

Inoculate IT™

Complete Virus Protection™

Enterprise Edition

Inoculate ITは、優れたウイルス検知とリアルタイム駆除を実現する、アンチウイルスソリューションです。ウイルスシグネチャ自動更新機能や容易な管理により、企業資産やネットワークをウイルス被害から守ります。小規模な環境から大規模でヘテロジニアスな環境にいたる様々なIT企業のニーズに合わせて、Inoculate ITは、複数のEditionを提供しています。

ウイルスプロテクションの必要性

今日、ほとんどの企業において、フロッピーディスクによるファイルの受け渡し、ファイルを添付した電子メールの送受信、インターネットによる情報へのアクセス、外部データベースの利用は、今やビジネスの世界では日常的になってきています。しかし、コンピュータウイルスが蔓延するほとんどの原因は、このような情報の共有によるものです。米国のICSA(International Computer Security Association)の調査によれば、コンピュータウイルスは何億ドルものコストと、生産性の低下による莫大な時間のロスを招いています。全体の90%を超える企業のコンピュータシステムにマクロ型ウイルスが常駐しており、ウイルスの検出、駆除、およびウイルスに起因する故障の修復には平均8千ドルもかかります。しかも、ウイルスを駆除できたコンピュータシステムの25%は30日以内に再度感染しています。ネットワークセキュリティポリシーを効果的に実現するためには、容易な管理、高度な機能そしてすべてのシステムを保護できるアンチウイルスソリューションが必要です。

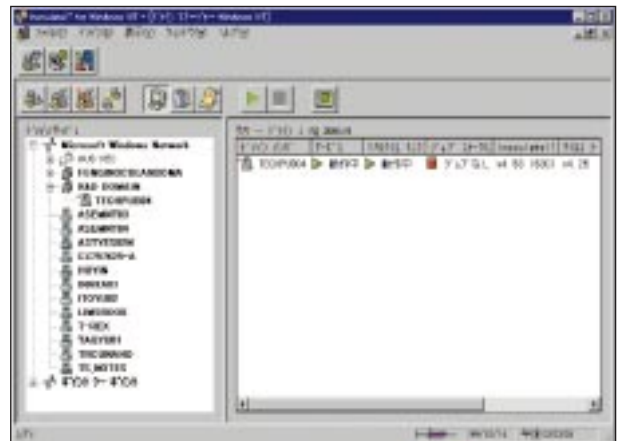
優れたウイルス検知と駆除

Inoculate ITは、リアルタイムにウイルス検出 / 駆除することができ、すべてのサーバとクライアントを含むエンタープライズ全体にウイルスプロテクションを提供します。Inoculate ITの中核にある高性能のウイルススキャンエンジンは、高度の技術を駆使して、急速に広まるステルスウイルスやマクロウイルスなどあらゆる種類のウイルスを検出 / 駆除します。

自動インストールと自動更新

Inoculate ITはネットワーク管理者のニーズに対応し、サーバやネットワーク上のクライアントへの自動インストールや自動更新など、高度な多数の機能を備えています。新種ウイルスへ対抗するためには、新種のウイルス情報をもった、最新のウイルスシグネチャファイルが必要となります。ウイルスシグネチャファイルは、無料でインターネットを通じ

て自動的にサーバにダウンロードでき、Inoculate ITサーバからネットワーク上のクライアントに配布されるため、すべてのエントリポイントでウイルス侵入から確実に保護し続けることができます。



Inoculate ITの一元管理機能を利用すれば、エンタープライズ全体を容易に保護できます。

主な特長

最新技術を結集したウイルス検知 Inoculate ITは、ブートセクタ感染型、マスターブートセクタ感染型、メモリ常駐型、マクロ感染型、ステルス型、ポリモフィック型などの感染することが判明しているウイルスを、100%検出します。

リアルタイム駆除 Inoculate ITのリアルタイムスキャンおよび自動駆除により、継続的な保護を実現します。

ヒューリスティックスエンジンを採用したウイルス検知

Inoculate ITは、高度なルールベースの検出方法により、未知のマクロウイルスも、ネットワークに被害をもたらす前に検出します。

一元的なコントロールと管理 Inoculate ITが保護するエンタープライズ内の全システムを、容易にグループ化して1台の中央コンソールから管理できます。独自のドメイン管理機能により、すべてのInoculate ITサーバの参照、環境設定、およびスキャンが可能なので作業が大幅に簡素化されます。

ウイルスシグネチャの更新 Inoculate ITは、新しいウイルスの攻撃に備えて、無料で最新ウイルスシグネチャをインターネットから毎月自動的にダウンロードでき、それをInoculate ITのサーバとクライアントに配布して、最新の保護を実現します。

