(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5015081号
(P5015081)

(45)発行日　平成24年8月29日(2012.8.29)　(24)登録日　平成24年6月15日(2012.6.15)

(51)Int.Cl.　　F I
G06F 3/042 (2006.01)　　G06F 3/042 421
H04L 9/08 (2006.01)　　H04L 9/00 601B
　　H04L 9/00 601E

請求項の数 19　(全 23 頁)

(21)出願番号　特願2008-174718 (P2008-174718)
(22)出願日　平成20年7月3日 (2008.7.3)
(65)公開番号　特開2010-15383 (P2010-15383A)
(43)公開日　平成22年1月21日 (2010.1.21)
審査請求日　平成22年11月11日 (2010.11.11)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100114236
弁理士　藤井　正弘
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100120260
弁理士　飯田　雅昭
(72)発明者　徳永　稔
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】取得したデータを暗号化する電子ペン、その電子ペンを制御する方法、及び、その電子ペンを含む情報システム

(57)【特許請求の範囲】
【請求項１】
ペン先の軌跡の座標情報を含むデータを取得し、前記取得したデータを暗号化して出力する電子ペンであって、
取得した前記データを保持するメモリと、前記メモリに接続されるプロセッサと、前記メモリ及び前記プロセッサに電力を供給する電源部と、を備え、
前記データの取得を開始した後、前記電子ペンを用いた筆記の中断を示す所定のイベントを検出したか否かを判定し、
前記所定のイベントが検出された場合、前記保持されたデータを暗号化することによって、暗号化されたデータを生成し、
前記暗号化されたデータを出力し、
前記所定のイベントは、前記電子ペンが最後に前記データを取得してから所定の時間が経過したこと、又は、前記電子ペンに電源切断要求が入力されたことであることを特徴とする電子ペン。
【請求項２】
前記電子ペンは、
第１暗号鍵を生成し、
前記所定のイベントが検出された場合、前記第１暗号鍵を用いて、前記暗号化されたデータを生成した後、前記保持されたデータを消去し、
前記第１暗号鍵を、公開暗号鍵を用いて暗号化した後、前記第１暗号鍵を消去し、

前記暗号化された第１暗号鍵を出力することを特徴とする請求項１に記載の電子ペン。
【請求項３】
前記電子ペンは、
前記第１暗号鍵を生成する前に前記公開暗号鍵を保持していない場合、所定の要求を出力し、
前記公開暗号鍵が入力されると、前記入力された公開暗号鍵を保持し、
前記公開暗号鍵が入力された後、前記データの取得を開始する前に、前記第１暗号鍵を生成することを特徴とする請求項２に記載の電子ペン。
【請求項４】
前記電子ペンは、
前記第１暗号鍵を消去した後、前記第１暗号鍵と異なる第２暗号鍵を生成し、
新たなデータを取得して保持し、
前記新たなデータの取得を開始した後、前記所定のイベントを検出したか否かを判定し、
前記所定のイベントが検出された場合、前記保持された新たなデータを、前記第２暗号鍵を用いて暗号化することによって、暗号化された新たなデータを生成することを特徴とする請求項２に記載の電子ペン。
【請求項５】
前記電子ペンは、
前記第１暗号鍵を消去した後、前記電源部による前記プロセッサ及び前記メモリへの電力供給を切断し、
電源投入要求が入力されると、前記電源部による前記プロセッサ及び前記メモリへの電力供給を開始した後、前記第２暗号鍵を生成することを特徴とする請求項４に記載の電子ペン。
【請求項６】
前記電子ペンにペン先を覆うキャップを取り付けることによって前記電源切断要求が入力され、前記電子ペンから前記キャップを取り外すことによって前記電源投入要求が入力されることを特徴とする請求項５に記載の電子ペン。
【請求項７】
前記電子ペンは、
前記第１暗号鍵と異なる第３暗号鍵を生成し、
第１座標範囲内の第１座標を示す前記座標情報を含む前記データを取得した後、前記第１座標範囲外の第２座標を示す前記座標情報を含む前記データを取得した場合、前記第１座標を示す前記座標情報を含む前記データを、前記第１暗号鍵を用いて暗号化し、前記第２座標を示す前記座標情報を含む前記データを、前記第３暗号鍵を用いて暗号化することを特徴とする請求項２に記載の電子ペン。
【請求項８】
ペン先の軌跡の座標情報を含むデータを取得し、前記取得したデータを暗号化して出力する電子ペンを制御するプログラムであって、
前記電子ペンは、取得した前記データを保持するメモリと、前記メモリに接続されるプロセッサと、前記メモリ及び前記プロセッサに電力を供給する電源部と、を備え、
前記プログラムは、
前記データの取得を開始した後、前記電子ペンを用いた筆記の中断を示す所定のイベントを検出したか否かを判定する手順と、
前記所定のイベントが検出された場合、前記保持されたデータを暗号化することによって、暗号化されたデータを生成する手順と、
前記暗号化されたデータを出力する手順と、を前記プロセッサに実行させ、
前記所定のイベントは、前記電子ペンが最後に前記データを取得してから所定の時間が経過したこと、又は、前記電子ペンに電源切断要求が入力されたことであることを特徴とするプログラム。

【請求項９】
前記プログラムは、さらに、
第１暗号鍵を生成する手順と、
前記暗号化されたデータを生成した後、前記保持されたデータを消去する手順と、
前記第１暗号鍵を、公開暗号鍵を用いて暗号化する手順と、
前記第１暗号鍵が暗号化された後、前記第１暗号鍵を消去する手順と、
前記暗号化された第１暗号鍵を出力する手順と、を前記プロセッサに実行させ、
前記暗号化されたデータを生成する手順は、前記第１暗号鍵を用いて、前記保持されたデータを暗号化することによって実行されることを特徴とする請求項８に記載のプログラム。
【請求項１０】
前記プログラムは、さらに、
前記第１暗号鍵を消去した後、前記第１暗号鍵と異なる第２暗号鍵を生成する手順と、
新たなデータを取得して保持する手順と、
前記新たなデータの取得を開始した後、前記所定のイベントを検出したか否かを判定する手順と、
前記所定のイベントが検出された場合、前記保持された新たなデータを、前記第２暗号鍵を用いて暗号化することによって、暗号化された新たなデータを生成する手順と、を前記プロセッサに実行させることを特徴とする請求項９に記載のプログラム。
【請求項１１】
前記プログラムは、さらに、前記第１暗号鍵と異なる第３暗号鍵を生成する手順を前記プロセッサに実行させ、
前記暗号化されたデータを生成する手順は、第１座標範囲内の第１座標を示す前記座標情報を含む前記データが取得された後、前記第１座標範囲外の第２座標を示す前記座標情報を含む前記データが取得された場合、前記第１座標を示す前記座標情報を含む前記データを、前記第１暗号鍵を用いて暗号化する手順と、前記第２座標を示す前記座標情報を含む前記データを、前記第３暗号鍵を用いて暗号化する手順と、を含むことを特徴とする請求項９に記載のプログラム。
【請求項１２】
電子ペンと、前記電子ペンと通信するインターフェースと、前記インターフェースに接続されるデータ振り分け計算機と、前記データ振り分け計算機に接続される一つ以上のデータ処理計算機と、を備える情報システムであって、
前記電子ペンは、前記電子ペンが取得したペン先の軌跡の座標情報を含むデータを保持する第１メモリと、前記第１メモリに接続される第１プロセッサと、前記第１メモリ及び前記第１プロセッサに電力を供給する電源部と、を備え、
前記データ振り分け計算機は、前記インターフェース及び前記一つ以上のデータ処理計算機と通信する第１通信装置と、前記第１通信装置に接続される第２プロセッサと、前記第２プロセッサに接続される第２メモリと、を備え、
前記各データ処理計算機は、前記データ振り分け計算機と通信する第２通信装置と、前記第２通信装置に接続される第３プロセッサと、前記第３プロセッサに接続される第３メモリと、を備え、
前記電子ペンは、
前記データの取得を開始した後、前記電子ペンを用いた筆記の中断を示す所定のイベントを検出したか否かを判定し、
前記所定のイベントが検出された場合、前記保持されたデータを暗号化することによって、暗号化されたデータを生成し、
前記暗号化されたデータを送信し、
前記所定のイベントは、前記電子ペンが最後に前記データを取得してから所定の時間が経過したこと、又は、前記電子ペンに電源切断要求が入力されたことであることを特徴とする情報システム。

