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
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
認証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
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

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22年11月25日から12月27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。

株式会社グローバルワイズ
株式会社ハーモニックセキュリティ

(2)　調査

警察庁が平成22年10月から平成22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

佐賀大学
信州大学
神奈川大学
北海道大学
国士舘大学
奈良先端科学技術大学院大学
岩手大学
東北大学
九州大学

イ　企業

シスメックスＲＡ株式会社
株式会社アクアシステムズ
ＫＤＤＩ株式会社
株式会社メトロ
三菱電機株式会社
株式会社日立ソリューションズ
株式会社シー・エス・イー
ヌリテレコム株式会社
株式会社インテリジェントウェイブ
ログイット株式会社

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、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

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、ウィ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年度から平成21年度にかけて以下の研究開発を実施し、委託研究開発を終了。

(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22年度

標準化を目指した応用研究としてNICTトレーサブルネットワークグループにてCYBEXやDNSSECなどとの連携技術の研究開発を実施。

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、ウィ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　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。
(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。

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検証し、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。

(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。

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FIPS800-5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。
(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。

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年度から次の研究開発を行い、現在、協力先団体にセンサを設置し、実証実験を実施している。

(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

・実環境でシステムの有効性等を評価し、平成22年度末に研究開発を完了する予定である。

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22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ー・攻撃検出機構の開発を進め、マルウェアの分析精度の高度化及び攻撃元のマルウェアをリアルタイムに識別する技術開発を行った。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。

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、従来までの公開鍵暗号を利用した方式に比較して高速化が可能な秘密鍵暗号による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進めた。また海外研究機関と連携し、APIシーケンスを自動分類し、高精度で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。

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

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及び自動駆除の仕組を実現することを目的とする。

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。

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。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。

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。

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。

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。

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。

研究開発状況（概要）

・　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速やかに完了する技術を確立する。

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）

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す。

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。

研究開発状況（概要）

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。

(1) 安全性評価基準の理論的枠組みの構築

(2) 証明可能安全性をもつキャンセラブル認証技術の研究開発

(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た。

(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

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た。

(4) バイオメトリクス認証を組込んだID連携認証技術のプロトタイプの構築

(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

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。

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～平成21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す。

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る。

研究開発状況（概要）

(1) 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

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た。また、情報漏えい対策型の技術（キャンセラブル・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た。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影響評価を行った。

(2) 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た。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を確立した。

(3) 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」をまとめた。

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
（Tel:044-549-1214　Fax:044-549-1382）

将来の方向性

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、上記のように、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。

（別添２）

企業名（及び略称）株式会社グローバルワイズ	
代表者氏名　代表取締役　伊原栄一	
所在地（郵便番号及び住所）愛知県刈谷市若松町2-55-1	
関連部署名及び電話番号　プロダクト事業部 NETMETRIX担当 03-5419-7980	
URL　http://www.g-wise.co.jp/	
対象技術	技術開発状況
侵入検知技術 2004年	同一ネットワーク上に存在する全てのノードに対してパケットを送信し、その応答によりノードの端末情報を収集する技術。 セグメントやV-LAN、WANなどネットワーク構成による制限はない。 事前に端末に管理用ソフトウェアをインストールする必要がないため、未知（未登録）の端末からも情報を取得することができる。 あらかじめ接続許可端末のリストを登録すれば、未許可の端末のネットワーク接続や、ログインユーザの変更など状態の変化を検知する。 【取得情報】 ・ＩＰアドレス ・ＭＡＣアドレス ・コンピュータ名 ・ＯＳ情報（Windows、MACOS、Linuxなど）　他

