

情報技術解析平成 22 年報

～平成 22 年中のインターネット観測結果等～

平成 23 年3月

警察庁情報通信局情報技術解析課

目次

1	はじめに.....	3
2	概説.....	4
3	DoS 攻撃.....	5
3.1	DoS 攻撃とは.....	5
3.2	DoS 攻撃被害観測システム.....	6
3.3	跳ね返りパケットの検知事例.....	7
3.4	対策.....	9
3.5	まとめ.....	9
4	不正プログラム Stuxnet の脅威.....	10
4.1	Stuxnet の特徴.....	10
4.2	対策.....	12
4.3	まとめ.....	12
5	SIP サーバへの不正接続.....	13
5.1	概要.....	13
5.2	5060/UDP の検知状況.....	14
5.3	SIP サーバの調査ツール.....	14
5.4	まとめ.....	15
6	標的型メール攻撃.....	16
6.1	標的型メール攻撃の概要.....	16
6.2	標的型メール攻撃の傾向.....	17
6.3	標的型メール攻撃の悪質性と関連技術.....	18
6.4	対策.....	19
6.5	まとめ.....	19
7	情報セキュリティの向上のために.....	20

平成 22 年中のインターネット観測結果等について

1 はじめに

警察庁では、国民生活や社会経済の活動に重大な影響を及ぼすおそれのある、情報システムに対する犯罪を、未然に防止するとともに、発生時の被害の拡大を防止するために必要となる情報を収集する手段の一つとして、インターネット定点観測システム(以下「定点観測システム」という。)を活用し、全国のインターネット接続点におけるアクセス情報等を観測・分析しています。

本資料は、サーバの管理者を始め、インターネット利用者のセキュリティ対策の参考としていただくため、インターネットを利用していく上で発生するリスクについて、警察庁が定点観測システムでの観測・分析した情報を含め、様々な方面から収集した情報を取りまとめて公表するものです。

本資料が、安全・安心なインターネット社会への取組みの一助となれば幸いです。

2 概説

平成 22 年中においては、日本の政府機関等に対するサイバー攻撃予告がなされ、これらのウェブサイトへのアクセスが集中する事案が発生したほか、IP 電話で利用される SIP サーバの探索とみられるアクセスの急増もみられました。また、海外では、イランの核施設で制御システムが一時停止する事案が発生しましたが、その原因は Stuxnet (スタックスネット)と呼ばれる不正プログラムを利用したサイバー攻撃によるものと報道されています。標的型メール攻撃では、添付されている不正プログラムの種類として、実行ファイルや PDF ファイルが多くみられました。

サイバー攻撃の手段としてよく用いられる DoS 攻撃は、サーバやネットワーク機器に対して、大量の通信や不正な通信を行い、サービスの提供を妨げる攻撃です。警察庁では、DoS 攻撃のうち、大量の通信を行う攻撃で発生する「跳ね返りパケット」を観測しています。22 年中は、日本政府機関や海外のウェブサイトから跳ね返りパケットを観測しました。

Stuxnet は、特定の制御システムを攻撃対象とした不正プログラムの一つです。国際原子力機関 (IAEA) は、22 年 11 月にイランの核施設で制御システムが一時停止したと発表しました。この原因は、Stuxnet を利用したサイバー攻撃である可能性が高いとの報道がなされました。この事例により、制御システムを利用している基幹システムに対しても、不正プログラムを用いた攻撃が可能という見方が強まり、サイバーテロの脅威が増大しました。

22 年 7 月、定点観測システムにより、インターネット上にある SIP サーバの探索とみられるアクセスの急激な増加を検知しています。インターネット上の SIP サーバに対し、不正に接続を試みているものと考えられます。SIP サーバが不正に利用された場合、通話料等の金銭的損害に直結する可能性があります。また、悪意のある発信者の身元を隠すために利用される危険性も考えられます。

標的型メール攻撃は、特定の組織や個人に標的を絞り、不正なプログラムを添付するなどした電子メールを送信する手法です。標的型メール攻撃では、受信者にメールや添付ファイルを開かせるために、職場の関係者等になりすますなど巧妙な手口が使われます。メールに添付される不正なプログラムは、ウイルス対策ソフトで検知できない最新のものである事例もみられ、メールの受信者が不正なプログラムに気付かなかった場合、その後の対応が遅れるなどして被害が一層大きくなる可能性があります。

サイバー攻撃の手法は日々変化しています。インターネットを利用される皆様、企業等の情報セキュリティ管理者等の皆様が、インターネット上の脅威や、その対策等について関心を持ち、状況に応じて可能な限り適切な措置を行っていただくことが大切です。

3 DoS 攻撃

平成 21 年7月に米国及び韓国の政府機関等のウェブサイトがサイバー攻撃を受けて、一時閲覧不能になるという事態が発生したことは、まだ記憶に新しいところです。

22 年9月には、日本の政府機関等に対するサイバー攻撃予告がなされ、これらのウェブサイトへのアクセスが集中し、一部のウェブサイトが一時的に閲覧しにくい状況となりました。また、海外では、内部告発サイト「WikiLeaks」(ウィキリークス)をめぐる、WikiLeaks を支持するグループと支持しないグループとの間で、サイバー攻撃の応酬が行われたと報道されています。

ここでは、サイバー攻撃の手段としてよく用いられる DoS 攻撃(Denial of Service Attack、サービス不能攻撃)について、DoS 攻撃被害観測システムでの観測結果とともに、22 年中に見られた DoS 攻撃の事例と、DoS 攻撃の対策について紹介します。

3.1 DoS 攻撃とは

DoS 攻撃は、サーバやネットワーク機器に対して、大量の通信や不正な通信を行い、サービスの提供を妨げる攻撃です。このうち、大量の通信を行う攻撃には、次のような形態があります。

- 単一のコンピュータから直接攻撃(図3-1)
- 複数のコンピュータから直接攻撃(図3-2)
- ボットネットを使用した攻撃(図3-3)
- 中継サーバを経由した攻撃(図3-4)

複数のコンピュータから大量の通信を行う攻撃は、特に「DDoS 攻撃」(Distributed Denial of Service Attack、分散型サービス不能攻撃)と呼ばれます。DDoS 攻撃は、攻撃元コンピュータの数に比例して、攻撃の規模が大きくなります。

