＜NewsRelease＞
報道関係各位

NO MORE 情報漏えい
情報漏えいの「自分ごと化」プロジェクト。

MOTEX
2015年3月3日
エムオーテックス株式会社

～NO MORE 情報漏えい プロジェクト～

Webメールサービス 利用実態調査

約半数が“メール誤送信”経験アリ！
会社の信用損失リスクをはらむ“メール誤送信”
“メールチェック漏れ”に要注意！

エムオーテックス株式会社（本社：大阪市淀川区、代表取締役社長：河之口達也、以下MOTEX）は、社会的問題である「情報漏えい」の解決、防止に貢献していく**“NO MORE 情報漏えいプロジェクト”**を2014年10月に発足。今回、プロジェクトサイトにて、20～60代の男女140名に「Webメールサービスの利用実態」を調査いたしました。

今や、ビジネスシーンやプライベートを問わず利用されているWebメールサービス。**“NO MORE 情報漏えいプロジェクト”**では、Webメールサービスをテーマにインターネット調査を実施。調査結果については、本プロジェクトの監修者である**徳丸浩氏**（HASHコンサルティング株式会社代表）より解説をいただいています。

以下が調査結果となります。本調査結果を是非ご活用いただけますと幸いです。

＝　調査結果ダイジェスト　＝

- **業務・私用時ともにGmailが支持を集め、Webメールサービス利用率第1位に。**
- **約半数がメール誤送信の経験アリ！**
  誤送信経験者の7割以上が、2～4回誤ったメールを送信していることが明らかに。
- **約3割がメール誤送信未対策。会社の信用損失リスクをはらむ“メール誤送信”。**
  “メールチェック漏れ”に要注意！
- **悪質なメールの受信による被害増大。**
  6割以上がフィッシングメールや標的型攻撃メールの受信経験アリ！

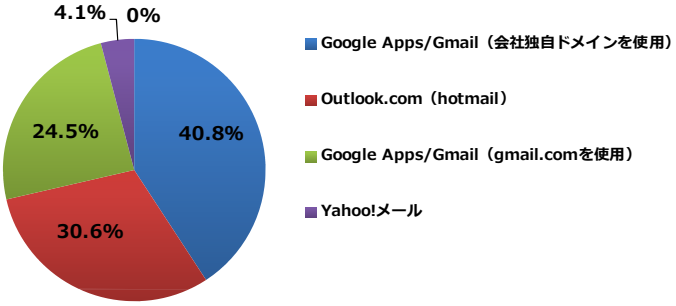
＝　調査概要　＝

- ■調査方法　：インターネット調査
- ■調査機関　：エムオーテックス株式会社
- ■調査期間　：2014年12月24日～2015年2月5日
- ■調査対象地域　：全国
- ■調査対象者　：20～60代の男女140名

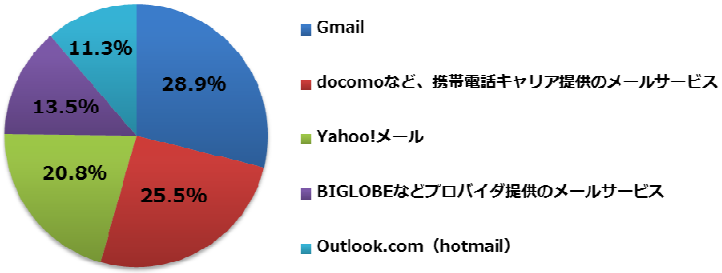
Webメールサービスの利用状況について

■業務・私用時ともにGmailが支持を集め、Webメールサービス利用率１位に。

Q:業務で利用しているメールサービスは何ですか？
（MA / N＝いずれかのメールサービスを利用していると回答した49件）



Q:私用で利用しているメールサービスは何ですか？
（MA / N＝いずれかのメールサービスを利用していると回答した318件）



業務・私用時に利用しているWebメールサービスの利用状況について調査。業務で利用しているメールサービスでは、有効回答49件（いずれかのメールサービスを利用している）のうち、**全体の40.8%（20件）が【Google Apps/Gmail（会社独自ドメインを使用）】を利用しており、利用率第1位に。**次いで、30.6%（15件）を占めた【Outlook.com（hotmail）】が第2位という結果になりました。

