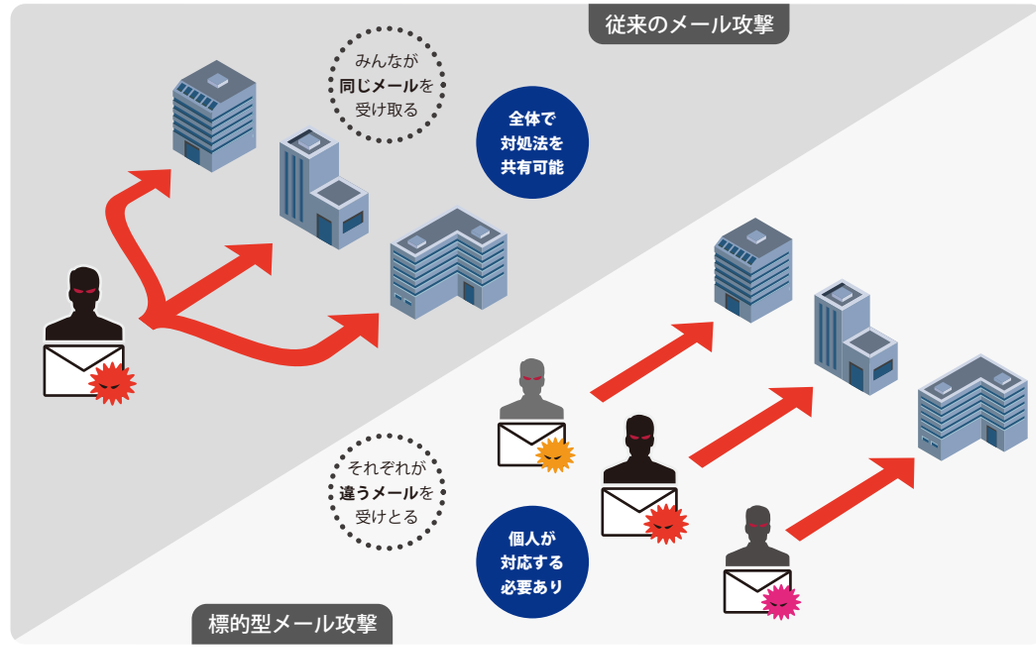
標的型メール攻撃とは

特定の人に向けて悪意ある文書や URL を添付した「なりすましメール」を送りつけることで個人情報などを盗み取る行為を**標的型メール攻撃**と呼びます。

不特定多数にウイルス付きメールをばらまくことでウイルス感染させる従来の攻撃とは異なり、情報を盗み取ることを目的として特定の組織や個人を狙った攻撃が「標的型攻撃」です。その中でも相手に合わせた内容のメールを送りつける「標的型メール攻撃」の被害報告が近年増えています。



特徴 1

情報の漏洩だけが目的とは限りません

- 攻撃者はあなたのアドレス帳などを利用して感染拡大を狙っています。
- あなたの PC を足がかりとして本学や関係機関のネットワークに侵入し，重要な機密情報を盗もうとします。
- 特に，国家レベルの組織を攻撃するために大きな大学は踏み台として利用されます。

特徴 2

特定の組織のみに狙いを絞っています

- 受信者の業務に関係の深い話題を利用してウイルス付きメールを本物らしく装います。
- 攻撃者は不信感を抱かせないように、いろいろな「だましのテクニック」を駆使します。
- 送信者は実在する組織や個人になりすまします。

特徴 3

重要な情報を持っていなくても狙われます

- 研究データや人事情報などの重要な情報を持っている人だけでなく，その周囲の人々も狙われます。
- 機密情報を持っている人との日常的なメールのやり取りが流出すると，それを真似た「なりすましメール」が作成されて最終的に重大な情報漏洩を招きます。

情報セキュリティ監査・危機管理専門委員会（東工大 CERT）
／情報基盤課 情報企画グループ

標的型メール攻撃がきっかけで大きな被害に !!

個人情報の漏洩数に対する推定被害額

1,000 人分の個人情報が漏洩した場合の予測される平均被害額は 600 万円～1,000 万円と言われています。

最近の事例では、他大学においてサイバー攻撃により 11 万人分の情報流出の疑いが生じました。

この事件では後日の調査によって実際には情報流出がなかったことが判明したにもかかわらず、管理不手際のお詫び文書の郵送するだけでも 80 円 × 11 万通 ×2 回の 1760 万円の費用が生じ、全体としては数千万円の損害が発生する結果となりました。

個人情報の漏洩数	推定被害額
100 人分	約 300 万円
1000 人分	約 800 万円
1 万人分	約 2000 万円
10 万人分	約 5500 万円
100 万人分	約 1 億 5000 万円
1000 万人分	約 4 億円
1 億人分	約 10 億円

