サイバー攻撃（標的型攻撃）対策
防御モデルの解説

付録4 システムログ一覧（証拠保全）

付録4 システムログ一覧（証拠保全）

#	ログとして扱うことができる情報							カテゴリ1	カテゴリ2	カテゴリ3	カテゴリ4	カテゴリ5	資産価値評価
	区分	機器設置場所	機器	EP・NW種別	種別	ログ項目	デフォルトの設定で出力される項目	被害事実（外部通信事実）の確認	被害箇所の確認	資産価値の高い（重要な情報をもった）マシンの確認	被害内容の確認	被害原因の確認	ノードが持つ資産価値を評価
1	標準構成機器	DMZ	ファイアウォール(FW)	NW	－	日時	○	○				○	
2						ファイアウォールホスト名	○						
3						ファイアウォールルール名及び番号	○						
4						インバウンドインタフェース	○						
5						アウトバウンドインタフェース	○						
6						MACアドレス	○						
7						パケットサイズ	○						
8						IPパケット優先度（TOS,PREC）	○						
9						IPパケット生存期間（TTL）	○						
10						IPフラグメントパケット識別子（ID）	○						
11						IPフラグメンテーション情報（DFビット）	○						
12						ソースIPアドレス	○						
13						ソースポート番号	○						
14						宛先IPアドレス	○						
15						宛先ポート番号	○						
16						プロトコル	○						
17						TCPウインドウサイズ（WINDOW）	○						
18						TCPフラグ	○						
19			ネットワーク型IPS/IDS	NW	－	日時	○	○				○	
20						送信元アドレス/ポート番号	○						
21						宛先アドレス/ポート番号	○						
22						同一セッションの送受信バイト数	○						
23						同一セッションの送受信パケット数	○						
24						プロトコル	○						
25						セッション継続時間	○						
26						セッションのユーザ名	○						
27						URL	○						
28						ファイル名	○						
29						脅威情報	○						
30			Webサーバ	EP	アクセスログ	リモートホスト名またはIPアドレス	○	○			○	○	5点 機密性：1点 完全性：2点 可用性：2点
31						クライアントの識別子	○						
32						認証されたユーザー名	○						
33						日時	○						
34						リクエストの最初の行の値	○						
35						最後のレスポンスのステータス	○						
36						送信されたバイト数（ヘッダーは含まず）	○						
37						リクエストに含まれるRefererの値	○						
38						リクエストに含まれるUser-Agentの値（ブラウザ情報）	○						
39					APログ（エラーログ）	日時	○	○			○	○	
40						エラーの重要度	○						
41						アクセスしたクライアントのIPアドレス	○						
42						メッセージ	○						
43			APサーバ	EP	アクセスログ	リモートホスト名またはIPアドレス	○	○			○	○	5点 機密性：1点 完全性：2点 可用性：2点
44						認証されたユーザー名	○						
45						日時	○						
46						メソッドとURL	○						
47						HTTPステータスコード	○						
48						レスポンスサイズ	○						
49					APログ	日時	○				○	○	
50						ログを生成したスレッド	○						
51						ログレベル	○						
52						カテゴリー名	○						
