金融当局等の指針とサイバーセキュリティ対策について

2017年7月10日
トレンドマイクロ株式会社
業種営業推進グループ　金融担当
シニアマネージャー　今泉　智

アジェンダ

・脅威動向
・サイバーセキュリティ対策金融指針
・クラウドセキュリティ
・まとめ、ご参考情報

※当日の講演から内容を省略しています。

本セッションの概要

- 金融指針のおさらいから、サイバー攻撃対策に触れていきます。海外では金融機関様自身がサイバー攻撃に遭う事案があるため、モバイルなど利用者側のみのセキュリティにフォーカスをしているわけではありません。

- FISC有識者検討会で取り扱っている金融機関様とベンチャー企業様が協業するような場面などを本セッションでは想定しています。

- 団体等の指針を説明致しますが、登壇者の調査によるものです。

脅威動向

2017年第1四半期～の脅威動向

重要脆弱性の悪用でWebサイトの被害が続発

- 国内利用者の情報を狙い継続される「ネット詐欺」
- Web、モバイル、IoT、脆弱性の発覚で高まるセキュリティリスク
- 多様化するランサムウェアの脅威

トピック

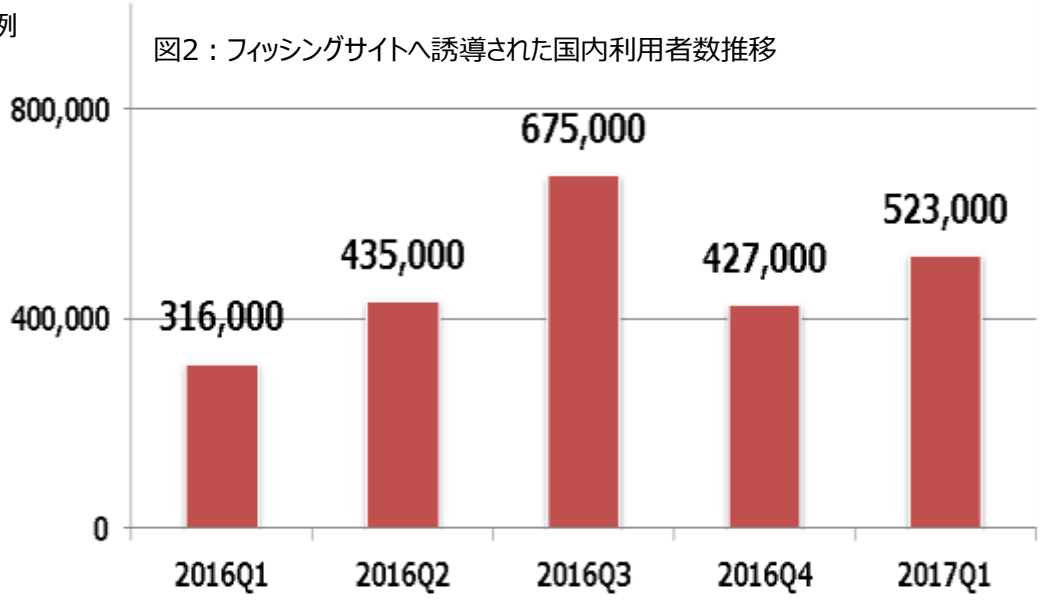
- 日本：
  - 重大脆弱性の続発から「公開サーバへの攻撃」が急増（継続）
  - 利用者の情報を狙い継続される「ネット詐欺」
  - 拡散は小康状態も金銭狙いの不正プログラムに新たな動き
- グローバル：
  - 脆弱性を悪用した公開サーバへのサイバー攻撃
  - 増加よりも巧妙化が顕著なランサムウェア
  - 深刻化するAndroid関連の脅威
  - 顕在化したIoT機器のセキュリティ課題

継続される「ネット詐欺」：フィッシング

- **520万件**：日本から詐欺サイトへ誘導された利用者数
- うちフィッシングサイトへの誘導が**52万件**で前年同期比**1.7倍**
- 詐取対象の情報はネットバンキングやクレジットカードに加え、マイクロソフトアカウントやAppleID、Googleアカウントが増加

