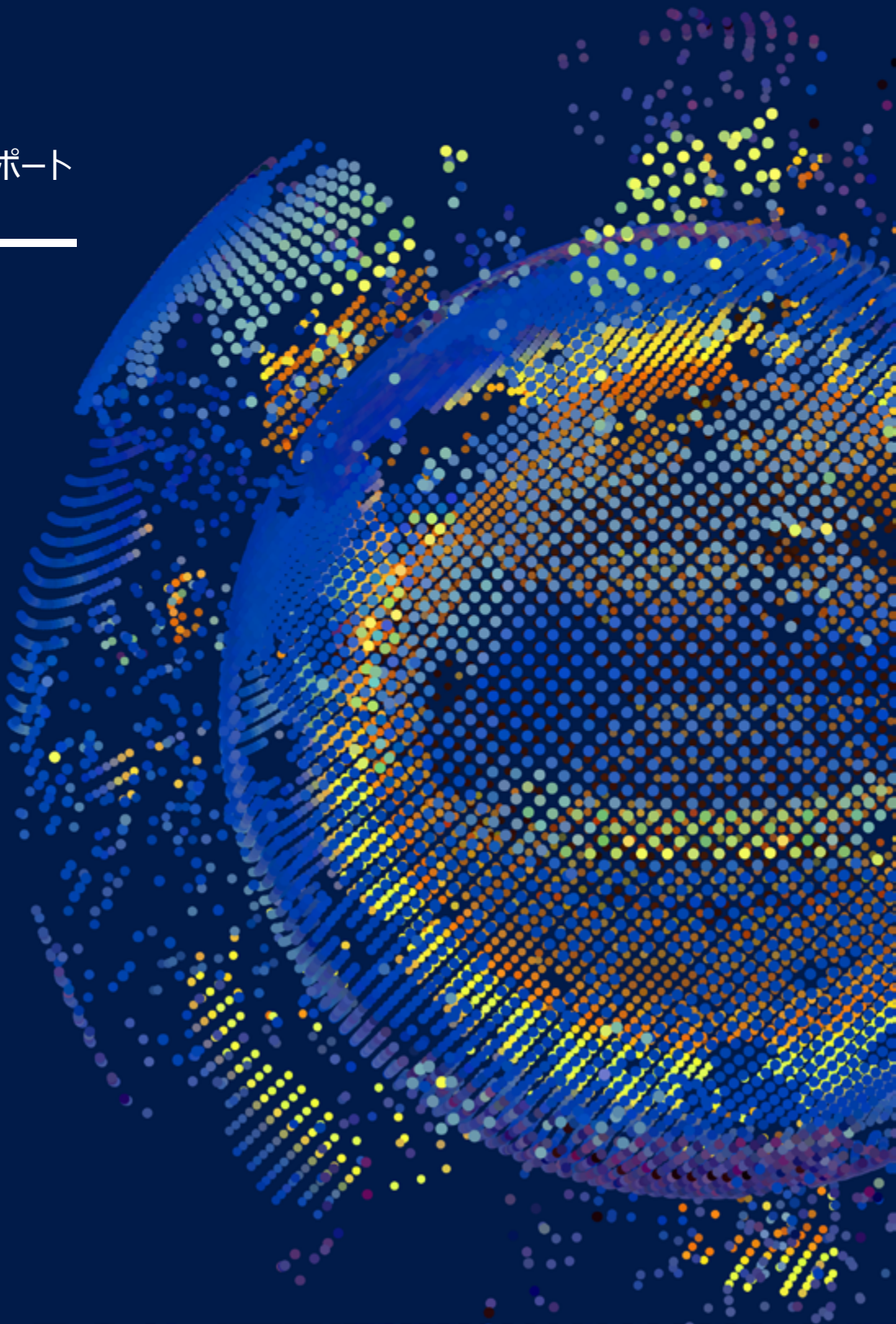
2015 総決算
2016 大予測

アンラボ・セキュリティレポート



AhnLab

2015年 情報セキュリティ総決算 Top 5

01 ランサムウェア 3

02 金融情報漏れリスク 4

03 Webエクスプロイト 5

04 モバイル環境アドウェア 6

05 ネットワークハブ、IoTを狙う脅威 7

2016年 情報セキュリティ大予測 Top 5

01 ランサムウェア凶悪化 8

02 国家の根幹を脅すサイバーテロ 9

03 クラウド、仮想化に伸びる魔の手 10

04 IoTを取り巻く脅威の実態 11

05 新フィールド、脅威の陣取り合戦 12

2015年 情報セキュリティ総決算 Top 5

01 ランサムウェア

近年ランサムウェアはセキュリティ分野最大の悩みの種になりつつある。北米及びヨーロッパを中心に爆発的な増加傾向を見せている中、韓国でも 2015年 4月に某大型コミュニティサイトでハングル化されたランサムウェア・CryptoLockerが大量に配布されたことから急速に感染が広がった。

また従来の手法としては、主に文書ファイル(doc、ppt等)と画像(jpeg等)を暗号化したが、最近は実行ファイル(exe)を含む 140以上の拡張子形式が暗号化対象にされていることが分かった。さらに不正にデータを暗号化する手法に加え画面ロックを発動させることで、PCを起動不能にするランサムウェアも登場した。

