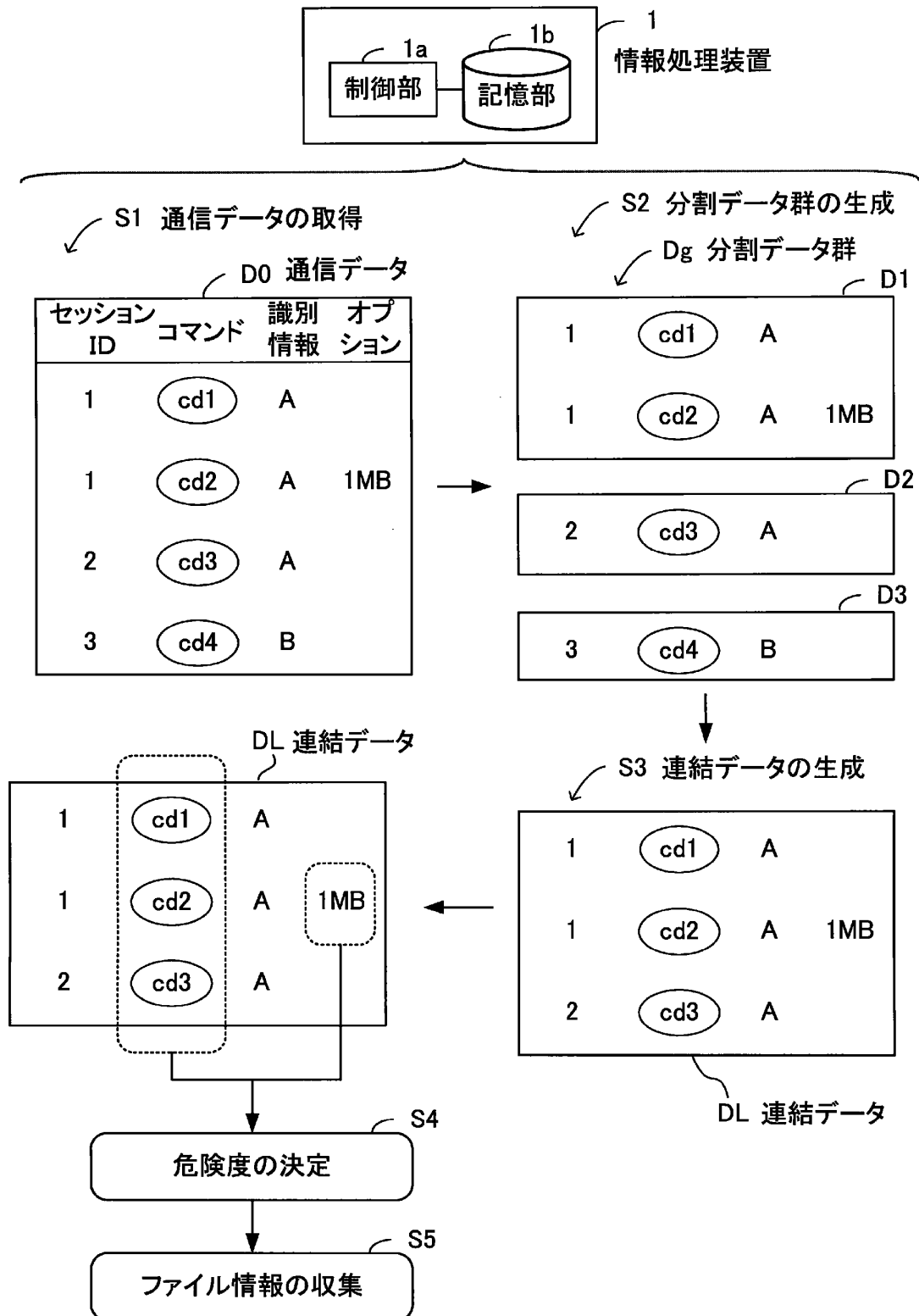
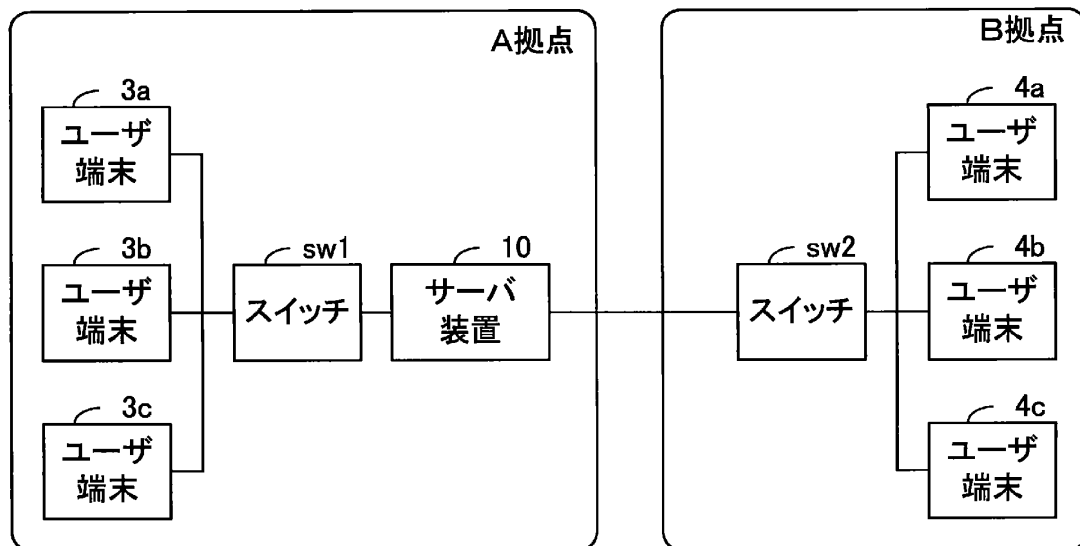