企業名（及び略称）株式会社ハーモニックセキュリティ	
代表者氏名　代表取締役　國米　仁	
所在地（郵便番号及び住所）〒558-0041　大阪市住吉区南住吉４丁目１２番３２号	
関連部署名及び電話番号　本社　06-6608-6765	
URL　http://www.mneme.co.jp	
対象技術	技術開発状況
その他認証技術 開発年 ２００５年～ ２００８年	故意による機密情報の持ち出しと思われる事件が続発しています。 意図的な持ち出しを防ぐのはなかなか困難ですが、正しくログインできても単独ではデータへのアクセスは許されず、複数の権限ある担当者が全てログインできた場合にのみデータへのアクセスが許される認証権限分散方式を採用すれば事件抑止の一助になります。 当社では認証権限分散機能を持つ『権限分散クリプトニーモ』を発表しています。これは、１０人の登録オペレータの中の任意の３人が共同で作業した場合にのみアクセスが完了する権限分散型本人認証ソフトに、常態では暗号鍵を存在させないデータ暗号化復号機能を付加したものです。データ暗号化機能を切り離して認証権限の分散化機能のみを使用することも可能です。復号後の平文データの持ち出しの可能性は残りますので故意による持ち出しを必ず根絶できるというものではありませんが、監視ソフトや行動抑制ソフトとの連携を適切に行えば故意による持ち出しの抑止に大きく貢献できるものと考えています。 製品概要とＱ＆Ａを以下のサイトに掲載しています。 http://www.mneme.co.jp/neme/img/bunsan.pdf（製品概要） http://www.mneme.co.jp/neme/pdf/qa.pdf（Ｑ＆Ａ）

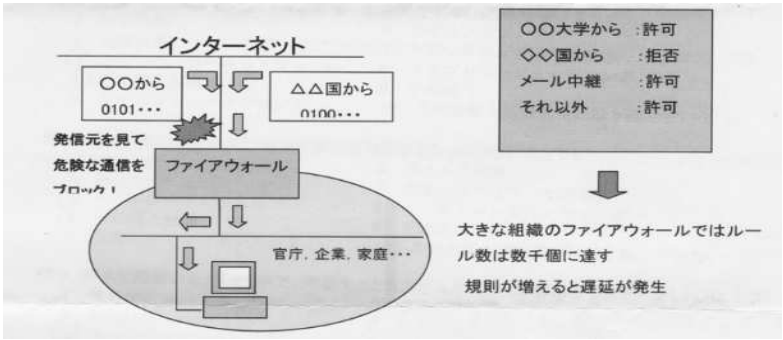
別添３

【大学】

大学名	佐賀大学総合情報基盤センター
所在地	〒840-8502　佐賀市本庄町１
窓口部署名／電話番号	／ 0952-28-8592
ホームページのURL	http://www.cc.saga-u.ac.jp/
対象技術	技術の概要・特徴など
ネットワーク	・無線LANや情報コンセントを利用する際に、利用者を認証するためのシステムです。 ・webによる平易なインターフェースを持ち特別なソフトウェアを導入することなく利用可能です。 ・利用者の認証後、ネットワークが利用でき、利用終了後、即座に閉鎖します。 ・IPv4だけでなく、IPv6にも対応しています。 ・既に10年以上の運用実績があります。

大学名	信州大学
所在地	〒380-8553　長野市若里4－17－1
窓口部署名／電話番号	総務Ｇ（庶務）／ 026-269-5004
ホームページのURL	http://wwweng.cs.shinsh-u.ac.jp
対象技術	技術の概要・特徴など
サーバ 通信情報 データ	PKI処理を高速に実行するアクセラレータ

大学名	信州大学
所在地	〒380-8553　長野市若里4－17－1
窓口部署名／電話番号	総務Ｇ（庶務）／ 026-269-5004
ホームページのURL	http://wwweng.cs.shinsh-u.ac.jp
対象技術	研究開発状況
ネットワーク 通信情報 データ	数多くの質問を用意し、それらを適宜提示して各個人のその人らしさを認証する

