IST Information Security Technology Study Group

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

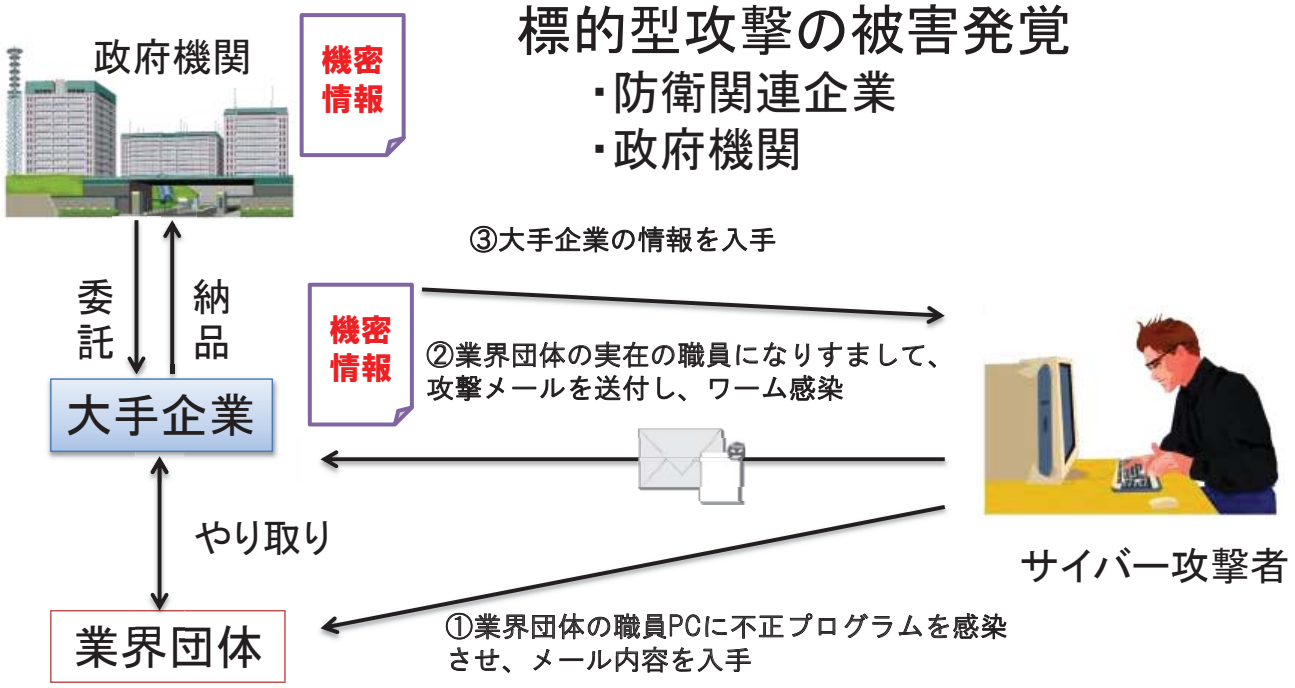
IST Information Security Technology Study Group

今年の象徴的な事例(1)

- 2011年4月末に以下サービスで不具合が発生し、全世界で1億アカウント超の個人情報が漏洩
  1. PlayStation®Network(PSN)およびQriocity™
  2. Sony Online Entertainment LLC
- 漏洩した情報にはクレジットカード、デビットカード情報が含まれる
- Anonumous、Lulzsecといった集団が次々とグループ企業も攻撃、陥落させる
- 2011年7月初旬にサービス再開
- 補償も含めた損害は最大12.5億ドルとも

企業　V.S.　個人・民意・リーダーなき集団

今年の象徴的な事例(2)



政府+企業　V.S.　海外組織？

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

IST Information Security Technology Study Group

◆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
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

