広　報　資　料
平成26年２月27日
警備企画課・情報技術解析課

平成25年中のサイバー攻撃の情勢及び対策の推進状況について

１　概況　－ 手口の巧妙化・多様化と周到な準備による計画的な攻撃 －

平成25年中は、引き続き、我が国の民間事業者等に対し、情報窃取を企図したとみられる標的型メール攻撃が発生。「ばらまき型」攻撃の減少により、前年と比べて大幅に減少したものの、「やりとり型」攻撃の増加、不正な外部接続の発覚を免れようとする手口の出現等、攻撃の手口は巧妙化

また、攻撃者が、特定の事業者等に関する情報を事前に収集した上で、標的型メールを送信していた事例を確認。周到に準備をした上で攻撃を敢行している状況が判明

さらに、「水飲み場型攻撃※」と呼ばれるサイバー攻撃を国内で初めて確認するなど、手口は巧妙化・多様化

詳細は別紙のとおり

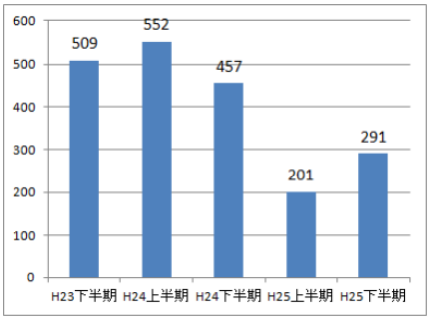
※　対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる手口

２　標的型メール攻撃の情勢と手口

○　平成25年中に警察が把握した標的型メール攻撃は492件で、前年比▲517件(▲51.2%)

○　前年に比べ「ばらまき型」攻撃が減少する一方、「やりとり型」攻撃が大幅に増加

○　不正な外部接続を正当な通信に紛れ込ませることで発覚を免れようとするものや解析が非常に困難な不正プログラムを確認



【警察が把握した標的型メール攻撃の件数】

○　特定の事業者等の同期職員等の情報交換に利用されていたグループメールサービスに、攻撃者が潜入していたことが判明。攻撃に先立ち、当該事業者等の名簿やメールアドレスを収集していた可能性

３　新たな手口によるサイバー攻撃

「水飲み場型攻撃」を国内において初めて確認したほか、平成26年に入り、広く利用されている無償ソフトウェアの更新を悪用して不正プログラムに感染させる手口も確認されており、サイバー攻撃の手口は巧妙化・多様化

４　警察のサイバー攻撃対策

(1)　態勢の強化

○　平成25年４月、13都道府県警察にサイバー攻撃特別捜査隊を設置。同年５月、警察庁に「サイバー攻撃対策官」とこれを長とする「サイバー攻撃分析センター」を設置

○　同年５月、サイバーフォースを都府県（方面）情報通信部まで拡充

(2)　実態解明

○　国際捜査共助要請件数　130件（前年比＋　23件）

(3)　官民連携を通じた情報共有の推進

○　サイバーテロ対策協議会

・　個別訪問を通じた情報提供・交換　3,329回（　＋1,935回）

・　セミナーの開催　236回（　＋　115回）

○　サイバーインテリジェンス情報共有ネットワーク

・　参加事業者等の拡充　6,020社（約　＋1,120社）

・　事業者等から提供を受けた標的型メールの数　492件（　▲　517件）

・　情報共有の結果新たに発見された標的型メールの数　4,805件（　＋4,035件）

○　不正プログラム対策協議会

・　会員に提供した情報数　117件（　＋　95件）

○　サイバーインテリジェンス対策のための不正通信防止協議会

・　会員に提供した情報数　220件（　－　）

(4)　被害未然防止措置

○　サイバー攻撃の呼び掛け等に関する情報を攻撃対象組織等に提供　20件（　－　）

(5)　対処訓練の実施　100回（　－　）

○　サイバーテロ対処要領を策定し、初動対処訓練を全ての都道府県（方面）警察において実施

○　重要インフラ事業者等の共同訓練を実施

別　紙

平成25年中のサイバー攻撃情勢について

1　概況

平成25年中は、前年に引き続き、我が国の民間事業者等に対し、情報窃取を企図したとみられる標的型メール攻撃が発生したことを把握した。警察では、「サイバーインテリジェンス情報共有ネットワーク[*1]」を通じ、標的型メール攻撃等のサイバー攻撃事案に係る情報を集約するとともに、事業者等による情報システムの防護に資する分析結果等の情報を共有している。

