2013 年 2 月 27 日

独立行政法人情報処理推進機構（IPA）

ENISA 脅威の展望 ～ 刻々と変わる脅威環境への対応 ～

本概要は、欧州ネットワーク情報セキュリティ庁（ENISA：European Network Information Security Agency）が発行する、“ENISA Threat Landscape- Responding to the Evolving Threat Environment”の抄訳となります。

内容の詳細につきましては、原文をご参照ください。（※本文中のリンク先は全て英文となります）

URL：

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

本報告書は、セキュリティベンダや研究機関などが公開している、2012 年に発行された 120 以上のレポートを基に、現在の脅威（原文第 4 章）、脅威をもたらす脅威主体（原文第 5 章）、今後注目される脅威（原文第 6 章）、まとめ（原文第 7 章）について纏めている。なお、脅威の地理的分布といった情報、および天災など、情報セキュリティに直結しない（IT の脆弱性を直接活用するわけではない）脅威は本レポートの対象範囲外とする。

1. 現在の脅威

以下に、現在の脅威トップ 16 を挙げる。

1 位 ドライブバイダウンロード攻撃

ウェブサイトの HTML ソースコードにマルウェアが埋め込み、ユーザのブラウザの脆弱性を利用し、ウェブサイトを観るだけで感染する。Java、Adobe などブラウザのプラグインを狙った攻撃が増加しており、2012 年には、初めてアンドロイドでも確認された。殆どのケースにおいて、正規のウェブサイトが侵害され、マルウェやリンクが埋め込まれて悪用されている。

2 位 ワーム／トロイの木馬

トロイの木馬はバックドアを作り込み、情報を窃取するのに適しており、金銭目的のサイバー犯罪者に今でも最も使われている。中でも、自動実行機能を利用するトロイの木馬とコンフィッカーが最も使われている。また、最も報告が多かったマルウェアでもある。

3 位 コードインジェクション攻撃

SQL インジェクション、クロスサイトスクリプティング、クロスサイトリクエストフォージェリ、リモートファイルインクルージョン等を含む。昨年、ウェブアプリケーションに対して最も一般的に使われたのは SQL インジェクションであった。また、クロスサイトスクリプティングの報告数も激増した。

4 位 攻撃ツール

攻撃ツールは、通常ドライブバイダウンロード攻撃に使われるケースが多い。技術的知識がなくても

簡単に使えることが最大の特徴。「Blackhoke」ツールキットが最もよく使われており、2012 年前半に検知されたツールは殆どこれであった。

5 位　ボットネット

ボットネットの安定した運用のため、最近はボットネットの制御ネットワークは C&C サーバの分散化が一般的となっている。引き続き「サービス」として売買されているが、警察やセキュリティ業界の追跡を避けるため、現在は大規模なボットネットでなく小規模なボットネットが主流となっている。

6 位　サービス運用妨害（DoS）

最近の手口として、UDP/ICMP/SYN パケットをただ大量に送りつけるといったシンプルやり方は行われていない。最近の DoS 攻撃ツールは、アプリケーションレイヤーを狙ったものとなっている。また動機も、ハクティビズム、バンダリズム、脅迫などが主である。

7 位　フィッシング

一般的に偽フィッシングサイトは金融機関のサイトが多いが、中には支払い代行サービス、ソーシャルネットワーク、宅配サービス、政府機関などのサイトが使われることもある。プラットフォームも、PC からモバイル機器に拡大している。攻撃ツールの普及等により、正規サイトに偽サイトをホスティングさせるのも容易となっている。

8 位　機密情報の漏洩

2011 年度は、情報漏洩事件が非常に多く発生した年でもあった。多くは不注意な内部の人間か、悪意ある外部の人間によるもので、外部犯ではサイバー犯罪者かハクティビストが主であった。10 件中 9 件は、ベストプラクティスが実践されていれば防げたと言われる。ウェブアプリケーションの脆弱性対策が重要となる。

9 位　偽ソフト／スケアウェア

引き続き偽セキュリティソフトが多く、皮肉にもユーザのセキュリティ意識が向上したことが、スケアウェアの被害が拡大する一因でもある。技術面では、偽ソフトに進歩は見られなかった。2011 年 11 月には Mac ユーザを標的とした偽ウイルス対策ソフトも確認された。

10 位　スパム

各国および国際的な取組みが功を奏し、2011 年のスパムは大きく減少した。2012 年もこの傾向は続くと思われる。その結果か、より標的型なスパムにシフトしている。また、その内容も、非常に信憑性が高く、騙され易いものとなってきている。

