CCDSSG

参考資料
重要生活機器連携セキュリティ研究会

生活機器の脅威事例集
Ver1.0

2014年6月13日
重要生活機器連携セキュリティ研究会
（CCDSSG）事務局

本事例集について

CCDSSG

- 自動車、省エネ、医療、AV家電、その他、IT技術を活用した生活機器に対する脅威は日々、増大しています。
- 10年前には、情報システムを狙ったワームがPOS端末にまで影響を与えたことがありましたが（事例C001）、最近ではPOS端末を狙ってカード情報を抜き出す攻撃が登場しています（事例C002）。これは、「①ターゲットが生活機器に拡大」、「②目的が愉快犯から金銭にシフト」という攻撃の傾向を表しています。
- また、10年前の「出荷時のセキュリティ設定が不十分なために脅威にさらされる」という事例（事例C003 ）と類似した脅威が近年も発生しており（事例C004）、メーカ側の意識の課題が伺えます。
- 本事例集は、重要生活機器連携セキュリティ研究会の活動の一環として、過去も含めて代表的な被害事例や攻撃手法の研究を整理することで生活機器に対する脅威の周知と対策促進を目指すものです。

目次

C001. 組込み機器へのワームの感染

分類	実例	分野	組込み機器全般	時期	2003/08	地域	各国

情報源

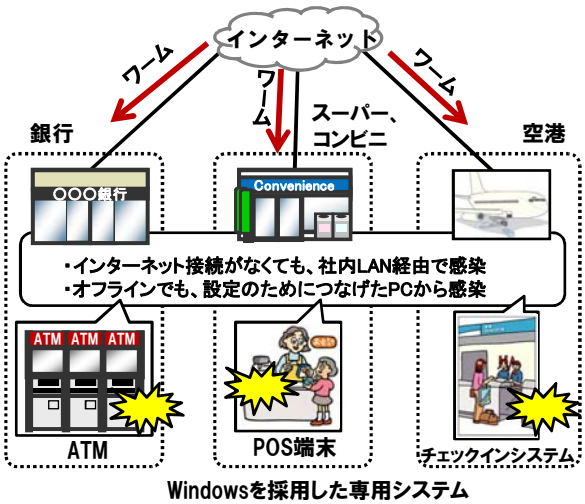
IPA「W32/MSBlaster」ワームに関する情報 http://www.ipa.go.jp/security/topics/newvirus/msblaster.html
IPA「組込みソフトウェアを用いた機器におけるセキュリティ」
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/booklet_manager.pdf

脅威

Windowsの脆弱性を利用したネットワーク型マルウェア(ワーム)が蔓延、Windowsを利用した組込み機器にも感染

概要

・マルウェア(悪意のあるソフトウェア)が組込み機器に影響を与えた初期の事例。
・不審な添付ファイルを開かなければ大丈夫と思われていたウイルスに対し、ネットワークに接続しているだけで感染するワームの登場により、ATM端末、POS端末、空港管制システムなどWindows を採用した様々な組込みシステムが攻撃を受けた。
・機器が直接インターネットに接続していなくてもLAN経由や設定の際につなげたPCから感染し、再起動を繰り返すなどのケースも多く、対策に時間を要した。



Windowsを採用した専用システム

(CCDSSG事務局作成。POS:Point Of Sales)

C002.マルウェアによるPOS上のカード情報の流出

分　類	実例	分野	POS端末	時期	2013/08	地域	米国

情報源

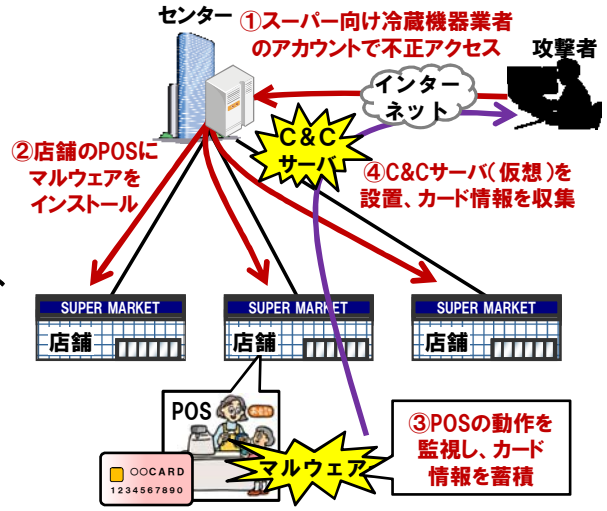
ITmedia記事　http://www.itmedia.co.jp/enterprise/articles/1401/17/news036.html
セキュリティ企業による手口の解説　http://www.barracuda.co.jp/column/detail/122
ビジネス＋IT記事　http://www.sbbit.jp/article/cont1/27507

