

危険な12の落とし穴

クラウドの重大セキュリティ脅威

+

2017 インシデント事例集



Cloud Security Alliance

Cloud Security Alliance 著作になる「重大脅威調査」の正式の所在場所は
<https://cloudsecurityalliance.org/group/top-threats/> です。

© 2017 Cloud Security Alliance – All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to The Treacherous 12 - Cloud Computing Top Threats in 2016 at <https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/>, subject to the following: (a) the Report may be used solely for your personal, informational, non-commercial use; (b) the Report may not be modified or altered in any way; (c) the Report may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to The Treacherous 12 - Cloud Computing Top Threats in 2016.

© 2017 Cloud Security Alliance — すべての権利は Cloud Security Alliance に帰属します。

以下の条件のもとに、ダウンロード、保存、コンピュータディスプレイへの表示、読み取り、印刷、
<https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/>にある「The Treacherous 12 - Cloud Computing Top Threats in 2016」へのリンクを行うことができます。

- a) このレポートが個人的、参照目的かつ非商業的目的に限定して利用されること
- b) このレポートをいかなる形・手段によらず修正もしくは変更しないこと
- c) このレポートの配布もしくは移転を行わないこと
- d) 商標、著作権その他の表示を削除しないこと

このレポートは、米国著作権法におけるフェアユース規定により認められている範囲で引用可能です。ただし、出典としてこのレポート名を明記すること。

日本語版提供に際しての告知及び注意事項

本書「危険な 12 の落とし穴 クラウドの重大セキュリティ脅威 + 2017 インシデント事例集」は、Cloud Security Alliance (CSA) が公開している「Treacherous 12 – Top Threats to Cloud Computing + Industry Insights」の日本語訳です。

本書は、一般社団法人日本クラウドセキュリティアライアンス (CSA ジャパン) が、CSA の許可を得て翻訳、公開するものです。

本書は、原文をそのまま翻訳したものです。また、本書内で参照されている URL 等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。

翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。

技術用語等について、一般に定訳があると判断したものは、極力それを使用していますが、文脈上その他の理由で、一般に用いられる訳語が妥当でないと考えた場合は、他の語に置き換えている場合があります。また、同様の理由で、技術用語に対して訳語を 1 対 1 で充てているとは限りませんので、ご了解ください。確認が必要と思われた場合は、原典に当たられることをお勧めします。

この翻訳版は予告なく変更される場合があります。以下の変更履歴 (日付、バージョン、変更内容) をご確認ください。

変更履歴

日付	バージョン	変更内容
2018 年 5 月 22 日	クラウドの重大セキュリティ脅威 2017 V1.0	初版発行

本翻訳の著作権は CSA ジャパンに帰属します。引用に際しては、出典を明記してください。無断転載を禁止します。転載および商用利用に際しては、事前に CSA ジャパンにご相談ください。

本翻訳の原著作物の著作権は、CSA または執筆者に帰属します。CSA ジャパンはこれら権利者を代理しません。

原著作物における著作権表示と、利用に関する許容・制限事項の日本語訳は、前ページに記したとおりです。なお、本日本語訳は参考用であり、転載等の利用に際しては、原文の記載をご確認ください。

【翻訳に際しての注記】

文中「**X.4 CCM V3.0.1 記載の管理策**」において、**赤字**表記は、CCM V3.0.1 の日本語版 (CSA ジャパン発行) 及び原文に照らして、本書が誤りであると考えられるものを、CCM V3.0.1 日本語版の表記に合わせたもの、control 番号以外の**青字**は、本書翻訳に際して、CCM V3.0.1 日本語版の表記が誤りであると考えられるものを、正しいものに修正したものです。

目次

謝辞	6
Executive Summary	7
調査方法	10
1. データ侵害	11
1.1. 説明	11
1.2. ビジネスインパクト	12
1.3. 文献と具体例	12
1.4. CCM V3.0.1 記載の管理策	12
1.5. リンク集	13
2. ID、認証情報、アクセス管理の不備	14
2.1. 説明	14
2.2. ビジネスインパクト	15
2.3. 文献と具体例	15
2.4. CCM V3.0.1 記載の管理策	15
2.5. リンク集	16
3. インタフェースと API のセキュリティ欠陥	17
3.1. 説明	17
3.2. ビジネスインパクト	17
3.3. 文献と具体例	18
3.4. CCM V3.0.1 記載の管理策	18
3.5. リンク集	18
4. システムの脆弱性	19
4.1. 説明	19
4.2. ビジネスインパクト	19
4.3. 文献と具体例	20
4.4. CCM V3.0.1 記載の管理策	20
4.5. リンク集	20
5. アカウントハイジャック	22
5.1. 説明	22
5.2. ビジネスインパクト	22
5.3. 文献と具体例	22
5.4. CCM V3.0.1 記載の管理策	23
5.5. リンク集	23
6. 悪意のある内部者	24
6.1. 説明	24

6.2.	ビジネスインパクト	24
6.3.	文献と具体例	25
6.4.	CCM V3.0.1 記載の管理策	25
6.5.	リンク集	25
7.	標的型攻撃の脅威	27
7.1.	説明	27
7.2.	ビジネスインパクト	28
7.3.	文献と具体例	28
7.4.	CCM V3.0.1 記載の管理策	28
7.5.	リンク集	28
8.	データの喪失	30
8.1.	説明	30
8.2.	ビジネスインパクト	30
8.3.	文献と具体例	31
8.4.	CCM V3.0.1 記載の管理策	31
8.5.	リンク集	31
9.	不十分なデューディリジェンス	32
9.1.	説明	32
9.2.	ビジネスインパクト	32
9.3.	文献と具体例	33
9.4.	CCM V3.0.1 記載の管理策	34
9.5.	リンク集	34
10.	クラウドサービスの悪用・乱用・不正使用	36
10.1.	説明	36
10.2.	ビジネスインパクト	36
10.3.	文献と具体例	37
10.4.	CCM V3.0.1 記載の管理策	37
10.5.	リンク集	37
11.	サービス妨害攻撃	39
11.1.	説明	39
11.2.	ビジネスインパクト	39
11.3.	文献と具体例	40
11.4.	CCM V3.0.1 記載の管理策	40
11.5.	リンク集	40
12.	共用技術の脆弱性	42
12.1.	説明	42
12.2.	ビジネスインパクト	42
12.3.	文献と具体例	42
12.4.	CCM V3.0.1 記載の管理策	43

12.5. リンク集	43
------------------	----

2017 年版 インシデント事例集

2017 年版 インシデント事例集	44
謝辞	45
Executive Summary	46
BOX の招待リンクの管理不備	47
ヤフーの漏えい問題	48
LinkedIn のパスワードハッシュ化に 際しての保全策の失敗	49
インスタグラムにおけるアカウント復旧機能の悪用	51
MongoDB におけるメキシコの有権者情報の漏えい	52
MongoDB の無防備に対するランサムウェアの攻撃	53
Moonpig モバイルアプリのセキュリティ欠陥	54
Dirty Cow Linux の特権奪取に関する脆弱性	55
OAuth のセキュアでない実装	57
Zynga 元従業員のデータ窃盗疑惑	58
T-Mobile における顧客情報盗難	59
NetTraveler 標的型攻撃脅威	60
Virlock ランサムウェア	62
ヤフーの漏えい問題	63
クラウドサービスを利用するマルウェアによるデータ抜き取りと検知逃れ	65
Zepto ランサムウェアのクラウド ストレージサービスをホストとした拡散	66
CloudSquirrel マルウェアによる Dropbox の C&C サーバのホスト利用	67
CloudFanta マルウェアによるクラウドストレージを利用したマルウェア拡散	68
Dyn DDoS 攻撃	69
オーストラリア統計局に対するサービス妨害	71
Cloudflare/Cloudbleed バッファオーバーフロー脆弱性	72

謝辞

共同リーダー

Jon-Michael C. Brook
Scott Field
Dave Shackleford

執筆・協力者

Jon-Michael Brook
Scott Field
Dave Shackleford
Vic Hargrave
Laurie Jameson
Michael Roza

CSA グローバルスタッフ

Victor Chin
Stephen Lumpe (Design)

CSA Chapters

CSA Greater Seattle Chapter
CSA Thailand Chapter

Executive Summary

誰も予測できなかった速さで、クラウドコンピューティングはビジネスや政府に等しく変容を迫り、そして新たなセキュリティ課題をもたらしている。クラウドのサービスモデルが開発されることで、ビジネスを支える技術はかつてないほど効率性の高いものになった。サーバを保有する発想からサービス利用ベースの思考への転換は、IT 部門にコンピューティングとアプリケーションの企画・設計・提供に関する考え方の刷新を迫っている。一方でこうした進化は新たなセキュリティ上の脆弱性を生み、以前からある脆弱性を助長し、またセキュリティ問題の本当のインパクトが完全には理解されない状態をもたらしている。クラウドコンピューティングによってもたらされるセキュリティリスクの最たるものの一つに、IT 部門あるいは情報管理責任者がバイパスされてしまう可能性の問題がある。全面的にクラウド技術にシフトすることはコストと生産性の面で利点がある一方、実施に際してはビジネスにおけるセキュリティに関するポリシー、実施手順、実践規範に注意を払わなくてはならない。そういった基準が整わない状態では、ビジネスはセキュリティ事故に対して脆弱となり、クラウドへのシフトで得られる利点を失うことにもなりかねない。

Cloud Security Alliance (CSA)は、クラウドコンピューティングの利点とリスクの両面を見据え、産業界全体に通じるクラウドセキュリティの標準を開発してきた。近年の例では、CSA は“Security Guidance for Critical Areas in Cloud Computing”(「セキュリティガイダンス」)と“Security as a Service Implementation Guidance”(「SecaaS 実装ガイド」)をリリースした。これらの著作は、「セキュリティガイダンス」では13のドメインで、また「SecaaS 実装ガイド」では 10 のサービスカテゴリで網羅的にセキュリティ課題をとらえ、クラウドコンピューティングをセキュアにするための実践規範の業界標準に、瞬く間になった。多くの企業、組織、政府機関がそのセキュリティ戦略にこれらのガイダンスを組み入れている。

上述の研究成果と同様に、“The Treacherous 12 - Cloud Computing Top Threats in 2016”(「危険な 12 の落とし穴ークラウドの重大セキュリティ脅威 2016」)は、CSA の研究体系の中で重要な位置を占めている。このレポートの目的は、組織に最新の、専門家によるクラウドセキュリティ問題の解説を提供し、クラウド活用戦略においての正しい知識に基づくリスク管理の判断をできるようにすることである。このレポートには、CSA に参加する専門家による、クラウドにおける最も深刻なセキュリティ課題についての共通認識を網羅している。

クラウドに関するセキュリティ上の懸念は多岐にわたるが、本レポートでは、クラウドコンピューティングの共有される点とオンデマンドである特性に特に関係する 12 の点に焦点を当てている。最重要課題を特定するために、CSA ではこの分野の専門家に調査を行い、クラウドコンピューティングにおける最重要のセキュリティ課題についての専門的意見を集約した。重大脅威ワーキンググループはこの調査結果を基に、その専門知識を加味して最終的に2016年度のレポートをまとめた。この最新

版のレポートでは、専門家たちは以下の12のクラウドセキュリティの重要課題を特定した。(調査結果における深刻度順となっている):

1. データ漏洩
2. 不十分なアイデンティティ・認証情報・アクセス管理
3. API のセキュリティ欠陥
4. システムとアプリケーションの脆弱性
5. アカウントの乗っ取り
6. 悪意ある内部者
7. 標的型攻撃の脅威 (APT)
8. データ喪失
9. 不適切なデューデリジェンス
10. クラウドサービスの誤用・悪用
11. DoS 攻撃
12. 共有技術の脆弱性

2016年版重大脅威のリリースは、クラウドコンピューティングに関わる意思決定における、枝葉末節のレベルから経営問題への移行を反映している。それは今や IT 部門の問題でなく経営陣の課題となっているのである。クラウドの成熟がその理由の一つかもしれないが、より重要なことは、クラウドの採用が経営陣による戦略的意思決定の対象となったことである。本書の 2013 年版は、開発者や IT 部門が自らセルフサービスでシャドーIT を取り込み、組織のセキュリティ要求事項をすり抜ける問題に焦点を当てた。2016 年には、クラウドの採用は、株主価値を最大にするという経営陣の戦略に、的確に即したものとなっていると考えられる。クラウドコンピューティングの常時稼働状態にある特性は、外部から見た時のイメージをゆがめ、企業の評価に影響を与えている。今回の調査では、アイデンティティ、認証情報とアクセス管理、API のセキュリティ欠陥、システムとアプリケーションの脆弱性といった、より広範囲に影響するアーキテクチャや設計問題が増加し、相対的にデータ喪失や個人アカウントの乗っ取りといった問題は低下した。

このレポートは、危険な 12 の落とし穴の説明と分析を行っている。クラウド利用者と事業者にとって、クラウドコンピューティングの戦略上、リスクを緩和することに向けた情報に基づく判断を行うに際しての、改訂版のガイドとして役立つであろう。この脅威分析レポートは、実践規範ガイドである「クラウドセキュリティガイダンス V3」および「Security as a Service 実装ガイド」とセットにして利用されたい。脅威分析は STRIDE の脅威モデル[1]に沿って行った。当ワーキンググループはまた、NIST のリスク管理フレームワーク[2]を情報技術リスク管理のためのガイダンスとして推奨する。これらすべてを取り込むことによって、クラウドセキュリティ戦略の総合的かつ的確な構築に際して、価値あるガイドが提供されることであろう。

2017 年に、最新の事例や出来事を更新した。

その内容は、2017 年インシデント事例集を参照されたい。

[1] STRIDE Threat Model:

[https://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx)

[2] NIST Risk Management Framework (RMF) Overview:

<http://csrc.nist.gov/groups/SMA/fisma/framework.html>

調査方法

危険な 12 の落とし穴ークラウドコンピューティング重大脅威 2016 年版作成に際して、CSA の重大脅威ワーキンググループは 2 段階の主要な調査を行った。どちらの調査も手法としてアンケート調査を用いた。