[図1]

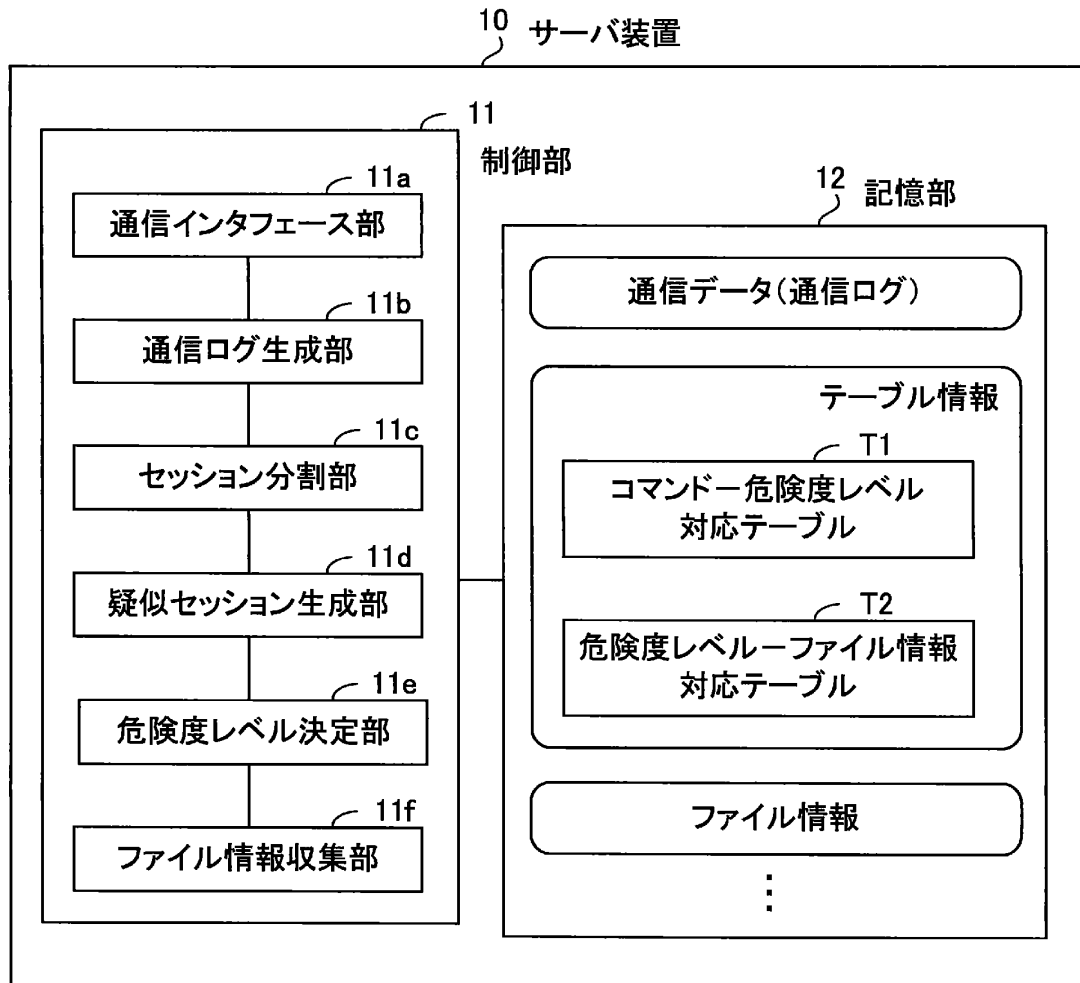


[図2]

