D．２　NIST SP 800-171 の要求事項と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
アクセス制御	3.1.1	システムアクセスを許可された利用者、許可された利用者を代行して動作するプロセス、またはデバイス(その他のシステムを含めて) に制限する。	・AC-2 アカウント管理 ・AC-3 アクセス制御の実施 ・AC-17 リモートアクセス	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 －パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 －新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 －暗号によって保護されたパスワードのみを保存・伝送する。 －パスワードの有効期間を組織が設定する。 －同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 －強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.1.2	システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。	・AC-2 アカウント管理 ・AC-3 アクセス制御の実施 ・AC-17 リモートアクセス	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 －パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 －新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 －暗号によって保護されたパスワードのみを保存・伝送する。 －パスワードの有効期間を組織が設定する。 －同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 －強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.1.3	承認された権限付与に従ってCUI のフローを制御する。	・AC-4 情報フロー制御の実施	CPS.AC-7	・適宜ネットワークを分離する(例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する	H.Advanced	・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可とする。 ・機密性の高いデータを取り扱う自組織のシステムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
						Basic	・組織は、システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、フローの制御を実施する。
				CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	H.Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。
	3.1.4	共謀のない悪意のあるアクティビティのリスク低減のため、個人の職務を分離する。	・AC-5 職務の分離	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	H.Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・組織は、非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。 ・システムは、特権の機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。
						Advanced	・組織は、自組織のシステムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.1.5	具体的なセキュリティ機能と特権アカウントを含め、特権の最小化の原則を採用する。	・AC-6 特権の最小化 ・AC-6(1) 特権の最小化 セキュリティ機能へのアクセスを許可する ・AC-6(5) 特権の最小化 特権アカウント	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	H.Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・組織は、非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。 ・システムは、特権の機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。
						Advanced	・組織は、自組織のシステムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.1.6	非セキュリティ機能をアクセスするときは、非特権アカウントまたは役割を使用する。	・AC-6(2) 特権の最小化 非セキュリティ機能の非特権アクセス				・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.7	非特権利用者による特権機能の実行とこのような機能の実行の監査を防止する。	・AC-6(9) 特権の最小化 特権機能の利用の監査 ・AC-6(10) 特権の最小化 特権機能の実行を非特権利用者に禁止する	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	H.Advanced	・組織は、非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。 ・システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。
	3.1.8	ログイン試行失敗を制限する。	・AC-7 ログイン試行の失敗	CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ	H.Advanced	・システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には管理者が解除しなければ再ログインできない機能を実装する。
						Advanced	・システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。
	3.1.9	適用可能なCUI 規則と整合性のあるプライバシーとセキュリティの通知を提供する。	・AC-8 システムの利用に関する通知	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.1.10	非アクティブな時間の経過後、データのアクセス及び閲覧を防止するため、パタンによる不可視化表示を用いてセションロックを使用する。	・AC-11 セションのロック ・AC-11(1) セションのロック パタンによる不可視化表示	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.1.11	定義された条件の後、利用者セションを(自動的に)終了する。	・AC-12 セションの終了	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
	3.1.12	リモートアクセスセションを監視し、制御する。	・AC-17(1) リモートアクセス 自動化された監視／管理	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.1.13	リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。	・AC-17(2) リモートアクセス 暗号化を用いた機密性／完全性の保護				
	3.1.14	管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。	・AC-17(3) リモートアクセス 管理されたアクセス制御ポイント				
	3.1.15	特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。	・AC-17(4) リモートアクセス 特権コマンド／アクセス				

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.1.16	無線のコネクションを許可する前に無線アクセスを許可する。	・AC-18 無線アクセスの制限	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
						Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
						Basic	・組織は、許可しているリモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。 ・組織は、自組織のシステムへのリモートアクセスの利用に関する承認ルール等を定める。 ・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。
	3.1.17	認証と暗号化を用いて無線アクセスを保護する。	・AC-18(1) 無線アクセス 認証と暗号化	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.1.18	モバイルデバイスのコネクションを制御する。	・AC-19 携帯機器に対するアクセス制御	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
						Advanced	・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。 ・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。
	3.1.19	モバイルデバイス及びモバイルコンピューティングプラットフォーム上のCUI を暗号化する。	・AC-19(5) 携帯機器に対するアクセス制御 デバイス全体／コンテナベースの暗号化	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.1.20	外部システムへのコネクション及び使用を検証し、制御／制限する。	・AC-20 外部情報システムの利用 ・AC-20(1) 外部情報システムの利用 許可された利用の制限	CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、保管する	Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上での自組織のポータブルストレージの使用を制限する。
	3.1.21	外部システム上での組織のポータブルストレージデバイスの使用を制限する。	・AC-20(2) 外部情報システムの利用 ポータブルストレージデバイス				
	3.1.22	公開アクセス可能なシステムにおいて掲載または処理されるCUI を制御する。	・AC-22 公的アクセス可能なコンテンツ	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う	Basic	・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。 ・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。 ・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化)
意識向上と訓練	3.2.1	組織のシステムの責任者、システム管理者、及び利用者が、彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー、基準、及び手順について周知されていることを、保証する。	・AT-2 セキュリティの意識向上 ・AT-3 ロールベースのセキュリティトレーニング	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデント発生を抑止するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施する	H.Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
						Advanced	・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。 ・組織は、情報セキュリティ要員の育成とレベル向上のためのプログラムを作成し、定期的に該当する要員に対して実施する。
				CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる関係組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施する	Advanced	・組織は、自組織におけるセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練、セキュリティ教育を実施を要求し、その実施状況を確認する。