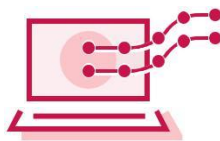
調査の第一段階における我々の狙いは、クラウドセキュリティに関する懸念事項について、簡単なリストを作ることにあった。最初に、昨年の 8 つの問題に新たに 12 の課題を加えて、セキュリティの懸念事項 20 件リストを作成した。その 20 の懸念事項について、ワーキンググループ(WG)のメンバーが各々の所属先でその重要性を示し、状況の聞き取りを行った。調査のこの段階では、調査対象企業がそれ以外の懸念事項を述べることもできるようにした。調査結果と追加で得られた情報を総合的に検討して、WG は特筆すべき 13 のクラウドセキュリティに関する懸念事項を抽出した。

調査の第 2 段階では、第 1 段階で得られたリストに対してランク付けすることが主たる目標となった。WG は、調査によって、人々が何を最も関心あるセキュリティの懸念事項と考えているかを把握しようとした。手法として 4 段階のリッカート尺度を用いることとした。リッカート尺度はアンケート調査でよく用いられる数値化手法で、あるテーマに対する人の態度を表すのに使われる。段階は 1:当てはまらない 2: 少し当てはまる 3:当てはまる 4:よく当てはまる とした。すべてのセキュリティの懸念事項に対して 1, 2, 3, 4 のどれかを選択してもらい、その数値が宛てられる。例えば「当てはまらない」としたセキュリティの懸念事項は 1 点が与えられ、「少し当てはまる」は 2 点といった具合に。各項目の数値は平均を取り、その数値によりセキュリティの懸念事項がランク付けされる。WG ではスコアの小さいセキュリティの懸念事項を振り落とし、最終的に 12 に絞った。

WG はまた、STRIDE 方式によりセキュリティの懸念事項の分析を行った。この方式はマイクロソフトにより開発され、セキュリティ脅威を評価するのに用いられる。本調査で取り上げたセキュリティの懸念事項が、特に以下の脅威のカテゴリのどれかに当てはまるかを評価するのに用いられた。

- ID の詐称(S)
- データの改ざん(T)
- 事後否認(R)
- 情報漏えい(I)
- サービス妨害(D)
- 特権の奪取(E)

1. データ侵害



調査では、271人がアンケートに回答した。その約半分(48.95%)はアメリカで、次に多いのはオーストラリア(5.02%)であった。

業種別では、44.65%が技術産業、15%が専門的サービス業、9.03%が公共部門であった。その他には教育、金融、健康医療等がある。

職務別では、87.33%がセキュリティ関係、12.22%がソフトウェア、9.95%がネットワークで、以下その他となっている。

1.1. 説明

データ侵害とは、機微情報、保護対象情報、または機密情報が外部に出たり、読み取られたり、盗まれたり、権限のない者に利用されたりする事象を言う。データ侵害は標的型攻撃の主たる目的である場合があり、または単に人的ミス、アプリケーションの脆弱性、もしくはセキュリティ対策の不足の結果であったりする。データ侵害は公開を想定していない情報が対象となり、それには個人の健康医療情報、金融資産の情報、個人識別情報(PII)、営業秘密、知的財産が含まれる。

ある組織がクラウドに置いてあるデータは、他の組織にとっては、別の理由で価値がある場合がある。例えば、犯罪組織は詐欺的な各種行為のために金融資産の情報や個人情報をもとめる。競合先や他国は固有の価値ある情報、知的財産や営業秘密に強い関心を示す。アクティビストはダメージや迷惑をもたらす情報暴露を目指す。権限のない内部者がクラウド上でデータを手に入れることは、組織の重大な関心事である。

データ侵害のリスクはクラウドコンピューティングに固有のものではないが、クラウド利用者の懸念事項としては常に上位にある。クラウド環境は従来型の企業ネットワークと同様の脅威にさらされる上に、共有リソースや、クラウド事業者の従業員や、クラウド事業者のパートナー企業といったルートからの攻撃にもさらされる。クラウド事業者へのアクセスは容易であり、そのホストする膨大なデータは魅力的なターゲットとなっている。

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメイン

**Domain 5: 情報管理と
データセキュリティ**

**Domain 10: アプリケー
ションセキュリティ**

**Domain 11: 暗号化と鍵
管理**

**Domain 12: アイデン
ティティ、権限付与、
アクセス管理**

Domain 13: 仮想化

STRIDE脅威分析

- ☐ IDの詐称(S)
- ☐ データの改ざん(T)
- ☐ 事後否認(R)
- ☒ 情報漏えい(I)
- ☐ サービス妨害(D)
- ☐ 特権の奪取(E)

1.2. ビジネスインパクト

ほとんどのデータ侵害が問題ではあるものの、一般にはダメージの深刻さはデータの機微性に左右される。世界中の国や地域で、法令や規制により、機微な情報を許可された以外の利用に対して保護するよう、しかるべき基準に基づいた対策を、組織に対して義務付けている。データ侵害が発生した場合には、企業は多額の罰金を科せられ、民事賠償訴訟を提起され、場合によっては罪に問われる。

企業にはまた、事故調査と影響を受けた顧客への通知のためのコストがかかる。事故対応をうまくやるために、専門家のコンサルティングや法務面の支援を受ける企業もある。データ侵害に遭った企業でよく行われるのは、被害に遭ったお客様の情報をモニタリングして、悪用が発見されればお客様に通知するサービスを受けることである。ブランド価値の毀損やそれに伴う事業機会の喪失といった間接被害は、算定が極めて困難である。顧客離れの度合いと、顧客獲得にかかるコストの変動分といった指標が、こういった損失の算出に用いられる。

クラウド事業者は一般的に、自らの責任範囲についてはセキュリティを充実させているが、クラウド利用者はどこまで行ってもクラウド上にある自らの管理下のデータの保護に対する責任がある。データ侵害に対する最善の保護策は、有効なセキュリティプログラムの導入である。企業がクラウド環境でセキュリティを確保するための重要な手段は、多要素認証と暗号化である。

1.3. 文献と具体例

2015 年の中頃、アンチウィルス企業である BitDefender は、AWS にホストされた自社のパブリッククラウドアプリケーションに内在したセキュリティ脆弱性の結果、顧客の名前とパスワードを窃取された。被害者の数は公表されていない。実行犯のハッカーは身代金として 15,000 ドルを要求した。

2015 年の Anthem における 8000 万人分の顧客データの流出は、社内ネットワーク上で認証情報を盗まれたことから始まった。第三者のクラウドサービスが利用されて企業内ネットワークからパブリッククラウドに多量のデータが送出され、ハッカーがダウンロードできる状態に置かれた。

イギリスの通信事業者である TalkTalk は 2014 年と 2015 年に起った複数のセキュリティインシデントを報告したが、その顧客個人情報の流出規模は 400 万人に達した。これに続いて、TalkTalk の顧客から銀行口座の情報を聞き出そうとするだましの電話の攻勢が起きた。TalkTalk は、顧客情報の暗号化を怠ったことに対して多方面から批判を浴びた。

1.4. CCM V3.0.1 記載の管理策

AIS-04: アプリケーションとインターフェースセキュリティ — データセキュリティ/完全性

CCC-02: 変更管理と構成管理 — 開発の外部委託

DSI-02: データセキュリティと情報ライフサイクル管理	－	データ保存/フロー
DSI-05: データセキュリティと情報ライフサイクル管理	－	非実稼働データ
DSI-06: データセキュリティと情報ライフサイクル管理	－	所有者/管理責任
DSI-07: データセキュリティと情報ライフサイクル管理	－	安全な廃棄
EKM-02: 暗号化と鍵管理	－	鍵作成
EKM-03: 暗号化と鍵管理	－	機微データの保護
EKM-04: 暗号化と鍵管理	－	保管とアクセス
GRM-02: ガバナンスとリスク管理	－	データフォーカスリスクアセスメント
GRM-10: ガバナンスとリスク管理	－	リスクアセスメント
HRS-02: 人事	－	経歴スクリーニング
HRS-06: 人事	－	モバイルデバイス管理
IAM-02: アイデンティティとアクセス管理	－	資格証明のライフサイクル / プロビジョニング管理
IAM-04: アイデンティティとアクセス管理	－	ポリシーと手順
IAM-05: アイデンティティとアクセス管理	－	職務の分離
IAM-07: アイデンティティとアクセス管理	－	第三者アクセス
IAM-09: アイデンティティとアクセス管理	－	ユーザアクセス権限
IAM-12: アイデンティティとアクセス管理	－	ユーザ ID 認証
IVS-08: インフラと仮想化のセキュリティ	－	本番 / テスト環境
IVS-09: インフラと仮想化のセキュリティ	－	区分
IVS-11: インフラと仮想化のセキュリティ	－	VMM セキュリティ - ハイパバイザ堅牢性
SEF-03: セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス	－	インシデントレポータリング
STA-06: サプライチェーンの管理、透明性、説明責任	－	ガバナンスのレビュー

1.5. リンク集

1. The Impact of a Data Breach Can Be Minimized Through Encryption
<https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/>
2. Dropbox and Box leak files in security through obscurity nightmare
<http://www.techrepublic.com/article/dropbox-and-box-leak-files-in-security-through-obscurity-nightmare/>
3. Anthem's Breach and the Ubiquity of Compromised Credentials
<https://blog.cloudsecurityalliance.org/2015/02/09/not-alone-92-companies-share-anthems-vulnerability/>
4. Stolen Passwords Used in Most Data Breaches
<http://www.darkreading.com/stolen-passwords-used-in-most-data-breaches/d/d-id/1204615>
5. Anti-Virus Firm BitDefender Admits Breach, Hacker Claims Stolen Passwords are Unencrypted
<http://www.forbes.com/sites/thomasbrewster/2015/07/31/bitdefender-hacked/>
6. TalkTalk Criticised for Poor Security and Handling of Hack Attack
<http://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack>

2. ID、認証情報、アクセス管理の不備



2.1. 説明

データ侵害や攻撃を可能にすることは様々な理由により生じる:適切なID・アクセス管理の欠如、多要素認証の失敗、弱いパスワード、暗号鍵・パスワード・電子証明書の継続的自動更新の仕組みの欠如などである。

認証情報や暗号鍵はソースコードに書き込んだり、GitHub のような公開のリポジトリで配布してはならない。見られたり悪用されたりする恐れが大きいからである。鍵管理が適切に行われるようにするためには、暗号鍵は適切に保管し、安全性の高い公開鍵基盤(PKI)を利用しなければならない。

ID 管理システムは拡張性を備え、何百万というユーザや多数のクラウド事業者に対応してライフサイクル管理が可能なものでなければならない。ID 管理システムは、即時的にリソースへのアクセス権を取り消す機能をサポートして、業務の終了や担当替えといった担当者の変更に対応できなければならない。

ID 管理システムは相互接続されることが多くなっており、ユーザ管理の負荷を軽減するためにクラウド事業者との ID 連携(例えば SAML アサーション)は以前にも増して一般的になりつつある。クラウド事業者との ID 連携を計画している組織は、クラウド事業者が実装している ID ソリューション廻りのセキュリティについて、プロセス、インフラ、利用者間の分離(共用 ID ソリューションの場合)などを確認しなければならない。

多要素認証-例えばスマートカード、OTP、電話認証など-はクラウドサービスのユーザとオペレータには必須である。この方式の認証は、盗まれたパスワードがユーザの同意なしにリソースへのアクセスを可能にした場合に、パスワード盗難を把握するのに役立つ。窃取されたパスワードは、"pass the hash"といったネットワーク上を探し回るタイプの攻撃に使われる。

旧式のシステムでパスワード認証しか使えない場合、認証システムは、ポリシーを厳格にする機能、例えばパスワード強度の検証や組織が指定する定期的更新を備えなければならない。

データを暗号化する暗号鍵やデータへのアクセスを保護する TLS 証明書は、保存時には定期的に更新しなければならない。そうすることで、暗号鍵が許可なく利用された場合に攻撃を検知するこ

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ダンスの対応ド メイン

**Domain 11: 暗号化と
鍵管理**

**Domain 12: アイデン
ティティ、権限付与、
アクセス管理**

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☒ 事後否認(R)
- ☒ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☒ 特権の奪取(E)

とができる。定期更新が行われない場合は、暗号鍵が盗難に遭うと、侵害に要する時間の短縮と範囲の拡大を著しく助長してしまう。

全てのデータ保護機能（パスワード、秘密鍵、利用者特定式データベース）を持つ中央集約型ストレージ構造は、攻撃者にとって極めて価値の高いターゲットになる。パスワードと暗号鍵の中央集中管理を選択することは誤りであり、組織は中央集中管理の利便性と、それが盗まれた場合の脅威のトレードオフを比較考量しなければならない。すべての重要資産と同様に、ID の保護と鍵管理システムは、最優先課題であるべきである。

2.2. ビジネスインパクト

正規のユーザ、オペレータ、または開発者になりすました不正行為者は、データの読み取り・盗み出し・改ざん・消去や、管理画面や管理コマンドの発行、送信中データの盗み見、正規のソースからを装った不正ソフトウェアの生成が可能になる。

2.3. 文献と具体例

GitHub に対するクラウドサービス認証情報の盗み出し攻撃と仮想通貨マイニングのためのアカウントハイジャック「GitHub 上のプロジェクトに格納してあったクラウドサービスの認証情報が、プロジェクト開始後 36 時間以内に、見つけ出され悪用された。」

Praetorian 社、クラウドベースのパスワード破りサービスを開始「テキサス州オースティンの情報セキュリティソリューション提供企業である Praetorian 社は、アマゾン AWS のコンピューティングパワーを活用した、パスワードハッシュを簡単に破るためのクラウドベースのプラットフォームの提供を開始した。」

2.4. CCM V3.0.1 記載の管理策

IAM-01: アイデンティティとアクセス管理	－ 監査ツールアクセス
IAM-02: アイデンティティとアクセス管理	－ 資格証明のライフサイクル/プロビジョニング管理
IAM-03: アイデンティティとアクセス管理	－ 診断/設定ポートアクセス
IAM-04: アイデンティティとアクセス管理	－ ポリシーと手順
IAM-05: アイデンティティとアクセス管理	－ 職務の分離
IAM-06: アイデンティティとアクセス管理	－ ソースコードアクセス制限
IAM-07: アイデンティティとアクセス管理	－ 第三者アクセス
IAM-08: アイデンティティとアクセス管理	－ 信頼された発行元
IAM-09: アイデンティティとアクセス管理	－ ユーザアクセス権限
IAM-10: アイデンティティとアクセス管理	－ ユーザアクセスレビュー
IAM-11: アイデンティティとアクセス管理	－ ユーザアクセス取り消し
IAM-12: アイデンティティとアクセス管理	－ ユーザ ID 認証
IAM-13: アイデンティティとアクセス管理	－ ユーティリティプログラムアクセス

