Vol.2021-DPS-186 No.70
Vol.2021-CSEC-92 No.70
2021/3/16

持続可能なセキュア共生情報システムの提案と デジタル寺院・ネバーダイプロフェッサ への応用

藤田茂[1]　滝雄太郎[2]　白鳥則郎[3]

概要：我々は，これまで，1)デジタル情報の生成消滅を管理するデジタル寺院，2)研究室における活動を 24 時間支援管理するネバーダイプロフェッサの概念を提唱し，これを実現するための基礎研究を行ってきた．本稿では，これらの概念を実現する基盤システムとして，社会の文化・法制度・慣習などが時代と共に変化しても，その変化を吸収し稼働する持続可能なセキュア共生情報システムを提唱し，その基本構造を示す．さらに評価について検討する．ここで安心・安全に実行するための``セキュア”を実現する方法として，これまで我々が研究し，得られた成果の秘密分散・秘密計算の一般化の効果的な適用を試みる．また，本稿で提唱する持続可能なセキュア共生情報システムの応用例として，デジタル寺院やネバーダイプロフェッサにおける重要課題の一つである，特に利用者の死後にも意図を反映して持続可能性や永続性を実現する技術について述べる．

キーワード：セキュア共生情報システム，秘密計算，秘密分散，デジタル寺院，ネバーダイプロフェッサ

1. はじめに

我々はこれまでに，自律・進化，持続可能な分散システムとして，共生情報システムを提唱してきた[3,4,37]．この中では，社会インフラとしての情報システムを，情報システムの変遷とパラダイムシフトの観点から述べた．社会インフラとなった情報システムは製造会社が吸収合併し消滅したとしても利用されて続けている．例えば文献[14]では，2050 年まで PDP-11 が利用されることが述べられている．

これまでの情報システムが，経済的合理性に基づいて発展し工業化社会の発展に寄与し豊かな情報社会に貢献したことを述べた．一方で，公害，自然破壊，地球温暖化などの負の側面がもたらされたことに触れ，新しく情報システムが，今後の地球環境の保全を目指すグリーンコンピューティング，人口減，高齢化社会の中でのシニア活動支援を行うシニアコンピューティング，人と情報システムとの共生を目指すシンビオティックコンピューティング（共生コンピューティング）を実現する共生情報システムについて述べた．また，我々は，ネットワークが災害に対して耐性を持つグリーン指向のネバーダイ・ネットワークを提案してきた[1,2].

共生情報システムとは，環境，利用者要求，社会の変化を自律的に認識，変化に対して自律的に柔軟に対応する持続可能な分散処理システムである．共生コンピューティングの概念[5-10,15-18]を構成する基本技術が共認知[11]である．

これまでの情報システムでは機器やサービスが停止しないことを信頼性の指標としてきた．また，情報システムに保存されるデータの暗号化や，通信の暗号化によってセキュアな情報処理を実現してきた．これらの技術の上に，持続可能性という観点を追加し情報システム構築技術とすることが，セキュア共生情報システム基盤である．

文献[33]では，「信用に基づく持続可能なネットワーク」のためには，社会，環境，経済の 3 つの調和が必要であることを述べている．一般に SDGs というと自然環境の保全のみが注目されるが，SDGs を達成し維持するためには，人間社会，自然環境，経済を考慮する必要がある．文献[12]で指摘されるように, 信用を前提とする処理は, 証明可能，追跡可能な信頼よりも検証コストが少なく，無闇に信用保証を要求すると社会コストが高くなる．

持続可能な情報処理システムを実現するために，人の保守活動負担が大きい．今日の情報処理システムは，信頼性を上げるために，電源，通信路，装置の二重化等によって無停止を達成し，なおかつ膨大なソフトウェアの維持開発に人的資源を投入し続けている．今のところ，情報処理システムの保守のきっかけとなる，計算機環境変化，ネットワーク環境変化，社会環境変化，利用者要求変化等への変化の対応は，人間が大きく関与する必要がある．これら環境変化に対して，人の関与量を減ずることをセキュア情報システムによって実現する．

環境変化の例としては，機器やサービスに付随する利用者登録情報の変化，機器の故障や更新情報の変化といった情報システムに不可欠な変化，これまでの情報システムでは，人間が対応していたために情報システムには組み込まれていなかったセキュリティポリシーの変更といった変化，おなじく情報システムの成り立ちや処理手順と大きくかかわるが人間が対応していた規則や法律の改訂という変化，利用者の変化，他の情報システムとの関係の変化などがあげられる．

我々はこれまでに情報システムの中で使われ実社会との連携を担うデジタル識別子の保存と管理が，企業毎や組織毎に別個に行われ，利用者の長期的な活動の中で，情報ト

1 千葉工業大学情報科学部
Faculty of Information and Computer Science, Chiba Institute of Technology
2 千葉工業大学大学院情報科学研究科
Graduate School of Information and Computer Science, Chiba Institute of Technology
3 中央大学研究開発機構
Research and Development Initiative, Chuo University

レースができず不利益を被ることや，遺族が故人の保有してきた機器や故人が利用してきたサービスを追跡できないことを指摘し，これらデジタル識別子の保存を企業や組織と独立して行う，デジタル寺院[3,4,30,34,36]の概念を提唱してきた．

データとして超長期に渡って保存可能な仕組み[19]の開発や，GitHub のパブリックな 21TB のデータをマイクロフィルムへ転写し北極圏の地下貯蔵庫に 1000 年間保存するプロジェクト[38]もあるが，これらはいずれも既存情報システムからのアクセスはできないため，デジタル寺院の概念とは一致が少ない．