図1：2017Q1に確認されたマイクロソフトアカウントを狙うフィッシングサイト例

図2：フィッシングサイトへ誘導された国内利用者数推移



※ トレンドマイクロによる調査。

継続される「ネット詐欺」：サポート詐欺＆ワンクリ

- サポート詐欺：2017Q1は650件の問い合わせで高止まり状態
- 3月にはサポート詐欺を真似たワンクリック詐欺を確認

図1：サポート詐欺関連問い合わせ数推移（トレンドマイクロ調べ）

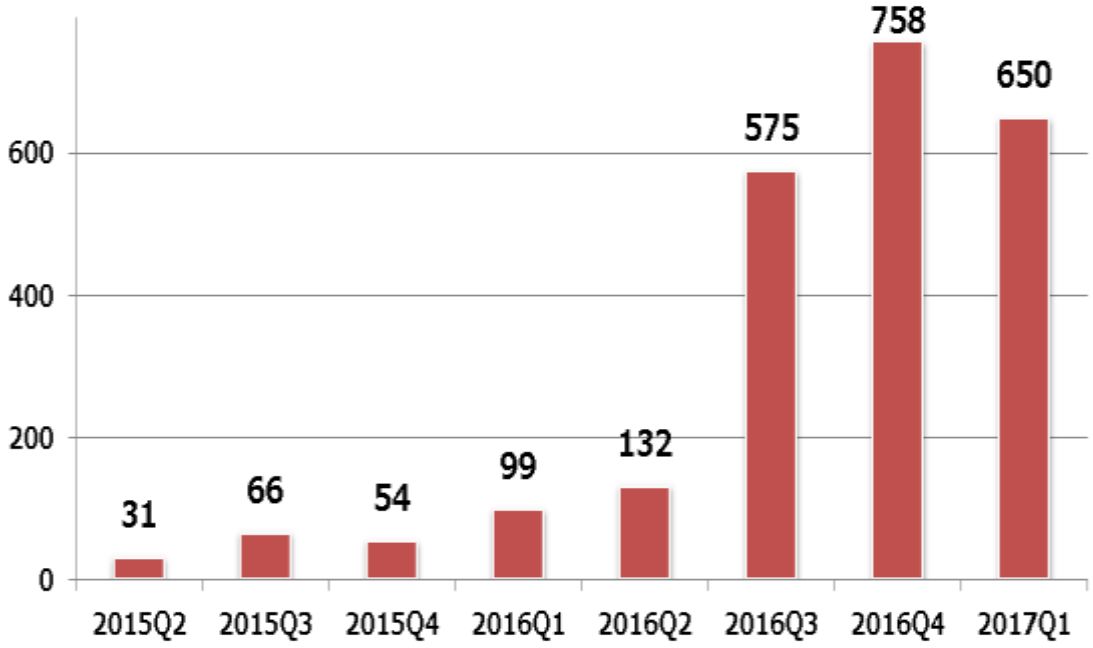
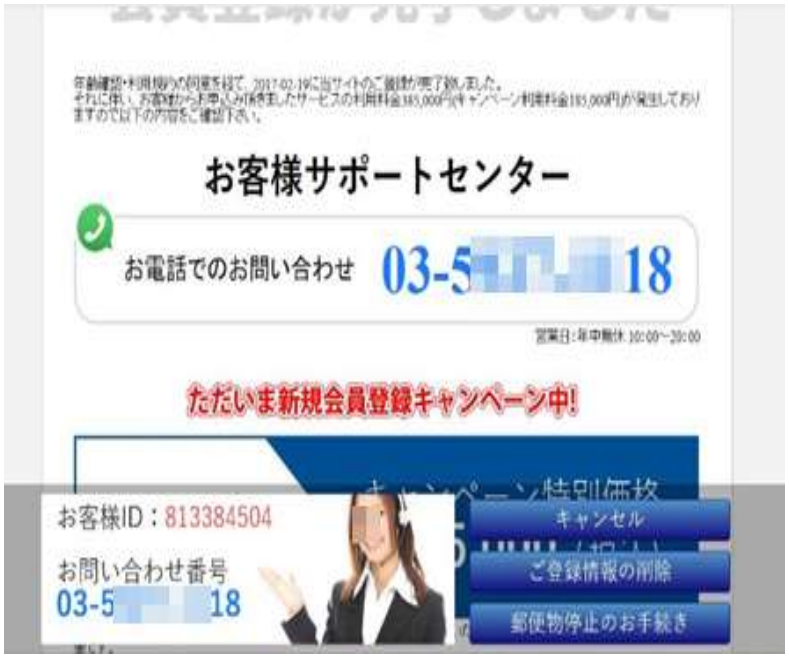


図2：サポートへの電話を促すワンクリック詐欺サイト画面例



※ トレンドマイクロサポートセンター調べ。

「Pawn Storm作戦」、巧妙なソーシャルエンジニアリング攻撃にOAuthを悪用

■ **Pawn StormによるOAuth利用の手順**

・不正アプリケーションを作成し、WebメールプロバイダにOAuthの利用を申請する
・Webメールプロバイダによる基本的なセキュリティチェックを通過し、OAuthのフィッシング攻撃への利用が可能に。
・標的に対して、OAuht認証を要求するページへのリンクを含んだメールを返信する。
・リクエストページは標的に対して不正なアプリケーションに対するOAuthの認可を要求する。
・不正なアプリケーションのOAuthが認可されると、メールアカウントにアクセスすることが可能に。
・パスワードを変更しても、トークンを無効化しない限り、メールアカウントへのアクセスが可能。