警察は、25年中、本ネットワークを通じて、事業者等に対する標的型メール攻撃492件（前年同期比▲517件(▲51.2%)）を把握した。また、政府機関に対する標的型メール攻撃に関する情報を集約・分析している内閣官房情報セキュリティセンター（NISC）と連携し、政府機関に送付された標的型メールの分析結果についても、本ネットワークを通じて事業者等と情報共有している。共有された情報を基に各事業者等が対策を講じた結果、新たに標的型メール攻撃の可能性のあるメールが4,805件（前年同期比＋4,035件（＋524%））確認されており、被害の未然防止や拡大防止につながっている。

警察では、25年中、情報窃取を企図したとみられるサイバー攻撃として、標的型メール攻撃のほか、「水飲み場型攻撃」と呼ばれる新たなサイバー攻撃の手口の発生を、国内において確認した。また、26年に入り、広く利用されている無償ソフトウェアの更新を悪用して不正プログラムに感染させる手口を確認しており、サイバー攻撃の手口は多様化している。

海外においては、25年３月、韓国の複数の金融機関及び放送局において、数万台に及ぶコンピュータが不正プログラムに感染し、同時多発的にデータが破壊された結果、金融取引やニュース原稿の作成に影響が及び、国民生活や社会経済活動に大きな支障が生じた。

このように、サイバー攻撃の手口は巧妙化・多様化の一途をたどっており、また、ITに対する社会経済活動の依存度が増す中、サイバー攻撃の脅威はこれまでになく増大している。

2　標的型メール攻撃の情勢と手口

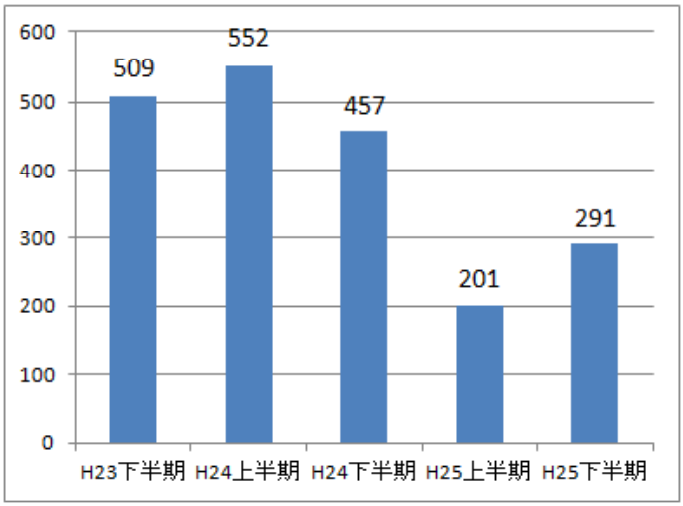
(1)　「ばらまき型」攻撃の減少

---

*1　23年８月、標的型メールに関する情報を共有することで被害拡大の防止を図ることを目的として、警察と先端技術を有する事業者等が構築した情報共有ネットワークで、26年１月現在、6,020社が参画している。

25年中、警察が把握した我が国の民間事業者等に対する標的型メール攻撃は492件（上半期201件、下半期291件）であり、24年（1,009件）に比べて大幅に減少した。

減少の主な原因としては、国内外の情勢を捉えた情報提供を装い多数の宛先に同一内容のメールを送付する「ばらまき型」攻撃が、24年に比べて大幅に減少したことが挙げられる。「ばらまき型」攻撃は、同じ文面や不正プログラムを多数送信することから、攻撃が発覚する可能性が高いため、攻撃者が避けたものとみられる。



【警察が把握した標的型メール攻撃の件数】

	ばらまき型[*2]	ばらまき型以外
24年中	88%(888件)	12%(121件)
25年中	53%(259件)	47%(233件)

【ばらまき型とそれ以外の標的型メール攻撃の割合】

(2)　「やりとり型」攻撃の増加

「ばらまき型」攻撃が減少したことで、標的型メール攻撃は大幅に減少したものの、攻撃先を限定した標的型メール攻撃は増加した。特に、攻撃対象にいきなり不正プログラムを送付するのではなく、採用活動や取引等の業務との関連を装った通常のメールのやりとりを何通か行うことにより、添付ファイル付きのメールが送られても不自然ではない状況を作った上で、不正プログラムを添付したメールを送り付ける「やりとり型」攻撃が、25年中は37