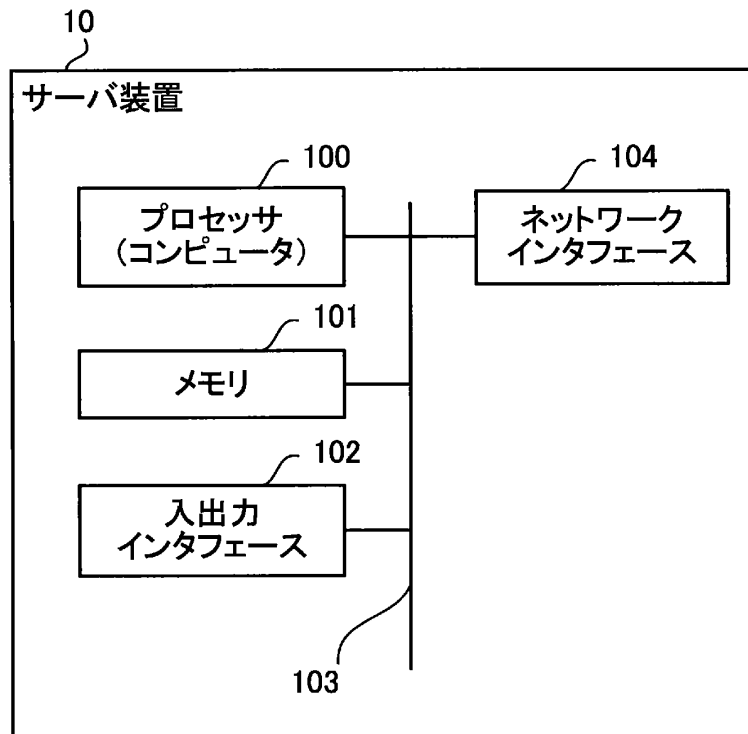
1-1 情報処理システム



[図3]



[図4]



[図5]

