(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0013940
(43) 공개일자 2008년02월13일

(51) Int. Cl.
G06F 9/44 (2006.01) *G06F 21/22* (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2007-7027514
(22) 출원일자 2007년11월26일
심사청구일자 없음
번역문제출일자 2007년11월26일
(86) 국제출원번호 PCT/JP2006/310764
국제출원일자 2006년05월30일
(87) 국제공개번호 WO 2006/129654
국제공개일자 2006년12월07일
(30) 우선권주장
JP-P-2005-00161358 2005년06월01일 일본(JP)

(71) 출원인
마츠시타 덴끼 산교 가부시키가이샤
일본 오오사카후 가도마시 오오아자 가도마 1006
(72) 발명자
마츠시마 히데키
일본국 오오사카후 가도마시 오오아자가도마 1006 마츠시타 덴끼산교 가부시키가이샤나이
가가와 다카후미
일본국 가나가와켄 요코하마시 즈즈키쿠 사에도쵸 600 파나소닉모바일 커뮤니케이션즈 가부시키가이샤나이
(뒷면에 계속)
(74) 대리인
김영철

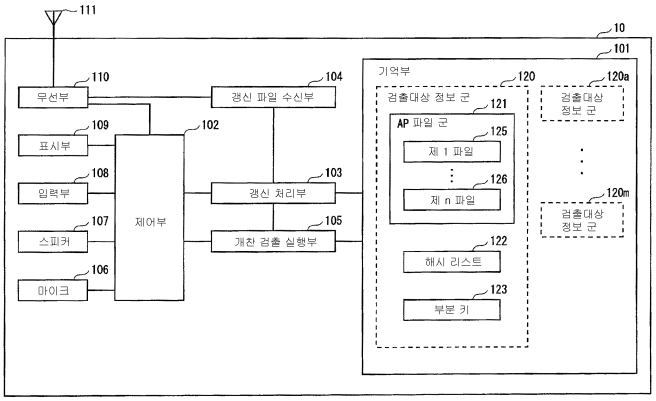
전체 청구항 수 : 총 35 항

(54) 전자기기, 갱신 서버장치, 키 갱신장치

(57) 요 약

소프트웨어에 관한 파일을 갱신하는 경우에 통신에 관한 데이터량을 종래보다도 억제할 수 있고, 또한, 개찬검출을 행하는 전자기기를 제공한다. 애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일을 가지며, 네트워크를 통해서 상기 애플리케이션 파일을 갱신하는 전자기기로, 하나 이상의 데이터로 이루어지는 애플리케이션 파일을 기억하며, 갱신데이터와, 상기 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 상기 네트워크를 통해서 외부장치로부터 수신하여, 상기 위치정보가 나타내는 위치에 존재하는 데이터를 상기 갱신데이터로 재기록하여 상기 애플리케이션 파일의 일부만을 갱신하고, 갱신된 상기 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행한다.

대표도 - 도2



(72) 발명자

하가 도모유키

일본국 오오사카후 가도마시 오오아자가도마 1006 마츠시타 덴끼산교 가부시키가이샤나이

오쿠야마 히로시

일본국 가나가와켄 요코하마시 즈즈키쿠 사에도쵸 600 파나소닉모바일 커뮤니케이션즈 가부시키가이샤나이

기무라 시게히코

일본국 오오사카후 가도마시 오오아자가도마 1006 마츠시타 덴끼산교 가부시키가이샤나이

오이와 야스키

일본국 가나가와켄 요코하마시 즈즈키쿠 사에도쵸 600 파나소닉모바일 커뮤니케이션즈 가부시키가이샤나이

이토 요시카츠

일본국 오오사카후 가도마시 오오아자가도마 1006 마츠시타 덴끼산교 가부시키가이샤나이

특허청구의 범위

청구항 1

애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일을 가지며, 네트워크를 통해서 상기 애플리케이션 파일을 갱신하는 전자기기로,

하나 이상의 데이터로 이루어지는 애플리케이션 파일을 기억하고 있는 기억수단과,

갱신데이터와, 상기 애플리케이션 파일에서 상기 갱신데이터에 의해서 갱신하는 위치를 나타내는 위치정보를 상기 네트워크를 통해서 외부장치로부터 수신하는 수신수단과,

상기 위치정보가 나타내는 위치에 존재하는 데이터를 상기 갱신데이터로 재기록(rewrite)하여 상기 애플리케이션 파일의 일부만을 갱신하는 갱신처리수단과,

갱신된 상기 애플리케이션 파일이 개찬(tampering)되어 있는가 여부의 확인을 행하는 개찬검출 실행수단을 구비하는 것을 특징으로 하는 전자기기.

청구항 2

제 1 항에 있어서,

상기 수신수단은 갱신데이터와 위치정보의 세트를 적어도 하나 이상 수신하고,

상기 갱신처리수단은,

상기 위치정보에서 나타내는 위치에 의거하여 상기 애플리케이션 파일의 갱신위치를 결정하는 위치 결정부와,

결정된 상기 갱신위치를 상기 갱신데이터의 기록개시위치로 하여 상기 갱신데이터를 기록하는 기록부와,

상기 수신수단에서 수신한 하나 이상의 모든 갱신데이터의 기록이 완료할 때까지 상기 위치 결정부와 상기 기록부의 처리를 행하도록 제어하는 갱신제어부를 구비하는 것을 특징으로 하는 전자기기.

청구항 3

제 2 항에 있어서,

상기 갱신제어부는, 모든 갱신데이터의 기록이 완료하면, 상기 개찬검출 실행수단의 처리를 개시하도록 제어하는 것을 특징으로 하는 전자기기.

청구항 4

제 3 항에 있어서,

상기 갱신처리수단은,

애플리케이션 파일이 갱신 중임을 나타내는 제 1 정보 또는 갱신 중이 아님을 나타내는 제 2 정보 중 어느 하나를 나타내는 플래그를 기억하고 있는 플래그 기억부와,

상기 플래그가 나타내는 정보를 변경하는 플래그 변경부를 더 구비하고,

상기 플래그 변경부는, 상기 수신수단이 갱신데이터와 위치정보의 세트를 적어도 하나 이상 수신한 때에 상기 플래그의 정보를 상기 제 1 정보로 변경하고, 상기 개찬검출 실행수단에서 개찬이 검출되지 않은 경우에 상기 플래그의 정보를 상기 제 2 정보로 변경하는 것을 특징으로 하는 전자기기.

청구항 5

제 4 항에 있어서,

상기 갱신제어부는, 상기 전자기기에 전원이 투입되면 상기 플래그가 나타내는 정보를 확인하고, 제 1 정보인 경우에는 상기 위치 결정부와 상기 기록부의 처리를 행하도록 제어하는 것을 특징으로 하는 전자기기.

청구항 6

제 3 항에 있어서,

상기 애플리케이션 파일은 하나 이상의 블록으로 분할되어 있고,

상기 갱신데이터는 상기 하나 이상의 블록 중 적어도 하나 이상의 갱신대상 블록에 포함되며,

상기 기억수단은 하나 이상의 상기 블록 각각에 대한 기준 개찬검출 값을 갖는 개찬검출 리스트를 기억하고 있고,

상기 수신수단은, 하나 이상의 상기 갱신대상 블록 각각에 대한 새로운 기준 개찬검출 값과, 상기 하나 이상의 상기 갱신대상 블록 각각에 대한 기준 개찬검출 값의 상기 개찬검출 리스트에서의 위치를 나타내는 개찬 검출 위치정보로 이루어지는 세트를 더 수신하며,

상기 갱신처리수단은 하나 이상의 새로운 기준 개찬검출 값과 상기 개찬검출 값 위치정보를 이용하여 상기 개찬검출 리스트를 더 갱신하고,

상기 개찬검출 실행수단은 상기 갱신된 개찬검출 리스트가 정당한 것인 경우에만 상기 갱신된 개찬검출 리스트가 갖는 적어도 하나 이상의 기준 개찬검출 값에 의거하여 개찬검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인하는 것을 특징으로 하는 전자기기.

청구항 7

제 1 항에 있어서,

상기 애플리케이션 파일은 하나 이상의 블록으로 분할되어 있고,

상기 기억수단은 하나 이상의 상기 블록 각각에 대한 기준 개찬검출 값을 갖는 개찬검출 리스트를 기억하고 있으며,

상기 개찬검출 실행수단은, 상기 애플리케이션 소프트웨어의 기동시에 처리를 개시하고, 상기 개찬검출 리스트가 정당한 것인 경우에만 상기 개찬검출 리스트가 갖는 적어도 하나 이상의 개찬검출 값에 의거하여 개찬 검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인하는 것을 특징으로 하는 전자기기.

청구항 8

제 7 항에 있어서,

상기 개찬검출수단은, 개찬검출대상인 블록에 대한 검출용 개찬검출 값을 산출하고, 산출한 검출용 개찬검출 값과 개찬검출대상인 블록에 대한 개찬검출 값이 일치하는가 여부를 판단하며, 일치한다고 판단한 경우에는 상기 애플리케이션 파일은 개찬되어 있지 않은 것으로 하고, 일치하지 않는 경우에는 상기 애플리케이션 파일은 개찬되어 있는 것으로 하는 것을 특징으로 하는 전자기기.

청구항 9

제 8 항에 있어서,

상기 기억부는 부분 키(partial key)를 기억하고 있고,

상기 개찬검출 실행수단은, 내 탬퍼화(tamper resistant) 되어 있으며, 마스터 키(master key)를 기억하고, 상기 부분 키와 상기 마스터 키를 이용하여 개찬검출 키를 생성하며, 생성한 개찬검출 키를 이용하여 상기 검출용 개찬검출 값을 산출하는 것을 특징으로 하는 전자기기.

청구항 10

제 9 항에 있어서,

상기 수신수단은 상기 부분 키와는 다른 부분 키(new partial key)와 상기 부분 키가 상기 기억부에 기억되어 있는 위치를 나타내는 키 위치정보를 수신하고,

상기 갱신처리수단은 상기 키 위치정보에 의거하여 상기 부분 키를 상기 다른 부분 키로 갱신하는 것을 특징으로 하는 전자기기.

청구항 11

제 7 항에 있어서,

상기 개찬검출 리스트는 상기 하나 이상의 블록 각각에 대한 기준 개찬검출 값을 포함하는 데이터부와 상기 데이터부에 대한 기준 데이터부 개찬검출 값을 포함하는 헤더부로 구성되며,

상기 개찬검출 실행수단은, 상기 데이터부에 대한 검출용 데이터부 개찬검출 값을 산출하고, 산출한 상기 검출용 데이터부 개찬 검출과 상기 기준 데이터부 개찬검출 값이 일치하는 경우에 상기 개찬검출 리스트가 정당한 것으로 하는 것을 특징으로 하는 전자기기.

청구항 12

제 11 항에 있어서,

상기 데이터부는 암호화되어 있고,

상기 개찬검출 실행수단은, 암호화된 상기 데이터부에 대한 검출용 개찬검출 값을 산출하며, 상기 개찬검출 리스트가 정당한 것인 경우에 암호화된 상기 데이터부를 복호 하는 것을 특징으로 하는 전자기기.

청구항 13

제 7 항에 있어서,

상기 개찬검출 리스트에서, 기준 개찬검출 값의 각각에 대해서, 대응하는 블록이 개찬 검출의 대상으로서 사용해야 하는가 여부를 나타내는 판단정보와 대응이 부여되어 있고,

상기 개찬검출 실행수단은 상기 판단정보가 블록을 개찬검출의 대상으로 하지 않는다는 취지를 나타내는 경우에는 당해 블록에 대한 개찬검출은 행하지 않는 것을 특징으로 하는 전자기기.

청구항 14

제 7 항에 있어서,

상기 개찬검출 리스트는 상기 하나 이상의 블록 각각에 대한 기준 개찬검출 값과 개찬검출의 대상이 되는 애플리케이션 소프트웨어의 종별을 나타내는 애플리케이션 종별을 상호 대응시킨 세트를 하나 이상 포함하고,

상기 개찬검출 실행수단은 기동 된 애플리케이션 소프트웨어에 대한 애플리케이션 종별에 대응하는 기준 개찬검출 값의 각각 중 적어도 하나 이상의 개찬검출 값에 의거하여 개찬검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인하는 것을 특징으로 하는 전자기기.

청구항 15

제 7 항에 있어서,

상기 애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일은 복수 개 있고,

상기 애플리케이션 파일 각각은 하나 이상의 블록으로 분할되어 있으며,

상기 개찬검출 리스트는, 애플리케이션 파일 각각에 대하여 하나 이상의 블록 각각에 대한 기준 개찬검출 값을 기준 값 군으로 하여 저장하고, 하나 이상의 상기 기준 값 군 중 상기 애플리케이션 소프트웨어의 기동시에 개찬 검출에 이용하는 적어도 하나 이상의 기준 값 군의 범위를 나타내는 범위정보를 가지며,

상기 개찬검출 실행수단은, 상기 애플리케이션 소프트웨어의 기동시에, 상기 개찬검출 리스트가 갖는 상기 범위정보에서 나타내는 적어도 하나 이상의 기준 값 군을 이용하여 개찬검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인하는 것을 특징으로 하는 전자기기.

청구항 16

제 2 항에 있어서,

상기 갱신처리수단 및 상기 개찬검출 실행수단은 내 탬퍼화 되어 있는 것을 특징으로 하는 전자기기.

청구항 17

네트워크를 통해서 전자기기에 대해서, 상기 전자기기가 가지며, 하나 이상의 데이터로 이루어지는 애플리케이션 파일의 갱신을 행하게 하는 갱신 서버장치로,

갱신 후의 애플리케이션 파일을 취득하는 제 1 취득수단과,

취득한 상기 갱신 후의 애플리케이션 파일로부터 갱신데이터와 갱신 전의 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 취득하는 제 2 취득수단과,

취득한 상기 갱신데이터와 상기 위치정보를 상기 전자기기에 송신하는 송신수단을 구비하는 것을 특징으로 하는 갱신 서버장치.

청구항 18

제 17 항에 있어서,

상기 갱신 전의 애플리케이션 파일은 소정의 크기로 이루어지는 하나 이상의 갱신 전 블록으로 분할되어 있고,

상기 제 1 취득수단은 하나 이상의 상기 갱신 전 블록 각각 및 상기 갱신 전 블록 각각에 대한 기준 개찬검출 값으로 이루어지는 갱신 전 개찬검출 리스트를 더 취득하고,

상기 갱신 서버장치는, 상기 갱신 후의 애플리케이션 파일을 상기 소정의 크기로 분할한 하나 이상의 갱신 후 블록을 취득하고, 취득한 하나 이상의 갱신 후 블록 각각에 대하여 기준 개찬검출 값을 재계산하여 새로운 개찬검출 리스트를 생성하는 개찬검출 리스트 생성수단을 더 구비하며,

상기 제 2 취득수단은,

상기 개찬검출 리스트 생성수단에서 생성된 새로운 개찬검출 리스트에서 상기 갱신데이터를 포함하는 갱신 후 블록과, 그 갱신 후 블록에 대응하는 재계산된 기준 개찬검출 값과, 그 갱신 후 블록에 대응하는 갱신 전 블록의 상기 갱신 전 개찬검출 리스트에서의 위치를 나타내는 개찬검출 값 위치정보를 더 취득하고,

상기 송신수단은 상기 제 2 취득수단에서 취득된 갱신 후 블록과 상기 기준 개찬검출 값 및 상기 개찬검출 값 위치정보를 상기 전자기기에 더 송신하는 것을 특징으로 하는 갱신 서버장치.

청구항 19

제 18 항에 있어서,

상기 개찬검출 리스트 생성수단은, 외부장치에 의해서 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 기억하고 있고, 상기 개찬검출 키를 이용하여 상기 하나 이상의 갱신 후 블록 각각에 대한 기준 개찬검출 값을 산출하는 것을 특징으로 하는 갱신 서버장치.

청구항 20

제 19 항에 있어서,

상기 갱신 서버장치는, 상기 외부장치에 의해 갱신된 부분 키와 상기 마스터 키를 이용하여 갱신된 개찬검출 키를 수신하면, 기억하고 있는 상기 개찬검출 키를 수신한 상기 갱신된 개찬검출 키로 갱신하고, 또한, 상기 갱신된 부분 키를 상기 외부장치로부터 더 수신하며,

상기 개찬검출 리스트 생성수단은 상기 갱신된 개찬검출 키를 이용하여 상기 하나 이상의 갱신 후 블록 각각에 대한 기준 개찬검출 값을 산출하고,

상기 제 2 취득수단은 상기 전자기기에서 상기 부분 키가 기억되어 있는 위치를 나타내는 키 위치정보를 더 취득하며,

상기 송신수단은 상기 갱신된 부분 키와 상기 키 위치정보를 상기 전자기기에 더 송신하는 것을 특징으로 하는 갱신 서버장치.

청구항 21

제 19 항에 있어서,

상기 개찬검출 리스트는 상기 하나 이상의 갱신 후 블록 각각 및 상기 갱신 후 블록 각각에 대한 기준 개찬검출 값으로 이루어지는 데이터부를 가지며,

상기 개찬검출 리스트 생성수단은 생성한 새로운 개찬검출 리스트의 데이터부를 암호화하는 것을 특징으로 하는 갱신 서버장치.

청구항 22

제 21 항에 있어서,

상기 갱신 후 개찬검출 리스트는 헤더부를 가지며,

상기 개찬검출 리스트 생성수단은, 외부장치에 의해 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 기억하고 있고, 상기 개찬검출 키를 이용하여 암호화된 데이터부에 대한 데이터부 개찬검출 값을 산출하여, 산출한 데이터부 개찬검출 값을 상기 헤더부에 저장하는 것을 특징으로 하는 갱신 서버장치.

청구항 23

제 19 항에 있어서,

상기 개찬검출 리스트는 헤더부와 상기 하나 이상의 상기 갱신 후 블록 각각 및 상기 갱신 후 블록 각각에 대한 기준 개찬검출 값으로 이루어지는 데이터부를 가지며,

상기 개찬검출 리스트 생성수단은, 외부장치에 의해 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 기억하고 있고, 상기 개찬검출 키를 이용하여 상기 데이터부에 대한 데이터부 개찬검출 값을 산출하여, 산출한 데이터부 개찬검출 값을 상기 헤더부에 저장하는 것을 특징으로 하는 갱신 서버장치.

청구항 24

제 23 항에 있어서,

상기 개찬검출 리스트 생성수단은 상기 데이터부 개찬검출 값의 산출 후에 상기 데이터부를 암호화하는 것을 특징으로 하는 갱신 서버장치.

청구항 25

제 19 항에 있어서,

상기 갱신 서버장치는 외부의 개찬검출 리스트 생성장치를 상기 개찬검출 리스트 생성수단으로 이용하는 것을 특징으로 하는 갱신 서버장치.

청구항 26

하나 이상의 블록으로 분할된 애플리케이션 파일에 대하여 블록별로 개찬검출 값을 산출하기 위해 이용되는 개찬검출 키를 생성하는 키 생성장치로,

상기 개찬검출 키는 마스터 키와 부분 키로부터 생성되고,

상기 키 생성장치는,

상기 마스터 키와 갱신된 부분 키를 취득하는 키 취득수단과,

상기 마스터 키와 상기 갱신된 부분 키를 이용하여 새로운 개찬검출 키를 생성하는 키 생성수단과,

상기 키 생성수단에 의해 생성된 개찬 검출 키를 상기 개찬 검출 값을 포함하는 개찬검출 리스트를 생성하는 외부장치에 배포하는 배포수단을 구비하는 것을 특징으로 하는 키 생성장치.

청구항 27

제 26 항에 있어서,

상기 배포수단은 상기 갱신된 부분 키를 상기 외부장치를 통해서 상기 애플리케이션 파일이 개찬되어 있는가 여

부의 확인을 행하는 전자기기에 배포하는 것을 특징으로 하는 키 생성장치.

청구항 28

애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일을 가지며, 네트워크를 통해서 상기 애플리케이션 파일을 갱신하는 전자기기에서 이용되는 갱신방법으로,

상기 전자기기는 하나 이상의 데이터로 이루어지는 애플리케이션 파일을 기억하고 있는 기억수단을 구비하며,

상기 갱신방법은,

갱신데이터와, 상기 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 상기 네트워크를 통해서 외부장치로부터 수신하는 수신스텝과,

상기 위치정보가 나타내는 위치에 존재하는 데이터를 상기 갱신데이터로 재기록하여 상기 애플리케이션 파일을 갱신하는 갱신처리스텝과,

갱신된 상기 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행하는 개찬검출 실행스텝을 포함하는 것을 특징으로 하는 갱신방법.

청구항 29

애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일을 가지며, 네트워크를 통해서 상기 애플리케이션 파일을 갱신하는 전자기기에서 이용되는 갱신프로그램으로,

상기 전자기기는 하나 이상의 데이터로 이루어지는 애플리케이션 파일을 기억하고 있는 기억수단을 구비하며,

상기 갱신프로그램은,

갱신데이터와, 상기 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 상기 네트워크를 통해서 외부장치로부터 수신하는 수신스텝과,

상기 위치정보가 나타내는 위치에 존재하는 데이터를 상기 갱신데이터로 재기록하여 상기 애플리케이션 파일을 갱신하는 갱신처리스텝과,

갱신된 상기 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행하는 개찬검출 실행스텝을 포함하는 것을 특징으로 하는 갱신프로그램.

청구항 30

제 29 항에 있어서,

상기 갱신프로그램은 컴퓨터 판독 가능한 기록매체에 기록되어 있는 것을 특징으로 하는 갱신프로그램.

청구항 31

네트워크를 통해서 전자기기에 대해서, 상기 전자기기가 가지며, 하나 이상의 데이터로 이루어지는 애플리케이션 파일의 갱신을 행하게 하는 갱신 서버장치에서 이용되고, 갱신에 필요한 정보를 취득하는 취득방법으로,

갱신 후의 애플리케이션 파일을 취득하는 제 1 취득스텝과,

취득한 상기 갱신 후의 애플리케이션 파일에서 갱신데이터와 갱신 전의 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 취득하는 제 2 취득스텝과,

취득한 상기 갱신데이터와 상기 위치정보를 상기 전자기기에 송신하는 송신스텝을 포함하는 것을 특징으로 하는 취득방법.

청구항 32

네트워크를 통해서 전자기기에 대해서, 상기 전자기기가 가지며, 하나 이상의 데이터로 이루어지는 애플리케이션 파일의 갱신을 행하게 하는 갱신 서버장치에서 이용되고, 갱신에 필요한 정보를 취득하는 취득프로그램으로,

갱신 후의 애플리케이션 파일을 취득하는 제 1 취득스텝과,

취득한 상기 갱신 후의 애플리케이션 파일에서 갱신데이터와 갱신 전의 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 취득하는 제 2 취득스텝과,

취득한 상기 갱신데이터와 상기 위치정보를 상기 전자기기에 송신하는 송신스텝을 포함하는 것을 특징으로 하는 취득프로그램.

청구항 33

제 32 항에 있어서,

상기 취득프로그램은 컴퓨터 판독 가능한 기록매체에 기록되어 있는 것을 특징으로 하는 취득프로그램.

청구항 34

애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일을 가지며, 네트워크를 통해서 상기 애플리케이션을 갱신하는 전자기기의 집적회로로,

상기 전자기기는 하나 이상의 데이터로 이루어지는 애플리케이션 파일을 기억하고 있는 기억수단을 구비하며,

상기 집적회로는,

갱신데이터와, 상기 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 상기 네트워크를 통해서 외부장치로부터 수신하는 수신수단과,

상기 위치정보가 나타내는 위치에 존재하는 데이터를 상기 갱신데이터로 재기록하여 상기 애플리케이션 파일의 일부만을 갱신하는 갱신처리수단과,

갱신된 상기 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행하는 개찬검출 실행수단을 구비하는 것을 특징으로 하는 집적회로.

청구항 35

네트워크를 통해서 전자기기에 대해서, 상기 전자기기가 가지며, 하나 이상의 데이터로 이루어지는 애플리케이션 파일의 갱신을 행하게 하는 갱신 서버장치의 집적회로로,

갱신 후의 애플리케이션 파일을 취득하는 제 1 취득수단과,

취득한 상기 갱신 후의 애플리케이션 파일에서 갱신데이터와 갱신 전의 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 취득하는 제 2 취득수단과,

취득한 상기 갱신데이터와 상기 위치정보를 상기 전자기기에 송신하는 송신수단을 구비하는 것을 특징으로 하는 집적회로.

명 세 서

기 술 분 야

<1> 전자기기가 보유하는 소프트웨어를 네트워크를 통해서 갱신하여 개찬(tempering)의 유무를 검출하는 기술에 관한 것이다.

배 경 기 술

<2> 프로그램의 부정한 개찬이나 해석을 방지하는 기술은 종래로부터 연구되고 있다. 예를 들어, 비 특허문헌 1에는 소프트웨어의 해석을 방지하기 위한 기본 원칙이나 구체적인 수법에 관하여 기술되어 있다. 또, 비 특허문헌 2에는 소프트웨어의 해석을 방지하기 위한 툴로 개발한 TRCS(Tamper Resistant Coding System)의 기술과제와 그 대책에 대하여 기술되어 있다. 이와 같은 소프트웨어의 부정한 해석이나 개찬을 방지하는 기술을 「내 탬퍼 기술(tamper resistant technologies)」이라고 한다. 이하에서는, 부정한 개찬을 단순히 「개찬」이라고 하고, 정당한 개찬을 「갱신」이라고 한다.

<3> 이상과 같은 내 탬퍼 기술은 이미 실용화되고 있다. 예를 들어, PC 상에서 시판의 DVD 콘텐츠를 재생하는 소프트웨어가 그것이다. DVD의 콘텐츠는 부정 복제를 방지하기 위하여 암호화되어 있고, 이를 재생하려고 하면 복호

화를 하기 위한 키가 필요하다. 이 키가 악의가 있는 사용자의 손에 들어가면 DVD 콘텐츠는 용이하게 복제되어 인터넷을 통해서 부정하게 퍼질 가능성이 있다. 따라서 전술한 소프트웨어는 내 탬퍼 기술에 의해 보호되고 있다.

<4> 이와 같이, 최근 DVD로 대표되도록 디지털 콘텐츠가 보급하고, 이들을 컴퓨터와 같은 사양의 공개된 시스템상에서 재생하는 소프트웨어에는 내 탬퍼 기술이 필요불가결로 되어있다.

<5> 휴대전화 등의 전자기기에서도 내 탬퍼 기술의 적용이 행해지고 있다. 특허문헌 1에서는 전자기기 내의 메모리에 대한 개찬을 방지하기 위하여 해시 함수(hash function)를 이용한 내 탬퍼 기술의 하나인 개찬검출방식이 개시되어 있다.