*2　同じ文面や不正プログラムが10か所以上に送付されていた標的型メール攻撃を「ばらまき型」として集計している。

件発生し、24年中の２件から大幅に増加した。

やりとりするメール本文に記載された内容は、約５割（17件）が職員採用に対する質問や応募を装ったものであり、約４割（13件）が製品に関する質問や不具合の報告を装ったものであった。不正プログラムは、履歴書、質問状、製品の不具合の状況、製品カタログ等を記録した文書ファイルと称して、送付されていた。やりとりを開始する１通目のメールの内容の多くは、問合せ先のメールアドレスを確認するものであったが、企業のウェブサイトに設置された問い合わせ用のメールフォームを利用したものも確認されている。

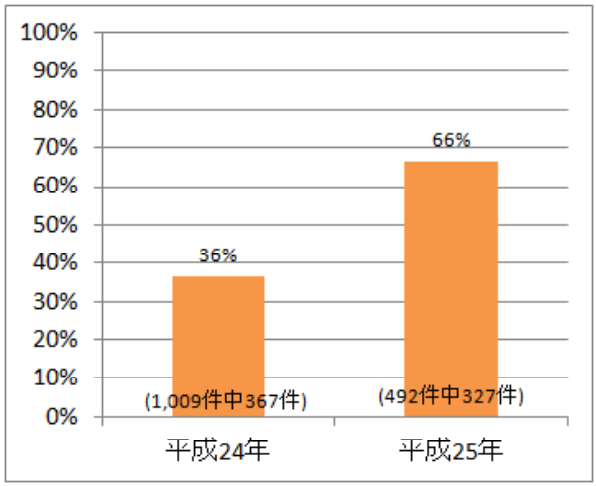
攻撃を受けたメールアドレスは、ウェブサイトで公開されているものや職員氏名等から容易に推測可能なものが、全体の約３割（確認した386個のアドレスのうち103個）を占めた。

不特定多数からのメールを受信する機会の多いパソコンは、組織内の通常業務用のネットワークとは分離し、不要なプログラムが動作しない仕組みを導入するなどの対策を講じることが重要である。

(3)　フリーメールアドレスを送信元とする攻撃の増加

標的型メール攻撃の送信元アドレスとして、フリーメールアドレス*3を使用するものの割合が増加した。特に「やりとり型」攻撃は、全てフリーメールアドレスを使用したものであった。

メールサーバの設定により、フリーメールアドレスから送信されたメールを受信した場合には、件名や本文に警告を表示し、受信者に注意を促すなどの対策を講じることが重要である。



【フリーメールアドレスを送信元とする
標的型メール攻撃の割合】

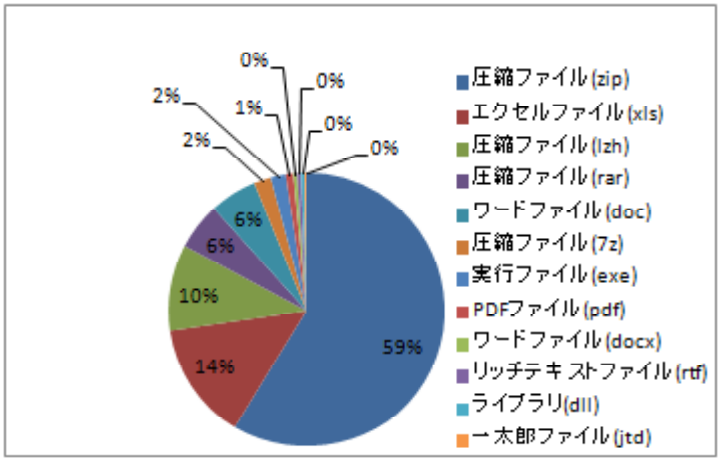
*3　無料で利用可能なメールアドレスであり、国内外の様々な事業者によるサービスが提供されている。

