

海外動向

JPCERT コーディネーションセンター
早期警戒グループ
小宮山 功一郎

講演者は、

- ◆ 前の人と同じです
 - テーマはセキュリティに関する海外動向
 - 脆弱性
 - 脅威(サイバー攻撃と標的型攻撃など)
- 時間が短いのでポイントを絞り込んで

CIOの関心

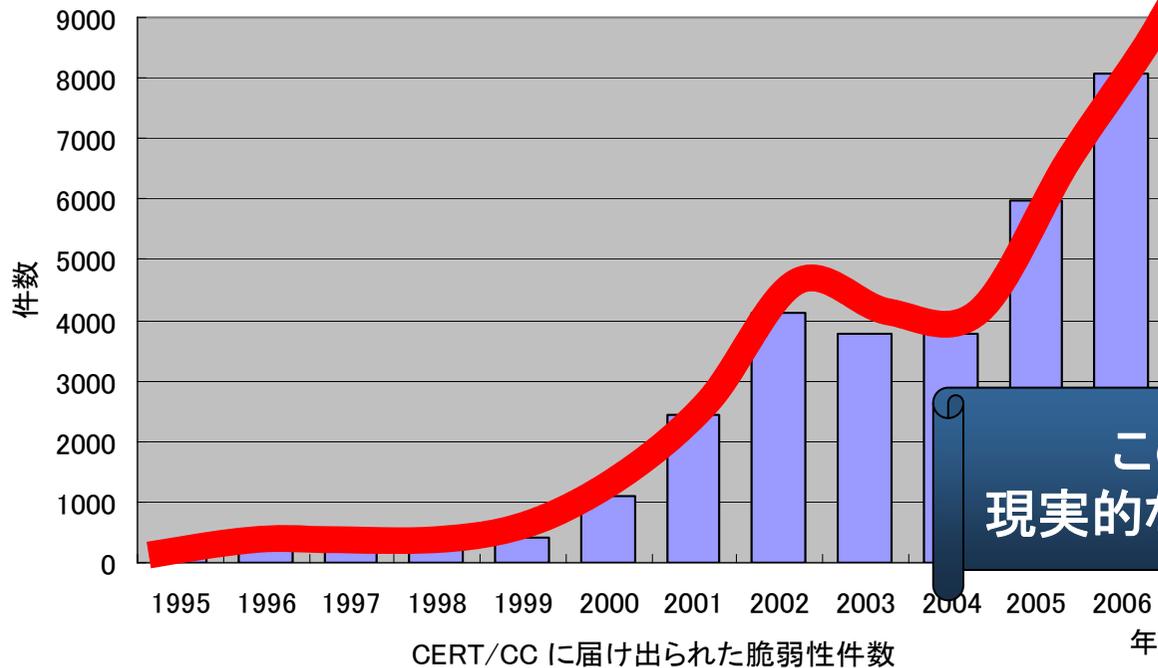
- セキュリティ業界の企業合併
 - 市場が成熟
 - セキュリティ関連企業のM&A成立件数
- CIOの関心
 - セキュリティへの関心薄れる

脆弱性

- ~どのようなセキュリティホールが見つまっているのか~

□ ソフトウェア脆弱性の発見は増加の一途

- 年間8,000件あまりの脆弱性
(2年間で2倍、10年間で20倍以上)



このままでは
現実的な対応が困難に!

脆弱性情報取引サイト

WabiSabiLabi

Open Office の脆弱性:

2000ユーロ (約30万円)

2007年 7月27日

The screenshot shows the WabiSabiLabi website interface. At the top, there is a navigation bar with links for 'Home', 'About', 'Contact', 'FAQ', and 'Privacy'. Below the navigation bar is the WabiSabiLabi logo with the tagline 'CLOSED TO ZERO RISK'. A yellow warning box contains text about the site's purpose and a disclaimer. Below the warning box is a table listing vulnerabilities.

Order	Vendor Name	Title	System	Impact type	CVSS
1	Open Office	Local User Enumeration	Open Office	Denial of Service	5.0
2	Open Office	Local Privilege Escalation	Open Office	Denial of Service	5.0
3	Open Office	OpenOffice (OO) Plug-in (Command Injection)	Open Office	Denial of Service	5.0
4	Open Office	OpenOffice (OO) Plug-in	Open Office	Denial of Service	5.0
5	Open Office	OpenOffice (OO) Plug-in (Command Injection)	Open Office	Denial of Service	5.0