<6> 또, 최근 휴대전화를 비롯한 전자기기는 네트워크화가 진행하여, 이미 내장된 소프트웨어에 대하여 제품의 출하 후에도 문제를 수정하는 소프트웨어를 네트워크를 통해서 배포하여 갱신할 수 있게 되어 있다.

<7> 비 특허문헌 1 : 「역 해석이나 개변으로부터 소프트웨어를 보호한다」 닛케이 일렉트로닉스 1998.1.5(P209-220)

<8> 비 특허문헌 2 : 「소프트웨어의 내 탬퍼화 기술」 후지 제록스 테크니컬 리포트 No.13(P20-28)

<9> 특허문헌 1 : 일본국 특표 2001-500293호 공보

<10> 특허문헌 2 : 일본국 특표 2005-018725호 공보

<11> 개찬검출을 행하는 전자기기가 네트워크를 통해서 소프트웨어를 갱신하는 경우, 갱신된 소프트웨어 자체가 네트워크를 통해서 전자기기에 배포되므로, 갱신된 소프트웨어의 사이즈가 커지면 커질수록 전자기기가 갱신된 소프트웨어를 수신하는 시간이 길어진다. 즉, 소프트웨어의 갱신시간이 길어지므로 이용자에게 있어서는 불만이 발생한다고 하는 문제가 있다.

<12> 이에, 본 발명은 소프트웨어에 관한 파일을 갱신하는 경우에, 통신에 관한 데이터량을 종래보다도 억제할 수 있고, 또한 개찬검출을 행하는 전자기기, 갱신 서버장치, 키 갱신장치, 갱신방법, 갱신프로그램, 소프트웨어의 갱신에 필요한 정보를 취득하는 취득방법 및 취득프로그램을 제공하는 것을 목적으로 한다.

발명의 상세한 설명

<13> 상기 목적을 달성하기 위하여, 본 발명은, 애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일을 가지며, 네트워크를 통해서 상기 애플리케이션 파일을 갱신하는 전자기기로, 하나 이상의 데이터로 이루어지는 애플리케이션 파일을 기억하고 있는 기억수단과, 갱신데이터와, 상기 애플리케이션 파일에서 상기 갱신데이터에 의해서 갱신하는 위치를 나타내는 위치정보를 상기 네트워크를 통해서 외부장치로부터 수신하는 수신수단과, 상기 위치정보가 나타내는 위치에 존재하는 데이터를 상기 갱신데이터로 재기록(rewrite)하여 상기 애플리케이션 파일의 일부만을 갱신하는 갱신처리수단과, 갱신된 상기 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행하는 개찬검출 실행수단을 구비하는 것을 특징으로 한다.

<14> 상기에서 설명한 구성에 의하면, 전자기기는 네트워크를 통해서 애플리케이션 파일에 포함되는 데이터에 대한 갱신데이터와 상기 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 수신하고, 수신한 위치정보에 의거하여 상기 데이터를 상기 갱신데이터로 재기록하여 애플리케이션 파일의 일부만을 갱신하므로, 외부장치에서 갱신된 애플리케이션 파일을 수신하는 경우보다도 통신에 관한 데이터량을 적게 할 수 있다.

<15> 여기서, 상기 수신수단은 갱신데이터와 위치정보의 세트를 적어도 하나 이상 수신하고, 상기 갱신처리수단은 상기 위치정보에서 나타내는 위치에 의거하여 상기 애플리케이션 파일의 갱신위치를 결정하는 위치 결정부와, 결정된 상기 갱신위치를 상기 갱신데이터의 기록개시위치로 하여 상기 갱신데이터를 기록하는 기록부와, 상기 수신수단에서 수신한 하나 이상의 모든 갱신데이터의 기록이 완료할 때까지 상기 위치 결정부와 상기 기록부의 처리를 행하도록 제어하는 갱신제어부를 구비해도 된다.

<16> 이 구성에 의하면, 전자기기는 수신한 위치정보에서 나타내는 위치에 의거하여 갱신데이터의 기록개시위치를 결정하고, 결정한 기록개시위치에서 상기 갱신데이터를 기록할 수 있다.

<17> 여기서, 상기 갱신제어부는 모든 갱신데이터의 기록이 완료하면, 상기 개찬검출 실행수단의 처리를 개시하도록 제어해도 된다.

<18> 이 구성에 의하면, 전자기기는 애플리케이션 파일의 갱신 후에 갱신한 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행할 수 있으므로, 갱신 후의 애플리케이션 파일의 정당성을 보증할 수 있다.

<19> 여기서, 상기 갱신처리수단은, 애플리케이션 파일이 갱신 중임을 나타내는 제 1 정보 또는 갱신 중이 아님을 나타내는 제 2 정보 중 어느 하나를 나타내는 플래그(flag)를 기억하고 있는 플래그 기억부와, 상기 플래그가 나타내는 정보를 변경하는 플래그 변경부를 더 구비하고, 상기 플래그 변경부는 상기 수신수단이 갱신데이터와 위치정보의 세트를 적어도 하나 이상 수신한 때에 상기 플래그의 정보를 상기 제 1 정보로 변경하고, 상기 개찬검출 실행수단에서 개찬이 검출되지 않은 경우에 상기 플래그의 정보를 상기 제 2 정보로 변경해도 된다.

<20> 이 구성에 의하면, 전자기기는 플래그를 이용함으로써 애플리케이션 파일이 갱신 중인지 여부를 식별할 수 있다.

<21> 여기서, 상기 갱신제어부는 상기 전자기기에 전원이 투입되면 상기 플래그가 나타내는 정보를 확인하고, 제 1 정보인 경우에는 상기 위치 결정부와 상기 기록부의 처리를 행하도록 제어해도 된다.

<22> 이 구성에 의하면, 전자기기는 전원 투입시에 플래그가 나타내는 정보가 제 1 정보인 경우에는 다시 애플리케이션 파일의 갱신을 행한다. 이에 의해, 전자기기는 애플리케이션 파일의 갱신 중에 전원이 끊어져도, 그 후 전원이 투입됨으로써 확실히 애플리케이션 파일의 갱신을 행할 수 있다.

<23> 여기서, 상기 애플리케이션 파일은 하나 이상의 블록으로 분할되어 있고, 상기 갱신데이터는 상기 하나 이상의 블록 중 적어도 하나 이상의 갱신대상 블록에 포함되며, 상기 기억수단은 하나 이상의 상기 블록 각각에 대한 기준 개찬검출 값을 갖는 개찬검출 리스트를 기억하고 있고, 상기 수신수단은 하나 이상의 상기 갱신대상 블록 각각에 대한 새로운 기준 개찬검출 값과, 상기 하나 이상의 상기 갱신대상 블록 각각에 대한 기준 개찬검출 값의 상기 개찬검출 리스트에서의 위치를 나타내는 개찬 검출 위치정보로 이루어지는 세트를 더 수신하며, 상기 갱신처리수단은 하나 이상의 새로운 기준 개찬검출 값과 상기 개찬검출 값 위치정보를 이용하여 상기 개찬검출 리스트를 더 갱신하고, 상기 개찬검출 실행수단은 상기 갱신된 개찬검출 리스트가 정당한 것인 경우에만 상기 갱신된 개찬검출 리스트가 갖는 적어도 하나 이상의 기준 개찬검출 값에 의거하여 개찬검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인해도 된다.

<24> 이 구성에 의하면, 전자기기는 개찬검출 리스트의 정당성을 확인하고 있으므로, 개찬검출 값 자체를 개찬함으로써 부정한 블록을 정당하다고 오인시키는 행위를 방지할 수 있다.

<25> 여기서, 상기 애플리케이션 파일은 하나 이상의 블록으로 분할되어 있고, 상기 기억수단은 하나 이상의 상기 블록 각각에 대한 기준 개찬검출 값을 갖는 개찬검출 리스트를 기억하고 있으며, 상기 개찬검출 실행수단은 상기 애플리케이션 소프트웨어의 기동시에 처리를 개시하고, 상기 개찬검출 리스트가 정당한 것인 경우에만 상기 개찬검출 리스트가 갖는 적어도 하나 이상의 개찬검출 값에 의거하여 개찬검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인해도 된다.

<26> 이 구성에 의하면, 전자기기는 개찬검출 리스트의 정당성을 확인하고 있으므로, 개찬검출 값 자체를 개찬함으로써 부정한 블록을 정당하다고 오인하는 행위를 방지할 수 있다.

<27> 여기서, 상기 개찬검출수단은 개찬검출대상인 블록에 대한 검출용 개찬검출 값을 산출하고, 산출한 검출용 개찬검출 값과 개찬검출대상인 블록에 대한 개찬검출 값이 일치하는가 여부를 판단하며, 일치한다고 판단한 경우에는 상기 애플리케이션 파일은 개찬되어 있지 않은 것으로 하고, 일치하지 않는 경우에는 상기 애플리케이션 파일은 개찬되어 있는 것으로 해도 된다.

<28> 이 구성에 의하면, 전자기기는 개찬검출대상의 블록에 대한 검출용 개찬검출 값과 개찬검출 리스트에 포함되는 상기 블록에 대한 개찬검출 값을 이용하여 상기 블록이 개찬되어 있는가 여부를 확인할 수 있다.

<29> 여기서, 상기 기억부는 부분 키를 기억하고 있고, 상기 개찬검출 실행수단은 내 탬퍼화 되어 있으며, 마스터 키를 기억하고, 상기 부분 키와 상기 마스터 키를 이용하여 개찬검출 키를 생성하며, 생성한 개찬검출 키를 이용하여 상기 검출용 개찬검출 값을 산출해도 된다.

<30> 이 구성에 의하면, 전자기기는 개찬검출 실행수단이 내 탬퍼화 되어 있고, 또한 마스터 키를 기억하고 있으므로, 개찬검출 키의 생성, 및 생성한 개찬검출 키를 부정 해석자에 의해 해석되지 않게 할 수 있다.

<31> 여기서, 상기 수신수단은 상기 부분 키와는 다른 부분 키와 상기 부분 키가 상기 기억부에 기억되어 있는 위치를 나타내는 키 위치정보를 수신하고, 상기 갱신처리수단은 상기 키 위치정보에 의거하여 상기 부분 키를 상기

다른 부분 키로 갱신하여 된다.

<32> 이 구성에 의하면, 전자기기는 부분 키를 갱신할 수 있다. 이에 의해, 전자기기는 개찬검출 키가 부정한 해석자에게 알려졌다고 해도 부분 키를 갱신함으로써 새로운 개찬검출 키를 생성할 수 있다.

<33> 여기서 상기 개찬검출 리스트는 상기 하나 이상의 블록 각각에 대한 기준 개찬검출 값을 포함하는 데이터부와 상기 데이터부에 대한 기준 데이터부 개찬검출 값을 포함하는 헤더부로 구성되며, 상기 개찬검출 실행수단은 상기 데이터부에 대한 검출용 데이터부 개찬검출 값을 산출하고, 산출한 상기 검출용 데이터부 개찬 검출과 상기 기준 데이터부 개찬검출 값이 일치하는 경우에 상기 개찬검출 리스트가 정당한 것이라고 해도 된다.

<34> 이 구성에 의하면, 전자기기는 개찬검출 리스트에 포함되는 데이터부에 대한 개찬검출 값을 확인함으로써 개찬검출 리스트의 정당성을 보증할 수 있다. 이에 의해, 애플리케이션 파일의 개찬 검출을 더 정확하게 행할 수 있다.

<35> 여기서, 상기 데이터부는 암호화되어 있고, 상기 개찬검출 실행수단은 암호화된 상기 데이터부에 대한 검출용 개찬검출 값을 산출하며, 상기 개찬검출 리스트가 정당한 것인 경우에 암호화된 상기 데이터부를 복호 해도 된다.

<36> 이 구성에 의하면, 전자기기는 데이터부가 암호화되어 있으므로, 개찬검출 리스트에 포함되는 각 블록의 개찬검출 값이 부정 해석자에게 알려지지 않게 할 수 있다.

<37> 여기서, 상기 개찬검출 리스트에서 기준 개찬검출 값의 각각에 대해서 대응하는 블록이 개찬 검출의 대상으로서 사용해야 하는가 여부를 나타내는 판단정보와 대응이 부여되어 있고, 상기 개찬검출 실행수단은 상기 판단정보가 블록을 개찬검출의 대상으로 하지 않는다는 취지를 나타내는 경우에는 당해 블록에 대한 개찬검출은 행하지 않아도 된다.

<38> 이 구성에 의하면, 전자기기는 판단정보가 개찬검출의 대상으로 하지 않는다는 취지를 나타내는 경우에는 그 블록에 대한 개찬검출을 행하지 않도록 할 수가 있다. 이에 의해, 애플리케이션 파일이 갱신된 결과, 일부의 블록이 불필요해진 경우에, 불필요해진 블록에 대한 개찬검출을 생략할 수 있다.

<39> 여기서, 상기 개찬검출 리스트는 상기 하나 이상의 블록 각각에 대한 기준 개찬검출 값과 개찬검출의 대상이 되는 애플리케이션 소프트웨어의 종별을 나타내는 애플리케이션 종별을 상호 대응시킨 세트를 하나 이상 포함하고, 상기 개찬검출 실행수단은 기동 된 애플리케이션 소프트웨어에 대한 애플리케이션 종별에 대응하는 기준 개찬검출 값의 각각 중 적어도 하나 이상의 개찬검출 값에 의거하여 개찬 검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인해도 된다.

<40> 이 구성에 의하면, 전자기기는 기동 된 애플리케이션 소프트웨어의 애플리케이션 종별에 대응하는 하나 이상의 개찬검출 값을 이용하여 개찬검출을 행할 수 있다.

<41> 여기서, 상기 애플리케이션 소프트웨어의 동작에 관한 애플리케이션 파일은 복수 개 있고, 상기 애플리케이션 파일 각각은 하나 이상의 블록으로 분할되어 있으며, 상기 개찬검출 리스트는 애플리케이션 파일 각각에 대하여 하나 이상의 블록 각각에 대한 기준 개찬검출 값을 기준 값 군으로 하여 저장하고, 하나 이상의 상기 기준 값 군(群) 중 상기 애플리케이션 소프트웨어의 기동시에 개찬검출에 이용하는 적어도 하나 이상의 기준 값 군의 범위를 나타내는 범위정보를 가지며, 상기 개찬검출 실행수단은 상기 애플리케이션 소프트웨어의 기동시에 상기 개찬검출 리스트가 갖는 상기 범위정보에서 나타내는 적어도 하나 이상의 기준 값 군을 이용하여 개찬검출의 대상이 되는 블록이 개찬되어 있는가 여부를 확인해도 된다.

<42> 이 구성에 의하면, 전자기기는 애플리케이션 소프트웨어의 기동시에, 범위정보에 나타내는 적어도 하나 이상의 기준 값 군을 이용하여 우선적으로 개찬의 검출을 행하므로, 애플리케이션 소프트웨어의 기동에 걸리는 시간을 모든 기준 값 군을 이용하여 개찬검출을 행하는 경우에 비하여 짧게 할 수 있다.

<43> 여기서, 상기 갱신처리수단 및 상기 개찬검출 실행수단은 내 탬퍼화 되어 있어도 된다.

<44> 이 구성에 의하면, 전자기기는 갱신처리수단 및 개찬검출 실행수단이 내 탬퍼화 되어 있으므로 갱신처리의 동작, 개찬검출의 동작이 부정 해석자에 의해 해석되지 않게 할 수 있다.

<45> 또, 본 발명은, 네트워크를 통해서 전자기기에 대해서, 상기 전자기기가 가지며, 하나 이상의 데이터로 이루어지는 애플리케이션 파일의 갱신을 행하게 하는 갱신 서버장치로서, 갱신 후의 애플리케이션 파일을 취득하는 제1 취득수단과, 취득한 상기 갱신 후의 애플리케이션 파일로부터 갱신데이터와 갱신 전의 애플리케이션 파일에서

상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 취득하는 제 2 취득수단과, 취득한 상기 갱신데이터와 상기 위치정보를 상기 전자기기에 송신하는 송신수단을 구비하는 것을 특징으로 한다.

<46> 이 구성에 의하면, 갱신 서버장치는 애플리케이션 파일에 포함되는 데이터에 대한 갱신데이터와 상기 애플리케이션 파일에서 상기 갱신데이터에 의해 갱신하는 위치를 나타내는 위치정보를 취득하고, 취득한 갱신데이터 및 위치정보를 네트워크를 통해서 전자기기에 송신하므로, 애플리케이션 파일을 송신하는 경우보다도 통신에 관한 데이터량을 적게 할 수 있다.

<47> 여기서, 상기 갱신 전의 애플리케이션 파일은 소정의 크기로 이루어지는 하나 이상의 갱신 전 블록으로 분할되어 있고, 상기 제 1 취득수단은 하나 이상의 상기 갱신 전 블록 각각 및 상기 갱신 전 블록 각각에 대한 기준 개찬검출 값으로 이루어지는 갱신 전 개찬검출 리스트를 더 취득하고, 상기 갱신 서버장치는 상기 갱신 후의 애플리케이션 파일을 상기 소정의 크기로 분할한 하나 이상의 갱신 후 블록을 취득하고, 취득한 하나 이상의 갱신 후 블록 각각에 대하여 기준 개찬검출 값을 재계산하여 새로운 개찬검출 리스트를 생성하는 개찬검출 리스트 생성수단을 더 구비하며, 상기 제 2 취득수단은 상기 개찬검출 리스트 생성수단에서 생성된 새로운 개찬검출 리스트에서 상기 갱신데이터를 포함하는 갱신 후 블록과, 그 갱신 후 블록에 대응하는 재계산된 기준 개찬검출 값과, 그 갱신 후 블록에 대응하는 갱신 전 블록의 상기 갱신 전 개찬검출 리스트에서의 위치를 나타내는 개찬검출 값 위치정보를 더 취득하고, 상기 송신수단은 상기 제 2 취득수단에서 취득된 갱신 후 블록과 상기 기준 개찬검출 값 및 상기 개찬검출 값 위치 정보를 상기 전자기기에 더 송신해도 된다.

<48> 이 구성에 의하면, 갱신 서버장치는 제 2 취득수단에서 취득된 갱신 후 블록과, 그 기준 개찬검출 값과, 개찬검출 값 위치정보를 전자기기에 송신하므로, 전자기기에서는 갱신된 블록에 대한 기준 개찬검출 값을 항상 최신의 값으로 할 수가 있다.

<49> 여기서, 상기 개찬검출 리스트 생성수단은 외부장치에 의해서 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 기억하고 있고, 상기 개찬검출 키를 이용하여 상기 하나 이상의 갱신 후 블록 각각에 대한 기준 개찬검출 값을 산출해도 된다.

<50> 이 구성에 의하면, 갱신 서버장치는 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 이용하여 기준 개찬검출 값을 계산할 수 있다.

<51> 여기서, 상기 갱신 서버장치는 상기 외부장치에 의해 갱신된 부분 키와 상기 마스터 키를 이용하여 갱신된 개찬검출 키를 수신하면, 기억하고 있는 상기 개찬검출 키를 수신한 상기 갱신된 개찬검출 키로 갱신하고, 또한 상기 갱신된 부분 키를 상기 외부장치로부터 더 수신하며, 상기 개찬검출 리스트 생성수단은 상기 갱신된 개찬검출 키를 이용하여 상기 하나 이상의 갱신 후 블록 각각에 대한 기준 개찬검출 값을 산출하고, 상기 제 2 취득수단은 상기 전자기기에서 상기 부분 키가 기억되어 있는 위치를 나타내는 키 위치정보를 더 취득하며, 상기 송신수단은 상기 갱신된 부분 키와 상기 키 위치정보를 상기 전자기기에 더 송신해도 된다.

<52> 이 구성에 의하면, 갱신 서버장치는 개찬검출 키를 갱신할 수 있다. 이에 의해, 갱신 서버장치는 개찬검출 키가 부정 해석자에게 알려졌어도 새로운 개찬검출 키를 외부장치에서 수신함으로써 부정 해석자에게 알려진 개찬검출 키를 이용하지 않고 새로운 기준 개찬검출 값을 산출할 수 있다.

<53> 여기서, 상기 개찬검출 리스트는 상기 하나 이상의 갱신 후 블록 각각 및 상기 갱신 후 블록 각각에 대한 기준 개찬검출 값으로 이루어지는 데이터부를 가지며, 상기 개찬검출 리스트 생성수단은 생성한 새로운 개찬검출 리스트의 데이터부를 암호화해도 된다.

<54> 이 구성에 의하면, 갱신 서버장치는, 데이터부가 암호화되어 있으므로, 개찬검출 리스트에 포함되는 각 블록의 개찬검출 값을 부정 해석자에게 알려지지 않게 할 수 있다.

<55> 여기서, 상기 갱신 후 개찬검출 리스트는 헤더부를 가지며, 상기 개찬검출 리스트 생성수단은 외부장치에 의해 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 기억하고 있고, 상기 개찬검출 키를 이용하여 암호화된 데이터부에 대한 데이터부 개찬검출 값을 산출하여, 산출한 데이터부 개찬검출 값을 상기 헤더부에 저장해도 된다.

<56> 이 구성에 의하면, 갱신 서버장치는 암호화된 데이터부에 대한 데이터부 개찬검출 값을 산출하므로 암호화된, 데이터부에 대한 정당성을 보증할 수 있다.

<57> 여기서, 상기 개찬검출 리스트는 헤더부와 상기 하나 이상의 상기 갱신 후 블록 각각 및 상기 갱신 후 블록 각각에 대한 기준 개찬검출 값으로 이루어지는 데이터부를 가지며, 상기 개찬검출 리스트 생성수단은 외부장치에

의해 부분 키와 마스터 키를 이용하여 생성된 개찬검출 키를 기억하고 있고, 상기 개찬검출 키를 이용하여 상기 데이터부에 대한 데이터부 개찬검출 값을 산출하여, 산출한 데이터부 개찬검출 값을 상기 헤더부에 저장해도 된다.

<58> 이 구성에 의하면, 갱신 서버장치는 데이터부에 대한 데이터부 개찬검출 값을 산출하므로, 데이터부에 대한 정당성을 보증할 수 있다.

<59> 여기서, 상기 개찬검출 리스트 생성수단은 상기 데이터부 개찬검출 값의 산출 후에 상기 데이터부를 암호화해도 된다.

<60> 이 구성에 의하면, 갱신 서버장치는, 데이터부가 암호화되어 있으므로, 개찬검출 리스트에 포함되는 각 블록의 개찬검출 값을 부정 해석자에게 알려지지 않게 할 수 있다.

<61> 또, 본 발명은, 하나 이상의 블록으로 분할된 애플리케이션 파일에 대하여 블록별로 개찬검출 값을 산출하기 위해 이용되는 개찬검출 키를 생성하는 키 생성장치로, 상기 개찬검출 키는 마스터 키와 부분 키로 생성되고, 상기 키 생성장치는 상기 마스터 키와 상기 갱신된 부분 키를 취득하는 키 취득수단과, 상기 마스터 키와 상기 갱신된 부분 키를 이용하여 새로운 개찬검출 키를 생성하는 키 생성수단과, 상기 키 생성수단에 의해 생성된 개찬검출 키를 상기 개찬검출 값을 포함하는 개찬검출 리스트를 생성하는 외부장치에 배포하는 배포수단을 구비하는 것을 특징으로 한다.

<62> 이 구성에 의하면, 키 갱신장치는 외부장치에서 개찬검출 키가 누설되었다고 해도 부분 키를 갱신하는 것만으로 부정행위를 행한 외부장치가 갖는 개찬검출 키와는 다른 새로운 개찬검출 키를 생성할 수 있다.

<63> 여기서, 상기 배포수단은 상기 갱신된 부분 키를 상기 외부장치를 통해서 상기 애플리케이션 파일이 개찬되어 있는가 여부의 확인을 행하는 전자기기에 배포해도 된다.

<64> 이 구성에 의하면, 갱신된 부분 키를 외부장치를 통해서 전자기기에 배포할 수 있다.

실 시 예

<113> (제 1 실시 예)

<114> 이하, 본 발명에서의 제 1 실시 예에 대하여 도면을 참조하면서 설명한다.

<115> 1. 1 프로그램 갱신시스템(1)의 개요

<116> 도 1은 제 1 실시 예에서의 프로그램 갱신시스템(1)의 전체 구성을 나타내는 도면이다.

<117> 프로그램 갱신시스템(1)은 휴대전화기(10), 갱신 서버장치(20) 및 키 갱신장치(30)로 구성되어 있다.

<118> 키 갱신장치(30)는 갱신 서버장치(20)나 휴대전화기(10)에서 사용되는 개찬검출 키를 갱신한다. 개찬검출 키가 부정하게 유출된 경우에는 새로운 개찬검출 키를 발행한다. 키 갱신장치(30)는 개찬검출 키를 생성하는 기관에 의해 엄중하게 관리되고 있다. 개찬검출 키는 마스터 키와 부분 키로 생성된다. 마스터 키는 한번 생성되면 변경되지 않는 키이고, 부분 키는 개찬검출 키의 갱신을 행할 때에 갱신되는 키이다.

<119> 휴대전화기(10)는 갱신 서버장치(20)에 애플리케이션 소프트웨어(이하, AP라 한다)에 관한 파일의 갱신을 요구하는 갱신요구정보를 송신하고, 갱신에 관한 데이터인 갱신데이터 리스트를 수신한다. 휴대전화기(10)는 수신한 갱신데이터 리스트에 의거하여 파일의 갱신을 행한다. 여기서, AP는 구체적으로는 음악 녹음·재생 소프트웨어나 동화상 녹화·재생 소프트웨어와 같은 애플리케이션이다. 또, AP에 관한 파일은 AP 그 자체나 AP로부터 호출되는 인코더, 디코더, 드라이버, AP가 동작하는 환경을 제공하는 Java(등록상표) VM과 같은 가상실행환경 등이며, 하나 이상의 데이터로 이루어진다.

<120> 또, 휴대전화기(10)는 애플리케이션 소프트웨어의 갱신 시 및 기동 시에 AP에 관한 파일이 개찬되어 있는가 여부의 확인을 행한다. 여기서 개찬은 부정하게 파일을 바꾸는 것(alteration)을 말한다.

<121> 갱신 서버장치(20)는 갱신데이터 리스트를 보유하고 있고, 휴대전화기(10)로부터의 갱신요구정보를 접수하면, 갱신요구의 대상인 파일에 대응하는 갱신데이터 리스트를 휴대전화기(10)에 송신한다.

