digicert®

SmartHR

DMARCでドメイン不正使用・なりすましをブロック BIMIとVMCで企業メールの信頼性と好感度もアップ

企業紹介

2013年1月設立。クラウド人事労務システム「SmartHR」を中心に、企業の人事・労務に関するサービスを開発、提供している。「社会の非合理を、ハックする。」をミッションに掲げ、既成概念や慣習に縛られて生じる企業の諸問題をハック（解消）することを目指している。「100の課題を100人で1問ずつ解く」と掲げているように、自律駆動型の社風を持つ。情報はオープンに、人間関係はフラット、スタートアップの気風にあふれている。

企業ミッションに「社会の非合理を、ハックする。」

人事労務業務はかなりアナログな世界だ。雇用契約、入社手続き、年末調整、給与明細など、多数の書類にあふれている。SmartHRはこうした人事労務業務をデジタルの力で一気に効率化するクラウドサービスだ。書類を自動作成し、ペーパーレスも実現。例えば雇用契約は労務担当がシステムのリストから対象者を選択して送付、対象者はパソコンやスマートフォンで確認、必要事項を入力して差し戻せばいい。紙やハンコ不要で、担当者の負担を大幅に削減できる。SmartHRはバックオフィス業務の効率化、生産性向上が実現できるだけではなく、SmartHRが持つ人事データを有効活用することで社員名簿、人事評価、従業員サーベイにも応用することも可能だ。

SmartHRを生み出す企業もまた興味深い。企業ミッションに「社会の非合理を、ハックする。（形骸化した非合理の解消を目指す）」と掲げ、自由闊達でスタートアップ気質にあふれている。同社の社員は指示を待つのではなく、自ら課題を見出して取り組む。「ワイルドサイドを歩こう」と未踏の地に挑もうとする果敢さもある。まだ誰もが挑戦していないところには、まだ誰も提供できていない価値があるからだ。クラウドの時流に乗り、快進撃を続けている。

株式会社SmartHR

SmartHRは個人情報を多く扱うため、セキュリティ対策には細心の注意を払うようにしている。なりすましメール対策にはDMARCで、ドメインの不正使用をブロックできるようにしている。このDMARCを設定していると、商標登録されたロゴをメールで表示できるBIMIが利用できるようになる。2021年からGmailがBIMIに対応したことで、SmartHRもBIMIを有効にした。

https://smarthr.co.jp/

業種：サービス業

課題：メールのなりすまし被害防止

導入サービス：DigiCert認証マーク証明書(VMC)

SmartHRはセキュリティ対策も最新鋭

SmartHRが主に扱うのは社員の情報であり、まさに個人情報の塊。クラウドを通じて提供するため、セキュリティ対策は技術面と組織面ともに徹底している。技術的には情報の暗号化、不正アクセス対策、脆弱性対策、なりすましメール対策を施しており、さらにシングルサインオン、二段階認証、接続元IPアドレス制限、操作ログ閲覧などセキュリティ機能も充実している。また組織的にもISO 27001（ISMS）の取得、SOC2 Type2 報告書を受領するなど万全を期している。

近年軽視できないのが、なりすましメールだ。なりすましはフィッシング詐欺やビジネスメール詐欺で起こる。前者は個人情報や企業ネットワークへのアクセス情報の漏えい、後者は金銭の窃取といったリスクがある。どちらも年々巧妙になっており、騙されてしまうと、後の痛手は大きい。それほど頻繁ではないものの「なりすましと見られるメールはいくつか受信しています」とSmartHRでセキュリティを担当する岩田季之氏は言う。

「リスクの元をどんどん潰していくこと、そうしてリスクを低減させていくことが大事だと考えています」

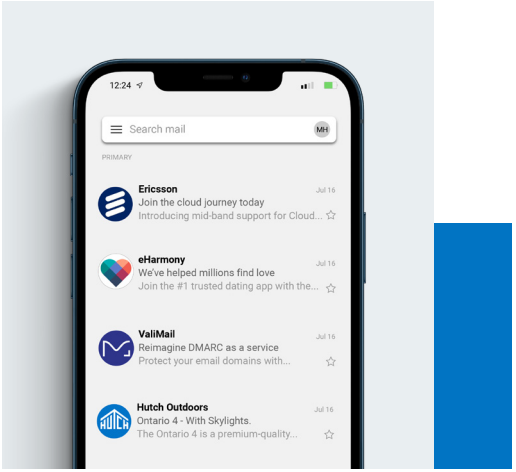
株式会社SmartHR、セキュリティエンジニア
岩田季之氏

なりすましメール対策としてDMARCを導入。ドメインの不正使用をブロック

なりすましメールは本物らしく見えれば見えるほど、受信者が騙されてしまうリスクが高くなる。技術的に有効な対抗手段の1つとなるのが送信ドメイン認証技術であるDMARC（Domain-based Message Authentication, Reporting, and Conformance）だ。DNSに設定を加えることで、ドメインの不正使用を防ぐことができる。

SmartHRではDMARCのためのレコード追加は早くからすませており、2020年9月からは不審なメール処理方法を「reject（拒否する）」に変更した。これで実質SmartHRドメインを不正使用したメールは誰も送信できなくなる。なお運用担当者にとっては「reject」への変更が難関となる。なぜなら正規のメール送信も拒否してしまわないか、細心の注意を払う必要があるからだ。マーケティングオートメーションや外注を利用し、メール発信の仕組みが多様化していると、より難しい。岩田氏も「時間をかけて慎重に確認しました」と話す。