また，文献[32]で述べられたように学術研究の基盤である学会，また学術出版を担う企業の解散や倒産によって，学術出版の持続性が失われることが指摘されている．我々はこれまでにこの課題を解決するために，ネバーダイプロフェッサの概念を提唱してきた．

社会システム基盤として情報システムが使われ続けており，通信路のみならず，保管と利用に関しても暗号化の必要性は増すばかりである．一方で，秘匿性と利便性は往々にしてバランスが要求され，秘匿性を増すことで情報システムの利便性を下げると，却って安全性が阻害されることが広く言われている．

社会システム基盤として，情報システムの重要性が増しており，複数の拠点にデータを保管するなど，バックアップを地理的に分散することが広く行われている．一方で複数の拠点にデータが存在することは，データ漏洩の危険があると言える．

これら二つの課題に対して，秘密分散[28,29]の考えがあり，データの保存や，プライバシーに配慮した処理を実現する仕組みが秘密計算を用いて実現されている[13,30,31].

2. 持続可能なセキュア共生情報システム

2.1 持続可能性

情報機器を含め，機械製品は一般に人間の保守作業が必要であり，単一の機械製品が永続的に利用できることはほぼ無い．一方で，我々の社会を支える情報システムに多くデータが保存され，またサービスが情報システムに依っており，持続可能な情報システムを実現する必要性は高い．

情報システムが稼働している短期間においても，例えばネットワークトラフィックの変化や，インターネットでの設定ミスによるサーバへのパケット不達が発生するなど，情報システムが変化に対応する必要があり人的コストが掛かっている．例えば，DNS の設定ミスによって，サーバの IP アドレスが引けなくなることや，インターネットサービスプロバイダーによる BGP の設定ミス，Google 等のクラウドサービス提供事業者の都合等である．

ここで，情報サービスの持続可能性を妨げ，利用者に対するサービス提供を変化させる，変化の例を挙げる．

1) 計算機環境の変化

サービスが実稼働している計算機環境の変化として，他のサービスの稼働状況に応じて変換する CPU 時間や利用可能な CPU 数，ネットワーク帯域がある．次いで，情報サービスを新しい計算機環境へ移動させたときの CPU 能力の変化，ネットワーク帯域の変化，メモリサイズ，メモリアクセス速度，ディスクアクセス速度，ディスク容量の変化がある．

2) 自然環境変化

情報サービスが稼働している実環境と自然環境は一見すると関係がないように見えるが，排熱処理等で熱負荷が影響を与える変化である．また，気温変化は CPU 速での制約となって情報サービスの性能に影響を及ぼす．

3) 社会変化

情報サービスの前提として，法や規制に抵触しない，社会慣習から逸脱しないことがある．情報サービスを設計するものがこれらを反映した設計を行う．しかしながら，長期に渡ってサービスが運営されると，設計時の法や規則から逸脱することになる．例えば，既に長期に渡って運営されている銀行業，保険業，国税に係わるシステムは，高いコストをかけて改修が実施され，社会変化に対応している．一方で，民間企業の実施するサービス等では，改修コストを負担できないために，法律変更や社会慣習の反映に伴って所定のサービス提供が終了し，利用者の予期せぬ時期に利用者の期待するサービスが受けられなくなる．

4) 利用者の変化

情報サービスの利用者が成長，加齢によって情報サービスが想定していた利用者モデルから変化する．例えば，大学受験生を対象としているサービスでは，利用者の大学合格をもって想定する利用者モデルから逸脱し，利用終了が想定される．一方で，それまでの利用者の情報を活用して，修学支援や就職活動支援に繋げることも考えられるが，情報サービスの変更は，通常，利用サイトの変更によって為され，利用者は新たなサイトの利用規約を読み，個人情報を登録する必要がある．

5) 参加者の変化

SNS に代表される情報サービスの参加者が指数関数的に増加する情報サービスがある．一方で流行の移り変わりにより，参加者の属性が変化することがある．例えば，自動車運転中の利用者を想定した招待性音声グループ対話サービスが，オフィスや自宅からの利用を行う参加者へシフトするなどである．この時，情報サービス側は想定と異なる利用時間帯や帯域の変化に直面する．

6) 時間変化

全ての変化は時間軸に沿って観測される．まったく利用者も参加者も，機器も変化しないように見えたとしても，

Vol.2021-DPS-186 No.70
Vol.2021-CSEC-92 No.70
2021/3/16

長期的には，すべてのものが変化する．また短期的にも，計算機負荷やネットワーク負荷，利用者の利用可能時間帯等の変化を，情報サービスの側が変化として認識する必要がある．

1-6)で述べた変化に対応するために，情報サービスの提供側では，人が情報サービスの保守を行う必要がある．これを本研究では，変化に対する人の関与量として定量的に評価することを検討している．図 1 では，同じ環境変化(A)に対して，現在の情報システムでは，人の作業量が大きいことを示し，一方で提唱するセキュア共生情報システムでは，人の作業量が中程度であることを示している．我々の提唱では，セキュア共生情報システムは，動作履歴から進化[20]して環境変化を吸収するため，環境変化(A)に対する人の作業量は減ずる．時間経過に従って環境変化に対する適切な変化吸収を自律的に実行できるようになり，より持続可能性が高くなり，環境変化(B)が新たに発生しても，人の作業量はより小さくなる．

変化に対してどのような処理を行うと利用者とセキュア共生情報システムに対して利益が大きいかを判断する，ベネフィット評価がセキュア共生情報システムには必要である．また，変化によって生じる新たなリスク評価が必要である．これを実現するための構造については，2.3 共生情報システムで述べる．