<122> 휴대전화기(10)와 갱신 서버장치(20)는 휴대 망(40) 및 인터넷(50)을 통해서 통신을 행한다.

<123> 1. 2 휴대전화기(10)의 구성

<124> 휴대전화기(10)는, 도 2에 도시한 바와 같이, 기억부(101), 제어부(102), 갱신처리부(103), 갱신파일 수신부(104), 개찬검출 실행부(105), 마이크(106), 스피커(107), 입력부(108), 표시부(109), 무선부(110) 및 안테나(111)로 구성되어 있다.

<125> (1) 기억부(101)

<126> 기억부(10)는, 도 2에 도시한 바와 같이, 검출대상정보 군(120, 120a, …, 120m)을 기억하고 있다. 또, 검출대상정보 군(120, 120a, …, 120m)은 모두 동일한 구성이므로, 여기에서는 검출대상정보 군 120의 구성에 대하여 설명한다.

<127> 검출대상 정보 군(120)은, 도 2에 도시한 바와 같이, AP 파일 군(121), 해시 리스트(122) 및 부분 키를 기억하고 있다.

<128> (AP 파일 군(121))

<129> AP 파일 군(121)은 제 1 파일(125), …, 제 n 파일(126)을 갖고 있다. 제 1 파일(125), …, 제 n 파일(126)은 개찬검출의 대상이 되는 파일이며, 구체적으로는, 상술한 바와 같이, AP 그 자체나 AP에서 호출되는 인코더, 디코더, 드라이버, AP가 동작하는 환경을 제공하는 Java(등록상표) VM과 같은 가상실행환경 등이다. 여기서, n은 하나 이상의 정수이다. 즉, AP 파일 군(121)에는 하나 이상의 파일이 저장되어 있다.

<130> 또, 이하에서는, 제 1 파일(125), …, 제 n 파일(126)의 각각의 파일 명을 「file_1」, …,「file_n」이라고 한다. 또, 각 파일은 국소적인 갱신이 가능해지도록 휴대전화기의 제조시에 고정된 어드레스에 기록되어 있다.

<131> (해시 리스트(122))

<132> 해시 리스트(122)는 제 1 파일(125), …, 제 n 파일(126)의 개찬검출용의 해시 값을 리스트로 보유하고 있다. 해시 리스트(122)는 국소적인 갱신이 가능해지도록 휴대전화기의 제조시에 고정된 어드레스에 기록되어 있다.

<133> 여기서, 해시 리스트(122)에 대하여 설명한다.

<134> 도 3은 해시 리스트(122)의 데이터 구조의 일 예를 나타내는 도면이다.

<135> 해리 리스트(122)는 암호화되어 있지 않은 헤더부(130)와 암호화되어 있는 데이터부(131)로 구성되어 있다. 여기서, 암호화에 이용되는 알고리즘은, 예를 들어 XOR과 같은 논리연산, 또는 DES(Data Encryption Standard), AES(Advanced Encryption Standard)와 같은 암호 알고리즘이다. 암호 알고리즘 DES, AES는 공지이므로 설명을 생략한다.

<136> 헤더부(130)는 해시 리스트 파일 사이즈(132)와 데이터부 해시 값(133)으로 구성되어 있다. 해시 리스트 파일 사이즈(132)는 헤더부(130)와 데이터부(131)를 합친 해시 리스트(122) 전체의 데이터 사이즈를 나타낸다. 데이터부 해시 값(133)은 데이터부(131)에 대하여 해시 계산 알고리즘을 적용하여 산출된 해시 값을 나타낸다. 여기서, 해시 계산 알고리즘은 SHA-1이나 MD5 등의 일 방향성 함수에 키 값(key value)을 포함하는 HMAC(Keyed-Hashing for Message Authentication) 알고리즘으로 한다. 이하에서는 해시 값을 산출하는 해시 계산 알고리즘은 HMAC 알고리즘으로 한다.

<137> 데이터부(131)는 하나 이상의 해시 정보로 구성되어 있다. 여기에서는, 데이터 부(131)는 해시 정보 134, …, 해시 정보 135로 구성되어 있는 것으로 한다. 해시 정보는 개찬검출대상이 되는 파일에 대하여 적어도 하나 존재한다.

<138> 해시 정보 134는 하나의 파일정보(140)와 복수의 MAC정보(141)로 구성되어 있다.

<139> 파일정보(140)는 개찬검출대상이 되는 파일을 분할하여 생성한 블록의 수를 나타내는 블록 수(142)와 개찬검출대상이 되는 파일을 나타내는 파일 명으로 구성되어 있다. 여기서, 파일 명은 개찬검출대상이 되는 파일의 파일 시스템상의 절대 패스(absolute path)나 상대 패스(relative path) 등 장소를 특정할 수 있는 패스를 포함한 형식으로 나타내고 있다.

<140> MAC정보(141)는 하나 이상의 엔트리로 구성되어 있다. 여기서, 엔트리의 수는 블록 수(142)에서 나타내는 값 +1 이다.

<141> 엔트리(144)는 파일 명(143)에 의해 나타내는 파일의 분할된 블록에 대한 선두 어드레스로부터의 오프 셋(offset)과, 블록의 사이즈와, 블록에 대하여 해시 계산 알고리즘을 적용하여 산출된 해시 값으로 구성되어 있

다. 또, (n-1)번째까지의 엔트리의 구성에 대해서는 동일하므로 설명을 생략한다. 해시 리스트(122)에 저장되어 있는 해시 값은 개찬 검출시에 개찬이 되어 있는가 여부를 판단하기 위한 기준이 되는 기준 값이다.

<142> MAC정보(141)의 최후에 위치하는 엔트리(145)는 갱신용으로 예약된 공 엔트리(empty entry)이며, 오프셋, 사이즈 및 해시 값이 기술되는 대신에 "Reserved"가 각각 기술되어 있다. 또, MAC정보(141)의 최후에 위치하는 엔트리를 최종 엔트리라고도 한다.

<143> 데이터부(131)의 최후에 위치하는 해시 정보에서의 최종 엔트리에는 해시 리스트(122)에서의 최후의 엔트리임을 나타내는 정보 "end of entry"가 채워져 있다. 여기에서는, 해시 정보 135가 데이터부(131)의 최후에 위치하는 해시 정보이므로, 그 최종 엔트리(146)에는 "end of entry"가 채워져 있다. 또, 해시 정보 135의 다른 구성요소는 해시 정보 134에서 최종 엔트리(145)를 제외한 다른 구성요소와 동일하므로 설명을 생략한다.

<144> 또, 상술한 바와 같이 데이터부(131)는 암호화되어 있다. 암호화는 파일정보(140)나 MAC정보(141)의 1 엔트리의 단위로 행해진다. 따라서 해시 리스트(122)의 갱신은 파일정보(140)나 MAC정보(141)의 1 엔트리의 단위로 가능해진다.

<145> 또, 여기에서는, 해시 리스트(122)는 해시 리스트(122)가 속하는 검출대상정보 군(120)에 포함되는 AP를 식별하는 AP 식별정보와 대응되어 있는 것으로 한다.

<146> (부분 키(123))

<147> 부분 키(123)는 개찬검출을 실행했을 때에 마스터 키와 함께 개찬검출 키의 산출에 이용된다. 부분 키(123)는 갱신이 가능해지도록 휴대전화기의 제조시에 고정된 어드레스에 기록되어 있다.

<148> 또, 여기에서는, 해시 리스트(122)와 마찬가지로 부분 키(123)는 부분 키(123)가 속하는 검출대상정보 군(120)에 포함되는 AP를 식별하는 AP 식별정보와 대응되어 있는 것으로 한다.

<149> (2) 제어부(102)

<150> 제어부(102)는 휴대전화기(10) 전체의 제어를 행한다.

<151> 제어부(102)는 무선부(110)로부터 통화에 관한 신호(음성신호)를 수신하면, 수신한 신호를 스피커(107)에 출력하기 위한 신호처리를 행한다.

<152> 제어부(102)는 마이크(106)로부터 통화에 관한 신호(음성신호)를 무선부(110)에 출력하기 위한 신호처리를 행한다.

<153> 제어부(102)는 입력부(108)로부터 AP에 관한 파일의 갱신의 갱신지시를 수신하면, 파일의 갱신처리의 개시를 나타내는 갱신개시명령을 갱신처리부(103)에 출력한다. 여기서, 갱신지시 및 갱신개시명령에는 갱신대상이 되는 AP를 나타내는 AP 식별정보가 포함된다.

<154> 제어부(102)는 갱신처리부(103)로부터 파일의 갱신완료의 통지를 수신하면, 표시부(109)를 통해서 갱신완료의 메시지를 표시한다.

<155> 제어부(102)는 갱신처리부(103)로부터 파일의 갱신 실패의 통지를 수신하면, 표시부(109)를 통해서 갱신 실패의 메시지를 표시한다. 또, 제어부(102)는 입력부(108)로부터 재갱신의 지시를 수신하면, 파일의 재갱신의 개시를 나타내는 재갱신 개시명령을 갱신처리부(103)에 출력한다. 제어부(102)는 입력부(108)로부터 재갱신을 행하지 않는다는 지시를 수신하면, 파일의 갱신처리의 종료를 나타내는 갱신종료명령을 갱신처리부(103)에 출력한다.

<156> 제어부(102)는 입력부(108)로부터 AP의 기동지시를 수신하면, 기동의 대상이 되는 AP의 기동을 행한다. 이때, 기동 된 AP는 자(自) AP가 개찬검출대상인 경우에는 검출개시명령과 자 AP를 식별하는 AP 식별정보를 제어부(102)에 의해 개찬검출 실행부(105)에 출력한다. 또, 개찬검출 실행부(105)에서는 검출개시명령을 제어부(102)로부터 수신하게 된다.

<157> 제어부(102)는 개찬검출 실행부(105)로부터 개찬되어 있지 않다는 통지를 수신하면 기동지시가 있은 AP에 관한 동작을 실행한다.

<158> 제어부(102)는 개찬검출 실행부(105)로부터 개찬이 검출되었다는 통지를 수신하면 기동지시가 있은 AP의 동작을 종료한다.

<159> (3) 갱신처리부(103)

<160> 갱신처리부(103)는 갱신파일 수신부(104)가 갱신 서버장치(20)에서 수신한 갱신데이터 리스트(150)에서 갱신 대상이 되는 파일이나 리스트, 또는 키 등의 데이터를 갱신한다.

<161> 여기서, 갱신데이터 리스트(150)는, 도 4에 도시한 바와 같이, 하나 이상의 갱신정보(151, …, 152)로 구성되어 있다. 갱신정보(151)는 위치정보(153), 데이터 사이즈(154) 및 갱신데이터(155)로 구성되어 있다. 위치정보(153)는 갱신하는 데이터의 위치를 나타내는 정보이다. 예를 들어, 위치정보(153)는 파일 명이나 파일의 선두로부터의 오프셋, 어드레스 정보 등으로 표시된다. 데이터 사이즈(154)는 갱신하는 데이터의 사이즈를 나타낸다. 갱신데이터(155)는 갱신해야 할 정보인 파일 중 갱신 대상이 되는 하나 이상의 블록, 해시 리스트(122)에서의 해시 리스트 파일 사이즈(132), 데이터부 해시 값(133), 파일정보, MAC정보에 포함되는 엔트리 등이 기록되어 있다.

<162> 여기서, 갱신데이터에는 하나 이상의 데이터가 포함되어 있고, 갱신데이터에 포함되는 데이터는 해시 리스트 파일 사이즈나 데이터부 해시 값 등과 같은 값이나, 애플리케이션 소프트웨어를 실행하기 위한 명령문 등이다.

<163> 예를 들어, 파일을 복수 개의 블록으로 분할하고, 2~4번째의 블록을 갱신하는 경우에는, 위치정보에는 2번째의 블록의 위치를 나타내는 오프셋이 저장되고, 데이터 사이즈에는 2~4번째 블록 각각의 사이즈를 합계한 합계 사이즈가 저장되며, 갱신데이터에는 갱신 후의 2~4번째의 블록이 저장된다. 또, 해시 리스트도 갱신할 필요가 있으므로, 이 경우에는 2번째 블록의 해시 값을 포함하는 엔트리 위치를 나타내는 오프셋이 위치정보에 저장되고, 2~4번째 블록의 해시 값을 포함하는 엔트리 각각의 사이즈의 합계 값이 데이터 사이즈에 저장되며, 갱신 후의 2~4번째의 블록에 대응하는 엔트리의 각각이 갱신데이터에 저장된다.

<164> 갱신처리부(103)는 갱신데이터 리스트(150)의 내용에 의거하여 파일이나 해시 리스트(122) 내의 해시 리스트 파일 사이즈(132), 데이터부 해시 값(133), 파일정보, MAC정보에 포함되는 엔트리 및 부분 키(123)의 갱신을 행한다.

<165> 갱신처리부(103)는, 도 5에 도시한 바와 같이, 플래그 기억부(161), 갱신제어부(162), 갱신데이터 판독부(163), 갱신데이터 해석부(164), 기록위치 결정부(165), 갱신데이터 기록부(166) 및 갱신 확인부(167)로 구성되어 있다.

<166> 갱신처리부(103)는 악의가 있는 사용자에 의한 해석에 대한 내성을 갖도록 내 탬퍼 기술로 보호되어 있다. 내 탬퍼 기술은 공지이므로 설명을 생략한다.

<167> (플래그 기억부(161))

<168> 플래그 기억부(161)는 AP에 관한 파일의 갱신을 행하고 있는가 여부를 나타내는 플래그를 기억하고 있다. 여기에서는, 플래그의 값이 「0」인 경우에는 갱신처리부(103)가 갱신을 행하고 있지 않다는 취지를 나타내고, 값이 「1」인 경우에는 갱신처리부(103)가 갱신을 행하고 있다는 취지를 나타낸다. 또한, 플래그 기억부(161)는 구체적으로는 불휘발성 메모리이다. 즉, 휴대전화기(10)의 전원을 꺼도 플래그 기억부(161)의 기억내용은 유지된다.

<169> (갱신제어부(162))

<170> 갱신제어부(162)는 제어부(102)로부터 갱신개시명령을 수신하면, 다른 명령에 의한 처리가 인터럽트(interrupt)하지 않도록 제어부(102)에 대하여 인터럽트 금지를 설정한다.

<171> 갱신제어부(162)는 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「1」로 설정한다.

<172> 갱신제어부(162)는 수신한 갱신개시명령에 포함되는 AP 식별정보를 갱신데이터 판독부(163)에 출력한다.

<173> 갱신제어부(162)는 갱신데이터 판독부(163)로부터 모든 갱신데이터의 기록이 완료했다는 취지의 기록완료명령을 수신하면, 개찬검출의 처리를 개시한다는 취지의 검출개시명령과 AP 식별정보를 개찬검출 실행부(105)에 출력한다.

<174> 갱신제어부(162)는 개찬검출 실행부(105)로부터 개찬되어 있지 않다는 통지를 수신하면 개찬 완료의 통지를 제어부(102)에 출력한다. 갱신제어부(162)는 제어부(102)에 대한 인터럽트 금지를 해제하고, 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「0」으로 설정한다.

<175> 갱신제어부(162)는 개찬검출 실행부(105)에서 개찬이 검출되었다는 통지를 수신하면 갱신 실패의 통지를 제어부(102)에 출력한다. 갱신제어부(162)는 제어부(102)로부터 재갱신 개시명령을 수신하면, 다시 AP 식별정보를 갱신데이터 판독부(163)에 출력한다.

<176> 갱신제어부(162)는 제어부(102)로부터 갱신종료명령을 수신하면, 갱신제어부(162)는 제어부(102)에 대한 인터럽트 금지를 해제하고, 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「0」으로 설정한다.

<177> 휴대전화기(10)에 전원이 투입되어 전원의 공급이 개시되면, 갱신제어부(162)는 플래그 기억부(161)에 기억되어 있는 플래그의 값을 확인한다. 값이 「1」인 경우에는 갱신 처리중인 상태라고 판단하고, 제어부(102)에 대하여 인터럽트 금지를 설정한다. 갱신제어부(162)는 갱신 처리의 재개시를 나타내는 재개시명령을 갱신데이터 판독부(163)에 출력한다. 갱신제어부(162)는 갱신데이터 판독부(163)로부터 갱신 처리의 재개시가 불필요하다는 취지를 나타내는 재개시 불요 명령을 수신하면, 제어부(102)에 대한 인터럽트 금지를 해제하고, 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「0」으로 설정한다.

<178> (갱신데이터 판독부(163))

<179> 갱신데이터 판독부(163)는 갱신제어부(162)로부터 AP 식별정보를 수신하면, 수신한 AP 식별정보를 갱신파일 수신부(104)에 출력한다.

<180> 갱신데이터 판독부(163)는 갱신파일 수신부(104)로부터 갱신 서버장치(20)에서 갱신데이터 리스트(150)의 수신이 완료했다는 취지의 수신완료 명령을 수신하면, 수신한 갱신데이터 리스트(150)에서 판독되지 않은 갱신정보를 하나 판독한다.

<181> 갱신데이터 판독부(163)는 갱신 확인부(167)로부터 갱신데이터의 기록이 정상으로 종료했다는 취지의 정상종료명령을 수신하면 수신한 갱신데이터 리스트(150)에 미 판독의 갱신정보가 존재하는가 여부를 판단한다. 존재한다고 판단한 경우에는 갱신데이터 판독부(163)는 판독하지 않는 갱신정보를 취득한다. 존재하지 않는다고 판단한 경우에는 갱신데이터 판독부(163)는 기록완료명령을 갱신제어부(162) 및 갱신파일 수신부(104)에 출력한다. 갱신데이터 판독부(163)는 갱신 확인부(167)로부터 갱신데이터의 기록이 실패했다는 취지의 이상종료명령을 수신하면 전 회에 판독한 갱신정보를 다시 판독한다.

<182> 갱신데이터 판독부(163)는 갱신제어부(162)로부터 재개시명령을 수신하면 수신한 재개시명령을 갱신파일 수신부(104)에 출력한다. 그 후, 갱신데이터 판독부(163)는 갱신파일 수신부(104)로부터 수신완료명령을 수신하면 상기와 동일한 동작을 행한다.

<183> 갱신데이터 판독부(163)는 재개시 불요 명령을 수신하면 수신한 재개시 불요 명령을 갱신제어부(162)에 출력한다.

<184> (갱신데이터 해석부(164))

<185> 갱신데이터 해석부(164)는 갱신데이터 판독부(163)에서 판독된 갱신정보를 위치정보, 데이터 사이즈 및 갱신데이터로 분할한다. 이에 의해, 갱신데이터 해석부(164)는 갱신정보로부터 위치정보, 데이터 사이즈 및 갱신데이터를 취득할 수 있다.

<186> (기록위치 결정부(165))

<187> 기록위치 결정부(165)는 갱신데이터 해석부(164)에서 취득된 위치정보에 의거하여 기억부(101)에서의 갱신데이터의 기록위치를 결정한다.

<188> (갱신데이터 기록부(166))

<189> 갱신데이터 기록부(166)는 기록위치 결정부(165)에서 결정된 기록위치를 기록개시의 선두 위치로 하여 갱신데이터 해석부(164)에서 취득된 갱신데이터를 기록한다.

<190> (갱신 확인부(167))

<191> 갱신 확인부(167)는 갱신데이터 기록부(166)에 의한 기록이 정상으로 종료하였는가 여부를 확인한다.

<192> 정상으로 종료했다고 판정한 경우에는 정상종료명령을 갱신데이터 판독부(163)에 출력하고, 정상으로 종료하지 않았다고 판단한 경우에는 이상종료명령을 갱신데이터 판독부(163)에 출력한다.

<193> (4) 갱신파일 수신부(104)

<194> 갱신파일 수신부(104)는 휴대전화기(10)를 식별하는 단말 식별자를 미리 기억하고 있다.

<195> 갱신파일 수신부(104)는 갱신처리부(103)로부터 수신한 AP 식별정보를 기억하는 AP 식별정보 기억영역 및 갱신서버장치(20)에서 수신한 갱신데이터 리스트(150)를 기억하는 리스트 기억영역을 갖는다. 여기서, AP 식별정보

기억영역 및 리스트 기억영역은 불휘발성 메모리이다.

<196> 갱신파일 수신부(104)는 갱신처리부(103)의 갱신데이터 판독부(163)로부터 AP 식별정보를 수신하면, 수신한 AP 식별정보와, 단말 식별자와, 갱신요구정보를 무선부(110)를 통해서 갱신 서버장치(20)에 송신하고, 수신한 AP 식별정보를 AP 식별정보 기억영역에 저장한다.

<197> 갱신파일 수신부(104)는 갱신 서버장치(20)로부터 무선부(110)를 통해서 갱신데이터 리스트(150)를 수신하면, 수신한 갱신데이터 리스트(150)를 리스트 기억영역에 저장한다. 또, 갱신파일 수신부(104)는 수신한 갱신데이터 리스트(150)의 저장이 완료하면, AP 식별정보 기억영역에 저장되어 있는 AP 식별정보를 소거하고, 수신완료명령을 갱신데이터 판독부(163)에 출력한다.

<198> 갱신파일 수신부(104)는 갱신데이터 판독부(163)로부터 기록완료명령을 수신하면 리스트 저장영역에 저장되어 있는 갱신데이터 리스트(150)를 소거한다.

<199> 갱신파일 수신부(104)는 갱신데이터 판독부(163)로부터 재개시명령을 수신하면 AP 식별정보 기억영역에 저장되어 있는 AP 식별정보가 존재하는가 여부를 판단한다. 존재한다고 판단한 경우에는, 갱신파일 수신부(104)는 저장하고 있는 AP 식별정보와 단말 식별자를 무선부(110)를 통해서 갱신 서버장치(20)에 송신하고, 상기와 동일한 동작을 행한다.

<200> AP 식별정보 기억영역에 AP 식별정보가 존재하지 않는다고 판단한 경우에는, 갱신파일 수신부(104)는 리스트 기억영역에 갱신데이터 리스트(150)가 저장되어 있는가 여부를 판단한다. 저장되어 있다고 판단한 경우에는 수신완료명령을 갱신데이터 판독부(163)에 출력한다. 저장되어 있지 않다고 판단한 경우에는 재개시 불요 명령을 갱신데이터 판독부(163)에 출력한다.

<201> (5) 개찬검출 실행부(105)

<202> 개찬검출 실행부(105)는, 도 6에 도시한 바와 같이, 검출제어부(171), 개찬검출 호출부(172), 개찬검출 처리부(173) 및 파일 판독부(174)로 구성되어 있다.

<203> 개찬검출 실행부(105)는 악의가 있는 사용자에 의한 해석에 대한 내성을 갖도록 내 탬퍼 기술에 의해 보호되어 있다. 내 탬퍼 기술은 공지이므로 설명을 생략한다.

<204> (검출제어부(171))

<205> 검출제어부(171)는 제어부(102) 또는 갱신처리부(103)의 갱신제어부(162) 중 어느 하나로부터 검출개시명령과 AP 식별정보를 수신하면, 수신한 검출개시명령과 AP 식별정보를 개찬검출 호출부(172)에 출력한다.

<206> 검출제어부(171)는 개찬검출 처리부(173)로부터 개찬되어 있지 않다는 통지 또는 개찬이 검출되었다는 통지 중 어느 하나를 수신한다.

<207> 검출제어부(171)는 수신한 통지를 검출개시명령 및 AP 식별정보의 출력 원(出力 元)인 제어부(102) 또는 갱신처리부(103)의 갱신제어부(162) 중 어느 하나에 출력한다. 구체적으로는, 검출개시명령을 제어부(102)로부터 수신한 경우에는, 검출제어부(171)는 개찬검출 처리부(173)에서 수신한 통지를 제어부(102)에 출력한다. 또, 검출개시명령을 갱신제어부(162)로부터 수신한 경우에는, 검출제어부(171)는 개찬검출 처리부(173)에서 수신한 통지를 갱신제어부(162)에 출력한다.

<208> (개찬검출 호출부(172))

<209> 개찬검출 호출부(172)는 검출제어부(171)로부터 검출개시명령과 AP 식별정보를 수신하면, 기억부(101)에서 수신한 AP 식별정보에 대응하는 해시 리스트(122)를 판독한다.

<210> 개찬검출 호출부(172)는 판독한 해시 리시트(122)와 수신한 검출개시명령 및 AP 식별정보를 개찬검출 처리부(173)에 출력한다.

<211> (개찬검출 처리부(173))

<212> 개찬검출 처리부(173)는, 도 6에 도시한 바와 같이, 마스터 키 기억부(175)를 가지고 있다. 마스터 키 기억부(175)는 마스터 키(176)를 기억하고 있다.

<213> 개찬검출 처리부(173)는 개찬검출 호출부(172)로부터 해시 리스트(122)와 검출개시명령 및 AP 식별정보를 수신하면 개찬검출의 처리를 개시한다.

<214> 개찬검출 처리부(173)는 수신한 AP 식별정보에 대응하는 부분 키(123)를 기억부(101)에서 판독한다.

<215> 개찬검출 처리부(173)는 판독한 부분 키(123)와, 마스터 키(176) 및 특정 알고리즘을 이용하여 개찬검출 키를 산출한다. 여기서, 특정 알고리즘은, 예를 들어 XOR(배타적 논리합)과 같은 논리연산, 또는 DES, AES와 같은 암호 알고리즘으로 한다.

<216> 개찬검출 처리부(173)는 산출한 개찬검출 키와 해시 계산 알고리즘을 이용하여 수신한 해리 리스트(122)의 데이터부(131)에 대한 해시 값을 산출한다. 개찬검출 처리부(173)는 산출한 해시 값과 해시 리스트(122)의 헤더부(130)에 포함되는 데이터부 해시 값(133)이 일치하는가 여부를 판단한다.

<217> 일치하지 않는다고 판단한 경우에는, 개찬검출 처리부(173)는 개찬이 검출되었다는 통지를 검출제어부(171)에 출력한다.

<218> 일치한다고 판단한 경우에는, 개찬검출 처리부(173)는 개찬검출 키를 이용하여 데이터부(131)를 복호 한다. 또, 복호에는 데이터부(131)를 암호화한 알고리즘에 대응하는 복호 알고리즘이 이용된다.

<219> 개찬검출 처리부(173)는 복호 한 데이터부에서 미 판독의 해시 정보를 판독한다. 개찬검출 처리부(173)는 판독한 해시 정보에 포함되는 파일정보를 파일 판독부(174)에 출력하고, 그 후, 파일 판독부(174)로부터 파일의 판독이 완료했다는 취지를 나타내는 파일 판독 완료명령을 수신한다.

