

**モバイル機器** から  
**シンプル** で **安全** に  
**企業データ** へ **アクセス**



#### 製品の概要

Mobile Access Software Bladeは、スマートフォンやPCからインターネットを介して安全かつ容易に企業アプリケーションへアクセスするためのソリューションです。これにより、電子メールやスケジュール、アドレス帳をはじめとする各種企業アプリケーションに、SSL VPN経由で簡単に確実かつ安全なリモート・アクセスが可能となります。

# Mobile Access Software Blade

#### 課題

今日、モバイル・デバイスはビジネスに欠かせない身近なツールであり、企業所有、個人所有を問わず広く利用されています。また、コンシューマ向けのITの普及により、スマートフォンやノートPC、タブレットなど個人所有のデバイスを使用して企業のリソースにアクセスする社員が増えています。社員の生産性を高めるために、モバイル・デバイスから企業リソースへ安全にリモート・アクセスできるようにしながら、同時にセキュリティ・リスクを最小限に抑えることが、セキュリティ管理者にとって大きな課題となっています。

#### 解決策

チェック・ポイントのMobile Access Software Bladeは、モバイル・ワーカーやテレワーカー、契約社員、エクストラネット・パートナー（エクストラネットで接続されたパートナー企業）などが、必要に応じて企業ネットワークへ安全なリモート・アクセスを可能とするための包括的なソリューションです。複数のリモート・アクセス手段を提供しながら、管理者が必要とするセキュリティの高さと管理の容易さを兼ね備えており、管理作業の負担を軽減します。

#### SSL VPN技術によりリモート・アクセスを暗号化

SSL VPN技術を使用すると、企業の管理下でないモバイル・デバイスやPCから企業アプリケーションにアクセスする際、通信を暗号化して保護することができます。Webベースのアクセスとネットワーク・レベルのアクセスのどちらについても、ほとんどのWebブラウザでSSLによる暗号化が可能です。

エンドユーザは、利用する要件に適した複数の手段からアクセスが可能となります。

#### Check Point Mobile クライアント

スマートフォンやPCから、安全かつ容易に企業リソースへアクセスしたい場合に最適です。

- 企業のWebアプリケーションにワンタッチ・アクセス
- 電子メールやスケジュール、アドレス帳を安全に同期
- クライアント・アプリケーションはダウンロード可能でセットアップが容易
- ビジネス・ポータルをユーザごとにカスタマイズし、許可された企業リソースに対してのみアクセスを承認
- シングル・サインオンに対応しているため、Webアプリケーションへのログインが容易

#### 製品の特徴

##### Mobile Access Software Bladeの機能:

- SSL VPN による安全なアクセス
- 2ファクタ認証
- デバイス / エンドユーザの関連付け
- モバイル・ビジネス・ポータル
- IPSやアンチマルウェア、ファイアウォールなど、その他のSecurity Gateway Software Bladeとの連携

##### エンドユーザは

##### 複数の手段でアクセス可能:

- Check Point Mobile アプリケーション
- SSL VPN ポータル(Webブラウザを使用)
- SSL Network Extender(SNX) (リモート・アクセス時にダウンロードして利用できるブラウザ・プラグイン)

#### 製品の利点

##### モバイル・デバイスから簡単アクセス

- スマートフォンやタブレット、デスクトップPC、ノートPCからの安全なアクセスを実現
- クライアント・ベースまたはWebベースでのVPN接続を提供
- 企業所有、個人所有を問わず、任意のデバイスを使用して外出先から容易にアクセスが可能

##### データの安全性を確保

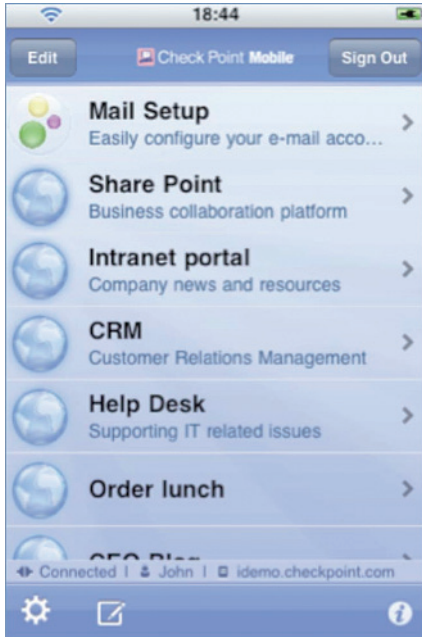
- 実績ある暗号化技術で通信内容を保護
- 2ファクタ認証により、権限のあるユーザによるアクセスのみを承認
- デバイス・ロックとリモート・ワイプ(データ消去など)の機能により、デバイスの紛失・盗難時にもデータを保護