53						メッセージ	○						
54			プロキシサーバ	NW	アクセスログ	UTCの時間	○	◎				◎	
55						継続時間	○						
56						クライアントのIPアドレス	○						
57						リザルトコード（結果コード）	○						
58						転送バイト数	○						
59						リクエストメソッド	○						
60						URL	○						
61						階層コード	○						
62						HTTPヘッダにリプライされてきたオブジェクトのコンテンツタイプ	○						
63						User-Agent							
64					APログ	日時	○						
65						メッセージ	○						
66			DNSサーバ	EP	－	日時		○			○	○	3点 機密性：1点 完全性：1点 可用性：1点
67						ログカテゴリ							
68						クライアントのIPアドレスとポート番号							
69						ファシリティ（ログの分類）							
70						ゾーン情報							
71			メールサーバ	EP	－	日時	○	○			○	○	3点 機密性：1点 完全性：1点 可用性：1点
72						サーバホスト名	○						
73						プロセスの情報（プロセスの所有者とプロセスID）	○						
74						メッセージID（Sendmailによって送信されたメッセージに割り当てられたID）	○						
75						メッセージの受信者または送信者	○						
76						メッセージサイズ	○						
77						メッセージ優先度	○						
78						メッセージ受信者数	○						
79						メッセージ識別番号	○						
80						プロトコル情報	○						
81						サーバデーモン名	○						
82						メッセージ送信サーバとIPアドレス	○						
83						ステータス	○						
84						添付ファイル名							
85		内部セグメント	スイッチ/ルータ	NW	－	日時						○	
86						送信元アドレス/ポート番号							
87						宛先アドレス/ポート番号							
88						同一フローの送受信バイト数							
89						同一フローの送受信パケット数							
90			ドメインコントローラー	EP	－	ログの名前	○		◎		○	○	6点 機密性：2点 完全性：2点 可用性：2点
91						ソース	○						
92						日時	○						
93						イベントID	○						
94						タスクのカテゴリ	○						
95						レベル	○						
96						キーワード	○						
97						ユーザー	○						
98						コンピュータ	○						
99						オペコード	○						
100			DHCPサーバ	NW	－	日時			◎			○	
101						ホスト名またはIPアドレス							
102						MACアドレス							
103						状態							
104			ファイルサーバ	EP	－	ログの名前	○				○	○	6点 機密性：2点 完全性：2点 可用性：2点
105						ソース	○						
106						日時	○						
107						イベントID	○						
108						タスクのカテゴリ	○						
109						レベル	○						
110						キーワード	○						
111						ユーザー	○						
112						コンピュータ	○						
113						オペコード	○						
114			DBサーバ	EP	－	日時	○				○	○	6点 機密性：2点 完全性：2点 可用性：2点
115						メッセージ	○						