アカウントの安全性を高めるために
「Google Defender」という
アプリケーションのインストールを推奨

Pawn Storm から届いた不審なメール

万が一クリックすると

正規の「accounts.google.com」のページが開く
「偽Google Defender」による権限認可リクエスト

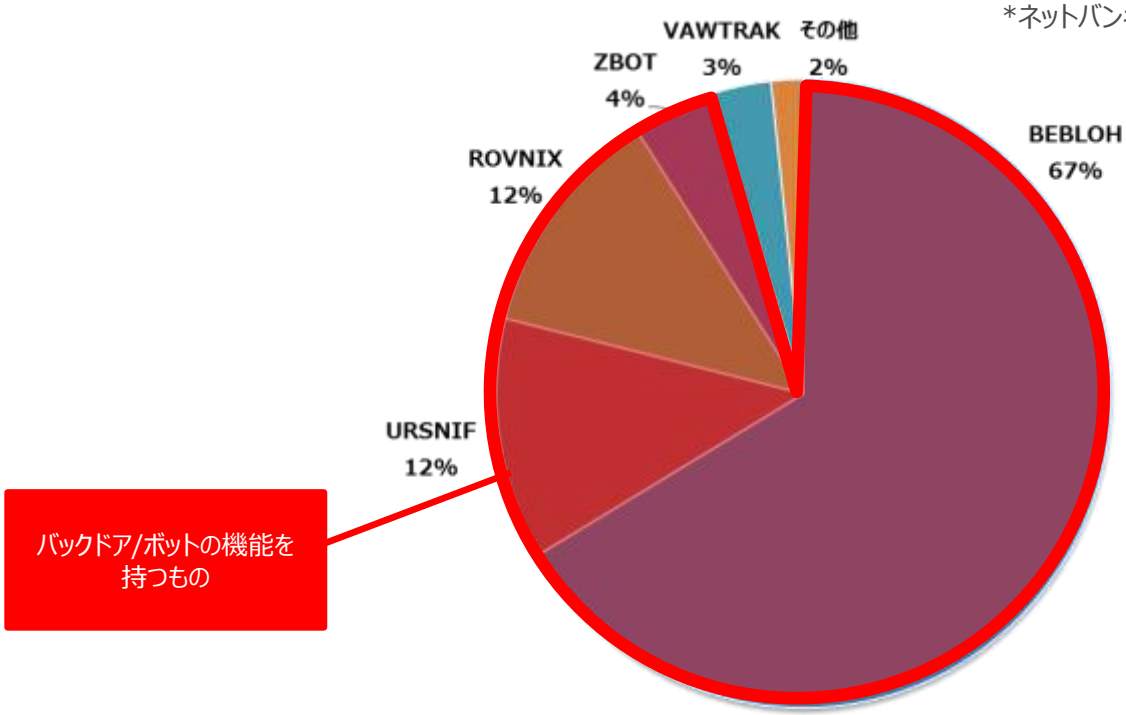
Gmailアカウントに対する巧妙なフィッシング攻撃、Google Docsに偽装したリンクに誘導
http://blog.trendmicro.co.jp/archives/14846
Pawn Storm は Gmail ユーザ以外にも、Yahoo メールを利用する重要人物を標的としたフィッシング攻撃も実行。
http://blog.trendmicro.co.jp/archives/14824

ネットバンキングを狙うウイルスの機能

95%

2016年1月-11月に国内で検出されたネットバンキングを狙うウイルス*のうち
バックドアやボットの機能を併せ持つタイプの割合

*ネットバンキングを狙うウイルス＝オンライン銀行詐欺ツール



- クレジットカード情報も詐取可能
- もともとバックドアやボットの機能を持っており、個人情報なども窃取

■グラフ：ネットバンキングを狙うオンライン銀行詐欺ツール
国内検出台数ファミリー別割合（2016年1~11月、n＝98,054）※

※ 2016年1月～11月 トレンドマイクロによる調査。

ネットバンキングを狙うウイルスの機能

- ネットバンキングの詐欺機能
  - 各種情報の取得及び送信
    - デジタル証明書
    - キー入力操作方法の取得
    - スクリーンショット
    - 保存されているEメールなどの認証情報
  - Webサーバのスクリプトへの攻撃スクリプトの挿入(Webインジェクション)
    - 実際の認証情報入力画面に上書きして、偽の認証情報入力画面を挿入
  - ルート証明書の書き換え
    - 偽サイトにて、ブラウザの証明書のエラーが表示されないように
  - インターネット閲覧の監視
    - オンライン銀行サイトの利用を監視
  - リモートでのコントロール
    - 隠れたデスクトップを利用して利用者に気付かれずに裏でコンピュータを操作
- 検知から逃れる機能
  - 自身のアンインストール
  - ダウンロードの都度実行プログラムを変更 (サーバサイドポリモーフィック技術)
  - C&Cの接続先のドメイン名をランダムに作成 (Domain Generation Algorism技術)
  - 仮想環境での実行を検知
  - ファイルレスの感染

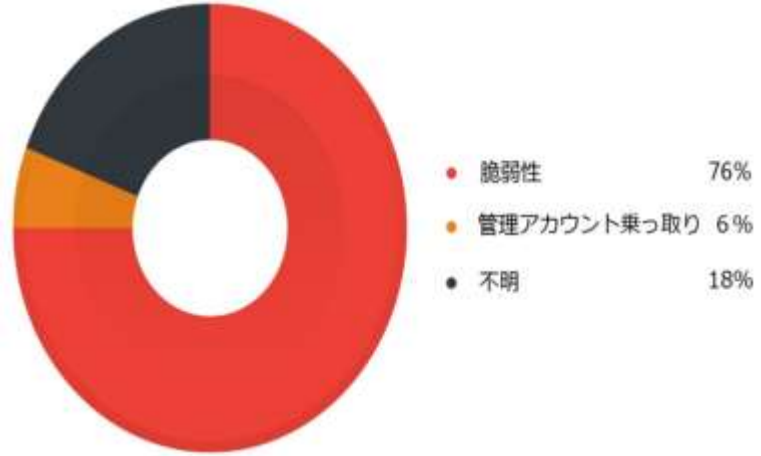
Web、モバイル、IoT、脆弱性の発覚で高まるセキュリティリスク：2017年Q1