##### 統一管理により、

##### 導入と運用管理を簡素化

- チェック・ポイントのセキュリティ・ポリシー管理に完全統合
- ユーザ証明書をワンクリックで有効化
- 既存のセキュリティ・ゲートウェイに導入可能





Check Point Mobile クライアント:  
企業リソースへワンタップで安全なアクセスを実現

## SSL VPNポータル

Webブラウザを使用してポータル経由で企業リソースへ安全にアクセスしたい場合に最適です。以下の基本機能と付加価値機能によりセキュリティを拡張します。

- **Webベースの安全なアクセス**  
 ユーザは、統合WebポータルからWebアプリケーションやWebベースのリソース、共有ファイル、電子メールにアクセスできます。また管理者は、複数言語によるサービス提供などWebポータルのデザインをカスタマイズすることができます。
- **Endpoint Security On Demand**  
 エンドポイントのコンプライアンス/マルウェア・スキャナ(オプション)  
 - リモート・アクセスを試みるエンドポイントが企業ポリシーを遵守しているかどうかを確認  
 - キーロガーやトロイの木馬などのマルウェアを検出  
 - ポリシーを遵守していないユーザには自己修復リソースへのリンクを提示
- **Secure Workspace**  
 エンドユーザは、チェック・ポイントの仮想デスクトップを使用することで、ユーザ・セッション中のデータを保護し、セッション終了後にキャッシュを消去できます。クライアントで作成されるセッション関連のすべてのデータは保護されます。  
 - ホストから切り離された安全な仮想環境を構築  
 - ブラウザおよびアプリケーションのキャッシュなど各種ファイルを暗号化し、セッション終了時に削除
- **DynamicID™によるダイレクトSMS認証**  
 Mobile Access Software Bladeは、エンドユーザの通信デバイス(携帯電話など)にSMSメッセージ経由でワンタイム・パスワード(OTP)を送信するように設定できます。SMSによる2ファクタ認証はセキュリティレベルをさらに高めると同時に、ハードウェア・トークンの管理に伴う

煩雑さを排除します。

- **侵入防御機能の統合**

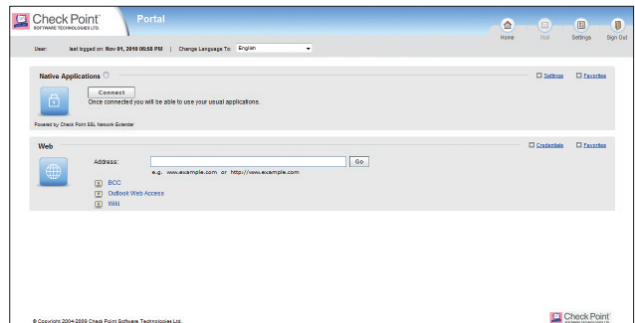
- Web関連のアプリケーションを経由する悪意のあるコードに対する防御を提供
- ワームや各種の攻撃(バッファ・オーバーフロー、SQL/コマンド・インジェクション、クロスサイト・スクリプティング、HTTPワーム、ディレクトリ・トラバーサル、ヘッダの拒否、悪意のあるHTTPコード)をブロック

## SSL Network Extender (オンデマンド・クライアント)

オンデマンドのブラウザ・プラグインを使用して、Webベースでない企業アプリケーションへ安全にアクセスしたい場合に適しています。

SSL Network Extender (SNX)は、Webベースでないネットワークアプリケーションにリモート・アクセスするためのブラウザ・プラグインで、リモート・アクセス機能と、IPベースのアプリケーションに対する完全なネットワーク接続機能を備えています。SSL Network Extenderを使用すると、企業リソースに接続するSSL VPNレイヤ3トンネルをオンデマンドで確立することができます。ICMP、TCP、UDPなどを使用するIPベースのアプリケーションをサポートしており、個々のアプリケーションを使用するために複雑な設定を行う必要はありません。また、管理者権限のないリモートPCでも動作します。