11 位　標的型攻撃

標的型攻撃は増加しており、スピアフィッシングやソーシャルエンジニアリングの活用が増えている。また、中小企業に対する標的型攻撃も増えている。産業制御システムの感染経路として最も一般的なのもスピアフィッシングである。2012 年の大事件の 1 つが Flame の発見であり、開発には 10 年以上が掛か

っているとも言われている。また、水飲み場型攻撃と呼ばれる攻撃手法も出てきている。

12 位　物理的盗難、紛失、損害

「モバイル」という特性上、データの紛失や盗難が増加している。BYOD は、機器の盗難・紛失が機密情報の盗難・紛失に直結することが考えられ、企業に大きな影響を及ぼす。モバイル機器の情報の暗号化が必要となる。

13 位　ID 詐欺

オンラインバンキングを狙ったトロイの木馬は、非常に高度で巧妙。中でも Zeus と SpyEye が有名で、柔軟にカスタマイズができる作りになっている。モバイル機器でオンラインバンキングを行うユーザが増えつつあり、サイバー犯罪者の標的となってきているほか、ソーシャルネットワークにおいて ID 詐欺に遭うリスクも非常に高くなっている。

14 位　情報漏洩

意図せず、または意図して漏らした情報を第三者に悪用されるケースが増えている。モバイルアプリによって漏洩したユーザ情報や位置情報がプライバシーの侵害につながる形で使われる可能性もある。また、性質の悪い広告アプリが、ユーザに無断でモバイル機器内の情報にアクセスしているケースもある。

15 位　検索結果の改ざん

検索エンジンの検索結果の改ざんは、悪意のあるウェブサイトにユーザを誘い込む手段として、サイバー犯罪者によく使われる主要な手口の 1 つである。特に、画像の検索結果の改ざんが非常に巧み、新たな流行となっている。

16 位　偽の証明書

電子証明書は、インターネット上での「信頼」の拠り所である。証明書が盗用や不正に作成されては、信頼が失われてしまう。Stuxnet、Dudu、Flame は、セキュリティ機能による検知を免れるために偽の証明書を使用していた。同じ手口によって大規模な中間者攻撃が行われるなど、サイバー犯罪からスパイ活動、サイバー戦争に使われた。

2. 脅威主体

以下に、これらの脅威もたらす脅威主体の種類について挙げる。

企業

競争上の優位性を持つことを動機とし、標的とする会社を定めた場合、敵対的な脅威主体となる。企業の規模によっては大きな力を持つ。

サイバー犯罪者

敵対的な脅威主体。金銭の取得を目的とし、近年はスキルも高い。ローカル、国家、または国際レベ

ルで組織化されていることも。サイバー犯罪者の間には、一定のつながりがあると考えるべきである。

従業員

従業員、請負業者、運用スタッフ、警備員等を指す。組織のリソースへのアクセス権を保有している。非敵対的な脅威主体となる可能性（不注意な従業員）も、敵対的な脅威主体となる可能性（不満を持つ従業員）もある。このような脅威主体は、非常に効果的な攻撃を行うことを可能にする多くの情報や知識を有している。

ハクティビスト

脅威主体の新たな流行であり、政治的、社会的思想に基づき、自分達の信念を誇示するために IT スキルを活用する個人である。通常、著名なウェブサイトや、企業、情報機関や軍事機関を標的とすることが多い。

国家

サイバー兵器を保有している可能性があり、敵対国に対してそれを行使する可能性があることから、サイバー戦争の脅威となりうる。

テロリスト

テロリストも活動の範囲を広げ、サイバー攻撃を行うようになった。動機は政治的かつ宗教的であり、スキルはピンキリである。攻撃を行う場合、狙うのは重要インフラの可能性が高い。但し、公開資料を分析した限りでは、サイバーテロリストの定義はまだ明確に決まっていない。

3. 今後注目される脅威

以下に、今後注目される分野とその分野における脅威について挙げる。

モバイルコンピューティング

モバイル機器の機能拡大、急速な普及による、IT 知識やセキュリティ知識の乏しいユーザ層による利用の拡大、BYOD 等の新たな利用形態の登場、LTE 等のより大量・高速な通信技術の進歩、セキュリティの弱い無線の利用、セキュリティが成熟していないモバイル OS やアプリケーション、モバイル機器におけるオンラインバンキングの利用による営利目的のサイバー犯罪者による標的化、持ち運びの便利さ故の紛失や盗難の増加といった、モバイル機器を取り巻く環境の変化に伴い、モバイル機器に対する脅威が出現している。

	モバイルコミュニティにおける今後注目される脅威	動向
1	ドライブバイダウンロード攻撃（モバイル OS、アプリを標的化）	↑
2	ワーム／トロイの木馬（モバイル OS や SMS を標的化）	↑
3	攻撃ツール（モバイル OS の脆弱性を悪用）	↑
4	物理的な盗難、紛失、損害（モバイル機器を標的化）	↑