T11

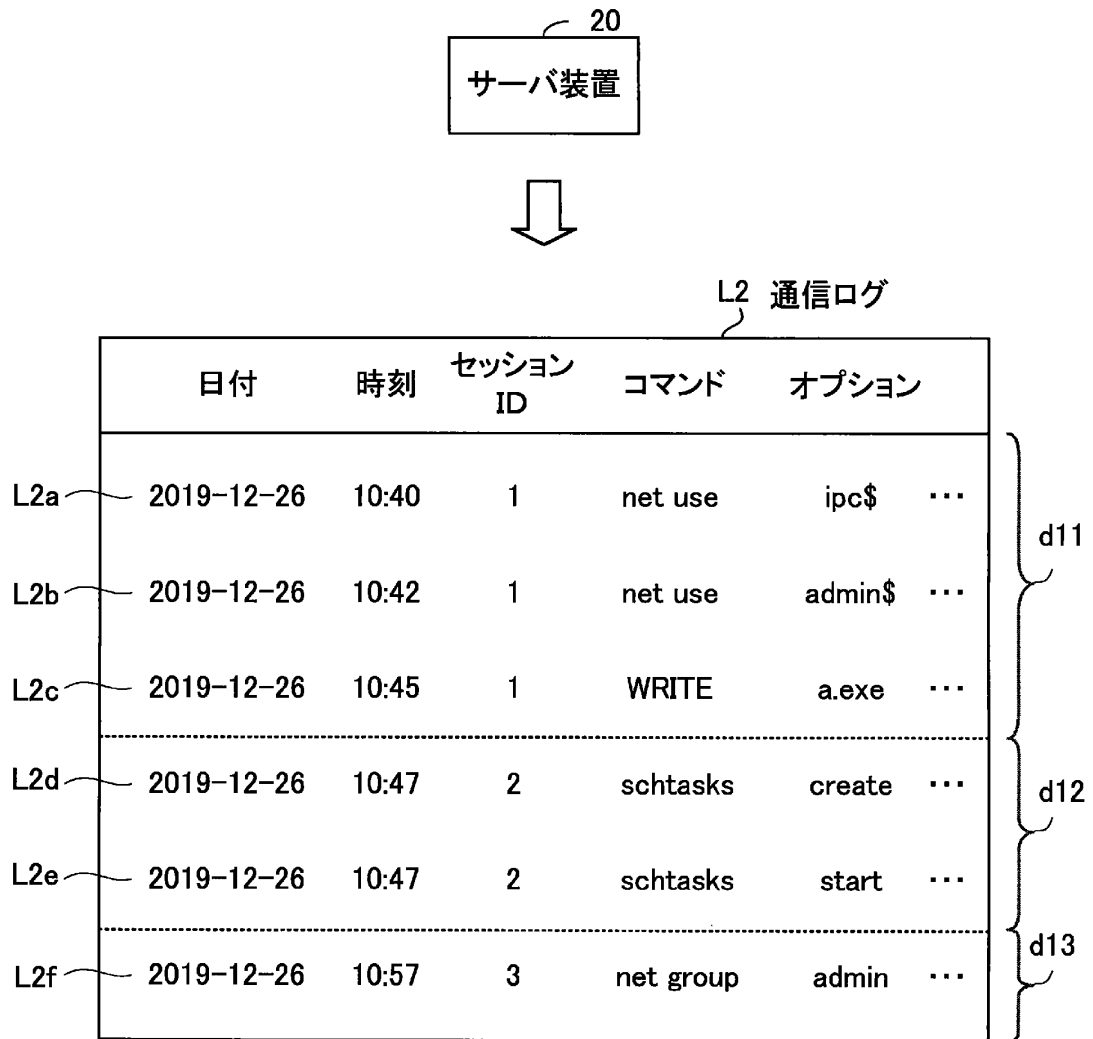
コマンド	危険度レベル
net group	1
net use	2
schtasks	3

[図6]

