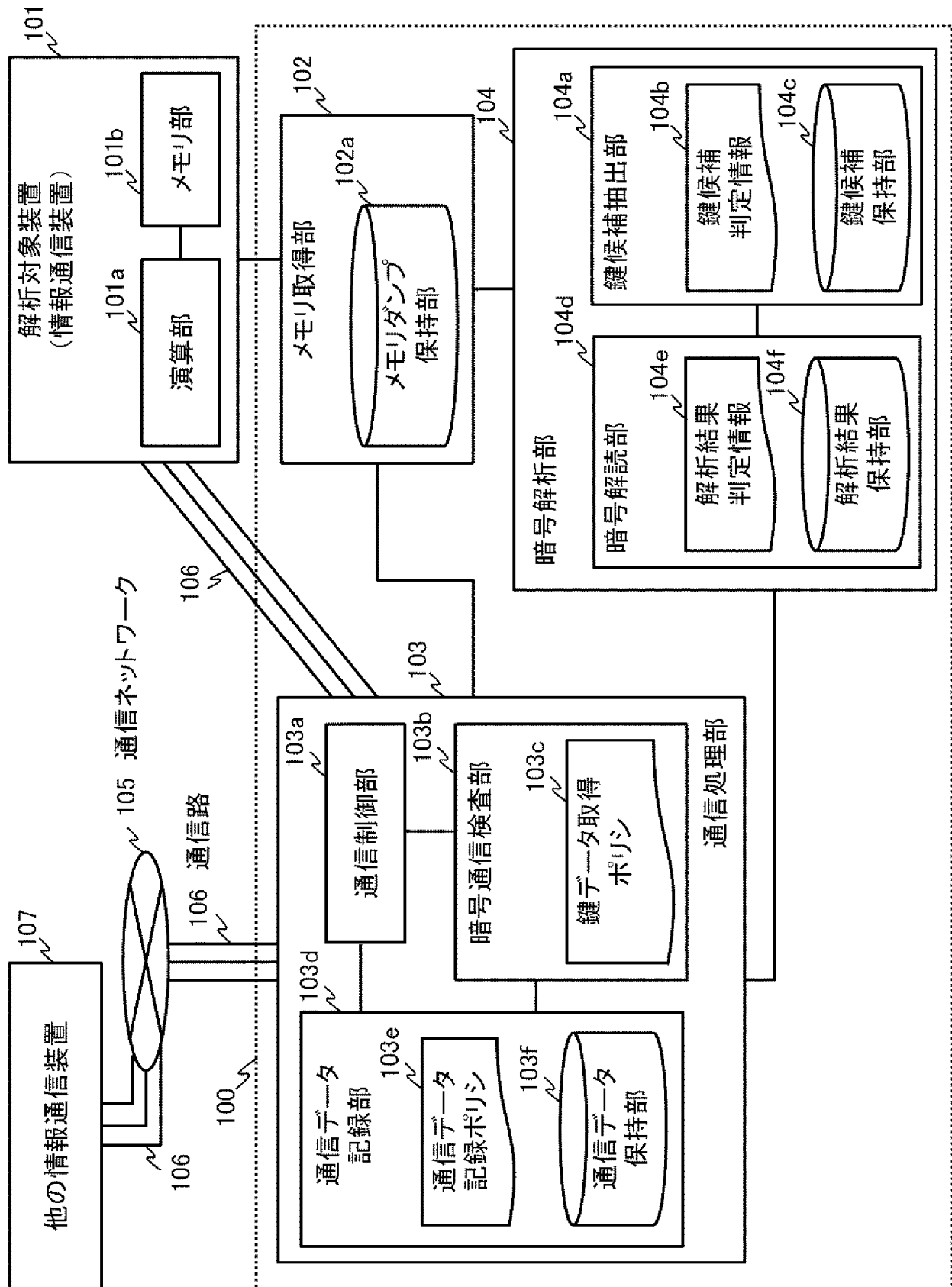
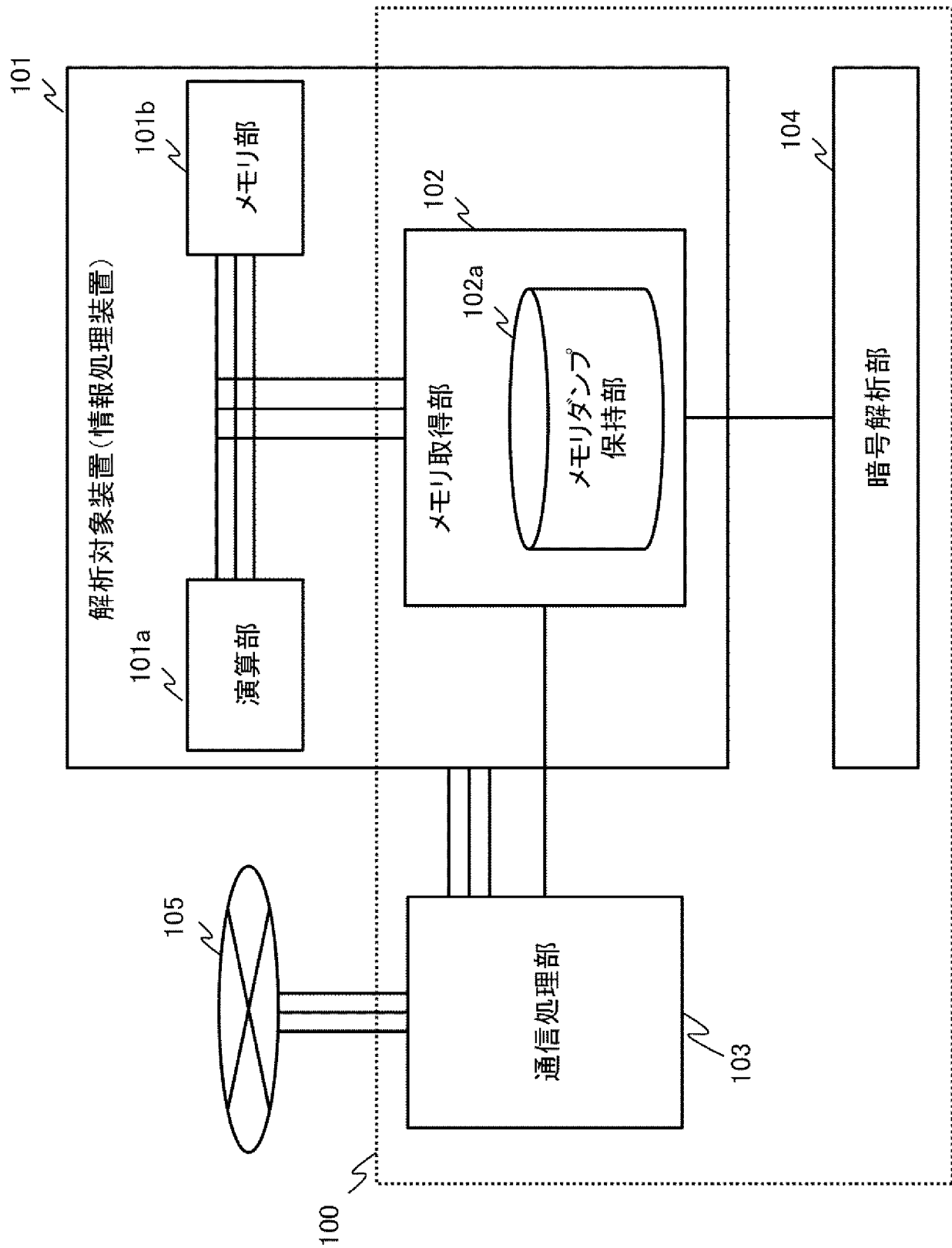


