

ビジネスケータイの情報セキュリティ対策は万全か？

How is the Way of Promoting Keitai Security for Business?

正田洋一 齊藤弘太 遊橋裕泰
Yoichi SHODA Kota SAITO Hiroyasu YUHASHI
株式会社エヌ・ティ・ティ・ドコモ モバイル社会研究所
Mobile Society Research Institute, NTT DOCOMO, INC.

要旨:

2005年4月に個人情報保護法が施行されて、企業の情報管理の責任が明確になり、企業が情報漏洩を発生させた場合、多額の賠償負担や社会的信用の失墜から事業の継続性が脅かされる情勢となってきた。企業の情報セキュリティ対策では、情報システムの脆弱性対策や社員のセキュリティマインドを向上させる教育施策を実施する一方で、ケータイ電話がそのスコープに入っていないのではないかと。だが、パーソナルコンピューター並みに機能が高まったケータイ電話にも機密性が求められる情報が格納されているのが現状であり、紛失・盗難等による情報漏洩の危険性は高い。

本研究では、ビジネスに利用されているケータイ電話におけるセキュリティ対策の状況をアンケート調査で把握し、態度変容モデルから最高情報責任者(CIO)として注目すべきポイントを明らかにする。また、ビジネスパーソンへのインタビューを踏まえ、事業継続管理のために企業が採るべきケータイ電話のセキュリティ対策を提案する。

Abstract:

Act for the Protection of Personal Information was enforced in April 2005; thereby the company's responsibility of the information management became clear. If a company causes the information leak, the business continuity will be threatened by a huge amount of compensation burden and loss of the social trust. As the measures for information security vulnerabilities, many companies defend against vulnerabilities of its information systems and educate the security mind to its employees. However, the Keitai (Mobile phone) seem not to be included in the scope. Since Keitai can store much confidential information, the risk of the information leak would be high in case of the loss or theft.

This research investigated the security mind and setting of password for Keitai on business by questionnaire survey. We elucidate duties of the Chief Information Officer (CIO) for Keitai security by the analysis of the Attitude Transformation Model. In addition, we suggest the measures for information security vulnerabilities for the Keitai which a company should adopt for the Business Continuity Management (BCM) on the basis of an interview to the business persons from some excellent company in security perspective.

1. 本研究の背景

2005年4月の個人情報保護法施行を背景に、企業では、適正に個人情報を取り扱うように厳しい責任が課せられることとなった。企業が情報漏洩事故を引き起こした場合、法的責任だけではなく取引先や顧客から契約解除等を受け、事業継続性が脅かされる場合も出てくる(岡村, 2005)。よって、企業にとって情報セキュリティは、事業継続管理(BCM)の視点から捉えるべき課題といえる。

小尾(2007)によれば、企業の最高情報責任者(CIO)の主たる任務は、組織内の情報・情報システムの管理・統括を含む戦略の立案と執行であるとされ、BCMに情報セキュリティが関わっている以上、CIOは情報セキュリティ対策を任務の1つとして認識する必要がある。

今日のケータイは、インターネット、メール、ICカード決済が搭載されて、高性能化している上に、

メモリーの大容量化に伴い多くの情報を持ち運ぶことができる。企業では情報システムの脆弱性対策や、社員への教育等のセキュリティ対策を実施してきているが、はたしてそのスコープにケータイが含まれているだろうか。

本研究では、ビジネスで使用されているケータイのセキュリティ対策状況をアンケート調査によって概観する。そして、消費者の態度変容モデルを利用して分析し、CIOがとるべきケータイの情報セキュリティ対策を提案する。

2. 先行研究のレビューと仮説の提示

情報セキュリティは、情報システムへの不正アクセス、改ざん、漏洩、物理的損傷を防ぐために用いられる方針、手順、そして技術的手段と定義される(Laudon, K. et al., 2007)。そして、可用性(Availability)、機密性(Confidentiality)、完全性(Integrity)の不備から

生じる損害から情報システムを利用する人々の利害関係を守ることを目的とする(OECD, 1992).