HRS-01: 人事 — 資産返却
HRS-03: 人事 — 雇用契約
HRS-04: 人事 — 雇用の終了
HRS-08: 人事 — 技術的に受け入れられる使用
HRS-09: 人事 — 訓練 / 認識向上
HRS-10: 人事 — ユーザ責任

2.5. リンク集

1. Attackers Scrape GitHub for Cloud Service Credentials, Hijack Account to Mine Virtual Currency
<http://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/>
2. Dell Releases Fix for Root Certificate Fail
<http://www.bankinfosecurity.com/dell-releases-fix-for-root-certificate-fail-a-8701/op-1>

3. インタフェースと API のセキュリティ欠陥



3.1. 説明

クラウド事業者は一連のソフトウェアによるユーザインタフェース(UI)やアプリケーションプログラミングインタフェース(API)を提供しており、利用者はこれを使ってクラウドサービスとやり取りし管理する。これらのインタフェースを使って、プロビジョニング、管理、統合管理、モニタリングを行う。一般的なクラウドサービスのセキュリティと可用性は、これらの基本的 API のセキュリティに依存する。認証とアクセス管理から暗号化、動作監視まで、これらのインタフェースはポリシーに反する事故や攻撃に対して防御できる設計にしなければならない。

更に、利用企業や第三者が、これらのインタフェース上に、自社の顧客向けに付加価値サービスを構築する場合がある。この場合、追加のレイヤーの API により事態は複雑となる。なぜなら、利用者は自分の利用を可能にするために、第三者に認証情報を委ねなければならないからである。

API と UI は一般的に、IP アドレスと並んで、安心できる組織の境界線の外から利用可能な、システムの露出部分である。こういった資源は激しい攻撃にさらされるので、その防御のための適切な管理策は、防衛と検知のための第一線の備えとなる。

3.2. ビジネスインパクト

ほとんどのクラウド事業者が、そのサービスモデルにセキュリティをしっかり組み込むように努めている一方、そのサービスを使うクラウド利用者においては、クラウドサービスの使用、管理、統合管理、モニタリングに関連するセキュリティの影響を理解することが重要である。脆弱な UI や API を信じ込んでいると、組織は機密性、完全性、可用性ならびに説明責任に関わるセキュリティ上の様々な問題にさらされることになる。

アプリケーションとシステムの脅威モデルを、データフローやアーキテクチャ、設計も含めて、作成することは開発ライフサイクルにおいて常に実施すべき重要な事項になる。セキュリティに焦点を当てたコードレビューに加え、厳しい侵入検査が必須要件となる。

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメ イン

Domain 5: 情報管理と
データセキュリティ

Domain 6: 相互運用性
と移植容易性

Domain 9: インシデント
レスポンス

Domain 10: アプリケー
ションセキュリティ

Domain 11: 暗号化と鍵
管理

Domain 12: アイデン
ティティ、権限付与、
アクセス管理

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☒ 事後否認(R)
- ☒ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☒ 特権の奪取(E)

3.3. 文献と具体例

IRS の事故事例と適切な API の重要性 – 「2015 年中頃、米国歳入庁 (IRS) で脆弱な API (“Get Transcript”) のために 30 万件以上のデータが流出した。」

なぜ API の暗号鍵や機微情報の漏えいが問題として深刻化しているのか – API のセキュリティは単に API 自体のセキュリティを意味するだけではない。そこには API の暗号鍵やクラウドの認証情報や機微なデータが外部の目にさらされることに対する防御が含まれている。 – この問題は時として開発者が見落とすことがある。

3.4. CCM V3.0.1 記載の管理策

AIS-01: アプリケーションとインターフェースセキュリティ – アプリケーションセキュリティ

AIS-04: アプリケーションとインターフェースセキュリティ – データセキュリティ/完全性

IAM-08: アイデンティティとアクセス管理 – 信頼された発行元

IAM-09: アイデンティティとアクセス管理 – ユーザアクセス権限

3.5. リンク集

1. Insecure API Implementations Threaten Cloud
<http://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550>
2. Web Services Single Sign-On Contains Big Flaw
<http://www.darkreading.com/risk-management/web-services-single-sign-ons-contain-big-flaws/d/did/1103454?>
3. IRS Breach and Importance of Adaptive API Security
<http://apigee.com/about/blog/technology/irs-breach-and-importance-adaptive-api-security>
4. OWASP API Security Project
https://owasp.org/index.php?title=OWASP_API_Security_Project&setlang=en
5. Your API Authentication is Insecure, and we'll tell you why
http://sakurity.com/blog/2015/03/04/hybrid_api_auth.html
6. Why Exposed API Keys and Sensitive Data are Growing Cause for Concern
<http://www.programmableweb.com/news/why-exposed-api-keys-and-sensitive-data-are-growing-causeconcern/analysis/2015/01/05>

4. システムの脆弱性



4.1. 説明

システムの脆弱性はプログラム上の悪用対象となるバグで、攻撃者はこれを用いてコンピュータシステムに侵入し、データの窃取、システムの乗っ取り、サービス提供活動の破壊を行う。OS のコンポーネントカーネル、システムライブラリ、アプリケーションツールに潜む脆弱性は、全てのサービスとデータを重大なリスクにさらす。

このタイプの脅威は今に始まったことではない。バグはコンピュータの発明以来の問題である。ネットワークが発明されたとき、それは遠隔から操れるものになった。クラウドコンピューティングにおいてマルチテナントが導入されたことで、複数組織のシステムが相互に近接して配置されることになった。そして共有メモリとリソースへのアクセスは新たな攻撃対象面を形成している。

システムの脆弱性に対する攻撃で生じる打撃は深刻だとしても、そのような攻撃は基本的な IT プロセスで軽減させることができる。システムへの脅威に対応して定期的にシステムをスキャンし、セキュリティパッチやアップグレードをインストールすることで、システムの脆弱性に伴う未解消のセキュリティギャップを埋める長い道のりを行くことができる。セキュアな設計とアーキテクチャにより、特定のシステムへのアクセス権を制限することで、攻撃者が情報システムの全てに対して完全な支配権を持つ可能性を減らすことができる。

4.2. ビジネスインパクト

システムの脆弱性にパッチが当たっていない状態の情報システムのセキュリティに対する影響は深刻でコストがかかる。しかしながら、防御のコストは他の IT 関連の支出ー攻撃されたシステムのクリーンアップなどーに比べれば小さいものである。OS のベンダーは脅威調査コミュニティからの情報に対応して、通常共通脆弱性識別子 (CVE) の公表から数日で、無償のパッチを提供している。

同様に、脆弱性を発見し修復するための IT プロセスを導入することのコストは、脆弱性によって生じる可能性のある損害に比較すれば小さいものである。

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメ イン

Domain 1: クラウドコン
ピューティングのアー
キテクチャフレーム
ワーク

Domain 2: ガバナンスと
エンタープライズリス
クマネジメント

Domain 7: 従来からの
セキュリティ対策、事
業継続性、災害復旧

Domain 8: データセンタ
運用

Domain 10: アプリケー
ションセキュリティ

Domain 13: 仮想化

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☒ 事後否認(R)
- ☒ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☒ 特権の奪取(E)

高度の規制対象である組織（例えば政府や金融機関）は、パッチ当てを迅速に行う能力がなければならないし、可能なら、自動反復できるようにすべきである。セキュリティの管理者は、脅威対応の情報収集機能を設置しなければならない。脆弱性が公表された時点（「ゼロデイ」と呼ばれる）からベンダーによりパッチが提供されるまでの期間のギャップを埋めるために。

重要システムの緊急パッチ当てと脆弱性による影響の広がりへの対応を行う変更管理プロセスを作成して、脆弱性の修復活動が、実施され検証され完了する前に、技術チームにより適切に文書化され点検されるようにしなければならない。その他の脅威への対処手段、除去、移転、受容についても同様に文書化しトラックしなければならない。

4.3. 文献と具体例

被害は膨れ上がる。サイバー攻撃への備えは益々必須に－「Heartbleed や Shellshock は、商用ソフトウェアより安全と考えられていたオープンソースのアプリケーションでさえも脅威に対して脆弱であることを示した。これらのマルウェアは特に Linux が走るシステムに影響を与えた。このことで、Linux がベースとしている UNIX を使う Web サイトが全体の 67.7%を占めることから、懸念が広がっている。」

2015 年のデータ侵害についてのベライゾンの調査報告－「Bush に潜む ShellShock バグは、2014 年の OSS 脆弱性で 2 番目に人騒がせなイベントであった。あまりに多くの攻撃が成功した結果、Heartbleed の影が薄くなったほどだ。」

2014 年サイバー脅威防衛レポート－「攻撃の 75%は商用ソフトウェアの既知の脆弱性をつくものであり、それは通常のパッチ当てをしていれば避けられるものであった。」

4.4. CCM V3.0.1 記載の管理策

AIS-01: アプリケーションとインターフェースセキュリティ	－	アプリケーションセキュリティ
AIS-02: アプリケーションとインターフェースセキュリティ	－	顧客アクセス要求
AIS-03: アプリケーションとインターフェースセキュリティ	－	データの完全性
AIS-04: アプリケーションとインターフェースセキュリティ	－	データセキュリティ/完全性
BCR-04: 事業継続管理と運用レジリエンス	－	文書
CCC-03: 変更管理と構成管理	－	品質検査
IVS-05: インフラと仮想化のセキュリティ	－	管理 - 脆弱性管理
IVS-07: インフラと仮想化のセキュリティ	－	OS 堅牢性と基本管理
TVM-02: 脅威と脆弱性の管理	－	脆弱性 / パッチ管理

4.5. リンク集

1. 2014 Cyberthreat Defense Report

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cyberedge-2014-cdr.pdf>

2. Magnified Losses, Amplified Need for Cyber-Attack Preparedness

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf>

3. Verizon 2015 Data Breach Investigations Report

<http://www.verizonenterprise.com/DBIR/2015/>

5. アカウントハイジャック



5.1. 説明

アカウントやサービスのハイジャックは新しい問題である。フィッシングやだまし手法、ソフトウェア脆弱性の悪用といった攻撃手法はいまだに成功を収めている。認証情報やパスワードはよく繰り返し利用され、そのような攻撃のインパクトを増幅している。クラウドというソリューションはこの状況に脅威を上乗せしている。もし攻撃者が認証情報を手に入れば、行為や取引を盗み見し、データを操作し、誤った情報を返し、違法なサイトにリダイレクトするといったことができってしまう。乗っ取られたアカウントやサービスインスタンスは、新たな攻撃基地となる。そこから、乗っ取ったアカウントの信用を力として活用して、更なる攻撃を展開できる。

組織はこうしたタイプの攻撃を認識し、一般的になっている多層防御の戦略を理解し、攻撃による被害や、場合によっては訴訟を抑え込む必要がある。組織はユーザやサービス間でアカウントの認証情報を共有することを禁止し、できれば二要素認証という強力な技術を活用することを検討すべきである。全てのアカウントとそのアカウントのふるまいを、サービスアカウントも含め、モニターし、管理者から追跡可能にするべきである。

5.2. ビジネスインパクト

アカウントやサービスのハイジャックは、通常盗まれた認証情報が使われることが多く、引き続き重要脅威である。盗んだ認証情報で、攻撃者はしばしばクラウドコンピューティングサービスの重要エリアにアクセスし、そのサービスの機密性、完全性、可用性を侵害する。

攻撃者はアカウントへのアクセスを利用してデータを盗み、クラウドのサービスとシステムを破壊し、利用組織の評判を傷つけ、更に多くのことができる。

5.3. 文献と具体例

2010 年 4 月、アマゾンでクロスサイトスクリプティング (XSS) バグが確認された。このバグは攻撃者

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ランスの対応ドメ イン

Domain 2: ガバナンスと
エンタープライズリス
クマネジメント

Domain 5: 情報管理と
データセキュリティ

Domain 7: 従来からの
セキュリティ対策、事
業継続性、災害復旧

Domain 9: インシデント
レスポンス

Domain 11: 暗号化と鍵
管理

Domain 12: アイデン
ティティ、権限付与、
アクセス管理

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☒ 事後否認(R)
- ☒ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☒ 特権の奪取(E)

にサイトからの認証情報の乗っ取りを許してしまう。2009 年には、アマゾンのシステムが数多くハイジャックされ、Zeus のボットネットのノードが走らされた。

2014 年 6 月、アマゾン AWS の Code Space 社のアカウントが、管理用コンソールを多要素認証で防御していなかった結果被害に遭った。全ての情報資産が破壊され、事業が継続不能となった。

5.4. CCM V3.0.1 記載の管理策

IAM-02: アイデンティティとアクセス管理	－ 資格証明のライフサイクル/プロビジョニング管理
IAM-08: アイデンティティとアクセス管理	－ 信頼された発行元
IAM-09: アイデンティティとアクセス管理	－ ユーザアクセス権限
IAM-10: アイデンティティとアクセス管理	－ ユーザアクセスレビュー
IAM-11: アイデンティティとアクセス管理	－ ユーザアクセス取り消し
IAM-12: アイデンティティとアクセス管理	－ ユーザ ID 認証
IVS-01: インフラと仮想化のセキュリティ	－ 監査ログ / 侵入検知
SEF-02: セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス	－ インシデント管理

5.5. リンク集

1. Amazon purges account hijacking threat from site
http://www.theregister.co.uk/2010/04/20/amazon_website_treat/
2. Zeus bot found using Amazon's EC2 as C&C Server
http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/
3. Code Spaces RIP: Code hosting provider ceases trading after “well-orchestrated” DDoS attack
<http://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceasestrading-after-well-orchestrated-ddos-attack/>

