ネットワークセキュリティ

2016年9月27日

情報アーキテクチャ学科
稲村　浩

連絡先

- 研究室　　225
- 電話　　0138-34-6225
- E-mail　　inamura@fun.ac.jp

相談があれば連絡してください

ネットワークセキュリティ」と関連科目

ネットワークセキュリティ

- システム管理方法論
- データベース工学
- 情報ネットワーク
- オペレーティングシステム
- アルゴリズムとデータ構造
- ネットワーク通信理論
- 情報数学
- 線形代数学

教科書

「情報セキュリティの基礎」

織茂著、日本理工出版会

(参考書)

1)「情報セキュリティの基礎」 手塚編　共立出版

2)「暗号とネットワークセキュリティ」 W.Stallings著
ピアソンエデュケーション

3)「暗号理論入門」 J.A.Buchmann著 ，など
シュプリンガーフェア ラーク東京

講義計画

□ 情報セキュリティ序説 □ インターネットプロトコル概説 □ 攻撃手法と対策	**情報ネットワークの安全性**
□ 認証、 アクセス制御 □ 暗号と共通鍵暗号 □ 公開鍵暗号 □ 鍵管理方式 □ メッセージ認証とハッシュ関数 □ 電子署名	**防御技術と 暗号アルゴリズム**
□ 電子メールのセキュリティ □ Webセキュリティ □ VPN、 IPsecセキュリティ	**インターネットセキュリティ**
□ 不正侵入・ウィルス・コンテンツ監視 □ 運用・管理とセキュリティ・ポリシー □ 施策・法令、知的所有権と情報倫理	**監視技術・運用・管理と 施策・法令・情報倫理**

講義資料/評価方法

- 講義資料

  manabaで事前に公開

  コース番号：le109501

  ネットワークセキュリティ 3-ABCDEF

- 成績評価

  出席状況，レポート課題，試験から総合的に評価

  次回からmanabaで出席をとります

  今回はレポートの提出で出席とみなします

情報化社会とは

- コンピュータの役割

  第３の波：1960年ころからの電子情報革命

  （アルビン・トフラー：アメリカの未来学者

  1980年著書「第３の波」で予言）

  脱工業化社会，情報化時代，**情報化社会**，情報革命

  → ICT

第１の波：農業革命（約15000年前，狩猟から農耕）

第２の波：産業革命(1872年蒸気機関発明）

新しい波は，古い文化と社会を脇へと押しやる

ICT（情報技術・情報通信技術）とは何か

□　ICT(Information and Communication Technology)とは

情報処理および情報通信、つまり、コンピュータやネットワークに関連する諸分野における技術・産業・設備・サービスなどの総称

政府・民間主導で多くの技術開発，サービス開発を実施

高度情報通信ネットワーク
→　通信革命　インターネットの変貌

電子商取引
→　貨幣の情報化で経済活動の革命

パソコン教育

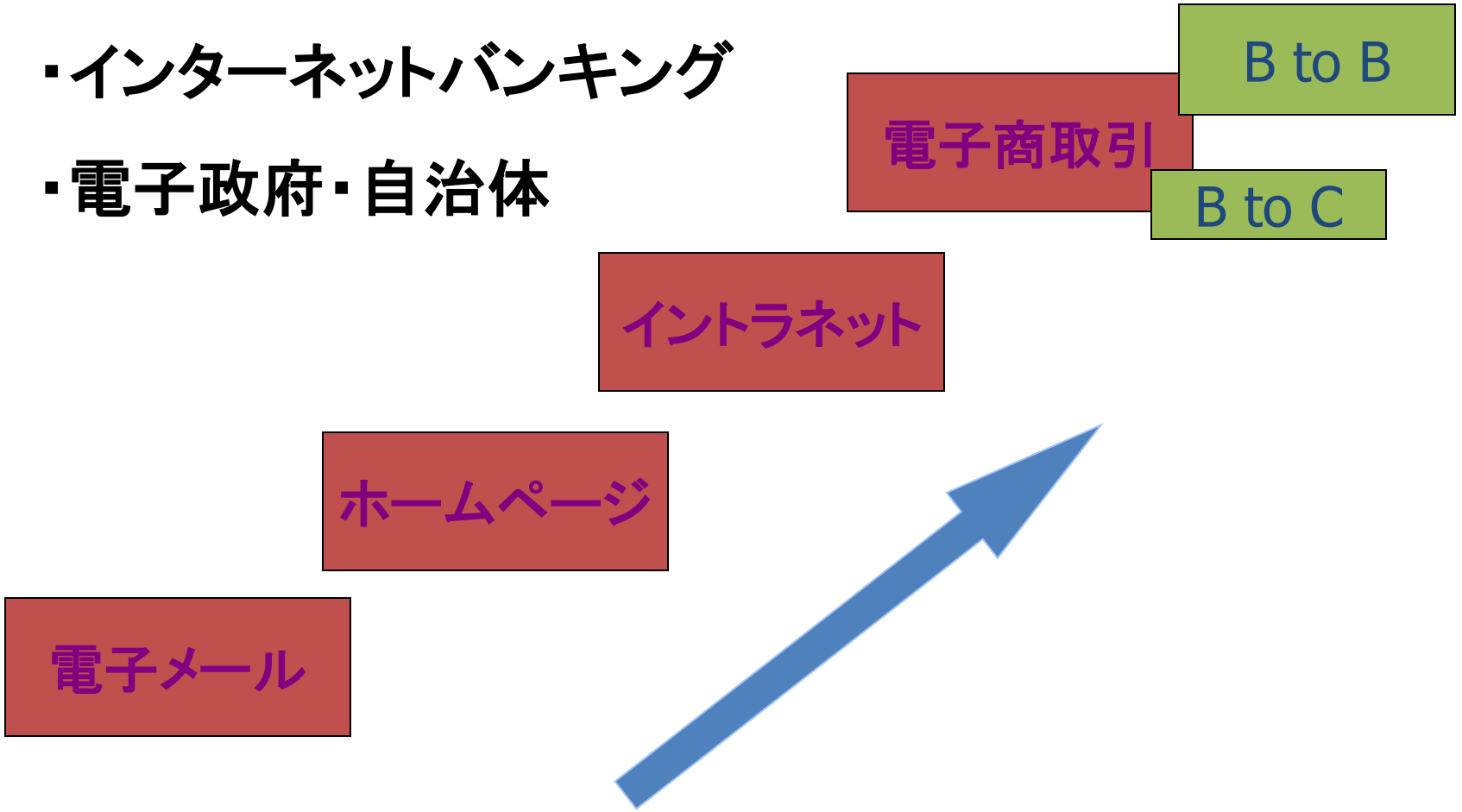
多様なサービス
→　SNSなど

ICTの発展形態

・電子商取引

・インターネットバンキング

・電子政府・自治体



高度情報通信社会形成推進基本法（IT基本法）
（2001年1月施行）

【基本理念】高度情報通信技術の恩恵があまねく享受され、活力のある成長発展が可能な社会の実現

【基本的視点】
①新たな経済取引を普及、新規産業を創出、就業機会増大など
②民間主導を原則とし、国および地方公共団体が環境整備

【施策の基本方針】
①世界最高水準の高度情報通信ネットワークの整備
②国民の教育、学習の振興、専門的人材の育成
③規制の見直し、消費者保護を通じた電子商取引の促進
④行政の情報化（電子政府、電子自治体）
⑤高度情報通信ネットワークの安全性確保、個人情報の保護

IT関連法律
http://www.kantei.go.jp/jp/singi/it2/hourei/link.html

高度情報通信ネットワーク社会推進戦略本部（政府にIT戦略本部設置）

- 2001年1月設置
- 2001年1月：e-Japan戦略策定
- 2006年1月：IT新改革戦略策定、u-Japan構想
- 2009年7月：i-Japan戦略2015（決定）
- 2012年6月：新たな情報通信技術戦略工程表
- 2013年6月：世界最先端 IT 国家創造宣言
- 2014年7月：世界最先端IT国家創造宣言」の変更

e-Japan戦略
（2001年1月決定）

- 我が国は、すべての国民が情報通信技術（IT）を積極的に活用し、その恩恵を最大限に享受できる知識創発型社会の実現に向け、早急に革命的かつ現実的な対 応を行わなければならない。市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、５年以内に世界最先端のIT国家となることを目指す。

IT新改革戦略

- 2009年1月策定：e-Japan戦略の引き継ぎ
- いつでも，どこでも，誰でもITの恩恵を実感できる社会の実現
- 「構造改革による飛躍」、「利用者・生活者重視」、「国際貢献・国際競争力強化」の三つを基本理念
- 2010年までに世界のIT革命をリードするフロントランナーになる

i-Japan戦略2015

2009年制定

i-Japan戦略2015 ～国民主役の「デジタル安心・活力社会」の実現を目指して～

2015年の我が国の将来ビジョン

- デジタル技術が「空気」や「水」のように受け入れられ、経済社会全体を包摂し（Digital Inclusion）、暮らしの豊かさや、人と人とのつながりを実感できる社会を実現
- デジタル技術・情報により経済社会全体を改革して新しい活力を生み出し（Digital Innovation）、個人・社会経済が活力を持って、新たな価値の創造・革新に自発的に取り組める社会等を実現

将来ビジョンを実現するための視点

- 人間中心のデジタル技術が水や空気のように使いやすく、普遍的に国民に受け容れられるデジタル社会を実現する戦略を立案。
- 4つの新たな視点に立ったデジタル戦略
  - 使いやすいデジタル技術
  - デジタル技術の活用に立ちはだかる壁の突破
  - デジタル技術の利用にあたっての安心の確保
  - デジタル技術・情報の経済社会への浸透を通じた新しい日本の創造

本戦略の柱

三大重点分野

電子政府・電子自治体

- 電子政府の推進体制の整備（政府CIOの設置など）、過去の計画のフォローアップとPDCAの制度化
- 「国民電子私書箱（仮称）」※）を、広く普及させ、国民に便利なワンストップ行政サービスの提供や「行政の見える化」を推進

※）「国民電子私書箱」は平成25年度までの整備を目指し、既存のシステムの利用を視野に社会保障番号・カード（仮称）と一体的に検討し、本年度中に基本構想を策定

医療・健康

- 地域の医師不足等の問題への対応
  - 遠隔医療技術の活用
  - 医師等の技術の維持・向上
  - 地域医療連携の実現　等
- 日本版EHR※）（仮称）の実現
  - 医療過誤の減少、個人の生涯を通じた継続的な医療の実現
  - 処方せん・調剤情報の電子化
  - 匿名化された健康情報の疫学的活用　等

