CCM (Cloud Controls Matrix)におけるマッピング手法の解説

執筆および協力者

Ahmed Maaloul
Ai-Ping Foo
Eleftherios Skoutaris
Damir Savanovic
Daniele Catteddu
Sean Cordero
Victor Chin
Alain Pannetrat
Michael Roza
Eric Tierling
Kimberley Laris

日本語版提供に際しての告知及び注意事項

本書「CCM (Cloud Controls Matrix)におけるマッピング手法の解説」は、Cloud Security Alliance (CSA)が公開している「METHODOLOGY FOR THE MAPPING OF THE CLOUD CONTROLS MATRIX (CCM)」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2018 年 12 月 27 日	日本語版 1.0	初版発行

日本語版作成に際しての謝辞

この日本語訳は、CSA ジャパンの「ガイダンスワーキンググループ」および「CCM/STAR ワーキンググループ」に参加するメンバーを中心とした、CSA ジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）

勝見　勉

目次

はじめに

Cloud Security Alliance による Cloud Controls Matrix (CCM) について

Cloud Security Alliance (CSA)の Cloud Controls Matrix (CCM)は、クラウドサービスのセキュリティリスクを総合的に評価しようとするクラウド事業者およびクラウド利用者に、指針となる基本的なセキュリティの原則を提供するものである。CSA の CCM には、CSA のセキュリティガイダンスと整合した、詳細なセキュリティ管理策のフレームワークを、16 のドメインに分けて記述している。

CSA の CCM には、業界で利用されている他のセキュリティフレームワーク（ISO27001/27002、ISACA の COBIT、PCI DSS、NIST、AICPA の TSP、FedRAMP、ENISA の IAF など）へのマッピングや、サービス提供事業者向けの付加的情報、クラウド事業者が提供する評価証明が含まれている。

マッピングは、主として、CCM ワーキンググループの有志によって行われ、また他の組織から CSA に対して提供されている。

Cloud Controls Matrix (CCM) におけるマッピングの方法

この文書が狙いとしているところは、マッピングにおける再現可能な一貫性を如何に作るかのガイドラインを示すことで、CCM のフレームワークや活動をサポートするメンバーや協力者が継続して作業できるようにすることにある。

この文書では、CSA の CCM におけるマッピングのプロセスとして、4 つの基本的な機能について述べる。

1) CCM ワーキンググループにおけるマッピングの仕方、ガイドライン、名前付けの基準について、明確であり透過的であること。

2) CSA のコミュニティからの作業手順に対するレビューや改良のための助言を得られるようにすること。

3) 組織にとって価値の高い参考情報を提供すること。特に、自組織のフレームワークを CCM にマッピングすることで、相互運用性への取り組みに貢献し、またそこから得るものを期待する組織に向けて。

4) 基準類をマッピングする経験によって、評価に携わる人たちの基準類の理解やあらゆるマッピングプロセスの解釈をよりよくしていくこと。

マッピングとリバースマッピング

マッピングー他の対象に対するベースとしての CCM

CCM に含まれる各管理策（基準）は、まず、他のフレームワーク上の管理策にマッピングされ、等しさの判断を行う。この方法で、どの CCM の管理策が他の既存のフレームワー

クにある基準と親和性があるか、そして相互にどの程度等価かを検討する。それにより、他のフレームワークを（CCM をベースとして）組み入れるのに必要な追加作業の程度を見積もる。

リバースマッピング－他の対象をベースとして CCM をマッピング

反対に、リバースマッピングは他のフレームワークを、CCM 内で同等の管理策を見い出すための主たるベースとして用いる。リバースマッピングを実施する場合は、対象とするフレームワークの各管理策は（可能な範囲で）CCM の内部に対して対照される。リバースマッピングの実施においてベースあるいは出発点となるのは、対象としたフレームワークである。

見方そのものが変化する場合を除き、他のプロセス、例えばマッピングプロセス、ギャップ分析、新たな要求条件の取り込みなどは全て同じである。

ギャップを発見し、分析し、報告すること

ギャップサマリには完全なギャップと部分的ギャップが示される。完全なギャップとは、特定の基準（管理策）が他のフレームワークに入っていないことを示す。部分的ギャップとは、類似の基準（管理策）があるが、完全に一致していないことを示す。

