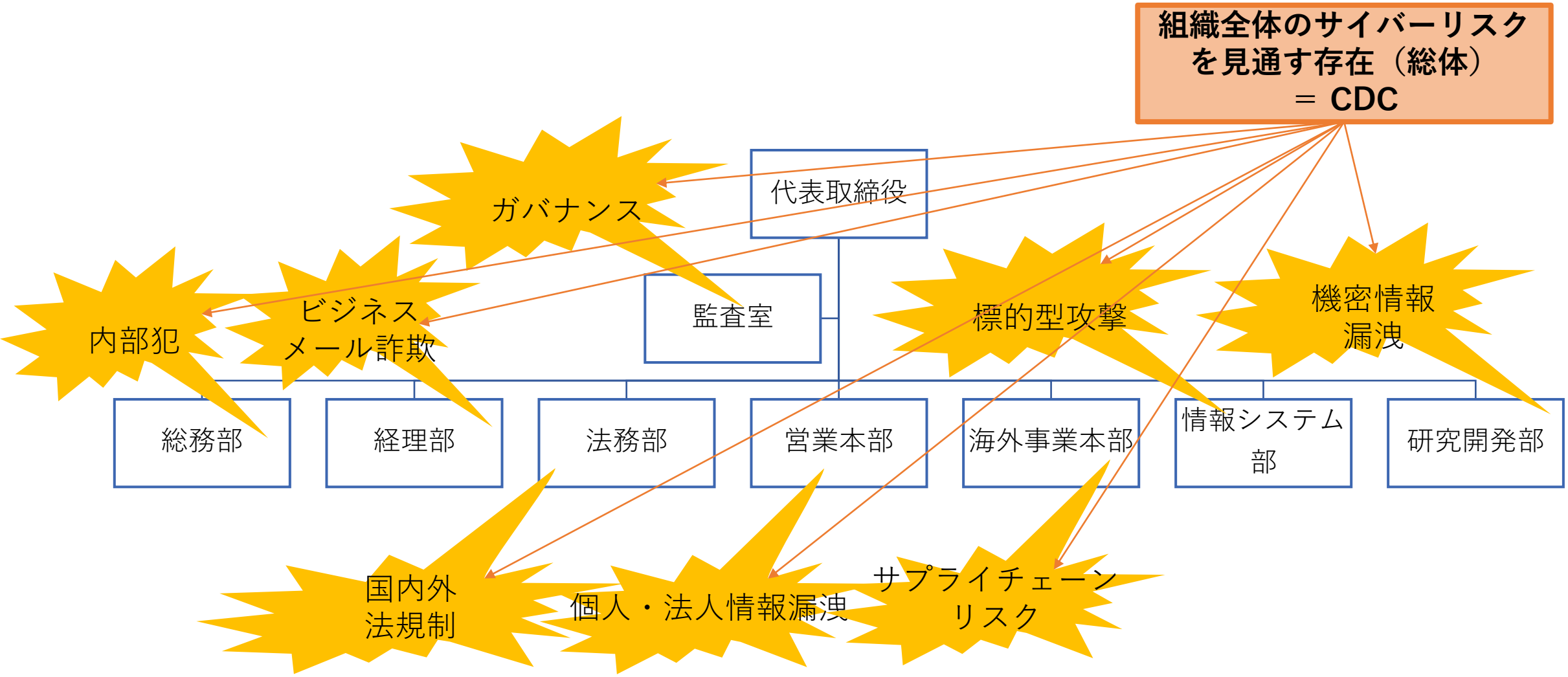
CDCはCISOの命を受け、セキュリティポリシーを有効化するためのサービスを業務定義、実装する