一方、私用時のメールサービスの利用状況を伺ってみると、有効回答318件（いずれかのメールサービスの利用している）のうち、**全体の28.9%（92件）が【Gmail】を利用。業務用と同様、1番利用されているWebメールサービスとなりました。**次いで、25.5%（81件）が【docomoなど、携帯電話キャリア提供のメールサービス】となり第2位、20.8%（66件）が【Yahoo!メール】を利用し、第3位という結果となりました。

また、日本ビジネスメール協会が発表した「ビジネスメール実態調査2014」※1においても、ビジネスメールの送受信に使っている主なメールサービスで【Gmail（Google Apps含む）】が第１位という結果になりました。環境を問わず無料で利用できる【Gmail（Google Apps含む）】の普及がうかがえます。

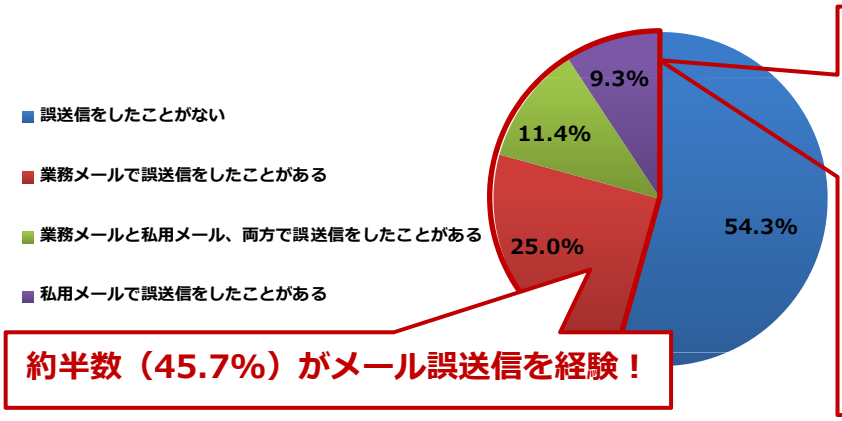
※1「ビジネスメール実態調査2014」（http://businessmail.or.jp/archives/2014/08/04/2226）

