システム要件定義成果物サンプル＆ガイド
DS-308 ： セキュリティ要件定義

第1.10版

2018年08月29日

１．概要

構築する情報システムに応じて検討すべきセキュリティに関する非機能要求を明らかにし、抜け漏れがないように検討する。
対象システムのセキュリティに関する「前提条件・制約条件」、開発時や運用時のセキュリティ管理に関する項目である「セキュリティリスク分析」、「セキュリティ診断」、セキュリティ対策の実機能である「アクセス・利用制限」、「データの秘匿」、「不正追跡・監視」、機能の組合せによるセキュリティ対策の主要なパターンとなる「ネットワーウェア対策」、「Web 対策」等の内容を設定する。
セキュリティ対策を実施するために、以下の手順で順次要件を定義する。

1 セキュリティに関わる前提条件、制約条件を洗い出し、準拠する内容を確認する。多くの場合は現行システムが準拠しているセキュリテイ対策に準ずることになる。
2 セキュリティ管理として、セキュリティリスクを分析するために、情報資産を洗い出し、利用者および脅威を特定した上で、各情報資産に対するセキュリティ対策を定義する。
セキュリティ対策は万全でなく、対策の結果を確認するため、また変化する状況への対応としてセキュリティ診断の受診を検討する。
3 セキュリティ機能として、各情報資産に対する認証と利用制限によってカバーする範囲を明確にする。それでもなお高度に秘匿すべき情報資産が存在する場合やインターネットを利用するなどセキュリティリスクが高い環境においては、暗号化を検討する。
また認証機能、利用制限機能が正常に機能しているかを確認するために、必要に応じて不正監視を行う。
4 インターネットからの攻撃、マルウェアによる不正利用等のシステムの脆弱性、不備を突く脅威に対するセキュリティ対策として、ネットワーク対策、マルウェア対策、Web対策の実施と実施内容を定義する。

２．使途

- お客様と以下を合意する。
  - セキュリティに関わる前提条件、制約条件が漏れなく洗い出されていること。
  - 対象となる情報資産が漏れなく洗い出されていること。
  - 現行システムが準拠しているセキュリティ対策と矛盾がないこと。
  - セキュリティリスク対策が回避、軽減、転嫁、受容いずれであってもそれが情報資産の価値、脅威と照らして妥当であること。
- 情報資産とセキュリティリスク対策の観点から、実現する必要がある事項について指標を設定し、方式設計のインプットとする。

３．記入要領

No	記述内容 (SX-XX-XXは、関連するプロセスIDを指す。)		記述内容説明	補足
1	1.1情報セキュリティに関するコンプライアンス S3-09-01	分類	セキュリティ対策の前提条件、制約条件となるドキュメントには様々なものがある。組織規程やガイドライン、法令等の分類を記述する。	
		名称	対象となるドキュメントの名称を記述する。	
		版	対象となるドキュメントの版を示す情報を記述する。	
		発行者	対象となるドキュメントの発行者を記述する。	
2	2.1.セキュリティリスク分析 1).情報資産 S3-09-02	資産分類	セキュリティリスク分析をするために情報資産を洗い出す。情報資産には情報・データ、ネットワーク、施設・設備、ハードウェア資産、ソフトウェア資産等がある。これらの分類を記述する。	※規約等で取引が終了したデータの完全削除が必要な場合がある。
		資産名称	対象となる情報資産の名称を記述する。記述粒度はシステム規模等による。	
		情報名称	情報・データに関する情報資産の場合は、エンティティのレベルの名称を記述する。	
		利用者	当該情報を操作もしくは参照する利用者を列挙する。	
		脅威	情報資産に対して想定される脅威について列挙する。	
		セキュリティ対策	情報資産の脅威に対するセキュリティ対策を選択する。	
	2.2.セキュリティ診断 1)ネットワーク診断 2)Web診断 3)DB診断 S3-09-03	対象情報資産	診断対象のネットワークまたはシステムの名称を記述する。	
		利用者	対象となるネットワーク/システムの利用者を記述する。 利用者を記述するのは、直接的な侵入、攻撃の経路となるためである。	
		脅威	対象となるネットワーク/システムの脅威および次項の対策を記述する。 セキュリティ診断の受診の判断材料とする。	
		対策	同上	
		診断実施	セキュリティ診断の実施の有無を記述する。 セキュリティ診断は高価なサービスである場合が多く、必要性とコストに応じて実施を検討する。	
		診断実施内容	脅威、リスクに応じた各セキュリティ診断の実施内容を記述する。	
		診断実施時期	セキュリティ診断の実施時期を記述する。	
		頻度	状況の変化等に応じる速度を鑑みてセキュリティ診断の実施頻度を記述する。	