(4)　標的型メールに添付されたファイルの傾向

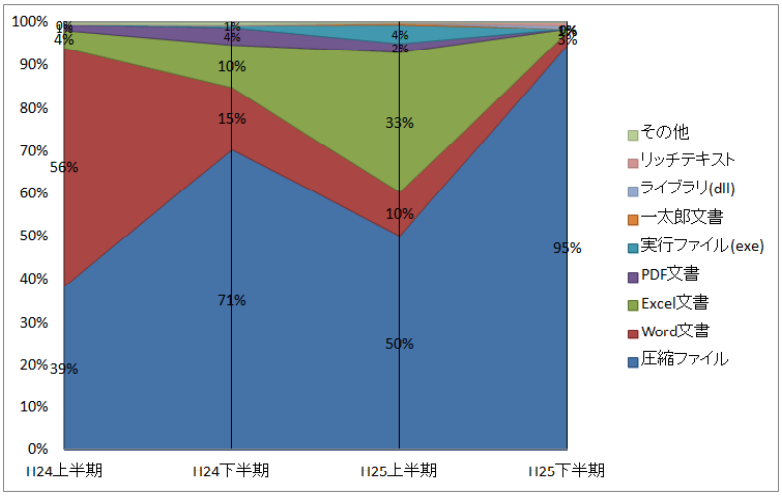
ア　圧縮ファイル形式が多数

標的型メール攻撃で添付されたファイルの形式の傾向を見ると、不正プログラムを含む文書ファイル等を直接メールに添付する手口が減少する一方で、圧縮ファイルを添付する手口の増加がみられた。25年中、標的型メールで添付されたファイル（453個）の形式は、圧縮ファイル形式の一種であるZIP形式が最も多く、全体の約６割（266個）を占めた。その他の圧縮形式（LZH、RAR及び7-zip）を合わせると、圧縮ファイルが添付されたものは、全体の約８割（346個）であった。また、これらの圧縮ファイルを展開（解凍）して生成されるファイルの約９割（349個中306個）が、実行ファイル形式の不正プログラムであった。

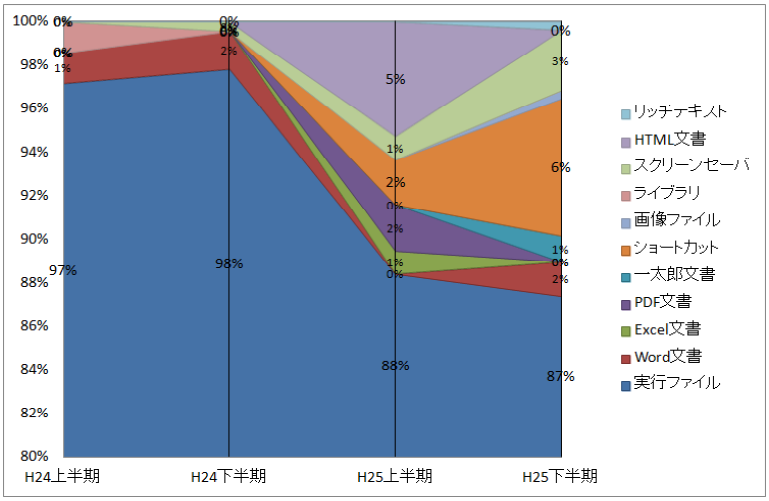
実行ファイルを添付したメールの送信が制限されているフリーメールサービスが存在することや、実行ファイルが添付されたメールの受信を拒否するメールサーバが存在することから、このような制限を回避するため、ファイルの圧縮を施したものとみられる。



