資料３－５

現在の情報通信環境における主な脅威・課題への対応について

総務省 情報通信政策局
情報セキュリティ対策室
2007年12月20日

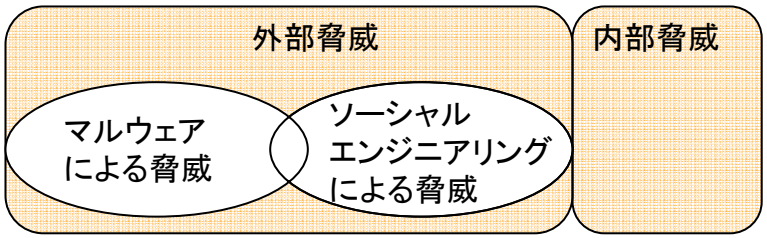
（1）主な脅威・課題及びその対策の整理

- 現在の情報通信環境における主な脅威・課題、及び各対策実施主体が行う対策について、次ページのとおり整理
- 対策の阻害要因や、対策が不十分な項目、さらに効果的な対策を講ずべき項目を検討

【主な脅威】

ア）ボットウイルス等マルウェアによる脅威
（ワーム型感染のウイルスによる脅威）
イ）ソーシャルエンジニアリングを駆使した脅威
（フィッシング等、人間の行為、行動の弱点、盲点等をついてマルウェアに感染させたり、情報を盗み出す脅威）
ウ）外部脅威（外部からの不正アクセス、自然災害等）
エ）内部脅威（人為的ミス、意図的な犯行等）

<主な脅威の関係>



【対策実施主体】

a.利用者（個人）
b.利用者（企業等）
c.情報セキュリティ関連事業者（AVV、情報セキュリティソリューション提供事業者等）
d.電気通信事業者（ISP、アクセス系、携帯電話系、無線通信系）
e.OS/アプリケーション/サービス提供事業者
f.機器開発事業者
g.政府機関

ア）ボットウイルス等マルウェアによる脅威

ボットウイルス等マルウェアによる脅威に対する取組							
その他	・ニュースなど一般情報源からの情報収集 ・ITリテラシーの取得	・運用ポリシーの設定 ・監査の実施 ・ニュースなどからの情報収集 ・社内教育 ・各種認証制度の取得	・教育の提供 ・アラートレポート ・アラートサービス	・運用の高度化 ・啓発活動 ・アラートレポート ・アラートサービス ・abuse対応 ・サポート	・啓発活動 ・アラートレポート ・アラートサービス		・啓発活動 ・関連法整備（企業） ・ガイドラインの制定等、運用の高度化支援（企業） ・情報セキュリティ対策の普及啓発
アプリケーション/ サービス	・パーソナルFWの導入 ・ウイルス対策ソフトの適用 ・ウイルス対策サービスの利用	・パーソナルFWの導入 ・ウイルス対策ソフトの適用 ・ウイルス対策サービスの利用 ・ネットワーク監視サービスの利用	・ウイルス対策ソフトの提供 ・企業ネットワーク監視サービスの提供 ・脆弱性対応	・ウイルス対策サービスの提供 ・ネットワーク監視サービス提供（企業） ・安全なWebサーバなどの提供	・脆弱性対応（パッチ作成・提供等）		・情報セキュリティ対策の普及啓発 ・各種調査実施
ＯＳ/ ミドルウェア	・バージョンアップ、パッチの適用	・バージョンアップ、パッチの適用	・ウイルス対策製品の提供		・脆弱性対応（パッチ作成・提供等）	・脆弱性対応（パッチ作成・提供等）	・情報セキュリティ対策の普及啓発 ・税制優遇（企業） ・各種調査実施
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ ホーム（企業） ネットワーク	・BBルータの導入 ・認証の適用 ・バックアップ、冗長化	・認証の適用 ・バックアップ、冗長化 ・ネットワークFW、IDS、IPS等対策機器の導入 ・運用 ・FW、IDS運用サービスの利用 ・サーバセキュリティ製品の導入 ・パッチの適用	・ウイルス対策製品の提供 ・FW、IDS等対策装置の提供 ・FW、IDS運用サービス提供（企業） ・企業ネットワーク監視サービスの提供	・FW、IDS運用サービス提供（企業） ・BBルータのファームウェア管理サービスの提供（個人） ・企業ネットワーク監視サービスの提供		・組み込みシステムの脆弱性対応 ・脆弱性対応（パッチ作成・提供等）	・税制優遇（企業） ・各種調査実施
ネットワーク（ インターネット ／公衆網）				・ネットワーク設備の運用・維持管理、緊急対応、事業者連携 ・ネットワーク監視 ・ＶＰＮ、専用線の提供 ・(不必要な通信の除去)			・ガイドラインの制定等、運用の高度化支援（企業）
要素技術			・収集技術 ・解析技術 ・検知技術 ・駆除技術	・ネットワーク設備 ・通信上の異常検出 ・フィルタ ・帯域制御	・設計段階からのセキュリティ対策 ・脆弱性の検出	・設計段階からのセキュリティ対策 ・脆弱性への対応	・研究開発の推進 ・関連団体による収集、解析、検知、駆除技術
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