技術部会の活動内容

IST Information Security Technology Study Group

情報セキュリティという観点から、これまで深く研究されていない電磁波による情報の漏洩や攻撃を中心に検討

各委員会の主な活動内容

委員会名	主な活動内容
統括・推進委員会	技術部会全体の方針策定及びガイドライン作成のための指針の策定
第一委員会	・漏洩電磁波からの情報再現技術の検討 ・対策技術の検討
第二委員会	・電磁波による意図的／非意図的攻撃事例の調査 ・対策技術の検討
第三委員会	電磁波に注目しつつ、情報セキュリティ技術動向一般の調査
第四委員会	漏洩電磁波による情報漏洩及び侵入電磁波によるIT機器の故障・誤動作に関する情報セキュリティ脅威のシナリオの検討
第一作業委員会	IT機器に対する電磁波セキュリティ対策基準の作成 （漏洩電磁波放出許容値・侵入電磁波許容値の検討、等）
第二作業委員会	建物に対する電磁波セキュリティ対策工事設計基準の作成

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

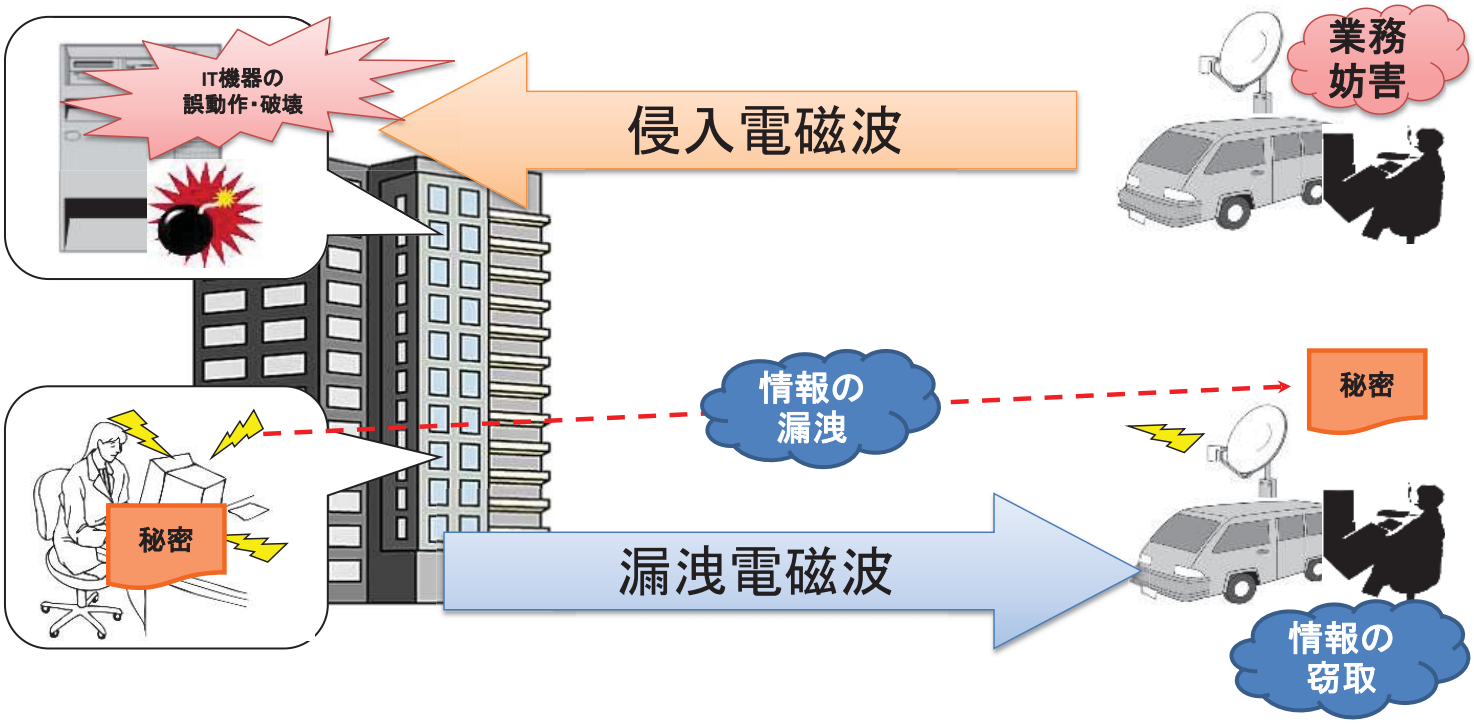
適用範囲

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」



ガイドラインの構成

- 1. はじめに
- 2. 電磁波セキュリティ概論
- 3. 適用範囲
- 4. 引用規格
- 5. 用語
- 6. 総合基準
- 7. 漏洩電磁波対策基準
- 8. 侵入電磁波対策基準
- 9. 建築工事設計基準
- 解説