#	ログとして扱うことができる情報							カテゴリ1	カテゴリ2	カテゴリ3	カテゴリ4	カテゴリ5	資産価値評価
	区分	機器設置場所	機器	EP・NW種別	種別		ログ項目	デフォルトの設定で出力される項目	被害事実（外部通信事実）の確認	被害箇所の確認	資産価値の高い（重要な情報をもった）マシンの確認	被害内容の確認	被害原因の確認	ノードが持つ資産価値を評価
116	標準構成機器	内部セグメント	エンドポイント(Windows)	EP	イベントログ		ログの名前	○						4点 機密性：2点 完全性：1点 可用性：1点
117							ソース	○						
118							日時	○						
119							イベントID	○						
120							タスクのカテゴリ	○				○	○	
121							レベル	○						
122							キーワード	○						
123							ユーザー	○						
124							コンピュータ	○						
125							オペコード	○						
126					プリフェッチ		日時	○				○	○	
127							ファイル名	○						
128					レジストリ		自動起動のファイル名	○				○	○	
129							接続したUSBメモリ等の情報	○						
130					タスクスケジューラ		ログの名前	○				○	○	
131							ソース	○						
132							日時	○						
133							イベントID	○						
134							タスクのカテゴリ	○						
135							レベル	○						
136							キーワード	○						
137							ユーザー	○						
138							コンピュータ	○						
139							オペコード	○						
140			エンドポイント(Linux)	EP	メッセージログ		日時	○				○	○	4点 機密性：2点 完全性：1点 可用性：1点
141							ログを出力したホスト名	○						
142							メッセージの出力元	○						
143							メッセージ	○						
144					cronログ		日時	○				○	○	
145							ログを出力したホスト名	○						
146							メッセージの出力元	○						
147							メッセージ	○						
148					カーネルログ		日時	○				○	○	
149							ログを出力したホスト名	○						
150							メッセージの出力元	○						
151							メッセージ	○						
152					セキュリティログ		日時	○				○	○	
153							ログを出力したホスト名	○						
154							メッセージの出力元	○						
155							メッセージ	○						
156			エンドポイント(OS)	EP	システムコールログ	ファイル操作ログ	日時					○	○	4点 機密性：2点 完全性：1点 可用性：1点
157							プロセスID							
158							プロセス名							
159							ファイルパス							
160						プロセス操作ログ	日時					○	○	
161							親プロセスID							
162							プロセスID							
163							プロセス名							
164							コマンドライン							
165						レジストリ操作ログ	日時					○	○	
166							プロセスID							
167							キー							
168							値							
169							データ							
170						API操作ログ	日時					○	○	
171							プロセスID							
172							API名							
173							APIの引数							
174							APIの戻り値							
175			エンドポイント(ブラウザ)	EP	―		日時	○				○	○	4点 機密性：2点 完全性：1点 可用性：1点
176							URL	○						
177			エンドポイント(AntiVirus)	EP	―		スキャン日時	○				○	○	4点 機密性：2点 完全性：1点 可用性：1点
178							プロセスID	○						
179							プロセス名	○						
180							スキャン結果	○						
181			L7FW(NGFW,APFW)	NW	―		日時	○					○	
182							送信元アドレス/ポート番号	○						
183							宛先アドレス/ポート番号	○						
184							同一セッションの送受信バイト数	○						
185							同一セッションの送受信パケット数	○						
186							プロトコル	○	○					
187							セッション継続時間	○						
188							セッションのユーザ名	○						
189							URL	○						
190							ファイル名	○						
191							脅威情報	○						
192			DLP(Data Loss Prevention)	NW			日時	○					○	
193							送信元アドレス/ポート番号	○						
194							宛先アドレス/ポート番号	○						
195							プロトコル		○					
196							URL							
197							検知キーワード	○						
198							検知ファイル名	○						
199			Mailゲートウェイ	NW			日時	○					○	
200							サーバホスト名	○						
201							メッセージID	○						
202							メッセージの受信者または送信者	○						
203							メッセージサイズ	○						
204							メッセージ受信者数	○						
205							プロトコル情報	○	○					
206							メッセージ送信サーバとIPアドレス	○						
207							ステータス							
208							件名	○						
209							検知名	○						
210							検知ファイル名	○						
211							検知URL	○						
212			WAF	NW			日時	○					○	
213							ログID	○						
214							送信元アドレス/ポート番号	○						
215							宛先アドレス/ポート番号	○	○					
216							検知タイプ	○						
217							優先度	○						
218							アラートメッセージID	○						
219	対策強化機器	DMZ					アラートメッセージIDに紐づく検知項目	○						
220			サンドボックス	NW			日時	○					○	
221							ログID	○						
222							送信元アドレス/ポート番号	○						
223							宛先アドレス/ポート番号	○						
224							プロトコル	○						
225							URL	○						
226							ファイル名	○						
227							ファイルタイプ	○	○					
228							ファイルサイズ	○						
229							ファイルハッシュ値	○						
230							悪性判定結果	○						
231							マルウェアのファイル操作ログ	○						
232							マルウェアのプロセス操作ログ	○						
233							マルウェアのAPI呼出し	○						
234							マルウェアの通信先アドレス/ポート番号	○						
239			改ざん検知	NW			日時	○					○	
240							ログID	○						
241							改ざん内容(ファイルサイズ変化：旧、新)	○	○					
242							検知ルール名(追加/削除/編集)	○						
243							検知ファイル名	○						
244							ユーザ名（検知した操作を行ったOSのアカウント名）	○						