大学名	神奈川大学
所在地	〒259-1293　平塚市土屋2946
窓口部署名／電話番号	理学部情報科学科／ 046-359-4111
ホームページのURL	
対象技術	研究開発状況
ネットワーク	パケットフィルタリングは、ネットワークセキュリティを確保する基本的手法である。フィルタ運用の際は、外部に脅威の存在が認められる度にルールが追加されるが、その脅威が除去されたことを確認する手段がないため、ルールは増加の一途を辿る。ルールの増加はパケット転送の遅延を招き、やがて通信品質の低下を引き起こす。 本研究では、ルールの構成と配置を最適化することで転送の遅延を最小にする方法を構築する。 ここで考案する方法は、パケット通信を行うあらゆるネットワーク機器に適用できることから、ネットワーク全体の通信の品質を向上することに広く貢献する。これまで、パケットフィルタを最適化するさまざまな研究が行われてきた。 神奈川大学田中研究室では、これまでにパケットフィルタリングをモデル化し、フィルタを構成するルール集合によって決まるネットワーク機器の負荷を定義した。そして、ルールの入れ替えと併合を行う場合に、負荷が減少するための必要十分条件を与えた。クワイン・マクラスキ法を基にしたルールの併合と入れ替え法に基づく最適化アルゴリズムを提案し、フィルタの負荷を50%程度に軽減できることを示した。 その後、課題とされた評価パケット数の計算量についても、多項式時間の概算値の計算法を提示し抜本的な解決をはかった。従来は、パケットの頻度分布が一様であることを仮定していたが、ネットワーク機器の到着パケットを観察することで評価パケット数に換える方法を提案し、現実のネットワーク機器の運表を継続しながら適応的にフィルタを再構成する方法に目途をつけた。今後は、これらの理論的結果を踏まえ、実際のネットワーク環境での実装実験を行い、実用化を目指す。 

大学名	北海道大学数学連携研究センター
所在地	〒060-0812　札幌市北区北12西7北海道大学
窓口部署名／電話番号	
ホームページのURL	http://www.math.sci.hokudai.ac.jp/center/
対象技術	研究開発状況
データ その他	ＰＤＦへの長期署名を埋め込み時刻認証との連携のもとにファイルの作成時刻を保証する。これにより、論文を電子ファイルのみで出版した場合でもプライオリティ(成果の先着権)が確実に担保される。現在、開発を終えており、今後の発展を模索している。

大学名	国士舘大学理工学部
所在地	〒154-8515　世田谷区世田谷4-28-1
窓口部署名／電話番号	国士舘大学理工学部／03-5481-3251
ホームページのURL	http://www.kokushikan.ac.jp
対象技術	研究開発状況
通信情報 データ	将来のクラウド化のもつ脆弱性について、検証を行うことを目的とし、その欠点を回避するためのクライアントが対応すべき技術を開発中であり未だ成果を公開するに至っていない。

大学名	国立大学法人奈良先端科学技術大学院大学
所在地	〒630-0192　奈良県生駒市高山町8916-5
窓口部署名／電話番号	
ホームページのURL	http://www.naist.jp
対象技術	研究開発状況
ネットワーク 通信情報	近年、インターネットにおいて、大量のパケットを送信することでサービスの妨害を行うサービス不能攻撃（DoS攻撃）が問題となっている。このDoS攻撃への対策として提案されている、攻撃元までの経路を追跡し攻撃者を特定するIP Tracebackという手法に関し、研究を行っている。

大学名	岩手大学工学部
所在地	〒020-8551 岩手県盛岡市上田4-3-5
窓口部署名／電話番号	工学研究科デザイン・メディア工学専攻 ／019-629-2838
ホームページのURL	http://www.mn.cis.iwate-u.ac.jp/research/index.html
対象技術	研究開発状況
サーバ	近年のコンピュータウィルスは実行可能圧縮という圧縮や難読化が施され、アセンブラコードの検査によるウィルス判定が難しくなってきている。 商用のアンチウィルス対策ソフトウェアは独自開発した解凍機能を有しているが、処理が複雑すぎて解凍できない場合が多発している。 そこで私たちはウィルスを実行させて、それ自身の解凍ルーチンでウィルスの中身をメモリに展開させた後に実行を止めて、その中身をベイジアンフィルタで検査する方法で80%の解凍・解析に成功した。 しかしながら、この方法では毎回ウィルスを実行するために処理に時間が掛かる。 現在、解凍前後の情報を記憶させることで、2回目以降の検査を実行可能圧縮のまま可能にする新方式について研究を進めている。

大学名	東北工業大学工学部情報通信工学科松田研究室
所在地	〒982-8577 宮城県仙台市太白区八木山香澄町35-1
窓口部署名／電話番号	情報通信工学科松田研究室／022-305-3424
ホームページのURL	http://www.ice.tohtech.ac.jp/jp_ng/labs/matsuda.html
対象技術	研究開発状況
ネットワーク サーバ クライアント	データリンク層における通信制御を、低コストに実現する研究を開発し、性能試験を実施している。