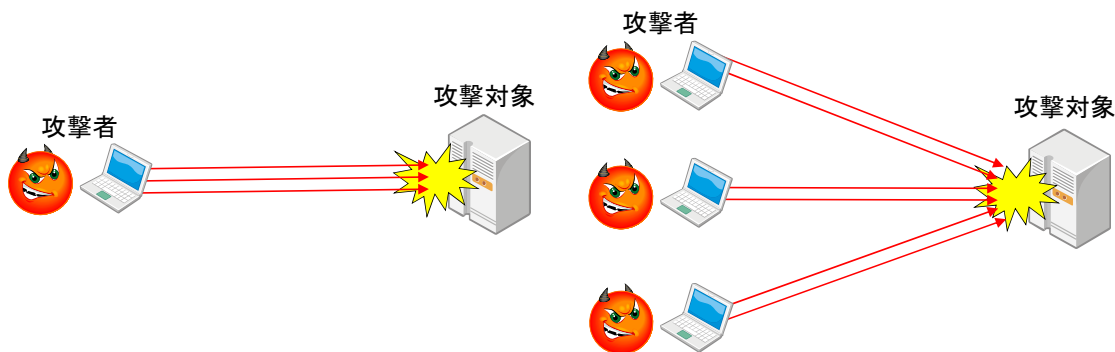


図3-1 単一のコンピュータから直接攻撃 図3-2 複数のコンピュータから直接攻撃

また、ボットネットを使用した攻撃や中継サーバを経由した攻撃では、攻撃者から直接、攻撃が行われないため、攻撃者の特定が困難となります。

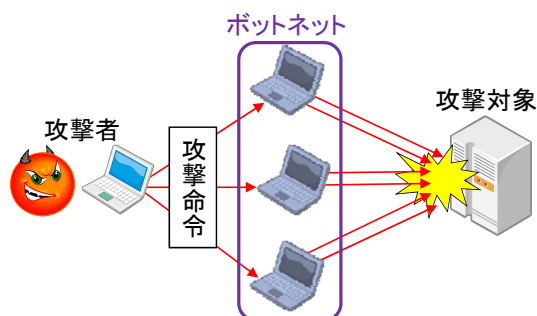


図3-3 ボットネットを使用した攻撃

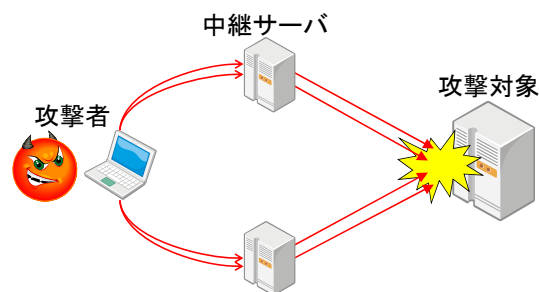


図3-4 中継サーバを経由した攻撃

3.2 DoS 攻撃被害観測システム

警察庁では、全国の警察に設置したセンサー(以下「センサー」という。)を利用したDoS 攻撃被害観測システムにより、DoS 攻撃の状況について観測を行っています。

DoS 攻撃の一種である SYN flood 等の攻撃では、標的となるサーバ(被害サーバ)の機能を停止させるため、大量の packets を送信します。この際、攻撃者の判別を困難にするために、不特定多数の IP アドレスが発信元であるように詐称することが多く、被害サーバはこの詐称された IP アドレスに対し、応答パケットを返信します。この応答パケットを「跳ね返りパケット」と呼んでいます。

IP アドレスの詐称は、無作為かつ大量に行われるため、詐称された IP アドレスがセンサーの IP アドレスと一致する場合があります。この場合、被害サーバは、センサーが通信の発信元であると誤認し、センサーに応答パケットを送信します。このようにして、センサーで検知する跳ね返りパケットを調べることで、被害サーバの IP アドレス及び被害サービスを知ることができます。

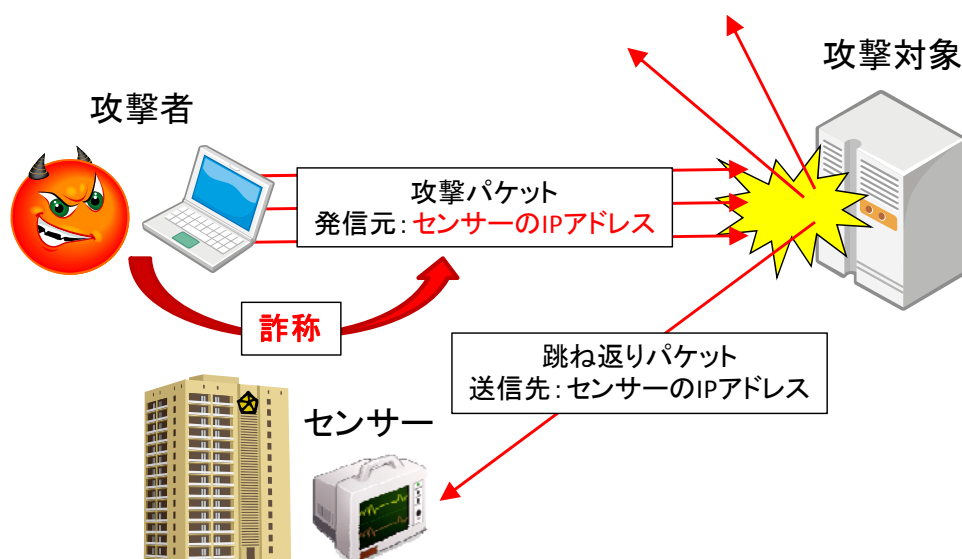


図3-5 DoS 攻撃被害観測システム

3.3 跳ね返りパケットの検知事例

3.3.1 平成 22 年 9 月 日本政府機関

平成22年9月、日本の政府機関等に対するサイバー攻撃予告がなされました。この予告との関連は確認できていませんが、予告日である9月18日前後に、警察庁を含む複数の日本政府機関等のウェブサイトへのアクセスが集中する事案が発生しました。

DoS 攻撃被害観測システムにおいても、日本政府機関のウェブサイトから、跳ね返りパケットを複数回にわたり検知しています(図3-6)。これは、日本政府機関のウェブサイトに対してDoS 攻撃の一種であるSYN flood^(注1) 攻撃が行われた可能性を示しています。

