

COBITとCiscoソリューションのマッピング

Objective (COBIT 4.0における統制項目)	ASA 5500	PIX	IPS	CSA	NAC	CCA	Guard	Cisco Works	IOS Router	Catalyst CIF	ACS	MARS	ICS	Wireless AP	NAM	CSM
DS1.5																
DS2.4																
DS5.3																
DS5.4																
DS5.5																
DS5.6																
DS5.7																
DS5.8																
DS5.9																
DS5.10																
DS5.11																
DS9.1																
DS9.2																
DS9.3																
DS10.2																
DS11.6																

参考: COBIT成熟度モデル

COBITでは、各統制項目ごとに成熟度レベルの規準を定義しています。各レベルの目安を要約すると、以下のようになります。

成熟度	要約
レベル0: 存在しない (Non-Existent)	IT セキュリティの必要性を認識していない。責任者が不明で管理されていない。
レベル1: 初歩的 (Initial / Ad Hoc)	IT セキュリティは事後対処的であり、実行責任が明確になっていない。
レベル2: 反復可能 (Repeatable but Intuitive)	実行責任が割り当てられており、セキュリティに関する情報が生成されるが、分析は行われていない。事故への対応は後手に回りがちである。
レベル3: 定義されている (Defined Process)	会社の方針に沿ったプロセスが定められている。計画やリスク分析に基づいた対応を行っているが、強制実行されるわけではない。
レベル4: 管理されている (Managed and Measurable)	実行責任が明確に割り当てられて、管理され、そのとおり運用(強制または制度化)されている。プロセスは全社的に整合性があり、経営目標とリンクしている。
レベル5: 最適化されている (Optimized)	リスクの変化と発生に応じて早期警告を発するための自動化されたシステムがあり、事故はツールの支援によって直ちに処理される。新たな処理や脆弱性についての情報はシステムチェックに収集・分析され、速やかに適切なコントロールが導入される。

原文	COBIT 4.0 の原文
要約	<ul style="list-style-type: none">• 原文の要約です
ネットワーク要件	<ul style="list-style-type: none">• このオブジェクト(COBIT 4.0 で定義されている統制項目) 達成のために、ネットワークで対応すべき要件を示します
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• 上記のネットワーク要件に対応する製品・ソリューションを示します• () 内は対応する成熟度レベルを示します

原文	Continuously monitor specified service level performance criteria. Reports are provided in a format meaningful to the stakeholders on achievement of service levels. The monitoring statistics are analyzed and acted upon to identify negative and positive trends for individual services as well as for services overall.
要約	<ul style="list-style-type: none">• モニタリングは継続的に行われなくてはならない• レポートは SLA のステークホルダー (利害関係者) に有効なフォーマットで提出されなくてはならない• モニタリングの統計情報は、個々のサービスに対しての正負の傾向を把握するために分析され、実践活用されなくてはならない• モニタリングの統計情報は、サービス全体に対しての正負の傾向を把握するために分析され、実践活用されなくてはならない
ネットワーク要件	<ul style="list-style-type: none">• サービスや、その構成要素たるネットワークをモニタリングする装置・仕組みを導入しなくてはならない• モニタリング装置だけでなく、その為に利用されるネットワークの冗長性の確保を考慮しなくてはならない• モニタリング装置は、あらかじめ決められたSLAに対して、現状が評価可能な内容のレポートを出力できること• モニタリング装置は、モニタリングの統計分析に必要なデータの出力や、分析結果の出力をサポートすべきである• モニタリング装置は、サービス全体および個々のサービスを分別した形式で、データや分析結果の出力をサポートすべきである
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• NAM(4) : ネットワークに流れるパケットの単純な統計情報だけでなく、アプリケーションのレスポンス タイムやビデオの品質などを計測し、レポート表示および外部機器へのデータ出力が可能。• IP SLA (4) : ルータやスイッチなどネットワーク機器自身が、IP パケットの到達性やジッタ、レイテンシなど SLA の計測を行い、更に計測結果に基づいて経路変更などのアクションを自律的に実行する。• 3rd Party製品 (Concord, CRANNOG)+IP SLA(5) : IP SLA 機能による計測結果を集計・加工し、顧客や管理者へのレポートの作成・表示、および契約した規準に対する合否判定などを自動化。

