中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（Cisco ASA）

Ver1.0（2023.07）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）

総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに 3
2 チェックリスト項目に対応する設定作業一覧 4
3 管理者向け設定作業 5
3-1 チェックリスト 3-2 への対応 5
3-1-1 アクセス制限の確認 5
3-2 チェックリスト 5-4 への対応 9
3-2-1 最新のセキュリティアップデート 9
3-3 チェックリスト 7-2 への対応 11
3-3-1 時刻同期確認 11
3-4 チェックリスト 7-3 への対応 14
3-4-1 ログ収集設定 14
3-5 チェックリスト 9-1 への対応 20
3-5-1 パスワードポリシーの設定 20
3-6 チェックリスト 10-2 への対応 23
3-6-1 管理者ログインパスワード設定 23

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、Cisco ASA を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業の理解を助けることを目的としています。

(イ) 前提条件

利用する機器により使用可能な機能が異なります。**本資料では Cisco ASA ソフトウェア 9.8 以上の利用を前提としております。**

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2022 年 11 月 1 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-2 アクセス制御・認可 **インターネット経由で社内システムにアクセスがあった際には、ファイアウォールやルーター等において、不要なポートへの通信や不要な IP アドレスからの通信を遮断する。**	・アクセス制限の確認	P5
5-4 脆弱性管理 **テレワーク端末から社内にリモートアクセスするための VPN 機器等には、メーカーサポートが終了した製品を利用せず、最新のセキュリティアップデートを適用する。**	・最新のセキュリティアップデート	P9
7-2 インシデント対応・ログ管理 **テレワーク端末と接続先の各システムの時刻を同期させる。**	・時刻同期	P11
7-3 インシデント対応・ログ管理 **テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集する。**	・ログ収集設定	P14
9-1 アカウント・認証管理 **テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。**	・パスワードポリシーの設定	P20
10-2 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用する。**	・管理者ログインパスワード設定	P23

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1　チェックリスト 3-2 への対応

3-1-1　　アクセス制限の確認

VPN ルーターはインターネットから社内に接続するために利用する機器です。一般的には、社内ネットワークとインターネットの境界に設置されています。そのため、インターネットからのアクセスを許可する通信が必要最小限となるよう、VPN ルーターのファイアウォールを設定することが重要です。インターネットからのアクセス許可ルールによって許可する通信を必要最小限とすることで、**不正アクセスによる内部データの改ざんや盗聴等、セキュリティ上のリスクを低減**させることができます。
以降の説明では、機器に設定されている、ファイアウォール設定の確認方法を解説します。

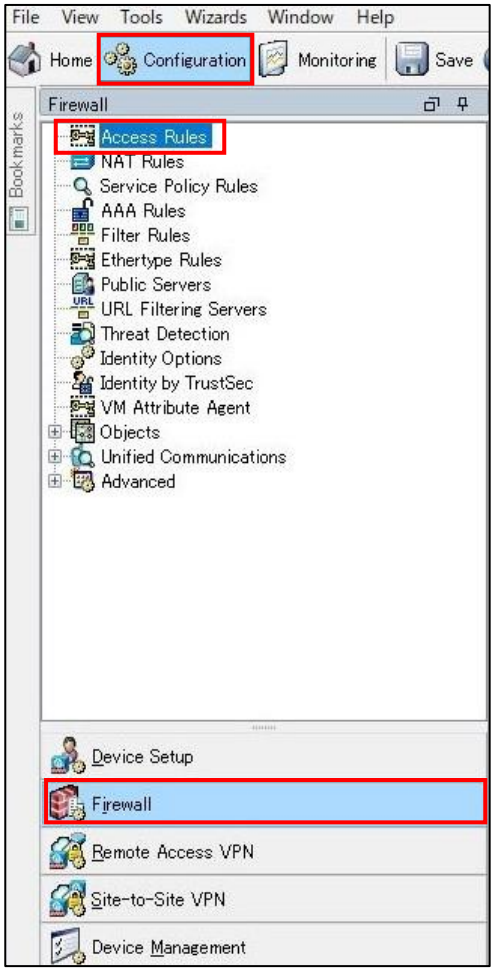
本書では、Cisco ASDM（Adaptive Security Device Manager）（※）を用いた設定や操作の方法を解説しています。

※　Cisco ASDM は、GUI ベースの設定管理インターフェースを提供する機能です。ただし、Cisco Community サイトで解説されている方法は、製品初期状態の環境を念頭に説明されているため、現在稼働中の機器へのアクセス方法は、構築担当者、構築ベンダー、または製品提供元に確認するようにしてください。
【参考】Cisco Community サイト
URL：https://community.cisco.com/t5/-/-/ta-p/3138282