【請求項１３】
前記電子ペンは、
第１暗号鍵を生成し、
前記所定のイベントが検出された場合、前記第１暗号鍵を用いて、前記暗号化されたデータを生成した後、前記保持されたデータを消去し、
前記第１暗号鍵を、前記データ振り分け計算機が保持する秘密暗号鍵に対応する公開暗号鍵を用いて暗号化した後、前記第１暗号鍵を消去し、
前記暗号化された第１暗号鍵を送信することを特徴とする請求項１２に記載の情報システム。
【請求項１４】
前記電子ペンは、前記第１暗号鍵を生成する前に前記公開暗号鍵を保持していない場合、所定の要求を、前記インターフェースを介して前記データ振り分け計算機に送信し、
前記データ振り分け計算機は、前記所定の要求を受信すると、前記データ振り分け計算機が保持する前記秘密暗号鍵に対応する前記公開暗号鍵を送信し、
前記電子ペンは、前記公開暗号鍵を受信すると、前記受信した公開暗号鍵を保持し、
前記公開暗号鍵を受信した後、前記データの取得を開始する前に、前記第１暗号鍵を生成することを特徴とする請求項１３に記載の情報システム。
【請求項１５】
前記電子ペンは、
前記第１暗号鍵を消去した後、前記第１暗号鍵と異なる第２暗号鍵を生成し、
新たなデータを取得して保持し、
前記新たなデータの取得を開始した後、前記所定のイベントを検出したか否かを判定し、
前記所定のイベントが検出された場合、前記保持された新たなデータを、前記第２暗号鍵を用いて暗号化することによって、暗号化された新たなデータを生成することを特徴とする請求項１３に記載の情報システム。
【請求項１６】
前記電子ペンは、
前記第１暗号鍵を消去した後、前記電源部による前記プロセッサ及び前記メモリへの電力供給を切断し、
電源投入要求が入力されると、前記電源部による前記プロセッサ及び前記メモリへの電力供給を開始し、前記第２暗号鍵を生成することを特徴とする請求項１５に記載の情報システム。
【請求項１７】
前記電子ペンは、
取得した前記データが、第１座標範囲内の第１座標を示す前記座標情報を含む場合、前記暗号化された第１暗号鍵、及び、前記第１座標範囲を識別する情報を、前記インターフェースを介して前記データ振り分け計算機に送信し、
前記データ振り分け計算機には、座標範囲と、前記各データ処理計算機とを対応付ける管理情報、及び、前記各データ処理計算機が保持する秘密暗号鍵に対応する公開暗号鍵があらかじめ保持され、
前記データ振り分け計算機は、
前記第１座標範囲を識別する情報を受信すると、前記管理情報に基づいて、前記第１座標範囲に対応する前記データ処理計算機を特定し、
前記暗号化された第１暗号鍵を、前記データ振り分け計算機が保持する秘密暗号鍵を用いて復号化し、
前記復号化された第１暗号鍵を、前記特定されたデータ処理計算機に対応する前記公開暗号鍵を用いて暗号化し、
前記特定されたデータ処理計算機を識別する情報、及び、前記特定されたデータ処理計算機に対応する前記公開暗号鍵を用いて暗号化された前記第１暗号鍵を、前記電子ペンに

送信し、
前記電子ペンは、前記暗号化されたデータ、及び、前記特定されたデータ処理計算機に対応する前記公開暗号鍵を用いて暗号化された前記第１暗号鍵を、前記特定されたデータ処理計算機に送信し、
前記特定されたデータ処理計算機は、
前記特定されたデータ処理計算機に対応する前記公開暗号鍵を用いて暗号化された前記第１暗号鍵を、前記特定されたデータ処理計算機が保持する前記秘密暗号鍵を用いて復号化し、
前記復号化された第１暗号鍵を用いて、前記暗号化されたデータを復号化することを特徴とする請求項１３に記載の情報システム。
【請求項１８】
前記電子ペンは、
前記第１暗号鍵と異なる第３暗号鍵を生成し、
第１座標範囲内の第１座標を示す前記座標情報を含む前記データを取得した後、前記第１座標範囲外の第２座標を示す前記座標情報を含む前記データを取得した場合、前記第１座標を示す前記座標情報を含む前記データを、前記第１暗号鍵を用いて暗号化し、前記第２座標を示す前記座標情報を含む前記データを、前記第３暗号鍵を用いて暗号化することを特徴とする請求項１７に記載の情報システム。
【請求項１９】
ペン先の軌跡の座標情報を含むデータを取得し、前記取得したデータを暗号化して出力する電子ペンを制御する方法であって、
前記電子ペンは、前記データを保持するメモリと、前記メモリに接続されるプロセッサと、を備え、
前記方法は、
前記データの取得を開始した後、前記電子ペンを用いた筆記の中断を示す所定のイベントを検出したか否かを判定する手順と、
前記所定のイベントが検出された場合、前記保持されたデータを暗号化することによって、暗号化されたデータを生成する手順と、
前記暗号化されたデータを出力する手順と、を含み、
前記所定のイベントは、前記電子ペンが最後に前記データを取得してから所定の時間が経過したこと、又は、前記電子ペンに電源切断要求が入力されたことであることを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本願明細書で開示される技術は、情報システムにおけるデータの盗聴防止技術に関し、特に、電子ペンを用いる情報システムにおけるデータの暗号技術に関する。
【背景技術】
【０００２】
情報システムにおけるデータの暗号技術として、特許文献１に記載の技術がある。特許文献１によれば、カメラで撮影した画像データが暗号化され、そのカメラに保存される。
【０００３】
また、情報システムにおけるデータの暗号技術として、非特許文献１に記載の技術がある。非特許文献１に記載されたＷＰＡ－ＰＳＫは、ネットワーク上のデータを暗号化する技術である。これによると、暗号化直前に暗号鍵が生成され、さらに、フレームごとに暗号鍵が変更される。
【特許文献１】特開２００７－２８８３８３号公報
【非特許文献１】“（平成１９年改訂版）安心して無線ＬＡＮを利用するために”、［ｏｎｌｉｎｅ］、平成１９年１２月、総務省、［平成２０年６月１０日検索］、インターネット＜URL:http://www.soumu.go.jp/joho_tsusin/pdf/071214_1_bt.pdf＞

【発明の開示】
【発明が解決しようとする課題】
【０００４】
上記の従来技術を組み合わせても、ネットワークに接続されていない状態におけるデータの発生源であるデータ作成装置内データの暗号化と、ネットワーク上の前記データの暗号化とを一貫してカバーすることができない。さらに、上記の従来技術の単なる組み合わせは、データ作成装置のリソースが乏しい場合に実現が困難である。
【課題を解決するための手段】
【０００５】
本願で開示する代表的な発明は、ペン先の軌跡の座標情報を含むデータを取得し、前記取得したデータを暗号化して出力する電子ペンであって、取得した前記データを保持するメモリと、前記メモリに接続されるプロセッサと、前記メモリ及び前記プロセッサに電力を供給する電源部と、を備え、前記データの取得を開始した後、前記電子ペンを用いた筆記の中断を示す所定のイベントを検出したか否かを判定し、前記所定のイベントが検出された場合、前記保持されたデータを暗号化することによって、暗号化されたデータを生成し、前記暗号化されたデータを出力し、前記所定のイベントは、前記電子ペンが最後に前記データを取得してから所定の時間が経過したこと、又は、前記電子ペンに電源切断要求が入力されたことであることを特徴とする。
【発明の効果】
【０００６】
本発明の一実施形態によれば、データの発生源であるデータ作成装置のリソースが乏しい場合でも、ネットワークに接続されていない状態におけるデータ作成装置内データの暗号化と、ネットワーク上の前記データの暗号化とを一貫してカバーすることができ、それによってデータの盗聴を防止できる。
【発明を実施するための最良の形態】
【０００７】
以下、本発明の実施の形態を、図面を用いて詳細に説明する。
【０００８】
図１は、本発明の実施形態の全体システム構成を示すブロック図である。
【０００９】
本実施形態は、ある帳票フォーマットをドットパターンとともに紙に印刷し、紙上に印刷されたドットパターンを電子ペンで読み取ることによって、紙上に手書きした文字又は図形を電子データ化する電子ペンシステムである。この電子ペンシステムにおいて、電子ペンクライアント１１１、データ振り分けサーバ１２１、データ処理サーバ１３１及びデータ処理サーバ１４１がネットワーク１０３を介して接続されており、各装置間でのデータ送受信が可能である。
【００１０】
電子ペン１０１は、例えば、国際公開第２００３／００１４４０号パンフレットに記載の技術によって実現される。この技術によれば、ある特殊な電子ペン１０１と、ドットパターンが印刷された電子ペン対応帳票とが用いられ、その電子ペン１０１を使って電子ペン対応帳票上に書き込んだ文字及び図形の軌跡をベクトル化して保存及び送信することができる。
【００１１】
図１には一つの電子ペン１０１のみを示すが、本実施形態の電子ペンシステムは、複数の電子ペン１０１を備えてもよい。
【００１２】
図２は、電子ペン１０１の構成及び機能を説明する図である。
【００１３】
電子ペン対応帳票１０２にはドットパターン２０１が印刷されている。ドットは一定間隔の格子点ごとに印刷されているが、その位置は格子点から所定の距離だけずれている。

電子ペン１０１は、ドットパターン２０１の印刷面に発光ダイオード２０２の光を射出して、内蔵カメラ２０３によってこのドットパターン２０１を読み取ることによって、電子ペン１０１のペン先がドットパターン空間上のどの位置にあるか、その絶対座標を正確に特定することができる。

【００１４】

ドットパターン空間は、その管理を容易にするため、用紙サイズの標準規格等の所定の大きさに区切られ、各区画にドットパターン固有識別子が割り当てられている。電子ペン１０１は、読み取ったドットパターン２０１のドットパターン固有識別子も出力する。ここでは、電子ペン対応帳票１０２のページごとにドットパターン固有識別子が割り当てられているものとし、このドットパターン固有識別子をＰａｇｅＩＤと呼ぶ。

【００１５】

電子ペン１０１は、発光ダイオード２０２、カメラ２０３、インクカートリッジ２０４、筆圧センサ２０５、プロセッサ２０６、メモリ２０７、時計２０８、バッテリ２０９及び通信装置２１０を内蔵している。

