keep reinventing

HPのセキュリティイノベーション と米国事例に学ぶデバイス調達戦略

Boris Balacheff,
HP Fellow & VP,
Chief Technologist for Security Research and Innovation

東京　2018年9月14日

サイバーセキュリティは
破壊的な力を持つ

2021年に
世界のサイバー犯罪
は6兆ドルの問題
となる[1]

2016年に世界で
1,700件以上の
重大な情報漏洩
があった[1]

[1] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

サイバーセキュリティの課題

攻撃者は
進化している

攻撃の洗練度は
向上している

問題は攻撃が成功**するかどうか**ではなく、
いつ成功するかということである

エンドポイントデバイスは
防御の最前線

エンタープライズ
データーセンターや
クラウドサービス

エンドポイントデバイスセキュリティの2つのポイント

セキュアなデバイス

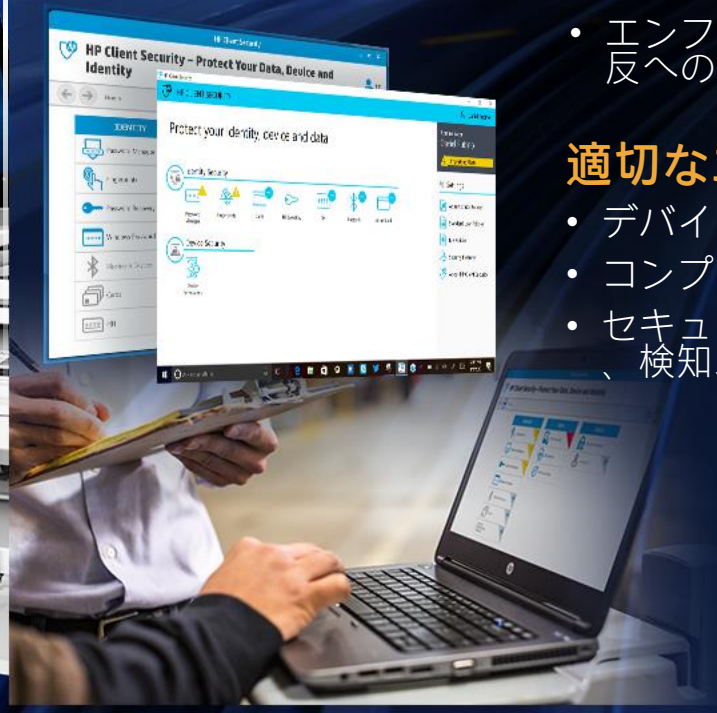
理想的:

最新の脅威に対応した最先端のハードウェア設計

最低限:

最新のセキュリティ標準への対応

デバイスセキュリティの管理



適切なソフトウェアで

- 安全な展開とプロビジョニング
- 継続的な管理とモニタリング
- エンフォースとコンプライアンス違反への対応

適切なエクスペリエンス

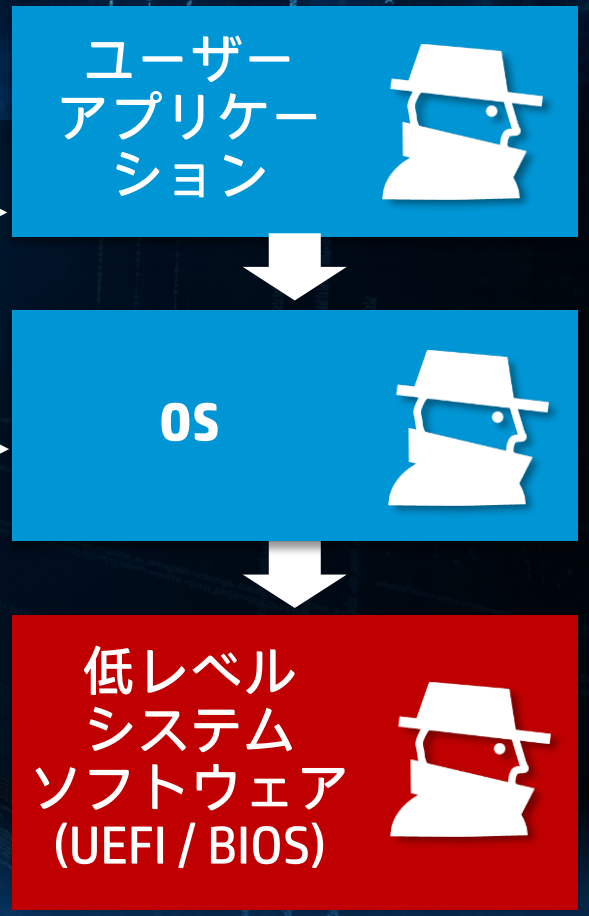
- デバイスのセキュリティ状態の把握
- コンプライアンスの管理とモニター
- セキュリティ・インシデントの分析、検知、対応