セキュア共生情報システムは，永続的に動作し持続可能なサービスを提供する．一方で受益者たる利用者，利用者グループが存続しているかの評価が必要である．この評価機構が無いと，一旦稼働したセキュア共生情報システムが，永遠に稼働し続けるために，地球環境全体，またセキュア共生情報システムを含むネットワークの負荷が上がり続けることになる．セキュア共生情報システムの寿命(Time To Live)を，予め組み込むことが考えられる．寿命の尽きたセキュア共生情報システムの持つ情報については，永続的に保存可能な媒体へ移転し，必要に応じて利用可能にすることが考えられる．

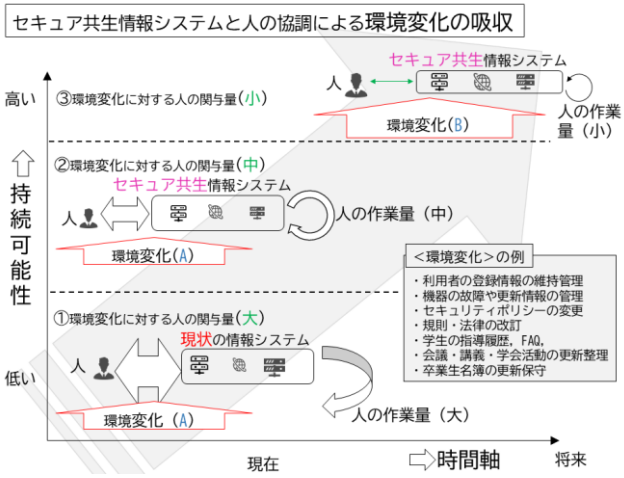

図 1 セキュア共生情報システムと人の協調による環境変化の吸収

2.2 セキュア共生情報システム基盤

人との共生を実現するセキュア共生情報システムを構築するための基盤技術が，セキュア共生情報システム基盤である．セキュア共生情報システム基盤は，分散処理システムとしてセキュアな永続性と持続可能性とを達成する．個別の実装技術は，既存計算機・ネットワーク技術を用いて作成される．図 2 にセキュア共生情報システムの階層モデルを示す．既存のネットワーク技術，分散処理技術，セキュリティ術の上に，セキュア共生情報システム基盤が構成される．この基盤の上にセキュア共生情報システムがあり，その上の応用例として，デジタル寺院，ネバーダイプロフェッサ，他の応用システムが作られる．

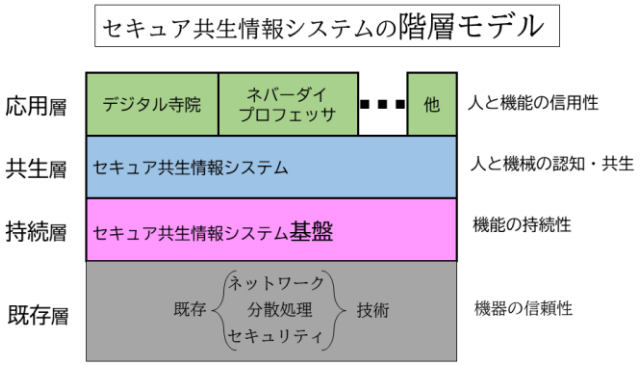

図 2: セキュア共生情報システムの階層モデル

セキュアなシステムを実現するために，唯一の情報システムを利用することが考えられるが，自然災害等によって情報システムが失われることが考えられるので，地理的な分散を行う必要がある．

単独の計算機アーキテクチャ，単一のオペレーティングシステム，単一のフレームワークに依存して情報システムを構成すると，ベンダーの都合による情報システムの稼働不能の発生や，脆弱性の発見によるサービス停止，更新作業が発生するため，特定の機能に依存せず，オープンシステムとして，機器，OS，フレームワーク独立に情報システムを分散構築する必要がある．

情報システムの稼働中に発生する計算機環境変化（CPU 負荷，ネットワーク負荷）へ対応するために，同一サービスが複数の計算機・ネットワーク上から，透過的に提供される必要がある．

情報システムの持つデータを時間的に分散保存することで，後世の検証や意図しないデータの破損，破壊に対する耐性を持たせることが，長期的にセキュア共生情報システムに必要である．

長期に渡ってサービスを提供するために，社会を構成する人，組織，法，規約，規則，慣習の変化が発生する．この時でも，その時々に応じた情報サービスを提供し，ある

いは一時的に情報サービスを停止し，将来に渡って利用者の意図を反映した動作を実行するために，物理的に分散した計算機・ネットワーク上に共生情報システムを構築する技術が必要である．

分散することの利点は多いが，一方で分散することで発生する問題として秘密保持, 同一性保証, 一回の実行保証, 停止性がある．

セキュア共生情報システムでは，複数の箇所にデータを保存するので，このデータが漏洩することを想定して暗号化する．暗号化にあたって，我々は秘密分散・秘密計算の枠組み[28,29,13]を使うことを想定している．

セキュア共生情報システムでは，長期に渡ってデータを保管することが想定されるので，既存の暗号技術の危殆化が想定される．この暗号技術の危殆化に関して，本研究ではデジタル寺院の構想を述べ，新たに開発される暗号技術によって，再度の暗号化を行い，秘密保持を確実なものにする手法を提案している[3,4].

