NetCommonsユーザカンファレンス2017

サイバーセキュリティトレンド2017

2017年8月22日

NTTテクノクロス株式会社

NTTテクノクロス

サイバーセキュリティトレンド

環境変化			サイバー空間の変化		技術変化	
政治	経済	社会	攻撃手法	防御技術	技術	サービス

重要課題　　インシデント事例　　革新技術

サイバーセキュリティトレンド

3～5年後のセキュリティ情勢を予見

企業経営・組織運営に反映

サイバーセキュリティトレンド2017

サイバーセキュリティトレンド2017

本日ご説明する範囲

1. 新たなﾎﾞｰﾀﾞﾚｽ時代が到来し、ｻｲﾊﾞｰﾌｨｼﾞｶﾙｾｷｭﾘﾃｨが進化する
2. 事業継続性を脅かすｻｲﾊﾞｰ攻撃対策が必要となる
3. ｻﾌﾟﾗｲﾁｪｰﾝ全体でのｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄが求められる
4. ｲﾝｼﾃﾞﾝﾄ対応組織の実行力強化が求められる
5. ｿﾌﾄｳｪｱの継続的かつ効率的な脆弱性ﾏﾈｼﾞﾒﾝﾄが益々重要になる
6. ﾌﾟﾗｲﾊﾞｼｰ保護とﾃﾞｰﾀ利活用の対策が進化する
7. 無線通信ｲﾝﾌﾗが整備され、ﾓﾊﾞｲﾙｾｷｭﾘﾃｨが重要になる
8. ｾｷｭﾘﾃｨ技術者の育成が進み、ｾｷｭﾘﾃｨｽﾏｰﾄｿｰｼﾝｸﾞが加速する
9. AIを活用したｾｷｭﾘﾃｨ対策が進化する
10. 加速するﾋﾞｼﾞﾈｽｽﾋﾟｰﾄﾞに対して継続的なｾｷｭﾘﾃｨ確保も必須になる


Resilient Security
トレンド2
サービス継続性を脅かす
サイバー攻撃対策が必要
となる

急増するランサムウェア

トレンド2

ランサムウェア　＝　身代金要求型マルウェア

- Ransom（身代金）＋Software（ソフトウェア）の造語
- 端末ロック型、暗号化型の2種類
- 端末ロック型はランサムウェアを駆除すれば、再び端末操作可能
- 暗号化型はランサムウェアを駆除しても、暗号化されたデータは復元不可
  - ✓ データを復元するためには、復号鍵が必要
  - ✓ 身代金を支払っても、復号鍵が提供されるとは限らない
- 現在の主流はほとんどが暗号化型

出所　http://techtarget.itmedia.co.jp/tt/news/1608/02/news03.html

事例 米ロサンゼルスの病院、ランサムウェアに感染して身代金支払う

トレンド2

マルウェアによりファイルが暗号化され、システムダウン。40ビットコイン（1万7000ドル相当）の身代金要求に応じて復旧。

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

February 17, 2016

I am writing to talk to you about the recent cyber incident which temporarily affected the operation of our enterprise-wide hospital information system.

It is important to note that this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way. Further, we have no evidence at this time that any patient or employee information was subject to unauthorized access.

On the evening of February 5th, our staff noticed issues accessing the hospital's computer network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically. Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The reports of the hospital paying 9000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the

- 2016年2月5日、攻撃が発覚、電子カルテシステムがロック
- 救急患者を別の病院に転院させる事態に！
- 同17日、要求された身代金を支払ってシステムを復旧させたと発表

出所　http://www.itmedia.co.jp/enterprise/articles/1602/19/news063.html

サンフランシスコ市交通局、ランサムウェアで一部システムに被害

駅の端末や券売機のディスプレイに脅迫メッセージが表示、暗号化を解除する代わりに7万3000ドルを要求

2112台のコンピュータが感染。
MUNIネットワーク8500台に被害。

- 2016年11月25日、感染が発覚、券売機を停止
- 同26日、乗車料金を無償化
- 同27日、システム復旧

出所　http://www.gizmodo.jp/2016/11/san-francisco-muni-hacked.html
http://www.itmedia.co.jp/enterprise/articles/1611/29/news076.html