エンドポイントセキュリティの脅威の現状

攻撃の経済性と
最近のマルウェアの傾向

攻撃者のエントリーポイント

- 人的攻撃
- ネットワーク経由の攻撃
- 物理アクセス 経由の攻撃



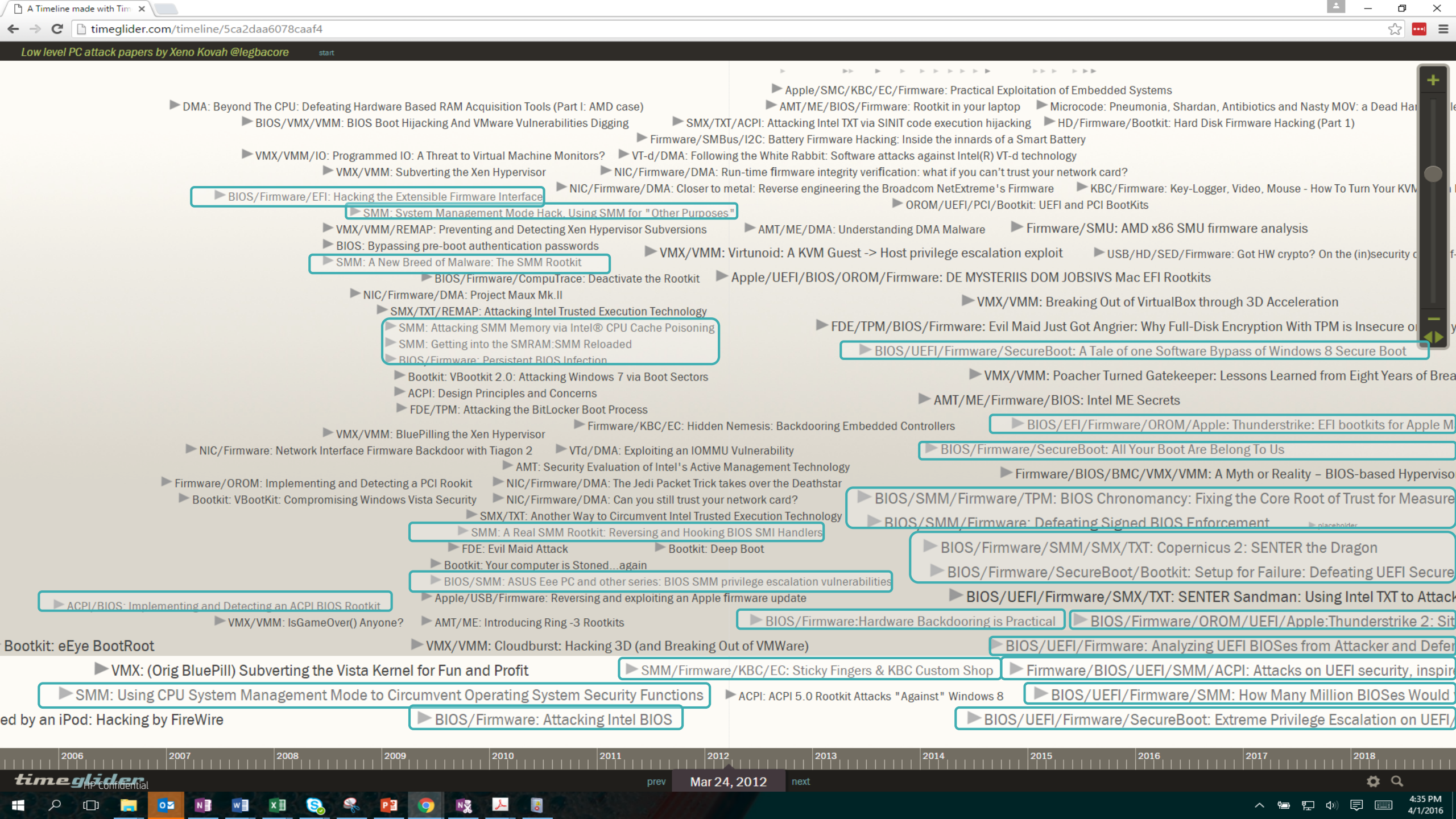
BIOS Root Kit の例

“Hacking Team” マルウェア

…セキュリティの研究者グループは“Hacking team”がRCS（リモートコントロールシステム）エージェントをターゲットシステムにインストールする際にUFEI BIOS Rootkitを利用していることを発見した。