複数の機器にまたがって構成されるセキュア共生情報システムでは，任意の時点で実行可能なセキュア共生情報システムが複数存在する．このため，ある時点で動作しているセキュア共生情報システムが唯一つであることを保証する仕組みが必要である．

また同様に，セキュア共生情報システムが実行するアクションが唯一回であることを保証する仕組みが必要である．

既に 2.1 の最後でセキュア共生情報システムが意図に反して永続的に実行する可能性と対策としての TTL の組み込みについて述べた．同様にセキュア共生情報システムの停止性保証を与える必要がある．意図せずしてセキュア共生情報システムを開始した後に，サービスを正当な権限をもって停止させる機能が必要である．

2.3 セキュア共生情報システム基盤の設計

2.2 セキュア共生情報システム基盤において，必要な機能を挙げた．本節では，これらの機能の中で特に重要である秘密分散，秘密計算の上に構成する共生情報システム基盤の設計について述べる．この設計によって，セキュア共生情報システムは，分散計算機環境の上で，たとえ構成要素が変更されたとしても永続的にサービスを提供できる持続可能性のシステムとなる．図 3 にセキュア共生情報システム基盤の概念図を示す．

セキュア共生情報システム基盤は，物理的には，複数のパーティ（Party）と呼ばれる，分散したデータを保存し，計算を実行する機器の集まりの上に作られる（図 3 中の P_1, P_2, P_3, …, P_n）．

パーティから設定に従って幾つかのパーティを選択すると，セキュア共生情報システム基盤を構成するメモリ（図 3 中の Considered Memory）が利用可能になる．このメモリを対象として，Stack, Environment, Code, Dump へのポインタを示す変数が同様に利用可能になる．このようにしてメモリと SECD スタックを構成し，SECD Machine[39, 40]を構成することができるため，関数型プログラミング言語の処理系を実装可能である．

この設計によって，セキュア共生情報システム基盤は，複数の計算機の上に分散して構成され，秘密計算，秘密分散の枠組みの中で，あるパーティが失われたとしても処理を継続でき，また順次パーティを構成する計算機を更新することで，永続的に処理を実行可能である．

セキュア共生情報システム基盤の上に作成されるプログラミング言語によって，2.2 で述べた，セキュア以外の課題について解決する機構を実装する．

2.4 セキュア共生情報システム基盤のエコシステム

共生情報システム基盤は複数のパーティによって構成される．この時，すべてのパーティを単独の権利者が保有することは，持続可能性を高める上で，障害となり，いくつかのパラメータによって自動的にパーティを選択することが必要である．いわゆるベンダーにサービスが固定されることを防ぐ．ここでは単純化するために，抽象的に

1) CPU 時間
2) 単位時間当たりの機器維持費用
3) 単位時間当たりのネットワーク維持費用
4) データ転送費用

を取り扱う．これに 2.5 で述べるセキュア共生情報システムの共生情報システム基盤利用頻度を合わせて，利用者の目的とするサービスを実現するための費用を計算する．利用者がこの費用をセキュア共生情報システムへ信託することで，その費用の範囲でセキュア共生情報システムが利用可能である．また，その費用を第三者が供出することでセキュア共生情報システムが持続可能となる．

この費用と持続可能な範囲については，1-4)の費用の変動に伴って変化する．

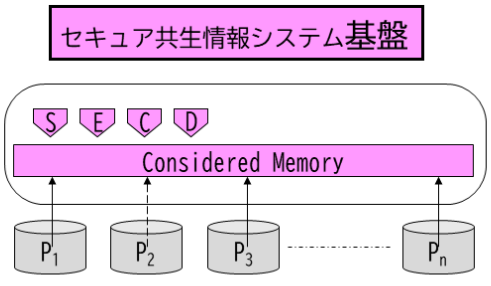

図 3: セキュア共生情報システム基盤の概念図

2.5 セキュア共生情報システム

機器としての永続性，持続可能性は 2.3 で述べたセキュ

Vol.2021-DPS-186 No.70
Vol.2021-CSEC-92 No.70
2021/3/16

ア共生情報システム基盤によって実現される．この上に社会的な変化に対応するセキュア共生情報システムを構築する．本節では，一般設計としてセキュア共生情報システムの内部構成について述べる．セキュア共生情報システムの内部構造概念図を図 4 に示す．

セキュア共生情報システムの外部の要素として，セキュア共生情報システムから知覚されるものは，人，環境，社会，時間，計算機・ネットワークである．

セキュア共生情報システムは，外部を知覚するための``Perception”機能，外部への動作を実行する``Kinetics”機能，知覚に基づいて外部の理解を反映する``World”，知覚に基づいて算出した利益``Benefit”，同様に算出したリスク``Risk”，これらの実行を制御する``update mechanism”，セキュア共生情報システムの予測する将来像を反映する``Assumption”，Perception から Knowledge の介在無しで Kinetics へ働く``reflex”，およびセキュア共生情報システムを代表する``Agent”からなる．

人がセキュア共生情報システムを安心して使うために，またセキュア共生情報システムが持続可能性を得るために，人を認知する必要がある．これは既存の情報システムと異なり，セキュア共生情報システムが常に利用者が特定の利用者であることを認識していることを意味する．また，利用者の側もセキュア共生情報システムが自分を認識していることを認識している．例えばパスワード認証で利用者認証をした後には自由にメールが読み書きできるメールクライアントプログラムとは異なり，セキュア共生情報システムとして構成されるメールクライアントでは常にカメラからの映像，キータイプの特性，マウス動作の特徴量，通常のメールクライアント利用時間の統計データなどから真の利用者が操作していることを認識していることになる．一方，利用者の側もセキュア共生情報システムがなりすました他のプログラムではないことを，セキュア共生情報システムを代表する Agent によって認識する．

