標的型メール攻撃対策について

三重大学総合情報処理センター・自然科学系技術部
松原　伸樹
matsubara@cc.mie-u.ac.jp

１．はじめに

標的型メール攻撃は年々増加しており、独立行政法人情報処理推進機構（IPA）によると、2017、2018ともに、脅威の一位は『標的型攻撃による情報流出』でした。そこで三重大学では、昨年度、初めて標的型メール攻撃訓練を教職員向けに実施し、今年度も引き続き標的型メール攻撃に対する対策を進めています。

ここでは、今年度実施した対策について報告したいと思います。

２．これまでの取り組み

昨年度行った取り組みとしまして、標的型メール攻撃訓練があります。工学部技術部の深澤さんが主体で、総合情報処理センターと協力して実施を行いました。今年度も実施予定です。

また、通常の攻撃メール対策としてトレンドマイクロ社の IMSVA (InterScan Messaging Security Virtual Appliance) というセキュリティソフトを導入しております。図 1 が、今現在のメールの流れです。ここで毎日 2000 通から、多いときは 5000 通もの迷惑メールを遮断しています。

ただし、それでも未知のウィルスメールや IMSVA では検知できなかったウィルスメールがエンドユーザのもとに届いてしまいます。

そこで、総合情報処理センターでは昨年度から今年度にかけていくつかの対策を導入してきました。

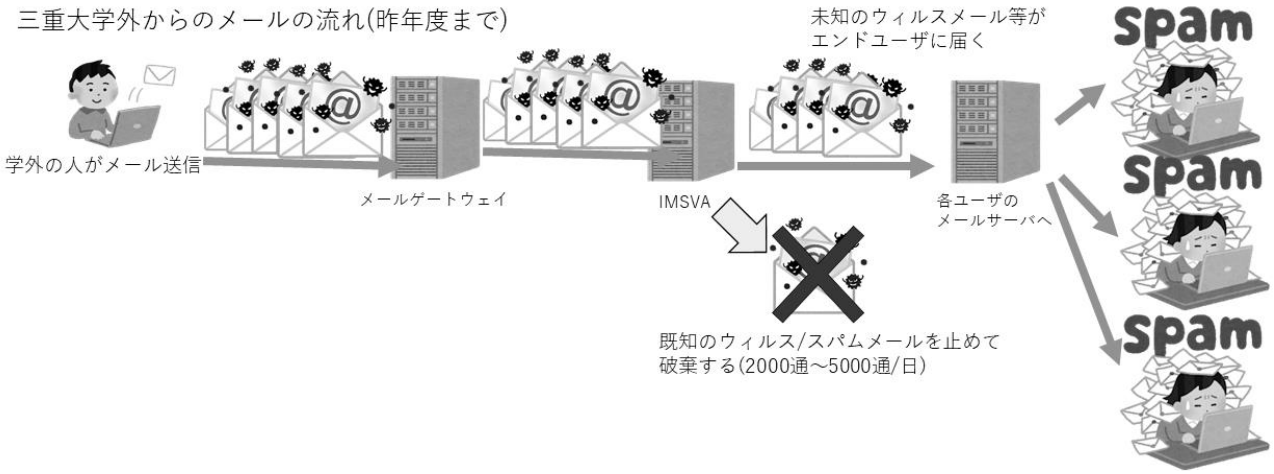

図 1. メールの流れ

３．昨今の取り組み

３－１．From 詐称メールの遮断及び、学内専用メーリングリストの登録

総合情報処理センターでは、学外から From 詐称メールを遮断することを進めてきました。

例えば、総合情報処理センターから送信する support@cc.mie-u.ac.jp のメールアドレスは、三重大学の総合情報処理センターからしか送られないメールアドレスです。

これが学外から送られてきた場合、ほぼ間違いなく迷惑メールです。これは、あたかも総合情報処理センターからお知らせメールが来たと利用者に思わせて、リンクをクリックさせてウィルス感染させる

ことを目的としています。これを防ぐため、学外から support@cc.mie-u.ac.jp のメールが送られてきた場合、遮断されるよう行いました。

これと同様の設定を承認が得られた組織のドメイン(@eng.mie-u.ac.jp @ab.mie-u.ac.jp 等)に対して行っていきました。

また、学外から受ける必要のないメーリングリスト等を学内専用メールアドレスとして登録を始めました。例えば、総合情報処理センターから学生に向けて一斉配信するメールは、総合情報処理センターの教職員からしか送らないメールです。誰もが送れるようにする必要はありませんので、学内専用メールアドレスとして使えるようにしました。Mailman 等のメーリングリストシステムでは標準搭載されていますが、普通のメールアドレスでも学内専用にすることが出来ます。

これらの対策が迷惑メールの遮断に一役買っており、この設定により遮断できた数を図 2 に示します。昨年 5 月頃には約 15,800 通のメールの遮断を行うことが出来ました。