						Basic	・組織は、自組織の要員へ割り当てられた役割を遂行するための適切な訓練、セキュリティ教育を実施を要求し、その実施状況を確認する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.2.2	組織の要員が、その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを、保証する。	・AT-2 セキュリティの意識向上 ・AT-3 ロールベースのセキュリティトレーニング	CPS.AT-2	・自組織におけるセキュリティインシデントに関係しうる関係組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施する	Advanced	・組織は、自組織におけるセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練、セキュリティ教育を実施を要求し、その実施状況を確認する。
	3.2.3	内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を提供する。	・AT-2(2) セキュリティの意識向上 内部の脅威	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデント発生を抑止するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施する	H.Advanced	・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。
監査と責任追跡性（説明責任）	3.3.1	非合法の、許可されない、または不適切なシステムアクティビティの監視、分析、調査、及び報告を可能とするために必要な範囲で、システム監査記録を作成、保護、及び維持する。	・AU-2 監査対象のイベント ・AU-3 監査記録の内容 ・AU-3(1) 監査記録の内容 追加の監査情報 ・AU-6 監査記録の監視、分析、及び報告 ・AU-12 監査の生成	CPS.SC-5	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先およびその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。
						Advanced	・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。 ・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能をシステムが提供する。 ・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。 ・組織は、手作業ないしはシステムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。 ・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。
				CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じ
	3.3.2	個別のシステム利用者のアクションが、彼らのアクションについての説明責任を維持可能にするよう、それらの利用者に対して一意に追跡が可能であることを保証する。	・AU-2 監査対象のイベント ・AU-3 監査記録の内容 ・AU-3(1) 監査記録の内容 追加の監査情報 ・AU-6 監査記録の監視、分析、及び報告 ・AU-12 監査の生成	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。
	3.3.3	監査された事象をレビューし、アップデートする。	・AU-2(3) 監査対象のイベント レビューとアップデート	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
						Basic	・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。 ・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。 ・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.3.4	監査プロセス失敗の事象においてアラート(警告) を発する。	・AU-5 監査処理エラーへの対応	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
	3.3.5	監査記録のレビュー、分析、及び調査のための報告プロセスを集めて相互の関係を比較し、不適切な、疑わしい、または異常なアクティビティの兆候に対応する。	・AU-6(3) 監査記録の監視、分析、及び報告 監査リポジトリとの相互の関連付け	CPS.SC-5	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する	H.Advanced	・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織は、特に重要な取引先およびその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。 ・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。
	3.3.6	オンデマンド分析と報告をサポートするため、監査の簡素化と報告書生成を提供する。	・AU-7 監査量の低減と報告書の作成	CPS.AN-2	・セキュリティ事象発生後に、デジタルフォレンジックを実施する	H.Advanced	・システムが、重要なセキュリティインシデントに関する監査記録について処理するプロシージャを提供する。
						Advanced	・組織は、媒体，装置及び装置の状態(例えば，電源が入っているか，切れているか)に従って，証拠の特定，収集，取得及び保存のプロシージャを規定する ・組織は、重要なセキュリティインシデントについて、発生後に下記の証跡を保全することが望ましい。 - 識別情報(インシデントの発生場所/発生日時/対象となるモノのシリアル番号/ホスト名/MACアドレス/IPアドレス等) - 証跡を収集・処理したヒトの役職、名前、連絡先 - 証跡保全処理の日時(タイムゾーンを含む)
						Basic	・組織は，証拠となり得るデータを特定，収集，取得及び保存するためのプロシージャを定め，運用する。
	3.3.7	監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し同期するようなシステム機能を提供する。	・AU-8 タイムスタンプ ・AU-8(1) タイムスタンプ 権威ある時刻ソースとの同期	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
	3.3.8	監査情報と監査ツールを不正なアクセス、改変、及び削除から保護する。	・AU-9 監査情報の保護	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
	3.3.9	監査機能の管理を特権利用者の一部に制限する。	・AU-9(4) 監査情報の保護 特権利用者のサブセットによるアクセス	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	H.Advanced	・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。 ・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。 ・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。 ・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。
						Advanced	・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。 ・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。 ・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。
構成管理				CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Advanced	・資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、システムコンポーネント上で利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織のシステムを構成する資産(ハードウェア、ソフトウェア、情報)を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP.33を参照することが可能である。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.4.1	個別のシステム開発ライフサイクル全体で、組織のシステム (ハードウェア、ソフトウェア、ファームウェア、及び文書を含めて) のベースライン構成とインベントリを確立し、維持する。	・CM-2 ベースライン構成 ・CM-6 構成設定 ・CM-8 情報システムコンポーネントのインベントリ ・CM-8(1) 情報システムコンポーネントのインベントリ インストレーション／除去中のアップデート	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	H.Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。
						Basic	・組織は、システムのネットワーク構成、資産、機器の設定情報、構成情報等のベースラインとなる情報を文書化し、内容が適切かどうかを定期的に確認する。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
						Basic	・IoT機器、サーバ等を含む資産の型番やソフトウェアのバージョン、サポート期限等を管理する台帳を作成し、定期的に棚卸する。 ・組織は、運用時に実施すべき対策（IoTデバイスの不正利用や盗難、パッチの適用、ログのチェック等）、IoT機器の状況を定期的に確認する。
	3.4.2	組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し、強制 (実施) する。	・CM-2 ベースライン構成 ・CM-6 構成設定 ・CM-8 情報システムコンポーネントのインベントリ ・CM-8(1) 情報システムコンポーネントのインベントリ インストレーション／除去中のアップデート	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	H.Advanced	・組織は、自組織のシステムを構成する資産(IoT機器等を含むハードウェア、ソフトウェア、情報)を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・システムは、認可されていない資産を自動的に検出するメカニズムを導入、運用している。 [参考] 重要度の算出方法には、"中小企業の情報セキュリティ対策ガイドライン ver.2.1"(IPA, 2018年)P.30～P.34に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、"制御システムのセキュリティスク分析ガイド"(IPA, 2018年)のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある
				CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。
						Basic	・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。 ・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-4で定めたポリシーに準じていない場合に、適切なものへと変更する。 ・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する
	3.4.3	組織のシステムへの変更を追跡、レビュー、承認／非承認、及び監査する。	・CM-3 構成変更管理	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
	3.4.4	実装に先立ち、変更のセキュリティへの影響を分析する。	・CM-4 構成変更の監視	CPS.IP-1	・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する	Advanced	・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。 ・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。 ・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。
