様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２４ 日現在

機関番号：１５４０１
研究種目：基盤研究(B)
研究期間：2012～2014
課題番号：２４３０００２５

研究課題名（和文）自己都合による廃止権を持つ組織間連携分散ファイル管理システムの研究開発

研究課題名（英文）Research and development of inter-organizational distributed file management system with the abolition rights by self convenience

研究代表者
西村　浩二（Nishimura, Kouji）

広島大学・情報メディア教育研究センター・教授

研究者番号：９０２６３６７３

交付決定額（研究期間全体）：（直接経費）　　13,900,000円

研究成果の概要（和文）：本研究では、組織が保有する重要な情報を秘密分散により冗長・分散化し、同様なセキュリティポリシーを持つ組織が連携して互いに重要情報を持ち合うシステムを開発した。
その際、組織の都合により連携を脱退する場合でも、冗長度や分散度を損なうことなく対応可能な管理手法を提案した。またシステムのクラウド対応として、秘密分散処理をクラウド上で安全に行うための処理委託方式を提案し、その性能評価によって有効性を確認した。

研究成果の概要（英文）：In this study, we developed the prototype system to store important information of organizations. This system is operated in the organizations which have similar security policy and federated each other by some contract. This system divides the information into several shares which are redundant and distributable form by using Secret Sharing Scheme and stores these shares among the federated systems.
We proposed the management techniques not to compromise redundancy and dispersity, even if some organization wants to leave from the federation by the convenience. We also proposed and evaluated the secure outsourcing scheme of Secret Sharing Scheme for cloud storage services and confirmed the effectiveness of our proposal.

研究分野：情報工学

キーワード：秘密分散法　分散ファイル管理システム　シングルサインオン　認証フェデレーション　ストリーム暗号　処理委託

１．研究開始当初の背景

(1) 教育研究活動および経済活動における電子情報の重要性が増すにつれて、災害やシステム障害等でそれが失われた場合の影響は深刻である。重要な電子情報のバックアップを保持することの必要性は、ほとんどの組織で認識されており、バックアップの作成は通常の業務の一環として広く行われている。しかし、組織の持つほとんどの機能が同時に大きな損害を受けるような大規模災害では、組織内で作成・保持されているバックアップ情報自体も同時に危険にさらされる可能性がある。

(2) 東日本大震災によって、事業継続計画（BCP：Business Continuity Plan）の早期策定、あるいは見直しの必要性があらためて認識されたが、地理的に離れた地点に電子情報のバックアップを保持することには、設備投資や人員確保に伴う財政的な負担の増加など、組織運営上の障壁が大きい。一方、クラウドを利用するバックアップソリューションの利用は、以下のように、組織の規則などによるもののほか、外部の組織に重要情報を預託することに対する心理的な抵抗感など、解決しなければならない問題が山積している。

- セキュリティポリシーに違反しないこと（組織外への重要情報の持ち出し禁止）
- 自組織以外の者に見られないこと（情報漏洩防止）
- データがどこにあるかわかること（情報システム監査対応）
- データを完全に消去できること（情報システム監査対応）

(3) これらを解決する技術として、暗号化や秘密分散法などがあるが、コンシューマ向けのサービスではこれらを効果的に組み合わせたソリューションはまだ存在しない。また外部の組織に重要情報を預託する心理的抵抗感を払拭するには、これまでと異なるアプローチが必要である。

(4) この問題に対し、同じセキュリティポリシーや目的を持つ組織同士が、相互にかつ安全に重要情報を保持し合う枠組みを構築することで、大規模な災害やシステム障害に備えようとする取り組みが始まっている。しかし、他組織の情報を預かることへの抵抗感から、これらの取り組みが機能するには、上記に加えて次の条件を満たす必要がある。

- 組織の都合でサービス停止や連携からの脱退（Graceful Shutdown）ができること

２．研究の目的

(1) 本研究はクラウド技術の応用による組織間連携分散ファイル管理システムの構築だけでなく、システムを構成する参加組織が後に廃止の選択ができるよう、それぞれの権利を留保した状態で協調的に動作するシステムの構築を目指す。