インターネットプロテクタ Inoculate ITのInternet Protector Optionはインターネットのゲートウェイにおけるウイルス対策を実現し、ウイルスや悪意のあるJavaやActiveXのアプレットがSMTP、FTP、HTTPなどの一般的なプロトコルを通じてネットワークに侵入するのを防ぎます。



リモート管理とスキャン InoculateITのサーバやワークステーションをリモートから環境設定し、スキャンできます。

圧縮ファイルのスキャン ZIP、ARJ、LZHやMicrosoft 圧縮フォーマットなどの圧縮ファイルアーカイブおよびインターネットからダウンロードしたファイルのスキャンします。

マクロウイルスアナライザ 独自の技術により、Microsoft Officeのファイルに多い、急速に広がっているマクロウイルスの検出/駆除ができます。

グループウェアシステムプロテクション グループウェアシステムが稼働している間、InoculateIT AntiVirus™ Agentsが電子メール、および添付ファイル内のウイルスを検出し、駆除します。

シグネチャファイルの配布保留機能 ダウンロードしたソフトウェアや最新のウイルスシグネチャファイルをネットワークを通じて自動配布する前に、特定のコンピュータでテストします。

ファイルウイルスウォール ウイルスに感染したファイルによって既存の未感染ファイルが上書きされ、ファイルサーバが感染することを防ぎます。

隔離機能 ウイルスに感染したファイルをネットワークで移動、コピー、または保存しようとしたユーザを自動的に隔離します。

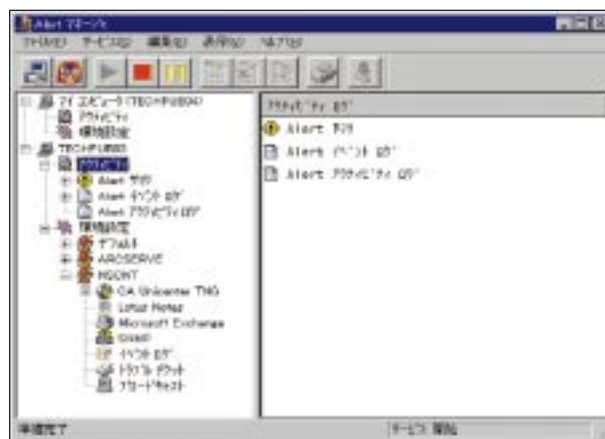
ウイルス感染源の追跡 InoculateITのウイルススキャンログにより、ウイルスイベントに関連するユーザを識別することができます。

アクティビティログの集中化 検証済みファイル、検出されたウイルス、その対応処置など、あらゆるウイルスに関するイベントが一元的に記録されるため、管理が容易になります。

負荷率の設定 InoculateITが使用する処理時間をコントロールして、システムのパフォーマンスを管理できます。

ウイルス処理オプション 駆除、名称変更、移動、レポート、削除、消去など、ウイルス発見時の処理方法を選択することができます。

バックアップ機能との統合 コンピュータ・アソシエイツのARCserve®IT™との統合により、バックアップ時にバックアップのパフォーマンスを低下させないで、ファイルをスキャンしウイルスを検出することができます。



InoculateITのアラートマネージャが、クリティカルなウイルスを管理者に知らせます。

エンタープライズマネジメントインフラストラクチャ

InoculateITは、今日最も求められているトータルなエンタープライズマネジメントインフラである、CAのUnicenter TNG®Framework™を基盤として構築されています。InoculateITはFrameworkの強力なレポート、一元的な警告、およびイベント管理の技術、ビジネスプロセスビュー、およびリアルワールドインタフェースを利用して、無類のエンタープライズセキュリティを実現します。

サポートする環境

InoculateIT 4.5.3 Enterprise Edition for Windows NT - Japanese

ハードウェア : Intel Pentium 以上のCPUを搭載したIBM PC/AT互換機 (Microsoft社 Windows Hardware Quality LabのHardware Compatibility Listに記載されているハードウェア)

OS : Windows NT Server 3.51 (Service Pack 5)
Windows NT Server 4.0 (Service Pack 5)

メモリ : 32MB以上

ディスク容量 : 16MB以上

必要メモリ容量、ハードディスク容量は、システム環境によって異なる場合がございますのでご注意ください。

すべての製品名および会社名は各社の商標または登録商標です。
製品の仕様・性能は予告なく変更する場合がありますので、ご了承下さい。

COMPUTER ASSOCIATES
Software that can think.

お問い合わせ先

コンピュータ・アソシエイツ株式会社

〒163-0439 東京都新宿区西新宿2-1-1 新宿三井ビル
お問い合わせ窓口: CAジャパン・ダイレクト (TEL: 0120-702-600)
WEBサイト: www.caj.co.jp
※記載事項は変更になる場合があります。

1999年11月現在

DSO58LEE01E-J

Printed in JAPAN