	3.4.5	組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し、文書化し、承認し、強制 (実施) する。	・CM-5 変更のためのアクセス制限				
	3.4.6	基本機能のみを提供するように組織のシステムを構成することによって、最小機能の原則を採用する。	・CM-7 機能の最小化	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する	H.Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する
	3.4.7	非基本プログラム、機能、ポート、プロトコル、及びサービスの使用を制限、無効化、及び防止する。	・CM-7(1) 機能の最小化 定期的なレビュー ・CM-7(2) 機能の最小化 プログラム実行の防止	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する	H.Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
		許可されないソフトウェアの使用を防止するために例	・CM-7(2) 機能の最小化	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する	H.Advanced	・組織は、自組織のシステム上で実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施するとともに、許可されていないソフトウェアのインストールを不可とする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.4.8	外による拒否 (ブラックリスト) ポリシーを、または許可されたソフトウェアの実行を許可するような例外による許可 (ホワイトリスト)ポリシーを適用する。	プログラム実行の防止 ・CM-7(5) 機能の最小化 許可されたソフトウェア／ホワイトリスト	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する	H.Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
	3.4.9	利用者がインストールしたソフトウェアを管理し、監視する。	・CM-11 利用者がインストールしたソフトウェア	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する	H.Advanced	・組織は、自組織のシステム上で実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施するとともに、許可されていないソフトウェアのインストールを不可とする。
						Advanced	・組織は、自組織のシステム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、モニタリングを実施する。
識別と認証	3.5.1	システム利用者、利用者を代行して動作するプロセス、またはデバイスを識別する。	・IA-2 ユーザ識別及び認証 ・IA-5 認証コードの管理	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、二つ以上の認証機能を組み合わせた多要素認証を採用する	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・システムは、自組織のシステムについて特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。
						Basic	・組織は、自組織のシステムについて特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、一意に識別する認証を実施する。
	3.5.2	組織のシステムへのアクセスの許可に対する必要条件として、それらの利用者、プロセス、またはデバイスのアイデンティティを認証(または検証)する。	・IA-2 ユーザ識別及び認証 ・IA-5 認証コードの管理	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.5.3	多要素認証を、特権アカウントへのローカル及びネットワークアクセスのために、及び非特権アカウントへのネットワークアクセスのために、使用する。	・IA-2(1) ユーザ識別及び認証 特権アカウントへのネットワークアクセス ・IA-2(2) ユーザ識別及び認証 非特権アカウントへのネットワークアクセス ・IA-2(3) ユーザ識別及び認証 特権アカウントへのローカルアクセス	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、二つ以上の認証機能を組み合わせた多要素認証を採用する	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
						Advanced	・システムは、自組織のシステムについて特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。
	3.5.4	特権及び非特権アカウントへのネットワークアクセスのために、リプレイ耐性のある認証メカニズムを採用する。	・IA-2(8) ユーザ識別及び認証 特権アカウントへのネットワークアクセスーリプレイ耐性 ・IA-2(9) ユーザ識別及び認証 非特権アカウントへのネットワークアクセスーリプレイ耐性	CPS.AC-6	・特権を持つユーザーのシステムへのログインに対して、二つ以上の認証機能を組み合わせた多要素認証を採用する	H.Advanced	・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。 ・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。 [参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。
	3.5.5	定義された期間について、識別コードの再利用を禁止する。	・IA-4 識別子の管理	CPS.AC-8	・IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データ)をサイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。
	3.5.6	定義された非アクティブな期間の後、識別子を無効化する。	・IA-4 識別子の管理				
						H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.5.7	新しいパスワードが作成されるとき、最小パスワード複雑性及び文字列の変更を強制(実施)する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.5.8	規定された生成回数の間、パスワードの再利用を禁止する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.5.9	永久パスワードへ直ちに変更するようなときのシステムログインのために一時的パスワードの使用を許可する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。
	3.5.10	暗号学的に保護されたパスワードのみを格納及び送信する。	・IA-5(1) 認証コードの管理 パスワードベース認証	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.5.11	認証情報のフィードバックを目に見えないようにする。	・IA-6 認証コードのフィードバック	CPS.AC-9	・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する	H.Advanced	・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。 ・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。
						Advanced	・組織は、ユーザの挙元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うカテゴリスクの強度を持った認証を実施する。 ・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。 ・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。 ・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。 - パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 - 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。 - 暗号によって保護されたパスワードのみを保存・伝送する。 - パスワードの有効期間を組織が設定する。 - 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。 - 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。 ・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。 ・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバ等に画面を切替えるとで、セッションをロックする。
インシデント対応	3.6.1	適切な準備、検知、分析、抑制 (封じ込め)、リカバリ、及び利用者対応アクティビティを含めて、組織のシステムのための運用上のインシデントハンドリング能力を確立する。	・IR-2 インシデント対応のトレーニング ・IR-4 インシデントの対応 ・IR-5 インシデントの監視 ・IR-6 インシデントの報告 ・IR-7 インシデント対応の支援	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、関係者間で対応プロセスの整備と訓練を行う	H.Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。 [参考]サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティインシデントを検知・分析・対応する体制を整える	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。プロセスの内容については、CPS.RP-1等を参照。 ・組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には下記を含むことが望ましい。 - ログ分析の分析結果 (対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) - モニタリングにおける今後の改善方針 [参考]セキュリティ対策組織(SOC/CSIRT)の業務、望まれる規模等については、"セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～"(IS0G-J, 2018年)等を参照することが望ましい。
				CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定している	Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。
				CPS.RP-1	・対応が必要なセキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する ・不適切なセキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後のIoT機器、サーバ等による振る舞いをあらかじめ定義し、実装する	Basic	・組織は、対処が必要と判断されたセキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスには、下記を例とする内容を含むことが望ましい。 - 緊急時の指揮命令と対応の優先順位の決定 - インシデントへの対応（インシデントレスポンス） - インシデントの影響と被害の分析 - 情報収集と自社に必要な情報の選別 - 社内関係者への連絡と周知 - 外部関係機関との連絡 [参考]セキュリティインシデント発生時の対応手順の検討において、"インシデントハンドリングマニュアル"(JPCERT/CC, 2015年)、"SP 800-61 rev.1"(NIST, 2008年)、"インシデント対応マニュアルの作成について"(JPCERT/CC, 2015年)を参照することが可能である。
