# アクセス制御機能に関する技術の研究開発の状況

## 1　国で実施しているもの

総務省又は経済産業省が取り組むアクセス制御機能の研究開発に関してとりまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは以下のとおりであり、その研究開発の概要は、別添1のとおりである。

ユビキタスネットワーク認証･エージェント技術の研究開発
異種ネットワーク相互接続環境下における最適情報通信サービス実現のための制御技術の研究開発
インターネットにおけるトレースバック技術に関する研究開発
大容量データの安全な流通･保存技術に関する研究開発
ネットワーク認証型コンテンツアクセス制御技術の研究開発
接続的な安全性を持つ暗号･電子署名アルゴリズム技術に関する研究開発　～安全な暗号技術を利用し続けるための暗号利用フレームワーク～
次世代ハッシュ関数の研究開発
適切な暗号技術を選択可能とするための新しい暗号等技術の評価手法　～暗号の技術的評価に関する研究開発～
インシデント分析の広域化･高速化技術に関する研究開発
ネットワークセキュリティ技術の研究開発
電子認証フレームワークとIPアドレス認証の展開に関する調査研究
生体認証サービスにおける情報漏えい対策（キャンセラブルバイオメトリクス）の研究開発
高信頼性端末の電子認証基盤の調査研究
情報漏えいに堅牢な認証･データ管理方式とそのソフトウェアによる安全な実装･検証手法に関する研究開発
ユビキタスネットワーク向けセキュアアセットコントロール技術の研究開発

## 2　民間企業等で研究を実施したもの

### (1)　公募

警察庁、総務省及び経済産業省が平成20年11月28日から12月26日までの間にアクセス制御技術に関する研究開発状況の募集を行ったところ、応募者は次のとおりであった。それぞれの研究開発の概要は、別添2のとおりである。

なお、別添2の内容は当該企業から応募のあった内容をそのまま掲載している。

株式会社カオスウェア
株式会社マインドトップ

(2) 調査

警察庁が平成20年12月から平成21年1月に実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして回答のあった大学及び企業は次のとおりである。

ア 大学

岡山大学
信州大学
東京工業大学
武蔵工業大学

イ 企業

株式会社ディー・ディー・エス
東北インフォメーション・システムズ株式会社
株式会社ブロードバンドタワー
三井情報株式会社

また、それぞれの研究開発の概要は別添3のとおりである。

なお、別添3の内容は、アンケート調査の回答内容（研究開発のうち実用化しているもののみ）をそのまま掲載している。

アンケート調査は、次の条件により抽出した1,300団体を対象に実施した。

・大学

国立・私立大学のうち理工系学部を設置するものから無作為に抽出

・企業

業種分類が「情報・通信」、「サービス」、「電気機器」又は「金融」である上場企業及び未上場企業から無作為に抽出

（別添1）

**対象技術** その他認証技術

**テーマ名** ユビキタスネットワーク認証・エージェント技術の研究開発

**開発年度** 平成15年度～平成19年度

**実施主体** (株)日立製作所 （総務省からの委託）

**背景、目的**

ユビキタスネットワークの進展とともに、地球上のあらゆる場所までネットワークが張り巡らされ、ユーザは自由に会話したり、情報コンテンツへ自由にアクセスできるようになる。一方これに伴い、通信内容の漏洩や不正な情報へのアクセスによって、ユーザのプライバシーが侵害されたり、データの遺失が発生したりする危険性が増加している。従来の中央集中型の認証システムでは、認証サーバに対して大量の端末・機器からのアクセス要求が発生するとサーバ処理がボトルネックとなる問題があった。また、認証サーバの障害がサービス全体に影響を及ぼすという問題や、ユーザ毎やサービス提供場所毎にきめ細かなセキュリティポリシを設定して認証・認可を行うには管理コストがかかり過ぎるという問題があった。これらの問題を解決し、いつでも、どこでも安心してコミュニケーションや電子商取引を行える、高性能かつ高信頼な分散型認証プラットフォーム技術を確立する。

**研究開発状況（概要）**

（1） 端末の位置情報やユーザの履歴情報等のコンテキスト情報を収集し、状況を判断して認証・認可を行うコンテキスト・アウェア利用者認証技術を開発。

（2） モバイルユーザに対して、異なるセキュリティレイヤ／ドメイン間で認証関連情報を安全かつ高効率に交換可能な認証エージェント連携技術を開発。

（3） 分散化した機器や提供される個々のサービスに対するアクセス制御ルールを動的かつ高効率に生成し配布するアクセス制御ポリシ自動構成技術を開発。

（4） ネットワークの利用状況に応じてピア・ツウ・ピアな通信経路を動的かつ階層的に構成し、これらの通信経路を利用して高効率なデータ交換を可能とする仮想アクセス空間構成・利用技術を開発。

上記技術の試作及び実フィールドでの実証評価を実施。

平成19年度末に開発終了。

**詳細の入手方法（関連部署名及びその連絡先）**

(株)日立製作所システム開発研究所 045-860-3088

**将来の方向性**

上記認証プラットホーム技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

**対象技術**　その他認証技術等

**テーマ名**　異種ネットワーク相互接続環境下における最適情報通信サービス実現のための制御技術の研究開発

**開発年度**　平成17年度～平成19年度

**実施主体**　エヌ・ティ・ティ・コミュニケーションズ(株)
（情報通信研究機構（NICT）が実施する委託研究の委託先）

**背景、目的**

我が国では2001年のIT戦略本部による「e-Japan戦略」を契機として、2003年の「e-Japan戦略Ⅱ」、2004年の「e-Japan戦略Ⅱ加速化パッケージ」等のIT国家戦略の中で地域の情報化を目指した様々な施策が実施され、政府及び地方自治体を取り巻く公共ネットワークの整備が急速に進められてきた。

これらの取り組みによって、我が国の公共ネットワークの整備は急速に進展し、世界でもトップクラスのIT国家の仲間入りを果たしたが、一方で、それらの公共ネットワークの整備はそれぞれの施策の中で異なる時期に、異なる目的、異なるポリシー等に基づき設計・構築されてきたため、多種多様なネットワーク仕様が混在するHeterogeneous（異種）ネットワーク環境下にあると言える。

しかしながら、これら異種ネットワークを相互に接続するための機構は未だ未整備の状況にあるため、各地域の様々なネットワーク上に散在する情報やサービスを必要に応じて有機的に連携させ、利用することが可能となれば、利用者にとって真に便利な高付加価値サービスを提供することが可能になると考えられる。このため、本研究開発では、国や自治体などが異種ネットワークによって相互に接続された環境において、サービスを効果的に相互提供・利用することを可能とする技術の開発を行う。

