装備品等及び役務の調達における情報セキュリティ基準の解説②

装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ実施手順について

第１．１版

令和５年７月１２日

防衛装備庁装備政策部

改版履歴

版数	改版日	改版内容	備考
1.0	令和５年６月２日	新規作成	
1.1	令和５年7月１２日	組織改編に基づく改版、その他誤字等修正	装備保全管理官⇒装備保全管理課長

はじめに

１．目的

本資料は、装備品等及び役務の調達における情報セキュリティの確保について（防装庁（事）第１３７号。令和４年３月３１日。）別添装備品等及び役務の調達における情報セキュリティ確保に関する特約条項（以下「特約条項」という。）別紙付紙「装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領」の解説資料として作成しています。

２．記載内容

資料本編の各ページには、特約条項別紙付紙装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領の規定、規定制定の解説等を記載しています。

３．その他注意事項

・目次の項番（「第〇」の部分）は、装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領の項番と対応しています。

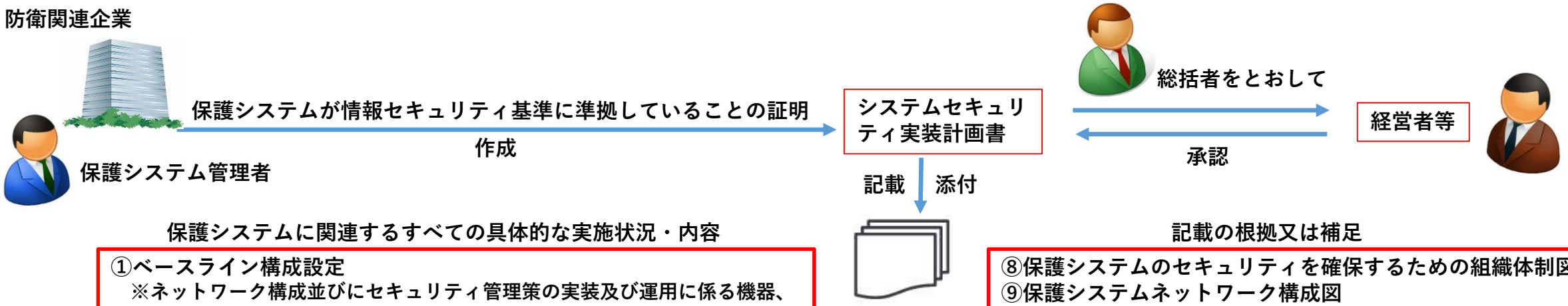
目　　次

第２　システムセキュリティ実装計画書

１ システムセキュリティ実装計画書の作成

(1) 防衛関連企業は、自社の保有又は利用する保護システムについて、セキュリティ基準に規定する措置を適切に実施し、本基準に適合していることを証明する資料として、システムセキュリティ実装計画書を作成するものとする。
(2) システムセキュリティ実装計画書には、自社の保有又は使用する保護システムに関する次に掲げる文書等を記載又は添付するものとし、同計画は保護システム管理者が作成し、総括者を通じて経営者等の承認を得るものとする。

ア　第３第２項第１号に規定するベースライン構成設定
イ　第３第２項第5号に規定するブラックリスト又はホワイトリスト
ウ　第３第４項第1号に規定する構成設定目録
エ　第４第２項第1号に規定する操作手順書
オ　第５第１項第1号に規定するアクセス制御方針
カ　第７第３項第1号及び第2号に規定する保護システムにおけるモバイルコード及びVoIP技術の利用に係る要件
キ　第７第３項第3号に規定する保護システムにおける各種のオフィス機器の利用に係る要件
ク　保護システムのセキュリティを確保するための組織体制図（経営者等、総括者及び情報システム管理者、その他保護システムのセキュリティに責任を有する者の具体的な責任の内容及び範囲を記載するものとする。）
ケ　保護システムのネットワーク構成図
コ　保護すべきデータのデータフロー図



保護システムに関連するすべての具体的な実施状況・内容

①ベースライン構成設定
※ネットワーク構成並びにセキュリティ管理策の実装及び運用に係る機器、保護すべき情報を格納又は中継する機器について記載
②ブラックリスト又は、ホワイトリスト
③構成設定目録
④操作手順書
⑤アクセス制御方針
⑥モバイルコード・VoIPの利用に係る要件
⑦各種のオフィス機器の利用に係る要件

記載の根拠又は補足

⑧保護システムのセキュリティを確保するための組織体制図
⑨保護システムネットワーク構成図
※使用設備・機器（サーバー、端末、DBなど）の構成、社内外の繋がりや、保護すべきデータの保護範囲が理解可能な構成図
⑩保護すべきデータのデータフロー図
※各構成部署でどのようなデータを扱い、そのデータがどのように移動及び保存されるのかが理解可能なフロー図

第２　システムセキュリティ実装計画書

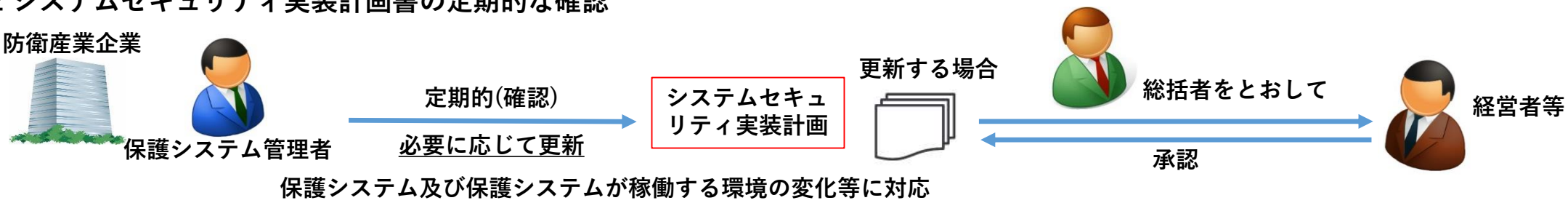
2 システムセキュリティ実装計画書の定期的な確認
　保護システム管理者は、保護システムの現状を正確に把握するためシステムセキュリティ実装計画書の内容を定期的に確認することとし、変更する場合は、第１項第2号により総括者を通じて経営者等の承認を得るものとする。

3 システムセキュリティ実装計画書の保存等
　保護システム管理者は、システムセキュリティ実装計画書を文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、少なくとも必要な期間保管又は保存するものとする。

4 システムセキュリティ実装計画書の周知
　保護システム管理者は、システムセキュリティ実装計画書を作成又は変更した場合は、これを周知するとともに、システム管理業務に従事する者以外にシステムセキュリティ実装計画書を配付又は閲覧させないものとする。

5 システムセキュリティ実装計画書の防衛省への提出等
　システムセキュリティ実装計画書を作成した場合及び防衛省からの求めがあった場合は、同計画書について防衛省の確認を受けるものとする。

2 システムセキュリティ実装計画書の定期的な確認



保護システム及び保護システムが稼働する環境の変化等に対応

3 システムセキュリティ実装計画書の保存等

文書：施錠したロッカー等
データ：暗号化

4 システムセキュリティ実装計画書の周知

システム管理業務に従事する者以外に配付又は閲覧させない

保護システムの契約担当者など職務上必要のある場合は配付又は閲覧可

システム管理業務に従事する者

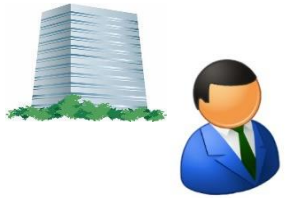
5 システムセキュリティ実装計画書の防衛省の確認

作成又は防衛省から要求があった場合
→防衛省の確認

1 セキュリティエンジニアリングの原則の適用

防衛関連企業は、保護システムの設計、開発、導入及び変更する場合において、セキュリティエンジニアリングの原則を適用するものとする。

防衛関連企業



保護システム管理者

保護システムの設計、開発、導入及び変更する場合

セキュリティエンジニアリングの原則（※）

システムエンジニアリング、ソフトウェアエンジニアリング
に基づく開発ライフサイクル全体を考慮したセキュリティ対策
を実施すること。

設計、開発、導入及び変更

保護システム

2 ベースライン構成設定等

(1) 保護システム管理者は、保護システムを構成するハードウェア、ソフトウェア、記憶媒体及びネットワーク（以下「保護システム構成要素」という。）について、次に掲げる要件を満たすために必要なベースライン構成設定を定め総括者の承認を得るものとする。

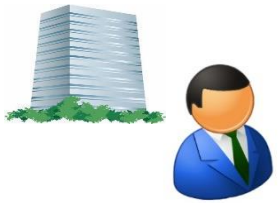
ア　情報セキュリティ基本方針等に基づく措置が実施可能なものであること。

イ　保護システムのセキュリティを確保するものであること。

ウ　保護システム構成要素の機能及び動作を業務遂行上必要な最小限度に制限するものであること。

(2) 保護システム構成要素の構成設定は、ベースライン構成設定に従って保護システム管理者が設定するものとする。

防衛関連企業



保護システム管理者

保護システム構成要素：　保護システムを構成するハードウェア、
ソフトウェア、記憶媒体、ネットワーク

ベースライン構成設定に基づき
設定

保護システム
構成要素

※ベースライン
構成設定

定める

承認

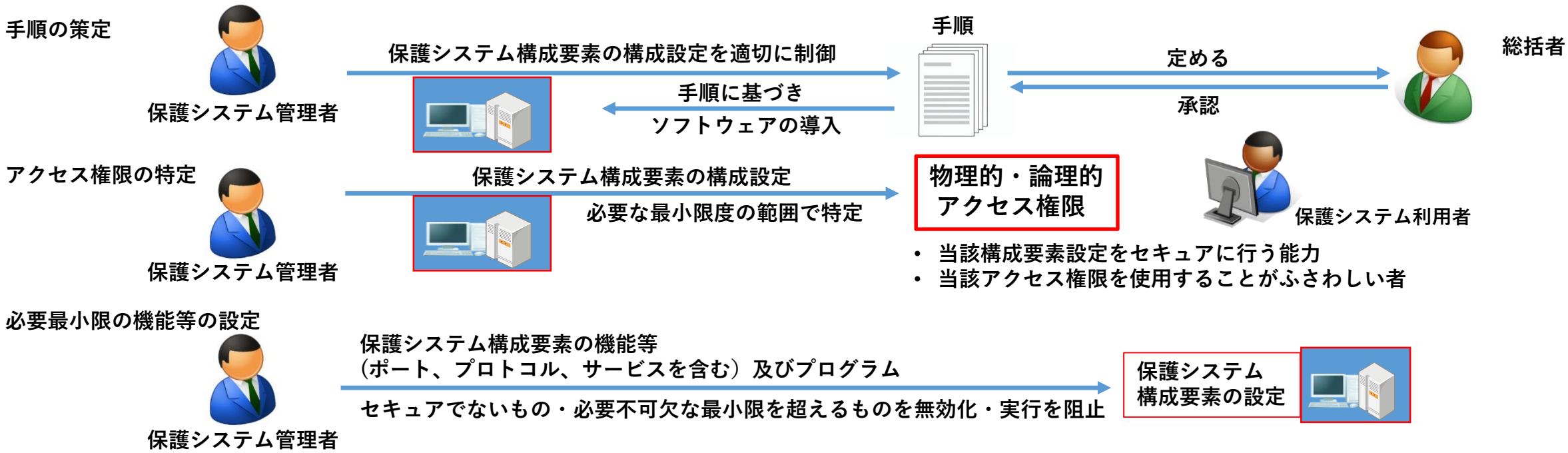
総括者

①情報セキュリティ基本方針等に基づく措置が可能
②保護システムのセキュリティを確保
③保護システム構成要素・機能→必要最小限度に制限

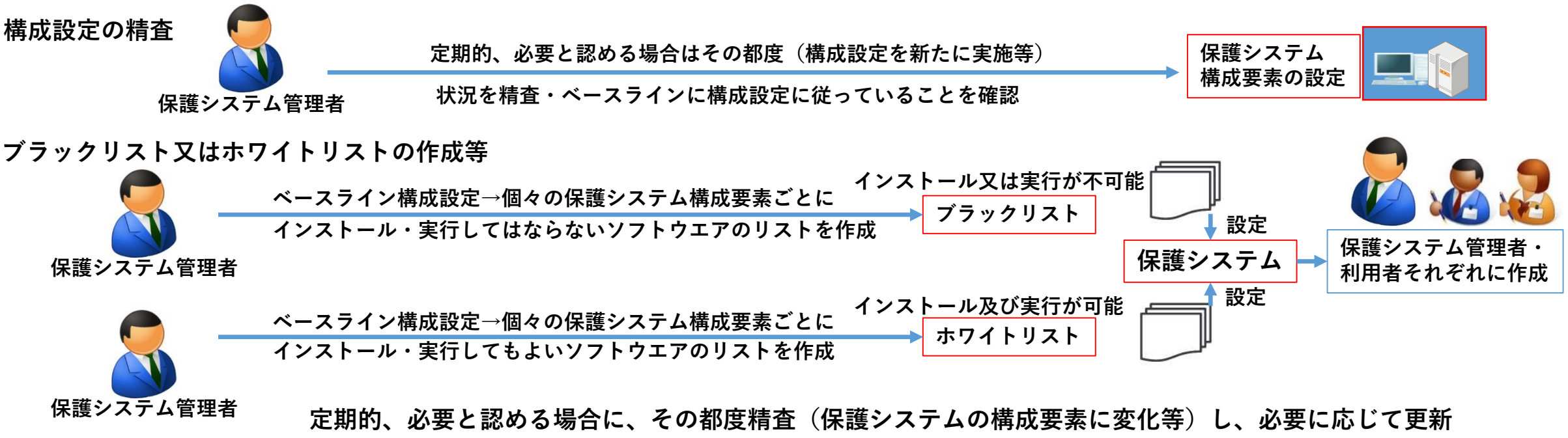
※ ベースラインは設定基準という意味で用いている

(3) 構成設定の方法
ア　保護システム管理者は、保護システム構成要素の構成設定を適切に制御するための手順を定めるとともに総括者の承認を得て、同手順に基づきソフトウェアの導入等を行うものとする。
イ　アクセス権限の特定等
(ｱ) 保護システム構成要素の構成設定を実施するための物理的及び論理的なアクセス権限は、当該構成設定を実施するために必要な最小限度の範囲に限定するものとする。
(ｲ) (ｱ)に規定する論理的なアクセス権限は、当該構成設定を安全に行える能力を有し、かつ、当該アクセス権限を使用することがふさわしい者に限り使用させることとする。
ウ　必要最小限度の機能等の設定
保護システム構成要素の構成設定は、当該保護システム構成要素の機能等（ポート、プロトコル及びサービスを含む。）及びプログラムのうち、安全でないもの及び必要不可欠な最小限を超えるものを無効化し、その実行を防止するものとする。