社内各部門において、CDCサービスを実働させる人員、機能を用意し、具体的に遂行する

具体的なサイバーディフェンスセンターの姿、形は？
CDC Concept: 既存の組織を包含するより広い概念

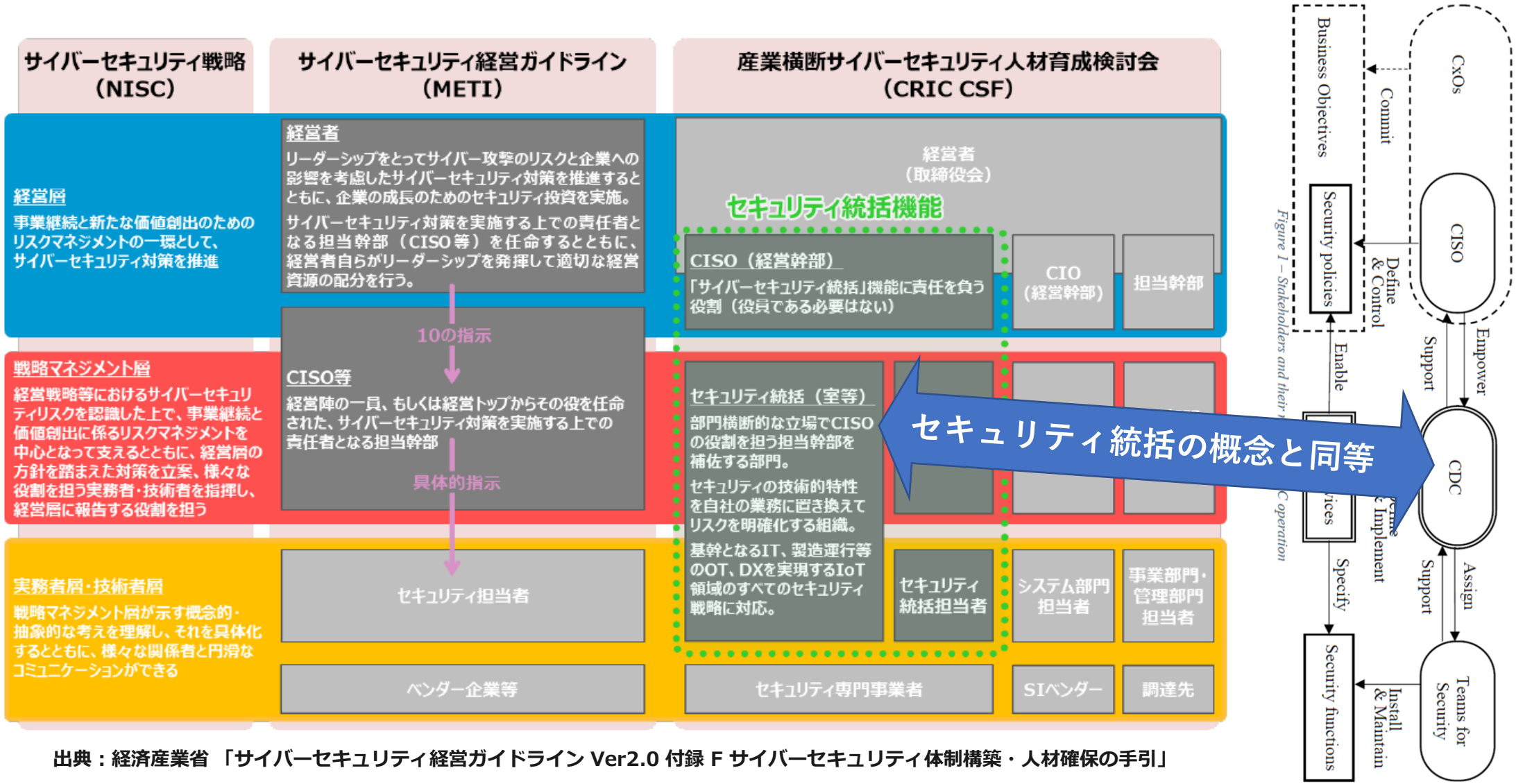
- CDCという言葉は新しい概念であるものの、「新たな組織」を持とうという話ではなく、すでに存在する組織が担っている場合もある。
- また必ずしも独立した一つの組織によって営まれるわけではなく、複数の組織に横断的に存在している場合もり、**X.1060で示されるようなサービスが、既に存在し、関係する組織が連携して活動している状態であれば、「その総体がCDCである」と言える。**
- 一般的にセキュリティに関わる組織として**CSIRTやSOCの存在があるが、CDCはそれらをサービスの一部として包含するより広い概念**である。
- 新たな概念としてCDCが必要となったのは、組織活動がデジタル化するにつれ、情報システムへの脅威が、単にシステムへの被害を発生させるだけでなく、経営的な被害や、より物理的あるいは人的な被害までをも引き起こすようになったからである。こういった**情報システムに留まらない、より広い範囲のリスクに対抗するための組織としてCDCの概念が重要**となる。

具体的なサイバーディフェンスセンターの姿、形は？



X.1060と日本のガイドラインとの整合性

CDCと日本の各種ガイドラインとの整合性：CDCの位置づけ



出典：経済産業省 「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引」

CDCと日本の各種ガイドラインとの整合性：戦略マネジメント層

サイバーセキュリティ戦略（NISC）

経営層
事業継続と新たな価値創出のための
リスクマネジメントの一環として、
サイバーセキュリティ対策を推進

戦略マネジメント層
経営戦略等におけるサイバーセキュリティリスクを認識した上で、事業継続と価値創出に係るリスクマネジメントを中心となって支えるとともに、経営層の方針を踏まえた対策を立案、様々な役割を担う実務者・技術者を指揮し、経営層に報告する役割を担う

