企業向けカスタムブラウザソリューションの展開

The Development of a Solution with Custom Browser for Business

畠山　誠基　Hatakeyama Seiki
庄司　秀明　Shoji Hideaki
稲葉　朋子　Inaba Akiko
工藤　英治　Kudo Eiji
阿部　諒平　Abe Ryohei

近年，スマートフォンなどの急速な普及に伴い，これらを企業の情報システムに活用しようとする動きが活発になっている。この急速に拡大する市場では新たなセキュリティの脅威として不正なアプリケーション（以下不正アプリ）の対策が急務になっている。先頃，発見された不正アプリは，バッテリの節約と称して機器内部の個人情報を採取するものであった。これは，従来のウィルスとは異なり，外部から不正アプリであることを見破ることが難しいとされている。

このような背景のもと，㈱日立東日本ソリューションズ（以下日立 TO）は，不正アプリの対策機能をもつ企業向けのセキュアブラウザ「Custom Browser for Android」を製品化し，企業の個別要件にも対応するカスタマイズサービスと合わせて販売を開始した。急成長する市場でより多くの企業がスマートフォンなどを安全に業務活用できる環境整備に向けて機能拡張を進めていく。

１．はじめに

近年，スマートフォンなどが急速に普及してきており一般家庭や個人で使用するだけでなく，企業の情報システムに活用する動きも活発になっている。その中でもタブレット端末は，近い将来 PC に置き換わる可能性も示唆されており，企業での関心も高まっている。このタブレット端末は，2007 年に登場した米 Amazon 社の電子書籍端末からはじまり，自社のクラウドサービスである書籍購買サイトへ優先的に接続させ，サービスの収益をアップさせる戦略が話題になった。その後，2010 年には米 Apple 社の iPad が続いた。こちらも AppStore や iTunesStore といった自社が運営するサービスサイトへの囲い込みが行われ，日本国内でも普及している。同年 2010 年，米 Google 社のオープンソースである Android OS を搭載した端末が日本国内の端末メーカや通信キャリア，中国，韓国，台湾の端末メーカから続々と発売された。この Android 端末も Google Play でアプリケーション（以下，アプリ）を配信するモデルである。

このように米国では 2007 年以降，日本国内では 2010 年以降に登場したタブレット端末は，クラウドサービスと密接な関係にあり，自社の運営するサービスのサイトに対する囲い込みのアプローチがとられている。このアプローチにより Web ブラウザも，URL を直接入力する汎用的なスタイルから，特定のサービスへ優先的に接続するアプリとして位置付けが変わりつつある。今回，日立 TO で開発した「Custom Browser for Android」（以下，本製品）は，こうした特定のサービスへアクセスするスタイルを実現する。そして，このスタイルは一般企業の情報システムでもセキュリティ対策として効果が期待できる。以下，第 2 章でタブレット端末を取り巻く環境，第 3 章で製品コンセプト，第 4 章で本製品の機能および他製品と連携したソリューションの展開について述べる。

２．タブレット端末を取り巻く環境

2.1　拡大するスマートフォンなどの市場

スマートフォンなどの市場は，世界規模で拡大[1)]している。日本国内でも 2009 年から 2011 年にかけて表1に示すように販売台数が 1.4 倍に伸びている。その中でも，

表１　スマートフォンのエンドユーザ販売台数

OS	2009	2011
iOS	7.4 %	**20.7 %**
Android	0.7 %	**44.4 %**
Symbian	50.3 %	19.2 %
RIM	0.5 %	0.3 %
Microsoft	1.2 %	0.3 %
その他	39.9 %	15.1 %
合計(100 万台)	17	25

（出典：総務省　平成 24 年度版情報通信白書）

iOS と Android が急激に伸びている。OS 別の人気機種では，米 Apple 社 iPhone4（iOS）が 2010 年 6 月発売開始から，韓国サムスン社 GALAXY S II（Android）が 2011 年 6 月発売開始から急速に伸びている。一方タブレット端末では米 Apple 社 iPad（iOS）が 2010 年 4 月販売開始，国内の端末メーカを含む Android 勢は 2010 年の後半から販売開始となっている。