大学名	九州大学
所在地	〒819-0395 福岡市西区元岡744
窓口部署名／電話番号	大学院システム情報化科学研究情報学部門／092-802-3801
ホームページのURL	http://itslab.cace.kyushu-u.ac.jp/
対象技術	研究開発状況
ネットワーク サーバ クライアント 通信情報 データ	暗号および暗号プロトコル技術、コンピュータシステムセキュリティ技術等の情報セキュリティ関連研究開発を実施している。 暗号および暗号プロトコル分野： 暗号技術に基づくデータプライバシー保護手法（2007-）、公開鍵認証基盤（2003-）、電子投票（2002-）、ハッシュ関数（2002-）、デジタルフィンガープリンティング（2002-）、配達保証付き電子メール（2002-）、ソフトウェア難読化（2002-）、認証付き鍵交換（2001-） コンピュータシステムセキュリティ分野： BFIDタグのプライバシ、侵入検知システム、VM-Basedl_ogging Scheme（2008-）、キャンセラブルバイオメトリクス（2006-）、オペレーティングシステム(OS)の安全性（2003-）、迷惑メール対策（2003-）、インサイダー脅威対策（2010-） ネットワークセキュリティ分野： パケット生存時間を用いた確率的パケットマーキングによるIPトレースバック手法、ネットワーク管理とセキュリティのための視覚化、P2P Trust Model(2008-)、Formal verification of access Control(2008-)、内容の類似性を用いたトラックスパム判別（2008-）、ポリモーフィックワームの検知手法（2007-）、ボット検知手法（2007-）、SIPにおけるend-to-mobileセキュリティ（2007-）、P2Pルーティングアルゴリズム（2007-）、ファイヤーウォールポリシーのフォーマルメソッド（2007-）、ポートスキャン検出（2005-）、ピアーツーピアネットワークの匿名性保護（2005-）、モバイルエージェントの安全性（2003-）

【企業】

企業名	シスメックスＲＡ株式会社
所在地	〒399-0702　長野県塩尻市広丘野村1850-3
窓口部署名／電話番号	ITX部営業課／ 03-5719-5587
ホームページのURL	http://www.sysmex-ra.co.jp/
対象技術	技術の概要・特徴など
通信情報	Ipsec暗号化アダプタBOX ■IPsecによる強固なセキュリティ機能： 強力な暗号化と認証機能を持ったIPsecにてプロトコルやアプリケーションに関係なく転送される通信データ(TCP/UDPパケット)のセキュリティ機能を高めることができます。 ■簡単接続： イーサネットインターフェースを２ポート装備し、通信機器とLANケーブルの間に中継器として挟み込むだけで通過する通信データは自動的に暗号化され送信先へと転送されます。 また、通信機器へは競って変更や特殊なアプリケーションをインストールする必要はなく、通信機器に迅速に組み込むことができます。 ■柔軟設定 設定はPC上から専用ツール(NSSetup)にて行います。 認証キーの設定のみで完了する基本的な対向通信から、詳細なセキュリティポリシーの設定による経路別の動作指定といった応用的な用途まで幅広く柔軟に対応できます。 ■高速・安定動作 ASICによるハードウェア処理により、最90Mbps(AES、512byte/pkt双方向通信時のSmartbit値)の高速で安定した動作を実現しています。 ■NAT対応 NAT-Traversal/UDP-EncapsulationによるNAT越えを実現 ■RoHS指令対応

企業名	株式会社アクアシステムズ
所在地	〒160-0022　新宿区新宿1-10-4
窓口部署名／電話番号	／ 03-5363-5556
ホームページのURL	http://www.aqua-systems.co.jp
対象技術	技術の概要・特徴など
通信情報	Oracleデータベースへのアクセスを監査しログを保管する