実務者層・技術者層
戦略マネジメント層が示す概念的・抽象的な考えを理解し、それを具体化するとともに、様々な関係者と円滑なコミュニケーションができる

出典：経済産業省 「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引」

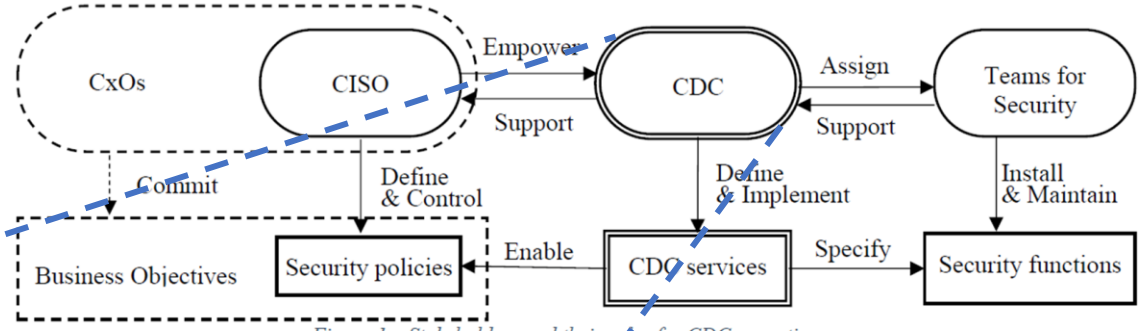


Figure 1 – Stakeholders and their roles for CDC operation

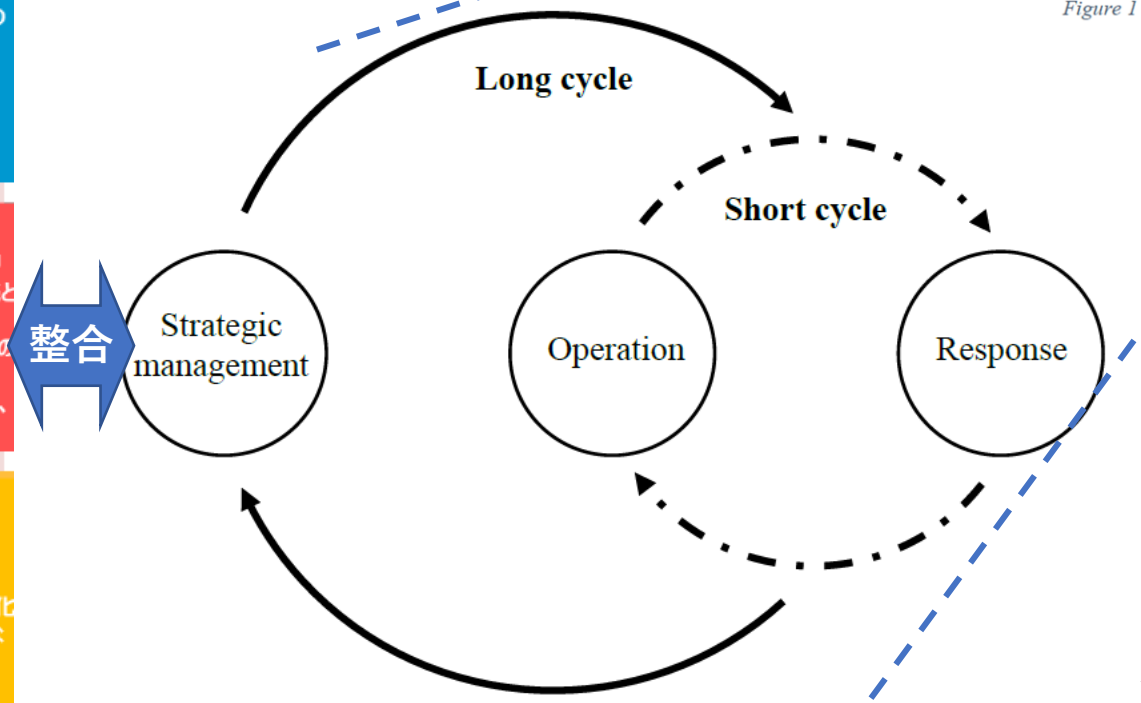


Figure 6 - CDC management process

整合

CDCのマネジメントプロセスにおいて
“Strategic management”を配置。
これは日本の戦略マネジメント層の営みと
整合するようになっている。

CDCと日本の各種ガイドラインとの整合性：ISOG-J「セキュリティ対応組織の教科書」との整合

インソース・アウトソースの判断基準

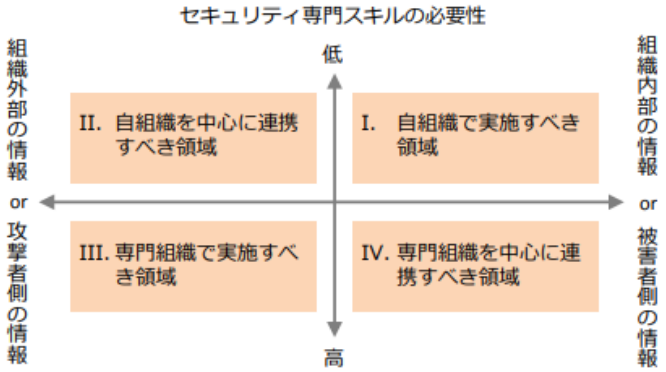


図 4　セキュリティ対応の4領域

整合

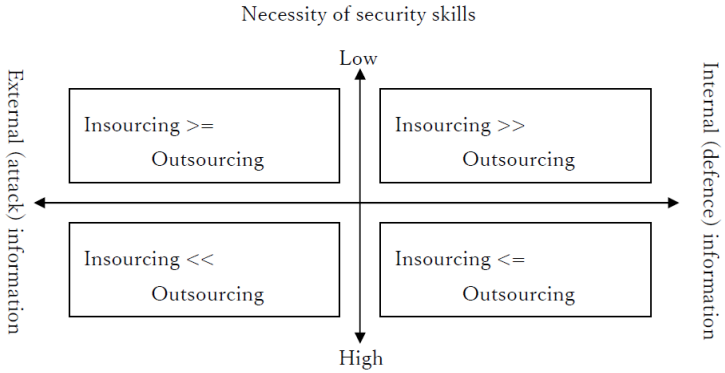


Figure 5 - Sourcing quadrants

アセスメントの基準

◆ インソースの場合：**属人ではなく組織的な営みになっているか**

明文化された運用は CISO など権限ある組織長に承認されている	+5 点
運用が明文化されており、担当者と交代して他者が業務を実施できる	+4 点
運用が明文化されておらず、担当者に代わり他者が臨時で一部の業務を代行できる	+3 点
運用が明文化されておらず、担当者が業務を実施できる	+2 点
実施できていない	+1 点
インソースでの実装を検討したものの、結果として実施しないと判断した	評価外

◆ アウトソースの場合：**サービスを活用しきれているか**

サービス内容と得られる結果を理解でき、想定通り	+5 点
サービス内容と得られる結果を理解できているが、想定未満	+4 点
サービス内容、得られる結果のいずれかが理解できていない	+3 点
サービス内容と得られる結果を理解できていない	+2 点
結果や報告を確認できていない	+1 点
アウトソースでの実装を検討したものの、結果として実施しないと判断した	評価外

整合

For insource:

Documented operation is authorized by CISO or other organizational director who has proper responsibilities	+5 points
Operation is documented and others can play the role of existing operator	+4 points
Operation isn't documented and others can play the partial role of existing operator temporarily	+3 points
Operation isn't documented and the existing operator can play role	+2 points
Operation isn't working	+1 point
Decided not to implement by insourcing	N/A

For outsource:

Content of service and expected output are understood and their outputs are as expected	+5 points
Content of service and expected output are understood but their outputs aren't as expected	+4 points
Either content of service or expected output isn't understood	+3 points
Both content of service and expected output aren't understood	+2 points