(2) 研究期間の前半において、参加組織の都合によって途中廃止が可能な組織間連携型の分散ファイル管理システムを構築する。これにより、大学等のセキュリティポリシーや目的が同様な組織間での運用が可能となる。大学では、重要情報のバックアップ、事業継続計画の策定が急務となっており、その受け皿としての利用を検討する。

(3) 研究期間の後半は、本研究で構築するシステムをビジネスモデルとして社会に還元する方法を検討する。大学のように認証とストレージの両方を自前で用意するもの、ストレージのみを提供するインフラ事業者、利用者情報のみで仮想ストレージサービスを展開する二次事業者など、さまざまなサービス形態が考えられ、拡大を続けるクラウド事業のサービスモデルのひとつとなることを目指す。

３．研究の方法

(1) 本研究では、利用者が所有するファイルを地理的に分散した複数の組織に設置されたファイルサーバ上に分散して保管するファイル管理システムを構築する。その際、これまでに発表されている暗号化技術や秘密分散技術等を調査検討し、要求仕様の明確化と実装を行う。実装にあたっては、本研究課題の独創的な点である、組織の都合によるシステムの停止や廃止を、システム全体の冗長性や地理的分散度を損なうことなく可能とするため、分散ファイルの管理方法に独自の工夫を施す。具体的には保管ファイルの再預託を行うが、地理的分散度を損なわないよう預託先に地理的条件を付したり、その条件が満たせない場合は再度分散させることで冗長度を維持したりすることで、一部のシステムの停止や廃止が全体に及ぼす影響を最小限に抑える管理手法を開発する。

(2) 平成 24 年度は、プロトタイプシステムを構築する上で必要となる以下について研究を行う。

① フェデレーションおよび分散ハッシュテーブルを構成するファイルサーバ群の構築

シングルサインオンのためのフェデレーションには、国立情報学研究所が運用を行っている「学認」を利用する。これにより容易にフェデレーションを構築できるほか、プロトタイプシステム構築後の動作検証においても、学認参加組織の協力を得ることが可能となる。また分

散ハッシュテーブルについては、ファイルサーバ群の規模拡張性を考慮して、コンシステントハッシング（Consistent Hashing）による分散をサポートするTokyoTyrantやRedisなどの利用、また地理空間インデックスにより地理情報を効率的に扱うことのできるMongoDBなどの利用を検討する。

② 暗号化および分散冗長化に使用するアルゴリズムの検討

暗号化については、利用者属性に基づく暗号化（属性ベース暗号）やシングルサインオンにより取得される利用者属性に基づくグループアクセス制御（mAP）など、ひとつのファイルを複数の利用者で共有する方式を検討する。また分散冗長化については、秘密分散法のほか、パリティ方式などファイルの重要度に応じて複数の分散方式から選択できるようにする。また分割ファイルが損傷あるいは消失した場合に、復元するには不十分な情報から分割ファイルを復元する方法についても検討を行う。

③ ファイルリストおよび検索テーブルへのアクセス制限に関する検討

本研究ではファイルへの管理リストへのアクセスを利用者のビュー、分割ファイルへの管理リストへのアクセスをファイルサーバ管理者のビューと呼び、それらへのアクセスを制御することでファイルサーバ管理者が元のファイルを復元する権限を持たないこと、保管する分割ファイルの再配置を可能にすることの相反する要求を満たす。

④ ファイルサーバが停止あるいは廃止する場合の対策の検討

ひとつのファイルを複数のファイルサーバで分割して保持する場合、運用途中に停止や廃止を行うことは一般に困難であり、組織が連携して相互保持を行うシステムの導入を躊躇う原因となっている。本システムでは、保持している分割ファイルを他のサーバに再預託することで組織の都合によるファイルサーバを停止あるいは廃止を可能とする。ただし無秩序な再預託はファイルの分散度の低下につながる可能性がある。そこで、地震等の災害やそれに伴う電源喪失等を考慮して、地理情報に基づく地理的分散度およびファイルの冗長度（分割ファイルの消失に対する耐性）が維持される再預託方法を検討する。