企業の情報セキュリティ対策に着目したこれまでの研究は、法制度、教育、技術の三分野に大別できる。法制度では、森(2006)が、個人情報保護法、会社法、金融商品取引法等は、企業に直接的に義務を課しており、市場での評価に無視できない事柄であり、対策を施している企業は高く評価されるべきであると述べている。また、教育分野では、田中(2005)が、情報セキュリティ教育が求められる社会的背景、リスク、事故分析をした上で、「情報セキュリティに関するより高度なテクニカルスキルやマネジメントスキルをもったスペシャリストを育成する」教育体系作りが重要であると述べている。また技術分野では、松本他(2000)が金融機関での具体的なセキュリティ対策を検討した上で、セキュリティ技術は、システムを守る側と攻撃する側のせめぎ合いから進歩してきており、現時点で優れた技術を導入しようとも、いつかは時代遅れとなると言及している。また、Djapic, M. et al.(2007)は、情報セキュリティの問題は、情報技術の問題でなく、最高水準の組織マネジメントにより対処されなければならない問題であると述べ、重要なのはリスクマネジメントであると述べている。しかし、これらの研究すべてが、ケータイに関する議論を取り上げていない。

一方、岩崎他(2006)が、利用者からみたケータイの安全性に関する意識を調査し、社会不安の増加に伴って、セキュリティ意識が向上すると述べているが、ケータイを扱った研究は稀である。ただし、CIOの目線でセキュリティ対策は議論されていない。

以上のことから、企業での情報セキュリティ対策の中にケータイがスコープにはっていないのではないかと、また、ケータイから情報漏洩するリスクが理解されていないのではないかと、という課題が生じてくる。以下、実態を確かめるべくおこなった定量調査について説明する。

3. 調査概要

3.1 サンプル方法とサンプルの特性

企業におけるケータイのセキュリティ対策の状況を調査するため、ビジネスパーソンを標本母集団とし、1都3県(東京・神奈川・埼玉・千葉)在住かつNTTドコモの第3世代ケータイ利用者を有意抽出した。このモニターに対して Web アンケートを実施し、501名の有効回答を得た(「goo リサーチ・ビジネス」利用, 2009年3月実査)。モニターの年齢層は、20代から70代までとなっており、40代前半がボリュームゾーンとなっている。また、アンケート調査を補足するため、インタビュー調査も実施した(2009年4月)。

3.2 研究のフレームワーク

OECD は、参加者(情報システムに関わる全ての人)は、自ら責任を持ってセキュリティを強化するための措置をとるべきであると提言している(1992)。つまり、企業では社員も対策の当事者に該当する。ゆえに、社員のセキュリティ対策に対する意識を調べることによって、CIOとして注力すべき対策のポイントを検討する。

社員の意識を定量化するフレームワークとして、消費者行動論における態度変容モデルを用いた。態度変容モデルとは、消費者の商品に対する態度が、認知(Cognition)から感情(Affect)、感情から行動(Behavior)へ遷移するとしたプロセスのモデルである(Solomon, 1992)。本研究ではそれにならい、NTTドコモが提供している第3世代ケータイのセキュリティ機能・サービスについてビジネスパーソンの態度を、「知っている(認知)」、「理解している(感情)」、「利用している(行動)」の3区分で捉えた。

3.3 研究対象とするセキュリティ機能・サービス

態度変容モデルに当てはめる NTT ドコモのセキュリティ機能・サービスを表1に示す。

iモードパスワード、ネットワーク暗証番号はドコモのサーバ上に設定される暗証番号である。それらがもし不正に使用された場合、公式サイトで課金されたり、電話の転送先の遠隔操作をされたりする(完全性の問題)。

また、端末暗証番号は、端末の各種設定や、データの一括操作、あるいはICカードロック、ダイヤルロックの解除に使用される。これが不正に使用された場合、セキュリティ設定を解除されたり、外部メモリーへデータをコピーされたりする(完全性及び機密性の問題)。

PIN1コード、PIN2コード、PINロック解除コードはSIMカード上に設定される暗証番号である(次項で詳述のため説明を割愛)。

ICカードロックは、ICカード機能を使えなくするもので、端末暗証番号が漏洩しない限りICカード機能の完全性は保たれる。ダイヤルロックは端末の操作や発信ができないようにするサービスで、端末暗証番号が漏洩しない限り、端末上のデータの機密性や完全性は保たれる。

遠隔ロック、おまかせロックは遠隔操作で端末にICカードロック、ダイヤルロックをかけることができるサービスである。前者は端末への事前設定が必要で、後者は不要。盗難・紛失時に効果を発揮するセキュリティサービスとなる。