IT機器及びその設置環境における電磁波セキュリティを確保するための全体指針を紹介する。「IT機器」、「建屋」、「距離」それぞれの組み合わせによる対策基準を示す。

「6. 総合基準」を実現するための各対策基準における、試験方法、試験に使用する測定器、基準値などを紹介する。

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

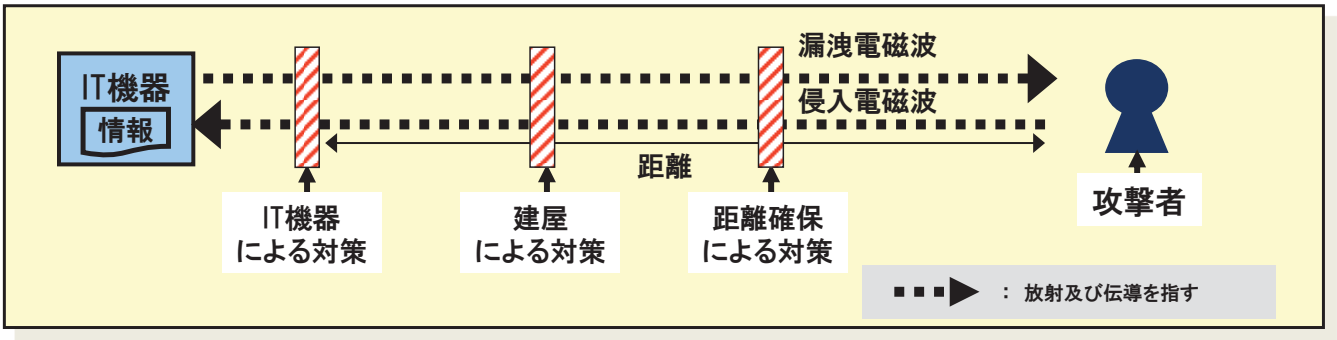
各基準の実現方法

電磁波セキュリティ対策として、以下の二つが要求される。

1. IT機器から漏洩する情報を含む電磁波を安全なレベルまで減衰させること
2. 攻撃者が発生する侵入電磁波を安全なレベルまで減衰させること

これらを実現するためには、IT機器による対策、建屋による対策、距離確保による対策を総合的に行うことが必要である。

対策に含まれる各要素の概念



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

今後の活動

ガイドラインの精度の向上及び運用、そして情報セキュリティの観点から見た電磁波に対する世の中の意識の向上が課題であり、今後の活動方針を検討中

（1）継続的な啓発活動
- 電磁波セキュリティの認知度向上　など

（2）ガイドラインの見直し
- ガイドラインの定期的な見直しについて
- ガイドラインの運用について　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

情報流出の可能性

- アナログ／デジタル記録による物理的持ち出し
- 有線ネットワークのタッピング
- 無線ネットワークの傍受
- ネットワークからの侵入
- スパイウエア、キーロガー
- LEDランプの点滅やレーザーを用いたデータ取得
- 無線機器による転送（音声・画像・データ）
  - 常時転送
  - 蓄積転送システム
- 意図しない、機器からのノイズ輻射に含まれる情報の解析(TEMPEST)

必要とされる場所

- 官公庁
  - 金融等、情報が多大な影響を及ぼす組織
  - 保安上、機密保持が必要な組織
- 自社、組織内のセキュリティ
  - 会議室、役員室、応接室
  - 研究室、企画部門
- セキュアなエリア、サービスを提供する業種
  - ホテル等の会議室
  - 弁護士
  - 病院、金融機関