SSL Network Extenderは、SSL VPNポータルからエンドポイントのマシンに自動ダウンロードされます。そのため、クライアント・ソフトウェアを前もってデスクトップPCやノートPCにインストールして設定しておく必要はありません。アプリケーションのトラフィックは、暗号化と認証で保護されたSSLトンネルを介してSSL VPNゲートウェイに送信されます。



SSL VPNポータル: カスタマイズ可能なWebポータルから、Webベースおよび非Webベースの企業アプリケーションへ安全なアクセスを実現



### クライアントの仕様

デバイス	オペレーティング・システム
iPhone 3G、3GS	3.1.3以降
iPhone 4	4/4.01以降
iPad	3.2.2以降
Android	近日対応予定
Windows	XP、Vista、Windows 7 - 近日対応予定
Symbian	近日対応予定 (現時点ではSecureClient Mobileが対応)
Windows Mobile	現時点ではSecureClient Mobileが対応

### SSL VPN ポータルの仕様

Webブラウザ	バージョン
Internet Explorer	5.5以降
Firefox	1.0.3以降
Safari	すべて

### SSL Network Extender (SNX: オンデマンド・クライアント)の仕様

クライアント・デバイス	オペレーティング・システム	Webブラウザ
PC	Windows 7 (32/64ビット)、Vista (32/64ビット)、XP (32ビット)	Internet Explorer 5.5以降 Firefox 1.0.3以降
Mac	Mac OS X 10.4/5 (32ビット)	Safari
Linux	Fedora 8、Ubuntu 7、RHEL 3.0、Suse 9以降、Red Hat 7.3	Firefox 1.0.3以降

### ゲートウェイの仕様

ハードウェア	R71.10 (UTM-1、Power-1、IASなど) を推奨
オペレーティング・システム	SecurePlatform
バージョン	R71.10+iPhone HFA

### 管理プラットフォームの仕様

(管理プラットフォームには Security Management Server R71.10 が必須となります)

プラットフォーム	オペレーティング・システム
チェック・ポイント	SecurePlatform
チェック・ポイント	IPSO 6.2ディスク・ベース
Windows	Server 2003/2008 (32ビット)
Linux	RHEL 5.0/5.4 (32ビット)
Sun/Oracle (SPARC)	Solaris 8、9、10



---

## 製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F

<http://www.checkpoint.co.jp/> E-mail : [info\\_jp@checkpoint.com](mailto:info_jp@checkpoint.com) Tel : 03(5367)2500

---

© 2003-2010 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Abra, AlertAdvisor, Application Intelligence, Check Point DLP, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Pointのロゴ, Check Point Full Disk Encryption, Check Point Horizon Manager, Check Point Media Encryption, Check Point NAC, Check Point Network Voyager, Check Point OneCheck, Check Point R70, Check Point Security Gateway, Check Point Update Service, Check Point WebCheck, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, DefenseNet, DLP-1, DynamicID, Endpoint Connect VPN Client, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IP Appliances, IPS-1, IPS Software Blade, IPSO, Software Blade, IQ Engine, MailSafe, More, better, Simpler Securityのロゴ, MultiSpect, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, puresecurityのロゴ, Safe@Home, Safe@Office, Secure Virtual Workspace, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, SiteManager-1, Smart-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, SmartEvent, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartReporter, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SmartWorkflow, SMP, SMP On-Demand, SofaWare, Software Blade architecture, softwarebladesのロゴ, SSL Network Extender, Stateful Clustering, Total Security, totalsecurityのロゴ, TrueVector, UserCheck, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Edge, VPN-1 MASS, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VE, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm DataLock, ZoneAlarm Extreme Security, ZoneAlarm ForceField, ZoneAlarm Free Firewall, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Security Toolbar, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd.あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company.その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、7,165,076、7,540,013、および 7,725,737により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。P/N 500030-J 2010.11 ※記載された製品仕様は予告無く変更される場合があります。