6. 悪意のある内部者



6.1. 説明

悪意のある内部者によるリスクは、セキュリティ業界で議論されてきた。その脅威レベルは議論の余地があるが、内部者の脅威が実在する敵であることは議論の余地がない。CERN は内部者の脅威を以下のように定義している。

組織にとっての内部者の脅威とは、退職した職員、下請先またはその他のビジネスパートナーであって、組織のネットワーク、システム、データへのアクセス権を過去または現在有し、そのアクセス権を意図的に超えまたは悪用して、組織の情報もしくは情報システムの機密性、完全性、可用性に悪影響を与えることである。

6.2. ビジネスインパクト

悪意のある内部者、例えばシステムアドミニストレータは、機微な情報にアクセスできる可能性がある。

IaaS から PaaS、SaaS まで、悪意のある内部者は、より高いレベルのアクセス権を持ち、より重要なシステムや、更に実際問題としてデータにまで、アクセスすることができる。セキュリティ面をクラウドサービス事業者だけに頼っているシステムは、その結果より大きなリスクにさらされることになる。

クラウド事業者の提供する暗号化を利用した実装は、例えきちんとした組織でデータストレージの管理と鍵管理が分離されている事業者であっても、悪意のある内部者からの攻撃に対しては脆弱である。その場合、鍵へのアクセスは、クラウド事業者の監査可能なプロセスの中にあり、アドホックで、または見つからない方法で、見ることはできる。悪意のある内部者のリスクを抑える対策には、暗号化プロセスと鍵自体を自ら管理すること、クラウド事業者が適切なポリシーを有していること確認すること、職務の分離、ロールベースでアクセス権を最小限に制限すること、アドミニストレータの行為をしっかりとロギング、監視、監査することがある。

気をつけなければいけないのは「悪意のある内部者」が必ず悪意を持って行動するとは限らないことである。内部者は必ずしも悪意がある訳でなく、単に「自分の仕事を仕上げてしまおうとしてい

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ランスの対応ドメイン

Domain 2: ガバナンスと
エンタープライズリス
クマネジメント

Domain 5: 情報管理と
データセキュリティ

Domain 11: 暗号化と鍵
管理

Domain 12: アイデンティ
ティ、権限付与、アク
セス管理

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☐ 事後否認(R)
- ☒ 情報漏えい(I)
- ☐ サービス妨害(D)
- ☐ 特権の奪取(E)

る」場合がある。例えば、誤ってお客様のデータを公開のリポジトリにアップしたり、機微な情報を法管轄や国をまたがってコピーするかもしれない。

6.3. 文献と具体例

クラウドコンピューティングにおける内部者の脅威 – 「全体として、「内部作業」がクラウドコンピューティングにおけるセキュリティの厄災の大半の原因である。企業は、自社の機微情報を防衛するためには、セキュリティ脅威に対して事前防止型の姿勢をもって解決策を探さなければならない。」

クラウドにおける特権付与の管理のずれが内部者の脅威を増幅している – 「組織はクラウドアーキテクチャの全体にわたって、共有アカウントに制限を加え、ユーザの行為のトラッキングを改善する必要がある。」

6.4. CCM V3.0.1 記載の管理策

DCS-04: データセンタセキュリティ – オフサイト認証
DCS-08: データセンタセキュリティ – 許可されていない個人エントリ
DCS-09: データセンタセキュリティ – ユーザアクセス
DSI-04: データセキュリティと情報ライフサイクル管理 – 処理 / ラベル付 / セキュリティポリシー
DSI-06: データセキュリティと情報ライフサイクル管理 – 所有者/管理責任
EKM-02: 暗号化と鍵管理 – 鍵作成
EKM-03: 暗号化と鍵管理 – 機微データの保護
GRM-07: ガバナンスとリスク管理 – ポリシーの強制適用
GRM-10: ガバナンスとリスク管理 – リスクアセスメント
HRS-02: 人事 – 経歴スクリーニング
HRS-07: 人事 – ロール / 責任
IAM-05: アイデンティティとアクセス管理 – 職務の分離
IAM-01: アイデンティティとアクセス管理 – 監査ツールアクセス
IAM-08: アイデンティティとアクセス管理 – 信頼された発行元
IAM-09: アイデンティティとアクセス管理 – ユーザアクセス権限
IAM-10: アイデンティティとアクセス管理 – ユーザアクセスレビュー
IVS-09: インフラと仮想化のセキュリティ – 区分
STA-09: サプライチェーンの管理、透明性、説明責任 – 第三者の監査

6.5. リンク集

1. Insider threats to cloud computing
<http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/>
2. Cloud's privileged identity gap intensifies insider threats
<http://www.darkreading.com/vulnerabilities---threats/clouds-privileged-identity-gap-intensifies-insiderthreats/d/d-id/1138974>
3. Insider Threats to Cloud Computing: Directions for New Research Challenges
http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_52385.pdf

4. The Insider Threat in Cloud Computing
<https://www.infosec.aueb.gr/Publications/CRITISCloud%20Insider.pdf>

7. 標的型(APT)攻撃の脅威



[訳注:Advanced Persistent Threat は直訳すれば「進化した執拗な脅威」であるが、初出段階で IPA は標的型攻撃または標的型攻撃脅威の用語を当てた。その後「高度標的型攻撃」や「高度サイバー攻撃」も用いている。また「標的型諜報攻撃」との語も確認される。従い定訳はないと判断し、仮に「標的型攻撃」とすると共に、APT または APT 攻撃も併せて用いることとする。]

7.1. 説明

標的型攻撃(APT)はサイバー攻撃の寄生虫のようなパターンで、標的とする会社のコンピューティングインフラの中に橋頭堡を築くためにシステムに侵入し、データや知的財産を密かに盗み出すものである。APT はその目的を達するために長期間目に見えない活動をする。防御のために張り巡らせた対策に順応することもよくある。APT の侵入口の一般的なものとしては、spearphishing(特定対象に向けたフィッシング)、システムへの直接ハッキング、USB デバイスを使った攻撃コードの運び込み、パートナーネットワークを通じた侵入、セキュリティの弱い第三者ネットワークの利用などがある。ひとたび侵入を果たせば、APT はデータセンタのネットワークの中を自在に動き回り、通常のネットワークトラフィックに紛れ込んで目的を達する。

IT 部門にとっては、企業や政府機関をターゲットとする最新の進化型サイバーセキュリティ攻撃の情報を入手することは割が合う。APT の検出や除去は困難だが、予防型対策を打つことで幾分かは阻止できる。例えば、APT の侵入によく使われる spearphishing のような、ソーシャルエンジニアリング手法に気づいて対処するための教育を、ユーザに施すことは大事である。

意識涵養プログラムを定期的に強化することは、この種の攻撃に対する最良の防御の一つである。なぜならば、この種の脆弱性の多くは、ユーザが阻止したり対処したりすることが必要だからである。スタッフは、添付ファイルを開く前やリンクをクリックする前にもう一度考える習慣が、染み着い

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメイン

Domain 1: クラウドコン
ピューティングのアー
キテクチャフレーム
ワーク

Domain 2: ガバナンスと
エンタープライズリス
クマネジメント

Domain 7: 従来からのセ
キュリティ対策、事業
継続性、災害復旧

Domain 8: データセンタ
運用

Domain 10: アプリケー
ションセキュリティ

Domain 13: 仮想化

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☒ 事後否認(R)
- ☒ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☒ 特権の奪取(E)

ていなければならない

7.2. ビジネスインパクト

複雑な APT と戦うには、より高いレベルのセキュリティ対策、プロセス管理、インシデント対応計画、IT スタッフの教育が必要で、そのためにはセキュリティ予算の増額が伴う可能性がある。コストは APT 攻撃の成功に伴う財務的損害に照らして評価する必要がある。

7.3. 文献と具体例

Carbanak: 10 億ドルの APT 攻撃はいかにして阻止されたか？ — 「…Carbanak という全世界の金融機関を対象とした APT 攻撃は、今までで最大のサイバー強盗とされている…通常のサイバー犯罪の手口である利用者の認証情報を盗んだりマルウェアを使って個人のオンラインバンキングのセッションを侵したりするのでなく、Carbanak は厚かましくも銀行の内部システムと運用をターゲットとし、複数の強奪のチャンネルを手に入れて、1 銀行当り平均で 8 百万ドルを奪った。」

APT の世界の最近のトレンド — 「中国のサイバースパイと疑われている件では、APT によって『早くも 2006 年から、複数の産業にわたって、少なくとも 141 の組織からの、何百テラバイトに上るデータ』が盗まれた。」

APT の世界の最近のトレンド — 「国土安全保障省のレポートによると、APT は、『事業会社に仕向けられており、こうした新興の危険な攻撃に対して戦うためのソリューションに対する必要は世界的に急拡大している。』」

7.4. CCM V3.0.1 記載の管理策

AIS-01: アプリケーションとインターフェースセキュリティ — アプリケーションセキュリティ
 AIS-02: アプリケーションとインターフェースセキュリティ — 顧客アクセス要求
 AIS-03: アプリケーションとインターフェースセキュリティ — データの完全性
 AIS-04: アプリケーションとインターフェースセキュリティ — データセキュリティ/完全性
 BCR-04: 事業継続管理と運用レジリエンス — 文書
 IVS-01: インフラと仮想化のセキュリティ — 監査ログ / 侵入検知
 IVS-02: インフラと仮想化のセキュリティ — 変更検知
 IVS-05: インフラと仮想化のセキュリティ — 管理 脆弱性管理
 IVS-07: インフラと仮想化のセキュリティ — OS 堅牢性と基本管理
 IVS-13: インフラと仮想化のセキュリティ — ネットワークアーキテクチャ
 TVM-01: 脅威と脆弱性の管理 — アンチウイルス / 悪質なソフトウェア
 TVM-02: 脅威と脆弱性の管理 — 脆弱性 / パッチ管理

7.5. リンク集

1. Advanced Persistent Awareness.

- <http://www.trendmicro.co.uk/media/misc/apt-survey-report-en.pdf>
2. Current Trends in the APT World.
<http://resources.infosecinstitute.com/current-trends-apt-world/>
 3. Carbanak: How Would You Have Stopped a \$1 Billion APT Attack?
<https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/>
 4. Managing Information Security.
<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
 5. Understand and combat advanced persistent threats and targeted attacks.
<http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/#what-happens-during-an-attack>

8. データの喪失



8.1. 説明

個人であれ企業であれ、自分のデータを永遠に失うと想像することは恐ろしい。

クラウド上に保存されたデータは、悪意を持った攻撃以外の理由でも失われることがある。クラウド事業者が偶発的に消してしまう場合や、より悪いケースでは火事や地震のような物理的破壊によっても、クラウド事業者またはクラウド利用者が、事業継続災害復旧ならびに、日次バックアップや、可能ならオフサイト保管といった実践規範を守って、データバックアップの適切な手立てを講じていない場合には、クラウド利用者のデータが永遠に失われることになりかねない。更に、データ喪失を回避する責務はクラウド事業者の肩にだけのしかかっているのではない。クラウド利用者がそのデータをクラウドにアップする前に暗号化していて、暗号鍵をなくした場合にも、データは失われる。

クラウド利用者は、契約のデータ喪失条項を確認し、クラウド事業者の対策の冗長性について問い合わせを行って、どちらがどんな条件の下にデータ喪失に対して責任を負うのか、知っておく必要がある。クラウド事業者の一部は地理的にまたがった冗長性や、クラウド内でのバックアップや、クラウドクラウド外施設間のバックアップを提供する。データの保管、バックアップ、保護についてクラウド事業者に依存するリスクと、同様の機能をインハウスで実施することを比較考量しなければならない。データが極めて重要な場合には、両者ともに選択することも必要となろう。

8.2. ビジネスインパクト

情報は重要な資産とは見られないかもしれないが、ほとんど全ての今日の組織にとって血液と同じなのだ。ほとんどの企業が保有する、単一種類の最も価値のある資産なのである。物品を売っている小企業であっても、日々の操業のための関連するサービスがデータへのアクセスに頼っている。在庫、仕入れ先リストや顧客リスト、受注、スケジュール管理、請求書の発行、給料支払い、財務などなどである。データ喪失は致命的になる。多くの企業が、クラウド上に保存した重要データを、復旧させられることを確実にするための手立てを講じることを、経営者が怠った結果、事業を畳まざるを得ないことになってきた。

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメイン

Domain 5: 情報管理と
データセキュリティ

Domain 10: アプリケー
ションセキュリティ

Domain 12: アイデンティ
ティ、権限付与、アク
セス管理

Domain 13: 仮想化

STRIDE脅威分析

- ☐ IDの詐称(S)
- ☐ データの改ざん(T)
- ☒ 事後否認(R)
- ☐ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☐ 特権の奪取(E)

新しい EU のデータ保護ルールの下では、データの破壊と個人データの毀損はデータ侵害の一形態とみなされ、適切な報告が求められる。

さらに、多くの法令遵守ルールでは、組織は監査記録その他の文書を保存するよう求められる。そのデータをクラウドに保存していた場合、そのデータ喪失は組織の法令遵守に関する立場を危うくしかねない。

8.3. 文献と具体例

2011 年 4 月、アマゾンの EC2 がクラッシュし、多くの利用者に莫大なデータ喪失をもたらした。

2014 年 11 月、ソニーが攻撃者に侵入され、個人識別情報や従業員間の e メールやり取りなどの秘密情報が漏洩した。2015 年第 1 四半期には、ソニーはハッキングにより継続している被害に対処するために、1500 万米ドルを投入した。

2014 年 6 月、オンラインホスティングとコード発行事業者の Code Spaces 社は、ハッキングに遭い、顧客データのほとんどが改ざんされ破壊される結果となった。同社は最終的にこの攻撃による被害から回復することができず、閉鎖に追い込まれた。

8.4. CCM V3.0.1 記載の管理策

BCR-11: 事業継続管理と運用レジリエンス – 保持ポリシー
BCR-05: 事業継続管理と運用レジリエンス – 環境リスク
BCR-06: 事業継続管理と運用レジリエンス – 機器の位置
GRM-02: ガバナンスとリスク管理 – データフォーカスリスクアセスメント