2.2 タブレット端末の利用シーン

タブレット端末は，タッチパネル式の液晶画面をもち，軽量で起動速度が速く，持ち運びに適しており，商品カタログやシミュレーション結果をその場で見せられるなど，プレゼンテーション効果を高めることに活用できる。図 1 にタブレット端末の利用シーンとシステム構成例を示す。利用シーンでは，様々な場所で利用できることから，業務効率や設備効率が上がることと，パンデミックや災害時の備えとしても BCP（Business Continuity Plan）対策に効果が期待できる。その他，柔軟なオフィスワークや展示会，出張店舗でのプレゼンテーションでは，モバイル PC にはない新たなアプローチも生まれることが期待できる。タブレット端末の利用形態としては，既存の Web システムやクラウドサービスなどが考えられる。タブレット端末には，Wi-Fi*1や 3G*2の通信機能が備わっているため，社内だけでなく，社外からもインターネットを介して業務システムにアクセスできる。その他，予めドキュメントなどをダウンロードしておき，通信回線を使用せずにドキュメントの閲覧やプレゼンテーションを行うこともできる。その場合は，ドキュメントのダウンロードや閲覧する専用のアプリを開発することで利便性を高めることができる。

2.3 ビジネス用途での課題

一方，タブレット端末の業務活用では，ハードウェアの制約などの課題もある。一般的な，タブレット端末導入時の検討課題を以下に示す。

① 無線通信により常時情報漏えいのリスクがある
② キー入力には慣れが必要である
③ バッテリによる駆動時間が短い
④ 無線通信環境が整備されていない場所や回線が混雑する時間帯にはつながりにくい
⑤ 端末製品のライフサイクルが短い
⑥ 既存 Web アプリケーション（業務システム）との I/F が合わない場合がある
⑦ セキュリティ対策製品が PC に比較すると成熟していない

上記の検討課題の①は，利便性とのトレードオフを考慮する必要がある。②～⑤は，端末メーカが公表する機器仕様を評価して選定する必要がある。⑥は，既存の業務システムが PC 用のブラウザを前提に設計されていることが多く，タブレット端末用のブラウザとの互換性がないケースもある。⑦は Android をターゲットにした新