X.1060が示すフレームワークとは？

CDCのフレームワークとは？

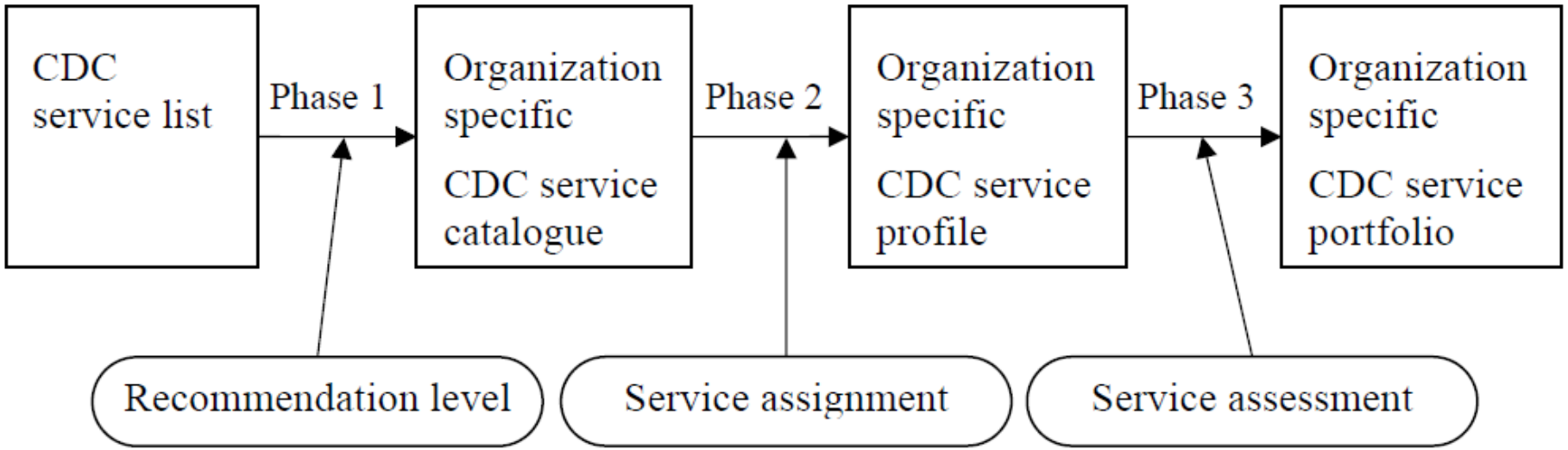
３つのプロセス【Build（構築）、Management（マネジメント）、Evaluation（評価）】を継続させる営みのこと。

Service list	Service catalogue	Service profile	Service portfolio
Build process			
Evaluation process		**Management process**	
Gap analysis		**Phases**	**Cycles**
Assessment		Strategic management	Long cycle
Assignment		Operation	Short cycle
Recommendation level		Response	

Figure 2 - Framework for the creation and operation of CDC

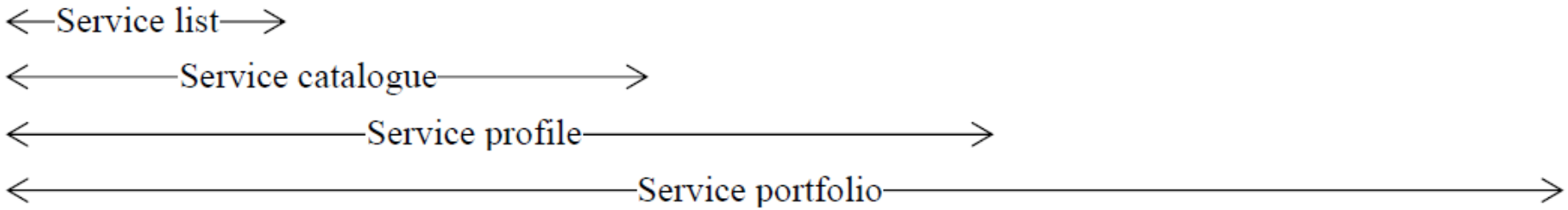
Build（構築）プロセスとは？

構築プロセス



構築プロセスのアウトプット

Service	Recommendation level	Service assignment	Service score	
			As-is	To-be
Service ex.1	Basic	Insourcing (AB dept.)	3	5
Service ex.2	Standard	Outsourcing (Z-MSSP)	2	4
Service ex.3	Advanced	Unassignable	1	2



CDCサービスリストの全体像

A	**Strategic management of CDC**
A-1	Risk management
A-2	Risk assessment
A-3	Policy planning
A-4	Policy management
A-5	Business continuity
A-6	Business impact analysis
A-7	Resource management
A-8	Security architecture design
A-9	Triage criteria management
A-10	Counter measures selection
A-11	Quality management
A-12	Security audit
A-13	Certification
B	**Real-time analysis**
B-1	Real-time asset monitoring
B-2	Event data retention
B-3	Alerting & warning
B-4	Handling inquiry on report
C	**Deep analysis**
C-1	Forensic analysis
C-2	Malware sample analysis
C-3	Tracking & tracing
C-4	Forensic evidence collection
D	**Incident response**
D-1	Incident report acceptation
D-2	Incident handling
D-3	Incident classification
D-4	Incident response & containment
D-5	Incident recovery
D-6	Incident notification
D-7	Incident response report
E	**Check and evaluate**
E-1	Network information collection
E-2	Asset inventory
E-3	Vulnerability assessment
E-4	Patch management
E-5	Penetration test
E-6	Defence capability against APT attack evaluation
E-7	Handling capability on cyber attack evaluation
E-8	Policy compliance
E-9	Hardening

F	**Collecting, analyzing and evaluating threat intelligence**
F-1	Post mortem analysis
F-2	Internal threat intelligence collection and analysis
F-3	External threat intelligence collection and evaluation
F-4	Threat intelligence report
F-5	Threat intelligence utilization
G	**Development and maintenance of CDC platforms**
G-1	Security architecture implementation
G-2	Basic operation for network security asset
G-3	Advanced operation for network security asset
G-4	Basic operation for endpoint security asset
G-5	Advanced operation for endpoint security asset
G-6	Basic operation for cloud security products
G-7	Advanced operation for cloud security products
G-8	Deep analysis tool operation
G-9	Basic operation for analysis platform
G-10	Advanced operation for analysis platform
G-11	Operates CDC systems
G-12	Existing security tools evaluation
G-13	New security tools evaluation
H	**Supporting internal fraud response**
H-1	Internal fraud response and analysis support
H-2	Internal fraud detection and reoccurrence prevention support
I	**Active relationship with external parties**
I-1	Awareness
I-2	Education & training
I-3	Security consulting
I-4	Security vendor collaboration
I-5	Collaboration service with external security communities
I-6	Technical reporting
I-7	Executive security reporting