【００１６】

筆圧センサ２０５が感圧しているときのみカメラ２０３はドットパターンを読み取り、そのドットパターンに基づいて、プロセッサ２０６がペン先の位置情報を取得する。すなわち、プロセッサ２０６は、電子ペン１０１によって電子ペン対応帳票１０２に書き込まれた文字又は図形の軌跡をデジタル化して取得する。このデジタル軌跡情報は、筆記データとして時系列にメモリ２０７に蓄積され、あるタイミングで通信装置２１０によって所定の機器に送信される。

【００１７】

例えば、送信ボックス２１１の領域内に電子ペン１０１で書き込みを行ったことを契機として、筆記データが送信されてもよい。電子ペン１０１は、送信ボックス２１１の領域が特別な座標領域であると認識し、その領域の座標を取得すると、それまでに蓄積されていた筆記データを、通信装置２１０を介して電子ペンクライアント１１１に送信する。

【００１８】

バッテリ２０９は、電子ペン１０１内の各部（例えば、発光ダイオード２０２、カメラ２０３、プロセッサ２０６及びメモリ２０７等）に電力を供給する電源部である。

【００１９】

電子ペン１０１は、電源の切断の要求を入力されると、電源を切断し（すなわち、バッテリ２０９による各部への電力の供給を停止し）、電源の投入の要求を入力されると、電源を投入する（すなわち、バッテリ２０９による各部への電力の供給を開始する）。

【００２０】

電子ペン１０１の電源の切断の要求は、例えば、図示しないキャップをペン先に被せることによって入力される。電子ペン１０１の電源の投入の要求は、例えば、図示しないキャップをペン先から外すことによって入力される。

【００２１】

メモリ２０７は不揮発であるため、電源を切断しても蓄積されたデータは消えない。メモリ２０７が容量不足になった場合、電子ペン１０１は、出力装置（図示省略）を用いてユーザに通知する。

【００２２】

プロセッサ２０６がメモリ２０７内のプログラムを順次読み込んで実行することによって、処理部としての役割を果たす電子ペンＰＧ２１２が機能する。電子ペンＰＧ２１２の具体的な動作は後述する。

【００２３】

さらに、メモリ２０７には、筆記データ管理テーブル２１３、暗号筆記データ管理テーブル２１４、鍵格納部２１５及びデータ振り分けサーバ情報格納部２１６が保持される。

【００２４】

鍵格納部２１５は、筆記データの暗号化に用いる暗号鍵を格納するための領域である。

【００２５】
データ振り分けサーバ情報格納部２１６は、電子ペンクライアント１１１が筆記データを送信するときに参照される。電子ペンクライアント１１１は、筆記データを送信するとき、その筆記データをどのデータ処理サーバに送信すべきかをデータ振り分けサーバ１２１に問い合わせる。データ振り分けサーバ情報格納部２１６は、その問い合わせ先となるデータ振り分けサーバ１２１を識別する情報を格納するための領域である。
【００２６】
図３は、本発明の実施形態の筆記データ管理テーブル２１３の構成を説明する図である。
【００２７】
筆記データ管理テーブル２１３は、筆記データを蓄積するためのテーブルであり、「筆記データ」を格納する。「筆記データ」は、前述のデジタル軌跡情報のほか、その属性も含むデータである。例えば、筆記データは、上記のデジタル軌跡情報に加えて、そのデジタル軌跡情報に含まれる座標が属するページを識別するＰａｇｅＩＤ、そのデジタル軌跡情報が取得された時刻を示す情報、及び、そのデジタル軌跡情報が取得されたときの筆圧を示す情報を含んでもよい。
【００２８】
図４は、本発明の実施形態の暗号筆記データ管理テーブル２１４の構成を説明する図である。
【００２９】
暗号筆記データ管理テーブル２１４は、暗号化された筆記データを蓄積するためのテーブルであり、「暗号筆記データ」を格納する。「暗号筆記データ」は、暗号化されたデジタル軌跡情報のほか、その属性も含むデータである。
【００３０】
電子ペンクライアント１１１は、電子ペン１０１から送信される筆記データをデータ処理サーバに中継するコンピュータ装置である。電子ペンクライアント１１１は、ＣＰＵ１１２、通信装置１１３、通信装置１１４、記憶装置１１５及びそれらの間のデータ通信等を制御する制御装置（図示省略）等を備える。
【００３１】
通信装置１１３は、無線通信又は有線通信によって電子ペン１０１と接続されるインターフェースである。通信装置１１４は、ネットワーク１０３と接続されるインターフェースである。
【００３２】
なお、電子ペン１０１は、筆記データを送信するときには通信装置１１３に接続される必要があるが、常に通信装置１１３に接続されている必要はない。一般に、電子ペン１０１は、筆記データを取得している間、通信装置１１３から切り離されている。
【００３３】
ＣＰＵ１１２が記憶装置１１５内のプログラムを順次読み込んで実行することによって、処理部としての役割を果たす電子ペンクライアントＰＧ１１６が機能する。電子ペンクライアントＰＧ１１６の具体的な動作は後述する。
【００３４】
データ処理サーバ１３１は、電子ペンクライアント１１１から送信される筆記データを利用するコンピュータ装置である。データ処理サーバ１３１は、筆記データをどのように利用してもよい。例えば、データ処理サーバ１３１は、文字認識技術を用いて筆記データをテキストデータに変換し、その後、そのテキストデータを従来と同様のアプリケーションプログラム（図示省略）によって処理してもよい。データ処理サーバ１３１は、ＣＰＵ１３２、通信装置１３３、記憶装置１３４及びそれらの間のデータ通信等を制御する制御装置（図示省略）等を備える。
【００３５】
通信装置１３３は、ネットワーク１０３と接続される。

【００３６】
ＣＰＵ１３２が記憶装置１３４内のプログラムを順次読み込んで実行することによって、処理部としての役割を果たすデータ処理サーバＰＧ１３５が機能する。データ処理サーバＰＧ１３５の具体的な動作は後述する。
【００３７】
記憶装置１３４には、さらに、鍵ペア格納部１３６が保持される。鍵ペア格納部１３６は、公開鍵暗号の鍵ペア（すなわち、公開鍵と、その公開鍵に対応する秘密鍵とからなるペア）を格納するための領域である。
【００３８】
データ処理サーバ１４１は、データ処理サーバ１３１と同様、電子ペンクライアント１１１から送信される筆記データを利用するコンピュータ装置である。データ処理サーバ１４１は、ＣＰＵ１４２、通信装置１４３、記憶装置１４４及びそれらの間のデータ通信等を制御する制御装置（図示省略）等を備える。
【００３９】
通信装置１４３は、ネットワーク１０３と接続される。
【００４０】
また、ＣＰＵ１４２が記憶装置１４４内のプログラムを順次読み込んで実行することによって、処理部としての役割を果たすデータ処理サーバＰＧ１４５が機能する。データ処理サーバＰＧ１４５の具体的な動作は、データ処理サーバＰＧ１３５と同様であるため、説明を省略する。
【００４１】
記憶装置１４４には、さらに、鍵ペア格納部１４６が保持される。鍵ペア格納部１４６は、鍵ペア格納部１３６と同様、公開鍵暗号の鍵ペアを格納するための領域である。ただし、鍵ペア格納部１３６及び鍵ペア格納部１４６には、それぞれ、データ処理サーバ１３１及びデータ処理サーバ１４１が使用する鍵ペアが格納される。
【００４２】
図１には二つのデータ処理サーバを示すが、本実施形態の電子ペンシステムは、一つのデータ処理サーバのみを備えてもよいし、三つ以上のデータ処理サーバを備えてもよい。
【００４３】
データ振り分けサーバ１２１は、電子ペンクライアント１１１が筆記データを適切なデータ処理サーバに送信できるように、電子ペンクライアント１１１からの問い合わせに答えるコンピュータ装置である。データ振り分けサーバ１２１は、ＣＰＵ１２２、通信装置１２３、記憶装置１２４及びそれらの間のデータ通信等を制御する制御装置（図示省略）等を備える。
【００４４】
通信装置１２３は、ネットワーク１０３と接続される。
【００４５】
ＣＰＵ１２２が記憶装置１２４内のプログラムを順次読み込んで実行することによって、処理部としての役割を果たすデータ振り分けサーバＰＧ１２５が機能する。データ振り分けサーバＰＧ１２５の具体的な動作は後述する。
【００４６】
記憶装置１２４には、さらに、鍵ペア格納部１２６、データ処理サーバ管理テーブル１２７およびページ管理テーブル１２８が保持される。
【００４７】
鍵ペア格納部１２６は、公開鍵暗号の鍵ペアを格納するための領域である。
【００４８】
図５は、本発明の実施形態のデータ処理サーバ管理テーブル１２７の構成を説明する図である。
【００４９】
データ処理サーバ管理テーブル１２７は、電子ペンシステムにおいてデータ処理サーバ

が筆記データを受け取れるようにするためのデータを管理するテーブルであり、データ処理サーバＩＤ７０１と公開鍵７０２とを対応付けて格納する。データ処理サーバＩＤ７０１は、ネットワーク１０３上で各データ処理サーバを一意に識別するアドレスである。公開鍵７０２は、各データ処理サーバで使用される公開鍵暗号の公開鍵（すなわち、各データ処理サーバが保持する秘密鍵に対応する公開鍵）である。