**研究開発状況（概要）**

・平成17年度より以下の研究開発を実施中。

（1）　マルチレイヤに跨る環境情報に基づく最適通信制御技術

（2）　高信頼ネットワークサービス環境構築技術

（3）　異種ネットワーク上での高度マッチメイキング技術

（4）　異種ネットワーク相互接続利用基盤を評価する実証実験

…全国地域情報化推進協会の協力を得て、防災情報の伝達・共有及び災害医療に関するフィールド実験を実施した。(平成 18 年 10 月～12 月)

・平成 19 年度末に開発終了。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

**将来の方向性**

国や自治体などが異種ネットワークによって相互に接続された環境において、サービスを効果的に相互提供・利用を可能とする基盤技術の確立に資する。

**対象技術** 侵入検知技術

**テーマ名** インターネットにおけるトレースバック技術に関する研究開発

**開発年度** 平成17年度～平成21年度

**実施主体** 日本電気(株)、奈良先端科学技術大学院大学、KDDI(株)、松下電工(株)、
(株)クルウィット、(財)日本データ通信協会
(情報通信研究機構(NICT)が実施する委託研究の委託先)

**背景、目的**

インターネットに対する攻撃・脅威によるインシデントは年々増大している。従来からインターネットを監視するという受動的な警戒に関しての技術開発が実施されているが、これに対し、攻撃の予兆を検出した時にその攻撃の発生場所を探索するという能動的な警戒が考えられる。

この能動的な警戒を実現するために必要となる「トレースバック技術」の研究開発については、IP層におけるトレースバックの研究は十数年にわたって進められており、理論は成熟しつつあるが、フィールド広域に対する実装が行われている例は少ない。またそれより上位のアプリケーション層に関しては、理論研究さえ未成熟である。このため、本研究開発では、インターネットにおけるトレースバック技術に関しての実運用環境への実装を目指した研究開発を行う。なお、不正アクセス、DoS攻撃、ウイルス発信等の攻撃はそのIPパケットのソースアドレスが詐称されている例も多く、攻撃源の把握が困難であるが、本研究開発ではソースアドレス詐称があってもその発信源を把握できるトレースバック技術を開発する。

**研究開発状況(概要)**

・平成17年度から以下の研究開発を実施中
(1)全体アーキテクチャーの設計
(2)トレースバック・アルゴリズム
(3)トレースバック用データ収集装置(プローブ装置)
(4)トレースバック・プラットフォームの実証実験
・平成21年度末に開発終了予定。

**詳細の入手方法(関連部署名及びその連絡先)**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ
(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話　042－327－6011

**将来の方向性**

不正アクセス、DoS攻撃、ウイルス発信等に対してその発信源を探索して対策を講じることができるようになると同時に、抑止力として期待される。

**対象技術** その他認証技術

**テーマ名** 大容量データの安全な流通･保存技術に関する研究開発

**開発年度** 平成17年度から平成19年度までの3年間

**実施主体** (株)日立製作所、東京理科大、エヌ･ティ･ティ･コミュニケーションズ(株)
(情報通信研究機構(NICT) が実施する委託研究の委託先)

**背景、目的**

近年社会生活において、ネットワークインフラはますます身近なものとなってきている。特に、わが国においては、すでに世界最高水準のブロードバンドネットワークインフラの整備が進み、現在は、さらにユビキタスネットワーク社会の実現に向けて、さまざまな取り組みがなされている。

ユビキタスネットワーク社会の技術環境の特徴として、

- 多様で複雑なブロードバンドネットワークの進展･普及
- コンテンツの大容量化･多様化
- 情報処理端末の小型化･モバイル化

の各点が挙げられるが、これらは、人々の生活をより便利に豊かにする上で望ましい特徴である反面、セキュリティの観点からは、逆に、情報漏洩の危険性や一旦漏洩した場合の被害の拡大につながる懸念がある。これらの懸念を払拭しなければ、ユビキタスネットワーク社会の進展は図れない。

本研究開発では、ユビキタスネットワーク社会における情報漏洩を防止する技術を確立するために、通信路、コンテンツ、ストレージの3つの観点から研究開発を実施する。

**研究開発状況 (概要)**

・ 平成 17 年度より以下の研究開発を実施中。

(1)機密情報を安全、高速、低消費電力で伝送する技術

(2)機密情報を利用者の役割等に応じ、選択的に開示する技術

(3)機密情報を安全かつ効率的に保存する技術

・ 平成19年12月18日 実験システムデモを実施。

・ 平成19年度末に開発終了。

**詳細の入手方法 (関連部署名及びその連絡先)**

独立行政法人情報通信研究機構 連携研究部門 委託研究グループ
(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話 042－327－6011

**将来の方向性**

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性･信頼性の確保に資する。

**対象技術**　その他認証技術

**テーマ名**　ネットワーク認証型コンテンツアクセス制御技術の研究開発

**開発年度**　平成18年度～平成20年度

**実施主体**　富士通(株)、東京工業大学
（情報通信研究機構（NICT）が実施する委託研究の委託先）

**背景、目的**

インターネットの普及、低価格化により、ネット上での情報流通、商取引などの機会の増加が見込まれている。また、医療、金融など、いわゆるミッションクリティカルな分野にもその利用が拡大し、遠隔診断、リアルタイム受発注などでの応用も計画されている。一方、インターネット上での詐欺、情報不正入手など、いわゆるネット犯罪も増加傾向にあり、健全なネットワーク社会の発展への影響が不安視されている。

ネットワークの危険性が高まる中、より高いセキュリティが通信システムにも求められている。現在の通信システムはID／パスワード、電子証明書など、単一の証明システムにより運営されているケースが多いが、脅威に対応するためにはこれらを複合的に利用し、セキュリティ強度を高めていく必要が出てきている。利用者の目的に従い複雑化する認証を統合的に扱い、その認証に応じてネットワークを制御し、コンテンツの流通を管理できる技術の開発を行う。

複数の認証技術・機関にまたがる認証技術を統合的に扱うためには、アプリケーションにおける利用者認証、利用している機器、ネットワークなどの利用環境の、それぞれのレイヤで認証と管理を行う仕組みが必要となる。しかし、現状では各レイヤでの管理は独立して行われているため、これを総合的に判断する仕組みは規定されていない。また、利用者、環境などは複数の対象、複数管理機関が存在するが、これらを含めた全体の状況を認証するシステムが必要となる。