イ）ソーシャルエンジニアリングを駆使した脅威

ソーシャルエンジニアリングを駆使した脅威　に対する取組							
その他	・知人等の啓発	・従業員等の啓発	・利用者の啓発	・利用者の啓発	・利用者啓発	・利用者啓発	・法執行機関による摘発強化 ・法律面、制度面からの、対策の促進 ・海外との連携の支援 ・利用者啓発
アプリケーション/サービス	・ウイルス/フィッシング/スパム対策ソフト・サービスの利用 ・パーソナルＦＷの導入 ・URLフィルタリングサービスの利用 ・バージョンアップ、パッチの適用	・ウイルス/フィッシング/スパム対策ソフト・サービスの利用 ・パーソナルＦＷの導入 ・URLフィルタリングサービスの利用 ・バージョンアップ、パッチの適用、サービスの導入	・脆弱性対応 ・ウイルス/フィッシング/スパム対策ソフトの提供 ・パーソナルＦＷソフトの提供 ・MSSの提供 ・バージョンアップ、パッチサービスの提供	・ウイルス/フィッシング/スパム対策サービスの提供 ・パーソナルＦＷサービスの提供 ・バージョンアップ、パッチサービスの提供 ・SPF/Sender ID（送信元アドレス偽装防止技術）の提供・利用	・対ソーシャルエンジニアリング的な機能の提供 ・安全な利用者認証の仕組みを提供(SSOなど) ・個人証明書の提供 ・SPF/Sender ID（送信元アドレス偽装防止技術）/証明書等の扱いに適したアプリケーションの提供 ・利用者に危険をもたらすサイトの警告・非表示		・アプリケーションの普及啓発 ・情報セキュリティ対策の普及啓発・促進（法律面、制度面）
ＯＳ/ミドルウェア	・バージョンアップ、パッチの適用 ・セキュリティの強いシステムの利用	・バージョンアップ、パッチの適用			・脆弱性対応 ・安全な利用・設定等の情報提供 ・保護/防止機能の提供		
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク	・端末認証・個人認証の適用 ・ルータ(FW)等の利用	・端末認証・個人認証の適用			・サーバー証明書(EVSSL)の利用	・脆弱性対応 ・安全な利用・設定等の情報提供 ・保護/防止機能の提供	
ネットワーク（インターネット／公衆網）	・ネットワーク上で違法有害情報フィルタリングを提供するISPの選択	・Proxyによる違法有害情報フィルタリング	・スパムフィルタの提供 ・利用者に危険をもたらすサイト等の情報共有	・DNSを利用したフィッシングサイト等の警告システム提供 ・利用者に危険をもたらすサイトの警告・非表示 ・送信元詐称や攻撃通信の排除	・ネットワーク上でのセキュリティサービス提供 ・利用者に危険をもたらすサイト等の情報共有		・ネットワーク上での対策の支援 ・海外との対策・法的措置の支援
要素技術			・ウイルス/フィッシング/スパム対策技術 ・パーソナルＦＷ ・URLフィルタリング ・バージョンアップ/パッチ適用技術	・ウイルス/フィッシング/スパム対策技術 ・パーソナルＦＷ ・URLフィルタリング ・通信の遮断・排除 ・個人認証・端末認証 ・Sender ID/SPF（送信元アドレス偽装防止技術）	・サーバー証明書(EVSSL) ・利用者認証（SSO） ・脆弱性対策 ・情報共有 ・Sender ID/SPF（送信元アドレス偽装防止技術）	脆弱性	
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