				CPS.CO-3	・復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又はコンティンジェンシープランの中に位置づける	Advanced	・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動およびインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。
				CPS.AN-1	・セキュリティ事象の全容と、推測される攻撃者の意図から、組織全体への影響を把握する	Advanced	・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。 ・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
				CPS.AN-3	・検知されたセキュリティ事象の情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する	Advanced	・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 ・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。 "SP 800-61 rev.1" では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。 - インシデントの現在の状況 - インシデントの概要 - 当該インシデントに対して自組織のとった行動の内容 - ほかの関係者(システム所有者、システム管理者等)の連絡先情報 - 調査の際に収集した証拠の一覧 - インシデントの処理担当者からのコメント - 次にとるべきステップ
				CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う	Basic	・組織(あるいはその構成員)は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション(たとえば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など)を実行する。 [参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質(例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような顕在化する脅威の差異)により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、"SP 800-61 rev.1"(NIST, 2008年)等を参照することが望ましい。
	3.6.2	組織の内部及び外部の両方の、適切な担当官及び／または権威に対して、インシデントについての追跡、文書化、及び報告を行う。	・IR-2 インシデント対応のトレーニング ・IR-4 インシデントの対応 ・IR-5 インシデントの監視 ・IR-6 インシデントの報告 ・IR-7 インシデント対応の支援	CPS.RP-4	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ(製品)に対して適切な対応を行う	Advanced	・組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。 ・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動およびインシデントの事後処理に関わる活動を調整する。その際、CPS.AM-2, CPS.AM-3にて記載している方法により、対応の対象となるモノを特定していることが望ましい。
				CPS.IM-1	・セキュリティ事象への対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する	Basic	・セキュリティインシデントの評価から得た脅威情報、脆弱性情報等は、再発する又は影響の大きいインシデントを特定するために利用することが望ましい。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又はコンティンジェンシープラン、教育／訓練に取り入れて、結果として必要となる変更を実施する。NIST SP 800-61には、教訓を抽出する際の観点として下記が例として示されている。 - 正確に何がいつ起きたか。 - スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。 - すぐに必要になった情報は何か。 - 復旧を妨げたかもしれないステップや行動があったか。 - 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。 - どのような是正措置があれば、将来にわたって同じ様な事件が起きるのを防げるか。 - 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。
				CPS.IM-2	・セキュリティ事象への対応から教訓を導き出し、事業継続計画又はコンティンジェンシープランを継続的に改善する	Basic	・組織は、セキュリティインシデントへの対応から、事業継続のためのプロシージャおよび関連する対策の機能が、事業継続のより上位の方針と合致しているかを確認する。 ・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又はコンティンジェンシープラン、教育／訓練に取り入れて、結果として必要となる変更を実施する。
	3.6.3	組織のインシデント対応能力をテストする。	・IR-3 インシデント対応のテストと実習 ・IR-3(2) インシデント対応のテストと実習 関連する計画との調整	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、関係者間で対応プロセスの整備と訓練を行う	H.Advanced	・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。 ・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。 [参考]サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。
						Advanced	・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。 ・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。
メンテナンス	3.7.1	組織のシステムにおいてメンテナンスを実施する。	・MA-2 定期的な保守 ・MA-3 保守ツール ・MA-3(1) 保守ツール ツールを検査する ・MA-3(2) 保守ツール メディアを検査する	CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する ・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する	H.Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.7.2	システムメンテナンスを実施するために使用されるツール、手法、メカニズム、及び要員における有効な管理策を提供する。	・MA-2 定期的な保守 ・MA-3 保守ツール ・MA-3(1) 保守ツール ツールを検査する ・MA-3(2) 保守ツール メディアを検査する	CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する ・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する	H.Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.3	オフサイトのメンテナンスのために除去される装置は、あらゆるCUI についてサニタイズされることを保証する。	・MA-2 定期的な保守	CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するデータID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする	H.Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等をを廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。
	3.7.4	組織のシステム内でメディアが使用される前に、悪意のあるコードが入っていないか診断及びテストプログラムを用いてメディアをチェックする。	・MA-3(2) 保守ツール	CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する ・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する	H.Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。 ・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
						Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
	3.7.5	外部のネットワークコネクションを介した非ローカルメンテナンスセションを確立するため、複数要素の認証を要求し、非ローカルメンテナンスの完了時にこのようなセションを終了する。	・MA-4 遠隔保守	CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守は、承認を得て、ログを記録し、不正アクセスを防げる形で実施している	Advanced	・組織は、実施した遠隔保守の実施記録を保管する。
						Basic	・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。 ・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。
	3.7.6	必要なアクセス許可なしにメンテナンス要員のメンテナンス活動を監督する。	・MA-5 保守要員	CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する ・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する	Advanced	・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。 ・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。 ・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。
						Basic	・組織は、メンテナンス要員が付添いなしでシステムのメンテナンスを行う場合に、その要員が必要なアクセス権限を有することを確認する。 ・組織は、必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要なアクセス権限と技術的能力を有する組織の要員を指定する。
メディア処理	3.8.1	紙及びディジタルの両方の、CUI を含む、システムメディアを保護する(即ち、物理的に制御及びセキュアに格納する)。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する	H.Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
						Basic	・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。
	3.8.2	システムメディア上のCUI へのアクセスを許可された利用者に制限する。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.AC-8	・IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データ)をサイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する	Basic	・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。 ・システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。 ・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。
	3.8.3	廃棄または再利用のために手放す前に、CUI を含むシステムメディアをサニタイズまたは破壊する。	・MP-2 メディアへのアクセス ・MP-4 メディアの保管 ・MP-6 メディア上の記録の抹消とメディアの廃棄	CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するデータID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする	H.Advanced	・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。