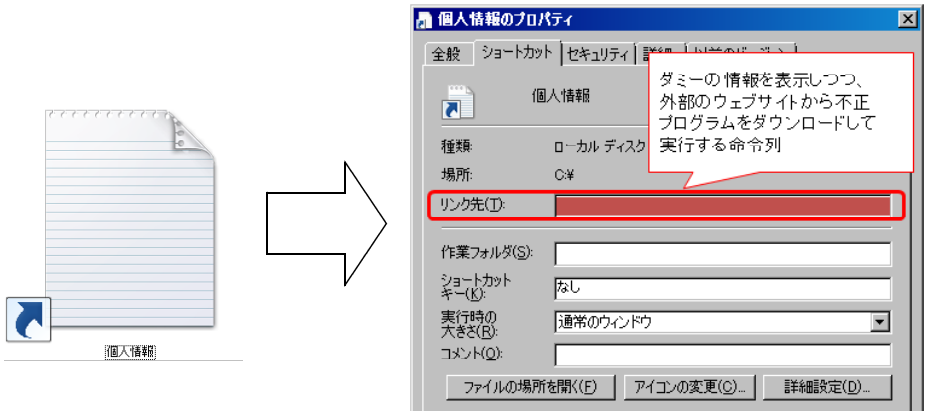
【標的型メールに添付されたファイルの形式】



【標的型メールに添付されたファイル形式の傾向】



【圧縮ファイルに格納されたファイル形式の傾向】
（縦軸の80%から100%の間を拡大したもの）

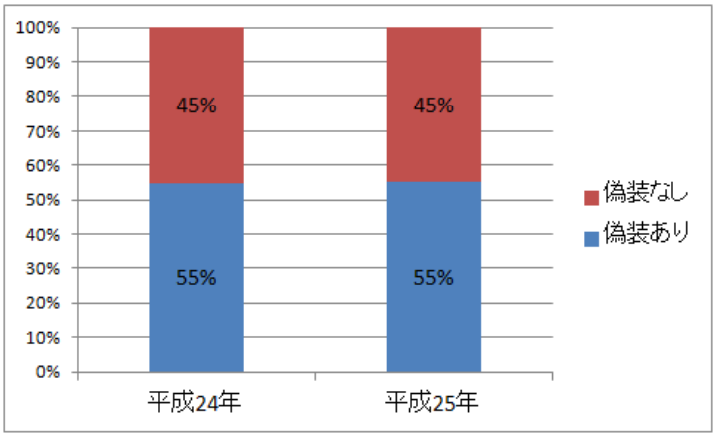


【ショートカット（LNK）ファイルの仕組みを利用する
不正プログラムの例】

また、圧縮ファイルに格納されたファイル形式の傾向を見ると、ショートカット（LNK）ファイルを利用したものが新たに確認されたほか、Word文書、Excel文書、PDF文書、画像（JPEG）ファイル、HTML文書等実行ファイル形式以外の多種多様な形式の増加が確認された。

イ　実行ファイルの約６割において見た目を偽装

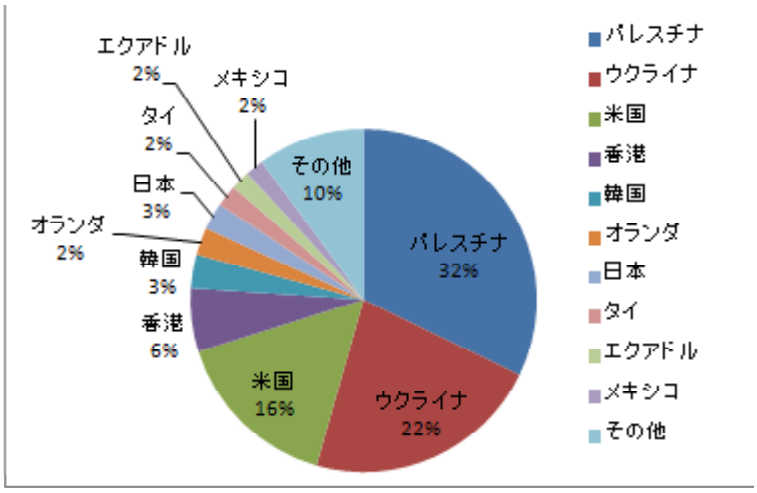
実行ファイルは、アイコンを変更することで、コンピュータ画面上での見た目を変化させることが可能であり、一般的なファイル形式のアイコンを使い、不正プログラムではないように偽装する手口が多数確認された。25年中は、標的型メールに添付された実行ファイル（圧縮ファイルに格納されていたものを含む。）の約６割（314個中174個）が、Word文書ファイル、PDF文書ファイル、画像（JPEG）ファイル等に偽装されていた。



【見た目を偽装する実行ファイルの割合】

ウ　不正な外部接続先の大半は外国

標的型メール攻撃に使用された不正プログラムによる通信の接続先[*4]は、パレスチナが32%、ウクライナが22%、米国が16%、香港が６％と、その大半が外国であった。



【標的型メール攻撃に使用された不正プログラムの接続先】

エ　解析を困難化する不正プログラムを確認

プログラムのサイズ縮小や暗号化を行うパッカー（packer）と呼ばれるプログラムを組み合わせ、何重にも暗号化をかけた不正プログラムを確認した。これは、ウイルス対策ソフトウェアによる検知の回避や、不正プログラムの動作解析を困難にすることを企図したものとみられる。

