

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。

[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](#)

[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](#)

[マルウェア対策ユーザサポートシステムの研究開発](#)

[証明可能な安全性をもつキャンセルブル・バイOMETRICS認証技術の構築とそれを利用した個人認証インフラストラクチャ実現に向けた研究開発](#)

[生体認証サービスにおける情報漏えい対策\(キャンセルブルバイOMETRICS\)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21年12月8日から12月28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。

[タレスジャパン株式会社](#)

[大日本印刷株式会社](#)

[デュアキシズ株式会社](#)

(2) 調査

警察庁が平成21年10月から平成21年11月にかけて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

[信州大学](#)
[東京都市大学](#)
[静岡大学](#)

イ 企業

[株式会社コア](#)
[三和コムテック株式会社](#)
[メディアファイブ株式会社](#)
[GMOインターネット株式会社](#)
[株式会社福山コンサルタント](#)

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、店頭公開企業及び未上場企業から無作為に抽出

(別添1)

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、(株)KDDI研究所、パナソニック 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	<p>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。</p> <p>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。</p>
研究開発状況(概要)	<ul style="list-style-type: none">・平成17年度から以下の研究開発を実施中<ul style="list-style-type: none">(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 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	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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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、その認証に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。</p>
研究開発状況(概要)	<ul style="list-style-type: none"> ・平成18年度より以下の研究開発を実施。 <ol style="list-style-type: none"> (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。
詳細の入手方法(関連部署名及びその連絡先)	<p>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 電話 042-327-6011</p>
将来の方向性	<p>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。(実証実験においては、特に、医療分野でのネットワーク利用におけるセキュリティ確保、利便性向上に効果があることが分かっている。)</p>

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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
研究開発状況(概要)	<ul style="list-style-type: none"> ・平成19年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> (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)	<p>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</p>
将来の方向性	<p>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。</p>

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	<p>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に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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> ・次世代ハッシュ関数 <ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> ・平成19年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> (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)	<p>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</p>
将来の方向性	<p>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。</p>

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	<p>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。</p> <p>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。</p> <p>他方、複数の異なる暗号要素技術を組み合わせるシステム等では、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。</p> <p>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らなず、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。</p> <p>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。</p> <p>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るシステム等での強度バランスを明確にする</p>
研究開発状況(概要)	<ul style="list-style-type: none"> ・平成19年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> (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)	<p>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</p>
将来の方向性	<p>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。</p>

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	<p>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の見間違い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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
研究開発状況(概要)	<ul style="list-style-type: none"> ・平成20年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> (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)	<p>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/itakukenyu.htm) 電話 042-327-6011</p>
将来の方向性	<p>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。</p>

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	<p>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。</p> <p>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。</p>
研究開発状況（概要）	<p>平成21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、マルウェアの収集機構・収集したマルウェアの分析機構に関して、日本全国規模の観測網構築に向けた観測対象ネットワークの更なる拡充、より高度な観測アーキテクチャ・攻撃検出機構の開発、マルウェアの分析精度の高度化を行った。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し、実運用に向け開発を進めた。</p> <p>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について更に高速化が可能なアルゴリズムを開発し、その有効性を検証した。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技術を開発し、逐次解析器による再現フローの自動化とデータ蓄積を開始した。また海外研究機関と連携し、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を進めた。</p>
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	その他認証技術
テーマ名	マルウェア対策ユーザサポートシステムの研究開発
開発年度	平成21年度～平成23年度
実施主体	株式会社日立製作所、KDDI株式会社
背景、目的	<p>本研究開発では、ユーザパソコンに負荷がかかる実行コードの解析をnicter等の解析機能を有する外部のシステムが担うことにより、効率的なマルウェアの検出および自動駆除の仕組みを実現することを目的とする。</p> <p>ユーザにおけるマルウェア対策として一般的なものは、セキュリティベンダ等が提供している、シグネチャ（マルウェア検査パターン）に基づくアンチウィルスソフトである。</p> <p>アンチウィルスソフトでは、シグネチャを採用しているため、既知のマルウェアに対しては十分対応できるが、未知のマルウェアや、一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードに対しては、現状十分に対応できていない。</p> <p>また、新しいマルウェアが現出した場合、セキュリティベンダ等が対応するパターンファイルを更新するまでに一定の時間を要するため、ユーザが必要なときに、必要なものをタイムリーに入手できるところまでには至っていない。</p> <p>その他にも、総務省、経済産業省の連携プロジェクトとして設置されたサイバークリーンセンター（CCC）において、ボット対策の一環として、ユーザ向けに、駆除ツール（CCCクリーナー）が提供されている。このような駆除ツール（CCCクリーナー）についても、既に感染行動が見られるボットや既知のボットのみを取り扱っており、アンチウィルスソフトと同様な問題が見受けられる。</p> <p>また、情報処理推進機構（IPA）では、ウィルス情報iPedia（ウィルス情報データベース）において、届出されたウィルスやボットなどを中心に、それらの主な動作内容や対処法などの解析結果を公開している。</p> <p>コード難読化やコード自己変貌化に代表されるように、昨今、マルウェアの高度化・巧妙化が進展する中で、上述のように未知のマルウェアや一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードのように、アンチウィルスソフトによる対応では十分カバーし切れない領域が存在している。</p> <p>セキュリティベンダ等による取り組みを補完しつつ、そのような未知のマルウェアも対応できるように、検体の解析に基づくマルウェア判定をベースとした駆除ツールを、実時間に近い形でユーザに提供していくことが必要になってきている。</p>
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成21年度より以下の研究開発を実施中。 （1）ユーザパソコンへの負荷をかけず、実行コードがマルウェアかどうかをユーザサポートセンターで解析するとともに、マルウェアを駆除するツールを自動的に提供するフレームワークを確立する。 （2）ユーザのパソコン上で検査プログラムを実行してから、ユーザに対して駆除ツールが提供されるまでの一連の手続きが10分程度で完了することを実現する。
詳細の入手方法（関連部署名及びその連絡先）	<p>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</p>
将来の方向性	<p>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。</p>

