

ふくしまPITネットワーク No.39

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for **I**llegal Leakage of **T**echnological Information

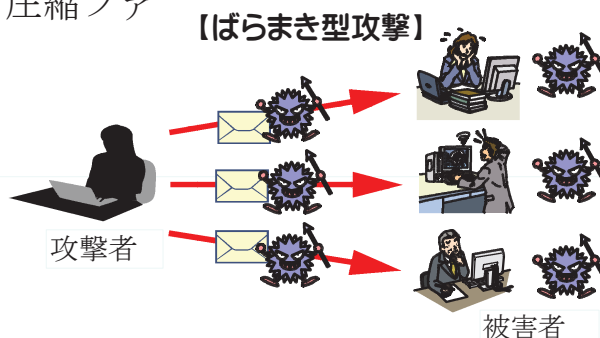
標的型メール攻撃の手口等



標的型メール攻撃の手口

- 「ばらまき型」攻撃※ の多発傾向が継続
「ばらまき型」攻撃が多数発生し、全体の85%を占め、引き続き高い割合となっています。
- 多数が非公開メールアドレスに対する攻撃
標的型メールの送信先メールアドレスについて、インターネット上で公開されていないものが全体の82%を占めています。
- 多くの攻撃において送信元メールアドレスを偽装
標的型メールの送信元メールアドレスについては、偽装されていると考えられるものが全体の90%を占めています。
- 標的型メールに添付されたファイルの形式の変化
標的型メールに添付されたファイルの形式については、2019年上半期は、前年約7割を占めたWord・Excel形式のファイルの割合が減少し、圧縮ファイルの割合が増加しました。

※ 標的型メール攻撃のうち、同じ文面や不正プログラムが10か所以上に送付されたものを「ばらまき型」として集計しています。



事例

- 注文内容の確認と称し、添付ファイルを開くよう誘導するメールが、事業者の非公開メールアドレスに対して送信された。
- 国際情勢に関する資料の送付と称して、添付された圧縮ファイルを解凍し、生成されたファイルを開くよう誘導するメールが、送信元メールアドレスを偽装して事業者に対して送信された。

これまで紹介した内容は、警察庁のホームページに詳しく掲載しておりますので、興味のある方は、警察庁のホームページをご覧ください。



ふくしまPITネットワーク No.40

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for Illegal Leakage of Technological Information

情報漏えい対策(視認性の確保に資する対策)



目につきやすい状況を作り出す対策

○ 防犯カメラの設置等

- ・ 秘密情報が記録された書類・電子媒体が保管された書庫や区域など、秘密情報の不正な取得や複製の現場となり得る場所に防犯カメラを設置して、情報漏えい行為を行おうとする者に「**見られている**」という認識を持たせるようにします。



- ・ この対策は、秘密情報の保管区域にアクセス権者のICカードでのみ入室を可能としている場合に、アクセス権を持たない者がアクセス権者のICカードを使用して入室したり、アクセス権を持たない者がアクセス権者と一緒に入退室することを防止するなど、アクセス権者とICカードの使用上の同一性を担保し、「接近の制御」(No. 23～26に掲載)に資する対策を補完する効果もあります。

- ・ 視認性の効果を高めるためには、見えやすいところに防犯カメラを設置するとともに、そのそばに「防犯カメラ作動中」といった掲示をすることが考えられます。この掲示は、本対策の効果を高めるとともに、従業員等が知らない間に撮影されていたということがないようにする意味でも重要です。



- ・ 抑止力の観点からは、必ずしも全時間帯の映像を記録しておく必要はないものの、情報漏えい行為者に対する責任追及の際に必要な証拠の確保の観点からは、より多くの時間帯で映像が記録されていることが望ましいと考えられます。

衣類メンテナンス業の防犯カメラ設置の事例として、顧客対応・洗浄等のすべての行程を撮影・録画しています。作業の録画をクレーム対応(従業員保護)、従業員自身のスキルチェックに活用し、高付加価値サービスの実現に貢献しています。



※ 平成28年2月経済産業省策定「秘密情報の保護ハンドブック～企業価値向上に向けて～」から抜粋

ふくしまPITネットワーク No.41

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for **I**llegal Leakage of **T**echnological Information

情報漏えい対策(視認性の確保に資する対策)



目につきやすい状況を作り出す対策

○ 外部へ送信するメールのチェック

外部へのメール送信の際に、上司の承認を必要とするシステムを使用したり、自動的に上司等にもCCメールが送信されるよう設定したり、従業員のメールの送受信内容を必要に応じて閲覧する場合があることを周知したりするなど、外部とのメールでのやり取りが上司等に把握される可能性があることを認識させることで、メールでの情報漏えい行為を行いにくい状況を作ります。

※ 本対策を講ずる前提として、「社内メールの業務目的以外の使用を禁止していること」、「メールのやりとりをモニタリングする可能性があること」を予め就業規則等の規定に盛り込んでおく等して社内に周知し、従業員等のメールが知らない間にチェックされていたということがないようにすることが重要です。



○ 内部通報窓口の設置

- 従業員等が、他の従業員の情報漏えい行為と思わしき行為を確認した場合の通報窓口を設置し、窓口が設置された旨を周知します。
- 内部通報を無用に躊躇することがないように、匿名での私書箱等を設置するなど通報者の匿名性を確保する工夫を行います。この場合、内部通報者に不利益を及ぼさないように配慮することも重要です。



匿名通報

内部通報窓口の設置は、自己の属する部門以外の部門へと通報することが可能となるよう、複数部門において窓口を設置することが考えられます。



※ 平成28年2月経済産業省策定「秘密情報の保護ハンドブック～企業価値向上に向けて～」から抜粋