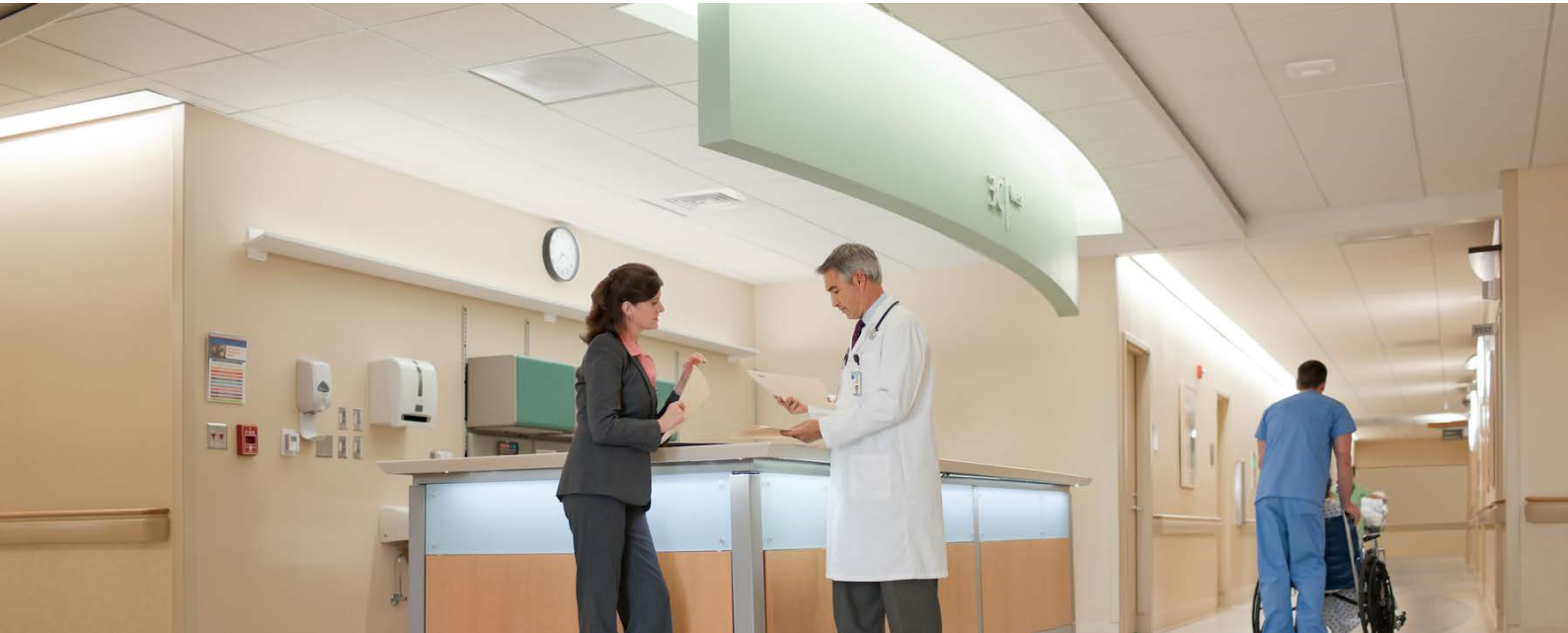
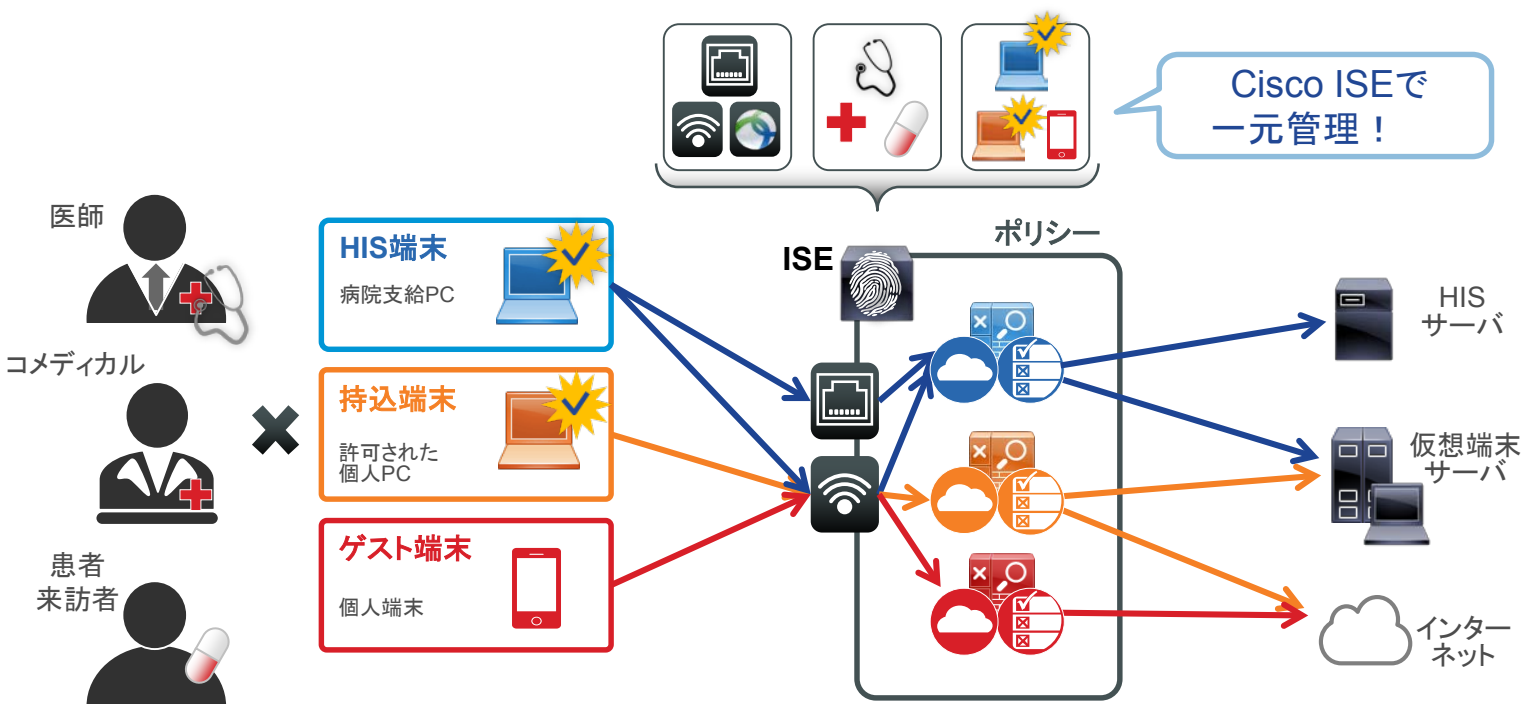