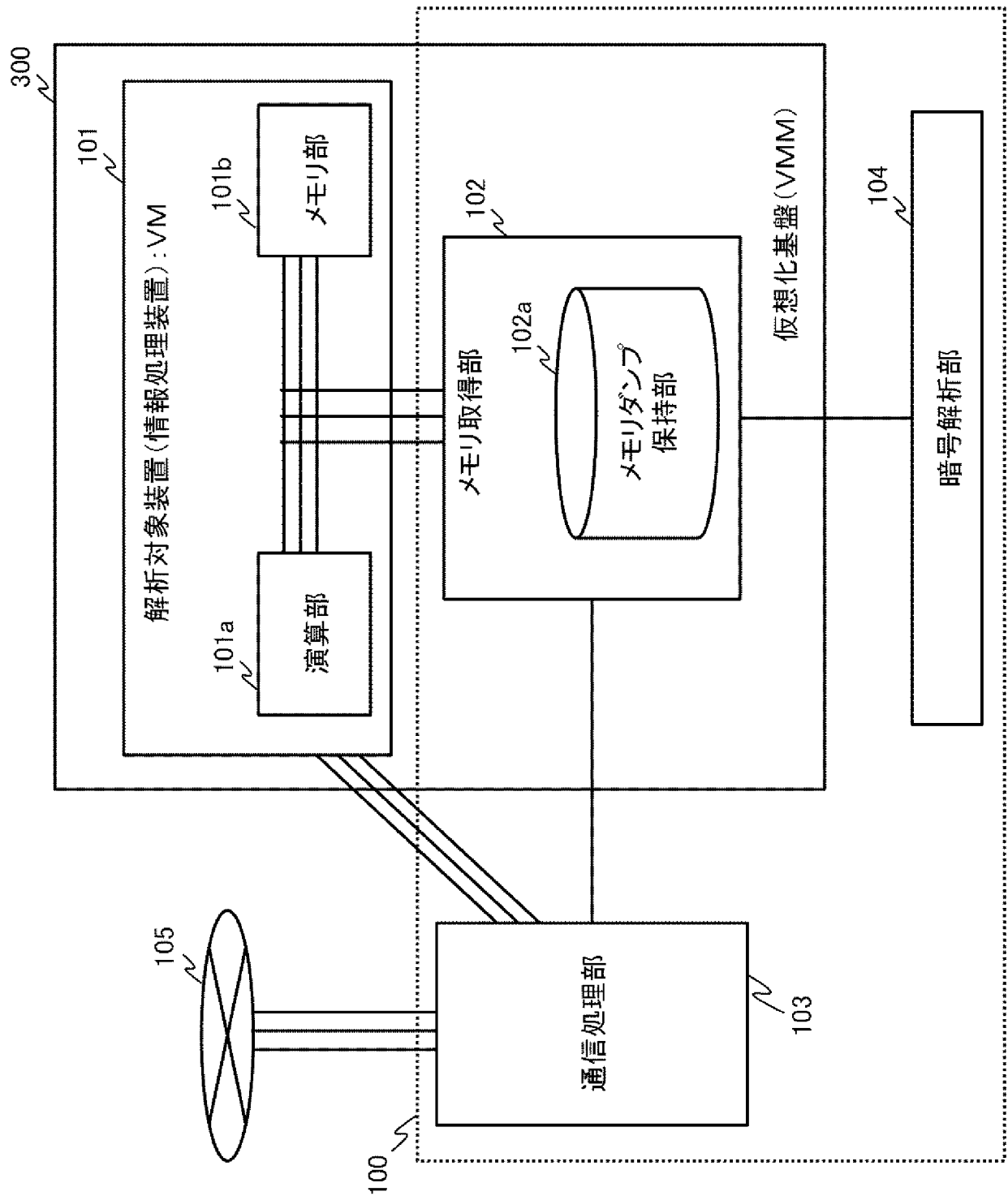
[図1]



[図2]



[図3]



[図4]

鍵データ取得ポリシー		
暗号通信 プロトコル	鍵データ取得基準	処理内容
SSL/TLS	(SSL/TLSサーバーからChangeCipherSpec が送信された後)、かつ、 (Application Dataの送受信が開始する前)	メモリ取得部にメモリを取得するよう指示する。 通信制御部に、通信の一時停止を指示する。
SSH	(SSH2_MSG_NEWKEYSが送受信された 後)	メモリ取得部にメモリを取得するよう指示する。 通信制御部に、通信の一時停止を指示する。
IPSec (IKE)	...	...
...	...	...

103c
~403
~402
~401
~

[図5]

103e
~

通信データ記録ポリシー		
501 ~	502 ~	503 ~
暗号通信 プロトコル	通信データ記録基準	処理内容
SSL/TLS	(Application Dataの送受信が開始された後)	通信データを発信者ごとに記録する。 各通信データについて、発信元、及び、 取得時刻を記録する。
SSH	...	...
IPSec (IKE)	...	...
...	...	...

[図6]

103f
~

通信データ保持部

601
~

602
~

603
~

発信元	暗号通信 プロトコル	記録データ
クライアント (情報通信装置)	SSL/TLS	時刻:YYYYMMDD-hh1mm1ss1 データ:XXXXXXXXX 時刻:YYYYMMDD-hh2mm2ss2 データ:XXXXXXXXX
サーバ	SSL/TLS	時刻:YYYYMMDD-hh3mm3ss3 データ:XXXXXXXXX 時刻:YYYYMMDD-hh4mm4ss4 データ:XXXXXXXXX
...	...	...
...	...	...

[図7]

鍵候補判定情報				
暗号 アルゴリズム	暗号パラメータ		実行環境情報	鍵候補判定基準
	鍵長 (単位: bit)	暗号利用 モード		
AES	128	CBC	A	エントロピーが特定の基準値以上である、 連続した16バイトのデータ領域
AES	256	CBC	B	エントロピーが特定の基準値以上である、 連続した32バイトのデータ領域
AES	128	GCM	C	0x30,0x02,0x00,0x00,0x4b,0x53,0x53,0x4Dから 開始する連続した560バイトのデータ
...	...	...	...	...

104b

704

703

702

701

[図8]