http://thehackernews.com/2015/07/hacking-uefi-bios-rootkit.html

Mebromi

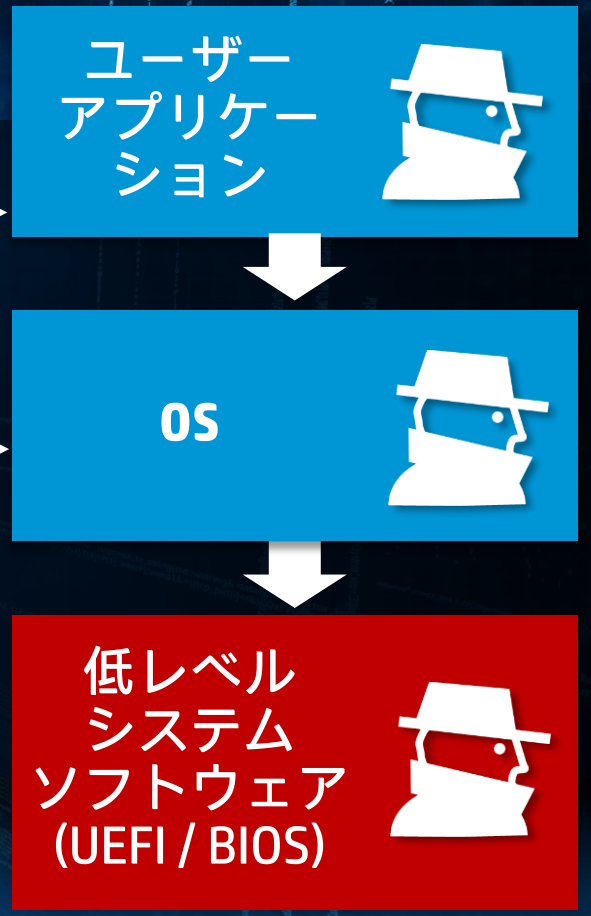
…Trojan.Mebromi という脅威はAward BIOSに悪意のあるコンポーネントを追加し、MBRの前段階からシステムの制御を奪うことを可能にする。
http://www.symantec.com/connect/blogs/bios-threat-showing-again


