参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	あなたのサイトのセキュリティポリシーを遵守し、適切なインシデント対処要員と法務要員を充てる。				
	可能である限り正確に、システムの全体像をキャプチャする。				
	詳細なノートをつける。これらは、日付と時間を含む必要がある。可能であれば、自動的に複製を生成する。(例: Unix システムにおいて、「スクリプト」プログラムが、利用可能。ただし、それが生成する出力ファイルは、証拠の部分であるメディアであってはならない。ノートと印刷物には、署名と日付が付される必要がある。				
	システム時間と UTC 間の時差をノートする。各タイムスタンプ期間において、UTC 時間もしくは現地時間のいずれかを示す。				
	(おそらく数年後に)あなたが行ったすべての行為と、その時刻を概説する証言に備える。詳細なノートは、決定的に重要である。				
	データを収集する際に、その変更を最小限にする。これは、内容の変更に限定されない。; ファイル／ディレクトリのアクセス時間を変更することを避ける必要がある。				
	変更するための外部経路を削除する。				
	収集と分析のどちらかを選択しなければならない場面においては、収集を優先し、分析を後にする必要がある。				
	ことさら述べるまでもないが、手順は実装可能である必要がある。インシデント対応ポリシーの、あらゆる観点において、特に危機における実行可能性を検証す るために手順は、テストされる必要がある。スピードと正確性の理由により、可能であれば、手順は自動化される必要がある。方法論的にせよ。				
	各デバイスについて、あなたの収集手順の中にあるガイドラインに従った方法論的アプローチが採用される必要がある。しばしば、スピードは、決定的に重要で あるので、検査しなければならないデバイスが数多くある場合、証拠を平行して収集するために、作業をあなたのチーム内で分担させるのが適切であろう。しか し、各々のシステムについては、収集は段階を踏んで行われなければならない。				
	揮発性の高いものから揮発性の低いものへの順に進行する。				
	システムのメディアのビットレベルの複製を作成する必要がある。法務分析を行いたい場合、そのために証拠資料のビットレベルの複製を作成する必要がある。 それは、分析によりファイルアクセス時刻を、ほぼ確実に変更してしまうことによる。証拠資料上で法務分析をすることは避けよ。				
	証拠を収集する際に、あなたは、揮発性の高いものから揮発性の低いものへの順に進行する必要があります。				
	証拠収集 を完了するまでは、シャットダウンしてはならない。多くの証拠が、失われる可能性があり、攻撃者は、証拠を破壊するために、スタートアップ／シャットダウンのスクリプト／サービスを置き換えた可能性がある。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	システム上のプログラムを信頼してはならない。適切に保護されたメディアから証拠収集プログラムを実行せよ。（下を見よ。）				
	システム上のあらゆるファイルのアクセス時刻を変更するプログラムは、実行するな。（例：'tar' または 'xcopy'。）				
	変更するための外部経路を削除する際に、単に接続を絶つこと、もしくはネットワークからフィルタリングすることが、ネットと接続されていないことを検知して証拠を消す「死人のスイッチ」の引き金を引く可能性があることを銘記せよ。				
	あなたの会社と司法管轄圏のプライバシーについてのルールとガイドラインを遵守せよ。特に、普段はこの情報へのアクセスを持たない者の誰にでも探している 証拠が入手可能である限り、情報が収集されていないことを確認せよ。これは、個人情報とともに、（ユーザ行為のパターンを明らかにする可能性がある）ログ ファイルへのアクセスを含む。				
	強い司法権なしに、人々のプライバシーを侵害してはならない。特に、本当にインシデントが起きているという十分な根拠を持たない限り、（個人的なファイルストレージのような）普段アクセスする理由をもたない領域から情報を収集してはならない。				
	インシデントの証拠を収集するために行う段階において、あなたの会社の確立された手順の支援があることを確認せよ。				
	採用可能：法廷に提出される前に、特定の法的ルーツに適合しなければならない。				
	真正：積極的に材料をインシデントと証拠論的に結びつけることが可能でなければならない。				
	完全：特定の観点のみならず、全体像を伝えるものでなければならない。				
