サイバー攻撃（標的型攻撃）対策
防御モデルの解説

付録3 暫定対処策一覧

付録3 暫定対処策一覧

検知観点			影響範囲	ユーザ					EP												セグメント										サービス	
			暫定対処策	注意喚起	PW変更	権限変更	無効化	削除	注意喚起	検知感度向上	マルウェア隔離	マルウェア駆除	DNS応答拒否	ポート番号遮断	プロトコル遮断	IPアドレス遮断	所属NWの変更	EPをIP遮断	EPをMAC遮断	抜線	電源断（証拠保全量が減る）	注意喚起	検知感度向上	ドメイン・URL遮断	DNS(ブラックホスト名)不在応答	DNS(ブラックドメイン名)不在応答	ポート番号遮断	プロトコル遮断	IPアドレス遮断	SRC/DSTセグメント間通信遮断	接続NWの変更	NWごと抜線	サービス一部停止	サービス全停止
			CIA影響 機密性	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
			CIA影響 完全性	○	○	○	○	○	○	○	○	△	○	△	△	△	△	△	△	△	○	○	○	○	○	△	△	△	△	△	△	○	○
			CIA影響 可用性	○	○	△	×	×	○	○	△	△	△	△	△	△	×	×	×	×	○	○	○	△	△	△	△	△	△	×	×	△	×
照合分析	既知の標的型攻撃事象との一致	URLブラックリスト		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	プロキシサーバ	DNSサーバ	DNSサーバ	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		攻撃コード/ファイルシグネチャ		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		LAN内でのPsExec利用		該当ユーザ	ドメインコントローラー	－	－	－	該当EP	検知感度向上ログ取得対象機器	－	－	－	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		既知の脆弱性		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		マルウェア		該当ユーザ	－	－	－	－	該当EP	検知感度向上ログ取得対象機器	該当EP（AntiVirus）	該当EP（AntiVirus）	－	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
	通常業務との不一致	通常の通信先/通信元国情報		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常の内部サーバ/アプリケーション情報		該当ユーザ	－	－	－	－	該当EP	検知感度向上ログ取得対象機器	－	－	－	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常利用のアプリケーション情報		該当ユーザ	－	－	－	－	該当EP	検知感度向上ログ取得対象機器	－	－	－	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常利用のサイトカテゴリ情報		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常利用の通信先ポート番号		該当ユーザ	－	－	－	－	該当EP	検知感度向上ログ取得対象機器	－	－	－	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常実行ファイルを取得するサイト情報		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常送信するファイル形式		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		IP直接指定のHTTPアクセス		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	プロキシサーバ	DNSサーバ	DNSサーバ	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通常アクセスするURLのクエリストリング情報		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	プロキシサーバ	DNSサーバ	DNSサーバ	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		CONNECT先ポート情報		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	プロキシサーバ	DNSサーバ	DNSサーバ	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
統計分析	既知の標的型攻撃事象との類似 通常業務からの乖離	通信先数		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		エラー応答数		該当ユーザ	ドメインコントローラー	ドメインコントローラー	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		一定間隔で発生する通信		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		通信回数		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器
		転送データサイズ		該当ユーザ	ドメインコントローラー	－	ドメインコントローラー	ドメインコントローラー	該当EP	検知感度向上ログ取得対象機器	－	－	DNSサーバ	ホスト型FW	ホスト型FW	ホスト型FW	スイッチ/ルータ	スイッチ/ルータ	－	該当EP	該当EP	該当セグメント	検知感度向上ログ取得対象機器	－	－	－	FW or スイッチ/ルータ	FW	FW or スイッチ/ルータ	FW or スイッチ/ルータ	スイッチ/ルータ	スイッチ/ルータ	サービス提供機器	サービス提供機器