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！

1.具体的実例

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？

2.これまでの経緯

海外

- 米国におけるTEMPEST対策（研究）への取り組みは1960年代から
- 規格等の作成・運用体制等の構築などの準備ののち、本格的なスタートは1974年であったといわれている
- NATO諸国との連携、NATO以外への流出

↓

「古くて新しい問題」

2.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
  - セキュリティー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

3.最近の動向

- 標準化
  - NDS C0012 電磁シールド室試験方法1998年8月
  - NDS C0013 漏洩電磁波に関する試験法 2003年6月9日
  - ITU-T　SG5
    - K.sec（電磁波セキュリティガイドライン）
    - K.leakage（電磁波による情報漏洩試験法）
    - K.hpem（HPEMによる通信設備要求条件）
  - IEC-SC77C/電気学会：調査
- 海外規格
  - MIL：MIL-STD-220B/285：シールド/フィルタ特性測定の規格
  - Non-MIL：NSTISSAM TEMPEST 1-92 (NSA)

    http://cryptome.org/nstissam1-92a.htm

    NSA/Naxxx-50xx番台

    （NSCSIM5000/NACCSI5004/NACSCI5005）

3.最近の動向

- 「金融機関等によるセキュリティーポリシー策定のための手引き」
  平成11年1月　金融情報システムセンター
- 「情報通信ネットワーク安全・信頼性対策実施登録規定等の整備」
  平成12年11月14日　総務省
- 「地方公共団体における情報セキュリティポリシーに関するガイドライン」
  平成13年3月30日　策定　平成15年3月18日　一部改定
- 「地方公共団体における情報セキュリティ対策に関する調査研究報告書」
  平成14年2月　＜地方公共団体における情報セキュリティ対策に関する調査研究会＞
- 「地域公共ネットワークに係る標準仕様」
  平成14年10月　策定　総務省 情報通信政策局
- 「情報セキュリティ監査制度の運用開始について」（経済産業省）
  個別管理基準（監査項目）策定ガイドライン
  電子政府情報セキュリティ管理基準モデル
- 「住民基本台帳ネットワークシステムの概要」
  （電磁波漏えい対策は、「個人情報保護のための施策」に記載）
- 新情報セキュリティ技術研究会（IST）民間向けのガイドライン
  平成15年10月
- 「政府機関の情報セキュリティ対策のための統一基準」
  平成17年12月

4.脅威の本質とは

テンペストの定義

- 業務における情報保全上の問題となるような、意図的でなく放出される電磁波を抑制すること。実際には、その技術、ノウハウと対策（盾と矛）の両面を指す
- 軍事用語で言うところの、SIGINT（COMINT/ELINT）/HUMINTのうち、ELINTに属すると思われる
- 日本のプレーヤーは案外少ない