						Advanced	・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。
						Basic	・組織は、自組織のIoT機器やサーバ等をを廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。
	3.8.4	CUI のマーク表示と配付制限が必要なメディアに対して表示を行う。	・MP-3 メディアへのラベル付け	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する	H.Advanced	・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。 ・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。 ・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。 ・システムは、規定したルールに従って、プログラムの実行を阻止する。
						Advanced	・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。 ・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する
						Basic	・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。 ・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。 ・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。
	3.8.5	CUI を含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの説明責任を維持する。	・MP-5 メディアの輸送	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Advanced	・資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、システムコンポーネント上で利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織のシステムを構成する資産(ハードウェア、ソフトウェア、情報)を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP.33を参照することが可能である。
	3.8.6	代替の物理的予防手段による保護がない限り、持ち出し中はディジタルメディア上に格納されたCUI の機密性を保護するための暗号学的メカニズムを実装する。	・MP-5(4) メディアの輸送 暗号学的保護	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	H.Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
	3.8.7	システムコンポーネント上の取り外し可能なメディアの使用を管理する。	・MP-7 メディアの利用	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Advanced	・資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、システムコンポーネント上で利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織のシステムを構成する資産(ハードウェア、ソフトウェア、情報)を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP.33を参照することが可能である。
	3.8.8	ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。	・MP-7(1) メディアの利用 所有者以外の利用を禁止	CPS.AM-1	・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する	Advanced	・資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、システムコンポーネント上で利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。 ・組織は、ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。
						Basic	・組織は、自組織のシステムを構成する資産(ハードウェア、ソフトウェア、情報)を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 ・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP.33を参照することが可能である。
	3.8.9	保存場所にあるバックアップCUI の機密性を保護す	・CP-9 情報システムのバックアップ	CPS.IP-4	・構成要素(IoT機器、通信機器、回線等)に対し、定期的	Advanced	・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。 ・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
		る。			なシステムバックアップを実施し、テストしている	Basic	・組織は、自組織のシステムに含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。
人的セキュリティ	3.9.1	CUI を含む組織のシステムへのアクセスを許可する前に、個人を審査する。	・PS-3 要員に対する審査 ・PS-4 要員の解雇 ・PS-5 人事異動	CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にサイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている	H.Advanced	・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。
						Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。
						Basic	・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。
	3.9.2	離職または配置転換等の人事措置の間と後で、CUI 及びCUI を含む組織のシステムが保護されることを保証する。	・PS-3 要員に対する審査 ・PS-4 要員の解雇 ・PS-5 人事異動	CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にサイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている	H.Advanced	・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。 ・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。
						Advanced	・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。 ・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。
						Basic	・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。 ・組織は、要員の退職時に以下を実施する。 -自組織のシステムに対するアクセスを一定期間内に無効にする。 -職員に関連する認証及びクレデンシャルを無効にする。 -セキュリティに関連するシステム関連の所有物をすべて回収する。 -退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。
物理的保護	3.10.1	組織のシステム、装置、及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。	・PE-2 物理的アクセス権限 ・PE-5 表示メディアへのアクセス制御 ・PE-6 物理的アクセスの監視	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設内の一般の人がアクセスできるエリアを定め、必要に応じてアクセス制御を実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客について、付き添う等して来客の行動を監視する。
	3.10.2	物理的設備を保護し、監視し、組織のシステムの基盤をサポートする。	・PE-2 物理的アクセス権限 ・PE-5 表示メディアへのアクセス制御 ・PE-6 物理的アクセスの監視	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	Advanced	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。
	3.10.3	訪問者をエスコートし、訪問者の活動を監視する。	・PE-3 物理的アクセス制御	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	Basic	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。 ・組織は、自組織の施設内の一般の人がアクセスできるエリアを定め、必要に応じてアクセス制御を実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客について、付き添う等して来客の行動を監視する。
	3.10.4	物理的アクセスの監査ログを維持する。	・PE-3 物理的アクセス制御	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	Advanced	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定および記録、監視を実施する	Advanced	・施設内の、一般の人がアクセスできる指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。 ・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア(執務室等)において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。
	3.10.5	物理的アクセスデバイスを制御し、管理する。	・PE-3 物理的アクセス制御	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	Advanced	・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。 ・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。
				CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定および記録、監視を実施する	Advanced	・施設内の、一般の人がアクセスできる指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。 ・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。 ・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。 ・自組織の保護すべき資産に直接アクセス可能なエリア(執務室等)において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。 ・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。 ・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。
						Basic	・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.10.6	代替の作業サイト(例、テレワークのサイト)でのCUIに対する防護対策を強制(実施)する。	・PE-17 代替作業拠点	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
