

会員企業ご紹介⑨

株式会社網屋

(<http://www.amiya.co.jp/>)



株式会社網屋は、1996年12月にITConsulting & Project Management事業をキーワードに、お客様によりハイクオリティなビジネス環境をご提供することを目的とし設立致しました。

昨年に入りましてからリスクマネジメントの運用を急務とする日本のお客様のニーズに合致した、情報セキュリティ監査ツール『bv-control』の日本語対応版リリースに向けて開発を開始し、今年の7月に販売を開始致しました。既に大型案件の導入も行った経験上、単なる製品販売だけでなく以下のようなセキュリティ診断サービスもお客様にご提供することが可能になりました。

御社のWindows環境のセキュリティ状況を調査します

Windows Security Check Service

情報セキュリティ意識の高まりにより、サーバ・ネットワーク装置のセキュリティ対策は進みつつありますが、最も脆弱となりやすくチェックを必要とするのは従業員のデスクトップPCです。

従ってデスクトップPC内を調査し、効果的な対策を行うことで企業全体の脆弱性を無くすというセキュリティ対策こそが、今最も企業に必要とされる「デスクトップセキュリティマネージメント」という考え方です。

『Windows Security Check Service』は、マイクロソフトが推奨するセキュリティ基準を満たした状態になっているかを調査します。

『Windows Security Check Service』は、弊社が国内販売をおこなう米国BindView社の情報セキュリティポリシー監査ツール『bv-Control』を使用しています。



『Windows Security Check Service』の特徴

■アプリケーションをサーバやクライアントにインストールする必要が無いため、システムへのインパクトを心配することなく、すぐに調査が可能です。

■項目例

【OSの脆弱性によるセキュリティ事故を防ぐ】

- ・最新のService Pack インストールの有無調査

【簡単に破られるパスワードを使わせない】

- ・極めて脆弱なパスワード利用ユーザの調査

【安定したディスク環境を保つ】

- ・ハードディスクの利用状況の調査

【情報漏洩のルートを減らす】

- ・リスクの高いアプリケーションのインストール状況の調査

お問い合わせ先

株式会社網屋

E-Mail : bv-info@amiya.co.jp

TEL : 03-5643-1331 FAX : 03-5643-1334

〒103-0014 東京都中央区日本橋茅場町1-2-3

ルート 蛸殻町第二ビル

株式会社インテリジェント ウェイブは1984年の創業以来、金融関連に特化し銀行系カード会社や大手証券会社などをクライアントにもつ独立系ソフトウェア会社です。

自社開発パッケージによるクレジットネットワークシステムおよび集配信システムの提供では国内70%のシェアを占め、さらにカード不正検知システム等でセキュリティ分野へも積極的に展開しており、2003年11月には内部情報漏洩・内部犯罪監視システム「CWAT」の発売を開始しております。

■ 主な事業内容

- カードビジネスのフロント業務 ● ディーリング・トレーディング業務及びパッケージの製造・販売・技術支援
- カードビジネスのバック業務 ● セキュリティシステム業務 ● 消費者向けパッケージ販売

■ 内部犯罪を防ぐ統合監視システム「CWAT」

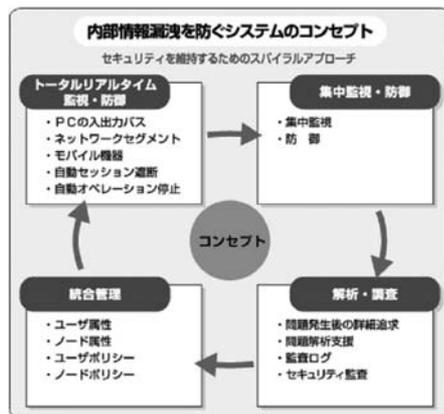
現在、多くの企業では外部からの犯罪に対して、FirewallやIDS(不正侵入検知システム)の導入で対応していますが、急激に増加しつつある内部情報漏洩・内部犯罪に対しては、ほとんどの企業が未対応な現状です。