また、サイバー攻撃予告に合わせて、インターネット上の掲示板やチャットを通じて複数の DoS 攻撃ツールが配布されました。警察庁において、これらの攻撃ツールの動作を確認したところ、SYN flood 攻撃のほか、Connection flood 攻撃^(注2) や UDP flood 攻撃^(注3) が可能であることを確認しました。配布されたこれらのツールを利用することにより、容易にサイバー攻撃を行うことが可能な状態にありました。

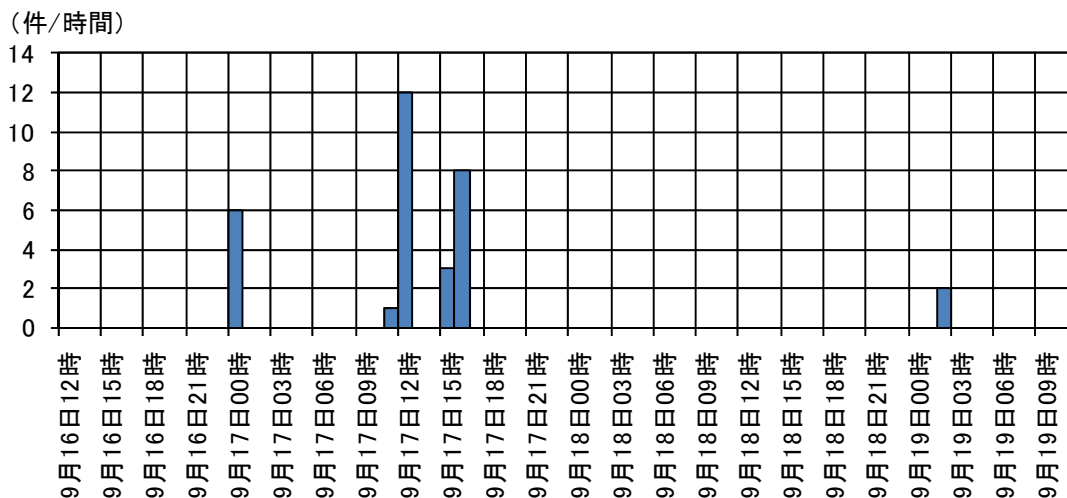


図3-6 日本政府機関からの跳ね返りパケット検知状況

注1: 攻撃対象のサーバへ通信の開始要求(SYN パケット)を大量に送り、サーバから送り返される SYN/ACK パケットには応答しないことで、サーバに ACK パケット待ちを大量に発生させ、新たな要求の受け付けを不可能にさせる攻撃

注2: 攻撃対象のサーバに長い時間オープン状態を続ける通信の接続を繰り返すことで、通信接続を占拠し、新たな接続の受け付けを不可能にさせる攻撃

注3: 攻撃対象のサーバにサイズの大きな UDP パケットを大量に送り付け、サーバやネットワーク機器に負荷をかけ、新たな要求の受け付けを不可能にさせる攻撃

3.3.2 平成 22 年 12 月 内部告発サイト「WikiLeaks」

平成 22 年 12 月上旬、内部告発サイト「WikiLeaks」(ウィキリークス)をめぐり、WikiLeaks の支持グループと支持しないグループとの間で、相互に DoS 攻撃が行われたとの報道がされています。

DoS 攻撃被害観測システムでは、WikiLeaks のウェブサイトと WikiLeaks との取引を停止したと言われる一般企業のウェブサイト(図3-7の取引停止サイト A、B)の双方から、跳ね返りパケットを検知しました(図3-7)。

多くの跳ね返りパケットに係る宛先ポート(攻撃パケットの発信元ポートと同一。)が 1024/TCP 又は 3072/TCP であるという特徴がありました。これは、21 年 10 月期報で取り上げた攻撃ツールと同一のものが使用された可能性が考えられます^(注)。また、これらの宛先ポート以外のポートを宛先とする跳ね返りパケットも見られることから、複数の攻撃手法が使われたと考えられます(図3-8)。

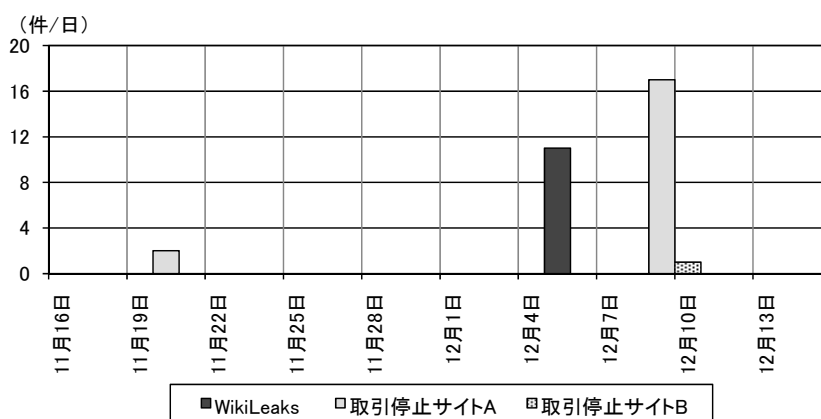


図3-7 WikiLeaks 関連サイトからの跳ね返りパケット検知状況(サイト別)

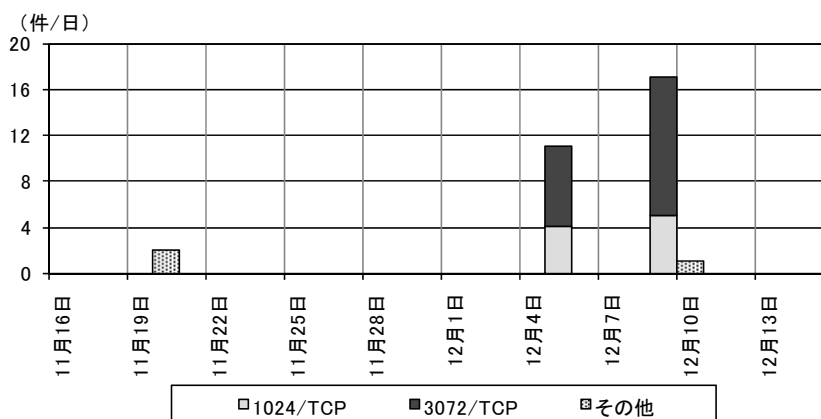


図3-8 WikiLeaks 関連サイトからの跳ね返りパケット検知状況(宛先ポート別)