<220> 개찬검출 처리부(173)는 판독한 해시 정보에서 미 판독 엔트리를 취득하고, 취득한 엔트리가 최종 엔트리인가 여부를 판단한다.

<221> 최종 엔트리가 아니라고 판단한 경우에는, 개찬검출 처리부(173)는 취득한 엔트리에 포함되는 오프셋 및 사이즈를 판독하고, 판독한 오프셋 및 사이즈에 의거하여 파일 판독부(174)에서 판독된 파일에서 검출대상의 블록을 취득한다. 개찬검출 처리부(173)는 산출한 개찬검출 키와 해시 계산 알고리즘을 이용하여 취득한 블록에 대한 검출용 해시 값을 산출한다. 개찬검출 처리부(173)는 산출한 검출용 해시 값과 취득한 엔트리에 포함되는 해시 값이 일치하는가 여부를 판단한다. 일치한다고 판단한 경우에는, 개찬검출 처리부(173)는 판독한 해시 정보에서 미 판독의 엔트리를 취득하고, 상기 동작을 행한다. 일치하지 않는다고 판단한 경우에는 개찬검출 처리부(173)는 개찬이 검출되었다는 통지를 검출제어부(171)에 출력한다.

<222> 취득한 엔트리가 최종 엔트리라고 판단한 경우에는 개찬검출 처리부(173)는 미 판독의 해시 정보가 존재하는가 여부를 판단한다. 존재한다고 판단한 경우에는 개찬검출 처리부(173)는 미 판독의 해시 정보를 판독하고, 상기의 동작을 행한다. 존재하지 않는다고 판단한 경우에는, 개찬검출 처리부(173)는 개찬되어 있지 않다는 통지를 검출제어부(171)에 출력한다.

<223> (파일 판독부(174))

<224> 파일 판독부(174)는 판독한 파일을 일시적으로 기억하는 파일 기억영역을 갖는다.

<225> 파일 판독부(174)는 개찬검출 처리부(173)로부터 파일정보를 수신하면, 수신한 파일정보에 포함되는 파일 명에 의거하여 개찬검출대상의 파일을 기억부(101)에서 판독한다.

<226> 파일 판독부(174)는 판독한 파일을 파일 기억영역에 저장하고, 파일 판독완료명령을 개찬검출 처리부(173)에 출력한다.

<227> (6) 마이크(106)

<228> 마이크는 사용자의 음성을 접수하고, 접수한 음성을 음성신호로 변환하며, 변환한 음성신호를 제어부(102)에 출력한다.

<229> (7) 스피커(107)

<230> 스피커(107)는 제어부(102)에서 처리된 음성신호를 음성으로 출력한다.

<231> (8) 입력부(108)

<232> 입력부(108)는 사용자의 조작에 의해 갱신지시를 접수하면 접수한 갱신지시를 제어부(102)에 출력한다.

<233> 입력부(108)는 개찬검출대상의 파일의 갱신이 실패한 경우에, 사용자의 조작에 의해 재갱신을 행한다는 지시를 접수하면 접수한 재갱신을 행한다는 지시를 제어부(102)에 출력한다. 또, 입력부(108)는 개찬검출대상의 파일의 갱신이 실패한 경우에, 사용자의 조작에 의해 재갱신을 행하지 않는다는 지시를 접수하면 접수한 재갱신을 행하

지 않는다는 지시를 제어부(102)에 출력한다.

<234> 입력부(108)는 사용자의 조작에 의해 AP의 기동지시를 접수하면 접수한 기동지시를 제어부(102)에 출력한다.

<235> (9) 표시부(109)

<236> 표시부(109)는 제어부(102)로부터 갱신완료의 메시지를 수신하면 수신한 메시지를 표시한다.

<237> 표시부(109)는 제어부(102)로부터 갱신실패의 메시지를 수신하면 수신한 메시지를 표시한다.

<238> (10) 무선부(110)

<239> 무선부(110)는 안테나(111)를 구비하고 있으며, 무선신호의 송수신을 행한다.

<240> 1. 3 갱신 서버장치(20)의 구성

<241> 갱신 서버장치(20)는, 도 7에 도시한 바와 같이, 기억부(201), 데이터 취득부(202), 해시 리스트 생성부(203), 해시 리스트 기록부(204), 갱신요구 처리부(205), 입력부(206) 및 송수신부(207)로 구성되어 있다.

<242> (1) 기억부(201)

<243> 기억부(201)는 휴대전화기(10)에 기억되어 있는 검출대상정보 군에 대한 갱신데이터 리스트를 하나 이상 기억하기 위한 영역과 해시 리스트를 기억하기 위한 영역을 갖는다.

<244> 여기에서는, 검출대상정보 군(120)에 대한 갱신데이터 리스트를 하나 이상 기억하는 것으로 한다. 또, 기억되어 있는 갱신데이터 리스트의 각각은 갱신대상의 파일을 포함하는 AP의 AP 식별정보와 대응되고, 또, 판(版) 수의 관리가 이루어지고 있다. 또, 휴대전화기(10)의 단말 식별자와 휴대전화기(10)에 송신한 갱신데이터 리스트의 판 수가 대응되어서 관리되는 것으로 한다. 또, 해시 리스트는 대응하는 AP의 AP 식별정보와 대응이 되어 있다.

<245> (2) 데이터 취득부(202)

<246> 데이터 취득부(202)는 입력부(206)로부터 초기설정지시를 수신하면 개찬검출대상이 되는 하나 이상의 파일 및 타깃 패스 리스트(target path list)를 더 취득한다. 이때, 취득 원은, 예를 들어 외부 장치이다. 데이터 취득부(202)는 수신한 초기설정지시와 취득한 하나 이상의 파일 및 타깃 패스 리스트를 해시 리스트 생성부(203)에 출력한다. 여기서, 타깃 패스 리스트는 개찬검출대상이 되는 하나 이상의 파일의 각각에 대한 파일시스템상에 저장되어 있는 저장장소를 나타내는 절대 패스나 상대 패스 등으로 이루어지는 패스 명이 저장되어 있는 리스트이다. 또, 초기설정 지시에는 생성되는 해시 리스트와 대응하는 AP의 AP 식별정보가 포함된다.

<247> 데이터 취득부(202)는 입력부(206)로부터 검출대상의 파일의 갱신이 있었다는 취지를 나타내는 제 1 갱신지시를 수신하면, 갱신대상이 되는 하나 이상의 파일의 각각에 대한 갱신파일 및 갱신대상이 되는 하나 이상의 파일의 타깃 패스 리스트를 더 취득한다. 또, 제 1 갱신지시에는 갱신의 대상이 되는 AP의 AP 식별정보가 포함되는 것으로 한다. 이때, 취득 원은, 예를 들어 외부장치이다. 데이터 취득부(202)는 기억부(201)에서 제 1 갱신지시에 포함되는 AP 식별정보에 대응하는 해시 리스트를 취득한다. 데이터 취득부(202)는 수신한 제 1 갱신지시와, 취득한 하나 이상의 갱신파일, 타깃 패스 리스트 및 해시 리스트를 해시 리스트 생성부(203)에 출력한다. 여기서, 갱신파일은 원래의 파일에 존재하는 문제가 해소된 최신 파일이다.

<248> 데이터 취득부(202)는 키 갱신장치(30)로부터 부분 키의 갱신이 있었던 취지를 나타내는 제 2 갱신지시와 갱신 후의 부분 키를 수신하면, 갱신된 부분 키를 이용한 개찬검출의 대상이 되는 하나 이상의 파일 및 타깃 패스 리스트를 더 취득한다. 또, 제 2 갱신지시에는 갱신된 부분 키에 대응하는 AP의 AP 식별정보가 포함되어 있는 것으로 한다. 이때, 취득 원은, 예를 들어 외부장치이다. 데이터 취득부(202)는 기억부(201)로부터 제 2 갱신지시에 포함되는 AP 식별정보에 대응하는 해시 리스트를 취득한다. 데이터 취득부(202)는 수신한 제 2 갱신지시 및 부분 키와 하나 이상의 파일, 타깃 패스 리스트 및 해시 리스트를 해시 리스트 생성부(203)에 출력한다.

<249> (3) 해시 리스트 생성부(203)

<250> 해시 리스트 생성부(203)는, 도 8에 도시한 바와 같이, 개찬검출 키 기억부(210), 데이터 수신부(211), 해시 리스트 생성 처리부(212), 암호화 처리부(213) 및 갱신데이터 리스트 생성부(214)로 구성되어 있다.

<251> 여기서, 해시 리스트 생성부(203)는 하나의 장치(해시 리스트 생성장치)로 해도 좋다.

<252> (개찬검출 키 기억부(210))

<253> 개찬검출 키 기억부(210)는 개찬검출 키(215)를 기억하고 있다.

<254> (데이터 수신부(211))

<255> 데이터 수신부(211)는 데이터 취득부(202)로부터 초기설정지시, 제 1 갱신지시 및 제 2 갱신지시 중 어느 하나를 수신한다.

<256> 데이터 수신부(211)는 초기설정지시를 수신하면, 개찬검출대상이 되는 하나 이상의 파일 및 타깃 패스 리스트를 더 수신하고, 수신한 초기설정지시, 하나 이상의 파일 및 타깃 패스 리스트를 해시 리스트 생성 처리부(212)에 출력한다.

<257> 데이터 수신부(211)는 제 1 갱신지시를 수신하면, 갱신대상이 되는 하나 이상의 파일의 각각에 대한 갱신파일, 갱신대상이 되는 하나 이상의 파일의 타깃 패스 리스트 및 해시 리스트를 수신하고, 수신한 제 1 갱신지시, 하나 이상의 갱신파일, 타깃 패스 리스트 및 해시 리스트를 해시 리스트 생성 처리부(212)에 출력한다.

<258> 데이터 수신부(211)는 제 2 갱신지시를 수신하면, 부분 키, 갱신된 부분 키를 이용한 개찬검출의 대상이 되는 하나 이상의 파일, 타깃 패스 리스트 및 해시 리스트를 더 수신하고, 수신한 제 2 갱신지시, 부분 키, 하나 이상의 파일, 타깃 패스 리스트 및 해시 리스트를 해시 리스트 생성 처리부(212)에 출력한다.

<259> (해시 리스트 생성 처리부(212))

<260> 해시 리스트 생성 처리부(212)는 데이터 수신부(211)로부터 초기설정지시, 제 1 갱신지시 및 제 2 갱신지시 중 어느 하나를 더 수신한다.

<261> <초기설정지시를 수신한 경우>

<262> 해시 리스트 생성 처리부(212)는 초기설정지시를 수신하면, 개찬검출대상이 되는 하나 이상의 파일 및 타깃 패스 리스트를 수신한다.

<263> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 파일 중 하나의 파일을 소정의 사이즈로 이루어지는 하나 이상의 블록으로 분할한다. 해시 리스트 생성 처리부(212)는 분할된 파일이 휴대전화기(10)에서 저장되어 있는 위치를 나타내는 패스 명을 타깃 패스 리스트에서 판독하고, 분할한 블록의 수와 판독한 패스 명으로 이루어지는 파일정보를 생성한다. 또, 해시 리스트 생성 처리부(212)는 개찬검출 키 기억부(210)에서 개찬검출 키(215)를 판독한다. 해시 리스트 생성 처리부(212)는 소정의 사이즈로 분할한 블록 단위로 판독한 개찬검출 키(215)와 해시 계산 알고리즘을 이용하여 해시 값을 산출하고, 각 블록에 대하여 블록의 선두 위치를 나타내는 오프셋과, 블록의 사이즈와, 산출한 해시 값으로 이루어지는 엔트리를 생성하며, 생성한 각 엔트리를 포함하는 MAC정보를 생성한다. 해시 리스트 생성 처리부(212)는 생성한 파일정보와 MAC정보로 이루어지는 해시 정보를 생성한다. 또한, 이때 해시 정보는 아직 암호화되어 있지 않다. 이 동작을 수신한 모든 파일에 대하여 행한다.

<264> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 파일의 각각에 대한 해시 정보를 생성하면 생성한 모든 해시 정보로 이루어지는 데이터부를 생성한다. 이때 데이터부는 암호화되어 있지 않다. 이하, 암호화된 데이터부를 구별하기 위해 암호화되어 있지 않은 데이터부를 비 암호화 데이터부라고 한다.

<265> 해시 리스트 생성 처리부(212)는 생성한 비 암호화 데이터부를 암호화 처리부(213)에 출력한다.

<266> 해시 리스트 생성 처리부(212)는 암호화 처리부(213)에서 암호화된 데이터부를 수신하면, 암호화된 데이터부에 대하여 해시 계산 알고리즘을 적용하여 해시 값을 산출하여 해시 리스트의 데이터부 해시 값에 기록한다. 해시 리스트 생성 처리부(212)는 해시 리스트의 사이즈를 산출하고, 산출결과를 해시 리스트 파일 사이즈에 기록한다. 이에 의해, 해시 리스트 생성 처리부는 해시 리스트의 헤더부를 생성할 수 있다.

<267> 해시 리스트 생성 처리부(212)는 생성한 헤더부와 암호화 처리부(213)에서 수신한 암호화된 데이터부로 이루어지는 해시 리스트를 생성한다.

<268> 해시 리스트 생성 처리부(212)는 생성한 해시 리스트를 기억부에 저장하는 동시에 해시 리스트 기록부(204)에 출력한다. 이때, 생성한 해시 리스트와 초기설정지시에 포함되는 AP 식별정보가 대응이 부여되어 있다.

<269> <제 1 갱신지시를 수신한 경우>

<270> 해시 리스트 생성 처리부(212)는 데이터 수신부(211)에서 제 1 갱신지시를 수신하면, 갱신대상이 되는 하나 이상의 파일의 각각에 대한 갱신파일, 갱신대상이 되는 하나 이상의 파일의 타깃 패스 리스트 및 해시 리스트를

더 수신한다. 이하에서는 데이터 수신부(211)에서 수신한 해시 리스트를 구 해시 리스트(old hash list)라고 한다.

<271> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 갱신파일 중 하나의 갱신파일을 소정의 사이즈로 이루어지는 하나 이상의 블록으로 분할한다. 해시 리스트 생성 처리부(212)는 분할된 갱신파일이 휴대전화기(10)에 저장되어 있는 위치를 나타내는 패스 명을 타깃 패스 리스트에서 판독하고, 분할한 블록의 수와 판독한 패스 명으로 이루어지는 파일정보를 생성한다. 또, 해시 리스트 생성 처리부(212)는 개찬검출 키 기억부(210)에서 개찬검출 키(215)를 판독한다. 해시 리스트 생성 처리부(212)는 소정의 사이즈로 분할한 블록 단위로 판독한 개찬검출 키(215)와 해시 계산 알고리즘을 이용하여 해시 값을 산출하고, 각 블록에 대하여 블록의 선두 위치를 나타내는 오프셋과, 블록의 사이즈와, 산출한 해시 값으로 이루어지는 엔트리를 생성하여, 생성한 각 엔트리를 포함하는 MAC정보를 생성한다. 해시 리스트 생성 처리부(212)는 생성한 파일정보와 MAC정보로 이루어지는 해시 정보를 생성한다. 또한, 이때, 해시 정보는 아직 암호화되어 있지 않다. 이 동작을 수신한 모든 갱신파일에 대하여 행한다.

<272> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 갱신파일의 각각에 대한 해시 정보를 생성하면, 생성한 모든 해시 정보로 이루어지는 비 암호화 데이터부를 생성한다.

<273> 해시 리스트 생성 처리부(212)는 생성한 비 암호화 데이터부를 암호화 처리부(213)에 출력한다.

<274> 해시 리스트 생성 처리부(212)는 암호화 처리부(213)에서 암호화된 데이터부를 수신하면, 암호화된 데이터부에 대하여 해시 계산 알고리즘을 적용하여 해시 값을 산출하고, 해시 리스트의 데이터부 해시 값에 기록한다. 해시 리스트 생성 처리부(212)는 해시 리스트의 사이즈를 산출하고, 산출결과를 해시 리스트 파일 사이즈에 기록한다. 이에 의해, 해시 리스트 생성 처리부는 해시 리스트의 헤더부를 생성할 수 있다.

<275> 해시 리스트 생성 처리부(212)는 생성한 헤더부와 암호화 처리부(213)에서 수신한 암호화된 데이터부로 이루어지는 신 해시 리스트(new hash list)를 생성한다.

<276> 해시 리스트 생성 처리부(212)는 제 1 갱신지시, 생성한 신 해시 리스트와, 데이터 수신부(211)로부터 수신한 구 해시 리스트 및 하나 이상의 갱신파일을 갱신데이터 리스트 생성부(214)에 출력한다.

<277> <제 2 갱신지시를 수신한 경우>

<278> 해시 리스트 생성 처리부(212)는 데이터 수신부(211)에서 제 2 갱신지시를 수신하면, 부분 키, 검출대상이 되는 하나 이상의 파일, 타깃 패스 리스트 및 구 해시 리스트를 더 수신한다.

<279> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 파일 중 하나의 파일을 소정의 사이즈로 이루어지는 하나 이상의 블록으로 분할한다. 해시 리스트 생성 처리부(212)는 분할된 갱신파일이 휴대전화기(10)에 저장되어 있는 위치를 나타내는 패스 명을 타깃 패스 리스트에서 판독하고, 분할한 블록의 수와 판독한 패스 명으로 이루어지는 파일정보를 생성한다. 또, 해시 리스트 생성 처리부(212)는 개찬검출 키 기억부(210)에서 개찬검출 키(215)를 판독한다. 해시 리스트 생성 처리부(212)는 소정의 사이즈로 분할한 블록 단위로 판독한 개찬검출 키(215)와 해시 계산 알고리즘을 이용하여 해시 값을 산출하고, 각 블록에 대하여 블록의 선두 위치를 나타내는 오프셋과, 블록의 사이즈와, 산출한 해시 값으로 이루어지는 엔트리를 생성하고, 생성한 각 엔트리를 포함하는 MAC정보를 생성한다. 해시 리스트 생성 처리부(212)는 생성한 파일정보와 MAC정보로 이루어지는 해시 정보를 생성한다. 또한, 이때, 해시 정보는 아직 암호화되어 있지 않다. 이 동작을 수신한 모든 파일에 대하여 행한다.

<280> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 파일의 각각에 대한 해시 정보를 생성하면, 생성한 모든 해시 정보로 이루어지는 비 암호화 데이터부를 생성한다.

<281> 해시 리스트 생성 처리부(212)는 생성한 비 암호화 데이터부를 암호화 처리부(213)에 출력한다.

<282> 해시 리스트 생성 처리부(212)는 암호화 처리부(213)로부터 암호화된 데이터부를 수신하면, 암호화된 데이터부에 대하여 해시 계산 알고리즘을 적용하여 해시 값을 산출하고, 해시 리스트의 데이터부 해시 값에 기록한다. 해시 리스트 생성 처리부(212)는 해시 리스트의 사이즈를 산출하고, 산출결과를 해시 리스트 파일 사이즈에 기록한다. 이에 의해, 해시 리스트 생성 처리부는 해시 리스트의 헤더부를 생성할 수 있다.

<283> 해시 리스트 생성 처리부(212)는 생성한 헤더부와 암호화 처리부(213)에서 수신한 암호화된 데이터부로 이루어지는 신 해시 리스트(new hash list)를 생성한다.

<284> 해시 리스트 생성 처리부(212)는 제 2 갱신지시와, 생성한 신 해시 리스트와, 데이터 수신부(211)에서 수신한

구 해시 리스트 및 부분 키를 갱신데이터 리스트 생성부(214)에 출력한다.

<285> (암호화 처리부(213))

<286> 암호화 처리부(213)는 해시 리스트 생성 처리부(212)로부터 비 암호화 데이터부를 수신하면 개찬검출 키 기억부(210)에서 개찬검출 키(215)를 판독한다.

<287> 암호화 처리부(213)는 판독한 개찬검출 키를 이용하여 수신한 비 암호화 데이터부를 암호화한다. 암호에 이용되는 알고리즘은, 예를 들어 XOR과 같은 논리연산 또는 DES, AES와 같은 암호 알고리즘이며, 휴대전화기(10)에 이용되는 복호 알고리즘에 대응하는 것이다. 이때, 암호화는 파일정보나 MAC정보의 1 엔트리를 단위로 행해진다.

<288> 암호화 처리부(213)는 암호화된 데이터부를 해시 리스트 생성 처리부(212)에 출력한다.

<289> (갱신데이터 리스트 생성부(214))

<290> 갱신데이터 리스트 생성부(214)는 제 1 갱신지시 및 제 2 갱신지시 중 어느 하나를 수신한다.

<291> <제 1 갱신지시를 수신한 경우>

<292> 갱신데이터 리스트 생성부(214)는 해시 리스트 생성 처리부(212)로부터 신 해시 리스트, 구 해시 리스트와 하나 이상의 갱신파일을 수신한다.

<293> 갱신데이터 리스트 생성부(214)는 수신한 구 해시 리스트와 신 해시 리스트를 비교하여 정보가 다른 개소를 해시 리스트에서 추출한다. 여기서, 추출되는 정보는 데이터부에서의 엔트리나 헤더부에서의 데이터부 해시 값이다.

<294> 갱신데이터 리스트 생성부(214)는 추출된 정보와 하나 이상의 갱신파일을 이용하여 갱신데이터 리스트를 생성한다. 이때, 갱신데이터 리스트 생성부(214)는 추출된 정보에 의해 갱신파일의 갱신 개소를 특정할 수 있다. 왜냐하면, 파일을 분할할 때에는 각 블록은 소정의 사이즈가 되도록 분할되어 있으므로 변경이 생기지 않는 블록의 해시 값은 이전의 해시와 동일해진다. 변경이 생긴 블록의 해시 값은 이전의 해시 값과 상이하므로, 변경된 개소를 포함하는 블록에 대한 엔트리는 구 해시 리스트와 신 해시 리스트의 비교에 의해 추출된다. 상술한 바와 같이, 블록은 소정의 사이즈가 되도록 분할되어 있으므로, 추출된 엔트리로부터 갱신파일에서의 갱신 개소를 특정할 수 있다. 갱신데이터 리스트 생성부(214)는 특정한 갱신 개소를 갱신데이터로 하고, 갱신데이터(즉, 갱신 개소를 포함하는 블록)의 위치정보 및 블록의 사이즈를 취득한다. 또한, 갱신 개소를 포함하는 블록이 연속해 있는 경우에는 하나의 갱신데이터로 결합해도 된다. 이때의 위치정보는 연속하는 블록 중 선두에 위치하는 블록의 위치정보가 되고, 사이즈는 연속하는 블록의 개수로부터 산출할 수 있다.

<295> 갱신데이터 리스트 생성부(214)는 갱신데이터, 위치정보 및 블록의 사이즈로 이루어지는 갱신정보를 하나 이상 생성하고, 또한, 생성한 하나 이상의 갱신정보로 이루어지는 갱신데이터 리스트를 생성한다.

<296> 갱신데이터 리스트 생성부(214)는 신 해시 리스트와 생성한 갱신데이터 리스트를 기억부(201)에 저장한다. 이때, 생성한 갱신데이터 리스트와 제 1 갱신지시에 포함되는 AP 식별정보가 대응이 부여되어 있다. 또, 기억부(201)에 기억되어 있는 구 해시 리스트는 소거된다.

<297> <제 2 갱신지시를 수신한 경우>

<298> 갱신데이터 리스트 생성부(214)는 해시 리스트 생성 처리부(212)로부터 신 해시 리스트와 구 해시 리스트 및 부분 키를 더 수신한다.

<299> 갱신데이터 리스트 생성부(214)는 수신한 구 해시 리스트와 신 해시 리스트를 비교하여 정보가 다른 개소를 신 해시 리스트에서 추출한다. 여기서, 추출되는 정보는 데이터부에서의 엔트리나 헤더부에서의 데이터부 해시 값이다.

<300> 갱신데이터 리스트 생성부(214)는 추출된 정보 및 수신한 부분 키 각각을 갱신데이터로 하는 갱신데이터 리스트를 생성한다. 부분 키를 갱신데이터로 하는 갱신정보의 생성은 이하와 같이하여 행한다. 갱신데이터 리스트 생성부(214)는 휴대전화기(10)에서의 부분 키의 기억위치를 나타내는 위치정보와 수신한 부분 키의 데이터 사이즈를 취득한다. 갱신데이터 리스트 생성부(214)는 취득한 위치정보와 데이터 사이즈 및 갱신데이터인 부분 키로 이루어지는 갱신정보를 생성한다.

<301> 또한, 추출된 정보를 갱신데이터로 하는 갱신정보의 생성은 제 1 갱신지시를 수신한 경우에서 설명한 갱신정보

의 생성과 동일하므로, 여기에서는 설명을 생략한다.

<302> 갱신데이터 리스트 생성부(214)는 생성한 하나 이상의 갱신정보로 이루어지는 갱신데이터 리스트를 생성한다.

<303> 갱신데이터 리스트 생성부(214)는 신 해시 리스트와 생성한 갱신데이터 리스를 기억부(201)에 저장한다. 이때, 생성한 갱신데이터 리스트와 제 2 갱신지시에 포함되는 AP 식별정보가 대응이 부여되어 있다. 또, 기억부(201)에 기억되어 있는 구 해시 리스트는 소거된다.

<304> (4) 해시 리스트 기록부(204)

<305> 해시 리스트 기록부(204)는 휴대전화기의 제조시에 제조 중(출하 전)인 휴대전화기와 접속되며, 휴대전화기의 기억부에 대한 액세스가 가능하다.

<306> 해시 리스트 기록부(204)는 해시 리스트 생성부(203)로부터 해시 리스트를 수신하면 수신한 해시 리스트를 접속된 휴대전화기의 기억부에 기록한다. 해시 리스트가 기록되는 어드레스는 상술한 바와 같이 고정된 어드레스이다.

<307> (5) 갱신요구 처리부(205)

<308> 갱신요구 처리부(205)는 송수신부(207)를 통해서 휴대전화기(10)로부터 AP 식별정보, 단말 식별자, 갱신요구정보를 수신하면, 수신한 AP 식별정보와 단말 식별자를 이용하여 휴대전화기(10)에 송신해야 할 갱신데이터 리스트의 판 수를 결정한다.

<309> 상술한 바와 같이, 갱신 서버장치(20)는 갱신데이터 리스트의 각각을, 갱신대상의 파일을 포함하는 AP의 AP 식별정보와 대응 부여, 및 판 수의 관리를 행하고 있고, 또, 휴대전화기(10)의 단말 식별자와 휴대전화기(10)에 송신한 갱신데이터 리스트의 판 수를 대응시켜서 관리하고 있으므로, 송신해야 할 갱신데이터 리스트를 결정할 수 있다.