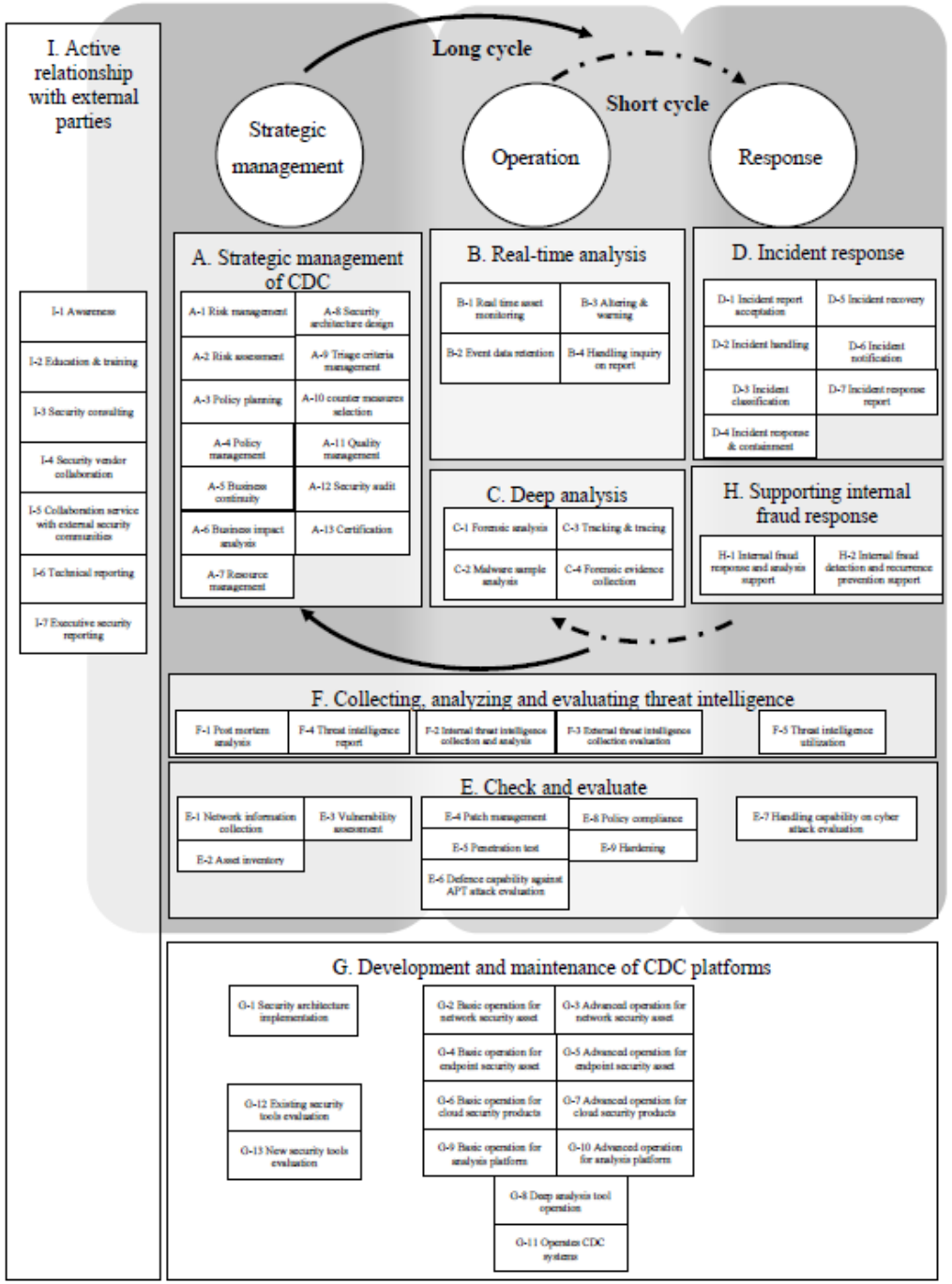


Figure 8 - CDC service categories

Build（構築）プロセスとは？
Phase 1. サービスカタログの作成

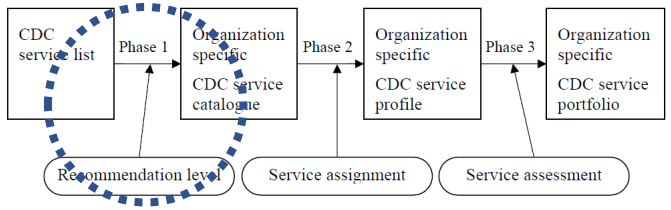


Figure 3 - Phases to build services for CDC

- X.1060 Annex Aを参考に、実施する（実施している）CDCサービスを選択する
- 選択に当たっては、以下のレベル分けをする

Weight	Description
Unnecessary	Services deemed unnecessary
Basic	Minimum services to be implemented
Standard	Services that are generally recommended for implementation
Advanced	Services required to achieve a higher-level CDC cycle
Optional	Services arbitrarily selected according to the expected form of CDC

- もしX.1060に無いもので、必要なサービスが存在するのであれば、それは独自に定義、追加する

Build（構築）プロセスとは？
Phase 2. サービスプロファイルの作成

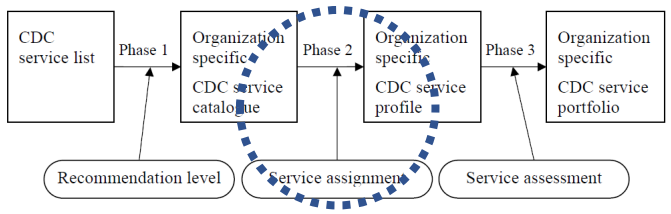


Figure 3 - Phases to build services for CDC

- Phase 1で作成したサービスカタログに掲載の各サービスについて具体的な実施組織を決定する
- アサインに当たっては、下記を参考に方針を決定する

Type	Description
Insourcing	Services are provided by a team within the organization. The organization should specify the team in charge.
Outsourcing	Services are provided by a team outside of the organization. The organization should specify the outsourcer.
Combination	The organization uses insourcing and outsourcing together. A responsible team and a contractor should be specified by the organization.
Unassigned	Although the organization recognises a service, but there is no assignee in the organization.