注：「我が国におけるインターネット治安情勢(平成 21 年 10 月期)」(@police) pp.2-7 「2 分析 - 1024/TCP と 3072/TCP を使用する SYN flood 攻撃」, <http://www.cyberpolice.go.jp/detect/pdf/20091214.pdf>

3.4 対策

DoS 攻撃に対しては、サイト運営者及び一般利用者それぞれに行うべき対策があります。

サイト運営者には、DoS 攻撃を受けた場合に備えて、攻撃を想定したシステムの構築、平素からの稼働状況の把握及び攻撃を受けた際の対策の検討が求められます。

実際に DoS 攻撃を受けた際は、攻撃のためのアクセスを自ら設置したネットワーク機器により、又はプロバイダを介して遮断することが、有効な対策となります。通常時のアクセス状況と比較して、単一のコンピュータからの極めて頻繁なアクセス、中継サーバを経由したとみられるアクセス等が攻撃のためのアクセスである可能性があります。

また、各種のログ等の確認と分析を行うことで、より有効な対策を打つ手助けとなります。

一般利用者は、自身が利用するパソコンがボット等の不正プログラムに感染することで、知らない間に DoS 攻撃に参加させられる可能性があります。そのため、ウイルス対策ソフトの導入や使用している OS やアプリケーションの更新プログラムの適用等のセキュリティ対策を行う必要があります。

また、サイバー攻撃の呼び掛けがなされることもありますが、犯罪行為に該当する場合もあり、事件に巻き込まれるおそれもありますので、参加してはなりません。

3.5 まとめ

平成 21 年7月の米国及び韓国の政府機関等のウェブサイトに対するサイバー攻撃の観測に加え、22 年9月には、日本政府機関や海外のウェブサイトへの DoS 攻撃の可能性を示す跳ね返りパケットを観測しました。また、日常的に世界各地から多くの跳ね返りパケットを観測しており、DoS 攻撃が頻繁に行われていることがうかがえます。

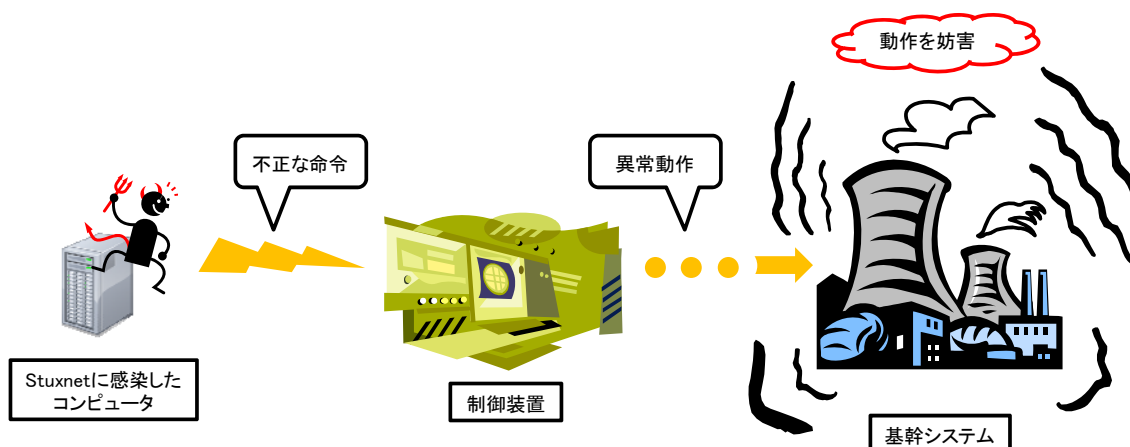
今後も DoS 攻撃は行われるものと考えられ、社会的に大きな被害が発生する可能性も否定できないことから、サイト運営者及び一般利用者それぞれにおいて、対策を行うことが重要です。

4 不正プログラム Stuxnet の脅威

Stuxnet (スタックスネット) は不正プログラムの一つであり、特定の制御システムを標的とするものです。Stuxnet の出現は、制御システムが攻撃されるという、これまでにない極めて深刻な脅威として世界の注目を集めています。

平成 22 年 11 月、国際原子力機関 (IAEA) は、イランの核施設で使用されていた遠心分離機が一時的に停止したと発表しました。その後、同国が、核濃縮のために使用されている遠心分離機の動作が不正プログラムにより妨害されたことを明らかにしたことから、核施設における遠心分離機の停止は、これを制御するシステムへの Stuxnet によるサイバー攻撃である可能性が高いとの報道がなされています。

この例にみられるように、制御システムを利用している基幹システムに対する、不正プログラムを用いたサイバー攻撃の実現の可能性が高まっており、サイバーテロの脅威が増大しました。



4.1 Stuxnet の特徴

4.1.1 高度な不正プログラム

Stuxnet は、5種類の Windows の脆弱性を悪用して感染する特徴を持っていますが、Stuxnet がウイルス対策ソフトで検知され始めた平成 22 年7月の時点では、4種類の脆弱性について修正プログラムが未公開でした。

Stuxnet においては、感染時に Windows が警告を出さないように、海外に実在する企業のデジタル署名が使用されていました。また、自動的に外部のコンピュータと情報交換を行って Stuxnet 自体を更新する機能も持っていました。