構成設定の方法



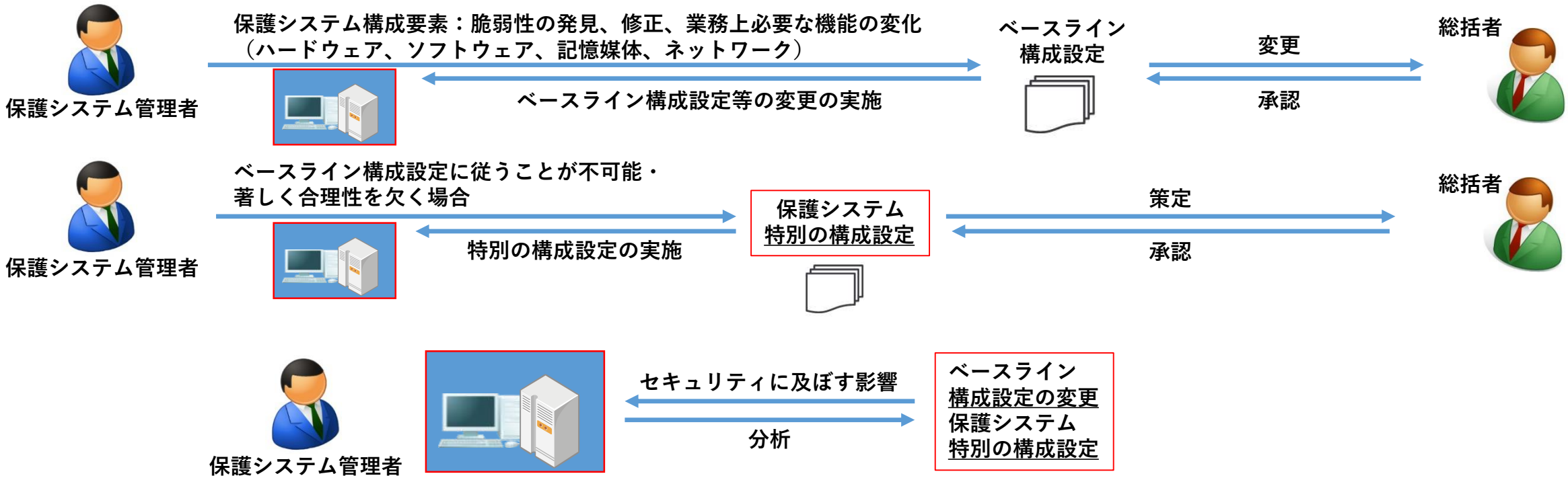
(4) 構成設定の精査
　保護システム管理者は、定期的に、及び保護システム構成要素の構成設定を新たに実施した場合など必要と認める場合には、保護システム構成要素の構成設定の状況を精査し、ベースライン構成設定に従っていることを確認するものとする。
(5) ブラックリスト又はホワイトリストの作成等
ア 保護システム管理者は、ベースライン構成設定に基づき、個々の保護システム構成要素ごとに、ブラックリスト又はホワイトリストを作成するものとする。その際、保護システム管理業務従事者とそれ以外の保護システム利用者で業務上使用するソフトウェアに違いがある場合は、それぞれに向けたリストを作成するものとする。
イ 保護システム管理者は、 ブラックリストを作成した場合は、保護システムが当該ブラックリストに掲載されたソフトウェアをインストール又は実行することが不可能となるように設定するものとする。
ウ 保護システム管理者は、ホワイトリストを作成した場合は、保護システムが当該ホワイトリストに掲載されたソフトウェアのみをインストール及び実行することが可能となるように設定するものとする。
エ 保護システム管理者は、定期的に、及び保護システム構成要素に変更が生じた場合など必要と認める場合には、イに規定するブラックリスト又はウに規定するホワイトリストを精査し、必要に応じ、当該リストを更新するものとする。



3 ベースライン構成設定等の変更等

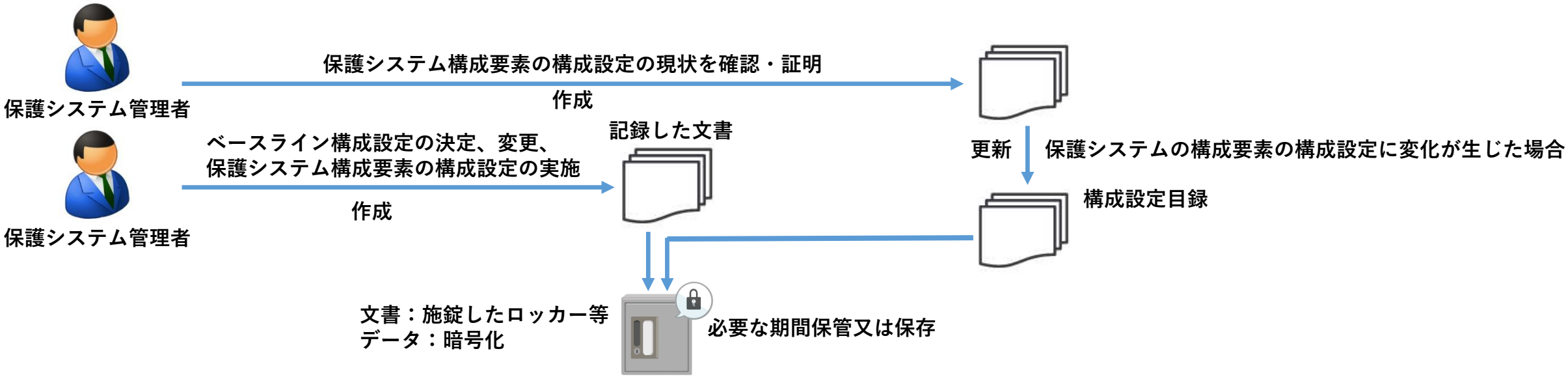
(1) 保護システム管理者は、保護システム構成要素に係る脆弱性の発見及び修正並びに業務上必要な機能の変化等が生じた場合には、総括者の承認を得て、ベースライン構成設定を変更するものとする。
(2) 保護システム管理者は、個々の保護システム構成要素において、ベースライン構成設定に従うことが不可能又は著しく合理性を欠く等の事情があると認めた場合に、総括者の承認を得て、特別の構成設定を行うものとする。
(3) 保護システム管理者は、第1号の規定によりベースライン構成設定を変更する場合及び前号の規定により特別の構成設定を行う場合は、当該構成設定が保護システムのセキュリティに及ぼす影響を分析した上で、実施するものとする。

ベースライン構成設定等の変更等



4　構成設定に係る記録及び保存等

(1) 構成設定目録
　ア　目録の作成
　(ｱ) 保護システム管理者は、保護システム構成要素の構成設定に係る現状を正確に確認及び証明するための目録（以下「構成設定目録」という。）を作成するものとする。
　(ｲ) 構成設定目録には、個々の保護システムの構成要素ごとに、保護システム管理者が指定した構成設定に責任を有する者の氏名及び連絡先等を明記するものとする。
　イ　目録の更新
　(ｱ) 保護システム管理者は、保護システム構成設定の現状に変化が生じた場合（保護システムにおけるソフトウェアのインストール及びアップデートを行った場合を含む。）は、構成設定目録を更新するものとする。
　(ｲ) 構成設定目録の内容を定期的に精査し、現状が正確に記載されていない場合は、速やかに目録を更新するものとする。
(2) 構成設定に係る記録
　保護システム管理者は、ベースライン構成設定の決定及び変更並びに保護システム構成要素構成設定の実施を記録した文書を作成するものとする。
(3) 目録等の保存等
　防衛関連企業は、構成設定目録及び第2号の規定に基づいて作成した文書を、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。



第４　保護システムの基本的防御

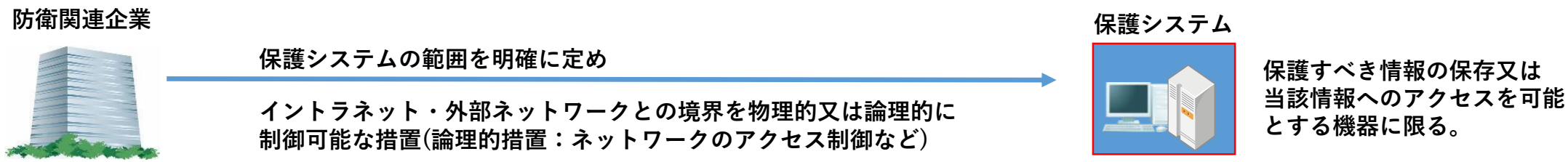
１　保護システムの領域の確定

防衛関連企業は、保護システム（保護すべき情報の保存又は当該情報へのアクセスを可能とする機器に限る。以下同じ。）における保護すべき情報を取り扱う領域を定め、イントラネット及び外部ネットワークとの境界に物理的又は論理的に制御可能な措置を行うものとする。

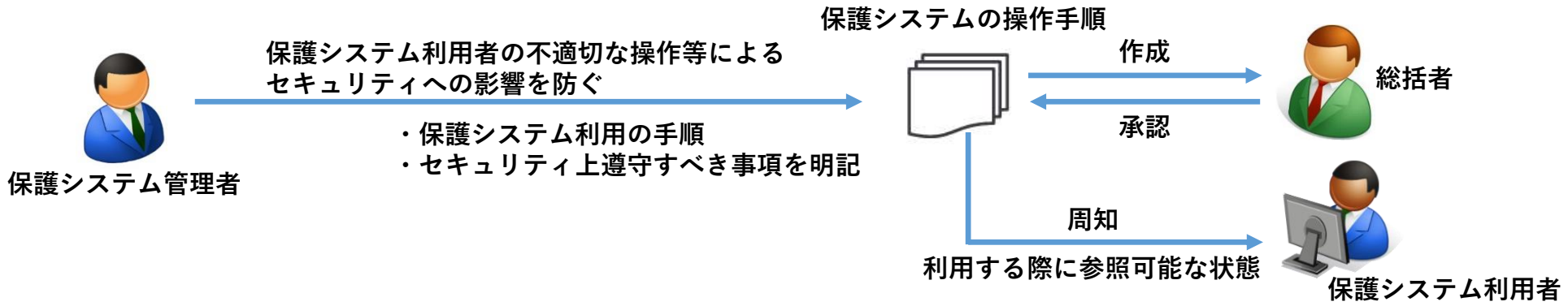
２　保護システムの操作手順書の策定

(1) 保護システム管理者は、保護システム利用者による不適切な操作が情報セキュリティに悪影響を及ぼすことを防ぐため、保護システムの利用に当たっての手順及び情報セキュリティ上遵守すべき事項等を明記した操作手順書を策定し、総括者の承認を得るものとする。
(2) 前号に規定する操作手順書は、保護システム利用者が保護システムを使用する際に参照することができる状態にするものとする。

保護システムの範囲の確定



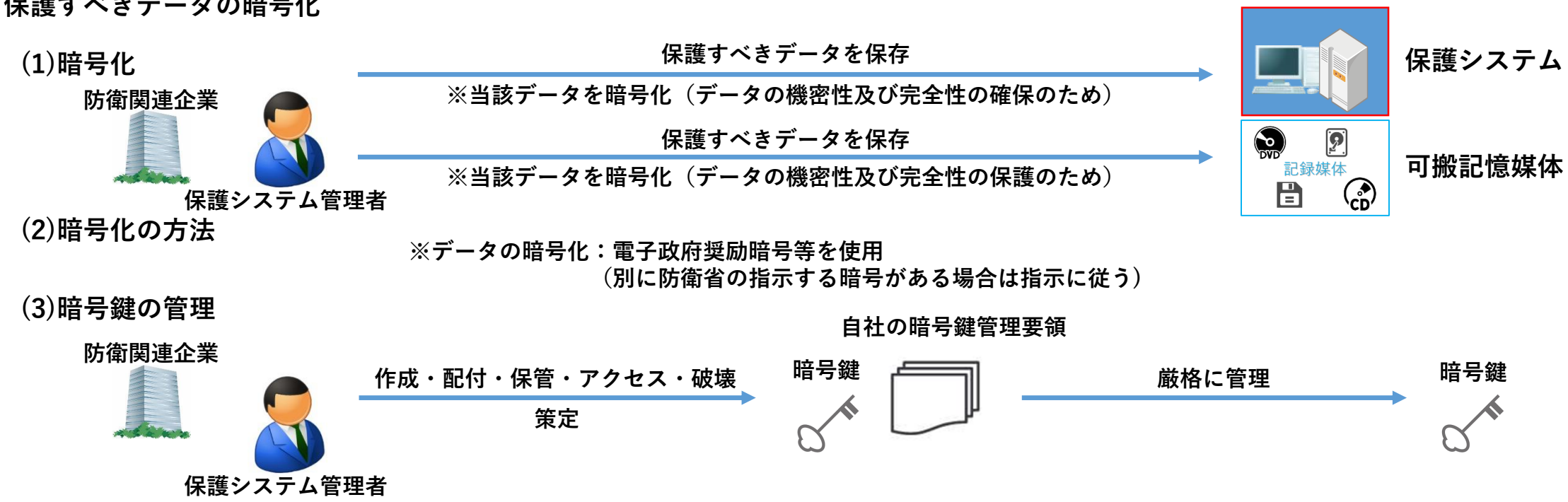
保護システムの操作手順の策定



３　保護すべきデータの暗号化

(1) 暗号化
　ア　防衛関連企業が保護システムに保護すべきデータを保存する場合は、当該データの機密性及び完全性を確保するため、 当該データを暗号化するものとする。
　イ　保護すべきデータを可搬記憶媒体に保存する場合は、当該データの機密性及び完全性を保護するため、当該データを暗号化するものとする。ただし、別に防衛省の指示がある場合には、その指示に従うものとする。
(2) 暗号化の方法
　防衛関連企業が保護すべきデータの暗号化など保護システムにおいて使用する暗号は、電子政府推奨暗号等を使用するものとする。ただし、別に防衛省が指示する場合には、その指示に従うものとする。
(3) 暗号鍵の管理
　防衛関連企業は、前号に規定する暗号の暗号鍵を、自社の管理要領により厳格に管理するものとする。

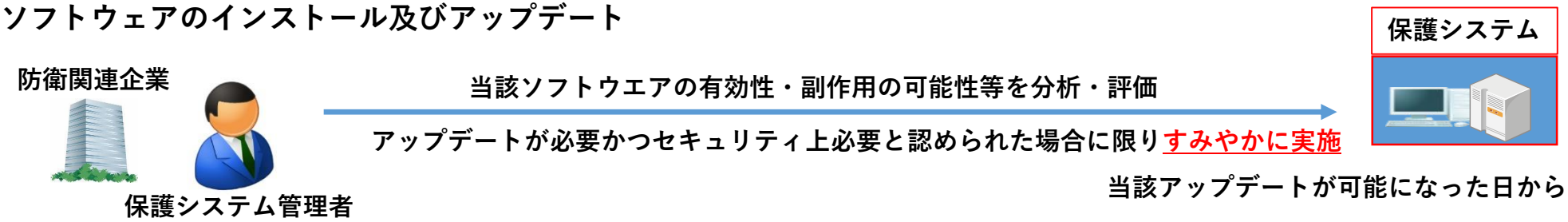
保護すべきデータの暗号化



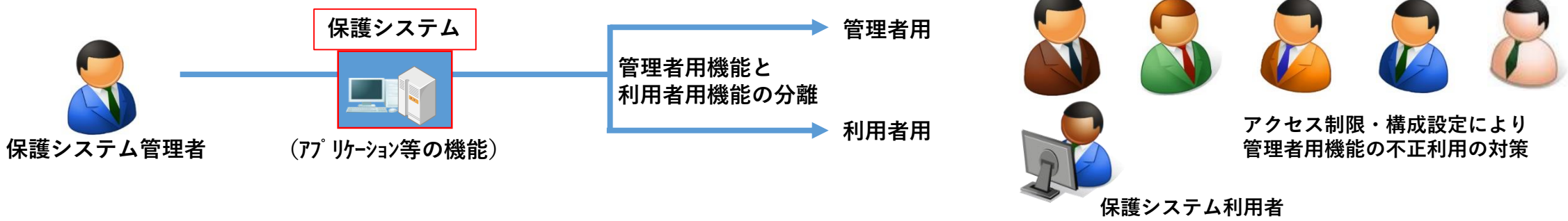
４　その他

(1) ソフトウェアのインストール及びアップデートの制限等
　ア 防衛関連企業が保護システムにおいてソフトウェアのインストール又はアップデートを行う場合は、保護システム管理者は、あらかじめその有効性や副作用の可能性等を分析及び評価し、必要かつセキュリティ上適切と認められる場合に限り実施するものとする。
　イ アに規定する分析及び評価によりソフトウェアのアップデート（パッチ及びアンチウイルスシグネチャを含む。）を実施することが必要かつセキュリティ上適切と認めた場合は、当該ソフトウェアのアップデートが利用可能となってから速やかに実施するものとする。
(2) 管理者用機能と利用者用機能の分離
　保護システム管理者は、 保護システムにおけるアプリケーション等の機能は、管理者用機能と利用者用機能を分離するものとする。
(3) 管理者用機能の不正利用防止
　保護システム管理者は、管理者権限を持たない保護システム利用者による管理者用機能の不正実行を防ぐため、アクセス制限や構成設定の実施などの対策を講じるものとする。