ファイアウォール設定の確認

【手順①】

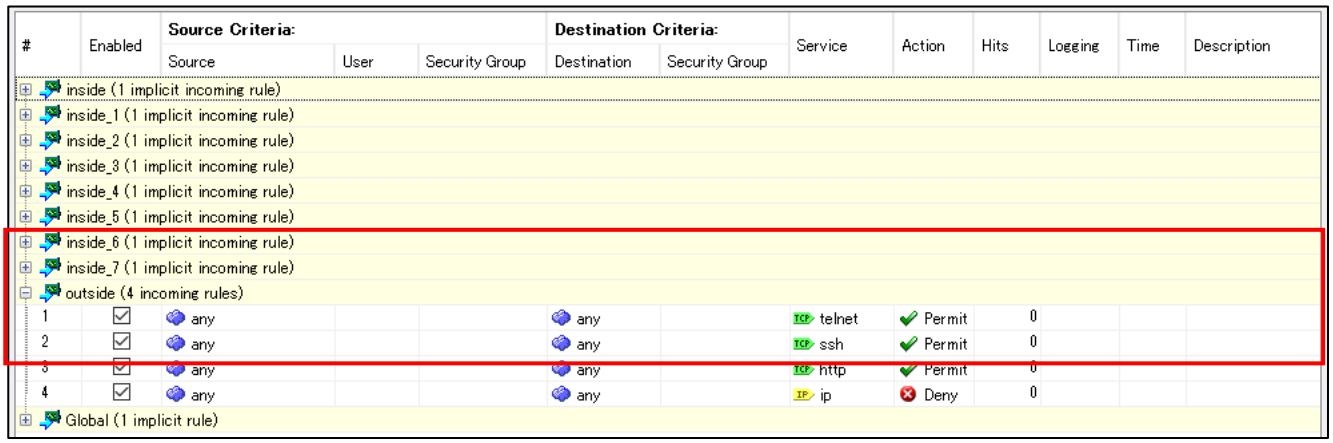
ASDM 管理画面にアクセスし、管理画面上部にある「Configuration」をクリック後、画面左下にある「Firewall」を選択します。表示の「Firewall」リストから、「Access Rules」をクリックします。



【手順②】

下図のようなアクセスルールのウィンドウが表示されます。このアクセスルールに業務上不要なサービスが許可されていないこと確認します。アクセスルールはインターフェース単位で設定しますが、特にインターネット側に相当するインターフェースのルールを確認します。（ここでは『outside』と記載されたインターフェースがインターネット側に相当する想定で解説しています。）一般的に、VPN ルーターとして利用している機器で、インターネット上のすべてのホストからのアクセスを許可しなければならないケースは少ないため（VPN 接続のためのルールを除く）、アクセス許可の制限がされていない場合や不要だと思われる許可ルールを確認した場合は、「本当に必要な通信ルールであるか」について、構築担当者や構築ベンダーに確認するようにしてください。なお、アクセスルールの見方については、後述の『**参考　ファイアウォールルール画面の見方**』を参照してください。

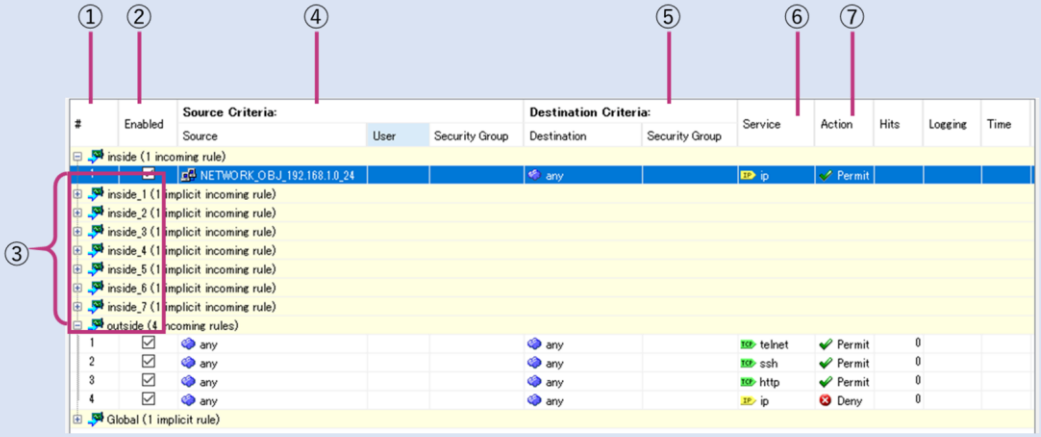
下図のアクセスルールは例として挙げています。最適なアクセスルールは環境によって異なるため、実際のルールは構築ベンダー等と協議の上、各社で適切なルールを作成して下さい。



#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits	Logging	Time	Description
inside (1 implicit incoming rule)												
inside_1 (1 implicit incoming rule)												
inside_2 (1 implicit incoming rule)												
inside_3 (1 implicit incoming rule)												
inside_4 (1 implicit incoming rule)												
inside_5 (1 implicit incoming rule)												
inside_6 (1 implicit incoming rule)												
inside_7 (1 implicit incoming rule)												
outside (4 incoming rules)												
1	☑	any			any		telnet	Permit	0			
2	☑	any			any		ssh	Permit	0			
3	☑	any			any		http	Permit	0			
4	☑	any			any		ip	Deny	0			
Global (1 implicit rule)												

※　VPN 機能を利用する場合、VPN 接続するために必要なプロトコルは明示的に許可せずとも、自動的に許可される設定となっています。

参考　ファイアウォールルール画面の見方



① アクセスルール番号

② ルールの有効/無効

③ 適用インターフェースの指定

ファイアウォールの設定とは別に、ASA 機器の各物理ポート（下図の「Gigabit Ethernet 1/1」など）に名前（下図の「outside」、「inside_1」など）を設定することができます。ファイアウォールのアクセスルールは、この名前を指定することで紐づくインターフェースに適用することができます。Global を選択すると、インターフェースを特定することなくファイアウォール全体でのルールを適用できます。

Interface	Name
BVI1	inside
GigabitEthernet1/1	outside
GigabitEthernet1/2	inside_1
GigabitEthernet1/3	inside_2
GigabitEthernet1/4	inside_3
GigabitEthernet1/5	inside_4
GigabitEthernet1/6	inside_5
GigabitEthernet1/7	inside_6
GigabitEthernet1/8	inside_7
Management1/1	