複数の認証技術・機関にまたがる認証を統合的に扱える技術「複数認証連携技術」と、その認証応じてネットワークを最適に制御する「ポリシーやコンテンツに応じたネットワーク制御技術」の二つの基盤技術の開発を行う。

**研究開発状況（概要）**

・平成18年度より以下の研究開発を実施中。

(1) 複数認証連携技術

(2) ポリシーやコンテンツに応じたネットワーク制御技術

(3) 複数認証ドメイン管理基盤技術

・平成20年度末に開発終了予定。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

**将来の方向性**

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

**対象技術**　その他認証技術

**テーマ名**　持続的な安全性を持つ暗号･電子署名アルゴリズム技術に関する研究開発
～安全な暗号技術を利用し続けるための暗号利用フレームワーク～

**開発年度**　平成19年度～平成21年度

**実施主体**　株式会社エヌ･ティ･ティ･データ
(情報通信研究機構 (NICT) が実施する委託研究の委託先)

**背景、目的**

計算機の演算能力の向上や暗号に対する解読技術の進展などを背景として、電子政府推奨暗号を始めとする暗号は、常に危殆化の危険にさらされている。暗号危殆化に関して、特に深刻な影響が予想されるのは、危殆化した公開鍵暗号アルゴリズムから計算された秘密鍵が漏洩するという問題である。また、ハッシュ関数が危殆化した場合においても、電子署名付き文書の改ざんや偽造文書へのすり替えという問題が起こり得る可能性があると考えられる。

こうした問題への対応策としては、より安全な公開鍵暗号アルゴリズムやハッシュ関数への移行が必要となるが、既に生成された電子署名付き文書や暗号化データがシステムやアプリケーションをまたがって分散された環境に広く流通している場合があり、移行上の制約要因となっている。

他方、既存の暗号技術においては、秘密鍵の漏洩などへの対処は考慮されているが、危殆化が発生した際に、電子署名及び暗号化データの有効性を継続的に保証することまでは考慮されていない。したがって、電子署名の更新を行う場合には、最初に電子署名生成者にデータを全て戻し、そのデータに対して安全なアルゴリズムで電子署名を再計算する必要がある。このため、これら一連の電子署名の更新に係る過重なコスト負担がネックとなり、危殆化対策が立ち行かなくなることが懸念されている。また、ネットワーク上のサーバやストレージ等にレプリケーションされたデータやRFIDタグに格納されている情報、デジタルコンテンツなどとして広く流通している暗号化データの再暗号化を行う場合においても、同様な問題が存在する。

このような状況を踏まえ、本研究開発では、危殆化対策の一環として、安全性や利便性、危殆化対策に係るコスト低減を十分考慮しつつ、電子署名の更新及び暗号化データの再暗号化を可能とし、それらの有効性を継続的に保証するための技術を確立する。

**研究開発状況 (概要)**

･平成19年度より以下の研究開発を実施中。

(1) 電子署名及び暗号化データの有効性を継続的に保証するための仕組みとその最適化手法

(2) 電子署名更新技術

(3) 再暗号化技術

･平成21年度末に開発終了予定。

**詳細の入手方法 (関連部署名及びその連絡先)**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ
(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話　042－327－6011

**将来の方向性**

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性･信頼性の確保に資する。

**対象技術**　その他認証技術

**テーマ名**　次世代ハッシュ関数の研究開発

**開発年度**　平成19年度～平成21年度

**実施主体**　株式会社日立製作所、国立大学法人神戸大学、国立大学法人福井大学
（情報通信研究機構（NICT）が実施する委託研究の委託先）

**背景、目的**

電子データの真正性確保やユビキタス機器を利用したシステムおけるユーザの認証などを実現するための技術など、安心・安全のための情報通信技術の必要性が高まっている。また、ユビキタス環境では、情報を発信・受信する計算機・端末が、サーバ、従来のPCといった処理能力に優れたものから、携帯電話やICカード等の小型で比較的制限が多い電子機器と多様化しており、これらの機能は、多様なプラットフォームで利用可能である必要がある。

このような課題の解決手段として、メッセージ認証子を用いて、改ざん検知や機器認証を行う方法や電子署名を用いて電子文書の真正性を確保する方法が利用されている。これらの方法はいずれもハッシュ関数を利用しており、ハッシュ関数の安全性がこれらの技術の根幹となっている。しかし、近年の学会において、現在最も広範に用いられている専用ハッシュ関数であるSHA-1やMD5が、衝突耐性という安全性に関して脆弱であることが報告されている。

このような背景から、安心・安全のための情報通信技術の研究開発の一環として、本研究では、下記に示すようなハッシュ関数（専用ハッシュ関数）を次世代ハッシュ関数と定め、その実現のための研究開発を実施する。

・次世代ハッシュ関数

衝突困難性、一方向性、第二原像困難性など、一般的にハッシュ関数に求められる安全性に関して理論的な根拠を有すること。

実運用上の各種安全性要件に応じた安全性強度を有すること。

多様な実装条件下における実装性能に優れた汎用性を有すること。

**研究開発状況（概要）**

・平成19年度より以下の研究開発を実施中。

(1) 次世代ハッシュ関数の設計技術

(2) 次世代ハッシュ関数の実装技術

・平成21年度末に開発終了予定。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

**将来の方向性**

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

**対象技術** その他認証技術

**テーマ名** 適切な暗号技術を選択可能とするための新しい暗号等技術の評価手法
～暗号の技術的評価に関する研究開発～

**開発年度** 平成19年度～平成21年度

**実施主体** 富士通株式会社
(情報通信研究機構(NICT)が実施する委託研究の委託先)

**背景、目的**

暗号に対する解読技術は日進月歩発展を遂げており、電子政府推奨暗号を始めとする暗号は、常に危殆化の危険にさらされている。広範な用途に利用されている公開鍵暗号技術であるRSA暗号においては、素因数分解問題の困難性を安全性の根拠としていたが、計算機の演算能力の向上から素因数分解が可能となる桁数が増えてきている。このような状況から、RSA暗号の次段階として、RSA暗号と比較して、より短い鍵長で同等の強度を実現できる、楕円曲線暗号が期待されている。