ソフトウェアのインストール及びアップデート



管理者用機能と利用者用機能の分離・管理者機能の不正使用防止

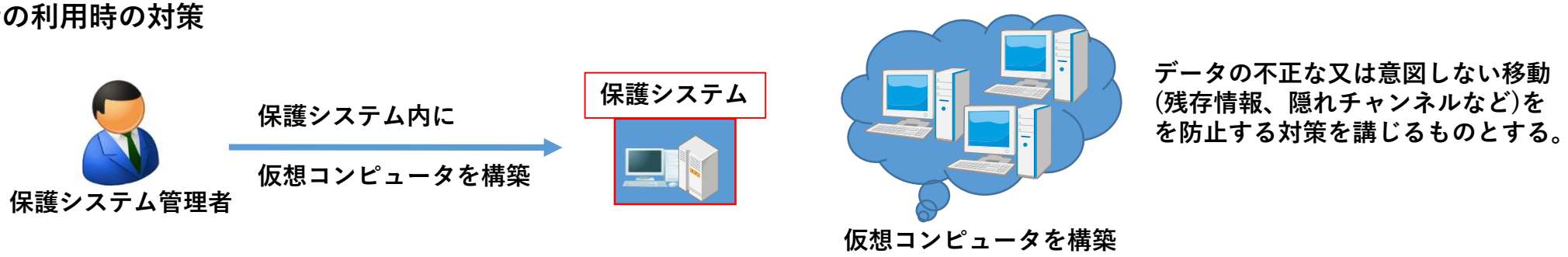


４　その他

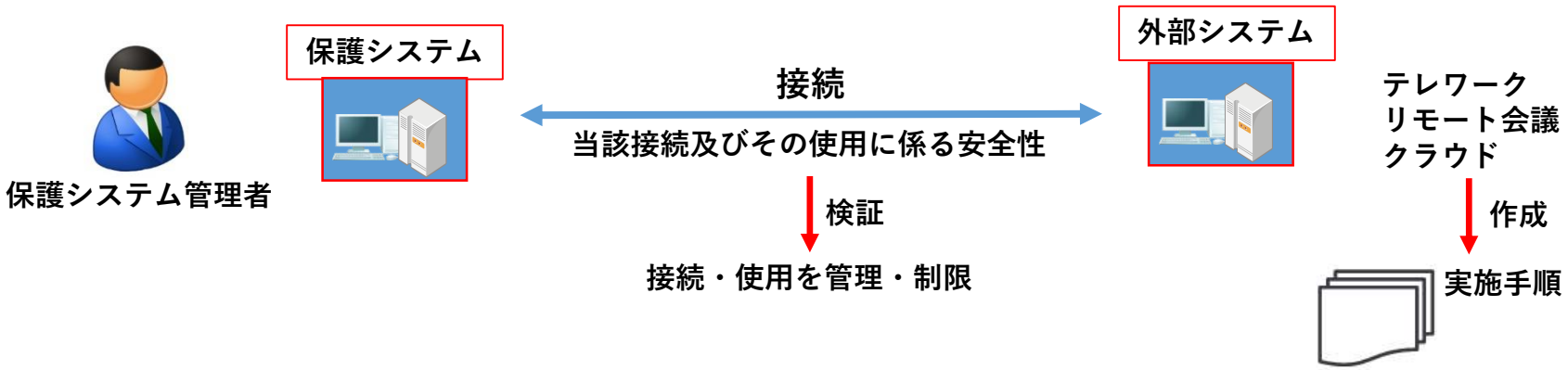
(4) 仮想化技術の利用時の対策
保護システム管理者は、保護システムを構成するハードウェア又はソフトウェアにおいて仮想化技術を利用して複数の仮想コンピュータを構築する場合は、当該仮想コンピュータ間でデータの不正な又は意図しない移動を防止する対策を講じるものとする。

(5) 外部システムとの接続制限
保護システム管理者は、保護システムを外部システムと接続する場合は、当該接続及びその使用に係る安全性を検証し、保護システムと外部システムとの接続及びその使用を管理・制限するものとする。

仮想化技術の利用時の対策



外部システムとの接続

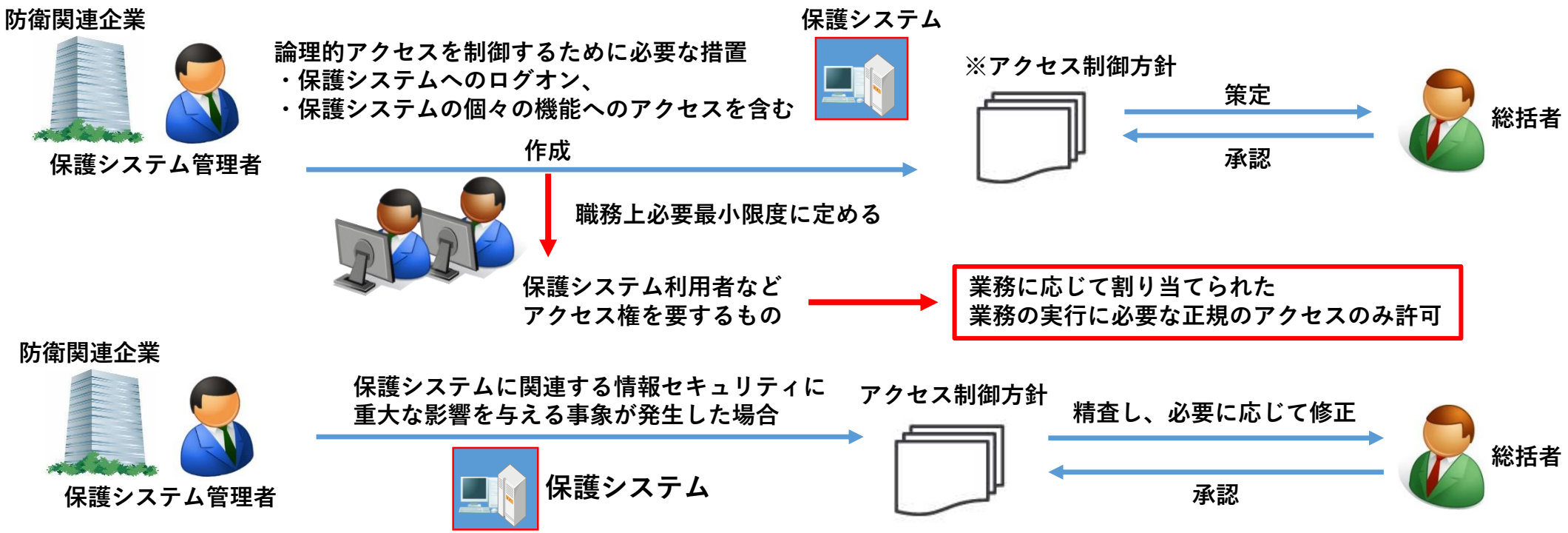


第５　アクセス制御

１　アクセス制御方針

(1) 防衛関連企業は、保護すべきデータ及び保護システムに対する論理的なアクセス（保護システムへのログオン及び保護システムの個々の機能へのアクセスを含む。以下同じ。）の制御を実施するために必要な措置を定めたアクセス制御方針を作成するものとする。
(2) アクセス制御方針は、保護システム管理者が作成し、総括者の承認を得るものとし、作成に当たっては、保護すべきデータ及び保護システムに対する論理的なアクセス権を有する者を業務遂行上必要最小限度となるよう定めるものとする。
(3) 保護システム管理者は、アクセス制御方針を定期的に、及び情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合には、その都度見直しを実施し、必要に応じてアクセス制御方針を修正するものとし、修正した場合は前号により総括者の承認を得るものとする。

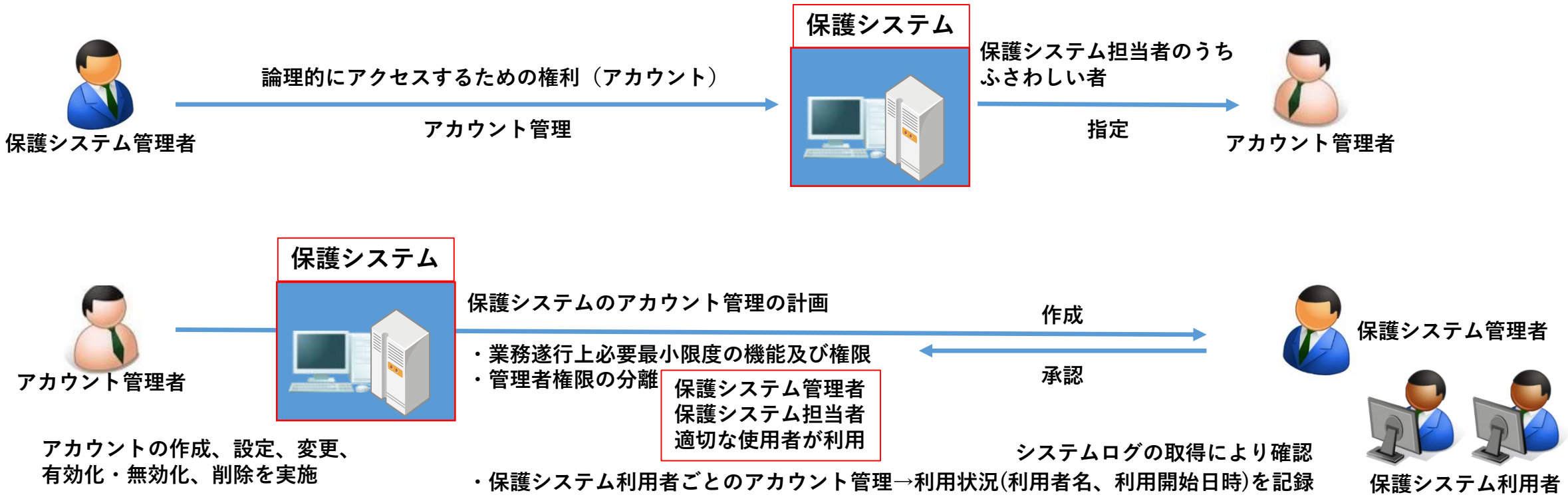
アクセス制御方針



２　アクセス制御方針に基づく管理策

(1)　アカウントの管理
ア 保護システム管理者は、保護システムへ論理的にアクセスするための権利（以下「アカウント」という。）について、保護システム担当者のうち、アカウントの設定、変更及び削除等（以下「アカウント管理」という。）を行う者としてふさわしい者をアカウント管理者に指定するものとする。
イ アカウント管理者は、業務遂行上必要最小限度の機能及び権限となるよう、アカウントの管理を計画し、保護システム管理者の承認を得て実施するものとする。その際、保護システム管理者、保護システム担当者、その他の者ごとに適切なアカウントの範囲を区別し、付与する者は必要最小限度に制限するものとする。
ウ アカウント管理者は、保護システム利用者ごとにアカウントの管理を実施するものとし、アカウントの利用状況（利用者名、利用開始日時）を記録するものとする。

アカウントの管理

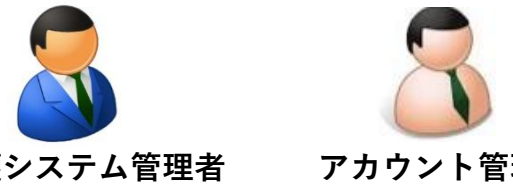


エ 保護システム利用者の退職、異動及び職務内容の変更などの事由がある場合は、当該保護システム利用者のアクセス権限を変更又は失効させるものとし、アカウント管理者は、事由の発生から定められた時間内に保護システム管理者の承認を得て必要なアカウントの管理を行うものとする。なお、これにより難い場合には、当該時間以内に、アクセス権の失効のみ実施するものとする。
オ エの規定により保護システム利用者のアクセス権限の全部又は一部を失効させる場合は、アカウント管理者は、次に掲げる措置を講じるものとする。
(ｱ) 保護システム利用者の失効するアクセス権限に関連する識別子(アカウントにあってはユーザＩＤをいい、保護システムを構成する機器にあってはホスト名等をいう。)及び認証子を無効化させること。
(ｲ) 当該保護システム利用者の失効するアクセス権限に関連する鍵、ＩＤカード等証明証及びトークン等に加え、保護システムの操作手順書等を返納させること。
(ｳ) アカウント失効日時等の記録を行うこと。
カ 保護システム管理者及び保護システム担当者が使用するアカウントなど管理者権限の一部を付与されたアカウントについては、当該権限を使用する必要がある場合にのみ使用させるものとする。

アカウントの管理

・識別子（アカウントにあってはユーザＩＤ、保護システムを構成する機器にあってはホスト名等）及び認証子(パスワードなど）の無効化
・鍵、ＩＤカード等証明証及びトークン等に加え、保護システムの操作手順書等の返納

管理者権限が付与されたアカウント



当該権限を使用する 必要がある場合にのみ使用

(2)　ログオンの管理
ア　ログオン試行
保護システム管理者は、保護システムへのログオン試行時に連続して失敗できる上限を定め、それを超えた場合には、当該ログオン試行を行ったアカウントを自動的にロックし、当該ロック時から定められた時間が経過するまで保護システムに対するログオンの再試行が行えないよう設定するものとする。
イ　保護システム利用者が保護システムにログオン試行を行う場合は、パソコンの画面上に不正なログオン試行に有用な情報を表示させないものとする。

ログオンの管理

保護システム利用者

ログオン試行
連続して失敗できる上限

アカウントをロック
ロック時から定められた期間ログオン試行できないように設定

保護システム

保護システム利用者が保護システムにログオン試行を行う際、
保護システムのパソコン上に不正なログオン試行に有用な情報を表示してはならない

(3)　ユーザセッションの管理
保護システム管理者は、保護システムにログオンした保護システム利用者のユーザセッションについて、次に掲げる方法により管理を行うものとする。
ア 非アクティブ状態であり続ける時間の上限を設定し、それを超えた場合は、当該ユーザセッションをロックすること。
イ 保護システム利用者がパソコン（保護システム）の置かれた席から離席する際には、当該ユーザセッションをロックさせること。
ウ 当該ユーザセッションをロックした場合の不正なアクセス及びデータの閲覧等を防止するため、パソコンのディスプレイの全面をスクリーンセーバ等により保護すること。
エ 当該ユーザセッションのロックを解除する場合は、保護システム利用者に対し、第６第１項第２号アに規定する多要素認証を行わせること。
オ 保護システム利用者が、保護システム上でログオフを要求した場合には、自動的に当該ユーザセッションを終了させること。
カ 当該ユーザセッションを終了させる場合には、保護システム利用者が継続実行を設定した計算処理プログラム等を除き、すべてのソフトウェアプログラムを終了させること。

ユーザーセッション の管理

保護システム利用者

・一定時間非アクティブになった場合に当該セッションをロック
・パソコンの置かれた席から離れる場合は、当該ユーザーセッションをロック
・当該セッションをロックした場合は、パソコンのディスプレイの前面をスクリーンセーバー等により保護
・ユーザーセッションのロックを解除するためには、保護システム利用者に多要素認証を行わせる
・保護システム利用者がログオフを要求した場合には、当該ユーザーセッションを終了させること
・ユーザーセッションを終了させる場合には、保護システムが継続実行を設定した計算処理プログラムを除きすべてのソフトウェアを終了させること

