

Nokia Secure Access System

Nokia Secure Access SystemはインテリジェントなSSL-VPNソリューション。インターネットに接続されたデバイスのブラウザからイントラネットやエクストラネットにアクセスする際に、認証技術を採用し、セキュアなアクセス・コントロールを提供します。

モバイル機器の普及により、ビジネス・ユーザーにとって、ビジネスの柔軟性と効率性がますます高まっています。しかし、同時にIT部門では新たな課題に直面しています。CIOおよびITマネージャーは、コストを削減しながら、ユーザーがどんなアクセス・デバイスを使っているかに係わらず、いつでもどこでも必要な企業内データにアクセスできるようなシステムを構築し、ユーザーのニーズに応えることが求められています。しかし、これらのニーズを満たすための技術が同時に企業資産を危険にさらす結果となっています。つまり、ユーザーの認証、使用している接続機器の種類、その接続機器のセキュリティ度を把握することが不可欠となってきており、これらの情報により適切だと判断されたデータのみが、アクセスされ、ローカルに保存され、あるいはネットワークへのアップロードされるように制限できる仕組みが求められています。

Nokia Secure Access Systemは、費用対効果に優

れたセキュアなアクセスを実現し、従業員やパートナー企業がブラウザからSSLを利用して企業内の電子メールやアプリケーションに接続できるようになります。ノキアのソリューションによって、ユーザーが誰であるか、使用している接続機器は何か、その時の接続機器のセキュリティ度はどのくらいであるかといった基準に応じて、同じユーザーであっても動的に、アクセスできる情報、ローカルに保存できる情報、あるいはネットワークにアップロードできる情報を制御することができます。ノキアは、ネットワークのインテグリティを確保しながら、いつでも、どこでも、どんな接続機器からでもアクセスを可能にし、ビジネスに柔軟性を提供します。

ビジネス上のメリット

生産性の向上：Nokia Secure Access Systemを使えば、企業のモバイル・ユーザー、在宅勤務者、企業から貸与されたデバイスを持たない従業員をもセキュアに接続することができます。情報の流れを合理化し、ビジネス・プロセスの最適化を図ることができます。

リモート・アクセスの総費用を削減：リモート・アクセス・システムにかかる莫大な費用は、数多くのクライアントの導入およびその管理に起因しています。標準のSSLブラウザを使用することで、Nokia

Secure Access Systemは容易な管理と高いROI（投資収益率）を実現します。

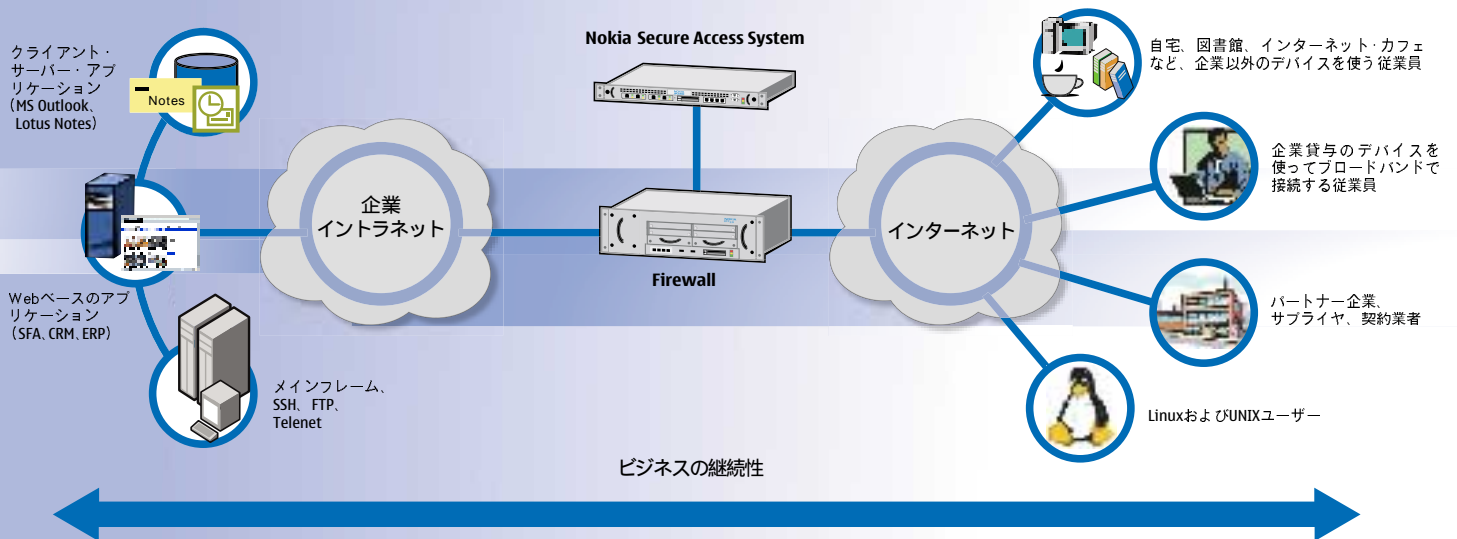
企業の情報資産を保護：Nokia Secure Access Systemは、企業内のアプリケーションと従業員やパートナー企業との簡素かつ拡張性のあるセキュアな接続を提供します。企業内の様々な情報へアクセスコントロールすることにより、企業の情報資産のセキュリティを確保します。