#	ログとして扱うことができる情報							カテゴリ1	カテゴリ2	カテゴリ3	カテゴリ4	カテゴリ5	資産価値評価
	区分	機器設置場所	機器	EP・NW種別	種別	ログ項目	デフォルトの設定で出力される項目	被害事実（外部通信事実）の確認	被害箇所の確認	資産価値の高い（重要な情報をもった）マシンの確認	被害内容の確認	被害原因の確認	ノードが持つ資産価値を評価
245	対策強化機器		ホスト型IPS/IDS	NW		日時	○	○				○	
246						ログID	○						
247						ホストIPアドレス	○						
248						ホスト名	○						
249						検知ルール	○						
250						検知したファイル操作	○						
251						検知したプロセス操作	○						
252						検知したレジストリ操作	○						
253						検知したAPI呼出し	○						
254		内部セグメント				日時	○					○	
255						ログID	○						
256						ホストIPアドレス	○						
257						ホスト名	○						
258						検知ルール	○						
259						検知したファイル操作	○						
260						検知したプロセス操作	○						
261						検知したレジストリ操作	○						
262						検知したAPI呼出し	○						

付録4 システムログ一覧（証拠保全）－各列の評価方法について

#	ログとして扱うことができる情報							カテゴリ1	カテゴリ2	カテゴリ3	カテゴリ4	カテゴリ5	優先順位付けのための評価 ※オプション
	区分	痕跡 取得 場所	機器	EP・NW種別(6/16追記)	種別	ログ項目	デフォルトの設定で出力される項目	被害事実（外部通信事実）の確認	被害箇所の確認	資産価値の高い（重要な情報をもった）マシンの確認	被害内容の確認	被害原因の確認	資産価値評価
説明	標準構成機器か否か	機器が設置されている場所。DMZもしくは内部セグメント	機器名	機器が情報資産を保持しているか否か	－	－	－	－	－	台帳を基に、被害箇所のうちで資産価値の高いマシンを確認する	－	本格分析によって全貌を把握する	保存されている情報資産にの資産価値を、機密性・完全性・可用性の観点から評価する。 カテゴリ4とカテゴリ5において〇が大量にあった場合、資産価値が高い情報資産を保持する機器を優先して取得する。(カテゴリ1とカテゴリ2は被害箇所を特定するための行動なので、ここで評価する資産価値によらずに情報を取得する)
評価方法	－	－	－	EP：情報資産を（永続的に）保持している機器 NW：EP以外 ※情報資産とは「攻撃者が窃取したい情報」とする。 ※情報資産の価値は「法規適合性に関するISMSユーザガイド」を参考とした。 ■資産価値（機密性）の基準例 ・資産価値小：第三者に開示・提供可能。内容が漏洩した場合でも、ビジネスへの影響はほとんど無い。 ・資産価値大：特定の関係者または部署のみに開示・提供可能。内容が漏洩した場合、ビジネスへの影響は大きい。 ■資産価値（完全性）の基準例 ・資産価値小：参照程度でしか利用されないので問題がない。 ・資産価値大：完全性が維できないとビジネスへの影響は重大である。 ■資産価値（可用性）の基準例 ・資産価値小：情報が利用できなくてもビジネスに支障がない。 ・資産価値大：必要時に確実に情報が利用できないとビジネスへのは重大である。	－	－	－	〇：インターネットとの境界(DMZ)に設置されている、かつIPアドレスが取得可能な機器 ◎：〇のうち、被害事実（日時・SRC IP・DST IP・内容）を正確（正常・異常によりログを取得するかしないかが変わらず、EPへ辿り着くためにIPを読み替える必要が無いこと）にログを保存する機器	〇：クライアントからの要求に対して、クライアントを一意に識別可能な情報（MAC・ホスト名・ユーザID）を基にカテゴリ1の外部通信事実に登場する情報を配布する機器 ◎：〇のうち、MAC・ホスト名・ユーザIDの中から保存される項目数が多い機器	－	〇：情報資産が保存される機器	〇：前年度定義した「被害の全貌把握（侵入経路・流出経路・流出情報・拡散元情報・拡散先情報・復旧必要情報）」のうち侵入経路・流出経路の把握に必要なログを出力する機器 ◎：〇のうち、被害内容（日時・SRC IP・DST IP・内容）を正確（正常・異常によりログを取得するかしないかが変わらず、EPへ辿り着くためにIPを読み替える必要が無いこと）にログを保存する機器	機密性、完全性、可用性の観点より、資産価値を数値化して記載する。資産価値が高いほど点数が高い。 ■機密性 ・内部セグメントに存在するEP:2点 ・DMZに存在するEP:1点 ■完全性 ・組織体として改ざんされるとビジネスに影響あるEP:2点 ・その他のEP:1点 具体的には、以下の通り採点する。 ・内部セグメントに存在するDC・ファイルサーバ・DBサーバおよびDMZに存在するWebサーバ・APサーバ：2点 ・上記以外の機器：1点 ■可用性 ・組織体として共用利用されていて利用できなくなるとビジネスに影響あるEP:2点 ・その他のEP:1点 具体的には、以下の通り採点する。 ・内部セグメントに存在するDC・ファイルサーバ・DBサーバおよびDMZに存在するWebサーバ・APサーバ：2点 ・上記以外の機器：1点