表1 NTTドコモのセキュリティ機能・サービス

サービス名	内容	設定場所	初期値
iモードパスワード	iモードサービスにて利用する数字4桁の暗証番号	ネットワーク上	0000
ネットワーク暗証番号	ネットワークサービスの設定の変更をするときに使用する暗証番号	ネットワーク上	契約時に決定
端末暗証番号	電話機の各種機能の設定や解除の際に必要な暗証番号	端末上	0000
PIN1コード	第三者による無断使用を防ぐため、SIMカードを端末に差し込むたびに、または、端末の電源を入れるたびに使用者を確認するために入力する4～8桁の番号(コード)	SIMカード上	0000
PIN2コード	ユーザー証明書利用時や発行申請、電子認証サービスに接続するとき、積算料金リセットを行なうときなどに使用する4～8桁の暗証番号	SIMカード上	0000
PINロック解除コード	PIN1・2コードを3回連続して間違えた際、自動的にかかる「PINロック」を解除するときを使う	SIMカード上	契約時に決定
ICカードロック	ICカード機能を使用できないようにする	端末上	—
ダイヤルロック	電話帳の呼び出し・修正、電話発信をはじめとするほとんどの機能を使用できなくする	端末上	—
遠隔ロック	遠隔操作でケータイにロックをかけることによりケータイの操作をできないようにして、他人が不正に使用するのを防ぐ。自動的にICカードロックも設定される	端末上	—
おまかせロック	オペレーターに電話し、離れたところから携帯電話をロックできる	(設定不要)	—

出展：NTTドコモホームページより作成

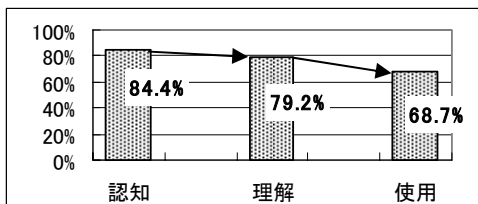
4. 分析

4.1 調査結果概要

表1で示した10種類のセキュリティ機能・サービスに関して、態度変容モデルに当てはめたところ、3つのグループ(A, B, C)にビジネスパーソンのセキュリティ対策の行動の実施傾向が大別された。

グループAの特徴をiモードパスワードで説明すると、認知84.4%、理解79.2%、使用68.7%となっており、3つのプロセス全てで高止まりしている。ネットワーク暗証番号、端末暗証番号も同様の傾向を示す。

図1 iモードパスワードの対策状況(グループA) n=501

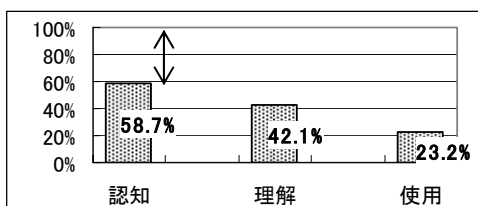


このグループAは、現時点で既にユーザにおけるセキュリティ対策が高い割合で実施されており、CIOとして対策が急務といえる状況にはない。

4.2 グループBの分析

グループBの特徴を表す図2のPIN1コードで説明する。認知58.7%、理解42.1%、使用23.2%となっており、他のグループと比較して認知度が低い。PIN2コード及びPINロック解除コードも同様の傾向を示している。

図2 PIN1コードの対策状況(グループB) n=501



4.2.1 堅牢なセキュリティ対策方法

PIN1コードは、電源を入れる度にコードの入力が求められる。正しいPIN1コードを入力しなければ、発着信および端末操作ができない。別の端末に差し替えても同様である。もし、PIN1コードが設定されていない場合、その端末でダイヤルロックをかけていたとしても、SIMカードを別の端末に差し替えられてしまえば、第三者になりすまして発着信することができてしまう。情報漏洩・なりすましを防ぐ上で、PIN1コードの設定は大変重要であり、端末自体をロックするダイヤルロックと組み合わせることで、はじめてケータイの堅牢な情報セキュリティを実現できる。

4.2.2 ケータイを利用した個人認証

ケータイを利用することでノートパソコンのリモートアクセス等でセキュリティを高めることができる。NTTドコモでは、従来のID/パスワード認証に代わるケータイによる電子認証サービスを提供している。あらかじめケータイのメモリーに保存しておいたユーザ証明書を電子認証サービス対応サイトへ送信することで、簡単にセキュリティの高い認証が行える(認証局はNTTドコモ)。そのユーザ証明書の送信の際、入力を求められるのがPIN2コードである。もしPIN2コードが設定されていない状態で端末が盗難に遭った場合、第三者が電子認証サービス対応サイトをなりすまして利用することができてしまう。ケータイがそのような悪用された場合、企業はセキュリティ対策の不備を指摘され、社会的信用を失うことになるだろう。社内イントラネットへ電子認証サービスを導入することによって、事業所の外からでも利便性が高く、セキュリティの高い個人認証を行うことができるようになる。PIN2コードの使用を徹底し、電子認証サービスを有効活用できれば、CIOは企業価値を高めることができる。

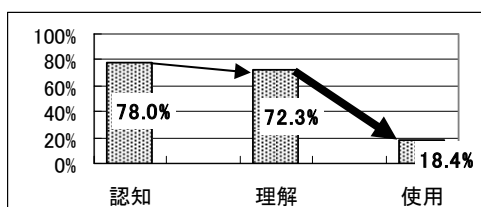
4.2.3 グループBの対策

グループBのセキュリティ対策は、「盗難・紛失経験者」において、PIN1コードの認知が77.0%、理解が60.8%、使用が33.8%と高い水準にあり、自身の体験にて実感を得ていると言える。グループBのセキュリティ対策を推進するためには、ケータイを紛失した時のリスクとして、悪用された時の顧客への謝罪対応、損害賠償請求の金額、企業の信用失墜等を、研修で擬似的に体験させることで危機感を与えて、セキュリティマインドを植えつけることが有効であると考えられる。