104c

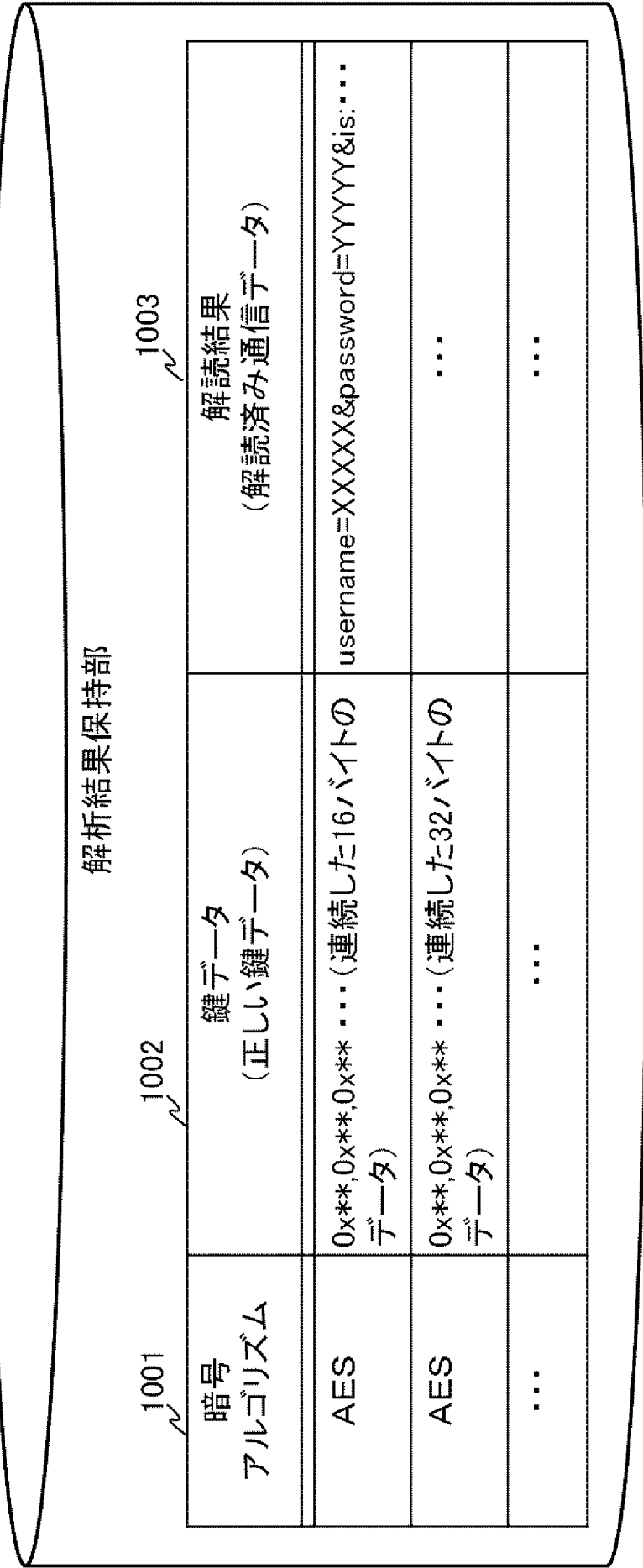
鍵候補保持部			
暗号 アルゴリズム	暗号パラメータ		鍵データ候補
	鍵長 (単位: bit)	モード	
AES	128	CBC	0x**,0x**,0x** ... (連続した16バイトのデータ)
AES	256	CBC	0x**,0x**,0x** ... (連続した32バイトのデータ)
AES	128	GCM	0x30,0x02,0x00,0x00,0x4b,0x53,0x53,0x4D... (連続した560バイトのデータ)
...	...	...	...

[図9]

解析結果判定情報	
901 解析結果判定基準	902 判定結果
(復号処理結果のエントロピー) $\leq$ (特定の基準値)	解読成功
(復号処理結果のエントロピー) $>$ (特定の基準値)	解読失敗
復号処理結果に含まれるペイロードの先頭4バイトが "GET"	解読成功
...	...

[図10]