原文	Establish a process to monitor service delivery to ensure the supplier is meeting current business requirements and is continuing to adhere to the contract agreements and service level agreements, and that performance is competitive with alternative suppliers and market conditions.
要約	<ul style="list-style-type: none">• 提供を受けているサービスが、<ul style="list-style-type: none">-現在のビジネス要求に合っているか-SLA や契約が守られているか-他のサービス提供者や市場の状況と対比して劣っていないか を監視するプロセスが必要である。
ネットワーク要件	<ul style="list-style-type: none">• ネットワーク要件は DS 1.5 と同等と考えられる• サービス提供者側の視点では、提供しているサービスを顧客が確認するために必要なレポート機能を提供する必要がある
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• 3rd Party製品 (Concord, CRANNOG)+IP SLA (5) : IP SLA で取得した SLA の評価情報を元にさまざまなレポートを表示したり、規定した SLA を満たしているか否か顧客へレポートする。

原文	<p>All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository.</p> <p>Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.</p>
要約	<ul style="list-style-type: none">• 派遣社員やエクストラネット接続も含めたすべてのユーザを、すべてのアプリケーション・IT システム上で識別できなければいけない• データやシステムに対するユーザのアクセス権は、ビジネス要件に沿って定義され、ドキュメント化されなければいけない• ユーザのアクセス権はセキュリティ責任者により集中管理され、各 IT システムのオーナーによって承認されなければいけない• これらの実現においては、効率的かつ体系化された手法が用いられるべきである
ネットワーク要件	<ul style="list-style-type: none">• MS-AD などのユーザ データベースにより、アプリケーションや OS へのアクセス時に認証が行われる事が前提条件として必要• データベースに登録されていない(識別されていない)侵入者がアプリケーションや OS の脆弱性を突いて不正侵入したり、ネットワーク上の盗聴によって正規ユーザになりすます行為を防止しなければいけない• ネットワークへのアクセス権は、アプリケーションや OS へのアクセス権と同じデータベースで集中管理されなければいけない
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• 802.1x+ACS(4) : 802.1x によりネットワーク接続時にユーザの認証を行う。認証サーバとして ACS を利用する事により、セキュアな認証方式を使用可能。ユーザデータベースとして LADP や Active Directory を利用可能。• CCA(4) : ID/パスワードによるユーザの認証と、端末 PC の脆弱性診断結果に基づくアクセス制限を実施。• CISF(Catalyst Integrated Security Features) (4) : DHCP-Snooping や Dinamic ARP Inspection といった Catalyst の高度なセキュリティ機能を実行することで、ARP や DHCP が潜在的に持っている脆弱性を突いたネットワーク上での盗聴行為を防御し、ID/パスワードの奪取によるアカウントの乗っ取り・なりすましを未然に防ぐ。

原文	Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.
要約	<ul style="list-style-type: none">• ユーザ アカウントおよび関連する特権についての要求、設定、発行、停止、修正および削除のプロセスが管理されていない• アカウントの承認プロセスは、システム オーナーが認めたアクセス特権(を持つ管理者)により実行されるべきである• 承認プロセスは、緊急的対応を含めたすべてのケースにおいて、すべてのユーザ(特権ユーザやエクストラネット接続も含む)に対して適用されなければいけない• すべてのユーザの権利と義務が、契約により合意されていない• 全アカウントと特権について、定期的にレビューされなければいけない
ネットワーク要件	<ul style="list-style-type: none">• ネットワーク機器自体へのアクセス権限も、アプリケーションや OS と同様に管理されなければいけない
対応ソリューション (成熟度レベル)	RBAC: Role-based AccessControl(4) : ネットワーク機器へアクセスするための管理者用アカウントに対して、その役割に応じた制限を設けることができる。機器へのログイン後に使用できるコマンドや、操作できるコンテキストなどをアカウントごとに柔軟に設定することが可能。