過去最悪のサイバー攻撃

2017年5月12日以降、世界150カ国、30万台超のマシンがWannaCryに感染

- WindowsのSMBv1(445/tcp)の脆弱性（注）を突いて感染
- ワーム（自己拡散）機能を搭載し、脆弱なシステムを探索して感染を拡大
- ファイルを暗号化して、身代金としてビットコインを要求($300相当)
- 多言語（28言語）対応
- ポート445は日本で約3万件、世界で50万件以上が開放。本脆弱性が残っているもの７割以上（ﾄﾚﾝﾄﾞﾏｲｸﾛ調査:5/18現在）

(注）SMB:Server Message Block(ファイル共有プロトコル)。2017年3月14日に修正パッチが公開。ハッカー集団Shadow Brokersが米国家安全保障局（NSA）から攻撃コード（EternalBlue）を盗み出し、2017年4月に公開。

出所　http://www.yomiuri.co.jp/science/goshinjyutsu/20170519-OYT8T50016.html
https://japan.cnet.com/article/35101490/
http://www.itmedia.co.jp/enterprise/articles/1705/16/news028.html
https://www.businessinsider.jp/post-33641

重要性を増すセキュリティレジリエンス

トレンド2

- 身代金を要求するランサムウェアが急増
- サイバー攻撃によってサービス継続性が脅かされる時代

- サイバーセキュリティの観点からBCP（事業継続計画）策定が必要
- 特に、ランサムウェア対策として、システム/ファイルのバックアップ対策が必要（復旧手順策定、訓練も重要）
- 未然防止のためには、ソフトウェアの最新化/脆弱性管理が重要