リスクアセスメント	3.11.1	組織のシステムの運用と関連するCUI の処理、ストレージ、または送信からの結果として組織運用(ミッション、職務、イメージ、または風評を含めて)、組織の資産、及び個人に対するリスクを定期的にアセスメントする。	・RA-3 リスクアセスメント	CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する ・IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する	Advanced	・組織は、システム、またはシステムが稼働する環境に大きな変化があった場合(新たな脅威や脆弱性の特定を含む)、もしくはシステムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。 ・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。 [参考]システムおよびモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。
	3.11.2	定期的に、及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに、それらのシステム及びアプリケーションの脆弱性についてスキャンする。	・RA-5 脆弱性のスキャン ・RA-5(5) 脆弱性のスキャン 特権アクセス	CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する	H.Advanced	・組織は、スキャンすべきシステムの脆弱性をすぐに更新できる脆弱性スキャンツールを使用する。 ・組織は、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、報告された場合に更新する。 ・組織は、指定された脆弱性スキャン活動に関して、対象システムのコンポーネントに対する特権的アクセスの許可制度を実施する。
						Advanced	・組織は、システムおよびアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる - プラットフォーム、ソフトウェアの欠陥、および誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [参考]脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、システムおよびアプリケーションの脆弱性のスキャンを定期的に実施する
	3.11.3	リスクのアセスメントに従い、脆弱性を修正する。	・RA-5 脆弱性のスキャン	CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する	Advanced	・組織は、システムおよびアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する ・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる - プラットフォーム、ソフトウェアの欠陥、および誤った設定を列挙する - チェックリストとテスト手順をフォーマットする - 脆弱性による影響を評価する ・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する ・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。 [参考]脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。
						Basic	・組織は、システムおよびアプリケーションの脆弱性のスキャンを定期的に実施する
セキュリティアセスメント	3.12.1	管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために、組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.IP-7	・セキュリティ事象への対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、資産を保護するプロセスを改善している	Advanced	・組織は、セキュリティ評価を適切に、かつ、計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ表亜 k を実施する。。 -セキュリティ評価の対象とするセキュリティ対策 -セキュリティ対策の有効性を図るために用いる評価手順 -セキュリティ評価を実施する環境や実施体制 -セキュリティ評価結果の取りまとめ方法とその活用方法
						Basic	・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。 ・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.12.2	欠陥を修正し、組織のシステムにおける脆弱性を軽減し、または取り除くために設計された行動計画を策定し、実施する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティインシデントを検知・分析・対応する体制を整える	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。プロセスの内容については、CPS.RP-1等を参照。 ・組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には下記を含むことが望ましい。 - ログ分析の分析結果 (対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) - モニタリングにおける今後の改善方針 [参考]セキュリティ対策組織(SOC/CSIRT)の業務、望まれる規模等については、"セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～"(ISOG-J, 2018年)等を参照することが望ましい。
	3.12.3	管理策の継続的な有効性を保証するため、継続的にセキュリティ管理策を監視する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.AE-3	・セキュリティインシデントの相関の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する	H.Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織でIDS,IPS,SIEMと言ったセンサーのポリシーチューニング(適用シグネチャ管理)と維持管理を行う。 ・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。
						Advanced	・"セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～"(ISOG-J, 2018年)では、主に下記のような機器のログを監視し、リアルタイムに分析を行うよう記載されている。 多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱うことが望ましい。 - ファイアウォールなどのネットワーク装置からのログやネットフロー - IPS/IDSなどのセキュリティ装置からのログ - Web サーバなどのアクセスログ - ActiveDirectoryやDNSなどの各種システムからのログ - ユーザ利用端末に関するログ
						Basic	・ファイアウォールやエンドポイントセキュリティ製品等の通知を個別に確認することで、影響を及ぼすようなセキュリティインシデントを特定する。
				CPS.DP-1	・セキュリティインシデントの説明責任を果たせるよう、セキュリティインシデント検知における自組織とサービスプロバイダーが担う役割と負う責任を明確にする	Basic	・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログ情報を決定する。 ・組織は、取引先(サービスプロバイダー)に対して、取得されるサービス利用者の活動，例外処理及びセキュリティインシデントを記録した監査ログの存在を確認する。 ・組織は，サービスプロバイダーにより取得される監査ログが，サービスの利用者の活動，例外処理及びセキュリティインシデントを記録できており、適切な方式で保護されていることを確認する。
				CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティインシデントを検知する	Basic	・組織は、モニタリング業務に関係する法制度、業界標準、顧客との契約事項等が存在するか、存在するならばどのような制約があるかを認識する。 ・組織は、上記で認識したルールに準拠してモニタリングを実施し、セキュリティインシデントを検知する。 ・組織は、自組織のモニタリング活動がルールに準拠したものかどうかを定期的にレビューし、確認する。
	3.12.4	システムの境界、システムの運用環境、セキュリティ要件の実装方法、及び他のシステムとの関係または他のシステムへのコネクションについて記述した、システムセキュリティ計画を策定、文書、及び定期的に更新する。	・CA-2 セキュリティア評価 ・CA-5 行動計画とマイルストン ・CA-7 継続的な監視 ・PL-2 システムセキュリティ計画	CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、保管する	H.Advanced	・システムは、自組織が利用している外部情報サービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。 ・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。 ・組織は、外部プロバイダによるサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。
						Advanced	・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。 a. 外部の情報システムから自組織の情報システムにアクセスすること b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること ・外部のシステム上での自組織のポータブルストレージの使用を制限する。
				CPS.RA-6	・リスクアセスメントに基づき、発生しうるセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する ・IoT機器およびIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対して適宜対応する	Advanced	・組織は，セキュリティリスク対応のプロセスについての文書化した情報を保管する。 ・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策および当該対応策を採用する理由を文書化することが望ましい。 ・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。 ・組織は、セキュリティリスク対応計画をレビューし、当該計画が、自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。 ・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。 ・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。
システムと通信の保護						H.Advanced	・システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする ・システムは、モバイルコードの使用を管理し、監視する。 ・システムは、VoIPの使用を管理し、監視する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.1	外部の境界及びシステムの鍵となる内部境界における通信 (即ち、組織のシステムによって送信または受信される情報) を監視し、制御し、保護する。	・SC-7 境界保護 ・SA-8 セキュリティエンジニアリングの原則	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	Advanced	・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント(DMZ: 非武装地帯)を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する
						Basic	・組織は、システムの外部境界、およびシステム内の主要な内部境界において通信をモニタリングし、制御する。
	3.13.2	組織のシステム内の有効な情報セキュリティを促進するような、アーキテクチャ設計、ソフトウェア開発手法、及びシステムエンジニアリングの原則を採用す	・SC-7 境界保護 ・SA-8 セキュリティエンジニアリングの原則	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入し、定めた各段階におけるセキュリティに関わる要求事項を明確化する	Basic	・組織は、システムを構築するに当たり仕様書、設計、開発、導入、及び変更に、システムのセキュリティエンジニアリング原則を適用する。