4.3 グループCの分析

グループCの特徴をダイヤルロックで説明する。ダイヤルロックは、認知78.0%、理解72.3%と高い水準を示しながら使用は18.4%となっており、理解と使用の差異が大きい。ICカードロック、遠隔ロック、おまかせロックも同様の傾向であった。

図3 ダイヤルロックの対策状況(グループC) n=501



グループCは、発着信や端末操作をできなくしたり、ICカード機能(ICカード決済、オフィスの入退室、PCのログオン等)を利用できないように設定したりするサービスが該当する。

4.3.1 グループCの対策

グループCのセキュリティ対策は、「金融業界」に勤めている人において、ダイヤルロックの認知が80.0%、理解が80.0%、使用が40.0%と、高い水準にある。金融業界では、金融庁から顧客情報管理が義務づけられており、他の業界に比べ、社員への指示に「強制力」が働いていると考えられる。

ダイヤルロック等の使用は、ケータイの機密性を守る上で重要だが、端末を操作する時に端末暗証番号を毎回入力する必要があり、利便性が損なわれる。社員の利便性ではなく企業の利益をまもるよう、CIOは必要に応じて、設定を義務化するような指示を出すことが必要である。

5. CIOのケータイセキュリティ対策

CIO視点でケータイセキュリティ対策を検討する場合、社員がビジネスに利用するケータイに対し、企業がコントロールすることは、プライバシーの侵害に当たるとはならないかと懸念される。

社員名義のケータイに対し、企業がセキュリティ設定のチェックを行うことはプライバシーの侵害となるため

一般的には認められない。

一方、企業名義のケータイに関しては、社員に一定のプライバシーが認められるとしても、社員名義のケータイと同程度の保護を期待することはできず、プライバシーの程度は相当程度低減される。

アンケートからは、ケータイの59.0%もが社員名義であった。これではCIOがケータイのセキュリティ対策をスコープに捉える上で好ましくない。

CIOは具体的にどのような対策をすべきかを、以下にまとめることで本論文の結びとする。

- ① CIOは、ケータイの盗難・紛失時の状況を擬似的に体験させ、危機感を与えてセキュリティマインドを植えつけるような研修を実施することを検討すべきである。
- ② CIOは社員に対し、ケータイのセキュリティ対策についての強制力のある指示を出すべきである。
- ③ CIOは、企業からケータイを必要な社員に支給すべきである。

以上、ケータイを情報セキュリティ対策のスコープに入れることにより、CIOは情報の漏洩やなりすましを防ぎ、企業価値を高めることができるようになる。

参考文献

- [1] Djapic, M., Lukic, L., *ISO/IEC 27000 SERIES STANDARDS THE BEST BUSINESS PRACTICE FOR INFORMATION SECURITY*, International Quality Conference, May. 11, 2007.
- [2] Laudon, K. C., Laudon, J. P., *MANAGEMENT INFORMATION SYSTEMS*, Pearson Education, Inc., 2007.
- [3] OECD, *Guidelines for the Security of Information Systems*, 1992.
- [4] 岩田匡寿, 伊藤卓朗, 西村由希子, 西村邦裕, 杉村武昭, 及川博道, 玉井克哉「利用者から見たケータイ電話の安全性に関する意識調査(科学技術と社会・倫理問題(1))」, 技術計画学会, 2006年.
- [5] 岡村久道『個人情報保護法の知識』日本経済新聞社, 2005年.
- [6] 小尾敏夫「CIO学の目指すもの」須藤修, 小尾敏夫, 工藤裕子, 後藤玲子編『CIO学IT経営戦略の未来』, 東京大学出版会, 2007年, 1-20ページ.
- [7] 田中信也「情報セキュリティにおける教育の重要性と人材の育成」『UNISYS TECHNOLOGY REVIEW』第86号, 2005年8月, 97-111ページ.
- [8] 松本勉, 岩下直行「情報セキュリティ技術の信頼性を確保するために」『IMES DISCUSSION PAPER SERIES』, 2000年12月.
- [9] 森純子「企業のコンプライアンスと情報セキュリティ」『InfoCom REVIEW』第40号, 2006年, 16-24ページ.
- [10] 「NTTドコモホームページ」 <http://www.nttdocomo.co.jp/> (May. 21, 2009)