※）Electronic Health Record

教育・人財

- 授業でのデジタル技術の活用等を推進し、子どもの学習意欲や学力、情報活用能力の向上
  - 教員のデジタル活用指導力の向上
  - 電子黒板等デジタル機器を用いたわかりやすい授業の実現　等
- 高度デジタル人財の安定的・継続的育成
  - 実践的な教育拠点の広域展開・充実
  - 産学官連携によるナショナルセンター的機能の充実　等

産業・地域の活性化及び新産業の育成

デジタル技術・情報の活用により全産業の構造改革と地域再生を実現し、我が国の産業の国際競争力を強化。

- 中小企業等の事業基盤整備、
- テレワーク就労人口の拡大（在宅型テレワーカーの倍増）
- グリーンIT・ITSの推進、
- 地域産業の新たな業態開発、
- クリエイティブな新市場の創出　等

デジタル基盤の整備

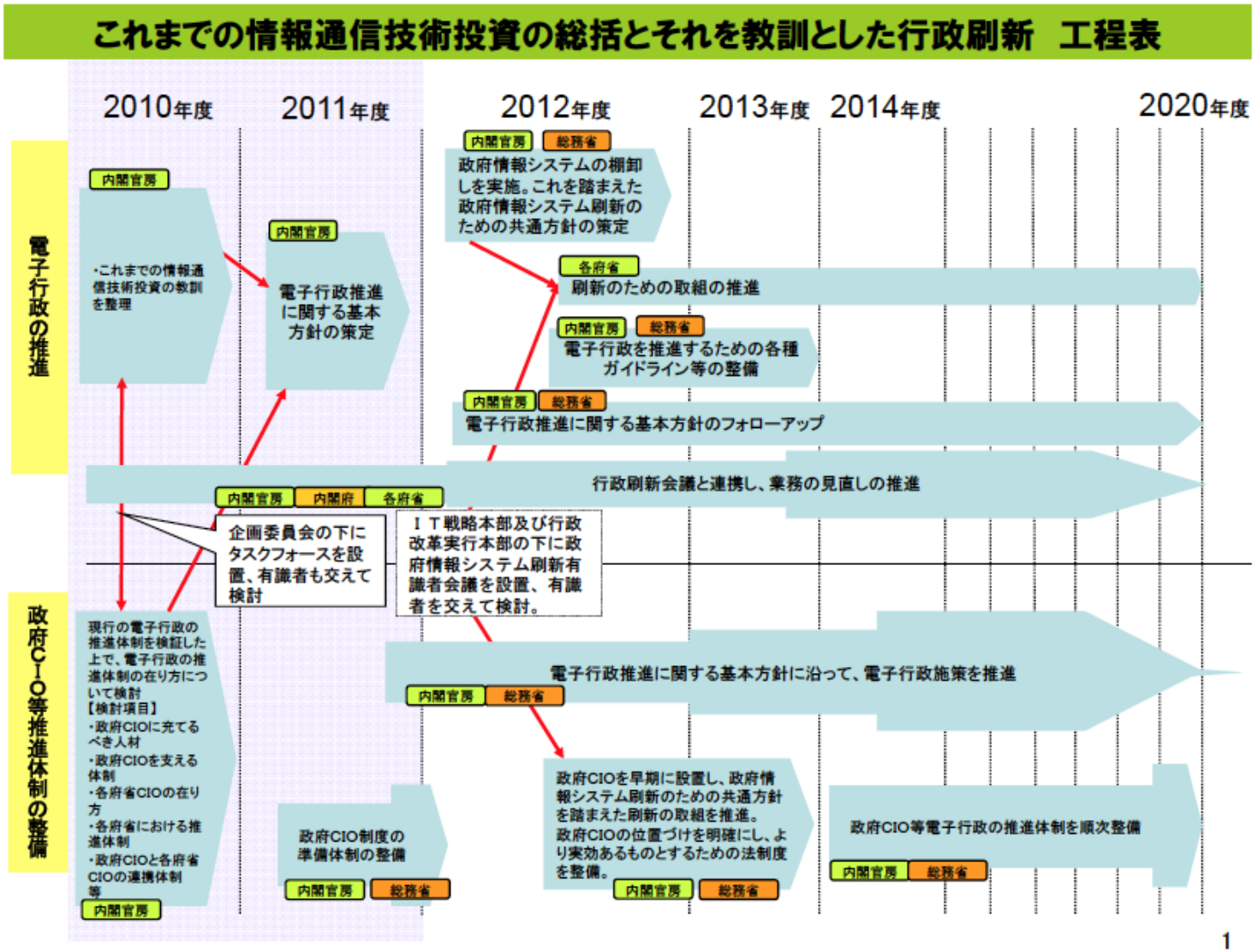
あらゆる分野におけるデジタル活用の進展を支え、成長を促進。

- ブロードバンド基盤の整備（移動系100Mbps超、固定系1Gbps）
- 情報セキュリティ対策の確立、
- デジタル基盤技術の開発の推進、
- デジタル情報の流通・活用基盤の整備 に取り組む。

今後一層の検討を行うべき事項

- 規制・制度・慣行等の「重点点検」の実施　：デジタル技術・情報の利活用を阻むような規制・制度・慣行等を抜本的に見直し、2009年中に第1次の「重点点検」を行い、その結果を踏まえて、所要の措置を講ずるとともに、以後も継続的に実施。
- 「デジタルグローバルビジョン（仮称）」の策定　：我が国のデジタル技術や関連産業の国際競争力の強化等について、2009年度末までに「デジタルグローバルビジョン（仮称）」を策定。

新たな情報通信技術戦略工程表（2012.7）



世界最先端 IT 国家創造宣言（2013.6.14）

（高度情報通信ネットワーク社会推進戦略本部）

I. 基本理念

閉塞を打破し、再生する日本へ，世界最高水準のIT利活用社会の実現

II. 目指すべき社会・姿

革新的な新産業・新サービスの創出及び全産業の成長を促進する

健康で安心して快適に生活できる、世界一安全で災害に強い社会

公共サービスがワンストップで誰でもどこでもいつでも受けられる社会

III.目指すべき社会・姿を実現するための取組

1．革新的な新産業・新サービスの創出と全産業の成長を促進する社会の実現

2．健康で安心して快適に生活できる、世界一安全で災害に強い社会

3．公共サービスがワンストップで誰でもどこでもいつでも受けられる社会の実現

IV. 利活用の裾野拡大を推進するための基盤の強化

1．人材育成・

2．世界最高水準の IT インフラ環境の確保

3．サイバーセキュリティ

4．研究開発の推進・研究開発成果との連携

V. 戦略の推進体制・推進方策

世界最先端IT国家創造宣言（1/3）

2015.6

世界最先端IT国家創造宣言及び工程表 改定（案）概要

Ⅱ．目指すべき社会・姿、 Ⅲ．目指すべき社会・姿を実現するための取組

2020年までに世界最高水準のIT利活用社会の実現と成果の国際展開を目標とし、以下の**４本柱**に取組む

※成長のエンジンであるITを利活用することで、政府の成長戦略である日本再興戦略に掲げる目標達成にも寄与

１．IT利活用の深化により未来に向けて成長する社会 ⇒ 目標:国・地方を通じたＩＴ化を促すための制度整備

- ○新たな**IT利活用環境**の整備 …［IT利活用を加速する新たな法制度の検討（新規）］
- ○IT利活用の裾野拡大を阻害する**規制・制度の見直し** …［パーソナルデータ利活用環境の整備］
- ○公共データの民間開放（**オープンデータ**）の推進 …［課題解決型のオープンデータの推進（新規）］

２．ITを利活用したまち・ひと・しごとの活性化による活力ある社会 ⇒目標:地方の雇用創出と地域経済活性化

- ○**地方創生IT利活用促進プラン**の推進
  …［情報共有基盤整備、RESASやSNS等を用いた情報分析・活用、政府CIOや成功経験者等によるIT人材派遣支援（新規）］
- ○起業家精神の創発 …［地域ITスタートアップファンド創設、IT人材発掘 等によるベンチャー企業等支援（新規）］
- ○雇用形態の多様化とワーク・ライフ・バランスの実現
  …［ふるさとテレワークの推進（新規）、ハローワーク業務・システムの見直しによる就職支援機能の強化］

３．ITを利活用した安全・安心・豊かさが実感できる社会

- ○適切な地域医療・介護等の提供、健康増進等を通じた**健康長寿社会**の実現⇒目標:2020年までに国民の健康寿命を１歳以上延伸
  …［医療情報連携ネットワークの全国展開、医療・健康情報等の各種データの活用による健康増進や発症・重症化予防等］
- ○ITを利活用した日本の**農業**・周辺産業の高度化・知識産業化と国際展開 ⇒目標:農林水産物輸出１兆円
  …［農業情報創成・流通促進戦略の推進（AI農業の推進、鳥獣被害対策等の農業IT化の浸透等）］
- ○世界で最も安全で環境にやさしく経済的な**道路交通社会**の実現 ⇒目標:2020年代後半以降に完全自動走行システム試用開始
  …［官民ITS構想・ロードマップ2015の策定、推進（高齢者等の移動支援、オリパラ競技大会に向けた最先端のITS構築等）］

４．ITを利活用した公共サービスがワンストップで受けられる社会

- ○**マイナンバー制度**の活用推進 ⇒ 目標:個人番号カードの普及
  …［利活用範囲の拡大検討、官民手続等での個人番号カード利活用推進、ワンカード化の推進］
- ○国・地方を通じた**行政情報システム**の改革 ⇒ 目標:自治体システムの運用コスト3割減 等
  …［IT総合戦略本部・eガバメント閣僚会議における、国・地方の行政のIT化・BPR推進の検討］

世界最先端IT国家創造宣言（2/3）

2015.6

世界最先端IT国家創造宣言及び工程表 改定（案）概要

Ⅳ. 利活用の裾野拡大を推進するための基盤の強化

1．人材育成・教育

※世界最高水準のIT利活用社会を通じて、「情報資源立国」となるため、それを「けん引する人材」、「それを支える人材」、「享受して豊かに生活する人材」を育成

※政府におけるIT人材の育成を図るため、キャリアパスの明確化等を図る。

○けん引する人材、それを支える人材の育成
…［IT・データを活用した起業や新サービスの創出を担う先端人材の発掘・支援、プログラミング等のIT教育の推進］

○ 享受して豊かに生活する人材の育成
…［国民全体の情報利活用力向上、安心・安全な利用環境整備、指導者等の育成、確保］

2．世界最高水準のITインフラ環境の確保

※世界最高水準のブロードバンド環境を確保し、膨大なデータを利活用できる、IoT時代に対応した環境整備を行う

○通信ネットワークインフラの整備
…［観光地や防災拠点等における無料公衆無線LANの整備（地方創生IT利活用促進プランにも記載）］
…［過疎地・離島等の条件不利地域での超高速ブロードバンド整備に取組む地方公共団体への支援］