- インソースにすべきか、アウトソースにすべきかは下記の指標を参考にする

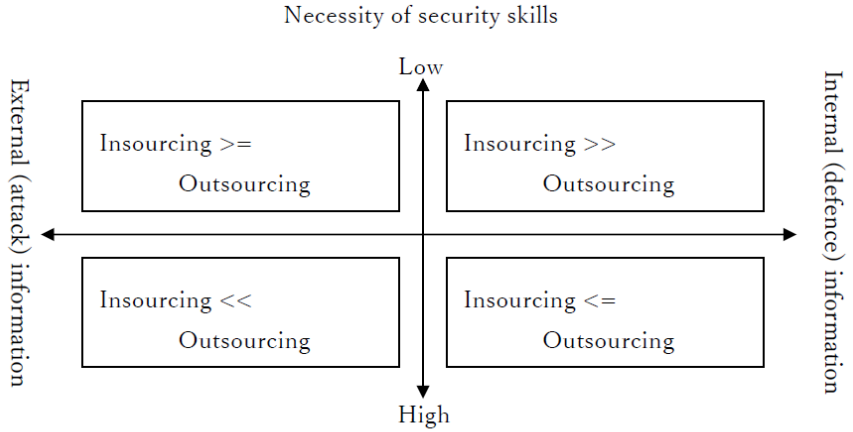


Figure 5 - Sourcing quadrants

Build（構築）プロセスとは？
Phase 3. サービスポートフォリオの作成

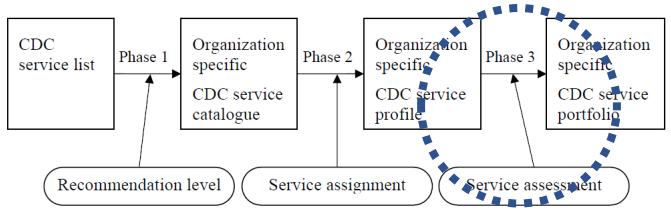


Figure 3 - Phases to build services for CDC

- Phase 2で作成したサービスプロファイルのアサイン状況に応じ、現状のスコアと目標スコアを設定する。
- スコアリングにおいては、下記の基準を参考とできる

For insource:

Documented operation is authorized by CISO or other organizational director who has proper responsibilities	+5 points
Operation is documented and others can play the role of existing operator	+4 points
Operation isn't documented and others can play the partial role of existing operator temporarily	+3 points
Operation isn't documented and the existing operator can play role	+2 points
Operation isn't working	+1 point
Decided not to implement by insourcing	N/A

For outsource:

Content of service and expected output are understood and their outputs are as expected	+5 points
Content of service and expected output are understood but their outputs aren't as expected	+4 points
Either content of service or expected output isn't understood	+3 points
Both content of service and expected output aren't understood	+2 points
Nether output nor report isn't reviewed	+1 point
Decided not to implement by outsourcing	N/A

Management（マネジメント）プロセスとは？

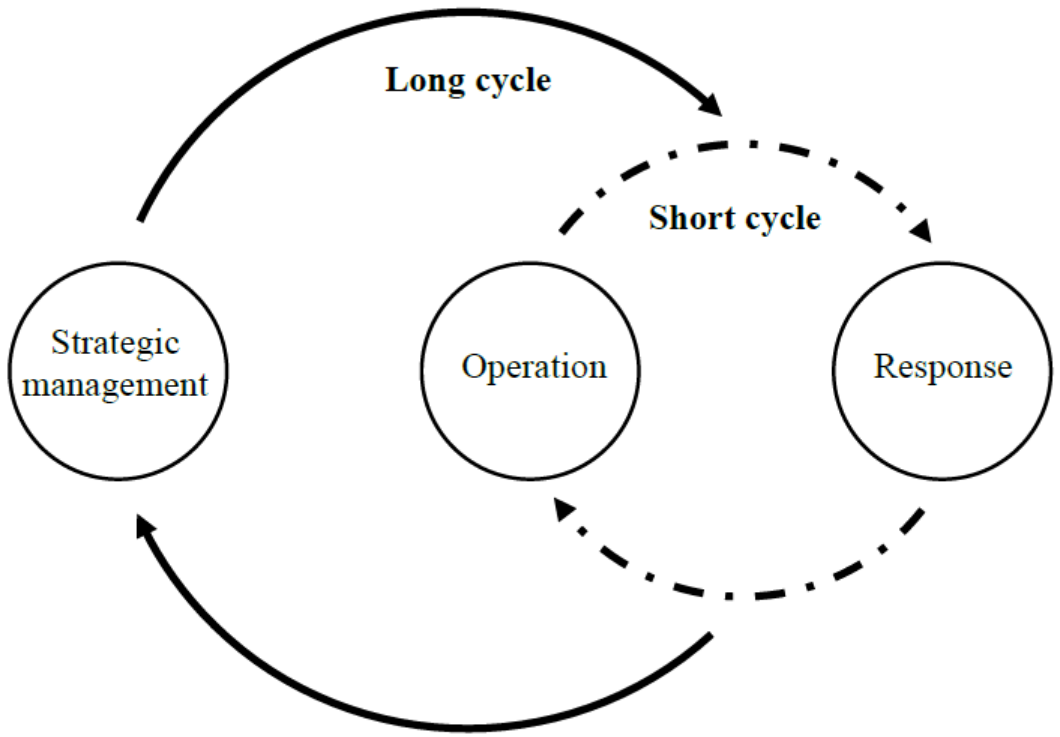


Figure 6 - CDC management process

3つのフェーズと2つのサイクルで成り立つ

- Strategic management（戦略マネジメント） phase
  - CDCの定義、全体のデザイン、計画や管理に関係する戦略的な視点が必要となるサービスの遂行に責任を持った活動。
- Operation（運用） phase
  - 平時の活動としてセキュリティの監視やそれに付随するサービスを遂行する。このような活動を主体とする組織は一般的にSOCと呼ばれる。
- Response（対応） phase
  - 運用フェーズでの発見事象に基づき、非常時に実施すべきサービスを遂行する。このような活動を主体とする組織は一般的にCSIRTと呼ばれる。