企業名	KDDI株式会社
所在地	〒102-8460　東京都千代田区飯田橋3-10-10ガーデンエアタワー
窓口部署名／電話番号	ネットワーク技術本部技術戦略部／ 03-3347-0077
ホームページのURL	http://www.kddi.com
対象技術	技術の概要・特徴など
サーバ	2000年に多数のWebサイトを一斉に改ざんされた事件や、2010年には多くの人が集まるサイトにウイルスが埋め込まれる事件など、今もなおホームページの改ざん事件が頻発しています。 企業のホームページの中には、200回/月の頻度で更新されるという統計結果も出ており、Webアプリケーションなどの脆弱性を完全に排除しきれないことで発生する改ざん攻撃に対する脅威が高まっています。 そこでKDDIでは、センター局から各地のWebサイトを巡回して、改ざんの有無を監視するシステムを開発しました。 これは定期的にリモートのWebサイトからホームページファイルをダウンロードして、前回取得したファイルと新たなファイルを比較します。 もし改ざん化が検知されると、ホームページの構文を解析し、改ざんに見られる特徴の有無とその組み合わせを検査して「更新」と「改ざん」を見分けてアラームを発信します。 また、Webサーバーの問題やネットワーク遅延も「障害」としてアラームを発信します。

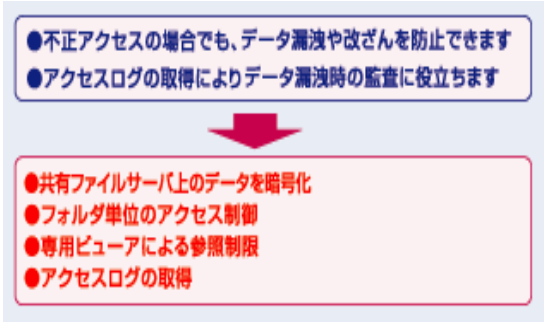
企業名	メトロ株式会社
所在地	〒141-0011　東京都品川区北品川5-9-15渡辺ビル
窓口部署名／電話番号	営業本部第三営業部／ 03-5789-1022
ホームページのURL	http://www.metro.co.jp/
対象技術	技術の概要・特徴など
クライアント	ハードディスク暗号化 ＯＳ領域やシステムファイル領域を含め、ハードディスク全体ををを自動で暗号化するため、ユーザが特別な操作をする必要がなく、暗号化を意識せずに、これまでと同様にＰＣを使用することが可能です。また、ロックを解除する鍵そのものも暗号化するため、ハードディスクを抜き取り、何らかのツールで解析を試みたとしても、除法を解読することは不可能です。 ＯＳ起動前のログイン認証 ＯＳ起動前の認証機能で、第三者による不正ログインを防止します。CheckPointFullDiscEncryptionの認証をパスしなければ、ＯＳを機動することさえできません。 またログイン試行回数の制限ができるため、設定回数を超えるパスワード入力失敗時にアカウントをロックすることが出来ます。

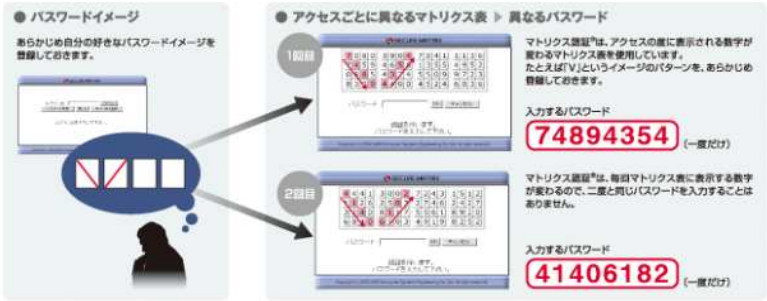
企業名	メトロ株式会社
所在地	〒141-0011　東京都品川区北品川5-9-15渡辺ビル
窓口部署名／電話番号	営業本部第三営業部／ 03-5789-1022
ホームページのURL	http://www.metro.co.jp/
対象技術	技術の概要・特徴など
クライアント	メディアの暗号化 USBメモリやCD/DVDメディア、外部メモリーカード、外付けハードディスクなど、リムーバルメディアは、MEが導入されていないＰＣでもデータの暗号・複合ができるので、利便性を損ないません。また CD-R/RW、DVD-R/RWへの複合書込も可能です。 デバイス制御機能 PCに損悪USBや工学ドライブ、無線LAN、Bluetooth、プリンタなど、各ポート/デバイスの利用を制限し、企業内のデータとエンドポイントＰＣを保護します。 外部メディアの利用が必要なユーザにのみの利用許可、また、通常利用禁止しているユーザに一時的に利用を許可するといった、臨機応変な対応も可能です。