[IPA/SEC『非機能要求グレード：システム基盤の非機能要求に関する項目一覧』[5]を参考に作成]

No	記述内容 (SX-XX-XXは、関連するプロセスIDを指す。)		記述内容説明	補足
3	3.1.認証機能 S3-09-04	対象情報資産	認証機能を施す情報資産について記述する。	
		利用者	対象となる情報資産の利用者を記述する。	
		権限	利用者に与えられた権限を記述する。	
		脅威	情報資産に対する脅威を記述する。	
		対策	脅威の対策となる認証機能を記述する。 秘匿すべき情報の重要度に応じて、強固なレベルの対策を検討する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	
	3.2.利用制限 S3-09-05	対象情報資産	利用制限を施す情報資産について記述する。	
		利用者	対象となる情報資産の利用者を記述する。	
		権限	利用者に与えられた権限を記述する。	
		脅威	情報資産に対する脅威を記述する。	
		対策	脅威の対策となる利用制限範囲を記述する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	
	3.3.データ暗号化 1)伝送データの暗号化 S3-09-06	対象情報資産	伝送データの送受信区間を記述する。	
		利用者	ネットワークの利用者を記述する。	
		脅威	各ネットワークの区間における脅威を記述する。	
		暗号化	暗号化対策の実施有無を記述する。	
		暗号化方式	選定する暗号化方式の内容を記述する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	

[IPA/SEC『非機能要求グレード：システム基盤の非機能要求に関する項目一覧』[5]を参考に作成]

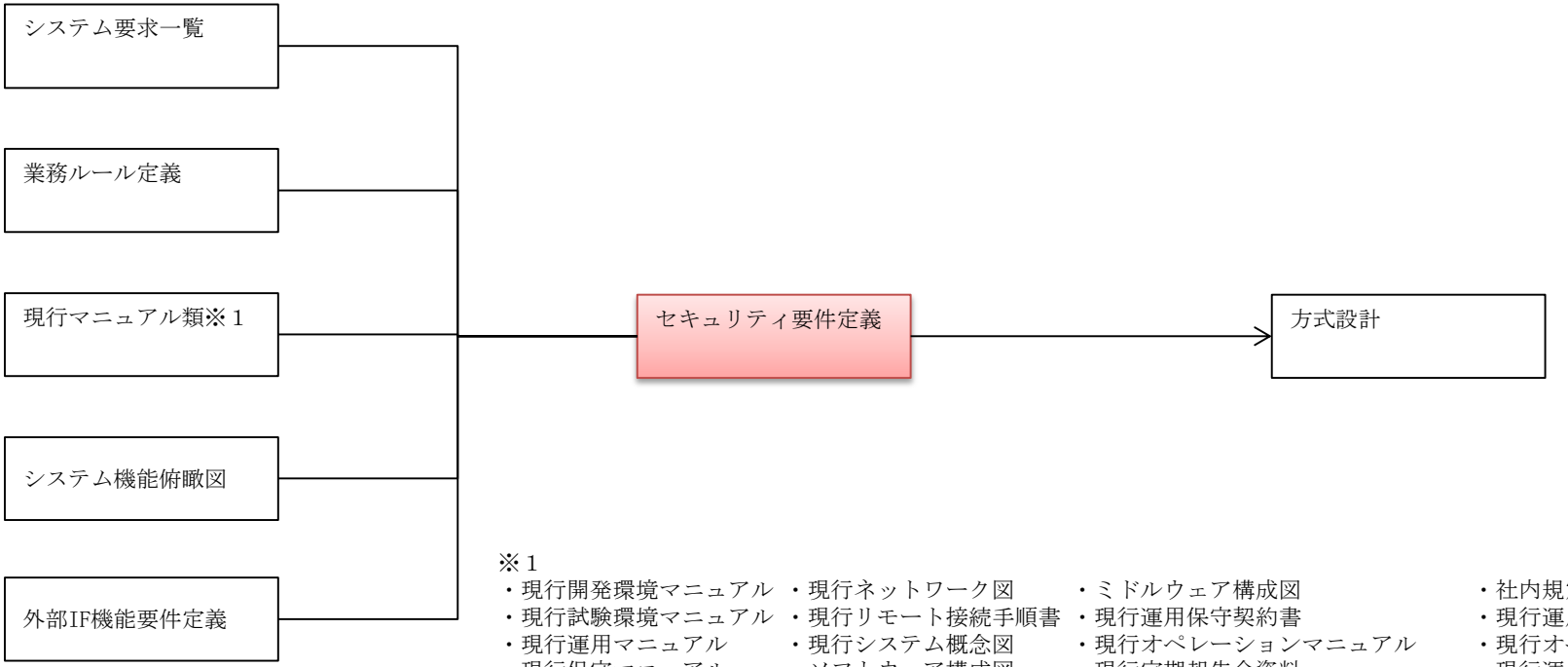
No	記述内容 (SX-XX-XXは、関連するプロセスIDを指す。)		記述内容説明	補足
3	3.3.データ暗号化 2)蓄積データの暗号化 S3-09-06	対象情報資産	蓄積データを暗号化する情報資産について記述する。	
		情報名称	同上	
		脅威	情報資産に対する脅威を記述する。	
		暗号化	暗号化する際は、その対象を記述する。 コンピュータリソースに関わるコストに留意する必要がある。	
		暗号化方式	暗号化方式の内容を記述する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	
	3.3.データ暗号化 3)鍵管理 S3-09-06	対象情報資産	暗号化を実施する箇所を記述する。	
		鍵種類	管理する鍵の種類を記述する。	
		保管場所	鍵を保管する場所を記述する。	
		バックアップ	保管した鍵の二次保管場所を記述する。 盗難に留意した場所を検討する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	
	3.4.不正監視 S3-09-07	対象情報資産	不正監視を実施する対象となる情報資産を記述する。	
		ログの取得	ログの取得の有無を記述する。	
		ログの保管期間	ログの保管期間のを記述する。	
		不正監視対象	不正監視対象となるログを記述する。	
		ログチェック頻度	不正監視として実施するログのチェック頻度を記述する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	