◆ Short cycle
  ◆ 日々の運用や対応において、現状のリソース内で可能な改善活動を継続的に実施する

◆ Long cycle
  ◆ 運用と対応のフェーズでは解決できないような、リソースの増強なども前提とした長期的な改善活動を継続的に実施する

Evaluation（評価）プロセスとは？

- Buildプロセスで定義した、サービスカタログ、プロファイル、ポートフォリオ一つずつ見直していくプロセス。

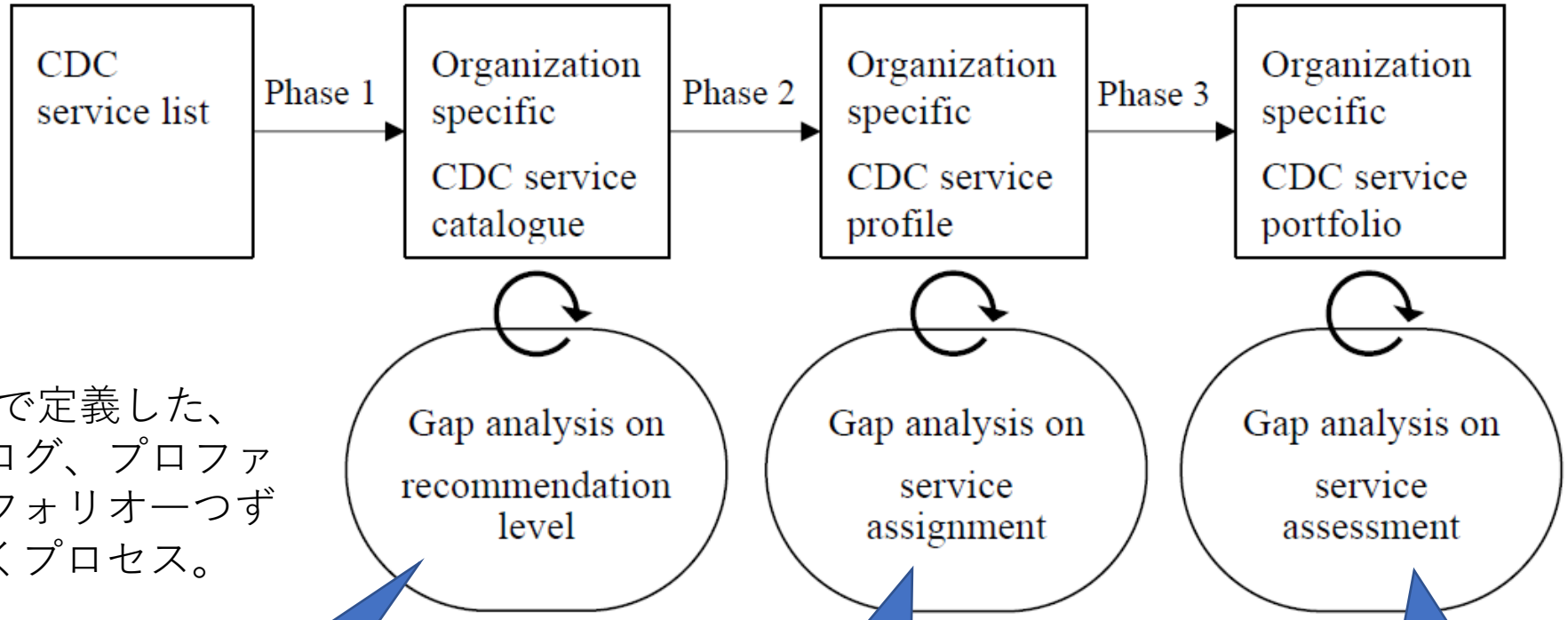


Figure 7 - CDC evaluation process

サービスカタログに選出したサービスに過不足はないか

サービスプロファイルで決めたアサインに無理はないか

サービスポートフォリオで定めた目標スコアを達成できているか