最近の個人情報流出事件などの殆どは、内部情報漏洩・内部犯罪であり、緊急な対処を必要としています。

これまで、内部犯罪に対しては「本人認証機能」と「アクセス管理機能」が有効と考えられてきましたが、権限者が行う内部犯罪が増加するにつれ、これらの機能だけで内部情報の漏洩は防止出来なくなっています。

弊社の「CWAT」は、ネットワークと端末上操作の両方を不正挙動と特異挙動の観点から監視し、集中監視制御を実現することにより、内部犯罪を強固に防ぎます。

【CWATのシステム構成】



【CWATの特徴】

● 特異挙動の監視

普段の行動を学習することで、通常と異なる行動を検知し、アクセス権限者であってもその操作を監視し不正利用の疑いがある場合は通知します。

● 外部接続デバイス監視

ネットワーク上を流れる情報を監視するだけでなく、個々端末の使用状況や外部接続パスを監視し、不正利用を通知・禁止します。

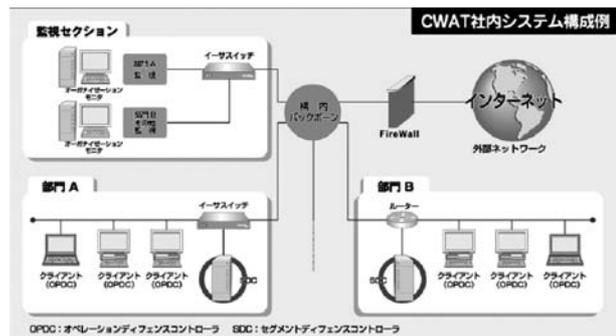
● 不正挙動の監視

ユーザやノードの属性情報も含めた細かなポリシー設定が可能で、ポリシー違反に対処することが可能です。

● モバイル機器の監視

モバイルPCに対応し、盗難や、持出し中の不正な操作など、様々な犯罪ケースに対応できます。

監視については、全ての監査ログに強固な暗号化を施された後に記録され、改竄等を防ぎます。又、ログのフィルタリング及びサンプリング機能を持っているため、リソースコストを抑えながら、柔軟に監査対応する事が可能です。全ての監視・防衛については、統合管理コンソールによる集中管理が可能となっています。



お問い合わせ先

株式会社インテリジェント ウェイブ 営業本部
〒135-0042
東京都江東区木場5-12-8 木場グリーンパークビル
Tel:03-5620-1051 Fax:03-5620-1060
e-mail:cwatsales@iwi.co.jp

監査法人トーマツ エンタープライズリスクサービス部

(<http://www.tohmatu.co.jp/services/ers>)