ランサムウェアタイプの地域化も顕著で、主に北米とヨーロッパでは「BitCrypt」、「CoinValut」が、ロシア及びトルコなど東欧エリアでは「TrolDesh」が頻繁に見られ、韓国では「CryptoLocker」、「CryptoWall」、「TaslaCrypt」「Nabucur」等のランサムウェア感染頻度が高かった。

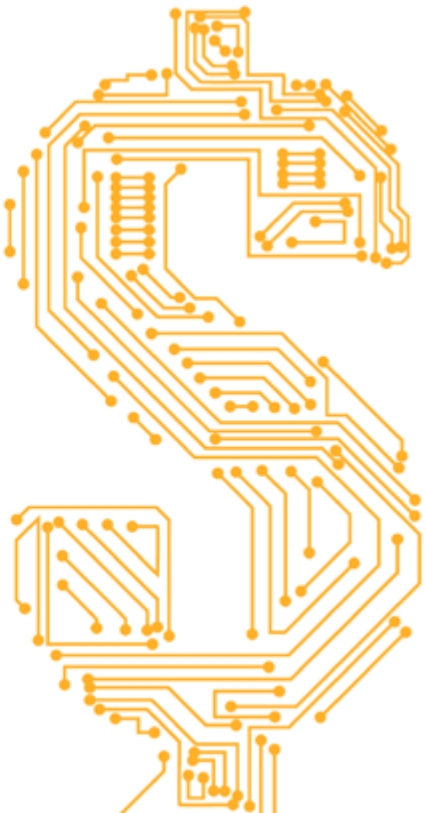
2015年 情報セキュリティ総決算 Top 5

02

金融情報漏れリスク

2015年も金融情報を狙ったマルウェアは猛威を振るった。世界で 1,000以上の銀行と企業を攻撃対象にした悪名高いマルウェア「Dyre」が、最近韓国の銀行をターゲットに含めたことから金融業界を緊張させた。最近はWindows 10と Edge Browserなど最新の OSやブラウザーでも情報が奪取されるなど、さらに厄介な存在となっている。不正サイトにユーザーを誘導して金融情報を奪取する Bankiタイプのマルウェアも、2015年下半期に配布手法を変化させるなど、その勢いは衰えを見せない。

そして金融情報を奪取するマルウェアの攻撃対象は銀行だけではない。2015年には POS(Point of Sale)システムからカード情報を流出する POSマルウェアが再び増加し始めた。Cherry Picker、ModPOSは 2015年に登場した代表的な POSマルウェアだ。2013年末、海外の大型マートで発生した大規模なカード情報流出事件をきっかけに POSマルウェアのリスクが急浮上している。韓国でも、POS端末からカード情報の流出及び金銭的な被害が発生するなど POSシステムを脅かす状況が日増しに増加している。