利用者の意図は，利用者の死後，セキュア共生情報システムによって実行可能である．このためにセキュア共生情報システム基盤の動作に必要な費用を信託する．

共生情報システムは，Perception によって得られた情報を一部ダイレクトに World へ反映し，一部は Knowledge での処理を経て，World に反映する．この World は BDI エージェントモデルでの Belief に相当する．World と Knowledge に基づいて算出される Benefit, Risk 及び将来の仮説的な World である Assumption を作成して，短期，中期，長期，超長期に渡って Benefit を最大化する動作を選択し，変化を吸収する動作（Kinetics）を実行する．図 4 の reflex と update mechanism はセキュア共生情報システムの機構を実行する自動機構であり，Knowledge の影響を受けない．

セキュア共生情報システムの変化への対応として，

1) 変化の吸収
2) 変化に応じた変更
3) 変化の受容
4) 再変化への待機

がある．

変化を吸収するためにパラメータ調整を行い，一連の Kinetics を計画実行する．また内部の構造を変更するために一時的に Knowledge を無効にする．Benefit, Risk の算出次第では，変化を受容し，サービスレベルを低下させる．また変化が激しくセキュア共生情報システムの変化への対応が出来ない場合には，状況が好転することを期待して，再変化への待機を実行する．

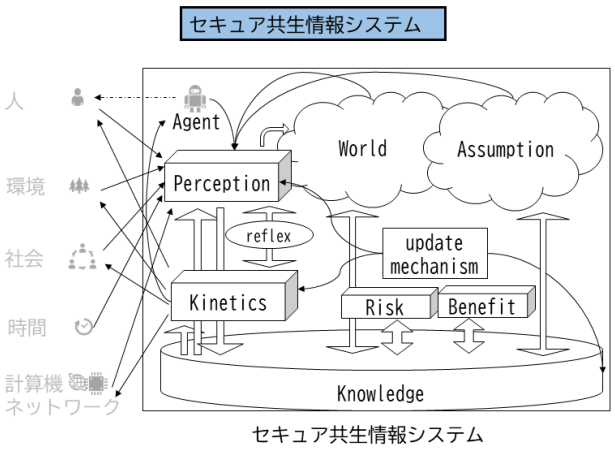

図 4: セキュア共生情報システムの内部構造概念図

セキュア共生情報システムはマルチエージェントシステム[21,22]である．また，Knowledge の実装においては機械学習技術[23,24]，深層学習応用技術[25-27]を反映させる

2.6 評価方法

セキュア共生情報システムの評価方法して

1) 計算機環境変化への追従
2) 変化に対する人の関与量
3) 自然環境負荷の測定

がある．

ネットワーク負荷や CPU 負荷を変動させた結果，この変化に対してセキュア共生情報システムが自律的に対応してサービスを維持することを評価する．

変化の状況に応じては，セキュア共生情報システムが単独では対応できないことがある．例えば OS の再インストールや機器の運搬，新たな計算機・ネットワークの敷設などである．これらが必要な状況下において，既存の情報システムに比べて人の関与量が減ったことを評価する．例えば，機器の移設に伴って，IP アドレスやドメインネームが変更になった時の，既存情報システム，セキュア共生情報システムとで作業量を比較する．

既存情報システムとセキュア共生情報システムとで，自

Vol.2021-DPS-186 No.70
Vol.2021-CSEC-92 No.70
2021/3/16

然環境に与える影響を評価する．例えば，利用電力量は費用ならびに自然環境へ与えるパラメータとして評価可能である．

3. 応用

3.1 デジタル寺院

セキュア共生情報システムとして，我々が提唱してきたデジタル寺院（図 5）を実装する．デジタル寺院は長期に渡って，デジタル識別子を保存することを，式年遷宮をモデルとしたシステム構築を織り込んだシステムモデルである．デジタル識別子を長期に渡って保存する場合，暗号技術の危殆化が問題となるが，式年遷宮のようにシステム構築を定期的に実行することで新たな暗号化技術の取り込みを可能にするモデルである．

現実空間では，ヒト，モノと人とモノの関係であるコトが発生する．これらについて，デジタル空間（既存の情報システム）では，データとデジタル識別子（Digital Identifier）を管理している．このデジタル識別子を長期に渡って保存管理する仕組みが，セキュア共生情報システムによるデジタル寺院である．

デジタル寺院では，利用者を認知する必要があるが，これはセキュア共生情報システムの基本機能として与えられる．同様に，利用者がデジタル寺院から認識され，利用時には常に本人確認が持続することから，機微な情報を含み得るデジタル識別子の利用状況を安心して預け入れることができる．

利用者の意図に沿って，デジタル識別子の情報を開示し，新たなサービスを受けることが必要である．例えば，遺族が故人の生前の意思に反して故人の情報を売買した例があり[35]，生前の情報が故人の意図通りに廃棄あるいは利用されないことを示している．このため，自分の死後には，自分の一切の情報を廃棄して欲しいという意思を持つ人も居る．一方で，これは情報のデジタル化が進む現代において，歴史的な資料が一方的に廃棄され続けられる可能性が高いことを示している．政府，行政機関，外交文書等では，現在は公開できないが後世公開の可能性のある文書が存在する．また私人においても，当時は合法あるいは黙認されていたが，今日的な基準では不適切な行動（例：日本におけるインターネット黎明期の研究者，技術者による自主的なケーブル配線工事）の記録は，公開すると非難が起こることが予想されるため，一部技術者，研究者によるブログや Twitter 等に僅かに記録として残るのみである．記録を残している当時の技術者，研究者自身が，後世への貴重な技術歴史的な記録が残らないことを危惧している．

このように現在は公開できないが，記録者の死後十分な時間間隔を空けて，利用者の意図に沿って情報を公開するような仕組みが必要である．これは，セキュア共生情報システムの Knowledge の中に，利用者意図を書き込むことで実現する．