	依拠可能：どのように証拠が収集され、扱われたかについて、その真正性と真実性についての疑いを招くことがあってはならない。				
	信用可能：法廷によってただちに信用可能であり、理解可能でなければならない。				
	あなたの収集手順は、可能な限り詳細化される必要があります。あなたのインシデント対処手順全般に関する限り、それらは、曖昧でない必要があり、収集手順において必要とされる意思決定の量を最小化する必要があります。				
	証拠を収集するために使用する手法は、透過的かつ再現可能である必要があります。あなたは、利用した手法を詳細に再現することを備える必要があり、それらの手法を独立の専門家によってテストされる必要があります。				
	証拠は、どこにあるか？どのシステムがインシデントに巻き込まれているか、また、どのシステムから証拠が収集されるかをリストする。				
	何が関連し、また管理可能でありそうかを確立する。失敗が疑われるとき、不足しているのではなく、集めすぎている。				
	各システムについて、関連する揮発性の順序を入手する。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	変更するための外部経路を削除する。				
	揮発性の順序に従い、第 5 章で検討するルールで証拠を収集する。				
	システムの時計のずれの程度を記録する。				
	収集段階を通じて作業する際に、他のものが証拠である可能性を問う。				
	各段階を文書化する。				
	巻き込まれた人を忘れない。誰が居て何をしていたか、何を観察し、どのように反応したか、のノートをつける。				
	実施可能である場合、あなたは、チェックサムを生成し、収集された証拠に暗号技術的に署名することを検討する必要があります。それは、これにより強い証拠の連鎖を保全することが一層容易になるからです。この際に、証拠を変更してはなりません。				
	証拠は、厳密にセキュアにしなければなりません。さらに、「カストディの連鎖」は、明確に文書化される必要があります。				
	あなたは、「どのように証拠が発見されたか」、「どのように扱われたか」および「それについて起きたすべての事項」を明確に記述することができるはずです。 －どこで／いつ／誰によって、証拠が発見、収集されたか。 －どこで／いつ／誰によって、証拠が対処、検査されたか。 －誰が証拠のカストディとなり、その期間は。どのように、それは保存されたか。 －いつ、証拠のカストディを変えたか、いつ、どのように転送が行われたか。（送付番号等を含む。）				
	可能な場合、（あまり使われていない保存メディアではなく）普通に利用されているメディアが、アーカイビングに利用される必要があります。				
	証拠へのアクセスは、厳格に制限される必要があり、明確に文書化される必要があります。認可されていないアクセスを検知することができる必要があります。				
	あなたは、証拠収集と法務に必要なプログラムを、読み取り専用メディア（例： CD）上に持つ必要があります。あなたは、利用する前に、あなたが管理している各 OS（オペレーティングシステム）用のこのようなツールセットを備える必要があります。 －プロセスを検査するためのプログラム（例： 'ps'） －システム状態を検査するためのプログラム（例： 'showrev'、'ifconfig'、'netstat'、'arp'） －ビットレベルで複製するためのプログラム（例： 'dd', 'SafeBack'） －チェックサムと署名を生成するためのプログラム（例： 'sha1sum'、チェックサムを使える'dd'、'SafeBack'、'PGP'） －core イメージを生成し、それらを検査するためのプログラム（例： 'gcore', 'gdb'） －証拠収集を自動化するスクリプト（例： The Coroner's Toolkit [FAR1999]）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	あなたのツール中のプログラムは、スタティック（静的）にリンクされている必要があり、読みとり専用メディア上のライブラリ以外のいかなるライブラリの利用を要求するものであってはなりません。				
	これでも、最近のルートキット（rootkit）は、ロード可能なカーネルモジュールとしてインストールされる可能性があるので、あなたは、あなたのツールがシステムの全体像を提供していない可能性があることを考慮する必要があります。				
	あなたは、あなたが利用するツールの真正性と依拠可能性について証言する準備をする必要があります。				