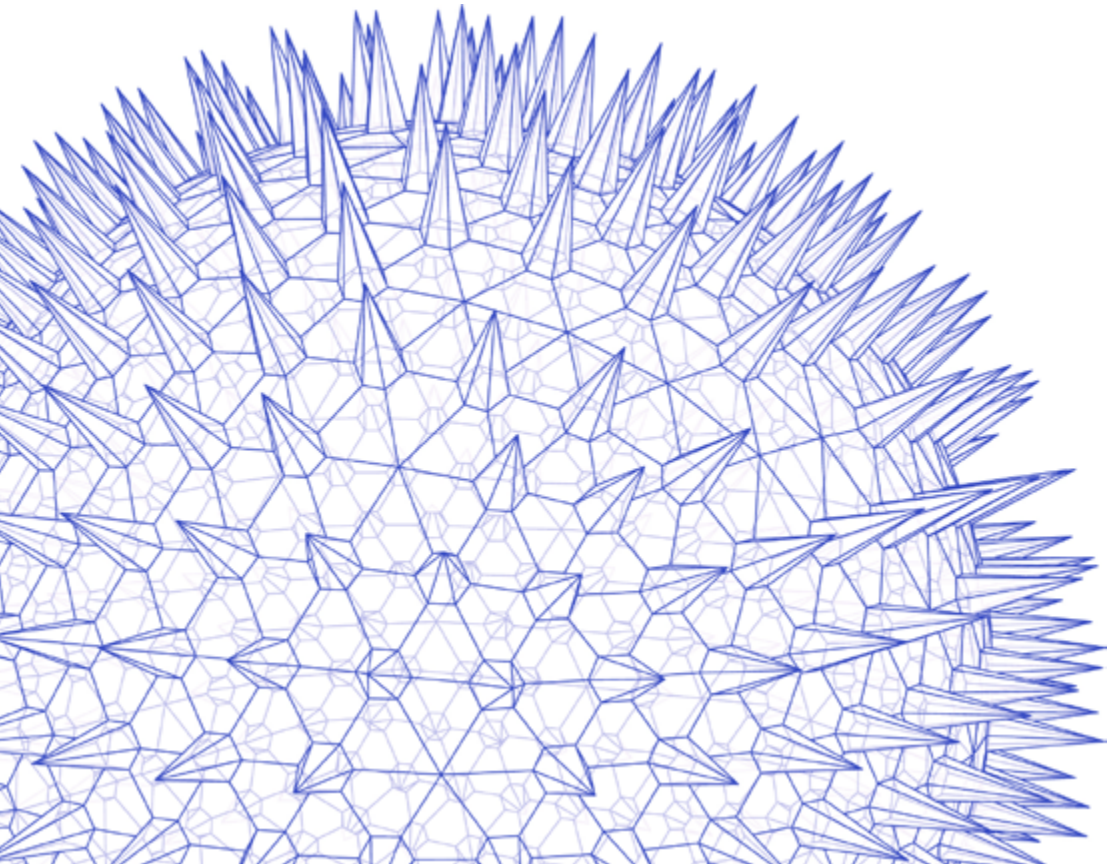
2015年 情報セキュリティ総決算 Top 5

03 Webエクスプロイト

2015年セキュリティ業界を震撼させた事件の背景には、常に Web Exploit ToolKitの存在が隠れていた。そして以前にも増して遥かに巧妙な方法で、その存在感を際立たせている。

これは多数の脆弱性を突いてユーザーPCを感染させる攻撃ツールであり、攻撃者はこのツールキットを使ってマルウェアを簡単に作成・配布することができる。2015年に猛威を振るった代表的なツールキットは「Angler ToolKit」だった。4月に韓国の某コミュニティで配布されたランサムウェアマルウェアの件の黒幕も、このツールキットであったことが分かった。

攻撃者はマルウェアの配布ルートをさらにトレースしにくくするため、多様なブログ作成ツールやコンテンツ管理システムを利用したり、動的コンテンツを作成する広告サイトをマルウェア配布に利用する「Malvertising」手法を駆使したりする。またセキュリティソフトの検知機能をバイパスするスキルもさらに発達し、ツールキットの危険レベルはますます磨きがかかっている。