対象技術 その他認証技術等
テーマ名 証明可能な安全性をもつキャンセラブル・バイオメトリクス認証技術の構築とそれを利用した個人認証インフラストラクチャ実現に向けた研究開発
開発年度 平成20年度～平成21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）
<p>背景、目的</p> <p>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。</p> <p>本事業では、生体情報が自由に取り換えのできない情報であることに起因する生体認証特有の脆弱性を解決するために、テンプレート保護技術と更新可能なバイオメトリクス認証の安全性評価について研究する。すでに、キャンセラブル・バイオメトリクスやバイオメトリック暗号と呼ばれる技術の枠組みの中で、これらの問題を解決するための様々な手法が提案されているが、明確な安全性の基準が存在せず、真に実用的な技術が生まれていない。よって、本事業では、安全性評価基準の理論的な枠組みの構築、証明可能な安全性をもつ生体認証技術の研究開発を主たる目的とする。また、各モダリティに対する認証プロトコルの開発や安全性に対する実験、開発したプロトコルの実装も併せて行う。</p>
<p>研究開発状況（概要）</p> <p>平成 20 年度より以下の研究開発を行っており、平成 21 年度末に開発終了予定である。</p> <p>(1) 安全性評価基準の理論的枠組みの構築</p> <p>(2) 証明可能な安全性をもつキャンセラブル認証技術の研究開発</p> <p>(1)、(2)において、暗号理論的なアプローチを用いて安全性の定式化を行うとともに、汎用性の高い安全な認証プロトコルの開発を行っている。</p> <p>(3) 各モダリティのアルゴリズム調査、解析と応用手法の研究開発</p> <p>各モダリティに対して、モダリティの特徴を生かした認証プロトコルの開発や、なりすまし攻撃に対する安全性評価実験などを行っている。</p> <p>(4) バイオメトリクス認証を組んだID連携認証技術のプロトタイプ構築</p> <p>(1)、(2)で開発した認証プロトコルのテスト実装として、開発プロトコルを組み込んだID連携システムのプロトタイプを構築する。</p>
<p>詳細の入手方法（関連部署名及びその連絡先）</p> <p>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</p> <p>電話：03-5298-4722 Web：http://www.rcis.aist.go.jp/</p>
<p>将来の方向性</p> <p>本人確認のための重要な基盤技術となりつつある生体認証システムの安全性評価基準や評価体制を確立することで、より安全で安心な社会の実現に貢献していく。</p>