画面だけにあらず、シリアル伝送される情報全般と言える

4.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

5.必要な技術

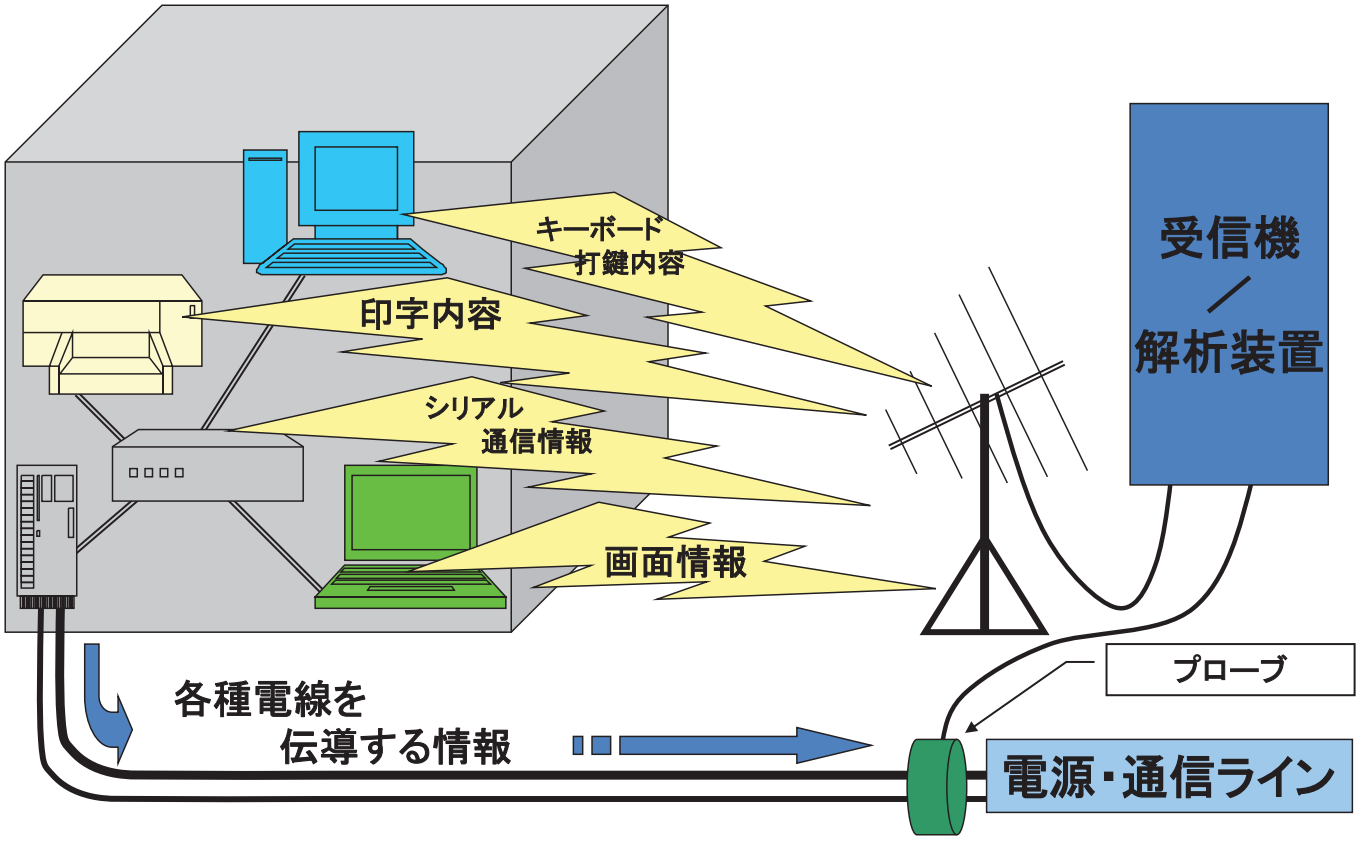
- EMC（ノイズ）に関する技術
  - 計測機器の特性
  - ノイズ発生のメカニズム
- 無線（通信）に関する技術
  - 微弱信号を受信するためのテクニック
  - 電波伝搬の原理、アンテナの知識
  - 受信信号処理の知識
- 端末のハードウエア、各IFのプロトコルに関する技術

6.実現の可能性

- 軍事目的レベル
  - 輸出制限付きながら、日本でも製品は入手可能
  - 億単位
- アマチュアレベル
  - 原理は公知であり、Internetでも入手可能
  - DSPを用いた無線通信機器の普及と性能向上
  - 画像処理なども、PCの性能向上とソフトウエアの充実によって、個人レベルでの実現も可能
  - 数十万円から数百万円

距離と性能はお金のかけ方次第

7.漏洩する原理とインターフェース



12.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！）

13.対策のポイント

- 遠距離まで届く可能性から先に抑える
  - 筐体表面からの輻射は、案外遠くへ届かない場合が多い
  - 伝導する可能性の高い電源／通信ケーブルも考慮する
  - 効率の良いアンテナになる可能性のある周辺機器ケーブルは重要なポイント
- 対策は、なるべく機器の直近で
  - ノイズ対策の基本
- 複合的な対策を効率よく組み合わせる
  - 受信機の能力を考えれば、数dBの減衰量では不十分
  - 一般のユーザ（メーカも含む）がどこのノイズに情報が含まれているかを知ることは困難