ギャップ分析が出来上がると、ある既存のコンプライアンス文書を他のフレームワークに適合するべく展開することの是非を判断するための取組みを企画するのに、役立つ情報となる。

CCM の場合は、「ギャップ分析」は特に、CCM と他のフレームワークの管理策の間のギャップをリストアップし説明するものである。

手法

プロジェクト管理

この文書のプロジェクト管理の部分は、第一義的には、CCM と他のフレームワークの間のマッピングに取り組むボランティアを指導する CSA の CCM ワーキンググループのためのものである。

マッピングプロセスには 4 つの主たる段階がある。準備、実施、ピアレビュー、公開である。

準備

最初の準備段階の手続きと判断が行われる必要がある。この段階で関与するのは、CSA のアナリスト、CCM ワーキンググループのリーダー、そしてマッピングプロジェクトに予定されているリーダーたちである。CCM ワーキンググループのボランタリな参加者はこの段階では関与しない。この段階で、様々な要素をよく検討し、グループによるプロジェクトの実行がスムーズに行くようにするべきである。例えば、プロジェクトの対象範囲、実施手順、責任者、作業用シートが、準備段階の完了までに、すべて明確に示され、用意され

ているべきである。

準備段階では、以下のことを実施する。

1. リーダーの選定
2. 作業用シートの作成
3. プロジェクトの対象範囲、目的、タイムスケジュールの決定
4. マッピング対象のフレームワークの明確な定義
5. 参加者の選定

実施

この段階では、実際のマッピングとギャップ分析が行われる。この段階では、プロジェクトリーダーとマッピングを実施するボランティアやプロジェクトメンバーの間のコミュニケーションをしっかりとしなければならない。すなわち、指示や納期や作業用シートや対象となるフレームワークやその他の材料の周知である。プロジェクトリーダーが用いるコミュニケーション手段には、キックオフの電話会議、e メール、プロジェクトソフトウェア（Basecamp など）の利用がある。

実施段階では、以下のことを実施する。

1. 管理策のマッピング
2. ギャップの確認
3. ギャップ分析

ピアレビューと公開

これら 2 つの段階に携わる者は、直接 CSA の文書である”Research Lifecycle”(https://cloudsecurityalliance.org/research/#_research-lifecycle)の中の CCM に関連する部分を参照する必要がある。

公開の段階では、「名付けの参照基準」（第 3 章）を参照して、首尾一貫したマッピングの基準と文法が適用されるようにするべきである。これらの確立した基準に準ずることで、CSA の CCM と STARWatch に、違和感なく組み入れることができる。

作業用シートとタスク

CCM のマッピングプロジェクトがうまく行くためには、作業用シートの内容は高い品質でなければならない。上手に組み立てられた作業用シートは、ボランティアやプロジェクトメンバーに、マッピングに際して期待されるものを、明確かつ精細に示すことができる。理想的には、その明確さによって、CSA CCM への新しいマッピングを行う際に起こる困難な課題を軽減できるであろう。

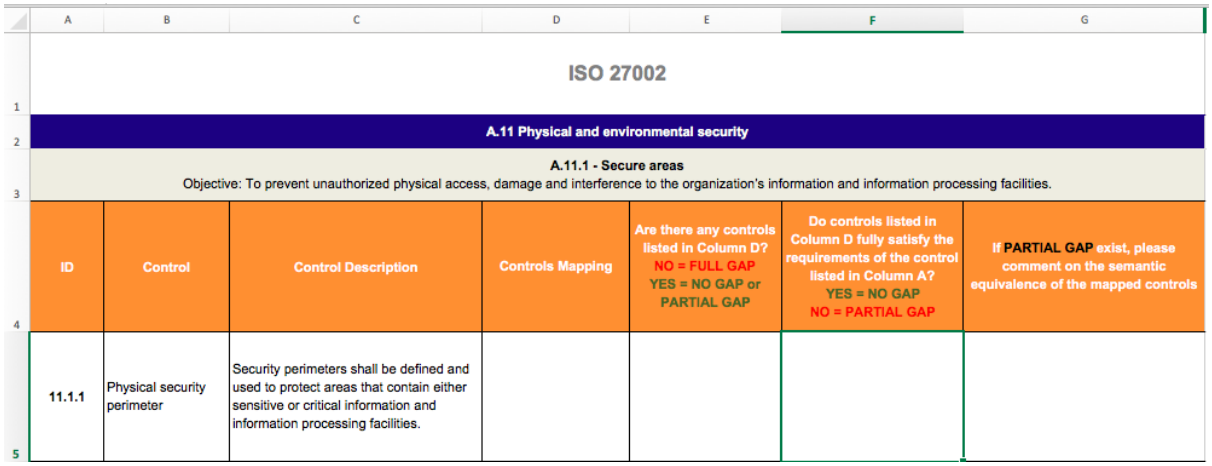
マッピングの作業用シートは、マッピングの実施前に作成し、以下の要素を備える必要がある。

