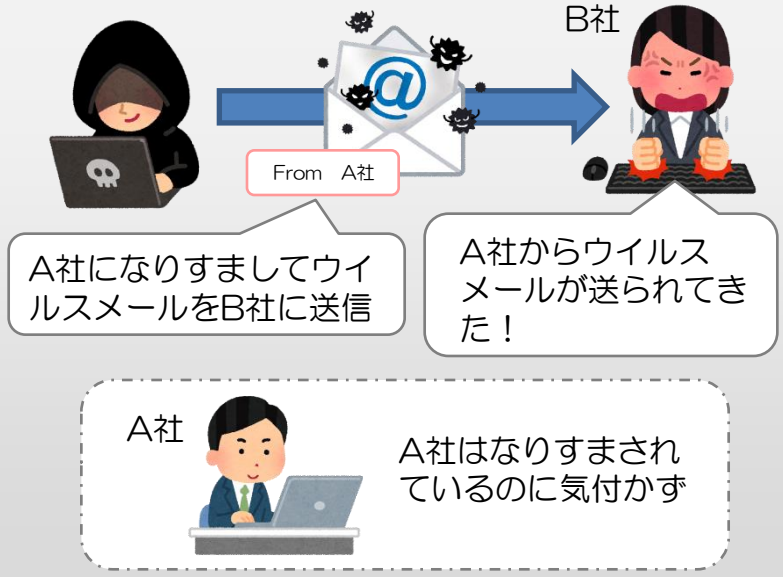
Ksisnetだより
発行:Ksisnet事務局
平成30年 1 月24日
Vol.42

なりすましメールを防ぐ 送信ドメイン認証について

　メールは簡単で便利なツールですが、送信元の偽装が簡単にできるなど、送信者が誰であるかを確認する仕組みが備わっていません。
　そのため、いわゆる「なりすまし」が容易にできてしまい、ウイルスの拡散に利用されるなどの問題があります。

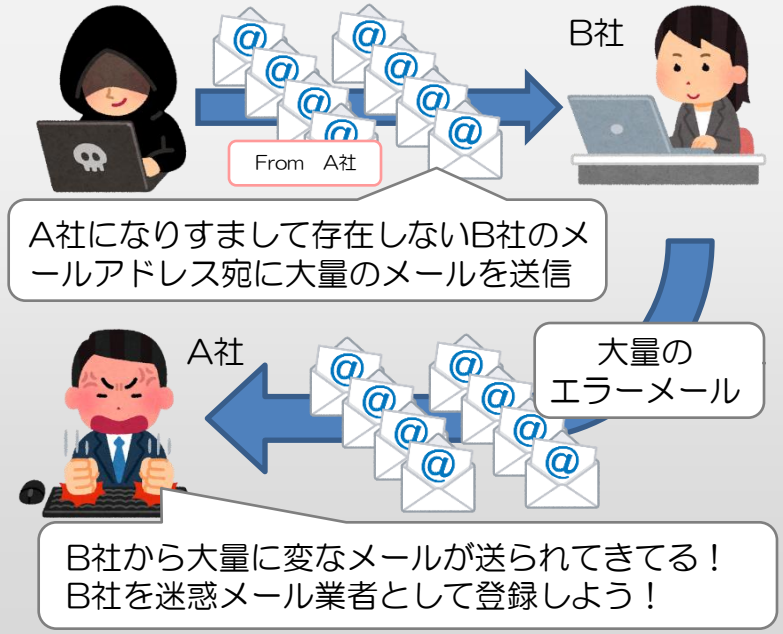
送ってないのに 攻撃者扱い！

　取引企業などになりすましてメールを送り付けて、添付ファイルを開封させたり、不正サイトにアクセスさせることでウイルスに感染させ、企業の重要情報を盗み出したりします。



送ってないのに 大量のエラーメール！

　送ってないのに謎のエラーメールが送られてくることから迷惑メールと勘違いされる。
　迷惑メールとして登録されてしまうと本当に必要なメールが届かなくなる。



送信ドメイン認証技術（DMARC）により なりすましの問題は解決できます

送信ドメイン認証技術とは、受信者が受け取ったメールについて、どこから送信されたものか確認することを可能とする技術です。

同技術の導入には、送信者・受信者の双方で、新たな設定や機能を追加する必要がありますが、従来の通信規格に直接影響を与えることなく導入可能です。

また、設定は利用者が個別にする必要はなく、メールサーバを管理しているプロバイダ等に対応を依頼することとなります。

DMARC（Domein-based Message Authentication Reporting and Conformance）は、SPF（Sender Policy Framework）とDKIM（Domein Key Identified Mail）の確認結果をもとに、総合的に送信者の確認を行います。

また、DMARCでは、確認に失敗したときの処理方法を送信者側で設定できたり、確認結果のレポートを受信者から送信者に送ることも可能です。

これにより、自社をかたるなりすましメールがどの程度送られているかを把握することも可能となっています。

	SPF	DKIM	DMARC
特徴	送信元のIPアドレスにより確認	電子署名の検証により確認	SPF・DKIMの確認結果を利用
導入コスト	送信者側はほぼない 受信者側で一定の処理が必要	送信者側での電子署名の作成や付加などの処理が必要 受信者側でも一定の処理が必要	既にSPF・DKIMを利用していれば導入は容易
長所	送信者側の導入が容易	メール本文の改ざんも検知できる	送信者側の導入が容易
短所	メール転送時に確認が失敗する場合がある	メール内容が変更されると認証に失敗する。	SPF・DKIM双方が失敗する場合には認証失敗となる。

送信ドメイン認証技術により、便利で安心なメール環境を構築し、サイバー攻撃の被害を防ぎましょう！