2016年11月

2017年の脅威予測

McAfee Labs

Intel Securityが2017年の脅威予測を行いました。

ランサムウェア

来年の中頃にピークを迎え、その後は減少していく

2016年のランサムウェアの動向

IoTデバイスに対するランサムウェアの攻撃

すぐに使えるランサムウェア

ランサムウェアのアフィリエイトプログラム

サービスとしてのランサムウェア

ランサムウェアの総数は2016年に80%増加

ランサムウェアのソース コード

セキュリティ業界の対応

捜査機関による取締り

WildFire ランサムウェアの阻止

Shadeランサムウェアの阻止

ランサムウェア対策技術

不正な暗号化の検出

動作監視技術

コラボレーション

ハードウェアに対する攻撃

2017年はハードウェア、システム ファームウェア、仮想マシンに対する攻撃が増加する

アプリケーションよりもハードウェアやファームウェアに対する攻撃が強化される

増大	ハードウェア/仮想マシン	先に実行
	プラットフォームのファームウェア（BIOS/UEFI）	
	ブート ローダー/マスター ブート レコード	
	オペレーティング システム	
減少	アプリケーション	後で実行

ハードウェアとファームウェアの既知の脆弱性

マイクロプロセッサー	DRAM	仮想マシン
システム ファームウェア	ハードドライブ	USBデバイス
ネットワーク カード	ホーム ルーター	プリンター

ソーシャル エンジニアリングによる攻撃

機械学習がソーシャル エンジニアリングによる攻撃を加速化させる

1 データ収集
データ侵害、ソーシャル メディア、公開情報

2 抽出、変換、読み込み、機能選択、生成
機械学習モデルを習得

3 目標捕捉
機械学習による予測

4 最初の接触
良く知られたソーシャル エンジニアリングの手口を利用

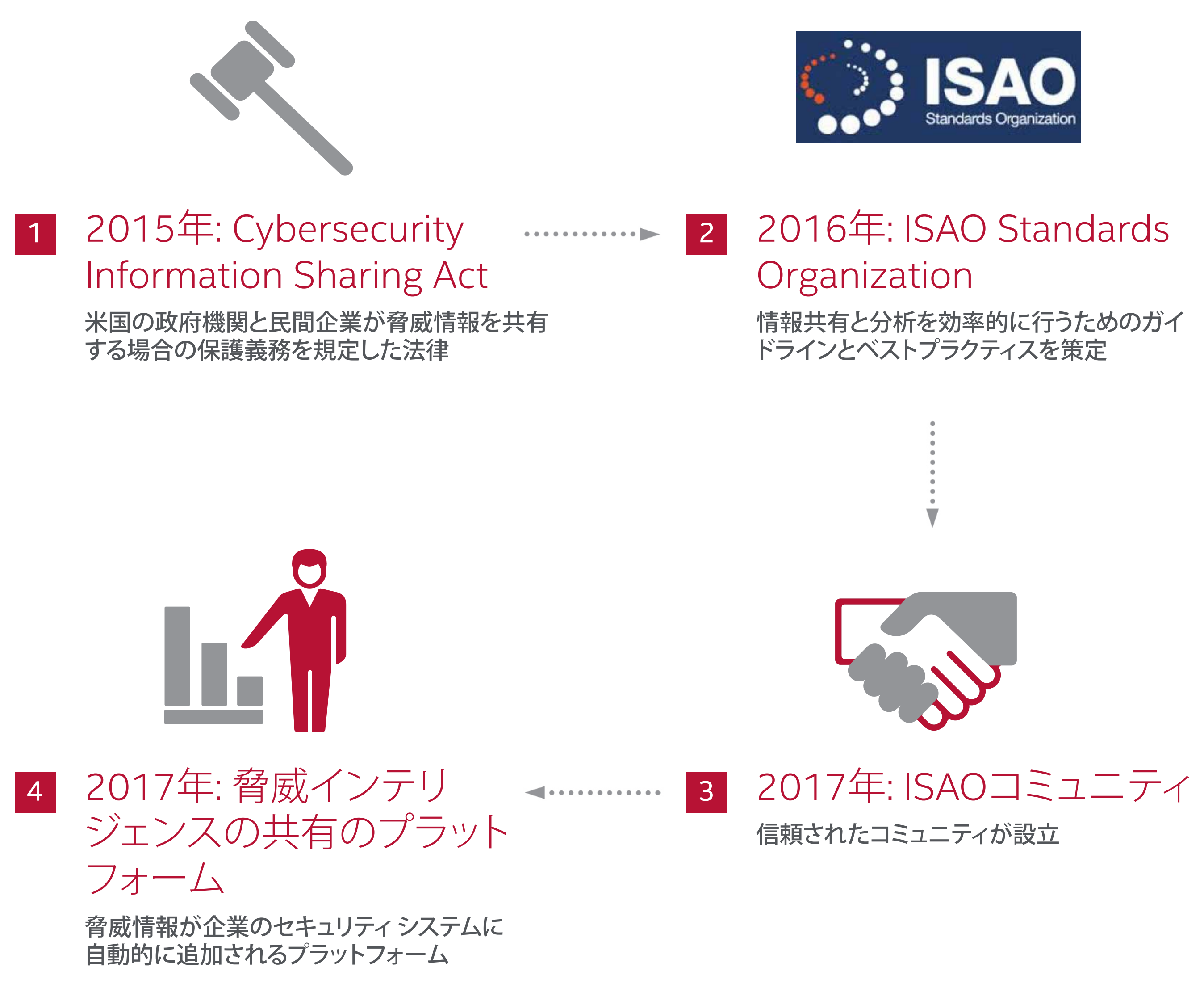
5 攻撃

2016年は機械学習を利用したデータ侵害が発生

医療記録	顧客情報	
メールとソーシャル メディアの記録	決算書類	盗まれたデータウェアハウス

脅威インテリジェンスの共有

2017年は脅威インテリジェンスの共有で大きな進展がある



1 2015年: Cybersecurity Information Sharing Act
米国の政府機関と民間企業が脅威情報を共有する場合の保護義務を規定した法律

2 2016年: ISAO Standards Organization
情報共有と分析を効率的に行うためのガイドラインとベストプラクティスを策定

3 2017年: ISAOコミュニティ
信頼されたコミュニティが設立

4 2017年: 脅威インテリジェンスの共有のプラットフォーム
脅威情報が企業のセキュリティ システムに自動的に追加されるプラットフォーム

McAfee Labs 2017年の脅威予測

レポートの完全版は、www.mcafee.com/2017Predictionsをご覧ください。

1833_1016_info_threats-predictions-2017-1