<310> 갱신요구 처리부(205)는 송신해야 할 갱신데이터 리스트를 기억부(201)에서 취득하고, 취득한 갱신데이터 리스트를 송수신부(207)를 통해서 휴대전화기(10)에 송신한다.

<311> (6) 입력부(206)

<312> 입력부(206)는 사용자의 조작에 의해 초기설정지시를 접수하면 접수한 초기설정지시를 데이터 취득부(202)에 출력한다.

<313> 입력부(206)는 사용자의 조작에 의해 제 1 갱신지시를 접수하면 접수한 제 1 갱신지시를 데이터 취득부(202)에 출력한다.

<314> (7) 송수신부(207)

<315> 송수신부(207)는 휴대 망(40) 및 인터넷(50)을 통해서 휴대전화기(10)로부터 수신한 정보를 갱신요구 처리부(205)에 출력한다.

<316> 송수신부(207)는 갱신요구 처리부(205)에서 수신한 정보를 인터넷(50) 및 휴대 망(40)을 통해서 휴대전화기(10)에 송신한다.

<317> 1. 4 키 갱신장치(30)의 구성

<318> 키 갱신장치(30)는, 도 9에 도시한 바와 같이, 키 취득부(301), 개찬검출 키 생성부(302), 개찬검출 키 배포부(303) 및 출력부(304)로 구성되어 있다.

<319> 키 갱신장치(30)는 개찬검출 키가 악의가 있는 사용자에 의해 해석되어서 부정하게 유출된 경우에 갱신 서버장치(20)에 기억되어 있는 개찬검출 키를 갱신한다. 키 갱신장치(30)는 키를 정식으로 발행하는 기관에 의해 엄중하게 관리되는 것으로 한다.

<320> (1) 키 취득부(301)

<321> 키 취득부(301)는 외부장치로부터 마스터 키 및 갱신된 부분 키와, 갱신된 부분 키에 대응하는 AP의 AP 식별정보를 취득한다. 또한, 취득하는 마스터 키는 휴대전화기(10)에 기억되어 있는 마스터 키와 동일한 것이다.

<322> 키 취득부(301)는 수신한 마스터 키 및 갱신된 부분 키를 개찬검출 키 생성부(302)에 출력한다.

<323> 키 취득부(301)는 개찬검출 키 배포부(303)로부터 갱신 서버장치(20)에 대하여 개찬검출 키의 배포가 완료했다

는 취지를 나타내는 배포완료명령을 수신하면, AP 식별정보를 포함하는 제 2 갱신지시와 갱신된 부분 키를 출력부(304)에 출력한다.

<324> (2) 개찬검출 키 생성부(302)

<325> 개찬검출 키 생성부(302)는 키 취득부(301)로부터 마스터 키 및 갱신된 부분 키를 수신하면, 수신한 마스터 키와, 갱신된 부분 키 및 특정 알고리즘을 이용하여 개찬검출 키를 산출한다. 또한, 여기에서 이용하는 특정 알고리즘은 휴대전화기(10)의 개찬검출 처리부(173)에서 이용되는 알고리즘과 동일한 것이다.

<326> 개찬검출 키 생성부(302)는 산출한 개찬검출 키를 개찬검출 키 배포부(303)에 출력한다.

<327> (3) 개찬검출 키 배포부(303)

<328> 개찬검출 키 배포부(303)는 갱신 서버장치(20)와 접속되며, 개찬검출 키 기억부(210)에 액세스 가능하다.

<329> 개찬검출 키 배포부(303)는 개찬검출 키 생성부(302)로부터 개찬검출 키를 수신하면, 수신한 개찬검출 키를 개찬검출 키 기억부(210)에 기록한다. 이때, 개찬검출 키 기억부(210)에 기억되어 있던 이전의 개찬검출 키는 소거된다.

<330> 개찬검출 키 배포부(303)는 개찬검출 키의 기록이 완료하면 배포완료명령을 키 취득부(301)에 출력한다.

<331> (4) 출력부(304)

<332> 출력부(304)는 갱신 서버장치(20)의 데이터 취득부(202)와 접속된다.

<333> 출력부(304)는 키 취득부(301)로부터 제 2 갱신지시와 갱신된 부분 키를 수신하면, 수신한 제 2 갱신지시와 갱신된 부분 키를 데이터 취득부(202)에 출력한다.

<334> 1. 5 갱신 서버장치(20)의 동작

<335> 여기에서는, 갱신 서버장치(20)에서의 갱신데이터 리스트 및 해시 리스트의 생성의 동작에 대해서 도 10에 도시한 흐름도를 이용하여 설명한다.

<336> 데이터 수신부(211)는 데이터 취득부(202)로부터 초기설정지시, 제 1 갱신지시 및 제 2 갱신지시 중 어느 하나를 수신한다(스텝 S5).

<337> 데이터 수신부(211)는 제 1 갱신지시를 수신하면(스텝 S10에서의 「제 1 갱신지시」) 갱신대상이 되는 하나 이상의 파일의 각각에 대한 갱신파일, 갱신대상이 되는 하나 이상의 파일의 타깃 패스 리스트 및 해시 리스트를 취득한다(스텝 S15).

<338> 데이터 수신부(211)는 수신한 제 1 갱신지시, 하나 이상의 갱신파일, 타깃 패스 리스트 및 해시 리스트(이하, 구 해시 리스트)를 해시 리스트 생성 처리부(212)에 출력한다. 해시 리스트 생성 처리부(212)는 데이터 수신부(211)로부터 제 1 갱신지시, 하나 이상의 파일의 각각에 대한 갱신파일, 갱신대상이 되는 하나 이상의 파일의 타깃 패스 리스트 및 구 해시 리스트를 수신한다.

<339> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 갱신파일 중 하나의 갱신파일을 소정의 사이즈로 이루어지는 하나 이상의 블록으로 분할한다. 해시 리스트 생성 처리부(212)는 분할된 갱신파일이 휴대전화기(10)에 저장되어 있는 위치를 나타내는 패스 명을 타깃 패스 리스트에서 판독하고, 분할한 블록의 수와 판독한 패스 명으로 이루어지는 파일정보를 생성한다. 또, 해시 리스트 생성 처리부(212)는 소정의 사이즈로 분할한 블록 단위로 해시 계산 알고리즘을 적용하여 해시 값을 산출하고, 각 블록에 대하여 블록의 선두 위치를 나타내는 오프셋과, 블록의 사이즈와, 산출한 해시 값으로 이루어지는 엔트리를 생성하며, 생성한 각 엔트리를 포함하는 MAC정보를 생성한다. 해시 리스트 생성 처리부(212)는 생성한 파일정보와 MAC정보로 이루어지는 해시 정보를 생성한다. 또한, 이때 해시 정보는 아직 암호화되어 있지 않다. 이 동작을 수신한 모든 갱신파일에 대하여 행한다.

<340> 해시 리스트 생성 처리부(212)는 수신한 하나 이상의 갱신파일의 각각에 대한 해시 정보를 생성하면, 생성한 모든 해시 정보로 이루어지는 비 암호화 데이터부를 생성한다(스텝 S20).

<341> 해시 리스트 생성 처리부(212)는 생성한 비 암호화 데이터부를 암호화 처리부(213)에 출력한다. 암호화 처리부(213)는 해시 리스트 생성 처리부(212)로부터 비 암호화 데이터부를 수신하면, 개찬검출 키 기억부(210)에서 개찬검출 키(215)를 판독한다. 암호화 처리부(213)는 판독한 개찬검출 키를 이용하여 수신한 비 암호화 데이터부를 암호화한다(스텝 S25). 이때, 암호화는 파일정보나 MAC정보의 1 엔트리를 단위로 행해진다.

<342> 암호화 처리부(213)는 암호화된 데이터부를 해시 리스트 생성부(212)에 출력한다. 해시 리스트 생성 처리부(212)는 암호화 처리부(213)로부터 암호화된 데이터부를 수신하면, 암호화된 데이터부에 대하여 해시 계산 알고리즘을 적용하여 해시 값을 산출하고, 해시 리스트의 데이터부 해시 값에 기록한다(스텝 S30).

<343> 해시 리스트 생성 처리부(212)는 해시 리스트의 사이즈를 산출하고, 산출결과를 해시 리스트 파일 사이즈에 기록한다. 이에 의해, 해시 리스트 생성 처리부는 해시 리스트의 헤더부를 생성할 수 있다.

<344> 해시 리스트 생성 처리부(212)는 생성한 헤더부와 암호화 처리부(213)에서 수신한 암호화된 데이터부로 이루어지는 신 해시 리스트를 생성한다(스텝 S35).

<345> 해시 리스트 생성 처리부(212)는 제 1 갱신지시, 생성한 신 해시 리스트와, 데이터 수신부(211)에서 수신한 구 해시 리스트 및 하나 이상의 갱신파일을 갱신데이터 리스트 생성부(214)에 출력한다. 갱신데이터 리스트 생성부(214)는 제 1 갱신지시, 해시 리스트 생성 처리부(212)에서 신 해시 리스트와, 구 해시 리스트 및 하나 이상의 갱신파일을 수신한다.

<346> 갱신데이터 리스트 생성부(214)는 수신한 구 해시 리스와 신 해시 리스트를 비교하여 정보가 다른 개소를 신 해시 리스트에서 추출한다. 여기서, 추출되는 정보는 데이터부에서의 엔트리나 헤더부에서의 데이터부 해시 값이다. 갱신데이터 리스트 생성부(214)는 추출된 정보와 하나 이상의 갱신파일을 이용하여 갱신데이터 리스트를 생성한다(스텝 S40).

<347> 갱신데이터 리스트 생성부(214)는 신 해시 리스트와 생성한 갱신데이터 리스트를 기억부(210)에 저장한다(스텝 S45). 이때, 생성한 갱신데이터 리스트와 제 1 갱신지시에 포함되는 AP 식별정보는 대응이 부여되어 있다. 또, 기억부(201)에 기억되어 있는 구 해시 리스트는 소거된다.

<348> 데이터 수신부(211)는 제 2 갱신지시를 수신하면(스텝 S10에서의 「제 2 갱신지시」), 부분 키, 검출대상이 되는 하나 이상의 파일, 타깃 패스 리스트 및 해시 리스트를 취득하고(스텝 S50), 스텝 S20에서 스텝 S45까지의 동작을 행한다. 또, 이 경우, 각 구성요소가 출력 및 수신하는 지시는 제 2 갱신지시가 된다. 또, 스텝 S40에서 생성되는 갱신데이터 리스트는 구 해시 리스트, 신 해시 리스트 및 부분 키로 생성된다. 또, 스텝 S45에서는 생성한 갱신데이터 리스트와 제 2 갱신지시에 포함되는 AP 식별정보가 대응이 부여되어 있다.

<349> 데이터 수신부(211)는 초기설정지시를 수신하면(스텝 S10에서의 「초기설정지시」), 개찬검출대상이 되는 하나 이상의 파일 및 타깃 패스 리스트를 취득한다(스텝 S55).

<350> 데이터 수신부(211)는 수신한 초기설정지시와 하나 이상의 파일 및 타깃 패스 리스트를 해시 리스트 생성부(212)에 출력한다.

<351> 해시 리스트 생성 처리부(212)는, 초기설정지시를 수신하고, 또한, 개찬검출대상이 되는 하나 이상의 파일 및 타깃 패스 리스트를 수신하면 해시 리스트를 생성한다(스텝 S60). 또한, 해시 리스트의 생성에 대해서는 스텝 S20에서 스텝 S35까지의 동작과 개념적으로는 동일하므로, 여기에서는 상세한 설명을 생략한다.

<352> 해시 리스트 생성 처리부(212)는 생성한 해시 리스트를 기억부에 저장하는 동시에 해시 리스트 기록부(204)에 출력한다. 해시 리스트 기록부(204)는 해시 리스트 생성부(203)로부터 해시 리스트를 수신하면 수신한 해시 리스트를 접속된 휴대전화기의 기억부에 기록한다(스텝 S65).

<353> 1. 6 해시 리스트 갱신시의 동작의 개요

<354> 여기에서는 해시 리스트 갱신시의 동작의 개요에 대해서 도 11에 도시한 흐름도를 이용하여 설명한다.

<355> 휴대전화기(10)에서의 갱신처리부(103)의 갱신제어부(162)는 갱신지시를 접수하면(스텝 S100) 제어부(102)에 대하여 인터럽트 금지의 설정을 행한다(스텝 S105).

<356> 갱신제어부(162)는 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「1」로 설정한다(스텝 S110).

<357> 갱신제어부(162)는 수신한 갱신개시명령에 포함되는 AP 식별정보를 갱신데이터 판독부(163)에 출력한다.

<358> 갱신파일 수신부(104)는 갱신처리부(103)의 갱신데이터 판독부(163)로부터 AP 식별정보를 수신하면, 수신한 AP 식별정보와, 미리 기억하고 있는 단말 식별자 및 갱신요구정보를 무선부(110)를 통해서 갱신 서버장치(20)에 송신한다(스텝 S115). 갱신파일 수신부(104)는 수신한 AP 식별정보를 AP 식별정보 기억영역에 저장한다.

<359> 갱신 서버장치(20)의 갱신요구 처리부(205)는 송수신부(207)를 통해서 휴대전화기(10)로부터 AP 식별정보와, 단

말 식별자 및 갱신요구정보를 수신한다(스텝 S120).

<360> 갱신요구 처리부(205)는 수신한 AP 식별정보와 단말 식별자를 이용하여 휴대전화기(10)에 송신해야 할 갱신데이터 리스트의 판 수를 결정한다. 갱신요구 처리부(205)는 송신해야 할 갱신데이터 리스트를 기억부(201)에서 취득하고(스텝 S125), 취득한 갱신데이터 리스트를 송수신부(207)를 통해서 휴대전화기(10)에 송신한다(스텝 S130).

<361> 휴대전화기(10)는 갱신 서버장치(20)로부터 갱신데이터 리스트를 수신하고, 갱신처리를 행한다(스텝 S135).

<362> 1. 7 갱신처리의 동작

<363> 여기에서는, 도 11의 스텝 S135에서 나타내는 갱신처리의 동작에 대해서 도 12 및 도 13에 도시한 흐름도를 이용하여 설명한다.

<364> 갱신파일 수신부(104)는 갱신 서버장치(20)로부터 무선부(110)를 통해서 갱신데이터 리스트를 수신하면 수신한 갱신데이터 리스트를 리스트 기억영역에 저장한다(스텝 S200).

<365> 갱신파일 수신부(104)는 수신한 갱신데이터 리스트의 저장이 완료하면, AP 식별정보 기억영역에 저장되어 있는 AP 식별정보를 소거하고, 수신완료명령을 갱신데이터 판독부(163)에 출력한다. 갱신데이터 판독부(163)는 갱신파일 수신부(104)로부터 갱신 서버장치(20)에서 갱신데이터 리스트의 수신이 완료했다는 취지의 수신완료명령을 수신한다.

<366> 갱신데이터 판독부(163)는 갱신파일 수신부(104)의 리스트 기억영역에 기억되어 있는 갱신데이터 리스트에서 미 판독의 갱신정보를 하나 판독한다(스텝 S205).

<367> 갱신데이터 해석부(164)는 갱신데이터 판독부(163)에서 판독된 갱신정보를 위치정보, 데이터 사이즈 및 갱신데이터로 분할한다(스텝 S210).

<368> 기록위치 결정부(165)는 갱신데이터 해석부(164)에서 취득된 위치정보에 의거하여 기억부(101)에서의 갱신데이터의 기록위치를 결정한다(스텝 S215).

<369> 갱신데이터 기록부(166)는 기록위치 결정부(165)에서 결정된 기록위치를 기록개시의 선두 위치로 갱신데이터 해석부(164)에서 취득된 갱신데이터를 기록한다(스텝 S220).

<370> 갱신 확인부(167)는 갱신데이터 기록부(166)에 의한 기록이 정상으로 종료하였는가 여부를 확인한다(스텝 S225).

<371> 정상으로 종료하고 있지 않다고 판단한 경우에는(스텝 S225에서의 「YES」) 갱신 확인부(167)는 이상종료명령을 갱신데이터 판독부(163)에 출력한다. 갱신데이터 판독부(163)는 갱신 확인부(167)에서 이상종료명령을 수신하면, 스텝 S205에서 판독한 갱신정보와 동일한 갱신정보를 다시 판독하고(스텝 S230), 스텝 S210에 되돌아간다.

<372> 정상으로 종료했다고 판정한 경우에는(스텝 S225에서의 「YES」) 갱신 확인부(167)는 정상종료명령을 갱신데이터 판독부(163)에 출력한다. 갱신데이터 판독부(163)는 갱신 확인부(167)로부터 정상종료명령을 수신하면 갱신파일 수신부(104)의 리스트 기억영역에 기억되어 있는 갱신데이터 리스트에 미 판독의 갱신정보가 존재하는가 여부를 판단한다(스텝 S235).

<373> 존재한다고 판단한 경우에는(스텝 S235에서의 「YES」) 갱신데이터 판독부(163)는 스텝 S205에 되돌아간다. 존재하지 않는다고 판단한 경우에는(스텝 S235에서의 「NO」) 갱신데이터 판독부(163)는 기록완료명령을 갱신제어부(162) 및 갱신파일 수신부(104)에 출력한다. 갱신파일 수신부(104)는 갱신데이터 판독부(163)로부터 기록완료명령을 수신하면 리스트 저장영역에 저장되어 있는 갱신데이터 리스트(150)를 소거한다. 갱신제어부(162)는 갱신데이터 판독부(163)로부터 기록완료명령을 수신하면 개찬검출의 처리를 개시하는 취지의 검출개시명령과 AP 식별정보를 개찬검출 실행부(105)에 출력한다.

<374> 개찬검출 실행부(105)는 갱신제어부(162)로부터 검출개시명령과 AP 식별정보를 수신하면 개찬검출 처리를 행한다(스텝 S240).

<375> 갱신제어부(162)는 개찬검출 실행부(105)로부터 개찬검출 처리의 처리결과를 수신하면, 수신한 처리결과가 개찬되어 있지 않다는 통지인가, 개찬이 검출되었다는 통지인가를 판단한다(스텝 S245).

<376> 개찬이 검출되어 있지 않은, 즉, 개찬되어 있지 않다는 통지를 수신하였다고 판단한 경우에는(스텝 S245에서의

「NO」) 갱신제어부(162)는 갱신완료의 통지를 제어부(102)에 출력한다. 제어부(102)는 갱신처리부(103)로부터 파일의 갱신완료의 통지를 수신하면 표시부(109)를 통해서 갱신완료의 메시지를 표시한다(스텝 S250).

<377> 갱신제어부(162)는 제어부(102)에 대한 인터럽트 금지를 해제하고(스텝 S225) 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「0」으로 설정한다(스텝 S260).

<378> 개찬이 검출된, 즉, 개찬이 검출되었다는 통지를 수신하였다고 판단한 경우에는(스텝 S245에서의 「YES」) 갱신제어부(162)는 갱신실패의 통지를 제어부(102)에 출력한다. 제어부(102)는 갱신처리부(103)로부터 파일의 갱신실패의 통지를 수신하면 표시부(109)를 통해서 갱신실패의 메시지를 표시한다(스텝 S265). 또, 제어부(102)는 입력부(108)로부터 재갱신의 지시를 수신하면 재갱신 개시 명령을 갱신처리부(103)에 출력한다. 제어부(102)는 입력부(108)로부터 재갱신을 행하지 않는다는 지시를 수신하면 갱신종료명령을 갱신처리부(103)에 출력한다.

<379> 갱신제어부(162)는 제어부(102)로부터 재갱신 개시명령 및 갱신종료명령 중 어느 하나를 수신하면 수신한 명령이 재갱신 개시명령인지 여부를 판단한다(스텝 S270). 재갱신 개시 명령, 즉, 재갱신을 행하는 것으로 판단한 경우에는(스텝 S270에서의 「YES」) 갱신제어부(162)는 다시 AP 식별정보를 갱신데이터 판독부(163)에 출력하고, 스텝 S200에 되돌아간다. 이 경우, 갱신데이터 판독부(163)는 다시 갱신데이터 리스트의 수신을 행한다.

<380> 갱신제어부(162)는 수신한 명령이 갱신종료명령인, 즉, 재갱신을 행하지 않는다고 판단한 경우에는(스텝 S270에서의 「NO」), 갱신제어부(162)는 제어부(102)에 대한 인터럽트 금지를 해제하고(스텝 S255), 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「0」으로 설정한다(스텝 S260).

<381> 1. 8 AP 기동시의 동작

<382> 여기에서는, AP 기동시의 동작에 대해서 도 14에 도시한 흐름도를 이용하여 설명한다.

<383> 제어부(102)는 입력부(108)로부터 개찬검출대상의 AP의 기동지시를 수신한다(스텝 S300). 제어부(102)는 AP의 기동을 행한다. 이때, 기동 된 AP는 자 AP가 개찬검출대상인 경우에는 검출개시명령과 자 AP를 식별하는 AP 식별정보를 제어부(102)에 의해 개찬검출 실행부(105)에 출력한다.

<384> 개찬검출 실행부(105)는 제어부(102)로부터 검출개시명령과 AP 식별정보를 수신하면 개찬검출처리를 행한다(스텝 S305).

<385> 제어부(102)는 개찬검출 실행부(105)로부터 개찬검출처리의 처리결과를 수신하면, 수신한 처리결과가 개찬되어 있지 않다는 통지인가, 개찬이 검출되었다는 통지인가를 판단한다(스텝 S310).

<386> 개찬이 검출되어 있지 않다는, 즉, 개찬되어 있지 않다는 통지를 수신하였다고 판단한 경우에는(스텝 S310에서의 「NO」) 제어부(102)는 기동지시가 있은 AP에 관한 동작을 실행한다(스텝 S315).

<387> 개찬이 검출된, 즉, 개찬이 검출되었다는 통지를 수신하였다고 판단한 경우에는(스텝 S310에서의 「YES」) 제어부(102)는 기동지시가 있은 AP의 동작을 종료한다(스텝 S320).

<388> 1. 9 개찬검출처리의 동작

<389> 여기에서는 도 12의 스텝 S240 및 도 14의 스텝 S305 각각에 나타내는 개찬검출처리의 동작에 대해서 도 15 및 도 16에 도시한 흐름도를 이용하여 설명한다.

<390> 검출제어부(171)는 제어부(102) 또는 갱신처리부(103)의 갱신제어부(162) 중 어느 하나로부터 검출개시명령과 AP 식별정보를 수신하면 수신한 검출개시명령과 AP 식별정보를 개찬검출 호출부(172)에 출력한다.

<391> 개찬검출 호출부(172)는 검출제어부(171)로부터 검출개시명령과 AP 식별정보를 수신하면, 기억부(101)로부터 수신한 AP 식별정보에 대응하는 해시 리스트를 판독한다(스텝 S400).

<392> 개찬검출 호출부(172)는 판독한 해시 리스트(122)와 수신한 검출개시명령 및 AP 식별정보를 개찬검출 처리부(173)에 출력한다. 개찬검출 처리부(173)는 개찬검출 호출부(172)로부터 해시 리스트(122)와 검출개시 명령 및 AP 식별정보를 수신하면, 개찬검출 처리부(173)는 수신한 AP 식별정보에 대응하는 부분 키(123)를 기억부(101)에서 판독한다. 개찬검출 처리부(173)는 판독한 부분 키(123)와, 마스터 키(176) 및 특정 알고리즘을 이용하여 개찬검출 키를 산출한다(스텝 S405).

<393> 개찬검출 처리부(173)는 산출한 개찬검출 키와 해시 계산 알고리즘을 이용하여 수신한 해시 리스트의 데이터부에 대한 해시 값을 산출한다(스텝 S410). 개찬검출 처리부(173)는 산출한 해시 값과 해시 리스트의 헤더부에 포

함되는 데이터부 해시 값이 일치하는가 여부를 판단한다(스텝 S415).

<394> 일치하지 않는다고 판단한 경우에는(스텝 S415에서의 「NO」) 개찬검출 처리부(173)는 개찬이 검출되었다는 통지를 검출제어부(171)에 출력한다. 검출제어부(171)는 개찬검출 처리부(173)로부터 개찬이 검출되었다는 통지 중 어느 하나를 수신하다. 검출제어부(171)는 수신한 통지를 호출 원(즉, 검출개시명령 및 AP 식별정보의 출력원)인 제어부(102) 또는 갱신처리부(103)의 갱신제어부(162) 중 어느 하나에 출력한다(스텝 S420).

<395> 일치한다고 판단한 경우에는(스텝 S415에서의 「YES」) 개찬검출 처리부(173)는 개찬검출 키를 이용하여 데이터부(131)를 복호 한다(스텝 S425). 또한, 복호에는 데이터부를 암호화한 알고리즘에 대응하는 복호 알고리즘이 이용된다.

<396> 개찬검출 처리부(173)는 복호 한 데이터부에서 미 판독의 해시 정보를 판독한다(스텝 S430).

<397> 개찬검출 처리부(173)는 판독한 해시 정보에 포함되는 파일정보를 파일 판독부(174)에 출력한다. 파일 판독부(174)는 개찬검출 처리부(173)에서 파일정보를 수신하면, 수신한 파일정보에 포함되는 파일 명에 의거하여 개찬검출대상의 파일을 기억부(101)에서 판독한다(스텝 S435).

<398> 파일 판독부(174)는 판독한 파일을 파일 기억영역에 저장하고, 파일 판독완료명령을 개찬검출 처리부(173)에 출력한다. 파일 판독부(174)로부터 파일의 판독이 완료했다는 취지를 나타내는 파일 판독완료 명령을 수신한다.

<399> 개찬검출 처리부(173)는 판독한 해시 정보에서 미 판독의 엔트리를 취득하고(스텝 S440), 취득한 엔트리가 최종 엔트리인가 여부를 판단한다(스텝 S445).

<400> 최종 엔트리가 아니라고 판단한 경우에는(스텝 S445에서의 「NO」), 개찬검출 처리부(173)는 취득한 엔트리에 포함되는 오프셋 및 사이즈를 판독하고, 판독한 오프셋 및 사이즈에 의거하여 파일 판독부(174)에서 판독된 파일에서 검출대상의 블록을 취득한다(스텝 S450). 개찬검출 처리부(173)는 산출한 개찬검출 키와 해시 계산 알고리즘을 이용하여 취득한 블록에 대한 검출용 해시 값을 산출한다(스텝 S455). 개찬검출 처리부(173)는 산출한 검출용 해시 값과 취득한 엔트리에 포함되는 해시 값이 일치하는가 여부를 판단한다(스텝 S460). 일치한다고 판단한 경우에는(스텝 S460에서의 「YES」) 개찬검출 처리부(173)는 스텝 S440으로 되돌아간다. 일치하지 않는다고 판단한 경우에는(스텝 S460에서의 「NO」) 스텝 S420으로 되돌아간다.