	3.13.3	利用者機能をシステム管理機能と分離する。	・SC-2 アプリケーションの分離	CPS.AC-5	・ユーザーが利用する機能と、システム管理者が利用する機能を分離する	H.Advanced	・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。 ・組織は、非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。 ・システムは、特権の機能の使用をチェックするため、システムが監査するメカニズムを導入している。 ・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。
						Advanced	・組織は、自組織のシステムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。 ・組織は、特定の職務権限に対して最小権限の原則を採用する。 ・組織は、担当者によって割り当てられた職務を分離し、明文化する。
	3.13.4	共有システム資源を介した、不正な予期せぬ情報の転送を防止する。	・SC-4 残存情報	CPS.DS-8	・自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、ファイル閲覧停止等の適切な対応を実施する	H.Advanced	・組織は、自組織の保護すべきデータが不適切なエンティティに渡らないように、自動化されたメカニズムを利用して検知を実施する。 ・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。
	3.13.5	内部ネットワークから物理的にまたは論理的に分離される、公開アクセス可能なシステムコンポーネント用には、サブネットワークを実装する。	・SC-7 境界保護	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	H.Advanced	・システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする ・システムは、モバイルコードの使用を管理し、監視する。 ・システムは、VoIPの使用を管理し、監視する。
						Advanced	・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント(DMZ: 非武装地帯)を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する
						Basic	・組織は、システムの外部境界、およびシステム内の主要な内部境界において通信をモニタリングし、制御する。
	3.13.6	デフォルトでネットワーク通信トラフィクを拒否し、また例外によってネットワーク通信トラフィクを許可する(即ち、すべて拒否、例外で許可)。	・SC-7(5) 境界保護 デフォルトで拒否／例外で許可	CPS.AC-7	・適宜ネットワークを分離する(例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する	H.Advanced	・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可とする。 ・機密性の高いデータを取り扱う自組織のシステムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
				CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	H.Advanced	・システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする ・システムは、モバイルコードの使用を管理し、監視する。 ・システムは、VoIPの使用を管理し、監視する。
						Advanced	・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント(DMZ: 非武装地帯)を構築する。 ・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する
	3.13.7	リモートデバイスが、組織のシステムとの非リモートコネクションの確立と同時に、外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。	・SC-7(7) 境界保護 リモートデバイスのスピリットトンネルを禁止	CPS.AC-7	・適宜ネットワークを分離する(例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する	H.Advanced	・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可とする。 ・機密性の高いデータを取り扱う自組織のシステムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。
	3.13.8	代替の物理的予防手段による保護がない限り、持ち出し中にCUI の不正な暴露を防止するために暗号学的メカニズムを実装する。	・SC-8 伝送する情報の完全性 ・SC-8(1) 伝送する情報の完全性 暗号学的保護または代替の物理的保護	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	H.Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.9	セション終了時または定義された非アクティブな時間の経過後に、通信セションに対応するネットワークコネクションを終了する。	・SC-10 ネットワークの切断	CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
	3.13.10	組織のシステムで採用された暗号のための暗号鍵を確立し、管理する。	・SC-12 暗号鍵の確立と管理	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	H.Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 CRYPTREC暗号リスト電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。
						Basic	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。
				CPS.DS-4	・送受信データ、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	Advanced	・組織は、秘密鍵が危殆化した際に遅滞なく適切な対処を行うため、必要に応じて下記のような事項について方針及び手順を定めることが望ましい。 - 秘密鍵の危殆化に対応するための体制(関係者と役割、委託先との連携を含む) - 秘密鍵が危殆化した、またはその恐れがあると判断するための基準 - 秘密鍵の危殆化の原因を調べること、及び、原因の解消を図ること - 当該鍵を利用するサービスの利用停止 - 新しい鍵ペアを生成し、新しい鍵に対する証明書を発行すること - 秘密鍵の危殆化についての情報の開示(通知先、通知の方法、公表の方針等) [参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。
						Basic	・組織は、全ての暗号鍵を，改変及び紛失から保護することが望ましい。
	3.13.11	CUI の機密性を保護するために使用されるとき、FIPS 認証された暗号を採用する。	・SC-13 暗号化の利用	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	H.Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
	3.13.12	共同コンピューティングデバイスのリモートからの活性化を禁止し、使用中のデバイスの兆候をデバイスに存在する利用者に提供する。	・SC-15 共同コンピューティングデバイス	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
	3.13.13	モバイルコードの使用を管理し監視する。	・SC-18 モバイルコード	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する	H.Advanced	・システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする ・システムは、モバイルコードの使用を管理し、監視する。 ・システムは、VoIPの使用を管理し、監視する。
	3.13.14	VoIP 技術の使用を管理し、監視する。	・SC-19 ボイスオーバーインターネットプロトコル (VoIP)				
	3.13.15	通信セションの真正性を保護する。	・SC-23 セションの真正性	CPS.AC-3	・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する	H.Advanced	・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。 ・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。 ・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。 ・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。 ・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。 ・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。
				CPS.DS-2	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	H.Advanced	・組織は、重要なデータを扱う通信路について、通信経路の暗号化を実装するか、あるいは、代替の物理面での対策によって保護する。
						Advanced	・システムは、暗号メカニズムを導入し、通信経路を暗号化する。 [参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.13.16	保存されたCUI の機密性を保護する。	・SC-28 保存情報の保護	CPS.DS-1	・情報(データ)を適切な強度の方式で暗号化して保管する	H.Advanced	・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。 ・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。 [参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。
						Advanced	・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リスト電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。
システムと情報の完全性	3.14.1	タイムリーなやり方で情報及びシステムフローを識別し、報告し、訂正する。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	H.Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。
	3.14.2	組織のシステム内の適切な場所で、悪意のあるコードから保護を提供する。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する ・サイバー空間から受ける情報(データ)が許容範囲内であることを動作前に検証する	H.Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃(例：コマンドインジェクション)に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性をチェックする。 ・システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント(IoT機器、サーバ等)において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。
						Advanced	・システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント(IoT機器、サーバ等)において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ※ 特にIoT機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものか確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。