(3) 平成24年度に構築するプロトタイプシステムでは、暗号化および分散冗長化の処理をCase 1とCase 2に分類し、それぞれクライアントまたは（利用者が最初にアクセスした）ファイルサーバ上で行うこととしていた。平成25年度は暗号化および分散冗長化の処理を流動性のあるメソッドとして独立・仮想化し、クライアント上あるいはファイルサーバ群（ストレージクラウド）上の任意の場所で実行できるように拡張する。これにより、スマートフォンや簡易なファイルサーバなど十分な処理能力を持たない端末やファイルサーバがシステム内に存在してもシームレスに使用できる環境を構築する。

(4) 本システムはシングルサインオン技術を応用することで、ファイル管理サービスを行う部分（SP: Service Provider）と、利用者認証を行う部分（IdP: Identity Provider）が明確に分割されている。したがって、本システムへの参加形態として、次の3つが考えられる。

① SP，IdPの両方を運用する組織
② SPのみを運用する組織
③ IdPのみを運用する組織

①は大学等が電子情報を相互に保持する利用形態を表している。一方、②は自らがサービス提供者としてシステムに参加する形態で、ストレージ事業者がバックアップサービスを提供する場合に相当する。③は自前のストレージシステムを保有せず、ストレージ事業者が提供するバックアップサービスを自らの利用者に2次プロバイダとして提供する場合に相当する。このように本システムの利用形態を整理し、ビジネスモデルとしての構築を試みる。そこで個人を含む小規模事業者をターゲットとした簡易ファイルサーバ（アプライアンス）の構築を行い、連携研究者や研究協力者の拠点に配置して実証実験を行う。

4．研究成果

(1) 平成24年度は以下の項目について研究を行い、それぞれに示す成果を得た。

① フェデレーションおよび分散ハッシュテーブルを構成するファイルサーバ群の構築

フェデレーション（学認）に基づくシングルサインオン認証を経て利用するファイルサーバプログラム（Javaサーブレット）を実装した（図1）。これにより、

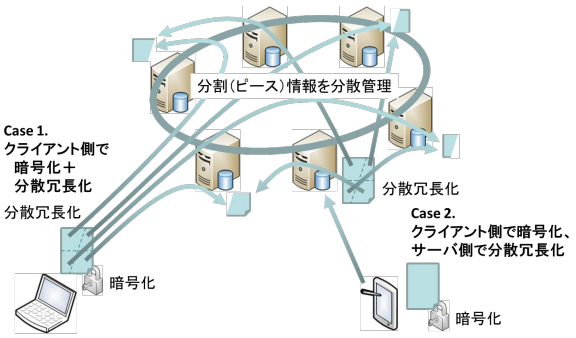

図1．プロトタイプシステム

フェデレーションに参加する複数の組織上にファイルの保管場所を確保し、シングルサインオンによりそれらにシー

ムレスにアクセスすることが可能となった。ファイルサーバはまた分散ハッシュテーブル（DHT）を構成するノードにもなっており、後述のファイル管理テーブルを保持する。また、秘密分散法によりシェアを生成して各ファイルサーバに送信したり、各ファイルサーバからシェアを取得して復号したりするクライアントプログラム（Java アプレット）を実装した。

② 暗号化および分散冗長化に使用するアルゴリズムの検討

クライアントプログラムに Shamir の秘密分散法を実装し、性能評価を行った。また利用者の属性に基づく属性ベース暗号により特定多数の利用者でファイルを共有する方式の検討、実装、評価を行った。

③ ファイルリストおよび検索テーブルへのアクセス制限に関する検討

ファイルサーバ管理者が必要（ファイル管理）以上の権限を持たない（復元権限を持たない）ようにするため、前述のファイル管理テーブルに階層構造を導入することで、「利用者のビュー（参照権限）」と「管理者のビュー（管理権限）」を分離した（図 2）。