メール誤送信について

■約半数がメール誤送信の経験アリ！

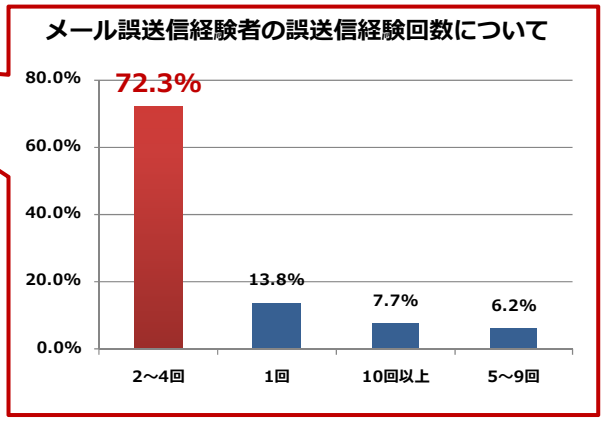
誤送信経験者の7割以上が、2～4回誤ったメールを送信していることが明らかに。

Q:メール誤送信の経験がありますか？（SA / N＝140）



約半数（45.7%）がメール誤送信を経験！

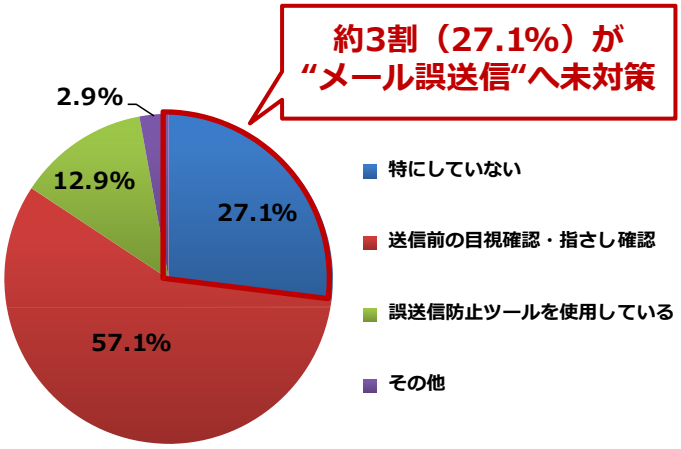
メール誤送信経験者の誤送信経験回数について



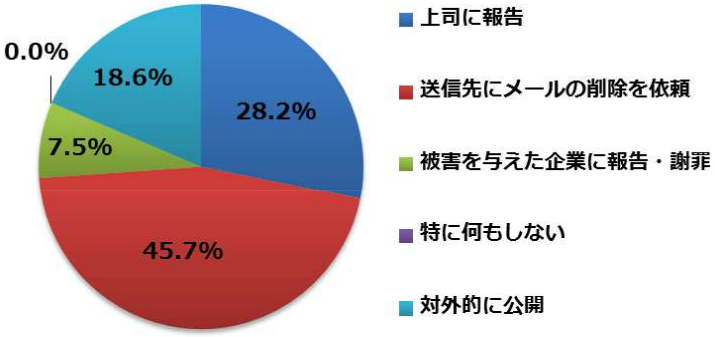
業務・私用時に、誤った内容や宛先のメールを送信してしまう**“誤送信メール”**の経験について伺いました。**業務・私用時に“誤送信メール”を経験したことがあると、全体の45.7%が回答。“誤送信メール”経験者は約半数に及ぶことがわかりました。**さらに、その経験者に対して、これまでに送った**“誤送信メール”**の回数を調査。2～4回ほど誤ったメールを送ったことがあるユーザーは7割以上（72.3%）もいることが明らかになりました。

■約3割がメール誤送信未対策。会社の信用損失リスクをはらむ“メール誤送信”。“メールチェック漏れ”に要注意！

Q:業務メールの誤送信の対策はしていますか？
（SA / N＝140）



Q:業務メールの誤送信後の対処はしていますか？
（SA / N＝140）

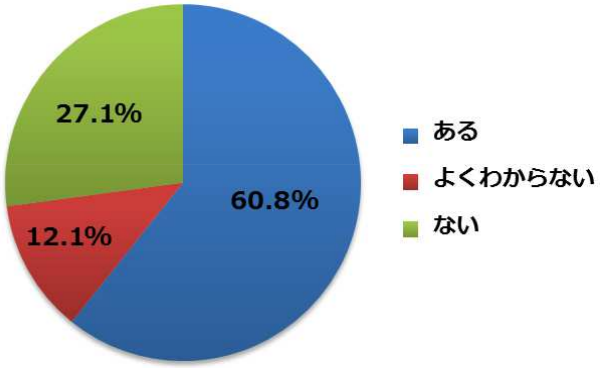


業務時の**“メール誤送信”**への対策有無を伺ったところ「送信前の目視確認・指さし確認（57.1%）」や「誤送信防止ツールを使用している（12.9%）」など、対策を講じている人は半数を占める結果となりました。一方、**調査対象の約3割（27.1%）は“メール誤送信”への対策を一切行っておらず、業務上においてリスクを抱えている状況であることがわかりました。**

また、**“メール誤送信”**をしてしまった後の対処について調査。「上司に報告（28.2%）」、「送信先にメール削除を依頼（45.7%）」という対処を取るケースが多い状況でした。しかし、中には「被害を与えた企業に報告・謝罪（7.5%）」というステージまで対処が及ぶ場合もあり、**“メール誤送信”**は信用失墜のリスクをはらんでいることが分かります。**“メール誤送信”**のリスクを減少させるには、内容および宛先のチェックがやはり重要と言えそうです。

■悪質なメールの受信による被害増大。フィッシングメールや標的型攻撃メールを6割以上が受信経験アリ！

Q:「フィッシングメール」や「標的型攻撃メール」を受信したことがありますか？
（SA / N＝140）



業務時に、誤ったメールを送信してしまうケースもあれば、一方で、自らが悪質なメールを受信してしまうケースもあります。調査では、**個人情報を盗み取ろうとする「フィッシングメール」、特定の組織や個人を狙って情報窃取などを行う「標的型攻撃メール」を6割以上が受信していることが分かりました。**中でもフィッシングについて、警視庁が2014年９月に発表した「平成26年上半期のインターネットバンキングに係わる不正送金事犯の発生状況について」によれば、2013年度より大幅に被害数、被害額は増大し、被害数は1254件、被害額は約18億5200万円という状況に。悪質なメールによる被害件数が増大していることが分かります。メールを利用する際は、メールの送信時に加え、受信時にも十分に注意を払う必要があります。