(4)　リモートアクセスの管理
ア　保護システム管理者は、保護システムへのリモートアクセスの利用を業務遂行上必要最小限度に制限するとともに、事前に承認するものとする。
イ　アの規定によりリモートアクセスを利用する場合は、当該アクセスを通じた通信を適切に保護するため、次に掲げる措置を実施するものとする。
(ｱ) 保護システムへのリモートアクセスに係る通信を暗号化すること。
(ｲ) リモートアクセス等を受ける保護システムの境界（プロキシサーバ、バーチャル・プライベート・ネットワーク（ＶＰＮ）サーバ等）を必要最小限度に制限すること。
(ｳ) 保護システムへのリモートアクセスを利用している場合は、同時に当該リモートアクセスに利用するものとは異なる通信経路を利用しないこと。
ウ　保護システムへのリモートアクセス等を利用している際の管理者権限の使用は、事前に保護システム管理者が承認した場合を除き、禁止するものとする。

リモートアクセスの管理

リモートアクセス等を利用する場合の措置

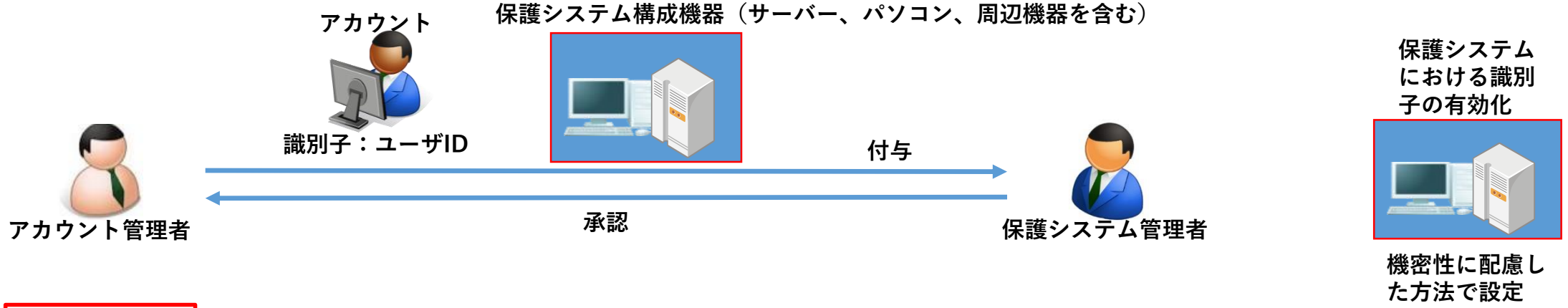
・保護システムとリモートアクセス等に係る通信経路を暗号化
・リモートアクセス等を受ける保護システムの境界（プロキシサーバー、バーチャルプライベートネットワークサーバー（VPN）サーバー等）を必要最小限度
・保護システムへのリモートアクセス等を利用している場合は、同時に当該リモートアクセスに利用するものとは異なる通信経路(スプリットトンネルの防止）を利用しない。管理者権限の使用の禁止（事前に保護システム管理者が承認した場合は除く）

第６　識別及び認証子

１　識別及び認証等の実施

(1)　識別の実施
ア　アカウント管理者は、アカウント及び保護システムを構成する機器（サーバ、パソコン及び周辺機器を含む。）に対し、識別可能な識別子を付与し、保護システム管理者の承認を得るものとする。
イ　アに規定する識別子を当該保護システムにおいて有効化する場合は、機密性に配慮した方法で設定するものとする。
ウ　アに規定する識別子を他のアカウント及び保護システムを構成する機器に対し再利用してはならない。ただし、当該識別子の使用を終えた日から定められた期間を経過した場合にはこの限りでない。
エ　アに規定する識別子が保護システムにおいて定められた期間以上使用されなかった場合は、当該識別子を無効化するものとする。
オ　保護システム利用者の代理として動作するプロセスを識別するものとする。

識別子及び認証子

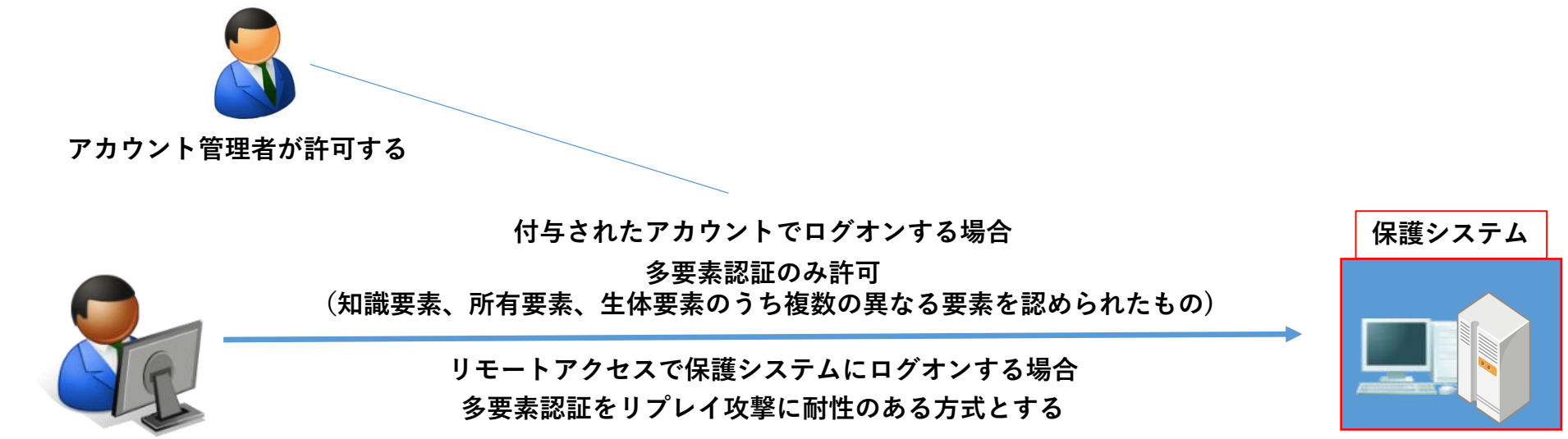


識別子の管理策

※識別子を他のアカウント・保護システムを構成する機器に対して再利用しない
　ただし、定められた期間を経過した場合はそのかぎりでない。
※識別子が保護システムにおいて定められた期間以上使用されなかった場合は、当該識別子を無効化
※保護システム利用者の代理として動作するプロセスを識別

(2)　認証の実施
ア　アカウント管理者は、保護システム利用者が第５第２項第1号の規定により付与されたアカウントで保護システムにログオンする場合は、本人だけが知る要素（以下「知識要素 」という。）、本人だけが所有する要素(以下「所持要素 」という。)及び本人の持つ生体的要素(以下「生体要素 」という。)のうち複数の異なる要素を保持すると認められた者のみを許可（以下「多要素認証」という。）するものとする。
イ　保護システム利用者がリモートアクセスにより保護システムにログオンする場合は、アに規定する多要素認証をリプレイ攻撃に耐性のある方式で行うものとする。
ウ　アに規定するログオンを認証する場合は、当該ログオンに使用される機器が、前号アの規定により識別子を付与された機器であることを識別するものとする。
エ　保護システム利用者の代理として動作するプロセスが保護システムに対しアクセスする場合は、当該プロセスが前号オの規定により識別されたプロセスであることを認証するものとする。

認証の実施



・保護システムログオンに使用される機器が識別子を付与された機器であることを識別する。
・保護システム利用者の代理として動作するプロセスが保護システムにアクセスする場合は、当該プロセスが識別されたプロセスであることを認証する。

(3) パスワードによる認証の実施
ア アカウント管理者は、 第１号アに規定するアカウントのユーザＩＤに係る初期パスワードを保護システム利用者に割り当てる場合は、容易に推測されず、かつ、アカウントごとに異なるパスワードを割り当てるものとする。
イ アに規定する初期パスワードを保護システム利用者に配付する場合は、機密性に配慮した方法により行うものとする。
ウ 保護システム利用者が初期パスワードを使用した認証により保護システムにログオンした場合は、直ちに当該パスワードを変更させるものとする。
エ 保護システム利用者が作成又は変更するアカウントのユーザＩＤに係るパスワードは、次に掲げる要件を満たすものとする。
(ｱ) 大文字英字、小文字英字、数字及び特殊文字をそれぞれ１文字以上使用した１４文字以上であり、容易に推測されないものであること。
(ｲ) 定められた期間以内に変更すること。
(ｳ) 世代にわたって同じパスワードを使用しないこと。
(ｴ) 紙等への記載又は記憶媒体への保存（オに規定する場合を除く。）が行われていないこと。
オ 保護システムへのログオンに使用されるパスワードを認証するため、当該保護システム内において保存・伝送する必要があるパスワード情報は、他の者が容易に復号できない方式を用いて保存・伝送するものとする。
カ 保護システム利用者が作成したパスワードを忘失した場合は、当該パスワードを無効化するとともに、当該保護システム利用者に対し、アの規定により初期のパスワードを配付するものとする。

保護システム管理者

アカウント管理者

初期又は仮のパスワードを配付する場合

容易に推測されず、アカウントごとに異なるパスワードを割り当てる機密性に配慮した方法により配付。
保護システム利用者が初期又は仮のパスワードを使用して保護システムにログオンした場合、当該パスワードを変更させる。

保護システム利用者

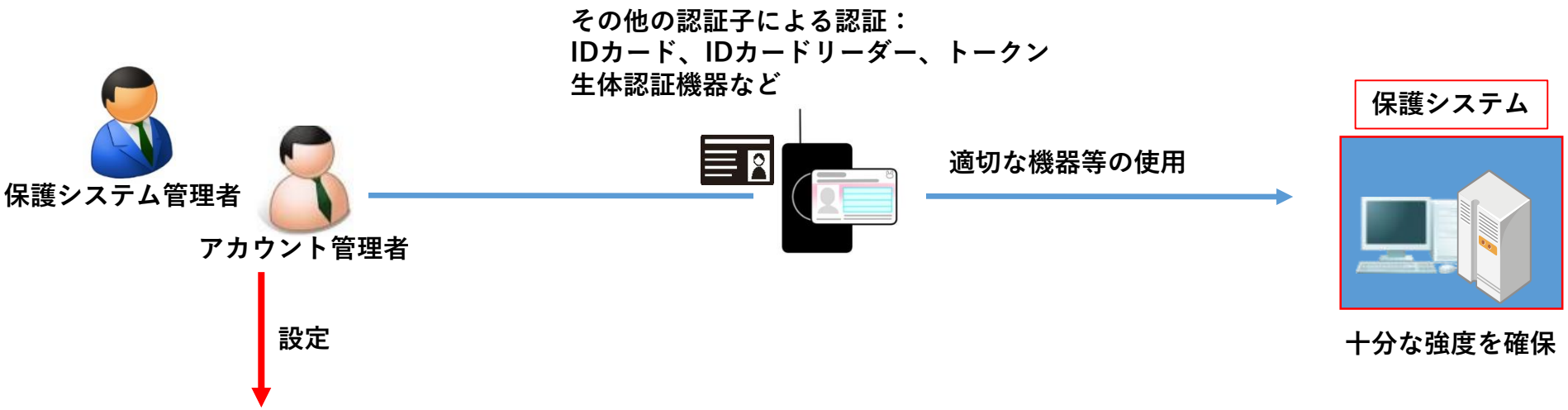
- パスワードを認証するため、当該保護システム内に保存・伝送する必要があるパスワード情報→バッシュ化等の復号不可能な暗号化方法を用いて保存・伝送。
- 保護システム利用者がパスワードを忘失した場合→当該パスワードを無効化するとともに当該システム利用者に仮のパスワードを配付。

パスワードの作成

・大文字英字、小文字英字、数字及び特殊文字をそれぞれ1文字以上使用した１４文字以上であり、容易に推測されないもの
・作成又は変更の日から定められた期間以内に変更
・世代にわたって同じパスワードを使用しない
・紙等への記載又は記憶媒体への保存が行われていないこと

２　識別及び認証におけるその他の留意事項

(1) 保護システム管理者は、その他の認証子による認証について、適切な機器等（ＩＤカード、ＩＤカードリーダー、トークン及び生体認証機器を含む。以下同じ。）を使用することにより、十分な強度を確保するものとする。
(2) 保護システム管理者は、 前号に規定する機器等は、不正なアクセス等から保護するため厳格に管理するものとする。
(3) 保護システム管理者は、第1号に規定する機器等を紛失又は破損等により交換する場合は、保護システムにおいて、当該機器等による認証を無効化するものとする。

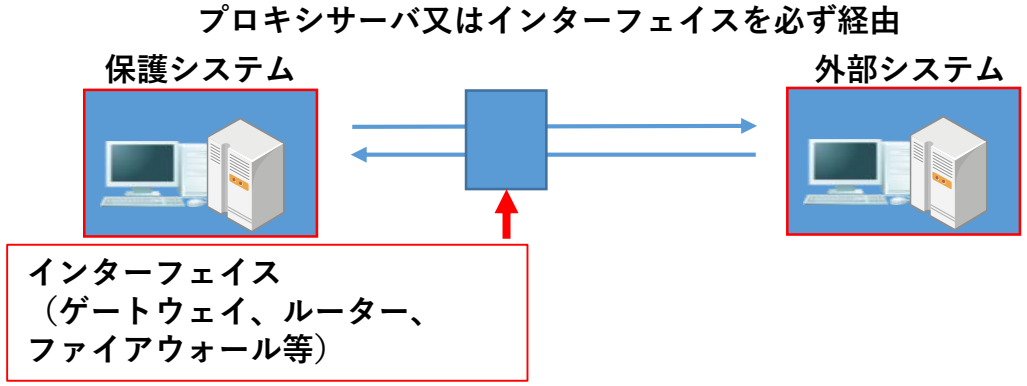


- その他の認証に該当する認証子を当該保護システムにおいて有効化する場合は、機密性に配慮した方法で設定。
- その他の認証については、不正なアクセス等から保護するため、厳格に管理。
- 紛失又は破損等により交換する場合には、保護システムにおいて当該機器等による認証を無効化。

１　通信の制御

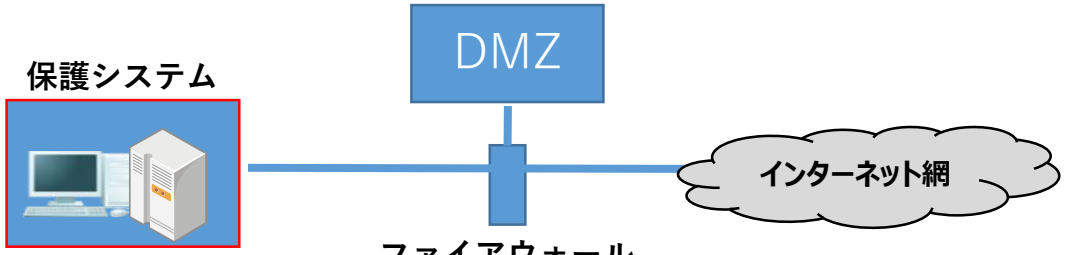
(1) 防衛関連企業が保護システムと外部ネットワークとの通信を行う場合は、プロキシサーバ又はインターフェイス(ゲートウェイ、ルーター及び、ファイアウォール等)を設置し、必ず当該機器を経由する通信を行うものとし、当該機器は許可された通信以外は拒否するよう設定するものとする。
(2) インターネットなど不特定多数の者がアクセス可能なウェブサーバ等を保有する場合は、当該ウェブサーバ等を含むサブネットワークを設置するものとし、リモートアクセスを実施する場合は、リモートアクセスを管理するインターフェイスを設置するものとする。