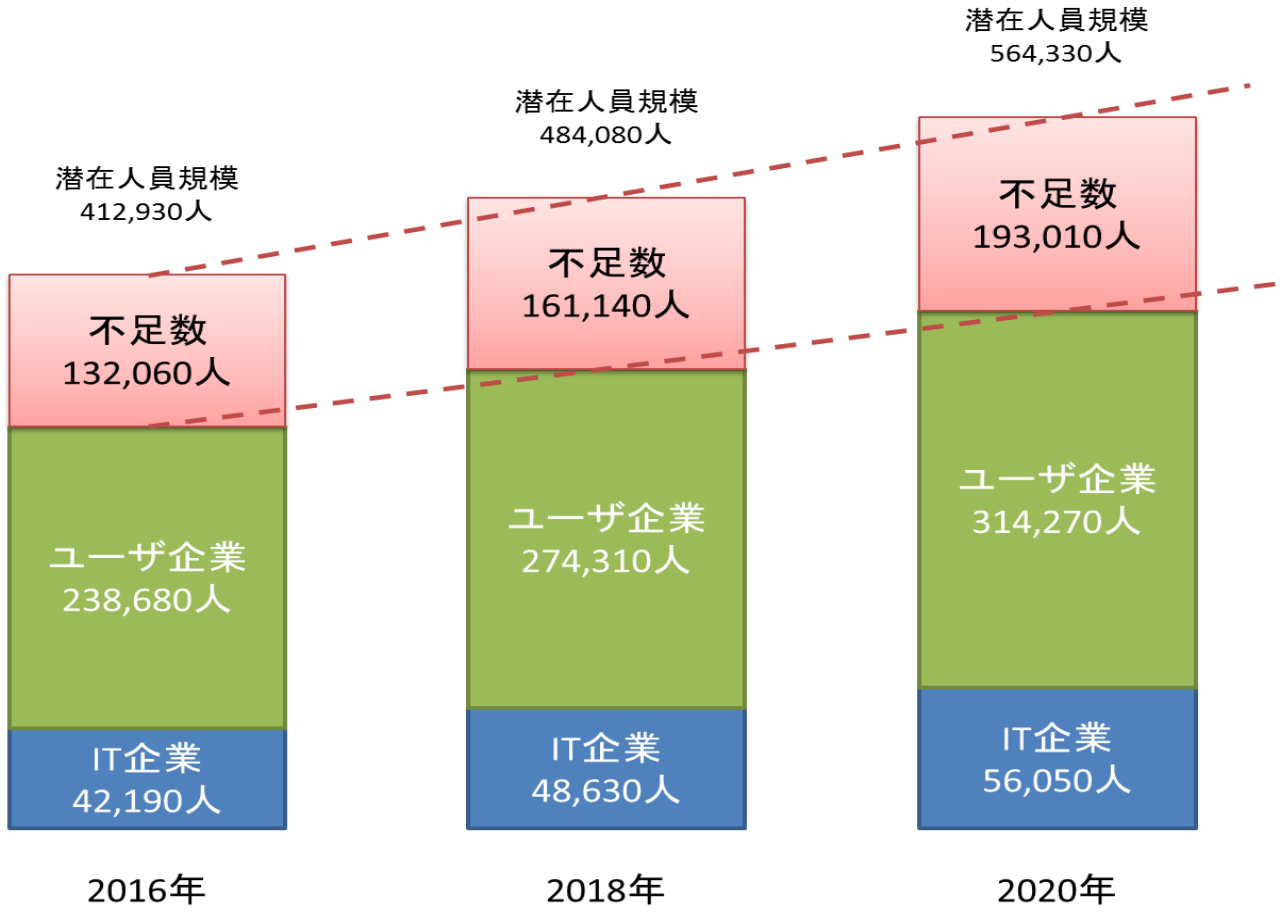
Resilient Security


トレンド８
セキュリティ技術者の育成が進み、セキュリティスマートソーシングが加速する

セキュリティ人材の不足数

トレンド8

現時点で情報セキュリティ人材は28万人、不足数は13万人
2020年までに不足数が19万人にまで拡大

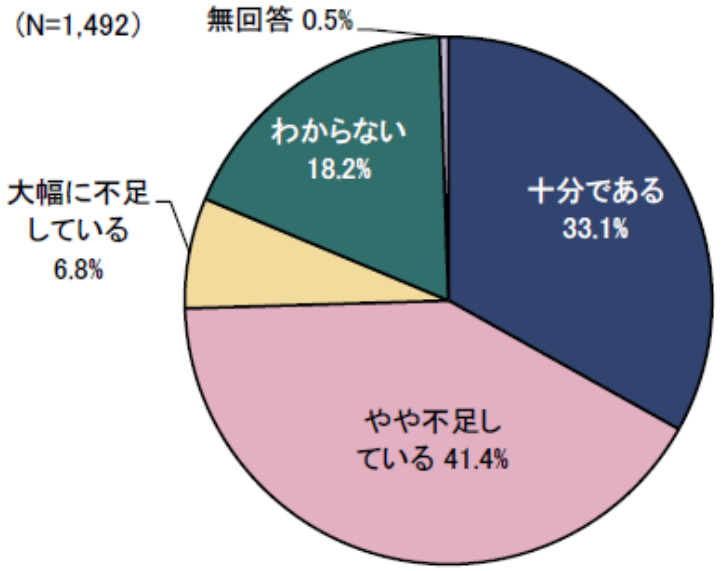


出所　経済産業省「IT人材の最新動向と将来推計に関する調査結果」（平成28年6月10日）

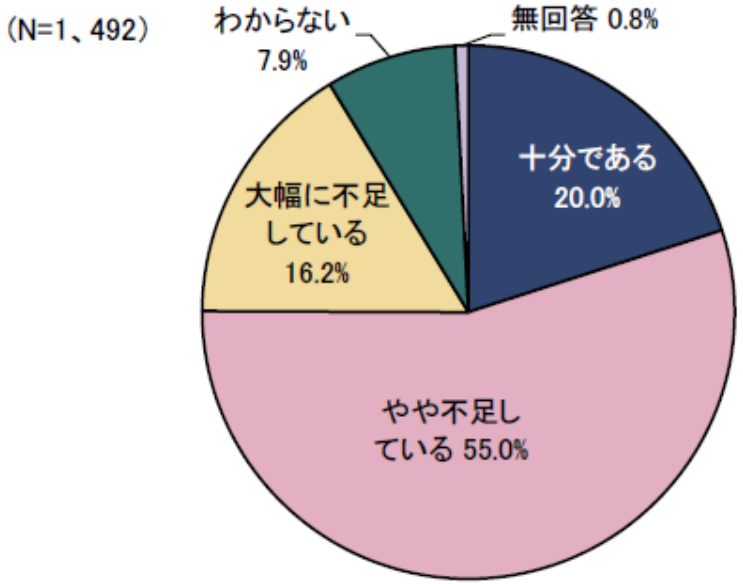
情報セキュリティ業務担当者の充足度（IPA調査）

量的充足度よりも質的充足度のほうが深刻。

量的な充足度



スキル面での充足度

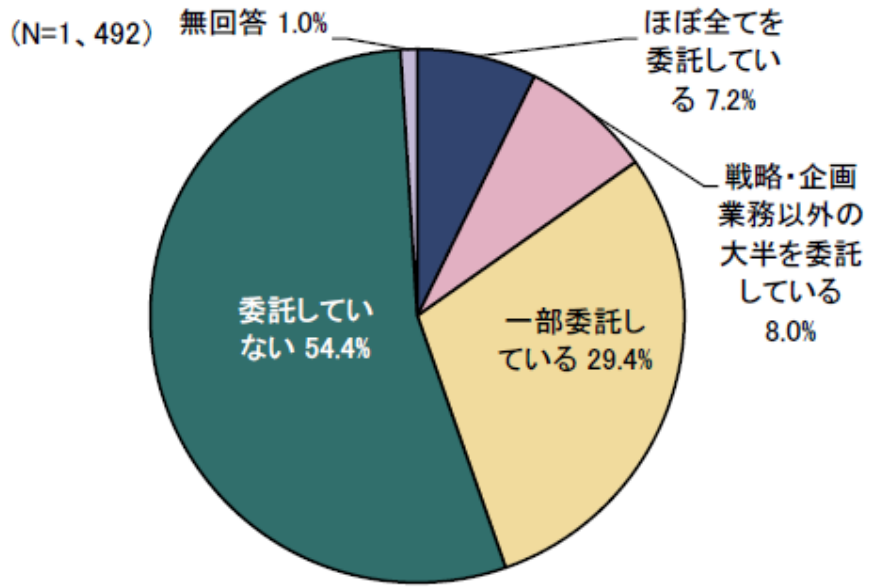


出所　IPA/ISEC「2014年度 情報セキュリティ事象被害状況調査 －報告書－」（2015年1月）

情報セキュリティ業務の外部委託（IPA調査）

トレンド8

半数以上の企業は情報セキュリティ業務を外部委託していない



出所　IPA/ISEC「2014年度 情報セキュリティ事象被害状況調査 －報告書－」（2015年1月）

ソーシングの最適化を図ったスマートソース時代へ

トレンド8

アウトソーシング戦略の巧拙が、将来にわたる企業のソーシング全体の成否を分ける

ガートナー、2016年以降の日本におけるソーシングとITサービスの展望を発表（2015年12月9日）

■ **重要なポイント**

✓インソース人材の育成と最適配置、キャリアパス

✓インソース/アウトソースの最適化

✓戦略的パートナーの選択（アウトソース先の妥当性）

出所　https://www.gartner.co.jp/press/html/pr20151209-01.html
http://www.bizcompass.jp/original/bu-growth-052-1.html