X.1060 Framework for the creation and operation of a cyber defence centre

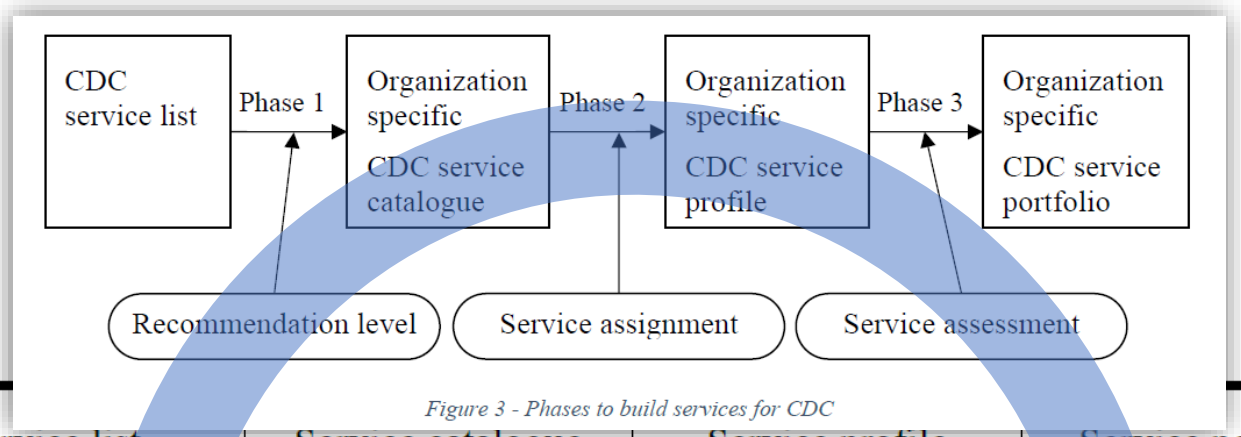
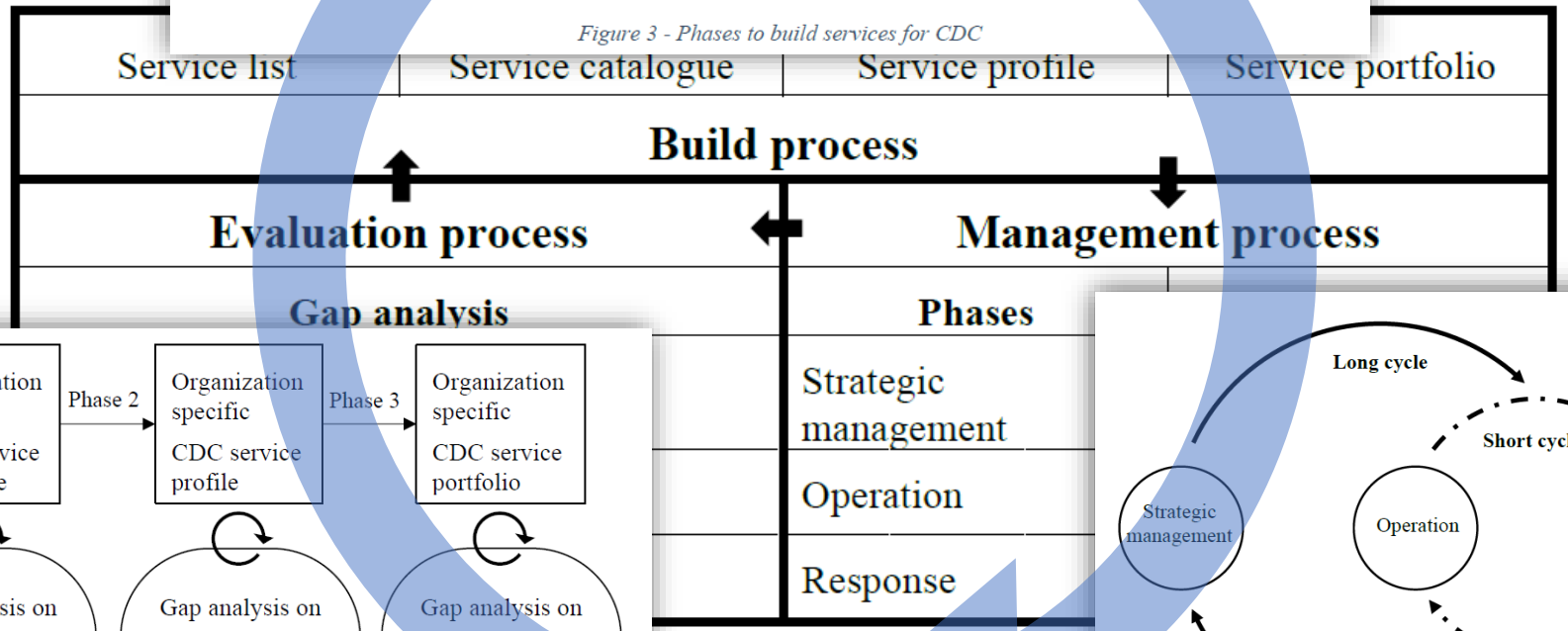


Figure 3 - Phases to build services for CDC



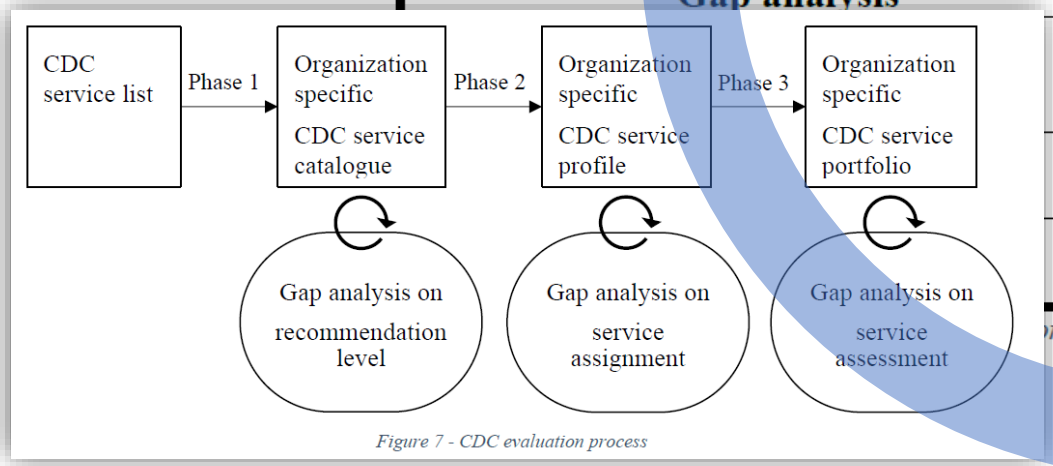


Figure 7 - CDC evaluation process

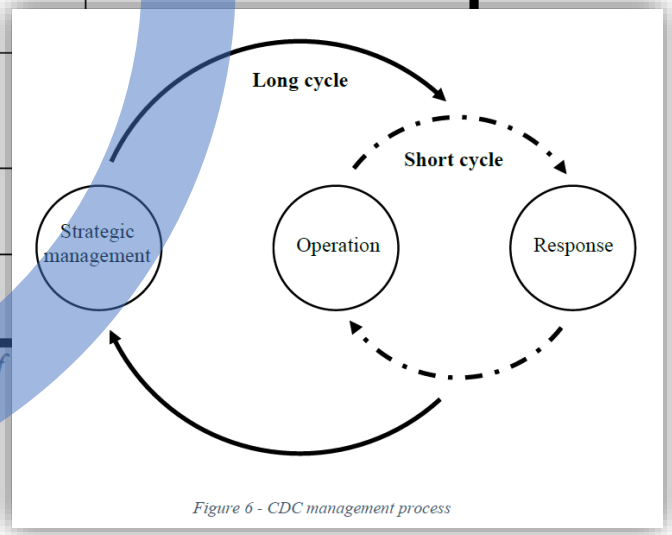


Figure 6 - CDC management process