【００５０】

図６は、本発明の実施形態のページ管理テーブル１２８の構成を説明する図である。

【００５１】

ページ管理テーブル１２８は、電子ペン１０１で筆記したページごとに、その筆記データを受け取るべきデータ処理サーバ（言い換えると、電子ペンクライアント１１１が筆記データを送信すべきデータ処理サーバ）を管理するためのテーブルであり、ＰａｇｅＩＤ８０１とデータ処理サーバＩＤ８０２とを対応付けて格納する。

【００５２】

なお、図１には、電子ペンクライアント１１１、データ振り分けサーバ１２１及びデータ処理サーバ１３１等がそれぞれ独立したハードウェアによって実現される例を示したが、これらが同一のハードウェアによって実現されてもよい。

【００５３】

例えば、データ振り分けサーバ１２１が通信装置１１３と同等のインターフェースを備え、さらに、記憶装置１２４に電子ペンクライアントＰＧ１１６と同等のプログラムが格納されていれば、データ振り分けサーバ１２１は、電子ペンクライアント１１１としても使用することができる。

【００５４】

あるいは、複数のデータ処理サーバの一つ、例えばデータ処理サーバ１３１の記憶装置１３４に、データ振り分けサーバＰＧ１２５、鍵ペア格納部１２６、データ処理サーバ管理テーブル１２７及びページ管理テーブル１２８と同等のものが格納されていれば、データ処理サーバ１３１は、データ振り分けサーバ１２１としても使用することができる。

【００５５】

次に、電子ペンシステムの処理の基本的な流れを説明する。

【００５６】

図７は、本発明の実施形態の電子ペンシステムの処理の全体を示すフローチャートである。

【００５７】

図７に示す処理は、電子ペンシステム導入時に開始される（ステップ３０１）。

【００５８】

データ振り分けサーバ１２１において、図示しない入出力装置を用いて管理者が指示を入力すると、データ振り分けサーバＰＧ１２５が公開鍵暗号の鍵ペアを生成し、生成した鍵ペアを鍵ペア格納部１２６に格納する（ステップ３０２）。

【００５９】

データ処理サーバ１３１においても、図示しない入出力装置を用いて管理者が指示を入力すると、データ処理サーバＰＧ１３５が公開鍵暗号の鍵ペアを生成し、生成した鍵ペアを鍵ペア格納部１３６に格納する。同様に、データ処理サーバ１４１においても、データ処理サーバＰＧ１４５が鍵ペアを生成し、それを鍵ペア格納部１４６に格納する。電子ペンシステムが上記以外のデータ処理サーバ（図示省略）をさらに含む場合、データ処理サーバごとに、そのデータ処理サーバにおける鍵ペア生成処理（ステップ３０２）が実行される。さらに、データ処理サーバが追加されると、その追加されたデータ処理サーバにおいて、鍵ペア生成処理（ステップ３０２）が実行される。

【００６０】

次に、データ処理サーバＰＧ１３５は、鍵ペア格納部１３６に格納されている鍵ペアのうち公開鍵Ｋａｕを、そのデータ処理サーバのデータ処理サーバＩＤとともに、データ振り分けサーバ１２１に登録する（ステップ３０３）。データ処理サーバからデータ振り分

けサーバ１２１への公開鍵の受け渡しは、図示しない入出力装置を用いて、各サーバの管理者によって手動で行われてもよいし、ネットワーク１０３を介して自動で行われてもよい。データ振り分けサーバＰＧ１２５は、データ処理サーバＩＤと公開鍵とのペアを、データ処理サーバ管理テーブル１２７に格納する。

【００６１】

データ処理サーバＰＧ１４５も、ステップ３０３において上記と同様の処理を実行する。

【００６２】

次に、電子ペン活性化処理（図８参照）が実行される（ステップ３０４）。

【００６３】

図８は、本発明の実施形態において実行される電子ペン活性化処理を示すフローチャートである。

【００６４】

電子ペン活性化処理は、電子ペン１０１ごとに、その電子ペン１０１の使用開始時に実行される。あらかじめ、ネットワーク１０３上でデータ振り分けサーバ１２１を一意に識別するアドレスであるデータ振り分けサーバＩＤが、電子ペンクライアント１１１に登録されている。

【００６５】

まず、電子ペンＰＧ２１２が、接続先の電子ペンクライアント１１１に活性化要求を送信する（ステップ４０１）。この送信は、例えば、送信ボックス２１１と同様に、活性化要求ボックス（図示省略）を用意しておき、電子ペン１０１によって活性化要求ボックスに書き込むことによって実行されてもよい。

【００６６】

あるいは、電子ペンＰＧ２１２は、電子ペン１０１の電源が投入されたときに、データ振り分けサーバ１２１の公開鍵が電子ペン１０１に格納されているか否かを判定してもよい。データ振り分けサーバ１２１の公開鍵が格納されていないと判定された場合、電子ペンＰＧ２１２は、活性化が必要である旨を、電子ペン１０１の出力装置（図示省略）を用いてユーザに通知してもよい。

【００６７】

あるいは、電子ペンＰＧ２１２は、後述する筆記データ取得処理が開始されたときに、データ振り分けサーバ１２１の公開鍵が電子ペン１０１に格納されているか否かを判定してもよい。データ振り分けサーバ１２１の公開鍵が格納されていないと判定された場合、電子ペンＰＧ２１２は、活性化が必要である旨を、電子ペン１０１の出力装置を用いてユーザに通知してもよい。

【００６８】

あるいは、筆記データ取得処理が開始される前に電子ペン１０１が電子ペンクライアント１１１に接続された時点で、電子ペンＰＧ２１２又は電子ペンクライアントＰＧ１１６は、データ振り分けサーバ１２１の公開鍵が電子ペン１０１に格納されているか否かを判定してもよい。データ振り分けサーバ１２１の公開鍵が格納されていないと判定された場合、電子ペンＰＧ２１２又は電子ペンクライアントＰＧ１１６は、活性化が必要である旨を、電子ペン１０１の出力装置又は電子ペンクライアント１１１の出力装置（図示省略）を用いてユーザに通知してもよい。

【００６９】

あるいは、上記のようにデータ振り分けサーバ１２１の公開鍵が格納されていないと電子ペンＰＧ２１２又は電子ペンクライアントＰＧ１１６によって判定された場合、電子ペンＰＧ２１２又は電子ペンクライアントＰＧ１１６は、活性化を実行するか否かを、電子ペン１０１の出力装置又は電子ペンクライアント１１１の出力装置を用いてユーザに問い合わせてもよい。

【００７０】

上記の通知又は問い合わせを受けたユーザは、活性化を実行するか否かを判定し、実行

すると判定した場合、活性化を指示するための操作を行う。この操作は、例えば、上記のような電子ペン１０１を用いた活性化要求ボックスへの書き込みであってもよいし、電子ペンクライアント１１１への所定の指示の入力であってもよい。電子ペンクライアント１１１に所定の指示が入力された場合、その指示が、ステップ４０１における活性化要求として扱われてもよい。

【００７１】

電子ペンクライアントＰＧ１１６は、活性化要求を受信する（ステップ４０２）と、登録されているデータ振り分けサーバＩＤに対して活性化要求を送信する（ステップ４０３）。

【００７２】

データ振り分けサーバＰＧ１２５は、活性化要求を受信する（ステップ４０４）と、鍵ペア格納部１２６に格納されている鍵ペアに含まれる公開鍵Ｋｅｕ（すなわち、データ振り分けサーバ１２１が保持する秘密鍵に対応する公開鍵）を電子ペンクライアント１１１に返信する（ステップ４０５）。

【００７３】

電子ペンクライアントＰＧ１１６は、データ振り分けサーバ１２１の公開鍵Ｋｅｕを受信する（ステップ４０６）と、その公開鍵Ｋｅｕを、登録されているデータ振り分けサーバＩＤとともに、接続されている電子ペン１０１に返信する（ステップ４０７）。

【００７４】

電子ペンＰＧ２１２は、データ振り分けサーバ１２１の公開鍵Ｋｅｕ及びデータ振り分けサーバＩＤを受信すると、それらをデータ振り分けサーバ情報格納部２１６に格納する（ステップ４０８）。

【００７５】

電子ペンＰＧ２１２は、その後、筆記データの暗号化に用いる暗号鍵を生成し、生成された暗号鍵を鍵格納部２１５に格納する（ステップ４０９）。ここでは、筆記データの暗号化に公開鍵暗号ではなく共通鍵暗号を用いる。共通鍵暗号を処理するための負荷が、公開鍵暗号を処理するための負荷より小さいためである。したがって、ステップ４０９で生成される暗号鍵は、共通鍵Ｋ１である。

【００７６】

不揮発性であるメモリ２０７に格納された情報（例えば公開鍵Ｋｅｕ及び共通鍵Ｋ１）は、意図的に消去されない限り、電源切断後も保持される。このため、電子ペン１０１において電子ペン活性化処理が一度実行された後に電源が切断され、さらにその後電源が投入された場合、その電子ペン１０１について、ステップ４０１～ステップ４０８を再び実行する必要はない。このため、例えば、電子ペン１０１は、電源が投入された後、公開鍵Ｋｅｕを保持しているか否かを判定し、保持していない場合にステップ４０１～ステップ４０８を実行してもよい。