デジタル寺院としてのセキュア共生情報システムは，利用者のライフサイクルを Knowledge として持つ．人が死に以降の動作について，生前の信託に基づいて動作する．また，誤認識によって死亡と判定した場合には速やかに復活処理を実施する．生前の信託によっては，デジタル識別子をすべて廃棄し，利用不能な状況にするように，という表現があり得る．一方で，誤認識によって死亡と判定してしまった後に，利用者の生存が確認されると，利用者の利益にならない．このため，利用者の意図の表現の如何に係わるが，一旦死亡と判定されても削除を実行せず，待機状態とすることも実装として必要である．これら意図の表現は，多くの人で共通して利用できるライブラリとして実装可能である．例えば，遺族へデータを委譲する．データを廃棄する．データを 100 年後に公開する．などである．この仕組みによって，生前は公開したくないが，死後，影響が無くなってから資料としてデータを公開する，といった運用が可能になる．

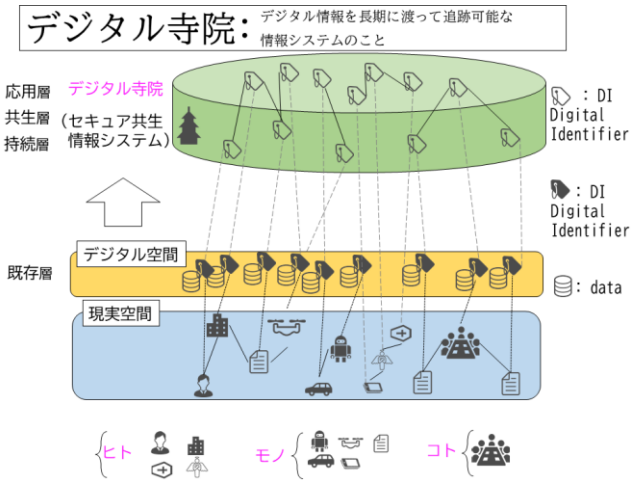

図 5: デジタル寺院の概念図

デジタル寺院は特定のサービスとして唯一つ存在するのではなく，いくつかのデジタル寺院ネットワークとして構成することを想定している[3,4]．これを含み，デジタル寺院を維持するための費用は利用者から信託を受ける．また，利用者の意図によっては，第三者が費用を拠出した場合にデータへのアクセスを許可する，データのコピーを許可するといった動作が可能である．

あるデジタル寺院のみを取り上げると，最終的に利用者とその関係者が存在しなくなり費用が尽き，デジタル寺院の持つデータが消失する可能性がある．例えば国会図書館に相当するようなアーカイブ機能が成立することを期待している．

Vol.2021-DPS-186 No.70
Vol.2021-CSEC-92 No.70
2021/3/16

3.2 ネバーダイプロフェッサ

セキュア共生情報システムの応用例として，研究活動，研究室活動を支援する，ネバーダイプロフェッサの例を示す．研究活動の例として論文作成と出版，保存，後世の閲覧の例を図 6 に示す．

研究者が実験を行い，研究成果としての論文を作成する．研究倫理として研究の裏付けとなったデータの保存が求められている．研究成果としての論文は出版社や学会・協会によって出版され，図書館に収蔵される．これらの機能が永続的であると期待できないことは文献[32]で考察されている．そこでネバーダイプロフェッサの利用者である研究者は，財を信託して，将来の権利消失後の論文保存や研究裏付けデータの保存を託す．また，図書館や出版社，学会，協会は，権利消失後にネバーダイプロフェッサへ論文を移転する．

権利をもつ機関はこれまで通りに出版社，学会，協会が財と引き換えに，論文を研究者へ提供する．一方で，ネバーダイプロフェッサへ信託された論文については，この論文を維持したい研究者が財を提供することでアクセスを行わせる．このようにして研究成果と研究活動が永続的に保存される仕組みを確保する．裏付けデータの保存支援を行う．

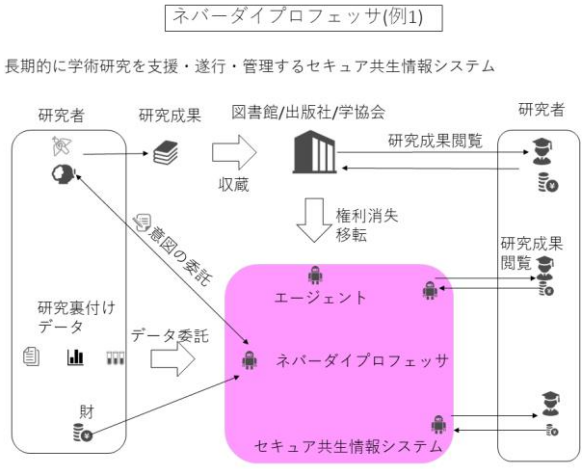

図 6: ネバーダイプロフェッサ（例 1: 論文，データ保存）

個人の研究活動以外に，大学で行われる研究活動の中心である研究室をネバーダイプロフェッサとして構成する例を図 7 ネバーダイプロフェッサ(例 2: 研究室活動)に示す．

研究室では，定期的なゼミナールによって研究室の構成メンバーに知見が蓄積する．また研究活動を支える資料・書籍は研究室の特徴を示す．このほか，研究に必要な機材の管理が必要である．また，大学での研究室では，他の研究室とのコミュニケーションや，卒業生との関係を維持する機能が必要である．他に研究室の活動の中で，予算申請や予算執行を管理する機能が必要である．

研究成果としての論文を維持管理するネバーダイプロフェッサと，研究成果を生み出すための活動を支援するネバーダイプロフェッサの二つを，セキュア共生情報システムによって構成する例を示した．