[IPA/SEC『非機能要求グレード：システム基盤の非機能要求に関する項目一覧』[5]を参考に作成]

No	記述内容 (SX-XX-XXは、関連するプロセスIDを指す。)		記述内容説明	補足
4	4.1.ネットワーク対策 S3-09-08	対象情報資産	ネットワーク対策の実施検討対象となる区間について記述する。	
		利用者	対象ネットワークの利用者について記述する。	
		ネットワーク制御	実施するネットワーク制御の内容について記述する。	
		不正検知	ネットワーク対策として実施する不正検知方法について記述する。	
		サービス停止攻撃の回避	サービス停止攻撃の回避を実施する箇所、方法について記述する。 専用設備を要する場合が多く、設備集約を含めて検討する必要がある。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	
	4.2.マルウェア対策 S3-09-09	対象情報資産	マルウェア対策を実施する情報資産を記述する。	
		リアルタイムスキャンの実施	リアルタイムスキャンの実施有無を記述する。 実施する場合には、運用体制、運用プロセスを定義しておき円滑な業務運営とする必要がある。	
		フルスキャンの定期実施タイミング	フルスキャンの定期実施タイミングについて記述する。 特にストレージに対する負荷が発生するため、実施頻度だけでなく実施時間も考慮すると良い。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	
	4.3.Web対策 S3-09-10	対象情報資産	Web対策を実施する情報資産を記述する。	
		セキュアコーディング	セキュアコーディングを実施する対象部分について記述する。 開発コストに影響するため、求められるセキュリティレベルに応じて定義する必要がある。	
		脆弱性検査	新たな脆弱性が発見される可能性がある。 脆弱性情報のチェックする運用だけでなく脆弱性検査を実施する頻度について記述する。	
		Webサーバ設定等による対策	Webサーバ設定等によって利用制限等の対策が実施でき、この活用を検討する。	
		WAFの導入	WAFの導入によって高いリスクから強固に守る必要性について記述する。	
		残存リスク対策	本対策でカバーできないセキュリティリスク対策について記述する。	

[IPA/SEC『非機能要求グレード：システム基盤の非機能要求に関する項目一覧』[5]を参考に作成]