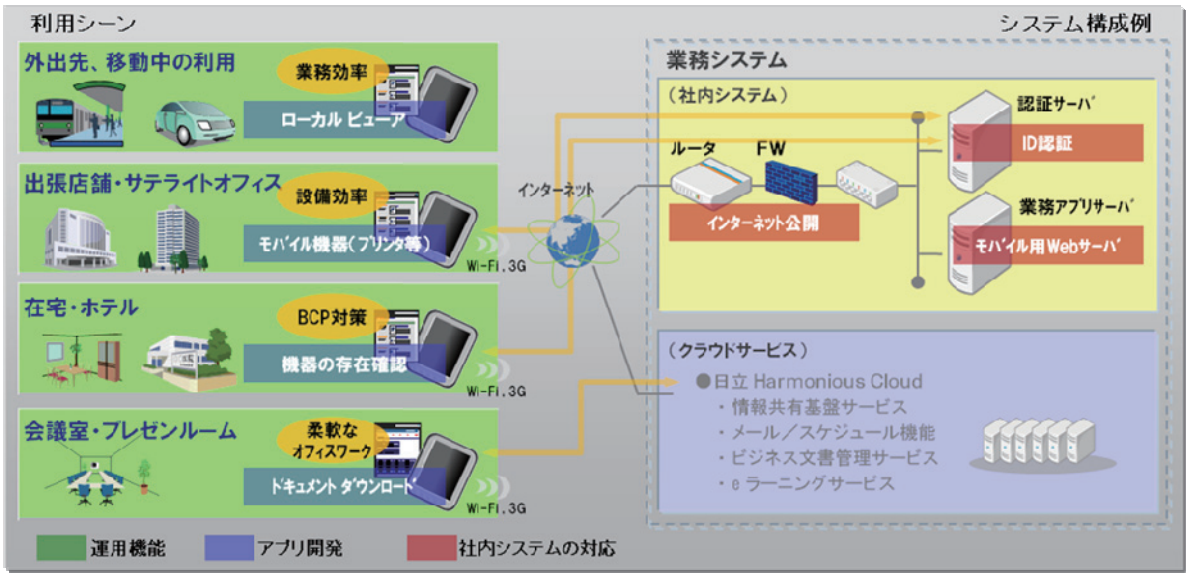

図 1 タブレット端末の利用シーンとシステム構成例

*1 Wi-Fi Alliance の認証する相互接続可能な無線機器
*2 3rd Generation，第三世代と呼ばれる携帯電話回線

種のマルウェアも発見されており，対策が強く求められている。

３．製品コンセプトと機能

3.1 Android 端末のセキュリティ脅威

Android 端末のセキュリティ脅威は，モバイル PC と同様にマルウェア感染，第 3 者による不正利用・不正アクセス，通信の盗聴・改ざん，紛失・盗難時の情報漏えいが挙げられる。この中でも特に Android 端末では，マルウェアへの対策が強く求められている。2012 年 5 月に発表された IPA の注意喚起 [2] にもあるように Android 端末をターゲットにした不審な動作をする不正なアプリが数多く発見されている。この不正アプリの中には，OS の脆弱性を狙ったものもあり，勝手に SMS メッセージ*3を送信したり，端末内の情報を盗んだりするものもある。こうした不正アプリの対策は，IPA のレポート [3] にあるとおり，端末ベンダの OS アップデートで対策されているものもある。しかしながら先頃発見されたマルウェア [4] の中には，普通のアプリを装い，外部から不正を見破ることが難しいものが現れた。この不正アプリは，バッテリの節約と称してユーザにインストールを促し，インストールした後に実行すると「お使いの端末は未対応のためご利用いただけません」と表示される。その間に連絡先などの個人情報が外部サイトへ送信されてしまうという手口である。通常，Android 端末は，アプリのインストール時にそのアプリが必要とする権限を図 2 に示すようなインストール画面で必ず通知する。

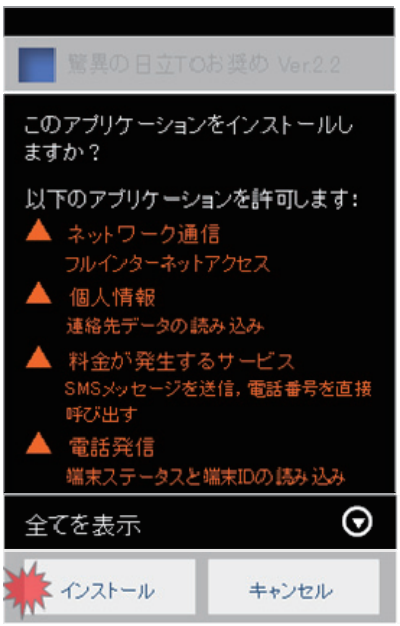

図 2 Android アプリのインストール画面

ユーザがインストールするアプリを不審に思った場合は，インストールをキャンセルすることもできる。このように Android 端末は PC のウィルスのようにネットワークに接続しただけで感染するタイプのものではなく，ユーザが注意深くインストール画面を確認すれば予防できる。しかし，この仕組みが提供されているにもかかわらず，それでも Android 端末のマルウェア被害が後を絶たない状況であることから，不正アプリ対策として，ユーザの確認だけに頼らないシステム的な対策が求められている。