しかしながら、楕円曲線暗号においては、一方向性関数の性質により、演算を行うことが非常に困難となる楕円曲線上の離散対数問題を安全性の根拠としているが、素因数分解問題の困難性を安全性の根拠とするRSA暗号と比べて、解読技術の研究開発や暗号強度等安全性の評価が必ずしも十分なされているとは言えないのが現状である。このような状況から、暗号に関する研究者の間に、楕円曲線暗号の安全性に対して疑問視する声があるのも事実である。

他方、複数の異なる暗号要素技術を組み合わせて使用するシステム等では、これらの暗号要素技術間の強度、性能のトレードオフを検討する必要があり、その際、鍵長と強度との関係を比較した、米国NISTのFIPS800-57(次頁の表1及び表2を参照)などが参考にされている。

しかしながら、これらについては、実験データが明らかになっておらず、データの入手についても制約を伴うことから、その実験結果が本当に正しいかどうかを付加的に検証することが困難となっている。

さらに、楕円曲線暗号の攻撃手法は、一般的な楕円曲線に適用できる手法、特殊な楕円曲線に適用できる手法など幾つか考えられており、使用される楕円曲線の種類も何種類か存在するが、攻撃実験を基にした、同一の評価基準による楕円曲線相互の暗号強度比較・評価・検証はこれまで行われていないのが実態である。

このような状況を踏まえ、本研究開発では、一般的な楕円曲線暗号を中心として、実際に攻撃実験を行い、その実験データを基に、各種楕円曲線間の鍵長と強度の比較や、RSA暗号等他の暗号要素技術との強度比較をより精密に行う。また併せて、鍵長の寿命を予測することにより、鍵更新時期などの運用方針に役立てるとともに、複数の異なる暗号要素技術を組み合わせて使用するシステム等での強度バランスを明確にする

**研究開発状況(概要)**

・平成19年度より以下の研究開発を実施中。

(1) 攻撃プログラムの設計・開発

(2) 暗号強度比較・評価・検証技術

・平成21年度末に開発終了予定。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ

（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

**将来の方向性**

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

**対象技術**　その他認証技術

**テーマ名**　インシデント分析の広域化・高速化技術に関する研究開発

**開発年度**　平成20年度～平成22年度

**実施主体**　株式会社ラック、財団法人九州先端科学技術研究所、株式会社セキュアウェア、株式会社セキュアブレイン、株式会社クリプト、ジャパンデータコム株式会社、KDDI株式会社

（情報通信研究機構（NICT）が実施する委託研究の委託先）

**背景、目的**

近年のコンピュータセキュリティインシデント（以下、「インシデント」と略す。）は、正規のWeb サイトを装いつつ、ユーザがそのWeb サイトを参照するだけで、マルウェアをダウンロードさせられたり、ソーシャルエンジニアリング手法を駆使して、特定の個人に関連する偽の情報を流したり、URL の見間違えを誘発するなどの工夫が施されており、ますます巧妙化の傾向を強めてきている。

こうした状況の中で、情報通信研究機構（NICT）においては、広域のネットワークを想定し、スキャンを中心とした攻撃検知とその原因となり得るマルウェア等の解析により、インシデントを迅速かつ正確に検知し、対策を導出するための研究開発を行うために、nicter（Network Incident analysis Center for Tactical Emergency Response）と呼ばれるインシデント分析センターの構築を進めている。

現状のnicter では、ネットワークにおける攻撃情報の収集地点に偏りがあり、攻撃情報の種別についても網羅性が乏しい。また収集した情報を一元管理しているため、その分析性能などに多くの課題を抱える。しかしながら、これまでのnicter において培われてきた高度な分析能力を十分に活用し、それらの効率的な機能配分を行うことにより、日本全土を広域にカバーする、高性能なインシデント分析システムの構築が可能であると考えられる。

本研究開発では、このような広域分散型のインシデント分析システムの構築により、広く日本でどのような攻撃が起こっているのか、その攻撃にどのような地域性があるのか、その攻撃は具体的にどのようなマルウェアに起因しているのか、その攻撃への対策をどのように講じるべきかを効率的に解決することを目的とする。

**研究開発状況（概要）**

・平成20年度より以下の研究開発を実施中。

(1) 攻撃及び関連マルウェアの高速・高精細攻撃検知・収集

(2) 階層拠点間の分散協調のための分析結果情報の匿名化・秘匿化技術

(3) 階層拠点における分散協調型セキュリティオペレーションの基盤技術

(4) 実環境で有効に機能させるための実証実験

・平成22年度末に開発終了予定。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　連携研究部門　委託研究グループ

（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

**将来の方向性**

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

**対象技術**　侵入検知技術

**テーマ名**　ネットワークセキュリティ技術の研究開発

**開発年度**　平成18年度～平成22年度

**実施主体**　独立行政法人情報通信研究機構

**背景、目的**

ネットワーク上におけるサイバー攻撃・不正通信等に耐えるとともに、それらを検知・排除するため、イベント（スキャン、侵入等）の収集・測定及びこれに基づく傾向分析・脅威分析を実時間で行い予兆分析を含めた対策手法の迅速な導出を行うインシデント対策技術の研究開発を行う。

また，対策手法の導出に当たって，再現ネットワークの活用による検証、発信元追跡技術の研究開発を行う。さらにDoS（サービス不能）攻撃によるネットワーク障害への耐性を高めるためのセキュアオーバーレイネットワーク技術の研究開発を行う。

**研究開発状況（概要）**

平成20年度には、これまでに研究開発・整備した広域に設置された観測点からのセキュリティログの分析手法、マルウエアの収集機構・収集したマルウエアの分析機構に関して、観測対象ネットワークの拡充、より高度な観測アーキテクチャ・攻撃検出機構の開発、マルウェアの分析能力の強化を行った。この結果をこれまでに構築したインシデント分析システムプロトタイプに反映する作業に着手した。

また、異なる機関に属する複数の観測点で収集したログから、その組織が有する情報を互いに開示することなく、共通の攻撃を解析する技術を開発し、実証実験を行った。攻撃ベクタの捕捉能力と解析能力の向上のため、仮想マシンモニタを用いて不正アクセス発生時点のメモリ、ディスク内容を捕捉する研究を進め、攻撃を受けたメモリのスナップショットをとるシステムを開発した。またメモリ内容を自動分類し、高精度でメモリ内の攻撃ベクタを捕捉できる機械学習アルゴリズムの開発に向けて、海外研究機関と連携した研究体制を確立した。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　情報通信セキュリティ研究センター推進室　042-327-5774