104f



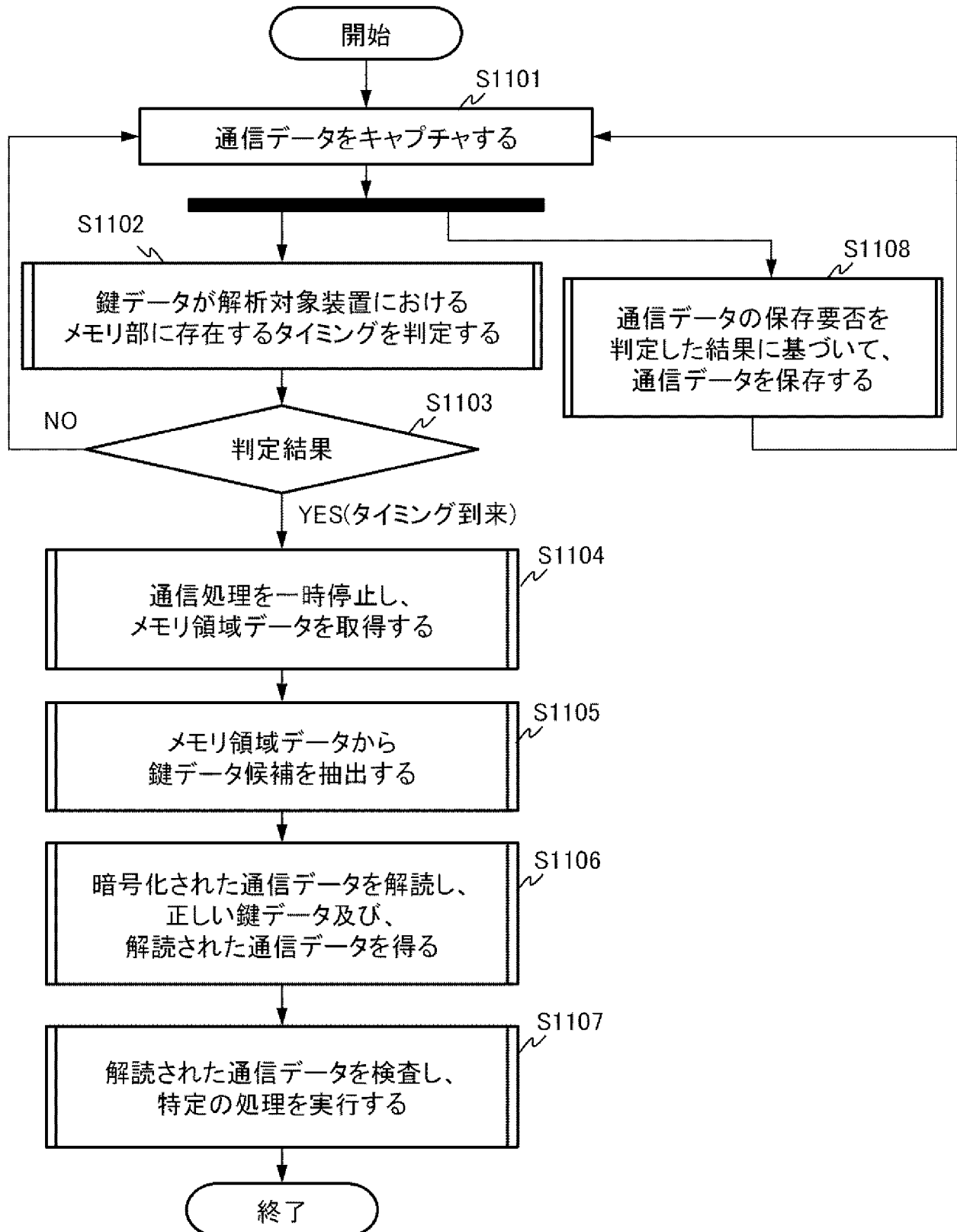
解析結果保持部

1001

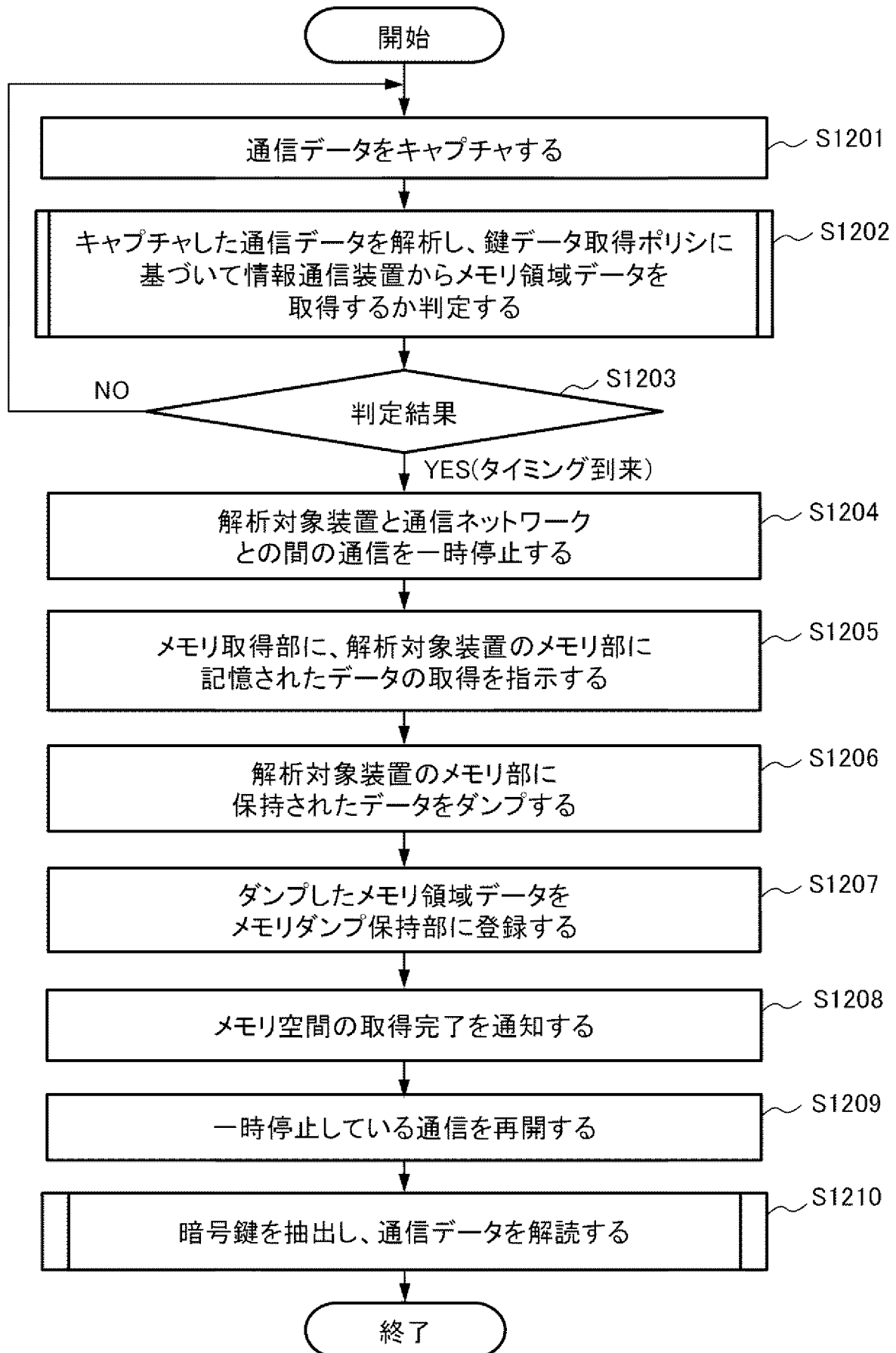
1002

1003

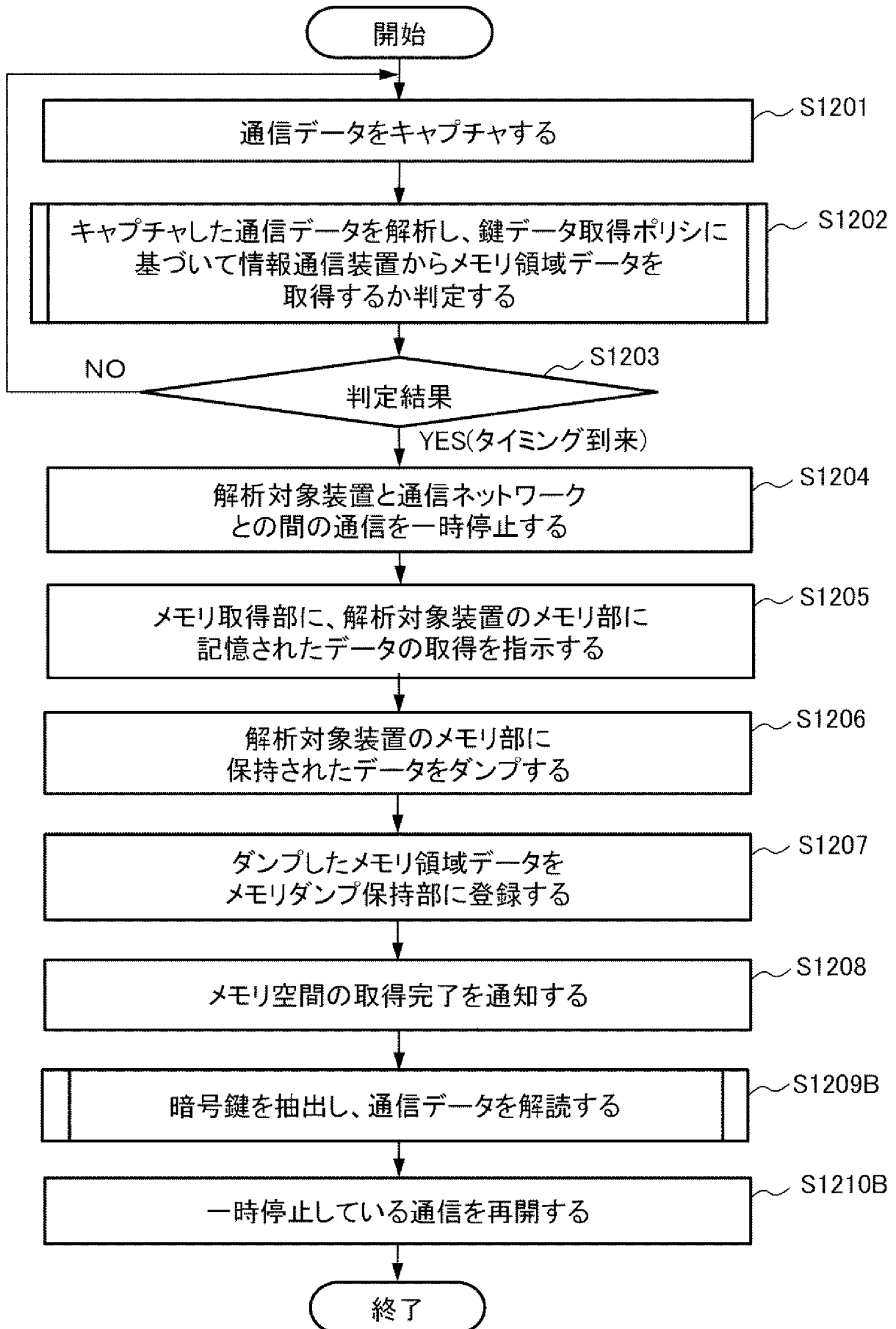
[図11]



