

BEC/なりすましメール対策ソリューション

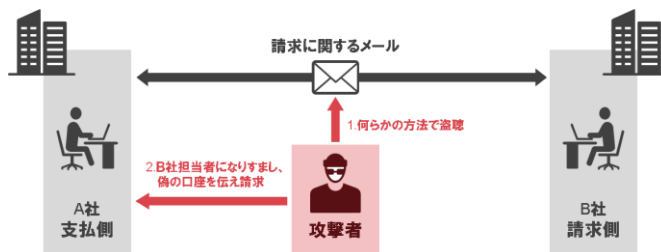
Application Platform for なりすましメール対策

ビジネスメール詐欺にDMARCで対策を。

「Cloudmark Security Platform for Email」をアプライアンス化し、スピーディーな導入を実現



巧妙化するなりすましメール詐欺



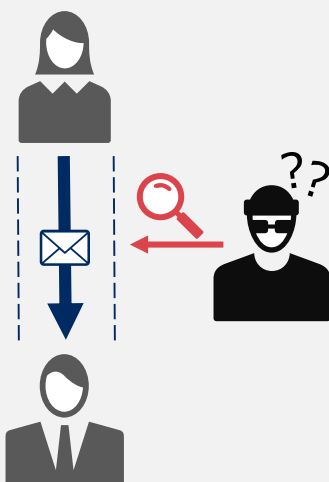
■なりすましメール詐欺の手法(例)

実際にある取引のメールを盗聴し、請求のタイミングで取引先になりすまし、偽の口座を伝える等、巧妙化。

ウイルスの添付や、悪質URLへの誘導が無いので、従来のメールセキュリティ（アンチウイルス、アンチスパム、サンドボックス等）では対応困難。

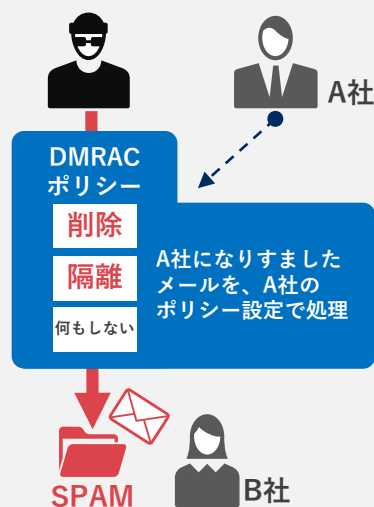
メールの盗聴/改ざんをブロック

取引先等とのメール通信を暗号化し、第三者による盗聴や改ざんを防ぎます。
※STARTTLSを用いた通信の暗号化



送信側主体のメールセキュリティ

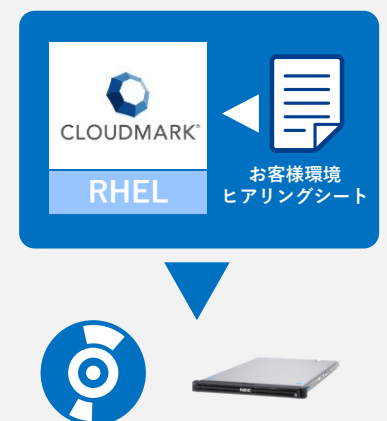
DMARCの採用により、自社になりすましたメールを、受信側に受け取らせません。



アプライアンスによるスピーディーな導入

「Cloudmark Security Platform for Email」をアプライアンスでご提供。ヒアリングシートに基づいた初期設定済みなので、スピーディーな導入が可能です。

仮想アプライアンスとHWアプライアンスの2モデルをラインナップ



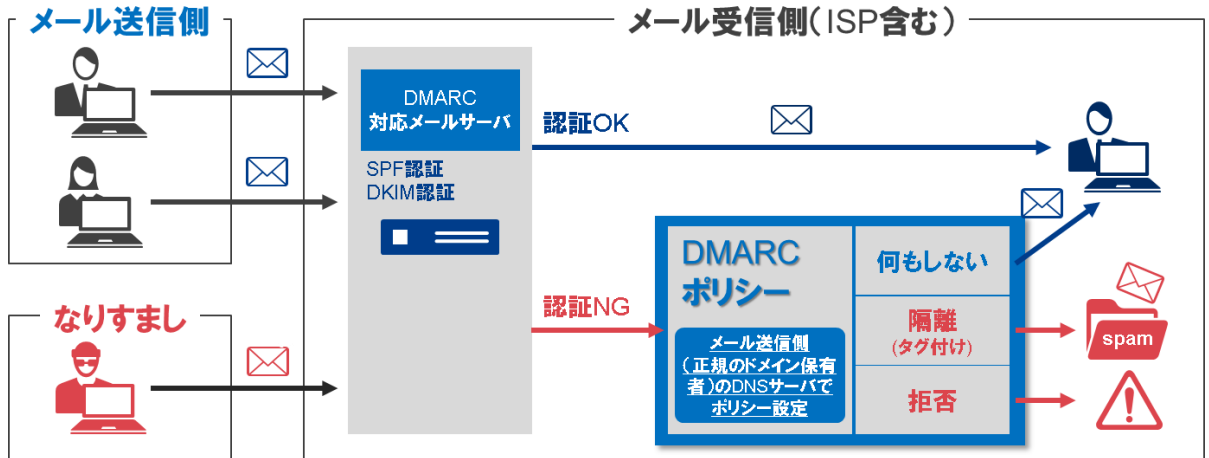
なりすましメール対策には、「通信経路の暗号化」と「送信ドメイン認証」が有効です。

通信経路の暗号化：メールの通信経路を暗号化することで、メールの盗聴や改ざんを防止
送信ドメイン認証：受信したメールアドレスのドメインを見て、正規なサーバから発信されていることを検証可能

送信側が主体となるメールセキュリティをDMARCで実現

「DMARC」は自社になりすましたメールを相手に受け取らせない仕組みです

- ・ 2種の送信ドメイン認証（SPF/DKIM）を掛け合わせることで、「DMARC」を実現
- ・ 「DMARC」は送信ドメイン認証でNG判定されたメールの処理を、送信側（正規のドメイン所有者）で設定可能



従来のメールセキュリティ ・ 受信したくないメールを受信側が探して処理

DMARC

- ・ 不正なメールの処理方法を送信側で指定
- ・ 正当性が証明されたメールだけを受信

送信者主体のメール
セキュリティを実現

製品ラインナップ/仕様

■ 基盤セットモデル(HWアプライアンス)

HWスペック

サーバ	Express5800(1Uサーバ)
CPU	インテル® Xeon® プロセッサ E3-1220 V6
メモリ	64GB
HDD	600GB×3 HDD：2.5型SAS,10000rpm



■ 仮想環境向けモデル(仮想アプライアンス)

動作要件

CPU	vCPU	4vCPU以上
	周波数	2.00GHz以上
メモリ		64GB以上
Disk	容量	430GB以上
	回転数	10krpm以上
	RAID	1,10



NEC プラットフォームソリューション事業部

〒108-8001 東京都港区芝5-7-1

URL: <http://jpn.nec.com/>

E-mail: info@naritai.jp.nec.com

凡例：

BEC：Business E-mail Compromise(ビジネスメール詐欺)

DMARC：Domain-based Message Authentication, Reporting & Conformance

SPF：Sender Policy Framework

DKIM：DomainKeys Identified Mail

STARTTLS：START Transport Layer Security

- 本誌に掲載された社名、商品名は各社の商標または登録商標です
- 本資料の内容は予告なく変更が入る場合がございます
- 御見積やご説明のご依頼は貴社担当の営業、または上記のメールアドレスへご連絡ください