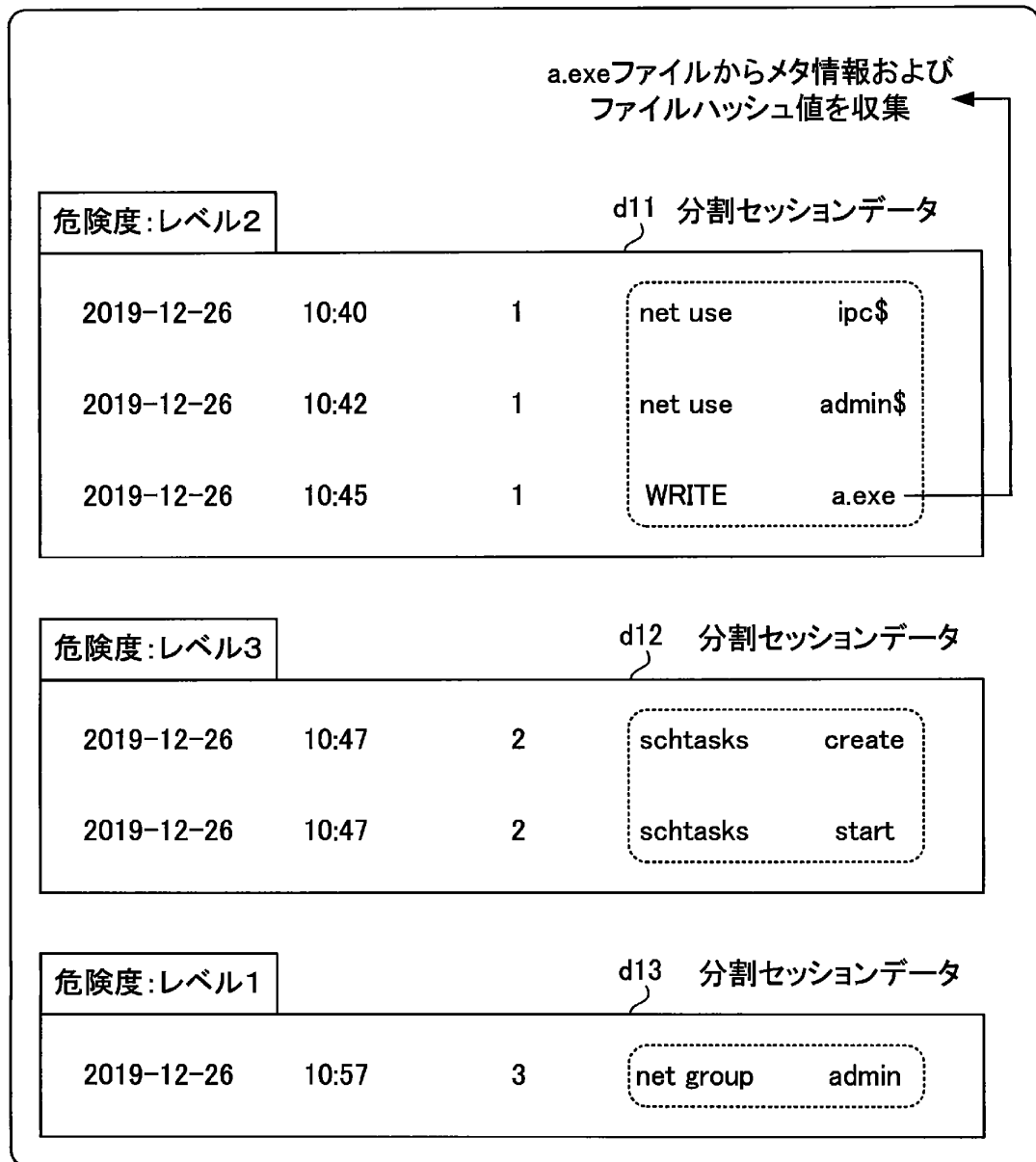
T12

危険度レベル	ファイル情報
1	メタ情報
2	メタ情報・ファイルハッシュ値
3	メタ情報・ファイルハッシュ値・ファイル本体

[図7]



[図8]



危険度レベル=3の通信ログにもかかわらず、
ファイル本体まで収集されない

[図9]

10
サーバ装置
(制御部11)

↓

L1 通信ログ

	日付	時刻	セッション ID	コマンド	オプション	
L1a	2019-12-26	10:40	1	net use	ipc\$ account:A	...
L1b	2019-12-26	10:42	1	net use	admin\$ account:A	...
L1c	2019-12-26	10:45	1	WRITE	a.exe account:A	1MB
L1d	2019-12-26	10:47	2	schtasks	create account:A	...
L1e	2019-12-26	10:47	2	schtasks	start account:A	...
L1f	2019-12-26	10:57	3	net group	admin account:B	...

[図10]

d1 分割セッションデータ

10:40	1	net use	ipc\$	account:A	...
10:42	1	net use	admin\$	account:A	...
10:45	1	WRITE	a.exe	account:A	1MB

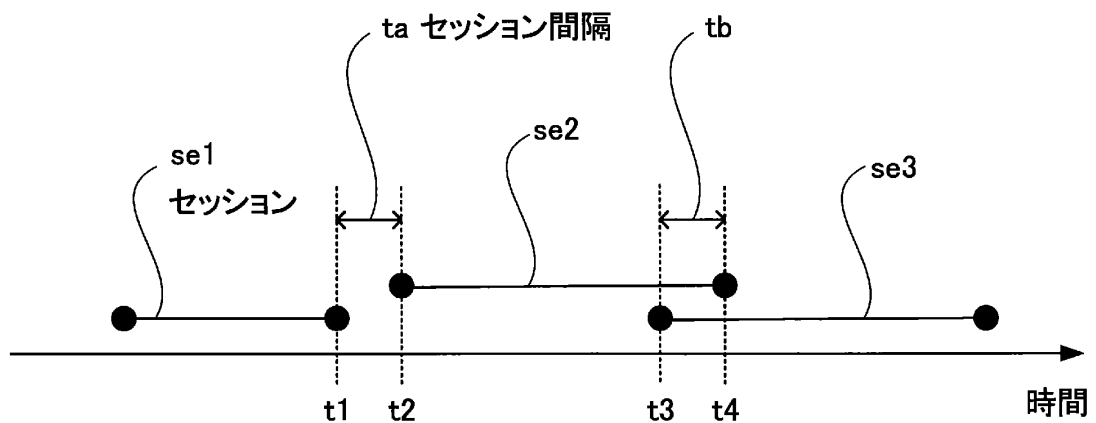
d2 分割セッションデータ

10:47	2	schtasks	create	account:A	...
10:47	2	schtasks	start	account:A	...

d3 分割セッションデータ

10:57	3	net group	admin	account:B	...
-------	---	-----------	-------	-----------	-----