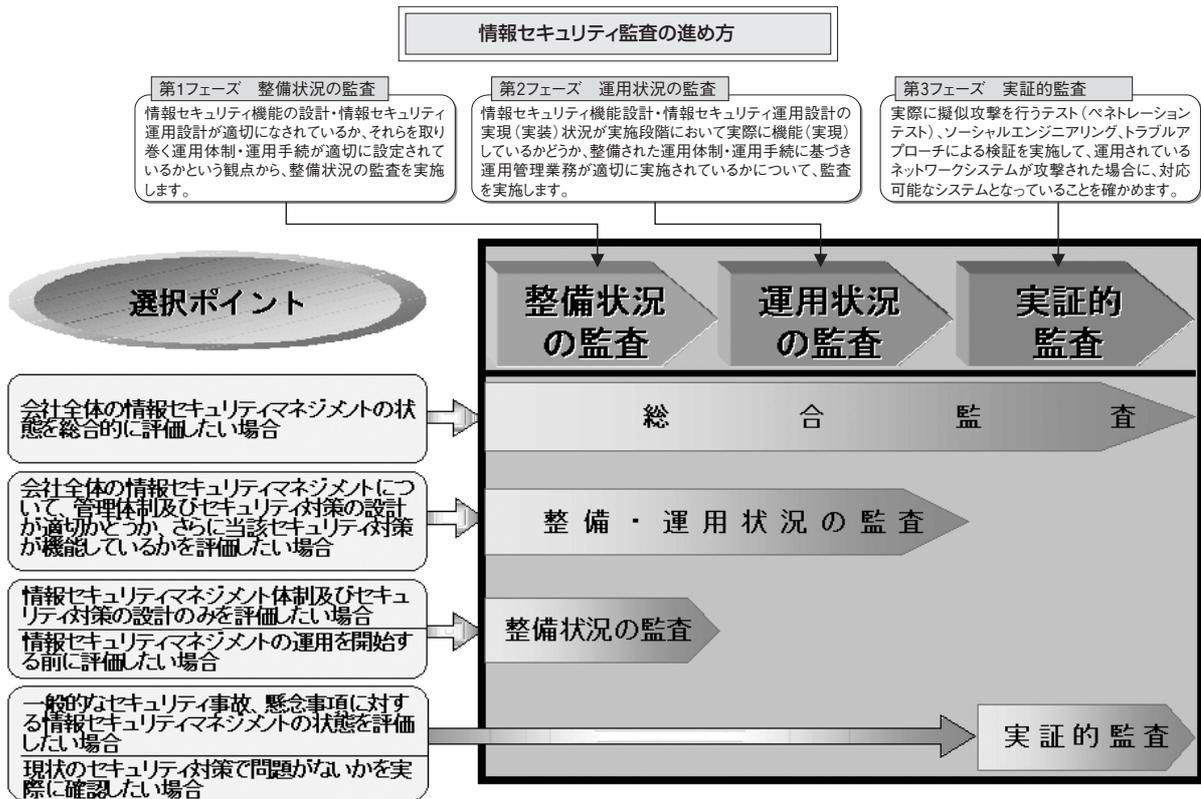
監査法人トーマツは、日本初の全国規模の監査法人として1968年に創立されました。以来、監査等の証明業務やアドバイザー業務、税務、コンサルティングサービスを提供しています。エンタープライズリスクサービス部では、情報リスクマネジメントの観点から企業組織、情報、業務、テクノロジー、財務に関わるリスクを識別し、リスクとその管理に関わる総合的な監査やコンサルティングサービスを提供しています。

情報セキュリティに関するサービス

インターネットの普及によって、情報セキュリティリスクマネジメントが喫緊の課題となっています。情報セキュリティを確保し、ビジネス戦略を成功裡に推進しなければなりません。トーマツは、情報セキュリティ強化により貴社のeビジネスを成功に導きます。

主なサービス内容

- 情報セキュリティ監査
- 情報セキュリティ方針・スタンダードの作成支援
- ISMS (BS 7799を含む)の導入支援
- ISMS (BS 7799を含む)の認証取得支援
- ネットワーク・セキュリティの評価・診断
- インターネット侵入によるセキュリティ検証
- プライバシーマーク取得支援
- WebTrust マーク取得支援
- 公開鍵インフラ(PKI)の導入支援
- 電子認証局の監査等