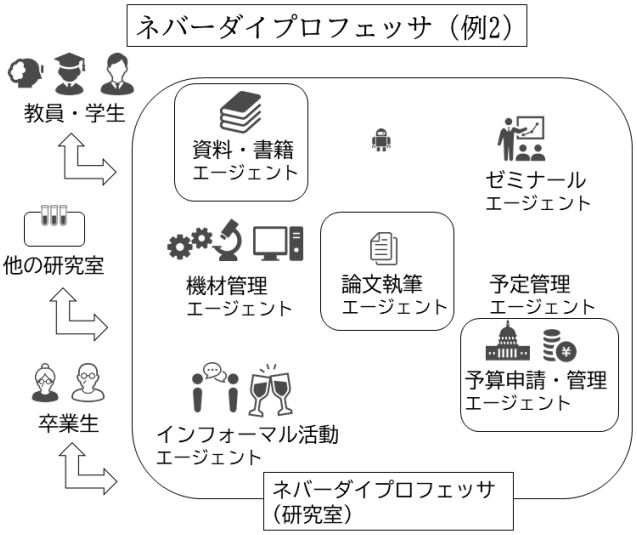

図 7: ネバーダイプロフェッサ(例 2: 研究室活動)

4. おわりに

本稿では，人と自然環境と機械の調和を狙って，持続可能な人との共生を行う情報処理システムとして，セキュア共生情報システムの概念を提唱した．また，これを実現する基盤システムとして，社会の文化・法制度・慣習などが時代と共に変化しても，その変化を吸収するための基本構造を示した．さらに評価方法について検討した．

機械システムとしての信頼性のみならず，人が安心安全であると信用できる``セキュア”を実現する方法として，これまで我々が研究し，得られた成果の秘密分散・秘密計算の一般化の効果的な適用による設計を示した．また，本稿で提唱する持続可能なセキュア共生情報システムの応用例として，デジタル寺院やネバーダイプロフェッサにおける重要課題の一つである，特に利用者の死後にも意図を反映して持続可能性や永続性を実現する技術について述べた．

謝辞 本研究は JSPS 科研費 JP18K11273 の助成を受けたものです．

参考文献

[1] Norio Shiratori, Noriki Uchida, Yoshitaka Shibata, Satoru Izumi “, Never Die Network towards Disaster-resistant Information Communication Systems,” ASEAN Engineering Journal Part D, Vol.1, No.2, pp.1-22, March 2013［Invited Paper］.

[2] 白鳥則郎，稲葉勉，中村直毅，菅沼拓夫，“災害に強いグリーン指向ネバーダイ・ネットワーク,” 情報処理学会論文誌, Vol.53, No.7, 1821-1831, July 2012［招待論文］