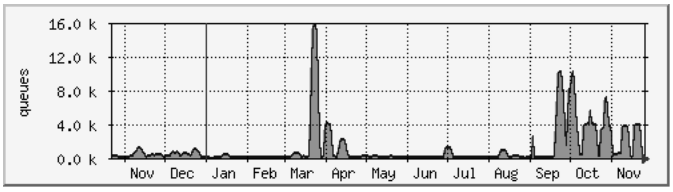

図 2. 遮断したメール数

３－２．特殊拡張子の遮断

今年 8 月頃に、図 3 のアイコンのような、.iqy で始まる添付ファイルのウィルスが送られてくることが多数ありました。これは、Microsoft Excel に関連付けされているファイルで、ダブルクリックすると Excel が起動します。

『Microsoft セキュリティに関する通知』(図 4 参照)というメッセージとともに、ここで有効を選択すると、ウィルスがダウンロードされます。

図3. iqy のアイコン

図 4. 『Microsoft セキュリティに関する通知』画面

.iqy という拡張子ファイルですが、普段パソコン操作をしている中で、ほぼ見ることはない拡張子と思われます。エンドユーザへウィルスメールの注意喚起をして自衛を促すのも必要ですが、利用者に届く前に使う事はないであろう拡張子を遮断することで、.iqy メールからの感染を防ぎました。

３－３．FireEye の導入

上記のような迷惑メール対策を行っても、どうしても未知のウィルスメールが通過してきてしまいます。この未知のウィルスメールを防ぐために、今年度 10 月末に、FireEye の導入を行いました。

FireEye とは、SandBox という仕組みを備えたシステムです。SandBox とはウィルスか否か判別がつかないすり抜けてきたファイルを、実際に仮想 OS で実行してみて、ウィルスのダウンロードを始めたり、ウィルスと同じ動きをし始めたら、遮断するという仕組みです(図 5 参照)

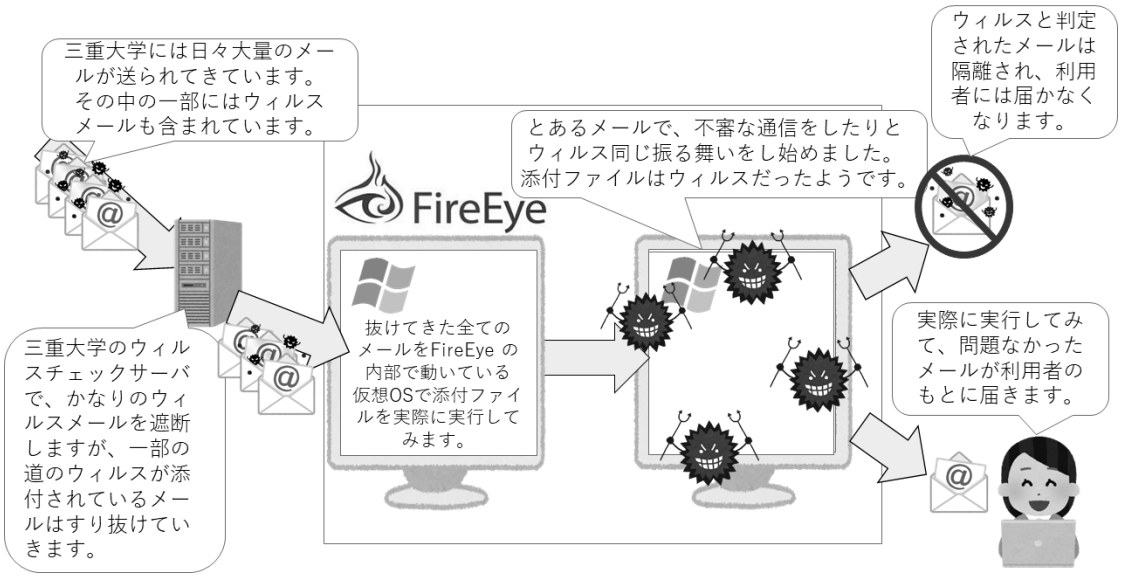

図 5. SandBox の仕組み

11 月 1 日からの FireEye でのメール遮断件数を図 6 に示します。

事前に複数の迷惑メール対策を入れているため、遮断件数自体は多くないですが、一定の効果が見られます。

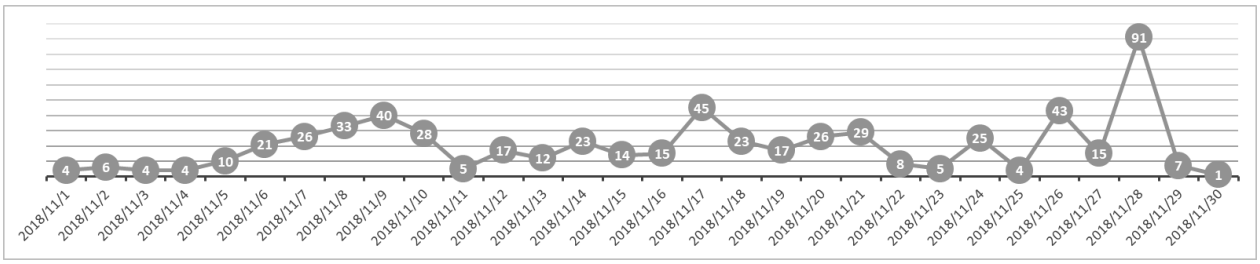

図 6. FireEye での遮断件数一覧

FireEye 導入直前、10 月 24 日にとある部署に、「件名：立替金報告書の件です。」という件名で、メールが来ました。未知のウィルスが添付されたメールだったため、利用者にまでメールが届いてしまうという事がありました。