[図11]



[図12]

dp 疑似セッションデータ

	10:40	1	net use	ipc\$	account:A	...
	10:42	1	net use	admin\$	account:A	...
L1c	10:45	1	WRITE	a.exe	account:A	1MB
L1d	10:47	2	schtasks	create	account:A	...
	10:47	2	schtasks	start	account:A	...

d3 分割セッションデータ

	10:57	3	net group	admin	account:B	...
--	-------	---	-----------	-------	-----------	-----

[図13]

T1 コマンドー危険度レベル対応テーブル

コマンド	危険度レベル
net group	1
net use	2
schtasks (ファイルサイズが閾値以上)	
schtasks (ファイルサイズが閾値未満)	3

[図14]

T2 危険度レベルーファイル情報対応テーブル

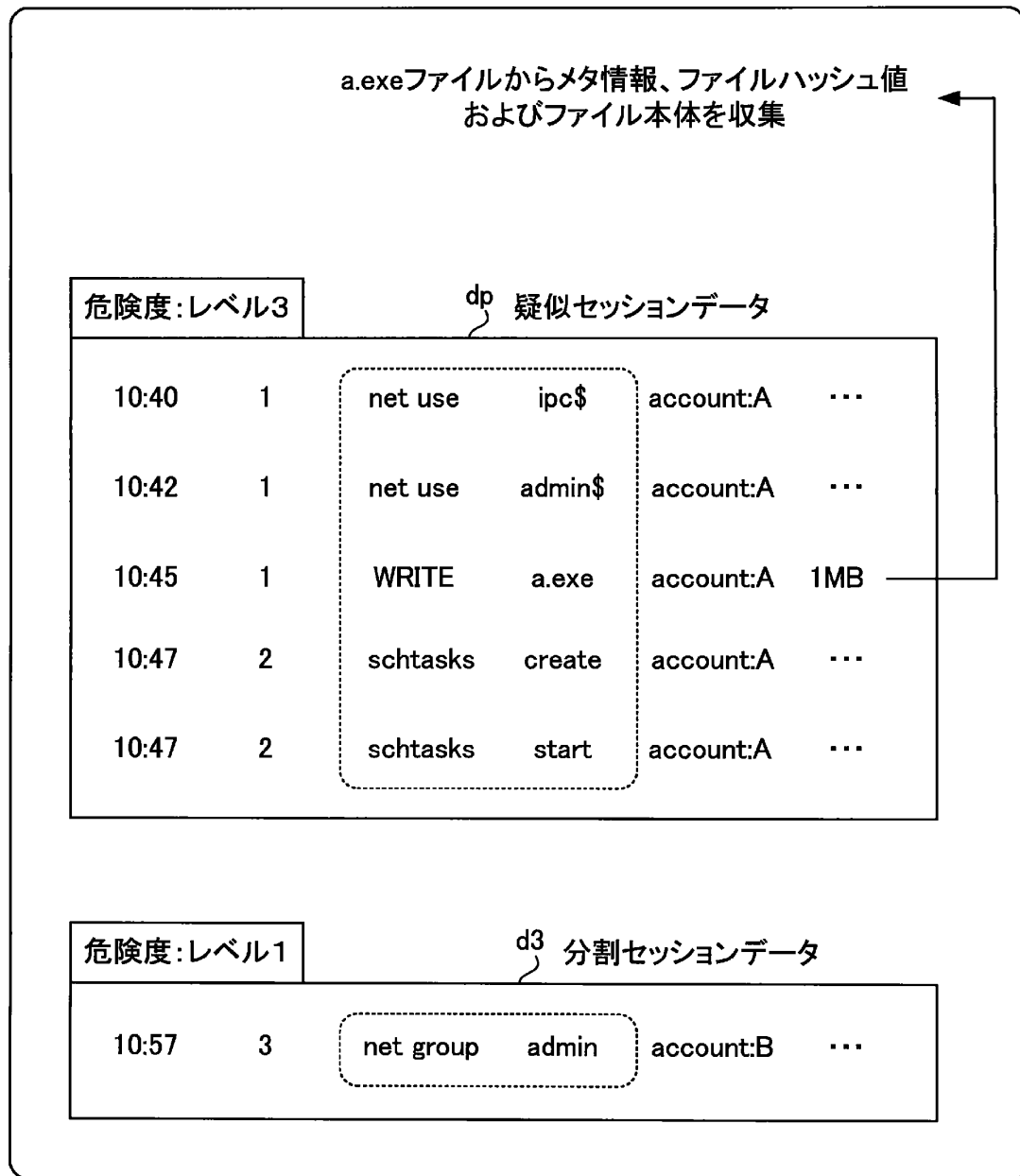
危険度レベル	ファイル情報
1	メタ情報
2	メタ情報・ファイルハッシュ値
3	メタ情報・ファイルハッシュ値・ファイル本体