DMARCの設定がすむと、認証済みメールにブランドのロゴを追加できるBIMI（Brand Indicators for Message Identification）が使えるようになる。しかしDMARCの設定を変更した2020年9月当時、まだBIMI対応したメールシステムが少なかった。岩田氏は「DMARCをやるならBIMIも設定したい。しかし今ではない」と時期を見計らうことにした。



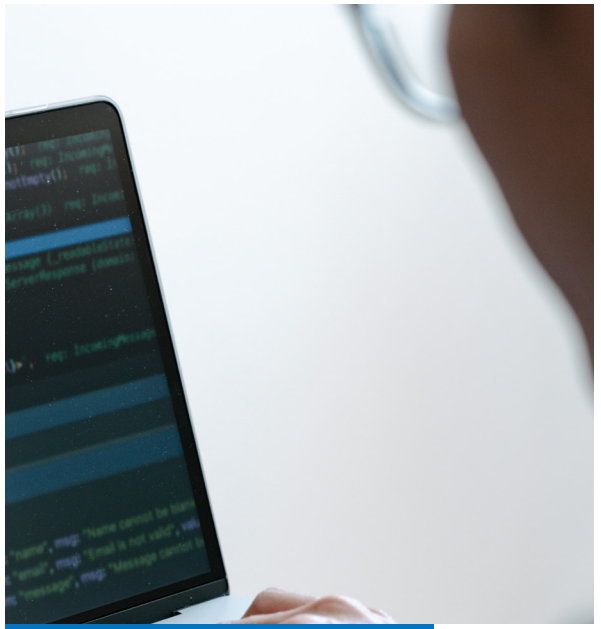
GoogleのBIMI対応を機にSmartHRもBIMIを有効化

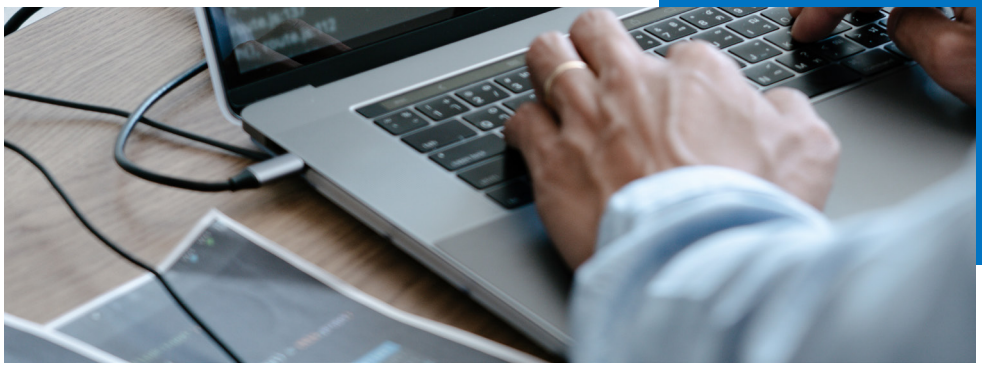
2021年7月、GoogleのGmailがBIMIに対応すると発表した。これを契機に岩田氏は動き出した。GmailおよびGoogle Workspaceを使用している顧客はそれなりに多いため、メリットを享受できると踏んだのだ。SmartHRがBIMIを設定すれば、SmartHRからのメールを受信したユーザーはメール一覧やメールでSmartHRのロゴを目にすることになる。多くの企業がBIMIをまだ設定していないため、現状ではデフォルトのそっけないイニシャルが多い。そのなかでロゴが表示されるとメール受信者に信頼性や好印象を与えることができる。岩田氏は「まだやっていないところが多いので、今なら目立てますよね」と笑う。いち早く新しいことに挑戦するところがSmartHRらしい。岩田氏にとっては「DMARC設定を乗り越えた勲章」でもあるそうだ。

なおBIMIを設定するには、VMC（Verified Mark Certificate）を取得する必要がある。そのVMC取得には商標登録済みのブランドロゴが必要だ。SmartHRではブランドロゴが商標登録済みだったため、手続きは1ヶ月程度ですんだ。

現在、SmartHRからのメールをGoogle WorkplaceやGmailといったBIMI対応メーラーで開くとロゴが表示される。DMARCを設定済みなので、ドメインのなりすましはブロックできており、ユーザーはなりすましメールを受け取らなくて済んだ状態にある。現時点で明確な数値で効果を証明するのは難しいものの、岩田氏は将来見込める効果として「ある程度の時間が必要ではあるものの、SmartHRからのメールにはロゴが表示されていることが認知されるようになれば、万が一、ロゴが表示されていないSmartHRのメールが届けば『これはあやしい』と気づいてもらえるようになります」と話す。

「セキュリティやなりすまし対策では『これさえすればOK』というような銀の弾丸はありません。リスクの元をどんどん潰していくこと、そうしてリスクを低減させていくことが大事だと考えています」（岩田氏）





© 2022 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere.
All other trademarks and registered trademarks are the property of their respective owners.