**将来の方向性**

上記の研究開発を通じて、将来のネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性の確保と、利用者にとって安全・安心な情報通信基盤の実現を目指す。

**対象技術**　認証技術

**テーマ名**　電子認証フレームワークとIPアドレス認証の展開に関する調査研究

**開発年度**　平成17年度～平成19年度

**実施主体**

社団法人日本ネットワークインフォメーションセンター（経済産業省からの委託）

**背景、目的**

高度情報通信ネットワークの基幹であるインターネットは、電子政府を始め、企業、教育機関、医療機関等において幅広く利用されており、その安全性を確保するための方法の1つとして、電子認証が行われている。

電子認証では、ネットワーク等を通じたアクセス元の本人性を電子的に確認する仕組みとして、第三者による証明となる認証局（Certification Authority）が構築・運営されているが、利用場面毎に体系だったフレームワークが構築されておらず、このことが適切な電子認証の利用や普及の妨げになっている。

本事業は、日本国内のIPアドレス等のネットワーク登録情報を活用した電子認証に係る実証試験を行い、電子認証の普及に必要な仕組みとなる「電子認証フレームワーク」を策定することにより、日本国内の情報インフラの根幹となる電子認証基盤の構築に資することを目的とする。

**研究開発状況（概要）**

社団法人日本ネットワークインフォメーションセンターが管理するIPアドレス、AS番号などの登録情報を活用した電子認証については、インターネットサービスプロバイダー（ISP）におけるルーティング（経路制御）の信頼性向上に役立つ「経路情報の登録機構」の技術開発を行い、実験運用を行った。

また電子認証の適切な普及に役立つノウハウをドキュメント化するため「電子認証プラクティスフォーラム」を立ち上げ、各組織の共通ノウハウを蓄積した。

**詳細の入手方法（関連部署名及びその連絡先）**

〒101-0047
東京都千代田区内神田2－3－4　国際興業神田ビル6階
社団法人日本ネットワークインフォメーションセンター　インターネット推進部
電話番号：03-5297-2311
URL：http://www.nic.ad.jp/

**将来の方向性**

当該事業で開発する電子認証を利用したIPアドレスとルーティングレジストリの連携機構の普及により、信頼のおけるIPアドレスの登録情報管理が実現し、我が国に対するIPアドレスの不正利用を排除することが可能になる。また、電子認証に関する汎用的なノウハウの蓄積と公開を継続していくことで、我が国の電子認証技術に関わる関係者の間で、新たな技術課題に対する対応策やノウハウ（Best Current Practice）を共有できる。

**対象技術** その他認証技術等

**テーマ名** 生体認証サービスにおける情報漏えい対策（キャンセラブルバイオメトリクス）の研究開発

**開発年度** 平成20年度～

**実施主体** 株式会社日立製作所（経済産業省からの委託）

**背景、目的**

現在、情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威が急速に変化・拡大しており、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。そこで「新世代情報セキュリティ研究開発事業」では、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を実施することを目指している。

本事業では、漏えいが許されない情報の一つである指紋や静脈、虹彩などのバイオメトリクス情報の安全な利活用の実現を目的として、生体特徴情報を無効化するキャンセラブルバイオメトリクス技術を生体認証サービスプロバイダに適用した場合の管理・運用の在り方について調査・研究を実施し、強度評価手法と、運用ガイドラインの作成を進めている。

**研究開発状況（概要）**

(a) 情報漏えい対策型の生体認証サービスフレームワークの研究開発

一般利用者への提供を想定した生体認証サービスシステムの運用モデルを検討し、リスク分析評価を行い、システム要件を明確にしている。さらに、実証実験に向けてサービスシステムのシステム設計および試作を進めている。この実証実験の結果をフィードバックし、情報漏えい対策型の生体認証サービスフレームワークの確立を目指している。

(b) 情報漏えい対策技術の強度評価に関する研究開発

情報漏えい対策技術の強度評価について、国内・海外の論文を中心に状況を調査し、有識者WGにて調査報告をレビュー、強度基準および強度評価方法を検討している。強度基準となる評価項目を明確化し、強度基準および評価方法の確立を目指している。

(c) 情報漏えい対策型の生体認証サービスの運用ガイドラインの研究開発

海外・国内の生体認証サービスについての事例や標準化動向を文献で動向を調査するとともに、上記システム要件、生体認証サービスに要求される運用時のセキュリティ要件について、有識者WGにて整理し、「情報漏えい対策型の生体認証サービスの運用ガイドライン」をまとめている。

**詳細の入手方法（関連部署名及びその連絡先）**

株式会社日立製作所 セキュリティ・トレーサビリティ事業部 セキュリティソリューション本部
中西 潤、山田 知明
Tel:044-549-1214 Fax:044-549-1382

**将来の方向性**

上記のような、対症療法的ではなく根本的な生体認証システム上の問題である「生涯不変な特徴の漏えい」に対して、解決に資する技術（キャンセラブル）および、その運用指針を確立することで、安全・安心な生体認証サービスを社会に提供することが可能となる。

**対象技術** その他認証技術等

**テーマ名** 生体認証サービスにおける情報漏えい対策（キャンセラブルバイオメトリクス）の研究開発

**開発年度** 平成20年度～

**実施主体** 株式会社日立製作所（経済産業省からの委託）

**背景、目的**

現在、情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威が急速に変化・拡大しており、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。そこで「新世代情報セキュリティ研究開発事業」では、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を実施することを目指している。

本事業では、漏えいが許されない情報の一つである指紋や静脈、虹彩などのバイオメトリクス情報の安全な利活用の実現を目的として、生体特徴情報を無効化するキャンセラブルバイオメトリクス技術を生体認証サービスプロバイダに適用した場合の管理・運用の在り方について調査・研究を実施し、強度評価手法と、運用ガイドラインの作成を進めている。

**研究開発状況（概要）**

(a) 情報漏えい対策型の生体認証サービスフレームワークの研究開発

一般利用者への提供を想定した生体認証サービスシステムの運用モデルを検討し、リスク分析評価を行い、システム要件を明確にしている。さらに、実証実験に向けてサービスシステムのシステム設計および試作を進めている。この実証実験の結果をフィードバックし、情報漏えい対策型の生体認証サービスフレームワークの確立を目指している。

(b) 情報漏えい対策技術の強度評価に関する研究開発

情報漏えい対策技術の強度評価について、国内・海外の論文を中心に状況を調査し、有識者WGにて調査報告をレビュー、強度基準および強度評価方法を検討している。強度基準となる評価項目を明確化し、強度基準および評価方法の確立を目指している。

