

最新のセキュリティ動向と 電磁波セキュリティについて

2011年12月19日
新情報セキュリティ技術研究会
技術部会長 宮坂肇

電磁波セキュリティの位置づけ

- 昨今の標的型攻撃に代表される、周到かつ執拗な攻撃の1ステップ
 - ソーシャルエンジニアリングを補完するもの
 - 時間を掛けて、低リスクで周辺情報を収集
- 海外でのStuxnetによる攻撃成功のほか、日本においても政府を目標とする攻撃が確認されている
 - 技術や資金力の必要な手段も実際に利用される
- DDoSのようにシステムの機能停止を目的とする場合、高出力電磁波による遠隔からの機能停止や破壊も手段となり得る

より現実味を帯びる

新情報セキュリティ技術研究会の紹介

◆概要(<http://www.ist-sg.jp/>)

平成13年9月27日に設立された任意団体であり、会員会社10社
(平成23年10月1日現在)で以下を活動目的としている。

- 電磁波漏洩を防ぐための技術および光無線技術の活用について検討する。
- 情報システムにおける情報漏洩の危険性、および対策方法に関して広く世の中の啓蒙活動を展開する。
- わが国のIT社会の健全な発展に貢献する

◆研究会の主な活動実績

平成14年3月29日 第1回公開セミナー

平成14年5月13日 ITU-T WorkShop on Security への参加

平成15年6月6日 プレスリリース「電磁波セキュリティガイドラインの策定について」

・
・
・

平成23年5月18日 10周年記念公開セミナー

ガイドラインの趣旨

電磁波セキュリティガイドラインは、電磁波の漏洩と侵入の脅威から情報システムを守るために作成したものである。

想定される脅威

漏洩電磁波の脅威

画面情報や打鍵情報などの入出力**情報の漏洩**

侵入電磁波の脅威

IT機器の**誤動作**、**破壊**による情報システム及びそのサービスへの影響

適用範囲

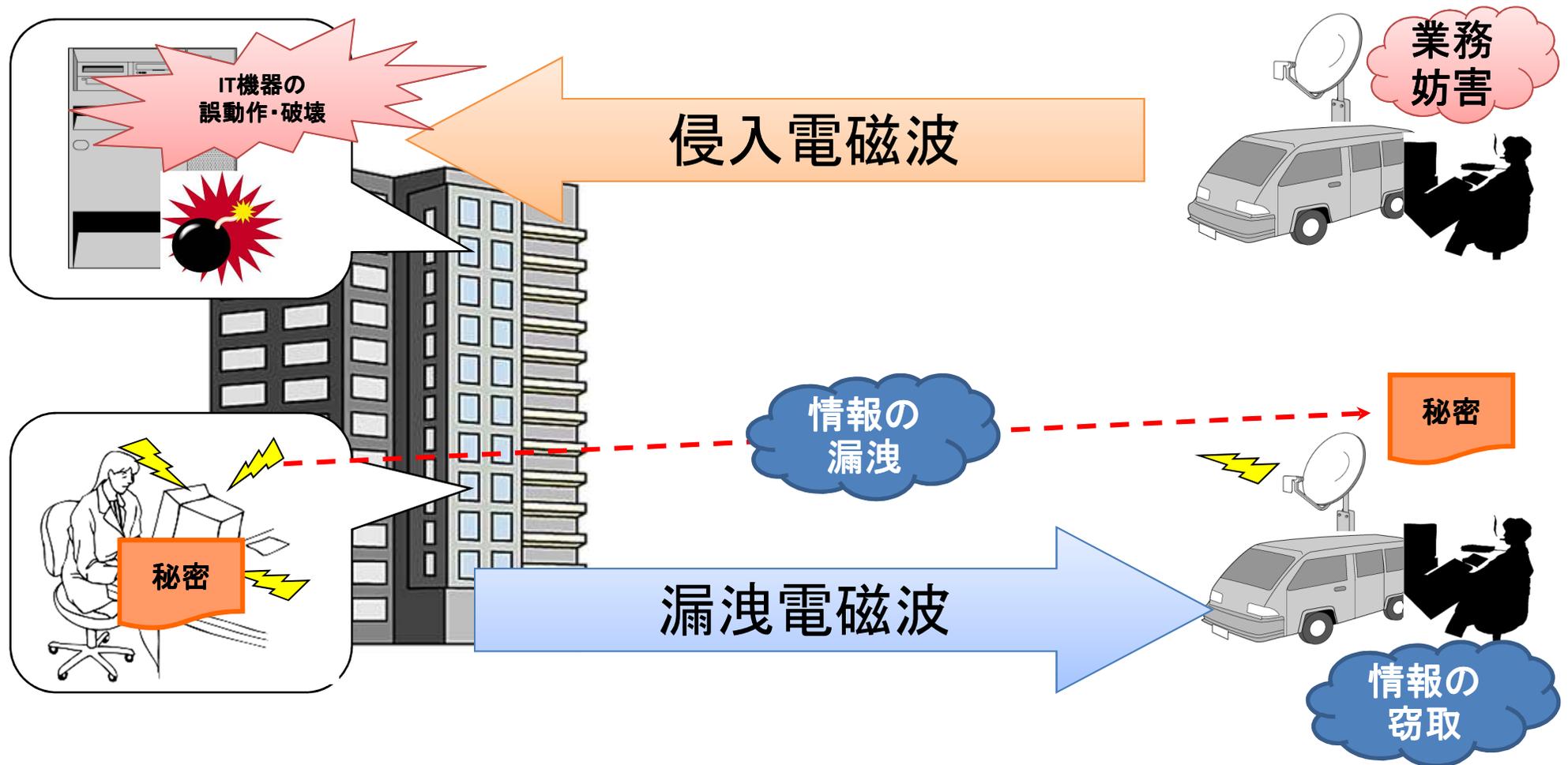
IT機器及びその設置環境

重要な情報を取り扱う電子政府等をはじめとした公的部門

および民間部門の情報系システムなど

情報システムへの脅威

電磁波の脅威は、「情報の漏洩」と「IT機器の誤動作・破壊」



総合基準と各対策基準の概要

(1) 総合基準

・IT機器、建屋、距離確保による対策の基本的な考え方などを示す。

(2) 漏洩電磁波対策基準

・IT機器における基本的な考え方、測定法、基準値などを示す。

(3) 侵入電磁波対策基準

・IT機器における基本的な考え方、試験法、動作判定基準などを示す。

(4) 建築工事設計基準