①保護システムと外部ネットワークとの通信を行う場合



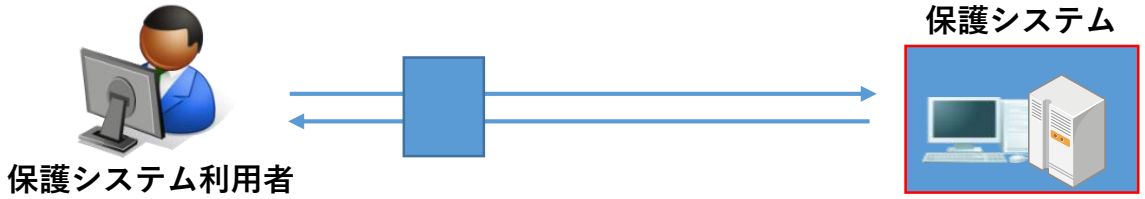
許可された通信以外は拒否するように設定

②インターネットなど不特定多数の者がアクセス可能なウェブサーバ等を保有する場合



当該ウェブサーバ等を含むサブネットワークを設置

③リモートアクセスを実施する場合

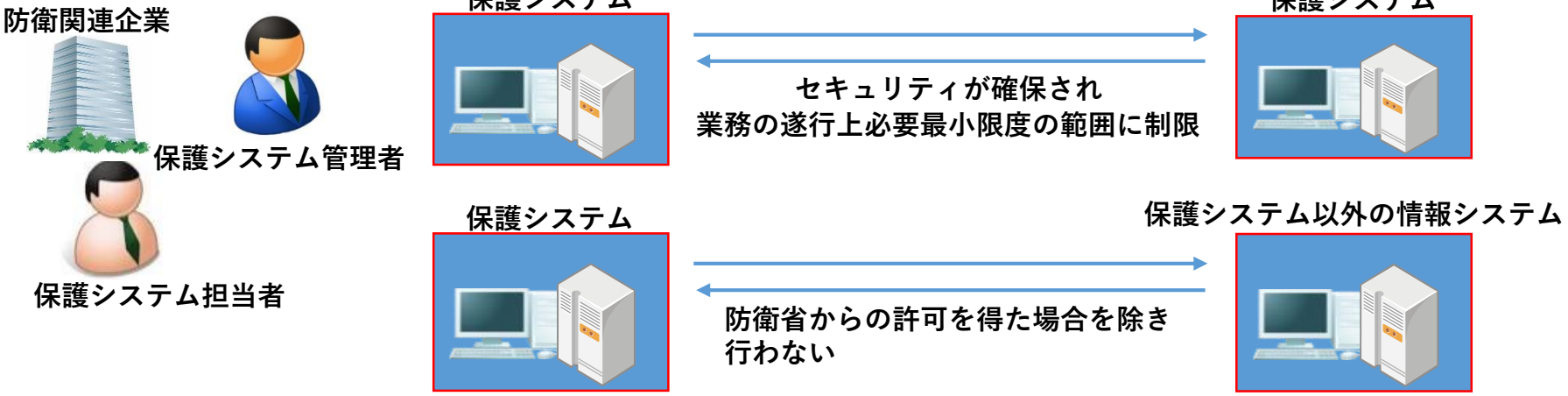


リモートアクセスを管理するインターフェース設置

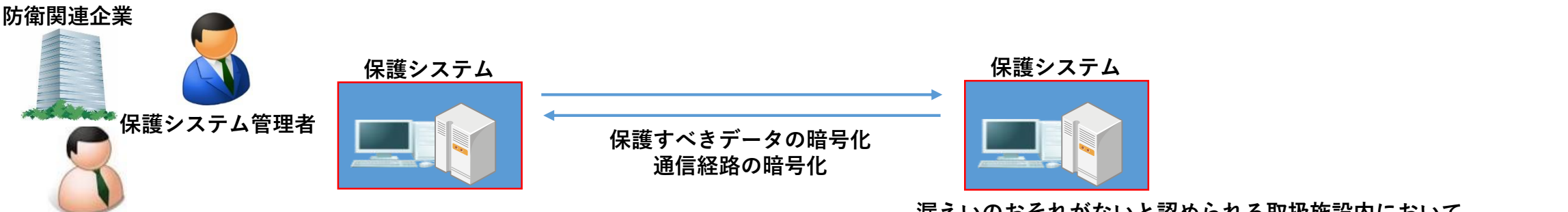
２　通信データ及び通信セッションの保護

(1) 保護すべき情報の通信制限
ア　防衛関連企業が保護すべきデータの通信を行う場合は、セキュリティが確保され、かつ、業務の遂行上必要最小限度の範囲に制限するものとし、防衛省からの許可を得た場合を除き、保護システム以外の情報システムとの間における保護すべきデータの通信を行わないものとする。
イ　保護すべきデータの通信を行う場合は、第４第３項第1号の規定により暗号化されたデータにより行うか、当該データを転送する通信経路を暗号化しなければならない。ただし、漏えいのおそれがないと認められる取扱施設内において、送配線（有線）等により通信が行われる場合は、この限りでない。

保護すべきデータの通信

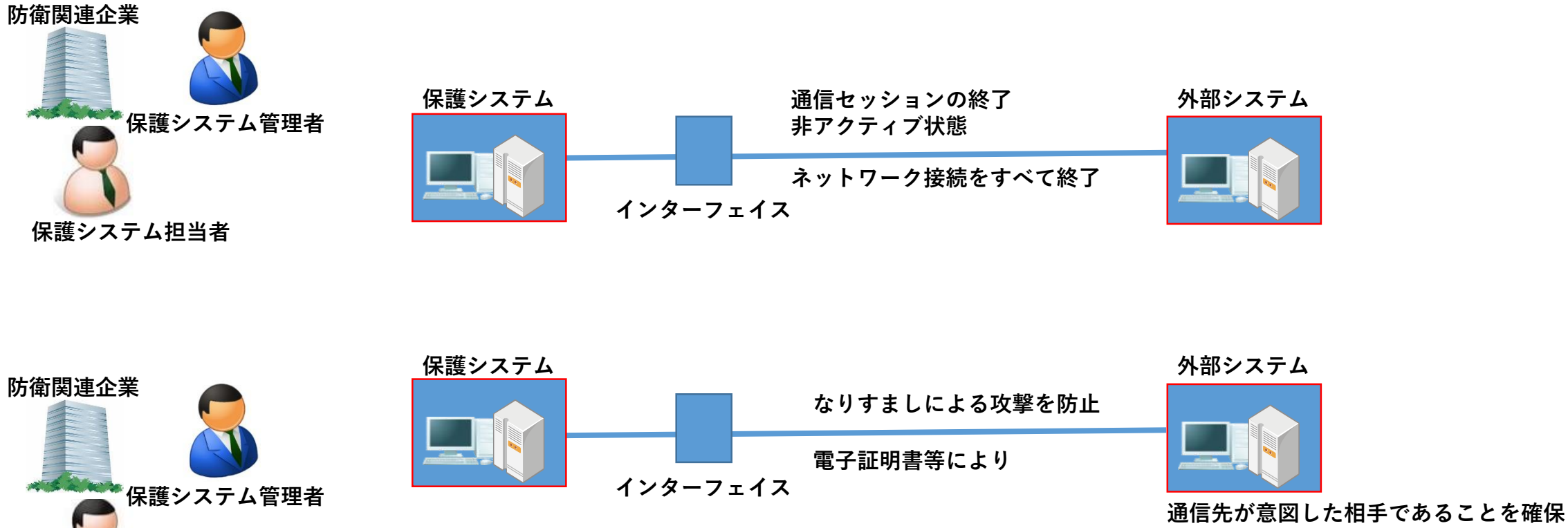


保護すべきデータの通信を行う場合



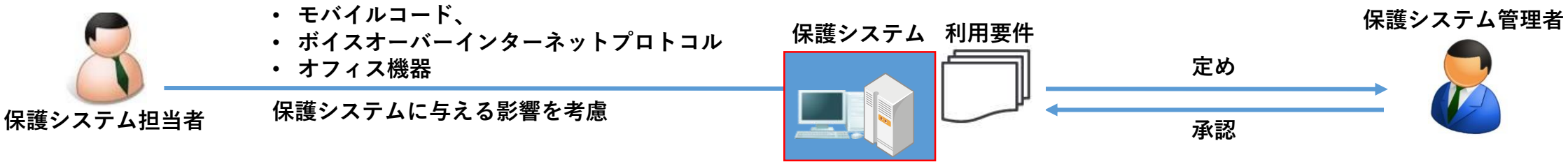
(2) 通信セッションの保護
ア 保護システムを利用した通信のセッションの終了時又は当該セッションが非アクティブ状態で定められた期間を経過した場合は、当該セッションに関連するネットワーク接続を全て終了させるものとする。
イ 保護システムと外部ネットワークにおける通信のセッションにおいては、なりすましによる攻撃等を防止するため、電子証明書等の方法により、通信先が意図した相手であることを確保するものとする。

通信セッション



３ 通信機能の利用制限

(1) モバイルコード
　ア　保護システム管理者は、モバイルコードが悪意のある者により利用された場合の保護システムに与える被害を考慮し、保護システムにおける利用の要件を定めるものとする。
　イ　保護システムにおけるモバイルコードの利用は、アに規定する利用の要件を満たす場合に限り許可することとし、当該許可に当たっては、保護システム管理者の承認を得るものとする。
(2) ＩＰネットワークによる音声伝達技術（以下「ＶｏＩＰ技術」という。）
　ア　保護システム管理者は、ＶｏＩＰ技術が悪意のある者により利用された場合の保護システムに与える被害を考慮(通話内容の改ざん及び漏えい等を防ぐための通信経路の暗号化を含む)した、保護システムにおける利用の要件を定めるものとする。
　イ　保護システム管理者は、保護システムにおけるＶｏＩＰ技術は、アに規定する利用の要件を満たす場合に限り許可することとし、当該許可に当たっては、保護システム管理者が承認するものとする。
(3)　オフィス機器
　ア　保護システム管理者は、保護システムに接続された電子ホワイトボード、ネットワークカメラ等の各種のオフィス機器等が悪意のある者により利用された場合の保護システムに与える被害を考慮し、次に掲げる事項を含めた保護システムにおける利用要件を定めるものとする。
　　(ｱ) 当該機器に対するリモートアクセスによる起動及び操作を禁止すること。
　　(ｲ) 当該機器が起動している場合には、外形的に明らかな表示を行うこと。
　イ　保護システムに接続されたオフィス機器等の利用は、当該利用の都度、アに規定する利用の要件を満たす場合に限り許可することとし、当該許可に当たっては、保護システム管理者の承認を得るものとする。

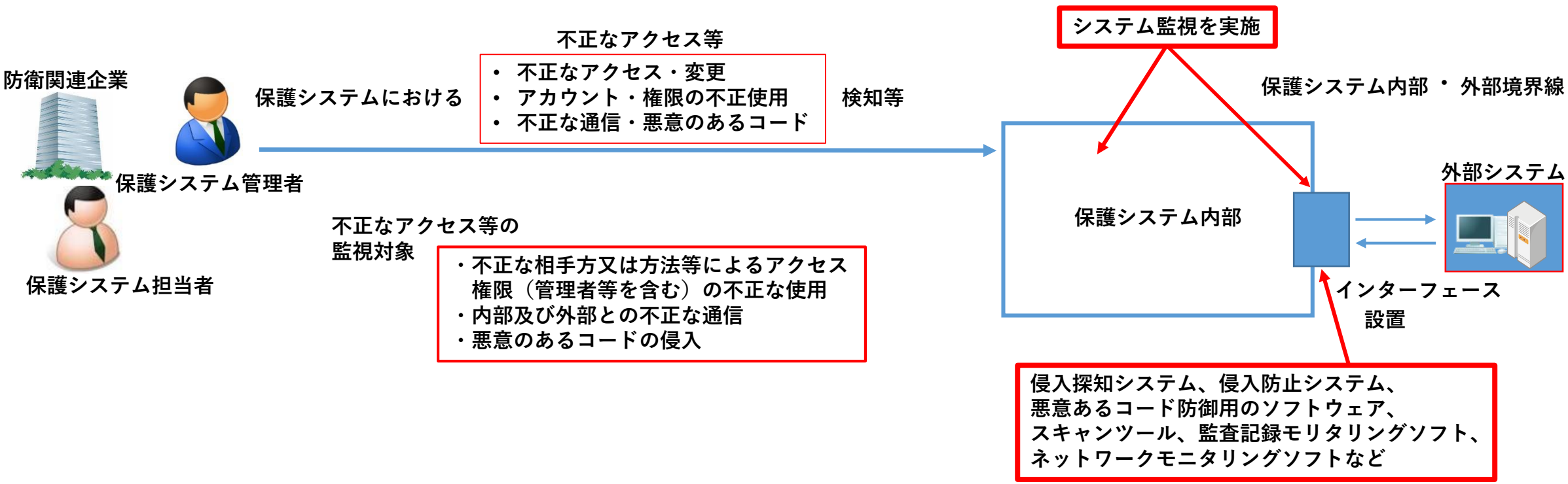


第８　システム監視

１ システム監視の実施

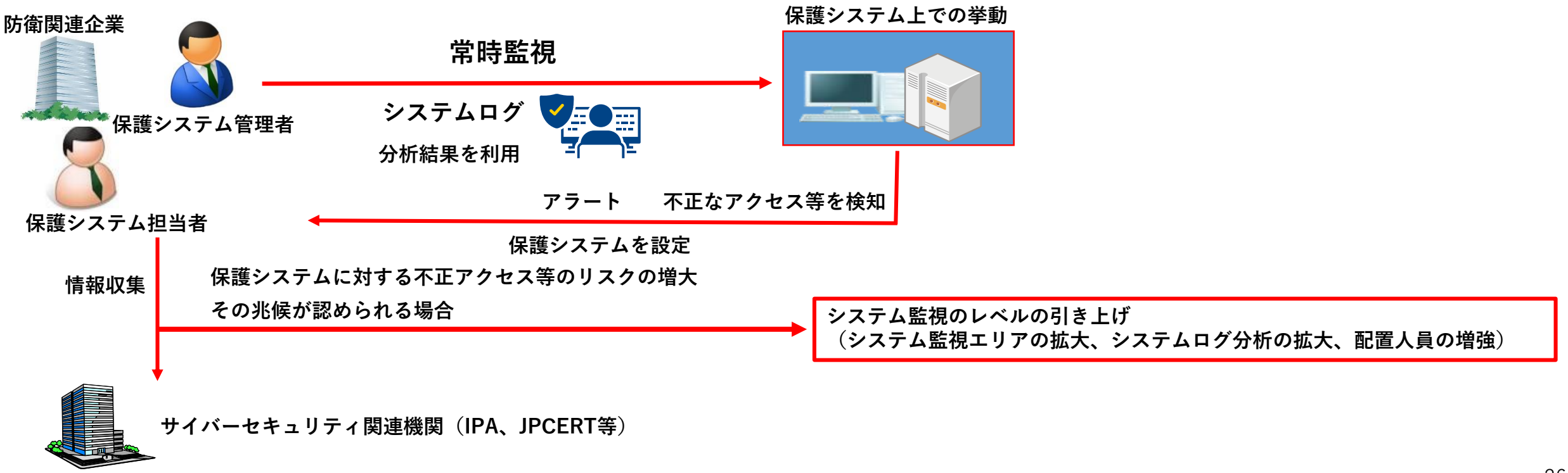
防衛関連企業は、保護システムにおける不正なアクセス及び変更、アカウント及び権限の不正な使用、不正な通信並びに悪意のあるコード等（以下「不正なアクセス等」という。）の検知に必要な情報の収集を行うための機器の設置、ソフトウェアのインストール等を実施し、次の事項について保護システムの内部及び外部境界に対する監視（以下「システム監視」という。）を実施するものとする。