【００７７】

しかし、後述するように、データの安全を確保するため、鍵格納部２１５に格納された共通鍵は、電子ペン１０１の電源が切断されるときに消去される。このため、電子ペンＰＧ２１２は、電源が投入されたとき、ステップ４０９を実行して新たな共通鍵を生成する必要がある。

【００７８】

再び図７を参照して、ステップ３０４の実行が終了した後の処理を説明する。

【００７９】

ステップ３０４の実行が終了した後、筆記データ取得処理（ステップ３０５）が実行される。筆記データ取得処理は、電子ペン１０１が筆記に使用されるたびに実行される。さらに、本実施形態の電子ペンシステムが複数の電子ペン１０１を備える場合、筆記データ取得処理は、電子ペン１０１ごとに実行される。

【００８０】

ステップ３０５において、電子ペンＰＧ２１２は、前述の方法で筆記データを時系列に

取得する。取得した筆記データおよびその筆記データに対応するＰａｇｅＩＤは、筆記データ管理テーブル２１３に格納される。取得した筆記データのＰａｇｅＩＤが変わると、その後に取得された筆記データは、次のレコードとして筆記データ管理テーブル２１３に格納される。すなわち、筆記データ管理テーブル２１３の１つのレコードには、１つのページ分の筆記データが格納される。

【００８１】

次に、電子ペンＰＧ２１２は、所定のイベントを検出したか否かを判定する（ステップ３０８）。ここで、所定のイベントとは、筆記データの暗号化を開始する契機となるべきイベントであり、例えば、暗号化を開始する必要が生じたこと（又は、必要性が高まったこと）を示すイベントであってもよいし、暗号化の実行が可能になったこと（又は、容易になったこと）を示すイベントであってもよい。暗号化の実行が可能（又は容易）になったこととは、例えば、筆記データ取得処理に影響を与えない筆記データ暗号化処理が可能になったことを意味する。

【００８２】

例えば、最後に筆記データが取得されてから所定の時間が経過した場合（言い換えると、筆記データが所定の時間取得されなかった場合）、電子ペン１０１のユーザが筆記を中断していると考えられる。プロセッサ２０６の処理能力が高くない場合であっても、筆記が中断している間は、筆記データ取得処理に影響を与えることなく筆記データの暗号化を実行することができる。すなわち、ユーザによる筆記の中断は、暗号化の実行が可能（又は容易）になったことを示すといえる。このため、上記の所定のイベントは、例えば、最後に筆記データが取得されてから所定の時間が経過したことであってもよい。

【００８３】

電子ペン１０１に電源切断要求が入力された場合も、上記と同様の理由によって、暗号化の実行が可能（又は容易）になったということができる。

【００８４】

さらに、電子ペン１０１の電源の切断は、ユーザが電子ペン１０１から離れる可能性をも示している。このような場合、電子ペン１０１が暗号化されていない筆記データを保持していると、第三者がその筆記データを読み出す可能性がある。これを防ぐためには、速やかに筆記データを暗号化する必要がある。すなわち、電源切断要求の入力は、暗号化の必要が生じた（又は必要性が高まった）ことを示すともいえる。

【００８５】

このため、上記の所定のイベントは、電子ペン１０１に電源切断要求が入力されたこと（すなわち、例えば電子ペン１０１のキャップが取り付けられたこと）であってもよい。

【００８６】

さらに、上記以外のイベントがステップ３０８において検出されてもよい。例えば、暗号化を実行する必要が生じたことを示すイベントとして、バッテリ２０９の残量が所定の閾値以下となったこと、及び、メモリの空き容量が所定の閾値以下となったことが挙げられる。

【００８７】

ステップ３０８において所定のイベントを検出したと判定された場合、筆記データを暗号化するタイミングが到来したため、電子ペンＰＧ２１２は、筆記データ暗号化処理（図９参照）を実行する（ステップ３０６）。

【００８８】

一方、ステップ３０８において所定のイベントを検出していないと判定された場合、電子ペンＰＧ２１２は、まだ筆記データ暗号化処理を実行せずに、所定のイベントの検出を待つ。所定のイベントが検出されるまでの間に電子ペン１０１が筆記に使用された場合、ステップ３０５が実行される。

【００８９】

図９は、本発明の実施形態において実行される筆記データ暗号化処理を示すフローチャートである。

【００９０】
電子ペン１０１の第一義は、筆記データを精度よく取得して蓄積することである。これを阻害する暗号方法は認められない。本実施形態では、電子ペン１０１の処理能力が乏しいため、筆記データ取得と暗号化は並列に処理できないことを前提とする。
【００９１】
電子ペン１０１は、筆記データを取得していないとき、すなわち、ステップ３０５の処理が行われていないときに、筆記データ管理テーブル２１３に格納されている筆記データを暗号化する（ステップ３０６）。例えば、ステップ３０８における所定のイベントが、最後に筆記データが取得されてから所定の時間が経過したこと、又は、電子ペン１０１に電源切断要求が入力されたこと、である場合、ステップ３０５の処理が行われていないときに筆記データの暗号化が実行される。
【００９２】
筆記データ管理テーブル２１３に筆記データが存在する間は、ステップ３０６が繰り返される。ステップ３０６の処理の途中で、電子ペン１０１が筆記に使用された場合、電子ペンＰＧ２１２は、ステップ３０６の処理を中断し、ステップ３０５の処理を実行する。
【００９３】
筆記データの暗号化に用いる共通鍵は、ある規則にしたがって変更される。電子ペン１０１が一つの共通鍵を長期に保持することは、セキュリティレベルを低下させる。ある一つの共通鍵で暗号化される対象データをユニットと呼ぶ。ユニットは、細か過ぎると処理効率が悪い。例えば、ストローク（すなわち一筆書き単位の筆記データ）ごと、又は、サンプル点（一点の座標データ）ごとのユニットでは、効率が悪い。一方、一つのユニットを、複数のデータ処理サーバが利用する場合、複数のデータ処理サーバに同じ共通鍵及びデータが保持されることになり、その結果セキュリティレベルが低下する。
【００９４】
これに対して、例えば、ユニットがページ単位であれば、効率がよく、かつ安全である。本実施形態では、筆記データ管理テーブル２１３の一つのレコードを一つのユニットとして扱う。その結果、一つのページから取得された筆記データ（すなわち、あるページへの筆記が開始されてから、その他のページへの筆記が開始されるまでの間に取得された筆記データ）が一つのユニットとして扱われる。
【００９５】
ただし、筆記データの安全を確保するためには、取得された筆記データを可能な限り早く暗号化することが望ましい。このため、最後に筆記データが取得されてから所定の時間が経過した場合、その時点で筆記データ管理テーブル２１３に格納されているすべてのデータ（すなわち、すべてのレコードに含まれるデータ）が暗号化されてもよい。このような処理は、ステップ３０８の所定のイベントが、最後に筆記データが取得されてから所定の時間が経過したこと、である場合に実現される。その場合、その暗号化が実行された後に取得された筆記データは、ＰａｇｅＩＤにかかわらず、その実行の前に取得された筆記データと異なるユニットとして扱われる。
【００９６】
以下、筆記データ暗号化処理をステップごとに説明する。この処理はすべて電子ペンＰＧ２１２によって実行される。
【００９７】
まず、電子ペンＰＧ２１２は、筆記データ管理テーブル２１３に格納されている最も古いレコードからユニット及びＰａｇｅＩＤを読み出し、それぞれを鍵格納部２１５に格納されている共通鍵を用いて暗号化する（ステップ５０１）。ここでは、筆記データ管理テーブル２１３に格納されている最も古いレコードのユニットをＵｎｉｔ１、鍵格納部２１５に格納されている共通鍵をＫ１と表記し、共通鍵Ｋ１によって暗号化されたＵｎｉｔ１をＫ１（Ｕｎｉｔ１）、共通鍵Ｋ１によって暗号化されたＰａｇｅＩＤをＫ１（ＰａｇｅＩＤ）と表記する。
【００９８】

次に、電子ペンＰＧ２１２は、ステップ５０１で暗号化に用いた共通鍵を、データ振り分けサーバ１２１の公開鍵Ｋｅｕを用いて暗号化し、暗号化された共通鍵を、ステップ５０１で暗号化した結果とともに、暗号筆記データ管理テーブル２１４に格納する（ステップ５０２）。ここでは、ステップ５０１で暗号化に用いた共通鍵がＫ１であるので、公開鍵Ｋｅｕを用いて暗号化された結果のデータはＫｅｕ（Ｋ１）と表記される。

【００９９】

その後、電子ペンＰＧ２１２は、ステップ５０１で暗号化されたレコード（上記の例ではＵｎｉｔ１を含むレコード）を筆記データ管理テーブル２１３から、暗号化に用いた共通鍵（上記の例ではＫ１）を鍵格納部２１５から、それぞれ消去する（ステップ５０３）。

【０１００】

最後に、電子ペンＰＧ２１２は、新たな筆記データの暗号化に用いる共通鍵を生成し、それを鍵格納部２１５に格納する（ステップ５０４）。ここでは、共通鍵Ｋ２が生成される。

【０１０１】

電子ペン１０１の電源を切断する要求を受けた場合、電子ペンＰＧ２１２は、すべてのデータの暗号化が終わってから、すなわち、筆記データ管理テーブル２１３に格納されているレコードがなくなるまで上記の筆記データ暗号化処理を実行してから、電源を切断する。さらに、電子ペンＰＧ２１２は、メモリ２０７の容量限界に達する前及びバッテリ２０９の残量がなくなる前に、暗号化を終了させることが望ましい。

