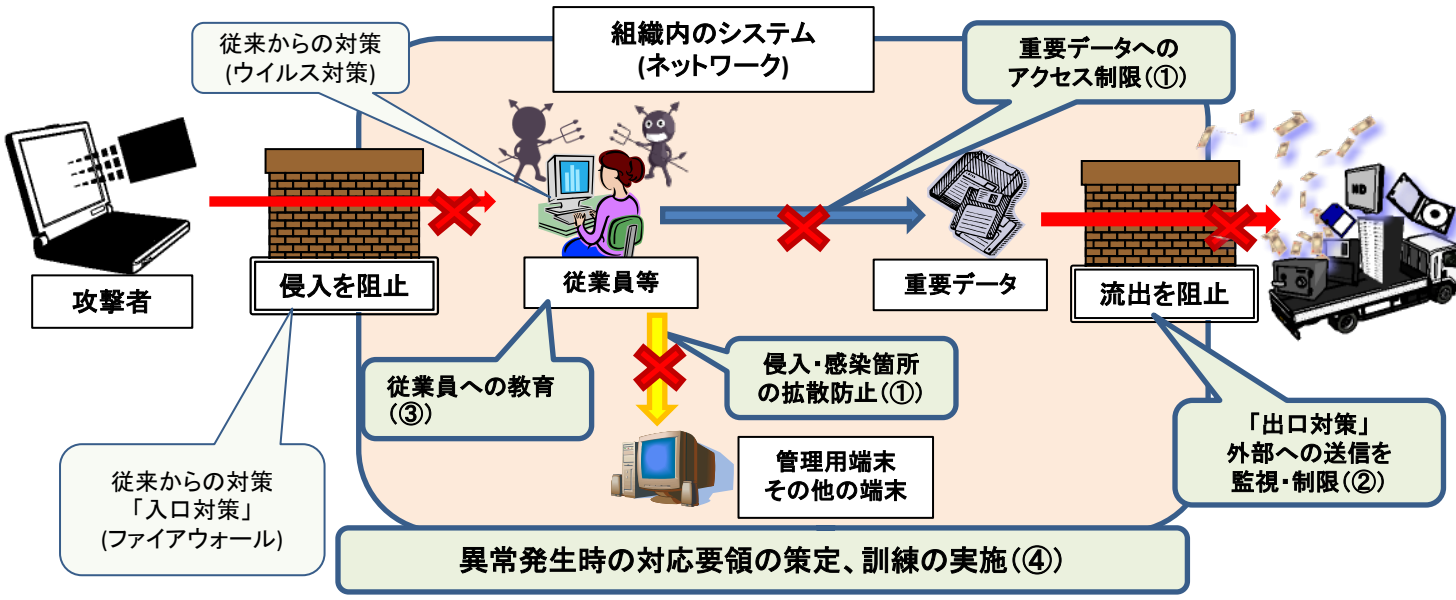
平成28年8月

「標的型メール攻撃」等による情報流出の防止について

外部からの不正なメールや通信により、**重要な情報が盗まれる被害が多発**しています。
この種被害を防止するには、**侵入を阻止するための対策(「入口対策」)だけでは不十分**です。
侵入されても被害を発生・拡大させないための対策(「出口対策」など)を併せて実施しましょう。



① ユーザーの権限、データ保管方法等の再検討

- ○ 重要なデータが保管された機器は、ネットワーク上で区別された場所への配置を検討する
- ○ 管理者としての権限を一般の利用者には付与せず、厳重に管理する
- ○ 業務に不必要な機能及びソフトウェアは、サービス停止又はアンインストールする

② 不正な通信を早期に検知できる仕組みの導入

- ○ インターネットへの接続はプロキシを経由する構成とし、外部との直接の通信を禁止する
- ○ 機器の利用や通信に関するログが記録されているか確認し、保管を徹底する
- ○ 侵入検知システム(IDS)、侵入防御システム(IPS)の導入を検討する

③ 前兆を察知し対処するための従業員への教育

- ○ 危険なメールの特徴(非公開アドレスへの着信やファイルの添付など)について啓発する
- ○ メールや端末動作に不審を感じた場合は、攻撃と確信できなくても報告されるよう徹底する