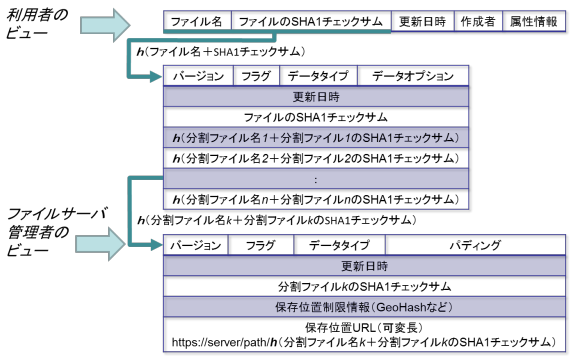

図 3. ファイルリストと検索テーブル

④ ファイルサーバが停止あるいは廃止する場合の対策の検討

ビューの分離を応用し、利用者の参照権限を損なうことなく、ファイルサーバ管理者の都合でファイルの保管場所を他のファイルサーバに変更する方法の検討を行った。シェアを保存できなくなったサーバはシェアをさらに秘密分散し、自身以外のサーバに配置する。ファイルサーバ管理者のビュー内で処理が可能であるため、利用者のビューは変更されない。

(2) 平成 25 年度は以下の項目について研究を行い、それぞれに示す成果を得た。

① 秘密分散処理の安全な委託方法の検討

平成 24 年度は、秘密分散処理をクライアントで行う場合（Case1）とクラウド上（ファイルサーバ等）で行う場合（Case2）について処理手順の検討を行った。平成 25 年度は、クライアント上で行う処理とクラウドに委託できる処理をより詳細に検討した。処理委託の際に情報漏えいを防ぐために行う暗号化処理に必要な秘密鍵が、データ復元時にも必要となることから、秘密鍵の管理コストを考慮に入れたシステム設計が必要である。

② 暗号化および秘密分散処理に使用するアルゴリズムの検討

秘密鍵の管理コストをなくすため、保存処理において秘密分散処理を委託する際に行う暗号化を秘密分散処理後に解除する方式を考案した。この実現には「排他的論理和の可換性」を応用した（図 3）。

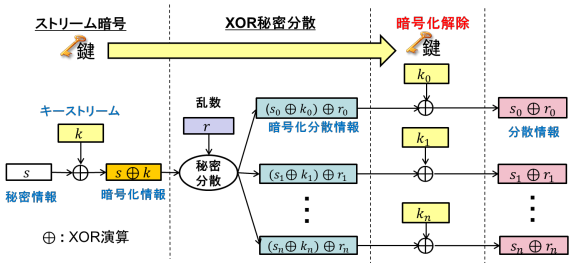

図 2. 排他的論理和の可換性

暗号化処理にはストリーム暗号（AES の CTR モード）を、秘密分散処理には XOR しきい値秘密分散法を使用した。秘密分散処理委託時に施したストリーム暗号を、秘密分散処理後の分散情報（暗号化シェア）に対して個別に復号することで、直接秘密分散法を適用したものと同一の分散情報（シェア）を得ることができる。そのため、処理のどの過程においても、計算量的安全性あるいは情報理論的安全性を維持しつつ、復元処理には秘密分散法の復元処理だけで元のデータを復元することができた。

③ 安全な委託方式を実現するプロトタイプシステム

上記の処理を行うプロトタイプシステムを構築し、動作確認および Case1 と Case2 の処理性能等に関する比較・評価を行った（図 4）。

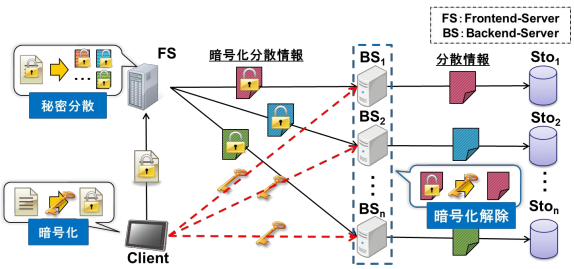

図 4. 排他的論理和の可換性

サービス全体の処理時間においては、秘密分散の処理をクライアント端末上で行う場合（秘密分散方式）とクラウド上で行う場合（提案方式）による違いは見られなかった（図 5）。しかし、クライア