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（キャンセル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）
<p>背景、目的</p> <p>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。</p> <p>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ル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。</p>
<p>研究開発状況（概要）</p> <p>(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</p> <p>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。また、情報漏えい対策型の技術（キャンセルラブルバイオメトリクス）を適用した場合と、従来型とを比較し、情報漏えい対策型の生体認証サービスフレームワークを確立している。さらに、本フレームワークに基づいた、情報漏えい対策型の生体認証サービスシステムに対するプライバシー影響評価を行っている。</p> <p>(b) 情報漏えい対策技術の強度評価に関する研究開発</p> <p>情報漏えい対策技術の強度について調査し、有識者WGにてレビューを実施し、強度基準および強度評価方法を検討している。これにより、上記のサービスフレームワークに対す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。</p> <p>(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</p> <p>海外・国内の生体認証サービスの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、実証システムによるガイドラインの有効性実証・フィードバックを行いながら、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。</p>
<p>詳細の入手方法（関連部署名及びその連絡先）</p> <p>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）</p>

将来の方向性

上記のような、対症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（キャンセルブル）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。

(別添2)

企業名(及び略称) タレスジャパン株式会社	
代表者氏名 ミッシェル テオヴァル	
所在地(郵便番号及び住所) 〒107-0052 東京都港区赤坂4丁目9番9号 赤坂MKビル4階	
関連部署名及び電話番号 インフォメーションシステムセキュリティー 03-5785-1975	
URL http://www.thalesgroup.com/	
対象技術	技術開発状況
その他認証技術等	<p>耐タンパー性のハードウェアセキュリティーモジュール(HSM)上で暗号秘密鍵だけでなく企業および政府機関独自の認証アルゴリズム保護実行することで、コンピュータウイルス感染や内部犯等による組織内ネットワークからの機密識別情報の漏洩や認証アルゴリズムの改ざんを防止することができます。</p> <p>この技術を既存のパスワード認証基盤や生体認証基盤に実装することで電子化された機密識別情報のエンド・ツー・エンドによる暗号化認証が可能となり強固な認証基盤が構築できます。認証処理中でもサーバー上のメモリやファイルシステムおよび認証データベース上において機密情報が平文で漏洩することを防ぎます。</p>

企業名(及び略称) 大日本印刷株式会社	
代表者氏名 代表取締役社長 北島 義俊	
所在地(郵便番号及び住所) 〒162-8001 東京都新宿区市谷加賀町一丁目1番1号	
関連部署名及び電話番号 I P S 事業部 セキュリティソリューション営業部	
URL http://www.dnp.co.jp/bf/ss/	
対象技術	技術開発状況
その他認証技術等 (2009年)	<p>【USBシンクライアント】</p> <p>専用USBデバイスをPCのUSBポートに挿入し、PCを起動することにより、そのPCをシンクライアント端末として利用できる。システムはUSBデバイス、認証用サーバ、業務用サーバで構成され、データ保存はサーバのみ可能で、PCのHDDや外部記憶装置への保存は不可能となる。USBデバイスには、USBフラッシュメモリのほかに小型のICカードが組み込まれており、フラッシュメモリ内のサーバ接続プログラムの正当性をICカードの電子署名機能により確認している。この手続きを経て、正当性が確認された端末のみ業務用サーバに接続できるため、不正な接続を排除し、企業のネットワークにおいて、高い安全性を確保することが出来る。</p>

企業名（及び略称）大日本印刷株式会社	
代表者氏名 代表取締役社長 北島 義俊	
所在地（郵便番号及び住所）〒162-8001 東京都新宿区市谷加賀町一丁目1番1号	
関連部署名及び電話番号 IPS事業部 セキュリティソリューション営業部	
URL http://www.dnp.co.jp/bf/ss/	
対象技術	技術開発状況
<p>その他認証技術等 (2005年)</p>	<p>【 S S F C 】</p> <p>「Shared Security Formats Cooperation」の略。190社以上の国内の主要な企業が参加している。1枚の非接触ICカードをIDカードとして用いて、セキュリティを向上させることを目的としたアライアンス。</p> <p>SSFC仕様では、ID情報と入室情報などは、共有情報として定義されている。他の同種の仕組みと比較して、SSFCで特徴的なところは、各セキュリティシステムが利用する情報は業界別に割り当てており、業界が同じ場合はその領域を共同利用する点である。現在定義されている業界は、ゲートシステムを中心とした業界、監視カメラ業界、ファニチャー業界、プリンター業界と、少し色合いが異なるがソフト業界もSSFC情報を利用している。</p> <p>最も大きな特徴は、異なる業界のシステムやアプリケーション間でデータ連携が可能となるようSSFCで仕様を策定している点である。</p> <p>この仕組みが仕様として策定されている為、副業の機器を一度に導入することになく、必要な時期に必要なセキュリティ機器を導入すればよいと言うメリットと、連携によるセキュリティの向上と利便性を利用者に提供可能としている。</p> <p>これらの各仕様はアライアンス参加企業にのみ限定して公開されており、物理的セキュリティ(入退室管理、監視カメラなど)とSSFC対応セキュリティ機器利用のための論理的セキュリティを、1枚のIDカードを用いて融合しているだけでなく、福利厚生面等でも利用者の利便性向上を実現している。</p> <p>現在、SSFCアライアンス事務局は大日本印刷株式会社内に設置されている。</p>