脅威

スーパーなどのPOS端末を狙ったマルウェアにより、約4000万件のカード情報が流出

概要

・攻撃者は、大手小売りチェーンのWebサーバに侵入し、レジなどのPOS端末上のクレジット・デビッドカード情報を読み出すマルウェア（悪意のあるソフトウェア）「BlackPOS」の亜種をPOS端末にインストール、さらに、社内ネットワークにC&C（コマンド&コントロール）サーバを設置し、カード情報を収集したと見られる。
・侵入は、スーパー向け冷蔵機器業者に対して遠隔管理用に与えられたアカウントを詐取したものと見られている。
・約4,000万件の情報流出に伴うTarget社の直接被害額は約20億ドル、それ以外にも多額の費用がかかる見込み。



（CCDSSG事務局作成。POS：Point Of Sales）

C003. HDDレコーダーの踏み台化

分　類	実例	分野	HDDレコーダー	時期	2004/10	地域	日本

情報源

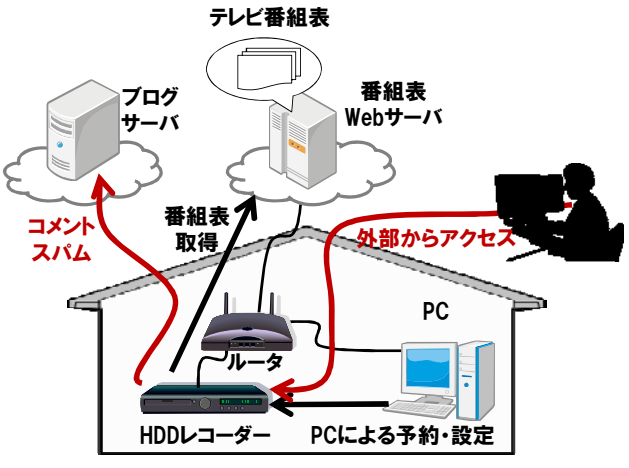
発見者のブログ投稿　http://nlogn.ath.cx/archives/000288.html
インターネットウォッチ http://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html

脅威

セキュリティ設定が無効になっていたHDDレコーダーがスパム攻撃の踏み台化

概　要

・情報家電に対する初期の攻撃事例。
・本機器は、PCからの予約受付のためのWebサーバ機能、テレビ番組表取得のための外部サーバアクセス機能を有していたため、踏み台として利用された模様。
・ID・パスワードによるアクセス制御は、装備されていたものの出荷時には無効となっていた。
・あるブログライターが、自分のブログに国内から大量のコメントスパムが届いていることを不審に思い、分析し、発見。



