



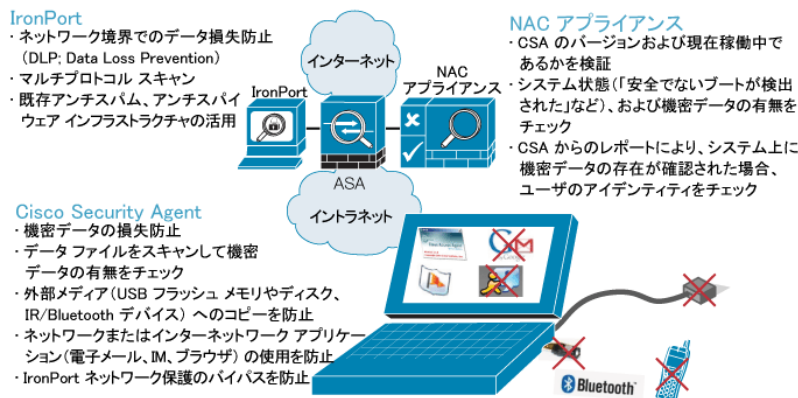
Management Center for Cisco Security Agents を使用して、あらかじめ定義またはカスタマイズされたポリシーを集中管理することで、すべてのデータ損失アクティビティの効率的なレポート作成と監査を実行できます。Management Center の管理インターフェイスでは、データ損失防止の設定変更、イベント分析、きめ細かいポリシー作成、レポート生成を行うことができます。また、データ損失防止のログとレポートにより、統合された単一のリポジトリですべての関連イベントを管理できます。機密データへのアクセスに関するユーザ承認の応答はログに記録されるため、監査およびコンプライアンスの目的に対応した包括的なレコードを残すことができます。

### 独自のネットワーク コラボレーション

Cisco Security Agent のデータ損失防止機能は、広範囲にわたってクリティカル ネットワークを保護するシスコ ソリューションの一部です。Cisco Security Agent はホスト上でコンテンツスキャンを実行し、ネットワーク境界において Cisco IronPort アプライアンスのコンテンツスキャンおよび保護の機能を補完します。Cisco Security Agent では、ユーザが社外にいる場合、企業 VPN アクセスの利用を適用できるので、Cisco IronPort のメール サービスや Web セキュリティ サービスがバイパスされることを防止できます。

Cisco Security Agent のデータ損失防止機能は、Cisco NAC (ネットワーク アドミッション コントロール) と連携して機密データの可視性と管理を強化します。Cisco NAC アプライアンスは、ホスト上の Cisco Security Agent の存在と動作ステータスをチェックするようにあらかじめ設定されています。Cisco Security Agent は、Cisco NAC アプライアンスへセキュリティ情報をレポートすることに加えて、機密データの存在をレポートできるため、Cisco NAC アプライアンスは必要に応じてホストを検疫して隔離できます。

図 3 ネットワーク統合ソリューション : CSA と NAC、DLP、および IronPort



以下の例について考えてみます。Cisco Security Agent が Cisco NAC アプライアンスに対して、多数の人事情報を記録したスプレッドシートがホストに保存されていることを通知します。このホストは営業部門に所属するものとして識別されています。これは企業のポリシーに違反しています。個人の特定が可能である情報 (PII) にアクセスできるのは人事部門のみでなければなりません。Cisco Security Agent は、エンドポイントとネットワークのセキュリティ メカニズムを独自の手法で連携させてホストの検疫やポリシー違反のユーザへの通知を行います。また警告の生成と記録により速やかな対処を可能にします。

### エンドポイントのセキュリティを常に監視

Cisco Security Agent 6.0 は、ゼロ更新の攻撃防御、ポリシー主導型のデータ損失防止、およびシグニチャベースのアンチウイルス検出の機能を組み合わせて 1 つのエージェントにした、初めてのエンドポイント セキュリティ ソリューションです。このような機能を独自に組み合わせることによって、巧妙な Day-Zero 攻撃からサーバおよびデスクトップを保護し、単一の管理インフラストラクチャの中で使用許可ポリシーとコンプライアンス ポリシーを適用できます。

© 2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0805R)

この資料に記載された仕様は予告なく変更する場合があります。