8.5. リンク集

1. Cloud Computing Users Are Losing Data, Symantec Finds
<http://www.investors.com/cloud-computing-data-loss-high-in-symantec-study/>
2. Kill the Password: Why a String of Characters Can't Protect Us Anymore
<http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/>
3. Code Spaces RIP: Code hosting provider ceases trading after "well-orchestrated" DDoS attack
<http://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceases-trading-after-well-orchestrated-ddos-attack/>
4. Everything You Ever Wanted to Know About the Amazon EC2 Crash
<http://siliconangle.com/blog/2011/04/29/everything-you-ever-wanted-to-know-about-the-amazon-ec2-crash/>
5. Inside the Hack of the Century
<http://fortune.com/sony-hack-part-1/>

9. 不十分なデューディリジェンス



〔訳注:デューディリジェンスは「詳細な調査に基づく評価」といった意味だが、より重いニュアンスがあり、一般にそのまま使われているので、それに倣うこととする。〕

9.1. 説明

経営者が事業戦略を立てるに当って、クラウド技術とクラウドサービス事業者の存在は考慮に入れるべきである。クラウド技術とクラウドサービス事業者の評価に際して、うまく行くようにするためには、デューディリジェンスの実施計画とチェックリストをうまく作り上げることが重要である。デューディリジェンスを実施せずにクラウド技術を取り入れ、クラウドサービス事業者を選択する組織は、その成功を危うくする無数のリスク―営業、財務、技術、法務、遵法のあらゆる面でのリスク―に身をさらすことになる。これは、企業がクラウドへの移行を検討する場合も、移行済みまたは移行検討中の企業の吸収合併を意図している場合でも、当てはまる問題である。

9.2. ビジネスインパクト

営業面:クラウド事業者が開発予定のシステムやプロセスに依存した新しい顧客サービスを設計しても、そのような開発はクラウド事業者の技術者にとって高い優先順位を持たないかも知れない。

技術面:クラウド技術に精通していない設計者やアーキテクトがクラウドに載せるアプリケーションを開発しても、想定外の運用上または構造上の問題が起きるかも知れない。

法務面:通常運転中に使用中、移送中または保存中のデータが国外の所在場所にある場合は、あるいは復旧過程の場合であっても、規制による制約を受ける恐れがある。

遵法面:「内部」ネットワークレベルのデータプライバシーとセキュリティ対策に頼っていたアプリケーションを、クラウドに移行することは、それらの対策が失われた時には危険である。

サービスモデル

IaaS PaaS SaaS

セキュリティガイダンスの対応ドメイン

Domain 1: クラウドコンピューティングのアーキテクチャフレームワーク

Domain 2: ガバナンスとエンタープライズリスクマネジメント

Domain 3: 法律問題: 契約と電子証拠開示

Domain 4: コンプライアンスと監査マネジメント

Domain 5: 情報管理とデータセキュリティ

Domain 6: 相互運用性と移植容易性

Domain 7: 従来からのセキュリティ対策、事業継続性、災害復旧

Domain 8: データセンタ運用

Domain 9: インシデントレスポンス

Domain 10: アプリケーションセキュリティ

Domain 11: 暗号化と鍵管理

Domain 12: アイデンティティ、権限付与、アクセス管理

Domain 13: 仮想化

Domain 14: Security as a Service

クラウド技術モデルへの移行を行おうとする企業や組織にとっての最低限必要なことは、幅広いデューディリジェンスを実施して、クラウドの技術モデルを採用し、その供給事業者と付き合うことによって引き受けることになる、リスクを理解することである。

9.3. 文献と具体例

機能を果たすリソース・コントロール・ポリシー — 2012 年、Netflix が、コンテンツを顧客に配信するのに利用していた AWS パブリッククラウドが、米国東部リージョン(AWS 内で複数のゾーンにまたがっている)で、機能停止に遭った。原因は、誤ってロードバランシングを制御していた情報を消してしまったことによる。

契約と財務面での存続可能性 — 2013 年、クラウドストレージ専業で、IBM や Dell や自社の顧客のデータをホストしていた Nirvanix は、連邦破産法 11 条を申請し、営業を停止した。利用者はデータを他のサービスに移すのに 2 週間未満の期間しか与えられず、以下のような問題を浮かび上がらせた:

- データ喪失:利用者がそのデータを 2 週間以内に取り戻せなかった場合、Nirvanix 上の顧客データはどうなるのか？
- 業務障害:映像と TV の制作スタジオである Relativity Media は、Nirvanix のクラウドを、世界に展開する従業員が共同作業し、膨大なデジタルファイルを共有することで生産性を上げるためのハブとして使っていた。
- セキュリティ侵害:金詰まりのサービス事業者はセキュリティのための技術と人をけちるかも知れなく、突然のペースダウンは通常とるべきセキュリティの手順を隙間に落としてしまうことになるかも知れない。
- 法令違反:医療機関や金融機関は、政府の規制を遵守するためにデータを保持しなければならない。データが失われた場合、これらのサービスは法令違反状態になる。

M&A — 2011年、Facebook は、同社がプライバシーに関する約束を守れなかったことで顧客を裏切ったとの、FTC からの責任追及を解決した。FTC の命令によれば、Facebook は、プライバシーに関する設定を変更する場合は、他の要件と合わせて、利用者の承認の同意を得なければならない。

米国司法省の前司法次官補である Jason Weinstein は、サイバーセキュリティのデューディリジェンスの問題について簡潔にまとめて、このように述べた:「企業を買収する場合、その企業のデータを買うことになる。それはデータセキュリティ問題を買うことになるかもしれない。」別の言い方をすれば「サイバーリスクは、財務や法務のデューディリジェンスを考慮に入れるのと全く同等に考えなければならない。」

STRIDE脅威分析

- ✓ IDの詐称(S)
- ✓ データの改ざん(T)
- ✓ 事後否認(R)
- ✓ 情報漏えい(I)
- ✓ サービス妨害(D)
- ✓ 特権の奪取(E)

9.4. CCM V3.0.1 記載の管理策

AIS-01: アプリケーションとインターフェースセキュリティ	－	アプリケーションセキュリティ
AIS-04: アプリケーションとインターフェースセキュリティ	－	データセキュリティ/完全性
AAC-01: 監査保証とコンプライアンス	－	監査計画
AAC-02: 監査保証とコンプライアンス	－	独立した監査
AAC-03: 監査保証とコンプライアンス	－	情報システムに関する規制の把握
BCR-01: 事業継続管理と運用レジリエンス	－	事業継続計画
BCR-02: 事業継続管理と運用レジリエンス	－	事業継続テスト
BCR-03: 事業継続管理と運用レジリエンス	－	データセンタのユーティリティ / 環境状態
BCR-04: 事業継続管理と運用レジリエンス	－	文書
BCR-05: 事業継続管理と運用レジリエンス	－	環境リスク
BCR-06: 事業継続管理と運用レジリエンス	－	機器の位置
BCR-07: 事業継続管理と運用レジリエンス	－	機器のメンテナンス
BCR-08: 事業継続管理と運用レジリエンス	－	機器の停電
BCR-09: 事業継続管理と運用レジリエンス	－	影響解析
BCR-10: 事業継続管理と運用レジリエンス	－	ポリシー
BCR-11: 事業継続管理と運用レジリエンス	－	保持ポリシー
GRM-01: ガバナンスとリスク管理	－	ベースライン要求
GRM-02: ガバナンスとリスク管理	－	データフォーカスリスクアセスメント
GRM-03: ガバナンスとリスク管理	－	管理の監視
GRM-04: ガバナンスとリスク管理	－	管理プログラム
GRM-05: ガバナンスとリスク管理	－	経営層による補強 / 関与
GRM-06: ガバナンスとリスク管理	－	ポリシー
GRM-07: ガバナンスとリスク管理	－	ポリシーの強制適用
GRM-08: ガバナンスとリスク管理	－	リスクアセスメントにおけるポリシーインパクト
GRM-09: ガバナンスとリスク管理	－	ポリシーレビュー
GRM-10: ガバナンスとリスク管理	－	リスクアセスメント
GRM-11: ガバナンスとリスク管理	－	リスク管理フレームワーク
IVS-06: インフラと仮想化のセキュリティ	－	ネットワークセキュリティ
IVS-09: インフラと仮想化のセキュリティ	－	区分

9.5. リンク集

1. Technology: A lack of due diligence still a top threat in the cloud
<http://www.insidecounsel.com/2013/12/06/technology-a-lack-of-due-diligence-still-a-top-threat>
 [訳注：URLが無効でリンクを張れない]
2. Due Diligence: 50 Questions for Cloud Computing Providers
<http://www.techbridge.org/documents/TechBridge%20-%20Due%20Diligence%20-%2050%20Questions%20for%20Cloud%20Providers.pdf> [訳注：URLが無効でリンクを張れない]
3. With All Due Diligence
http://www.tierpoint.com/index.php/download_file/364
4. Cloud Service Vendor Evaluation and Due Diligence
<http://blog.itil.org/2015/01/itil/cloud-service-vendor-evaluation-and-due-diligence/>
5. ISO Standards Catalogue
http://www.iso.org/iso/catalogue_detail?csnumber=56269

6. How long will big-name customers like Netflix put with Amazon cloud outages?
<http://www.networkworld.com/article/2162488/cloud-computing/how-long-will-big-name-customers-like-netflix-put-up-with-amazon-cloud-outages-.html>
7. Summary of the December 24, 2012 Amazon ELB Event in the U.S.-East Region
<http://aws.amazon.com/message/680587/?tag=viglink125435-20>
8. Avoiding the Fallout From a Bankruptcy in the Cloud
<http://www.cruxialcio.com/nirvanix-bankruptcy-2037>
9. FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition
<https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed>

10. クラウドサービスの悪用・乱用・不正使用



10.1. 説明

セキュリティが不十分なまま配備されたクラウドサービス、クラウドの無償試用、支払い手段を悪用した詐欺的なアカウントのサインアップは、IaaS、PaaS、SaaS といったクラウドのコンピューティングモデルを悪意ある攻撃に曝してしまう。

悪いことを企てる者は、クラウドコンピューティングのリソースを、クラウド利用者や組織や、あるいは他のクラウド事業者を標的にする際に活用する。クラウドサービスをベースにしたリソースの悪用の事例としては、DDoS 攻撃、スパムメール、フィッシングの実行や、デジタル通貨のマイニングや、大規模なワンクリック詐欺や、認証情報データベースを盗み出してブルートフォース攻撃を仕掛けること、更には悪性のコンテンツや海賊コンテンツのホスティングがある。

クラウドサービスの悪用に対する対策としては、クラウド事業者が支払い手段偽装やクラウドサービスの悪用を検知することがあり、例えばネットワーク上の発信側・着信側の DDoS 攻撃の検出といったことである。クラウド事業者はインシデント対応の仕組みを用意して、リソースの悪用を把握しなければならないし、クラウド事業者から発信されている悪用について、クラウド利用者に通知する手段を持たなければならない。クラウド事業者はまた、クラウド利用者が自らのワークロードの状態をモニターできるための対策手段を、備えなければならない。

10.2. ビジネスインパクト

クラウドサービスのリソースが悪用されると、そのクラウド事業者にホストされた正規のクラウド利用者にとって利用可能な能力を減衰させる恐れがある。悪用に対応していると、その他のお客様サポート対応のためにあるリソースの利用が、制限される可能性がある。

不正な支払い手段を用いられた場合、その不正と無縁の存在、例えば金融機関やクラウド事業者に余計なコストを背負わせ、ひいてはクラウド利用者やその他の存在のコスト負担になる可能性がある。

クラウド事業者発の、もしくはクラウド事業者を標的とした DDoS 攻撃は、同じクラウドプラットフォー

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメイン

Domain 3: 法律問題: 契約と電子証拠開示

Domain 7: 従来からのセキュリティ対策、事業継続性、災害復旧

Domain 9: インシデントレスポンス

STRIDE脅威分析

- ☐ IDの詐称(S)
- ☐ データの改ざん(T)
- ☐ 事後否認(R)
- ☐ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☐ 特権の奪取(E)

ムにホストされた他のサイトにとって、利用可能性を失わせたり、ビジネスを阻害されたり、収益を毀損したりといった結果をもたらす恐れがある。

例えば、ある組織がこれら行為を一切行っていないとしても、クラウドサービスの共同利用という性質上、その組織にとって、データやサービスが失われるという脅威となって迫ってくる。

10.3. 文献と具体例

インターネットを破壊しかねなかった DDoS 攻撃 – 「攻撃側は、自分たち自身は恐らくその 100 分の 1 のアクセス幅しかないネットワークを使って、300Gbps 以上というトラフィックを発生することに成功した。」

ハッカーは DDoS 攻撃の発信元ハブとして利用するべく AWS に侵入した – 「アマゾンの EC2 部門は、特定されていないハッカー集団の非常に巧妙な攻撃に悩まされていた。ハッカーは、proof-of-concept のコードをリバースエンジニアリングすることによって、アクセスが容易なバックドアを仕掛け、アマゾンの提供する膨大な処理能力に侵入した。」

10.4.CCM V3.0.1 記載の管理策

- HRS-01: 人事 – 資産返却
- HRS-02: 人事 – 経歴スクリーニング
- HRS-03: 人事 – 雇用契約
- HRS-04: 人事 – 雇用の終了
- HRS-07: 人事 – ロール／責任
- HRS-08: 人事 – 技術的に受け入れられる使用
- HRS-10: 人事 – ユーザ責任
- SEF-01: セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス – 管轄当局との接点の維持
- SEF-02: セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス – インシデント管理
- SEF-03: セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス – インシデントレポーティング
- SEF-04: セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス – インシデントレスポンスの法的準備

10.5. リンク集

1. The DDoS That Almost Broke the Internet
<https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/>
2. Password Cracking in the Cloud
<http://www.networkworld.com/article/2194881/cloud-computing/password-cracking-in-the-cloud.html>
3. Hackers Sneak Back into AWS for DDoS Launch Hub

<https://vpncreative.net/2014/07/29/hackers-sneak-back-aws-ddos-launch-hub/>

4. **Praetorian Launches Cloud-based Password Cracking Service**
<http://www.securityweek.com/praetorian-launches-cloud-based-password-cracking-service>