（CCDSSG事務局作成）

C004. 複合機蓄積データの意図せぬ公開

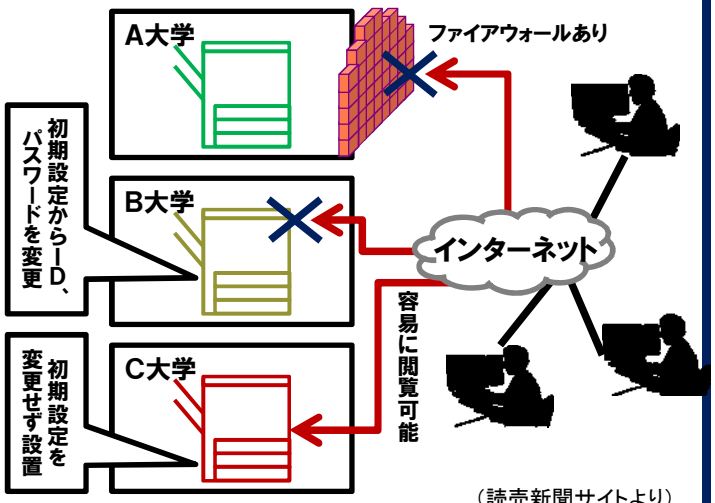
分　類	実例	分野	複合機	時期	2013/11	地域	日本

情報源
「住民票・答案…複合機の蓄積データ、公開状態に」YOMIURI ONLINE（現在はリンク切れ）
セキュリティ通信記事　http://security-t.blog.so-net.ne.jp/2013-11-11
アクセス可能な組込み機器の検索サイト　http://shodanhq.com/

脅威
住民票など、コピープリンタ複合機の蓄積データがインターネット上に公開

概　要

・複数の大学の複合機の蓄積データがインターネットから参照できる状態になっていた。ファイアウォールがなく初期設定からID・パスワードを変更していない場合、外部から容易にアクセスが可能であった。
・蓄積データには、試験答案や住民票、免許証などの個人情報が含まれていたとのこと。
・インターネットに公開された組込み機器を検索するサイトも存在する。



（読売新聞サイトより）

C005. スマート家電からの大量不正メール送信？

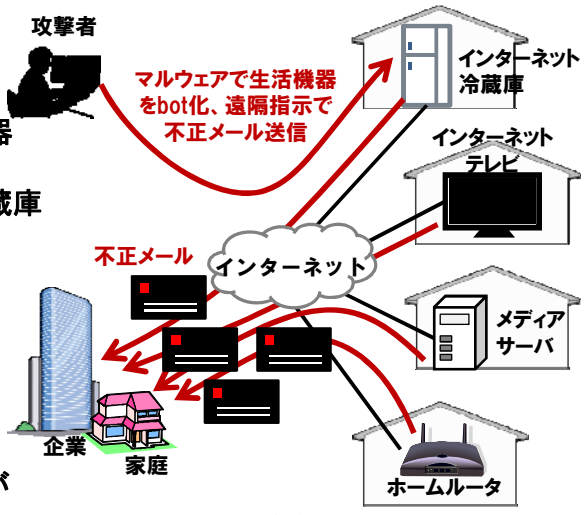
分　類	実例	分野	スマート家電	時期	2014/1	地域	米国

情報源
ITPro記事 http://itpro.nikkeibp.co.jp/article/NEWS/20140120/530845/
元記事 http://www.proofpoint.com/about-us/press-releases/01162014.php
反論記事 http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam

脅威
10万台以上のスマート家電がハッキングされ、大量の不正メールを送信？

概　要

・米セキュリティ企業の調査によれば、2013年末から2014年初に発信されたフィッシング及びスパムメールのうち25%は約10万台の生活機器であり、ホームルータ、マルチメディアセンター、インターネットテレビ、そして少なくとも1台の冷蔵庫が含まれていたとのこと。
・一つのIPアドレスからは10通以下のメールしか送付されていないため、スパム対策も難しく、莫大な生活機器がインターネットに接続される将来に対して懸念が示された。
・別のセキュリティ企業のブログで、スパムメールはすべてWindows OS搭載システムによるものという反論もあったが、組込み用Windows OSが普及している状況も考慮する必要がある。