2015年 情報セキュリティ総決算 Top 5

04 モバイル環境アドウェア

過剰な広告表示でユーザーの不便を招くアドウェア(adware)がモバイル環境にも進出した。2015年発見されたモバイルアドウェアの数は前年対比約 2.5倍増加し、個人情報収集、過剰な広告表示、アプリのすり替えなど、スマートフォンユーザーにとって、多くの悪意ある動作で被害をもたらしている。最新のモバイルアドウェアは、他のアプリになりすましたり、Root権限を獲得して削除を妨害するなど、一層巧妙化した手法でユーザーを狙っている。

アドウェア以外のモバイル向け脅威は前年に比べ多少減少気味にあった。2012年から毎年 2倍増だったモバイルバンキングマルウェアは前年度水準を維持し、モバイルマルウェアの配布手法として利用されたスミッシングも、2015年下半期に入って減少していた。これは韓国の政府機関、KISA(Korea Internet & Security Agency、韓国インターネット振興院)、警察庁の積極的な啓蒙キャンペーンによる努力の賜物といえる。スミッシングメッセージ及びネットワーク遮断、セキュリティベンダーとキャリアなど民間会社の利用者保護措置、マスコミ報道及びキャンペーンによる国民意識の向上が、モバイルセキュリティ分野において実を結んだといえよう。

2015年 情報セキュリティ総決算 Top 5

05

ネットワークハブ、IoTを狙う脅威

2014年に続いて 2015年は初頭から韓国の有名メーカーの有・無線ネットワークハブの脆弱性を狙ったハッキングの試みが相次いで発見された。ネットワークハブの場合、管理権限を奪取するとハブに繋がるモバイル端末やPCを同時に攻撃できるようになるため非常に危険だ。

ネットワークに繋がるデバイスへの脅威は、ハブだけでなく IoT(モノのインターネット)までも攻撃範囲としている。最近多様なウェアラブルデバイス(Wearable device)の登場により、個人向け IoTデバイスが増加していることから、セキュリティへの懸念も高まっている。IoTの代表的な端末である IPカメラ、NAS(Network Attached Storage)、CCTVなどは一般コンピューターと類似した OS構造を持つため、攻撃者が比較的簡単にアクセスできる。特にこれらのデバイスは常時ネットワークに繋がっている反面、まだこれといったセキュリティ対策が存在しない。ネットワークハブや IoTは常に接続状態を基本とするため、デバイスを安全に保護するには各メーカーで提供するファームウエアのアップデートや管理パスワードを随時変更するなど、ユーザーの定期的な管理が求められる。

2016年 情報セキュリティ大予測 Top 5

01 ランサムウェア凶悪化

ランサムウェアの脅威は 2016年さらに悪化し、暗号化対象の拡大、画面ロックなどユーザーの対応を妨害する機能を追加し、継続的な進化が予想される。悪意ある行為に対抗するための、セキュリティベンダーのランサムウェア診断率も向上していることから、セキュリティ製品の検知をバイパスしたり、対応を妨げるなど高度化されたランサムウェアが登場する可能性もある。

そしてモバイルランサムウェアの登場も考えられる。まだ韓国ではスマートフォンランサムウェアの感染が確認されていないが、PC ランサムウェアがそうだったように、今にハングル化されたモバイルランサムウェアが登場してスマートフォンユーザーが被害をこうむるのも時間の問題といえる。Android向けランサムウェア数は 2014年 2,220件から 2015年 27,845件と 1年間で 12倍も増加した。2016年もモバイルランサムウェアの変種は持続的な増加を見せるだろう。モバイルランサムウェアがスマートフォンユーザーをターゲットにすると、2014年社会的な問題となったスミッシングマルウェアとは比べものにならないほど大きな被害をもたらす可能性もある。

2016年 情報セキュリティ大予測 Top 5

02

国家の根幹を脅すサイバーテロ

2015年末パリで起こったテロ事件は全世界に衝撃を与えた。このような宗教・理念の葛藤による国家間対立はサイバー世界でも同様で、物理的なダメージに限定されていた過去のテロ活動に比べて、最近のテロリストは布教活動や宣伝及び情報収集、敵対勢力の盗聴・傍受及び情報流出などはネットワークを利用するため、現状サイバー環境に深く侵透している状況だ。