3．サイバーセキュリティ

○ IT総合戦略本部、サイバーセキュリティ戦略本部及び国家安全保障会議が緊密に連携し、「サイバーセキュリティ戦略」及び年次計画に基づく具体的な施策を推進

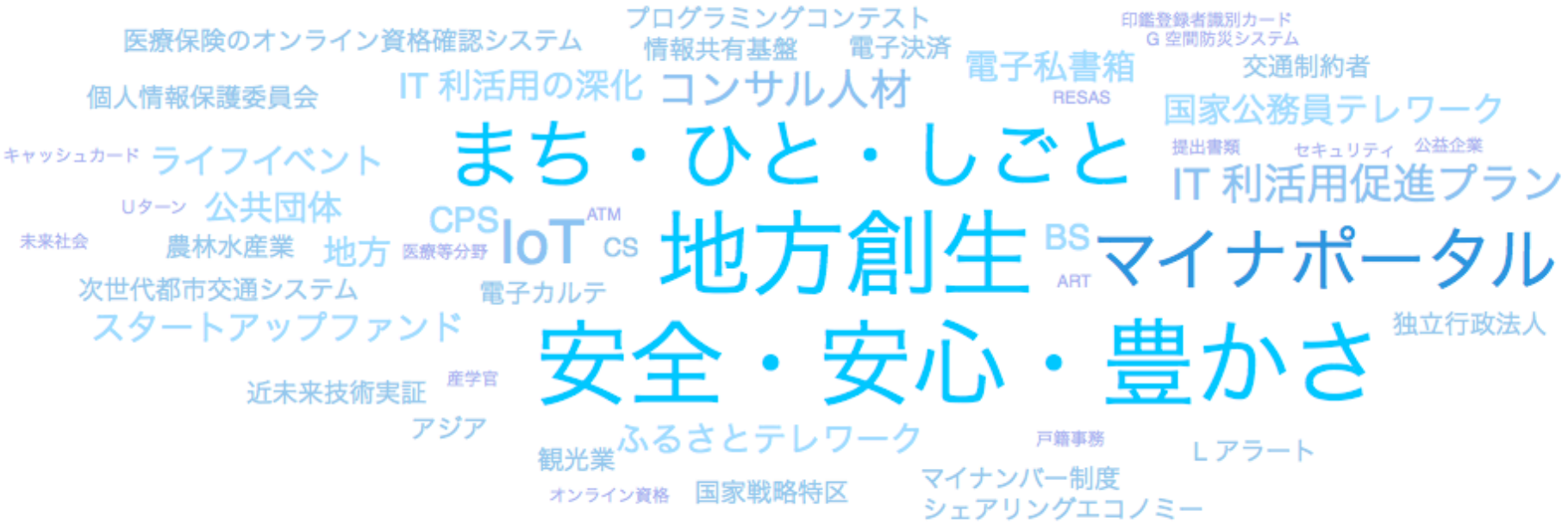
○ 国民・社会を守るためのサイバーセキュリティ確保
…［政府機関等の対応能力の抜本的強化］及び「システム効率化等による節減分のセキュリティ施策への振り向け」
…［マイナンバー制度のセキュリティ確保の徹底］

4．研究開発の推進・研究開発成果との連携

○ IoT時代に対応する技術、超高速ネットワーク伝送技術、認識技術、情報弱者に配慮した技術のほか、防災・減災対策に有効なセンサ技術やロボット技術など、研究成果を迅速かつ的確にIT戦略と連携させることが必要であり、総合科学技術・イノベーション会議等と緊密に連携

世界最先端IT国家創造宣言（3/3）

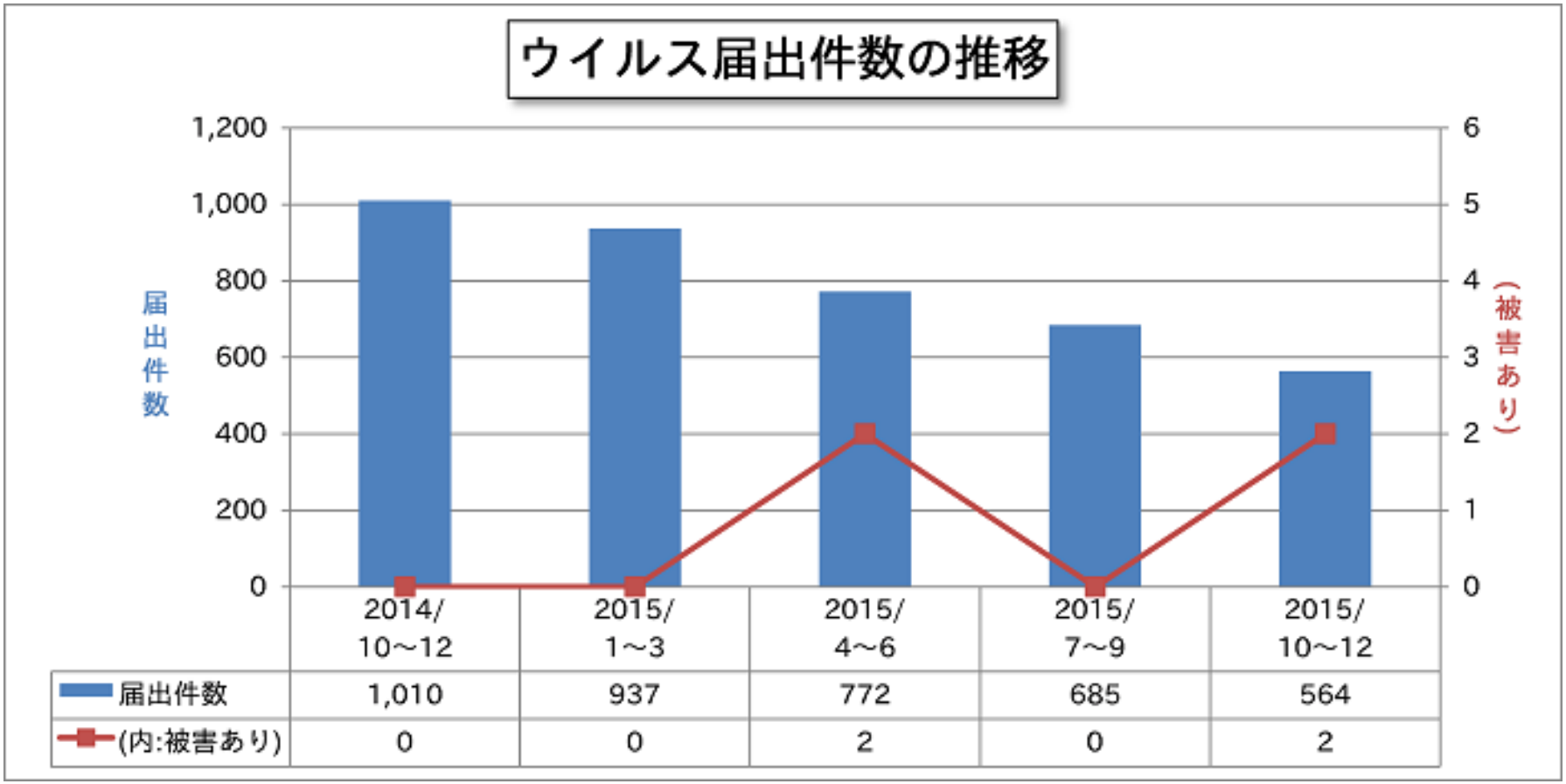
2015.6



高度情報通信ネットワークの安全性及び信頼性の確保

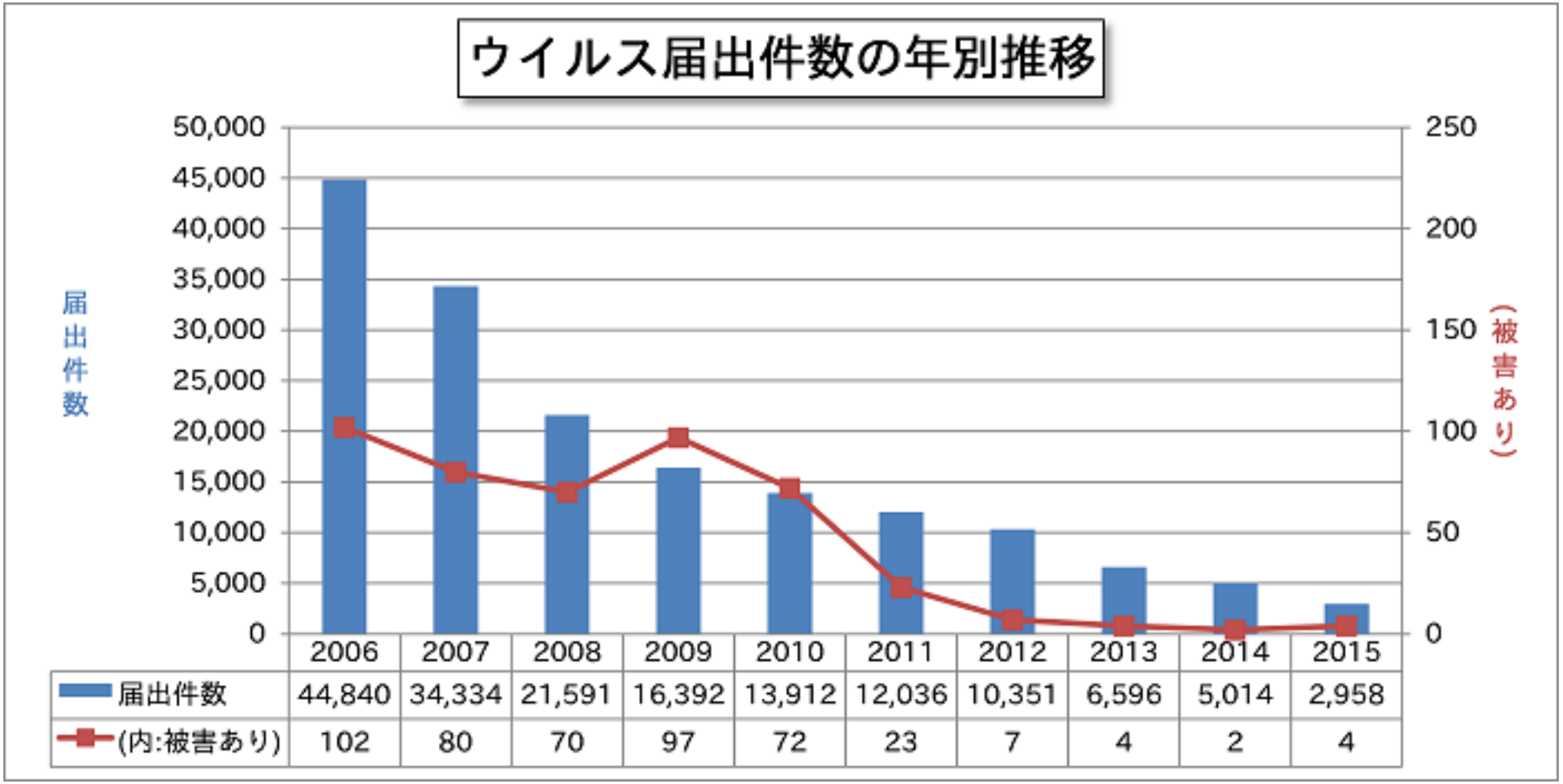
- 情報セキュリティの確保は、ICT化を進める上での前提条件
- 一方、コンピュータウイルスの届出件数や、不正アクセス被害の届出件数は増加
- 電子政府におけるセキュリ ティ体制や，いわゆるサイバーテロに対する対応体制の構築、民間におけるセキュリティ水準の向上等を重点的に図る