1. マッピングの作業用シート
    a. 管理策のマッピング
    b. ギャップの確認

c. ギャップ分析

作業用シートの作成に際しては、そのプロジェクトの段階で最新の CCM のバージョンを使うことが大事である。
(https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview)

作業用シートのサンプル（下記イメージ参照）：ISO27002 の CCM V3.0.1 へのマッピングを実施するためのマッピングおよびギャップ分析用作業用シートである。作業用シートの D4, E4, F4, G4 のセルに、作業指示が示されている。作業を行うには、指示に従って左から右へ、D 列から始めて G 列まで、埋めて行く。（訳注：原文は D5, E5, F5, G5 となっているが、図から 5 行であるのは明らかなので変更した。）



	A	B	C	D	E	F	G
1	ISO 27002						
2	A.11 Physical and environmental security						
3	A.11.1 - Secure areas Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.						
4	ID	Control	Control Description	Controls Mapping	Are there any controls listed in Column D? NO = FULL GAP YES = NO GAP or PARTIAL GAP	Do controls listed in Column D fully satisfy the requirements of the control listed in Column A? YES = NO GAP NO = PARTIAL GAP	If PARTIAL GAP exist, please comment on the semantic equivalence of the mapped controls
5	11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.				

マッピングのプロセスと正確性

マッピングプロセスの主たる目的は、あるフレームワークから他のフレームワークに対して管理策をマッピングし、両管理策の間の意味するところの同一性を明らかにすることである。意味するところの同一性の評価は、CCM の管理策を他のフレームワークの管理策に対して比較することで可能となる。その際評価に用いる要素としては、以下のものがある。

1. ドメイン名のマッチング

2. セキュリティ管理策のマッチング

3. CCM と他のフレームワークにあるセキュリティ管理策の要求事項とキーワードのマッチング。対象となるフレームワークの中のセキュリティ関連のキーワードは、一つ一つ、CCM の中に意味的に同じキーワードがあるかどうかチェックする必要がある。

4. CCM と対象のフレームワークにおけるセキュリティ管理策の内容のマッチング。このアプローチは、キーワード検索のアプローチよりも厳格に内容を吟味することになり、うまく合致するマッチングは容易には見つからない。

意味的に同等のもののマッピングは、複数のフレームワーク内の 2 つ以上の管理策が、適用範囲の面で完全に同等であるということを意味する。そのような管理策は、意味的に相

互に同等であると言える。

ギャップの抽出と分析：ギャップなし、部分的ギャップ、完全なギャップ

プロジェクトの対象範囲と目的によっては、ギャップの抽出と分析は、最初のマッピングでは同等とみなされなかったその他の項目についても実施する場合がある。ギャップの抽出は本質的には（2 つ以上のフレームワークの）分析であり、フレームワーク間の意味的な同等性の判断を模索する行為である。ギャップ抽出プロセスでは、3 つのありうるケースを想定する。ギャップなし、部分的ギャップ、完全なギャップ、である。このいずれが当てはまるかを決めるには、以下の要素を検討する必要がある。