ウ）外部脅威

外部脅威（A：全般　B：不正アクセス　C：自然災害）に対する取組							
その他		・BCPの策定（A） ・運用ポリシーの策定 ・監査の実施 ・データセンターの利用 ・組織内CSIRT設置 ・ISMS（取得） ・セキュリティ啓発(受ける側)	・注意喚起/AlertCon ・ISMS(取得支援) ・セキュリティコンサルティング ・ハニーポットによる脅威分析 ・ネットワークの脆弱性診断	・(通信サービスに関する)CSIRT設置 ・事業者連携･協調の枠組 ・サイバー攻撃対応演習	・データセンター設備提供	・(製品に関する)CSIRT設置	・ガイドラインの作成等、対策の普及啓発（A） ・CEPTOAR-Council(設置検討の支援) ・情報セキュリティ啓発 ・国際協調の枠組み作り ・情報セキュリティに関する法律
アプリケーション/サービス	・Personal Firewallアプリケーションの導入（B） ・バージョンアップ、パッチの適用（B） ・データバックアップソフト/サービスの適用（A）	・バージョンアップ、パッチの適用（B） ・企業ネットワーク監視サービスの適用（B） ・認証サービスの適用 ・データバックアップソフト/サービスの適用 ・ウィルス・スパム対策等ソフト・サービスの利用	・企業ネットワーク監視サービスの提供（B） ・脆弱性対応（B） ・脆弱性情報の提供 ・認証サービスの提供 ・コードレビュー ・Web脆弱性診断 ・PKIサービスの提供 ・ウイルス対策ソフトの提供	・データバックアップソフト/サービスの適用（A） ・ウィルス・スパム対策等サービスの提供	・データバックアップソフト/サービスの提供（A） ・FW/IDS/IPS等セキュリティソリューション(開発・提供) ・脆弱性対応（B） ・認証サービスの提供（B） ・ペネトレーションテスト	・FW/IDS/IPS等セキュリティソリューション(開発・提供) ・脆弱性対応	・情報セキュリティ対策の普及啓発（B） ・対策導入支援(税制)（C）
ＯＳ/ミドルウェア	・Personal Firewall機能付きOSの導入（B） ・バージョンアップ、パッチの適用（B） ・データのバックアップ（A）	・バージョンアップ、パッチの適用（B） ・データのバックアップ（A） ・ハードディスク暗号化			・Personal Firewall機能付きOSの提供（B） ・脆弱性対応	・脆弱性対応	・情報セキュリティ対策の普及啓発（B） ・対策導入支援(税制)（C）
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク		・ネットワークFW、IDS、IPS等対策機器の導入 ・VPN装置の導入（B） ・認証の実施（B） ・UPSの適用（C） ・システムの二重化	・ネットワークFW、IDS、IPS等対策機器の提供 ・FW、IDS運用サービス提供			・認証サーバの提供（B） ・脆弱性対応（B） ・UPSの提供（C） ・生体認証端末(指紋認証携帯電話機等)	・情報セキュリティ対策の普及啓発（B） ・対策導入支援(税制)（C）
ネットワーク（インターネット／公衆網）		・VPN・専用線サービスの導入（B）		・ネットワーク設備の運用・維持管理、緊急対応、事業者連携(A) ・ネットワーク監視サービスの提供（B） ・VPN・専用線サービスの提供（B）			・運用の高度化支援（B）
要素技術			・解析・対策技術の高度化（B） ・CVE（脆弱性識別番号）	・ネットワーク設備（A）	・設計段階からのセキュリティ・故障対策（A） ・CVE（脆弱性識別番号） ・脆弱性自動パッチサービス	・設計段階からのセキュリティ・故障対策（A） ・CVE（脆弱性識別番号） ・DPI ・ハードウエアベース暗号方式(量子暗号等)	・研究開発の推進（A）
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