（1）不正な相手方又は方法等によるアクセス
（2）権限（管理者権限を含む。）の不正な使用
（3）内部及び外部との不正な通信
（4）悪意のあるコードの侵入



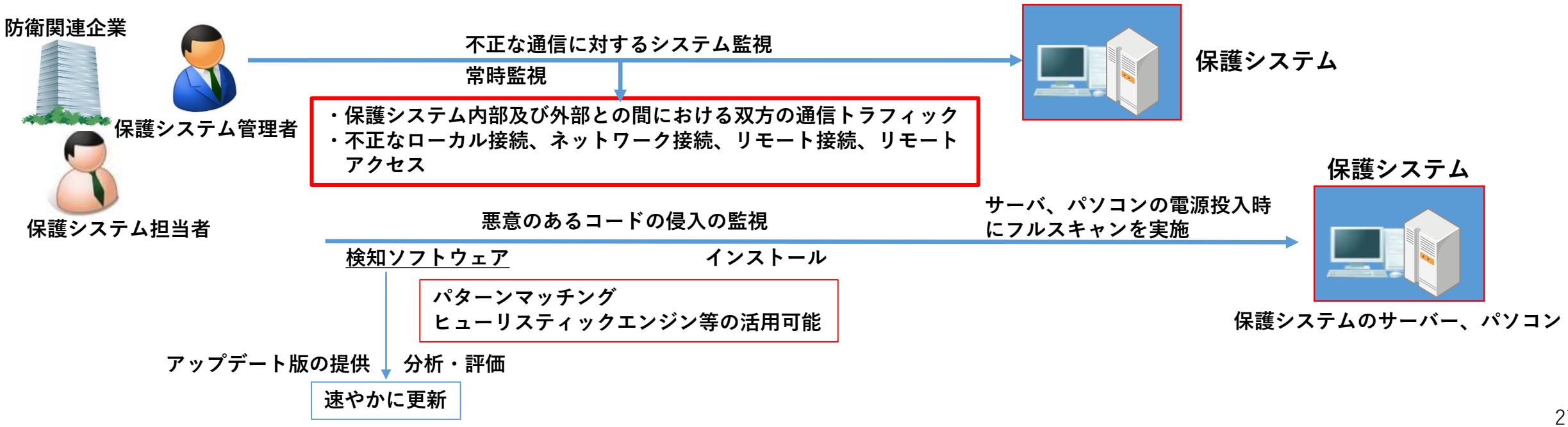
２　システム監視の実施方法

(1) システム監視の実施に係る共通事項
ア　防衛関連企業がシステム監視を実施する場合は、システム上での挙動を常時監視するとともに、第９第１項の規定により作成されたシステムログの分析結果を利用するものとする。
イ　システム監視により不正なアクセス等を検知した場合は、保護システム管理者及び保護システム担当者にアラートが発せられるよう、保護システムを設定するものとする。
ウ　保護システムに対する不正なアクセス等のリスクの増大又はその兆候等が認められる場合には、必要に応じ、システム監視のレベルを引き上げるものとする。



第８　システム監視

(2) システム及び通信の監視方法
　ア　防衛関連企業が第１項第3号に掲げる不正な通信に対するシステム監視を実施する場合は、次に掲げる事項に対する常時監視を行うものとする。
　　(ｱ)保護システムの内部及び外部との間における双方向の通信トラフィック
　　(ｲ)不正なローカル接続、ネットワーク接続、リモート接続及びリモートアクセス
　イ　悪意のあるコードの検知
　　(ｱ)第１項第4号に掲げる悪意のあるコードの侵入の監視は、保護システムを構成するサーバ及びパソコンにおける悪意のあるコードを検知するためのソフトウェア（以下「検知ソフトウェア」という。）として、ウイルス定義を用いたパターンマッチング手法のほか、未知の脅威に対応するためのヒューリスティックエンジン等の高度な手法を活用可能なソフトウェアをインストールするものとする。
　　(ｲ)ウイルス定義及び検知ソフトウェアのアップデート版が提供された場合において、第４第４項第１号に規定する分析及び評価によりそれらのアップデートを実施することが必要かつ適切と認められるときは、速やかにアップデートを行うものとする。
　　(ｳ)悪意のあるコードを検知するため、保護システムに対する検知ソフトウェアによるフルスキャンを定期的に実施するものとする。なお、一定の期間以上電源の切断された状態にあるサーバ又はパソコン等については、再度の電源投入時に当該処置を実施するものとする。
　　(ｴ)検知ソフトウェアにより、保護システムにおけるファイルのダウンロード、開封及び実行等の都度、当該ファイルに対する、悪意のあるコードを検知するためのリアルタイムスキャンを実施するものとする。



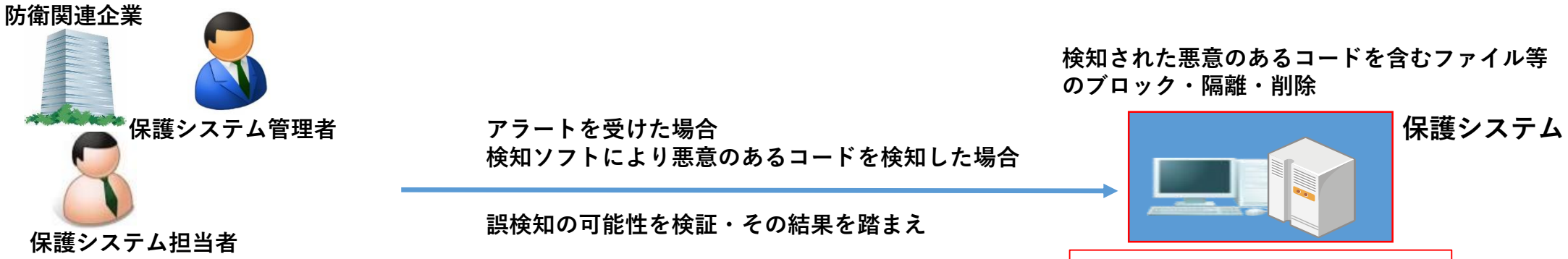
３　不正なアクセス等を検知した際の対応

保護システム管理者が第２項第1号イに規定するアラートを受けた場合又は検知ソフトウェアによる悪意のあるコードを検知した場合は、検知ソフトウェアによる誤検知の可能性を検証し、その結果を踏まえ、検知された悪意のあるコードを含むファイル等のブロック、隔離若しくは削除又はそれらを適切に 組み合わせた措置を実施するものとする。

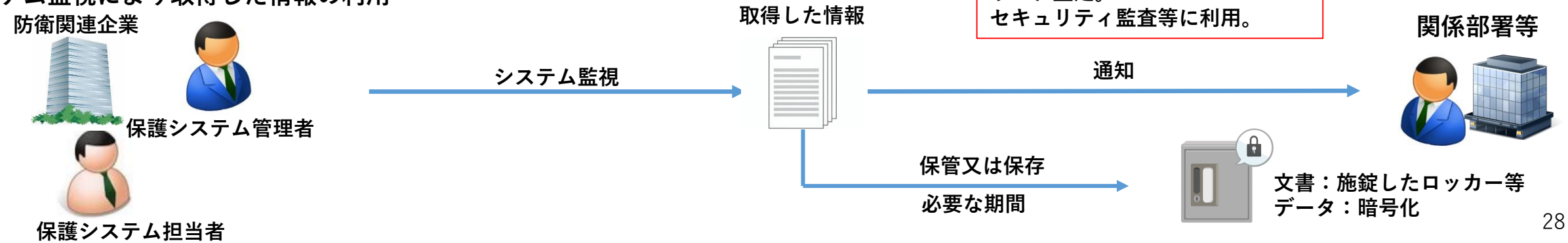
４　システム監視により取得した情報の利用及び保管

(1) 防衛関連企業は、システム監視により取得した情報を、情報セキュリティ事故等への対処などに利用するものとし、保護システム管理者は、取得した情報を関係部署等に通知するものとする。
(2) システム監視により取得した情報に対する不正なアクセス、改ざん及び消去等を防ぐため、当該取得した情報は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保存又は保管するものとする。

不正なアクセス等を検知した際の対応



システム監視により取得した情報の利用

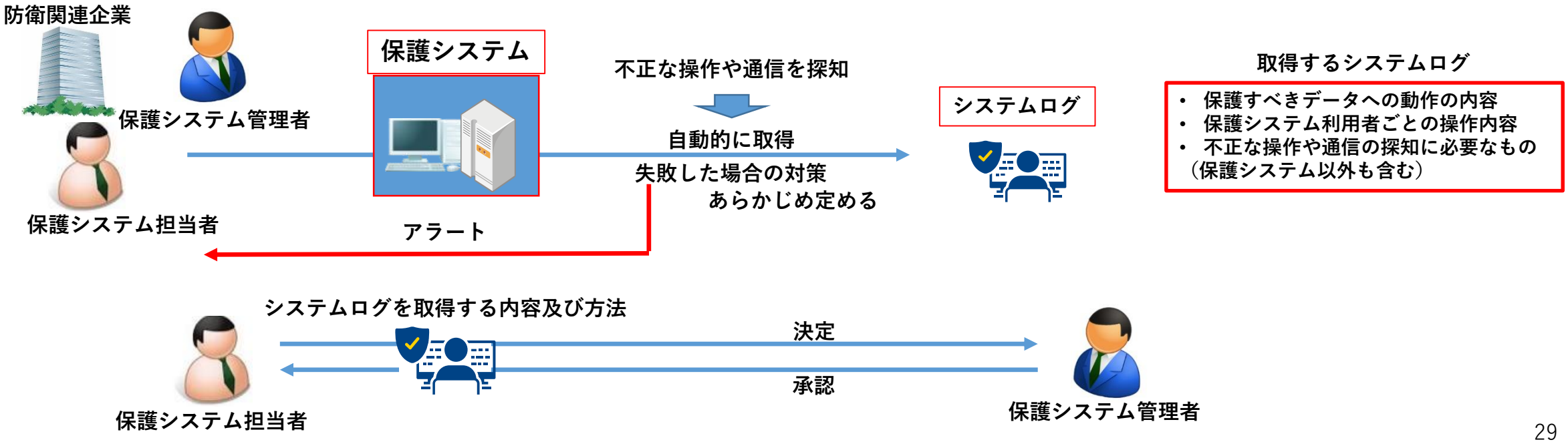


第９　システムログ

１　システムログの取得及び分析

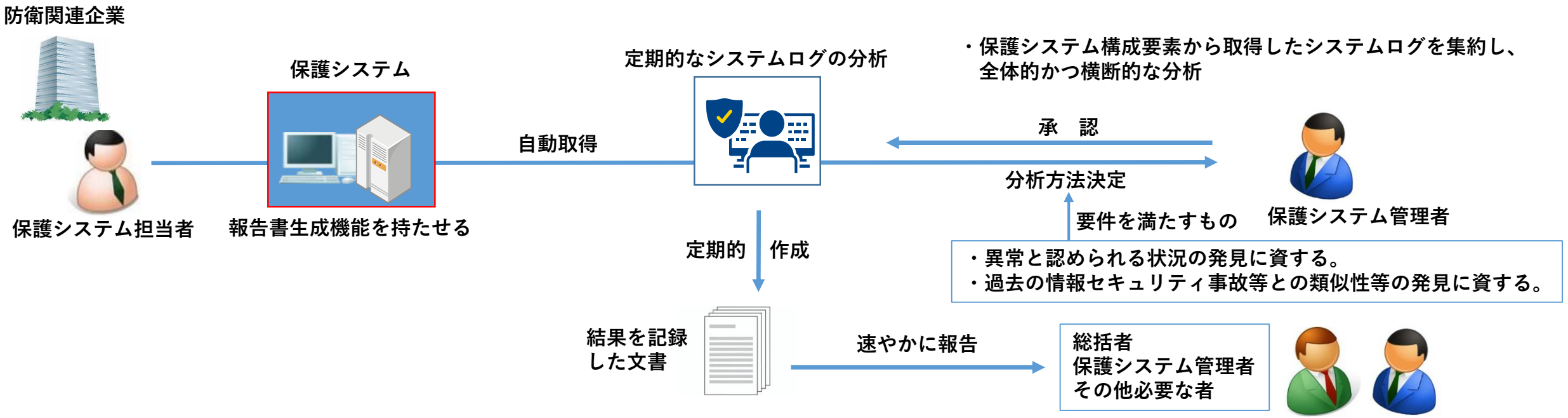
(1)　システムログの取得
ア　防衛関連企業は、保護システムにおける不正な操作や通信を探知するため、次に掲げる事項に係る記録をシステム上で自動的に取得するものとする。
　(ｱ)保護すべきデータへの動作の内容
　(ｲ)保護システム利用者ごとの操作内容
イ　保護システム担当者はアに規定するシステムログのほか、保護システムにおける不正な操作や通信を探知するために必要となるシステムログの内容並びにその取得に係る対象及び方法を決定し、保護システム管理者の承認を得るものとする。
ウ　ア及びイに規定するシステムログの内容並びにその取得に係る対象及び方法は、保護システムにおいて取得可能であることを事前に検証するものとし、取得困難である場合は、当該保護システムにおいて実施可能な監視手法の再設計を検討するものとする。
エ　システムエラー等によりシステムログの取得に失敗する場合に備え、当該失敗の影響の低減及び復旧等に係る対策をあらかじめ定めるものとし、取得に失敗した場合は、保護システム担当者等必要な者に対しアラートを発するとともに、ウに規定する措置を行うものとする。
オ　ア及びイに規定するシステムログの内容並びにその取得に係る対象及び方法は、定期的に精査し、必要に応じて変更するものとする。

システムログの取得



第９　システムログ

(2) システムログの分析
　ア　保護システム担当者は、定期的にシステムログの分析を実施するものとし、分析を行う場合は、保護システム構成要素から取得したシステムログを集約し、全体的かつ横断的な分析を行うものとする。
　イ　システムログの分析の方法は、次に掲げる要件を考慮して選択し、保護システム管理者の承認を得るものとする。
　　(ｱ)異常と認められる状況の発見に資すること。
　　(ｲ)過去の情報セキュリティ事故等との類似性等の発見に資すること。
　ウ　システムログの分析及び分析結果の報告をサポートするため、保護システムに報告書生成機能を持たせるものとする。
　エ　システムログの分析を行った場合は、その結果を記録した文書を作成し、速やかに総括者及び保護システム管理者その他必要な者に報告するものとする。
　オ　エに規定するシステムログの分析に係る結果を記録した文書の作成においては、システムログの内容（時刻の順序を含む。）を変更しないものとする。