企業名（及び略称）大日本印刷株式会社	
代表者氏名 代表取締役社長 北島 義俊	
所在地（郵便番号及び住所）〒162-8001 東京都新宿区市谷加賀町一丁目1番1号	
関連部署名及び電話番号 IPS事業部 セキュリティソリューション営業部	
URL http://www.dnp.co.jp/bf/ss/	
対象技術	技術開発状況
<p>その他認証技術等 (2006年)</p>	<p>【ICカードによるネットワーク管理型PC個人認証】 情報システム利用者の権限情報と認証情報をサーバで集中管理し、PCの不正利用、情報漏洩をシャットアウトする、ICカードを利用したPCセキュリティシステム。SSFC製品との連携も可能。</p> <p>クライアント機能 ICカードログオン認証/スクリーンロック、外部記憶デバイス利用制御、電子証明書(PKI)の利用、SSFC連携機能(ICカードの入室情報チェック)、操作ログ送信、など。</p> <p>管理サーバ機能 ユーザ認証情報、ポリシーをサーバにて一括管理</p> <p>管理者機能 PINロック時やカード紛失時など、ユーザに対する緊急サポートをWeb上から容易に行うことが可能。</p>

企業名（及び略称）大日本印刷株式会社	
代表者氏名 代表取締役社長 北島 義俊	
所在地（郵便番号及び住所）〒162-8001 東京都新宿区市谷加賀町一丁目1番1号	
関連部署名及び電話番号 IPS事業部 セキュリティソリューション営業部	
URL http://www.dnp.co.jp/bf/ss/	
対象技術	技術開発状況
<p>その他認証技術等 (1999年,2009年)</p>	<p>【ICカード用PKIドライバ】</p> <p>ICカード内に格納された電子証明書や秘密鍵とブラウザ等の上位アプリケーションソフトとのI/F機能を提供するドライバソフトウェアで、各社の認証アプリケーションの部品として利用されている。</p> <p>CSP(1)とPKCS#11規格に対応している。</p> <p>また新たに、異なるカードベンダーが提供するICカードとPKI(2)でも、相互利用が可能なPKIアプリケーション規格「JIS X 6320-15」に準拠したICカードとPKIドライバ(Windows,Linux)の提供を2009年12月より開始した。</p> <p>(1)</p> <p>CSPドライバは、Microsot社が定めた暗号ライブラリの規格である『CryptoAPI』に準拠しており、WebブラウザのInternet ExplorerやメールのOutlook ExpressやWindowsメールがこれをサポートしています。</p> <p>(2)</p> <p>PKI(公開鍵暗号認証基盤;Public Key Infrastructure)とは、公開鍵暗号方式を用いて暗号化、デジタル署名、認証などを行うセキュリティインフラ。信頼できる認証局が電子証明書を発行して公開鍵の名義人を証明する。</p>

企業名（及び略称）デュアキシズ株式会社	
代表者氏名 名古屋 貢	
所在地（郵便番号及び住所）〒103-0015 東京都中央区箱崎1 - 2 日本総合地所サンワールドビル2F	
関連部署名及び電話番号 開発部 050-5808-4021	
URL http://www.duaxes.co.jp/	
対象技術	技術開発状況
その他認証技術等	<p>通信データ中のヘッダからデータ部分までをハードウェアでチェックできる高速回路の開発を行っている。ハードウェア処理するため、1Gbpsや10Gbps、さらに高速な40Gbpsや100Gbpsの処理速度に対応することが可能な王である。この回路で、通信データの監視やユーザ毎の認証機能を実現することが可能である。</p> <p>本技術は通信機器のプラットフォーム技術であり、多数の特許を包括的に取得済みである。出願件数を含めると、関連特許は300件近くに及んでいる。開発年は2004年である。</p> <p>本技術を用いた製品開発も行っている。主な用途としてURLフィルタリング装置やメールフィルタリング装置、帯域制御装置などであり、既に、これらの装置を販売している。</p>