5	機微な情報の漏洩（モバイル機器内の情報や通信中の情報を標的化）	↑
6	コードインジェクション（モバイル機器用の不正なコードの普及）	→
7	フィッシング詐欺（モバイルユーザを狙ったフィッシング）	↑
8	情報漏洩（ユーザによるエラーや、セキュリティの弱いモバイルアプリからのデータの外部への漏洩）	→
9	ID 詐欺（トロイの木馬等によるモバイル機器上の ID 情報の窃取）	↑
10	ボットネット（ウイルス感染によるモバイル機器の踏み台化）	↑

【凡例】 ↓減少、 →変わらず ↑増大

ソーシャルテクノロジー

ユーザーが多く、多くのアプリケーションとつながり、セキュリティ対策の成熟度がまだ不足しており、モバイル機器をインターフェースとし、あまりセキュリティ意識の高くないユーザ層を持つソーシャルネットワークに代表されるソーシャルテクノロジーは、ソーシャルエンジニアリング攻撃だけでなく、あらゆるタイプの攻撃に晒され易く、脅威が増大している。

また、ソーシャルテクノロジーが今後他のシステムと連携していく中で、新たな脅威が出現する可能性もある。

	ソーシャルテクノロジーにおける今後注目される脅威	動向
1	ワーム／トロイの木馬（ソーシャルネットワークでの信頼関係を悪用し、マルウェアに感染させる）	↑
2	情報漏洩（役立つ情報の窃取）	↑
3	物理的な盗難、紛失、損害（ユーザデータを含むモバイル機器を標的化）	↑
4	フィッシング詐欺（ソーシャルネットワークの情報を活用したソーシャルエンジニアリング）	↑
5	スパム（減少しているものの、ソーシャルメディアの活用に注力）	→
6	攻撃ツール（ソーシャルネットワークを通じて悪意のある広告サイトに誘導）	→
7	ID 詐欺（モバイル機器上の ID 情報を盗み、ソーシャルネットワークに不正アクセス）	↑
8	ドライブバイダウンロード攻撃（ソーシャルネットワークでの信頼関係を悪用）	↑
9	偽ソフト／スケアウェア（ソーシャルネットワークでの信頼関係を悪用してインストールを誘導）	→
10	標的型攻撃（ソーシャルエンジニアリングを利用したスピアフィッシング）	↑

【凡例】 ↓減少、 →変わらず ↑増大

重要インフラ

重要インフラシステムは、市民の生活および国家安全保障の観点からも重要なシステムだが、様々なサブシステムから構成されており、セキュリティの確保が非常に困難である。また、通信技術、攻撃ツール等が進歩し、サイバー戦争にも利用可能な程の成熟度に既に達していると思われる。

	重要インフラにおける今後注目される脅威	動向
1	ドライブバイダウンロード攻撃（重要インフラシステムのマルウェア感染）	↑
2	ワーム／トロイの木馬（トロイの木馬の増加傾向が、重要インフラシステムにもの影響を及ぼす可能性）	↑
3	コードインジェクション（クロスサイトスクリプティングが、重要インフラで使用されているウェブアプリケーションにも影響を及ぼす可能性）	↑
4	攻撃ツール（重要インフラ構成機器・ソフトウェアの脆弱性の発見・悪用）	↑
5	サービス運用妨害（比較的低いスキルで、多大な影響を及ぼすことが可能）	→
6	フィッシング詐欺（ソーシャルエンジニアリングを活用したフィッシング攻撃）	→
7	ボットネット（モバイルコンピューティングの発展を通じて脅威が増大）	→
8	機微な情報の漏洩（攻撃に有用な情報の窃取）	↑
9	標的型攻撃（スピアフィッシングや APT の活用）	↑
10	物理的な盗難、紛失、損害（モバイル機器の紛失および情報の漏洩）	↑

【凡例】 ↓減少、 →変わらず ↑増大

信頼性基盤

堅固な認証とセキュアな通信を提供する信頼性基盤は、通常、強力な暗号技術と鍵管理によって実現される。信頼性基盤への攻撃の成功は、情報セキュリティのみならず国家の安全保証にも大きな影響をもたらすことになる。信頼性基盤のセキュリティについてより真剣に検討し、コンプライアンス基準を定めて実装および検証を行う必要がある。

