



# 東京海上日動リスクコンサルティング株式会社様

## Lotus Notes/Domino モバイル アクセス最前線 ～リスク管理のプロ集団に学ぶ Notes モバイル活用法～

ご購入ライセンス: 300名

グループウェア: Lotus Notes/Domino

東京海上日動リスクコンサルティング株式会社 (TRC) は、東京海上のノウハウをもとに 1996 年に誕生した、企業を取り巻くリスクを的確に発見・評価し、実効性の高いリスクソリューションを提案するコンサルティング会社である。

豊富な実績に加え、さまざまな研究を行う専門機関との提携や事故災害データベースなどを活かし、企業のニーズに合った高度なコンサルティングで信頼に込めている。

\*この事例紹介は、2009年1月に都内で開催された「Lotus Notes/Domino モバイルアクセス最前線! ～リスク管理のプロ集団に学ぶ Notes モバイル活用法～」と題するセミナーにおける東京海上日動リスクコンサルティング株式会社経営企画室の菊地氏による講演と、それに続くパネルディスカッションの内容をまとめたものです。

### 東京海上日動リスクコンサルティング株式会社

設立 1996年8月1日  
本社所在地 東京都千代田区丸の内 1-2-1  
資本金 100,000,000円  
代表取締役社長 上垣内 健

組織 企業財産事業部  
BCM 事業部  
ERM 事業部  
製品安全・環境事業部  
自動車グループ  
開発グループ  
経営企画室

### 実は出張の多いリスクコンサルティングの現場

地震などの自然災害や火災、事件・事故などで会社にどのような被害が生じるかを想定し、そのリスクを管理 (マネジメント) するのがリスクマネジメントである。

一方、企業を取り巻くリスクを評価して、コンサルティングするのがリスクコンサルティングというわけだ。

TRC の社内システムの企画・運用を担当する菊地氏は、「コンサルティングは事務所中心の仕事と思われる方が多いと思いますが、実は、リスク評価で現地出張することが結構多いのです。」という。

となると、出張先からメールを使いたいという要望が出てくるのは当然だろう。

TRC ではグループウェアとして Lotus Notes/Domino を採用しており、2006 年に社外からメールを利用できる環境を構築した。

このときはメール本文のみを対象として、外部サービス (ASP) を利用したが、運用コストの問題もあり、利用できるのは一部の社員に限られていた。

ところが、最近になって社外からメールを利用したいという人が増え、また、Notes のカレンダーやアドレス帳も使いたいという要望も増えてきたこともあり、システムの拡張を検討し始めた。

### リスク管理の考え方を取り入れたシステムの社内提案

セミナーでは、投資対効果 (Return On Investment) をもじって、リスク対投資 (Risk On Investment) という言葉を使い、「モバイル アクセスなどのセキュリティシステムを社内提案する場合は、リスク対投資が重要。」と説明した。

「リスクがあるから実行しないのではなく、どこにどのようなリスクがあるかを明確にし、それをマネジメント (管理) していく発想が大切」という。

モバイル アクセス システムの場合、様々なセキュリティのリスクに対して、どのように対処するか (もしくは対処しないか) を明確にすることが大切だということだ。



東京海上日動リスクコンサルティング株式会社  
経営企画室 管理グループ  
主任研究員 菊地 隆司 氏

## PC アクセスと携帯アクセスはシステムを分けて考える

モバイル アクセス システムの導入にあたっては、まず「どのようなデバイスからアクセスするのか。」ということを考える必要がある。

ノート PC を使ってモバイル アクセスを行えば、社内と変わらない環境を実現できるが、持ち運びが大変だ。逆に、携帯電話は手軽だが機能は制限される。

社内要望を分析した結果、携帯電話ではメールとスケジュールのみで良いことが分かった。

このため、携帯電話向けには機能を絞ったシステムを導入することにした。

ノート PC 向けと携帯電話向けにシステムを分けることで、セキュリティ対策を単純化することができる。

TRC では、結果的に1つのシステムを導入するより総投資額を抑えることができた。

これも、リスク対投資 (ROI) のバランスをとった結果と言える。

## ASP 型か自社運用型か

次に考えるべきなのは、システムの運用形態を ASP 型と自社運用型のどちらにするかということだ。

一般には、ASP 型は自社運用に比べて運用管理の手間がかからないとされている。

ところが、「システム運用の設計がしっかりしていれば、ASP 型でも自社運用型でも、運用負荷はそれほど変わらない。むしろ、システム管理者の運用業務のほとんどが、ID 管理 (ユーザーの追加、削除等) である。」という。