ント端末上での処理時間は通信量を大幅に削減できることで、大幅に短縮することができた（図 6）。

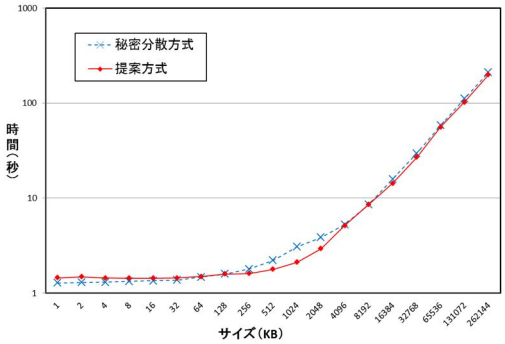

図 5. サービス全体の処理時間

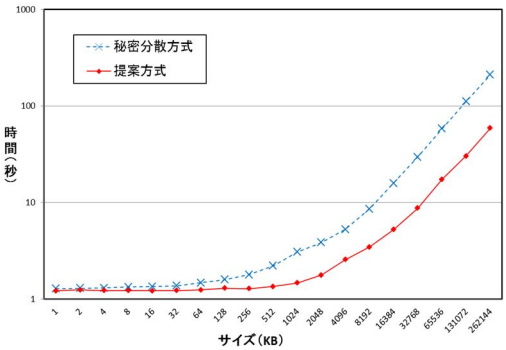

図 6. サービス全体の処理時間

(3) 平成 26 年度は、分散して配置するファイルサーバをシングルサインオンにより設置組織間で連携し、クライアントから複数のファイルサーバに対してシームレスにアクセスできるようにした。

① シングルサインオンはファイル管理サービスを行う部分(SP: Service Provider）と、利用者認証を行う部分（IdP: Identity Provider）を明確に分離する。これにより、本システムの活用形態を 3 つに分類した。「(組織 A) SP, IdP の両方を運用する組織」は大学等が電子情報を相互に保持する利用形態を表している。一方、「(組織 B) SP のみを運用する組織」は自らがサービス提供者としてシステムに参加する形態で、ストレージ事業者がバックアップサービスを提供する場合に相当する。「(組織C)IdPのみを運用する組織」は自前のストレージシステムを保有せず、ストレージ事業者が提供するバックアップサービスを自らの利用者に2次プロバイダとして提供する場合に相当する。このように、本システムはクラウドビジネスへの展開可能性がある。

② また、個人を含む小規模な事業者が参加する場合を想定した簡易ファイルサーバ（アプライアンス化）の構築の検討を行った。安価なサーバとストレージで構築が可能である。連携研究者や研究協力者の拠点に配置する実証実験は行えなかったが、ローカルネットワーク上での動作検証を行うことができた。

(4) クラウド技術は、ひとつの管理主体が大規模な資源を提供するのに対して、本研究では、複数の管理主体（組織）がそれぞれ管理する資源を連携させる仕組みを構築した点に特徴がある。またこれまでのシングルサインオンにおいては、フェデレーションを構成するサービス提供者のサービスの間を渡り歩くものであったが、本研究では複数のサービス提供者がフェデレーションの関係を利用してひとつのサービスを構成・提供するという点で独創的である。

(5) 本研究および関連研究の進展をきっかけに、各大学等における重要情報を扱うシステムのクラウド利用に向けた検討が進み、クラウドサービス利用のためのガイドラインやサービスカタログの策定、それらを利用した事例等の展開・集積が急速に進みつつある。

５．主な発表論文等

〔雑誌論文〕（計１５件）

① 吉田耕太，西村浩二，大東俊博，相原玲二，“秘密分散法を利用したクラウドストレージサービスにおけるモバイル機器を考慮した安全な処理委託方式”，情報処理学会論文誌，Vol.55，No.3，pp.1117-1125（2014 年 3 月）査読有.

② 大東俊博，後藤めぐ美，西村浩二，相原玲二，“暗号文ポリシー属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と性能評価”，情報処理学会論文誌，Vol.55，No.3，pp.1126-1139（2014 年 3 月）査読有.

〔学会発表〕（計８２件）

① 合田憲人，山地一禎，中村素典，横山重俊，吉岡信和，政谷好伸，西村浩二，棟朝雅晴，“アカデミッククラウド実現にむけたクラウド支援サービス”，電子情報通信学会インターネットアーキテクチャ（IA）研究会，2014 年 10 月 7 日，グランフロント大阪（大阪府・大阪市）.

② 西村浩二，“クラウドサービス利用ガイドラインと広島大学の取り組み”，京都大学学術情報メディアセンターセミナー，2014 年 6 月 24 日，京都大学（京都市左京区）.