脆弱性の悪用で情報漏えい事例が続発

- 公開サーバへの攻撃による情報漏えい事例
  - 2017年1月から3月までに**17件**が報道された
  - **約215万件**の情報が漏えいの被害に遭った

公開サーバからの情報漏えい
全体の**76%**は脆弱性が原因

■図：公開サーバへの攻撃による情報漏えい事例における被害原因の割合
（2017年第１四半期）※



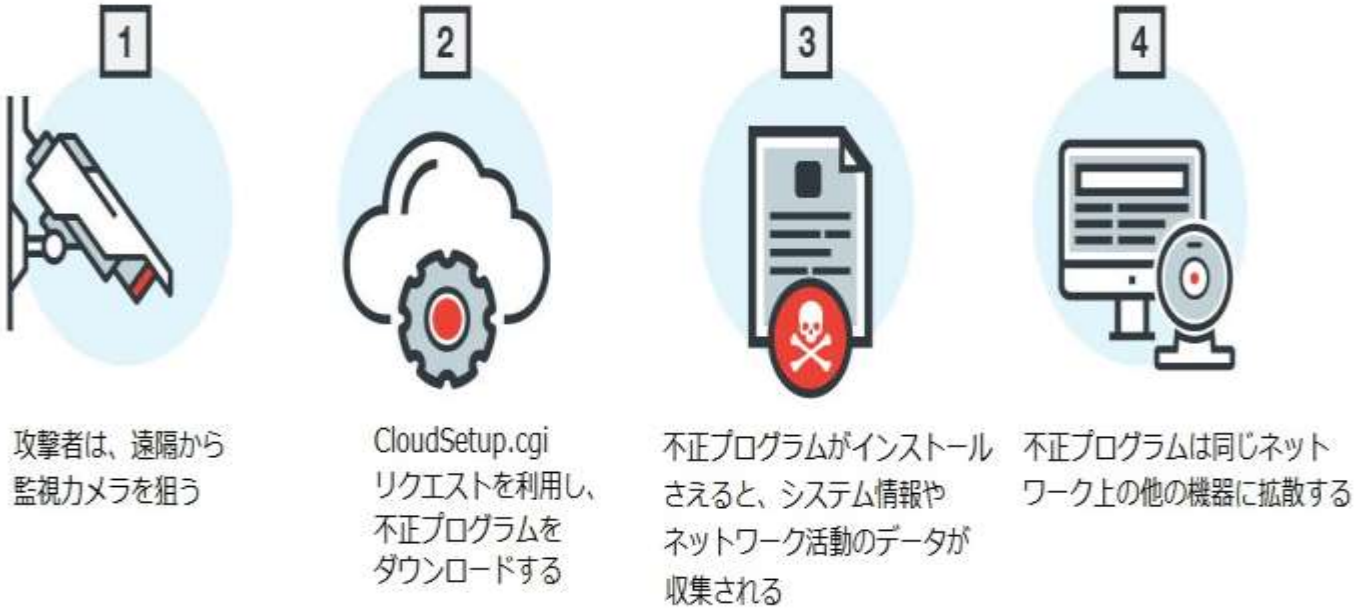
※公表・報道内容をもとにトレンドマイクロが独自に整理

Web、モバイル、IoT、脆弱性の発覚で高まるセキュリティリスク：

顕在化したIoT機器のセキュリティ課題

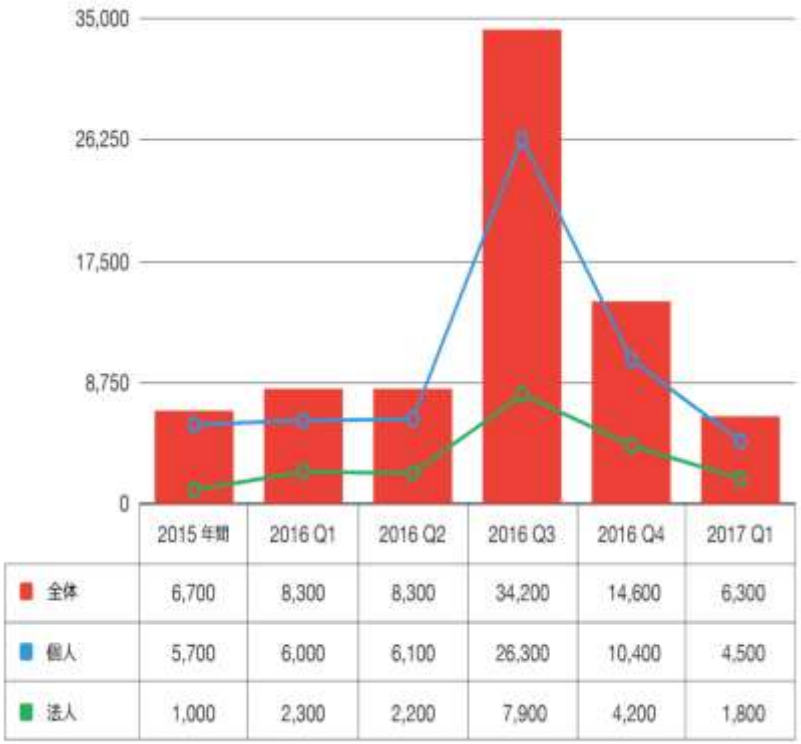
- IoT機器に潜む脆弱性を狙った攻撃
  - 2017年2月に「AVTech」製品の脆弱性を狙う「IMEJ」
  - **ハードコード化**された認証情報を用いた攻撃に警戒