3.2 一般的な不正アプリ対策

このような不正アプリの対策には，MDM（Mobile Device Management）ツールやウィルス対策ソフトを適用するのが一般的になっている。これらのツールでは，モバイル PC と同様にリアルタイムで端末の状態を監視し，定期的にウィルスをスキャンして不正アプリを検知する機能が提供される。一度，端末内に不正アプリがインストールされると端末内の情報が盗み取られてしまうことから，検知の精度を上げるために監視のサイクルは可能な限り短くすることが必要である。しかし，このような運用では，次のような影響も考えられる。

(1)バッテリ消費の影響

MDM ツールは，端末と管理サーバ間で頻繁に通信を行う。また，ウィルススキャンは端末内のデータをすべてスキャンする。これらはバッテリの消費を早める。そのため，充電可能な環境でだけこれらのツールを運用するしかなく，持ち運び時の運用が行えない。そのため，不正アプリの検知にリアルタイム性が損なわれてしまい，検知のタイミングによっては，不正に情報が抜き取られた後に検知することになる。

(2)管理サーバを経由しない Wi-Fi 通信

多くの Android 端末でサポートされている Wi-Fi 通信機能は，3G 回線を経由せずにインターネットアクセスができる。そのため，MDM ツールなどの管理サーバが提供する一般サイトのフィルタリングが行われず，ユーザは，アプリを追加することができてしまう。この Wi-Fi 通信の対策として，強制的に通信を無効化することもで

*3 ショートメッセージサービス。電話番号を利用するメッセージの送受信サービス。

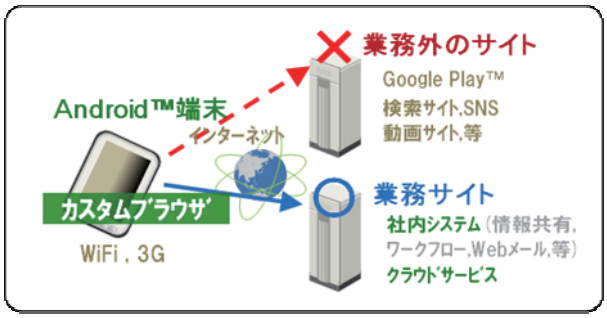

図 3　URL フィルタリング機能

きるが，その場合，社内の利用シーンでも 3G 回線を使用することになり，オフィスの立地条件や回線の混雑状況によっては，社内システムの利用に影響がでることもある。

3.3「Custom Browser for Android」のアプローチ

前述のように一般的な不正アプリの対策には Android 固有の課題がある。そこで，本製品ではこれらの課題も踏まえて，バッテリ消費の影響が少ない方式でなおかつ端末内で閉じた不正アプリ対策の機能を開発した。図 3 に URL フィルタリング機能を示す。本製品は URL をキー入力する領域をもたない。端末でアクセスする業務サイトの情報は，URL リストとして設定ファイルを端末内に配置する。ユーザは，この設定ファイルを追加・編集することができないため，設定ファイルに定義されていないサイトは，一切アクセスできない。この設定ファイルは，管理者がホワイトリスト方式で設定して端末に配布しておく。この方式により，不正アプリを配布する可能性のある一般サイトをすべて禁止し，不正アプリの対策ができる。さらに，許可された業務サイト内に一般サイトへの外部リンクがある場合や JavaScript で外部リンクする場合もフィルタリングの対象となる。またフィルタリングは不正アプリを配布するサイトへのアクセスばかりでなく，多くの企業で規制している業務に関係のないサイトの閲覧も防止することが可能となる。このように，端末内で閉じたフィルタリングになるため，管理サーバへ頻繁にアクセスすることもなく，バッテリ消費の影響も軽減できる。また，Wi-Fi 通信でもフィルタリングが適用されるため，タブレット端末に適した対策であると考える。

3.4「Custom Browser for Android」の前提条件

「Custom Browser for Android」で一般サイトへのフィルタリングを行っていても，Google Play および標準ブラウザなどが使用可能であればセキュリティの確保は行えない。外部への接続手段が「Custom Browser for Android」だけとなるよう，端末のキッティング*4 を実施する必要がある。

