NJS 日本情報システム株式会社

BizLite メールセキュリティサービス

アンチウイルスソフトだけでは防ぎきれない **未知の脅威**
クラウド上の最新判定エンジンによる検知で、巧妙化する **標的型メール** の脅威を軽減

疑わしいメール

脅威が懸念される
メールはクラウド上の
メールボックスに隔離

メールサーバーでの
メール受信前に脅威を診断・検知。
脅威を食い止めます

SPAM検知

SPAM検出率※
96.83%
誤検出率※
0.05%

未知の脅威に備える

- ランサムウェア
- ウイルス マルウェア
- 標的型メール攻撃分析 (クラウドサンドボックス)

フィルターを通過した
メールだけを受信

※ 出典：Opus One, Comparative Performance of Anti-Spam Gateways

そのメール、そのファイル、本当に開封して大丈夫?

企業や組織をターゲットにした標的型攻撃の**91%**※が標的型メールを使用。
日々その手口が巧妙化し、より実際のビジネスメールとの判別がつきづらくなっています。

※Trend Labs調べ

ソフトウェアのアップデート通知メール?

でも差出人のアドレスに違和感……
アップデート用のURLも少し不自然

本物と見分けのつきにくいwebサイトに誘導して相手を油断させ、ウイルスやランサムウェアの実行ファイルをダウンロードさせる。

差出人は取引先 本文も現在進行中の案件

差出人・本文に違和感はないが
メールアドレスが少しおかしい……

企業間で実際にやりとりされているメールを不正に入手した上で、差出人や本文を偽装する標的型メールは、判断が非常に困難。なりすましから現金を騙し取るケースも発生しています。

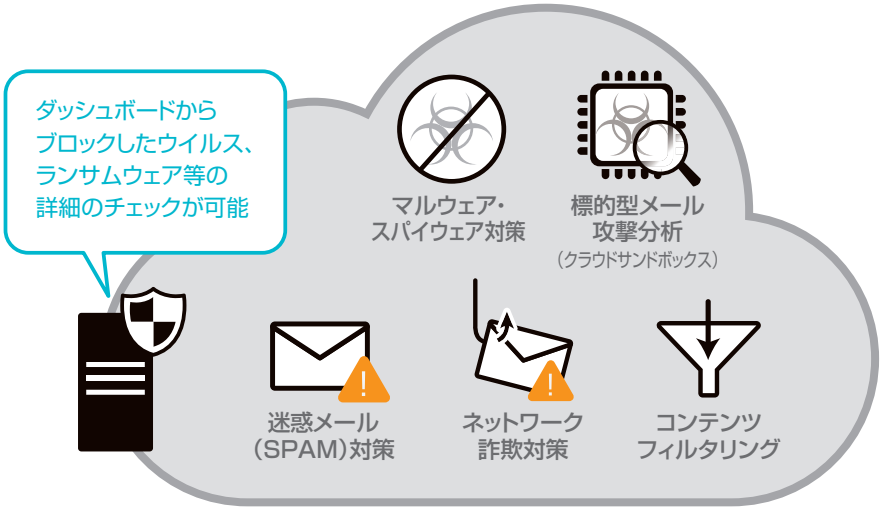
パワーポイントの文書添付?

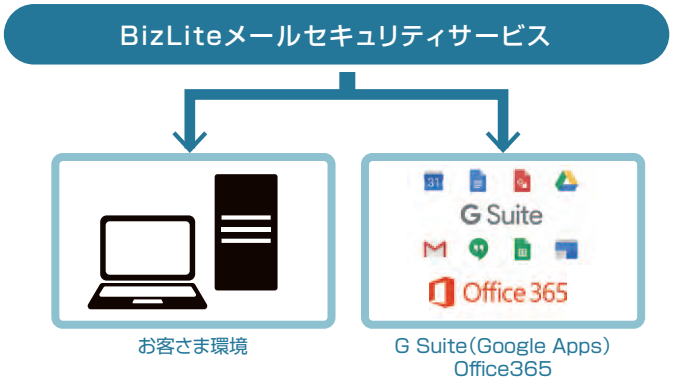
でも、日常パワーポイント文書を
やりとりする取引先ではない

開封するとウイルスに感染するファイルのアイコンを、word・excel・power point・PDF等ビジネスメールで多様されるアイコンに偽装している可能性があります。

5つのセキュリティ機能で脅威を除去

最新のメールセキュリティ基盤・トレンドマイクロ社の
“Trend Micro Hosted Email Security（HES）”をベースにしています。
管理サーバー不要のクラウド型メールセキュリティサービスです。





1 マルウェア・スパイウェア対策

コンピュータウイルスやワームなど悪質なソフトウェアを検知・ブロック。

2 標的型メール攻撃分析（クラウドサンドボックス）

不審なファイルをクラウド上で仮想実行して動作確認し脅威を判定。様々な脅威を分析・検出。

3 迷惑メール（SPAM）対策

メールサーバーに負担をかける迷惑メールを検知・ブロック。

4 ネットワーク詐欺対策

偽のホームページに接続させて、個人情報を盗み出すフィッシングメールを検知・ブロック。

5 コンテンツフィルタリング

お客様の業務内容に基づいて、ポリシーを作成し、特定のファイルタイプを指定して、そのやり取りを禁止することが可能。

導入のメリット

管理サーバー不要で初期投資費用を削減

お客さま側で管理サーバー構築やソフトウェアインストールの必要がなく、導入時の初期投資や構築に関わる時間、費用、人員を抑えたサービス導入が可能。

常に最新の攻撃や国内特有の脅威に対応

常に最新状態で、メールに起因して進入する不正プログラム・スパムメール・フィッシング詐欺対策を実現。さらに標的型メール等の新たな脅威は、クラウドサンドボックス機能で発見・対処可能。

お客様環境・クラウド環境双方に対応

お客さまの環境と、G Suite（Google Apps）やOffice365などのクラウドと双方のメールサーバーに対応しており、幅広い環境で利用できます。

ご利用要件

メールセキュリティサービスをご利用いただくには、右記の要件が必要となります。

①お客さまの独自ドメインで運用されていること。
②お客さまドメインのDNS MXレコードを変更可能であること。
③お客さまメールサーバーでHESからのSMTPを受信出来ること。

製品に関するお問い合わせ

NJS 日本情報システム株式会社
https://www.njs-net.co.jp/
〒350-1304 埼玉県狭山市狭山台4-22-2
TEL 04-2958-2221 Email isales@njs-net.co.jp
9:00～17:45（土・日祝日及び弊社指定休日を除く）