確かに ID 管理については、ASP 型でも自社運用型でも、必要とされる運用負荷はまったく同じだ。

また、自社運用型の場合は、セキュリティポリシーの変更に対応しやすいが、ASP 型の場合は、ベンダーが対応できない可能性があることも問題視している。

これらと、5年間の TCO (総支払費用) の比較から、TRC では自社運用型の方がメリットがあると判断したようだ。

## 個体識別認証かマトリクス認証か

モバイル アクセスのセキュリティを考える上で非常に重要なのが、認証方式だ。

携帯電話には、電話番号とは別に、機器自身が持つ個体識別番号がある。

ID とパスワード以外に個体識別番号を使って認証できると、セキュリティ上非常に効果が大きい。

しかし、この方式では、端末を変更する度に再設定が必要となり、ID 管理の負荷が増大する。

利用するか否かは企業ごとの状況に応じて選択すべきである。

ConnectONE の個体識別番号による認証機能は、セキュリティポリシーの変更に対する運用の柔軟性があると TRC に評価された。

これに対し、ASP 型は標準機能としてマトリクス認証が用いられていることが多い。

マトリクス認証は、キーロガーなどのパスワード アタックからの防御を目的としているが、パスワード入力力が非常に面倒である。

ConnectONE は、個体識別番号による認証を利用できるので、マトリクス認証を使わなくともセキュリティを確保することができる。

## 携帯専用アプリの導入が不要

他社の製品では、携帯電話に専用アプリを導入するタイプがある。

このタイプは、ユーザーインターフェースの表現力は高いが、メール閲覧時の処理速度が遅い傾向にある。

また、新機種への対応が遅れる可能性があり、運用面での不安が残る。

しかし、ConnectONE は専用アプリを導入しない方法のため操作性に優れ、TRC にこれらの点が評価された。

モバイルアクセスの機能比較表  
(セミナー資料より抜粋: TRC 菊地氏作成)

比較項目	ConnectONE	A社	B社	C社
提供形態	ソフトウェア	ソフトウェア	ASP	ASP
端末個体認証	◎標準	×	◎標準	×
マトリクス認証	×	×	◎標準	◎標準
携帯専用アプリ	不要	必須	どちらも可能	不要
画面メモ対策	◎標準	◎標準	×	×
添付ファイル	◎標準	◎標準	×	×
カレンダー	◎標準	◎標準	◎標準	△ (オプション)
アドレス帳	◎標準	◎標準	◎標準	△ (オプション)
パソコンでの利用	◎標準	×	△ (オプション)	◎標準
総費用 (5年間累計)	1	1.9	2.1	6

\*総費用は ConnectONE を 1 とした場合の相対値

## 各社製品の主要機能の比較

TRC はモバイル アクセス システムの導入前に、極めて詳細な機能上の比較検討を行った。今回のセミナーでは、その検討結果を特別に紹介してくれた。

### 画面メモ対策

携帯ブラウザ経由のアクセスの場合、携帯電話の画面メモ機能を使って表示内容を携帯に保存することができるため、情報漏えいのリスクが生じる。しかし、ConnectONE は画面メモでも携帯電話に表示内容を残すことができない。

この点が、TRCに評価された。

### 添付ファイルの閲覧

メールの添付ファイルは、TRC では「見えた方が良さそうだが、どうしても必要というわけではない。」と考えた。

ConnectONE は添付ファイルの閲覧にも対応しているので、TRC では今後の社内要望をみて対応する予定とのことだ。

### メール、スケジュール

メールとスケジュールは、最も多い要望だったので、対応しているかは非常に重要なポイントとなる。



### アドレス帳

ConnectONE は、Lotus Notes/Domino のアドレス帳をそのまま使えるので、携帯電話内にアドレス帳を持つ必要がない。また誤送信するリスクも少なくなるので、非常に安全である。

### PC アクセス

ConnectONE は PC アクセスも携帯アクセスもサポートしているが、TRC では、携帯のソリューションと PC のソリューションを分けており、相互にはアクセスできないようになっている。これにより、セキュリティの確保を狙っている。

## 圧倒的なコストパフォーマンスが ConnectONE の強み

TRC での導入時に実際に運用コストを計算したところ、結果は予想を上回るものだった。(前ページの表)

ConnectONE を採用した場合の5年間のTCO(総支払額)は、あるASP サービスと比べて約1/6と、圧倒的であることがわかった。

ASP 型は初期投資を抑制できるが、機能的にほぼ同等で、システム運用の負荷がそれほど変わらないとなると、運用コストが高いASP方式を選択するメリットは低くならざるを得ない。