■図：「IMEIJ」の感染フロー



ランサムウェアは「急増」から「定着」へ

- 国内の検出台数は前四半期期比**57%**減
- 登場した新ファミリー数は**58**



	2015 年期	2016 Q1	2016 Q2	2016 Q3	2016 Q4	2017 Q1
全体	6,700	8,300	8,300	34,200	14,600	6,300
個人	5,700	6,000	6,100	26,300	10,400	4,500
法人	1,000	2,300	2,200	7,900	4,200	1,800

図１：ランサムウェア国内検出台数推移（※）

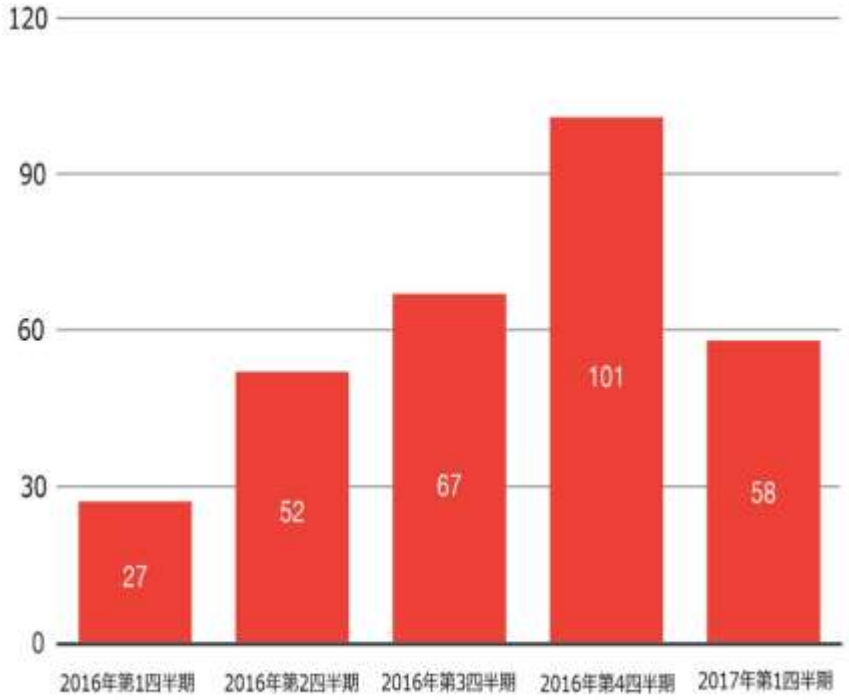


図2：ランサムウェア新ファミリー数推移（※）

※ トレンドマイクロ調べ

多様化するランサムウェアの脅威

ご参考：モバイルランサムの新種・亜種が急増

- 2017年1月-3月の新規種類数※1が**12万**を突破

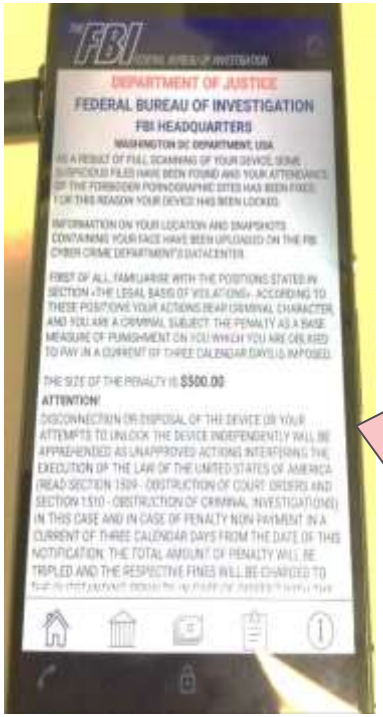
（前年同期比**約5.6倍**）

■グラフ：モバイルランサムウェアの新規種類数の推移※2

※1　新規種類数：トレンドマイクロが新たに確認したユニークなモバイルランサムウェア検体（APK)の数
※2 トレンドマイクロSPNによる

ご参考：スマホを操作できなくするモバイルランサムウェアに注意

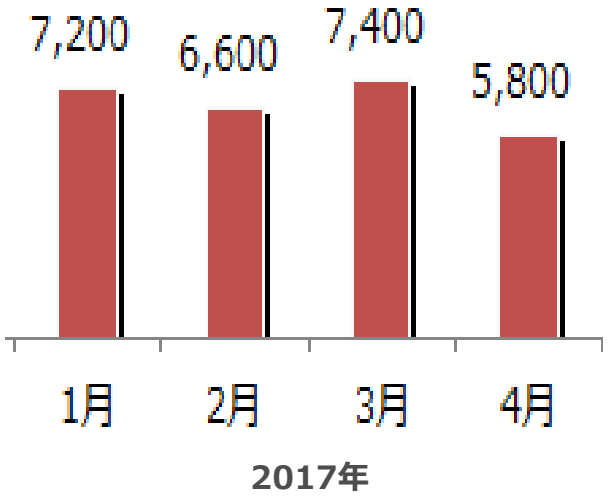
- 感染すると画面がロックされ、スマホの操作が行なえなくなる
- 機種によっては電源も落とせなくなり、端末初期化でしか復旧できない場合も