【０１０２】

なお、使用者が電子ペン１０１の電源を切断した後も、その電子ペン１０１が共通鍵を保持し続けることは、セキュリティレベルを著しく低下させる。例えば、使用者が電源を切断した電子ペン１０１を机上に放置して離席した場合、第三者（すなわちその電子ペン１０１が取得した筆記データを閲覧すべきでない者）が電子ペン１０１から共通鍵を読み出す可能性がある。その後使用者が電子ペン１０１を用いて筆記データを取得し、それを暗号化しても、共通鍵を取得した第三者は、暗号化された筆記データを容易に復号化することができる。

【０１０３】

このようなセキュリティレベルの低下を防ぐために、電源が切断された電子ペン１０１は共通鍵を保持しないことが望ましい。例えば、ステップ３０８において電源切断要求が入力されたために図９の筆記データ暗号化処理が実行される場合、ステップ５０４の実行が省略される。その結果、電源が切断された電子ペン１０１は、共通鍵を保持しない。これによって、第三者によるデータの盗聴を防ぐことができる。

【０１０４】

電子ペンＰＧ２１２は、ステップ４０９又はステップ５０４において複数の共通鍵（すなわち、次回以降の筆記データ暗号化処理において使用されるべき共通鍵）を作成してもよい。この場合、鍵格納部２１５には複数の共通鍵が格納される。この場合において電子ペン１０１の電源が切断される場合、上記のようにデータの安全を確保するために、電子ペンＰＧ２１２は、ステップ５０３において鍵格納部２１５に格納されているすべての共通鍵を消去する。

【０１０５】

上記の筆記データ暗号化処理は、ユーザによって暗号化を明示的に指示された場合に実行されてもよい。具体的には、例えば、送信ボックス２１１の場合と同様に、電子ペン１０１が所定のドットパターンを読み込んだときに、その対象ページ、又は、電子ペン１０１が保持する全筆記データを対象として、筆記データ暗号化処理が実行されてもよい。

【０１０６】

再び図７を参照して、ステップ３０６の実行が終了した後の処理を説明する。

【０１０７】

ステップ３０６の実行が終了すると、筆記データ転送処理が実行される（ステップ３０

７）。
【０１０８】
図１０は、本発明の実施形態において実行される筆記データ転送処理を示すフローチャートである。
【０１０９】
筆記データ転送処理は、電子ペン１０１ごとに実行される。
【０１１０】
まず、電子ペンＰＧ２１２が、暗号筆記データ管理テーブル２１４に格納されているすべての暗号筆記データを、データ振り分けサーバ情報格納部２１６に格納されているデータ振り分けサーバＩＤとともに、接続先の電子ペンクライアント１１１に送信し、その後、暗号筆記データ管理テーブル２１４に格納されているすべての暗号筆記データを消去する（ステップ６０１）。ここで、暗号筆記データはＫ１（Ｕｎｉｔ１）、Ｋ１（ＰａｇｅＩＤ）及びＫｅｕ（Ｋ１）であり、これらが送信され、その後消去される。以下、上記の暗号筆記データが送信された場合を例として説明する。
【０１１１】
この送信は、例えば、電子ペン１０１による送信ボックス２１１への書き込みを契機として実行される。なお、この送信のタイミングで、電子ペンＰＧ２１２は、筆記データ管理テーブル２１３における筆記データの存在を確認し、筆記データが存在する場合はステップ３０６の処理を実行することによって、暗号化されていない筆記データをなくしてから（すなわち格納されているすべての筆記データを暗号化してから）ステップ６０１の処理を実行する。
【０１１２】
電子ペンクライアントＰＧ１１６は、暗号筆記データ及びデータ振り分けサーバＩＤを受信する（ステップ６０２）と、暗号筆記データのうち、暗号化されたＰａｇｅＩＤ（すなわちＫ１（ＰａｇｅＩＤ））、及び、その暗号化に用いた共通鍵Ｋ１をデータ振り分けサーバ１２１の公開鍵Ｋｅｕで暗号化した結果（すなわちＫｅｕ（Ｋ１））を、受信したデータ振り分けサーバＩＤによって識別されるデータ振り分けサーバ１２１に送信する（ステップ６０３）。
【０１１３】
データ振り分けサーバＰＧ１２５は、ステップ６０３で送信された、暗号化されたＰａｇｅＩＤ（Ｋ１（ＰａｇｅＩＤ））、及び、Ｋｅｕによって暗号化された共通鍵（Ｋｅｕ（Ｋ１））を受信する（ステップ６０４）と、その暗号化された共通鍵（Ｋｅｕ（Ｋ１））を、鍵ペア格納部１２６に格納されている鍵ペアにおける秘密鍵Ｋｅｒで復号化することによって、共通鍵Ｋ１を得る（ステップ６０５）。
【０１１４】
次に、データ振り分けサーバＰＧ１２５は、ステップ６０４で受信した、暗号化されたＰａｇｅＩＤ（Ｋ１（ＰａｇｅＩＤ））を、ステップ６０５で得た共通鍵Ｋ１で復号化することによって、ＰａｇｅＩＤを得る（ステップ６０６）。
【０１１５】
さらに、データ振り分けサーバＰＧ１２５は、ステップ６０５で得た共通鍵Ｋ１を、ステップ６０６で得たＰａｇｅＩＤに対応するデータ処理サーバの公開鍵Ｋａｕで暗号化する（ステップ６０７）。ステップ６０６で得たＰａｇｅＩＤに対応するデータ処理サーバとは、これから送信しようとする筆記データを処理すべきデータ処理サーバ、すなわち、これから送信しようとする筆記データの送信先となるべきデータ処理サーバである。
【０１１６】
ＰａｇｅＩＤに対応するデータ処理サーバの公開鍵Ｋａｕは、ＰａｇｅＩＤをキーとしてページ管理テーブル１２８を検索することによって、対応するデータ処理サーバＩＤを取得し、そのデータ処理サーバＩＤをキーとしてデータ処理サーバ管理テーブル１２７を検索することによって得られる。
【０１１７】

以下、ステップ６０６で得たＰａｇｅＩＤにデータ処理サーバ１３１が対応する場合を例として説明する。

【０１１８】

データ振り分けサーバＰＧ１２５は、ステップ６０５で得た共通鍵をデータ振り分けサーバ１２１から消去（ステップ６０８）する。

【０１１９】

次に、データ振り分けサーバＰＧ１２５は、ステップ６０６で得たＰａｇｅＩＤをキーとしてページ管理テーブル１２８を検索することによって得られるデータ処理サーバＩＤ（この例では、データ処理サーバ１３１を識別する情報）と、ステップ６０７において公開鍵Ｋａｕによって暗号化された共通鍵（Ｋａｕ（Ｋ１））と、を電子ペンクライアント１１１に返信する（ステップ６０９）。

【０１２０】

電子ペンクライアントＰＧ１１６は、データ処理サーバＩＤと、暗号化された共通鍵（Ｋａｕ（Ｋ１））と、を受信する（ステップ６１０）。

【０１２１】

次に、電子ペンクライアントＰＧ１１６は、ステップ６１０において受信した、公開鍵Ｋａｕによって暗号化された共通鍵（Ｋａｕ（Ｋ１））と、ステップ６０２で受信した暗号筆記データのうち暗号化されたユニット及びＰａｇｅＩＤを、受信したデータ処理サーバＩＤによって識別されるデータ処理サーバ１３１に送信する（ステップ６１１）。

【０１２２】

データ処理サーバＰＧ１３５は、ステップ６１１において送信された、暗号化された共通鍵（Ｋａｕ（Ｋ１））、共通鍵によって暗号化されたユニット（Ｋ１（Ｕｎｉｔ１））及びＰａｇｅＩＤ（Ｋ１（ＰａｇｅＩＤ））を受信する（ステップ６１２）。

【０１２３】

次に、データ処理サーバＰＧ１３５は、暗号化された共通鍵（Ｋａｕ（Ｋ１））を、鍵ペア格納部１３６に格納されている鍵ペアにおける秘密鍵Ｋａｒで復号化することによって、共通鍵Ｋ１を得る（ステップ６１３）。

【０１２４】

次に、データ処理サーバＰＧ１３５は、ステップ６１２で受信した、暗号化されたユニット（Ｋ１（Ｕｎｉｔ１））及びＰａｇｅＩＤ（Ｋ１（ＰａｇｅＩＤ））を、ステップ６１３で得た共通鍵Ｋ１で復号化することによって、ＰａｇｅＩＤと、そのＰａｇｅＩＤに対応するユニットとを得る（ステップ６１４）。

【０１２５】

次に、データ処理サーバＰＧ１３５は、ステップ６１３で得た共通鍵Ｋ１をデータ処理サーバ１３１から消去し（ステップ６１５）、ステップ３０７を終了する。なお、ステップ６０２で受信した暗号筆記データが複数存在する場合、それぞれの暗号筆記データについて、ステップ６０３からステップ６１５が繰り返される。

【０１２６】

上記の処理によれば、少なくともＰａｇｅＩＤ以外の筆記データは、電子ペン１０１において共通鍵を用いて暗号化された後、その筆記データを処理するデータ処理サーバに到達するまで、一度も復号化されることがない。これによって、電子ペン１０１のような、常にネットワーク１０３に接続されているわけではないデータ作成装置におけるデータの暗号化と、ネットワーク１０３におけるデータの暗号化とが一貫して処理される。