A Timeline made with Tim
timeglider.com/timeline/5ca2daa6078caaf4
Low level PC attack papers by Xeno Kovah @legbacore
start
Apple/SMC/KBC/EC/Firmware: Practical Exploitation of Embedded Systems
DMA: Beyond The CPU: Defeating Hardware Based RAM Acquisition Tools (Part I: AMD case)
AMT/ME/BIOS/Firmware: Rootkit in your laptop
Microcode: Pneumonia, Shardan, Antibiotics and Nasty MOV: a Dead Ha
BIOS/VMX/VMM: BIOS Boot Hijacking And VMware Vulnerabilities Digging
SMX/TXT/ACPI: Attacking Intel TXT via SINIT code execution hijacking
HD/Firmware/Bootkit: Hard Disk Firmware Hacking (Part 1)
Firmware/SMBus/I2C: Battery Firmware Hacking: Inside the innards of a Smart Battery
VMX/VMM/IO: Programmed IO: A Threat to Virtual Machine Monitors?
VT-d/DMA: Following the White Rabbit: Software attacks against Intel(R) VT-d technology
VMX/VMM: Subverting the Xen Hypervisor
NIC/Firmware/DMA: Run-time firmware integrity verification: what if you can't trust your network card?
BIOS/Firmware/EFI: Hacking the Extensible Firmware Interface
NIC/Firmware/DMA: Closer to metal: Reverse engineering the Broadcom NetExtreme's Firmware
KBC/Firmware: Key-Logger, Video, Mouse - How To Turn Your KVM
OROM/UEFI/PCI/Bootkit: UEFI and PCI BootKits
SMM: System Management Mode Hack, Using SMM for "Other Purposes"
VMX/VMM/REMAP: Preventing and Detecting Xen Hypervisor Subversions
AMT/ME/DMA: Understanding DMA Malware
Firmware/SMU: AMD x86 SMU firmware analysis
BIOS: Bypassing pre-boot authentication passwords
VMX/VMM: Virtunoid: A KVM Guest -> Host privilege escalation exploit
USB/HD/SED/Firmware: Got HW crypto? On the (in)security
SMM: A New Breed of Malware: The SMM Rootkit
BIOS/Firmware/CompuTrace: Deactivate the Rootkit
Apple/UEFI/BIOS/OROM/Firmware: DE MYSTERIIS DOM JOBSIVS Mac EFI Rootkits
NIC/Firmware/DMA: Project Maux Mk.II
VMX/VMM: Breaking Out of VirtualBox through 3D Acceleration
SMX/TXT/REMAP: Attacking Intel Trusted Execution Technology
FDE/TPM/BIOS/Firmware: Evil Maid Just Got Angrier: Why Full-Disk Encryption With TPM is Insecure o
SMM: Attacking SMM Memory via Intel® CPU Cache Poisoning
SMM: Getting into the SMRAM:SMM Reloaded
BIOS/Firmware: Persistent BIOS Infection
BIOS/UEFI/Firmware/SecureBoot: A Tale of one Software Bypass of Windows 8 Secure Boot
Bootkit: VBootkit 2.0: Attacking Windows 7 via Boot Sectors
VMX/VMM: Poacher Turned Gatekeeper: Lessons Learned from Eight Years of Brea
ACPI: Design Principles and Concerns
AMT/ME/Firmware/BIOS: Intel ME Secrets