■画面ロック型モバイルランサムウェアの感染例
（検出名：AndroidOS_Locker.AXBO ）

このタイプのランサムウェアの主な特徴

・FBIなど法執行機関をよそおう
・感染被害者に「法を犯した罰金」の名目で金銭支払いを要求
・アダルト動画再生用アプリにみせかけインストールさせる例を確認



■国内でのモバイルランサムウェアの検出数推移（※1）

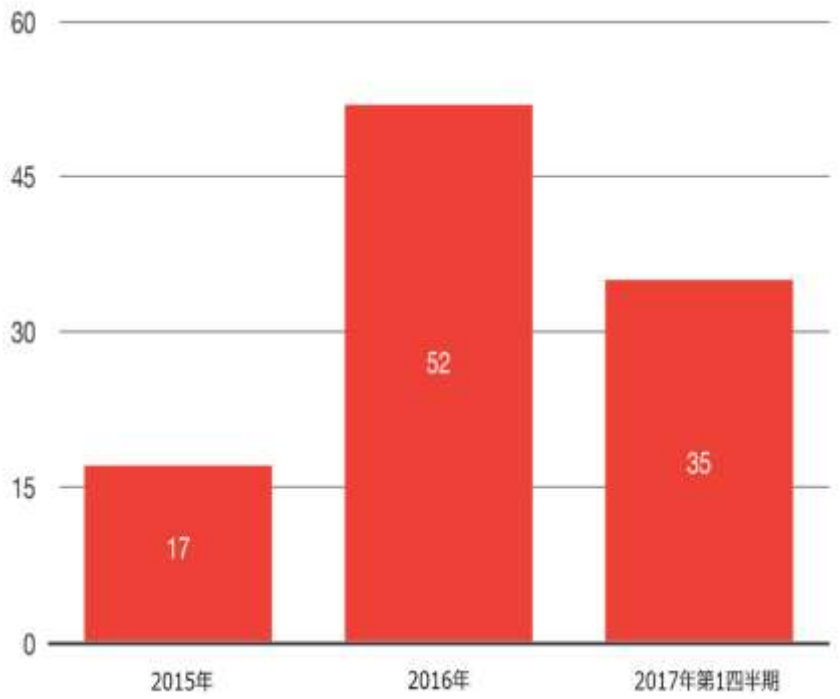
※1 トレンドマイクロ調べ（2017年5月）

Web、モバイル、IoT、脆弱性の発覚で高まるセキュリティリスク：2017年1Q

深刻化するAndroid関連の脅威

- Android関連の脆弱性が多数発覚
  - 2017年1月から3月までに**35件**
  - うち15件が**「Mediaserver」**

■グラフ：Android関連脆弱性の推移※



※トレンドマイクロ調べ

脅威動向まとめ

- 様々な分野で**脆弱性**が大きなセキュリティリスクとなっている
- **ランサムウェア**は「急増」期を過ぎ、サイバー犯罪者のビジネスとして「定着」
- 変化を続けながら継続される**ネット詐欺**にも注意

クラウドセキュリティについて

AWS/MS対応　FISCセキュリティリファレンス

現在金融機関様でもパブリッククラウドの利用が進んでいます。金融機関様にパブリッククラウドをご活用頂くために、弊社では2013年より、AWS、MS Azure/O365対応のセキュリティリファレンス作成に、セキュリティベンダーとしては唯一参画しています。