【０１２７】

なお、ＰａｇｅＩＤとデータ処理サーバ１４１のデータ処理サーバＩＤとが対応する場合、ステップ６０９において、データ処理サーバ１４１のデータ処理サーバＩＤが送信される。その場合、ステップ６１１においてユニット等はデータ処理サーバ１４１に送信され、データ処理サーバＰＧ１４５においてステップ６１２～ステップ６１５に相当する処理が実行される。

【０１２８】

使用する公開鍵暗号及び共通鍵暗号の具体的なアルゴリズム及び鍵長は、計算機の処理能力及び記憶装置の容量のほか、安全性及び高速性を考慮して決めればよい。例えば、ＲＳＡ、ＡＥＳ又はＭＵＬＴＩ－Ｓ０１等が用いられてもよい。

【０１２９】

筆記データの暗号化に用いる共通鍵を電子ペン１０１で生成する理由は、電子ペン１０１が他の構成要素と常に通信できるわけではないからである。

【０１３０】

アルゴリズム及び鍵長によって異なるが、共通鍵生成も電子ペン１０１に負荷を与える。電子ペンＰＧ２１２は、電子ペン１０１の負荷が軽いときに、次の暗号化処理に使用する共通鍵を１つ生成する。具体的には、電子ペンＰＧ２１２は、電子ペン活性化直後、及び、前のユニットを暗号化した後に、共通鍵を１つ生成する。

【０１３１】

なお、電子ペンＰＧ２１２は、複数個の共通鍵を生成できるときに生成しておいてもよいが、生成された複数の共通鍵を格納するためのメモリ領域は必要となる。共通鍵生成処理の途中で、ステップ３０５の処理が発生した場合、電子ペンＰＧ２１２は、共通鍵生成処理を中断し、ステップ３０５の処理を行う。また、共通鍵生成処理の途中で、ステップ３０６の処理が発生した場合、電子ペンＰＧ２１２は、共通鍵生成処理を中断し、ステップ３０６の処理を行う。ただし、鍵格納部２１５に共通鍵がない場合（すなわち、これから使用されるべき共通鍵がまだ生成されていない場合）、電子ペンＰＧ２１２は、ステップ３０６の処理を行うための共通鍵を生成する。

【０１３２】

上記の本発明の実施形態は、電子ペン１０１が取得した筆記データを処理する情報システムを例示しているが、電子ペン１０１が他のデータ作成装置（例えばデジタルカメラ）によって置き換えられてよい。その場合、データ作成装置の処理能力が十分でなくても、データ取得処理を妨げずにデータ暗号化を実行することができる。これによって、データ取得処理の性能を維持しながら、セキュリティレベルを改善することができる。

【図面の簡単な説明】

【０１３３】

【図１】本発明の実施形態の全体システム構成を示すブロック図である。

【図２】本発明の実施形態の電子ペンの構成及び機能を説明するための図である。

【図３】本発明の実施形態の筆記データ管理テーブルの構成を説明する図である。

【図４】本発明の実施形態の暗号筆記データ管理テーブルの構成を説明する図である。

【図５】本発明の実施形態のデータ処理サーバ管理テーブルの構成を説明する図である。

【図６】本発明の実施形態のページ管理テーブルの構成を説明する図である。

【図７】本発明の実施形態の電子ペンシステムの処理の全体を示すフローチャートである。

【図８】本発明の実施形態において実行される電子ペン活性化処理を示すフローチャートである。

【図９】本発明の実施形態において実行される筆記データ暗号化処理を示すフローチャートである。

【図１０】本発明の実施形態において実行される筆記データ転送処理を示すフローチャートである。

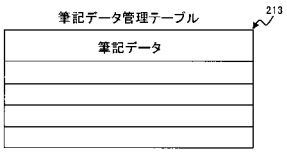
【符号の説明】

【０１３４】

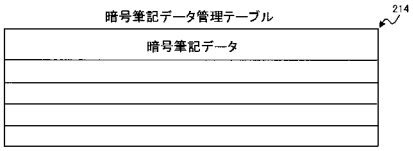
１０１　電子ペン
１０２　電子ペン対応帳票
２０１　ドットパターン
２０２　発光ダイオード
２０３　カメラ
２０４　インクカートリッジ

２０５　筆圧センサ
２０６　プロセッサ
２０７　メモリ
２０８　時計
２０９　バッテリ
２１０　通信装置
２１１　送信ボックス
２１２　電子ペンＰＧ
２１３　筆記データ管理テーブル
２１４　暗号筆記データ管理テーブル
２１５　鍵格納部
２１６　データ振り分けサーバ情報格納部

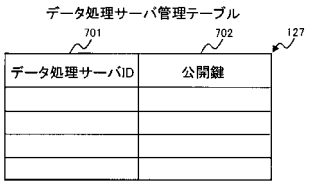
【図３】



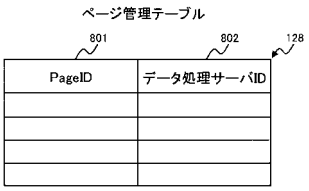
【図４】



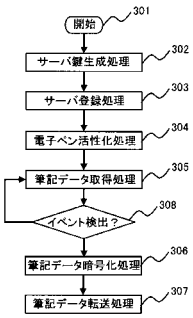
【図５】



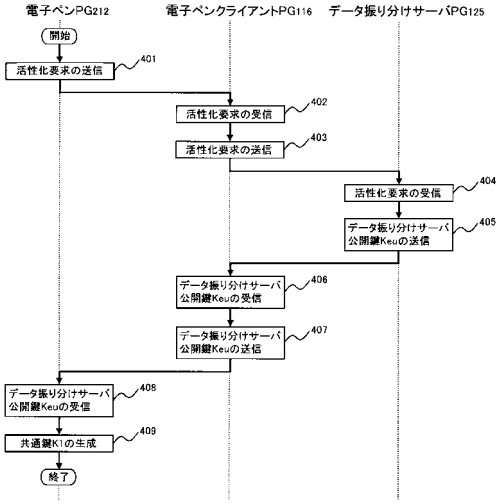
【図６】



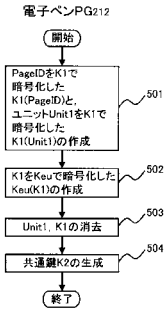
【図７】


開始
301
サーバ鍵生成処理
302
サーバ登録処理
303
電子ペン活性化処理
304
筆記データ取得処理
305
イベント検出？
308
筆記データ暗号化処理
306
筆記データ転送処理
307

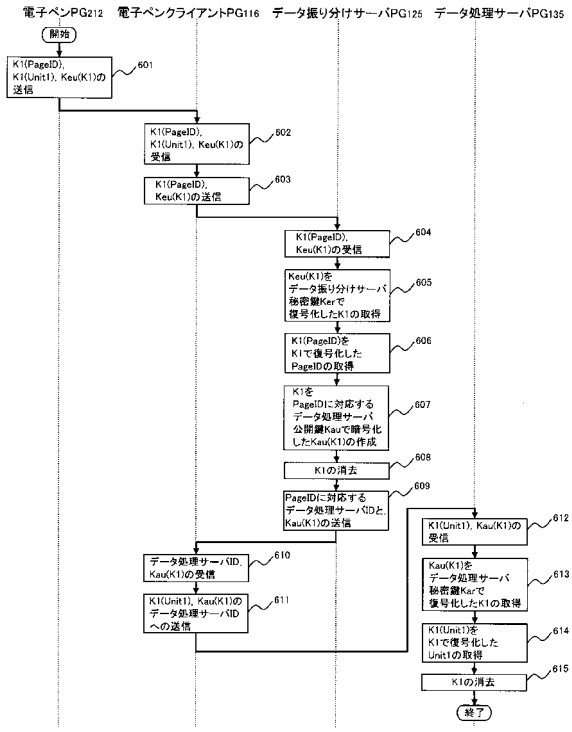
【図８】


電子ペンPG212
電子ペンクライアントPG116
データ振り分けサーバPG125
開始
活性化要求の送信
401
活性化要求の受信
402
活性化要求の送信
403
活性化要求の受信
404
データ振り分けサーバ
公開鍵Keuの送信
405
データ振り分けサーバ
公開鍵Keuの受信
406
データ振り分けサーバ
公開鍵Keuの送信
407
データ振り分けサーバ
公開鍵Keuの受信
408
共通鍵K1の生成
409
終了