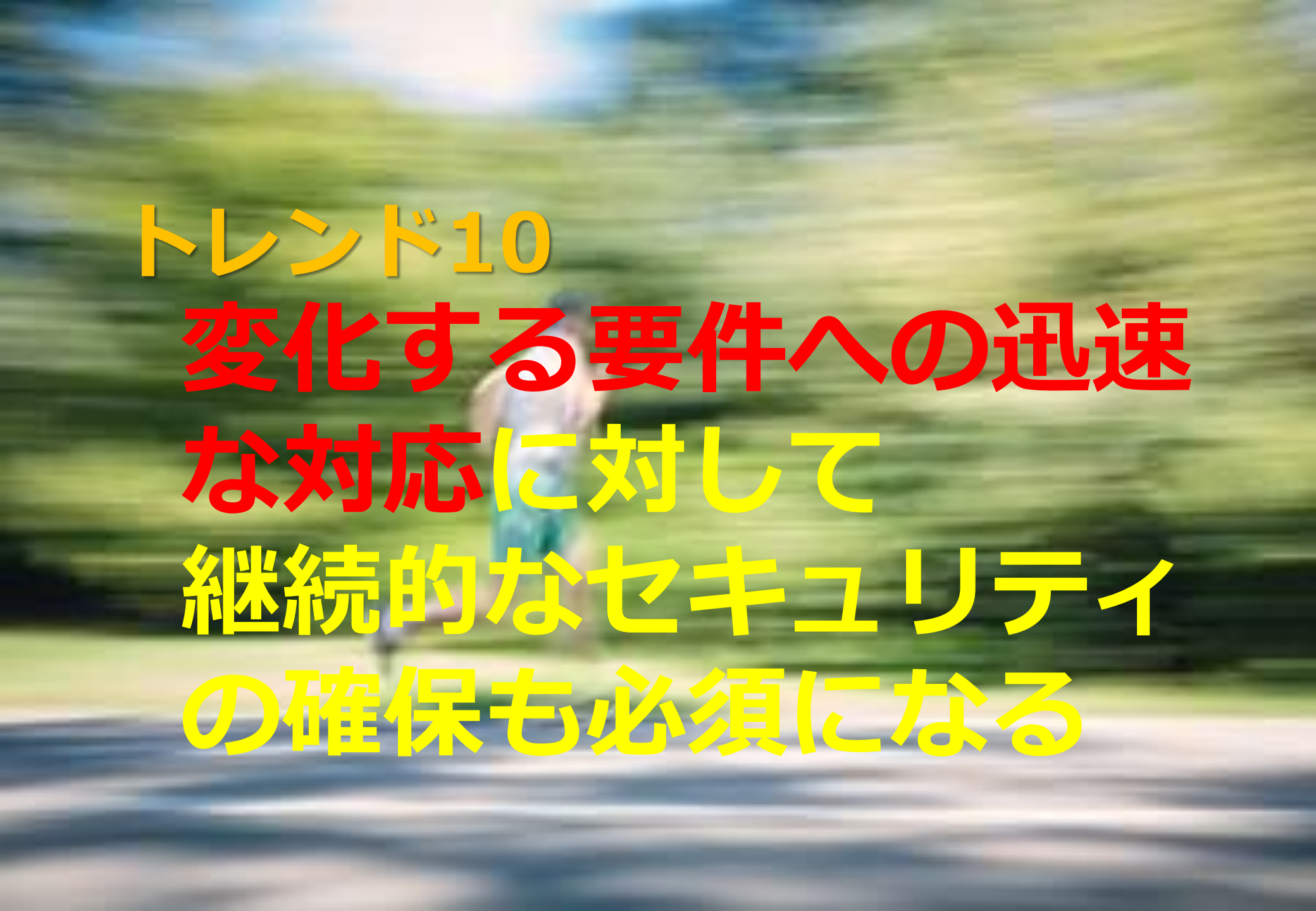
セキュリティ人材の育成とスマートソーシングの拡大

トレンド8

- セキュリティ技術者が量的、質的に決定的に不足
- セキュリティ業務の外部委託も少ない

- 自社内に必要なインソース人材の定義と育成が必要
- 自社の実態、目標に合わせてインソース/アウトソース戦略を立案し、徐々に全体最適化していくべき
- アウトソース先としてのパートナー戦略が益々重要