④ 送信元の設定

- ●Source（送信元アドレス）
  any とすることで全てのアドレスを指定可能
- ●User（送信元ユーザー）
- ●Security Group（送信元セキュリティグループ）

⑤ 宛先の設定

- ●Destination（宛先アドレス）
- ●Security Group（送信元セキュリティグループ）

⑥ サービス名

TCP/UDP 等のプロトコル指定と制限したいポート番号の値もしくは ssh 等のサービス名を指定

⑦ アクション

値	説明
Permit	トラフィックの許可
Deny	トラフィックの拒否

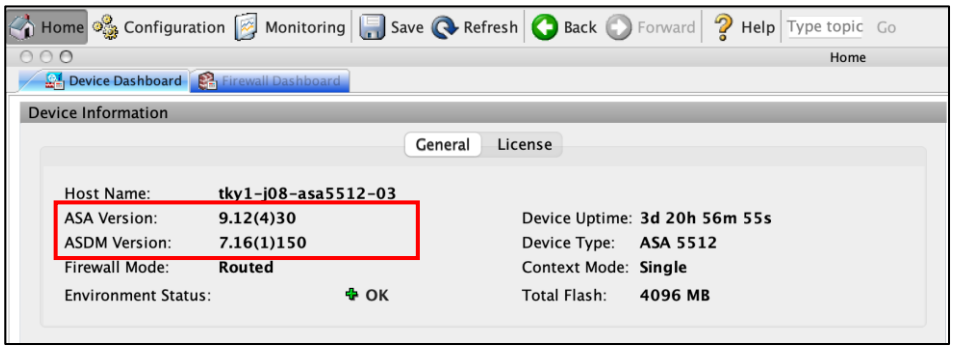
3-2　チェックリスト 5-4 への対応

3-2-1　　最新のセキュリティアップデート

VPN 機器を利用する際は、製品提供元からリリースされる最新バージョンを利用します。古いバージョンの VPN 機器は脆弱性をついたサイバー攻撃や不正アクセス等の標的となりやすいため、特に注意します。最新バージョンにアップデートすることは、**脆弱性をついたサイバー攻撃に対して有効な対策**となるため、定期的にアップデートがないか確認することを推奨します。

現在のバージョン確認

ASDM 管理画面上部にある「Home」をクリックします。「Device Information」に ASA Version を含めた各項目の現在のバージョンが表示されます。

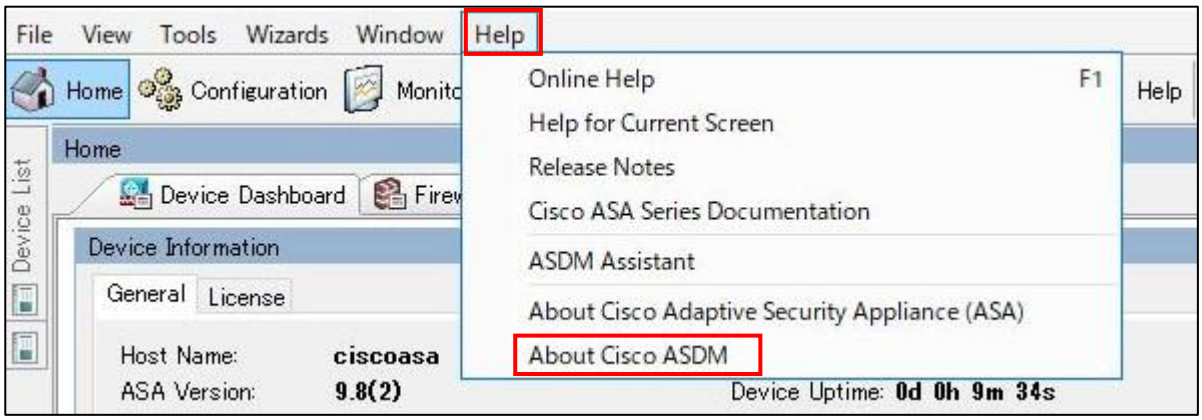


【参考】ASA バージョンの確認方法

現在使用している ASA のバージョンと ASDM ソフトウェアのバージョンは以下の手順でも確認することができます。

【手順①】

ASDM 管理画面上部にある「Help」-「About Cisco ASDM」をクリックします。



【手順②】

下図画面が表示されるので、ASA Version 含めた各項目の現在のバージョンを確認します。

3-3　チェックリスト 7-2 への対応

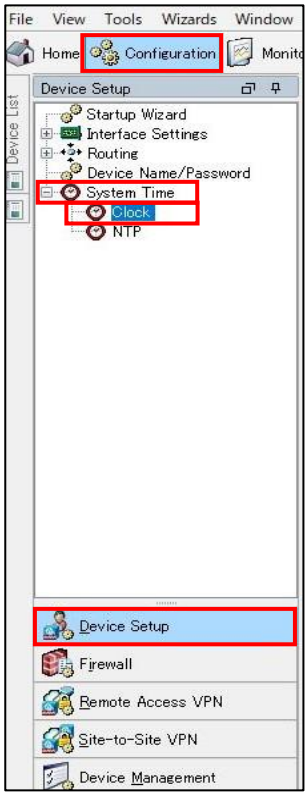
3-3-1　　時刻同期設定

VPN 機器とアクセス先の各システムの時刻を同一のものにするため、VPN 機器の時刻設定を行います。
各機器の時刻を一致させることで、**インシデント発生時のアクセスログ等の調査の際に、正確な調査を行う**ことができます。