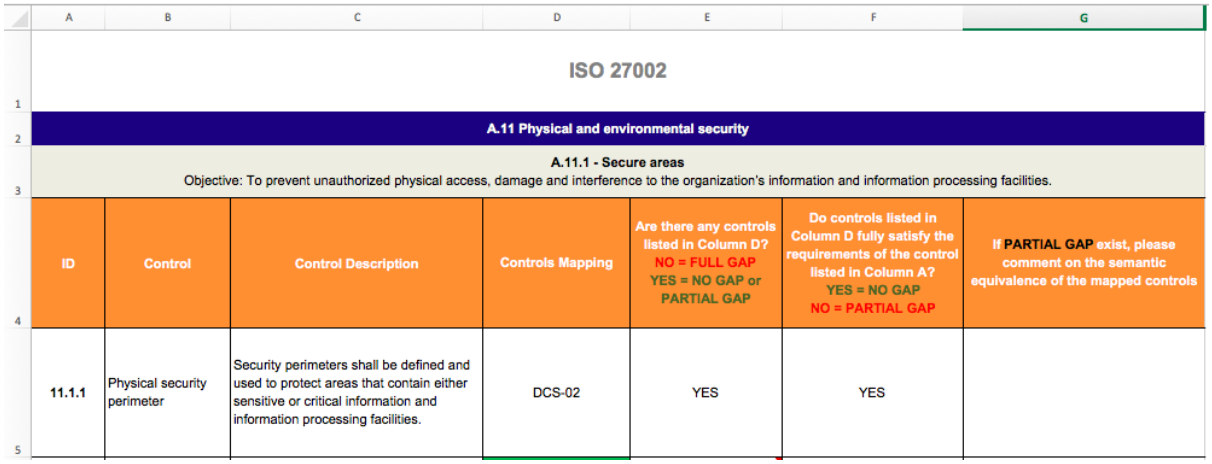
1. ギャップなし：CCM の管理策のあるものとその要求事項は、（対象となるフレームワークの中に）同等の管理策または管理策の組があり、対応する CCM の管理策の要求事項を完全に満たしている場合がある。

2. 部分的ギャップ：CCM の管理策のあるものとその要求事項は、（対象となるフレームワークの中に）管理策または管理策の組があるが、対応する CCM の管理策の要求事項を完全には満たしていない場合がある。部分的ギャップとするためには、CCM の管理策のうちの 1 つの管理策と意味的に同等の管理策が少なくとも一つ、対象となるフレームワークの中にある必要がある。対象となるフレームワークの中のその他の関連する管理策は、作業用シートに記載しなければならない。

3. 完全なギャップ：CCM の管理策のあるものとその要求事項は、（対象となるフレームワークの中に）意味的に同等の管理策または管理策の組がない。基本的に、その意味するところは、CCM の管理策が、対象となるフレームワークの中のどの管理策によってもカバーされていないということである。

更に、ギャップ分析は、対象となるフレームワークの間のギャップを埋めるのに、どの程度の労力を要するかの指標をもたらす。

こういった指示は、ボランティアに提供される作業用シートに反映されなければならない。シートに示した例（図表参照）は、ISO/IEC27002:2013.11.1.1 の物理的境界のセキュリティ管理策を CCM にリバースマッピングしてギャップの抽出を行った記入済みの作業用シートである。



	A	B	C	D	E	F	G
1	ISO 27002						
2	A.11 Physical and environmental security						
3	A.11.1 - Secure areas Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.						
4	ID	Control	Control Description	Controls Mapping	Are there any controls listed in Column D? NO = FULL GAP YES = NO GAP or PARTIAL GAP	Do controls listed in Column D fully satisfy the requirements of the control listed in Column A? YES = NO GAP NO = PARTIAL GAP	If PARTIAL GAP exist, please comment on the semantic equivalence of the mapped controls
5	11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	DCS-02	YES	YES	

参照情報の記述方法

CCM マッピングにおいて一貫性を確保するには、参照情報のためのガイドラインと推奨事項のセットを用意するのが有効である。CSA で CCM マッピングの作業に関わる者は、以下のガイドラインに従うべきである。

ルールと推奨事項

以下において”SHOULD”と”MUST”は RFC(Request for Comments)2119 の記述に従って解釈されるべきである。

ルール 1

参照情報(reference)は 1 つ以上の以下の要素の組合せで表さなければならない(MUST)。

- アルファベット、小文字または大文字
- 10 進数
- ハイフン／マイナス(U+002D)
- ピリオド (U+002E)
- 左カッコ (U+0028)
- 右カッコ (U+0029)
- 空白を示す文字 (U+0020) 前後に文字または数字がある場合に限る

例

- 正
  - “A1.2”
  - “1.4.5(3)”
  - “Annex 1-a”
- 誤
  - “A1,7” (コンマの使用)
  - “1:7” (コロンの使用)
  - “1. 2” (文字または数字が前にない空白)

ルール 2

参照情報の前又は後にくる全ての空白を示す文字 (U+0020)は無視される。

例

以下の参照情報はすべて同じものとみなされる：

- “6.4”
- “ 6.4”
- “6.4 ”