FDE/TPM: Attacking the BitLocker Boot Process
Firmware/KBC/EC: Hidden Nemesis: Backdooring Embedded Controllers
BIOS/EFI/Firmware/OROM/Apple: Thunderstrike: EFI bootkits for Apple M
VMX/VMM: BluePilling the Xen Hypervisor
NIC/Firmware: Network Interface Firmware Backdoor with Tiagon 2
VTd/DMA: Exploiting an IOMMU Vulnerability
BIOS/Firmware/SecureBoot: All Your Boot Are Belong To Us
AMT: Security Evaluation of Intel's Active Management Technology
Firmware/BIOS/BMC/VMX/VMM: A Myth or Reality – BIOS-based Hyperviso
Firmware/OROM: Implementing and Detecting a PCI Rookit
NIC/Firmware/DMA: The Jedi Packet Trick takes over the Deathstar
BIOS/SMM/Firmware/TPM: BIOS Chronomancy: Fixing the Core Root of Trust for Measure
Bootkit: VBootKit: Compromising Windows Vista Security
NIC/Firmware/DMA: Can you still trust your network card?
SMX/TXT: Another Way to Circumvent Intel Trusted Execution Technology
BIOS/SMM/Firmware: Defeating Signed BIOS Enforcement
SMM: A Real SMM Rootkit: Reversing and Hooking BIOS SMI Handlers
FDE: Evil Maid Attack
Bootkit: Deep Boot
BIOS/Firmware/SMM/SMX/TXT: Copernicus 2: SENTER the Dragon
Bootkit: Your computer is Stoned...again
BIOS/Firmware/SecureBoot/Bootkit: Setup for Failure: Defeating UEFI Secure
BIOS/SMM: ASUS Eee PC and other series: BIOS SMM privilege escalation vulnerabilities
Apple/USB/Firmware: Reversing and exploiting an Apple firmware update
BIOS/UEFI/Firmware/SMX/TXT: SENTER Sandman: Using Intel TXT to Attack
ACPI/BIOS: Implementing and Detecting an ACPI BIOS Rootkit
VMX/VMM: IsGameOver() Anyone?
AMT/ME: Introducing Ring -3 Rootkits
BIOS/Firmware:Hardware Backdooring is Practical
BIOS/Firmware/OROM/UEFI/Apple:Thunderstrike 2: Sit
Bootkit: eEye BootRoot
VMX/VMM: Cloudburst: Hacking 3D (and Breaking Out of VMWare)
BIOS/UEFI/Firmware: Analyzing UEFI BIOSes from Attacker and Defer
VMX: (Orig BluePill) Subverting the Vista Kernel for Fun and Profit
SMM/Firmware/KBC/EC: Sticky Fingers & KBC Custom Shop
Firmware/BIOS/UEFI/SMM/ACPI: Attacks on UEFI security, inspir
SMM: Using CPU System Management Mode to Circumvent Operating System Security Functions
ACPI: ACPI 5.0 Rootkit Attacks "Against" Windows 8
BIOS/UEFI/Firmware/SMM: How Many Million BIOSes Would
ed by an iPod: Hacking by FireWire
BIOS/Firmware: Attacking Intel BIOS
BIOS/UEFI/Firmware/SecureBoot: Extreme Privilege Escalation on UEFI
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
timeglider
HP Confidential
prev
Mar 24, 2012
next
4:35 PM
4/1/2016