情報のモバイル化：電子メールおよびミッション・クリティカルなアプリケーションへ、インターネットに接続されたデバイスであれば、企業貸与または個人のデバイス問わずアクセスできるようになり、今後このようなモバイル化を通して、情報の可用性が高まると考えられます。

複数の言語を一台でサポート：複数の言語を一台のNokia Secure Access Systemで同時にサポートし、海外拠点や海外パートナー企業との容易な接続を可能にします。

主な機能とメリット

クライアント・インテグリティ・スキャン：クライアント・インテグリティ・スキャンはNokia Secure Access Systemの独自の機能で、リモート・デバイ



スのオープンTCPポート、悪いファイル、良いファイル、アクティブ・プロセスを調べることにより、企業データのセキュリティを向上させます。例えば、異常なオープン・ポートが見つかった場合、リモート・デバイスにトロイの木馬が存在している可能性があります。既知のウイルスは、悪いファイルの一例です。良いファイルは、最新のアンチ・ウイルス定義によって識別されます。また、Windowsタスク・リストには、パーソナル・ファイアウォールなどのアクティブなプロセスが動作中であることが表示され、疑わしいソフトウェアのアクティビティが通知されます。

アドバンスド・アクセス・コントロール: Nokia Secure Access Systemは接続状態に基づくアクセス・コントロールを実現し、独自の方法でセキュリティを向上させます。リモート・ユーザーのアクセス・レベルは、クライアント・インテグリティ・スキャンの結果またはデジタル証明の有無に応じて、変更が可能です。例えば、リモート・デバイスが一定レベルのウイルス対策機能を備えている場合に限り、ファイルのアップロードやダウンロードを許可するように設定することができます。リモート・デバイスを個別に認識するデジタル証明書がクライアント側に存在することで、ユーザーに許可された認証レベルをコントロールすることも可能です。アクセス・コントロールの構成は、ユーザーやユーザー・グループを直接リソースに追加することができるため、非常に簡単です。

セッション・パーシステンス機能: Nokia Secure Access Systemの独自機能であるセッション・パーシステンス機能を利用すれば、操作をせずに一定時間が経過してしまったためSSLセッションがタイムアウトしてしまっても、データを損失することなく仕事を再開することができます。Nokia Secure Access Systemを使って接続していれば、仕事が中断されてしまっても安心です。

認証および監査:

- デジタル証明書ベースの認証とアクセス権許可が可能で、システム管理者はひとつのユーザーIDに対して複数のクライアント証明書を適用することができます。また、一人のユーザーに対して、リモート・デバイスごとに異なるレベルのアクセス権を設定することが可能です。
- システム管理者はユーザーおよびユーザー・グループを直接リソースに割り当てることでアクセス構成を行うことができるため、管理の簡素化が図

れます。また、RADIUS上でSecureIDを介し、2段階の認証を利用することができます。

- ローカル、RADIUS、LDAP、NTDメイン、NISなどの幅広い認証方式をサポートしています。
- ユーザー・アクティビティの詳細なログを保存することが可能。ログはsyslogサーバーに転送することが可能で、システム・イベントのみをログするように設定することができます。

標準Webブラウザをクライアントとして利用: 幅広く利用されているSSL対応ブラウザにより、リモート・クライアントの配布の必要を解消。セキュリティが向上するだけでなく、企業内リモート・アクセス・システムにかかる費用の節減と管理の複雑さの軽減が実現できます。

SSL暗号化: SSL暗号化を利用した監査、認証、アクセス・コントロールを組み合わせて、さらに独自のセキュリティおよび生産性向上機能を統合化することで、ノキア・ソリューションは、Webブラウザを搭載したデバイスでインターネットに接続し、企業内アプリケーションにアクセスする際に、セキュアで認証かつコントロールされたアクセスを提供します。SSL技術はインターネットで利用され、年間で数十億ドルにも相当するビジネス・トランザクションを保護。この広く普及している技術を活用することにより、Nokia Secure Access Systemは、企業のリモート・アクセス・システムにおけるROIを向上します。