[図15]

危険度:レベル3		dp 疑似セッションデータ			
10:40	1	net use	ipc\$	account:A	...
10:42	1	net use	admin\$	account:A	...
10:45	1	WRITE	a.exe	account:A	1MB
10:47	2	schtasks	create	account:A	...
10:47	2	schtasks	start	account:A	...

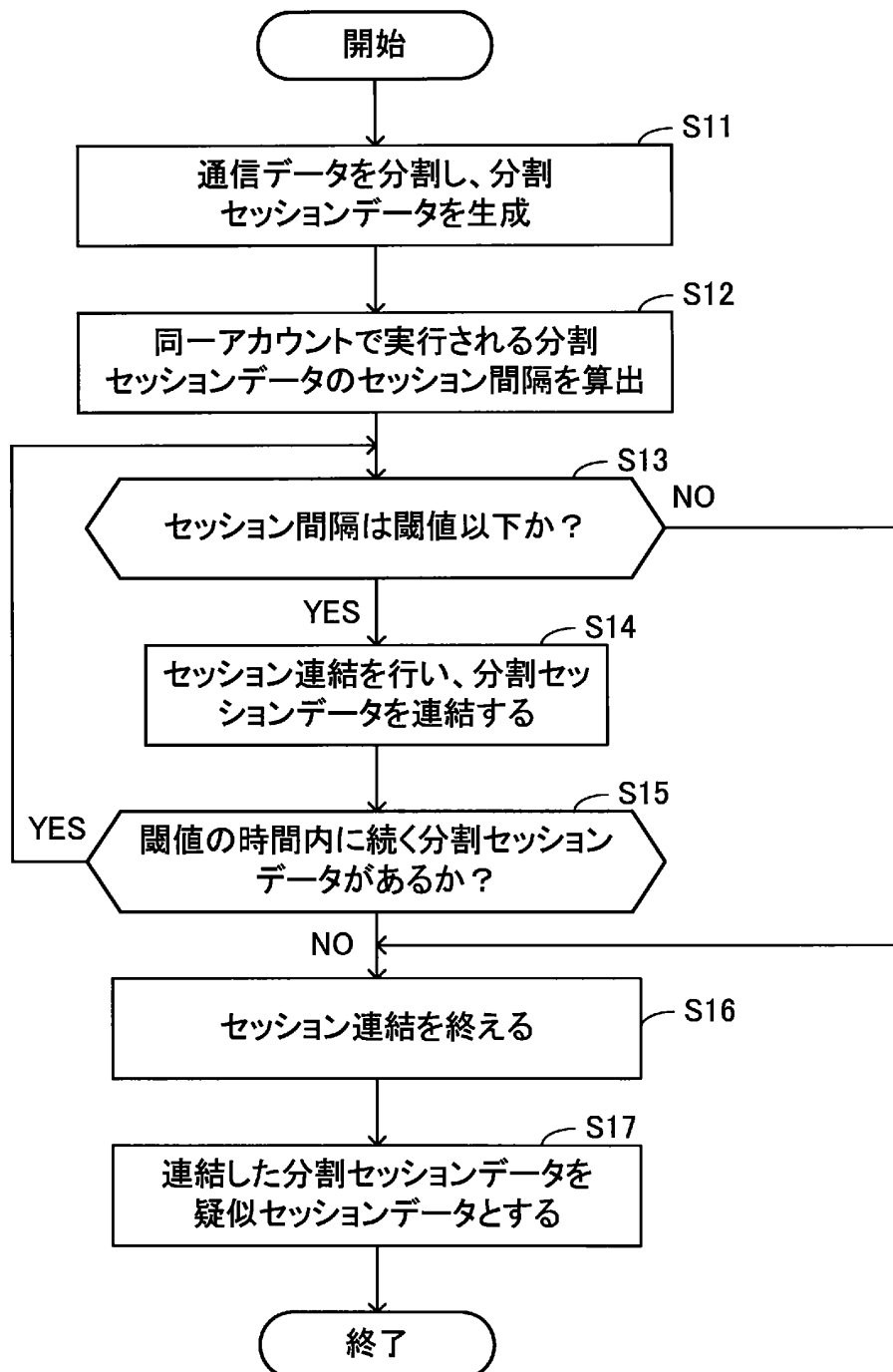
危険度:レベル1		d3 分割セッションデータ			
10:57	3	net group	admin	account:B	...