④ 異常発生時の対処要領策定と訓練の実施

- ○ 情報セキュリティポリシーや異常発生時の対処要領を策定し、有事の対応を迅速化する
- ○ 擬似的な攻撃を体験させるなどの実戦的訓練を実施し、対処要領の確認と意識向上を図る

標的型攻撃対策については、IPA(独立行政法人情報処理推進機構)のウェブサイトにも掲載されています。
(http://www.ipa.go.jp/security/ta/index.html)

三重県警察本部生活安全部サイバー犯罪対策課
〒514-8514津市栄町1丁目100番地　電話　059-222-0110

「標的型メール攻撃」等による情報流出の防止について

① ユーザーの権限、データ保管方法等の再検討

○ 重要なデータが保管された機器は、ネットワーク上で区別された場所への配置を検討する

→ 個人情報やマイナンバーなど重要な情報を保存するサーバー、それらの情報にアクセスする機器などについては、ネットワークセグメントの分離を検討してください。

○ 管理者としての権限を一般の利用者には付与せず、厳重に管理する

→ 重要な情報を扱う機器の認証情報や管理者としてのアカウントは、悪用や流出による影響が特に深刻なものとなることから、より厳重に管理してください。

○ 業務に不必要な機能及びソフトウェアは、サービス停止又はアンインストールする

→ ソフトウェアに含まれる脆弱性の影響を最小限にするため、不要なソフトウェアを削除するほか、個々の使用者が独断でソフトウェアをインストールできないようにするなど、機器の管理を徹底してください。

② 侵入を早期に検知できる仕組みの導入

○ インターネットへの接続はプロキシを経由する構成とし、外部との直接の通信を禁止する

→ 機器の側でプロキシを使用する設定にするだけでなく、ファイアウォールの設定についても確認し、機器と外部の直接の接続を遮断するようにしてください。

○ 機器の利用や通信に関するログが記録されているか確認し、保管を徹底する

→ プロキシ、DNS、DHCPのログは確実に記録し、１年程度は保存するようにしてください。
（攻撃を受けてから被害が判明するまで、相当の期間を要する傾向にあります。）

○ 侵入検知システム(IDS)、侵入防御システム(IPS)の導入を検討する

→ IDS、IPSの設置にはコストと運用者の知識を要しますが、システムの規模や情報の重要度などによっては大きな効果を発揮する装置なので、導入も検討してください。

③ 前兆を察知し対処するための従業員への教育

○ 危険なメールの特徴（非公開アドレスへの着信やファイルの添付など）について啓発する

→ 一般の端末利用者に対して注意すべきメールの特徴などを具体的に示すなど、早期に攻撃の兆候を捉えることができるようにしてください。

○ メールや端末動作に不審を感じた場合は、攻撃と確信できなくても報告されるよう徹底する

→ 攻撃の兆候は様々であるため、通報すべき要件を限定しすぎると兆候を見逃すことにつながります。攻撃を早期に察知するためには、「疑い」の段階で組織的に対応する必要があります。端末利用者が何らかの「違和感」を覚えた際に通報しやすいよう、配慮をすることも有効です。

④ 異常発生時の対処要領策定と訓練の実施

○ 情報セキュリティポリシーや異常発生時の対処要領を策定し、有事の対応を迅速化する

→ ウイルス感染や情報流出等の異常が発生した際、ネットワークの遮断や機器の分離などの対応を迅速かつ的確に行うためには、機器の構成や設定内容などを定期的に確認し、状況を常に把握した上で、あらかじめ異常発生時の対応要領を定めておくことが重要です。

○ 擬似的な攻撃を体験させるなどの実戦的訓練を実施し、対処要領の確認と意識向上を図る

→ 異常の発生を想定した実戦的訓練などにより、対処要領や対処体制が実際に機能するか確認しておくことが重要です。また、実戦的な訓練は端末利用者の意識を向上させる面でも非常に有効です。

三重県警察本部生活安全部サイバー犯罪対策課
〒514-8514津市栄町１丁目100番地　電話　059-222-0110