日付と時刻確認（手動設定）

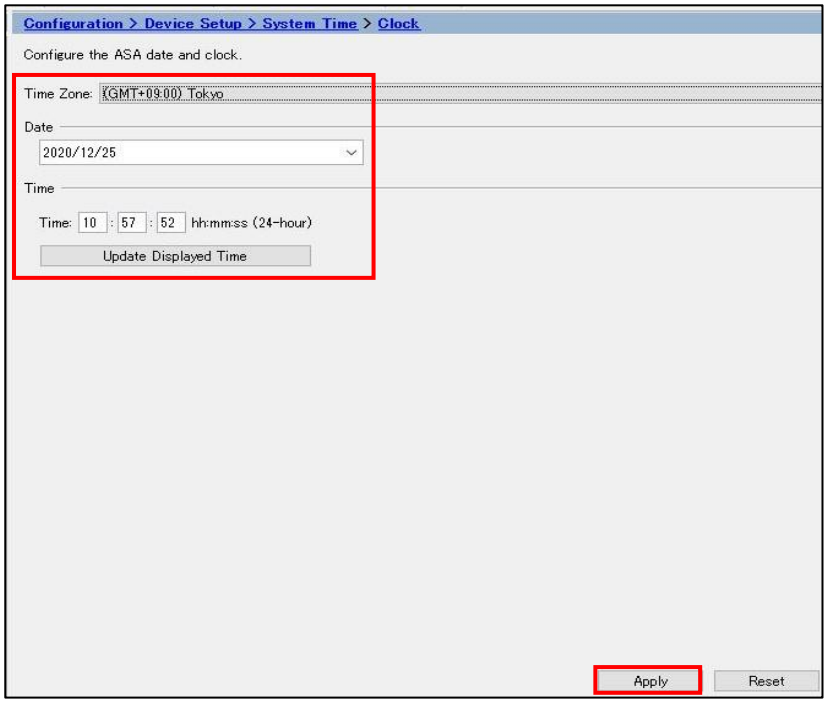
【手順①】

ASDM 管理画面上部にある「Configuration」をクリック後、画面左下にある「Device Setup」を選択します。
中央の「Device Setup」リストから、「System Time」-「Clock」をクリックします。



【手順②】

右側の日時設定情報から、任意のタイムゾーンと時刻で設定します。入力後、「Apply」をクリックします。



日付と時刻確認（NTP 設定）

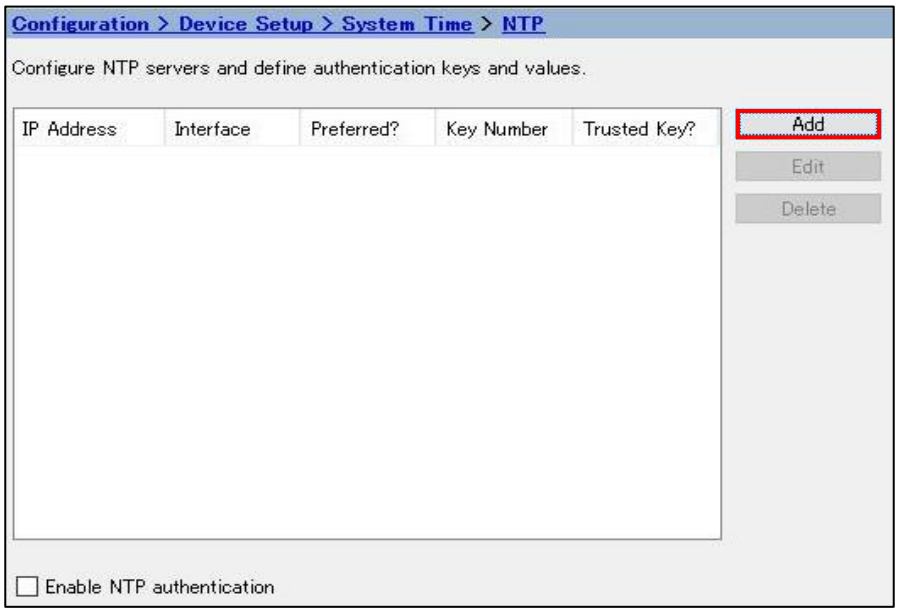
【手順①】

ASDM 管理画面上部にある「Configuration」をクリック後、画面左下にある「Device Setup」を選択します。

中央の「Device Setup」リストから、「System Time」-「NTP」をクリックします。

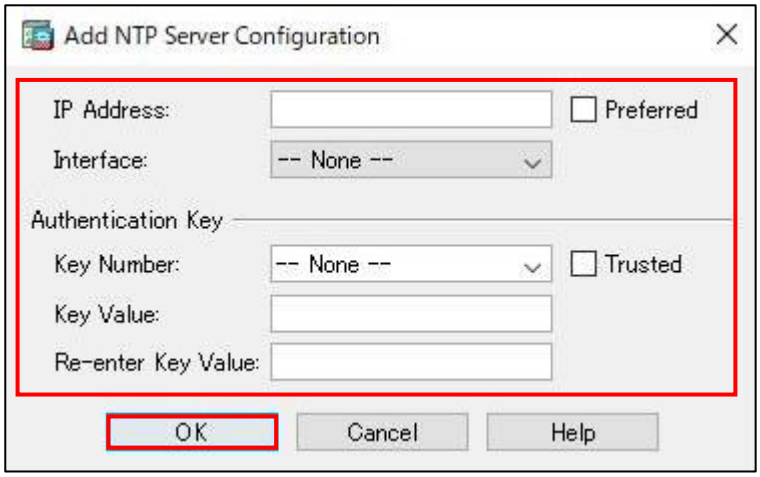
【手順②】

以下のウィンドウが表示されます。ここでは、接続する NTP サーバーリストが表示されます。この手順では新規の NTP サーバーを登録するため、「Add」をクリックします。



