

名称	gINCクラウド型 ver2.4.3	gINCサーバ ver2.4.3
製品タイプ	クラウドサービス	オンプレミス型
◆攻撃手法 添付ファイル		
ワード(.doc/.docx)	●	●
エクセル(.xls)	●	●
PDF(.pdf)	●	●
HTML(.html)	●	●
実行ファイル(.exe)	●	●
ショートカットリンク(.lnk)*1	●	●
ZIP化	●	●
ZIP暗号化	●	●
RLO機能*2	●	●
◆攻撃手法 URLリンク		
直接型	●	●
リダイレクト型	●	●
URL偽装型	●	●
ショートリンク	●	×
オリジナルHTML	●	●
◆アドレス帳		
グループ化	●	●
CSVインポート	●	●
◆メール送信		
スケジュール設定	●	●
曜日指定	●	●
時間指定	●	●
非送信時間指定	●	●
一斉送信	●	●
連続送信	●	●
ランダム送信	●	●
送信中断・再開機能	●	●
インターバル設定	●	●
送信者偽装(アドレス偽装)	●	●
返信先設定*3	●	●
HTMLメール	●	●
PLAIN TEXTメール	●	●
やり取り型	●	×
HTML既読確認	●	●
テンプレート保存	●	●
サンプル文提供	●	●

*1 ショートカットリンクで使用できる偽装アイコンは、.doc(x), ppt(x), xls(x)です。*2 RLO (文字の流れを右から左の向きに変えるための制御文字の一つ) 機能は、訓練者のPCにインストールされているzipアプリケーションによっては正しく表記されない場合がございます。*3 デフォルトの設定はgINCサーバに返送されますが設定変更で偽装アドレスに返送することができます。*4 OSのバージョンによっては使用できない場合がございます。

*5 Windows,Mac,iPhone,iPad,Android,Linuxを判別できます。*6 Word,Excel,PDF,exe,Internet Explorer,Chrome,Firefox,Safari,Operaを判別できます。*7 表紙,copyright,問い合わせ先のカスタマイズが可能です。*8 gINCサーバにPDF,HTML,JPEG,GIF,PNG,ICOのファイルをアップロードすることができます。*9 メール環境によってはインターネット接続が必要な場合もございます。*10 標準は1ドメインのみに送信可能です。別途ドメイン追加オプションをご用意しております。*11 ご契約期間中のみの対応となります。

■サービスに関するお問い合わせ

<https://www.gateway.co.jp/ja/service/it-solution/ginc/>



標的型攻撃メール訓練の お悩みございませんか?

訓練が形骸化して
効果が今ひとつ
感じられない

毎年訓練しているが
開封率がさがらない

コスト削減のために
訓練を内製化したい

巧妙なメールは
開いてしまう
可能性があり不安

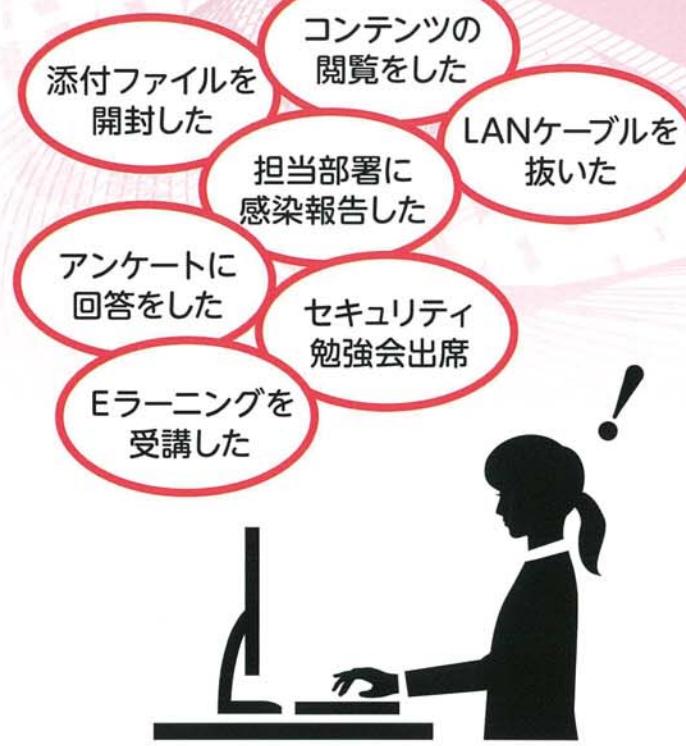
アプリケーションの
セキュリティで
訓練ができない

その訓練で
本当に会社の情報
守れますか?





開封率にこだわりすぎる訓練の落とし穴



何も実践していないので
何も経験できていない…



標的型攻撃メールは 唯一人感染させれば成功なのです。

1人感染が成功すれば、ネットワーク上で感染が拡大するだけでなく、さらに他のマルウェアを感染させたり、PCを乗っ取り、重要な情報を窃取し、外部に流出させるなどの犯罪行為が進んでいきます。

標的型攻撃メールを完全に防ぐことは 不可能と言われています。

標的型攻撃メールに使用されるマルウェアは、従来のアンチウイルスソリューションでは検知できない場合が多く、**毎日約100万種類の新種**が発生していると言われています。よって、対策が間に合わず、完全に防ぐことは困難です。

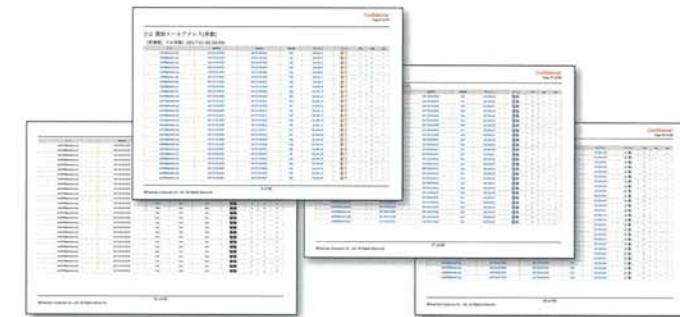
全員参加型の行動訓練を 実施しましょう。

訓練には必ず行動が伴います。訓練対象者全員が疑似標的型メールを活用し行動訓練を実施して下さい。



訓練の重要ポイント

- セキュリティルールに基づいた行動を実践訓練する。
- 全員が参加し、全員が実践する。
- 実践訓練後にメールシミュレーションを実施し訓練成果を確認する。
- 繰り返し実施し、訓練効果を持続する。



gINCはクラウド版、サーバ版共に何時でもレポート作成が可能です。

*注1:html形式メールのみ開封確認が可能となります。Plain textは対象外です。

*注2:gINCサーバのみの機能です。接続されるネットワークの環境によっては動作が制限される場合があります。

訓練目的	標的型攻撃メールの添付ファイルやURLを開いた際に、組織のセキュリティルールに基づいて実際に行動することを体で覚えてもらうこと。
事前通知	事前に疑似標的型攻撃メールの送信スケジュールと内容、受信～開封後に実施する行動ルールを徹底します。
全員参加	全員が訓練行動を実践し、インシデント発生時の対応を経験していただきます。
実施方法	開封した添付ファイルやWebサイト上で具体的な報告をしていただきます。未開封者や未報告者には催促通知をします。