（CCDSSG事務局作成）

C006. アイロンの中のハッキングチップ

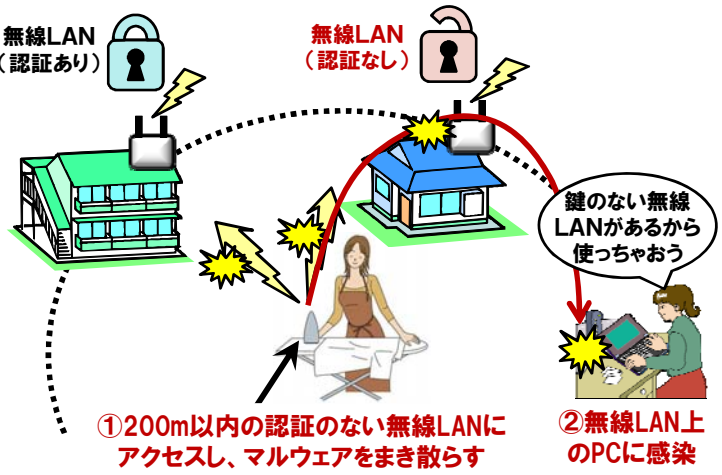
分　類	実例	分野	家電	時期	2013/10	地域	ロシア

情報源
英国BBCサイト(「TV番組ロシア24」の放映内容より)
http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337
(日本語記事　http://gigazine.net/news/20131029-spam-chips-hidden-in-iron/)

脅威
周囲の無線LAN上のPCにマルウェアを撒き散らす、アイロンの中のハッキングチップ

概要

・中国製のアイロンの中に、近隣200m以内の無線LANにアクセスし、同LAN上のPCにマルウェアを撒き散らすチップが埋め込まれていることが発見された。
・同様のものがモバイルフォンや車載カメラでも見つかった模様。
・出荷を停止したが、既に小売店に出荷されたものもあるとのこと。



(CCDSSG事務局作成)

C007. ホテルの電子錠の不正な解錠

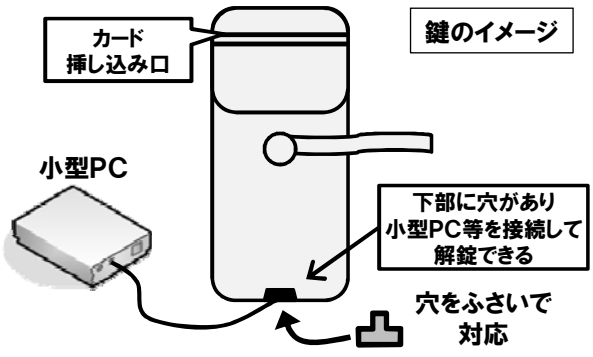
分　類	実例	分野	ビル設備	時期	2012/9	地域	米国

情報源
Black Hatセキュリティカンファレンス論文 http://daeken.com/blackhat-paper
盗難事件 Forbes記事　http://www.forbes.com/sites/andygreenberg/2012/11/26/security-flaw-in-common-keycard-locks-exploited-in-string-of-hotel-room-break-ins/

脅威
ホテルの電子錠の脆弱性を指摘する論文の発表、及びそれに関連すると想定される盗難事件

概要

・Black Hat 2012でホテルの電子錠の脆弱性に関する論文発表あり。電子錠の下部の穴に電子ボードを接続し、電源を供給しつつ、あるアドレス値を送ると、格納された鍵データを入手、解錠することができる。
・2012年9月には盗難事件が発生、鍵を使用した形跡がないことから、ホテルマネージャーはハッキングによるものと推定。
・世界中の400万に上る錠前に影響するため、メーカは下部の穴を塞ぐ部品で対応する予定。



(CCDSSG事務局作成)

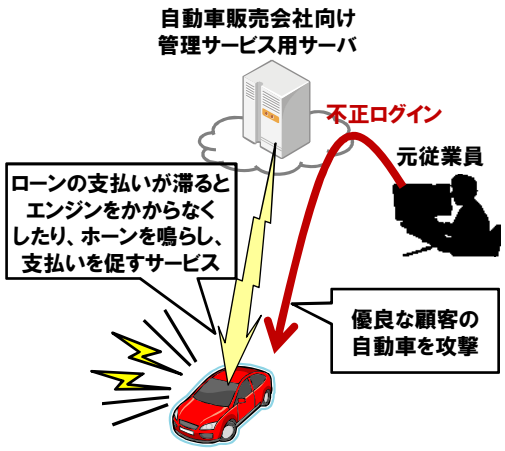
C008. 遠隔イモビライザー機能の不正利用

分　類	実例	分野	自動車	時期	2010/03	地域	米国

情報源	WIRED記事　http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/
脅威	自動車の遠隔管理サーバに不正ログインし、遠隔イモビライザー機能を不正利用