ウィルス届け出状況（情報処理推進機構）



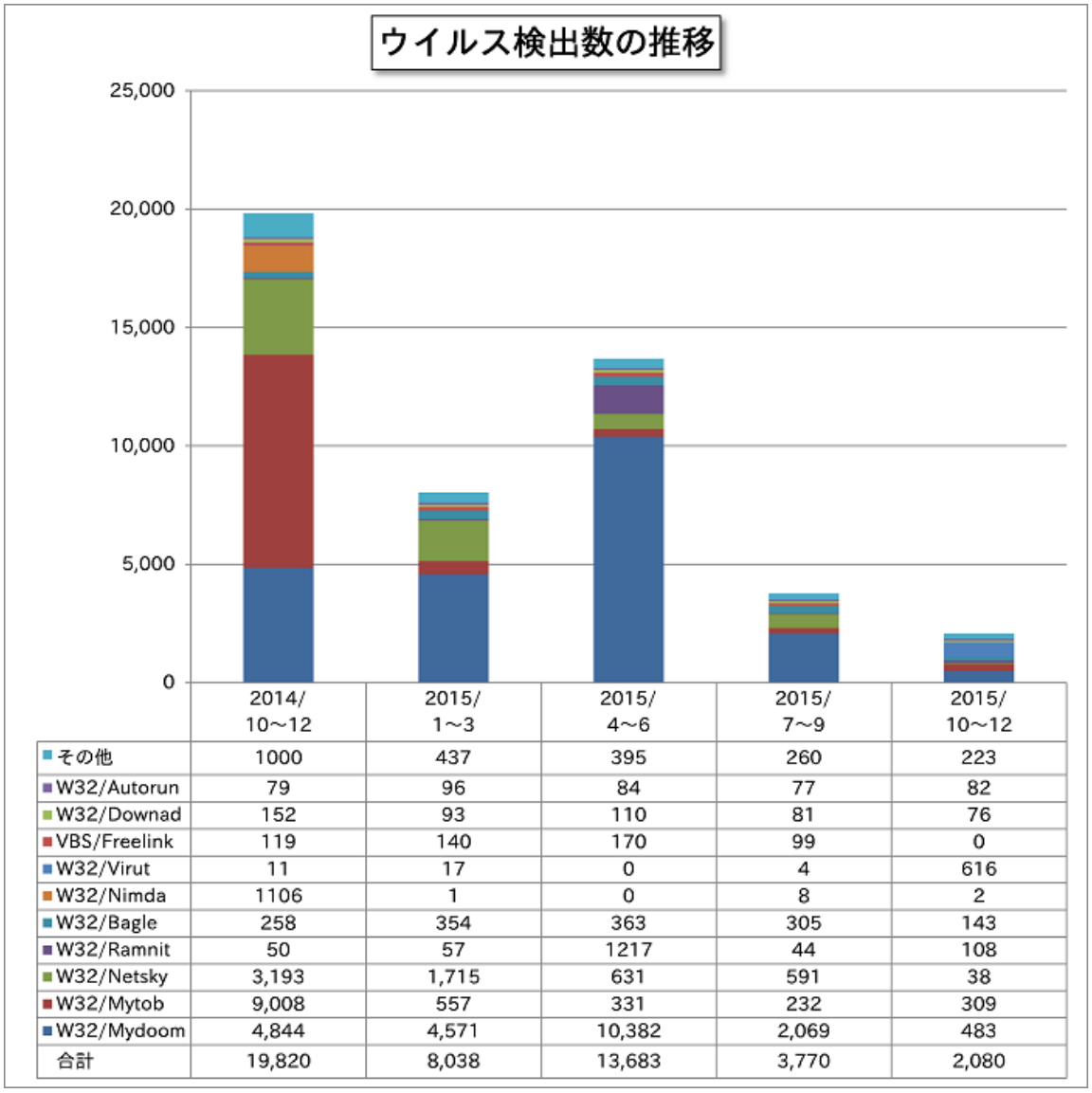
	2014/10～12	2015/1～3	2015/4～6	2015/7～9	2015/10～12
届出件数	1,010	937	772	685	564
(内:被害あり)	0	0	2	0	2

ウィルス届け出状況（情報処理推進機構）



	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
届出件数	44,840	34,334	21,591	16,392	13,912	12,036	10,351	6,596	5,014	2,958
(内:被害あり)	102	80	70	97	72	23	7	4	2	4

ウィルス検出数（情報処理推進機構）



	2014/10～12	2015/1～3	2015/4～6	2015/7～9	2015/10～12
その他	1000	437	395	260	223
W32/Autorun	79	96	84	77	82
W32/Downad	152	93	110	81	76
VBS/Freelink	119	140	170	99	0
W32/Virut	11	17	0	4	616
W32/Nimda	1106	1	0	8	2
W32/Bagle	258	354	363	305	143
W32/Ramnit	50	57	1217	44	108
W32/Netsky	3,193	1,715	631	591	38
W32/Mytob	9,008	557	331	232	309
W32/Mydoom	4,844	4,571	10,382	2,069	483
合計	19,820	8,038	13,683	3,770	2,080

2015年第4四半期の検出ウイルスの種類

i) Windows/DOS ウイルス	検出数
W32/Virut	616
W32/Mydoom	483
W32/Netsky	309
W32/Ramnit	143
W32/Bagle	108
W32/Downad	82
W32/Autorun	76
W32/Sality	49
W32/Mytob	38
W32/Mumu	22
W32/Klez	17
W32/Antinny	14
W32/Fakerecy	7
W32/Wapomi	7
W32/Rontokbro	4
W32/Gammima	3
W32/Lovgate	3
W32/Nimda	2
WM/Cap	2
W32/Looked	2
W32/Zafi	2
Stoned	2
W32/Expiro	1
W32/Sohanad	1
W32/Cryptolocker	1
W32/Dorkbot	1
Dropper	1
小計　(27 種類)	1,996

スクリプトウイルス	検出数
VBS/DUNIHI	4
VBS/Solow	2
VBS/LOVELETTER	1
VBS/Redlof	1
小計　(4 種類)	8

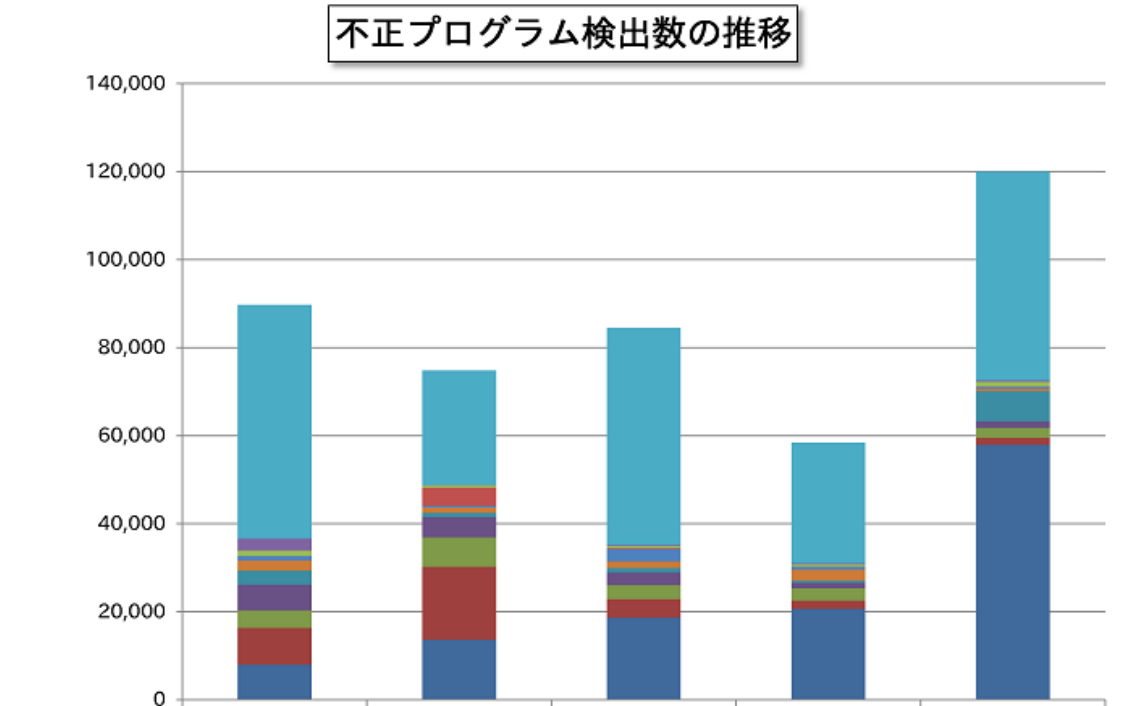
マクロウイルス	検出数
XM/Laroux	27
WM/Concept	12
XM/Mailcab	8
W97M/Marker	8
X97M/Divi	3
W97M/Ethan	3
W97M/Relax	2
W97M/Chack	2
小計　(8 種類)	65