原文	Ensure that IT security implementation is tested and monitored proactively. IT security should be reaccredited periodically to ensure the approved security level is maintained. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Access to the logging information is in line with business requirements in terms of access rights and retention requirements.
要約	<ul style="list-style-type: none">• 導入されている IT セキュリティのテストと監視を積極的に行わなくてはならない• 認可されたセキュリティ レベルが確保されていることを保証するために、IT セキュリティは定期的に再認可を受けるべきである• ログ情報へのアクセスは厳重に管理されるべきである
ネットワーク要件	<ul style="list-style-type: none">• 定期的なセキュリティ診断サービスもしくは装置が必要• セキュリティ ログから攻撃および不審な活動を把握できる仕組みが必要• ログを集積する装置では、権限に基づいたデータの参照・操作が可能でなくてはならない
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• MARS (5) : ネットワーク機器やホストからセキュリティに関するログを収集し、ネットワーク トポロジとの相関分析によって、発生しているインシデントの原因と対処方法を管理者に通知する。トラフィックの統計情報を分析することで、ログだけでは発見できない異常を検知することが可能。MARS が収集したログ情報に対して参照・操作できる権限は、アカウントごとに厳密に設定することが可能。• CSA + Antivirus (4) : ソフトウェアの不振な振る舞いを検知し、ユーザや管理者への警告および実行の可否を制限する。• nCircle, Qualys (4) : 脆弱性診断を可能にするこれらの製品によって、現在システムが抱えているセキュリティ上の問題点を洗い出すことができる。

原文	Ensure that the characteristics of potential security incidents are clearly defined and communicated so security incidents can be properly treated by the incident or problem management process. Characteristics include a description of what is considered a security incident and its impact level. A limited number of impact levels are defined and for each the specific actions required and the people who need to be notified are identified.
要約	<ul style="list-style-type: none">• 潜在的なセキュリティ侵害の可能性について明確に定義され、議論されるべきである• このセキュリティ侵害自身がどういったものなのかと、それによる被害の大きさ(被害レベル)をまとめる• 被害レベルは限られた数の範囲で定義していなくてはならない(1~5までなど)• それぞれの被害レベルに応じた対応策、通知されるべき人物が定義されていなくてはならない
ネットワーク要件	<ul style="list-style-type: none">• 単なるログや警報の発出だけでなく、攻撃の対象範囲や被害レベルを正確に把握し、適切なオペレータへの報告および対応を支援することのできるネットワーク機器・監視装置が必要
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• IPS、IOS-IPS、AIP-SSM(5) : 発生したインシデントの攻撃対象となっている端末の重要性や攻撃の有効性などを基に、管理者へリスク重要度を示すことが可能。リスク重要度に応じて自律的に実行されるアクションを任意に設定することが可能。• Trendmicro DCS + ICS(5) : IPS で防御されたウイルスの情報を収集し、感染した PC から駆除を行う。• MARS(4) : 同じ原因から派生した複数のログを、相関分析によってひとつのインシデントとして集約する。管理者がインシデントの重要性を正しく把握することを支援する。

原文	Ensure that important security-related technology is made resistant to tampering and security documentation is not disclosed unnecessarily, i.e., it keeps a low profile. However, do not make security of systems reliant on secrecy of security specifications.
要約	<ul style="list-style-type: none">• セキュリティ システム自身への侵害に対して、耐久性を有していなければならない• 不必要にセキュリティに関するドキュメントを開示してはならない
ネットワーク要件	<ul style="list-style-type: none">• セキュリティ製品に対する攻撃に対して、製品自身がセキュアであること• ネットワーク製品に対する攻撃に対して、製品自身がセキュアであること• システムを構成している機器が特定不可能である必要がある
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• NFP:Network Foundation Protection (4) : Control Plane Policing や UnicastRPF など、ネットワーク機器自体への攻撃を防御し、攻撃元を調査するための機能群。• Guard (4) : セキュリティ製品・ネットワーク デバイス自身に対する DOS 攻撃による、不正侵入やサービス妨害から保護する。

原文	Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.
要約	<ul style="list-style-type: none">• 暗号鍵の取り扱いに関する手順やポリシーを決定しなければならない
ネットワーク要件	<ul style="list-style-type: none">• 暗号鍵の管理を行うシステムがあるとよい• 暗号鍵が解読されることのないようなプロトコルを採用しなければならない• 暗号鍵が漏洩しないように、端末を防衛する仕組みが必要• 暗号鍵の受け渡しを行う際には、その通信路を必ず暗号化しなければならない
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• CSA(4) : PC に対するさまざまな操作を制限する。証明書のエクスポートを拒否したり、アプリケーションに記憶されている暗号を含む設定情報の閲覧を禁止することなどが可能。端末からの暗号鍵の漏洩リスクを最小限に止める。• WPA, EAP-FAST(4) : 無線区間において暗号鍵が解読されるリスクに対して、一定の耐性を確保する。認証偽造などの不正を防ぎ、暗号鍵を保護する。• VPN(4) : 通信路の暗号化を行う。VPN 専用装置だけでなく、Firewall や IOS ルータでも VPN を利用することができる。