攻撃の経済性と
最近のマルウェアの傾向

攻撃者のエントリーポイント

- 人的攻撃
- ネットワーク経由の攻撃
- 物理アクセス 経由の攻撃



新たな攻撃対象になってきた

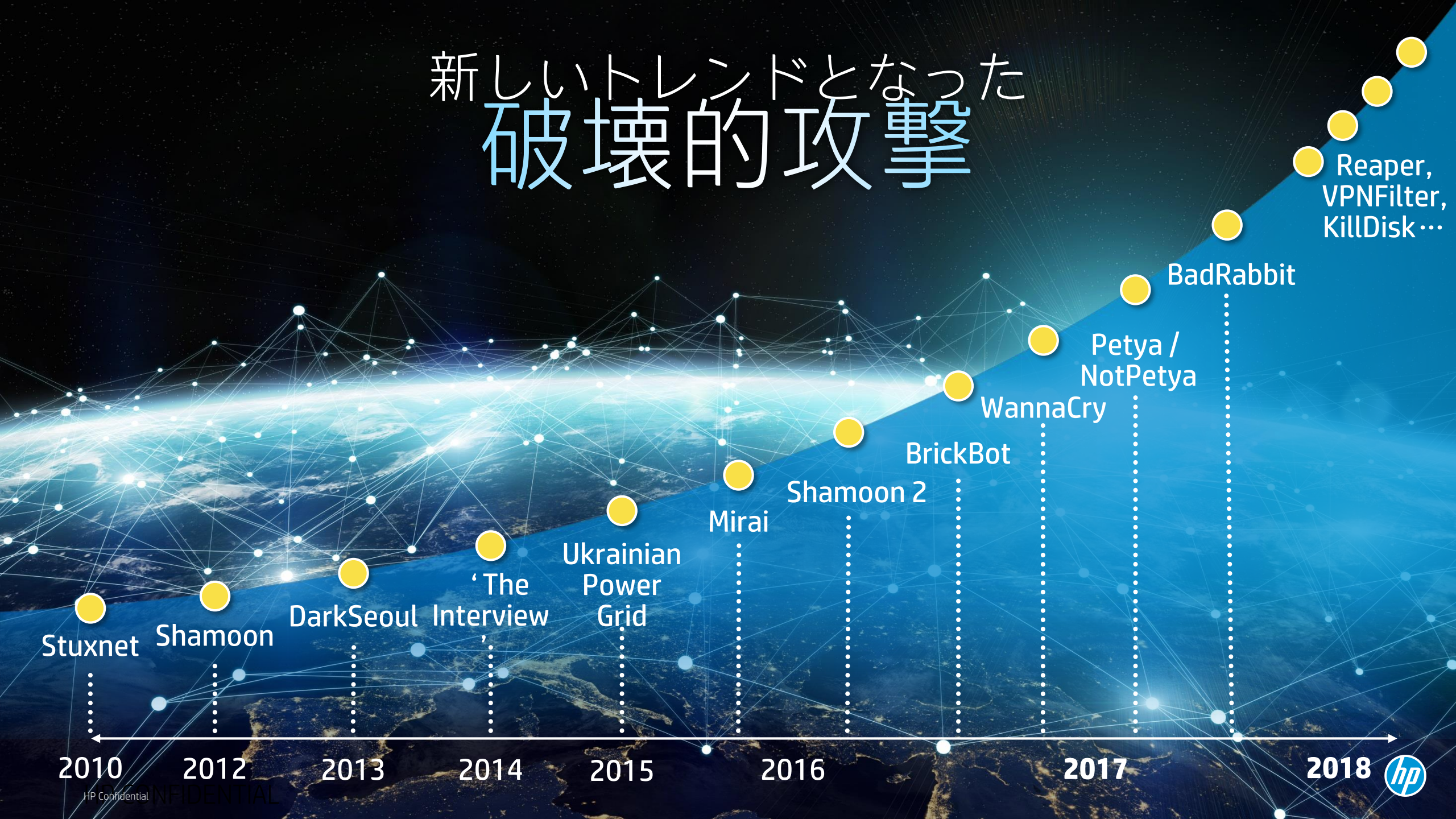
接続されたデバイス

容易なセキュアでないプリンターのハッキング

“我々はプリンターを最初の足掛かりとして多くの企業に侵入してきた。プリンターから始めてActive Directoryを探し出し、プリンターのアカウントで検索をかけると、見つかった！宝の山だ…”

PETER KIM
業界トップの 侵入テスター、ハッカー、著者

新しいトレンドとなった
破壊的攻撃



これらのトレンドが何を意味し我々は何ができるのか？

サイバーレジリエンスのための設計

ハードウェアから サイバーセキュリティを創りこむ

ソフトウェア/ネットワーク
セキュリティは
十分ではない

ハードウェア
からスタートすべき

HPのH/Wにより強制されたサイバーレジリエンス

HP Sure Click

HP Sure Run

HP Sure Recover

HP Sure Start

H/Wがセキュアなソフトウェアの隔離をサポート
（安全なブラウジングと文書の扱いのため）

H/Wでキーとなるセキュリティ S/Wの永続性を
監視し強制する

H/Wベースの安全なフルOSリカバリ
（ローカル or ネットワーク経由）

H/Wでファームウェアの完全性の侵害を検知
し自己回復

専用のセキュリティH/W
（第三者機関で認定）

デバイスの選択は
セキュリティの意思決定である

HPのエンドポイントにおける
セキュリティリーダーシップ

2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

標準化 TPMデバイスセキュリティ標準の立案と (ISO 11889)

標準化 TCG 技術委員会の議長

認定TPM初出荷 業界初

暗号化による安全なBIOS 更新 業界初

標準化 BIOS セキュリティの標準化 (NIST SP800-147, ISO 19678)

業界初 自己回復BIOS (PC & Print)

業界初 ファームウェア侵入検知(PC & Print)