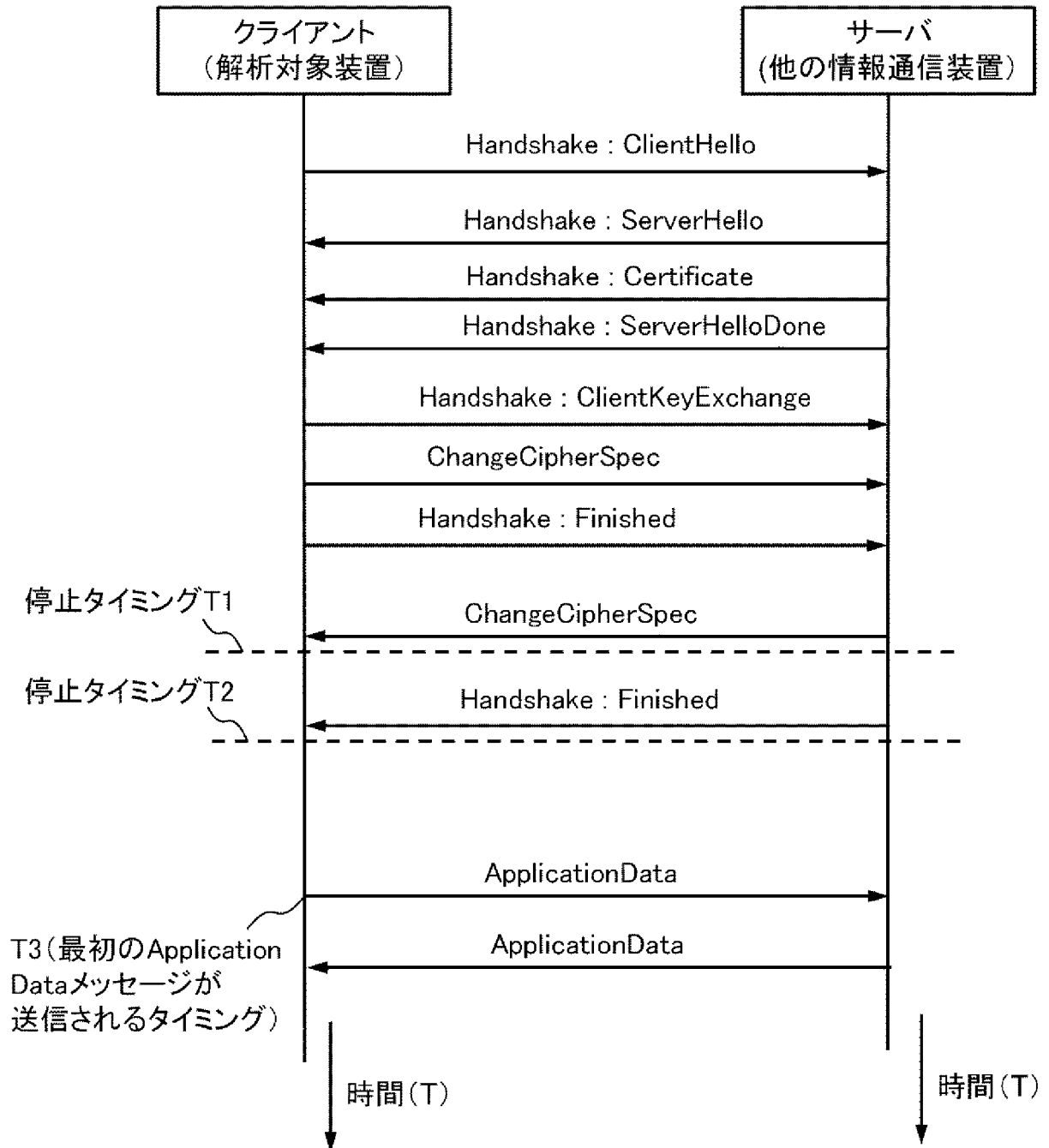
[図12A]



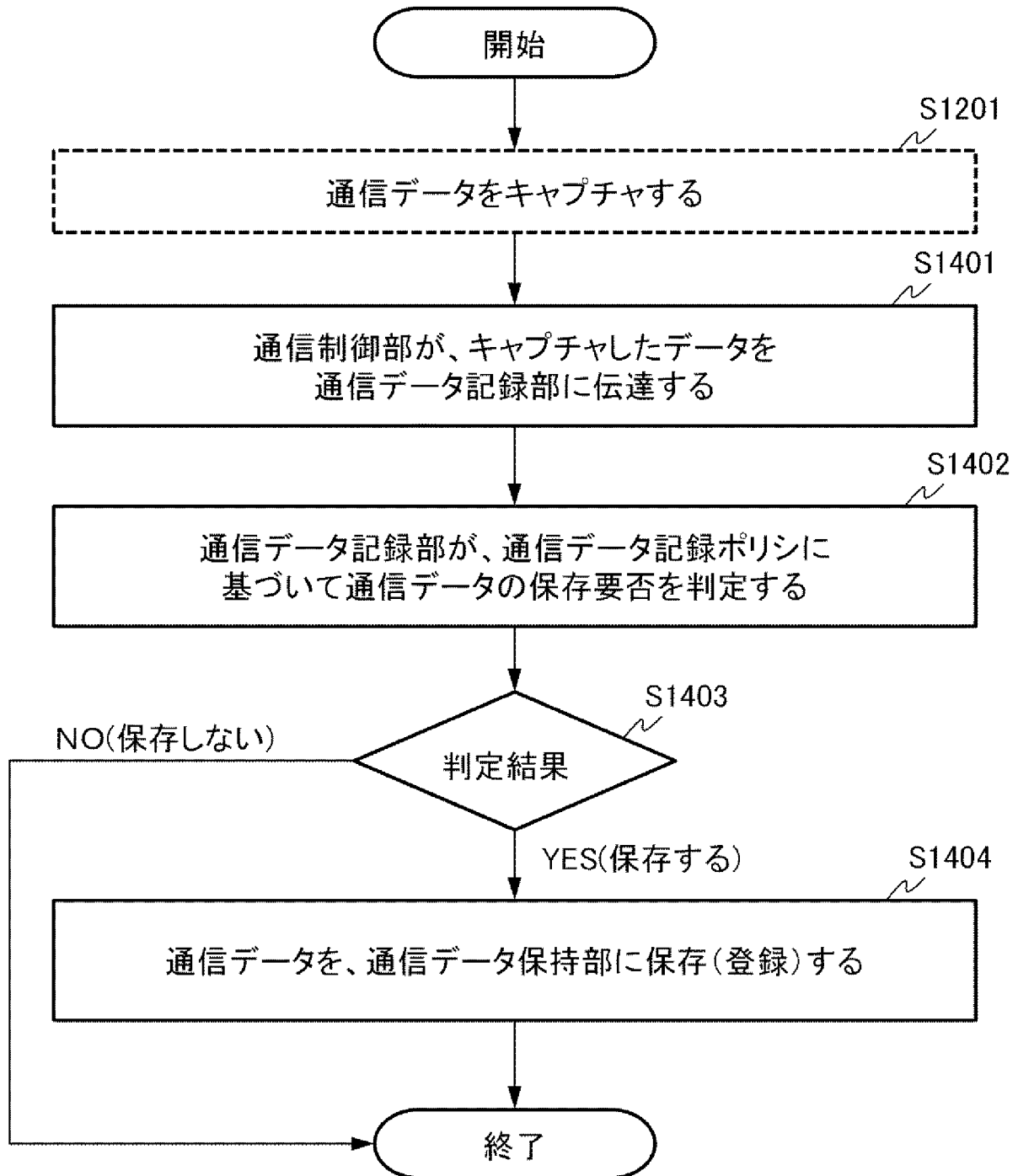
[図12B]