【手順③】

接続する NTP サーバーの各情報を入力後、「OK」をクリックします。



3-4　チェックリスト 7-3 への対応

3-4-1　　ログ収集設定

ログ収集の設定を行っていない場合、悪意のある第三者から攻撃を受けた際に原因究明や調査を行うことができなくなってしまいます。VPN 機器でログを収集することで、**悪意のある第三者から不正アクセス等のサイバー攻撃にあった際に、原因を調査することが可能**となるため、ログ確認やログ収集の設定を行います。

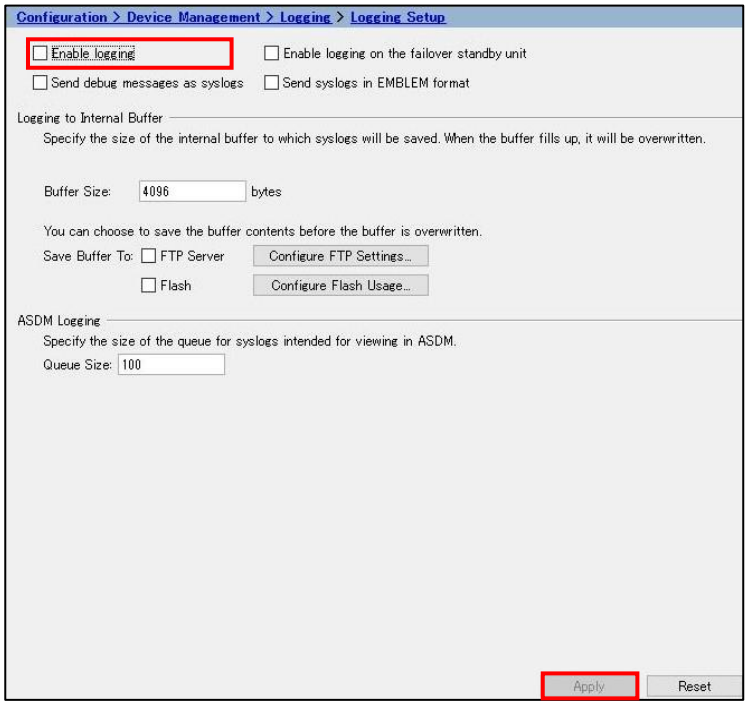
ログ取得設定

【手順①】

ASDM 管理画面上部にある「Configuration」をクリックし、画面左下にある「Device Management」を選択します。
「Device Management」リストから、「Logging」-「Logging Setup」をクリックします。

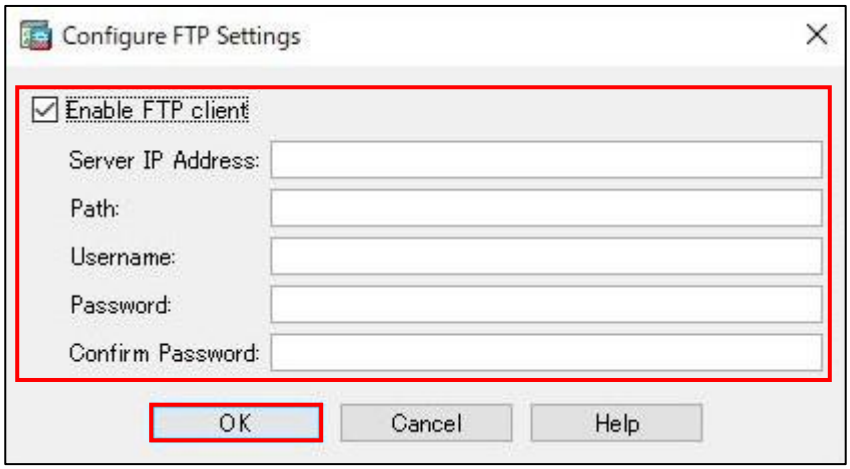
【手順②】

以下のウィンドウが表示されます。「Enable logging」にチェックを入れ、「Apply」をクリックします。ただし、FTP サーバーを使用したログの管理や、物理記憶装置を使用したログの管理を行う場合は、先に次の手順を実施します。



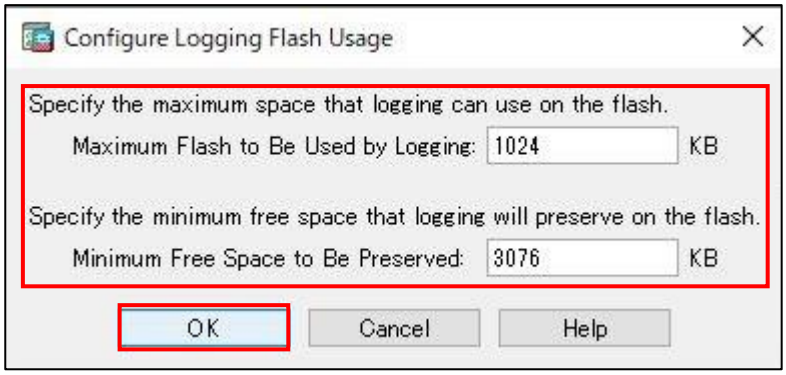
- FTP サーバーを使用してログを管理する場合

FTP サーバーを使用する場合は、「Apply」をクリックする前に「Configure FTP Settings」をクリックします。下図のような画面の表示後、必要な情報を入力し、「OK」をクリックします。【手順②】の画面に遷移後、「Apply」をクリックします。