テロは大衆に向けて恐怖感を煽ることを目的とするが、中でも非常に恐れられているのが国家インフラ施設を狙う高度化された知能型脅威(Advanced Persistent Threat、APT)である。もちろん国家インフラの場合は幾重もの厳戒なセキュリティシステムに保護されているうえ、ほとんどはインターネットに接続しないことを原則とした閉鎖型網環境で運用されているため脅威にさらされる可能性が低い。しかしイランの原子力発電所が Stuxnetに感染し、日本では原子力発電所の情報流出事件があった。さらに最近確認された米ニューヨーク・ダム制御システムのインシデントなど、国レベルのインフラ施設を狙ったサイバー攻撃は持続的に発生している。政治的な葛藤と長期的な景気低迷の影響で国際情勢が不安定になり、大規模なインフラ施設のセキュリティはますます重要になっている。

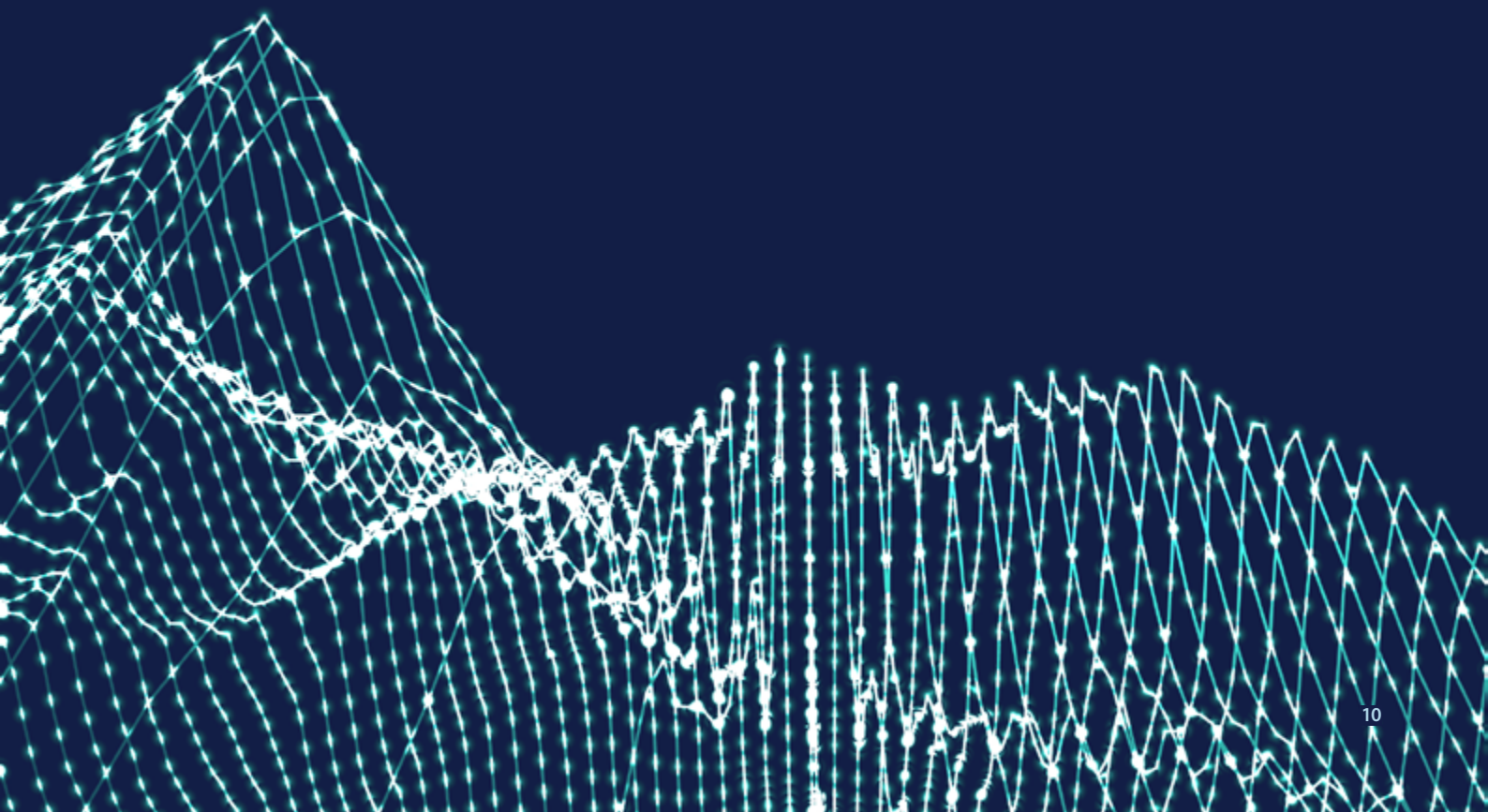
2016年 情報セキュリティ大予測 Top 5

03

クラウド、仮想化に伸びる魔の手

最近 ITインフラの効率性を高めるために、クラウドまたは仮想化インフラの導入を検討している組織も多い。だがこれらの環境変化によるセキュリティ対策も、一緒に考慮されるべきだろう。