医療業務用スマート デバイスの活用 病院内のさまざまな端末を一元管理して運用



Cisco Identity Services Engine (ISE) で各種端末のポリシー コントロールを実現できます。

現状、医療現場では、PHSによる呼び出しや会話に代わる新たなコミュニケーション方法への移行が志向されています。医師や看護師へのPC、タブレットやスマートフォンなど、在籍する病院から支給あるいは使用許可された端末を、それぞれの役割に応じて最適に利用できるようになります。また、患者や来院者が各自のスマートフォンを利用できるように管理することも可能になります。



ポリシー コントロール実現に向けての課題と解決

検討事項	解決策	シスコ製品	
安定性と広帯域	<ul style="list-style-type: none"> 4 × 4:3 MU-MIMO デュアル 5 GHz モード ClientLink 4.0 	<ul style="list-style-type: none"> 450 Mbps の広帯域と安定した通信 クライアント デバイスのキャパシティが増加 ダウンリンク パフォーマンスが向上 	AP3800 WLC
電波干渉	<ul style="list-style-type: none"> Clean Air 	<ul style="list-style-type: none"> 無線品質の監視、干渉源の特定 	PI MSE
管理端末と個人端末のセキュリティポリシー	<ul style="list-style-type: none"> ポリシー ベース アクセス コントロール 	<ul style="list-style-type: none"> 柔軟なネットワーク アクセス ポリシーを実現 	ISE PI
クラウド サービスの利用	<ul style="list-style-type: none"> クラウド特化のフィルタリング 	<ul style="list-style-type: none"> フィッシング、マルウェア、ランサムウェア サイトへの接続を事前にブロック 	ISE PI

ポリシー コントロール実現のためのインフラ製品紹介

Cisco Aironet 3800 シリーズ アクセス ポイント



CleanAir、デュアル無線 5 GHz Cisco High Density Experience (HDX)

Cisco 5520 シリーズ ワイヤレス コントローラ



500 AP 収容可能 無線コントローラ

Cisco Prime infrastructure (PI)



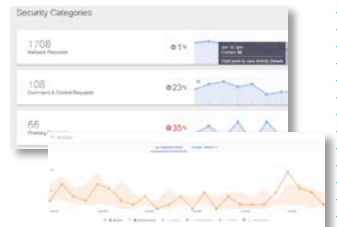
クラウドおよびシステム管理

Cisco Identity Services Engine (ISE)



ユーザ、デバイスの認証 セキュリティ プロファイル

Cisco Umbrella

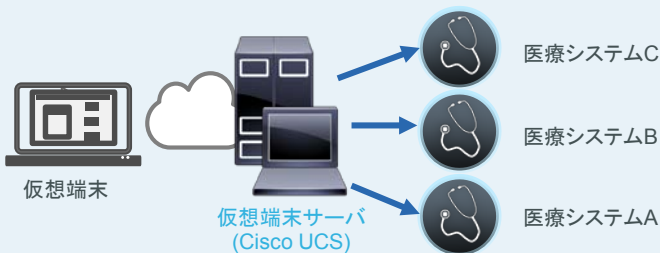


クラウド型インターネット セキュリティ

ポリシー コントロールを行う際のオプション

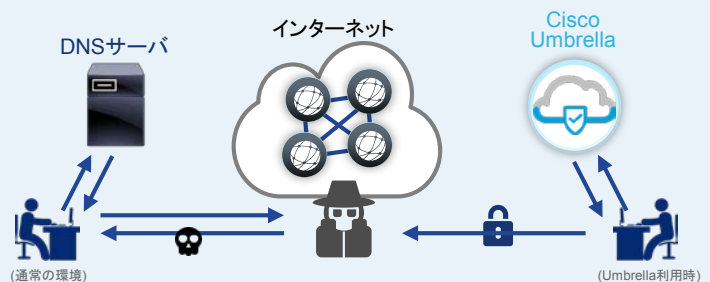
仮想端末の利用

仮想端末の利用により端末の集約と端末の紛失によるデータ漏えいを防ぎます。また、画面転送型を選択することによりデスクトップがサーバ上に保存され、不意の作業中断にも対応できます。



通信の安全性

DNS通信を使った端末はすべて防御対象とし、ポートやプロトコルにかかわらず最新の攻撃手法対策ができます。多くの環境で既存のDNSサーバの設定変更のみでのシンプルな導入が可能です。



©2017 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。(1502R)

この資料の記載内容は2017年9月現在のものです。

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。



シスコシステムズ合同会社
〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
<http://www.cisco.com/jp>

お問い合わせ先