(c) 情報漏えい対策型の生体認証サービスの運用ガイドラインの研究開発

海外・国内の生体認証サービスについての事例や標準化動向を文献で動向を調査するとともに、上記システム要件、生体認証サービスに要求される運用時のセキュリティ要件について、有識者WGにて整理し、「情報漏えい対策型の生体認証サービスの運用ガイドライン」をまとめている。

**詳細の入手方法（関連部署名及びその連絡先）**

株式会社日立製作所 ｾｷｭﾘﾃｨ・ﾄﾚｰｻﾋﾞﾘﾃｨ事業部 ｾｷｭﾘﾃｨｿﾘｭｰｼｮﾝ本部
中西 潤、山田 知明 Tel:044-549-1214 Fax:044-549-1382

**将来の方向性**

上記のような、対症療法的ではなく根本的な生体認証システム上の問題である「生涯不変な特徴の漏えい」に対して、解決に資する技術（キャンセラブル）および、その運用指針を確立することで、安全・安心な生体認証サービスを社会に提供することが可能となる。

**対象技術** 認証技術

**テーマ名** 高信頼性端末の電子認証基盤の調査研究

**開発年度** 平成17年度～平成19年度

**実施主体** 社団法人日本画像情報マネジメント協会（経済産業省からの委託）

**背景、目的**

現在、情報通信ネットワークを介したさまざまなサービスが利用可能となり利便性は大きく向上している一方、ネット・バンク等に利用されるパーソナルコンピュータ(PC)等、特定の端末を標的とした図利目的でのセキュリティ上の攻撃も増加している。また、通常のセキュリティ・ホールを悪用した攻撃等に加え、OSの起動時に、利用者に気づかれずに動作するマルウェア（ルートキット等のソフトウェア）の使用など、新たな脅威も増している。

本事業では、こうした現状を踏まえ、国際的な業界団体TCG(Trusted Computing Group)が提唱する強い耐タンパ性を持つTPM(Trusted Platform Module(*))を搭載したPCに注目し、安全性確保の観点からTPM搭載PCを活用するためのガイドラインを作成する。

その際、国際的な整合性と相互運用性に留意しつつ、TPM搭載PCのソフトウェアの設定等を遠隔で管理することを可能とする構成検証プロトコルを作成するとともに、TPM搭載PCを利用して医療情報等の情報資産を取扱う実証的調査も行う。

*TPM（Trusted Platform Module）耐タンパ性の高機能セキュリティチップ

**研究開発状況（概要）**

（ガイドラインの策定）

信頼できるコンピューティング環境を構築する業界団体TCG（Trusted Computing Group）が策定するTPMに関する業界標準について調査研究を行い、各種デバイスのセキュリティ・アーキテクチャに係るガイドラインを、医療分野を事例として作成した。

（通信仕様の試験実装及び実証）

モジュール構成証明(Attestation)を行うネットワークプロトコルであるTNC(Trusted Network Connect)仕様に基づいた試験実装と実証を実施した成果を踏まえ、TPMを搭載したPCにおける情報資産の重要性に応じた運用管理マニュアルを作成した。

**詳細の入手方法（関連部署名及びその連絡先）**

〒101-0032

東京都千代田区岩本町2－1－3和光ビル7階

社団法人日本画像情報マネジメント協会

電話番号：03-5821-7351

URL：http://www.jiima.or.jp

**将来の方向性**

TPMを搭載したPC間でモジュール構成証明を行うTNC(Trusted Network Connect)仕様に基づいた試験実装並びに運用管理マニュアル等の成果は、今後、TCG及びIETFにおける同仕様の国際標準策定作業に向けた提案をするとともに、先導的な事例として同仕様の普及の促進に貢献すると期待される。

**対象技術** その他認証技術等

**テーマ名** 情報漏えいに堅牢な認証･データ管理方式とそのソフトウェアによる安全な実装･検証手法に関する研究開発

**開発年度** 平成17～19年度

**実施主体** 独立行政法人産業技術総合研究所（経済産業省からの委託）

**背景、目的**

情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威は急速に変化･拡大していることから、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を行っていくことが極めて重要となっている。そこで本研究開発では、このような根本的な問題解決を目指した研究開発を実施することを目的とし、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術であって、情報セキュリティ総合戦略に掲げられている「高回復力･被害局限化の確保」及び「高信頼性」のための基盤強化に資する研究開発を実施する。具体的には「事故は起こりうるもの」との前提に立ち、仮に情報の一部が漏洩したりシステムの一部に脆弱性が存在したとしてもある程度の安全性を確保するための技術（フェールセーフなセキュリティ技術）に関する研究開発を、方式の設計から実装にいたるまでの各工程を見直すことにより行う。それによりビジネス継続性や人災を含む災害復旧能力の向上に貢献する。

**研究開発状況（概要）**

平成19年度までに、以下のような特徴を持つ認証･データ管理方式のプロトタイプ実装を行いアイデアが実現可能であることを示した。1）不正アクセスにより記録情報が漏えいしたり、認証トークンや携帯端末などが盗まれたりしたとしても、それらから、保存されている平文やパスワードを求めることが困難。2）一つのノードがクラッシュしたとしても保存データの復元が可能。3）フィッシング詐欺などにより入力パスワードが取られたとしても利用者へのなりすましが困難。また、実行時に攻撃によりウィルス等の不正コードを実行させられることを防ぐ安全性検証･保証機能付きC言語コンパイラFail-Safe Cについて、実用プログラムを処理できる処理系を完成させ、ホームページ上で一般に公開した。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人産業技術総合研究所 情報セキュリティ研究センター

電話：03-5298-4722　　Web: http://www.rcis.aist.go.jp/

**将来の方向性**

上記のような、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術を確立することで、安全･安心な社会の構築を実現する。本事業で開発した技術については、継続的に開発維持を行い、実用に供していく。