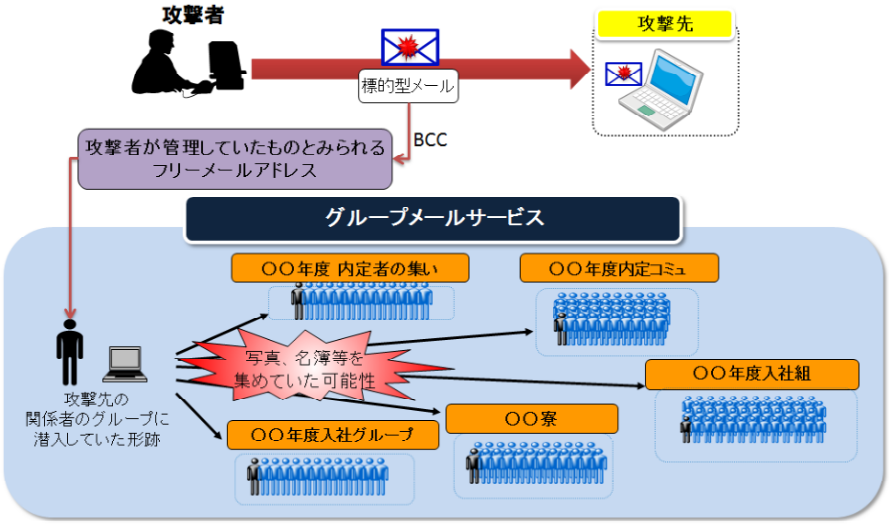
*4　接続先国については警察において不正プログラムを調査した時点のものである。

3　標的型メール攻撃の事例

(1)　周到な準備に基づく計画的な攻撃

標的型メール攻撃の攻撃者が管理していたものとみられるフリーメールアドレスについて調査したところ、特定の事業者等の同期職員や寮入居者の間で情報共有に利用されている、複数のグループメールサービス[*5]に潜入していたことが判明した。攻撃者が潜入していたグループの中には、同期職員の顔写真付き名簿ファイルが共有されているものもあり、攻撃者も閲覧可能な状態であった。

攻撃者は、事前にこのようなサービスを利用して当該事業者等の名簿やメールアドレス等の情報を入手し、周到に準備した上で計画的に標的型メール攻撃を行っていたとみられる。



【グループメールサービスを通じた情報収集活動】

(2)　東京オリンピック・パラリンピック大会のボランティア募集に関する情報提供を装った攻撃

25年９月、2020年にオリンピック・パラリンピック大会が東京で開催されることが決定した後、同大会のボランティア募集に関する情報提供を装った標的型メールが送付されたことを確認した。当該メールには、外部のウェブサイトへのリンクが記載されていた。

(3)　スマートフォンへの不正プログラムの感染を狙う攻撃

Android OSを搭載したスマートフォンへの不正プログラムの感染を狙った標的型メール攻撃を確認した。これは、Androidの緊急のセキュリティアップデートに関する情報提供を装ったものであり、メールの受信者に対し、メー

---

*5　参加者に対してメールや掲示板による連絡を一斉に行ったり、文書ファイルを共有したりすることができる情報共有サービスである。

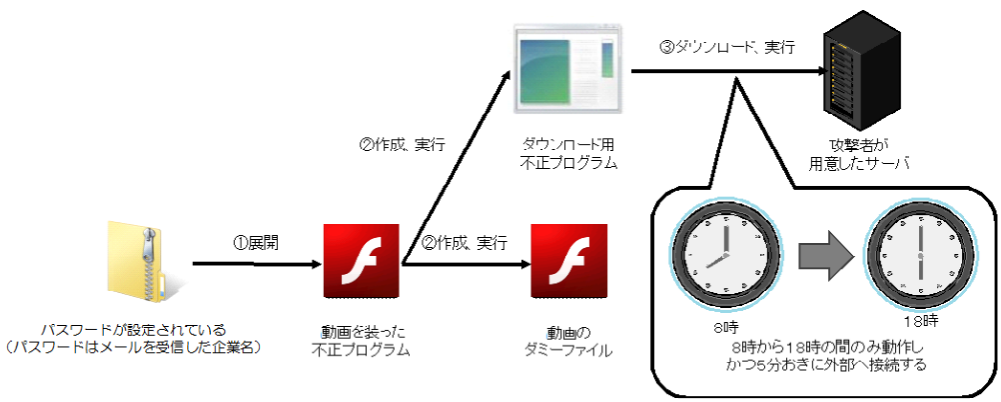
ル本文中に貼り付けられたQRコード（２次元バーコード）をスマートフォンのカメラで読み取り、海外のウェブサーバに蔵置されたAPKファイル（Android向けソフトウェアのファイル形式）をダウンロードさせようと仕向けるものであった。一般的なAndroid搭載スマートフォンは、開発元企業や携帯電話会社の公式サイトに限り、ソフトウェアをダウンロードして導入することができるよう制限がかかっているが、同メール本文中には、この制限を外すための手順を解説した図も添付されていた。