概要

・ローンで販売された自動車の支払いが滞った際にエンジンのエンジンをかからなくしたり、ホーンを鳴らして督促するサービスが悪用され、自動車を利用できなくなったり、真夜中にホーンが鳴らされた。
・販売会社には電話が殺到し、当初原因も分からず、解除も走行もできなかったため、バッテリーを外してレッカーで工場に移動するしかなかったとのこと。
・逮捕された犯人は、前の月に販売会社に人員整理された元従業員で、他の従業員のID/パスワードで不正ログインしていた。



（CCDSSG事務局作成）

C009. タイヤ空気圧モニタ（TPMS）の脆弱性

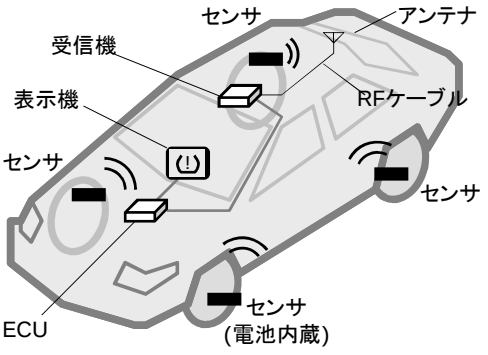
分　類	研究	分野	自動車	時期	2010/08	地域	米国

情報源	MITテクノロジーレビュー http://www.technologyreview.com/news/420168/wireless-car-sensors-vulnerable-to-hackers/
脅威	タイヤ空気圧モニタ（TPMS）の無線通信を傍受して攻撃を行える脆弱性の研究の論文が発表

概要

・米国ではTREAD法によりタイヤ空気圧監視システムTPMS（Tire Pressure Monitoring Systems）の）装着が2007年から完全義務化。
・南カリフォルニア大とラトガーズ大は、TPMSのプロトコル解析に成功、近傍の車両の無線通信と区別するため、車輪毎に32bitの固有IDが割当てられていることを発見。
・車輪IDを読み出すことで、車両を追跡したり、誤った情報の送信により誤った警告灯の表示が可能。攻撃ツールの開発に要した原価は$1,500程度。

TPMSのイメージ



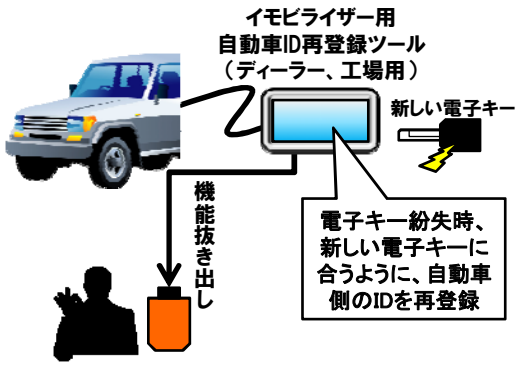
（2011 年度自動車の情報セキュリティ動向に関する調査http://www.ipa.go.jp/files/000014119.pdf より）

C010. イモビカッターによる自動車窃盗

分　類	実例	分野	自動車	時期	2010/11	地域	日本
情報源	「高級車窃盗団、修理道具悪用し電子ロック解除」asahi.com（現在はリンク切れ）						
脅威	自動車のイモビライザーの鍵を入れ替えるメンテナンス用ツールが悪用され、「イモビカッター」として自動車窃盗に利用						

概要

- イモビライザーは、電子キーのIDと自動車のIDを照合する方式となっており、電子キー紛失時には新しい電子キーに合わせて自動車のIDを再登録する必要がある。
- 自動車の整備ツールから、再登録機能を抜き出し、車両のOBD-II（故障診断装置）端子に装着するだけでイモビライザーを解除できるツール「イモビカッター」が中国で製造され、インターネットで販売されている。
- 2012年11月には、イモビカッターを使用して自動車を盗んでいたグループが逮捕された。
- 愛知県では2013年7月から、正当な理由なくイモビカッターを所有することを罰する条例が施行された。