③ 西村浩二，吉田耕太，大東俊博，相原玲二，“秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式の実装と評価”，第 4 回地域間インタークラウドワークショップ，2014 年 3 月 27～28 日，おきでんふれあいホール（沖縄県・那覇市）.

④ Toshihiro Ohigashi, Kouta Yoshida, Kouji Nishimura, Reiji Aibara, “Implementation and Evaluation of Secure Outsourcing for Secret Sharing Scheme on Cloud Storage Services”, the 2nd International Workshop on Architecture, Design, Deployment and Management of Networks and Applications (ADMNET 2014), 2014年7月21～25日, Västerås (Sweden).

⑤ Kouta Yoshida, Kouji Nishimura, Toshihiro Ohigashi, Reiji Aibara, “Implementation and Evaluation of Secure Outsourcing Scheme for Cloud Storage Services using Secret Sharing Scheme”, the 8th International Workshop on Security (IWSEC 2013), 2013年11月18～20日, (沖縄県・那覇市).

⑥ 吉田耕太, 西村浩二, 大東俊博, 相原玲二, “秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式の実装と評価”, 情報処理学会コンピュータセキュリティシンポジウム2013 (CSS 2013), 2013年10月21～23日, かがわ国際会議場 (香川県・高松市).

⑦ 吉田耕太, 西村浩二, 大東俊博, 相原玲二, “秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式”, 情報処理学会インターネットと運用技術 (IOT) 研究会, 2013年8月1日, 武蔵大学 (東京都・練馬区).

⑧ 後藤めぐ美, 大東俊博, 西村浩二, 相原玲二, “ファイル名／ディレクトリ名を秘匿可能なクラウド向け暗号化ファイル共有システム”, 電子情報通信学会2013年暗号と情報セキュリティシンポジウム (SCIS2013), 2013年1月22～25日, ウェスティン都ホテル京都 (京都府・京都市)

⑨ 後藤めぐ美, 大東俊博, 西村浩二, 相原玲二, “属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と評価”, 電子情報通信学会情報通信システムセキュリティ (ICSS) 研究会, 2012年11月22日, 国民宿舎みやじま杜の宿 (広島県・廿日市市)

⑩ 熊谷悠平, 西村浩二, 大東俊博, 近堂徹, 相原玲二, “認証フェデレーションに基づく分散ファイル管理システムの開発”, アカデミッククラウドシンポジウム2012@北海道大学, 2012年8月28日, 北海道大学 (北海道・札幌市).

⑪ 熊谷悠平, 西村浩二, 大東俊博、近堂徹, 相原玲二, “認証フェデレーションに基づく分散ファイル管理システムの提案”, 情報処理学会インターネット運用技術 (IOT) 研究会, 2012年6月28日, 東京学芸大学 (東京都・小金井市).

〔図書〕(計　0件)

〔産業財産権〕
○出願状況 (計　0件)
○取得状況 (計　0件)

〔その他〕

6．研究組織

(1)研究代表者
西村　浩二 (NISHIMURA, Koji)
広島大学・情報メディア教育研究センター・教授
研究者番号：９０２６３６７３

(2)研究分担者
近堂　徹 (KONDO, Toru)
広島大学・情報メディア教育研究センター・准教授
研究者番号：９０４３７５７５

田島　浩一 (TASHIMA, Koichi)
広島大学・情報メディア教育研究センター・助教
研究者番号：５０３２５２０５

大東　俊博 (OHIGASHI, Toshihiro)
広島大学・情報メディア教育研究センター・助教
研究者番号：８０５０８１２７

岡村　耕二 (OKAMURA, Koji)
九州大学・情報基盤研究開発センター・教授
研究者番号：７０２５２８３０

天野　浩文 (AMANO, Hirofumi)
九州大学・情報基盤研究開発センター・准教授
研究者番号：８０２３１９９２

柏崎　礼生 (KASHIWAZAKI, Hiroki)
大阪大学・情報推進機構・助教
研究者番号：８０４２２００４

(3)連携研究者
相原　玲二 (AIBARA, Reiji)
広島大学・情報メディア教育研究センター・教授
研究者番号：５０１８４０２３

岸場　清悟 (KISHIBA, Seigo)
広島大学・情報メディア教育研究センター・助教
研究者番号：３０２７４１３７