[3] 藤田茂，樋地正浩，滝雄太郎，宮西洋太郎，角田篤泰，菅原研次，白鳥則郎, "デジタル寺院": 設計と開発へ向けて，情報処

理学会研究報告, Vol.2019-DPS-180, Vol.2019-EIP-85, No.10, pp.1-8,2019/9/19.
[4] 藤田茂, 樋地正浩, 滝雄太郎, 宮西洋太郎, 角田篤泰, 菅原研次, 白鳥則郎, "デジタル寺院" : モデルと基盤技術", 情報処理学会研究報告, Vol.2019-MBL-92, Vol.2019-CDS-26, No.10, pp.1-8, 2019/8/30.
[5] Fujita, S., Sugawara, K., Kinoshita, T., and Shiratori, N., “An Approach to Developing Human-Agent Symbiotic Space”, Proc. of 2nd Joint Conference on Knowledge-based Software, pp.11-18, Bulgaria, 1996.
[6] Takahide Maemura, Shigeru Fujita Tetsuo Kinoshita, "Flexible Distributed System for Symbiotic Computing," 8th IEEE International Conference on Cognitive Informatics (ICCI 2009), pp. 141-144, 2009.
[7] Kenji Sugawara, Shigeru Fujita, "Non-verbal Interface of a Personal Agent based on Symbiotic Computing Model," ICCI*CC2011, 2011.
[8] Shigeru Fujita, Kenji Sugawara, "A Design Method for User Centric System Development by Symbiotic Computing," Centric2012, 2012.
[9] Kenji Sugawara, Shigeru Fujita, "Mobile Symbiotic Interaction between a User and a Personal Assistant Agent," ICCI*CC2012, 2012.
[10] Norio Shiratori, et.al., "Symbiotic Computing Based Approach Towards Reducing Users Burden Due to Information Explosion", Journal of Information Processing, 2012.
[11] Kenji Sugawara, Shigeru Fujita, "Interaction Zone between an office worker," CSCWD 2011, 2011.
[12] 西田豊明, @toyoakinishida, on Twitter, 2020/08/17, https://twitter.com/toyoakinishida/status/1295171859747463168.
[13] 滝雄太郎, 藤田茂, 宮西洋太郎, 白鳥則郎 : 軽量 N パーティ秘匿関数計算の一般化, 情報処理学会論文誌, Vol. 59, No. 10, pp. 1895-1902, 2018.
[14] Richard Chirgwin, “Nuke plants to rely on PDP-11 code UNTIL 2050! Programmers and their walking sticks converge in Canada”, Wed 19 Jun 2013 // 05:59 UTC, https://www.theregister.com/2013/06/19/nuke_plants_to_keep_pdp11_until_2050/ (last accessed 2020/08/19).
[15] 藤田茂, “スマートシステムのための共生コンピューティングモデル”, 情報処理学会研究報告, Vol. 2014-DPS-160(11), pp.1-8. 2014/07/17.
[16] 藤田茂, “エージェント指向システムによる情報システム構築のためのエージェントに対する要求仕様”, 情報処理学会研究報告, 2013-DPS-157(11),pp. 1-6, 2013/10/10.
[17] 藤田茂, “共生コンピューティング基盤の設計(2)”, 情報処理学会研究報告, 2012-DPS-152(2),pp.1-6, 2012/09/06
[18] 藤田茂, “共生コンピューティング基盤の設計(1)”, 情報処理学会研究報告, 2012-DPS-151(12), pp.1-5 , 2012/05/14
[19] Eternal 5D data storage could record the history of humankind, published: 18 February 2016, https://www.southampton.ac.uk/news/2016/02/5d-data-storage-update.page (last accessed: 2020/08/19)
[20] Takahiro Uchiya, Tetsuo Kinoshita, "Surveillance Architecture of Evolutional Agent System on Repository-based Agent Framework", Proc. of the 8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA2013), pp.614-617, 2013.
[21] HORLING, BRYAN; LESSER, VICTOR., “A survey of multi-agent organizational paradigms”, The Knowledge Engineering Review; Cambridge, Vol.19, No. 4, pp. 281-316, 2004/12.
[22] Yokoo, M., Sakurai, Y., & Matsubara, S., “Robust multi-unit auction protocol against false-name bids”. IJCAI International Joint Conference on Artificial Intelligence, 1089-1094, 2001
[23] Esteban Real, Chen Liang, David R. So, Quoc V. Le, “AutoML-Zero: Evolving Machine Learning Algorithms From Scratch”, https://arxiv.org/abs/2003.03384, last revised 30 Jun 2020, (last accessed: 2020/08/19)
[24] Esteban Real, “AutoML-Zero: Evolving Code that Learns”, July 9, 2020, https://ai.googleblog.com/2020/07/automl-zero-evolving-code-that-learns.html, (last accessed: 2020/08/19).
[25] 高橋裕太, 佐藤亮介, 亀井靖高, 鵜林尚靖, “Stack Overflow 投稿を用いた深層学習による自動バグ修正にむけて”, 情報処理学会研究報告, Vol.2018-SE-200, No.3, pp.1-7, 2018
[26] Zack Whittaker, “Amazon’s facial recognition moratorium has major loopholes”, https://techcrunch.com/2020/06/10/amazon-rekognition-moratorium/, June 11, 2020, (last accessed: 2020/08/19).
[27] Devin Coldewey, “IBM ends all facial recognition business as CEO calls out bias and inequality”, https://techcrunch.com /2020/06/08/ibm-ends-all-facial-recognition-work-as-ceo-calls-out-bias-and-inequality/ June 9, 2020, (last accessed: 2020/08/19).
[28] Adi Shamir, “How to share a secret", Communications of the ACM, Vol. 22, No.11, pp.612–613, 1997.
[29] Blakley, G.R., “Safeguarding Cryptographic Keys”, International Workshop on Managing Requirements Knowledge, (AFIPS) Vol.48, pp. 313–317,1997.
[30] 樋地正浩, 橋祐一, 菊池一彦, 藤田茂, 宮西洋太郎, 白鳥則郎, "秘密分散法が切り開くデジタルコンテンツの相続 ーデジタル寺院の実現に向けてー", 情報処理学会東北支部研究報告, Vol.2019, 2020/02/08,pp.1-5
[31] 宮西洋太郎, 韓嘯公, 北上眞二, 金岡晃, 佐藤文明, 浦野義頼, 白鳥則郎, "クラウドサービス利用者の安心感を高める簡易的秘密計算法の提案",電子情報通信学会情報・システムソサエティソフトウェアインタプライズモデリング研究会, 2014 年度, 第 1 回 SWIM 研究会
[32] 橋本誠志, “ペーパレス社会における学会の破産と知的成果のサステナビリティに関する一考察”, 情報処理学会研究報告, Vol. 2019-EIP-85, No. 12, pp.1-8, 2019/09/20
[33] Jin-Hee Cho, Kevin S. Chan, “Building Trust-Based Sustainable Network", IEEE Technology and Society Magazine, Summer, pp.32-38, 2013.
[34] 角田篤泰, 山澤昌夫, 五太子政史, 白鳥則郎,"デジタル・アイデンティティの危殆化に抗う「デジタル寺院」構想",日本セキュリティマネジメント学会, 第 32 回全国大会研究報告書, pp.1--6, 2018/6.
[35] 日本経済新聞, “007 作者の恋文競売, ボンド顔負けの色男？”, https://www.nikkei.com/article/DGXMZO52147930U9A111C1CR0000/, (last accessed: 2019/12/13)
[36] 藤田茂, “ソフトウェアエージェントとデジタル寺院”, 知能と情報, 日本知能情報ファジイ学会, Vol.32, No.6, pp.180-185(2020).
[37] 藤田茂, 白鳥郎, 滝雄太郎, “共生情報システム : 自律・進化・持続可能な分散システムの提唱”, 情報処理学会研究報告, マルチメディア通信と分散処理 (DPS) ,2020-DPS-184(11), pp.1-7 (2020-09-03) 2188-8906
[38] Julia Metcalf, “GitHub Archive Program : 世界のオープンソースコードを北極圏へ届ける旅” , https://github.blog/jp/2020-07-20-github-archive-program-the-journey-of-the-worlds-open-source-code-to-the-arctic/, 2020-07-20, (last accessed: 2021/02/18).
[39] Peter J. Landin. The Mechanical Evaluation of Expression. Computer Journal, 6, pp.308-320. 1964.
[40] Olivier Danvy: “A Rational Deconstruction of Landin's SECD Machine”. BRICS research report RS-04-30, 2004.