（CCDSSG事務局作成）

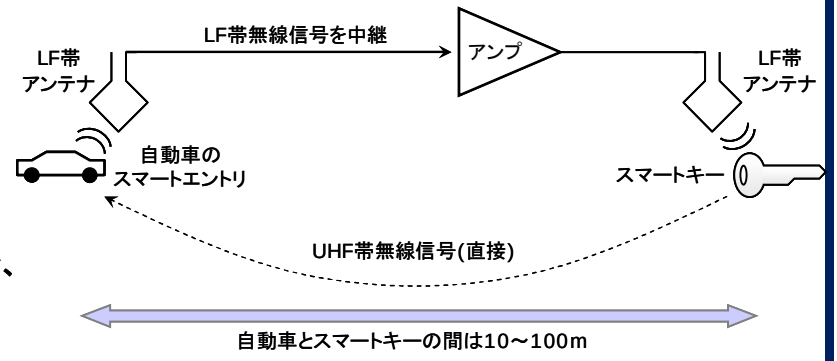
C011. スマートキーに対する無線中継攻撃

分　類	研究	分野	自動車	時期	2010/06	地域	スイス
情報源	チューリッヒ工科大学論文 http://eprint.iacr.org/2010/332						
脅威	スマートキーの無線通信を中継することで、所有者が離れていても動作させる研究の論文が発表						

概要

- スマートキーPKES（Passive Keyless Entry and Start)はキーを携帯して近づくだけで開錠でき、着座してボタンを押すだけでエンジンを始動できる。
- 研究では、キーと自動車間の無線通信を中継することで、所有者が遠隔にいても開錠や始動を行える脅威が指摘された。

無線通信を中継する攻撃のイメージ



（チューリッヒ工科大学論文より）

C012. 遠隔から車載LANへの侵入実験

分　類	研究	分野	自動車	時期	2010/06	地域	米国

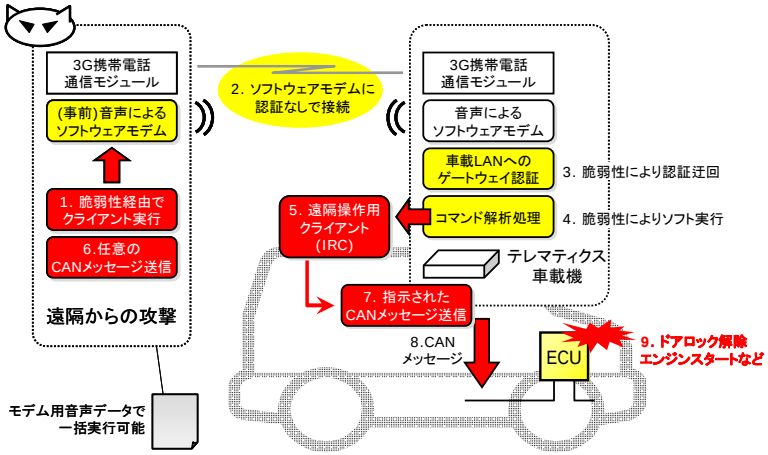
情報源
ワシントン大学Kohno氏ら論文　http://www.autosec.org/pubs/cars-usenixsec2011.pdf
デモビデオ　http://www.youtube.com/watch?v=bHfOzilwXic

脅威
遠隔から車載LANに侵入する実験の論文が発表

概要

・3G携帯電話（自動車との通信はBluetooth経由）、CDによるメディアプレーヤーのアップデートなどを含め広範囲の侵入経路を検証。
・遠隔操作によるドア解錠、テレマティクスユニットの乗っ取りによる特定の自動車内の音声・ビデオ・位置等の記録データの入手についてデモを実施。

遠隔からの攻撃のイメージ



（2011 年度自動車の情報セキュリティ動向に関する調査http://www.ipa.go.jp/files/000024413.pdf より）

C013. PC接続による自動車の不正操作

分　類	研究	分野	自動車	時期	2013/09	地域	米国

情報源
ロイター記事　http://jp.reuters.com/article/topNews/idJPTYE96S04820130729
ARS Technica 記事 http://arstechnica.com/security/2013/07/disabling-a-cars-brakes-and-speed-by-hacking-its-computers-a-new-how-to/
不正操作ビデオ　http://wired.jp/2013/09/05/hack-a-car/