	3.14.3	システムセキュリティ警報及びアドバイザリを監視し、適切な対応アクションを取る。	・SI-2 欠陥の修正 ・SI-3 悪意のコード(不正プログラム) からの保護 ・SI-5 セキュリティ警報と勧告	CPS.IP-10	・脆弱性管理計画を作成し、計画に沿って構成要素の脆弱性を修正する	Advanced	・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。
				CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する ・サイバー空間から受ける情報(データ)が許容範囲内であることを動作前に検証する	H.Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃(例：コマンドインジェクション)に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性をチェックする。 ・システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント(IoT機器、サーバ等)において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。
						Advanced	・システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。 ・エンドポイント(IoT機器、サーバ等)において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。 ※ 特にIoT機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものか確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。
	3.14.4	新しいリリースが利用可能となったとき、悪意のあるコードからの保護メカニズムをアップデートする。	・SI-3 悪意のコード(不正プログラム) からの保護	CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する	H.Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、自動化されたメカニズムを通じて適切なパートナーと適時双方向で共有をすることができる環境を整備する。
						Advanced	・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。
				CPS.AE-3	・セキュリティインシデントの相関の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する	H.Advanced	・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。 ・組織は、自組織でIDS,IPS,SIEMと言ったセンサーのポリシーチューニング(適用シグネチャ管理)と維持管理を行う。 ・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。
	3.14.5	組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、	・SI-3 悪意のコード(不正プログラム) からの保護	CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する ・サイバー空間から受ける情報(データ)が許容範囲内であることを動作前に検証する	H.Advanced	・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃(例：コマンドインジェクション)に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。 ・システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性をチェックする。 ・システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。 ・エンドポイント(IoT機器、サーバ等)において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。 ・組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.14.5	外部情報源からのファイルのリアルタイムスキャンを実行する。	SI-3 悪意のコード（不正プログラム）からの保護	CPS.CM-4	IoT機器、サーバ等において、送受信する情報(データ)の完全性および真正性を動作前に確認する	H.Advanced	・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 ・システムは、通信セッションの真正性を保護する。
						Advanced	・システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。 ・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。
	3.14.6	内向き及び外向きの通信トラフィクを含めて、攻撃や潜在的な攻撃の兆候を検知するため、組織のシステムを監視する。	・SI-4 情報システムの監視ツールと監視技法 ・SI-4(4) 情報システムの監視ツールと監視技法 内向きと外向きの通信トラフィク	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	H.Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。
				CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える	Advanced	・組織は、リスクアセスメントの結果等を参照しし、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。プロセスの内容については、CPS.RP-1等を参照。 ・組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には下記を含むことが望ましい。 - ログ分析の分析結果 (対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) - モニタリングにおける今後の改善方針 [参考]セキュリティ対策組織(SOC/CSIRT)の業務、望まれる規模等については、"セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～"(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.CM-5	・発生する可能性のあるセキュリティ事象を検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスをモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
				CPS.DP-4	・セキュリティインシデントの検知プロセスを継続的に改善する	Advanced	・組織は、経営層等の組織内の適切な要員に、定期的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。 組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば下記のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※下記のリストは、"セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0 "(ISOG-J, 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード ・ 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 ・各セキュリティ製品における検知名
				CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する	H.Advanced	・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。 ・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。 ・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク			
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例	
	3.14.7	組織のシステムの不正な使用を識別する。	・SI-4 情報システムの監視ツールと監視技法	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える	Advanced	・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。 - モニタリングするシステムの範囲をどこまでとするか - どのような機器のログを収集し、分析するか (CPS.AE-3を参照) ・組織は、モニタリングにより収集した監査ログを定期的にレビューする。 ・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。 ・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。プロセスの内容については、CPS.RP-1等を参照。 ・組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には下記を含むことが望ましい。 - ログ分析の分析結果 (対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等) - モニタリングにおける今後の改善方針 [参考]セキュリティ対策組織(SOC/CSIRT)の業務、望まれる規模等については、"セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度 ～"(ISOG-J, 2018年)等を参照することが望ましい。
				CPS.CM-5	・発生する可能性のあるセキュリティ事象を検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする	Advanced	・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。 ・組織は、関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。 ・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。 ・組織は、外部サービスプロバイダーおよびシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。
				CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する	Advanced	・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。 ・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる ・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める ・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。 ・システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。 ・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。
				CPS.DP-4	・セキュリティインシデントの検知プロセスを継続的に改善する	Advanced	・組織は、経営層等の組織内の当るべき要員に、定期的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。 ・例えば下記のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※下記のリストは、"セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0 "(ISOG-J, 2017年)より引用している。 ・ 攻撃の特徴 攻撃の特徴 ➢ 攻撃形態、関連する通信の内容 ➢ 核心となる攻撃コード ・ 攻撃によって残る痕跡 ➢ 被害を受けた後の通信内容 ➢ サーバやクライアントに残るログ ➢ サーバやクライアントに残るその他特徴 ・ 各セキュリティ製品における検知名