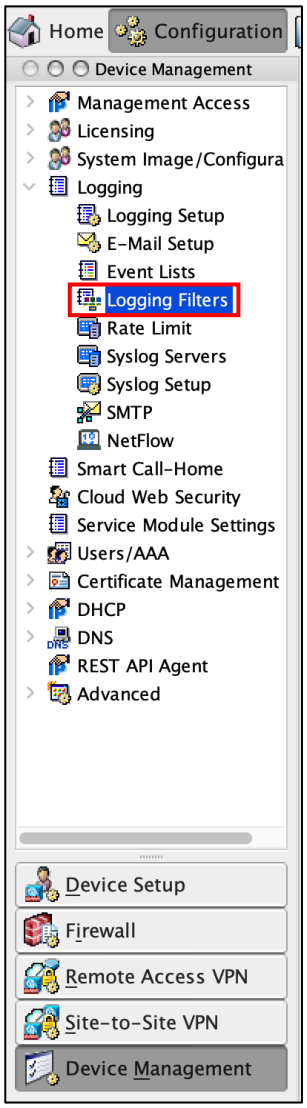
- 物理記憶装置を使用してログを管理する場合

物理記憶装置を使用する場合は「Apply」をクリックする前に、「Configure Flash Usage」をクリックします。下図のような画面の表示後、必要な情報を入力し、「OK」をクリックします。【手順②】の画面に遷移後、「Apply」をクリックします。



【手順③】

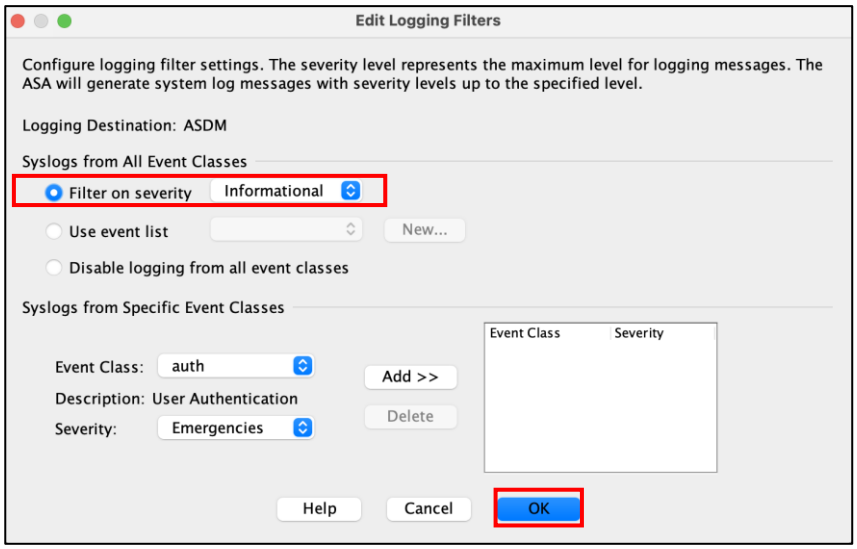
「Logging Filters」をクリックします。



【手順④】

「ASDM」を選択し、「Edit」をクリックします。「Filter on severity」で適切なレベルのログを選択し、「OK」をクリックします。

【手順②】の画面に遷移後、「Apply」をクリックします。



【参考】syslog サーバーを指定してログを管理する場合

syslog サーバーを指定してログ保存を行う場合は、以下の URL を参考に設定を行ってください。

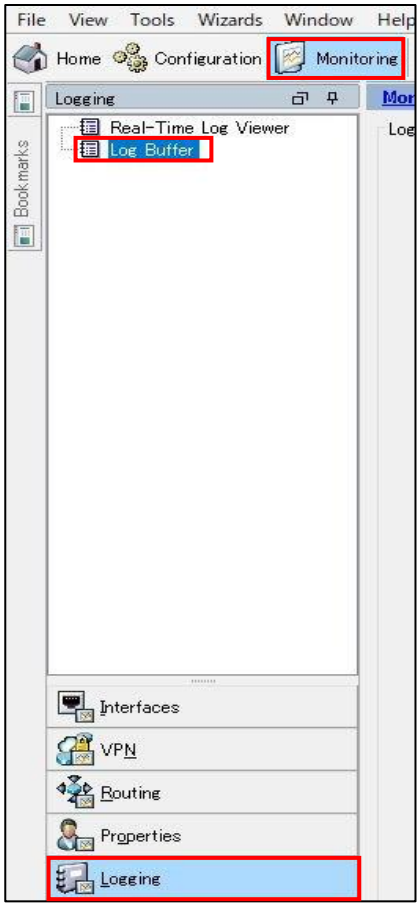
https://www.cisco.com/c/ja_jp/support/docs/security/pix-500-series-security-appliances/63884-config-asa-00.html#anc17

ログ確認

以降の手順では機器内に保存されている情報を確認する方法を記載しています。前項の手順で外部にログを保存している場合は、外部の保存先でログを確認してください。

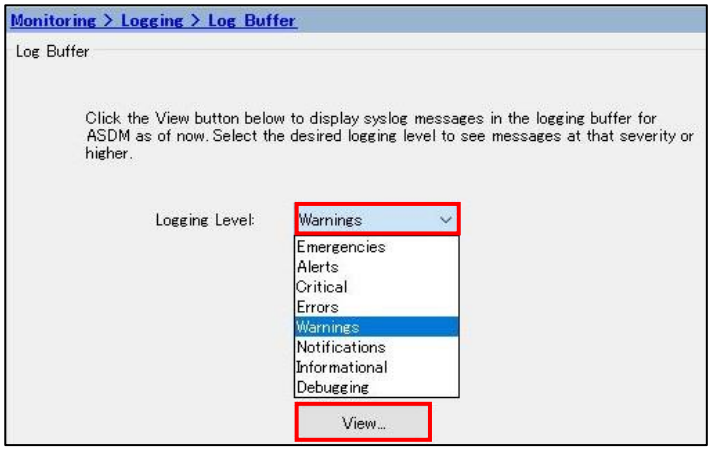
【手順①】

ASDM 管理画面上部にある「Monitoring」をクリック後、画面左下にある「Logging」を選択します。「Logging」リストから、「Log Buffer」をクリックします。