クラウドシステムの脆弱性だけでなく、クラウドにアクセスする Hostシステムの脆弱性もまた、クラウド及び仮想化環境を脅かす要素の一つだ。通常クラウドや仮想化環境は、ITリソースを物理的に中央に集めて共有する方式であるため、これに接続する Hostシステムが掌握されればネットワーク全般に脅威が拡散しやすくなる。特に各種のアプリケーション脆弱性を狙った攻撃が持続的に増加することによって、クラウド及び仮想化環境に接続するシステムへの感染の拡散が懸念されている。



2016年 情報セキュリティ大予測 Top 5

04

IoTを取り巻く脅威の実態

IT技術とデバイスの発展速度が加速化する中、サイバー脅威の範囲は、もはや PCという媒体にとどまらない。コンピューターとは性能と機能面で大差ない IoTデバイスが次々リリースされ、インターネットに繋がるデバイスの種類が増えるほど、新たなサイバー脅威の様相も多様化していく。

今や一般家庭でも見られる無線ネットワークハブをはじめとする家庭用電源コントロール、空調などの家電制御システムに至るまで、スマートホーム技術の発展によりセキュリティ側面でも強固な対策が求められる。この外、現在各国で有効性検証と関連法令の整備が進行中のドローン(Drone)やインターネットに接続して駆動する自動車(Connected Car)およびスマートカーも、今後の脅威対策の範囲に含めるべきだ。