4．タブレット端末ソリューション

4.1「Custom Browser for Android」の機能

企業がタブレット端末を安全に利用するためには，第 3 者の不正利用・不正アクセスにも防御が必要である。通常，これらの対策には端末の個体識別番号が使われることが多い。しかし Android 端末は，個体識別番号をもたないものやリセットにより番号が変わるものもあり，業務サイトで厳格な認証が行えないケースが発生する。そこで，本製品では端末の不正使用を防ぐことを目的に，端末毎にユニークな識別情報をもたせるアカウント認証機能を提供する。図 4 にアカウント認証機能を示す。

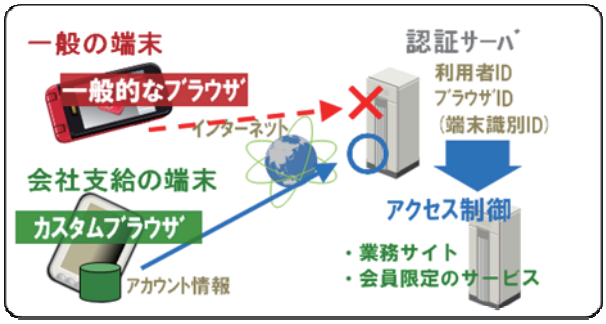

図 4　アカウント認証機能

アカウント認証には，端末の識別情報による端末認証と，利用者 ID による個人認証の 2 とおりの認証方法がある。どの認証機能を利用するかは管理者が選択可能である。管理者の選択によっては，利用者 ID での個人認証だけとし端末認証を省略することで利用者に ID/パスワードを何度も繰り返し入力することを抑えることができる。

その他，本製品では，盗聴・改ざんや情報漏えい対策として次の機能も提供する。

- SSL/VPN
- ファイルダウンロードの抑止
- JavaScript，スクリーンショットの抑止
- Cookie，キャッシュの自動クリア

上記の JavaScript や Cookie を抑止する機能は，業務システムの状況に合わせてカスタマイズ可能である。

4.2 カスタマイズサービス

4.2.1 専用端末化のアプローチ

(1) 顧客専用のブラウザ

スマートフォンなどでは,特定の Web サイトやクラウドサービスへの接続環境がアプリとして提供されるのが一般的である。例えば，Google Play や YouTube のサービスは，端末を購入した時点からホーム画面にサービスのブランド名でアイコンが配置されている。このように特定のサービスへの入り口としてブラウザが位置付けられている。本製品を利用することで，各企業の業務サイトへの接続も各企業の専用アプリのイメージで見せることが可能となる。また，より各企業のブランド色を出すため，アイコンの差し替えなど見た目のカスタマイズにも積極的に対応する。

(2) 特定の業務専用端末化

Android 端末の特徴は，様々なセンサーや機器を接続する際の障壁が低いところにある。Android OS がオープンソースであることから，アプリの枠に収まらず，ドライバやミドルウェアを用意することで，特殊な装置や計測器にも対応できるケースがある。例えば，スマートフォン端末によるクレジットカード決済は一部実用化が行われ，今後の普及が見込まれている。これらの潜在的なニーズについて積極的に対応していく。また，特定の業務専用端末化の取り組みでは，本製品の URL フィルタリング機能を最大限に活かすために，タブレット端末にバンドルされている標準のブラウザや SMS，e メールといったファイルの操作が可能なアプリをすべてアンインストールすることが望ましい。そこで，本製品の初期導入時には,キッティングサービスも合わせて提供する。

4.2.2 顧客ニーズ

本製品の拡販活動で寄せられた顧客ニーズについて表 2 に示す。これらの顧客ニーズは，カスタマイズサービスや次バージョンでのサポートを検討していく方針である。表 2 のタブレット端末のもつリッチメディア機能を活かしつつ安全に使う技術や，PC 向けに作成された Web ページやコンテンツをスマートフォンなどのユーザインターフェースに適合するように自動変換する技術については，研究開発部で研究・開発を行っている。これらの機能については，研究開発部と協力して製品化を検討していく。