(別添3)

【大学】

大学名 信州大学工学部	
所在地(郵便番号及び住所) 〒380-8553 長野市若里四丁目17番1号	
関連部署及び電話番号 総務グループ 庶務係 / 026-269-5004	
URL http://www.eng.cs.shinshu-u.ac.jp/	
対象技術	技術の概要・特徴など
その他	「いつ、どこで、だれが」印刷するのを、印刷物受取人と印刷が許可されたプリンタによるPKI処理により制御するプリンティングシステムを研究し、これを塩尻市役所の業務で評価。

大学名 東京都市大学 情報処理センター研究室	
所在地(郵便番号及び住所) 〒158-8557 世田谷区玉堤1-28-1	
関連部署及び電話番号	
URL	
対象技術	技術の概要・特徴など
ネットワーク	IPパケットごとに認証情報をうめ込むことでパケット単位での認証を可能とするシステム。

大学名 静岡大学 情報基盤センター	
所在地(郵便番号及び住所) 〒422-8529 静岡市駿河区大谷836	
関連部署及び電話番号 情報基盤センター / 054-238-4683	
URL http://www.ipc.shizuoka.ac.jp/icenter/	
対象技術	技術の概要・特徴など
ネットワーク サーバ クライアント 通信情報 データ	大学の教員、学生の教育研究業務全般における情報リスクを最小にするような情報セキュリティ管理システム(ISMS)を構築し運用中である。 ISO27001を2007年に取得している。

【企業】

事業体(研究所)名 株式会社コア	
所在地(郵便番号及び住所) 〒154-8552 東京都世田谷区三軒茶屋1-22-3	
関連部署及び電話番号 社長室 / 03-3795-5111	
URL http://www.core.co.jp/	
対象技術	技術の概要・特徴など
ネットワーク クライアント 通信情報 その他	ITILver3に準拠し、データセンターからPCプラットフォームまですべてのIT資産の「見える化」とコスト削減を実現します。

事業体(研究所)名 三和コムテック株式会社	
所在地(郵便番号及び住所) 〒106-0032 東京都港区六本木3-4-3 三和ビル	
関連部署及び電話番号 カスタマーサービス企画 / 03-3583-2518	
URL http://www.sct.co.jp/	
対象技術	技術の概要・特徴など
サーバ 通信情報	<ul style="list-style-type: none"> ・ Webサイトを365日診断し、発見された弱点(脆弱性)とその対策を365日お知らせするセキュリティサービス ・ 診断に合格したサイトに証明マークを表示することで安全性を証明 ・ PCI-DSS(ペイメントカード業界データセキュリティ基準)、VISAが定めているAIS/CISP、MasterCardのSDPや、米国連邦政府系機関、また国際的かつ最高水準のセキュリティ基準に準拠・適合 ・ ハッカーが狙う対象となるWebサーバー以外のサーバーや、各種Webアプリケーションも対象とする ・ 診断項目は10,000を超え、ほぼすべてのサイト構成要素を診断対象とする。

事業体(研究所)名 三和コムテック株式会社	
所在地(郵便番号及び住所) 〒106-0032 東京都港区六本木3-4-3 三和ビル	
関連部署及び電話番号 カスタマーサービス企画 / 03-3583-2518	
URL http://www.sct.co.jp/	
対象技術	技術の概要・特徴など
ネットワーク サーバ 通信情報	<p>IBM(AS/400, System I)のセキュリティに特化した製品。</p> <ul style="list-style-type: none"> ・FTP、データ転送、ODBC接続などによる不正ダウンロードを防止 ・重要なファイルのアクセス監視及び変更履歴監視 ・ユーザーの操作履歴を画面で記録(画面遷移の記録) ・ログオンしたまま放置された端末の不正使用を防止 ・不当なパスワードの作成防止 ・不正アクセスログに対するリアルタイム検知(メッセージ送信やアクションを実行) ・ユーザープロファイルの一元管理(一覧表示、変更) ・監査帳票・アクセスログ集計帳票を簡単に作成可