＝　徳丸先生の調査総括　＝

メールの誤送信の対策は難しいのですが、今回の調査でも、誤送信対策の難しさが浮き彫りになったと改めて感じました。先日も、IT大手企業が過去の求人応募者に対して誤って約2万3千件の「不採用通知メール」を送信してしまうという事故がありました。このような事故を減らすために、メール運用を見直すとよいでしょう。メールの誤送信を完全になくすことは難しいのですが、工夫次第で誤送信を減らすことは可能で、私もいくつかの工夫を実践しています。

例えば、アドレス帳登録時の工夫です。同姓の方など間違いやすい場合も多いので、アドレス帳の表示名を区別しやすくするとか、他社の場合のみ敬称をつけ、社内のメールアドレスと識別しやすくする、などです。不要になったアドレスは定期的に削除しておくとよいでしょう。
また、メールの暗号化も運用次第では有効です。暗号化に決める鍵やパスワードを送信の都度送るのではなく、あらかじめ決めておくのです。そうすると、いざ誤送信があっても、メールの本文は漏洩しなくてすみます。
当然ながら、メールの送信は重大事故を招く可能性が常にあるので、送信前に一呼吸置いて再度チェックするとよいでしょう。可能であれば、第三者にチェックしてもらうことも有効です。
また、フィッシングや標的型攻撃のメールについても、常に見破ることができるとは限りません。少しでも怪しいと思えば添付ファイルを開く前に、電話などで確認するとともに、Adobe ReaderやMicrosoft Officeなど閲覧に用いるソフトウェアを常に最新の状態にしておくことを心がけましょう。

徳丸 浩（とくまる・ひろし）
HASHコンサルティング株式会社代表
エムオーテックス株式会社技術顧問
独立行政法人情報処理推進機構(IPA)非常勤研究員

1985年京セラ株式会社入社後、ソフトウェアの開発、企画に従事。
1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年に同分野を事業化し、2008年独立。脆弱性診断やコンサルティング業務のかたわら、ブログや勉強会などを通じてセキュリティの啓蒙活動を行っている。

NO MORE 情報漏えいプロジェクト 特設サイト

　プロジェクト発足に合わせて特設サイトをオープン。本サイトでは、「情報漏えい」に対する知識を深め自分ごと化していただくためにケーススタディやコラムを公開。そのほか、一般公開アンケートによる意識調査レポートの発表や「情報漏えい」のリスクを分かりやすく覚えることのできる、妖怪キャラクターを用いた“情報漏えい 百鬼夜行”という診断コンテンツを展開しています。

サイト名　　：NO MORE 情報漏えいプロジェクトサイト
サイト公開日　：2014年10月27日（月）
サイトURL　　：http://www.motex.co.jp/nomore/
Facebook　　：www.facebook.com/motex.nomore

「 Webサービス×パスワード管理利用実態調査」
パスワード情報漏えい“パス漏れ”に要注意!!

本プロジェクトサイトにて、20～60代の男女150名に「Webサービスとパスワード管理の実態」を調査。
昨今、Webサービスの拡大に比例して、増大するパスワード管理の煩雑化と情報漏えいのリスクを調査。3人に1人が同じパスワード設定で複数のWebサービスを利用していることが明らかに。パスワードの使い回しによる情報漏えいリスクの増加についてレポートしています。

▼調査レポート詳細について
http://www.motex.co.jp/nomore/report/1105/

エムオーテックスについて

ネットワークセキュリティ、IT資産管理ソフトウェアLanScopeシリーズを展開するソフトウェア開発会社です。主力製品**“LanScope Cat”**は、1996年の発売以来、時代のニーズに応じて進化しつづけ、その結果多くの企業の信頼を集め、2014年12月時点、7,800社が導入、国内シェア※1ならびに顧客満足度※2において国内No.1の実績を誇ります。スマートデバイス管理ツール**“LanScope An”**と連携することで、IT資産の統合管理・セキュリティ対策を実現します。また、ソフトウェア開発・販売のみならず、LanScope活用事例コンテスト「LanScope AWARD」や全国各地を巡るセミナー「革新者サミット」など、利用価値を高める情報提供活動にも積極的に取り組んでいます。

※1　富士キメラ総研「2014年ネットワークセキュリティビジネス調査総覧　上巻」の「IT資産/PC構成管理ソフトウェア」分野
※2　日経BP社「日経コンピュータ 顧客満足度調査 2014-2015」の統合運用管理ソフト（サーバ/ネットワーク管理系）部門

【会社概要】

社名	：エムオーテックス株式会社
代表取締役社長	：河之口 達也
設立	：1996年
資本金	：2,000万円
本社所在地	：大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル