サイバーセキュリティトレンド2018

～ 急増するビジネスメール詐欺の動向を中心に ～

2018年5月23日

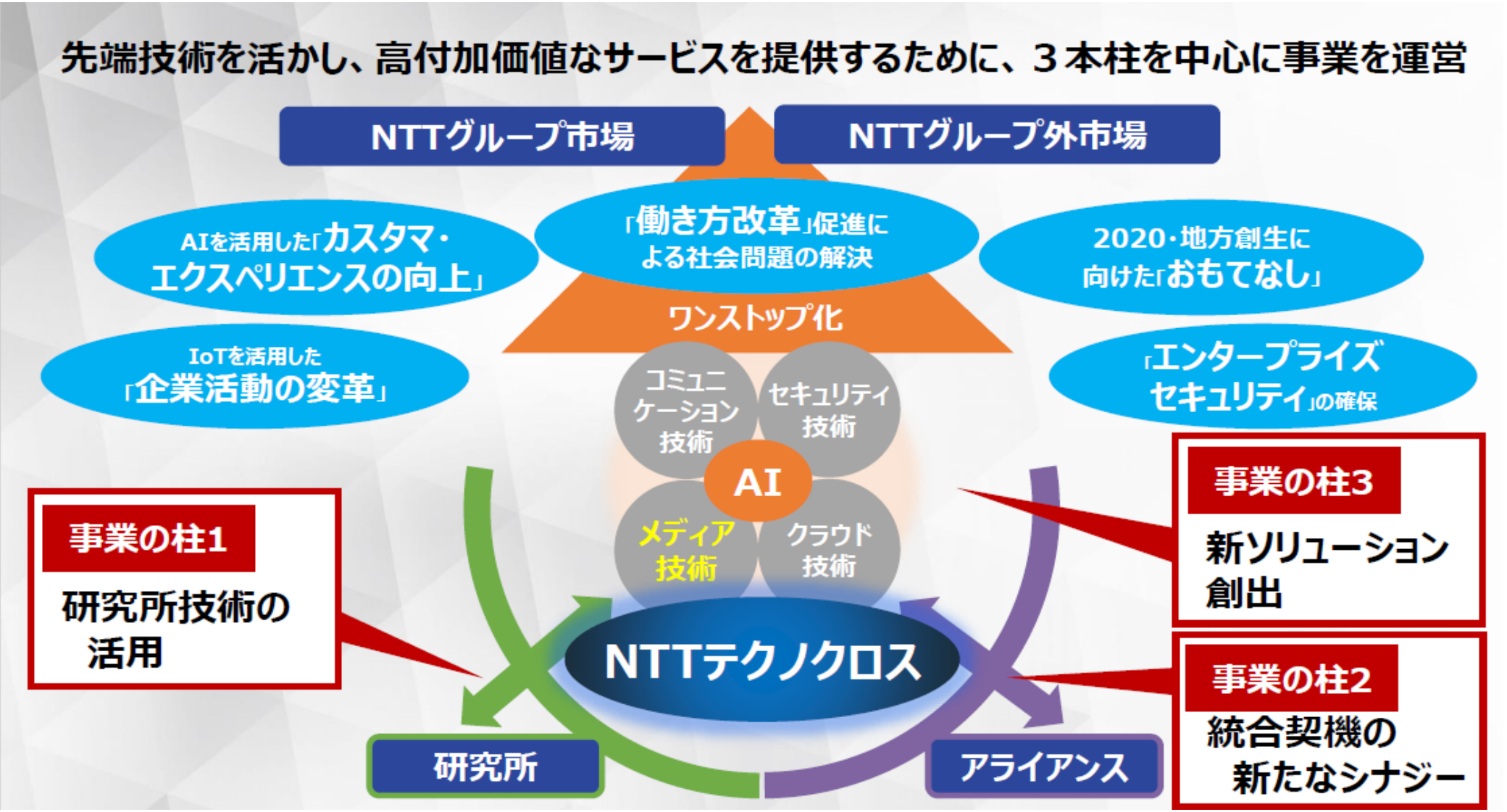
NTTテクノクロス株式会社

NTTテクノクロス

NTTテクノクロス株式会社（2017年4月1日新会社発足）

商号	ＮＴＴテクノクロス株式会社 NTT TechnoCross Corporation
設立	2017年4月1日 ←旧NTTｿﾌﾄｳｪｱ/旧NTTｱｲﾃｨ(合併)、NTTｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ・音響映像事業(統合)
資本金	5億円
売上高	32,243百円（2017年3月期）＜旧NTTｿﾌﾄｳｪｱの数値＞
社員数	1,735名(2018年3月末日現在)
代表取締役社長	串間　和彦
業務内容	1.情報通信ネットワークを利用する情報提供、情報処理、決済(代理徴収を含む)など各種サービスの提供、各種情報制作およびそれらサービス提供に必要なシステムの賃貸・販売に関すること。 2.情報通信システムの設計、開発、建設、販売、賃貸、管理、運用・保守およびシステム評価に関すること。 3.ソフトウェアの設計、開発、販売、賃貸、運用・保守および品質管理に関すること。 4.ハードウェアの開発、製造、販売、賃貸、設置、および保守に関すること。 5.前各号に係わる新技術の調査、その応用開発、コンサルティング、教育および研修に関すること。

事業の３つの柱



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

組織運営に反映

サイバーセキュリティトレンド2018

本日お話する内容

強化 1. IoT脆弱性があらゆるものをｻｲﾊﾞｰ攻撃に加担させる

強化 2. 事業継続性を脅かすｻｲﾊﾞｰ攻撃対策が益々重要となる

強化 3. ｻﾌﾟﾗｲﾁｪｰﾝ/ﾋｭｰﾏﾝﾈｯﾄﾜｰｸに介在するｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ攻撃が増大する

4. ｲﾝｼﾃﾞﾝﾄ対応組織の実践力が問われる

5. IT資産管理/脆弱性管理/ｼｬﾄﾞｰIT対策が加速する

6. ﾌﾟﾗｲﾊﾞｼｰ保護対策が進み、ﾊﾟｰｿﾅﾙﾃﾞｰﾀ利活用のﾁｬﾚﾝｼﾞが進行する

7. ﾓﾊﾞｲﾙ利用の加速に伴い、攻撃のﾀｰｹﾞｯﾄがﾓﾊﾞｲﾙにｼﾌﾄする

強化 8. AIを悪用した攻撃技術とAIを活用した防御技術がしのぎを削り、ﾏｼﾝ戦争時代に突入する

9. 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となる

New 10. 仮想通貨をﾀｰｹﾞｯﾄとしたｻｲﾊﾞｰ攻撃が増大する

情報セキュリティ10大脅威2018（IPA）

■「情報セキュリティ 10 大脅威 2018」　　NEW：初めてランクインした脅威

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	インターネットバンキングやクレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
3 位	スマートフォンやスマートフォンアプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃によるサービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化（アンダーグラウンドサービス）	9 位

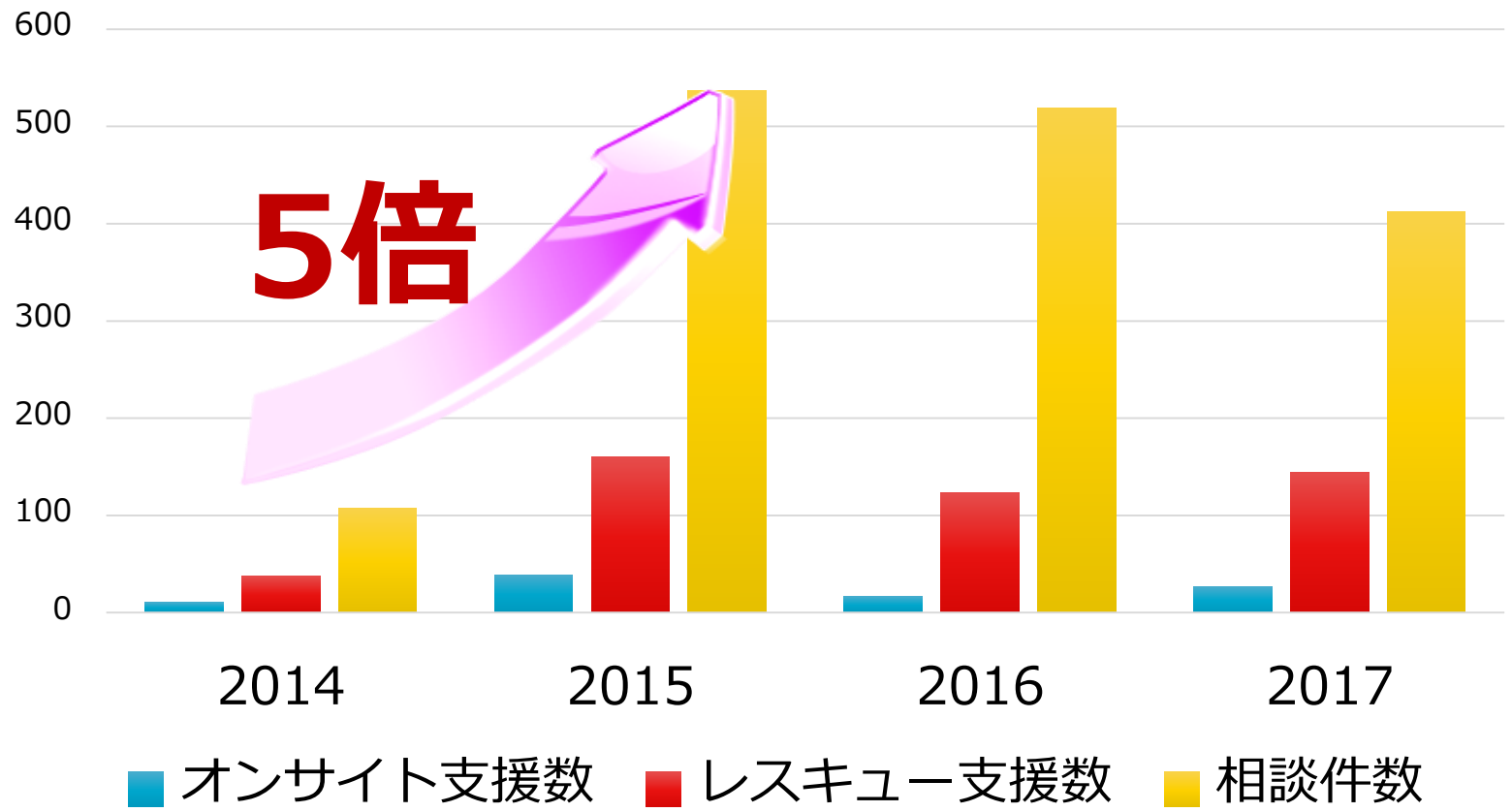
出所　https://www.ipa.go.jp/security/vuln/10threats2018.html


Supply Chain Security
トレンド3
サプライチェーン/
ヒューマンネットワーク
に介在するソーシャル
エンジニアリング攻撃が
増大する

サイバーレスキュー隊の標的型サイバー攻撃支援の推移

トレンド3

「標的型サイバー攻撃特別相談窓口」に寄せられた相談件数は減少傾向にあるが、オンサイト/レスキュー支援数は減少していない

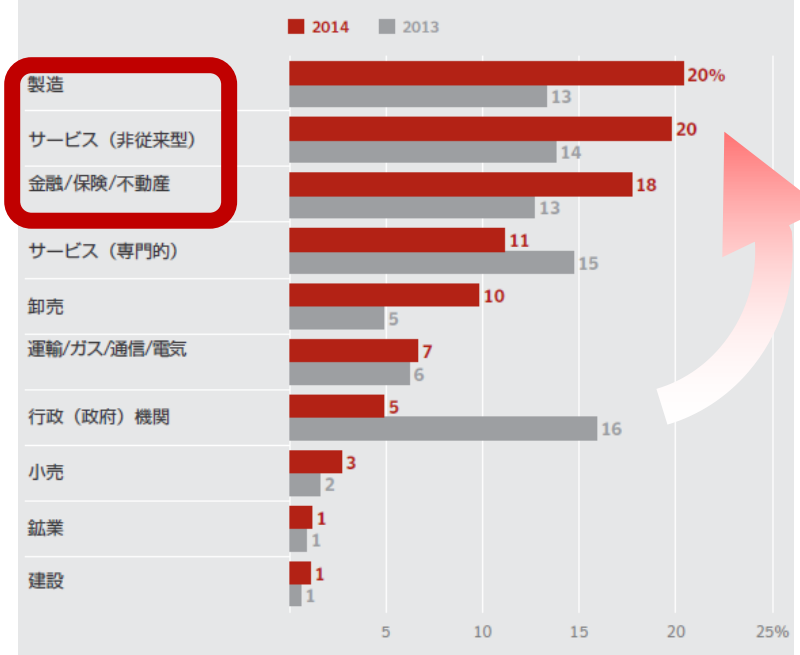


出所　https://www.ipa.go.jp/security/J-CRAT/　から作成

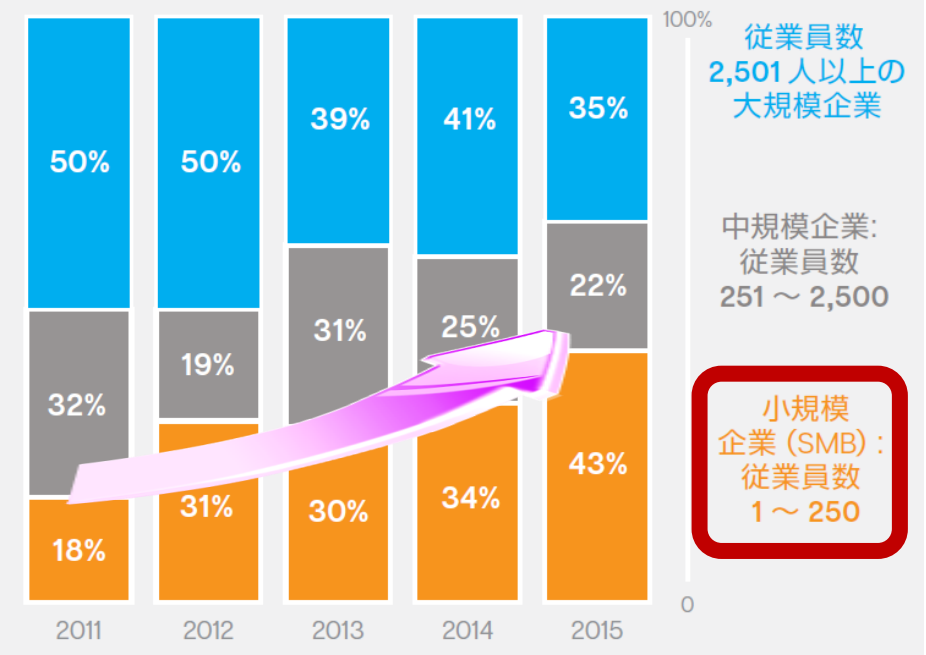
標的となる業種・企業規模

トレンド3

民間企業への攻撃が拡大



中小企業への攻撃にシフト

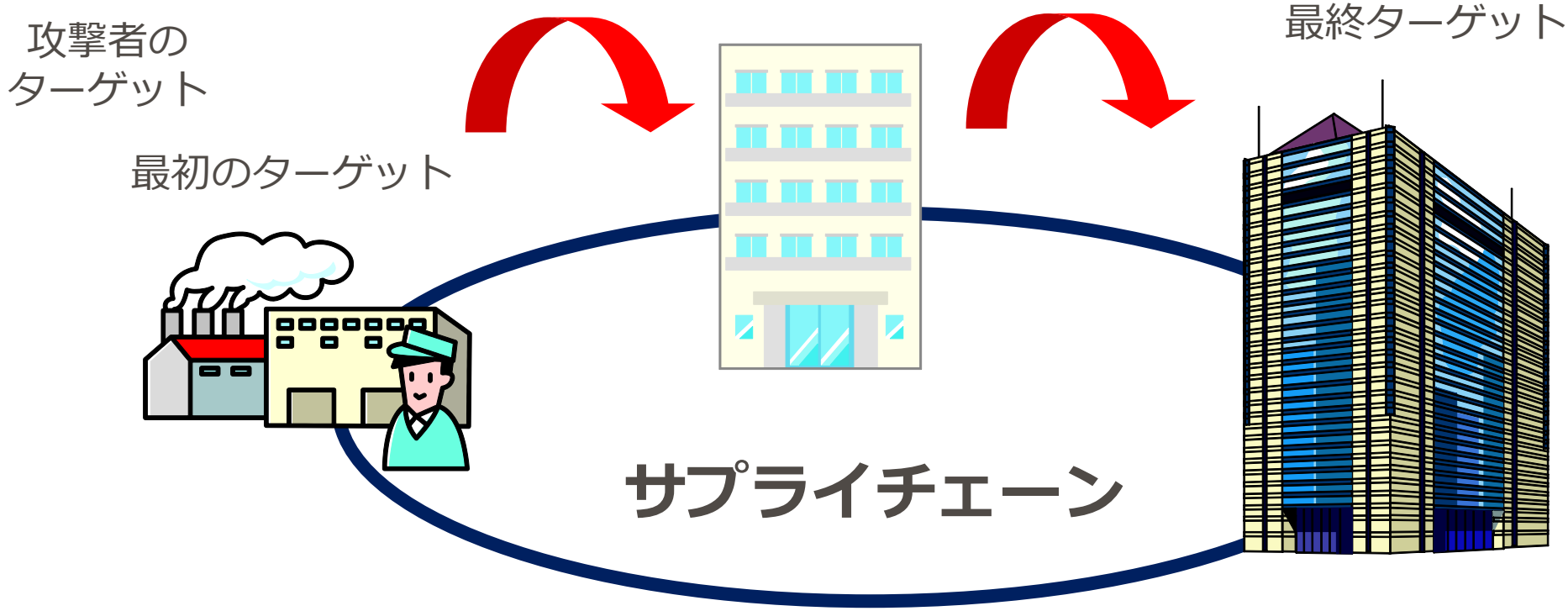


出所　シマンテック「インターネット脅威レポート2015年4月第20巻」
シマンテック「インターネット脅威レポート2016年4月第21巻」

サプライチェーンリスク

トレンド3

攻撃者はセキュリティレベルの低いところから攻め込んでくる



巧妙化・深刻化するビジネスメール詐欺（BEC）

ビジネスメール詐欺(Business E-mail Compromise)

偽の電子メールを組織・企業に送り付け、従業員を騙して不正な送金処理を実施させる詐取の手口

タイプ１）取引先との請求書の偽装
（例）取引のメールの最中に割り込み、偽の請求書（振込先）を送る

タイプ２）経営者等へのなりすまし
（例）経営者を騙り、偽の振込先に振り込ませる

タイプ３）窃取メールアカウントの悪用
（例）メールアカウントを乗っ取り、取引先に対して詐欺を行う

タイプ４）社外の権威ある第三者へのなりすまし
（例）社長から指示を受けた弁護士といった人物になりすまし、振り込ませる

タイプ５）詐欺の準備行為と思われる情報の詐取
（例）経営層や人事部になりすまし、今後の詐欺に利用するため、社内の従業員の情報を窃取する

出所　IPA「ビジネスメール詐欺「BEC」に関する事例と注意喚起」（2017年4月3日）

メールアドレスなりすましの手口

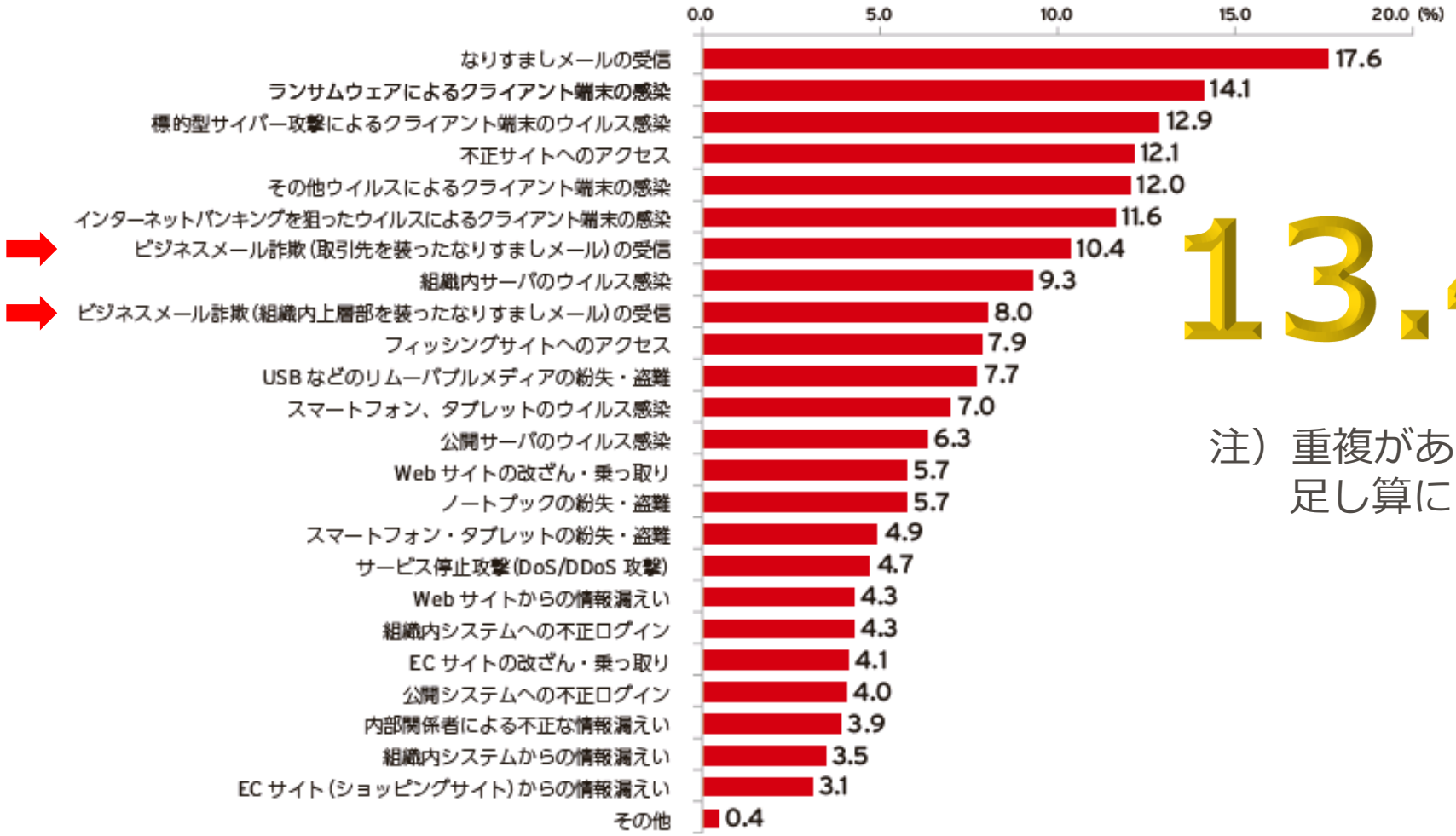
メールアドレスを1文字変えて、「見た目」からは偽物と気付き難い

■本物のメールアドレス		alice @ company-a . com	
■偽物のメールアドレス	①	alice @ compnay-a . com	1文字入替
	②	alice @ companys-a . com	1文字追加
		aalice @ company-a . com	
	③	alice @ comp ny-a . com	1文字削除
	④	alice @ cornpany-a . com	誤認し易い文字に置換
	⑤	alice-company-a @ freemail.com	それらしいフリーメールアドレス

出所　IPA「ビジネスメール詐欺「BEC」に関する事例と注意喚起」（2017年4月3日）

高まるインシデント発生率(トレンドマイクロ調査)

2016年度セキュリティインシデント発生率内訳



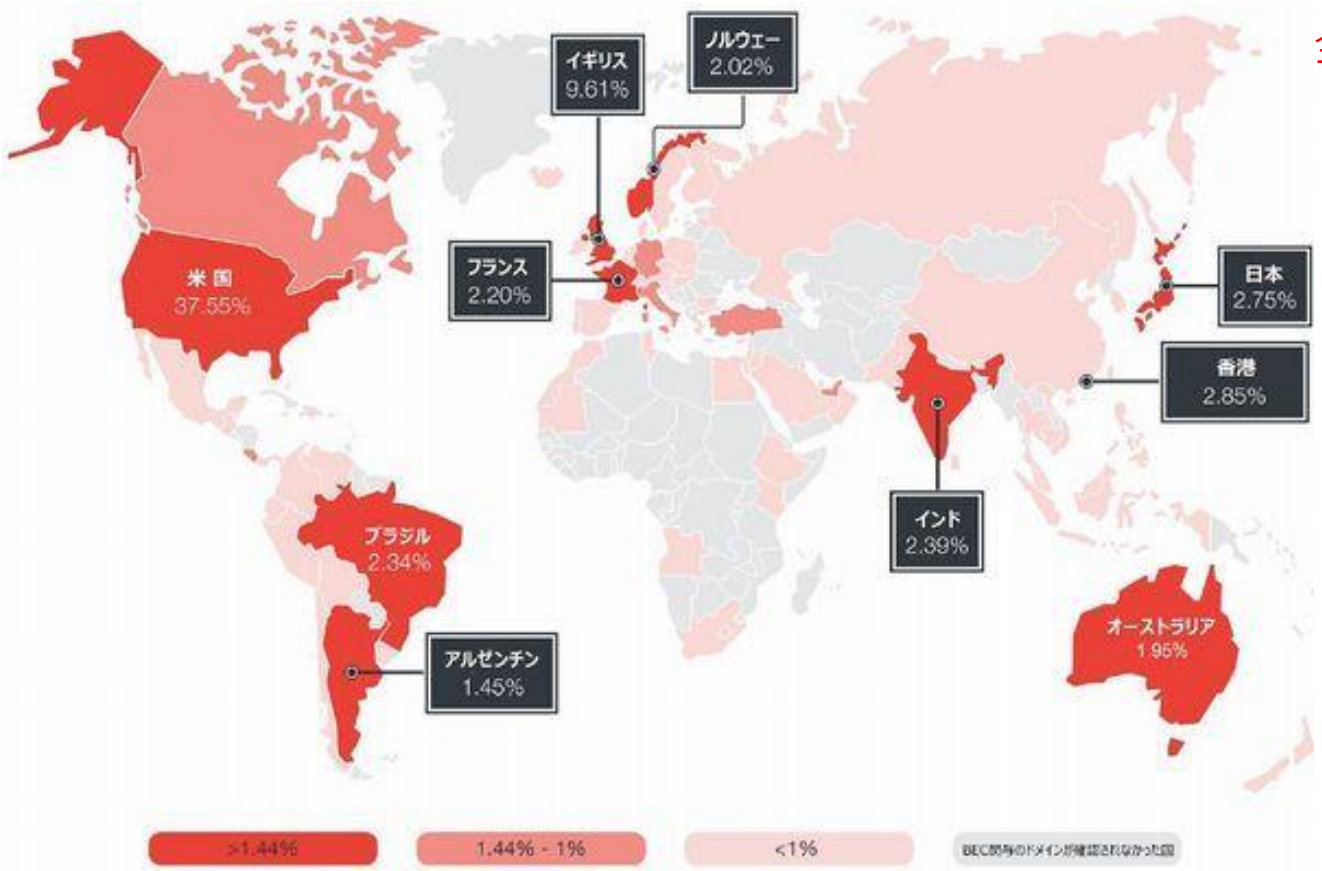
13.4%

注）重複があるため単純な足し算にはならない

出所　トレンドマイクロ「法人組織におけるセキュリティ対策実態調査2017年版」(2017年9月)

BECメール受信組織数(トレンドマイクロ調査)

BEC関連のなりすましメールを受信した法人組織数毎の国別マップ(2016年)



全世界92カ国の法人組織でBEC受信

米国：37.55%
英国：9.61%
香港：2.85%
日本：2.75%
インド：2.39%
ブラジル：2.34%
フランス：2.20%
ノルウェー：2.02%
オーストラリア：1.95%
アルゼンチン：1.45%

出所　トレンドマイクロ「世界中で被害が拡大するビジネスメール詐欺（BEC）の脅威」

サプライチェーンにおけるセキュリティ

トレンド3

- 攻撃者は狙いを定めた標的に、最も効果的な手段で侵入を試みる
- セキュリティ対策の弱い取引先、系列会社が狙われ易い

- 取引先、系列会社等も含めたサプライチェーン全体でのセキュリティレベルの底上げが必要
- 業務プロセスの中に入り込んだビジネスメール詐欺が横行中なので、異変を感じるメールは発信者へ確認

Supply Chain Security

結びに

弊社ソリューションの紹介を兼ねて

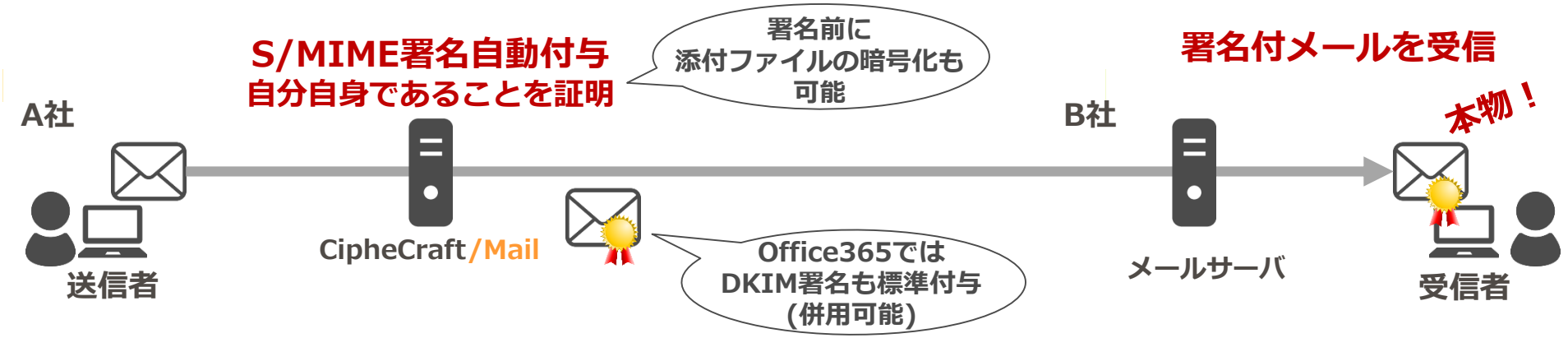
CipherCraft/Mailの新機能（電子署名）

CipherCraft®/Mail 7

悪意のある攻撃者に「なりすまし」をされないようにするためには、
普段から**電子署名を付加したメールを利用するのが有効**です！

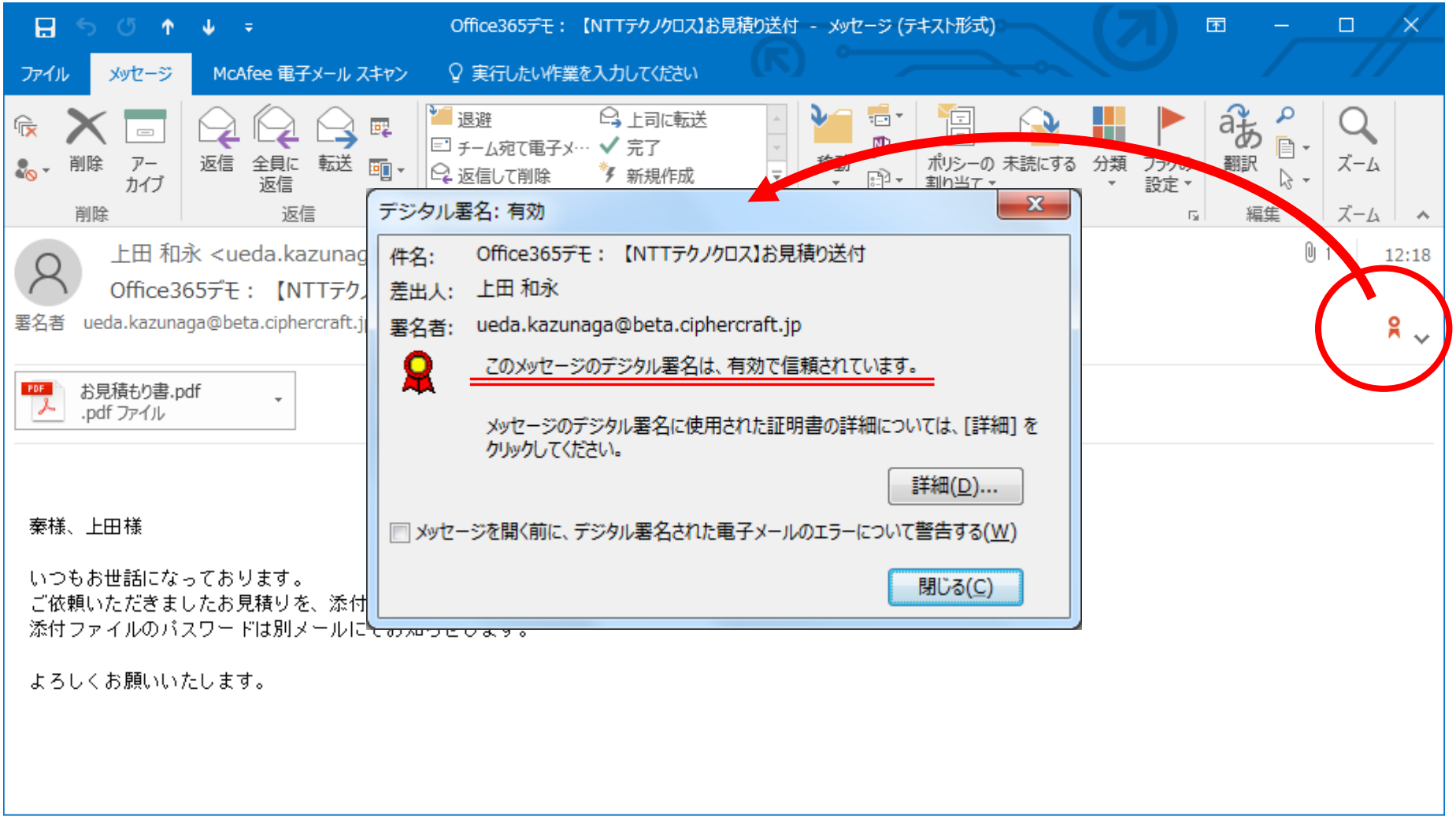
例　A社を装いB社から資金をだましとるビジネスメール詐欺

- S/MIMEは、Microsoft社のOutlookを始め多くのメールソフトが対応しています。
- CipheCraft/Mail では、サーバが証明書を自動付与するので、付与忘れを防ぎます。



電子署名による本人確認

メール受信者に差出人が本人であることを証明



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2018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