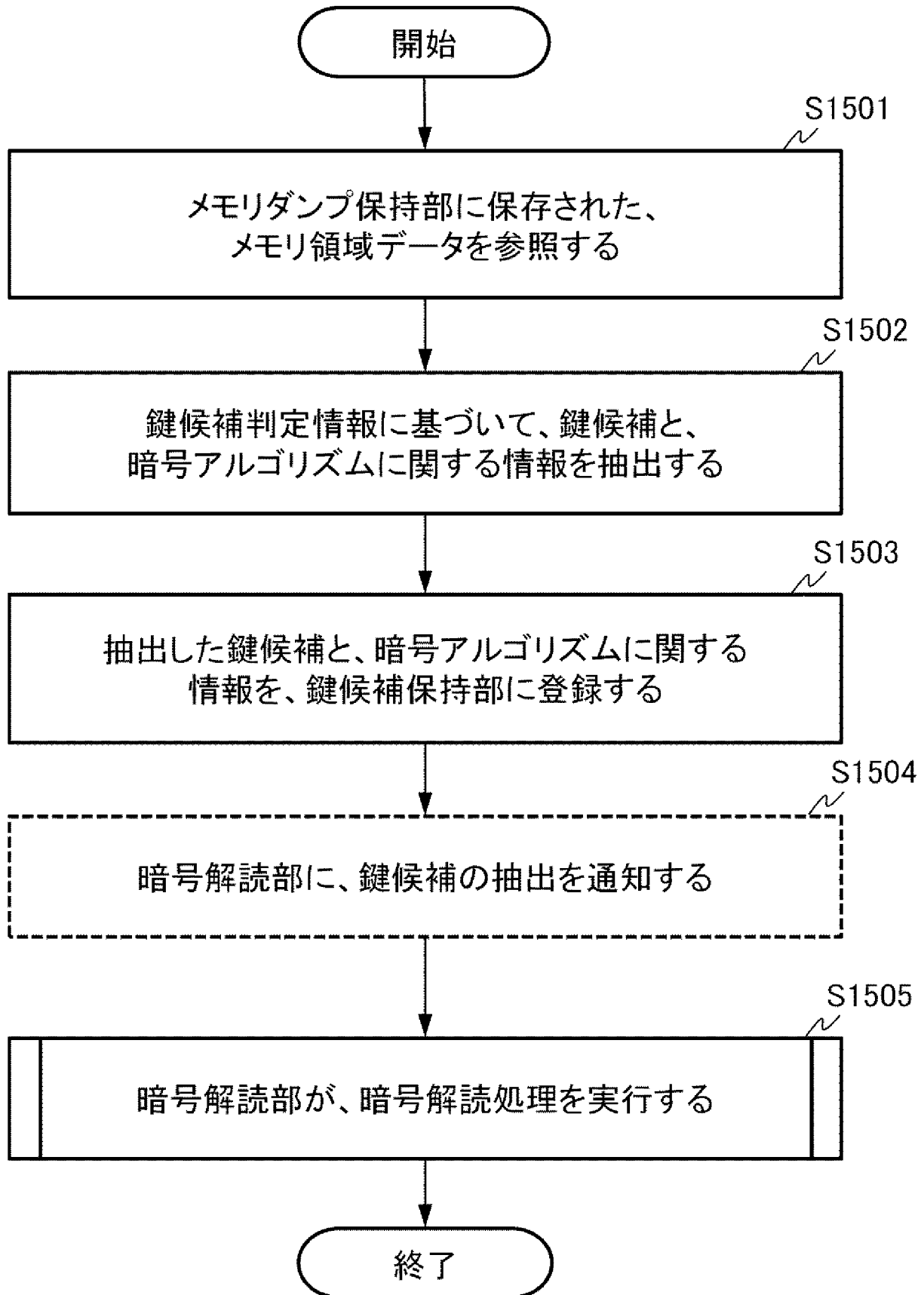
[図13]



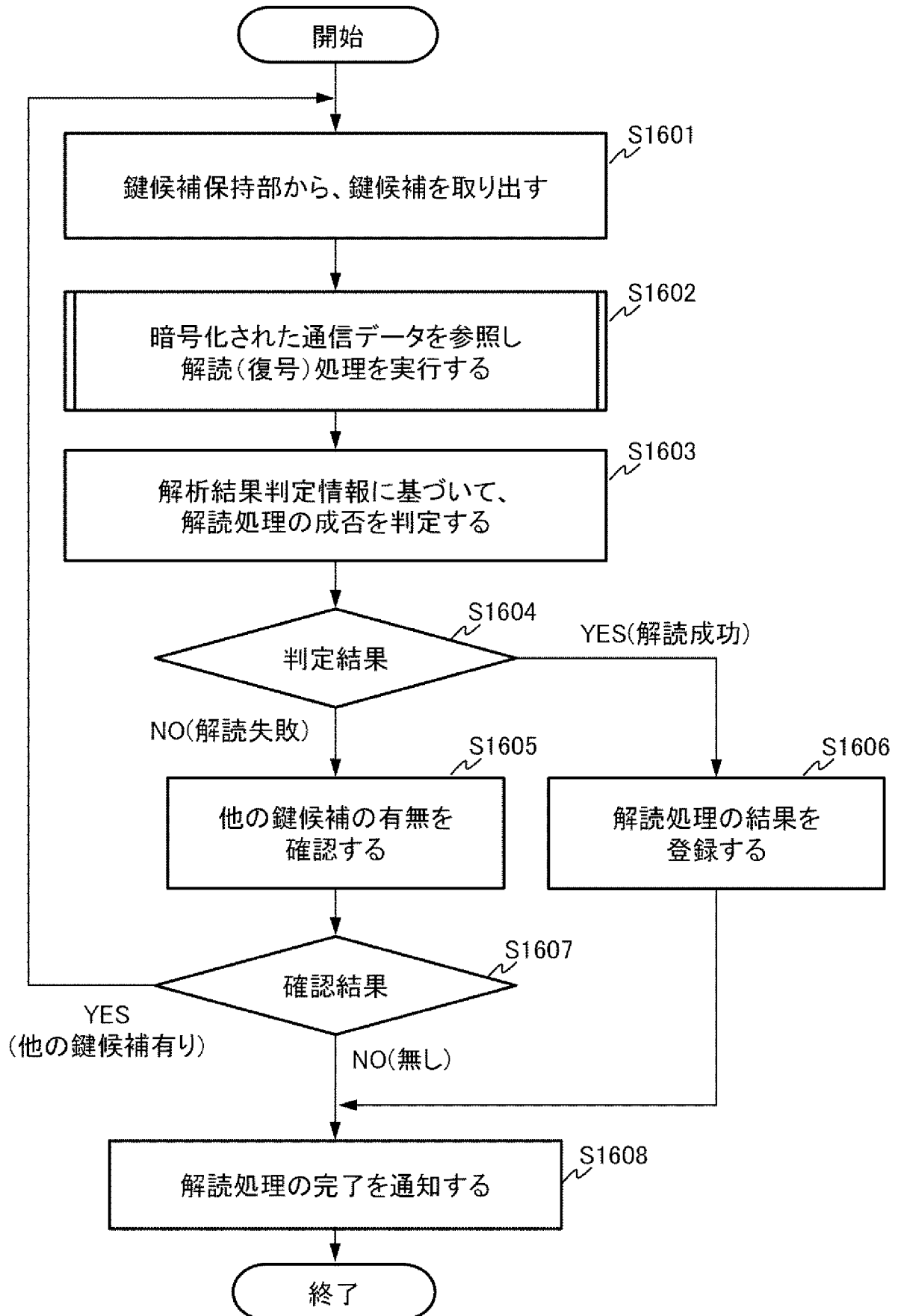
[図14]