４．他成果物との関係



※１

・現行開発環境マニュアル	・現行ネットワーク図	・ミドルウェア構成図	・社内規定
・現行試験環境マニュアル	・現行リモート接続手順書	・現行運用保守契約書	・現行運用マニュアル
・現行運用マニュアル	・現行システム概念図	・現行オペレーションマニュアル	・現行オペレーションマニュアル
・現行保守マニュアル	・ソフトウェア構成図	・現行定期報告会資料	・現行運用保守契約書

５．表記例

１．セキュリティに関する前提条件・制約条件

１．１．　情報セキュリティに関するコンプライアンス

分類	名称	版	発行者
法令・法規等	個人情報保護法 プライバシーマーク ・・・		
ガイドライン	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン ・・・		
社内規定	個人情報保護規定 情報セキュリティ管理規定 サーバシステム管理規則 パソコン等利用規則 コンピュータウィルス対策規則 ・・・		

２．セキュリティ管理

２．１．　セキュリティリスク分析

１）情報資産

資産分類	資産名称	情報名称	利用者	脅威	3.1.認証機能	3.2.利用制限	3.3.データ暗号化	3.4.不正監視	4.1.ネットワーク対策	4.2.マルウェア対策	4.3.Web対策	備考
情報、データ	販売管理システム	商品マスター	販売管理システム	改ざん、漏洩	○	○						
		受注情報	個人顧客、営業担当、コールセンター	改ざん、漏洩	○	○						
		出荷情報	経理担当、営業担当	改ざん、漏洩	○	○						
		請求情報	経理担当、営業担当	改ざん、漏洩	○	○						
	顧客管理システム	個人顧客	個人顧客、営業担当、コールセンター	改ざん、漏洩	○	○	○					
		法人顧客	営業担当	改ざん、漏洩	○	○						
		アカウント	システム担当	改ざん、漏洩	○	○						
	システム共通	システムデータ	システム担当	システムの停止、不正利用	○	○						
		ログデータ	システム担当	改ざん	○	○						
	・・・	・・・	・・・	・・・								
ネットワーク	拠点LAN		社員	侵入、盗聴								
	拠点間WAN		社員	侵入、盗聴								
	対外接続		システム	侵入、盗聴			○		○			
	インターネット		個人顧客	侵入、盗聴、攻撃			○		○			
	DC内DMZ		システム	侵入、盗聴					○			
	DC内内部ネットワーク		システム	侵入、盗聴					○			
	・・・	・・・	・・・	・・・								
施設、設備	データセンター		システム担当	侵入、盗難	○							
	執務室		社員	侵入、盗難	○							
	・・・	・・・	・・・	・・・								
ハードウェア資産	Webサーバ		システム担当	不正利用、脆弱性をつく攻撃	○	○		○		○		
	アプリケーションサーバ		システム担当	不正利用、脆弱性をつく攻撃	○	○		○		○		
	データベースサーバ		システム担当	不正利用、脆弱性をつく攻撃	○	○		○		○		
	クライアントPC		社員	不正利用、脆弱性をつく攻撃	○	○		○		○		
	・・・	・・・	・・・	・・・								
ソフトウェア資産	販売管理システム		システム担当	不正利用、脆弱性をつく攻撃	○	○		○			○	
	顧客管理システム		システム担当	不正利用、脆弱性をつく攻撃	○	○		○			○	
	・・・	・・・	・・・	・・・								

２．２．　セキュリティ診断

１）　ネットワーク診断

対象情報資産	利用者	脅威	対策	診断実施	診断実施内容	診断実施時期	頻度
拠点LAN	社員	クライアントのマルウェア感染	ウィルス対策ソフトの導入	なし			
		不正利用	認証機能による利用制限	なし			
	・・・	・・・	・・・				
拠点間WAN	社員	クライアントのマルウェア感染	ウィルス対策ソフトの導入	なし			
	・・・	・・・	・・・				
DC内DMZ	Webシステム	外部からの侵入、攻撃	ファイアウォールによる監視、制限	あり	侵入テスト	初期、定期	年1回
	システム管理者	不正利用	認証機能による利用制限	なし			
DC内内部ネットワーク	システム	マルウェア感染	ウィルス対策ソフトの導入	なし			
		不正利用	認証機能による利用制限	なし			
	システム管理者	不正利用	認証機能による利用制限	なし			
・・・	・・・	・・・	・・・	・・・			