	信頼性基盤における今後注目される脅威	動向
1	サービス運用妨害（信頼性基盤を構成するコンポーネントを攻撃し、アクセスを妨害）	↑
2	偽証明書（正規の信頼関係の侵害と、偽の信頼関係の確立）	↑
3	機微な情報の漏洩（攻撃に有用な情報の窃取）	→
4	標的型攻撃（スピアフィッシングや APT の活用）	→
5	物理的な盗難、紛失、損害（モバイル機器の紛失および情報の漏洩）	→
6	誤った実装（鍵管理など、既存の暗号基準の実装ミス）	↑
7	ID 搾取（システムにアクセスするための ID 情報の搾取	→
8	情報漏洩（攻撃に役立つ情報の窃取）	→

【凡例】 ↓減少、 →変わらず ↑増大

クラウドコンピューティング

多くの IT 専門家が市場革新であり技術革新ではないとしつつも、殆どのビジネスでクラウドの利用が計画されている。攻撃が成功すれば一度に大量のデータにアクセスできるクラウドは、攻撃者にとって時間とリソースを投資する価値のある標的といえる。また、モバイル機器との連携強化も、攻撃者に優位に

働くと見られる。

	クラウドコンピューティングにおける今後注目される脅威	動向
1	コードインジェクション（SQL インジェクション、ディレクトリトラバーサルの危険性）	↑
2	ワーム／トロイの木馬（データ損失、漏洩）	→
3	ドライブバイダウンロード攻撃（クラウド上にホスティングしているウェブサイトへのマルウェアの挿入）	↑
4	情報漏洩（（とりわけモバイル機器の利用拡大に伴い）クラウド環境で増加）	↑
5	機微な情報の漏洩（外部犯・内部犯による攻撃。多大な影響を及ぼす可能性）	↑
6	ボットネット（クラウド機能（SaaS 等）の悪用によるボットネットの実現）	→
7	サービス運用妨害	→
8	ID 窃盗（トロイの木馬による ID 情報の搾取。モバイル機器の普及により増加）	↑
9	物理的盗難、損失、損害（データが纏まっているため、とりわけ内部犯による物理的攻撃などが懸念に）	→
10	標的型攻撃（増加傾向にあり。頻度は減ったが、影響は大きい）	↑

【凡例】 ↓減少、 →変わらず ↑増大

ビッグデータ

ソーシャルテクノロジーの発達、クラウドコンピューティングやモバイル機器の普及、インターネットの更なる一般化に伴い、「ビッグデータ」が口にされるようになった。あまりに膨大過ぎて取り扱いは困難だが、ビッグデータが悪用されると、プライバシーの侵害に繋がりかねない。

	ビッグデータにおける今後注目される脅威	動向
1	ドライブバイダウンロード攻撃（ビッグデータの活用により、攻撃者がマルウェアをより効果的に仕掛けることが可能に）	↑
2	ワーム／トロイの木馬（ビッグデータの活用により、攻撃者がマルウェアをより効果的に仕掛けることが可能に）	↑
3	攻撃ツール（ビッグデーの活用により、攻撃者が攻撃に有用な情報をより多く入手することが可能に）	↑
4	フィッシング詐欺（ビッグデータ（プライバシー情報）の利用を利用することで、より標的型なスピアフィッシングが可能に）	→
5	機微な情報の漏洩（ビッグデータがデータ侵害に対する知見を提供）	↑
6	スパム（ビッグデータの活用により、スパムメールが更に標的型に）	→
7	標的型攻撃（ビッグデータが標的型攻撃に利用される）	→
8	ID 窃盗（ビッグデータの活用により ID 窃盗が促進される）	↑
9	情報漏洩（ビッグデータの分析により、漏洩情報の発見が促進される）	↑

【凡例】 ↓減少、 →変わらず ↑増大

4. まとめ

多くのレポートの分析の結果、以下が重要と思われる。

- 攻撃経路（ベクトル）に関する、より深い理解と証拠の収集：攻撃の経路を知り、標的を知るのに重要
- 敵の攻撃による影響に関する、より深い理解と証拠の収集：標的の特定と、対策の実施に重要
- 攻撃の目的（標的）に関する、より定性的な情報の収集と維持：脅威主体とインシデントの関連性を見出すのに役立つ
- 共通の用語の利用
- ユーザの観点を入れる：エンドユーザへの影響度を示し、脅威の認識向上策を検討するのに役立つ
- 脅威情報の活用例を示す：活用例を提示し、ユーザが情報セキュリティマネジメント／ライフサイクルに組み込めるようにする
- セキュリティインテリジェンスの収集：脅威、リスク、対策などを組織間で共有する
- セキュリティ対策のシフト：境界中心型のセキュリティ対策から、情報（データ）中心方の、包括的、エンド・ツー・エンドのセキュリティ対策を検討する

以上