サイバー攻撃対策通信

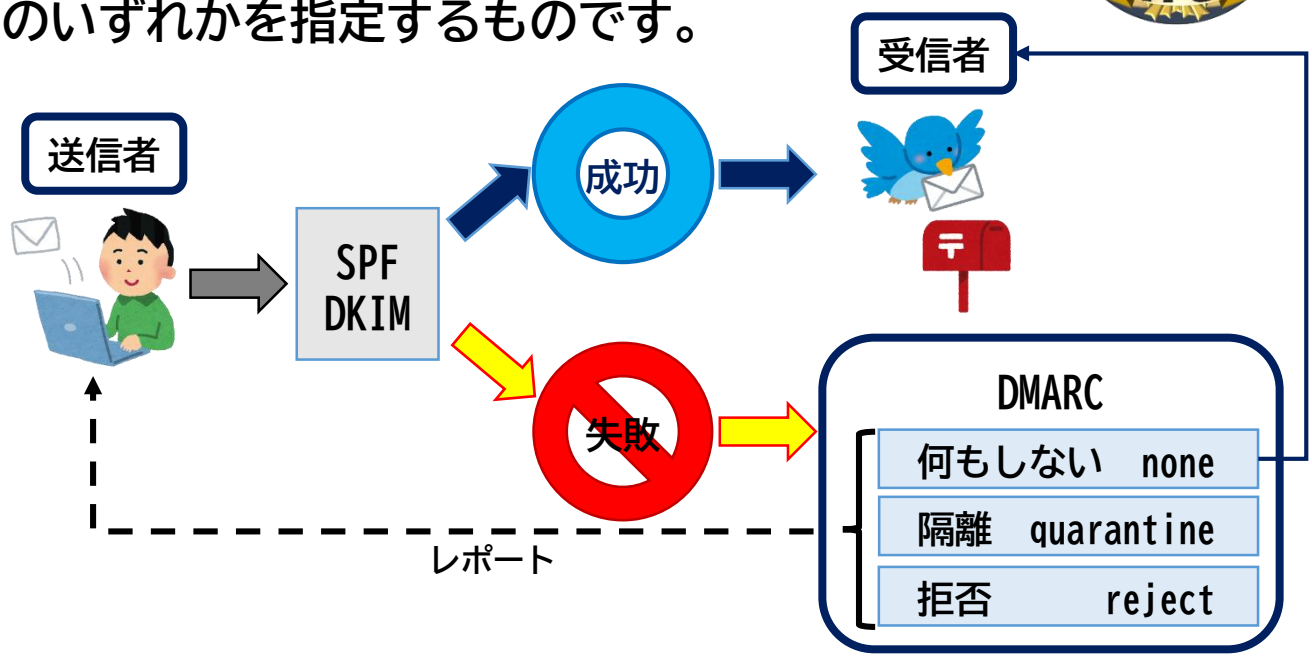
令和７年６月２日
令和７年度第４号
栃木県警察本部
警備部警備第一課
（サイバー対策センター）

DMARCでなりすましメール対策

DMARCは、メールの送信元偽装によるなりすましを防ぐ認証技術で、SPFやDKIMによる送信元認証に失敗したメールについて、送信元がメールの受信者に対し、処理方式として

- none　（何もせず受信させる）
- quarantine（隔離する）
- reject　（拒否する）

のいずれかを指定するものです。



DMARCで効果的になりすましメールを遮断するためには、「quarantine」や「reject」に設定する必要があります。

しかし、正規のメールが認証に失敗するおそれもあるため、導入当初は「none」で運用し、DMARCのレポート（※）で送信状況を確認して、SPFやDKIMの設定を見直しながら「quarantine」や「reject」へと移行するようにしてください。

※ レポート受信用のメールドレスを設定する必要があります

栃木県警察サイバー対策センター
TOCHIGI POLICE CYBERCRIME CONTROL CENTER