Verizon 2015 年 データ漏洩／侵害調査報告書 より
https://www.verizonenterprise.com/jp/DBIR/2015/

情報流出の疑いがあるだけでも，数百万から数千万円の被害が生じることがあります

個人情報などの流出はプライバシーの侵害だけでなく，漏洩させてしまった組織に対しても大きな被害を与えることになります。

標的型攻撃の被害者がいつの間にか加害者として扱われることがあります

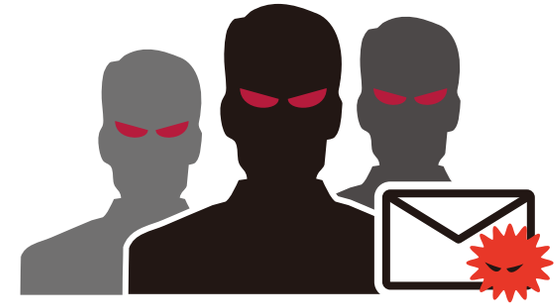
日本年金機構は，厚生省を騙った標的型メール攻撃の被害者でもありましたが，125 万件の個人情報流出や正しい事後対応ができなかったことから，まるで加害者のように糾弾される結果となりました。

感染端末を放置すると内部感染が拡大し，大規模な情報漏えい事件に繋がる可能性があります

ネットワーク内部にウイルス感染した端末が 1 台でもあると，感染したあなたの PC を踏み台にして更なる情報流出を招く危険性があります。

情報セキュリティ監査・危機管理専門委員会（東工大 CERT）
／情報基盤課 情報企画グループ

メールを受信したら



1 少しでも怪しいと思ったら まずは周りの人に相談しましょう

周りと相談することで被害を減らすことができます。
一人でも開いてしまったら攻撃は成功です。

2 そのメールに心当たりはありますか？

たくさんの「なりすましメール」が毎日送信されています。
心当たりのないメールは，差出人に問い合わせるくらいの慎重さが必要です。

3 普段やりとりしている業務メール だからといって安心ですか？

メールの相手が標的型攻撃によりウイルス感染し、
盗まれたメールが悪用されているかもしれません。

4 興味を惹く内容だからといって 安易に開いてはいけません

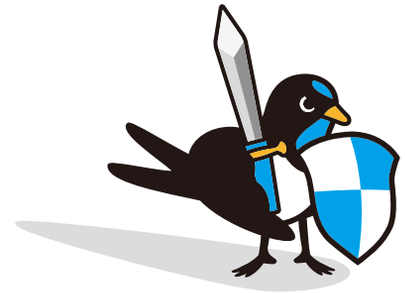
あなたが何に興味を持つか知られている可能性があります。

5 あなたのクリックが「不審なファイルを開く」という命令となるかもしれません

PC は「命令」がないと何も出来ません。不審なファイルに対するあなたのクリックは、「ウイルスファイルを実行しなさい」という命令であるかもしれません。
メールの添付ファイルや URL リンクをクリックする際は十分注意を払う必要があります。

情報セキュリティ監査・危機管理専門委員会（東工大 CERT）
／情報基盤課 情報企画グループ

不審なメールを開封してしまったら



しまった！と思ったら

不審なメールの添付ファイルを開いたり，URL をクリックしてしまった場合は落ち着いて次の手順で対応しましょう。

❶ ネットワークから切り離す

まずは LAN ケーブルを外す，または無線 LAN をオフにしましょう。被害の状態を確認できるようにするため，電源はつけたままにしましょう。

❷ 周りの人に相談する

できるだけ早く身近な人に相談しましょう。標的型メールであった場合，すぐに状況を伝えることで被害を最小限に抑えることができます。

❸ 東工大CERTにご連絡を

感染が疑われる場合や標的型攻撃と思われるメールを受け取った場合はすみやかに東工大 CERT へご連絡ください。

[連絡先]　**情報システム緊急対応チーム**

東工大 CERT（サート）

http://cert.titech.ac.jp

内線：

3272

e-mail:

contact@cert.titech.ac.jp

情報セキュリティ監査・危機管理専門委員会（東工大 CERT）
／情報基盤課 情報企画グループ

被害を防ぐための対策

「標的型メール攻撃」に限らず，様々なサイバー攻撃から身を守るためには利用者全員が意識してその対策に取り組む必要があります。アップデートなどの技術的な対策と普段からメール内容をチェックするなどの意識的な対策の双方に取り組むことが重要です。

1

ソフトウェア／ウイルス定義ファイルは最新に

ウイルス対策ソフトを導入しているだけで安心してはいけません。常に最新の OS ／ソフトウェアを利用し，それと同時にウイルス定義ファイルを最新に保つことが最低限のウイルス対策です。

2

パスワードを使いまわさない／複雑なパスワードを使用する

同じパスワードを使いまわしていると一度パスワードが漏れるだけで，大学のアカウントなどを不正に利用されるだけでなく、個人使用の PC やクラウド上のデータが盗まれるなど被害を招いてしまいます。

技術的な対策

3

不審なメールの見分け方と取扱方法を学ぶ

「なりすましメール」による攻撃は，いくつかのポイントを確認することで多くの被害を避けることができます。また攻撃を受けた際の対応方法を知っていると被害を最小限に留めることができます。

4

誰もが標的型攻撃の対象であることを認識する

重要な情報を持たない PC でも踏み台としての利用価値があります。自分は無関係と考えていると結果的に大規模な被害を招きかねません。自身が攻撃対象であることを意識し、左記の対策を常に心がけてください。

意識的な対策

情報セキュリティ監査・危機管理専門委員会（東工大 CERT）／情報基盤課 情報企画グループ