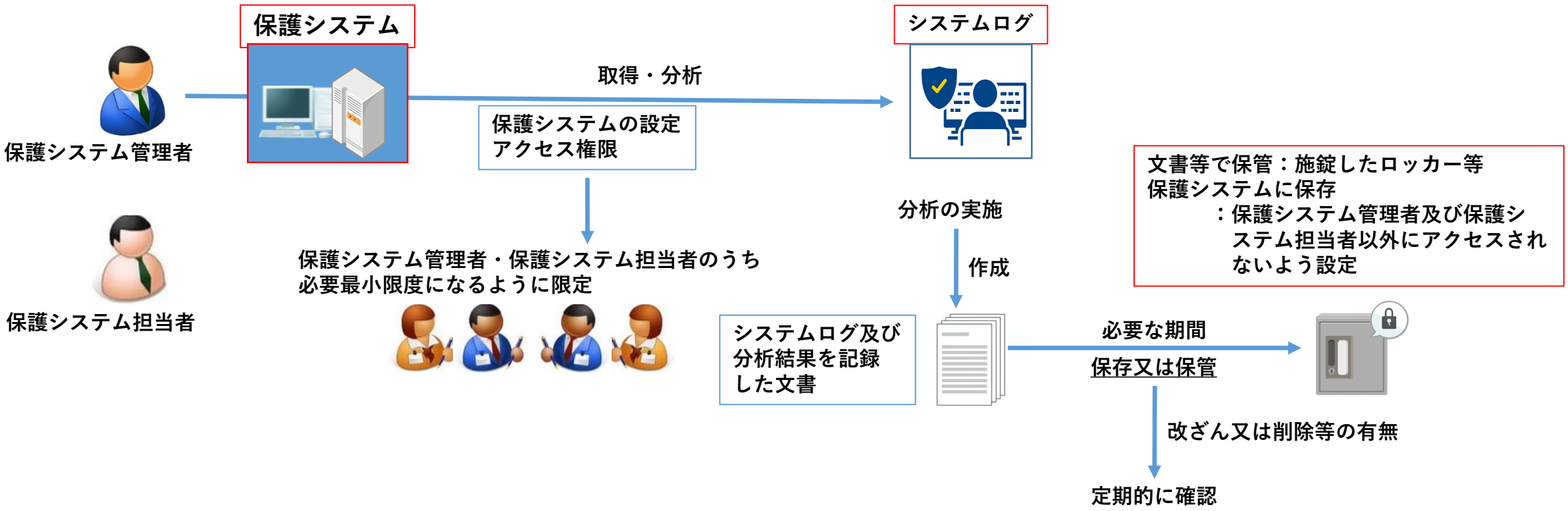


システムログの内容（時刻の順序を含む）を変更してはならない

２　システムログの管理

(1) 保護システム管理者は、システムログの取得及び分析に関わる保護システムの設定を行うために必要なアクセス権限を、必要な者に限定して付与するものとする。
(2) システムログ及びその分析の結果の記録は、文書等の場合は施錠したロッカー等により、電子データを保護システムに記録する場合は保護システム管理者及び保護システム担当者以外にアクセスされないよう設定することにより、必要な期間保存又は保管するものとする。
(3) 保護システム管理者は、前号の規定により保存又は保管しているシステムログは、定期的に改ざん又は削除等が行われていないか確認するものとする。

システムログの管理



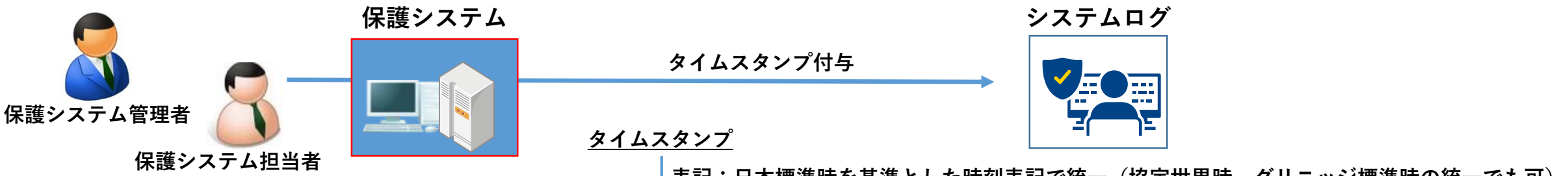
３　システムログに付与するタイムスタンプ

(1) 保護システム管理者は、システムログに対し、保護システムの内部におけるシステムクロックを使用して、タイムスタンプを付与するものとする。
(2) システムログのタイムスタンプは、日本標準時（ＪＳＴ）を基準とした時刻表記で統一するものとする。これにより難い場合には、協定世界時（ＵＴＣ）又はグリニッジ標準時（ＧＭＴ）を基準とした時刻表記で統一するものとする。
(3) タイムスタンプに使用するシステムクロックの同期は、保護システムに外部の権威ある機関が運営するＮＴＰサーバ等から得られる日付及び時刻と同期する機能を持たせるものとする。

４　システムログを取得するツールの保護

保護システム管理者は、システムログを取得するツールを不正なアクセス、改ざん又は削除から保護するものとする。

システムログに付与するタイムスタンプ



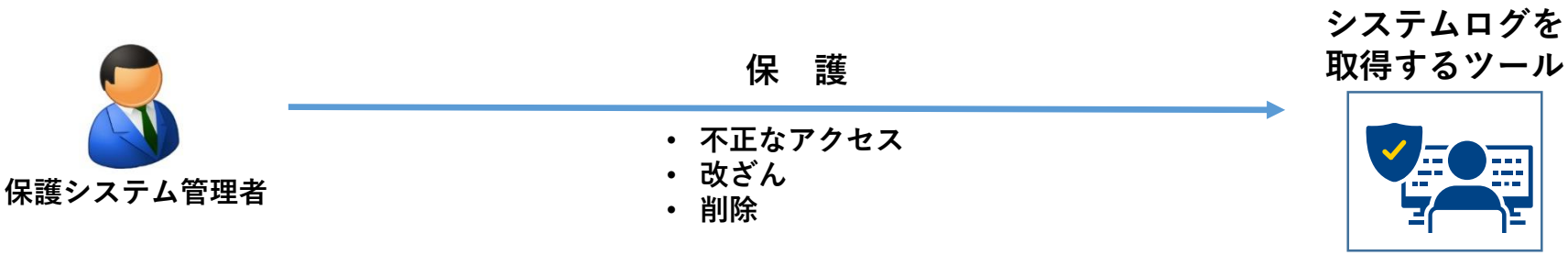
タイムスタンプ

表記：日本標準時を基準とした時刻表記で統一（協定世界時、グリニッジ標準時の統一でも可）

システムクロックの同期

保護システムに外部の権威ある機関が運営するNTPサーバから得られる日付及び時刻と同期する機能を付与。

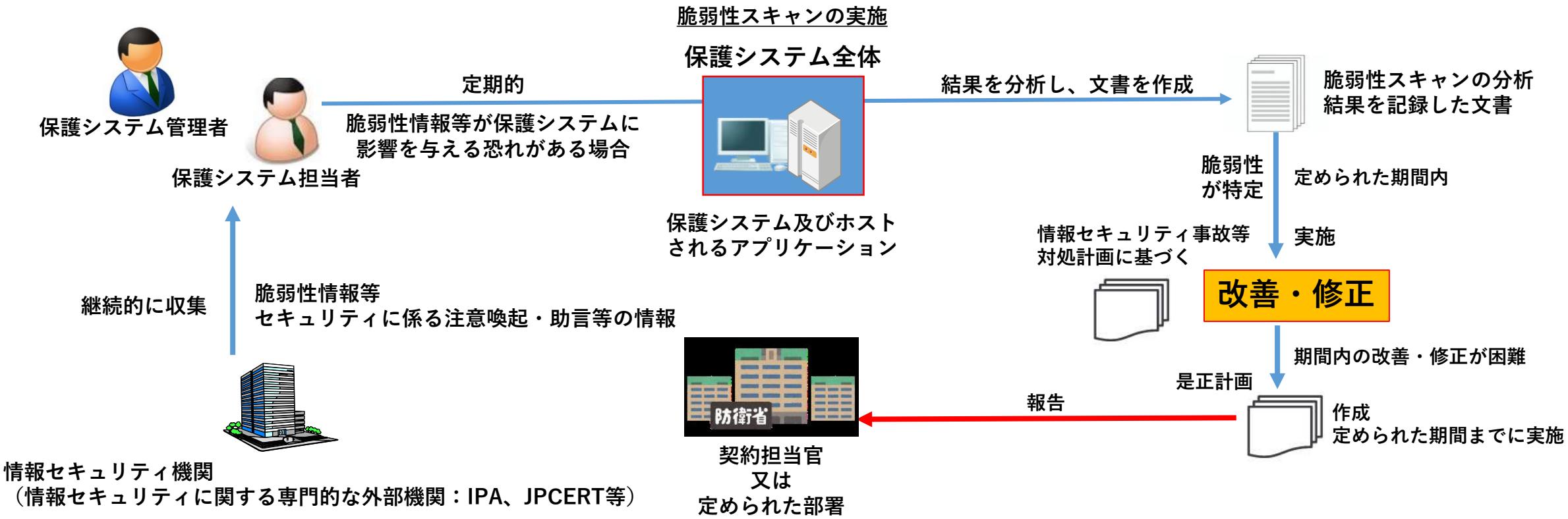
システムログを取得するツールの保護



第１０　脆弱性スキャン等

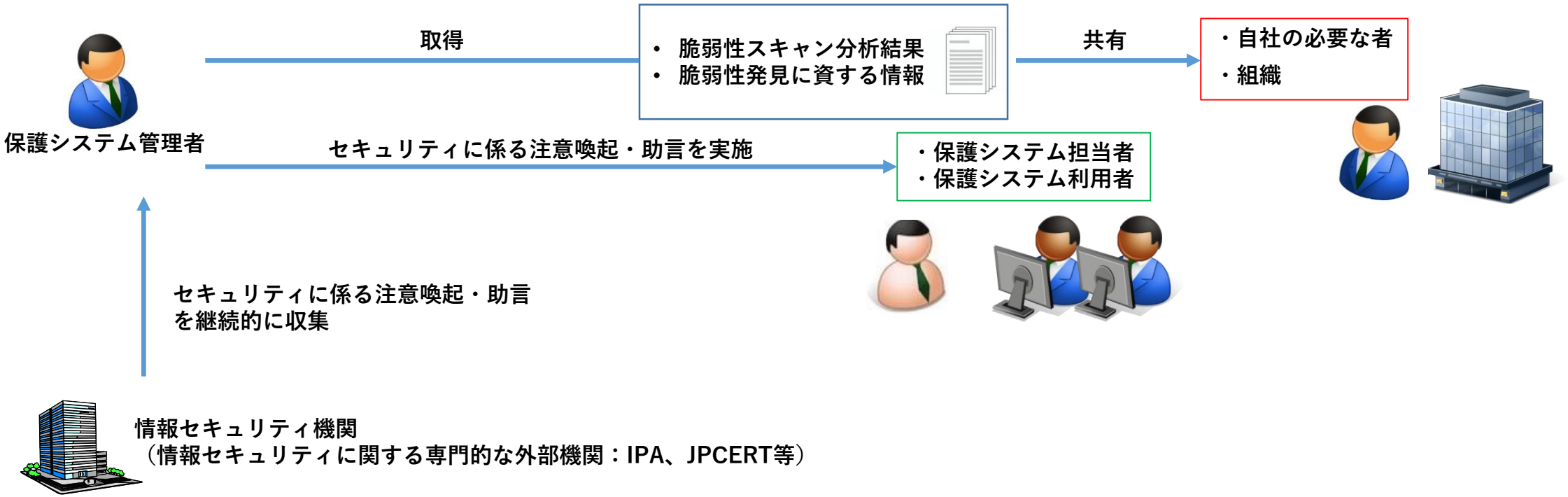
１　脆弱性スキャンの実施

(1) 保護システム管理者は、保護システム全体に対する脆弱性スキャンを定期的に行い、その結果を分析するものとする。
(2) 保護システム管理者は、社内からの脆弱性情報に加え、情報セキュリティに係る専門的な外部機関（以下「情報セキュリティ機関」という。）が発信する脆弱性情報等セキュリティに係る注意喚起及び助言等の情報を継続的に収集するものとし、当該脆弱性が保護システムに対し悪影響を与える可能性があると認められる場合に、保護システム全体に対し当該脆弱性に係る脆弱性スキャンを実施し、その結果を分析するものとする。
(3) 保護システム管理者は、前２号による分析の結果を記載した文書を作成するものとし、脆弱性が特定された場合は、本基準第１１第１項第４号及び第２項第１号の措置を行うものとする。



２　分析結果等の利用

(1) 保護システム管理者は、自社における保護システム以外の情報システムにおける脆弱性の発見及び修正等に資するため、脆弱性スキャン結果の分析など脆弱性の発見に資する情報を自社の必要な者及び組織に共有するものとする。
(2) 保護システム管理者は、社内又は前項第２号の情報セキュリティ機関から収集した情報に基づき、保護システム担当者及び保護システム利用者（保護システムを利用する 下請負者を含む。）等に対し、適切なセキュリティに係る注意喚起及び助言等を行うものとする。
(3) 保護システム管理者は、前２号により脆弱性が特定された場合は、定められた時間内に特定された脆弱性を修正するものとする。



第１１　バックアップ

1　保護システム管理者は、保護システムのサーバ及びパソコンに保存している全ての保護すべきデータ（防衛省が提供した保護すべきデータは除く。）及び保護システムにおけるシステムデータについて、定期的にバックアップを行うものとする。
2　前号の規定によりバックアップされたデータは、少なくとも次回のバックアップの完了まで保存するものとする。
3　バックアップは、自社が定めた保護システムの目標復旧時間に応じた頻度で行うものとする。
4　保護システム管理者は、第１項の規定によりバックアップされたデータの機密性、完全性及び可用性を保護するものとする。
5　保護システム管理者は、バックアップに関する手順を定めるものとする。

防衛関連企業

保護システム管理者

- サーバ、パソコン保存しているすべての保護すべきデータ
- 保護システムにおけるシステムレベルのデータ

定期的にバックアップ

バックアップデータ

定める

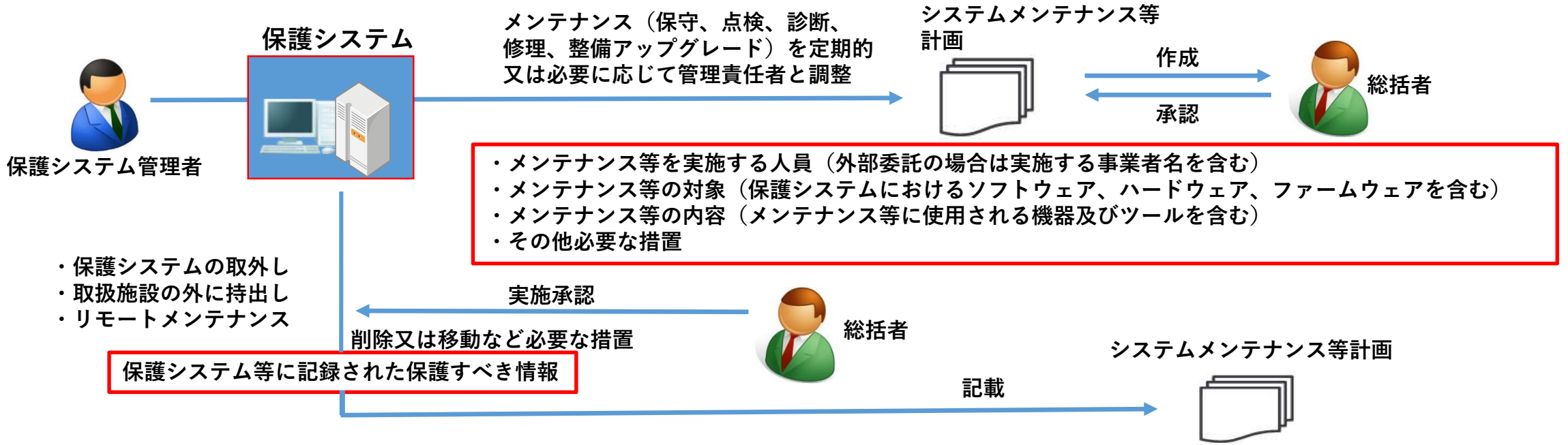
バックアップに
関する手順

・バックアップデータは次回のバックアップの完了まで保管
・バックアップされたデータに基づく保護システムの復旧に要する目標時間を定める
・バックアップにより複製されたデータの機密性、完全性、可用性を保護