2016年 情報セキュリティ大予測 Top 5

05

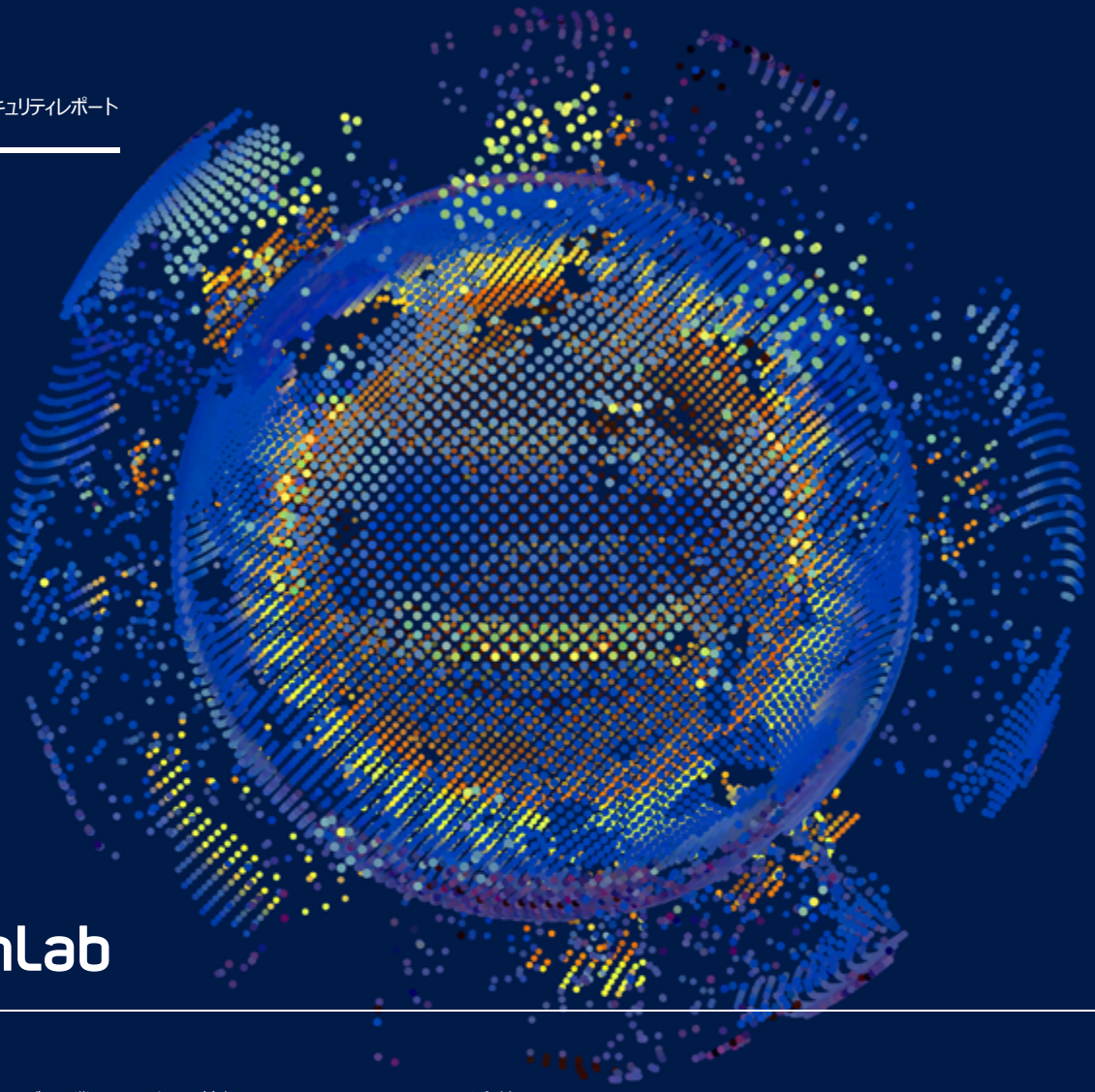
新フィールド、脅威の陣取り合戦

金融システムは常にサイバー脅威の最重要ターゲットであり、金融環境がオンライン化されるほど脅威の深刻さも増していった。2016年は韓国にもインターネット専門銀行が発足され、金融業界におけるセキュリティ脅威がさらに増加すると思われる。

インターネット専門銀行はオフラインの営業店舗が存在しないため、本人確認の際に非対面の実名確認手順が欠かせない。このため本人確認手順が最重要課題として浮上したが、これは PCに限ってのことではなくスマートフォンでもモバイル金融取引きに関する悩みが深い。インターネット専門銀行が本格的に稼働すれば、スマートフォンを利用したモバイルの金融取り引きも当然多くなるからだ。ここ数年間、モバイルマルウェアによる金融情報の奪取も頻繁に発生、そしてスマートフォンユーザーを狙うパーミング攻撃も増加している。インターネット専門銀行をきっかけに、広がる新領域から派生するモバイル金融取引きのセキュリティ強化が求められる。

2015 総決算
2016 大予測

アンラボ・セキュリティレポート



AhnLab

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。

1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。

今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

発行所　株式会社アンラボ
発行者　AhnLab Security Emergency Response Center
編集　アンラボ・コンテンツ企画チーム

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

© 2015 AhnLab, Inc. All rights reserved.

著作権者の許可なくこのコンテンツの内容の全て又は一部をいかなる手段においても複製・転載・流用・転売・複写等することを固く禁じます。

AhnLab.com