表 2 拡販活動での顧客ニーズ

顧客ニーズ	対応方針
①iPhone / iPad 版の対応	検討中
②ファイル持ち出しを許可してセキュアに管理したい	カスタマイズ
③業務システム側の影響を最小限にしたい （モバイル機器向けの HTML コンバータが欲しい）	検討中
④業務 PC と同じ認証方式としたい	カスタマイズ
⑤ファイル毎やユーザ権限毎にダウンロードを許可したい	カスタマイズ
⑥ HTML5 への対応	検討中
⑦ PDF をブラウザに同梱してインストールさせたい	カスタマイズ
⑧アカウントを切り替えて端末を複数人で共有したい	製品機能

4.3 連携製品

4.3.1 モバイル認証デバイス「KeyMobileMSD」

「Custom Browser for Android」では，日立製作所の「KeyMobileMSD」 [5] と連携することでタブレット端末の第 3 者による不正利用や不正アクセス防止を実現している。「KeyMobileMSD」は，IC チップと大容量のフラッシュメモリを microSD の I/F（形状）で利用できるため，モバイル機器に適した IC カードと言える。また，USB タイプのアダプタを利用することで，PC の認証にも利用できるため，企業内の多様な端末で統一されたセキュリティレベルの認証を実現できる。この IC チップは，耐タンパ性と呼ばれる物理的にも論理的にもハッキングを防御する機能で守られている。この IC チップの PIN 認証*4や IC チップ内の電子証明書を利用して強固ななりすまし防止を実現する。

4.3.2 「秘文」に対応したタブレット端末「BizPad」

タブレット端末の紛失や盗難時に発生する情報漏えい対策では，日立ソリューションズの「秘文」[6] に対応したパナソニック社の業務用タブレット端末「BizPad」[7] と連携する計画である。Android 端末は，内部メモリの他に外部メモリとして microSD カードを標準で利用できることから端末内のデータ保護も企業にとって重要な課題となる。この課題に対して「Custom Browser for Android」では，ファイルのダウンロードを禁止するアプローチとしているが，表 2 の顧客ニーズにもあるようにファイルダウンロードのニーズもあり，カスタマイズサービスとして，安全なファイル管理方式の検討を進めていく。また，「BizPad」はビジネス向けタブレットとしてサポートが万全であり，「KeyMobileMSD」との連携開発による親和性の高さにより「Custom Browser for

*4 Personal Identification Number。個人識別番号による認証。

Android」の販売では推奨端末と位置付けている。本製品は，セキュリティ対策の機能も提供することから，新たなセキュリティ脅威に Android OS レベルで対応が求められるケースも考慮して，アライアンスを進めていく。

５．ソリューション展開

5.1 企業情報システムへの適用

TechTarget ジャパンの会員を対象にした「企業のスマートデバイス利用」に関するアンケート結果によると，スマートデバイス導入状況(図 5)では，71.9%がスマートデバイスを許可もしくは検討している中，20.3%が「今後も導入する予定はない」とし，導入を拒む理由は，セキュリティ面の不安が費用対効果やデータ通信料金の負担よりも多いと公表している。また，スマートデバイスを許可もしくは検討していると回答した企業のスマートデバイス導入時の懸念事項(図 6)でも，上位 3 つがセキュリティ関連であり，セキュリティ対策がスマートデバイス普及の鍵を握っていると言える。このスマートデバイス導入時の懸念事項は，本ソリューションで対応可能である。ソリューションの対応状況を表 3 に示す。