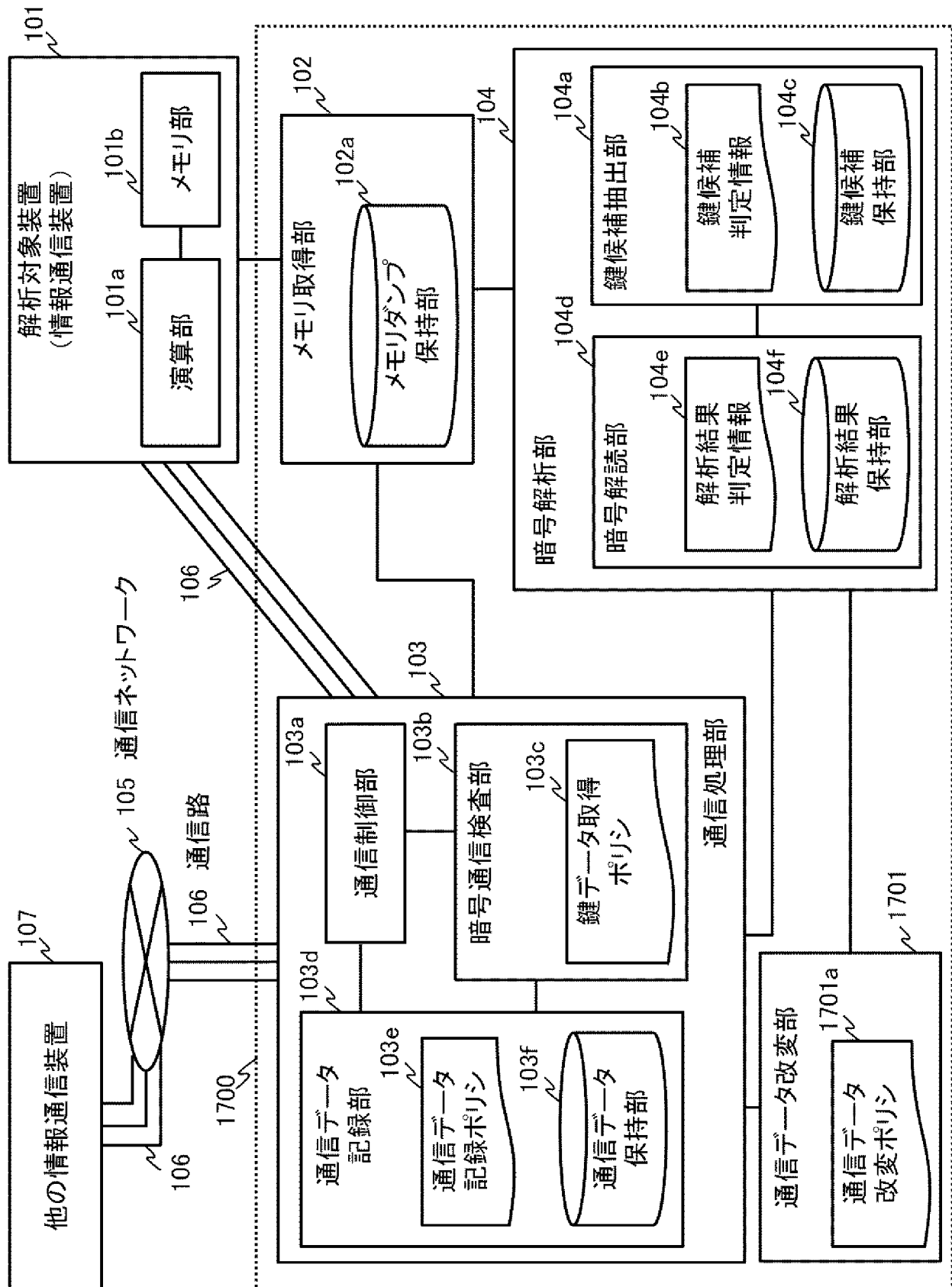
[図15]



[図16]



[図17]

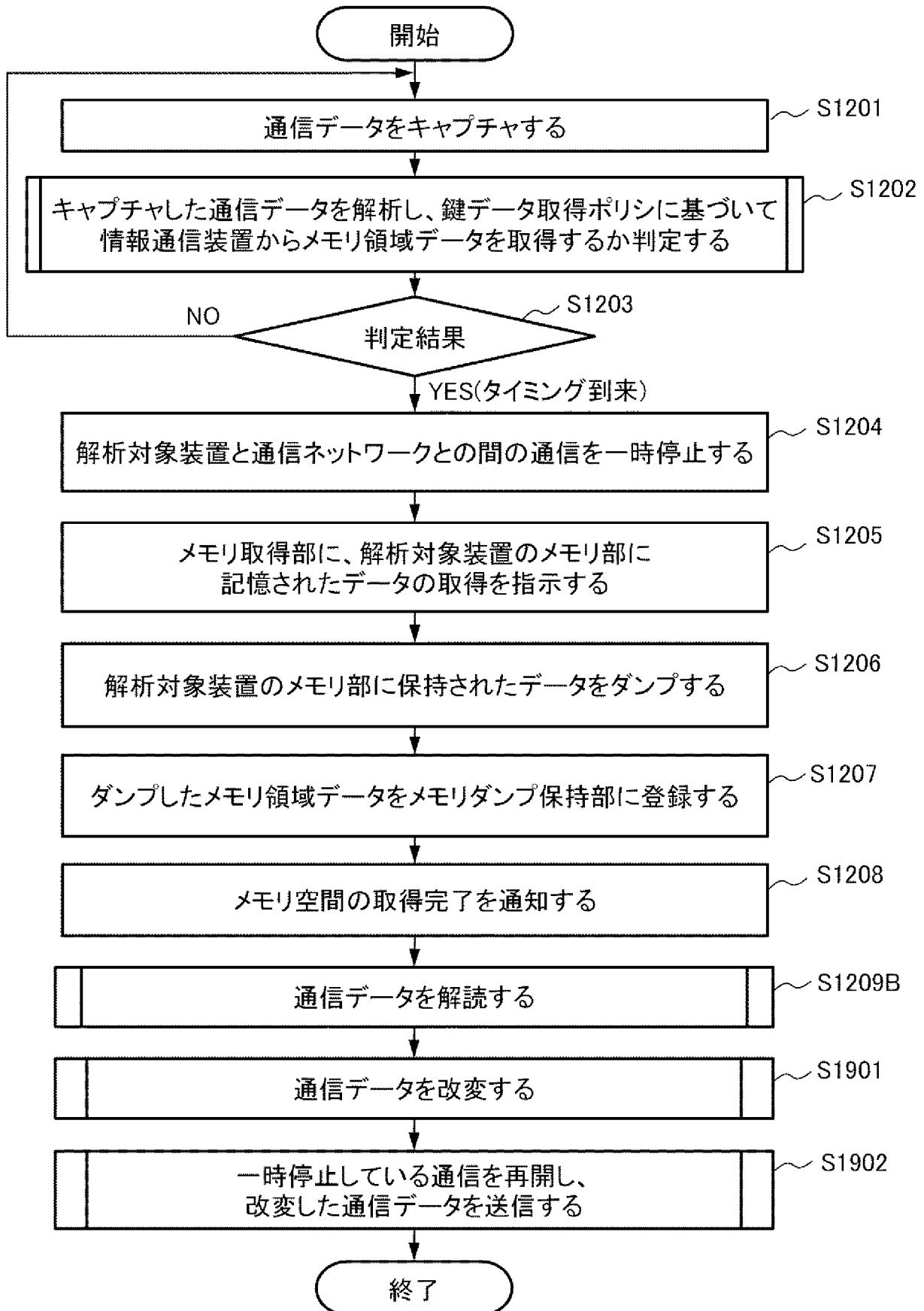


[図18]