11. サービス妨害攻撃



11.1. 説明

サービス妨害 (Denial-of-service (DoS)) 攻撃とは、サービスの利用者が自らのデータやアプリケーションにアクセスできることを妨げる攻撃である。標的となるクラウドサービスに、プロセッサ、メモリ、ディスクスペース、ネットワーク帯域といった有限の資源を異常な度合いで消費させることで、攻撃者または攻撃者集団は、分散 DoS (DDoS) 攻撃の場合のように、耐え難いシステムシャットダウンを引き起こし、正規のサービス利用者全てを混乱させ、サービスが反応しないことに憤らせる。

DDoS 攻撃は、特に犯人が政治的ハクティビズムの発想で行為に及ぶ場合には、恐怖を呼びメディアの関心を引き付けるが、それが DoS 攻撃のやり方の全てではない。非同期型のアプリケーションレベルの DDoS 攻撃は、Web サーバやデータベースやその他のクラウドリソースの脆弱性を悪用し、悪意を持った人間が、単純な極小サイズ-場合によっては 100 バイト未満-の攻撃コードでアプリケーションを取り去ることを許してしまう。他の種類の攻撃は、同様に限りある資源を標的にする。エコノミック DoS 攻撃は、クラウドのダイナミックな特性を利用して、企業のキャッシュフローを危機にさらし、スタートアップの支払い能力を麻痺させてしまう。別の形態では、組織の人的資源が官僚主義的 DoS 攻撃*のための法務対応でひっ迫させられ、企業は同様に、サービス提供ができなくなる状態に陥らされる。

[*訳注:原語は bureaucratic DoS。意味は定かでないながら、文脈からは、IT 以外のクレーム等を DoS 的に仕掛けることで、法務などの人的資源を浪費させる攻撃と推量される。]

11.2. ビジネスインパクト

DoS 攻撃に遭うことは、ラッシュアワーの交通渋滞に巻き込まれるのと似ている。目的地に到達する手段はなく、ただじっと座って待つこと以外にできることもない。利用者の立場からは、サービスの停止はフラストレーションを引き起こすだけでなく、インフラコスト削減のために重要データをクラウドに移行したことは、本当に熟慮すべきことだったと考えこませてしまう。さらにひどいことには、クラウド事業者は顧客に、コンピューティング回数とディスクスペースをベースに課金するので、攻撃が完全に自社のサービスをインターネットから締め出すに至らなくても、処理時間を大量に消費させられ、付けを回されることになる。

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメイン

Domain 8: データセンタ
運用

Domain 9: インシデント
レスポンス

Domain 10: アプリケー
ションセキュリティ

Domain 13: 仮想化

Domain 14: Security as a
Service

STRIDE脅威分析

- ☒ IDの詐称(S)
- ☒ データの改ざん(T)
- ☒ 事後否認(R)
- ☒ 情報漏えい(I)
- ☒ サービス妨害(D)
- ☒ 特権の奪取(E)

場合によっては、DDoS 攻撃は、防御側を DDoS への防戦に忙殺させることで、環境のどこかに仕掛けてある攻撃に対する煙幕として用いられる。リスクの観点からは、DoS 攻撃は、他のテナントも巻き込むので、クラウドにおける方が起きやすい。しかし、クラウド事業者は一般的に DoS 攻撃への対応により優れている。

DDoS 攻撃は、まずもって見えなければならない。故に検知が必要である。例えば Web サイトの反応が遅いということは企業にとって十分な検知方法とは言えない。検知した後にに関して言えば DDoS 攻撃に対応するカギとなるのは、発生前に備えを整えておくことである。システムアドミニストレータは、DDoS 対策として活用できるリソースに直ちにアクセスできることが必須である。

11.3. 文献と具体例

クラウドの利用が増えるに連れて、DDoS 攻撃の頻度も増す — 「クラウド事業者は DDoS 攻撃の増加に直面している。プライベートなデータセンターはすでに直面している問題[状況は似通っている]ではあるが。」

Evernote や Deezer への攻撃に続いて、Feedly も DDoS 攻撃を受け、オフラインに追い込まれた。 — 「犯罪集団による一連の連携型サイバー攻撃と同様の事象により、最近、3 つの主要なクラウドベースのサービスがオフラインに追い込まれた。ニュースまとめ事業者の Feedly、ノート機能アプリの Evernote、音楽ストリーミングサービスの Deezer は、この数日の間に相次いで犯罪集団からの攻撃に遭い、3 社ともサービス停止に追い込まれた。」

11.4. CCM V3.0.1 記載の管理策

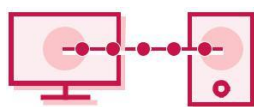
AIS-01: アプリケーションとインターフェースセキュリティ — アプリケーションセキュリティ
BCR-08: 事業継続管理と運用レジリエンス — 機器の停電
GRM-01: ガバナンスとリスク管理 — ベースライン要求
IVS-04: インフラと仮想化のセキュリティ — 情報システム文書

11.5. リンク集

1. As Cloud Use Grows, So Will Rate of DDoS Attacks
<http://www.infoworld.com/article/2613310/cloud-security/as-cloud-use-grows--so-will-rate-of-ddos-attacks.html>
2. Computerworld: DDoS is Cloud's security Achilles heel (September 15, 2011)
http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel
3. OWASP: Application Denial of Service
https://www.owasp.org/index.php/Application_Denial_of_Service
4. Radware DDoSPedia
<http://security.radware.com/knowledge-center/DDoSedia/>

5. DDoS Attacks, The Necessity of Multi-Layered Defense
<https://blog.arbornetworks.com/ddos-attacks-the-necessity-of-multi-layered-defense/>
6. Wave Of DDoS Attacks Down Cloud-Based Services
<http://www.darkreading.com/attacks-breaches/wave-of-ddos-attacks-down-cloud-based-services/d-id/1269614>
7. How New Types of DDoS Affect the Cloud
<http://www.datacenterknowledge.com/archives/2014/10/22/as-apps-move-to-the-cloud-ddos-attacks-take-new-shape/>
8. Feedly Knocked Offline by DDoS Attack Following Evernote and Deezer Attacks
<http://www.ibtimes.co.uk/feedly-knocked-offline-by-ddos-attack-following-evernote-deezer-attacks-1452237>

12. 共用技術の脆弱性



12.1. 説明

クラウド事業者は、インフラストラクチャ、プラットフォーム、アプリケーションを共用にすることで、そのサービスを伸縮自在に提供している。クラウド技術は、“as a Service”の機能を、既製品のハードウェア・ソフトウェアに大幅な変更を加えることなく分割している。一時としてセキュリティを犠牲にして、クラウドサービスの配備を担うインフラストラクチャを構成する仮想レイヤのコンポーネント（例：CPU、キャッシュ、GPU 等）は、必ずしも強力な隔離 - IaaS ではマルチテナントアーキテクチャ、PaaS では再配備可能なプラットフォーム、SaaS では複数利用のアプリケーション - の特性を示すようには設計されていない。このことは、共用技術の脆弱性につながる可能性があり、全ての配備モデルにおいて、悪用される可能性を秘めている。サービスモデルが IaaS であれ PaaS であれ SaaS であれ、多層防御の戦略が望ましく、その対象にはコンピュート機能、ストレージ、ネットワーク、アプリケーション、ユーザへのセキュリティ強化およびモニタリングを含めるべきである。大事なことは、単発の脆弱性や設定のミスでも、事業者のクラウド全体に害を及ぼす可能性があることである。

共用リソースにおける侵害を阻止する対策を実装すべきである。例えば全てのホストに多要素認証を適用、内部ネットワークに HIDS（ホストベースIDS）と NIDS（ネットワークベースIDS）を導入、最小権限と職務の分離をリンクさせるコンセプト、共用リソースのパッチの維持などである。

12.2. ビジネスインパクト

ハイパーバイザー、共用プラットフォームのコンポーネント、SaaS 環境のアプリケーションといった共用技術に不可欠の要素が攻略されると、侵害に遭った顧客を危険にさらすだけでなく、むしろ全体の環境が攻略され侵害を受ける可能性に曝される。この脆弱性は危険であり、時にクラウド全体に影響を及ぼす恐れがある。

12.3. 文献と具体例

VM 間サイドチャネル攻撃とそれを利用した秘密鍵の抜き出し - 「…アクセスドリブン型のサイドチャネル攻撃が組み込まれ、同一の物理コンピュータ上で走る標的の仮想マシンから、攻撃側の仮

サービスモデル

IaaS PaaS SaaS

セキュリティガイド ンスの対応ドメイン

Domain 1: クラウドコン
ピューティングのアー
キテクチャフレーム
ワーク

Domain 5: 情報管理と
データセキュリティ

Domain 11: 暗号化と鍵
管理

Domain 12: アイデンティ
ティ、権限付与、アク
セス管理

Domain 13: 仮想化

STRIDE脅威分析

- ☐ IDの詐称(S)
- ☐ データの改ざん(T)
- ☐ 事後否認(R)
- ☒ 情報漏えい(I)
- ☐ サービス妨害(D)
- ☒ 特権の奪取(E)

想マシンが精度の高い情報を抜き出し。。。」

VENOM 脆弱性を知ること — 「QEMU の仮想フロッピーディスクコントローラのコードにはバッファチェック欠落脆弱性 (CVE-2015-3456) がある。この脆弱性を衝くバッファオーバーフロー攻撃が成功すると、攻撃者はそのコードをハイパーバイザーのセキュリティ環境内で実行でき、ゲスト OS を躲してホスト全体を乗っ取ることが可能になる。」


12.4.CCM V3.0.1 記載の管理策

DSI-04: データセキュリティと情報ライフサイクル管理 — 処理 / ラベル付 / セキュリティポリシー
EKM-03: 暗号化と鍵管理 — 機微データの保護
GRM-01: ガバナンスとリスク管理 — ベースライン要求
IAM-02: アイデンティティとアクセス管理 — 資格証明のライフサイクル / プロビジョニング管理
IAM-05: アイデンティティとアクセス管理 — 職務の分離
IAM-12: アイデンティティとアクセス管理 — ユーザ ID 認証
IVS-01: インフラと仮想化のセキュリティ — 監査ログ / 侵入検知
IVS-09: インフラと仮想化のセキュリティ — 区分
TVM-02: 脅威と脆弱性の管理 — 脆弱性 / パッチ管理

12.5.リンク集

仮想化の隔離とベアメタルの実行のための共用技術の例:

1. EC2 Maintenance Update
<https://aws.amazon.com/blogs/aws/ec2-maintenance-update/>
2. The VENOM “virtual machine escape” bug – what you need to know
<https://nakedsecurity.sophos.com/2015/05/14/the-venom-virtual-machine-escape-bug-what-you-need-to-know/>
3. Escaping VMWare Workstation through COM1
https://docs.google.com/document/d/1sIYgqrryPK-CFWfqDntraA_Fwi2Ov-YBgMtl5hdrYd4/preview
4. Seriously, get off my cloud! Cross-VM RSA Key Recovery in a Public Cloud
<https://eprint.iacr.org/2015/898.pdf>



2017 年版 インシデント事例集

危険な 12 の落とし穴 – クラウドの重大セキュリティ脅威



2017 Edition: Industry Insights

The Treacherous 12 – Top Threats to Cloud Computing

謝辞

共同リーダー

Jon-Michael C. Brook
Scott Field
Dave Shackleford

文献と具体例の執筆・寄稿者

Fitzgerald Barth
Victor Chin
Moshe Ferber
Sean Hittel
Laurie Jameson
Nathaniel Mason
Hardeep Mehrotara
Ashish Mehta
Mihir Mohanty
Krishna Narayanaswamy
Michael Roza

CSA グローバルスタッフ

Victor Chin
Frank Guanco
John Yeoh

特別協力

Dan Hiestand

Executive Summary

この付録は、Cloud Security Alliance (CSA) の Top Threats ワーキンググループが 2016 年に発行した「危険な 12 の落とし穴ークラウドの重大セキュリティ脅威 2016」と題する調査に盛り込まれた事例の改訂版である。この 2017 年版の産業界事例集では、2016 年版で取り上げた 12 のセキュリティ問題のカテゴリに関連する最近の事故や事象 21 件を取り上げている。

本書で取り上げた産業界の事例は以下の通りである：

- BOX の招待リンクの管理不備 — データ侵害
- ヤフーの漏えい問題 — データ侵害
- LinkedIn のパスワードハッシュ化に際しての保全策の失敗 — ID、認証情報、アクセス管理の不備
- インスタグラムにおけるアカウント復旧機能の悪用 — ID、認証情報、アクセス管理の不備
- OAuth のセキュアでない実装 — アカウントハイジャック
- Zynga 元従業員のデータ窃盗疑惑 — 悪意のある内部者
- ヤフーの漏えい問題 — 不十分なデューディリジェンス
- MongoDB におけるメキシコの有権者情報の漏えい — ID、認証情報、アクセス管理の不備
- Dyn DDoS 攻撃 — サービス妨害
- Dirty Cow Linux の特権奪取に関する脆弱性 — システムの脆弱性
- T-Mobile における顧客情報盗難 — 悪意のある内部者
- MongoDB の無防備に対するランサムウェアの攻撃 — ID、認証情報、アクセス管理の不備
- クラウドサービスを利用するマルウェアによるデータ抜き取りと検知逃れ — クラウドサービスの悪用・乱用・不正使用
- オーストラリア統計局に対するサービス妨害 — サービス妨害攻撃
- Virlock ランサムウェア — データの喪失
- Zepto ランサムウェアのクラウドストレージサービスをホストとした拡散 — クラウドサービスの悪用・乱用・不正使用
- CloudSquirrel マルウェアによる Dropbox の C&C サーバのホスト利用 — クラウドサービスの悪用・乱用・不正使用
- CloudFanta マルウェアによるクラウドストレージを利用したマルウェア拡散 — クラウドサービスの悪用・乱用・不正使用
- Moonpig モバイルアプリのセキュリティ欠陥 — インタフェースと API のセキュリティ欠陥
- Cloudflare/Cloudbleed バッファオーバーフロー脆弱性 — 共用技術の脆弱性
- NetTraveler 標的型攻撃脅威 — 標的型攻撃の脅威

Top Threats ワーキンググループは、2016 年版で取り上げた 12 のセキュリティ問題に関する実事例を更新することで、読む人たちに、類似の内容を持った最新事例を知ってもらうと共に、セキュリティの世界で今何が起きているかを届けられればと考えている。