ii) 携帯端末ウイルス	検出数
AndroidOS/Lotoor	10
AndroidOS/Adware	1
小計　(2 種類)	11

iii) Macintosh	検出数
なし	

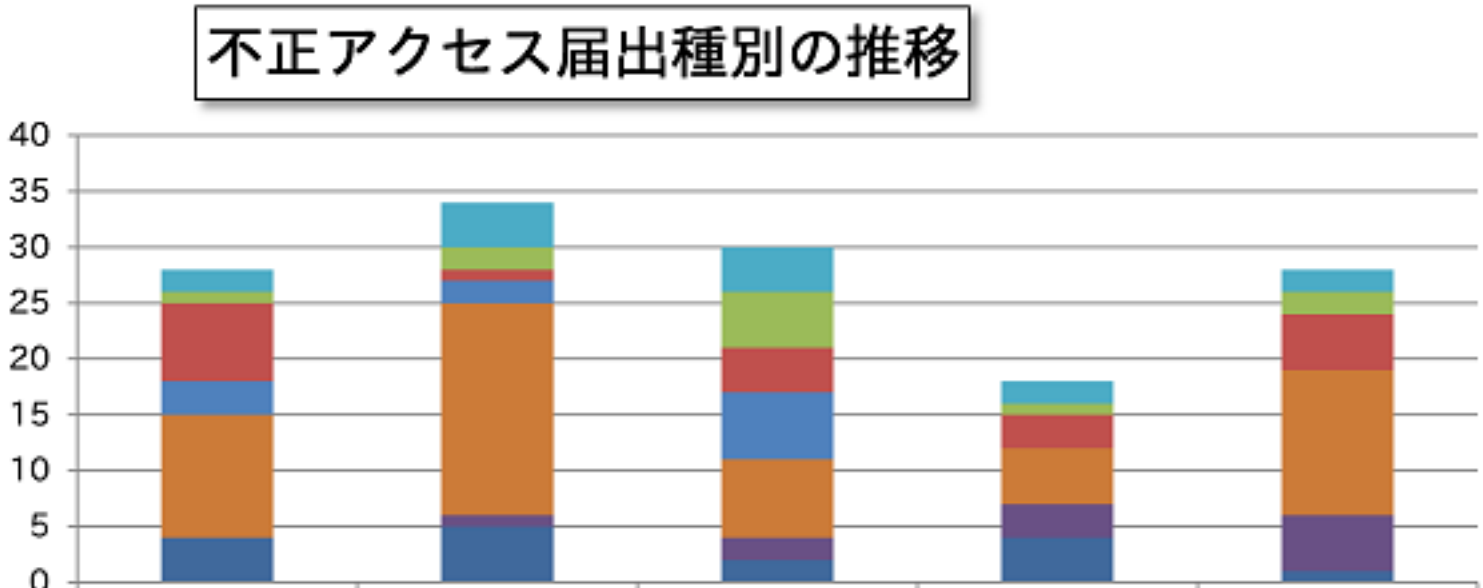
iv) OSS(Open Source Software) Linux・BSD を含む	検出数
なし	

不正プログラム検出数（情報処理推進機構）



	2014/10～12	2015/1～3	2015/4～6	2015/7～9	2015/10～12
その他	53,155	26,078	49,353	27,418	47,484
Packed	2,742	54	209	269	298
Dropper	1,247	523	503	486	1,098
Obfuscated	0	4,098	220	0	20
Trojan/Horse	1,033	345	2,812	665	467
Fakeav	2,284	1,261	1,476	2,526	527
Bancos	3,203	979	1,012	488	6,903
Redirect	5,851	4,632	2,890	1,255	1,434
Adware	3,961	6,638	3,206	2,801	2,302
Backdoor	8,355	16,637	4,140	1,854	1,554
Downloader	7,941	13,577	18,662	20,650	57,932
合計	89,772	74,822	84,483	58,412	120,019

不正アクセス届出数（情報処理推進機構）



		2014/10～12	2015/1～3	2015/4～6	2015/7～9	2015/10～12
被害なし	その他（被害なし）	2	4	4	2	2
被害なし	アクセス形跡（未遂）	1	2	5	1	2
被害あり	その他（被害あり）	7	1	4	3	5
被害あり	不正プログラム埋込	3	2	6	0	0
被害あり	なりすまし	11	19	7	5	13
被害あり	DoS	0	1	2	3	5
被害あり	侵入	4	5	2	4	1
	合計	28	34	30	18	28

人類が経験する新しい問題と課題

- 情報犯罪

- 情報化社会は、人間社会を豊かにする一方で、人間を疎外する環境を容易に作りだす可能性

- 情報機器の普及と利用者の戸惑い、情報による主張の伝達と表現の自由の問題、情報の活用法と倫理の問題など新たな課題が提起

セキュリティ対策は社会の根幹に関わる問題

- サイバーテロ　公共施設のシステムに侵入
- コンピュータ犯罪・情報犯罪の増加
- 電子マネーの偽造・不正使用による経済の混乱
- 著作権の侵害
- 不正・迷惑文書
- プライバシー侵害

主な情報関連法

- プライバシー保護：　個人情報保護法(2003.4)
- 情報の法的問題：　IT基本法(2001.1)
  （情報処理システムに蓄積される個人情報を保護するための法律）
- 著作権の保護：　著作権法
- 情報公開の規制：情報公開法(2003.4)
- 情報犯罪：　不正アクセス禁止法(2000.2)
- 電子取引における消費者の保護：
  電子（消費者）契約法（2001.12）
- 情報倫理の確立：　情報倫理綱領
- 電子商取引：　電子署名法（2001.4）
- 児童の保護：　出会い系サイト規制法（2003.9）
- スパムメール対策：　特定電子メール法（2004.7）
- 偽造/盗難カード対策：　預貯金社保護法（2006.1）
- 内部統制報告書（日本版SOX法）（2008），etc

情報セキュリティ

１） 安全性を提供するサービス

２） セキュリティに対する攻撃

３） 安全性を提供するメカニズム

ネットワークアクセスのセキュリティ

情報システム

- 情報への不正なアクセス
- サービスの悪用

攻撃

・人間

（クラッカーなど）

・ソフトウェア

（ウィルス、ワームなど）

門番機能

計算機資源
（プロセッサ、メモリ、等）
データ
プロセス
ソフトウェア

内部のセキュリティ制御

情報セキュリティの基本要件

定義 「情報の機密性、完全性及び可用性を確保し維持すること」

ーISO/IEC 17799, JISX 5080

- **機密性（confidentiality）**
  アクセスを許可された者だけが、情報にアクセスできることを確実にすること（アクセス権限のある関係者にしか読めないことを保証すること）
- **完全性（integrity）**
  情報および処理方法が正確であることおよび完全であることを保護すること（権利をもった関係者だけが、情報システムや情報の更新ができること）
- **可用性（availability）**
  許可された利用者が、情報および関連する資産にアクセスできることを確実にすること（必要なときに、その権利のある関係者にコンピュータシステムが使用できること）

考えてみよう

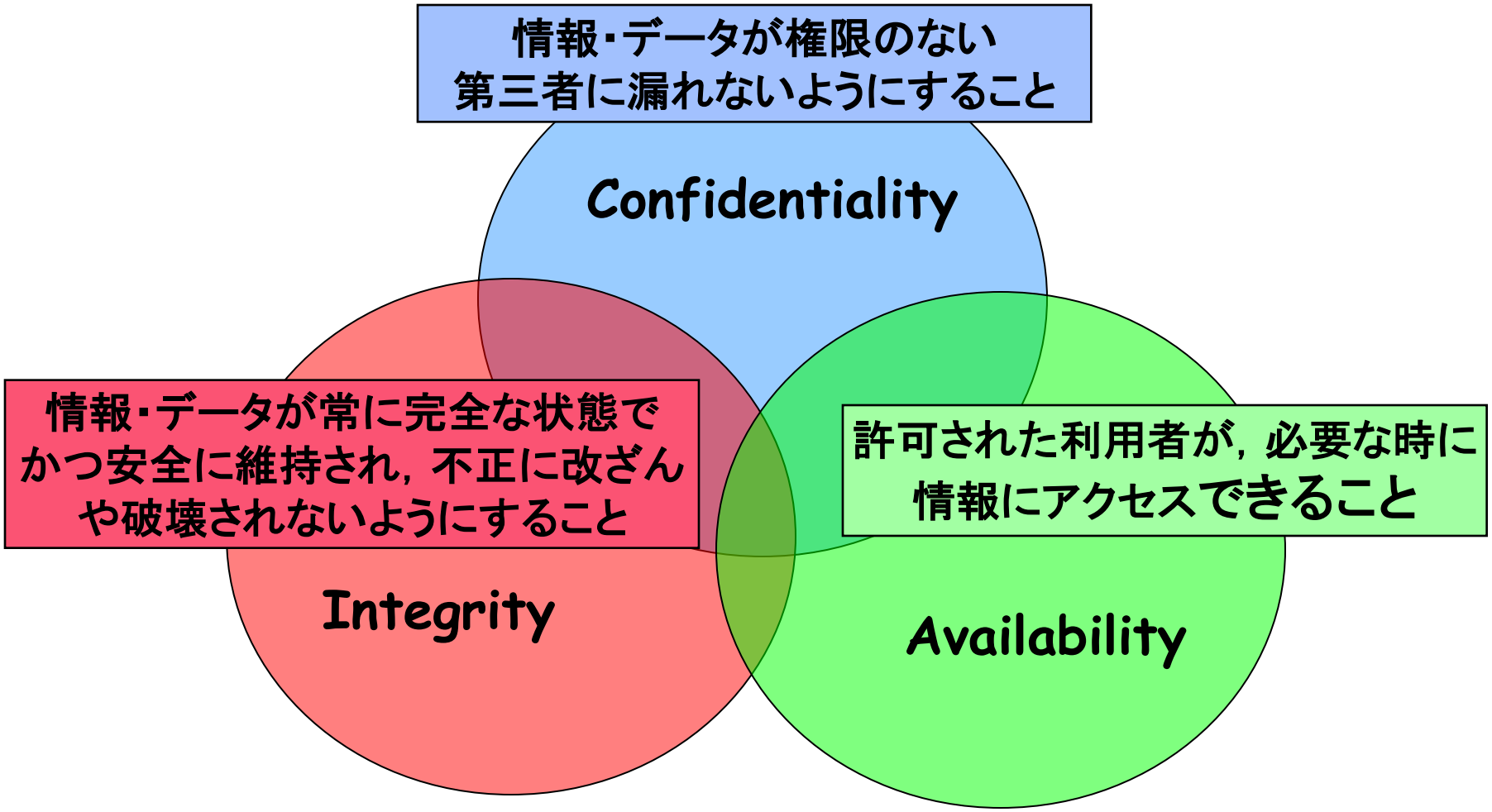
下記の攻撃の例は、基本要件のどれに該当するか？

例１：外部からの不正アクセスや，企業内部の犯行による機密データ持ち出し等により，権限のない第三者に情報が漏れた

例２：いくつかのサーバを踏み台にして，一気に大量のデータを送りつけられたことで，メールサーバの処理速度が著しく低下し，必要な情報へのアクセスや業務の継続が困難になった

例３：不正アクセスによるWebやメールの改ざん，ウィルスによるパソコン中のデータ削除・破壊等により情報（データ）が安全かつ完全な状態に維持できなくなった

Security Goals



“3つの要件すべてをバランスよく満足させることが重要”

情報セキュリティ

1） 安全性を提供するサービス

2） セキュリティに対する攻撃

3） 安全性を提供するメカニズム

脅威の分類

- 人為的かつ意図的な脅威
  不正アクセスに代表される侵入や攻撃（ by クラッカー）
- 人為的かつ非意図的な脅威
  操作ミスや不注意による脅威（ヒューマンエラー）
- 非人為的かつ非意図的な脅威
  ハードウェアの故障や障害等の事故
  火災や地震などの災害による脅威

人為的かつ意図的な脅威例(攻撃手法)

不正アクセス(侵入者)

盗聴

サービスの妨害
(情報漏洩・転売)

マルウェア
(ボット，ウィルス，スパイウェア)

セキュリティ被害例

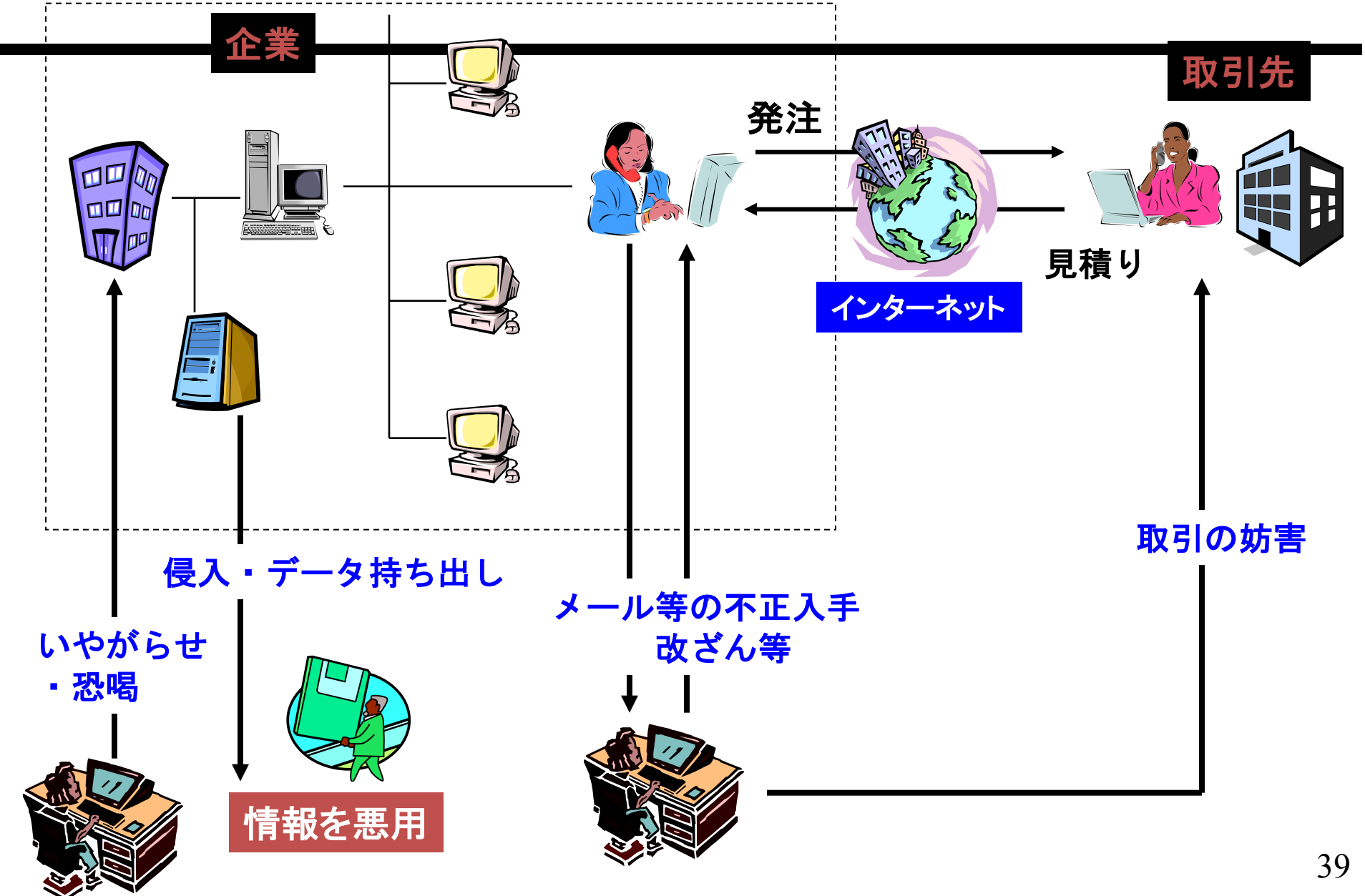
不正アクセス： 印刷・出版業者において，セキュリティ対策の弱い子会社から本社の社内ネットワークに侵入され，商談情報，議事録などのデータや，画像処理のソフトなどが流出。

盗難： 人材派遣会社において，登録されている数万人分のデータが流出。派遣会社のシステムプログラマーがパソコンにてデータを持ち出した。

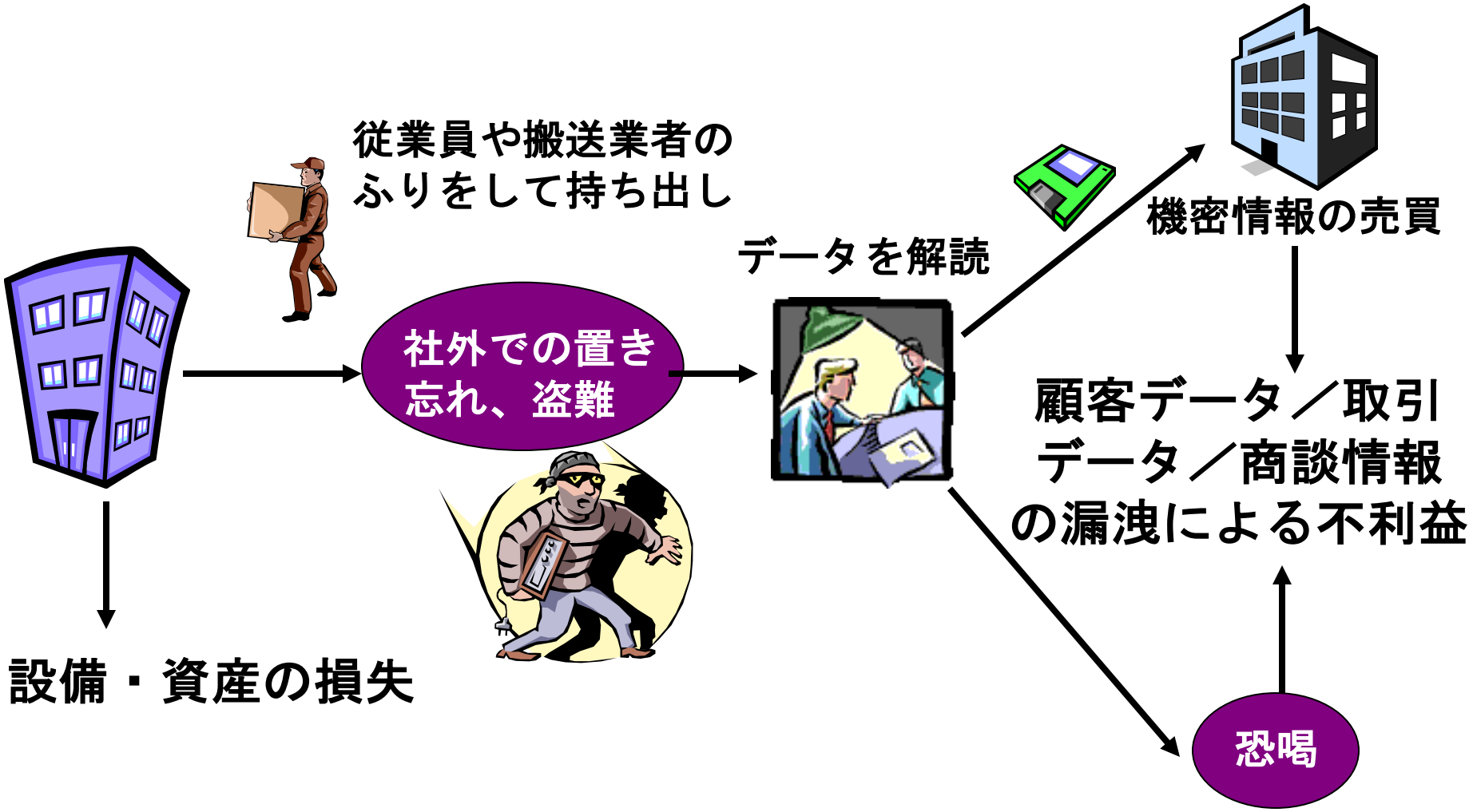
情報漏洩・転売： 既に退職した幹部社員が在籍時に使用していたID/パスワードで社内に侵入。社員情報をリサーチ会社に漏洩し，利益を得ていた。