原文	Ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.).
要約	<ul style="list-style-type: none">• 脆弱性からの防御、脆弱性の検知、セキュリティパッチの適用を実現する仕組みを導入しなければならない• ウイルスからの防御、ウイルス定義ファイルの更新状況チェック、定義ファイルの適用を実現する仕組みを導入しなければならない• ウイルスだけでなく、ワームやスパイウェアなど、さまざまなマルウェアからの防御を実現しなければならない
ネットワーク要件	<ul style="list-style-type: none">• 同上
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• IPS (4) : システムの脆弱性に対する攻撃から防御する。ネットワーク ウイルスによる攻撃 / 感染活動などからシステムを保護する。• IPS +ICS (4) : 危険度の高い新たなウイルスが発見された場合に、ベンダーから正規のシグニチャが配信される前に、ウイルスの拡散を自律的に防止する。• CSA (4) : 脆弱性に対する攻撃や、未知のものを含むウイルスの発症を防ぐ。その他のさまざまなマルウェアの引き起こす悪影響を防止する。• CSC-SSM (4) : Web や E メール の通信を利用して拡散するウイルスやアドウェア、マルウェアを検知し、削除するなどの防御を行う。• NAC/CCA (4) : ネットワークへアクセスする端末に対して、OS のパッチやウイルス定義ファイルのバージョンなど状態を把握し、任意に定められるポリシーに準拠しているか否かを判断して、接続制限などを行う• ITAM +NAC (4) : ネットワークへアクセスする端末に対して、適切な資産管理用クライアントが動作していること、および辞書データベースのバージョンがポリシーに合致していることを確認し、資産管理を完全なものとする

原文	Ensure that security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) are used to authorize access and control information flows from and to networks.
要約	<ul style="list-style-type: none">• Firewall、IDS/IPS などのセキュリティ製品や、ネットワークのセグメンテーションなどによる運用手法を活用し、ネットワークのアクセスを適切にコントロールしなくてはならない
ネットワーク要件	<ul style="list-style-type: none">• ネットワーク機器での、VLAN や豊富なアクセス リストのサポートが必要• セキュリティ機器との連携により、ネットワーク機器でのコントロールが可能であればよりよい• Firewall をはじめとしたセキュリティ機器が必要だが、さまざまな脅威に対処できる必要がある
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• Cisco Self Defending Network (4) : Firewall 装置, VPN 装置など個別のセキュリティ機器を設置するだけでは昨今の多様なセキュリティの脅威には十分な対応ができないという認識に基づき、あらゆるネットワーク機器とセキュリティ機能が有機的に連携し、インシデントからの自律的な防御と対策を行う。• CISF (4) : ARP や DHCP のプロセスを不正に操作することで行われる「なりすまし」や盗聴などから通信を防御する。Catalyst シリーズに標準で実装される。

原文	Ensure sensitive transaction data are exchanged only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.
要約	<ul style="list-style-type: none">• 重要な通信は、信頼できる経路上のみでやりとりされる必要がある• もしくは、内容の確認・提出の証明・受領の証明とデータ源の承認が提供されるメディア上でやりとりされる必要がある
ネットワーク要件	<ul style="list-style-type: none">• セキュアな暗号化通信を可能にする仕組みが必要• 盗聴・改ざん・なりすましなど、通信データに対する脅威からデータを防御することができる仕組みが必要
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• VPN(4): 通信路を暗号化する。VPN 機能は、専用装置だけでなく、Firewall 装置や IOS ルータなどで幅広く提供されており、さまざまな要件に応じて構成可能である。• CISF(4): ARP や DHCP のプロセスを不正に操作することで行われる、なりすましや盗聴などから通信を防御する。Catalyst シリーズに標準で実装される。

原文	Establish a central repository to contain all relevant information on configuration items. This repository includes hardware, application software, middleware, parameters, documentation, procedures and tools for operating, accessing and using the systems and services. Relevant information to consider is naming, version numbers and licensing details. A baseline of configuration items should be kept for every system and service as a checkpoint to which to return after changes.
要約	<ul style="list-style-type: none">• さまざまな IT 資産を中央管理するためのシステムが必要• 変更後もすぐに戻せるように、基本となるデータは保持しておくべきである
ネットワーク要件	<ul style="list-style-type: none">• ネットワーク機器、セキュリティ機器のバージョン管理や設定変更の管理が必要• IT 資産全般の管理が必要
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• CiscoWorks(4) : ネットワーク機器のバージョン管理、設定変更の履歴管理などを行う。• CSM(4) : セキュリティ機器のバージョン管理、設定変更の履歴管理などを行う。