さらに、メールが届いた人は不審に思い ウィルス対策ソフトの Eset Endpoint Security で検査を行っていたにもかかわらず、未知のウィルスであったため検査に引っかからず、該当ファイルを開くという事がありました。

FireEye は該当ファイルを実行後にどのような動きをするかによってウィルスかどうかを判断しますので、このような未知のウィルスを検知し感染防止することに役立ちます。

FireEye には、利用者に遮断したメールの通知機能があります。図 7 のような画面のメールが各利用者に送られます。もし誤検知されてしまった場合でも、利用者はこのメール通知を見て、総合情報処理センターに連絡して解除することが出来ます。

毎日 7 時に、メールが送られてきますので、朝一でチェックしてみて、もし問題なさそうなメールが遮断されていたら、ご一報いただければ幸いです。FireEye 以外の部分では、利用者に通知機能がないため、本来届くはずのメールが届いていないなどあればご連絡ください。


三重大学
MIE UNIVERSITY

[redacted]@cc.mie-u.ac.jp 宛メールレポート

FireEyeにてメールをブロックしました、ご不明な点は、総合情報処理センターにお問い合わせ下さい。

電話番号：059-231-9772(内線 9772)

メールアドレス：support@cc.mie-u.ac.jp

ブロックしたメール一覧

From	Subject	Reason	Date
		Advanced Threat	Oct 29, 2018 07:23 UTC
		Advanced Threat	Oct 29, 2018 07:09 UTC
		Advanced Threat	Oct 29, 2018 05:58 UTC
		Advanced Threat	Oct 29, 2018 04:04 UTC

図 7. 遮断したメールの通知

３－４．取組後のメールの流れ

取組後のメールの流れを図 8 に示します。いままで、IMSVA というシステムのみで止めていたウィルスメールを、多重化して止めているため、より利用者には正常なメールのみが届くようになりました。

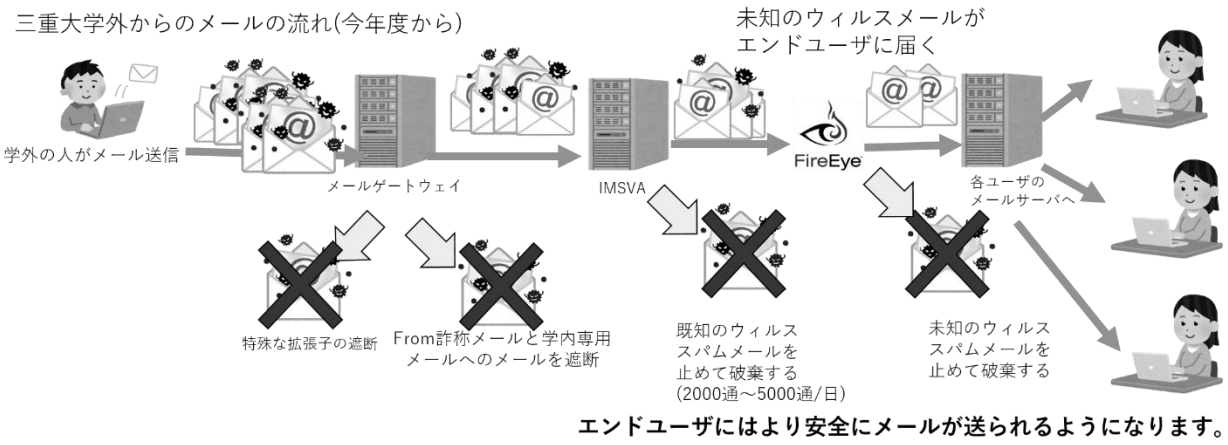

図 8. 取組後のメールの流れ

４．終わりに

今年度実施した対策を書いていきましたが、これでもなおすり抜けて届いてしまうメールもあります。また、対策を増やしていくと、正常なメールにもかかわらず、スパムメールだと誤判断して、メールを遮断してしまう事もあります。

個人のメールでも、メールアドレス遮断は受け付けていますので、大量に特定のメールから迷惑メールが来るという事があったら、総合情報処理センターまでご連絡いただければ、対応させていただきますので、ぜひご一報ください。

参考資料

1) 情報セキュリティ 10 大脅威 2018 https://www.ipa.go.jp/security/vuln/10threats2018.html
2) IQY ファイルを悪用する攻撃手口に関する注意点 https://www.ipa.go.jp/files/000068065.pdf
3) FireEye 各種資料