## パネル ディスカッション

パネル ディスカッションでは、ITmedia エンタープライズの浅井編集長がモデレータとして参加。さらに菊地氏、日本アイ・ピー・エムの森島氏、TIS の吉原氏、コネクワンの吉田が加わり、活発な議論が行われた。

浅井氏が ASP サービス のセキュリティについて尋ねると、菊地氏はポリシーの変更とセキュリティ レベルの関係について指摘した。

「自社のセキュリティ ポリシーを変更した場合、ASP ベンダーが対応できないことが考えられ、それは可能な限り避けたい。社内情報システムのセキュリティレベルがモバイル アクセスの ASP のセキュリティレベルに依存するのはハイリスクと言える。」ということだった。

一箇所でも脆弱な部分があると、それが企業のセキュリティ リスクになってしまうからだ。



アイティメディア株式会社  
エンタープライズ・メディア事業部  
執行役員  
エンタープライズ・メディア事業部長  
兼 ITmediaエンタープライズ編集長  
浅井 英二 氏



日本アイ・ピー・エム  
ソフトウェア事業部  
ブランド・マーケティング  
森島 秀明 氏

## 災害時の緊急連絡にも、モバイル アクセスを利用

TRC がユニークなのは、総務や人事など、バックオフィスのスタッフにも ConnectONE のアカウントを提供していることだ。

通常、外出する機会の少ない部門には、アカウントを発行しない会社がほとんどではないだろうか。

ConnectONE のコストが低いとはいえ、一見効果が低いと思われる投資をなぜ行うのか？ 実はここに、リスクコンサルティングの会社ならではの発想が隠されていた。

企業の重要なリスク管理として BCP (Business Continuity Plan = 事業継続計画) がある。

BCP は、災害や事故などの予期せぬ出来事が発生した場合にも事業を継続できるように、あらかじめ行動計画を作っておくもので、従業員の安否確認も BCP の重要な項目の一つである。

もちろん、TRC でも安否確認システムを導入しているが、さらに ConnectONE を BCP のツールとして使うことを考えているのだ。

菊地氏は、「安否確認システムなどは、日常のオペレーションとはかけ離れていることが多いのです。緊急時だけ、ほとんど使ったこともないシステムを使うのはハードルが高いし、間違いも起こりやすい。そこで、利用頻度の高い ConnectONE を安否確認のツールとすることで、安否確認をスムーズに行うことができます。安否確認の手段は多いほど良いのです。」という。

モバイル アクセスを使って災害に備える、というのはなかなか出てこない発想である。リスク管理の専門家であるからこそその発想ではあるが、他の企業も見習うべき点はあるだろう。

## 東京海上日動リスクコンサルティング株式会社 (TRC) が ConnectONE を選んだ理由 ～まとめ～

さまざまな角度から 4 つの製品・サービスを比較してきた TRC だが、最終的に ConnectONE を採用した理由として、以下の 5 つを挙げている。

### 圧倒的なコストパフォーマンス

ConnectONE の 5 年間の TCO (総支払費用) は、他社に比べて最も差がある場合で 1/6 だった。

この圧倒的なコストパフォーマンスにより、全社員が利用することが可能となり、BCP ツールとしても活用可能になった。

### 操作の軽さ

ConnectONE は、処理速度がダントツに速く、菊地氏は通勤中の地下鉄でも使用している。

「駅で受信、走行中に作成、次の駅で送信」も簡単にでき、今まででは想像できない効率的な時間の使い方が可能だ。

### システムがシンプルで管理が容易

ConnectONE の運用を開始して数カ月経過したが、TRC では ID 管理以外のシステム運用業務は行ったことがない。

シンプルなほど障害が発生せず、また、障害が発生しても簡単に復旧できるので、システムの運用負荷は非常に少ない。

### 機能アップの頻度が多い

ConnectONE は、サポート品質が高く、また、新機能への要望も真摯に対応できる製品と TRC から評価を得ている。

「セキュリティポリシーを変更してもコネクトワンは必ず対応すると確信できる。」というほど絶大な信頼を寄せている。

### 情報漏洩への高いセキュリティ

ConnectONE のサーバーは情報を保存せず、携帯電話の画像メモでもメール情報を保存できない。

万一、携帯電話を紛失・盗難した場合でも、ConnectONE なら企業の機密情報は漏洩しない。



株式会社 コネクトワン

〒100-0047 東京都千代田区内神田 1-12-3 翔和内神田ビル 3F

TEL 03-3293-8880 FAX 03-6368-6912

Mail: contact2008@connectone.co.jp

http://www.connectone.co.jp/

お問い合わせ