原文	<p>Put procedures in place to:</p> <ul style="list-style-type: none">• Identify configuration items and their attributes• Record new, modified and deleted configuration items• Identify and maintain the relationships among configuration items in the configuration repository• Update existing configuration items into the configuration repository• Prevent the inclusion of unauthorized software <p>These procedures should provide proper authorization and logging of all actions on the configuration repository and be properly integrated with change management and problem management procedures.</p>
要約	<ul style="list-style-type: none">• 管理対象となるアイテムとそれらの属性を定義する<ul style="list-style-type: none">- 新規作成、編集、削除の履歴を記録する- 管理データベースに記録されている管理対象となるアイテム間の関係を明確化し、管理する- 現在の状態のアップデートを管理データベースに対して行う- 非認可ソフトウェアの混入を阻止する <p>これらの手順が、適切に変更管理や問題管理の手順と統合されているべきである</p>
ネットワーク要件	<ul style="list-style-type: none">• 変更管理、資産管理などを実現した上で、それを強制する仕組みが必要
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• ITAM +NAC (4) : ネットワークへアクセスする端末に対して、適切な資産管理用クライアントが動作していること、および辞書データベースのバージョンがポリシーに合致していることを確認し、資産管理を完全なものとする。• CSA (5) : アプリケーションのインストールを禁止することが可能。

原文	Review and verify on a regular basis, using, where necessary, appropriate tools, the status of configuration items to confirm the integrity of the current and historical configuration data and to compare against the actual situation. Review periodically against the policy for software usage the existence of any personal or unlicensed software or any software instances in excess of current license agreements. Errors and deviations should be reported, acted on and corrected.
要約	<ul style="list-style-type: none">• 実装されているシステムの完全性のレビューを、定期的実施しなければならない• ソフトウェアのライセンスに違反しているようなことがないか、確認する必要がある• エラーと改善方針はレポートされ、実行され、改善されなくてはならない
ネットワーク要件	<ul style="list-style-type: none">• ネットワーク機器の設定のバージョン管理・ライセンス管理を行う必要がある
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• CiscoWorks(4) : ネットワーク機器のバージョン管理、設定変更の履歴管理などを行う。• CSM(4) : セキュリティ機器のバージョン管理、設定変更の履歴管理などを行う。

原文	<p>The problem management system should provide for adequate audit trail facilities that allow tracking, analyzing and determining the root cause of all reported problems considering:</p> <ul style="list-style-type: none">• All associated configuration items• Outstanding problems and incidents• Known and suspected errors <p>Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management should escalate the problem, perhaps referring it to an appropriate board to increase the priority of the request for change (RFC) or to implement an urgent change as appropriate. The progress of problem resolution should be monitored against SLAs.</p>
要約	<ul style="list-style-type: none">• 問題管理システムは、根本原因の特定や分析、追跡などを可能にする監査記録を持つ必要がある• 変更管理システムと問題管理システムは協調して活用され、問題を迅速に解決する仕組みが必要である• 問題解決の進捗状況は、SLA に照らして評価されるべきである
ネットワーク要件	<ul style="list-style-type: none">• 発生する問題(サービスレベルの低下、障害、攻撃など)を、原因特定可能な情報を含んで管理するシステムが必要• 問題管理と変更管理が統合されているシステムが必要
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• MARS(4):セキュリティインシデントの記録、および上位の監視装置へのエスカレーションを行う。

原文	Establish arrangements to identify and apply security requirements applicable to the receipt, processing, physical storage and output of data and sensitive messages. This includes physical records, data transmissions and any data stored offsite.
要約	<ul style="list-style-type: none">• 物理メディアやデータ転送、データ蓄積用地などを含んだデータの取り扱い方法について、セキュリティを確保可能な取り決めを策定しなくてはならない
ネットワーク要件	<ul style="list-style-type: none">• データの転送においては、安全な暗号化が必要である• データを蓄積する際には、暗号化して保存することのできる装置などが必要である
対応ソリューション (成熟度レベル)	<ul style="list-style-type: none">• VPN(4): 通信路を暗号化する。VPN 機能は、専用装置だけでなく、Firewall 装置 や IOS ルータなどで幅広く提供されており、さまざまな要件に応じて構成可能である。