■AWSセキュリティリファレンス

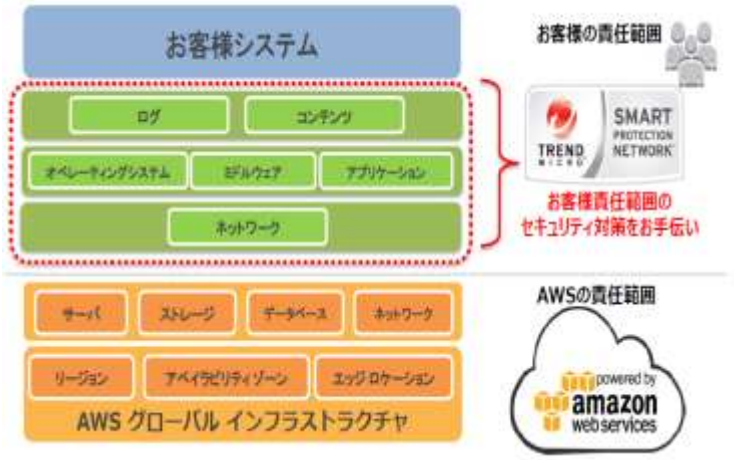
2016年11月リリース
FISC 8版追補改訂AWSセキュリティリファレンス
旧運108の廃止　108～113の新設項目に対する対応
http://www.trendmicro.co.jp/jp/business/solutions/publiccloud/awssrf/index.html

■MS Azure/O365セキュリティリファレンス

2015年1月28日リリース
FISC8版追補改訂AWS/O365セキュリティリファレンス
旧運108の廃止　108～113の新設項目に対する対応
- 138の設備基準、120の運用基準、53の技術基準、全311項目で構成

http://www.trendmicro.co.jp/jp/business/solutions/finance/azuresrf/index.html

IaaS利用における責任共有モデル



利用者（金融機関様、SI等）とクラウドベンダーの責任範囲やクラウド特有の管理について、安全対策基準をベースに整理
- クラウドは標準サービス
- 既存のセキュリティ対策とは異なる部分がある

■ご参考：テクノロジーアライアンス

弊社製品対応としては、AWS/Azure/Bluemixの他、GCPに対応（2017年6月）
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20170607013200.html?cm_re=news-_-corp-_-press

シンガポール　金融当局対応AWSリファレンス

2016年8月リリース　NRI様＆NRIセキュア様＆TM3社のワーキング（無償で公開中）

日本企業に比較的なじみのあるISOやFISCをベースに、ガイドラインの概要を理解
セキュリティ等に対する要求事項は同様の項目も多いため、ベースラインと照らし合わせ
各国固有の項目の洗い出し。

3. 経営・シニアマネジメントによる監督
4. 技術リスクの枠組み
5. ITアウトソーシングのリスク管理
6. ITシステムの開発と取得
7. ITサービスの管理
8. システムの信頼性、可用性、復元可能性
9. 運用基盤セキュリティ管理
10. データセンタの防災・統制
11. アクセス制御
12. オンライン金融サービス
13. 決済カードセキュリティ
14. IT監査

A	MAS TRM の項番と要求項目（英語）
B	MAS TRM 要求項目の日本語訳
C	AWS利用における責任分界の考え方 共有（Shared）, 利用者固有（Customer Specific）
D	要求項目に対するAWSの対応状況と考え方 参照すべきホワイトペーパー等
E	ISO27001（情報セキュリティ）、ISO27017（クラウドサービスセキュリティ）とのマッピング
F	FISC安対第8版追補改訂とのマッピング

Item	TRMG Section	Guideline Description	和訳	責任分界	リファレンス	ISO27001:2013	ISO27017:2015	FISC第8版追補改訂 中項目
9.6 Security Monitoring （セキュリティ監視）								
28	9.6.5	Security logs of systems, applications and network devices are regularly reviewed for anomalies.	システム、アプリケーション、およびネットワークデバイスのセキュリティログを異常検知のために定期的に見直していること	共有 （Shared）	■AWSのプログラム、プロセス群、及びウイルス/マルウェア対策ソフトウェアの管理はISO 27001認証に準拠しています。AWS SOC1 タイプ2レポートにさらなる詳細情報が記載されています。 <参照先> セキュリティプロセスの概要 （p.21　セキュリティログ）	A12.4.1　イベントログ取得 A12.4.3　実務管理者及び運用担当者の作業ログ A16.1.7　証拠の収集	12.4.1 12.4.3 16.1.7	V. 運用基準 サイバー攻撃対応態勢の整備 VI. 技術基準 不正使用防止(予防策(アクセス権限確認)) 不正使用防止(外部ネットワークからのアクセス制限) 不正プログラム防止(検知策)

A　B　C　D　E　F

シンガポール　金融当局対応AWSリファレンス

シンガポールMAS TRMG概要とFISCとの比較

	FISC Security Guidelines	MAS TRM Guidelines
発行元 Publisher	金融情報システムセンター（FISC） The Center for Financial Industry Information Systems	シンガポール金融管理局（MAS） Monetary Authority of Singapore
正式名称 Official Name	FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions	MAS Technology Risk Management Guidelines
目的 Objective	金融機関等のコンピュータシステムに関する安全対策の具体的指針	金融機関の健全な実務と技術を管理するためのプロセスの採用促進（2.0.2 より）
リリース Release	2015/6　※第8版追補改訂	2013/6　※Effective at 2014/7
主な新要件 Main New Requirements on Latest Release	・サイバー攻撃対応 ・クラウドサービス利用 ・外部委託先による不正な引き出し事例への対応	・ITサービス管理（変更管理、インシデント管理） ・ITアウトソーシングリスク管理（クラウド等） ・データセンター保護（脅威・リスク評価）
特長 Feature	・6章構成 ・セキュリティポリシーや体制は巻末の資料編に記載 ・金融検査マニュアルから参照されている	・14章構成、付録6章 ・過去の通達類を統合し、ガイドラインとして体系化 ・呼称はガイドラインであるが、**遵守レベルは必須**