CSA Top Threats Working Group

BOX の招待リンクの管理不備

データ侵害



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 9](#)

文献と具体例

セキュリティの研究者がサーチエンジンを使っていて、数多くの個人や企業のアカウントに帰属するプライベートなデータに協同作業のリンクが張られているのを発見した。協同作業のリンクは、ユーザにファイルとフォルダへの共有アクセスを許可しており、それはファイルのダウンロード、アップロード、閲覧、編集、名前変更の許可を伴っていた。デフォルトでは、協同作業のリンクは編集者の許可に基づいて発行される。Box.com はユーザが共有範囲を広げすぎ、招待リンクを公開していることが原因だとした。だが同時に手当てを行い、以後、公開の協同作業のリンクがサーチエンジンで検索されないよう措置を取った。

リンク

<https://threatpost.com/box-com-plugs-account-data-leakage-flaw/122810/>

日付

2017 年 1 月 3 日

ヤフーの漏えい問題

データ侵害



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 9](#)

文献と具体例

2016 年 9 月、ヤフーは 10 億人以上のユーザアカウントが 2013 年 8 月に被害に遭っていたと認めた。さらに続いて、5 億人のユーザアカウントが 2014 年に侵害に遭っている。二つを合わせると、これらのセキュリティ上の失策は史上最大のデータ侵害となる。同社はデータに対する複数のハッキングは相互に連携しており、侵害は「国家の後ろ盾で行われた」、と考えている。ヤフーの CISO である Bob Lord は、ハッカーは「forged cookie」すなわちユーザのブラウザ内のキャッシュにとどまっているコードにより、web サイトへのアクセスに際して都度ログインを求められなくするやり方を利用したとしている。こうしたクッキーにより、侵入者はユーザアカウントにパスワードなしでアクセスできていた。

ヤフーが侵害を疑いだしたのは、捜査当局者が同社に接触し、ヤフーのユーザのアカウント名とパスワードが、ダークネット上のマーケットサイト「TheRealDeal」で売られていることを確認したと告げたことによってだった。売りに出していたのは「Peace of Mind」と呼ばれる者で、VICE 誌と WIRED 誌の秘密インタビューに答え、彼はある時にそのデータを手に入れ、2015 年後半から個人的に売っていたと語った。ヤフーは、盗まれたユーザアカウント情報には、名前、e メールアドレス、電話番号、生年月日、パスワードハッシュと、一部のケースでは秘密の質問と答えが暗号化または平文で含まれていたことを確認している。

ヤフーの、本件侵害に関する発見と報告の遅れは、セキュリティ対策の改善の実装と合わせて、同社に対する批判の対象となっている。

リンク

<http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html>

日 付

2016 年 9 月 22 日

LinkedIn のパスワードハッシュ化に

際しての保全策の失敗 —

ID、認証情報、アクセス管理の不備



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 12](#)

文献と具体例

報道によれば、2012年に、LinkedInは、1億6700万アカウントの認証情報をデータ侵害により紛失した。ハッカーがサイトから暗号化されたパスワードを盗み出し、侵入し、盗み出したものを翌日にロシアの犯罪集団に売り渡した。”Peace_of_Mind”の名で知られるハッカー集団は、eメールとパスワードの組み合わせがダークウェブのマーケットプレイスで売られていることを確認している。

インターネットセキュリティの専門家は、パスワードの解読は容易だったと指摘している。なぜならば、LinkedInは、ハッシュ化に際してソルトを使っていなかったからである。これは攻撃者に容易に乱数化のプロセスを遡ることを許すため、セキュアでないやり方だとされている。攻撃者は既存の標準的なレインボーテーブルを利用したり、予め作っておいた乱数化前と後の照合リストを用いたりする。

このLinkedInへの侵害は、Citrix Systemsなど他の組織におけるデータ盗難の数多くの事案につながった。

2016年6月18日、Citrixは、事故により、同社が全顧客のパスワードをリセットせざるを得なくなったことを告げる警告を発した。Citrixの製品ラインの責任者であるJohn Bennettは、Threatpostに掲載した記事の中で、問題について以下のように説明している。

「Citrixは、最近起きた事故はパスワード再利用攻撃であったと確認した。攻撃者は、ユーザ名とパスワードを他のwebサイトから盗み出し、”GoToMyPC”のアカウントにアクセスするのに利用した。」

セキュリティの研究者は、LinkedInのリストを入手した攻撃者は、ある人物の名前、職歴、パスワードを知ることができ、攻撃可能な標的のリストと、出発点になるベースのパスワードをいくつか得ることができたことを確認している。

リンク

<http://arstechnica.com/security/2016/05/then-there-were-117-million-linked-in-password-breach-much-bigger-than-thought/>

日 付

2016 年 5 月 18 日

Instagramにおけるアカウント復旧機能の悪用

ID、認証情報、アクセス管理の不備



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 12](#)

文献と具体例

セキュリティの研究者は、Instagramのパスワードリセットプロセスは、攻撃者が認証情報の入力をせずにパスワードリセットページに容易にアクセスできるようにしてしまうと結論付けた。ハッカーがアカウント ID の名前を知っていさえすれば攻撃は成功できるが、その情報は容易に推測できるものだったと研究者は推測している。パスワードリセットページから、攻撃者は一時的にロックされているアカウントの e メールアドレスと電話番号を書き換え、e メール経由でパスワードリセットを行い、アクセス権の全てを得ることができる。

おおよそ 4%に相当する、2 千万アカウントが、そうした攻撃に対して脆弱であった。しかし、この方法で侵害を受けたInstagramのアカウントの報告は今のところない。

リンク

<http://www.infosecurity-magazine.com/news/20m-instagram-accounts-vulnerable/>

日 付

2016 年 5 月 23 日

MongoDB におけるメキシコの有権者情報の漏えい

ID、認証情報、アクセス管理の不備



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 12](#)

文献と具体例

2016 年 4 月、MacKeeper 社のセキュリティ研究者である Chris Vickery は、MongoDB のオープンポート(ポート 27017)に向けて Shodan 検索エンジンを働かせていた。検索過程で、Vickery は偶然に、AWS にホストされた MongoDB の生きているインスタンスに、サービスを保護するための認証やアクセスコントロールが伴っていないことを発見した。彼はまた、メキシコ人の個人識別情報と思われる大量の情報を発見した。この情報は後に、メキシコ選挙管理委員会が所管する 9300 万人のメキシコの有権者の投票記録であることが判明した。

リンク

<http://www.informationweek.com/cloud/infrastructure-as-a-service/93-million-mexican-voter-database-exposed-on-amazon-cloud/d/d-id/1325259>

<http://www.csoonline.com/article/3060204/security/mongodb-configuration-error-exposed-93-million-mexican-voter-records.html>

https://www.theregister.co.uk/2016/04/25/mexico_voter_data_breach/

日付

2016 年 4 月 26 日

MongoDB の無防備に対するランサムウェアの攻撃

ID、認証情報、アクセス管理の不備



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 12](#)

文献と具体例

ハッカーがランサムウェアを用いてユーザデータの全部または一部を暗号化した典型例。身代金の支払い要求は、通常足がつかないビットコインという暗号通貨を使うよう要求される。最近起きたランサムウェアの攻撃はやはり、オンラインの MongoDB のインスタンスを狙い、そのインターネットからのアクセスが可能なデータベースのインストールにおける設定の脆弱性を衝いたものだった。

その手法とは:インターネットから直接アクセスが可能なデータベースは、特定のポートでクエリーリクエストを受け付けるようになっていた。クエリーリクエストが到着すると、実行の前に認証が行われる。しかしこのケースでは、データベースがインターネットからアクセス可能であるため、ポートを盗聴することで容易にその情報を入手できる。アドミニストレータにパスワードが設定されていない結果、どんな変更もアドミン権限でパスワードなしで実行できてしまう。すべてのデータを移動させて代わりに身代金要求書を置いてくることまで。データベースの所管者は、データを取り戻すために身代金を払わざるを得なかった。

他のランサムウェアの攻撃とは違い、このケースでは、予めマルウェアを感染させたり攻撃を仕掛けたりする必要がなかった。最も単純な実践規範すら怠っていたので、このデータベースは脆弱だった。攻撃を防ぐには、データベースはインターネットから見えるようにすべきでなく、むしろセットアップ段階ではローカルホストからのみアクセス可能にすべきである。更に、その他の防御策、例えばパスワードやその他のアクセス制御で適切に設定を行い、インターネット接続を可能にする前に認証の仕組みを備えるべきである。

リンク

http://www.networkworld.com/article/3154536/security/hacker-wiping-unprotected-mongodb-installs-and-holding-data-for-ransom.html#tk.twt_nww

日付

2016 年 1 月 4 日

Moonpig モバイルアプリのセキュリティ欠陥

インタフェースと API のセキュリティ欠陥



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 15](#)

文献と具体例

2015 年、ヨーロッパのオンライン挨拶カードベンダーで、e カードを送ることができるモバイルアプリを開発した Moonpig 社は、API のセキュリティの不備の結果生じたデータ侵害の被害者となった。Moonpig のモバイルアプリは固定的な認証方法を取っていて、全てのユーザに同一の証明書セットしか提供していなかった。さらに加えて、顧客 ID はシーケンシャルに番号が振られており、実践規範であるランダムシードやパディングを組み入れていなかった。攻撃者は Moonpig の顧客情報を、順番に顧客番号を試すだけで簡単に収集できた。盗み出されたイギリス、アメリカ、オーストラリアの Moonpig の顧客 360 万人は、クレジットカード番号を全部入れてはいなかったが、それでも、氏名、カードの番号下 4 桁と有効期限の情報を盗まれた。

リンク

<http://computerworld.com/article/2865794/moonpig-jeopardizes-data-of-millions-of-customers-through-insecure-api.html>

日 付

2015 年 1 月 6 日

Dirty Cow Linux の特権奪取に関する脆弱性

システムの脆弱性



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 17](#)

文献と具体例

Dirty Cow Linux の脆弱性は、2016 年 11 月にパッチが提供されるまで、少なくとも 8 年間存在していた。

この脆弱性は、カーネル内の競合状態を引き起こすことを利用して、ゲストユーザに Linux マシンに対するルート/アドミン権限レベルのアクセスを許してしまうものである。ゲストユーザのアクセスを回避するには多層防御のアプローチが有効である。

この脆弱性を衝かれると、サーバレベル（特にデフォルトで自動パッチを設定していないサーバや安全でないインターネットアクセスが可能なサーバ）と、Android マシンからのアクセスによるクライアントレベルが影響を受ける。しかも、この脆弱性へのパッチは、Android のバージョン 7.0 以降しか提供されない。

この脆弱性は可能性として 3 つのレベルでクラウドコンピューティングに影響を与える：(1)クラウド事業者は下層にあるインフラストラクチャを防御しなければならない；(2)IaaS（Infrastructure as a Service）方式を利用しているシステムは保護しなければならない；(3)アドミニストレータが使うデバイスもまた、防衛が必要である。世界で使われる全 Android マシンの 2% しか最新バージョンの 7.0 にアップデートされていない現状からすると、10 億台以上という巨大なインストールベースが攻撃される膨大な可能性を抱えている。

リンク

<https://www.linux.com/blog/how-bad-dirty-cow>

<https://threatpost.com/dirty-cow-vulnerability-patched-in-android-security-bulletin/122266/>

<https://threatpost.com/google-releases-supplemental-patch-for-dirty-cow-vulnerability/121843/>

<https://source.android.com/security/bulletin/2016-12-01.html>

<https://developer.android.com/about/dashboards/index.html>

<https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/>

<https://www.statista.com/statistics/385001/smartphone-worldwide-installed-base-operating-systems/>

日 付

2016 年 10 月 24 日

OAuth のセキュアでない実装 —

アカウントハイジャック



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 19](#)

文献と具体例

研究者たちは、市場に出回っているモバイルアプリの 40%以上は、テストしてみれば、マンインザミドル攻撃に対して脆弱であることを明らかにした。これは OAuth2.0 の実装がセキュアでないためであり、攻撃者はユーザアカウントを攻略できてしまう。根本原因は、モバイルアプリから受け取る認証情報を誤って信頼することにある。

リンク

<https://threatpost.com/oauth-2-0-hack-exposes-1-billion-mobile-apps-to-account-hijacking/121889/>

日 付

2016 年 11 月 10 日

Zynga 元従業員のデータ窃盗疑惑

悪意のある内部者



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 21](#)

文献と具体例

ゲーム企業の Zynga において、機密性の高いファイルにアクセスできる権利を持った複数の従業員が、同社の Google Drive アカウントから、大量の知的財産価値のあるデータを、ローカルの USB ドライブにコピーして退職し、ライバルのゲームメーカーに就職していた。

リンク

<http://arstechnica.com/tech-policy/2016/11/zynga-sues-2-former-employees-over-alleged-massive-data-heist/>

日付

2016 年 11 月 29 日

T-Mobile における顧客情報盗難

悪意のある内部者



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 21](#)

文献と具体例

チェコ共和国にある T-Mobile の子会社では、防ぐのが極めて難しい悪意ある内部者の犯行が見つかった。2016 年 6 月に報じられた複数のニュース配信によれば、「顧客情報を取り扱う小さなチーム」の一員だったある従業員は、闇市場で 150 万人分の顧客情報を売ろうとして逮捕された。

リンク

<http://thehackernews.com/2016/06/t-mobile-hacked.html>

日付

2016 年 6 月 20 日

NetTraveler 標的型攻撃脅威 一

標的型攻撃の脅威



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 23](#)

文献と具体例

2016 年以降一連のサイバー攻撃使われている NetTraveler という標的型攻撃脅威は、標的型フィッシングによってロシア、モンゴル、ベラルーシその他のヨーロッパの国々を標的にする集団によってばらまかれている。NetTraveler は CVE-2012-0158 脆弱性を衝くトロイの木馬で、MNKit によりビルドされたもので、URL (Uniform Resource Locator) を RAR (Roshal Archive) 形式の実行型圧縮ファイルとマイクロソフト Office の添付ファイルに変換する。