<401> 취득한 엔트리가 최종 엔트리라고 판단한 경우에는(스텝 S445에서의 「YES」) 개찬검출 처리부(173)는 미 판독의 해시 정보가 존재하는가 여부를 판단한다(스텝 S465). 존재한다고 판단한 경우에는(스텝 S465에서의 「YES」) 스텝 S430으로 되돌아간다. 존재하지 않는다고 판단한 경우에는(스텝 S465에서의 「NO」) 개찬검출 처리부(173)는 개찬되어 있지 않다는 통지를 검출제어부(171)에 출력한다. 검출제어부(171)는 개찬검출 처리부(173)에서 개찬되어 있지 않다는 통지를 수신한다. 검출제어부(171)는 수신한 통지를 호출 원(즉, 검출개시명령 및 AP 식별정보의 출력 원)인 제어부(102) 또는 갱신처리부(103)의 갱신제어부(162) 중 어느 하나에 출력한다(스텝 S470).

<402> 1. 10 휴대전화기(10)의 기동시의 동작

<403> 휴대전화기(10)의 기동시의 갱신처리 및 개찬검출처리의 동작에 대하여 설명한다.

<404> 휴대전화기(10)에 전원이 투입되어 전원의 공급이 개시되면, 갱신제어부(162)는 플래그 기억부(161)에 기억되어 있는 플래그의 값을 확인한다.

<405> 플래그의 값이 「0」인 경우에는, 휴대전화기(10)는 전회의 갱신처리는 완료했다고 판단하고, 갱신처리 및 개찬검출 처리는 행하지 않는다.

<406> 플래그의 값이 「1」인 경우에는, 갱신 처리중인 상태라고 판단하고, 제어부(102)에 대하여 인터럽트 금지를 설정한다. 갱신제어부(162)는 갱신처리의 재개시를 나타내는 재개시명령을 갱신데이터 판독부(163)에 출력한다.

<407> 갱신데이터 판독부(163)는 갱신제어부(162)로부터 재개시명령을 수신하면 수신한 재개시명령을 갱신파일 수신부(104)에 출력한다.

<408> 갱신파일 수신부(104)는 갱신데이터 판독부(163)로부터 재개시명령을 수신하면 AP 식별정보 기억영역에 저장되어 있는 AP 식별정보가 존재하는가 여부를 판단한다. 존재한다고 판단한 경우에는, 휴대전화기(10)는 도 11에 나타낸 스텝 S115 이후의 동작을 행한다.

<409> AP 식별정보 기억영역에 저장되어 있는 AP 식별정보가 존재하지 않는다고 판단한 경우에는 갱신파일 수신부

(104)는 리스트 기억영역에 갱신데이터 리스트가 저장되어 있는가 여부를 판단한다.

<410> 갱신데이터 리스트가 저장되어 있다고 판단한 경우에는 수신완료명령을 갱신처리부(103)에 출력한다. 갱신처리부(103)의 갱신데이터 판독부(163)는 갱신파일 수신부(104)로부터 수신완료명령을 수신한다. 갱신처리부(103)는 도 12에 나타낸 스텝 S205 이후의 동작을 행한다.

<411> 갱신데이터 리스트가 저장되어 있지 않다고 판단한 경우에는 재개시 불요 명령을 갱신데이터 판독부(163)에 출력한다. 갱신데이터 판독부(163)는 재개시 불요 명령을 수신하면 수신한 재개시 불요 명령을 갱신제어부(162)에 출력한다. 갱신제어부(162)는 갱신데이터 판독부(163)에서 갱신처리의 재개시가 불필요하다는 취지를 나타내는 재개시 불요 명령을 수신하면, 제어부(102)에 대한 인터럽트 금지를 해제하고, 플래그 기억부(161)에 기억되어 있는 플래그의 값을 「0」으로 설정한다.

<412> 2. 검출 키와 각 동작과의 관계

<413> 도 17은 본 실시 예에서 이용되는 각 키의 관계와 키가 이용되는 장면의 관계를 나타낸다.

<414> 개찬검출 키는 마스터 키, 부분 키 및 특정 알고리즘을 이용하여 산출된다. 이 생성작업은 키 갱신장치(30)의 개찬검출 키 생성부(302) 및 도 15에 나타낸 스텝 S405에 의해 휴대전화기(10)에서 행해진다.

<415> 생성된 개찬검출 키는 이하와 같이 해시 리스트 생성시 및 해시 리스트를 이용한 개찬검출 처리시에 이용된다.

<416> (해시 리스트 생성시)

<417> 개찬검출 키는 검출대상인 파일에서의 하나 이상의 블록 각각에 대한 해시 값을 산출하는 경우에 이용된다. 구체적으로는, 도 10에서 나타내는 스텝 S20의 동작에 대응한다.

<418> 또, 개찬검출 키는 해시 리스트의 데이터부를 암호화하는 경우에 이용된다. 구체적으로는, 도 10에서 나타내는 스텝 S25의 동작에 대응한다.

<419> 또, 개찬검출 키는 해시 리스트의 데이터부의 해시 값(데이터부 해시 값)을 산출하는 경우에 이용된다. 산출된 해시 값은 해시 리스트의 헤더부에 매설(embed)된다. 구체적으로는, 도 10에서 나타내는 스텝 S30의 동작에 대응한다.

<420> (개찬검출 처리시)

<421> 개찬검출 키는 해시 리스트의 데이터부의 해시 값을 산출하는 경우에 이용된다. 구체적으로는, 도 15에서 나타내는 스텝 S410의 동작에 대응한다. 이때, 휴대전화기(10)는 산출된 해시 값과 미리 매설된 해시 값(데이터부 해시 값)을 비교함으로써 개찬의 유무를 확인한다.

<422> 또, 개찬검출 키는 해시 리스트의 데이터부를 복호 하는 경우에 이용된다. 구체적으로는, 도 15에서 나타내는 스텝 S425의 동작에 대응한다.

<423> 또, 개찬검출 키는 검출대상의 파일에서의 각 블록의 해시 값(검출용 해시 값)을 산출하는 경우에 이용된다. 구체적으로는, 도 16에서 나타내는 스텝 S455의 동작에 대응한다. 이때, 휴대전화기(10)는 산출된 검출용 해시 값과 미리 저장되어 있는 해시 값을 비교함으로써 개찬의 유무를 확인한다.

<424> 3. 변형 예

<425> 또, 본 발명을 상기 실시 예에 의거하여 설명하였으나, 본 발명은 상기 실시 예에 한정되지 않음은 당연하다. 이하와 같은 경우도 본 발명에 포함된다.

<426> (1) 상기 제 1 실시 예에서는 개찬을 검출하는 장치로 휴대전화기를 이용하였으나, 이에 한정되는 것은 아니다.

<427> 개찬을 검출하는 장치는 통신기능을 구비한 HDD 리코더/DVD 리코더, 게임기기, PDA와 같은 기기라도 좋다. 즉, 갱신 서버장치와 네트워크 등에 의해 접속 가능한 전자기기면 된다.

<428> (2) 해시 리스트의 데이터부의 암호화는, 시큐어리티 강도(security strength)를 고려하여, 데이터부(131)의 암호화 단위는 데이터부 전체에 공통 키 암호방식에서의 연쇄(chaining mode, 連鎖)와 같은 암호 알고리즘을 적용해도 된다. 이때의 해시 리스트의 갱신 단위는 해시 리스트 전체가 된다.

<429> (3) 상기 제 1 실시 예에서, 해시 리스트의 갱신 시에 개찬검출대상의 파일의 사이즈가 증대하여 갱신 전의 MAC 정보의 엔트리 수가 증가한 경우에는, 갱신 서버장치는, 도 18에 도시하는 해시 리스트(122a)를 생성해도 된다.

도 18에서 파일정보 140a에 대응하는 MAC정보 141a의 최후의 엔트리는 MAC정보 1000에 포함되는 엔트리 1001의 어드레스를 가리키는 링크 엔트리(link entry) 144a로 되어 있다. 통상의 엔트리와 링크 엔트리는 사이즈 및 해시가 다르다. 링크 엔트리의 각각에는 수치가 저장되지 않고 「-」가 저장된다. 이에 의해, 통상의 엔트리와 링크 엔트리를 구별할 수 있다.

<430> 링크 엔트리 144a의 오프셋에는 엔트리 1001의 어드레스를 가리키는 값으로 해시 리스트 내에서의 파일로부터의 오프셋이 저장된다.

<431> 이때, 파일정보(140a)에 포함되는 블록 수(142a)는 MAC정보 141a와 MAC정보 1000에서 링크 엔트리 144a와 MAC정보 1000의 공 엔트리(1002)(최종 엔트리)를 제외한 엔트리 수인 "4"로 되어 있다.

<432> 이 경우의 해시 리스트의 생성방법의 일 예를 이하에 설명한다.

<433> 해시 리스트 생성 처리부(212)는 개찬검출 키(215)를 판독한다. 그리고 개찬검출 키(215)를 이용하여 구 해시 리스트의 데이터부의 복호를 행하여 복호 된 구 해시 리스트를 생성한다. 이하에서는 복호 된 구 해시 리스트를 복호 해시 리스트라고 한다.

<434> 해시 리스트 생성 처리부(212)는 데이터 수신부(212)로부터 수신한 하나 이상의 갱신파일에 대하여 소정의 사이즈로 분할한 블록 단위로 개찬검출 처리부(173)와 동일한 해시 계산 알고리즘을 적용하여 해시 값을 산출하고, 타깃 패스 리스트에서 휴대전화기(10)에서의 파일 패스를 판독해서, 복호 해시 리스트와 비교하여, 데이터부가 암호화되어 있지 않은 해시 리스트를 생성한다. 이때, 생성한 해시 리스트의 사이즈가 복호 해시 리스트보다도 큰 파일의 갱신인 경우에는, 해시 리스트 생성 처리부(212)는 생성한 해시 리스트를 도 18에 도시한 것과 같은 링크 엔트리를 이용한 해시 리스트로 변환한다.

<435> (4) 상기 제 1 실시 예에서, 개찬검출 실행부(105)의 개찬검출 처리부(173)와 파일 판독부(174)를 개별 구성으로 하였으나, 이에 한정되는 것은 아니다.

<436> 개찬검출 처리부(173)와 파일 판독부(174)를 하나의 구성요소로 해도 된다.

<437> (5) 상기 제 1 실시 예에서, 파일의 갱신시에는 지정된 AP를 포함하는 검출대상정보 군을 갱신의 대상으로 하였으나, 이에 한정되는 것은 아니다.

<438> 1회의 갱신지시에 의해 모든 검출대상정보 군을 갱신의 대상으로 해도 된다.

<439> (6) 상기 제 1 실시 예에서, 갱신데이터 리스트만을 이용하여 AP에 관한 파일을 갱신하였으나, 이에 한정되는 것은 아니다.

<440> 갱신 서버장치는 휴대전화기에 갱신데이터 리스트와 함께 갱신 대상이 되는 하나 이상의 갱신파일을 송신해도 된다. 이때, 송신되는 갱신데이터 리스트에는 해시 리스트에 관한 갱신정보만으로 구성된다.

<441> (7) 상기 제 1 실시 예에서, 검출대상인 파일은 미리 정해진 사이즈의 블록 단위로 분할되었으나, 이에 한정되는 것은 아니다.

<442> 갱신 서버장치는 사용자의 조작에 의해 입력 값으로 분할되는 블록의 사이즈를 접수하는 구성이어도 된다. 이에 의해, 블록의 사이즈를 유연하게 설정할 수 있다.

<443> (8) 상기 제 1 실시 예에서, 갱신 서버장치는 데이터부 해시 값의 산출을 데이터부의 암호화 후에 행하였으나, 이에 한정되는 것은 아니다.

<444> 갱신 서버장치는 데이터부의 암호화의 전에 데이터부 해시 값의 산출을 행해도 된다.

<445> 이때, 개찬검출의 실행 시에는 데이터부의 복호 후에 데이터부에 대한 해시 값을 산출하고, 해시 리스트 자체의 개찬검출을 행하게 된다.

<446> (9) 상기 제 1 실시 예에서, 해시 리스트의 데이터부의 암호화에 이용되는 키와 해시 계산에 이용되는 키는 동일한 키(개찬검출 키)로 하였으나, 동일하지 않아도 된다.

<447> (10) 상기 제 1 실시 예에서, 갱신데이터 리스트는 해시 리스트의 갱신 내용과 함께 갱신파일의 갱신내용 및 갱신된 부분 키를 포함하는 것으로 하였으나, 이에 한정되는 것은 아니다.

<448> 갱신데이터 리스트는 해시 리스트용의 갱신데이터 리스트, 갱신파일용의 갱신데이터 리스트 및 부분 키 용의 갱신데이터 리스트로 구분해도 된다.

<449> (11) 상기 제 1 실시 예에서, 해시 리스트의 갱신은 휴대전화기를 사용하는 사용자의 요구에 의한 것으로 하였으나, 갱신 서버장치로부터의 강제 업 데이트여도 된다.

<450> 예를 들어, 키 갱신장치에서 갱신 서버장치에 새로운 개찬검출 키가 매설된 경우에는, 갱신 서버장치는 갱신된 부분 키를 휴대전화기에 송신하기 위해서 갱신데이터 리스트를 생성하고, 생성한 갱신데이터 리스트를 바로 휴대전화기에 송신한다.

<451> (12) 상기 제 1 실시 예에서, 다른 휴대전화기는 휴대전화기 10과 동일한 마스터 키를 보유하고 있어도 좋고, 다른 마스터 키를 보유하고 있어도 좋다.

<452> 휴대전화기 간에 다른 마스터 키를 보유하는 경우에는, 키 갱신장치는 복수의 마스터 키를 관리하고 있고, 갱신된 부분 키로부터 산출되는 개찬검출 키도 다르므로, 갱신 서버장치에서도 복수의 개찬검출 키를 관리하게 된다.

<453> (13) 상기 제 1 실시 예에서 설명한 해시 리스트를 도 19에 도시한 해시 리스트(122b)로 해도 된다. 도 19에 도시한 해시 리스트(122b)는 헤더부(130b)에 해시 리스트의 판 수를 나타내는 해시 리스트 버전 번호(1010)를 갖는다.

<454> 이 경우, 휴대전화기는 갱신 서버장치에 갱신요구정보를 송신할 때에 해시 리스트 버전 번호(1010)도 송신한다.

<455> 갱신 서버장치는 생성한 해시 리스트의 해시 리스트 버전 번호별로 갱신데이터 리스트를 관리해 두고, 휴대전화기에서 수신한 해시 리스트 버전 번호(1010)에 따른 갱신데이터 리스트를 휴대전화기에 송신한다.

<456> (14) 상기 제 1 실시 예에서, 개찬검출처리는 해시 리스트에 포함되는 MAC정보가 갖는 모든 엔트리를 이용하여 개찬검출을 행하였으나, 이에 한정되는 것은 아니다.

<457> 속도가 더 요구되는 경우에는, 각 MAC정보에서 오프셋이 0번의 엔트리만을 체크하는 순서로 해도 좋다. 또, 파일정보의 블록 수를 판독하고, 그 절반의 블록 수를 체크하는 순서로 해도 좋다.

<458> 즉, 개찬검출처리는 각 MAC정보에서 하나 이상의 엔트리를 체크하는 순서이면 된다.

<459> (15) 상기 제 1 실시 예에서, 개찬검출의 실행은 해시 리스트의 갱신 시 및 검출대상의 AP의 기동 시로 하였으나, 이에 한정되는 것은 아니다.

<460> 개찬검출의 실행은 휴대전화기의 기동 중에 행하여도 되고, 검출대상의 AP를 실행하고 있을 때에는 백그라운드에서 실행해도 된다.

<461> 또는, 휴대전화기는 당해 휴대전화기의 기동 중에 정기적으로 개찬검출을 실행하여도 되고, 검출대상의 AP가 기동하고 있는 동안에 기동하고 있는 AP에 대한 개찬검출을 정기적으로 실행해도 된다.

<462> (16) 도 15에서 나타내는 스텝 S425에서 휴대전화기는 데이터부 전체를 복호하고 있으나, 이에 한정되는 것은 아니다.

<463> 휴대전화기는 MAC정보의 1 엔트리마다 복호를 행하는 구성이어도 된다.

<464> 이때, 휴대전화기는 도 15에서 나타내는 스텝 S415를 실행한 후, 스텝 S425를 생략하고, 스텝 S430에서 스텝 S440까지를 실행한다. 이때, 판독한 엔트리는 암호화되어 있다. 휴대전화기는 그 후 판독한 엔트리를 복호하고 스텝 S445 이후를 실행한다. 또는, 휴대전화기는 도 15에서 나타내는 스텝 S415를 실행한 후, 스텝 S425를 생략하고, 스텝 S430에서 스텝 S445까지를 실행하며, 그 후 복호 해도 된다.

<465> (17) 상기 제 1 실시 예에서, 해시 리스트의 갱신시에 개찬검출대상의 파일의 사이즈가 작아진 경우에는, 불필요해지는 엔트리에 포함되는 사이즈를 「0」으로 설정한다.

<466> 도 20에 파일의 블록 수가 「8」에서 「7」로 감소한 경우의 일 예를 나타낸다.

<467> 이 경우, 갱신 전인 해시 정보(1020)에서 8번째의 블록의 엔트리(1021)에 포함되는 사이즈는 120이 저장되어 있다. 파일의 갱신에 의해 블록 수가 「8」에서 「7」로 감소하면, 8번째의 블록의 엔트리(1031)에 포함되는 사이즈를 「0」으로 하여 해시 정보(103)가 생성된다. 이때, 엔트리(1031)도 갱신의 대상이 되는 것은 말할 것도 없다.

<468> 개찬검출을 실행할 때에는, 휴대전화기는 엔트리에 포함되는 사이즈가 「0」인 경우에는 그 엔트리를 무시하고,

그 엔트리에 대한 개찬의 체크는 행하지 않는다.

<469> 또, 엔트리(1031)에 포함되는 해시 값은 갱신 전의 값으로 하고 있으나, 해시 값을 "0"으로 해도 된다.

<470> 이에 의하면, 휴대전화기는 사이즈에 저장되는 값을 당해 사이즈를 포함하는 엔트리가 개찬검출의 대상인지 여부를 판단하는 판단정보로 이용할 수 있다. 즉, 값이 「0」이면 개찬검출의 대상이 아니라고 판단하고, 「0」 이외의 값인 경우에는 개찬검출의 대상이라고 판단할 수 있다.

<471> (18) 2개의 휴대전화기(여기서는, 휴대전화기 11, 12로 한다)에서, 휴대전화기 11이 기능 A(예를 들어, 오디오 데이터의 재생기능)을 포함하는 제 1 AP와, 기능 B(예를 들어, 콘텐츠를 암호화하여 SD 카드에 저장하는 SD-Binding 기능)을 포함하는 제 2 AP를 구비하고, 휴대전화기 12가 기능 A 및 기능 B의 쌍방을 포함하는 통합 AP를 구비하는 경우, 상기의 제 1 실시 예에서 설명한 바와 같이, AP별로 다른 해시 리스트가 부여되어도 되고, 이하에 설명하는 바와 같이, 하나의 해시 리스트가 부여되어도 된다.

<472> 도 21에 제 1 AP, 제 2 AP 및 통합 AP에 대하여 부여된 하나의 해시 리스트(122c)의 데이터 구성의 일 예를 나타낸다. 또, 헤더부(130c)의 데이터 구성은 제 1 실시 예에서 설명한 해시 리스트(122)의 헤더부(130)의 데이터 구성과 동일하므로 여기에서는 설명을 생략한다.

<473> 제 1 실시 예에서 설명한 해시 리스트(122)와 다른 점은 파일정보에 종별이 추가되어 있는 점이다. 종별은 개찬검출의 실행시에 사용하는 해시 정보를 식별하기 위한 것으로, 예를 들어 수치 1, 2, …, 및 ALL로 이루어진다. 종별에 ALL이 설정되면 해시 리스트에 포함되는 모든 해시 정보가 검출에 이용되는 것을 나타내고, 수치가 설정되면 설정된 종별(수치)을 포함하는 파일정보를 갖는 해시 정보가 검출의 대상이 된다.

<474> 이 경우, 각 AP(제 1 AP, 제 2 AP 및 통합 AP)는 자신의 종별을 기억하고 있고, 기동시에 기억하고 있는 종별을 개찬검출 실행부에 인도한다. 여기서, 제 1 AP, 제 2 AP 및 통합 AP 각각에는 종별 1, 2, ALL이 설정되어 있는 것으로 한다.

<475> 휴대전화기 11에서 제 1 AP가 기동 되면, 도 21에 도시한 바와 같이, 종별 「1」을 포함하는 파일정보(1040)를 갖는 해시 정보(134c)가 개찬검출의 대상이 된다.

<476> 또, 휴대전화기 11에서 제 2 AP가 기동 되면, 종별 「2」를 포함하는 파일정보(1041)를 갖는 해시 정보(135c)가 개찬검출의 대상이 된다.

<477> 휴대전화기 12에서 통합 AP가 기동 되면, 통합 AP는 종별 「ALL」을 기억하고 있으므로, 데이터부(131c)에 포함되는 모든 해시 정보가 개찬검출의 대상이 된다.

<478> (19) 상기 제 1 실시 예에서 설명한 해시 리스트에서 개찬검출의 대상이 되는 적어도 하나 이상의 파일을 우선적으로 개찬검출을 실행하는 우선도를 설치해도 된다. 이때, 예를 들어 우선적으로 개찬검출되는 파일에 대해서는 AP의 기동시에 개찬검출이 실행되고, 다른 개찬검출대상의 파일에 대해서는 AP의 기동이 완료하고, AP가 갖는 기능의 동작 중에 백그라운드에서 개찬검출이 실행된다.

<479> 도 22에 우선도를 이용한 해시 리스트(122d)의 데이터 구성의 일 예를 나타낸다. 또, 헤더부(130d)의 데이터 구성은 제 1 실시 예에서 설명하는 해시 리스트(122)의 헤더부(130)의 데이터 구성과 동일하므로 여기에서는 설명을 생략한다.

<480> 제 1 실시 예에서 설명하는 해시 리스트(122)와 다른 점은 데이터부(131d)에 제 1 오프셋(1050)과 제 2 오프셋(1051)으로 이루어지는 세트가 추가되어 있다는 점이다.

<481> 제 1 오프셋은 우선적으로 개찬검출을 행하는 해시 정보의 선두 위치를 나타내는 오프셋 값이고, 제 2 오프셋은 우선적으로 개찬검출을 행하는 해시 정보의 최종 위치를 나타내는 오프셋 값이다.

<482> 예를 들어, 제 1 오프셋에 해시 정보(134d)의 선두 위치를 나타내는 오프셋 값이 저장되고, 제 2 오프셋에 해시 정보(134d)의 최종 위치를 나타내는 오프셋 값이 저장되어 있는 경우에는, 파일 명이 「file_1」인 파일에 대한 개찬검출은 AP 기동시에 행해지고, 다른 파일에 대한 개찬검출은 동작 중에 백그라운드에서 행해진다.

<483> 또, 제 1 오프셋에 해시 정보(134d)의 선두 위치를 나타내는 오프셋 값이 저장되고, 제 2 오프셋에 해시 정보(136d)의 최종 위치를 나타내는 오프셋 값이 저장되어 있는 경우에는, 파일 명이 「file_1」인 파일 및 파일 명 「file_2」인 파일의 각각에 대한 개찬검출은 AP 기동시에 행해지며, 다른 파일에 대한 개찬검출은 동작 중에 백그라운드에서 행해진다.

<484> (20) 상기 제 1 실시 예에서, 하나의 AP 파일 군, 즉, 하나의 AP에 대하여 하나의 해시 리스트가 부여되었으나, 이에 한정되는 것은 아니다.

<485> 하나 이상의 AP 파일 군에 대하여 하나의 해시 리스트 및 부분 키를 부여해도 된다.

<486> 이 경우의 기억부(101)의 구성을 도 23에 나타낸다.

<487> 도 23에서 기억부(101)는 하나의 검출대상정보 군(1200)을 갖는다.

<488> 검출대상정보 군(1200)은 하나 이상의 AP 파일 군(1060, 1061, …, 1062)과, 해시 리스트(122e) 및 부분 키(123e)를 갖는다.

<489> 해시 리스트(122e)의 데이터부에는 AP 파일 군(1060, 1061, …, 1062)의 각각에 포함되는 각 파일에 대한 해시 정보가 포함되어 있다.

<490> 검출대상정보 군(1200)에 포함되는 하나의 AP가 기동 된 경우, 휴대전화기는 검출대상정보 군(1200)에 포함되는 모든 파일을 개찬검출대상으로 하여도 되고, 기동 된 AP에 관한 하나 이상의 파일만을 개찬검출의 대상으로 해도 된다.

<491> (21) 상기 제 1 실시 예에서, 휴대전화기(10)의 전원투입시에 갱신제어부(162)는 플래그의 값의 체크를 행하고, 플래그의 값이 「1」인 경우에는 파일의 갱신을 자동으로 행하였으나, 이에 한정되는 것은 아니다.

<492> 휴대전화기(10)는, 갱신제어부(162)가 플래그의 값이 「1」이라고 판단한 경우에는 파일의 갱신을 다시 행할지 여부를 통지하여, 사용자로부터 다시 갱신을 한다는 지시를 수신한 경우에 파일의 갱신을 다시 해도 된다.

<493> 또는, 파일의 갱신을 자동으로 행하는 경우에 다시 갱신을 행한다는 취지를 사용자에게 통지해도 된다.

<494> 또는, 휴대전화기(10)의 전원 투입시에 갱신제어부(162)는 플래그의 값의 체크를 행하고, 플래그의 값이 「1」인 경우에는 미 갱신의 데이터에 대해서만 갱신을 행해도 된다. 즉, 휴대전화기(10)는 갱신처리 도중(휴대전화기(10)의 전원의 차단시에 동작하고 있던 시점)에서부터 갱신의 동작을 해도 된다.

<495> (22) 상기 제 1 실시 예에서, 해시 리스트의 데이터부는 암호화되어 있는 것으로 하였으나, 이에 한정되는 것은 아니다.

<496> 데이터부는 암호화하지 않아도 된다.