エ）内部脅威

内部脅威（人為的ミス、意図的な犯行等）に対する取組

その他	・Ｐ２Ｐアプリケーション等の利用の自粛 ・個人向け情報セキュリティに関する啓発	・運用ポリシーの設定 ・監査、教育、運用の実施 ・データ保護（バックアップ）、現物保管、散逸防止 ・入退出管理、映像監視 ・セキュリティポリシーの策定 ・セキュリティマネジメントの確立 ・各種認証制度の取得 ・委託業者との適切な契約		・運用の高度化 ・インシデント・故障対応演習 ・機械操作・保守訓練 ・ヒューマンエラー抑止に関する技術導入（組織マネジメント、ＭＭＩ）	・サーバ証明書の取得	・暗号モジュールの提供 ・放出電磁波による情報漏洩に対する対策	・情報システム運用等に関するガイドラインの作成等、運用の高度化支援 ・情報セキュリティ対策の普及啓発 （セキュアなシステム開発運用フレームワーク）
アプリケーション/サービス	・ウイルス対策ソフトの適用、サービスの導入 ・バージョンアップ、パッチの適用 ・パーソナルFWの適用	・ウイルス対策ソフトの適用、サービスの導入 ・バージョンアップ、パッチの適用 ・目的外利用対策 ・企業内情報管理ソリューションの採用 ・Ｐ２Ｐアプリケーション利用対策	・脆弱性対応 ・ウイルス対策ソフトの提供 ・企業ネットワーク監視サービスの提供 ・ログ管理ソリューションの提供 ・Ｐ２Ｐアプリケーション検知ソフトウェアの提供 ・情報漏洩ソリューションの提供	・ウイルス対策サービスの提供 ・ログ管理サービスの提供 ・誤操作防止インターフェースの導入	・脆弱性対応 ・アプリケーションによる不正検知 ・企業内情報管理ソリューションの提供 ・Ｐ２Ｐアプリケーション利用監視サービスの提供	・ハード化装置の提供 ・企業内情報管理ソリューションの提供	・情報セキュリティ対策の普及啓発
ＯＳ/ミドルウェア	・バージョンアップ、パッチの適用	・バージョンアップ、パッチの適用 ・安全なOS/ミドルウェアの選択			・脆弱性対応 ・ロバスト化（要塞化・ハード化）	・ハード化装置の提供	・情報セキュリティ対策の普及啓発
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク	・認証の適用 ・バックアップ・冗長化 ・セキュアクライアント（モバイル含む）	・認証の適用 ・FW、IDS等対策機器の導入 ・企業ネットワーク監視サービスの適用 ・バックアップ・冗長化 ・アクセス制御（認証・識別の適用　等） ・暗号化による管理 ・シンクライアント化 ・セキュアクライアント（モバイル含む） ・ネットワークの物理的隔離	・FW、IDS等対策装置の提供 ・VPN装置の提供 ・企業ネットワーク監視サービスの提供	・電波漏洩対策 ・企業ネットワーク監視サービスの提供	・利用者認証･Webアクセス認証 ・利用者情報ディレクトリ ・操作監視・持出制御	・組み込みシステムの脆弱性対応 ・情報漏えい防止アプライアンスの提供 ・シンクライアントシステムの提供 ・暗号化機器の提供 ・画面遮蔽フィルター	・情報セキュリティ対策の普及啓発
ネットワーク（インターネット／公衆網）		・バックアップ・冗長化		・ネットワーク設備の運用・維持管理、緊急対応、事業者連携 ・ネットワーク監視 ・ＶＰＮ、専用線の提供 ・Ｐ２Ｐ暴露ウイルス感染者への対策注意喚起 ・検疫ネットワークサービスの提供	・ネットワークの分離（セキュリティドメイン）		・ガイドラインの作成・支援 ・運用の高度化支援
要素技術			・解析・対策技術の高度化 ・暗号、認証 ・電子透かし	・ネットワーク設備 ・データ秘匿（暗号化） ・無線ＬＡＮセキュリティ ・携帯電話セキュリティ	・設計段階からのセキュリティ対策 ・不正利用防止	・設計段階からのセキュリティ対策 ・耐タンパ、暗号アルゴリズム、高速実装 ・TEMPEST技術研究開発 ・利用者認証、機器アクセス制御 ・本人認証、電子証明書、電子署名	・情報漏えい対策の研究開発
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

（2）現状の対策実施状況の概観

- ボット等マルウェアの感染に対する対策は、電気通信事業者による電気通信設備への対策等も行われているが、おおよそ利用者（個人）及び利用者（企業）のエンドポイント（ネットワークでの接続ポイント）での対策が主である。脅威の変化や高度化を踏まえ、引き続き、適切な対策を講じていくことが重要であると考えられる。

