



AEP IDpoint

- IBAC (Advanced Identity-Based Access Control)-

- ◇ データセンター、データサーバーの高度なセキュリティ管理
- ◇ IDに基づく管理、報告、監査
- ◇ end-end に渡るインテリジェントなアクセスポリシー付与 (LAN,WAN,リモート接続,モバイル)

ID を利用した新しいセキュリティモデル

ユーザーまたは PC の ID を使用し、対応するポリシーを適用しユーザーの権限を管理するアクセス管理 (IBAC = Identity Based Access Control) です。個人情報 - クレジットカード、医療情報、銀行口座番号、財務情報、電子 ID や、企業情報 - 価格表、見積書、財務情報、人材情報等々外部に漏れてはならない機密情報を保管するサーバーや **ファイル毎へのアクセス** を ID の認識により権限差別化する方法です。ID に紐づくポリシー管理となります。

ポリシーとアクセス管理

NAC やエッジセキュリティでは不足する詳細なアクセス制御を IDpoint で補う必要があります。データを管理するサーバー群の直前にゲートウェイとして配置され IDpoint は以下の機能を提供します。

- ◇ ネットワーク層、アプリケーション層アクセスの権限管理
- ◇ 企業アクセスルールのコンプライアンス確保
- ◇ ID でユーザーを選り分けデータセンター内の不要なトラフィックを排除
- ◇ 現ネットワーク構造の変更無く設置できセキュリティを高度化
- ◇ 高セキュリティアプリケーションやデータ・アクセス管理と監査
- ◇ 医療、金融、政府システム等のように個人、企業、政府情報の管理

AEP PacketTag によるトラフィック ID

IDpoint のトークンによりユーザーが発する全パケットに暗号化された PacketTag = ID が付けられます。これを発することで IDpoint がポリシーに準拠したアクセスポリシーを付します。

監査とコンプライアンス管理

IDpoint はコンプライアンス遵守に、ナリスマシ可能な認証情報や、IP/MAC アドレスなどを超越した高度なユーザーID によりアクセス管理が可能です。

- ◇ IP アドレスログの人為的変更や高価な報告検証ツールの必要性を削減
- ◇ 何時、何処から、誰が、どの情報にアクセスしたか ID 毎に把握
- ◇ 全ての規則に対応しコンプライアンスを履行されているかを管理し報告

ICH

正規一次代理店

株式会社アイシーエイチ

東京都品川区西五反田 3-5-17-408 TEL: 03-3432-3336 <http://www.ich-one.com>

e-mail: ich-info@ich-one.com



ネットワークのユーザーセグメント分離

IDpoint はネットワークのトポロジー情報を得る行為も ID により禁止できます。許可なきユーザーには全く検知は出来ませんし見えません。

- ◇ 外注業者、取引業者、訪問者全ての差別、区別化
- ◇ ネットワークの分離を行い、機密情報のあるネットワークに許可なきユーザーのアクセスを禁止
- ◇ ピングリクエストへの拒否
- ◇ IDpoint でセキュリティゾーンの“壁”を作り、許可有るリクエストのみに対応

既存のアクセス制御と違う点

ID によるアクセス制御

ユーザー、グループ ID は既存の認証方法とディレクトリーデータから生成しますので認証関連の変更は必要ありません。機体認証は定評ある AEP の CMID (Client Machine Identity) を使用します。

包括的ログ、リポーティングと管理

ポリシーや PacketTag (ユーザー ID, ソース IP, 時刻、ポリシー違反、ポリシー付与手順遵守等) の内容変更は全て記録され、表示されます。SNMP と Syslog をサポートしています。

スタイルスでポリシー付与

1Gbps や 10Gbps (近日中に対応) などのネットワーク速度でトランスペアレントにパケットを検証し重要ネットワークを隔離しながらアクセスの許認可をネットワーク層で (ホストアドレス、サブネット、ポート、プロトコル及びユーザー ID を使用して) 判断します。