２）　Web診断

対象情報資産	利用者	脅威	対策	診断実施	診断実施内容	診断実施時期	頻度
顧客管理システム	個人顧客	外部からの侵入、攻撃	ネットワーク対策、Web対策	あり	脆弱性検査	初期、定期	年1回
	社員	内部からの侵入、攻撃	なし	なし			
販売管理システム	個人顧客	外部からの侵入、攻撃	ネットワーク対策、Web対策	あり	脆弱性検査	初期、定期	年1回
	社員	内部からの侵入、攻撃	なし	なし			
・・・	・・・	・・・	・・・	・・・			

３）　DB診断

対象情報資産	利用者	脅威	対策	診断実施	診断実施内容	診断実施時期	頻度
顧客管理システム	システム	システムの不正利用	不正利用監視	なし			
	システム管理者	システムの不正利用	不正利用監視	なし			
販売管理システム	システム	システムの不正利用	不正利用監視	なし			
	・・・	・・・	・・・	・・・			

３．セキュリティ機能

３．１．　認証機能

対象情報資産	利用者	権限	脅威	対策	残存リスク対策
顧客管理システム	個人顧客	利用者	改ざん、漏洩、不正利用	ID、パスワード認証	利用制限
	社員	登録、変更、削除	改ざん、漏洩、不正利用	ID、パスワード認証	利用制限
	業務管理担当	マスター登録、データ管理	改ざん、漏洩、不正利用	ID、パスワード認証	利用制限
	・・・	・・・	・・・	・・・	・・・
販売管理システム	個人顧客	利用者	改ざん、漏洩、不正利用	ID、パスワード認証	利用制限
	社員	登録	改ざん、漏洩、不正利用	ID、パスワード認証	利用制限
	業務管理担当	マスター登録、データ保全	改ざん、漏洩、不正利用	ID、パスワード認証	利用制限
	・・・	・・・	・・・	・・・	・・・
クライアントPC	社員	登録、変更、削除	不正利用	ID、パスワード認証	利用制限
Webサーバ	システム担当	システム管理	不正利用	複数回の認証	利用制限
アプリケーションサーバ	システム担当	システム管理	不正利用	複数回の認証	利用制限
データベースサーバ	システム担当	システム管理	不正利用	複数回の認証	利用制限
バッチサーバ	システム担当	システム管理	不正利用	複数回の認証	利用制限
	・・・	・・・	・・・	・・・	・・・
データセンター	システム担当	システム管理	侵入、盗難	IDカード認証	入退館記録、ビデオ
執務室	社員	業務全般	侵入、盗難	IDカード認証	利用制限
・・・	・・・	・・・	・・・	・・・	・・・

３．２．　利用制限

対象情報資産	利用者	権限	脅威	対策	残存リスク対策
顧客管理システム	個人顧客	利用者	改ざん、漏洩、不正利用	利用者機能	不正監視
	社員	登録、変更、削除	改ざん、漏洩、不正利用	必要最小限の機能の利用	不正監視
	業務管理担当	マスター登録、データ管理	改ざん、漏洩、不正利用	必要最小限の機能の利用	不正監視
	・・・	・・・	・・・	・・・	・・・
販売管理システム	個人顧客	利用者	改ざん、漏洩、不正利用	利用者機能	不正監視
	社員	登録、変更、削除	改ざん、漏洩、不正利用	必要最小限の機能の利用	不正監視
	業務管理担当	マスター登録、データ保全	改ざん、漏洩、不正利用	必要最小限の機能の利用	不正監視
	・・・	・・・	・・・	・・・	・・・
クライアントPC	社員	登録、変更、削除	改ざん、漏洩、不正利用	業務以外の利用の制限	なし
Webサーバ	システム担当	システム管理	改ざん、漏洩、不正利用	システム管理用端末からの利用	不正監視
アプリケーションサーバ	システム担当	システム管理	改ざん、漏洩、不正利用	システム管理用端末からの利用	不正監視
データベースサーバ	システム担当	システム管理	改ざん、漏洩、不正利用	システム管理用端末からの利用	不正監視
バッチサーバ	システム担当	システム管理	改ざん、漏洩、不正利用	システム管理用端末からの利用	不正監視
・・・	・・・	・・・	・・・	・・・	・・・