ポートフォワーディング・プロキシ: Nokia Secure Access Systemを使用すれば、パートナー企業や従業員に対して、クライアント・サーバー・アプリケーションへのセキュアなアクセスを提供することができます。遠隔地からノートPCを使って接続している従業員は、Nokia Secure Access Systemを利用し、MS Outlookクライアントを使って電子メールにアクセスすることが可能です。ERPクライアントを使用している契約製造業者は、セキュアなコネクションを確立して、最新の製造データを入力することができます。

ノキアのコンプライト・システム・アプローチ: 実績あるノキアのコンプライト・システム・アプローチに基づいたNokia Secure Access Systemは、SSLリモート・アクセス市場に、セキュリティ、信頼性、管理性をもたらします。ノキアIPセキュリティ・プラットフォーム・シリーズは、一流企業やサービス・プロ

バイダの大きな信頼を得ており、クリティカル・ファイアウォール、VPN、IDS機能の運用に利用されています。Nokia Secure Access Systemは、SCP認定のグローバル・サポート＆サービスによってサポートされています。

仕様

サポートしているノキアIPセキュリティ・プラットフォーム

- Nokia IP130
- Nokia IP350
- Nokia IP380
- Nokia IP1260

ソフトウェアライセンス

- 10、25、50、100、250、500、1200ユーザーライセンス

セキュリティ機能

- 堅牢なノキアIPS0オペレーティング・システムを搭載したセキュア・アプライアンス
- SSL/TLS暗号化によるアクセス・セキュリティ
- サポートしている暗号化アルゴリズム: RSA, 3DES, AES, RC4, DES, RC2
- アドバンスド・アクセス・コントロール機能
- 接続状態に基づく認証
- リモート・デバイスにより、アクセス・レベルをダイナミックに変更可能
- クライアント・インテグリティ・スキャン機能
- ログイン情報の暗号化
- 非キャッシュ動作モード
- 複数のイーサネット・ポートが実装されているため、物理的なセキュリティ・パーティショニングが可能

認証および監査機能

- 幅広い認証方式: ローカル・パスワード、RADIUS、LDAP、NTDメイン、NIS
- 2段階の認証方式: RADIUS上のSecureID
- PKIによるユーザー認証のためのクライアント証明書
- PKI以外のX.509証明書を使用するRSAパブリックキーのユーザー認証
- ひとつのユーザーIDに複数の証明書の割り当てが可能
- ユーザーおよびユーザー・グループをリソースに割り当て可能
- ユーザー、アプリケーション、リソース、時間、イベントによってログイン、システム・イベントのみをログするように設定可能
- syslogサーバーへのレポート機能

サポートしているアプリケーション

- ブラウザ: IE5.0以降、Netscape 6.2xおよび7.x、Mozilla 1.0
- Webプロトコル: HTTP, HTTPS
- Webスタンダード: HTML, Java Applets, JavaScript
- ファイル共有プロトコル: Windows (CIFS), UNIX (NFS), FTP
- クライアント・サーバー・アプリケーション: MS Exchange, Lotus Notes, Citrix
- 電子メールおよびファイル転送プロトコル: SMTP, POP, IMAP
- 端末エミュレーション・プロトコル: Telnet, VT100, TN 3270

管理および操作性に関する機能

- Webベースの管理インターフェイス
- Telnet, FTP, HTTPS, SSHを使って、構成および管理が可能
- Nokia Horizon Managerを使って、アプリケーション・パッケージのバックアップ、リストア、プッシュを実行
- トランスベアレント・モードにより、外部URLをマッピング
- セッション・パーシステンス機能により、SSLタイムアウトによるデータ損失を防止

ノキア・ジャパン株式会社

エンタープライズ・ソリューションズ事業部 www.nokia.co.jp

〒153-0064 東京都目黒区下目黒1-8-1 アルコタワー
Tel: 03-5437-3250 Fax: 03-5745-7943
E-Mail: info.nes-jp@nokia.com

Copyright Nokia 2004. All rights reserved. NokiaおよびNokia Connecting People は Nokia Corporation の登録商標です。Check Point, Check Pointロゴ, FireWall-1, VPN-1は Check Point Software Technologies, Ltdまたは同関係各社の商標または登録商標です。ここに記載されたその他の社名は、各所有者の商標または商号である可能性があります。ノキアは継続的開発という方針を実践しており、したがってノキアは、本文書に記載されたいずれの製品についても、予告なく変更や改善を行う権利を保有します。ノキアはいかなる状況においても、いかなる原因による直接的、特殊、偶発的、結果的、または間接的な損害に対しても、責任を負わないものとします。

NSAS-0406

代理店/販売店

株式会社富士通ソーシアルサイエンスラボラトリー
営業本部 ソリューション推進部

〒211-0063 川崎市中原区小杉町1-403

武蔵小杉タワープレイス

TEL 044-739-1251

E-mail: ssl-info@cs.jp.fujitsu.com

URL: <http://www.ssl.fujitsu.com/>

NOKIA
CONNECTING PEOPLE