Source：“AWS Security Reference for MAS-TRMG” by NRI, NRI Secure, Trend Micro

シンガポール　金融当局対応AWSリファレンス

2016年8月31日　AWS様セミナーでの講演内容

1．シンガポール現地　FinTech動向＆金融機関様がAWS等利用を公表
MAS Sandbox：http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/MAS-Proposes-a-Regulatory-Sandbox-for-FinTech-Experiments.aspx
DBS：https://www.dbs.com/newsroom/DBS_to_leverage_Amazon_Web_Services_Cloud

2．クラウド化により、統制上も利点がある
高度に抽象化された環境、プログラミング可能なインフラストラクチャが利用可能となり、ログ取得・監視実行などの自動化が以前より容易となる

3．統制方法としてThree Lines of Defenseの考え方を活用する
⇒　Second lineの日々の運用が課題

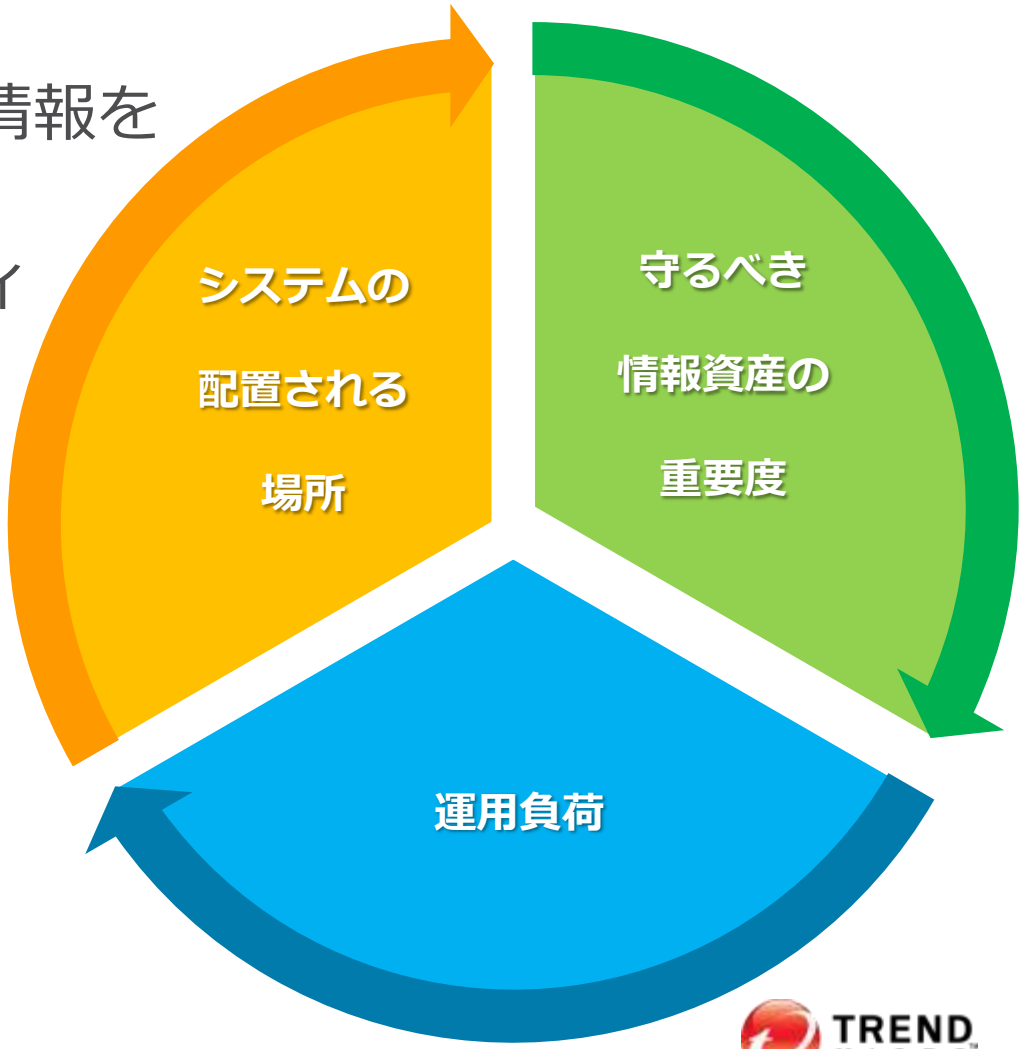
Source：“AWS Solution Day MAS-TRMG” by NRI Secure, TrendMicro

セキュリティ対策を考える

とはいえ、複雑な実装をしても運用できないと意味がない。

- どこにあるどのような情報を守りたいのか？
- 適材適所のセキュリティ

自社で運用できることは？
何をアウトソースするか？



クラウド環境のセキュリティの検討

既にプリセットされたテンプレートを利用

自動化実装例）
AWSサービスとのAPI連携
～Github公開のフリーツールを利用して開発
※一部開発中のものあり