ウィルス： 国内某メーカーにおいて2000通ものウィルスが届き，ローカルマシンやサーバのファイルが多数破壊された。

不正侵入によるデータ漏洩・改ざん



パソコンの盗難による被害



なりすましによるパソコンの不正使用

利用者本人

①会議・出張等
による離席

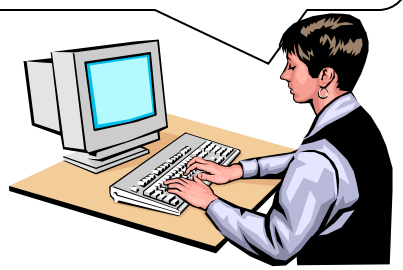
誰にでも利用
できる状態

③混乱

この決済は何？

あれ？受注日が今ごろ
変更？

混乱



混乱

業務に関係ないサービス
の利用が多いな。

権限のない利用者

②なりすまし
ID/パスワードの
不正入手

ウィルスの定義

『第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり,次の機能を1つ以上有するもの』

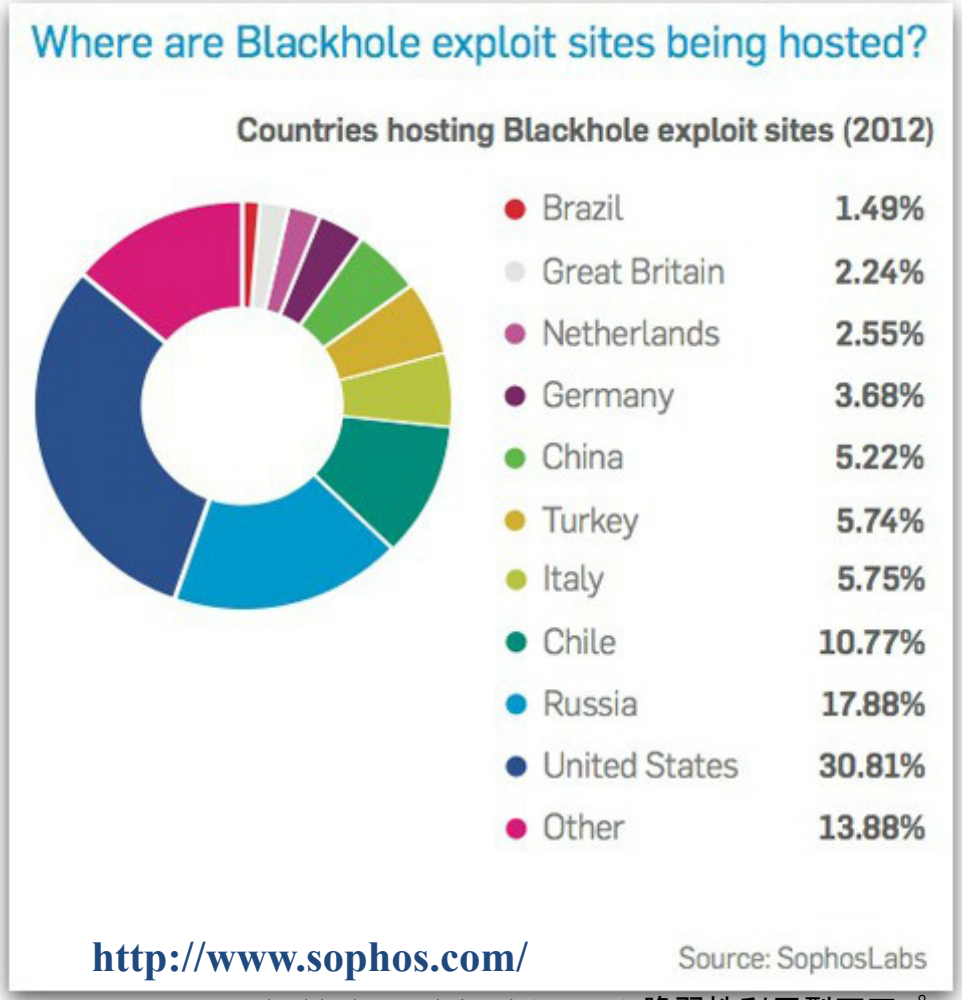
（経済産業省告示「コンピュータウィルス対策基準」より）

1）**自己伝染機能**：　自らの機能によって他のプログラムに自らをコピーし又は，システム機能を利用して自らを他のシステムにコピーすることにより，他のシステムに伝染する機能