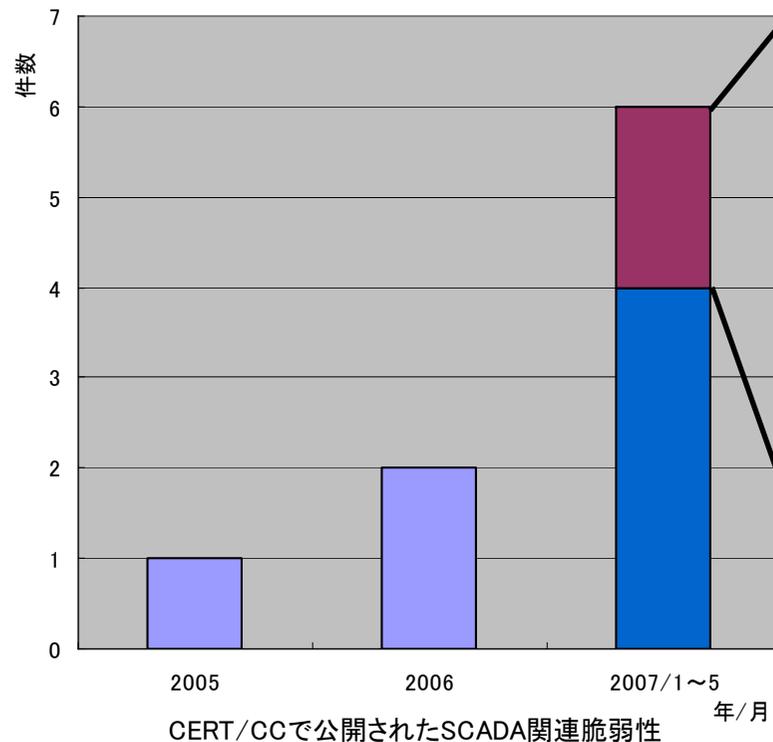
脆弱性情報の売買取引市場の形成

脆弱性/攻撃コード	価格	情報ソース
"ある"攻撃コード	\$200,000 - \$250,000	米政府当局者
Internet Explore	\$60,000 - \$120,000	H.D. Moore
Vista exploit	\$50,000	Raimund Genes, Trend Micro
Weaponized exploit	\$20,000 - \$30,000	David Maynor, SecureWorks
ZDI, iDefense purchases	\$2,000-\$10,000	David Maynor, SecureWorks
WMF exploit	\$4000	Alexander Gostev, Kaspersky
Microsoft Excel	\$1200	Ebay auction site
Mozilla	\$500	Mozilla bug bounty program

The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales
Charlie Miller, PhD, CISSP

SCADAシステムの脆弱性

□ 増加するSCADAシステム
関連脆弱性



□ 日本でも情報を公開

- [JVNVU#296593](#):
NETxAutomation 社製 NETxEIB OPCServerに
OPC server handle を適切に処理できない脆弱性
- [JVNVU#202345](#):
デバイスエクスプローラMELSEC OPC サーバに
バッファオーバーフローの脆弱性
- [JVNVU#346577](#):
デバイスエクスプローラ MODBUS OPC サーバに
バッファオーバーフローの脆弱性
- [JVNVU#926551](#):
デバイスエクスプローラ TOYOPUC OPC サーバに
バッファオーバーフローの脆弱性
- [JVNVU#581889](#):
デバイスエクスプローラ SYSMAC OPC サーバに
バッファオーバーフローの脆弱性
- [JVNVU#907049](#):
デバイスエクスプローラ FA-M3 OPC サーバに
バッファオーバーフローの脆弱性
- [JVNVU#347105](#):
デバイスエクスプローラ HIDIC OPC サーバに
バッファオーバーフローの脆弱性

脅威

サイバー攻撃と標的型攻撃について

多国間でサイバー攻撃が行われている?

- Web,新聞,雑誌などで色々な報道がされていますが...
- どうなってる?
 - 中国(人民解放軍?)が西側諸国(アメリカ、ドイツ、フランス、NZ)の政府に攻撃
 - マルウェアの情報送信先/フォントの設定/開発ツール
 - エストニアへのサイバー攻撃
 - CERT-EEの調査

慎重な判断/対応を!

標的型攻撃

- 攻撃の対象が限定
- メールを使った攻撃
 - Targeted Trojan AttackとSpear Phishing
 - 対象: 政府機関、軍、企業の重役や経理担当、航空産業
- 被害額の推定が困難

標的型攻撃への対策

- メールのなりすましを防ぐ
 - SPF, DKIM, メッセージ署名
- 特定の添付ファイルをメールゲートウェイで遮断
- 標的型攻撃への訓練 = 予防接種
 - 社員や職員を対象に疑似攻撃
 - [New York State Office](#) (アメリカ)
 - [IRS](#) (アメリカ)
 - [TWNCERT](#) (台湾)

お問い合わせ先

□ JPCERTコーディネーションセンター

- Email: office@jpcert.or.jp
- Tel: 03-3518-4600
- <http://www.jpcert.or.jp/>

□ インシデント報告

- Email: info@jpcert.or.jp
PGP Fingerprint : BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
- 報告様式
<http://www.jpcert.or.jp/form/>