お問い合わせ先

監査法人 **トーマツ** エンタープライズ リスク サービス (ERS) 部

東京・本部 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル

TEL 03-6213-1112 FAX03-6213-1117

大阪事務所 〒541-0052 大阪市中央区安土町2-3-13 大阪国際ビルディング

TEL 06-6262-4558

名古屋事務所 〒450-0002 名古屋市中村区名駅3-13-5

名古屋ダイヤビルディング3号館 TEL 052-565-5511

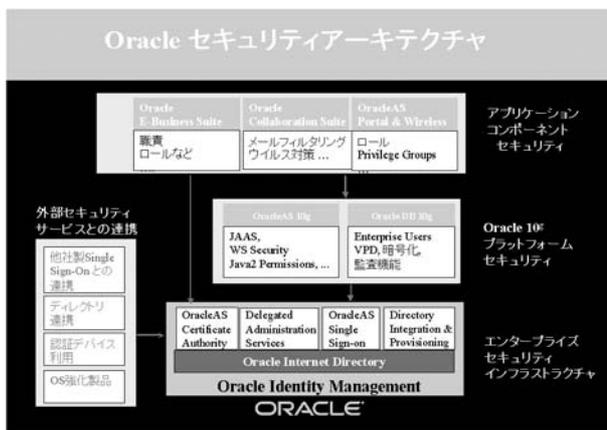
福岡事務所 〒810-0001 福岡市中央区天神1-10-24 福岡三和ビル

TEL 092-751-0931

日本オラクル株式会社

(<http://www.oracle.co.jp>)

日本オラクル株式会社では2003年10月、Oracle Database 10g、Oracle Application Server 10gを発表致しました。(2004年1月出荷予定)オラクルでは顧客が保有する最も価値の高い情報資産の多くはデータベースに格納されていることから、データベースでの情報保護対策が非常に重要であると考えています。またシステムと顧客規模が大きくなってくるとユーザ認証・アクセス制御・ユーザ管理が一元的かつ合理的に行われなければならないなりません。オラクル製品にはさまざまな形でセキュリティ機能・オプション製品等が実装されており、情報保護のために利用できます。



1. データベースでのセキュリティ対策

(1) 仮想プライベートデータベース

従来リレーショナル・データベースではオブジェクト(表・ビューなど)の単位でしかアクセス権限を制御できませんでした。オラクルでは仮想プライベートデータベース(VPD)を使うことにより行レベルでのアクセス制御を行うことが可能です。この機能はアプリケーション・コンテキストを利用することによって、オブジェクトを共有しているWebアプリケーションのユーザに対してもアクセス制御ができます。

(2) 格納データの暗号化

データファイルの盗難などに備えて、機密性の高い情報については各表の列単位で暗号化を行い、更にハッシュ関数を使った改ざん検知などの仕組みを実装することができます。

(3) 通信データの暗号化(Oracle Advanced Security)

データベースサーバとクライアント、またはアプリケーションサーバとの間の通信経路上における盗聴対策としてOracle Advanced Security(オプション)を使うことで通信データの暗号化が可能です。

(4) ファイングレイン監査

従来の監査機能に加えて、更に詳細な監査ポリシーを設定して監査を実施することができます。さらに監査動作を行った後、任意の動作(管理者にメール通知を行う等)をプログラムできます。

2. アプリケーションサーバを使ったユーザ認証とディレクトリ管理

(1) シングルサインオンとディレクトリ管理

Oracle Application Server 10gではそのコンポーネントとしてOracle Single Sign-on Server、Oracle Internet Directory、Oracle Certificate Authorityを実装し、配下のWebアプリケーションに対するシングルサインオンとアクセス制御を実施します。また従来のパスワード方式だけでなく、ディレクトリにデジタル証明書をインポートし、クライアント証明書を使ったSSLクライアント認証・シングルサインオンを実現することが可能です。これによりICカードなどの認証デバイスやPKIを使った認証基盤に対して高い親和性を発揮することができます。

(2) 他社製品との連携動作

Oracle Single Sign-on Server、Oracle Internet Directoryはユーザの既存のシングルサインオンサーバ製品やディレクトリサーバとも相互に連携しながら導入を進めることが可能です。

3. セキュリティ評価・認証について

セキュリティに関する社会的関心の高まりとともに各種のセキュリティ関連国際標準が制定されています。オラクルではお客様にセキュリティ機能を安心してお使い頂けるようISO/IEC 15408(Common Criteria)EAL4、FIPS-140-1など合計17の各種国際標準のセキュリティ評価・認証を取得しています。