企業名	三菱電機株式会社
所在地	〒100-8310　東京都千代田区丸の内2-7-3
窓口部署名／電話番号	総務部企画課／ 03-3218-9075
ホームページのURL	http://www.mitsubishielectric.co.jp
対象技術	技術の概要・特徴など
データ	ファイルの暗号化による情報漏洩防止 ハードディスクの逐次暗号化

企業名	三菱電機株式会社
所在地	〒100-8310　東京都千代田区丸の内2-7-3
窓口部署名／電話番号	総務部企画課／ 03-3218-9075
ホームページのURL	http://www.mitsubishielectric.co.jp
対象技術	技術の概要・特徴など
サーバ	WebシステムのSaas型診断サービス

企業名	ログイット株式会社
所在地	〒170-0005　東京都豊島区南大塚2-25-15
窓口部署名／電話番号	監理部／ 03-5918-1531
ホームページのURL	http://www.logit.co.jp
対象技術	技術の概要・特徴など
通信情報	Eメールのアーカイブでの監査認証

企業名	株式会社日立ソリューションズ
所在地	〒140-0002 東京都品川区東品川4-12-7日立ソリューションズタワーA
窓口部署名／電話番号	広報・宣伝部広報グループ／ 03-5780-2111
ホームページのURL	http://www.hitachi-solutions.co.jp/
対象技術	技術の概要・特徴など
サーバ 通信情報 データ	■ファイルサーバの暗号化、アクセス制御、ログ取得 ファイルサーバ上のデータを暗号化、フォルダ単位でのアクセス制御でデータの漏洩や改ざんを防ぎます。また、ファイルサーバ上の暗号化したデータへのアクセスログを取得します。   データ参照ための認証も、ID、パスワードを入力する手動ログイン、自動ログイン、USBトークンを資料した証明書ログイン等があります。 ■秘文シリーズ 「秘文」はオフィスのIT環境において、情報の持ち出しのコントロール、また持ち出した情報を保護することで安全な情報の活用を実現する「秘文AEシリーズ」、セキュリティ運用状況の把握と可視化により、マネージメントを実現する「秘文MEシリーズ」、システム管理者が不在でも、「ファイル持ち出し」や「暗号化」など機能をPC一台から低コストで導入・運用できる「秘文LEシリーズ」があります。

企業名	株式会社シー・エス・イー
所在地	〒150-0044　東京都渋谷区円山町23-2アレトゥーサ渋谷ビル
窓口部署名／電話番号	事業企画部マーケティング課／ 03-3463-5633
ホームページのURL	http://www.cseltd.co.jp/
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	SECUREMATRIXは、株式会社シー・エス・イーが開発した、認証デバイスを一切使わない本人認証システムです。人が頭の中に思い描くイメージからワンタイムパスワードを生成する「マトリクス認証」方式を採用し、セキュリティおよび利便性の向上、コスト削減のすべてを同時に実現します。 ＜マトリクス認証の仕組み＞ 「マトリクス認証」は、ユーザがあらかじめ設定した「位置」と「順番」(＝イメージパスワード)を使って、マトリクス表(アクセスするたびにランダムに表字が変わる乱数表)から、その位置と順番に当てはまる数字を抜き出してワンタイムパスワードとして認識させる認証方式です。パスワードは「ワンタイム(使い捨て)」になるため、強固な認証を実現できます。  複雑なパスワードをもう覚える必要はありません。また高価な認証デバイスを利用する必要はありません。コストを削減したい「企業」や、セキュリティを高めたい「IT管理者」、また面倒なことはしたくない「社員」など、様々な立場の方が抱えるパスワードに関する悩みを一気に解決するのが「SECUREMATRIX」です。