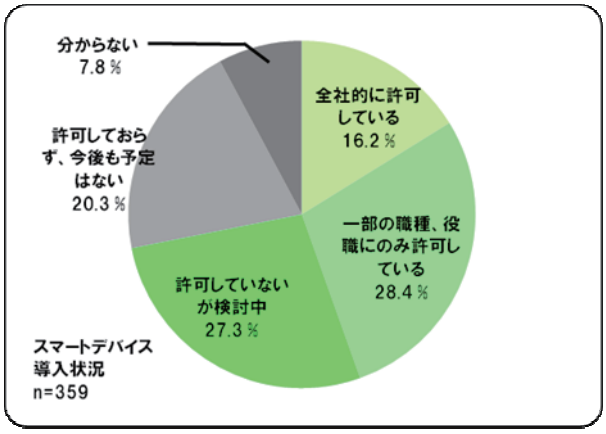

図 5　スマートデバイス導入状況
（出典：TechTarget ジャパン）

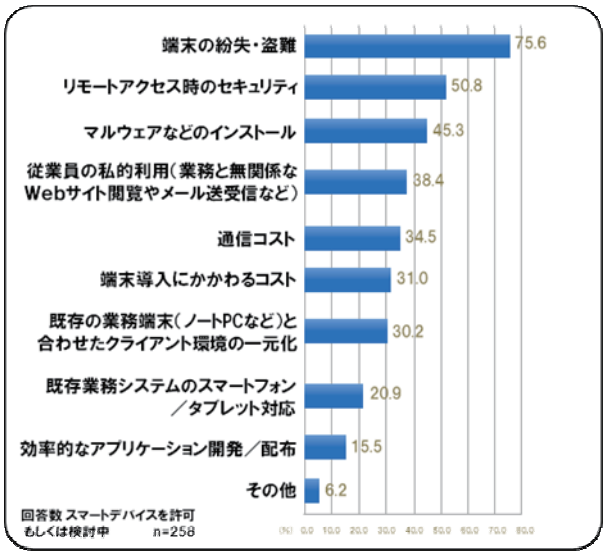

図 6　スマートデバイス導入時の懸念事項
（出典：TechTarget ジャパン）

表 3　ソリューションの対応状況

スマートデバイス導入時の懸念事項	対応状況	
	Custom Browser	連携製品
① 端末の紛失・盗難	○	「秘文」＋「BizPad」
② リモートアクセス時のセキュリティ	○	KeyMobile
③ マルウェアなどのインストール	○	
④ 従業員の私的利用（業務と無関係な Web サイト閲覧やメール送受信など）	○	
⑤ 既存の業務端末（ノート PC など）と合わせたクライアント環境の一元管理	○	KeyMobile

端末の紛失・盗難(①)は，本製品を適用して端末に情報をもたない方式と，「秘文」と「BizPad」を組み合わせて端末内の情報をすべて暗号化する方式がある。

リモートアクセス(②)やクライアント環境の一元管理(⑤)では，KeyMobileMSD と連携した認証方式を提供する。マルウェア(③)と従業員の私的利用(④)は，本製品のフィルタリング機能を提供する。

一方，既存業務システムの対応や効率的なアプリケーション開発／配布では，顧客の業種や業態のニーズに合わせたサービスを提供していく。

5.2 今後の展開

本製品は，Web 化された企業の業務システムに適用していく。その業務システムは，オンプレミス*5型の社内システムと SaaS などのクラウドサービス型がある。これら業務システムの拡張や維持では，クロスブラウザ対応*6の悩みを抱えている。特に SaaS のサービス提供者は，サービスを利用するユーザ数を増やすために，より多くの対応機種をサポートすることが求められており，2.1 章に示したように，Android 端末，iOS 端末，PC のそれぞれのバージョンや Web ブラウザに対応していくことになる。さらに，それらの端末は半年や 1 年で新機種が登場し，旧機種の供給やサポートが強制的に終了することもめずらしくない。このことは，統一されたセキュリティレベルで業務システムを維持し続けることを難しくしている。そこで本ソリューションでは，端末に業