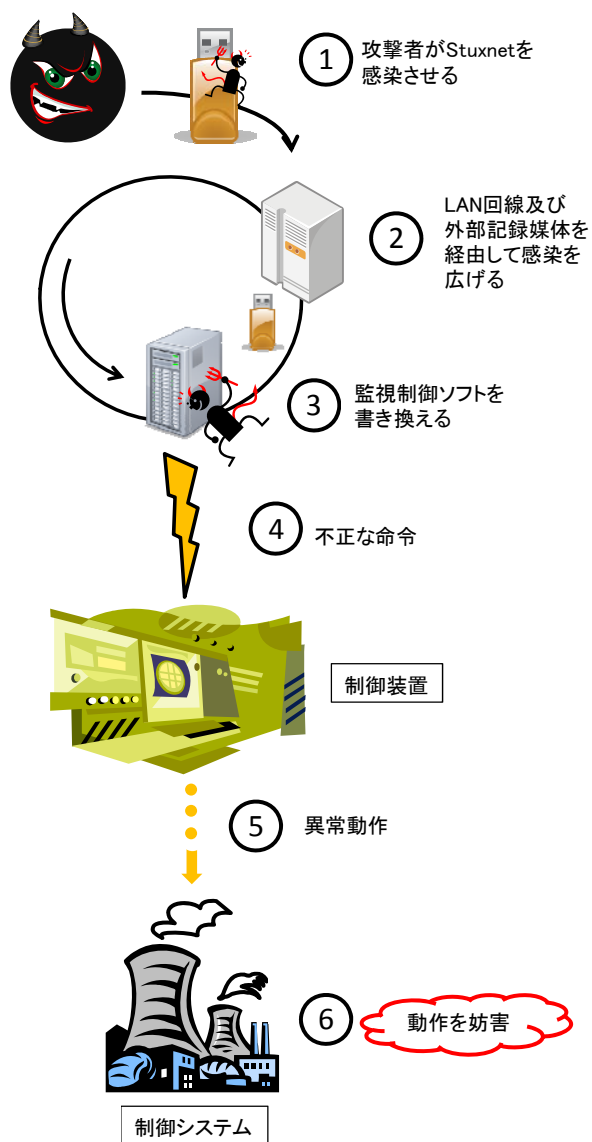
この他にも、コンピュータに侵入後すぐに感染活動を開始しないことや、複数のファイルが存在する外部記録媒体にしか感染しないなど、Stuxnet 自体の発見を妨害する機能を持っていることも確認しています。

Stuxnet は、これらの複数の技術を組み合わせ合わせた非常に高度な機能を備えた不正プログラムであるといえます。

4.1.2 攻撃対象

Stuxnet が標的としたのは、Windows で動作するドイツのシーメンス社製の監視制御ソフトである「SIMATIC STEP7」又は「SIMATIC WinCC」が導入されたシステムでした。この監視制御ソフトは、制御システムの監視及び制御を行うために使用されるものです。

このため、Stuxnet は、コンピュータだけでなく制御システムに関する専門知識を有する者によって、特定の制御システムを攻撃するためだけに作成された不正プログラムである可能性があります。



4.1.3 動作概要

Stuxnet は、外部記録媒体を経由してコンピュータに感染し、ネットワークを経由して次々と感染を広げます。そして、感染したコンピュータのシーメンス社製の監視制御ソフトを、制御装置に不正な命令を与えるように書き換えてしまいます。最終的には、不正な命令を与えられた制御装置によって、制御システムの正しい動作が妨害されてしまいます。

4.2 対策

Stuxnet は、特定の制御システムを攻撃するために作成された不正プログラムですが、他のコンピュータに対しても感染活動を行うことを確認しています。日本語版の Windows コンピュータに対しても感染することを確認していますので、注意が必要です。

また、今後 Stuxnet を応用した新種や亜種の不正プログラムが作成された場合、攻撃対象が他の制御システムを利用している基幹システム等にも広がる可能性があります。企業や一般利用者もしっかりと感染防止対策を行うことが重要です。

このような制御システムを攻撃する不正プログラムの感染を防止するためには、OS やアプリケーションの修正プログラムを適用する、ウイルス対策ソフトを常に最新の状態に更新するといった基本的な対策を行うことが有効と考えられます。

しかし、新種や亜種の不正プログラムが登場した時点では、修正プログラムは存在せず、ウイルス対策ソフトによる対応も間に合わない可能性があります。したがって、インターネットからの侵入や標的型メール攻撃等による不正プログラムの感染に注意するほか、隔離されたネットワークに対しても USB メモリ等による感染を防止するため、日頃から外部記録媒体の管理を行うなどのセキュリティ対策を講じることが必要です。

特に重要な基幹システムを運用している企業では、未知の不正プログラムが実行されてしまった場合を想定して、不正プログラムの動作状況を検証できるログの採取を行い、定期的なログの確認による、異常の早期発見のための措置を講じることをお勧めします。

上記の措置を講じることが困難な環境にあっても、他の対策方法が提供されている場合がありますので、システムベンダーやウイルス対策ベンダー等のセキュリティ情報に関心を持ち、感染防止対策に関する新たな情報を得た際には、速やかに対応することが大切です。

4.3 まとめ

Stuxnet は、高度な技術と攻撃対象に関する詳細な調査結果を反映させることによって、特定の制御システムに対する攻撃を可能にする不正プログラムです。

制御システムへのサイバー攻撃は、コンピュータ関連技術のみならず、制御システムに関する専門知識が必要なことから、これまで難しいと考えられていました。Stuxnet は、外部ネットワークに接続されていない制御システムでも USB メモリ等の外部記録媒体を経由して感染します。これは、制御システムを利用している基幹システムにも攻撃が可能であることを示しています。

皆様の管理するコンピュータが、サイバーテロに利用されないことがないよう、日頃からのセキュリティ対策をお願いします。また、基幹システムへの攻撃を把握した場合は、警察へのご連絡もお願いします。

5 SIP サーバへの不正接続

5.1 概要

定点観測システムでは、平成 22 年 7 月に、5060/UDP に対するアクセスの急激な増加を検知しています^(注1)。5060/UDP は、IP 電話機等の VoIP/SIP 機器の通信プロトコルである SIP(Session Initiation Protocol)で利用されており、このアクセスは、インターネット上にある SIP サーバの探索を目的としたものと思われます。

悪意のある何者かが、SIP サーバに接続し、海外等の通話先に発信しようとして試みている可能性があります。22 年 11 月には、IP 電話が不正に利用され、架電した覚えがないのに国際電話料金が請求されたという事例について、通信事業者等から注意喚起が発表されております^(注2)(図5-1)。

SIPサーバにインターネット経由での接続を許可する場合は、ID、パスワードの設定を適切に行い、不要な発信元からのサーバへの接続を遮断するなどの対策を行うことをお勧めします。