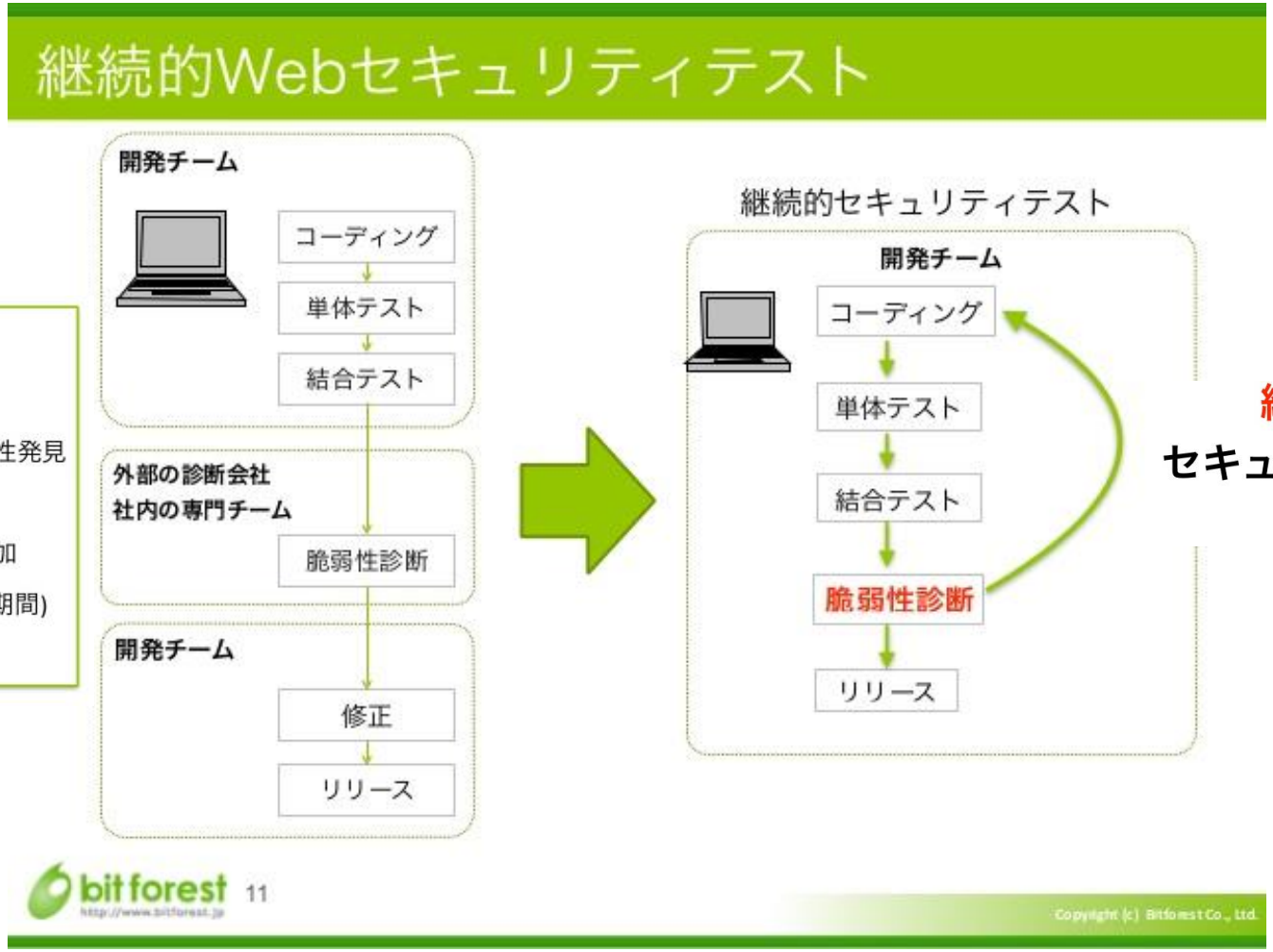
Security Smartsourcing


トレンド10
変化する要件への迅速な対応に対して
継続的なセキュリティの確保も必須になる

開発プロセスの中に継続的なセキュリティ診断を組み込む

トレンド10

リリース直前、リリース後の診断のみでは開発スケジュールの遅延やコスト増を招くため、継続的なセキュリティ診断が必要。



出所　株式会社ビットフォレスト・市川「Jenkinsを使った継続的セキュリティテスト」（2015年1月11日）

継続的インテグレーション/継続的デリバリやテスト自動化の中にセキュリティを組み込むというアプローチ

- セキュアプロダクトライフサイクル（SLPC）を規定
- 「アジャイル」を推進
- 「Secure by Design」を維持
- アジャイル開発において描かれる「ユーザーストーリー」と同様に「セキュリティストーリー」を作成し、対等に扱う
- セキュアな開発フレームワークやツールを標準化
- 属人性を排除して、ルーチンの中に自動的にセキュリティを組み入れる

出所　http://www.atmarkit.co.jp/ait/articles/1603/22/news035_2.html
https://www.paypal.com/jp/home

求められる継続的なセキュリティ

トレンド10

高まるセキュリティ脅威と求められるスピード開発の中において、継続的なセキュリティの確保が必要

高まる脅威

- 日々発見される脆弱性
- 悪質化する攻撃

求められるスピード開発

継続的なセキュリティの確保

Continuous Security

結びに

まとめ

- 急増するサイバー攻撃
- 先を見通したリスクコントロールが必要
- サイバーセキュリティトレンド2017をご紹介

ランサムウェアの急増により、サービス継続のためのサイバー攻撃対策が必要

セキュリティ技術者が不足しており、インソース/アウトソースの最適化と戦略的パートナーの選択が重要

高まるセキュリティ脅威と求められるスピード開発の中において、継続的なセキュリティの確保が必要

ダイジェスト版、詳細版がダウロード可能

弊社HPから、サイバーセキュリティトレンド2017がダウンロードできます。

https://www.ntt-tx.co.jp/products/cs-trend/

ダイジェスト版

詳細版

ご清聴ありがとうございました