- ネットワークを利用するソーシャルエンジニアリングを駆使した脅威については、マルウェア感染同様、利用者（個人）及び利用者（企業）のエンドポイント（ネットワークでの接続ポイント）での対策が主であり、また、利用者が安易にクリックしたり、個人情報を書き込んだりしないようにするといった個人の基本的なリテラシーに依存するところが大きいと考えられる。

- 外部脅威と内部脅威については、主として利用者（企業）において対策が求められてきたところであるが、今後も内部統制の強化が必要であり、不断の対策の実施・改善が必要であると考えられる。

（3）対策実施を阻害する要因と考えられる事項等

- 利用者（個人）は、情報セキュリティ対策への意識やスキルに大きな差があり、一律に対策実施を求めるのは難しい。また、極度に不安感を抱くあまり、インターネット等、ICT利用を敬遠する事態となることは好ましくない。

- 電気通信事業者が法律上対応可能な範囲について、十分に検証されていないこと等により、効果的な対策を実施できない状況にあるのではないか。さらに、こうした状況が電気通信事業者の設備増強コスト等に影響を及ぼしているのではないか。

- インターネットという性質上、複数の電気通信事業者が連携して対策を実施しなければならない場合が多いと考えられるが、個々の電気通信事業者の協力・関与には温度差があり、事案を根治するための十分な連携が出来ていないのではないか。

- 対策の実施フェーズは、予防、検知、対策立案・実施、効果測定（恒久的な予防策として継続するのか、対策を終了するのか等の検証・判断）であると考えられるが、個別の対策実施主体が実施している対策の実施フェーズを適切に共有できておらず、対策の遅延や不具合を生じているのではないか。

（4）重点的に取組むべき課題及び対応策（案）

これまで様々な脅威に対して実施してきている各主体の情報セキュリティ対策は、今後も継続して対策を実施していくことが重要である。
昨今の脅威の状況等を踏まえ、以下の項目については、より一層の対応の強化について検討していくべきと考えられる。

I. 基本的な対策の徹底

【脅威・課題の例】

〇ボット感染PCを踏み台にした様々なインシデントの継続・被害の甚大化

〇ウイルス感染や人為的ミス等による情報漏えいの継続、等

〇いたずらに危険性のみを強調するあまり、ICTの利用促進が阻害される可能性があるとする問題点

【対応策】

◆利用者個人、企業の職員等に対して、「どのようにすれば、比較的安全にICTが利用できるのか」という基本的な対策の徹底について、普及・啓発を継続。

◆また、誤ってウイルス等に感染してしまった場合等に、容易に相談等ができて、迅速な復旧が可能となるような取組をより一層推進。

II. ソーシャルエンジニアリングを駆使したマルウェア感染方法の高度化等への対応

【脅威・課題の例】

〇Webのリダイレクトやダウンローダを複数回組み合せて、マルウェアに感染させる手法等への対処

〇いわゆるスピア型アタック等、ソーシャルエンジニアリングを駆使したマルウェア配布・拡散手法への対処

〇ボット感染PCを踏み台にした様々なインシデントの継続・被害の甚大化

【対応策】

◆解析技術等の高度化（研究開発の促進、人材育成の推進、等）

◆関係機関の連携強化（電気通信事業者、事業者団体、研究機関、政府機関等、産学官連携スキーム）

III. 電気通信事業者が積極的に情報セキュリティ対策を実施できる環境の整備

【脅威・課題の例】

〇利用者（個人）の情報セキュリティ対策が充分ではない。

〇ボット感染PCを踏み台にした様々なインシデントの継続、被害の甚大化

〇事業者が法律上対応可能な範囲について、十分に検証されていないこと等により、効果的な対策を実施できない状況にあり、また事業者間の協力や連携が十分ではないとする問題点

【対応策】

◆マルウェア配布サイトなどへのアクセスやウイルス感染等による通常の利用方法ではない通信に対して、警告したり遮断したりするなど、電気通信事業者が積極的に情報セキュリティ対策を実施できるための環境整備に向けた検討（電気通信事業者の正当業務行為等として対策実施可能な範囲の更なる検討、モデルシステムによる対策有効性の検証等）

IV. 事案解決のための国際連携の促進

【脅威・課題の例】

〇海外から（海外へ）のDDos、スパム等の継続

〇ボット感染PCを踏み台にした様々なインシデントの継続・被害の甚大化

〇各対策実施主体の対策内容を十分に共有できていない状況にあるとする問題点

【対応策】

◆政府、電気通信事業者、関係機関等による迅速な情報共有