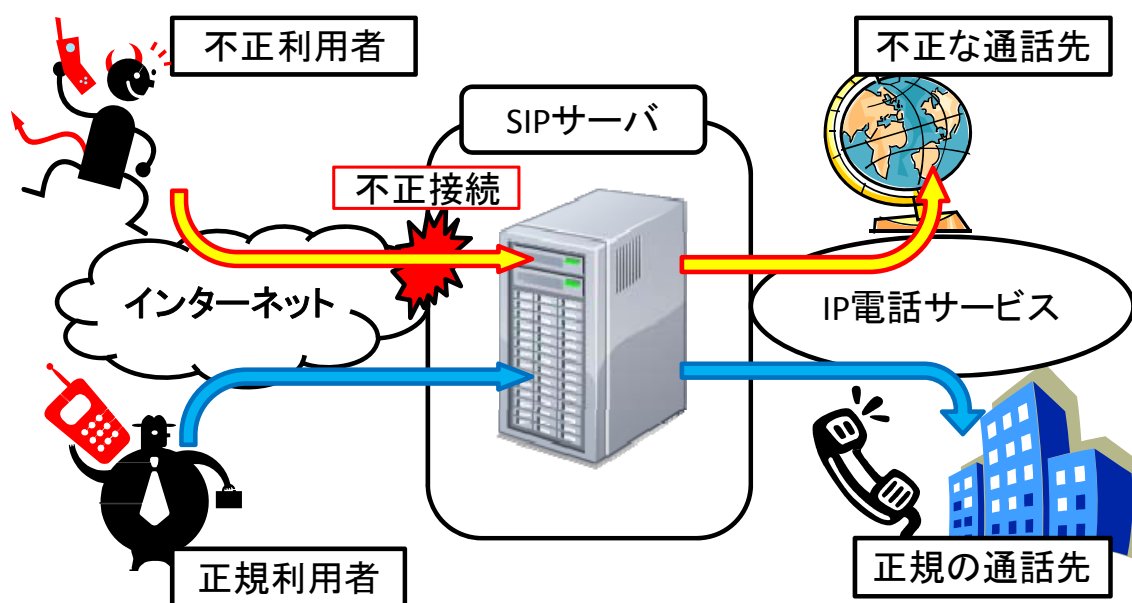


図5-1 SIP サーバの不正利用について

注1: 「5060/UDP に対するアクセスの増加について」(@police),
<http://www.cyberpolice.go.jp/detect/pdf/20100714.pdf>

注2: 「かけた覚えのない国際通話にご注意ください」(東日本電信電話株式会社),
<http://www.ntt-east.co.jp/release/1011/pdf/101124a.pdf>

5.2 5060/UDP の検知状況

平成 22 年 7 月 9 日に、5060/UDP に対する急激なアクセスの増加を検知しました(図5-2)。全体の 59.5%が中国からのアクセスですが、急増が見られたのは中国だけではなく、それ以外の国からのアクセスについても同時に増加しています。これは、一斉に指令を受けて動作するボットによるアクセスである可能性が考えられます。

今回のアクセスで使用されていると考えられるツールは、スクリプト言語で作成されており、いずれの国のアクセスも日周変化が見られないことから、24時間稼働しているサーバで構成されたボットネットが使用されている可能性が考えられます。

アクセス数は減少傾向にあります。7月9日の急激な増加以外にも、9月4日及び10月6日に、短期間の急激なアクセスの増加が見られます。また、日々新しい発信元からのアクセスも検知しており、脅威は継続していると考えられます。

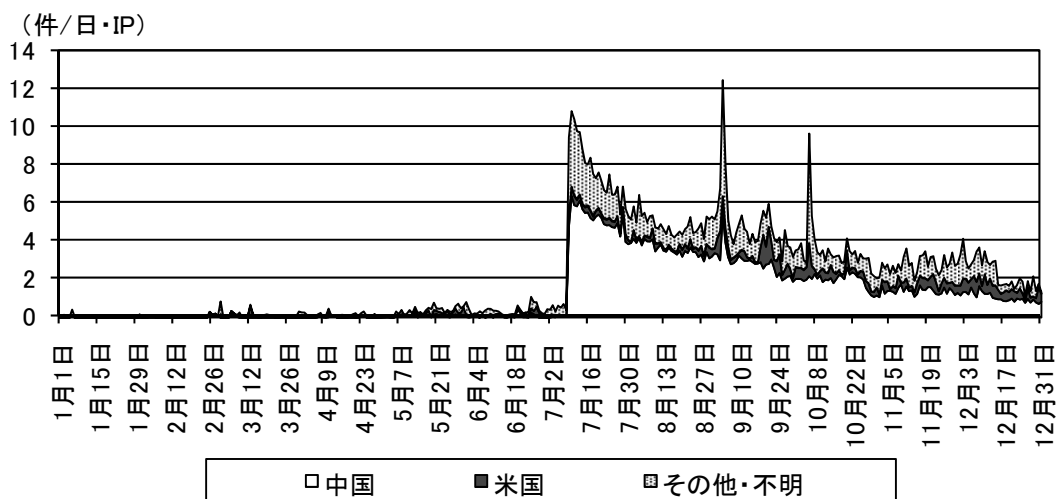


図5-2 5060/UDP に対するアクセスの検知件数の推移

5.3 SIP サーバの調査ツール

今回検知した 5060/UDP のアクセスは、すべて SIP の通信によるものであり、通信内容の特徴から、複数のグループに分類できます。この中の一つは、インターネット上で配布されている、SIP サーバを調査するツールと特徴が一致しています(表5-1)。

表5-1 SIP サーバ調査ツールの機能

- 指定した範囲内の IP アドレスに対する、SIP サーバの有無の調査
- 対象の SIP サーバに対し、指定した範囲のユーザ名の有効/無効の調査
- 対象の SIP サーバ、ユーザ名に対し、パスワードの総当たり攻撃及び辞書攻撃によるパスワードの調査

他の特徴を持つグループからのアクセスについても、このツールが改造されたものや、異なる別のツールが存在し、使用されている可能性があります。

5.4 まとめ

今回の 5060/UDP に対する大量のアクセスは、インターネットに接続された SIP サーバに対する不正な接続を試みているものと思われます。SIP サーバが不正に利用された場合、通話料等の金銭的損害に直結する可能性があり、また、悪意のある発信者の身元を隠すために利用される危険性も考えられます。

対策として、外部からの不正な接続を防ぐため、

- 必要が無い場合は、サーバをインターネットに公開しない
- 正規の接続元以外からの通信を遮断する
- ユーザ名、パスワードを適切に設定する

などが考えられます。

また、万が一、外部から不正に接続された場合、安易に外部へ発信できないよう、

- 外線発信できる内線番号を制限する
- 必要が無い場合は、国際電話の利用を停止する

などの防御策も有効です。

SIP サーバへの脅威は依然として継続しています。探索行為は引き続き行われているほか、探索により発見された SIP サーバに対し、今後更なる攻撃が行われる可能性もあります。SIP サーバをインターネットに接続している場合には、サーバのセキュリティの設定を見直すとともに、ログの確認や外線通話を適切に設定するなど、引き続き注意が必要です。