**対象技術** その他認証技術等

**テーマ名** ユビキタスネットワーク向けセキュアアセットコントロール技術の研究開発

**開発年度** 平成17年度～平成19年度

**実施主体** 独立行政法人産業技術総合研究所（経済産業省からの委託）

情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威は急速に変化・拡大していることから、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を行っていくことが極めて重要となっている。そこで本研究開発では、このような根本的な問題解決を目指した研究開発を実施することを目的とし、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術であって、情報セキュリティ総合戦略に掲げられている「高回復力・被害局限化の確保」及び「高信頼性」のための基盤強化に資する研究開発を実施する。ユビキタスネットワークの進展に伴い国民生活の至るところに情報デバイスが浸透し，これらを使った新しい便利なサービスが次々に開発されつつあり，これらのサービスの発展が今後の日本の国際競争力を高めると期待されている．しかし，現状では利便性とスピードを優先するあまり，莫大な量に及ぶ個人のプライバシー情報と機密情報をデバイス等を通じて獲得するにもかかわらず，提供するユビキタスサービス自体の不正利用者に対する安全性や利用者のプライバシーや機密に関わる情報管理は必ずしも重視されていない．

そこで本事業では，産業技術総合研究所がこれまでに蓄積している暗号／認証技術，脆弱性検証技術，不正利用者追跡技術などに関する最新の理論的な知見を生かし，ユビキタスネットワーク関連分野のリーディング企業がとパートナーシップを組むことにより，次世代の信頼性の高いユビキタスネットワークを構築する基盤技術の確立を目指す．

**研究開発状況（概要）**

匿名認証と匿名情報連携、不正利用者追跡、脆弱性検証等の想定される課題について基礎技術開発を行い、プライバシー保護と適切なサービス提供を両立するために必要な、検索内容をも秘匿できる匿名検索技術、ユーザの統計情報のみを収集可能とする匿名通信方式、複数の不正者による結託にも対処できる効率的な不正者追跡法、広く個人認証で用いられているバイオメトリクス認証の悪意ある行為を考慮した安全性指標の定式化、ICカード攻撃技術の限界の調査、その結果を用いた攻撃のモデル化を行った。さらにこれらの成果に基づき、リーディング企業とのパートナーシップの下、インフラ協調セーフティシステムを実現するための、耐タンパー技術を応用した情報信頼性確保技術開発を行った。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人産業技術総合研究所 情報セキュリティ研究センター

電話：03-5298-4722　　Web: http://www.rcis.aist.go.jp/

**将来の方向性**

対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術を確立することで、より高次元で安全・安心を実現可能とする社会基盤となっていく。

(別添 2)

| | |
|---|---|
| 企業名（及び略称） 株式会社カオスウェア | |
| 代表者氏名　　梅野　健 | |
| 所在地（郵便番号及び住所）〒184-8795 東京都小金井市貫井北町４－２－１ | |
| 関連部署名及び電話番号　研究開発部　TEL: 042-359-6299 | |
| ＵＲＬ　http://www.chaosware.com/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術<br>２００８年 | Web上で、文書、ファイルを公開鍵等を用いて暗号化送信するサービス「暗号便」http://www.angobin.jp/ 上において、SSLで接続されたWeb上の操作で，暗号化用の公開鍵とは別に、電子署名用の公開鍵と秘密鍵にアクセスし電子署名を行う“署名Web”という、Web上で、送信者、送信内容、送信日時の真正性を証明し、フィッシング詐欺等を防ぐ認証技術を開発し、2008年10月10日からサービス提供した。開発期間は1年である。この電子署名がQRコードとしても表示されるので、携帯電話を用いて、何処でも、何時でも、ユビキタスに電子署名の付与･検証ができる様になっている。 |

| | |
|---|---|
| 企業名（及び略称） 株式会社マインドトップ | |
| 代表者氏名　　荒牧　晴彦 | |
| 所在地（郵便番号及び住所）<br>〒101-0021 東京都千代田区外神田6-15-9明治安田生命末広町ビル8F | |
| 関連部署名及び電話番号　ITソリューション事業部　０３－５８０７－２３３５ | |
| ＵＲＬ　http://www/mindtop.co.jp | |
| 対象技術 | 技術開発状況 |
| その他認証技術等<br>２００８年開発 | OSとアプリケーションとの通信に割り込んで、本人認証を行う技術。生体認証（指紋認証）との連携により、本人を確実に特定する認証基盤。<br>本技術の最大の特徴は、既存のWindowsアプリケーションやWebアプリケーションの画面表示やボタンクリックなどのイベントをフックして、各種の認証処理等のアクセス制御を差し込めることです。これにより、エンドユーザが利用中の各種アプリケーションの起動や重要な画面の操作・処理を、特定の操作者に限定して他者から保護することができます。<br>また、指紋センサやICカードリーダライタなどの周辺装置との連携も付属しており、より強固な本人特定が可能です。 |

(別添3)

[大学]

| 大学名　岡山大学 | |
|---|---|
| 所在地（郵便番号及び住所）　〒700-8530　岡山県岡山市津島中1-1-1 | |
| 関連部署名及び電話番号　総合情報基盤センター/086-251-7231 | |
| URL　http://www.okayama-u.ac.jp/user/cc/ | |
| 対象技術 | 技術開発状況 |
| データ | 大学などの組織においてLANアクセス環境を提供する場合、特に学会などのイベント開催時には組織内利用者とそれ以外の利用者(部外者)が混在して利用することが多い。このような場合、部外者でも組織内限定サービスを利用できるなどの問題が生じる。この問題に対して、本システムでは、部外者からの組織内限定サービスへのアクセス保護を、管理コストを増加させずに可能にする。すなわち、部外者が組織内限定サービスへアクセスした場合でも、サーバ側での設定に基づいたアクセス制御を行うことが可能である。また、本システムは既存の組織内ネットワークを利用するため、LANアクセス環境の提供が場所によらず容易に行えるという特徴を持つ。 |

| 大学名　信州大学　大学院　工学系研究科　セキュリティ学講座 | |
|---|---|
| 所在地（郵便番号及び住所）　〒380-8553　長野県長野市若里4-17-1 | |
| 関連部署名及び電話番号　信州大学　工学部/026-269-5476 | |
| URL　http://security.cs.shinshu-u.ac.jp/ | |
| 対象技術 | 技術開発状況 |
| ネットワーク<br>サーバ<br>通信情報 | 現在、インターネット等におけるセキュアな通信の確保には、VPNを用いた暗号通信路が一般的である。しかし、VPNは装置を対向で利用することが前提であるため、データベースセンター側のVPN装置に障害が発生した場合、そのVPNを経由する全ての通信が途絶してしまう問題がある。更にVPNは接続する2点間に1つの暗号通信路を作り、全ての通信がこの通信路を共有する為、同じ暗号通信路を使う他の通信の傍受が容易である他、端末の操作者に応じてサービスを制限する事が出来ない等の問題がある。そこで、操作者の権利に応じて限定されたサービスを行う個別の暗号通信路を動的に確保するシステム（PCC:Private　Certificated　Connection）を新たに開発した。また、PCCにおける、個人認証をベースとして個別暗号通信路を開設するプロトコルの開発を行い、動的経路制御技術と併せてPCCを完成させた。また、プロトコルのシミュレーションと性能評価を実施した。要素技術として、動的な経路確保と認証局に関する技術開発で得られた要素技術を組み合わせ、個人認証をベースとしたアプリケーション単位での暗号化通信路の確保に関する技術開発を行った。さらに、RSA公開鍵暗号方式を用いた個人認証をベースに、アプリケーション対アプリケーションで利用される個別の暗号化通信路を、通信要求に応じて動的に開設・経路制御するプロトコルの実装を行った。この暗号化通信路の開設要求に対し、操作者の権利に応じてその開設を制御するために個人認証局の開発も行った。 |