<497> (23) 본 발명에서의 애플리케이션 파일은 애플리케이션 소프트웨어 그 자체나, 애플리케이션 소프트웨어로부터 호출되는 인코더, 디코더, 드라이버, 애플리케이션 소프트웨어가 동작하는 환경을 제공하는 Java(등록상표) VM과 같은 가상실행환경 등이다. 또, 애플리케이션 파일의 개념에 부분 키를 포함해도 된다.

<498> (24) 상기 제 1 실시 예에서, 키 갱신장치는 외부장치에서 갱신된 부분 키를 취득하는 것으로 하였으나, 이에 한정되는 것은 아니다.

<499> 키 갱신장치에서 새로운 부분 키를 생성하여 취득해도 된다.

<500> 또, 마스터 키는 키 갱신장치에 기억해 두어도 되고, 외부장치에서 취득해도 된다.

<501> (25) 상기 제 1 실시 예에서, 갱신데이터 리스트에 포함되는 갱신데이터는 갱신해야 할 정보인 파일 중 갱신대상이 되는 하나 이상의 블록, 해시 리스트에서의 해시 리스트 파일 사이즈, 데이터부 해시 값, 파일정보, MAC정보에 포함되는 엔트리 등이 기록되어 있는 것으로 하였으나, 이에 한정되는 것은 아니다.

<502> 갱신해야 할 정보인 파일 중 갱신대상이 되는 하나 이상의 블록을 갱신데이터로 기록하는 대신에 애플리케이션 소프트웨어를 실행하기 위한 명령문 등과 같은 갱신된 데이터만을 기록해도 된다.

<503> 또, 갱신대상이 되는 블록을 본원 발명의 「데이터」의 개념에 포함시켜도 된다.

<504> (26) 상기 제 1 실시 예에서, 개찬검출용의 값(개찬검출 값)으로 해시 값을 이용하여 개찬의 검출을 행하였으나, 이에 한정되는 것은 아니다.

<505> 해시 값과는 다른 값이나 데이터를 이용해도 된다. 예를 들어, 검출대상의 데이터를 암호화한 결과 등을 개찬검출 값으로 이용할 수 있다.

<506> (27) 상기의 각 장치는, 구체적으로는, 마이크로프로세서, ROM, RAM, 하드디스크 유닛, 디스플레이 유닛, 키보

드, 마우스 등으로 구성되는 컴퓨터 시스템이다. 상기 RAM 또는 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써 각 장치는 그 기능을 달성한다. 여기서 컴퓨터 프로그램은 소정의 기능을 달성하기 위해 컴퓨터에 대한 지령을 나타내는 명령코드가 복수개 조합되어서 구성된 것이다.

<507> (28) 상기의 각 장치를 구성하는 구성요소의 일부 또는 전부는 하나의 시스템 LSI(Large Scale Integration: 대규모 집적회로)로 구성되어 있어도 된다. 시스템 LSI는 복수의 구성부를 하나의 칩 상에 집적하여 제조된 초 다기능 LSI이며, 구체적으로는, 마이크로프로세서, ROM, RAM 등을 포함하여 구성되는 컴퓨터 시스템이다. 상기 RAM에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써 시스템 LSI는 그 기능을 달성한다.

<508> 여기에서는 시스템 LSI로 하였으나, 집적도의 차이에 의해 IC, LSI, 시스템 LSI, 슈퍼 LSI, 울트라 LSI로 호칭되는 경우도 있다.

<509> 또, 집적회로 화의 수법은 LSI에 한정되는 것은 아니며, 전용회로 또는 범용 프로세서로 실현해도 된다. LSI 제조 후에 프로그램할 수 있는 FPGA(Field Programmable Gate Array)나 LSI 내부의 회로 셀의 접속이나 설정을 재구성 가능한 리컨피규러블 프로세서(reconfigurable processor)를 이용해도 된다.

<510> 또, 반도체 기술의 진보 또는 파생하는 다른 기술에 의해 LSI로 치환되는 집적회로 화의 기술이 등장하면 당연히 그 기술을 이용하여 기능 블록이 집적화를 행해도 된다. 바이오 기술의 적응 등이 가능성으로 있을 수 있다.

<511> (29) 상기의 각 장치를 구성하는 구성요소의 일부 또는 전부는 각 장치에 착탈 가능한 IC카드 또는 단일체의 모듈로 구성되어 있어도 된다. 상기 IC카드 또는 상기 모듈은 마이크로프로세서, ROM, RAM 등으로 구성되는 컴퓨터 시스템이다. 상기 IC 카드 또는 상기 모듈은 상기의 초 다기능 LSI를 포함해도 된다. 마이크로프로세서가 컴퓨터 프로그램에 따라서 동작함으로써 상기 IC 카드 또는 상기 모듈은 그 기능을 달성한다. 이 IC 카드 또는 이 모듈은 내 탬퍼성을 갖는 것이어도 된다.

<512> (30) 본 발명은 상기에서 설명한 방법으로 해도 된다. 또, 이들 방법을 컴퓨터에 의해 실현하는 컴퓨터 프로그램으로 해도 되고, 상기 컴퓨터 프로그램으로 이루어지는 디지털 신호로 해도 된다.

<513> 또, 본 발명은 상기 컴퓨터 프로그램 또는 상기 디지털 신호를 컴퓨터 판독 가능한 기록매체, 예를 들어 플렉시블 디스크, 하드 디스크, CD-ROM, MO, DVD, DVD-ROM, DVD-RAM, BD(Blu-ray Disc), 반도체 메모리 등에 기록한 것이어도 된다. 또, 이들 기록매체에 기록되어 있는 상기 디지털 신호여도 된다.

<514> 또, 본 발명은 상기 컴퓨터 프로그램 또는 상기 디지털 신호를 전기통신회선, 무선 또는 유선통신회선, 인터넷을 대표로 하는 네트워크 등을 경유하여 전송하는 것으로 해도 된다.

<515> 또, 본 발명은 마이크로프로세서와 메모리를 구비한 컴퓨터 시스템으로, 상기 메모리는 상기 컴퓨터 프로그램을 기억하고 있고, 상기 마이크로 프로세서는 상기 컴퓨터 프로그램에 따라서 동작해도 된다.

<516> 또, 상기 프로그램 또는 상기 디지털 신호를 상기 기록매체에 기록하여 이송함으로써, 또는, 상기 프로그램 또는 상기 디지털 신호를 상기 네트워크 등을 경유하여 이송함으로써 독립한 다른 컴퓨터 시스템에 의해 실시해도 된다.

<517> (31) 상기 실시 예 및 상기 변형 예를 각각 조합해도 된다.

<518> 4. 종합

<519> 본 발명에 의하면, 프로그램의 갱신이 가능한 전자기기에서도 실현할 수 있는 개찬검출방식의 제공이 가능해진다. 또, 갱신시의 갱신 개소를 최소한으로 줄이고, 갱신시에 드는 통신비용을 억제할 수 있다. 또한, 전자기기가 갖는 사양에 따라서 실행시의 속도 튜닝이 가능한 개찬검출방식의 제공이 가능해진다.

<520> 또, 개찬검출시에 필요한 키의 생성에 필요한 정보를 갱신 서버와는 다른 장소에서 관리할 수 있으므로, 만일 그 키가 누설되어도 키의 발행이나 전자기기의 키를 갱신할 수 있는 개찬검출방식을 제공할 수 있게 된다.

산업상 이용 가능성

<521> 상기에서 설명한 프로그램 갱신시스템을 구성하는 각 장치는 전자기기 제조산업에서 경영적, 즉, 반복적이면서도 계속적으로 이용할 수 있다.

<522> 또, 본 발명에 관한 프로그램의 갱신이 가능한 전자기기에서의 개찬검출방식은 시큐어 한 프로그램의 실행을 필요로 하는 휴대전화를 비롯한 내장 기기가 프로그램의 갱신기능을 구비하고 있는 경우에 유용하다.

도면의 간단한 설명

<65> 도 1은 프로그램 갱신시스템(1)의 개요를 나타내는 도면이다.

<66> 도 2는 휴대전화기(10)의 구성을 나타내는 블록 도이다.

<67> 도 3은 해시 리스트(122)의 데이터 구조의 일 예를 나타내는 도면이다.

<68> 도 4는 갱신데이터 리스트(150)의 데이터 구조의 일 예를 나타내는 도면이다.

<69> 도 5는 갱신처리부(103)의 구성을 나타내는 블록 도이다.

<70> 도 6은 개찬검출 실행부(105)의 구성을 나타내는 블록 도이다.

<71> 도 7은 갱신 서버장치(20)의 구성을 나타내는 블록 도이다.

<72> 도 8은 해시 리스트 생성부(203)의 구성을 나타내는 블록 도이다.

<73> 도 9는 키 갱신장치(30)의 구성을 나타내는 블록 도이다.

<74> 도 10은 갱신 서버장치(20)에서 행해지는 갱신데이터 리스트 및 해시 리스트의 생성의 동작을 도시한 흐름도가다.

<75> 도 11은 해시 리스트 갱신 시의 동작의 개요를 도시한 흐름도가다.

<76> 도 12는 휴대전화기(10)에서 행해지는 갱신처리의 동작을 도시한 흐름도가다. 도 13에 이어진다.

<77> 도 13은 휴대전화기(10)에서 행해지는 갱신처리의 동작을 도시한 흐름도가다. 도 12에서 이어진다.

<78> 도 14는 휴대전화기(10)에서 행해지는 AP 기동시의 동작을 도시한 흐름도가다.

<79> 도 15는 휴대전화기(10)에서 행해지는 개찬검출처리의 동작을 도시한 흐름도가다. 도 16에 이어진다.

<80> 도 16은 휴대전화기(10)에서 행해지는 개찬검출처리의 동작을 도시한 흐름도가다. 도 15에서 이어진다.

<81> 도 17은 제 1 실시 예에서 이용되는 각 키의 관계와 키가 이용되는 장면의 관계를 나타내는 도면이다.

<82> 도 18은 해시 리스트(122a)의 데이터 구조의 일 예를 나타내는 도면이다.

<83> 도 19는 해시 리스트(122b)의 데이터 구조의 일 예를 나타내는 도면이다.

<84> 도 20은 파일의 블록 수가 「8」에서 「7」로 감소한 경우의 해시 정보(1030)의 일 예를 나타낸다.

<85> 도 21은 해시 리스트(122c)의 데이터 구조의 일 예를 나타내는 도면이다.

<86> 도 22는 해시 리스트(122d)의 데이터 구조의 일 예를 나타내는 도면이다.

<87> 도 23은 하나 이상의 AP 파일 군에 대하여 하나의 해시 리스트 및 부분 키를 부여하는 경우에서의 기억부(101)의 구성을 나타내는 블록 도이다.

<88> (부호의 설명)

<89>	1	프로그램 갱신시스템	10	휴대전화기
<90>	20	갱신 서버장치	30	키 갱신장치
<91>	30	키 갱신장치	40	휴대 망
<92>	50	인터넷	101	기억부
<93>	102	제어부	103	갱신처리부
<94>	104	갱신파일 수신부	105	개찬검출 실행부
<95>	106	마이크	107	스피커

<96> 108 입력부 109 표시부

<97> 110 무선부 111 안테나

<98> 161 플래그 기억부 162 갱신제어부

<99> 163 갱신데이터 판독부 164 갱신데이터 해석부

<100> 165 기록위치 결정부 166 갱신데이터 기록부

<101> 167 갱신 확인부 171 검출제어부

<102> 172 개찬 검출 호출부 173 개찬검출 처리부

<103> 174 파일 판독부 175 마스터 키 기억부

<104> 176 마스터 키 201 기억부

<105> 202 데이터 취득부 203 해시 리스트 생성부

<106> 204 해시 리스트 기록부 205 갱신요구 처리부

<107> 206 입력부 207 송수신부

<108> 210 개찬검출 키 기억부 211 데이터 수신부

<109> 212 해시 리스트 생성 처리부 213 암호화 처리부

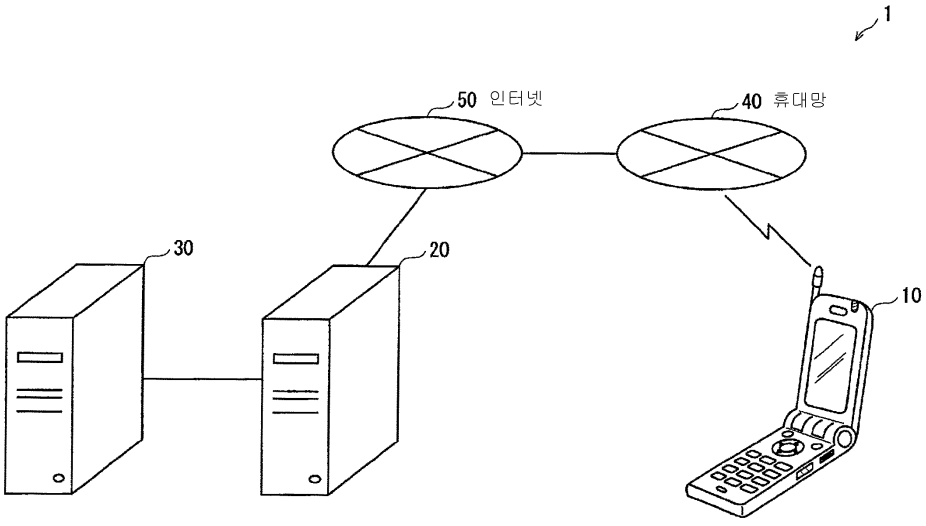
<110> 214 갱신데이터 리스트 생성부 215 개찬검출 키

<111> 301 키 취득부 302 개찬검출 키 생성부

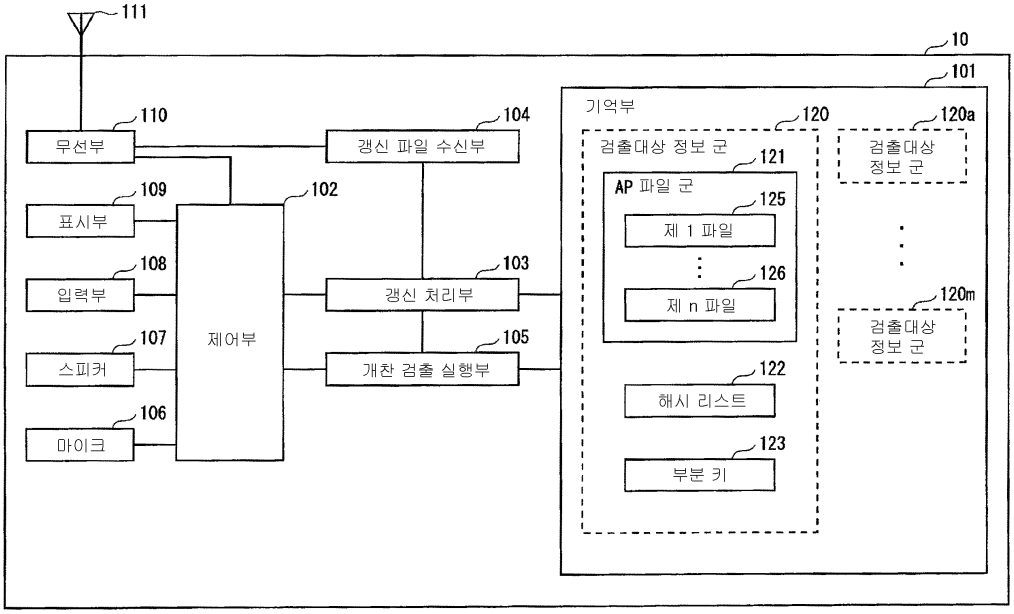
<112> 303 개찬검출 키 배포부 304 출력부

도면

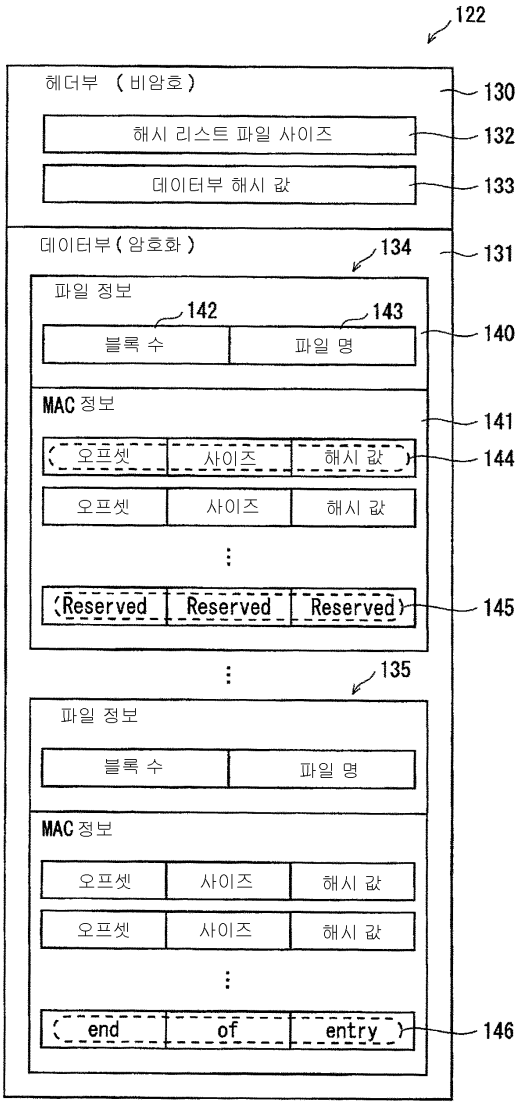
도면1



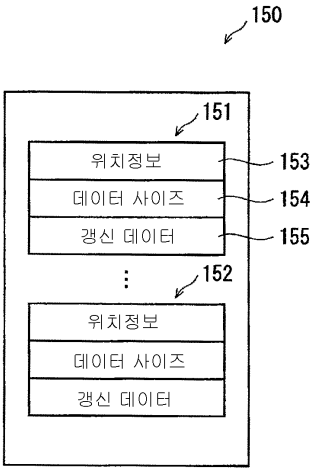
도면2


111
10
101
기억부
110
무선부
104
갱신 파일 수신부
120
검출대상 정보 군
120a
검출대상
정보 군
109
표시부
102
121
AP 파일 군
125
제 1 파일
108
입력부
103
갱신 처리부
126
제 n 파일
120m
검출대상
정보 군
107
스피커
제어부
105
개찬 검출 실행부
122
해시 리스트
106
마이크
123
부분 키

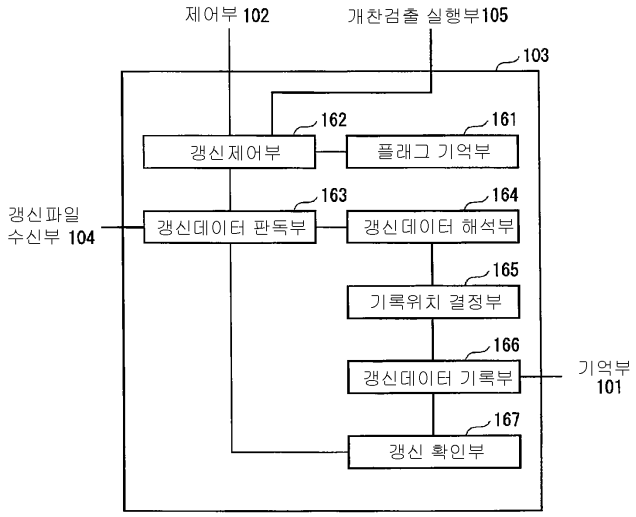
도면3


122
헤더부 (비암호)
130
해시 리스트 파일 사이즈
132
데이터부 해시 값
133
데이터부(암호화)
134
131
파일 정보
142
143
블록 수
파일 명
140
MAC 정보
141
오프셋
사이즈
해시 값
144
오프셋
사이즈
해시 값
Reserved
Reserved
Reserved
145
135
파일 정보
블록 수
파일 명
MAC 정보
오프셋
사이즈
해시 값
오프셋
사이즈
해시 값
end
of
entry
146

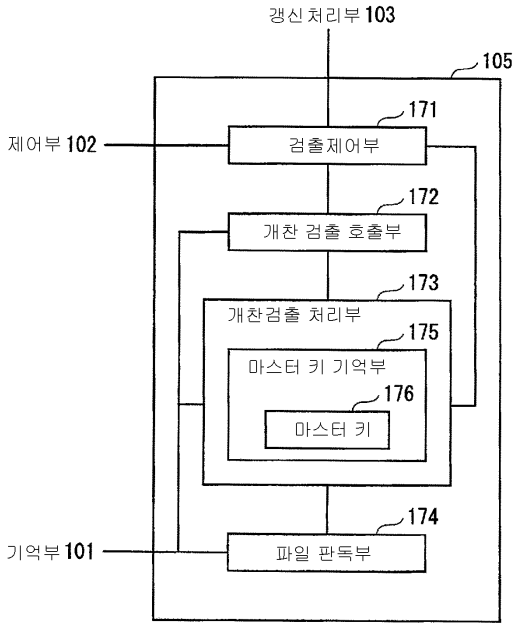
도면4


150
151
위치정보
153
데이터 사이즈
154
갱신 데이터
155
152
위치정보
데이터 사이즈
갱신 데이터

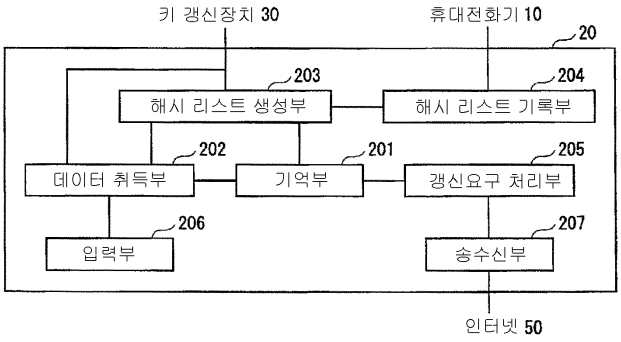
도면5


제어부 102
개찬검출 실행부105
103
162
161
갱신제어부
플래그 기억부
갱신파일
수신부 104
163
164
갱신데이터 판독부
갱신데이터 해석부
165
기록위치 결정부
166
갱신데이터 기록부
기억부
101
167
갱신 확인부

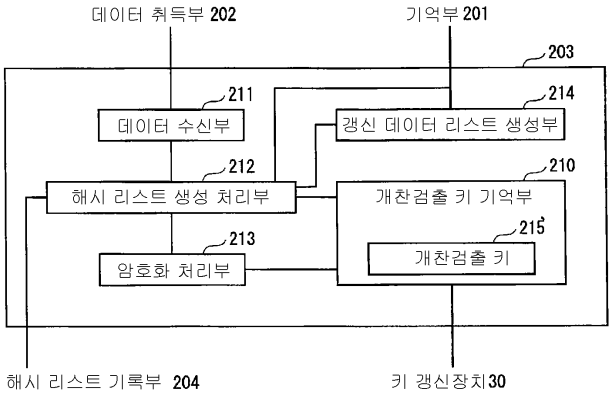
도면6


갱신처리부 103
105
171
제어부 102
검출제어부
172
개찬 검출 호출부
173
개찬검출 처리부
175
마스터 키 기억부
176
마스터 키
174
기억부 101
파일 판독부

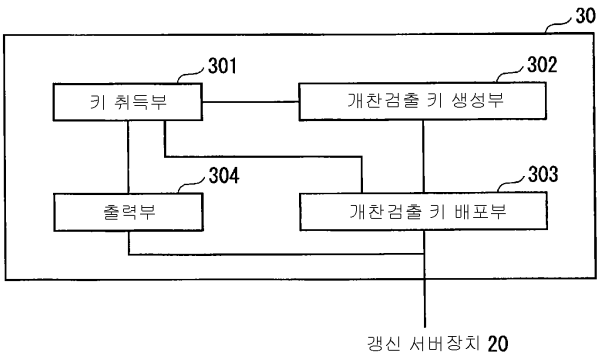
도면7


키 갱신장치 30
휴대전화기 10
20
203
해시 리스트 생성부
204
해시 리스트 기록부
202
201
205
데이터 취득부
기억부
갱신요구 처리부
206
207
입력부
송수신부
인터넷 50

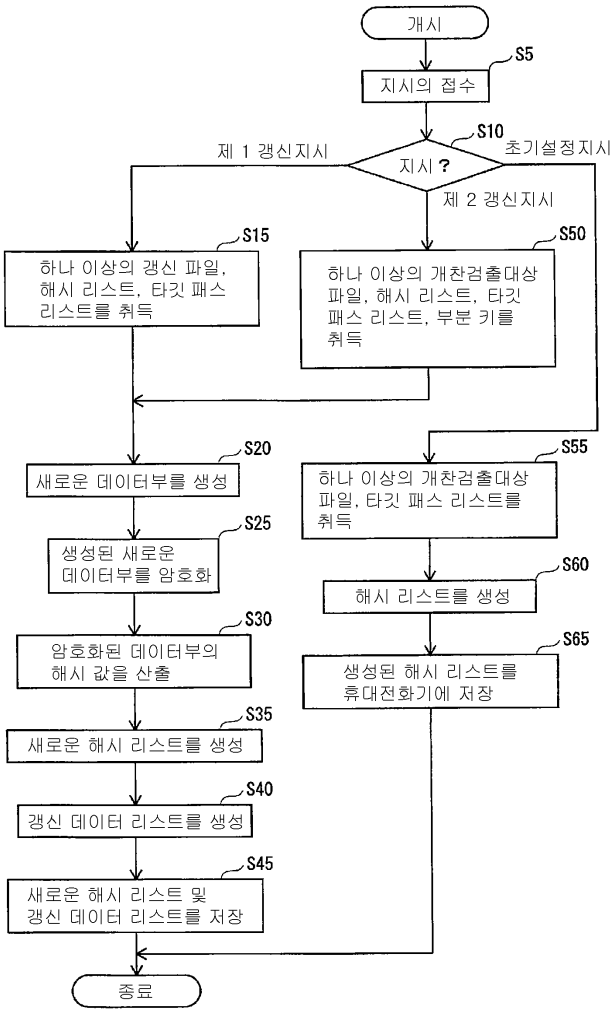
도면8


데이터 취득부 202
기억부 201
203
211
214
데이터 수신부
갱신 데이터 리스트 생성부
212
210
해시 리스트 생성 처리부
개찬검출 키 기억부
215
213
개찬검출 키
암호화 처리부
해시 리스트 기록부 204
키 갱신장치30