*5 自社で用意した設備でソフトウェアを配備，運用。
*6 Web サイトがあらゆるブラウザで正常に動作し閲覧できること。

務サイトの Web アプリケーションを合わせていくのではなく，端末に顧客専用の Web ブラウザを適合させるアプローチを提案していく。予め業務サイトと顧客専用の Web ブラウザで親和性を確認しておけば，そのブラウザを端末に配布することで，異なる端末や機種であっても Web アプリケーションの対応は不要となる。なおかつ，統一されたセキュリティ環境も提供できる。ただし，そのためには，本製品の前提端末や OS，バージョンなどサポート範囲の拡大が必要である。今後，発売される端末のサポートは，市場動向や顧客ニーズを判断して対応を進める予定である。このように顧客専用の Web ブラウザのアプローチは，業務サイトの維持に密接にかかわることになる。そのため，本製品の保守サポートサービスは，2 年や 3 年単位の長期的な契約パターンも提供していく予定である。

６．おわりに

企業での情報セキュリティ対策は，場当たり的な対策ではなく，継続的かつ網羅的な対策が望まれる。そのため，スマートフォンなどのビジネスでの利用では，特に Android 端末は，セキュリティの懸念から導入に踏み込めない，あるいは漠然とした不安を抱えつつ運用している現状がある。

一方で，リッチメディアを実現するタブレット端末は抜群のモビリティと斬新なプレゼンテーションで新たなセールスチャネル開拓が可能であり，営業，保守員，店頭販売員達にとっては魅力的なデバイスと言える。

今回，製品化した「Custom Browser for Android」はその名のとおり，カスタマイズ可能な Web ブラウザを目指した。その第一歩として，セキュリティ対策の機能拡充にフォーカスして取り組み，企業の社内システムへの適用やクラウドサービスとの連携に向けて拡販を推進している。今後は，国内でも登場しはじめた電子書籍の専用端末のように，企業が提供するサービスのブランド戦略の１つとしての専用端末も視野に入れて，国内市場の活性化に貢献していきたいと考える。

参考文献

1) 総務省：平成 24 年度版情報通信白書スマートフォン等の普及がもたらす ICT 産業構造・利用者行動の変化，
http://www.soumu.go.jp/johotsusintokei/whitepaper/
2) 独立行政法人情報処理推進機構(IPA)：Android OS を標的とした不審なアプリに関する注意喚起，
http://www.ipa.go.jp/about/press/pdf/120523press.pdf
3) 独立行政法人情報処理推進機構(IPA)：スマートフォンへの脅威と対策に関するレポート，
http://www.ipa.go.jp/about/technicalwatch/pdf/110622report.pdf
4) Symantec：「奇跡のバッテリ節約アプリ」がスパム送信のために電子メールアドレスを収集，
http://www.symantec.com/connect/blogs-5
5)（株）日立製作所：モバイル認証デバイス KeyMobileMSD，
http://www.hitachi.co.jp/products/it/keymobile/index.html
6)（株）日立ソリューションズ：情報漏えい防止ソリューション秘文 ,http://www.hitachi-solutions.co.jp/hibun/sp/
7) Panasonic：業務用タブレット端末 BizPad，
http://panasonic.biz/it/bizpad/

畠山　誠基　　1991 年入社
金融組込みソフト開発グループ
KeyMobileソリューション拡販およびICカード関連サービスの提供
sehatake@hitachi-to.co.jp

庄司　秀明　　1990 年入社
金融組込みソフト開発グループ
組込み向けコンパイラ開発・取り纏め
hideaki@hitachi-to.co.jp

稲葉　朋子　　2001 年入社
金融組込みソフト開発グループ
エンタープライズ系アプリケーション開発
a-inaba@hitachi-to.co.jp

工藤　英治　　1992 年入社
金融組込みソフト開発グループ
自社ソリューション適用・取り纏め
ekudo@hitachi-to.co.jp

阿部　諒平　　2010 年入社
金融組込みソフト開発グループ
組込み向けコンパイラ開発
ryouhei.abe.01@hitachi-to.co.jp