・建築工事における基本的な考え方、性能設計、性能測定法などを示す。

民間で利用可能な具体的基準値を記した、
初のガイドライン

適用例

代表モデル(参考)

公的部門 :

電子調達システム、電子申請システム、
電子投票システム、職員の執務環境 など

民間部門 :

業務系システム、情報系システム、勘定系システム、
電子商取引システム、研究開発系システム、
人事情報システム、データセンター など

意図しない、気付かない漏洩電磁波による IT機器からの情報流出を防ぐ

電磁波による情報漏えい(TEMPEST)の脅威と実態

電波を利用した情報流出の特徴

- 証拠が残らない
 - 受信されたことを知ることが出来ない
 - 送信側に盗んだ情報を保持しておく必要がない

盗る側のリスクが低い



**目に見えない電波から
情報を守る！**

具体的事例

盗聴装置による情報漏えいの被害報告例は、何故か少ない

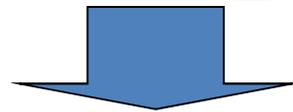
1. スウェーデン国営放送による政府関係者の証言
2. 米国CIAが旧ソ連の軍需工場に近接して情報収集装置を設置していたとの話
3. 小説上の話

現実での報告が少ない原因とは？

これまでの経緯

国内（官公庁等）

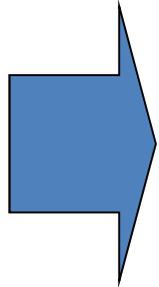
- － 報道は常に控えめである
 - 米国での国家機密的扱いに対する戸惑い
 - 実証の困難さ/都市伝説化
 - セキュリティレベルを公開することになる



**最近の情報化の進展、個人情報
の重要性認識に伴い2000年頃から再び
注目される**

脅威の本質とは

- 画面などの情報そのもの
 - 個人情報、財産的情報
 - 比較的「古典的」な目的といえる
- 「入り口」としての情報
 - ログに残らない侵入への糸口
 - ネットワーク時代の脅威
- 「風評被害」的インパクト
 - 愉快犯～国家的信用失墜まで
 - 情報保護への不信感に乗じて。。。



情報の価値は、「盗る側」が決める

必要な技術

- EMC(ノイズ)に関する技術
 - 計測機器の特性
 - ノイズ発生メカニズム
- 無線(通信)に関する技術
 - 微弱信号を受信するためのテクニック
 - 電波伝搬の原理、アンテナの知識
 - 受信信号処理の知識
- 端末のハードウェア、各IFのプロトコルに関する技術

現状での対策

- 現実的な解

- 環境ノイズに埋もれてしまえば再生は困難
- 妨害電波発生装置の場合、周囲の無線通信への影響も考慮が必要
- 部屋全体のシールド、離隔距離など、様々な候補からコストパフォーマンスでのバランスが必要

ユーザーが選択して対策を行う方が効率的(脅威の本質に留意！)