2016 年 1 月、Palo Alto Networks のブログは以下のように報じた:「2015 年 12 月 12 日、1 本の標的型フィッシングメールが、ウズベキスタン大使館の外交官に送られた。e メールタイトルと中身は偽装されており、そのメールはロシアの外相から送られたように見え、添付ファイルは上海協力機構を構成する加盟国首脳会議 (CHS Council of Heads of Member States) の公式年次報告と想定できるものであった。」

この添付ファイルは MNKit ツールキットにより作成されたものと判明した。

このメールで送られた文書を開くと、ユーザのシステムに実行ファイルが搭載され、マイクロソフトメディアサーバ (MMS) の MSCOMCTL0CX (Windows Common Controls ActiveX control) にある脆弱性を衝くもので、遠隔からの攻撃者に、被害者レベルの権限でシステム上任意のコードの実行を許すものである。

NetTraveler で使われた CVE (Common Vulnerability and Exposures) である CVE-2012-0158 は、MS Office の現バージョンでは対応済みである。しかし、この標的型攻撃は現存しており、武器製造業者、人権主義活動家や、プロ外交官のグループなどの組織を攻撃するのに使われている。

リンク

https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-a4.pdf
- Page 18 – NetTraveler APT Targets Russian, European Interests

<https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests>

<http://researchcenter.paloaltonetworks.com/2016/01/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/://thehackernews.com/2016/06/t-mobile-hacked.html>

日 付

2016 年 7 月 7 日

Virlock ランサムウェア

データの喪失



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 25](#)

文献と具体例

Virlockはランサムウェアの特異なケースで、ファイルを暗号化すると共に、そのファイルに感染し、それをポリモーフィック型ファイル生成ランサムウェアにしまうものである。その結果、次にその感染したファイルを開いたユーザは感染し、そのユーザのシステムの全てのファイルがやられて暗号化されてしまう。Virlock ランサムウェアは、ランサムウェア型とファイル感染型の組合せという新しいタイプの活動を示すもので、企業組織に害をもたらすものとなる。この感染拡大に対しては、全てのリソースを、クラウド上の共有リソースも含め、適切なセキュリティスキャンすることが必要となる。

リンク

<https://resources.netskope.com/h/i/290799411-cloud-malware-fan-out-with-virlock-ransomware>

日付

2016 年 9 月 27 日

ヤフーの漏えい問題

不十分なデューディリジェンス



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 27](#)

文献と具体例

2016 年 7 月、Verizon は Yahoo の中核のインターネット事業を 48 億ドルで買収することに合意したが、最終の買収はペンディングとなっている。この合意以降、Yahoo のセキュリティに関する 2 つの重大な侵害が明らかになっている。最初の問題 – 2013 年 8 月に発生したもの – は、2016 年 12 月に報告された。この攻撃では、約 10 億人のユーザアカウントが影響を受けた。最近の事案 – 2014 年の遅くに発生し 2016 年 9 月に報告された – は 5 億人のアカウントが被害に遭った。

開示の問題、セキュリティポリシー、セキュリティ対策、そして明らかにシステム全体にわたるセキュリティインフラ投資が不十分であったこと、に対して問題視する声が上がっている。なぜ、報告までそれほど長期を要したのか？なぜ旧式の暗号技術が使われていたのか？なぜ秘密の質問と答えは暗号化されずに保存されていたのか？

最も重要なコメントが Verizon の法務責任者である Craig Silliman によって出されている：「当社は現時点で影響が重大であると信じる合理的な根拠を有している。そして Yahoo が問題の全体像を示すことを求めている。もし Yahoo が重要性を否定するなら、それを実証する必要がある。」

攻撃の結果として、両社は 2017 年 2 月 17 日、当初の価格から 3 億 5 千万ドル引き下げるという修正後の合意を発表した。新たな条件の下では、Yahoo はこれに加えて、株主訴訟および連邦証券取引委員会 (SEC) の調査に伴う負債に責任を負うとしている。さらに、買収が完了した後も、Yahoo は引き続き、SEC 以外の調査に関するもの並びに当該侵害に関して提起される第三者の訴訟に伴って負担する負債の 50%を引き受けることになる。本件買収は、依然、2017 年第 2 四半期のどこかで完了するものと見られている。

リンク

https://en.wikipedia.org/wiki/Yahoo!_data_breaches

<https://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf>

<http://fortune.com/2016/12/19/yahoo-hack-cyber-security/>

<http://www.nbcnews.com/tech/tech-news/your-yahoo-account-was-probably-hacked-company-set-confirm-massive-n652586>

<http://www.reuters.com/article/us-verizon-yahoo-cyber-idUSKCN12D2PW>

<http://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement>

日 付

2016 年 7 月 1 日

クラウドサービスを利用するマルウェアによるデータ抜き取りと検知逃れ

クラウドサービスの悪用・乱用・不正使用



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 30](#)

文献と具体例

クラウドサービスは、アプリケーションを作成するための素晴らしいインフラストラクチャやプラットフォームを提供する。正しく設計すれば、クラウドサービスは、堅固で、アクセスが容易で、コストメリットが多くあるものである。しかしながら、その利点があるまま、ハッカーにとっても魅力的である。なぜならば、クラウドのインフラストラクチャは、ボットネットの C&C (Command and Control) をホストするにも魅力的な場所なのである。組織は大規模クラウド事業者へのアクセスをブロックすることはほとんどなく、つまりクラウドサービスは常にアクセス可能であることを意味する。なぜならば、正規のトラフィックも不正のトラフィックと同時に使われており、不正のトラフィックだけを検知することは困難だからである。

2015 年 12 月、FireEye 社のレポートは一連の標的型フィッシング—香港のメディア企業に仕向けられたもの—を報じたが、それは内部ネットワークを狙って LOWBALL マルウェアの亜種を使ったものだった。マルウェアは HTTPS プロトコルを使い、Dropbox の API にアクセスし、Dropbox の共有フォルダにあるコンフィグレーションファイルをダウンロードする。このような一般の API を商用サービスの正規のポートで使うやり方は、「群衆に紛れる」ために攻撃者に利用される手口で、ネットワーク上のある種の検出ツールを逃れることが可能になる。

リンク

<http://www.securityweek.com/malware-used-china-apt-group-abuses-dropbox>

日付

2015 年 12 月 1 日

Zepto ランサムウェアのクラウド

ストレージサービスをホストとした拡散

クラウドサービスの悪用・乱用・不正使用



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 30](#)

文献と具体例

2016 年 7 月、セキュリティ研究者たちは、クラウドユーザの間に Zepto ランサムウェアの新種が広がっていることを発見した。この Zepto ランサムウェアの新種はスパムメールによって運ばれるが、メールには気を引くようなメッセージ内容とファイル名が付けられ、受け取った者にメールを開けさせて感染したファイルをダウンロードする気にさせる。そのファイルは拡張子.wsf を付しており、ウィンドウズにスプレッドシートと似た外見のアイコンをアサインするようにさせる。このアイコン(ファイル名 spreadsheet_286.wsf)は注意深い受信者でもほとんど添付ファイルを正規のものとするようにする力がある。その結果、送られたファイルやメッセージは、マイクロソフトワンドライブ、グーグルドライブ、BOX、Dropbox といったクラウドの SaaS アプリケーションを利用する仲間たちに広まってしまう。

リンク

<https://resources.netskope.com/h/i/273457617-zepto-variant-of-locky-ransomware-delivered-via-popular-cloud-storage-apps>

日 付

2016 年 7 月 19 日

CloudSquirrel マルウェアによる Dropbox の C&C サーバのホスト利

用 —

クラウドサービスの悪用・乱用・不正使用



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 30](#)

文献と具体例

CloudSquirrel はブラジル製と見られる(名前とパラメータから)が、Java で書かれ、ServInt 社の Jelastic という PaaS を利用して拡散する。Jelastic は CloudApp という協同作業プラットフォームにリダイレクトするが、このプラットフォームは一方で、バックエンドのクラウドサービスとして AWS を使っている。このクラウド上のマルウェアはその C&C (Command and Control) 通信に Dropbox を多く使う。

CloudSquirrel の攻撃はフィッシングメール攻撃により届く。この攻撃メールは、受信者をだまして、納税通知書またはその他の公的な感じのするリンクを使って開封させようとする。メールを開封すると、CloudSquirrel は、JAR ファイルによって別の暗号化されたマルウェアのペイロードをダウンロードしてユーザを感染させる。クラウドマルウェアが Dropbox 上の C&C サーバと接続を完了すると、そのコマンドは.mp4、.wmv、.png、.dta、.wma といった偽の拡張子を伴ったプレーンテキストファイルを偽装する。

リンク

<https://resources.netskope.com/h/i/272453388-cloudsquirrel-malware-squirrels-away-sensitive-user-data-using-popular-cloud-apps>

日 付

2016 年 7 月 15 日

CloudFanta マルウェアによるクラウド

ストレージを利用したマルウェア拡散

クラウドサービスの悪用・乱用・不正使用



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 30](#)

文献と具体例

CloudFanta は標的型フィッシングメールの添付ファイルまたはリンクの形で送りつけられ、受信者を騙してファイルの実行かリンクのクリックをさせるように仕向ける。CloudFanta マルウェアは SugarSync というクラウドストレージアプリを利用して、ダウンローダーとして働く JAR ファイルを拡散する。JAR ファイルのダウンローダーは再び SugarSync を用いて “.png” 拡張子を持つ DLL ファイルをダウンロードする。この DLL ファイルは、その後 “.twerk” という拡張子に変更され、受信者の e メール認証情報を盗み、受信者に成りすましてマルウェア e メールを送信し、また同時に、受信者のオンラインバンキングの動きをモニターする。

リンク

<https://resources.netskope.com/h/i/295875750-cloudfanta-pops-with-the-cloud-using-sugarsync>

日 付

2016 年 10 月 18 日

Dyn DDoS 攻撃

サービス妨害



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 32](#)

文献と具体例

この攻撃は、侵害された IoT デバイスを利用するもので、それらの IoT デバイスはパスワード保護なしでデフォルトパスワードが有効なものであった。攻撃者は著名なセキュリティジャーナリスト Brian Krebs 氏を攻撃した後、DNS 業者である Dyn 社を標的とした。

この攻撃は、同社の顧客が主要なクラウドベース企業の多くにアクセスする際に障害となった。そのアクセス先には Twitter や Spotify や、その他の認証や暗号化といった各種のクラウドベースのサービスを提供しているクラウドサービス事業者が含まれる。これら企業のほとんどはドメインネームサービスに Dyn 社だけを使用しており、攻撃を避けることができなかった。

この攻撃の対策には、インハウスで第 2DNS を用意するか、第三者の DNS 業者をバックアップとして起用するかがある。

攻撃は最終的に感染した IoT デバイスを全てインターネットからブロックすることで収束した。IoT デバイスのメーカーがデフォルトパスワードやレガシーなネットワークプロトコル (telnet) を使い続ける限り、このような攻撃は将来も起こり続けるだろう。

リンク

<http://www.darkreading.com/attacks-breaches/ddos-attack-on-dns-provider-disrupts-okta-twitter-pinterest-reddit-cnn-others/d/d-id/1327252>

https://www.nanog.org/sites/default/files/20161016_Madory_Backconnect_S_Suspicious_Bgp_v2.pdf

<https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>

<https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/>

<http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>

<http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>

<https://blog.cloudmark.com/2016/10/21/circumventing-the-dyn-ddos-attack-and-preventing-others-like-it/>

<http://searchsecurity.techtarget.com/news/450401962/Details-emerging-o>

[n-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet](#)

日 付

2016 年 10 月 21 日

オーストラリア統計局に対するサービス妨害

サービス妨害



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 32](#)

文献と具体例

2016 年 8 月 9 日、オーストラリア統計局 (ABS) は国勢調査を初めて完全オンラインで実施する試みをしようとしていた。予想される負荷に伴う問題への対応計画と事前のシステムテストにも拘らず、調査の当夜、調査用 Web サイトはクラッシュしオフラインになった。結果として、誰も国勢調査のフォームを埋めること (法的義務) ができなかった。

ABS は 8 月 10 日以下の声明を発表した: 「2016 年オンライン国勢調査フォームは、4 種類の性質と激しさの異なるサービス妨害攻撃を受けた。最初の 3 つは小規模な障害をもたらした。... 4 番目の攻撃の後、午後 7 時 30 分過ぎに、ABS は、データの完全性を確保するために、予防的なシステムの閉鎖を行った。」

その後行われた上院の査問で、責任者は、Web サイト閉鎖をもたらした DDoS 攻撃のトラフィックの主なものはシンガポール経由でルーティングされていたと報告した。IBM の経営層は、同社が同社のルーターを「切って入れる」操作をしていれば、システム停止は起きなかっただろうことを認めた。

リンク

<http://www.cso.com.au/article/604910/attack-australian-census-site-didn-t-register-global-ddos-sensors/>

<http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbyReleaseDate/617D51FA32D27BF9CA25800A0077B7BD?>

<http://www.abc.net.au/news/2016-10-25/abs-officials-face-parliamentary-grilling-over-census/7960480>

日 付

2016 年 8 月 11 日

Cloudflare/Cloudbleed バッファオーバーフロー脆弱性

共用技術の脆弱性



オリジナルの情報

[The Treacherous 12: Cloud Computing Top Threats in 2016 - Pg. 34](#)

文献と具体例

Cloudflare はよく知られた web ベースのオンラインセキュリティサービスである。同サービスは、コンテンツの送り込み、サービス妨害攻撃やその他の Web ベースの攻撃に対する防御を提供する。2017 年 2 月、Google の Project Zero セキュリティチームの Tavis Ormandy は Cloudflare の 3 つの機能には、メモリーリークを引き起こすバッファオーバーフロー脆弱性が含まれていることを発見した。この脆弱性は、ページ内のバランスの取れていない HTML タグによって引き起こされる。Cloudflare の複数の顧客のパスワードや、API キーや、秘密のチャットがリークしたデータに含まれており、検索エンジンにキャッシュされた可能性がある。この脆弱性はその後”Cloudbleed”と名付けられ、3,438 のドメインと 150 件の顧客が影響を受けたと報じられている。

リンク

https://www.theregister.co.uk/2017/02/24/cloudbleed_buffer_overflow_bug_spaffs_personal_data/

<https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/>

日付

2017 年 2 月 23 日