業界初 プリンタマルウェアの振る舞い検知

業界初 プリンタセキュリティサービス

業界初 PC OSとソフトウェアのレジリエンス

プラットフォームF/Wのレジリエンスのガイドライン (NIST SP800-193)

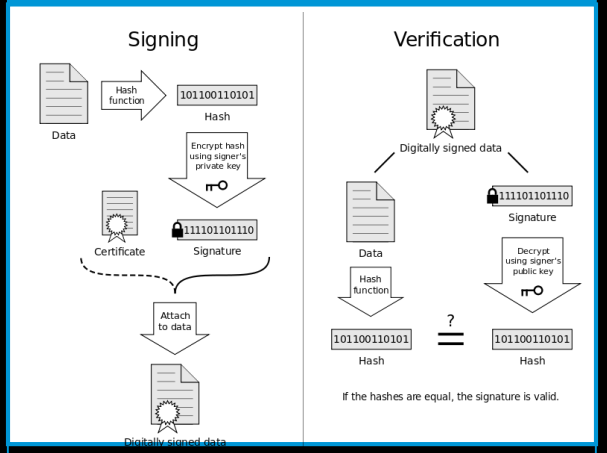
標準化

デバイスセキュリティの要件を定義する

- 最低限：デバイスセキュリティの標準
  - SP 800-147 （ISO 19678） - BIOSのセキュリティ
  - SP 800-193 - プラットフォームファームウェアのレジリエンス
  - SP 800-88 - セキュアイレース
  - TCG のTrusted Platform Module（ISO 11889）
  - H/Wのルート・オブ・トラストに第三者機関による認定を要求する
- 理想的：最新の脅威に対応する
  - 標準以上
  - NIST CyberSecurity FrameworkとNIST SP800-53を用いて最新のセキュリティの導入を検討する