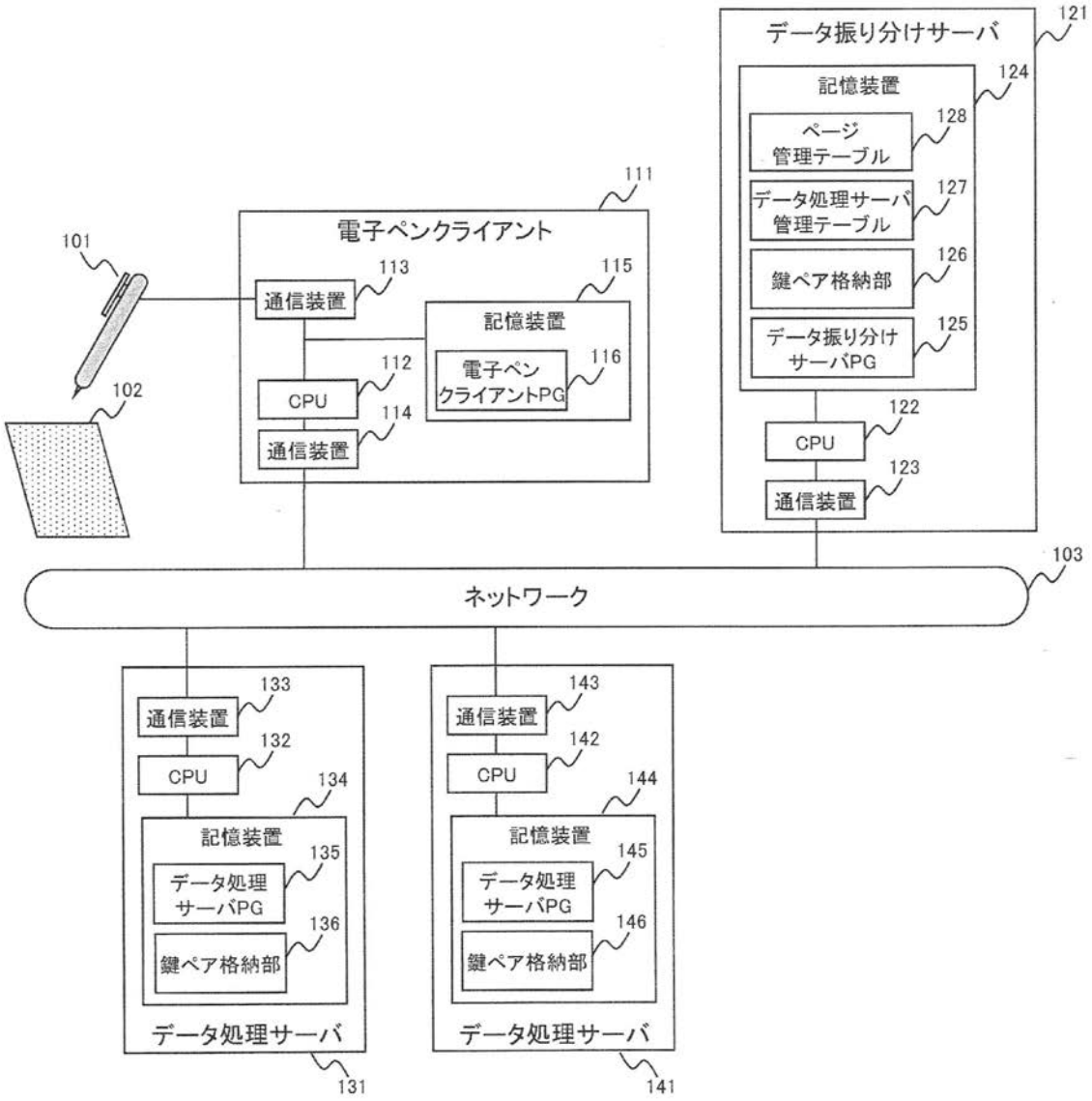
【図９】


電子ペンPG212
開始
PageIDをK1で
暗号化した
K1(PageID)と，
ユニットUnit1をK1で
暗号化した
K1(Unit1)の作成
501
K1をKeuで暗号化した
Keu(K1)の作成
502
Unit1，K1の消去
503
共通鍵K2の生成
504
終了

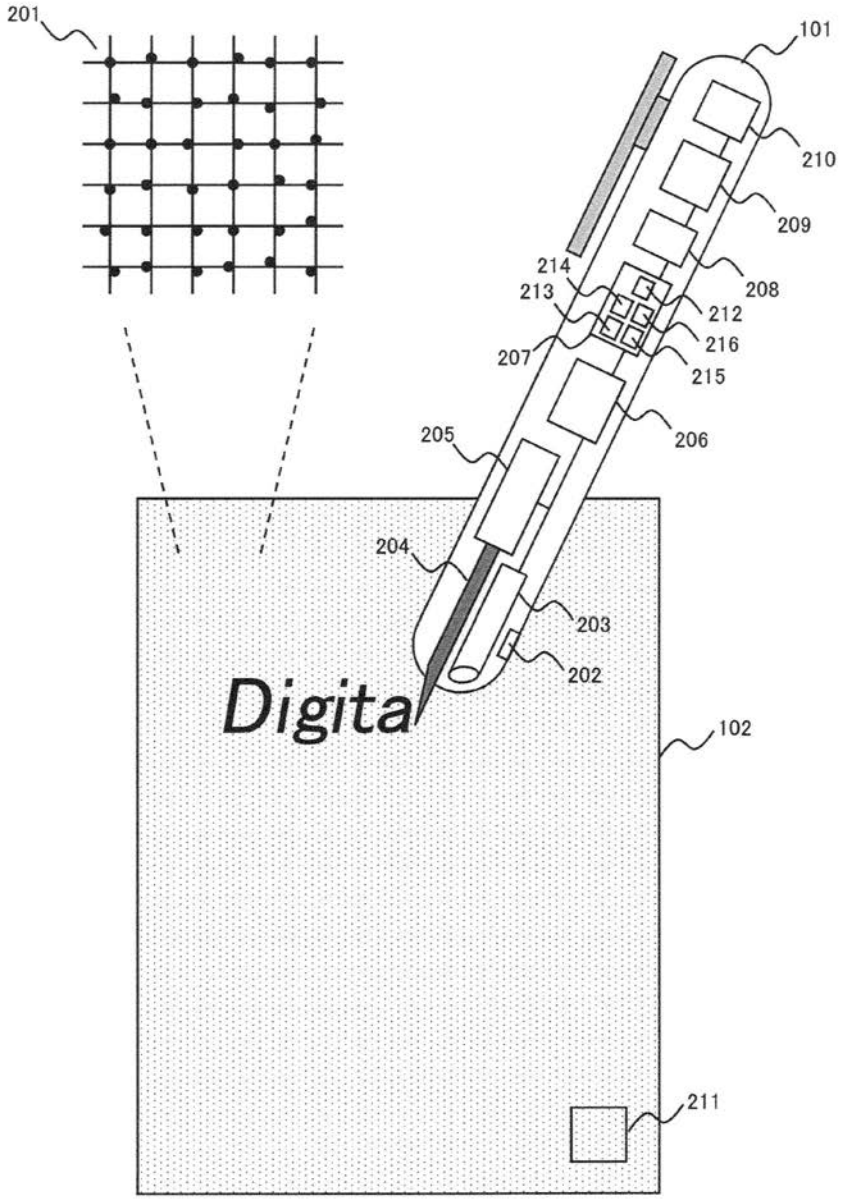
【図１０】


電子ペンPG212
電子ペンクライアントPG116
データ振り分けサーバPG125
データ処理サーバPG135
開始
K1(PageID)，
K1(Unit1)，Keu(K1)の
送信
601
K1(PageID)，
K1(Unit1)，Keu(K1)の
受信
602
K1(PageID)，
Keu(K1)の送信
603
K1(PageID)，
Keu(K1)の受信
604
Keu(K1)を
データ振り分けサーバ
秘密鍵Kerで
復号化したK1の取得
605
K1(PageID)を
K1で復号化した
PageIDの取得
606
K1を
PageIDに対応する
データ処理サーバ
公開鍵Kauで暗号化
したKau(K1)の作成
607
K1の消去
608
PageIDに対応する
データ処理サーバID，
Kau(K1)の送信
609
データ処理サーバID，
Kau(K1)の受信
610
K1(Unit1)，Kau(K1)の
データ処理サーバID
への送信
611
K1(Unit1)，Kau(K1)の
受信
612
Kau(K1)を
データ処理サーバ
秘密鍵Karで
復号化したK1の取得
613
K1(Unit1)を
K1で復号化した
Unit1の取得
614
K1の消去
615
終了

【図１】


データ振り分けサーバ
121
記憶装置
124
ページ
管理テーブル
128
データ処理サーバ
管理テーブル
127
鍵ペア格納部
126
データ振り分け
サーバPG
125
CPU
122
通信装置
123
111
電子ペンクライアント
101
113
通信装置
115
記憶装置
112
CPU
116
電子ペン
クライアントPG
102
114
通信装置
103
ネットワーク
133
通信装置
132
CPU
134
記憶装置
135
データ処理
サーバPG
136
鍵ペア格納部
データ処理サーバ
131
143
通信装置
142
CPU
144
記憶装置
145
データ処理
サーバPG
146
鍵ペア格納部
データ処理サーバ
141

【図２】


201
101
210
209
214
213
208
212
216
207
215
205
206
204
203
202
Digita
102
211

フロントページの続き

(72)発明者　林　工
東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内

審査官　田中　純一

(56)参考文献　特開平０５－０９４４５８（ＪＰ，Ａ）
特開２００６－２１２０４３（ＪＰ，Ａ）
特開平１１－２０２７６５（ＪＰ，Ａ）
特開２００２－３５１３１７（ＪＰ，Ａ）
特開２００７－０２５７６３（ＪＰ，Ａ）
特開２００４－１１８７９５（ＪＰ，Ａ）
特開２００６－１２７３９６（ＪＰ，Ａ）
特開２００５－２１０２２０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　３／０３３　－　３／０４１
Ｇ０９Ｃ　１／００　－　５／００
Ｈ０４Ｋ　１／００　－　３／００
Ｈ０４Ｌ　９／００　－　９／３８