お問い合わせ先

日本オラクル株式会社

〒102-0094 東京都千代田区紀尾井町4-1

ニューオータニガーデンコート

Oracle Direct TEL : 0120-155-096

URL : <http://www.oracle.co.jp/contact/>

株式会社ネットマークスは、メーカーにとらわれることなく時代に即したネットワーク構築というニーズの高まりを背景に、マルチベンダ環境でのネットワークシステムインテグレータとして1997年に設立いたしました。

ネットマークスでは、『We are here on customer's side.』をスローガン掲げ、お客様の立場で考えた最適なソリューションと誠実できめの細かいサービスを提供することを目指しております。

最新技術にも柔軟に対応するネットワークシステムの構築をベースに、重要な情報を確実に守るセキュリティシステム、データを安全に保管し最大限に有効活用するためのストレージネットワークシステム、また構築したシステムの運用・監視を行なうアウトソーシングサービスの4つのソリューションを基幹ビジネスと位置付け、これらを融合させ、設計、構築、運用・監視、保守にいたるまでトータルにお客様をサポートしております。

ネットワークセキュリティについては、最新の技術を取り入れたインターネットVPNシステムやエンドポイントセキュリティ、マルチデバイス認証など幅広いセキュリティソリューションをご提供しております。また、お客様におけるコストや人員を最小限に押さえるためのアウトソーシングサービスなども提供しております。

今後も、常にネットワークインテグレーション業界をリードし、グローバルな視野に立った企業を目指してまいります。

<代表的なセキュリティソリューション>

・高速ファイアウォールソリューション

インターネットの普及に伴うユーザ数や通信データ量の増加によりボトルネックとなりやすいファイアウォールの負荷分散を実現したソリューションです。アプリケーションレベルでの帯域制御やリアルタイムでのアクセスコントロール設定が可能なアプライアンスサーバの組み合わせで、強固なセキュリティを実現することが可能です。

・マルチデバイス認証ソリューション

アプリケーション、ネットワーク、OSへのログオン時などにおいて、指紋、虹彩等の生体情報とICカード、USBトークン等を組み合わせ、認証を行ないます。個々の認証デバイスの欠点を補完し、より強固で柔軟性のあるシステムを構築できます。

・セキュリティアウトソーシングサービス

『SecurePlanet』

セキュリティシステム構築後の運用や監視も非常に重要です。ネットマークスの提供する「SecurePlanet」は、運用・監視・保守とトータルにサポートを行い、高い信頼性・安定性・効率性を提供するセキュリティアウトソーシングサービスです。システムの認証代行、外部・内部からの不正アクセスやポリシー違反などの運用・監視をお客様に代わってセキュリティのエキスパートが24時間365日行い、トラブル発生時には迅速に対応します。



<運用・監視センター>

お問い合わせ先

株式会社ネットマークス 広報宣伝室
〒107-0051 東京都港区元赤坂1-3-12
TEL 03-3423-5782 FAX 03-3423-5902
E-Mail info@netmarks.co.jp

株式会社日立製作所

(<http://www.hitachi.co.jp/secureplaza/>)

日立のトータルセキュリティソリューション — Secureplaza —

企業情報システムの進化が加速する一方、インターネットが企業の基幹ネットワークの役割を担う時代となってきました。こうしたなか、不正アクセスやコンピュータウイルス、情報漏えいなどのセキュリティトラブルが飛躍的に増加しています。日立は、グループ全体でトータルセキュリティソリューション「Secureplaza」において、多岐にわたるセキュリティ対策を、実際のシステムやサービスの広がり即した9つのステップで提案する「ステップ別ソリューション」と、お客様の導入目的に合わせた製品／サービスをパッケージ化した「目的別ソリューション」という2つのソリューションでハイレベルなセキュリティ維持に貢献します。

■セキュリティ対策を適切コストでスピーディに実現

セキュリティの脅威は、自社の損害だけでなく、企業としての信頼を著しく失墜させる危険性を秘めています。コーポレートガバナンスの観点からも、情報セキュリティが企業のビジネス資源となる時代、信頼度の高いビジネスを実現するには、確固たるセキュリティポリシーの策定と、外部からの攻撃を遮断し、内部の情報を確実に保護するトータルなセキュリティ対策が不可欠です。