【手順②】

右側に表示されている下図の画面から任意のログレベル（Logging Level）を選択し、「View...」をクリックします。



【手順③】

画面遷移後、ログが表示されます。

例えば、インシデント対応の際にログを見る場合は以下のような観点でログを確認します。

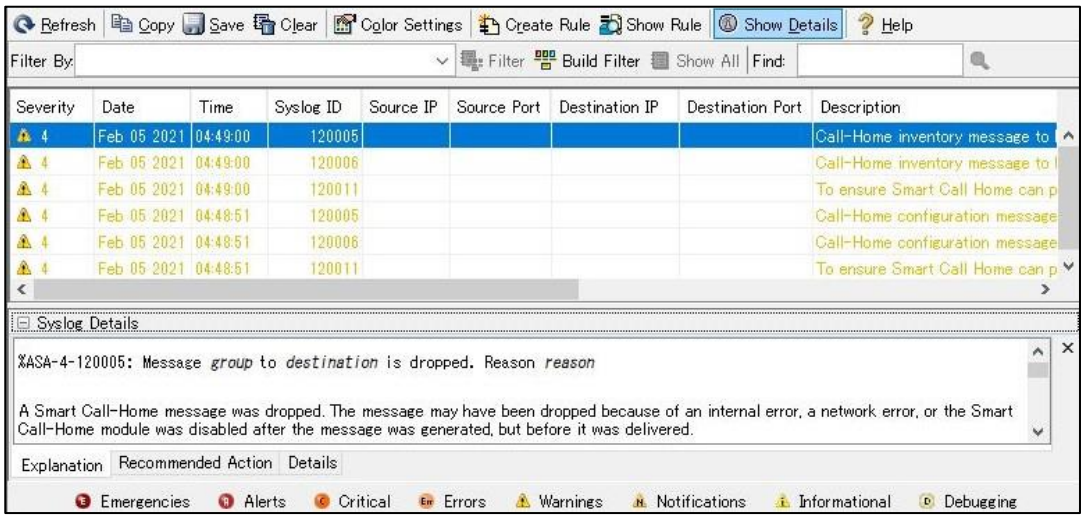
・インシデントが発生した前後の日時

・インシデントが発生した端末/サーバーに対する通信

・インシデントが発生した端末/サーバーからの通信の中で業務上行われたものではないと想定される不審な履歴

※　詳細のログ確認方法については、以下の製品ベンダーサイトをご確認してください。

https://www.cisco.com/c/ja_jp/td/docs/security/asa/syslog/b_syslog.html



3-5　チェックリスト 9-1 への対応

3-5-1　　パスワードポリシーの設定

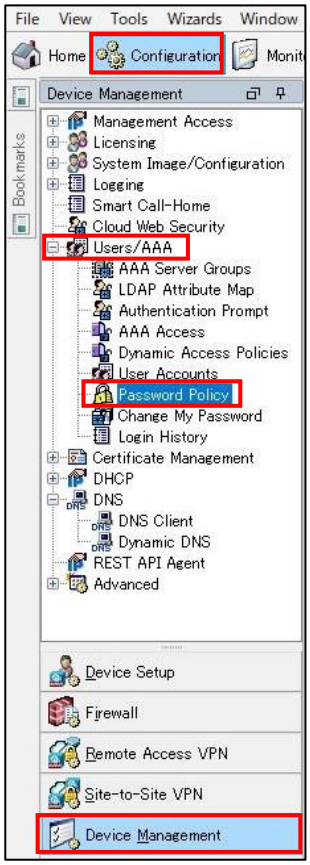
ここでは、管理ユーザーのパスワードポリシーの設定を行います。パスワードポリシーを設定することにより、強度の高いパスワード設定をユーザーに要求できます。**これにより、強度の低いパスワードが使用されるリスクを低減することができます。**