事業体(研究所)名 メディアファイブ株式会社	
所在地(郵便番号及び住所) 〒810-0001 福岡県福岡市中央区天神3丁目14-31 天神リンデンビル2階	
関連部署及び電話番号 092-761-0078	
URL http://www.media5.co.jp/	
対象技術	技術の概要・特徴など
通信情報	<p>キャノンITソリューションズ製のメールフィルタリングソフトを利用し、企業内から送信される電子メールに対して監視を行い、検出された異常内容を提携企業にレポートとして提出するサポート業務。提携企業からの技術面、運用面に関する問い合わせ対応。</p>

事業体(研究所)名 GMOインターネット株式会社	
所在地(郵便番号及び住所) 〒150-8512 東京都渋谷区桜丘町26番-1号 セルリアンタワー	
関連部署及び電話番号 システム本部 / 03-5456-2687	
URL http:// www.gmo.jp/	
対象技術	技術の概要・特徴など
クライアント 通信情報	ASP型のVPNサービス <ul style="list-style-type: none"> ・ファイル共有(セキュア) ・リモートデスクトップで自宅PCの操作 ・Webカメラのチェック

事業体(研究所)名 株式会社福山コンサルタント	
所在地(郵便番号及び住所) 〒812-0013 福岡市博多区博多駅東三丁目6番18号	
関連部署及び電話番号 システム課 / 092-471-0211	
URL http://www.fukuyamaconsul.co.jp/	
対象技術	技術の概要・特徴など
データ	<p>1. 製品概要</p> <p>感熱式指紋センサー</p> <p>現在の多くの機器に採用されている静電式センサーに比べて、強度・耐久性が高く、光学式センサーにくらべて軽量・コンパクトな感熱式センサーを採用。さらに、残留指紋が残らないスワイプ式(センサーに指を滑らせます)。残留指紋からの指紋採取は不可能であり、利用者の心理的不安もありません。</p> <p>指紋はUSBメモリ内の秘匿領域へ保存</p> <p>登録された指紋情報はPC内へは一切保存せず、製品本体に保存されます。</p> <p>この保存領域はPCからは一切アクセス不能な秘匿領域です。また、指紋情報は特徴点をデータ化して保存しているため、指紋情報の不正利用はできません。</p> <p>指紋照合は1秒以内、360度スワイプ対応</p> <p>入力された指紋は、1秒以内に照合されます。高精度認証テクノロジーにより、センサーに対して斜めや180度反対からスキャンを行っても、認証判断が可能です。</p> <p>ドライバーのインストールレス</p> <p>ユーザー権限のPCで使用する際に、専用USBドライバーのインストールが不要です。</p>

ハードウェア暗号化

リムーバブルディスクに書き込まれるデータは、コントローラチップにより自動暗号化されます。

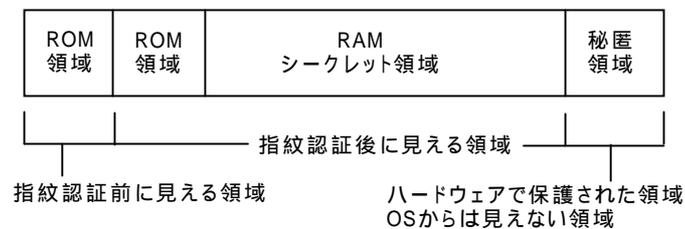
Windowsオートラン機能搭載（サスライト社特許）

BioDataSec2.0はCD-ROM領域とファイルの読み書きができるリムーバブルディスクで構成されています。CD-ROM領域にアプリケーションを格納することにより、指紋認証後にアプリケーションを自動起動することができます。

シンククライアントの起動デバイス対応

CD-ROM領域にLinuxOSを搭載することができます。高価なシンククライアントPCがなくても、既存のPCにBioDataSec2.0を接続することにより、シンククライアント環境を実現することができます。

概念図



2. ハードウェア仕様

対応OS	Windows XP/2000/VISTA
インターフェース	USB2.0
外形寸法(mm) (L x H x W)	102.5 x 11.5 x 24.0 (使用時) 83.5 x 11.5 x 24.0 (持ち運び時)
重量	約19g
消費電力	140mA (最大)
指紋センサ	感熱式スワイプセンサ
動作温度	0 ~ 60
動作湿度	20% ~ 90%
登録指数	10指
FAR (他人誤認率)	0.001%未満
FRR (本人拒否率)	0.1%未満
メモリサイズ	512MB, 2GB