付録3 暫定対処策一覧 （機密性・可用性・完全性の評価方法）

	ユーザ	該当EP	セグメント	サービス
機密性	**アクセス許可されたユーザのみが該当ユーザの情報資産にアクセスできること。** 〇: 暫定対処後にアクセス許可されたユーザのみが、該当ユーザの情報資産にアクセスできる。 △: 暫定対処後にアクセス許可されたユーザ以外が、該当ユーザの情報資産の一部にアクセスできる。 ×: 暫定対処後にアクセス許可されたユーザ以外が、該当ユーザの情報資産全てにアクセスできる。	**アクセス許可されたユーザのみが該当EP内の情報資産にアクセスできること。** 〇: 暫定対処後にアクセス許可されたユーザのみが、該当EPの情報資産にアクセスできる。 △: 暫定対処後にアクセス許可されたユーザ以外が、該当EPの情報資産の一部にアクセスできる。 ×: 暫定対処後にアクセス許可されたユーザ以外が、該当EPの情報資産全てにアクセスできる。	**アクセス許可されたユーザのみが該当セグメント内の情報資産にアクセスできること。** 〇: 暫定対処後にアクセス許可されたユーザのみが、該当セグメントの情報資産にアクセスできる。 △: 暫定対処後にアクセス許可されたユーザ以外が、該当セグメントの情報資産の一部にアクセスできる。 ×: 暫定対処後にアクセス許可されたユーザ以外が、該当セグメントの情報資産全てにアクセスできる。	**アクセス許可されたユーザのみが該当サービス内の情報資産にアクセスできること。** 〇: 暫定対処後にアクセス許可されたユーザのみが、該当サービストの情報資産にアクセスできる。 △: 暫定対処後にアクセス許可されたユーザ以外が、該当サービスの情報資産の一部にアクセスできる。 ×: 暫定対処後にアクセス許可されたユーザ以外が、該当サービスの情報資産全てにアクセスできる。
完全性	**ユーザの情報資産の破壊、改ざんが起きないよう保障されていること。** 〇: 暫定対処後にユーザの情報資産の破壊、改ざんが起きない。 △: 暫定対処後にユーザの情報資産の一部が破壊、改ざんされる。 ×: 暫定対処後にユーザの情報資産の全てが破壊、改ざんされる。	**該当EP内の情報資産の破壊、改ざんが起きないよう保障されていること。** 〇: 暫定対処後に該当EPの情報資産の破壊、改ざんが起きない。 △: 暫定対処後に該当EPの情報資産の一部が破壊、改ざんされる。 ×: 暫定対処後に該当EPの情報資産の全てが破壊、改ざんされる。	**該当セグメント内の情報資産の破壊、改ざんが起きないよう保障されていること。** 〇: 暫定対処後に該当セグメントの情報資産の破壊、改ざんが起きない。 △: 暫定対処後に該当セグメントの情報資産の一部が破壊、改ざんされる。 ×: 暫定対処後に該当セグメントの情報資産の全てが破壊、改ざんされる。	**該当サービス内の情報資産の破壊、改ざんが起きないよう保障されていること。** 〇: 暫定対処後に該当サービスの情報資産の破壊、改ざんが起きない。 △: 暫定対処後に該当サービスの情報資産の一部が破壊、改ざんされる。 ×: 暫定対処後に該当サービスの情報資産の全てが破壊、改ざんされる。
可用性	**ユーザが必要な時に該当ユーザの情報資産にアクセスできること。** 〇: 暫定対処後、ユーザが必要な時に該当ユーザの情報資産にアクセスできる。 △: 暫定対処後、ユーザが必要な時に該当ユーザの情報資産の一部にアクセスできない。 ×: 暫定対処後、ユーザが必要な時に該当ユーザの情報資産の全てにアクセスできない。	**ユーザが必要な時に該当EP内の情報資産にアクセスできること。** 〇: 暫定対処後、ユーザが必要な時に該当EPの情報資産にアクセスできる。 △: 暫定対処後、ユーザが必要な時に該当EPの情報資産の一部にアクセスできない。 ×: 暫定対処後、ユーザが必要な時に該当EPの情報資産の全てにアクセスできない。	**ユーザが必要な時に該当セグメント内の情報資産にアクセスできること。** 〇: 暫定対処後、ユーザが必要な時に該当セグメントの情報資産にアクセスできる。 △: 暫定対処後、ユーザが必要な時に該当セグメントの情報資産の一部にアクセスできない。 ×: 暫定対処後、ユーザが必要な時に該当セグメントの情報資産の全てにアクセスできない。	**ユーザが必要な時に該当サービス内の情報資産にアクセスできること。** 〇: 暫定対処後、ユーザが必要な時に該当サービスの情報資産にアクセスできる。 △: 暫定対処後、ユーザが必要な時に該当サービスの情報資産の一部にアクセスできない。 ×: 暫定対処後、ユーザが必要な時に該当サービスの情報資産の全てにアクセスできない。