PC BIOSセキュリティのためのNIST SP800-147

正真性

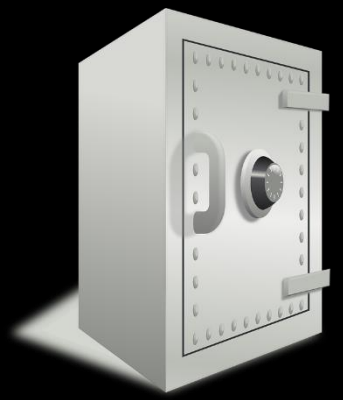


暗号技術で
署名されたコード

完全性

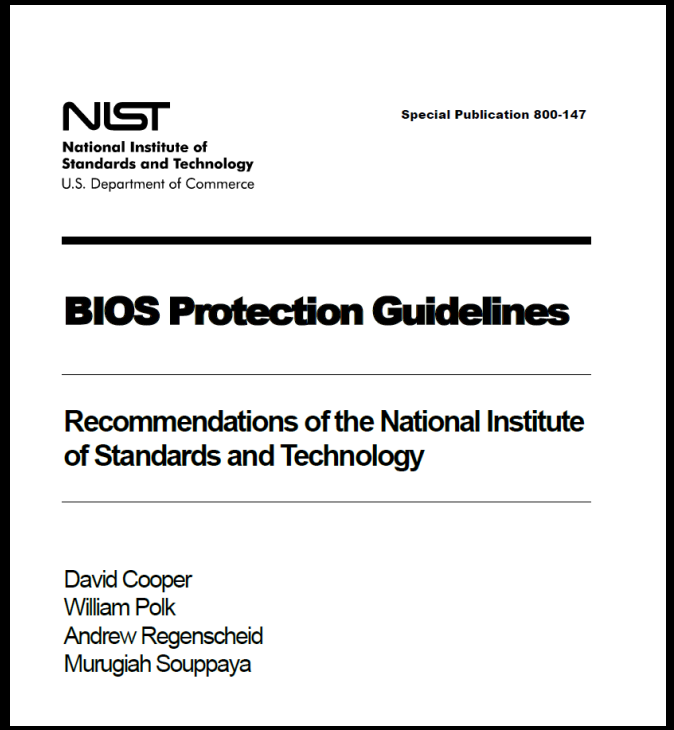
意図しないあるいは
悪意のある変更から
の保護

非バイパス性



認証されたアップ
デートプロセス

NIST Special Publication
800-147
2011年4月


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-147

BIOS Protection Guidelines

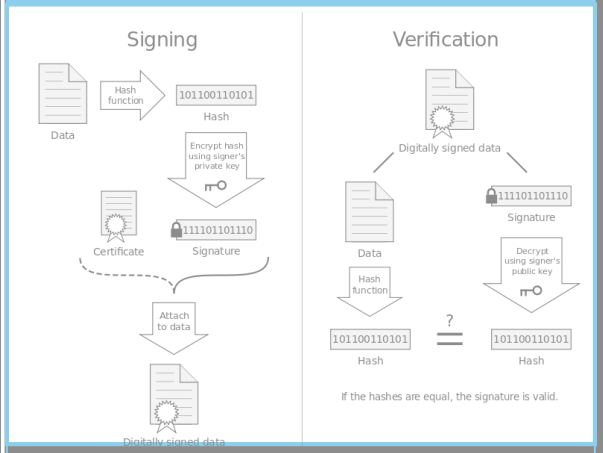
Recommendations of the National Institute of Standards and Technology

David Cooper
William Polk
Andrew Regenscheid
Murugiah Souppaya

または
ISO/IEC 19678:2015

ファームウェアレジリエンスのための新ガイドラインNIST SP800-193

正真性

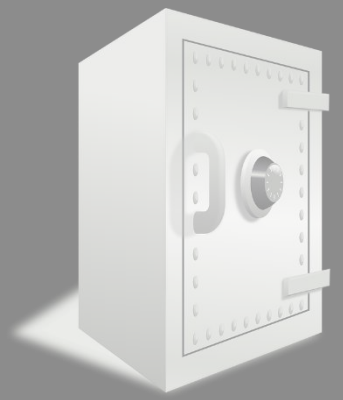


暗号技術で
署名されたコード

完全性

意図しないあるいは
悪意のある変更から
の保護

非バイパス性



認証されたアップ
デートプロセス

検知＆復旧

セキュアで自動化され
大規模に対応する
検知＆回復

NIST Cybersecurity Framework とSP 800-53の利用
デバイスセキュリティを全社的サイバーセキュリティ獲得に活用する

特定(ID)
システム、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深める。

防御 (PR)
重要インフラサービスの提供を確実にするための適切な保護対策を検討し、実施する。

検知 (DE)
サイバーセキュリティイベントの発生を検知するための適切な対策を検討し、実施する。

対応 (RS)
検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し、実施する。

復旧 (RC)
レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを復旧するための適切な対策を検討し、実施する。

ファームウェアやハードウェアの完全性の予防、検知、復旧の重要性は複数のセキュリティ対策に及び（PR-DS6、PR-DS8、…）、その具体的対策はSP800-53に記述されている。

SP 800-53 SI-7 ソフトウェア・ファームウェア・情報の完全性

SI-7 (1)ソフトウェア、ファームウェア、および情報の完全性 | 完全性チェック

SI-7 (2)ソフトウェア・ファームウェア・情報の完全性 | 完全性違反の自動通知

SI-7 (5)ソフトウェア、ファームウェア、および情報の完全性 | 自動化された、完全性違反に対する対応

SI-7 (7)ソフトウェア、ファームウェア、および情報の完全性 | 検知と対応の一体化

セキュリティは文化

将来の脅威は
さらなる研究を必要とする

医療
製造、…

暗号技術

AI 対 AI

まとめ

- 低レベルのデバイスのファームウェアへの攻撃が増加
- デバイスの選択はセキュリティの意思決定である
- 新しいデバイスのハードウェアとファームウェアはこれからの脅威に備えるためにレジリエントであるべき
- デバイスの調達はセキュリティの要件を含むべき
  - 最低限のレベルはセキュリティ標準への準拠
  - 理想的レベルは最新の脅威に対応可能なセキュリティ


ありがとうございました