[図16]

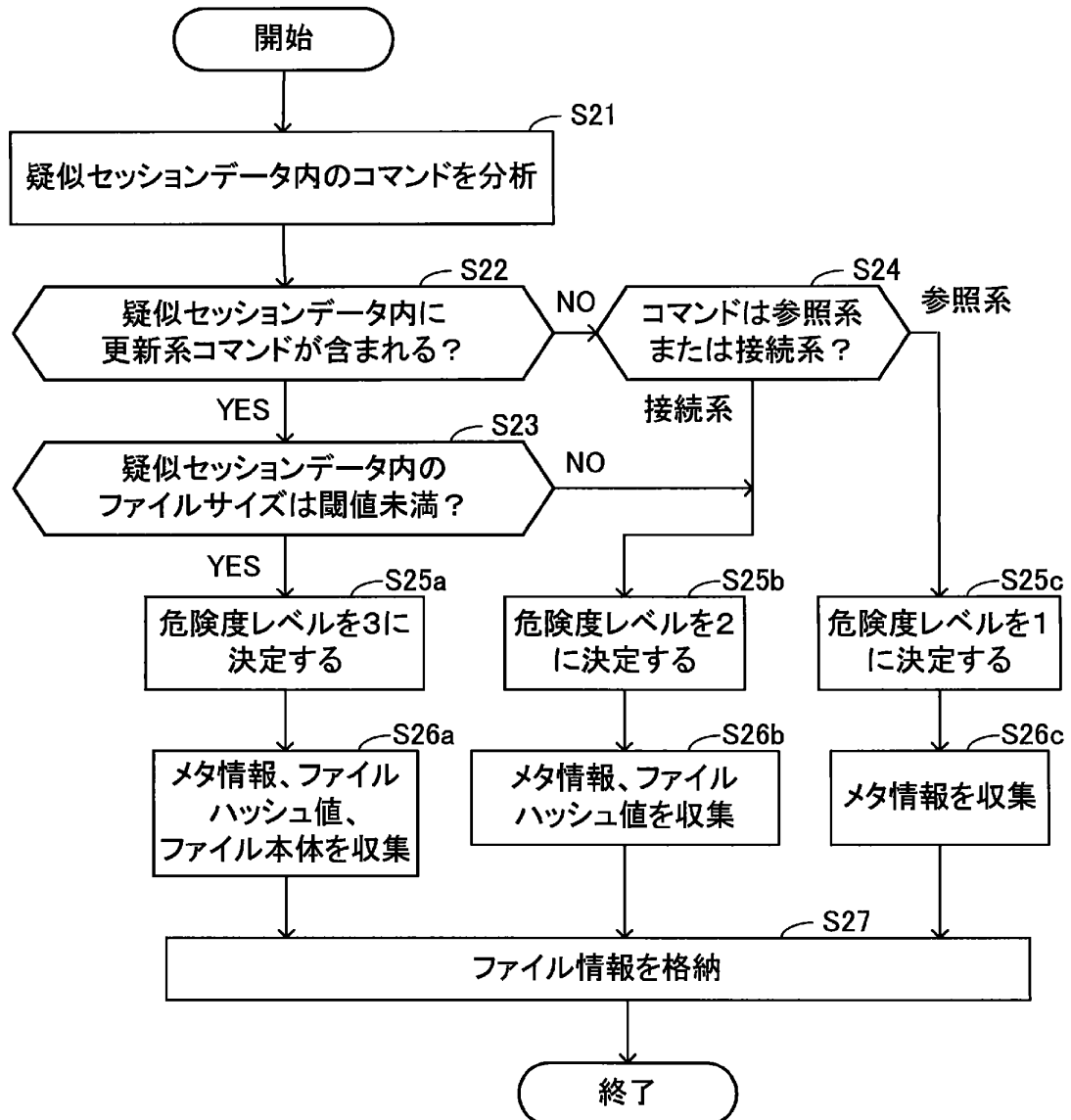


危険度レベル=3の通信ログから、
ファイル本体まで収集できる

[図17]



[図18]



[図19]