脅威
特定の自動車の車載ネットワークにPCを接続し、不正操作

概要

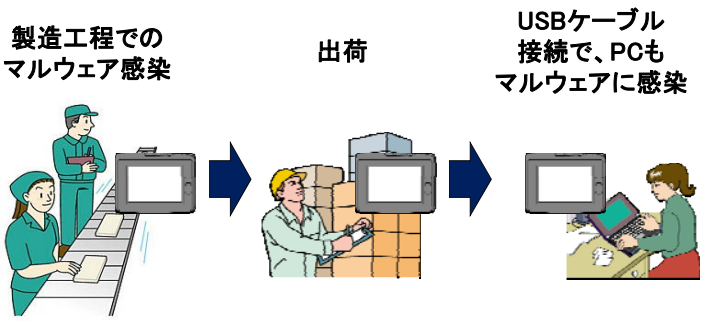
・PCを車載ネットワーク（CAN）に接続し、ECU（電子制御ユニット）にコマンドを送り、自動車を操作。
・時速約130kmで走行中に急ブレーキをかけたり、運転手の意思とは関係なくハンドルを動かしたり、走行中にブレーキを利かなくすることが可能。
・またパネルに誤った数値（例えば時速300km超の速度）を表示させることも可能。
・ビデオでは、ダッシュボードを外していたが、床のシートをはがすことでCANに接続できる車種も多い。

（CCDSSG事務局作成）

C014. マルウェアに感染したカーナビの出荷

分　類	実例	分野	カーナビ	時期	2007/01	地域	オランダ（日本の事例もあり）
情報源	ITmedia記事 http://itpro.nikkeibp.co.jp/article/NEWS/20070130/260032/						
脅威	製造工程でマルウェア感染したカーナビを出荷、PCに接続すると感染拡大						
概要							

・カーナビの一部ロットの製品がマルウェアに感染していることが明らかになり、メーカが対応をアナウンス。
・USBワームのため、OSがWindowsでなくても感染し、本体単独では影響が無いものの、PCとUSBケーブルで接続した際に感染が広がる。
・C社の場合、ユーザの指摘で発覚した模様。



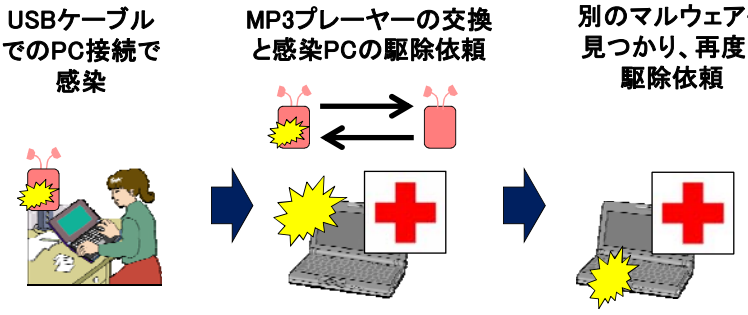
想定される感染経路

（CCDSSG事務局作成）

C015. マルウェアに感染したMP3プレーヤーの配布

分　類	実例	分野	家電	時期	2006/08	地域	日本
情報源	ITPro記事 http://itpro.nikkeibp.co.jp/article/NEWS/20061014/250731/						
脅威	製造工程でマルウェア感染したMP3プレーヤーを景品として配布、PCに接続すると感染拡大、一回駆除を依頼した後、別のマルウェアも見つかる						
概要							

・景品として配布したMP3プレーヤーがマルウェアに感染していることが明らかになり、メーカが対応をアナウンス。
・PCとUSBケーブルで接続した際に感染が広がる。
・後から別のマルウェアも発見され、再度、駆除依頼。



（CCDSSG事務局作成）

C016. 心臓ペースメーカー等の不正操作

分　類	研究	分野	医療機器	時期	2013/08	地域	米国

情報源

米国議会の調査部門である米会計検査院(GAO)のレポート
http://www.gao.gov/assets/650/647767.pdf 19～20P
上記を受けた米国食品医薬品局(FDA)のアナウンス
http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