2）**潜伏機能**：　発病するための特定時刻，一定時間，処理回数等の条件を記憶させて，条件が満たされるまで症状を出さない機能

3）**発病機能**：　プログラムやデータ等のファイルの破壊を行ったり，コンピュータに異常な動作をさせる等の機能

攻撃の分析例



Blackhole Exploit Kit(BHEK):脆弱性利用型不正プログラムの一種,
Javaのゼロディ脆弱性騒動（2013年1月）

Cyber Threat Real-time Map (Kaspersky)
https://vimeo.com/88976652

情報セキュリティ

１） 安全性を提供するサービス

２） セキュリティに対する攻撃

３） 安全性を提供するメカニズム

安全性を提供するメカニズム

安全性への攻撃を発見したり、守ったり、その攻撃から回復するために設計されたメカニズム

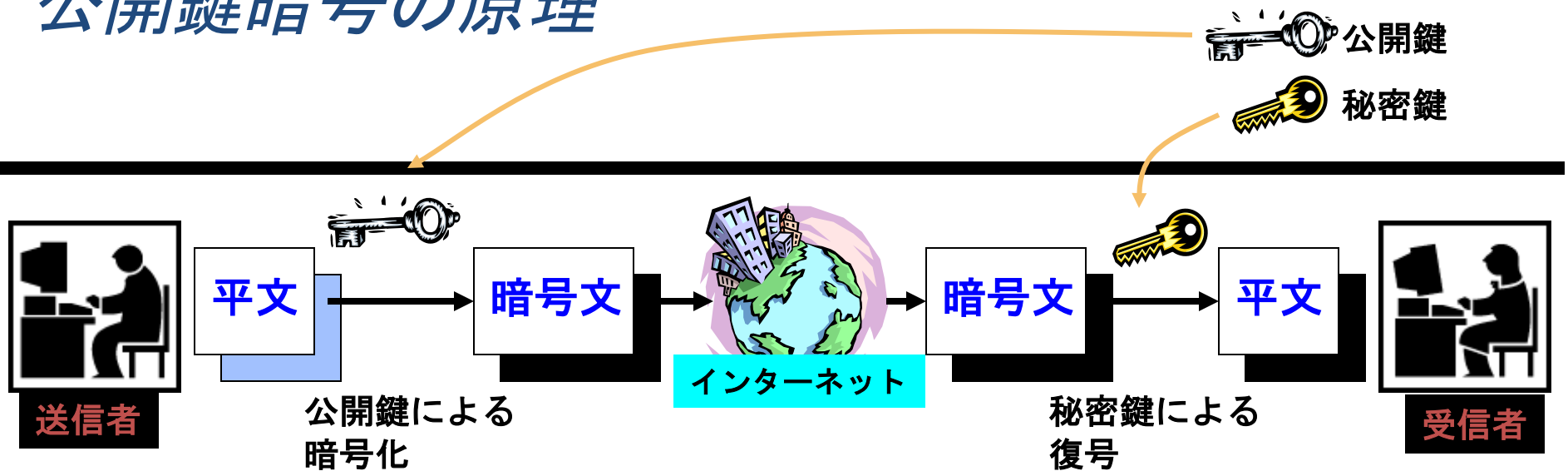
利用されているほとんどの安全上のメカニズムの基礎となる要素：　暗号化技術

暗号化や暗号化のような形での情報の変形は、安全性を提供するもっとも一般的な方法である。

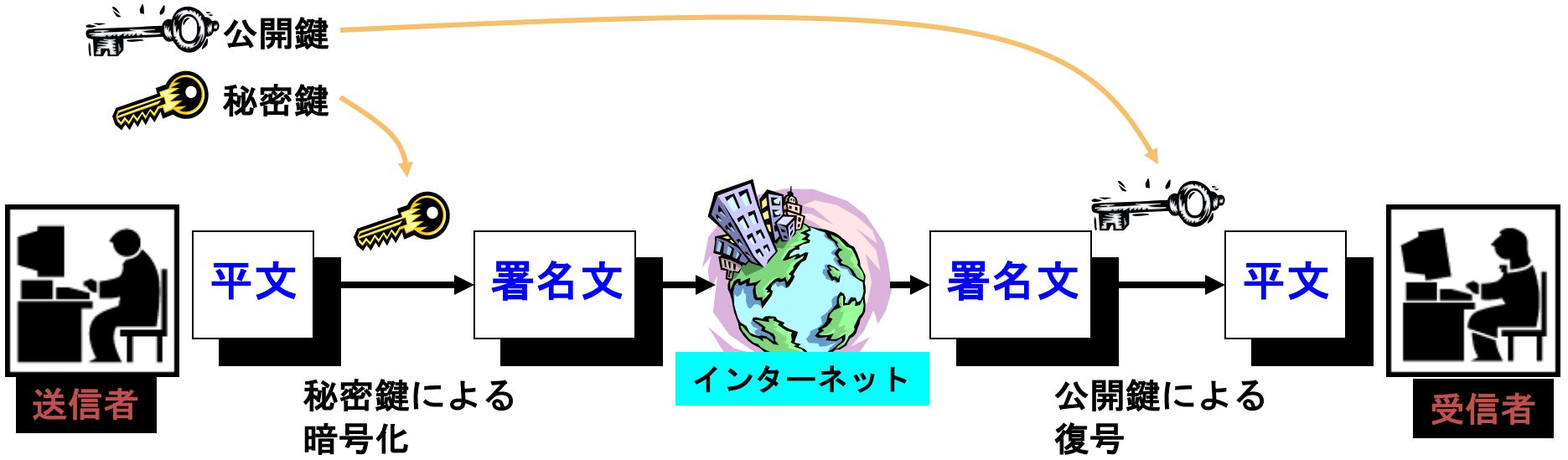
⇩

暗号技術の開発、利用、管理

公開鍵暗号の原理



a. 暗号化処理概要



b. 電子署名処理概要

セキュリティ対策の分類

- 技術面での対策
  - 防御

    認証、アクセス制御、暗号、電子署名
  - 予防・検知

    不正侵入監視、ウィルス監視、コンテンツ監視
- 運用・管理面での対策
  - セキュリティポリシー

不正侵入監視　－侵入の検知

・統計的な異常検知：　通常あるいは予想される振る舞いを定義

1)閾値に基づく検出

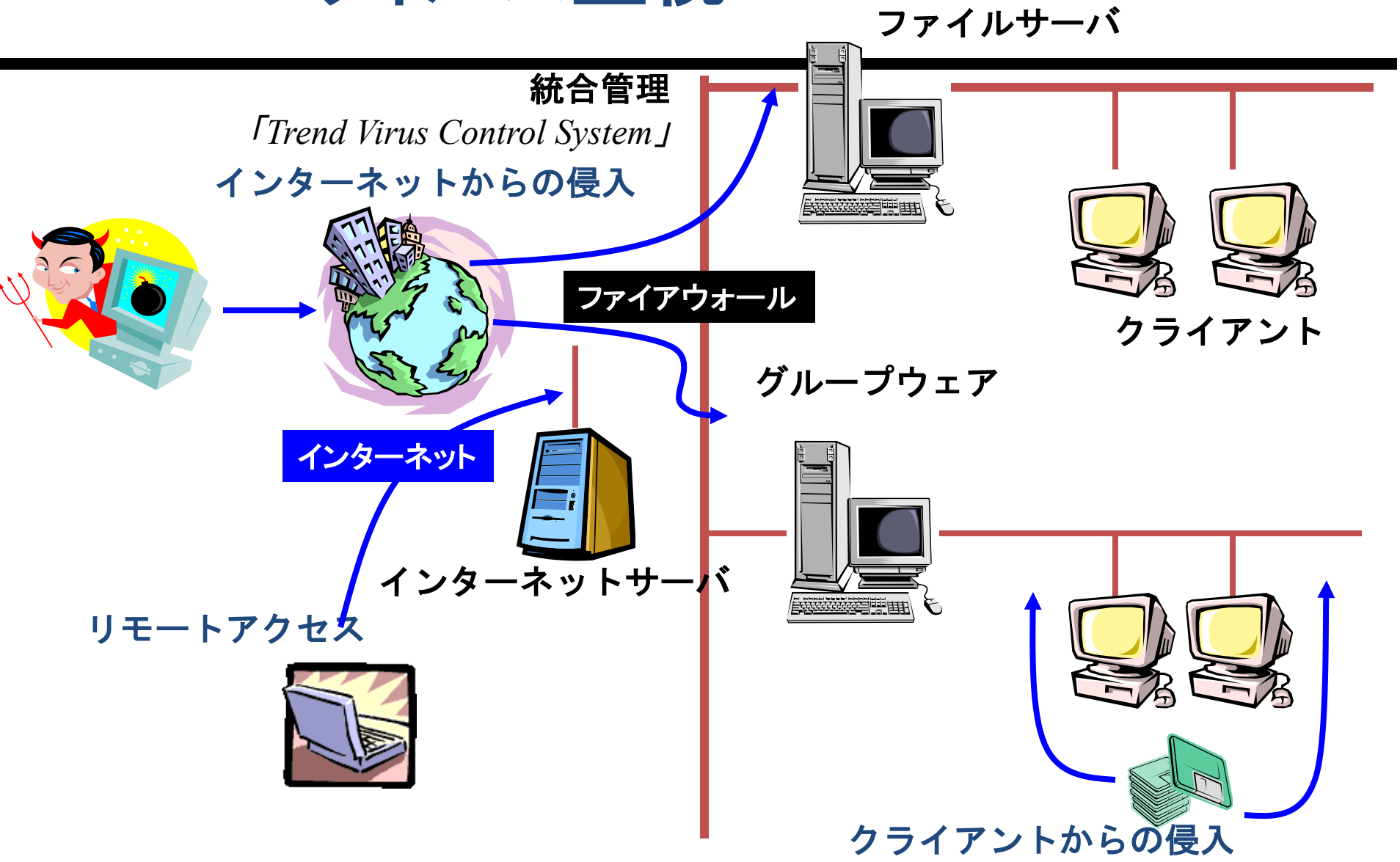
2)行動記録に基づく検出

・ルールに基づく検出：　ある振る舞いを侵入行為とみなす基準、適切な行動を定義

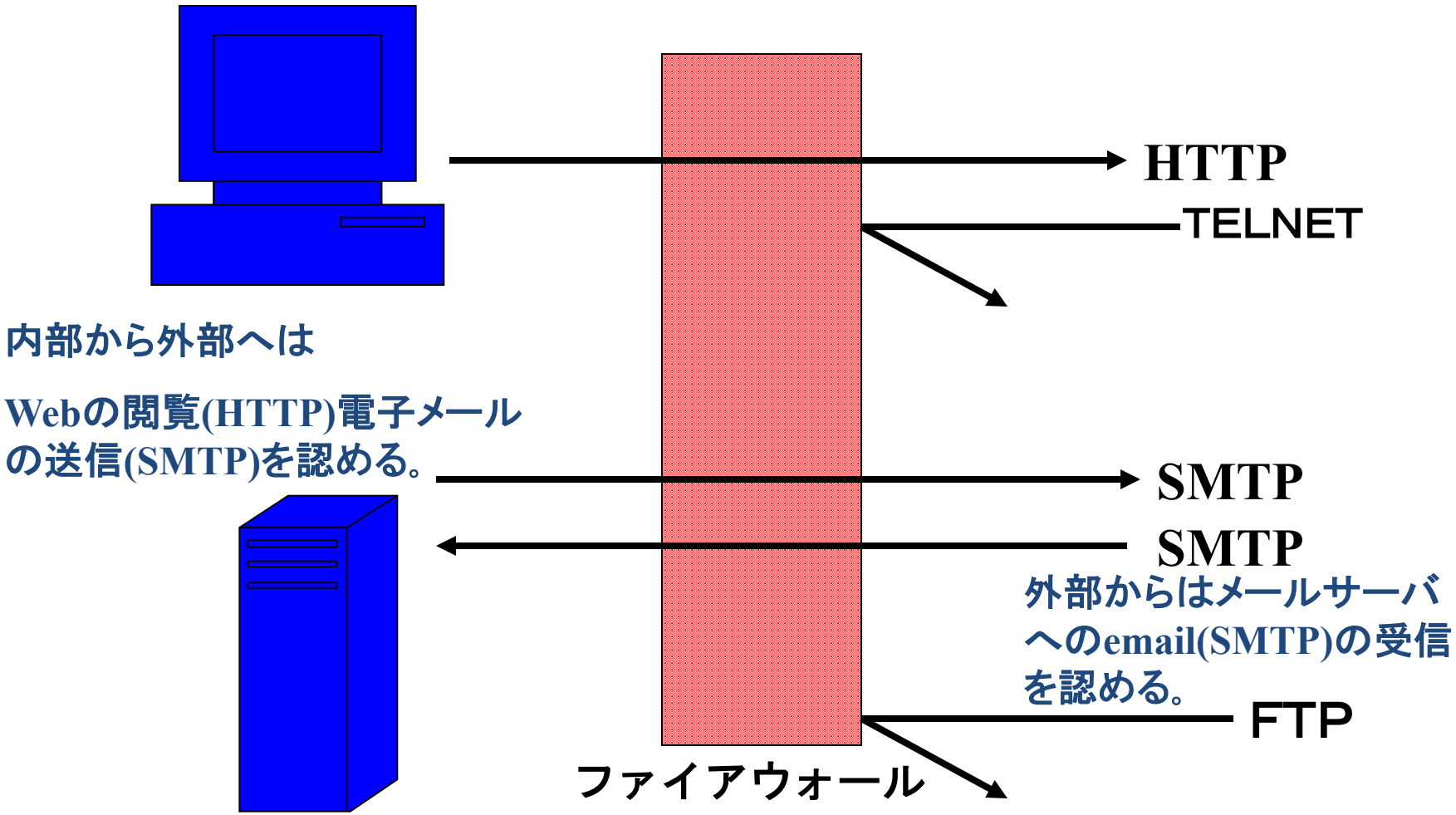
1)異常検出

2)侵入の識別

ウィルス監視


ファイルサーバ
統合管理
「Trend Virus Control System」
インターネットからの侵入
ファイアウォール
クライアント
グループウェア
インターネット
インターネットサーバ
リモートアクセス
クライアントからの侵入

ファイアウォールによるアクセス制御



セキュリティ対策の分類

・技術面での対策

ー防御

認証、アクセス制御、暗号、電子署名

ー予防・検知

不正侵入監視、ウィルス監視、コンテンツ監視

・運用・管理面での対策

ーセキュリティポリシー

セキュリティポリシーとは

企業（経営者）のセキュリティに対する考え方，及びセキュリティ対策を実施するための基本方針や，運用ルール等をドキュメント化したもの。

情報セキュリティ基本規程：
セキュリティポリシーの企業の中での位置付けや強制力（罰則），推進部門や企業理念との関係等の大枠を定めたもの。

情報セキュリティ共通基準：
利用者が具体的に何をすべきかを考える際のベースラインとなるもの。

セキュリティ対策のポイント

1　利用者の確認（本人確認の対策）

2　情報漏洩対策

3　盗難対策

4　ウィルス対策

5　運用体制（利用者意識の向上）

情　報　倫　理

１　他者の生命、安全、財産を侵害しない。

２　他者の人格とプライバシーを尊重する。

３　他者の知的財産権と知的成果を尊重する。

４　情報システムや通信ネットワークの運用
　　規則を遵守する。

５　社会における文化の多様性に配慮する。

（情報処理学会倫理綱領）

情報リテラシー教育
（2003年度から高校の授業で）

A　情報活用の実践力
自分で情報機器やシステムを操作し、情報の発信や利用などができるようにするための利用技術の習得

B　情報の科学的な理解
情報活用の基礎となる情報手段の特性の理解と情報を適切に扱い、自らの情報活用を評価・改善するための基礎的な理論や方法の理解を目的とする。

C　情報社会に参画する態度
情報化社会の構造や状況がどのようになっているのか、情報に関する自分の生活がどのような情報の環境になっているかを正しく理解し、認識すること。

情報セキュリティの基本原理・基本的考え方

情報倫理

情報関連法律・制度
セキュリティ・ポリシー

セキュリティ技術

暗号理論

・情報セキュリティに関する教育啓発

・セキュリティ管理の能力を持つ人材

・条約や標準化など国際的な調整

a Culture of Security

演習問題

（1） 情報セキュリティに関して、これまでに
経験したこと、あるいは、関心のあった
こと、について述べよ。

（2）「ネットワークセキュリティ」で何を学び
たいか。特に、興味のある事柄は何か。

締め切り 10/10(火) 15:00

休講

- **10/4 休講**