第１２　システムメンテナンス等

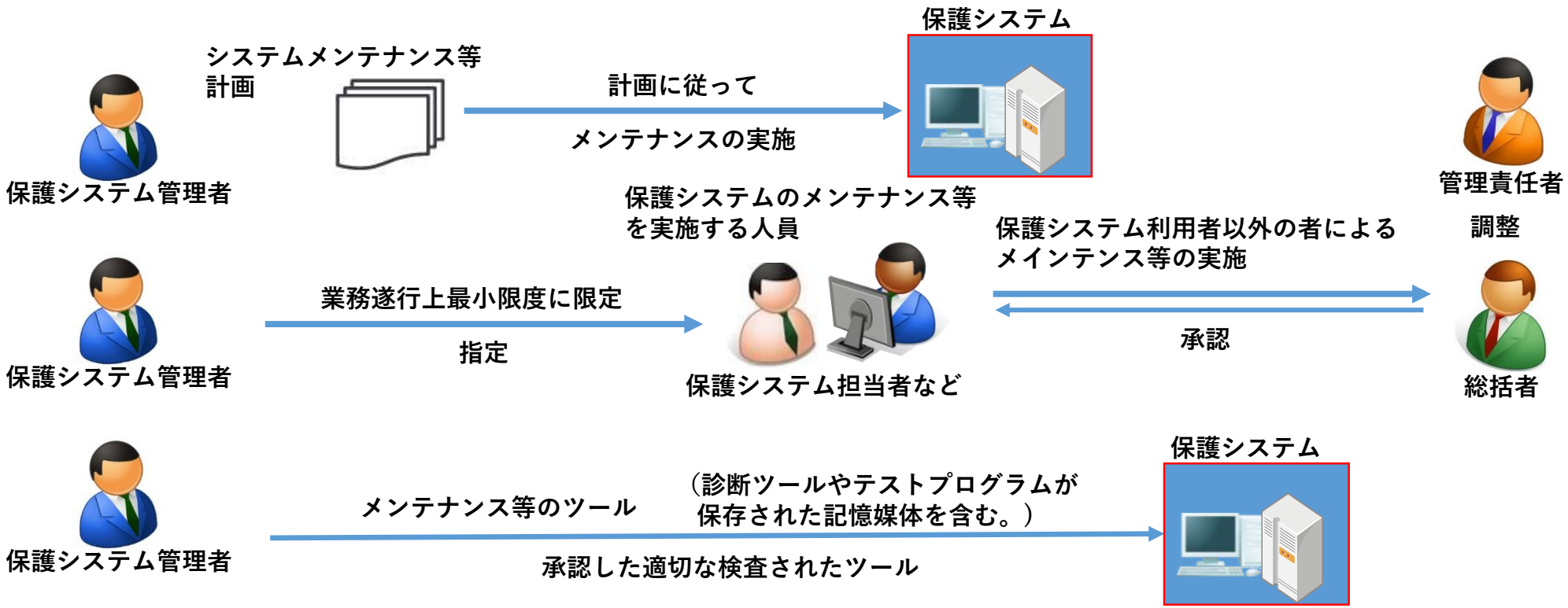
１　システムメンテナンス等の計画

(1) 保護システム管理者は、保護システムのメンテナンス等（保守、点検、診断、修理、整備及びアップグレードを含む。以下同じ。）を定期的に、及び必要な場合にはその都度行うものとする。
(2) 保護システム管理者は、次に掲げる事項を定めた計画（以下「システムメンテナンス等計画」という。）を管理責任者と調整の上作成し、総括者の承認を得るものとする。
ア　メンテナンス等を実施する人員
イ　メンテナンス等の対象（保護システムにおけるソフトウェア、ハードウェア及びファームウェアを含む。）
ウ　メンテナンス等の内容（メンテナンス等に使用される機器及びツールを含む。）
エ　アからウに掲げるほか、第２項及び第３項に規定する措置を実施するために必要な事項
(3) 保護システムを取り外す場合、取扱施設の外に持ち出す必要がある場合又は保護システム等に対しネットワークを経由したメンテナンス等（以下「リモートメンテナンス等」という。）を実施する必要がある場合は、保護システム管理者は、前号による承認を得るとともに、あらかじめ当該保護システム等に記録された保護すべき情報を削除又は移動させるなど必要な措置を講じ、システムテナンス等計画にその旨を記載するものとする。



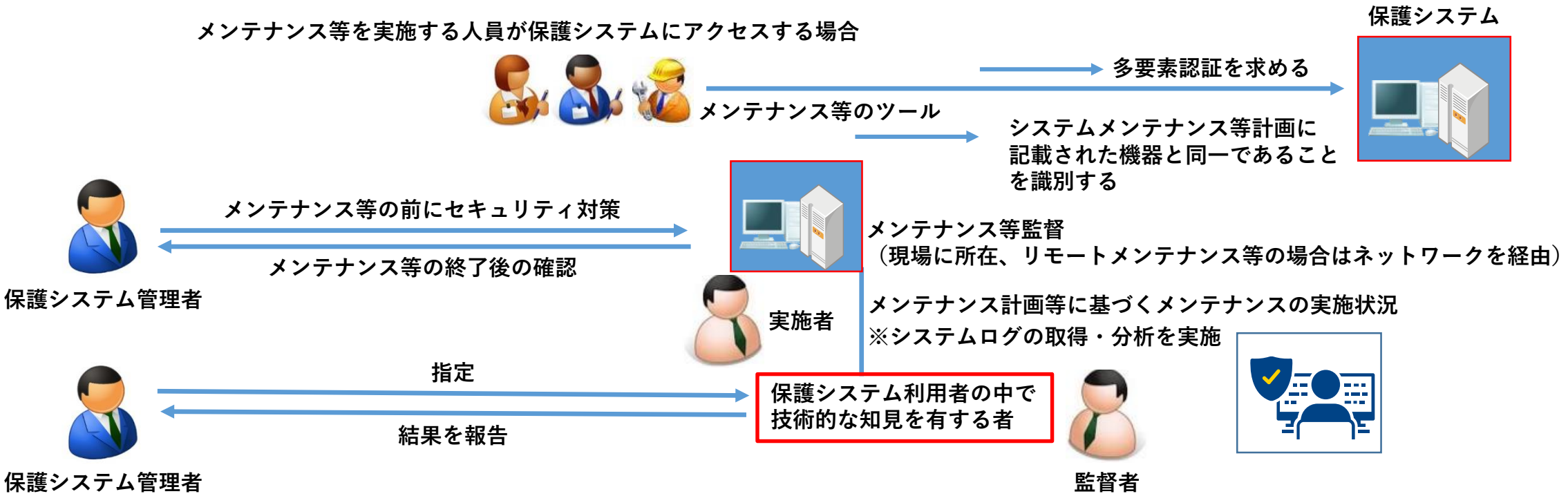
２　システムメンテナンス等の実施

保護システム管理者は、システムメンテナンス等計画に従って、保護システムのメンテナンス等を実施するものとする。
（1）　人員の指定
　ア 保護システム管理者は、保護システムのメンテナンス等を実施することができる人員を保護システム利用者のうちから業務の遂行上必要最小限度に制限したうえで、指定するものとする。
　イ 保護システム利用者以外の者によるメンテナンス等を実施する必要がある場合は、保護システム管理者が前項第２号による承認を得て実施させるものとし、メンテナンス等の完了後、直ちに当該人員による保護システム及び取扱施設へのアクセスを含むメンテナンス等への関与を終了させるものとする。
（2）ツールの検査
　保護システムのメンテナンス等の実施に当たっては、保護システム管理者が承認した適切な検査されたツール（診断ツールやテストプログラムが保存された記憶媒体を含む。）のみを使用させるものとする。



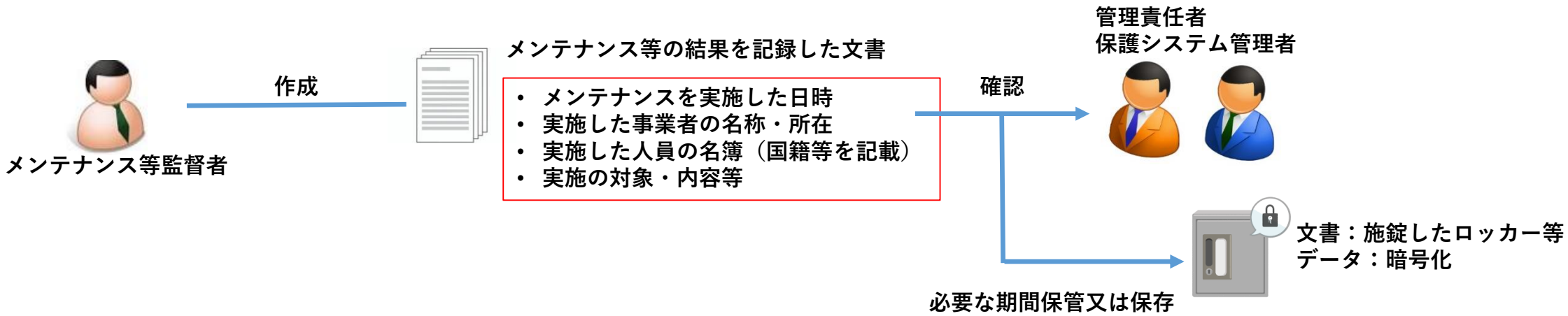
第１２　システムメンテナンス等

(3)　システムへのアクセスの認証等
　ア　保護システムのメンテナンス等を実施する人員が保護システムにアクセスする必要がある場合は、当該人員に対し多要素認証を求めるものとする。
　イ　保護システムのメンテナンス等に使用する機器は、システムメンテナンス等計画に記載された機器と同一であることを識別するものとする。
(4)　システムメンテナンス等の監督等
　ア　保護システムのメンテナンス等を実施する場合は、保護システム管理者は保護システム利用者の中から技術的な知見を有する者を監督者として指名し、監督結果を管理責任者及び保護システム管理者に速やかに報告させるものとする。
　イ　アにより指定された監督者は、保護システムのメンテナンス等を実施する者とともに現場に所在（リモートメンテナンス等の場合はネットワークを経由）して、メンテナンス等の実施状況を監督するものとする。
　ウ　システムメンテナンス等の実施状況の監督に当たっては、第９に規定するシステムログの取得及び分析を実施するものとする。
(5)　保護システム管理者は、保護システムのメンテナンス等を実施する前に、メンテナンス等により影響を受けることが予測される事象についてのセキュリティ対策を実施し、メンテナンス等の終了後、当該セキュリティ対策がメンテナンス等の実施前と同様に適切に機能していることを確認するものとする。



３　システムメンテナンス等の記録

(1) 前項第４号アにより指定された監督者は、メンテナンス等を実施した日時、事業者の名称及び所在、人員の名簿（国籍等を記載）、実施の対象及び内容等の記録を文書により作成し、管理責任者及び保護システム管理者の確認を得るものとする。
(2) 前号に規定するシステムメンテナンス等の結果を記録した文書を、文書により保存する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。



（付録）　用語の説明

#	名　称	説　明
1	**保護システム**	保護すべき情報の保存又は当該情報へのアクセスを可能とする機器。
2	**ベースライン構成設定**	保護システムとシステムコンポーネントの構成の把握並びに保護システムの更新及び変更時のベース(基準)となる構成設定。
3	**ブラックリスト**	保護システムにインストール又は保護システムで実行してはならないソフトウェアのリスト。
4	**ホワイトリスト**	保護システムにインストール及び保護システムで実行してもよいソフトウェアのリスト。
5	**構成設定**	情報システムを構成する構成要素（ハードウェア、ソフウェア、ネットワーク及び記憶媒体）の機種、バージョン等及び当該構成要素の機能並びに動作等を制御する設定値を決定すること。
6	**保護システム構成要素**	保護システムを構成するハードウェア、ソフトウェア、記憶媒体及びネットワークのこと。
7	**モバイルコード**	インターネット等のネットワークを通じて、自動的にダウンロード及び実行されるプログラム。
8	**VoIP技術**	インターネット回線経由で音声データを送受信する技術。
9	**アクセス制御方針**	保護すべきデータ及び保護システムに対する論理的なアクセス（保護システムへのログオン及び保護システムの個々の機能へのアクセスを含む。）の制御を実施するために必要な措置を定めた方針。
10	**保護システム管理者**	保護システム利用者のうち、保護システムの運用管理に責任を負う者。
11	**保護システム担当者**	保護システム利用者のうち、保護システム管理者の業務遂行を補佐する者。
12	**保護システム利用者**	経営者等が指定する保護システムを利用する者。
13	**保護システム管理業務従事者**	保護システム管理者及び担当者のこと。
14	**アカウント管理者**	保護システム担当者のうち、アカウントの設定、変更、削除等を行う者として保護システム管理者に指定された者。
15	**機密性**	認可されていないものに対して、情報を使用不可又は非公開にする特性。

16	**完全性**	情報の正確さ及び完全さを保護する特性。
17	**可用性**	認可されたものが要求したときに、アクセス及び使用が可能である特性。
18	**可搬記憶媒体**	パソコン又はその周辺機器に挿入又は接続して情報を保存することができる媒体又は機器のうち可搬型のもの。
19	**電子政府推奨暗号等**	電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合に電子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段。
20	**アンチウィルスシグネチャ**	アンチウィルスソフトがウィルス検出の際に使用する、ウィルスに特徴的なデータ断片や攻撃者の通信パターン等。
21	**仮想化技術**	ハードウェアの機能をソフトウェアで（論理的に）実現する技術。
22	**識別子**	アカウントの場合はユーザーID、保護システムを構成する機器の場合はホスト名のこと。
23	**認証子**	パスワードのこと。
24	**ユーザーセッション**	ユーザーが保護システムにログインしてからログアウトするまでのセッションのこと。
25	**多要素認証**	本人だけが知る要素（「知識要素」）、本人だけが所有する要素（「所持要素」）及び本人の持つ生体的要素（「生体要素」）のうち複数の異なる要素を保持すると認められた者のみを許可するもの。
26	**リモートアクセス**	システム利用者が外部ネットワークを通じて内部の情報システムにアクセスすること。
27	**リモート接続**	システム利用者が外部ネットワークを介して情報をやりとりするデバイスと接続すること。
28	**プロキシサーバ**	内部ネットワークからインターネット接続を行う際、高速なアクセスや安全な通信を確保するための中継的な役割を行うサーバ。
29	**バーチャル・プライベート・ネットワーク（VPN）**	一般的なインターネット回線を利用してつくられる、仮想的な専用線（仮想的なネットワーク）のこと。
30	**リプレイ攻撃**	保護システム利用者の確認に用いられる認識データをそのまま用いて利用者になりすます方式。

31	**トークン**	一定期間毎にパスワード（ワンタイムパスワード）を生成する機器。
32	**ゲートウェイ**	プロトコルが異なるネットワーク同士が通信を行う際に、中継する役割を持つ機器やそれに関するソフトウェアのこと。
33	**通信セッション**	マシン同士の接続の際等の、通信開始から終了までの一連の通信のこと。
34	**悪意のあるコード**	情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウイルス及びスパイウェア等。
35	**システムログ**	情報システムにおける動作履歴に関する記録。
36	**通信トラフィック**	端末やネットワーク機器等を繋いでいる回線でやり取りされるデータのこと。
37	**検知ソフトウェア**	保護システムを構成するサーバ及びパソコンにおける悪意のあるコードを検知するためのソフトウェア。
38	**パターンマッチング手法**	あらかじめ過去のウィルスに特徴的なデータ断片のデータベースを用意し、検査対象と比較してウィルスを検出する手法。
39	**ヒューリスティックエンジン**	既知のウィルスの動作等を解析して、ウィルス感染動作やデータ破壊等、ウィルスに特徴的な処理パターンを解析して検出する技術。
40	**タイムスタンプ**	システムログファイル等にシステムの動作履歴と共に当該動作が起こった日付、日時、時間を保存すること。
41	**NTPサーバ**	正確な時刻情報をサーバやクライアント等に配信し、機器間の時刻を同期させるサーバ。
42	**脆弱性**	アプリケーション、OS、ソフトウェア、ネットワーク等で意図しない動作に繋がる可能性のあるセキュリティ上の弱点。
43	**監督者**	保護システム利用者の中から保護システム管理者によって指定された者で、保護システムのメンテナンス等を実施する場合に、その現場に所在してメンテナンス等を監督する者のこと。
44	**管理責任者**	取扱施設等の物理的セキュリティに責任を有する者で管理者の中から総括者が指定した者をいう。