脅威

無線で遠隔から埋込み型医療機器を不正に操作する研究を基に、行政機関が警告

概要

・埋込み型医療機器の電池寿命は5～10年と長く、利用中に設定変更を行うための無線通信機能が内蔵されているが、保護が不充分。
・米会計検査院(GAO)は、ペースメーカーやインシュリンポンプを遠隔から不正に設定変更する研究(2008～2011年)を基に米国食品医薬品局(FDA)に検討を促した。
・FDAは上記を受け、リスクを医療機器メーカに警告。

(CCDSSG事務局作成)

C017. 標的型攻撃メールによる設計情報漏えい

分　類	実例	分野	企業一般	時期	2005以降	地域	各国

情報源

IPA「標的型メール攻撃』対策に向けたシステム設計ガイド」 http://www.ipa.go.jp/security/vuln/newattack.html
JAXAプレスリリース http://www.jaxa.jp/press/2012/03/20120327_security_j.html

脅威

特定の対象に知人を装うマルウェア付きメールにより、設計情報などが情報が漏えい

概要

実際に発生した事例

・不特定多数にマルウェアを撒く攻撃と異なり、特定の対象を狙ったメール攻撃。
・設計情報やソースコード、バグデータベースなどの漏えい事例あり。近年ではロケット開発機関が攻撃され、マルウェアに感染しており、情報が漏えいした可能性がある。
・IPAの標的型攻撃メール対策の調査報告書のpdfにマルウェアを仕込み、IPA担当者名で政府関係組織に送付した事例もある。

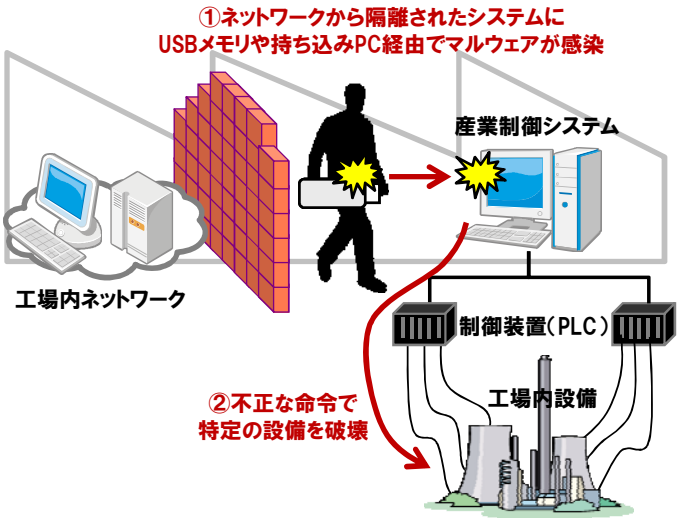
(IPA資料(http://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf)を参考にCCDSSG事務局作成)

参考）マルウェアによる工場の生産設備の破壊

分　類	実例	分野	制御システム	時期	2010	地域	イラン
情報源	Stuxnet の脅威と今後のサイバー戦の様相(検証論文) http://www.bsk-z.or.jp/kenkyucenter/pdf/23kennshouronnbunnjyushousakuhinn.pdf						
脅威	ネットワークから隔離されている制御システムにマルウェアを感染させ、設備を破壊						

概　要

- ネットワークから隔離されている産業制御システムにUSBメモリや持ち込みPC経由でマルウェアが感染、不正な命令を実行させられた結果、工場の設備を大規模に破壊された。
- マルウェアには電動機の回転数制御用インバータの周波数を変更して回転数を不正に操作する機能が備わっていた。また目立たないよう、他の機能は攻撃しない仕様になっていた。
- マルウェアは未知の複数の脆弱性を突いたものであり、完全な防御は困難であったと指摘されている。



（論文の情報を基にCCDSSG事務局作成）

- コンテンツ提供：株式会社ユビテック　ユビキタス研究所
- 問い合わせ先：
  - 株式会社ユビテック　ユビキタス研究所　伊藤、遠山、志田
  - TEL：03-5487-5590　E-MAIL: ubilab-info@ubiteq.co.jp