ルール 3

2 つ以上の参照情報が 1 つの Excel シートのセル内に置かれる場合、それらは以下のいずれかにより分けられなければならない(MUST)

- 各参照情報を別の行に置く
- 各参照情報をセミコロン(U+003B)で区切る

例

参照先である 6.3.1 と 6.3.2 を同居させる：

- 正

6.3.1; 6.3.2
6.3.1 6.3.2

- 誤

6.3.1 6.3.2
6.3.1, 6.3.2
6.3.1-2
6.3.1,2
6.3.1 and 6.3.2

推奨事項 1

参照情報では、章/節/部(chapters/sections/subsections)の区分にピリオド(U+002E)を用いるべきである。(SHOULD)

例

Annex A, section 1, subsection 2 の表記は”A.1.2”とし、”A-1.2”や”A1.2”は避ける。

推奨事項 2

あるフレームワークの中では、参照情報の記述は、一貫した章、節、部、項(paragraphs)の表記の基準を用いるべきである。(SHOULD)

例

- 一貫性のある表記
  - “Annex A 1.3”
  - “Annex A 1”

- “Annex A 2.3.5(c)”

- 一貫性のない表記
  - 記述法の乱れ
    - Annex A 1.3
    - Annex A.1.1
    - Clause 4.2.3 e)
    - Clause 4.2.5b
  - 章・節名の欠落
    - Clause 6.1
    - 6.4.3
    - Annex A.1.3
    - A.1
  - 記号の追加
    - PA12
    - PA-13

推奨事項３

参照先の文章内容は参照情報に含めるべきでない。(SHOULD NOT)

例

- 良い
  - “AR-7”
- 悪い
  - “AR-7 The organization designs information systems to support privacy by automating privacy controls.”

推奨事項４

１つのフレームワークの中では、大文字にする部分の一貫性を持つべきである。

例

“Annex A”, “annex A”, “annex a” の混在を避けること。

まとめ

この文書「CCM (Cloud Controls Matrix)におけるマッピング手法の解説」は、マッピングの作業をより分かりやすくするために書かれた。そのために、一般的なマッピングの作業の細部、例えば作業用シートの作成、様々なギャップの概要解説、参照情報の記述法など、を示し、CCM マッピングが機械で読めることと一貫性があることを目指した。

この文書は、ダウンロード可能な作業用シートのサンプルと併せて公開し、今後のマッピングプロジェクトの指針となるようにしたい。CSA は、CCM の進化に対応してこの文書を改訂し改良する積りである。そのために、いかなるコメントも気兼ねなく以下宛に送っていただきたい。 research-support@cloudsecurityalliance.org

定義

用語	定義
Candidate Framework 対象となるフレームワーク	一般に知られている評価のための基準全て（例：標準、規制、実践規範）。国際、国内、あるいは技術、業界固有のいずれも対象。
Domain ドメイン	特定のテーマに分類される、関連するセキュリティ管理策のセット。例えば、CSA の CCM のテーマは、CSA の 14 のドメイン（訳注：ガイダンスのドメイン）に対応している。
Full Gap 完全なギャップ	類似の規則（管理策）が対象のフレームワークの中にない。
Gap Analysis ギャップ分析	あるフレームワークの管理策の要求事項を他のフレームワークのそれにつなげるために必要な、追加の表現や行為を展開したもの。
Mapping(s) マッピング	CCM の管理策を一つ一つ CCM 以外のフレームワークに対応付けたもの。1 対 1 の場合と 1 対 n の場合がある。
No Gap ギャップなし	あるフレームワークの中の管理策の要求事項が他のフレームワークの関連する管理策の要求事項と完全に同等であること。
Partial Gap 部分的ギャップ	2 つのフレームワークの中の管理策が類似しているが完全に同等ではないこと。
Reverse Mapping リバースマッピング	マッピングと同じ。ただし、CCM でなく CCM 以外の（候補）フレームワークから見た形。
Semantic Equivalence 意味的な同等性	2 つのフレームワークの中の管理策が、内容（どのような記述でどのように分類されたか）から見て同じ意味を持つと判断された状態。
Security Controls セキュリティ管理策	組織にとっての情報セキュリティリスクを変化させるための、技術的もしくは管理的予防措置または対策。

以上