３．３．　データ暗号化

１）伝送データの暗号化

対象情報資産	利用者	脅威	暗号化	暗号化方式	残存リスク対策
個人顧客～Webサーバ間	個人顧客	盗聴	あり	SSL/TLSによる暗号化	Web対策、鍵管理
社員～Webサーバ間	社員	盗聴	なし		なし
サーバ間通信	システム	盗聴	なし		なし
対外接続I/F通信	システム	盗聴	あり	SSL/TLSによる暗号化	Web対策、鍵管理
・・・	・・・	・・・	・・・	・・・	・・・

２）蓄積データの暗号化

対象情報資産	情報名称	脅威	暗号化	暗号化方式	残存リスク対策
販売管理システム	商品マスター	改ざん、漏洩	なし		データのバックアップ
	受注情報	改ざん、漏洩	なし		データのバックアップ
	出荷情報	改ざん、漏洩	なし		データのバックアップ
	請求情報	改ざん、漏洩	なし		データのバックアップ
顧客管理システム	個人顧客	改ざん、漏洩	個人情報を暗号化	データベース機能による暗号化	データのバックアップ
	法人顧客	改ざん、漏洩	なし		データのバックアップ
	アカウント	改ざん、漏洩	なし		データのバックアップ
システム	システムデータ	改ざん、漏洩	なし		データのバックアップ
	ログデータ	改ざん、漏洩	なし		データのバックアップ
・・・	・・・	・・・	・・・	・・・	・・・

３）鍵管理

対象情報資産	鍵種類	保管場所	バックアップ	残存リスク対策
個人顧客～Webサーバ間	PKI秘密鍵	サーバ上に暗号化して保管	キーペアを記憶媒体に複写し金庫保管	なし
対外接続	PKI秘密鍵	サーバ上に暗号化して保管	キーペアを記憶媒体に複写し金庫保管	なし
・・・	・・・	・・・	・・・	・・・

３．４．　不正監視

対象情報資産	ログの取得	ログの保管期間	不正監視対象	ログチェック頻度	残存リスク対策
クライアントPC	あり	1週間	なし		なし
Webサーバ	あり	2年	システムログ、操作ログ	5分以内に1回	ログのバックアップ
アプリケーションサーバ	あり	2年	システムログ、操作ログ	5分以内に1回	ログのバックアップ
データベースサーバ	あり	2年	システムログ、操作ログ	5分以内に1回	ログのバックアップ
バッチサーバ	あり	2年	システムログ、操作ログ	5分以内に1回	ログのバックアップ
・・・	・・・	・・・	・・・	・・・	・・・
顧客管理システム	あり	2年	システムログ、操作ログ	5分以内に1回	ログのバックアップ
販売管理システム	あり	2年	システムログ、操作ログ	5分以内に1回	ログのバックアップ
・・・	・・・	・・・	・・・	・・・	・・・

４．セキュリティ対策

４．１．　ネットワーク対策

対象情報資産	利用者	ネットワーク制御	不正検知	サービス停止攻撃の回避	残存リスク対策
拠点LAN	社員、システム	なし	なし	なし	異常トラフィック監視
拠点間WAN	社員、システム	既定の通信のみ許可	既定の通信以外を監視	なし	異常トラフィック監視
DC内公開セグメント	不特定多数	Web、メールのみ許可	WAFにて検知	ファイアウォールにて遮断	ネットワーク診断
DC内DMZ	システム	既定の通信のみ許可	既定の通信以外を監視	なし	ネットワーク診断
DC内内部セグメント	システム	既定の通信のみ許可	既定の通信以外を監視	なし	ネットワーク診断
・・・	・・・	・・・	・・・	・・・	・・・

４．２．　マルウェア対策

対象情報資産	リアルタイムスキャンの実施	フルスキャンの定期実施タイミング	残存リスク対策
クライアントPC	あり	週1回	なし
Webサーバ	あり	週1回	Web診断
メールサーバ	あり	週1回	なし
アプリケーションサーバ	あり	週1回	Web診断
データベースサーバ	あり	週1回	DB診断
対外接続サーバ	あり	週1回	なし
バッチサーバ	あり	週1回	なし
・・・	・・・	・・・	・・・

４．３．　Web対策

対象情報資産	セキュアコーディング	脆弱性検査	Webサーバ設定等による対策	WAFの導入	残存リスク対策
販売管理システム	インターネット受付部分	年1回	あり	あり	Web診断
顧客管理システム	インターネット受付部分	年1回	あり	あり	Web診断
・・・	・・・	・・・	・・・	・・・	・・・