付録3 暫定対処策一覧 （暫定対処策の説明）

効果を及ぼす対象	暫定対処策	説明	効果確認箇所
ユーザ（アカウント）	注意喚起	該当ユーザに対し、検知したこと（および可能であれば検知したことに対する対処策）を周知し注意を喚起する。	－
	PW変更	該当ユーザのパスワードを変更する。	ドメインコントローラ Proxyサーバ
	権限変更	該当ユーザの権限を変更する。	ドメインコントローラ
	無効化	該当ユーザを無効化する。	ドメインコントローラ
	削除	該当ユーザを削除する。	ドメインコントローラ
EP	注意喚起	該当EPに対し、検知したこと（および可能であれば検知したことに対する対処策）を周知し注意を喚起する。	－
	検知感度向上	検知感度向上ログの取得を開始する。検知感度向上ログの取得を開始する機器は、検知感度向上ログの取得対象となっている機器全てとする。	各機器
	マルウェア隔離	該当EPのマルウェアを隔離する。	AntiVirus
	マルウェア駆除	該当EPのマルウェアを駆除する。	AntiVirus
	接続先URL遮断	該当URLとの通信を遮断する。	Proxyサーバ
	ポート番号遮断	該当EPの該当ポート番号での通信を遮断する。方向に関しては攻撃に応じて設定する。	ホスト型FW
	プロトコル遮断	該当EPの該当プロトコルでの通信を遮断する。方向に関しては攻撃に応じて設定する。	ホスト型FW
	IPアドレス遮断	該当EPと接続するIPアドレスとの通信を遮断する。方向に関しては攻撃に応じて設定する。	ホスト型FW
	所属NWの変更	該当EPを現在所属しているネットワークならびに他のネットワークから隔離する。	EPおよびスイッチ/ルータ
	EPをIP遮断	該当EPのIPアドレスでの通信をできないようにする。	スイッチ/ルータ
	抜線	該当EPのLANケーブルを抜線し物理的に通信できないようにする。NICを無効化することによってもLANケーブルを抜線するのと同様の効果を期待できるが、NICを無効化してもARPリクエストに応答する場合があるなど実装によってはLANケーブル抜栓とは異なる挙動を示すことがあるため、NICの無効化により抜線扱いとする場合は注意を要する。	－
	電源断 （証拠保全量が減る）	該当EPの電源を停止する。	－
セグメント	注意喚起	該当セグメントに対し、検知したこと（および可能であれば検知したことに対する対処策）を周知し注意を喚起する。	－
	検知感度向上	検知感度向上ログの取得を開始する。検知感度向上ログの取得を開始する機器は、検知感度向上ログの取得対象となっている機器全てとする。	各機器
	ドメイン・URL遮断	セグメントと該当ドメインまたはURLとの通信を遮断する。	Proxyサーバ
	DNS(ブラックホスト名) 不在応答	該当ホストの名前解決要求に対し、該当ホスト名は存在しないと応答する。	DNSサーバ
	DNS(ブラックドメイン名) 不在応答	該当ドメインの名前解決要求に対し、該当ドメイン名は存在しないと応答する。	DNSサーバ
	ポート番号遮断	該当セグメントと他セグメント間の該当ポート番号での通信を遮断する。方向に関しては攻撃に応じて設定する。	FW
	プロトコル遮断	該当セグメントと他セグメント間の該当プロトコルでの通信を遮断する。方向に関しては攻撃に応じて設定する。	FW
	IPアドレス遮断	該当外部IPアドレスとの通信を遮断する。方向に関しては攻撃に応じて設定する。	FW
	SRC/DSTセグメント間 通信遮断	該当送信元IPアドレスと該当送信先IPアドレスそれぞれの所属するセグメント間の通信を遮断する。	FW
	接続NWの変更	該当EPの所属するネットワークと他のネットワークと隔離する。	EPおよびスイッチ/ルータ
	NWごと抜線	当該EPの所属するネットワークと他のネットワークから切り離す。	－
サービス	サービス一部停止	該当サービスを一部停止する。	サービス提供機器
	サービス全停止	該当サービスを全て停止する。	サービス提供機器