パスワードポリシー設定

【手順①】

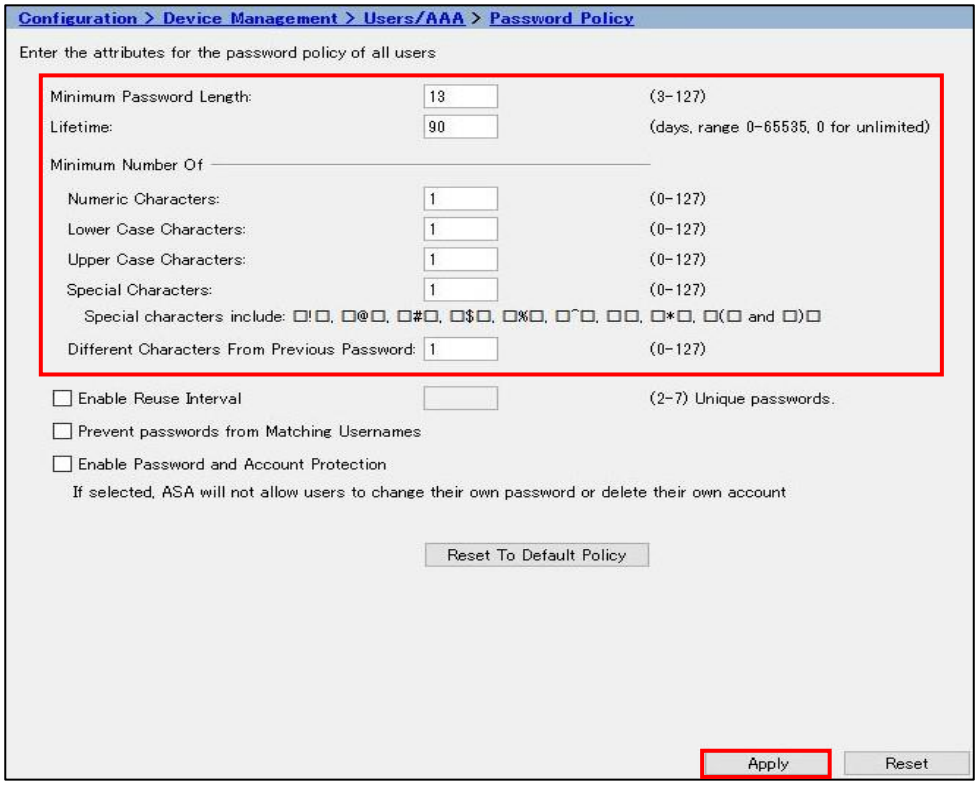
ASDM 管理画面上部にある「Configuration」をクリック後、画面左下にある「Device Management」を選択します。

「Device Management」リストから、「Users/AAA」-「Password Policy」をクリックします。



【手順②】

右側に表示の画面から任意のパスワードポリシーを設定します。



項目毎の詳細は以下です。

[Minimum Password Length]：

パスワードの最短長を入力します。有効値の範囲は 3～127 文字です。推奨されるパスワードの最小長は 8 文字です。

[Lifetime]：

- リモートユーザー（SSH、Telnet、HTTP）のパスワードの有効期間を日数で指定します（コンソールポートのユーザーが、パスワードの有効期限切れでロックされることはありません）。
- 有効な値は、0～65536 です。デフォルト値は 0 日です。「0」に設定されている場合、パスワードが期限切れになることはありません
- パスワードの有効期限が切れる場合、7 日前に警告メッセージが表示されます。パスワードの有効期限が切れると、リモートユーザーのアクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。
  - 他の管理者にパスワードを変更してもらいます。
  - 物理コンソールポートにログインして、パスワードを変更します。

[Minimum Number Of]：次のタイプの最短文字数を指定します。

[Numeric Characters]：パスワードに含まれなければならない数字の最短文字数を入力します。有効な値は、0～127 文字です。デフォルト値は 0 です。

[Lower Case Characters]：パスワードに含まれなければならない小文字の最短文字数を入力します。有効値の範囲は 0～127 文字です。デフォルト値は 0 です。

[Upper Case Characters]：パスワードに含まれなければならない大文字の最短文字数を入力します。有効値の範囲は 0～127 文字です。デフォルト値は 0 です。

[Special Characters]：パスワードに含まれなければならない特殊文字の最短文字数を入力します。有効値の範囲は 0～127 文字です。特殊文字には、!、@、#、$、%、^、&、*、（、）があります。デフォルト値は 0 です。

[Different Characters from Previous Password]：新しいパスワードと古いパスワードで違わなければならない最小文字数を入力します。有効な値は、0～127 文字です。デフォルト値は 0 です。

※ この機能の文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

3-6　チェックリスト 10-2 への対応

3-6-1　　管理者ログインパスワード設定

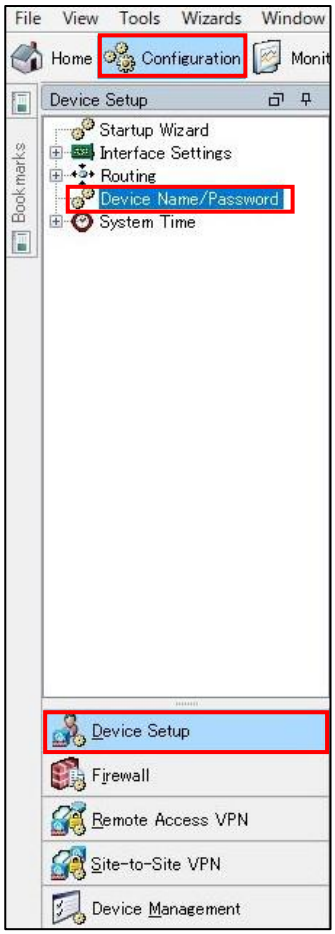
パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「中小企業等向けテレワークセキュリティの手引き」のP.96 に記載の「パスワード強度」を参考に設定することを推奨します。

VPN 機器の管理者のパスワードを長いものや複雑なものにすることで**悪意のある第三者からの意図しない不正アクセスや設定変更等の攻撃リスクを低減**することができます。

管理アカウントパスワード変更

【手順①】

ASDM 管理画面上部にある「Configuration」をクリック後、画面左下にある「Device Setup」を選択します。
「Device Setup」リストから、「Device Name/Password」をクリックします。



【手順②】

Enable Password 項目の[Change the Privileged mode password.]にチェックを入れ、長く複雑なパスワードを設定します。設定するパスワードは「中小企業等向けテレワークセキュリティの手引き」の P.96 に記載の「パスワード強度」を参考に設定することを推奨します。