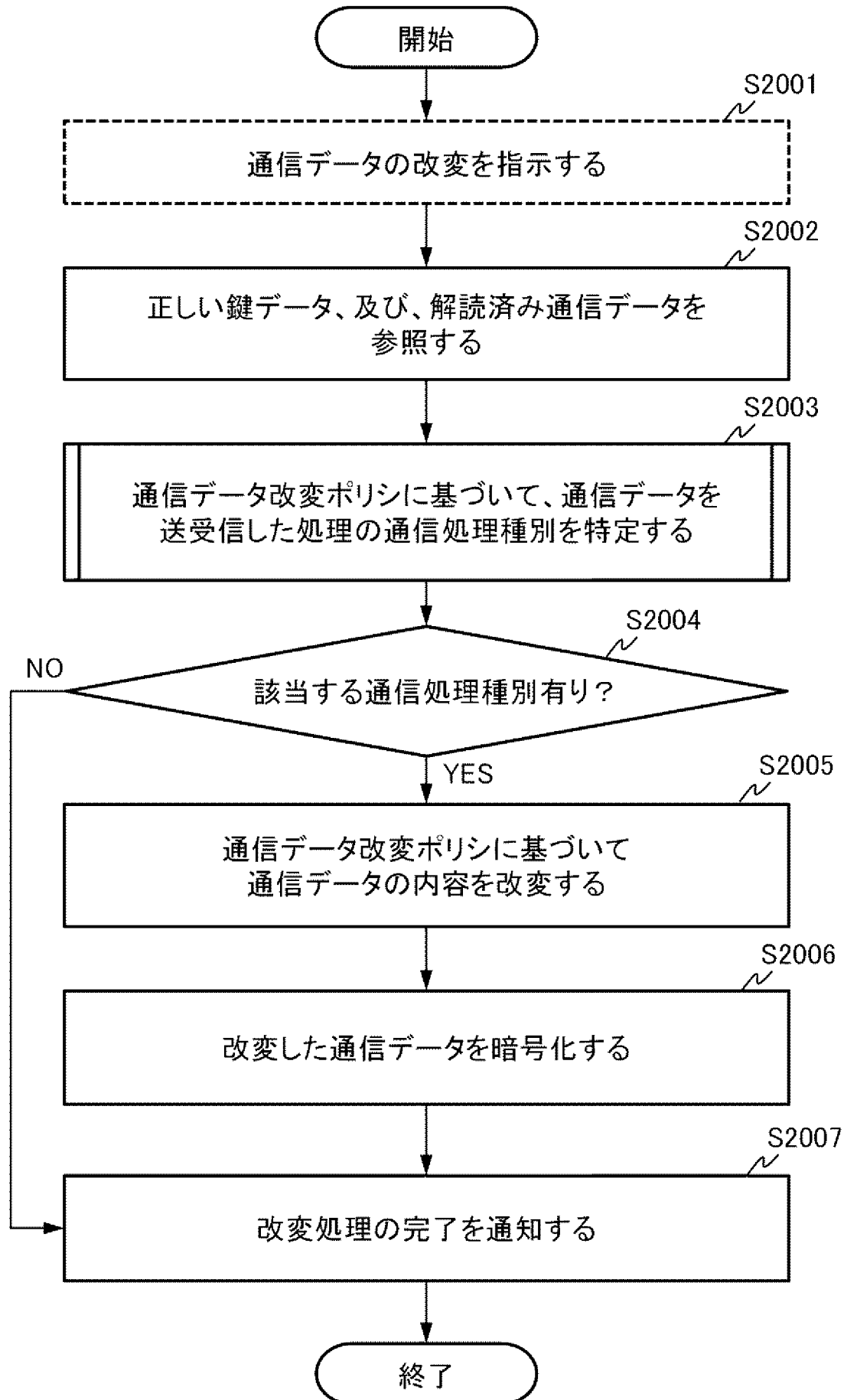
通信データ改変ポリシー				
1801 通信処理種別	1802 通信元	1803 通信先	1804 判定基準	1805 改変情報
マルウェアXによる認証処理	ローカルネットワーク	インターネット	・(通信先IPアドレス) = aaa.bbb.ccc.dd ・通信データの先頭Nバイトに” GET /login.cgi ”という文字列が含まれる	・通信データに含まれるユーザID相当部分(”username”)を、”AAAA”に変更する。 ・認証情報相当部分(”password”)を”BBBB”に変更する。
...	...	...	...	...

1701a

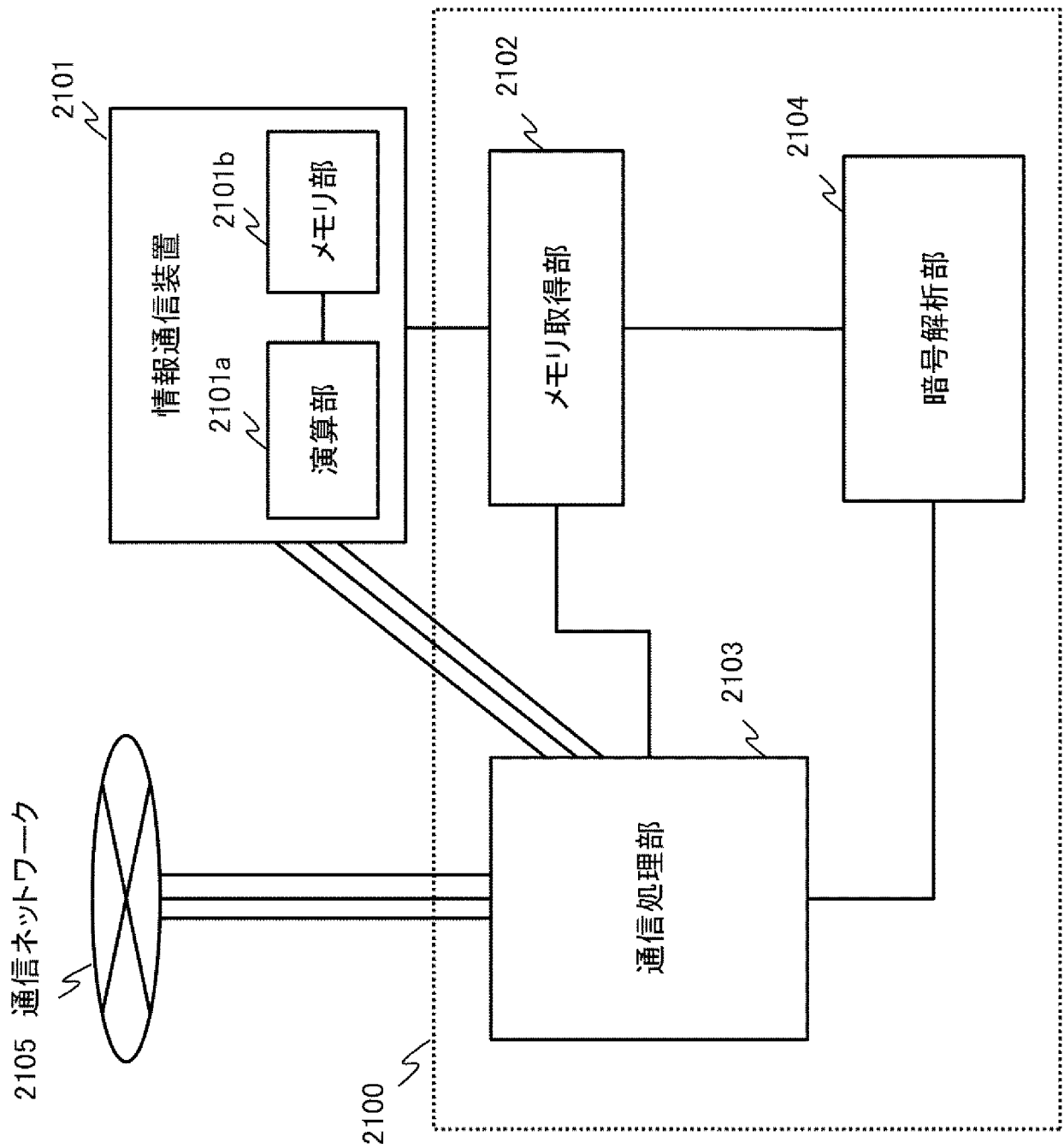
[図19]



[図20]



[図21]



[図22]