| 大学名　東京工業大学　学術国際情報センター | |
|---|---|
| 所在地（郵便番号及び住所）　〒152-8550　東京都目黒区大岡山2-12-1 | |
| 関連部署名及び電話番号　研究情報部情報基盤課/03-5734-3962 | |
| URL　http://www.gsic.titech.ac.jp/ | |
| 対象技術 | 技術開発状況 |
| ネットワーク<br>サーバ<br>通信情報<br>データ | ICカード身分証を用いたPKIクライアント認証とウェブシングルサインオンシステムを組み合わせ、さまざまなウェブアプリケーションにセキュアかつ効率的に誘導するシステム。特徴としては、ICカードリーダがない環境で補助的に利用するマトリクスコード認証機構を設けたこと、また、運用管理の負荷に関して考慮したことが挙げられる。 |

| 大学名　武蔵工業大学 | |
|---|---|
| 所在地（郵便番号及び住所）　〒158-8557　東京都世田谷区玉堤1-28-1 | |
| 関連部署名及び電話番号　情報処理センター/03-3703-3111 | |
| URL　http://www.musashi-tech.ac.jp/ | |
| 対象技術 | 技術開発状況 |
| ネットワーク | AIPSは認証ネットワークシステムの一種で、IPヘッダに認証情報を埋め込むことでアクセス制御を実現している。クライアントにはWindows XPとLinuxが対応しており、ソフトウェアをインストールする必要がある。サーバはLinuxで、ゲートウェイとして機能する。特別な機器を必要とせず、一般的なハブなどの環境でも使用可能なため、低コストでの認証ネットワークを実現できる。 |

【企業】

| 事業体(研究所)名　株式会社ディー・ディー・エス | |
|---|---|
| 所在地（郵便番号及び住所）　〒450-0003　愛知県名古屋市中村区名駅南1-27-2<br>日本生命笹島ビル16F | |
| 関連部署及び電話番号　開発本部/052-533-1110 | |
| URL　http://www.dds.co.jp/ | |
| 対象技術 | 技術開発状況 |
| クライアント（PC等）<br>施設 | EVE-MAは、ActiveDirectoryを中心とした大規模ユーザ環境における認証基盤の役割を果たすソフトウェアである。認証手段をプラグインとして追加できる構造を持ち、例えばパスワード等の知識に基づく認証、指紋に代表される生体情報による認証、FeliCa等のICカードを用いた所有物による認証を、アクセス先に応じた条件で組み合わせて認証できる特徴を持つ。認証の実行はサーバ側に集約し、証明書ベースのサーバ・クライアント間の相互認証に基づいた認可を行う等、セキュリティを強く意識した構成としている。なお、通信及び内部で用いる暗号については、電子政府推奨暗号リストに記載された暗号を全面的に採用している。 |

| 事業体(研究所)名　東北インフォメーション・システムズ株式会社 | |
|---|---|
| 所在地（郵便番号及び住所）　〒980-0021　宮城県仙台市青葉区中央2-9-10 | |
| 関連部署及び電話番号　経営企画室/022-799-5555 | |
| URL　http://www.toinx.co.jp/ | |
| 対象技術 | 技術開発状況 |
| | PKIを活用した暗号化技術により、セキュリティを確保すると同時に、インターネットの向こう側の取引相手が誰であるかを当社が証明するサービス。平成14年12月に「特定認証業務の認定」を取得し、電子認証用ICカードの販売の他、様々なソリューションを提供している。 |

| 事業体(研究所)名　株式会社ブロードバンドタワー | |
|---|---|
| 所在地（郵便番号及び住所）　〒107-0052　東京都港区赤坂4-2-6<br>住友不動産新赤坂ビル7F | |
| 関連部署及び電話番号　人事総務部/03-5573-8181(代表) | |
| URL　http://www.bbtower.co.jp/ | |
| 対象技術 | 技術開発状況 |
| ネットワーク | 1. 既存サイト全域へのサービス提供<br>2. 高いサービスへの継続性を確保<br>3. 接続条件に依存しないサービス<br>4. 短納期、およびスポット対応の実現<br>＊詳細はURL参照 |

| 事業体(研究所)名　三井情報株式会社 | |
|---|---|
| 所在地（郵便番号及び住所）　〒105-6215　東京都港区愛宕2-5-1<br>愛宕グリーンヒルズMORIタワー | |
| 関連部署及び電話番号　事業開発本部　エンジニアリング部/03-6376-1040 | |
| URL　http://www.mki.co.jp/ | |
| 対象技術 | 技術開発状況 |
| ネットワーク<br>サーバ | サービスの提供から記録までの流れを、認証（Authentication）、承認（Authorization）、アカウンティング（Accounting）の3つの段階に分けて提供するAAA（Authentication、Authentication、Authorization）モデルアーキテクチャーをベースとしたRADIUS（Remote Authentication Dial In User Service）プロトコルを実装したサーバ・ソフトウェア・シリーズです。また、ワンタイム・パスワード認証機能のサポートやローミング機能などを始めとする各種拡張機能を備え、Windows版では、ODBCサポートによるリレーショナルデータベースとの連携（アカウンティング出力）も可能です。ユーザ・アクティビティの容易な分析（アカウントログの多様な出力形式）や、正確な課金情報の収集等、現在の市場ニーズにも対応したRADIUSサーバ・管理ソフトウェアです。IEEE802.1xとEAPを用いたよりセキュアなネットワーク環境の構築を行うサーバ・ソフトウェア・パッケージも提供しています。 |