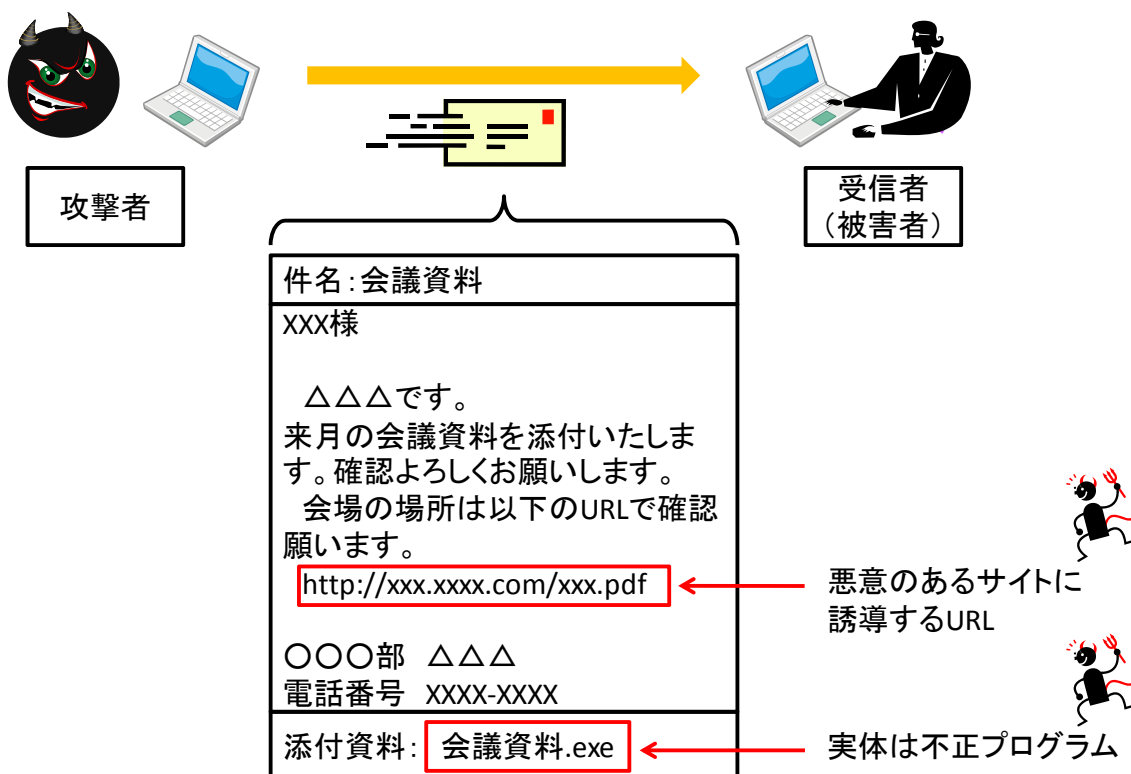
6 標的型メール攻撃

6.1 標的型メール攻撃の概要

標的型メール攻撃とは、特定の組織や個人に標的を絞って、電子メールを送信する手法による攻撃であり、メールに不正なプログラムが添付されていたり、不正プログラムを感染させるような悪意のあるサイトへ誘導するリンクが記載されていたりします。スパイ(槍)のように、標的を絞って攻撃することから、「スパイメール攻撃」とも呼ばれています。

標的型メール攻撃の主な目的は、政府関係者や企業関係者のコンピュータに不正プログラムを感染させて、政府機関や企業の機密情報、個人情報等を盗み出すことであると考えられます。

標的型メール攻撃は、受信者にメールや添付ファイルを開かせるため、職場の関係者等になりすますなど巧妙な手口が使われています。メールに添付される不正なプログラムは、ウイルス対策ソフトで検知できない最新のものである事例もみられ、メールの受信者が不正なプログラムに気付かなかった場合、攻撃の存在そのものが表面化しないため、その後の対応が遅れるなどして被害が一層大きくなる可能性があります。



6.2 標的型メール攻撃の傾向

6.2.1 標的型メール攻撃の内容

標的型メール攻撃は、受信者が関心を示すような政治的なニュースや国際的なニュース等がタイトルに用いられることがあるとともに、メールの本文に「添付ファイルを確認してください」のように、受信者に添付ファイルを開かせ、不正プログラムを実行させるように仕向けた手法が多く用いられています。

6.2.2 不正プログラムの種類と機能

標的型メール攻撃に添付されている不正プログラムの種類としては、実行ファイルやPDFファイルが多く、その他にも様々なファイル形式が用いられています。

また、標的型メール攻撃に添付されている不正プログラムの多くは、外部にある他のコンピュータに接続する機能を持っています。これは攻撃者に感染したことを知らせるためや、他の不正プログラムをダウンロードするためです。その他、キーボードの操作情報を記録するキーロガー機能を持つものも多く確認されています。

このような機能によって、受信者のコンピュータの情報や、受信者がキーボード入力した情報が外部回線によって攻撃者に送信されてしまいます。

6.2.3 感染防止対策の困難な標的型メール攻撃

標的型メール攻撃には、受信者が不正プログラムの感染に気付かない場合、攻撃の存在そのものが長期間にわたって表面化しないという問題があります。また、標的型メール攻撃には、攻撃者が攻撃対象専用で作成した不正プログラムが使用されることも多く、ウイルス対策ベンダーが不正プログラムの検体を入手することが難しいことから、メールの受信時には、ウイルス対策ソフトで検知できない場合があります。そのため、標的型メール攻撃に添付された不正プログラムは、他の不正プログラムに比べ、ウイルス対策ソフトによる感染防止対策が困難であるといえます。

6.3 標的型メール攻撃の悪質性と関連技術

6.3.1 ファイル種別の偽装

標的型メール攻撃は、受信者に添付ファイルを実行させるため、送信者が実在する関係者や団体等であるかのように詐称している場合が多く見られます。また、受信者の取引先や友人等の知人を送信者として詐称している場合もあります。