企業名	株式会社インテリジェントウェイブ
所在地	〒104-0033　東京都中央区新川1-21-2芽場町タワー
窓口部署名／電話番号	セキュリティシステム事業部／ 03-6222-7151
ホームページのURL	http://www.iwi.co.jp
対象技術	技術の概要・特徴など
クライアント データ	＜概要＞ ＣＷＡＴは、インテリジェントウェイブが金融企業向けシステムのインフラ構築で培った技術を基に開発した、パソコンからの情報漏洩を防止するソフトウェアです。 ユーザのパソコン操作を監視し、セキュリティポリシーに違反した操作を検知し、管理者に通知するとおもに、警告情報(警告ログ)とパソコンの操作情報(監視ログ)を蓄積します。外部デバイスの接続や外部記憶メディアへのデータ書出し、印刷、メール送信、Web操作、閲覧中のウインドウタイトル等、ユーザのPC操作をきめ細かく監視できます。また、セキュリティポリシーに違反した不正な操作については監視サーバにリアルタイムに警告を発信するとともに、操作の中止等の対処を行うことも可能です。さらに、ＣＷＡＴで蓄積した「警告ログ」によって不正操作を即座に把握し、不正操作を「監査ログ」によって追跡する(つきとめる)ことができます。これにより効率かつ効果的にログ運用が可能になります。社内のPCを集中管理し、企業の生産性を低下させることなく柔軟な企業情報セキュリティ環境を実現できます。 ＜特徴＞ ・トータルな企業情報セキュリティ 「情報漏洩の防止」、「フォレンジック(証跡管理)」双方の観点から企業情報セキュリティを管理します。 ・類のない充実した「ログ」機能 情報セキュリティ管理の基本となる「ログ」。ＣＷＡＴでは、記録される操作内容・項目が極めて充実しているのが特長です。 ・優れたリアルタイム性 ＣＷＡＴが検知した様々な操作に対して、警告の発言や操作の中止など、リアルタイムに対処することが可能です。 ・グローバルに展開可能 マルチ言語対応により海外を含めたワールドワイドなセキュリティ対策が可能。 ・柔軟なセキュリティポリシー設計 ＣＷＡＴのポリシーは、端末、ユーザ、組織、エリア、ユーザーグループ、端末グループを対象に適用でき、さらに曜日・時間帯毎に設定できるので、企業の業務に沿った柔軟な運用が可能です。

企業名	株式会社インテリジェントウェイブ
所在地	〒104-0033　東京都中央区新川1-21-2茅場町タワー
窓口部署名／電話番号	セキュリティシステム事業部／ 03-6222-7151
ホームページのURL	http://www.iwi.co.jp
対象技術	技術の概要・特徴など
データ その他	１.概要 Microsoft OfficeやAdobe PDFなどで作成した文書ファイルを暗号化し捜査権限を付与することで、情報漏洩/改竄を防止し、文書ファイルの操作ログを取得することにより内部統制強化を支援します。 ２.特徴 ①まったく意識せず文書ファイルの暗号化が可能 EUCSecureは、利用するPCにEUCSecureクライアントプログラムをインストールすることにより、細かな設定なしにWord形式、Excel形式、PDF形式の文書ファイルの暗号化、複合化を行うことができます。また、AES(Advanced Encryption Standard)暗号方式の暗号エンジンを採用しているため、標準かつ安全性の高い情報セキュリティが容易に実現します。ファイル単位はもちろん、フォルダ単位でのファイル一括暗号化、利用制限設定もすることができます。 ②文書ファイルの利用用途に合わせた利用条件設定が可能 EUCSecureは、文書ファイルを暗号化する際に文書ファイルは配布利用先の利用用途に合わせてファイルの「参照・編集(更新)・印刷・削除」といった利用条件を付与することが可能です。サーバと接続できない状態やコピーされたファイルの利用条件も設定することができます。ファイル利用の有効期限を設定することもできます。 ③文書ファイル操作ログの取得と蓄積 文書ファイルの暗号化・利用条件の設定により、その文書ファイルで行われた参照、編集(更新)、印刷といったファイル操作の利用履歴(ログ)を取得します。また、取得したログは簡易ビューワ機能により文書ファイル内での参照が可能です。また、専用のログサーバプログラムを特定のサーバ機器に導入することにより、上記のファイル操作に加え、文書ファイルの削除操作についてもログを取得することが可能となります。この機能により、多数の文書ファイルの操作履歴をログサーバで一元的に管理、参照することが可能となります。