日立の「Secureplaza」は、セキュリティの脅威からお客様のビジネスと信頼をプロテクトするため、豊富なソリューションメニューをご用意しています。

■ステップ別ソリューション

ステップ別ソリューションではシステムやサービスの広がり即して考慮していくべきセキュリティ対策を、大別して9つのステップで構成しています。

高信頼なライフラインをトータルに支える9つのソリューション		
お客様のシステムは？	対策	典型的なお客様層
Step8 万が一の際の金融的、対外的な対策が必要なら…	保険	公共システム・金融システム 大規模インターネット 商取引システム 中小規模インターネット
Step7 システムの定常的な監査が必要なら…	監査／教育	
Step6 大規模システムで、統合的な管理が必要なら…	統合運用管理	
Step5 サイトを出入りする情報の制御なら…	コンテンツ監視	
Step4 ネットワークやサーバの監視が必要なら…	不正アクセス監視	
Step3 外部からの不特定の指手を交信するなら…	認証システム	
Step2 ネットワークに「圏」データなどをやり取りするなら…	VPN	
Step1 インターネットに接続するなら…	ファイアウォール	
Step0 複数でリソースを共有しているなら…	セキュリティポリシー	

Secureplaza ステップ別ソリューション

■目的別ソリューション

お客様の導入目的に合わせたソリューションをパッケージ化した目的別ソリューションをご紹介します。

◇Secureplaza/HS(Healthcare Service)

お客様のシステムをホームドクターのコンセプトで診断・管理します。セキュリティ状況を総合診断し、対策事項を的確にご提案すると同時に、システムの常時監視・運用、改善策の提言までお客様に代わってトータルにご支援します。

◇Secureplaza/IM(Identity Management)

PKI(公開鍵基盤)を実現する認証基盤システムをはじめ、署名法対応/GPKI相互認証対応、電子署名/タイムスタンプ、ヒステリシス署名、属性認証等最先端のソリューションを提供します。

◇Secureplaza/LG(Leak Guard)

5 W1Hの考え方で、「いつ・どこで・誰が・何の目的で・どうやって・何の情報が」漏えいするのかをトータルに診断・分析。情報漏えいルートやリスク分析結果に基づき、幅広いツール群の中から最適な情報漏洩防止ソリューションを提案します。

◇Secureplaza/TZ(Trusted Zone)

個人情報データ等、お客様の情報資産の中でも特に機密性の高いものを、物理的脅威、サイバーの脅威両面から保全します。また、外部からの不正PCの持込によるウイルス感染を防止するネットワークガードのソリューションも提供します。

◇Secureplaza/CS(Consultation Service)

セキュリティポリシーの策定からISMS 認証取得、ISO15408 対応セキュアシステム構築、個人情報保護法対応等幅広いコンサルティングメニューを提供します。

守備力レベルの維持 Secureplaza/HS	時間とともに低下しがちなセキュリティレベルを定期的な診断・検査により目標レベルに保ちます。
個々を見分ける洞察力 Secureplaza/M	ネット取引や電子書類の内容などの安全性を確保するため、PKIなど最新技術を駆使した仕組みを提供します。
味方のエラーをガード Secureplaza/LG	情報漏えいのさまざまな可能性を業務フローに照らし検証・診断。適切なツール導入や監視により、ホール解消を目指します。
鉄壁の内野陣 Secureplaza/TZ	堅ろうな情報金庫とデータセンターの提供により、天災などの物理的脅威とサイバーテロなどネット上の脅威、双方に備えます。
トータルで見極める Secureplaza/CS	セキュリティ全体の基本方針となるポリシー策定やISMS認証取得などを、経営策定の観点から支援します。

Secureplaza 目的別ソリューション

お問い合わせ先

株式会社日立製作所
 情報・通信グループ
 セキュリティソリューション推進本部
info-sec@system.hitachi.co.jp