NAC のエンドポイント検証

IDpoint は NAC には無いウィルス、クライアント FW、スパイウェア対策の状態確認を行います。

既存のネットワークの変更不要

IDpoint の内側ポートのネットワーク IP アドレスは不要です。従ってルーティング、スイッチ構造、認証、ファイアウォール、IDS/IPS、IP アドレスのトポロジーやその他のアプリケーションから独立して稼働します。ネットワークのトポロジーを表示させません。

PacketTag の強制適用

IP パケットに強制的に付加される PacketTag 付きのパケットは通常ネットワークに影響なくトラフィックとしてネットワークを通過できますので IDpoint には ID 付きパケットと認識されます。

リモートアクセス ID 適用

Netilla SSLVPN と IDpoint を併用するとリモート PC にも同様の PacketTag 使用が可能です。

WAN との互換性

公衆回線を利用したエクストラネット上での暗号化は AEP NET (IPsec 暗号器) で実現され、同様に PacketTag の適用が可能です。

ICH

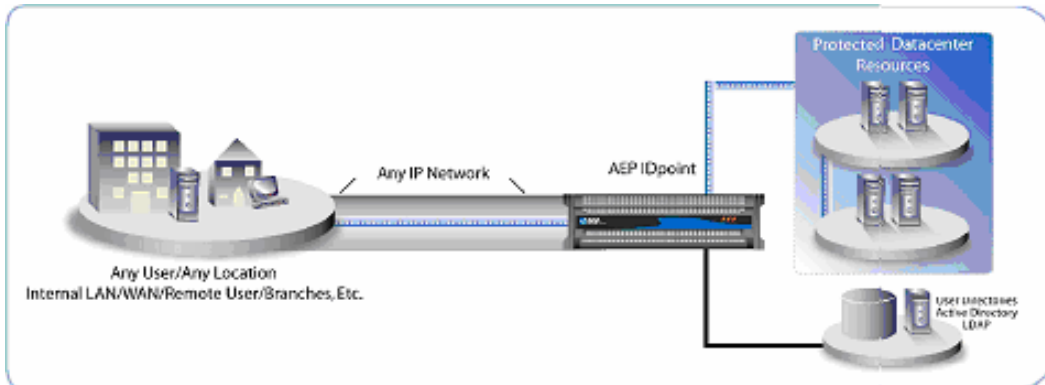
正規一次代理店

株式会社アイシーエイチ

東京都品川区西五反田 3-5-17-408 TEL: 03-3432-3336 <http://www.ich-one.com>

e-mail: ich-info@ich-one.com

AEP IDpoint™

**仕様**

寸法: 3U, 132X437X648mm

電源: 100-240VDC 60/50Hz

対応認証システム: Transparent Microsoft® Windows logon、(NTLM)、NT/2000/2003、Kerberos、SMB/Active Directory、RADIUS/Groups、LDAP (OpenLDAP、Novell Directory、iPlanet) VascoR、Digipass (Built-in)、RSA SecurIDR、ActivCardR、AladdinR Client-side PKI certificates with CRL revocation、Local、Microsoft Windows Global、and Active Directory / LDAP groups Web-based portal login for guests、最大1000までのポリシーグループ生成可能 (V-Realm)

規格対応: Payment Card Industry (PCI DSS)、Health Insurance Portability and Accountability Act (HIPAA)、Sarbanes-Oxley (SOX)、Homeland Security Presidential Directive (HSPD-12)、Gramm-Leach-Bliley Act (GLBA)、Basel II

PC 必要条件

Microsoft® Windows XP SP2またはVista、クライアントトークン設定に管理者権限(ソフトウェア配布対応、ブラウザのダウンロード機能)

ICH

正規一次代理店

株式会社アイシーエイチ

東京都品川区西五反田 3-5-17-408 TEL: 03-3432-3336 <http://www.ich-one.com>e-mail: ich-info@ich-one.com