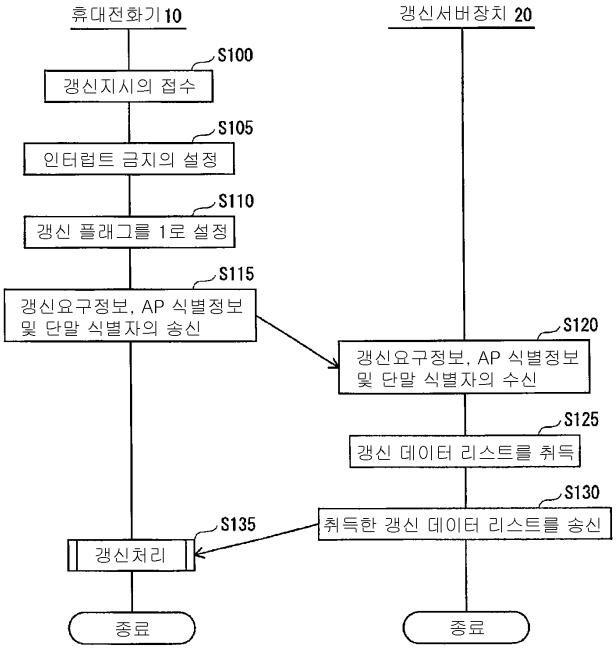
도면9


30
301
302
키 취득부
개찬검출 키 생성부
304
303
출력부
개찬검출 키 배포부
갱신 서버장치 20

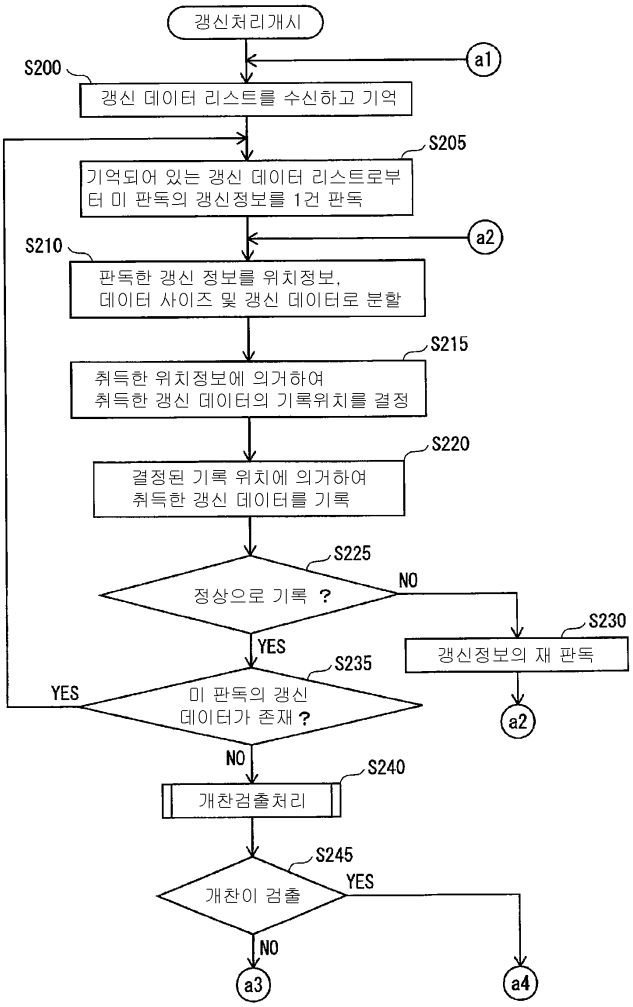
도면10


개시
S5
지시의 접수
S10
지시 ?
제 1 갱신지시
초기설정지시
제 2 갱신지시
S15
하나 이상의 갱신 파일, 해시 리스트, 타깃 패스 리스트를 취득
S50
하나 이상의 개찬검출대상 파일, 해시 리스트, 타깃 패스 리스트, 부분 키를 취득
S20
새로운 데이터부를 생성
S25
생성된 새로운 데이터부를 암호화
S30
암호화된 데이터부의 해시 값을 산출
S35
새로운 해시 리스트를 생성
S40
갱신 데이터 리스트를 생성
S45
새로운 해시 리스트 및 갱신 데이터 리스트를 저장
S55
하나 이상의 개찬검출대상 파일, 타깃 패스 리스트를 취득
S60
해시 리스트를 생성
S65
생성된 해시 리스트를 휴대전화기에 저장
종료

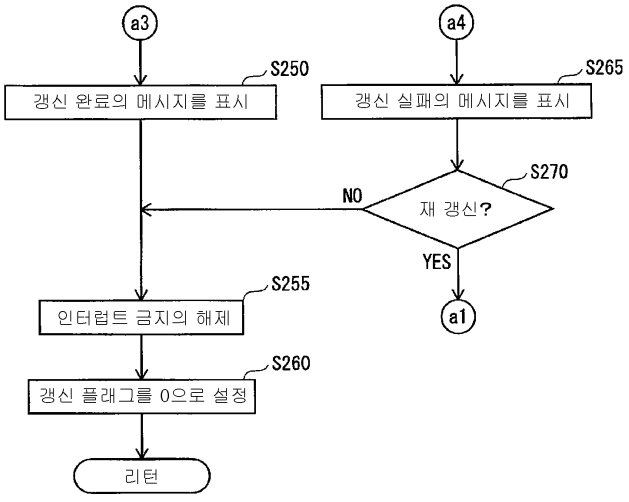
도면11


휴대전화기 10
갱신서버장치 20
S100
갱신지시의 접수
S105
인터럽트 금지의 설정
S110
갱신 플래그를 1로 설정
S115
갱신요구정보, AP 식별정보 및 단말 식별자의 송신
S120
갱신요구정보, AP 식별정보 및 단말 식별자의 수신
S125
갱신 데이터 리스트를 취득
S130
취득한 갱신 데이터 리스트를 송신
S135
갱신처리
종료
종료

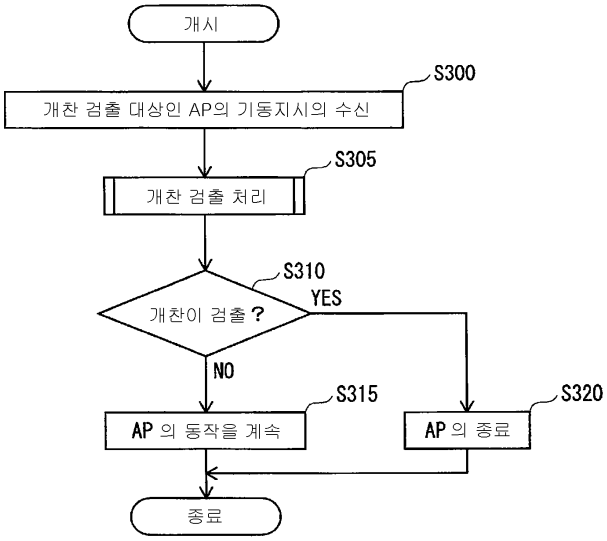
도면12


갱신처리개시
a1
S200
갱신 데이터 리스트를 수신하고 기억
S205
기억되어 있는 갱신 데이터 리스트로부터 미 판독의 갱신정보를 1건 판독
a2
S210
판독한 갱신 정보를 위치정보, 데이터 사이즈 및 갱신 데이터로 분할
S215
취득한 위치정보에 의거하여 취득한 갱신 데이터의 기록위치를 결정
S220
결정된 기록 위치에 의거하여 취득한 갱신 데이터를 기록
S225
정상으로 기록 ?
NO
S230
갱신정보의 재 판독
a2
YES
S235
미 판독의 갱신 데이터가 존재 ?
YES
NO
S240
개찬검출처리
S245
개찬이 검출
YES
NO
a3
a4

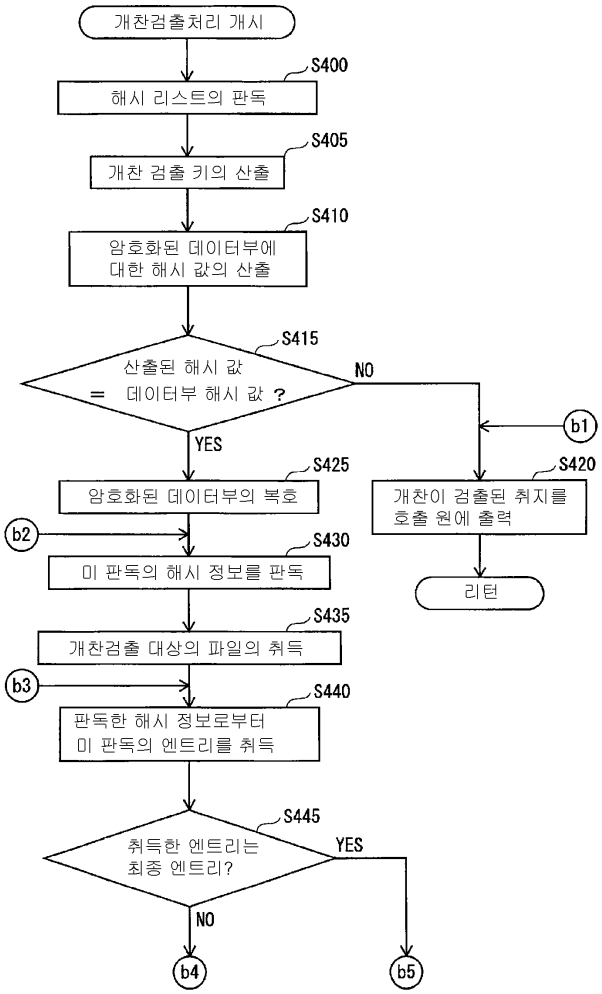
도면13


a3
a4
S250
갱신 완료의 메시지를 표시
S265
갱신 실패의 메시지를 표시
S270
NO
재 갱신?
YES
a1
S255
인터럽트 금지의 해제
S260
갱신 플래그를 0으로 설정
리턴

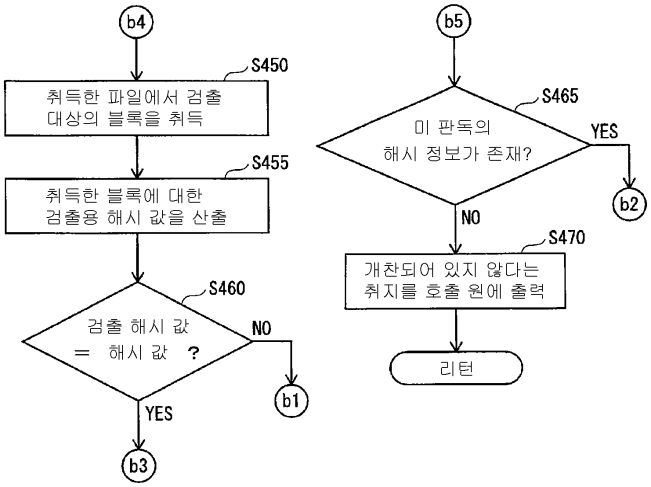
도면14


개시
S300
개찬 검출 대상인 AP의 기동지시의 수신
S305
개찬 검출 처리
S310
YES
개찬이 검출?
NO
S315
AP 의 동작을 계속
S320
AP 의 종료
종료

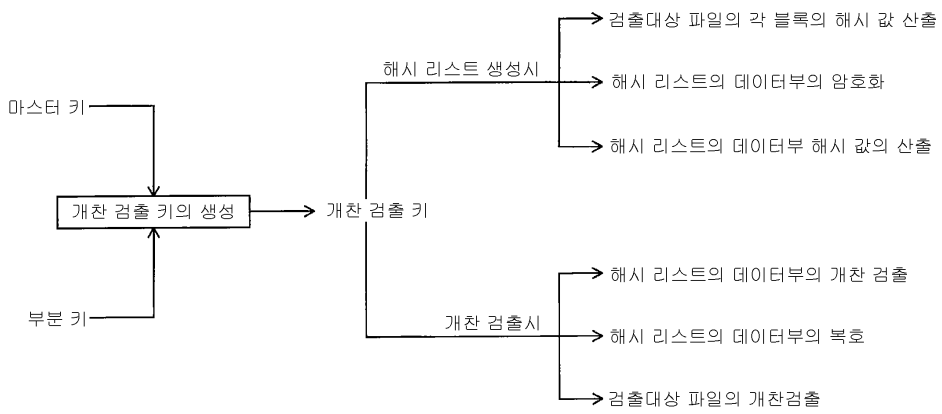
도면15


개찬검출처리 개시
S400
해시 리스트의 판독
S405
개찬 검출 키의 산출
S410
암호화된 데이터부에
대한 해시 값의 산출
S415
산출된 해시 값
= 데이터부 해시 값 ?
NO
YES
b1
S420
개찬이 검출된 취지를
호출 원에 출력
리턴
S425
암호화된 데이터부의 복호
b2
S430
미 판독의 해시 정보를 판독
S435
개찬검출 대상의 파일의 취득
b3
S440
판독한 해시 정보로부터
미 판독의 엔트리를 취득
S445
취득한 엔트리는
최종 엔트리?
YES
NO
b4
b5

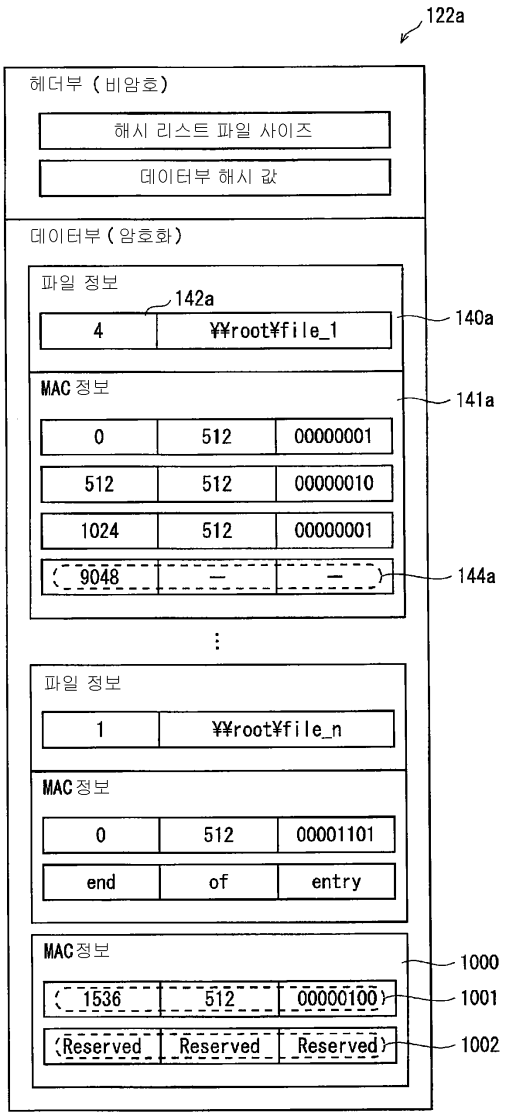
도면16


b4
S450
취득한 파일에서 검출
대상의 블록을 취득
S455
취득한 블록에 대한
검출용 해시 값을 산출
S460
검출 해시 값
= 해시 값 ?
NO
YES
b1
b3
b5
S465
미 판독의
해시 정보가 존재?
YES
NO
b2
S470
개찬되어 있지 않다는
취지를 호출 원에 출력
리턴

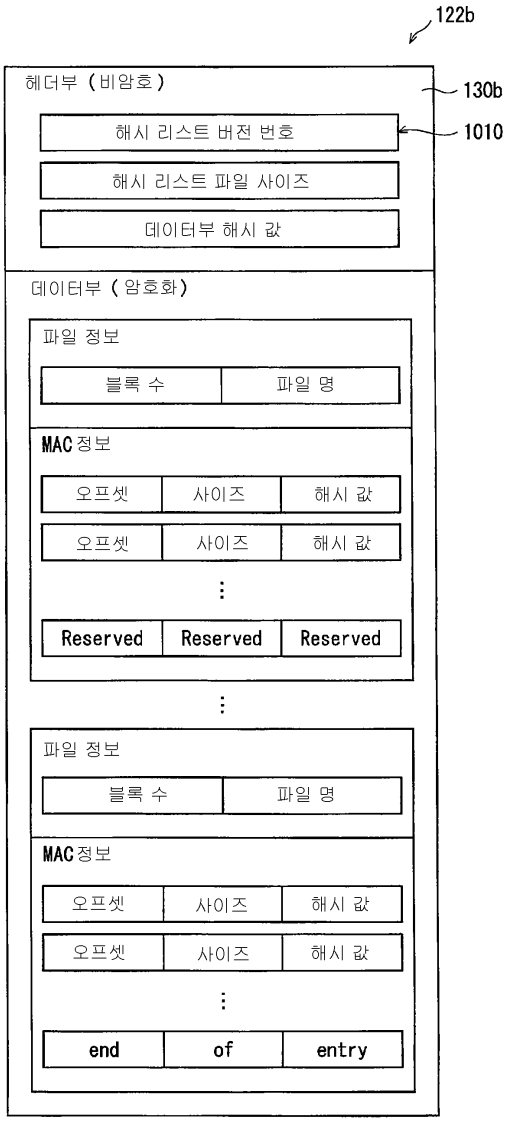
도면17


검출대상 파일의 각 블록의 해시 값 산출
해시 리스트 생성시
해시 리스트의 데이터부의 암호화
마스터 키
해시 리스트의 데이터부 해시 값의 산출
개찬 검출 키의 생성
개찬 검출 키
해시 리스트의 데이터부의 개찬 검출
부분 키
개찬 검출시
해시 리스트의 데이터부의 복호
검출대상 파일의 개찬검출

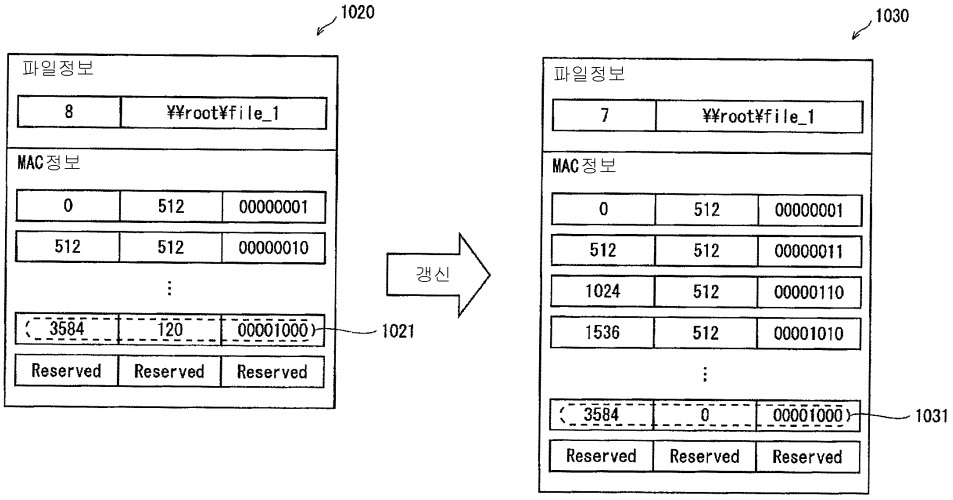
도면18


122a
헤더부 (비암호)
해시 리스트 파일 사이즈
데이터부 해시 값
데이터부 (암호화)
파일 정보
142a
4
¥¥root¥file_1
140a
MAC 정보
141a
0
512
00000001
512
512
00000010
1024
512
00000001
9048
-
-
144a
파일 정보
1
¥¥root¥file_n
MAC정보
0
512
00001101
end
of
entry
MAC정보
1000
1536
512
00000100
1001
Reserved
Reserved
Reserved
1002

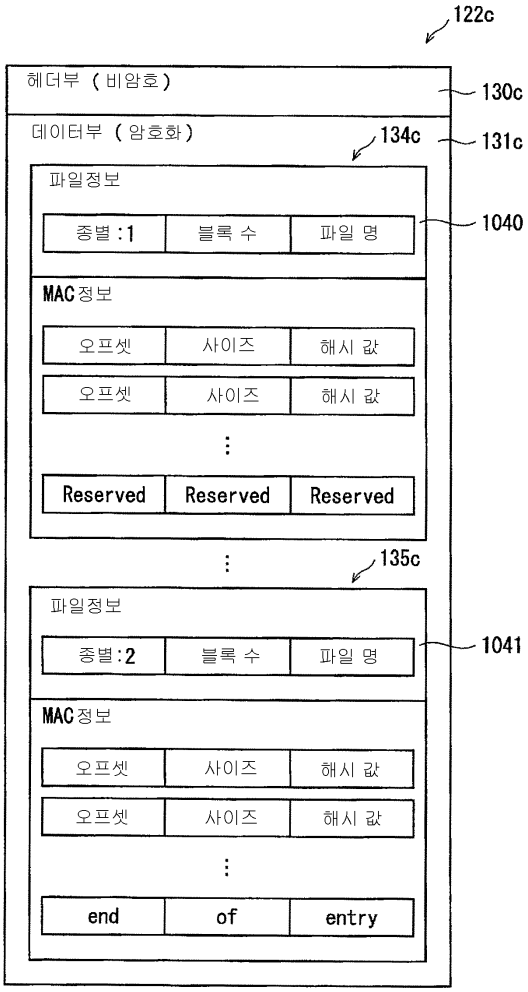
도면19


122b
헤더부 (비암호)
130b
해시 리스트 버전 번호
1010
해시 리스트 파일 사이즈
데이터부 해시 값
데이터부 (암호화)
파일 정보
블록 수
파일 명
MAC 정보
오프셋
사이즈
해시 값
오프셋
사이즈
해시 값
Reserved
Reserved
Reserved
파일 정보
블록 수
파일 명
MAC 정보
오프셋
사이즈
해시 값
오프셋
사이즈
해시 값
end
of
entry

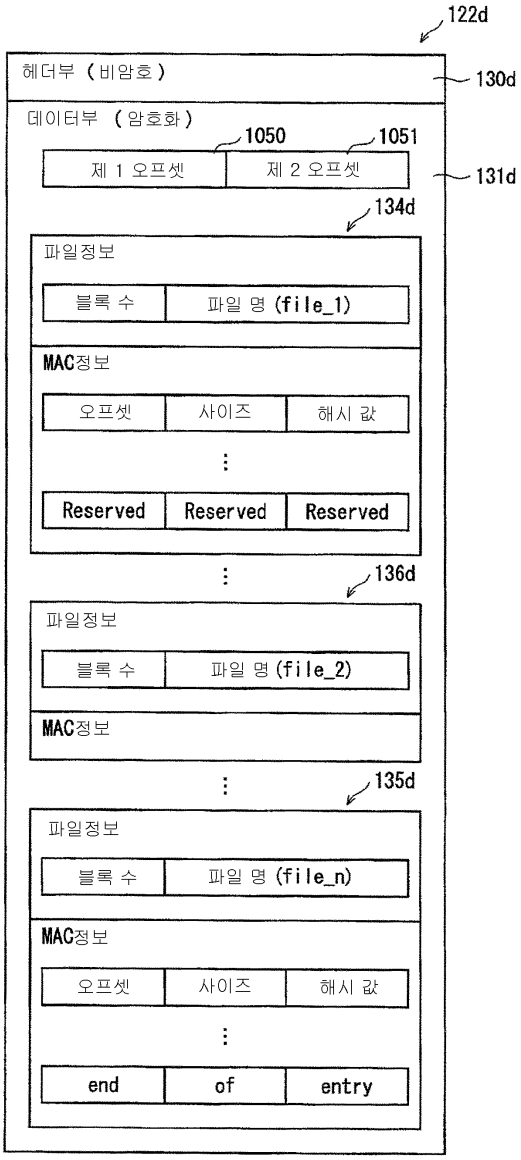
도면20


1020
파일정보
8
¥¥root¥file_1
MAC정보
0
512
00000001
512
512
00000010
3584
120
00001000
1021
Reserved
Reserved
Reserved
갱신
1030
파일정보
7
¥¥root¥file_1
MAC정보
0
512
00000001
512
512
00000011
1024
512
00000110
1536
512
00001010
3584
0
00001000
1031
Reserved
Reserved
Reserved

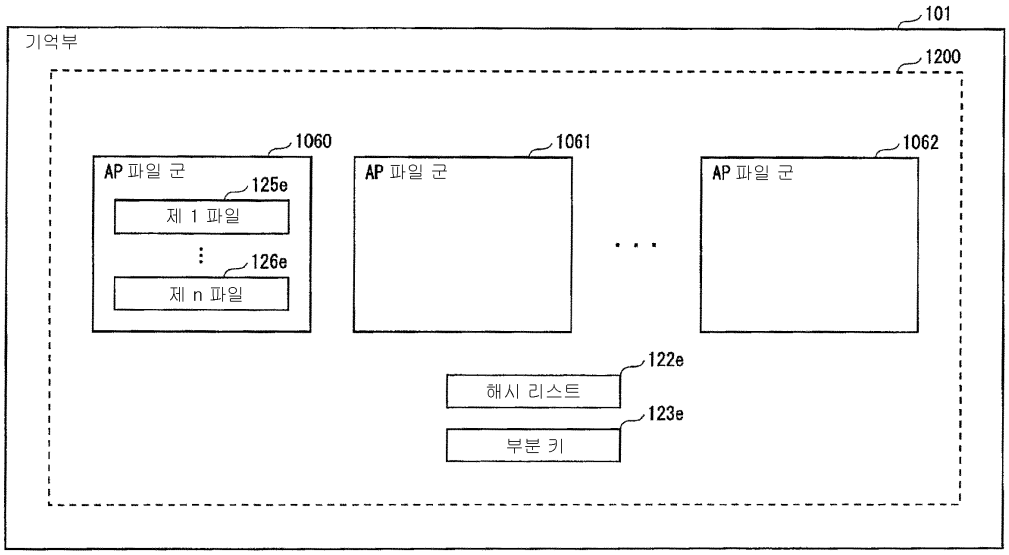
도면21


122c
헤더부 (비암호)
130c
데이터부 (암호화)
131c
134c
파일정보
종별:1
블록 수
파일 명
1040
MAC정보
오프셋
사이즈
해시 값
오프셋
사이즈
해시 값
Reserved
Reserved
Reserved
135c
파일정보
종별:2
블록 수
파일 명
1041
MAC정보
오프셋
사이즈
해시 값
오프셋
사이즈
해시 값
end
of
entry

도면22


122d
헤더부 (비암호)
130d
데이터부 (암호화)
1050
1051
제 1 오프셋
제 2 오프셋
131d
134d
파일정보
블록 수
파일 명 (file_1)
MAC정보
오프셋
사이즈
해시 값
Reserved
Reserved
Reserved
136d
파일정보
블록 수
파일 명 (file_2)
MAC정보
135d
파일정보
블록 수
파일 명 (file_n)
MAC정보
오프셋
사이즈
해시 값
end
of
entry

도면23


101
기억부
1200
1060
AP 파일 군
125e
제 1 파일
126e
제 n 파일
1061
AP 파일 군
1062
AP 파일 군
122e
해시 리스트
123e
부분 키