ダウンロードされるAPKファイルを実行すると、感染した端末のOSのバージョン、Android_IDと呼ばれる端末固有の値、電話番号等を外部に送信する動作が確認されており、情報流出や遠隔操作の危険性があった。

(4)　年末年始の挨拶を装った攻撃

年末年始の挨拶を装った標的型メール攻撃を確認した。メールの文面からは、不審なメールであるかどうかを判断することが困難なものであった。

添付されていた不正プログラムは、攻撃先の組織名をパスワードとして入力すると展開（解凍）できるよう圧縮されていた。不正プログラムを実行すると、ダミーの動画が再生されるとともに、外部ネットワークへの通信が行われ、新たに別の不正プログラムをダウンロードして実行する仕組みとなっていた。この不正プログラムは、８時から18時までの間に限り動作し、かつ、外部ネットワークへの通信を５分おきに限り行う仕組みとなっていた。これは、不正プログラムが行う通信を日中の業務時間帯の通信に紛れ込ませることで、不正な通信の発覚を困難にするためのものとみられる。



【不正な外部接続を正当な通信に紛れ込ませようとする不正プログラムの例】

４　新たな攻撃の手口

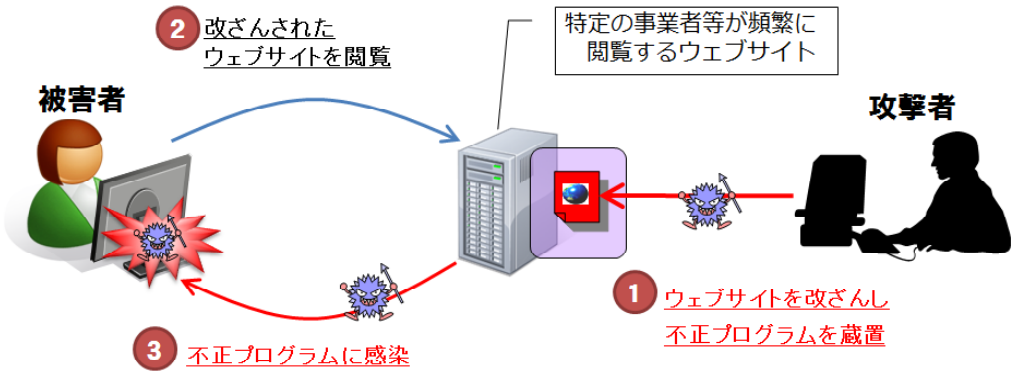
情報窃取を企図したサイバー攻撃については、従来その大半が標的型メール攻撃によるものであったが、25年には、「水飲み場型攻撃」と呼ばれる新たな手口によるものを国内で初めて確認した。

「水飲み場型攻撃」は、攻撃先の職員が頻繁に閲覧するウェブサイトを改ざ

んし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる手口である。ウェブサイトを改ざんし、当該サイトを閲覧した不特定多数のコンピュータを不正プログラムに感染させる攻撃手法は、「ドライブ・バイ・ダウンロード攻撃」と総称されており、「水飲み場型攻撃」は「ドライブ・バイ・ダウンロード攻撃」の一類型に分類されるが、「水飲み場型攻撃」では、改ざんするサイトを巧妙に選定することで、標的を絞り込んでいることが特徴となっている。

国内で確認した「水飲み場型攻撃」では、改ざんされたウェブサイトを特定のIPアドレスから閲覧した場合にのみ、不正プログラムに感染させる仕組みとなっており、標的を絞ることで発覚を免れようとする巧妙な手口であった。

26年に入ってからも、広く利用されている無償ソフトウェアの更新を悪用して不正プログラムに感染させる手口の発生を確認しており、サイバー攻撃の手口は巧妙化・多様化している。



【水飲み場型攻撃の例】