また、標的型メール攻撃の多くは、添付ファイルが実行プログラムと気付かれないように、添付ファイルのアイコンや拡張子を、Word ファイルや PDF ファイルに偽装しています。その他、「RLO (Right-to-Left Override)」と呼ばれる機能を使用した不正プログラムもあります。この機能は、文章を右読みから左読みに変える機能です。例えばファイル名「fdp.exe」に RLO を使用すると「exe.pdf」と表示することが可能になり、実行ファイルを PDF ファイルのように偽装させることができます。

さらに、標的型メールに添付されている不正プログラムには、自身の動作を隠蔽するため、添付ファイルを開くと、受信者の注意をそらすための Word ファイルや PDF ファイルの文書が開かれる一方で、不正プログラムが不正な指令を実行するものもあります。

これらの偽装技術により、受信者は不正プログラムであることに気付かずに添付ファイルを開いてしまう可能性が高くなります。

6.3.2 代替データストリーム (ADS: Alternate Data Streams)

代替データストリームとは、一つのファイルやフォルダに複数のファイルを作ることができる Windows の機能の一つです。代替データストリームを使用したファイルやフォルダは、Windows のバージョンによってはエクスプローラーやタスクマネージャに表示されません。この機能を不正プログラムに使用されてしまうと、発見や駆除が非常に困難になります^(注)。

6.3.3 ヒープスプレー (heap spray)

ヒープスプレーとは、Windows が持っている不正プログラムの実行防止機能を回避し、攻撃成功率を高めるための手法です。ヒープと呼ばれるメモリ領域に対して不正なプログラムをスプレーで塗りつぶすように大量に書き込み、不正プログラムが実行される可能性を高めるものです。ヒープスプレーが使用された場合、メモリ使用量が一時的に大きく増加することがあるため、不正プログラムの存在に気付くことができる場合があります。PDF ファイル型の不正プログラム等で多く使用されています。

注：マイクロソフト社から代替データストリームを使用したファイルやフォルダの検索及び削除を行うことができるツールが提供されています。

「Streams」(マイクロソフト社), <http://technet.microsoft.com/en-us/sysinternals/bb897440>

6.4 対策

標的型メール攻撃による被害を防止するためには、アプリケーションの修正プログラムを適用することや、ウイルス対策ソフトを常に最新の状態に更新しておくといった基本的な対策を実施することが大切です。

しかし、標的型メール攻撃に添付された不正プログラムが OS やアプリケーションの脆弱性を悪用するものである場合は、感染時点で修正プログラムが公開されていない可能性があります。また、ウイルス対策ベンダーの対応が間に合わない場合、ウイルス対策ソフトによる対策も困難となります。そのため、基本的な対策と併せて、受信したメールに対する注意も必要です。例えば、実行プログラムや文字表記が正常でないファイル等不審な添付ファイルは開かない、重要なメールについては開く前に送信者に確認するといった対策が、これまで以上に重要になってくるといえます。また、送信者側のモラルとして、メールにファイルを添付する場合は、事前に受信者にファイルを添付する旨を伝えるといった心遣いも大切です。

企業等では、従業員等に対して、メールを利用する際に何らかの不審な点に気が付いた場合には、システムを管理する担当者へ報告するといったことを周知しておくことも重要です。また、未知の不正プログラムが実行されてしまった場合を想定して、不正プログラムの動作状況を検証できるログの採取を行い、例えば、組織の外に対してファイルを不正に送付するような通信がないか、組織内のコンピュータ同士で不正な調査を行うような通信がないか、定期的にログを確認することにより、異常の早期発見に努めることも有効です。

6.5 まとめ

標的型メール攻撃は、今後も手法を変えながら継続して行われるものと考えられます。標的型メール攻撃の被害を受けないためには、日頃からセキュリティに対する意識を高めていくことが重要です。万が一、標的型メール攻撃を受信した場合は、ウイルス対策ベンダーに情報を知らせるなど、被害の拡大防止を図ることが大切です。

7 情報セキュリティの向上のために

平成 22 年中は、特定のウェブサイトに対して大量の通信を行う DoS 攻撃の発生、特定の基幹システムを攻撃対象とした Stuxnet の確認等、サイバーテロが現実になり得るものと認識させられる事象がみられました。

このようなインターネット上の脅威から、情報資産を守り、意図に反してサイバー攻撃に加担させられてしまうことがないように、インターネットを利用する際は、最低限、以下のような措置を講じることが大切です。

- OS やアプリケーションの更新プログラムの適切な適用
- ウイルス対策ソフトやファイアウォールソフト等の適切な運用
- メールに添付されたファイルや、メール中のリンク先を不用意に閲覧しない

この他、コンピュータの利用状況に応じて、次の対策を実施することも有効です。

- パソコンやユーザ・アカウント等の使い分け
- 使用していないパソコン等のシャットダウン
- 不要な機能を導入しない、又は使用不可にする
- パスワード等の秘密データを安易にパソコン等へ保存しない
- セキュリティ更新プログラムが提供されなくなったソフトウェアの適切な更新

これらに加えて、企業等の情報セキュリティ管理者等の皆様にとって、情報資産に対する様々な被害を未然に防止したり、軽減したりするために、推奨される措置の例として、以下の対策があります。

- パソコン、ウェブサーバ等の機器の適正な設定
- データベースを運用している場合は、外部からのデータベースへの不正な命令を遮断するといった、データベースを不正に操作されないような対策についての検証
- ログ等の定期的な確認による、異常の早期発見と必要な措置

なお、前述した対策の実施に当たっては、事前に実施に伴う不具合の発生等を検証するため、各種ソフトウェアやコンピュータ機器の販売元等から提供されているセキュリティ情報の確認に配慮してください。

このような対策に加えて、情報セキュリティ対策及び事業継続計画等についても、

十分に検討の上、障害原因の究明や障害の兆候の迅速な発見・対応ができるよう、守るべき情報資産等に応じて、組織としての態勢を適切に構築することが重要です。

サイバー攻撃の手法は日々変化しています。これに対処するため、インターネットを利用される皆様、企業等の情報セキュリティ管理者等の皆様が、可能な限りインターネット上の脅威や、その対策等について関心を持ち、状況に応じて適切な措置を行っていただくことが大切です。

警察庁では、今後とも様々な機会をとらえて、情報セキュリティ対策に資する情報を提供するなどして、皆様が安心して利用できる安全なインターネット社会の確立に努めてまいります。